DISSERTATION

Security Aspects of Quantum Cryptographic Protocols in Multi-Qubit Systems

ausgeführt zum Zwecke der Erlangung des akademischen Grades eines Doktors der technischen Wissenschaften unter der Leitung von

Univ.-Doz. Dipl.-Ing. Dr. Martin Suda

E141
Atominstitut der Österreichischen Universitäten

eingereicht an der Technischen Universität Wien
Fakultät für Physik

von

Dipl.-Ing. Stefan Schauer

Matrikelnummer: 9960230
Heimgasse 6, 9131 Grafenstein

Wien, am 16. Mai 2011

Abstract

In the last years extensive research in the field of quantum cryptography and in particular in quantum key distribution (QKD) has been done. Most of the QKD protocols studied and implemented today are based on the idea presented in a pioneering work by Bennett and Brassard in 1984, the BB84 protocol. But there are other protocols based on the phenomenon of entanglement, e.g. the first protocol was suggested by Ekert in 1991. Further, protocols going beyond key distribution, for example protocols realizing authentication or secret sharing using quantum mechanics, make heavy use of entanglement in multi-qubit systems.

The main goal of the thesis is to provide a deeper insight into the security of protocols based on entanglement in multi-qubit systems and to give a connection to the security thresholds of the BB84 and equivalent protocols.

In this thesis we focus on protocols based on entanglement in multi-qubit systems. Starting from an attack strategy we developed where an adversary entangles herself with the legitimate parties the security of such protocols using multi-qubit systems is analyzed in detail. The security analysis is based on the violation of the correlations given by entanglement swapping and we could show that for some protocols the adversary is able to obtain full information about the key. Further, we discuss the effect of noise in connection with entanglement swapping. Based on the detailed security analysis thresholds for the fidelity of the initial states are defined. In detail, we show that for a fidelity of the initial entangled states greater than 94.28% a natural error rate of at most 11% is introduced, which is the maximal tolerable error rate for the BB84 and equivalent protocols. Furthermore, we relate this fidelity to the length of the quantum channel and find 1.19 km as the maximum length for secure communication. Using different models of quantum channel we obtain a maximum length of up to 5.98 km. To enlarge these distances entanglement purification protocols are of great interest and their effect on the attack strategy we developed is investigated.

Zusammenfassung

In den letzten Jahren wurden auf dem Gebiet der Quantenkryptographie, speziell der Quantum Key Distribution (QKD) große Fortschritte in der Forschung gemacht. Viele der QKD Protokolle, die heutzutage studiert und implementiert werden, basieren auf einer Idee von Bennett und Brassard aus dem Jahr 1984, dem BB84 Protokoll. Andere Protokolle hingegen, wie das von Artur Ekert aus dem Jahr 1991, verwenden das Phänomen des Entanglement. Vor allem Protokolle, die über die bloße Verteilung von Schlüsseln hinausgehen, basieren auf Entanglement in Multi-Qubit Systemen. Dazu gehören etwa Protokolle zur Authentifizierung oder zum Secret Sharing.

Das vornehmliche Ziel dieser Arbeit ist es, einen tieferen Einblick in die Sicherheit von Protokollen basierend auf Entanglement in Multi-Qubit Systemen zu geben und eine Verbindung zu den Sicherheitsparametern des BB84 und ähnlichen Protokollen herzustellen.

In dieser Dissertation gehen wir auf eben diese Protokolle, die Entanglement in Multi-Qubit Systemen einsetzen, ein. Ausgehend von einem Angriffsszenario, das von uns entwickelt wurde und bei dem sich der Angreifer mit den Parteien verschränkt, wird die Sicherheit von Protokollen gegenüber dieser Attacke betrachtet. Die Sicherheit in diesen Protokollen basiert auf den Korrelationen gegeben durch das Entanglement Swapping und wir konnten zeigen, dass für einige Protokolle ein Angreifer volle Information über den Schlüssel erhält. Im Zuge der Sicherheitsanalyse werden auch die Auswirkungen von natürlichen Störungen auf die Korrelationen des Entanglement Swapping untersucht. Durch die Erkenntnisse aus diesen Sicherheitsanalysen ergeben sich Schwellwerte für die Fidelity der Initialsysteme. Im Einzelnen ergibt sich bei einer Fidelity von nicht mehr als 94.28% ein natürlicher Fehler von weniger als 11%, was die maximale Fehlerrate beim BB84 und ähnlichen Protokollen darstellt. Darüber hinaus bringen wir die Fidelity mit der Länge des Kanals in Zusammenhang und erhalten, basierend auf unterschiedlichen Modellen, eine Länge von 1.19 km bis hin zu 5.98 km als die maximale Distanz, um sichere Kommunikation zu garantieren. Um diese Distanzen zu überschreiten sind Entanglement Purification Protokolle von großem Interesse und werden in Hinsicht auf ihre Auswirkungen auf die von uns entwickelte Attacke untersucht.

Declaration

I declare that the thesis hereby submitted for the Technical Doctor degree at the Technical University of Vienna is my own work and has not been previously submitted at another university for any degree. Wherever contributions of others are involved, every effort is made to indicate this clearly, with due reference to the literature, and acknowledgement of collaborative research and discussions.

Stefan Schauer
16. Mai 2011

Acknowledgement

First of all I would like to give a special thanks to my supervisor, Martin Suda, for giving me advice and support during the research for my thesis. He was always open for discussions on any topic and brought interesting questions to my attention. If it wasn't for him, I would have struggled with several problems more than I already did and surely lost focus some time in the last years.

Further, I want to thank the AIT – Austrian Institute of Technology GmbH for giving me the opportunity to write this thesis and for funding my research. In person I want to thank Wolfgang Knoll and Elvira Welzig, who raised the funding for my last year. Additionally, I want to thank my colleagues at Klagenfurt, Christian Kollmitzer, Oliver Maurhart and Katharina Lessiak, as well as my colleagues at Vienna, Momtchil Peev, Christoph Pacher and Stefano Bettelli, for insightful discussions and extensive explanations.

Furthermore, I would like to thank Beatrix Hiesmayr and the Quantum Particle group at the University of Vienna for the great and very interesting collaboration and numerous Wednesday-lunch-discussions. Among the people from the Quantum Particle Group I want to especially thank Marcus Huber and Andreas Gabriel for quite revealing dialogs about various topics.

List of Publications

S. Schauer, M. Huber, B. Hiesmayr
"Experimentally feasible security check for n-qubit quantum secret sharing"
Physical Review A, 82 (2010), 6; 062311

S. Schauer
"Attack Strategies on QKD Protocols"
Lecture Notes in Physics, 797 (2010); 71 – 95

K. Lessiak, C. Kollmitzer, S. Schauer, S. Rass, J. Pilz
"Statistical Analysis of QKD Networks in Real-life Environments"
The Third International Conference on Quantum, Nano and Micro Technologies, Cancun, Mexico; 01.02.2009 - 07.02.2009
in: "ICQNM 2009", IARIA, IARIA (2009), ISSN: 1942-2636

C. Kollmitzer, O. Maurhart, S. Schauer, S. Rass
"Application Framework for High Security Requirements in R&D Environments Based on Quantum Cryptography"
Third International Conference on Risks and Security of Internet and Systems, Tozeur, Tunisia; 28.10.2008 - 30.10.2008
in: "CRiSIS'2008", (2008)

S. Schauer, M. Suda:
"A Novel Attack Strategy on Entanglement Swapping QKD Protocols"
International Journal of Quantum Information, 6 (2008), 4; 841 – 858

Contents

List of Abbreviations

BB84	first QKD protocol published by C. Bennett and G. Brassard in 1984
BSM	Bell-state measurement, a way to distinguish between all four Bell states
CCNR	computable cross norm or realignment criterion, used in connection with separability of quantum states
CHSH	reference to J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt in connection with inequalities to test for non-local behavior
CNOT	controlled NOT, a quantum operation performing a conditional bit flip
EPR	reference to A. Einstein, B. Podolski and N. Rosen in connection with entangled 2-qubit states and the famous gedankenexperiment
GHZ	reference to D. Greenberger, M. A. Horne and A. Zeilinger in connection with multipartite entanglement
HBB	quantum secret sharing protocol published by M. Hillery, V. Buzek and A. Berthiaume
I&R	intercept and resend, a basic attack strategy on QKD protocols
KKI	quantum secret sharing protocol published by A. Karlsson, M. Koashi and N. Imoto
LOCC	local operations and classical communication
PKI	public key infrastructure

PNS	photon number splitting, an attack strategy on QKD protocols
PPT	positive partial transpose, used in connection with the criterion of Peres and Horodecki for separability of quantum states
QBER	quantum bit error rate, the amount of noise introduced by physical limitations
QKD	quantum key distribution, distributing classical key using quantum channels
QPA	quantum privacy amplification, an entanglement purification scheme
QSS	quantum secret sharing, sharing classical secrets using quantum channels
QSTS	quantum state sharing, sharing quantum secrets
RSA	algorithm for public key cryptography by R. L. Rivest, A. Shamir and L. Adleman
SFG	sum frequency generation, a non-linear operation where two photons are transformed into one photon
ZLG	an attack strategy published by Y.-S. Zhang, C.-F. Li and G.-C. Guo

List of Symbols

$\|\Phi^{\pm}\rangle, \|\Psi^{\pm}\rangle$	Bell states
$\|\omega^{\pm}\rangle, \|\chi^{\pm}\rangle$	Bell states after a Hadamard transformation
$\|P_{ij}^{\pm}\rangle$	GHZ states
$\|\delta\rangle$	initial state of the simulation attack
$\|x\pm\rangle$	basis states of the X-basis
$\|y\pm\rangle$	basis states of the Y-basis
$\|z\pm\rangle$	basis states of the Z-basis
$\sigma_x, \sigma_y, \sigma_z$	Pauli operations
$\tau_{ABC}(\rho)$	tangle of a 3-qubit state ρ
$C(\rho)$	concurrence of a 2-qubit state ρ
$C^2_{(m)}(\rho)$	m-flip concurrence
$D(\rho)$	yield of a purification protocol
$E_B(\rho)$	distance measure based on the Bures metric of a state ρ
$E_C(\rho)$	entanglement cost of a state ρ
$E_D(\rho)$	entanglement of distillation of a state ρ
$E_E(\rho)$	entropy of entanglement of a state ρ
$E_F(\rho)$	entanglement of formation of a state ρ
$E_{\mathcal{N}}(\rho)$	logarithmic negativity of a state ρ

$E_R(\rho)$	relative entropy of entanglement of a state ρ
F	fidelity of a quantum state
F_0	fidelity above which secure communication is possible
F_{EC}	fidelity above which error correction is possible
F_{seg}	fidelity of a quantum state over one segment of nested purification
F_{swap}	fidelity of a quantum state after entanglement swapping
H	Hadamard transformation
$H(S\|M)$	conditional Shannon entropy of S given M
I_{AE}	information gain of E
l_c	coherence length of a quantum channel
$p(s\|m)$	conditional probability of s given m
p_0	error probability for secure communication ($\simeq 11\%$)
p_{EC}	error probability for error correction ($\simeq 15\%$)
$P_c(m)$	collision probability of m
P_{corr}	probability to obtain correlated results from a measurement
$P_e(m)$	error probability of m
P_{err}	probability not to obtain correlated results from a measurement
$\langle P_c \rangle$	expected collision probability
$\langle P_e \rangle$	expected error probability
$R_i(\theta)$	rotation of an angle θ about the i-axis
$R(S\|M)$	conditional Renyi entropy of S given M
$T_i(\theta)$	transformation into the i-basis using an angle θ
$S(\rho)$	von Neuman entropy
U	twirl operation

List of Figures

Chapter 1

Introduction

Quantum Cryptography

Quantum cryptography is an interdisciplinary field of quantum mechanics, classical cryptography and information theory. It mainly addresses a central problem from classical cryptography, the confidential distribution of secrets, i.e. keys, between two or more parties. To achieve that quantum cryptography uses laws and phenomena of quantum physics to provide unconditional secure communication between these parties. This separates it from classical methods like public key cryptosystems [43, 123], which depend on computational assumptions.

The most studied part of quantum cryptography is quantum key distribution (QKD) [57, 48, 126, 94, 22]. With QKD it is possible to generate a classical key based on quantum mechanical phenomena between two parties which initially do not need to share a common secret but only need an authenticated channel. In classical cryptography a public key infrastructure (PKI) based on the RSA [123] or Diffie-Hellman algorithm [43] serves a similar purpose because anyone who is able to obtain the public key of some other person can send a secret message to this person. That means by distinguishing between a public and a private key the two communication parties do not have to share a common secret. The major problem of this scheme is that its security is based on computational assumptions. Today there is no efficient way to extract the private key from the public key but if an sophisticated algorithm or some new technology like the quantum computer [41] is realized these schemes become totally insecure [137]. On the other hand, QKD provides unconditional security and an adversary will have no better chance than

guessing the key whatever technology or computational power the adversary has.

The first QKD protocol was presented by Bennett and Brassard in 1984 [8]. They used the polarization of photons to represent information and showed that any attempt by an adversary to eavesdrop this information will be detected by the two parties with arbitrarily high probability. This argument and consequently the security is based on two major laws of quantum mechanics, i.e. the fact that an unknown quantum state can not be copied perfectly (which is also called the no cloning theorem [166]) and the fact that the observation of a quantum system alters its state.

Based upon the results of Bennett and Brassard several other protocols using similar ideas have been published [5, 24, 82, 125]. These protocols have been studied intensively and various proofs of their security have been published [7, 81, 96, 97, 135]. In these proofs it has been shown that the protocols are secure against individual and coherent attacks as long as the error rate is below a certain threshold value.

In 1991 a QKD protocol based on a different technology, i.e. the phenomenon of entanglement, has been proposed by Ekert [51]. Two entangled particles have the property that if one of them is measured the other one immediately collapses into a correlated state regardless of the distance between them. This phenomenon has first been stated by Einstein, Podolsky and Rosen in their famous gedankenexperiment [50]. In this way two communication parties, each in possession of one particle of an entangled state, are able to create a secret key. The security of this type of QKD protocols is based on the inequalities stated by Bell [2], who proposed an experiment to test the conjecture of Einstein et al., and their extended version published by Clauser at al. [33]. A violation of these inequalities indicates a non-local behavior as stated by quantum mechanics (cf. section 2.3). Although several kinds of particles can be entangled we focus in this thesis only on photons since they are the most commonly used carrier of information in QKD protocols.

A major practical problem of QKD protocols is the distance between the two communication parties. Photon sources and detectors are not perfect and introduce further errors into the protocol. The quantum channels over which most QKD protocols are performed are common optical fibers at telecom wavelength or free-space links. Due to the attenuation of optical fibers and atmospheric influences in free space links as well as the polarization mode and chromatic dispersion the visibility of the photons is lowered and their state is altered permanently. Hence,

the information can not be recovered after the photons traveled a certain distance.

Relation to Current Research

The continuous improvement of the physical apparatus – photon sources as well as quantum channels – in the last years made it possible to enlarge the distance over which QKD is feasible from 23 km in the first experiments outside the laboratory up to over 200 km for optical fibers (cf. [106, 140, 58, 143]). Regarding free-space communication, an experiment over 144 km has been realized in 2007 [150]. Unfortunately, the secret key rate is too low for a reasonable communication at such large distances [143, 150]. Nevertheless, at distances of about 20 - 25 km high rates can be achieved [118]. A first experiment to shown that QKD is of practical use was performed in 2004, when a bank transfer in Vienna has been encrypted using a key generated by QKD [117].

One possibility to overcome the distance problem is to use quantum networks. Like in classical networks there are various nodes connected by several quantum channels. The classical information is decoded at every node and passed on to the next node. In the course of the research of quantum networks the SECOQC project has been started in the sixth framework program of the European Union [112]. The goal of this project was to determine whether a global network for secure communication based on quantum cryptography is possible and thus to give a hint how to solve the distance problem in QKD. In October 2008 a prototype of such a network was presented in Vienna to show how quantum cryptography can be employed efficiently to secure today's communication [118, 112].

A second solution for the distance problem are quantum repeaters. Unlike classical repeaters which are able to read and copy the necessary information quantum repeaters have to follow a different concept – entanglement swapping [172, 20, 110, 21] – due to the laws given by quantum physics. Entanglement swapping is a special case of quantum teleportation [10, 12, 85] where two particles become entangled although they never interacted in the past. Schemes for quantum repeaters have been presented, for example, by Duan et al. [44] and by Dür et al. [45]. The latter is of particular interest because it combines entanglement swapping and entanglement purification [12, 14, 42] to achieve efficient quantum repeaters over long distances. In 2008, an actual implementation [168] of such a scheme has shown that a realization

of quantum repeaters is feasible with today's technology.

Besides the problem of key distribution, there are a lot of other primitives (e.g. secret sharing or multiparty communication) in the field of classical cryptography which can also be formalized in quantum terms. Some of the classical protocols like Shamir's secret sharing scheme [133] already provide unconditional security and therefore a quantum version of secret sharing is not that big of an interest. Further, it is often stressed that classical cryptography can be done as long as the keys are distributed using QKD protocols. Nevertheless, it is interesting to look at quantum protocols for sharing classical secrets from a theoretical point of view. Furthermore, to share quantum secrets between several parties the quantum version of secret sharing is necessary.

For multi-qubit protocols the technology used for BB84-like protocols is often not enough. Many of these protocols make extensive use of entanglement as a resource and entanglement swapping as a method to transport the information between the involved parties. Nevertheless, the major problem of entanglement based protocols is the implementation due to today's physical limitations. For example, the creation of entangled pairs at a high rate is rather sophisticated but has improved over the last years. Moreover, the physical implementation of entanglement swapping is even more challenging since it is based on complete Bell state measurements (BSM). Due to this high complexity none of the multi-qubit protocols discussed in this thesis have been physically implemented yet. But the first steps towards an implementation have been made, for example, by Pan et al., who presented four-photon entanglement and a corresponding teleportation scheme [111].

Hypothesis

In this thesis we are going to focus on quantum cryptographic protocols for quantum key distribution and quantum secret sharing based on multiple Bell pairs and multi-qubit states, eg. GHZ states [60]. Such protocols use entanglement swapping and the respective correlated measurement results to establish a secure classical communication. Since particles have to be in transit to share the entanglement between the legitimate parties, they can be intercepted by an adversary. In principle, the adversary is able to perform any quantum operation on the intercepted particles to gain some knowledge about the key. Our main question is how much information

the adversary is able to obtain about the key from the intercepted particles without being detected?

It has already been shown by Zhang, Li and Guo [170] that an adversary is able to obtain full information about the secret key in a specific scenario [27]. Since this attack strategy by Zhang, Li and Guo (in the following called ZLG attack) is just defined for one other QKD protocol by Cabello [26] it is not a good candidate for a generalized approach. Furthermore, these two protocols can also be secured against the ZLG attack [28, 90]. We define an attack strategy based on the same concept but providing a more general approach. The main idea of our attack strategy is to simulate and furthermore to preserve the correlations between the legitimate parties which provide the basis for the security of protocols using on entanglement swapping. Further, we show that our attack strategy is not only an generalization of the ZLG attack, i.e. it gives the same results when applied on the protocols described in [27, 26], but a more powerful extension since it provides an adversary with more information when applied on [90]. Additionally, our attack strategy is applicable on a whole family of QKD protocols.

A crucial point which has not been addressed in most of the protocols is that entanglement swapping uses, in theory, perfectly entangled states which is not possible per se due to noise in optical fibers. Therefore, we analyze how the results of entanglement swapping change in a system where non-maximally entangled states are used. A damage of the correlation to a certain amount allows an adversary great latitude in the choice of his attack strategies. As a result an adversary might stay undetected where he would not if the entanglement was pure. While discussing entanglement swapping with mixed states we are going to define the amount of natural error tolerable in QKD protocols. Here we are giving threshold values for the fidelity of the initial states for some specific protocols. Additionally, we analyze the decrease of the fidelity over distance and its implications on the security.

To overcome the transmission losses entanglement purification protocols are used [6, 12, 14, 42]. Such protocols take several impure entangled states as input and produce one entangled pair with a higher amount of entanglement. Based on the thresholds values on the initial entangled states we analyze the overhead necessary to guarantee security in cryptographic protocols, i.e. how many entangled states are necessary to successfully use entanglement swapping.

Outline of the Thesis

In the following chapter we are going into detail on the definition of entanglement. We also describe the basic phenomena which are applied in the protocols later on. In chapter 3 we give a short overview on entanglement measures for 2-qubit and multi-qubit systems to characterize the entanglement between two or several qubits. Chapter 4 deals with different models of noisy quantum channels and how the entanglement is affected if qubits of an entangled state are transmitted over a noisy channel. In this context some basic entanglement purification procedures are discussed.

Chapter 5 gives a basic introduction into quantum cryptography and the ideas behind it. The most relevant QKD and QSS protocols are described and we also give a short overview on physical implementations. In chapter 6 we discuss the security of the protocols described in chapter 5. We present decision trees as a basic method to calculate Eve's information about the sifted key and provide detailed security considerations for the basic protocols.

The simulation attack strategy is characterized in detail in chapter 7 together with the concept of the ZLG attack. There we present our main idea of simulating the correlations between Alice's and Bob's measurement results as well as simulating rotations and basis transformations. Chapter 8 deals in detail with the application of the simulation attack onto several protocols. There we show how much information an adversary is able to obtain from the simulation attack. We also provide strategies to secure quantum cryptographic protocols against the simulation attack.

In chapter 9 we bring the protocols from chapter 8 into a noisy environment and look at the natural error rate for these protocols. Further, we relate the fidelity to the respective length of the quantum channel and we analyze how the noisy environment affects the adversary's attack strategy and information. In the end we give a short overview on the most important results and refer to open questions arising from these results.

Chapter 2

Entanglement

One of the most significant quantum effects is *entanglement*, which has first been described in 1935 by Schrödinger [130] and has been heavily discussed by Einstein, Podolsky and Rosen [50]. Einstein called it a "*spooky action at a distance*" since entanglement describes effects on two particles which seem to violate the basic concepts of realism and locality (cf. section 2.3 for further details on the EPR gedankenexperiment). Although Einstein used the concept of entanglement to proof that quantum mechanics is not a complete theory, it has later been shown by Bell [2] that entangled states exist. Since then a large number of experiments have been performed in connection with entanglement and several applications have been described (cf. section 2.5 below). Throughout this thesis we focus on entanglement of qubits, i.e. systems with two degrees of freedom, since they are the carrier of information used in the protocols described later on.

2.1 Bipartite Entanglement

2.1.1 Pure State Entanglement

Considering a quantum system consisting of two particles located at distant locations, one in Alice's laboratory and one in Bob's laboratory, one particle can be fully described by an element of a 2-dimensional complex vector space, a so called *Hilbert Space*. Such a state can be written in the Dirac notation as

$$|\varphi\rangle = \alpha|i\rangle + \beta|j\rangle. \tag{2.1}$$

Here, $|i\rangle$ and $|j\rangle$ form a basis of the 2-dimensional Hilbert space $\mathcal{H}$. In general, the *computational basis* is used, where $|i\rangle = |0\rangle$ and $|j\rangle = |1\rangle$, due to its direct connection to the building block of classical information, the bit. Accordingly to the classical version, a single quantum state is called *qubit*. Nevertheless, any other two vectors forming a basis can be used to describe a quantum state. The only restriction is that quantum states have to be of unit length, i.e. $|\alpha|^2 + |\beta|^2 = 1$.

To describe the composite system $|\varphi\rangle_{AB}$ of both Alice's and Bob's particle the formal concept of the tensor product is used to describe this larger Hilbert space $\mathcal{H}_{AB}$

$$\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B \tag{2.2}$$

which is one of the four postulates of quantum mechanics (cf. for example the textbook of Nielsen and Chuang [109] for details on the postulates of quantum mechanics). Such a state $|\varphi\rangle_{AB}$ is called a *product state* or *separable state* if and only if there exist states $|\psi_1\rangle_A \in \mathcal{H}_A$ and $|\psi_2\rangle_B \in \mathcal{H}_B$ such that

$$|\varphi\rangle_{AB} = |\psi_1\rangle_A \otimes |\psi_2\rangle_B, \tag{2.3}$$

i.e. the state can be written as a product of states of the smaller Hilbert spaces.

As it has been pointed out by Einstein et al. and Schrödinger [50, 130], there exist states $|\Phi\rangle_{AB}$ in the combined Hilbert space $\mathcal{H}_{AB}$ that can not be written as presented in eq. (2.3). Such states are called *entangled*. The best known examples for entangled states in the 2-qubit case are the *EPR-* or *Bell-states*. They can be written as (here the $\otimes$ is omitted)

$$\begin{aligned} |\Phi\rangle^{\pm} &= \frac{1}{\sqrt{2}}\big(|0\rangle_A|0\rangle_B \pm |1\rangle_A|1\rangle_B\big) \\ |\Psi\rangle^{\pm} &= \frac{1}{\sqrt{2}}\big(|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B\big). \end{aligned} \tag{2.4}$$

One special property of these states is that they give completely correlated results when qubits A and B are measured separately. From eq. (2.4) we can see that the results coming from a measurement on qubits A and B in the computational basis are either the same or the opposite, depending on the Bell state. The Bell states themselves form an orthonormal basis of the 4-dimensional Hilbert space $\mathcal{H}_{AB}$ and thus can be distinguish by a so called complete *Bell state measurement*, which is heavily used in various protocols described later on (cf. section 2.4 for details on the Bell state measurement).

2.1.2 Mixed State Entanglement

A more complex scenario occurs if Alice and Bob obtain their particles from a source which does not emit a specific state but one of several states. In this case Alice and Bob only know the set of possible states, for example the four Bell states, but not which state is emitted at a specific time. In the most general case Alice and Bob only know that some states $|\psi_i\rangle_{AB} \in \mathcal{H}_{AB}$ are emitted with a certain probability but they are not aware if these are entangled states. The resulting system of Alice and Bob is called a *mixed state* and can be described by an element of the Hilbert-Schmidt space, a so called *density matrix*

$$\rho_{AB} = \sum_i p_i |\psi_i\rangle\langle\psi_i|_{AB} \tag{2.5}$$

where the $p_i \geq 0$ and $\sum p_i = 1$. The density matrix ρ_{AB} is a complex matrix with non-negative eigenvalues and $\mathrm{Tr}(\rho_{AB}) = 1$ because of the fact that all probabilities p_i sum up to 1. As we will see later on, mixed states are also used to describe states that are transmitted over a noisy channel (cf. section 4.1).

Entanglement for the mixed states is defined accordingly to eq. (2.3) such that a state is a product state if it can be written as

$$\rho_{AB} = \delta_A \otimes \delta_B \tag{2.6}$$

with δ_A and δ_B states from the respective smaller Hilbert-Schmidt spaces A and B. Regarding mixed states, separable states are defined similar to the definition above, i.e. as a convex sum of product states

$$\rho_{AB} = \sum_i p_i \big(\delta_A^{(i)} \otimes \delta_B^{(i)}\big). \tag{2.7}$$

At last, a state that is not separable is an entangled state. For the 2-qubit case the terms separable state and product state can be used interchangeably. When we consider higher dimensions or more particles there exist separable states which are no product states.

2.1.3 Separability

As a next step we want to address the problem of how to distinguish between separable and entangled states. To achieve that several *separability criteria* have

been defined which can also be used to detect entanglement. As we will see in the following paragraphs the problem to identify separable states is solved for the 2-qubit case using the PPT criterion. Nevertheless, we want to describe some other criteria as well, which focus on higher dimensions. For further information we want to refer to the book of Bengtsson and Zyczkowski [3] and the extensive overviews by Gühne and Toth [64] and by Horodecki et al. [76] as well as the literature within.

In 1996 Peres and Horodecki et al. presented a separability criterion based on the partial transpose of a density matrix called the *PPT criterion* [114, 70]. The PPT criterion makes use of the partial transpose ρ^{T_B}, i.e. the transpose of the system B of a state ρ, which is defined as

$$\rho^{T_B} = \sum_{ijkl} p_{ijkl} |i\rangle_A \otimes |l\rangle_B \langle k|_A \otimes \langle j|_B. \tag{2.8}$$

for the general matrix of a 2-qubit state $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$

$$\rho = \sum_{ijkl} p_{ijkl} |i\rangle_A \otimes |j\rangle_B \langle k|_A \otimes \langle l|_B \tag{2.9}$$

with $p_{ijkl} \geq 0$ and $\sum p_{ijkl} = 1$. In a block matrix representation this can be written as

$$\rho = \begin{pmatrix} P & Q \\ R & S \end{pmatrix} \qquad \rho^{T_B} = \begin{pmatrix} P^T & Q^T \\ R^T & S^T \end{pmatrix} \tag{2.10}$$

with P, Q, R and S being 2×2 matrices in the 2-qubit case.

The PPT criterion states that if ρ is entangled, then $\rho^{T_B} < 0$ which means that it has at least one negative eigenvalue. In general this criterion is just a necessary but not sufficient condition for separability such that one or more negative eigenvalues of ρ^{T_B} indicate entanglement but non-negative eigenvalues are an inconclusive result. It has been proven that for systems of size $2 \otimes 2$ (qubits) and $2 \otimes 3$ (qutrits) the condition is necessary and sufficient [70]. These properties together with the fact that the PPT criterion is simple to compute makes it very useful for the protocols we are discussing later on.

Since the PPT criterion is not able to find all separable states in higher dimensions or in case of more particles other separability criteria have been developed. One of these is the *CCNR criterion* [30, 124] which detects entanglement in many scenarios where the PPT criterion fails to do so. Nevertheless, the CCNR criterion fails to detect all entangled states in the 2-qubit case, which the PPT criterion does. To

describe this criterion the Schmidt decomposition has to be applied in operator space (a definition of the Schmidt decomposition can be found in several textbooks, for example in [109]). Any density matrix ρ can be written as

$$\rho = \sum_k \lambda_k \big(\gamma_k^{(A)} \otimes \gamma_k^{(B)}\big) \tag{2.11}$$

where $\lambda_k \geq 0$ and γ_k^A and γ_k^B are orthonormal bases of the spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. The CCNR criterion now states that if $\sum \lambda_k \leq 1$ then the state is separable. In other words, a state is entangled if $\sum \lambda_k > 1$.

A necessary and sufficient condition for separability provides the *positive map criterion* presented in [70]. This criterion defines a state ρ as separable, if and only if $\rho' = (\Lambda \otimes \mathbb{1})\rho$ is positive for all positive maps Λ. In contrary to the PPT criterion, this is in general rather hard to use since all positive maps have to be considered. The simple cases are the $2 \otimes 2$ and $2 \otimes 3$ systems where also the PPT criterion is necessary and sufficient as pointed out above. To apply this criterion the positive transpose T_A has to be used, which leads to the *Peres-Horodecki criterion* [114, 70]. Hence, the positive map criterion declares that a state acting on a Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ of dimension $\dim(\mathcal{H}) \leq 6$ is separable if and only if ρ^{T_A} has non-negative eigenvalues. Here, the authors show that all bipartite states can be divided into two classes: the class of PPT states and not-PPT states (NPPT). For the simple case of qubits and qutrits these are exactly the classes of separable states (PPT) and entangled states (NPPT) but for the general case there exist entangled states which fulfill the PPT criterion and thus give the impression that they are separable.

Due to the fact that there are PPT entangled states it is desirable to find a way to detect them. One possibility to achieve that is the *range criterion* presented by Horodecki [74] which states that if ρ is a separable state there exists a set of pure product states $|\psi_i\rangle \otimes |\varphi_i\rangle$ such that they span the range of ρ and the partial transpose $(|\psi_i\rangle \otimes |\varphi_i\rangle)^{T_B}$ span the range of ρ^{T_B}. Using this criterion the first PPT entangled state was found by Horodecki in the $2 \otimes 4$ system. The criterion is also constructive such that it shows how PPT entangled states can be build.

Another necessary but not sufficient condition for separability is stated in the *reduction criterion* [29, 75]. Here, if a state ρ is separable, the reduced states $\rho_A = \mathrm{Tr}_B(\rho)$ and $\rho_B = \mathrm{Tr}_A(\rho)$ satisfy

$$\big(\rho_A \otimes \mathbb{1}\big) - \rho \geq 0 \qquad \text{and} \qquad \big(\mathbb{1} \otimes \rho_B\big) - \rho \geq 0. \tag{2.12}$$

This criterion is closely related to the positive maps criterion but not stronger than the PPT criterion [3]. Nevertheless, it has an important consequence, as shown in [75]: any state ρ that violates the reduction criterion stated in eq. (2.12) is distillable. That means, there exists a protocol based only on local operators and classical communication (in short $LOCC$) such that a maximally entangled state can be generated out of several copies of ρ. In contrary, states that do not violate eq. (2.12) are called *bound entangled*. Examples in the composite Hilbert space with $\dim(\mathcal{H}) \leq 6$ are obvious: PPT states are separable and NPPT states entangled and distillable. In higher dimensions, as already pointed out, there exist PPT entangled states of which all are not distillable [71]. Furthermore, also the NPPT states don't seem to be distillable [46].

2.2 Multipartite Entanglement

2.2.1 Pure States

In the multi-qubit case the structure of entanglement is much deeper than in the 2-qubit case, since entanglement can be found between a larger number of qubits. Moreover, there are several classes of multipartite entanglement which are inequivalent, which means they can not be transformed into each other by local operations and classical communications. In contrary to the bipartite case there are several versions of separability regarding multipartite states. The simplest version are *fully separable states* which have the form

$$|\varphi\rangle_{A_1 \ldots A_n} = |\alpha_1\rangle_{A_1} \otimes |\alpha_2\rangle_{A_2} \otimes \cdots \otimes |\alpha_n\rangle_{A_n} \tag{2.13}$$

for a system of n parties. Further, there are *p-separable states* which are generated by grouping several parties together. For $p = 2$ a so called biseparable state can be written as

$$|\psi\rangle_{A_1|A_2 \ldots A_n} = |\beta_1\rangle_{A_1} \otimes |\beta_2\rangle_{A_2 \ldots A_n}. \tag{2.14}$$

Of course, there are several possibilities for the grouping and p can go up from 2 to n where the n-separable state is the fully separable state from eq. (2.13). Any state the is not fully separable or p-separable is called *genuine entangled*.

There are several classes of genuine entanglement in the multipartite case. When looking at entangled 3-qubit states there are the *GHZ states* and the *W-states*

[60, 47]. The GHZ states have first been studied by Greenberger, Horne and Zeilinger can be described as

$$|P_{ij}^{\pm}\rangle = \frac{1}{\sqrt{2}}\big(|0ij\rangle \pm |1\bar{i}\bar{j}\rangle\big) \tag{2.15}$$

where $i, j \in \{0, 1\}$ and $\bar{i}$ is the complement of i, thus giving 8 different GHZ states for the 3-qubit case. GHZ states are maximally entangled states and a multipartite generalization of the Bell states presented in eq. (2.4). They further have the property that when one of the qubits is measured all other qubits collapse into a state completely determined by the result of the measurement.

The second class of genuine entangled 3 qubit states are the W-states, for example

$$|W_3\rangle = \frac{1}{\sqrt{3}}\big(|001\rangle + |010\rangle + |100\rangle\big). \tag{2.16}$$

The main difference to the GHZ states is that the entanglement in W-states is much more robust against loss of particles and decoherence [63]. If one of the particles is measured or gets lost (i.e. is traced out) the remaining qubits collapse into a Bell state, i.e.

$$\mathrm{Tr}_C\big(|W_3\rangle\langle W_3|_{ABC}\big) = \frac{1}{3}|00\rangle\langle 00|_{AB} + \frac{2}{3}|\Psi^+\rangle\langle\Psi^+|_{AB}. \tag{2.17}$$

When going to higher systems there are even more inequivalent entanglement classes [154] but they are not very well studied yet.

2.2.2 Mixed States

The definition of multipartite mixed entangled states is analogous to the bipartite case using convex sums of the respective states. Accordingly, *fully separable mixed states* consist of a convex sum of fully separable pure states as presented in eq. (2.13), i.e.

$$\rho_{A_1\ldots A_n} = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|_{A_1\ldots A_n}. \tag{2.18}$$

Similarly, *p-separable mixed states* are defined as a convex sum of p-separable pure states. Taking the biseparable state from eq. (2.14) the respective mixed state can be written as

$$\rho_{A_1|A_2\ldots A_n} = \sum_i p_i |\psi_i\rangle\langle\psi_i|_{A_1|A_2\ldots A_n}. \tag{2.19}$$

As already pointed out above there are several possible partitions for separable states. Therefore, a general p-separable mixed state can consist of different partitions of p-separable pure states. Additionally, separate classes for the respective

partitions of p-separable mixed state can be defined which contain only states from one partition [64].

Any mixed state that is not fully separable or p-separable is then called *entangled*. It has already been mentioned that in the multipartite case there exist several inequivalent entanglement classes such that the mixed entangled state can again be divided into classes according to the pure states they consist of. For example, in the 3-qubit case there are 2 inequivalent classes of genuine entangled states, the GHZ states and the W-states. Thus, there are also two classes of entangled mixed states: a state is in the GHZ class if it is described by a convex combination of pure GHZ states and a state is in the W-class if it is described by a convex combination of pure W-states. When going to higher qubit and qudit systems this becomes even more sophisticated. In a recent article Huber et al. described a framework to identify genuinely multipartite entangled mixed quantum states in arbitrary-dimensional systems [79].

2.2.3 Separability

Also in the multipartite case there is the question how to decide whether a state is separable or not. Since there are much more possible combinations of entanglement as compared to the bipartite case it is much more difficult to find separability criteria for multipartite entanglement. We just want to shortly describe one of the criteria since it is directly derived from the PPT criterion for bipartite states. For more information on separability of multipartite states see, for example, the review by Gühne and Toth [64].

The criterion we want to describe is the *permutation criterion*. This is a generalization of the PPT and the CCNR criterion presented in section 2.1.3 above to more than two parties [164, 73, 32]. Let the state ρ be

$$\rho = \sum_{i_1 j_1 \ldots i_N j_N} p_{i_1 j_1 \ldots i_N j_N} |i_1\rangle\langle j_1| \otimes \cdots \otimes |i_N\rangle\langle j_N| \tag{2.20}$$

then the permutation criterion states that ρ is separable if

$$\|p_{\pi(i_1 j_1 \ldots i_N j_N)}\|_1 \leq 1. \tag{2.21}$$

where, $\pi()$ is some permutation of the indices and $\|\rho\|_1 = \mathrm{Tr}(\sqrt{\rho\rho^\dagger})$ is the trace norm. It has been shown in [164, 32] that not all permutations π result in different criteria. For example, in the 2-qubit case there are the PPT and the CCNR

criterion, in the 3-qubit case there are 6 criteria and in the 4-qubit case there are 22 independent permutation criteria. Nevertheless, all these criteria can only rule out fully separable states, i.e. they can not distinguish between p-separable and entangled states.

2.3 EPR Argument and Bell Inequalities

In their article in 1935 [50] Einstein, Podolsky and Rosen tried to show that quantum mechanics could not be a complete theory if such a thing as entanglement should be considered. They pointed out that entanglement would violate the concept of local realism and their argument was based on the following gedankenexperiment: suppose two parties, Alice and Bob, are in possession of a source emitting entangled states of the form

$$|\Phi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\big(|00\rangle_{AB} + |11\rangle_{AB}\big). \tag{2.22}$$

Alice and Bob each take one particle of the state $|\Phi^+\rangle$ and travel in different directions. Then Alice performs a measurement in the computational basis on her particle (c.f picture (1) in figure 2.1) using the operators

$$M_0 = |0\rangle\langle 0| \otimes \mathbb{1} \qquad M_1 = |1\rangle\langle 1| \otimes \mathbb{1}. \tag{2.23}$$

Since her particle is in a completely mixed state as pointed out in section 2.1.1 above, she obtains both $|0\rangle$ and $|1\rangle$ with equal probability of $1/2$, i.e.

$$\begin{aligned} p_0 &= \langle\Phi^+|M_0^\dagger M_0|\Phi^+\rangle = \frac{1}{2} \\ p_1 &= \langle\Phi^+|M_1^\dagger M_1|\Phi^+\rangle = \frac{1}{2} \end{aligned} \tag{2.24}$$

as it would be expected. Further, due to the measurement the entangled state collapses into a product state of the form

$$\begin{aligned} |\varphi_0\rangle_{AB} &= \frac{1}{\sqrt{p_0}} M_0^\dagger M_0 |\Phi^+\rangle_{AB} = |00\rangle_{AB} \\ |\varphi_1\rangle_{AB} &= \frac{1}{\sqrt{p_1}} M_1^\dagger M_1 |\Phi^+\rangle_{AB} = |11\rangle_{AB} \end{aligned} \tag{2.25}$$

if Alice obtains $|0\rangle$ or $|1\rangle$, respectively. As it can be clearly seen from $|\varphi_0\rangle_{AB}$ and $|\varphi_1\rangle_{AB}$ Bob's particle is in the exact same state as Alice's particle whatever result she obtains. This is shown in picture (2) of figure 2.1 where it is assumed that Alice

obtained $|0\rangle$ as a result from her measurement. Additionally, Bob's particle collapses into the same state in the very same moment Alice performs her measurement, no matter how far the two parties are apart. Einstein et al. stressed in their article that this would be a violation of locality.

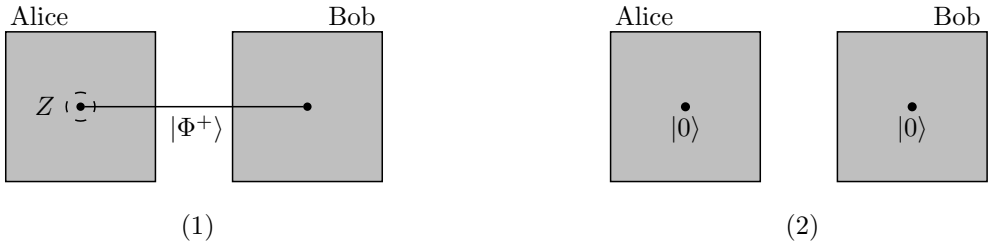

Figure 2.1: *(EPR gedankenexperiment)* Alice and Bob share a Bell state of the form $|\Phi^+\rangle_{AB}$ and the dashed circle indicates a measurement in the computational basis.

The principle of locality denotes in classical physics that an action performed at one place should not have any immediate impact at a distant instance. That would mean information is transmitted faster than the speed of light which is not possible. When looking at the gedankenexperiment it seems to violate this principle because Bob's qubit collapses into a state determined by Alice's measurement in the very same moment she performed her measurement. Further, the principle of realism states that the properties of Alice's and Bob's particles have definite values which exists independent of their observation. In case of the gedankenexperiment it seems that the properties of Alice's and Bob's particles have no definite value at all until the moment of measurement. The violation of these two principles was the main point of criticism of Einstein, Podolsky and Rosen at the theory of quantum mechanics. As pointed out in the next paragraphs it has been shown in various experiments that entangled states behave as described in the gedankenexperiment. Hence, quantum mechanics suggests that one of the two principles, locality or realism, is not valid.

After Einstein, Podolsky and Rosen published their article a number of other physicists began to question the EPR argument since it seems not really convincing. Finally, about 30 years after the original article was published, Bell proposed an experiment to actually show that the argumentation of Einstein et al. was not correct [2]. In this experiment Charlie prepares two particles in whatever way he likes (with the only restriction that the preparation has to be repeatable) and sends one particle to Alice and the other one to Bob. When Alice receives the particle

she performs a measurement on it. Therefore, she has two measurement apparatus such that she can choose one of them completely at random. Let's denote the two properties measured by each apparatus P_Q and P_R, respectively, with the outcomes Q and R. We want to stress that the properties P_Q and P_R are only revealed by Alice's measurement and can not be accessed in any other way. Similarly, Bob is also able to measure two properties P_S and P_T resulting in the outcomes S and T. For reasons of simplicity Alice's as well as Bob's results will take the values ± 1. Further, their measurements are arranged in a way that they take place at the same time, such that no information can be transmitted between the two parties.

When looking at the quantity $QS + RS + RT - QT$ we see immediately that either $(Q + R)S = 0$ or alternatively $(Q - R)T = 0$ since $Q, R = \pm 1$ and

$$QS + RS + RT - QT = (Q + R)S + (R - Q)T \tag{2.26}$$

As a result we know that $QS + RS + RT - QT = \pm 2$. Taking $p(q, r, s, t)$ as the probability that Charlie initially prepared $Q = q$, $R = r$, $S = s$ and $T = t$ the mean value of this expression is

$$\begin{aligned} E\big(QS + RS + RT - QT\big) &= \sum_{qrst} p\big(q, r, s, t\big)(qs + rs + rt - qt) \\ &\leq 2 \sum_{qrst} p\big(q, r, s, t\big) = 2 \end{aligned} \tag{2.27}$$

Further, from the same expression we get

$$\begin{aligned} E\big(QS + RS + RT - QT\big) =& \sum_{qrst} p\big(q, r, s, t\big)qs + \sum_{qrst} p\big(q, r, s, t\big)rs \\ &+ \sum_{qrst} p\big(q, r, s, t\big)rt - \sum_{qrst} p\big(q, r, s, t\big)qt \\ =& E\big(QS\big) + E\big(RS\big) + E\big(RT\big) - E\big(QT\big) \end{aligned} \tag{2.28}$$

Combining these two results we get the *Bell inequality*

$$E\big(QS\big) + E\big(RS\big) + E\big(RT\big) - E\big(QT\big) \leq 2 \tag{2.29}$$

which is also known as the *CHSH inequality* [33].

The argumentation for getting to the Bell inequality above is based solely on classical physics, i.e. the particles have been prepared by Charlie in a certain state with a certain probability. When quantum mechanics comes into play everything

gets a little more sophisticated. In this case Charlie prepares the Bell state $|\Psi^-\rangle$ and again sends the first particle to Alice and the other particle to Bob. For the observables Alice and Bob use

$$\begin{aligned} Q &= \sigma_z & R &= \sigma_x \\ S &= \frac{1}{\sqrt{2}}\big(-\sigma_z - \sigma_x\big) & T &= \frac{1}{\sqrt{2}}\big(\sigma_z - \sigma_x\big) \end{aligned} \tag{2.30}$$

Calculating the average value $\big\langle QS\big\rangle = \langle\Psi^-|(Q \otimes S)|\Psi^-\rangle$ we get

$$\begin{aligned} \big\langle QS\big\rangle =& \langle\Psi^-|\bigg(\sigma_z \otimes \frac{1}{\sqrt{2}}\big(-\sigma_z - \sigma_x\big)\bigg)|\Psi^-\rangle \\ =& \frac{1}{\sqrt{2}}\Big(\langle\Psi^-| - \langle\Phi^+|\Big)|\Psi^-\rangle = \frac{1}{\sqrt{2}} \end{aligned} \tag{2.31}$$

and similarly for the other three observable

$$\big\langle RS\big\rangle = \big\langle RT\big\rangle = \frac{1}{\sqrt{2}} \qquad \big\langle QT\big\rangle = -\frac{1}{\sqrt{2}} \tag{2.32}$$

which results in

$$\big\langle QS\big\rangle + \big\langle RS\big\rangle + \big\langle RT\big\rangle - \big\langle QT\big\rangle = 2\sqrt{2}. \tag{2.33}$$

Comparing this result with eq. (2.29) from above we see that for an entangled state the CHSH inequality is violated which stands in contrary to the classical assumptions. The violation of the CHSH inequality and the Bell inequality has first been done in a laboratory by Aspect in 1982 [1] thus invalidating the critics by Einstein, Podolsky and Rosen. Using the CHSH inequality it can be tested in a laboratory whether particles coming from a source are entangled or not.

2.4 Bell State Measurement

As we have mentioned in section 2.1 above the four Bell states $|\Phi^\pm\rangle$ and $|\Psi^\pm\rangle$ form an orthonormal basis of the 2-qubit space. Hence, an arbitrary 2-qubit state can be described in this basis, i.e. according to the four Bell states. Therefore this special measurement is called *Bell state measurement* (BSM) with the addition *complete* if all four Bell states are discriminated perfectly. Since we are making extensive use of the complete Bell state measurement throughout the thesis we are going into detail on the mathematical and physical background of this measurement.

From the definition of the Bell states the measurement operators can be directly defined as

$$\begin{aligned}
|\Phi^+\rangle\langle\Phi^+| &= \frac{1}{2}\left(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\right) \\
|\Phi^-\rangle\langle\Phi^-| &= \frac{1}{2}\left(|00\rangle\langle 00| - |00\rangle\langle 11| - |11\rangle\langle 00| + |11\rangle\langle 11|\right) \\
|\Psi^+\rangle\langle\Psi^+| &= \frac{1}{2}\left(|01\rangle\langle 01| + |01\rangle\langle 10| + |10\rangle\langle 01| + |10\rangle\langle 10|\right) \\
|\Psi^-\rangle\langle\Psi^-| &= \frac{1}{2}\left(|01\rangle\langle 01| - |01\rangle\langle 10| - |10\rangle\langle 01| + |10\rangle\langle 10|\right)
\end{aligned} \tag{2.34}$$

Using these operators any 2-qubit state can be projected onto the Bell basis. Additionally, an arbitrary 2-qubit state can be written directly in the Bell basis, i.e.

$$\begin{aligned}
|\varphi\rangle &= \alpha_0|00\rangle + \alpha_1|01\rangle + \alpha_2|10\rangle + \alpha_3|11\rangle \\
&= \frac{1}{\sqrt{2}}\left(\alpha_0 + \alpha_3\right)|\Phi^+\rangle + \frac{1}{\sqrt{2}}\left(\alpha_0 - \alpha_3\right)|\Phi^-\rangle \\
&+ \frac{1}{\sqrt{2}}\left(\alpha_1 + \alpha_2\right)|\Psi^+\rangle + \frac{1}{\sqrt{2}}\left(\alpha_1 - \alpha_2\right)|\Psi^-\rangle
\end{aligned} \tag{2.35}$$

From this equation we can directly obtain the probability of getting a specific Bell state as result of the measurement and it can be extended straightforward to multi-qubit systems. Therefore, we prefer this representation throughout the thesis whenever a Bell state measurement is described.

Although the discrimination of all four Bell states can be conveniently described in theory a practical realization of a Bell state measurement is rather difficult. To give a basic idea how such a measurement can be implemented we want to sketch an experiment presented by Kim et al. [85] where a complete Bell state measurement is realized using photons as qubits. The main part of this experiment is the sum frequency generation (SFG), also called "upconversion". This non-linear operation takes two photons with a certain polarization and transforms them into one photon with a different polarization. Here, two different types of SFG crystals are needed [85]: the type-I SFG takes photons with the same polarization, i.e. either the state $|00\rangle$ or $|11\rangle$, and transforms them into one photon in the state $|1\rangle$ or $|0\rangle$, respectively. The type-II SFG takes two photons of different polarization, i.e. photons in the state $|01\rangle$ and $|10\rangle$ and also transforms them either in the state $|1\rangle$ or $|0\rangle$, respectively. Every sum frequency generation consists of two crystals which perform the transformation either on horizontal or vertical polarized photons. Using this method the four Bell states can be distinguished perfectly.

In [85] an EPR state enters the setup with photons of wavelength 730 nm and 885 nm. They are sent into the type-I SFG where the first crystal changes $|00\rangle$ to $|1\rangle$ and the second changes $|11\rangle$ to $|0\rangle$. After the SFG the photons hit on the dichroic beam splitter which reflects the photons that have been altered by the type-I SFG. The reflected photon is then going through a $\pm 45°$ polarization projector and hits one of two detectors thus discriminating between $|\Phi^+\rangle$ and $|\Phi^-\rangle$.

The transmitted photon reaches the type-II SFG, which performs the transformation from $|01\rangle$ to $|1\rangle$ and from $|10\rangle$ to $|0\rangle$. Since there are only these four possibilities we can be sure that all the photons entering the type-II SFG are transformed. Again, a $\pm 45°$ dichroic beam splitter and two detectors are located behind the type-II SFG crystals. The photon travels through the beam splitter and hits one of the detectors which discriminate between $|\Psi^+\rangle$ and $|\Psi^-\rangle$, respectively.

2.5 Applications of Entanglement

There are several applications and phenomena where entanglement plays a major role and has been studied extensively. In the following sections we want to shortly describe the schemes for dense coding, teleportation and entanglement swapping. In particular entanglement swapping is extensively used in the protocols discussed later on in chapters 7 and 8. Quantum cryptography, the most important field where entanglement is used, will be covered in detail in section 5 below.

2.5.1 Dense Coding

One application where entanglement provides a significant advantage is *dense coding* which was presented by Bennett and Wiesner in 1992 [4]. Here the challenge for Alice is to send a message to Bob consisting of 2 classical bits but she can only send one qubit. The *Holevo bound* [69] states that one qubit can carry at most one bit of classical information. Hence, this would suggest that Alice's attempt is not possible but Bennett and Wiesner suggest the following procedure: As a preliminary setting, Alice and Bob share the entangled state $|\Phi^+\rangle_{AB}$ such that each party is in possession of one particle. The information about Alice's classical string is then carried by both qubits of the state. Depending on which of the four messages (00,

01, 10, or 11) Alice wants to send, she performs one of the four *Pauli operators*

$$\begin{aligned} \mathbb{1} &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \sigma_x &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} & \sigma_z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned} \tag{2.36}$$

on her qubit (cf. picture (1) in figure 2.2). These operators have the property to map the Bell states onto one another if they are applied on one of the two qubits of the state. For example, a Pauli operation applied on the first qubit of the state $|\Phi^+\rangle_{AB}$ – as it is the case here – gives

$$\begin{aligned} \mathbb{1} \otimes \mathbb{1} \, |\Phi^+\rangle_{AB} &= |\Phi^+\rangle_{AB} & \sigma_x \otimes \mathbb{1} \, |\Phi^+\rangle_{AB} &= |\Psi^+\rangle_{AB} \\ \sigma_y \otimes \mathbb{1} \, |\Phi^+\rangle_{AB} &= |\Psi^-\rangle_{AB} & \sigma_z \otimes \mathbb{1} \, |\Phi^+\rangle_{AB} &= |\Phi^-\rangle_{AB} \end{aligned} \tag{2.37}$$

and analog for the other three Bell states (for a full overview of the mapping cf. table 4.1 in section 4.2.2 below). Then Alice sends her qubit to Bob who performs a complete Bell measurement to discriminate between all four states (cf. picture (2) in figure 2.2). Since he knows the initial state $|\Phi^+\rangle_{AB}$ of both qubits Bob is able to infer which operation Alice performed on her qubit. Using a mapping between the Pauli operators and the messages, i.e.

$$\mathbb{1} \longmapsto 00 \qquad \sigma_x \longmapsto 01 \qquad \sigma_y \longmapsto 10 \qquad \sigma_z \longmapsto 11 \tag{2.38}$$

Bob knows exactly the two classical bits of Alice. Hence, Bob receives the full 2-bit message from Alice although she only sent one qubit.

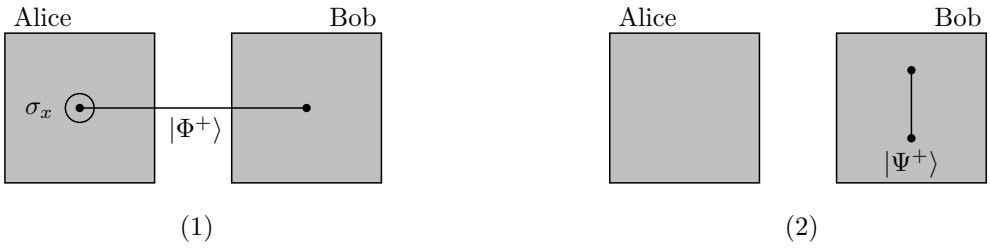

Figure 2.2: *(Dense Coding)* Alice and Bob share a Bell state of the form $|\Phi^+\rangle_{AB}$. Here, the circle indicates the application of an operation, i.e. the σ_x operation.

Although this procedure seems to violate the Holevo bound it needs in fact two qubits to be sent to make the dense coding work. In the setup of the protocol it is

assumed that an entangled state is somehow shared between Alice and Bob. But to achieve that one qubit has to be transmitted (either from Alice to Bob or from Bob to Alice). This qubit also counts for the communication although it transports no actual information. Only in connection with the second qubit coming from Alice the full information can be extracted from the entangled state, which fits perfectly into the Holevo bound.

2.5.2 Teleportation

Bennett et al. also described a scheme of how to send an unknown quantum state

$$|\varphi\rangle_C = \alpha|0\rangle_C + \beta|1\rangle_C \tag{2.39}$$

from Alice to Bob with the help of entanglement [10]. Without entanglement this task can only be achieved rather poorly: Alice would perform a measurement in some basis on the qubit to determine it's state and tell it Bob over a classical channel. However, if she does not accidentally choose the correct basis most of the information about the state is lost due the measurement and Bob gets an insufficient version of the state. In a classical environment Alice would be able to make copies of the unknown state to perform several measurements in different bases and thus improve her estimation of the state. In a quantum setting this is not possible since it violates the *no cloning theorem* presented by Wooters and Zurek in 1982 [166].

Nevertheless, if Alice and Bob share an entangled state, e.g. $|\Phi^+\rangle_{AB}$ as in the last section, Alice can perfectly achieve the task of sending Bob an unknown state using *teleportation*. As presented by Bennett et al. Alice performs a complete Bell state measurement on her particle of the entangled state together with the unknown state $|\varphi\rangle_C$ as shown in picture (1) of figure 2.3. A complete discrimination of the four Bell states can be achieved using nonlinear optics, as described in [85]. This brings the overall state $|\Phi^+\rangle_{AB}|\varphi\rangle_C$ to

$$\begin{aligned} |\Phi^+\rangle_{AB} \otimes |\varphi\rangle_C = \frac{1}{2}\Big(& |\Phi^+\rangle_{AC} \otimes \big(\alpha|0\rangle_B + \beta|1\rangle_B\big) \\ & + |\Phi^-\rangle_{AC} \otimes \big(\alpha|0\rangle_B - \beta|1\rangle_B\big) \\ & + |\Psi^+\rangle_{AC} \otimes \big(\beta|0\rangle_B + \alpha|1\rangle_B\big) \\ & + |\Psi^-\rangle_{AC} \otimes \big(\beta|0\rangle_B - \alpha|1\rangle_B\big)\Big). \end{aligned} \tag{2.40}$$

From this equation we see that the projection of particles A and C at Alice's side onto the Bell states leaves the particle B at Bob's side immediately in a state very

similar to the unknown state $|\varphi\rangle$ (cf. picture (2) in figure 2.3). To finally bring Bob's particle into the state $|\varphi\rangle$ he just has to perform one of the four Pauli operations onto it. Which operation he has to use fully depends on the result of Alice's measurement, which she tells Bob over a classical channel.

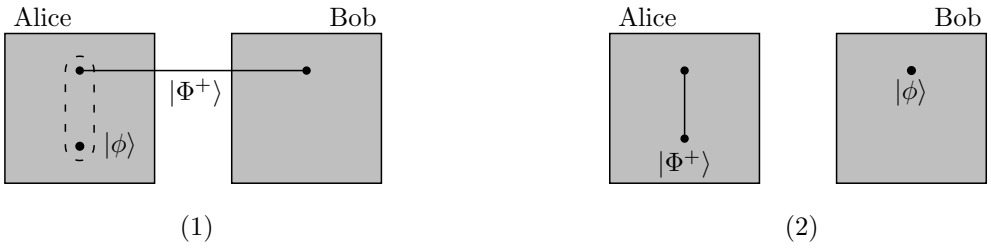

Figure 2.3: *(Teleportation)* Alice and Bob share a Bell state of the form $|\Phi^+\rangle_{AB}$. Here, the dashed line indicates a measurement in the Bell basis.

When we look at the states at Alice's and Bob's side we see that the no-cloning theorem has not been violated by teleportation. Alice's qubits are in one of the four Bell states with equal probability and she has no information about the unknown state $|\varphi\rangle$. Furthermore, the unknown state has been moved to Bob using the entangled state $|\Phi^+\rangle$ and no other copy is present. Additionally, Bob has no information about the state in his possession until he receives Alice's classical information about her measurement result ruling out the argument of faster than light communication brought up in the discussion of the EPR gedankenexperiment in section 2.3 above.

2.5.3 Entanglement Swapping

The last phenomenon we want to discuss in connection with entanglement is *entanglement swapping*, which has been introduced by Bennett et al. [10], Zukowski et al. [172] as well as Yurke and Stolen [169], respectively. Entanglement swapping provides the unique possibility to generate entanglement from particles that never interacted in the past. The procedure works similar to teleportation described above but now the unknown state Alice wants to teleport to Bob is part of an entangled state. In detail, Alice and Bob share two Bell states of the form $|\Phi^+\rangle_{A_1B_1}$ and $|\Phi^+\rangle_{A_2B_2}$ such that Alice is in possession of qubits A_1 and A_2 and Bob of qubits B_1 and B_2. Then Alice performs a complete Bell state measurement on the two qubits

in her possession (cf. picture (1) in figure 2.4) which results in

$$|\Phi^+\rangle_{A_1B_1} \otimes |\Phi^+\rangle_{A_2B_2} = \frac{1}{2}\Big(|\Phi^+\rangle_{A_1A_2}|\Phi^+\rangle_{B_1B_2} + |\Phi^-\rangle_{A_1A_2}|\Phi^-\rangle_{B_1B_2} + |\Psi^+\rangle_{A_1A_2}|\Psi^+\rangle_{B_1B_2} + |\Psi^-\rangle_{A_1A_2}|\Psi^-\rangle_{B_1B_2}\Big) \tag{2.41}$$

Thus, after the measurement the two qubits B_1 and B_2 at Bob's side collapse into a Bell state although they originated at completely different sources. Moreover, the state of Bob's qubits is fully correlated to Alice's result. As presented in eq. (2.41) Bob always obtains the same result as Alice when performing a Bell state measurement on his qubits. This is shown in picture (2) of figure 2.4 where we assumed that Alice obtains $|\Phi^+\rangle_{A_1A_2}$ from her Bell state measurement. For different initial states Alice's and Bob's result also change but the correlation between them is preserved (cf. table 2.1 below).

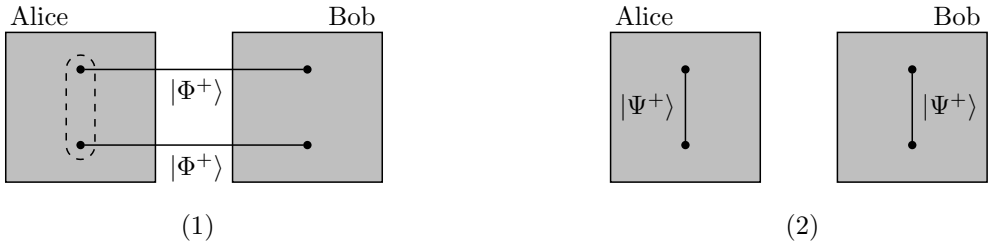

Figure 2.4: *(Entanglement Swapping)* Alice and Bob share two Bell states each of the form $|\Phi^+\rangle$. Here, the dashed line indicates a measurement in the Bell basis.

If there are three parties, Alice, Bob and Charlie, which share two Bell states $|\Phi^+\rangle_{AB}$ and $|\Phi^+\rangle_{BC}$ the scheme works analog. Since Bob is the only one to perform a Bell state measurement it has the effect that in the end Alice and Charlie share an entangled state. Such a scheme is used in a quantum repeater setup as presented by Dür et al. [45] to establish an entangled state over several hops to overcome long distances (cf. also section 4.4 for details).

	$\|\Phi^+\rangle_{A_1A_2}$	$\|\Phi^-\rangle_{A_1A_2}$	$\|\Psi^+\rangle_{A_1A_2}$	$\|\Psi^-\rangle_{A_1A_2}$
$\|\Phi^+\rangle_{A_1B_1}\|\Phi^+\rangle_{A_2B_2}$	$\|\Phi^+\rangle_{B_1B_2}$	$\|\Phi^-\rangle_{B_1B_2}$	$\|\Psi^+\rangle_{B_1B_2}$	$\|\Psi^-\rangle_{B_1B_2}$
$\|\Phi^+\rangle_{A_1B_1}\|\Phi^-\rangle_{A_2B_2}$	$\|\Phi^-\rangle_{B_1B_2}$	$\|\Phi^+\rangle_{B_1B_2}$	$-\|\Psi^-\rangle_{B_1B_2}$	$-\|\Psi^+\rangle_{B_1B_2}$
$\|\Phi^+\rangle_{A_1B_1}\|\Psi^+\rangle_{A_2B_2}$	$\|\Psi^+\rangle_{B_1B_2}$	$\|\Psi^-\rangle_{B_1B_2}$	$\|\Phi^+\rangle_{B_1B_2}$	$\|\Phi^-\rangle_{B_1B_2}$
$\|\Phi^+\rangle_{A_1B_1}\|\Psi^-\rangle_{A_2B_2}$	$\|\Psi^-\rangle_{B_1B_2}$	$\|\Psi^+\rangle_{B_1B_2}$	$-\|\Phi^-\rangle_{B_1B_2}$	$-\|\Phi^+\rangle_{B_1B_2}$
$\|\Phi^-\rangle_{A_1B_1}\|\Phi^+\rangle_{A_2B_2}$	$\|\Phi^-\rangle_{B_1B_2}$	$\|\Phi^+\rangle_{B_1B_2}$	$\|\Psi^-\rangle_{B_1B_2}$	$\|\Psi^+\rangle_{B_1B_2}$
$\|\Phi^-\rangle_{A_1B_1}\|\Phi^-\rangle_{A_2B_2}$	$\|\Phi^+\rangle_{B_1B_2}$	$\|\Phi^-\rangle_{B_1B_2}$	$-\|\Psi^+\rangle_{B_1B_2}$	$-\|\Psi^-\rangle_{B_1B_2}$
$\|\Phi^-\rangle_{A_1B_1}\|\Psi^+\rangle_{A_2B_2}$	$\|\Psi^-\rangle_{B_1B_2}$	$\|\Psi^+\rangle_{B_1B_2}$	$-\|\Phi^-\rangle_{B_1B_2}$	$-\|\Phi^+\rangle_{B_1B_2}$
$\|\Phi^-\rangle_{A_1B_1}\|\Psi^-\rangle_{A_2B_2}$	$\|\Psi^+\rangle_{B_1B_2}$	$\|\Psi^-\rangle_{B_1B_2}$	$\|\Phi^+\rangle_{B_1B_2}$	$\|\Phi^-\rangle_{B_1B_2}$
$\|\Psi^+\rangle_{A_1B_1}\|\Phi^+\rangle_{A_2B_2}$	$\|\Psi^+\rangle_{B_1B_2}$	$-\|\Psi^-\rangle_{B_1B_2}$	$\|\Phi^+\rangle_{B_1B_2}$	$-\|\Phi^-\rangle_{B_1B_2}$
$\|\Psi^+\rangle_{A_1B_1}\|\Phi^-\rangle_{A_2B_2}$	$-\|\Psi^-\rangle_{B_1B_2}$	$\|\Psi^+\rangle_{B_1B_2}$	$\|\Phi^-\rangle_{B_1B_2}$	$-\|\Phi^+\rangle_{B_1B_2}$
$\|\Psi^+\rangle_{A_1B_1}\|\Psi^+\rangle_{A_2B_2}$	$\|\Phi^+\rangle_{B_1B_2}$	$-\|\Phi^-\rangle_{B_1B_2}$	$\|\Psi^+\rangle_{B_1B_2}$	$-\|\Psi^-\rangle_{B_1B_2}$
$\|\Psi^+\rangle_{A_1B_1}\|\Psi^-\rangle_{A_2B_2}$	$-\|\Phi^-\rangle_{B_1B_2}$	$\|\Phi^+\rangle_{B_1B_2}$	$\|\Psi^-\rangle_{B_1B_2}$	$-\|\Psi^+\rangle_{B_1B_2}$
$\|\Psi^-\rangle_{A_1B_1}\|\Phi^+\rangle_{A_2B_2}$	$-\|\Psi^-\rangle_{B_1B_2}$	$\|\Psi^+\rangle_{B_1B_2}$	$-\|\Phi^-\rangle_{B_1B_2}$	$\|\Phi^+\rangle_{B_1B_2}$
$\|\Psi^-\rangle_{A_1B_1}\|\Phi^-\rangle_{A_2B_2}$	$\|\Psi^+\rangle_{B_1B_2}$	$-\|\Psi^-\rangle_{B_1B_2}$	$-\|\Phi^+\rangle_{B_1B_2}$	$\|\Phi^-\rangle_{B_1B_2}$
$\|\Psi^-\rangle_{A_1B_1}\|\Psi^+\rangle_{A_2B_2}$	$-\|\Phi^-\rangle_{B_1B_2}$	$\|\Phi^+\rangle_{B_1B_2}$	$-\|\Psi^-\rangle_{B_1B_2}$	$\|\Psi^+\rangle_{B_1B_2}$
$\|\Psi^-\rangle_{A_1B_1}\|\Psi^-\rangle_{A_2B_2}$	$\|\Phi^+\rangle_{B_1B_2}$	$-\|\Phi^-\rangle_{B_1B_2}$	$-\|\Psi^+\rangle_{B_1B_2}$	$\|\Psi^-\rangle_{B_1B_2}$

Table 2.1: Correlation between Alice's and Bob's measurement result based on all possible initial states.

Chapter 3

Entanglement Measures

As pointed out in chapter 2 entanglement is a central resource in several quantum mechanical primitives like teleportation and entanglement swapping. In such scenarios a major question is how much entanglement is given between the two communication parties. Due to the effects of noisy channels or operations on the entangled states the amount of entanglement is reduced, which has influence on the communication between the parties. Therefore, it is important to quantify the amount of entanglement in a certain system, which is achieved using *entanglement measures*.

3.1 Entanglement of Distillation and Entanglement Cost

Taking a set of mixed entangled states ρ, which have been, for example, tampered by a noisy channel, it is possible to perform certain operations on these states to create a smaller set of states which are in a pure entangled state, e.g. $|\Psi^-\rangle$. This procedure is called *entanglement distillation* and is described in further detail in chapter 4. The idea of entanglement distillation can also be used to define a measure of entanglement, the so called *Entanglement of Distillation* $E_D(\rho)$. The entanglement of distillation is given as the maximal number of pure states $|\Psi^-\rangle$ that can be generated from the input state ρ. It has to be stressed that only local operations and classical communication (LOCC) are used to manipulate the mixed

state ρ. A more formal definition is [64]

$$E_D(\rho) = \sup_{LOCC} \lim_{n \mapsto \infty} \frac{m}{n} \tag{3.1}$$

where n is the number of input states ρ and m is the number of output states $|\Psi^-\rangle$. Here we want to denote $m = f(n)$ to stress that the number of output states is directly related to the number of input states. This relation $f(n)$ may not be given explicitly or may vary depending on the number of input states but it shows that $E_D(\rho)$ does not go to 0 for $n \mapsto \infty$. Moreover, it is important that the conversion to the output states has to be perfect only in the asymptotic limit. Overall, the higher the rate of perfect entangled states to mixed input states is the more entanglement is present in the input states.

There is also a dual version of the entanglement of distillation, which is called *entanglement cost*. Here, the setting is reversed as there is a number of perfectly entangled states $|\Psi^-\rangle$ given which have to be used to produce mixed states of the form ρ by LOCC. The entanglement cost $E_C(\rho)$ is then the minimal number of entangled states needed to create one mixed state ρ. Again, the formal description is [64]

$$E_C(\rho) = \inf_{LOCC} \lim_{m \mapsto \infty} \frac{n}{m} \tag{3.2}$$

where n is the number of mixed states ρ to be created and m the number of pure entangled input states. As stated above, we can describe n as a function $g(m)$ of the input states to stress that $E_C(\rho)$ does not go to 0 for $m \mapsto \infty$ but that the number of mixed output states is in some way related to the number of pure entangled input states.

It has been shown in [72] that the entanglement of distillation and the entanglement cost describe a lower and an upper bound for any entanglement measure satisfying the basic axioms presented in the following section. In other words, $E_D(\rho) \leq E_C(\rho)$ and therefore E_D and E_C are called *extreme measures*. When dealing with pure states it has been shown [14] that E_D and E_C coincide such that $E_D(\rho) = E_C(\rho)$ is given by the von Neuman entropy (cf. section 3.3.1 below). Looking at bound entangled states introduced in section 2.1.3 we know that no entanglement can be distilled out of them (i.e. $E_D = 0$) but that they need entanglement for their creation (i.e. $E_C > 0$) [75]. Thus, bound entangled states can have $E_D(\rho) \neq E_C(\rho)$.

3.2 Properties for Entanglement Measures

Before we explicitly discuss several measures for 2-qubit and multi-qubit systems we want to present some properties which an entanglement measure E has to meet. It can be distinguished between properties for measurements on pure states and on mixed states as it has been done in [107]. We will not go into such a detail since the properties in connection with pure states are just special cases of the properties in connection with mixed states.

1. The first and most intuitive property for a general entanglement measure E is that $E(\rho) = 0$ if ρ is separable.

2. The next property, which comes also quite natural, requires the measure E to be invariant under local unitary transformations, i.e.

$$E\big(\rho\big) = E\Big(\big(U_A \otimes U_B\big)\ \rho\ \big(U_A^\dagger \otimes U_B^\dagger\big)\Big). \tag{3.3}$$

3. The third property deals with the evolution of entanglement under LOCC and it states that entanglement does not increase on average under LOCC. In detail,

$$\sum_i p_i E\Big(\Lambda_i\big(\rho\big)\Big) \leq E\Big(\rho\Big) \tag{3.4}$$

where the Λ_i is a LOCC transformation which maps ρ onto some ρ_i with probability p_i. Although this is a rather strong requirement it is fulfilled by numerous entanglement measures. A somewhat weaker property, which can also be found in literature, states

$$E\Big(\Lambda\big(\rho\big)\Big) \leq E\Big(\rho\Big). \tag{3.5}$$

These two versions of the property also correspond to the fact that entanglement can not be created by local operations and classical communication.

4. Another property required for an entanglement measure is *convexity*. That is the overall entanglement decreases when two or more states are mixed, i.e.

$$E\Big(\sum_i p_i\rho_i\Big) \leq \sum_i p_i E\big(\rho_i\big). \tag{3.6}$$

This property states that loosing the information about the specific states ρ_i in an ensemble is equivalent to a decrease of the entanglement. The convexity

property is very strict and since it is not fulfilled by all entanglement measures it has been discussed to relax this condition such that $E(\rho)$ should not increase if locally distinguishable states are mixed [115].

5. The last property of an entanglement measure we will discuss here is *additivity*. This addresses the scenario where two or more copies of a state are analyzed. Then, an entanglement measure should satisfy

$$E\big(\rho^{\otimes n}\big) = nE\big(\rho\big). \tag{3.7}$$

A stronger version is the *full additivity*, which extends the property to different states such that

$$E\big(\rho_1 \otimes \rho_2\big) = E\big(\rho_1\big) + E\big(\rho_2\big) \tag{3.8}$$

Such additivity is very difficult to prove [116] and is not fulfilled by some entanglement measures.

As we have seen in section 3.1 above it is not straightforward to define an entanglement measure. One way is to take a certain task as a measure of entanglement, for example the distillation process. Then the optimal distillation rate $E_D(\rho)$ for some state ρ is an entanglement measure, as we have seen in case of the entanglement of distillation. Nevertheless, it is obvious that such quantities are difficult to compute since a computation involves an optimization over all possible distillation protocols, which is almost impossible to accomplish.

Another possibility to define an entanglement measure is to first define a measure $E(|\varphi\rangle)$ on pure states and then bring it to mixed states as [149]

$$E\big(\rho\big) = \inf_{p_i, |\varphi_i\rangle} \sum_i p_i E\big(|\varphi_i\rangle\big) \tag{3.9}$$

where $\rho = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|$ and the infimum is taken of all possible decompositions of ρ. This method is called the *convex roof construction*, since $E(\rho)$ is defined as the largest convex function smaller than $E(|\varphi\rangle)$. The convex roof construction has the great advantage that the resulting entanglement measure comes with some desirable properties such as, for example, that $E(\rho)$ is convex. Additionally, from the properties of $E(|\varphi\rangle)$ one can directly deduce which properties $E(\rho)$ fulfills [155].

Also the measures constructed by the convex roof are difficult to compute since all possible decompositions of a mixed state have to be taken into account. Nevertheless,

it is straightforward to find lower and upper bounds for the respective measures [64]. The main idea is to take a convex function $F(\rho)$ which is easy to compute and find a lower bound for F on pure states. Since the convex roof $E(\rho)$ resulting from the measure E on pure states is the largest convex function smaller than E, the lower bound F holds also for the mixed states measure $E(\rho)$.

3.3 Measures for 2-Qubit Systems

3.3.1 von Neuman Entropy

The most fundamental measure to determine the amount of entanglement in a pure states is the *von Neuman entropy* which has been published in 1932 [158] and is defined as

$$S\big(\rho\big) = -\mathrm{Tr}\big(\rho \log \rho\big) \tag{3.10}$$

where log is the binary logarithm. It is usually calculated using the eigenvalues of ρ, i.e.

$$S\big(\rho\big) = -\sum_i \mathrm{Tr}\big(\lambda_i \log \lambda_i\big). \tag{3.11}$$

The von Neuman entropy is defined very similar to the Shannon entropy known from classical information theory [134] which comes from the fact that the Shannon entropy is based on the von Neuman entropy.

There is also another version of the von Neuman entropy, which acts on the reduced density matrix of a state ρ. Accordingly, this version is called *reduced von Neuman entropy* or *entropy of entanglement* [12] and is defined as

$$E_E\big(\rho\big) = -\mathrm{Tr}\big(\rho_A \log \rho_A\big). \tag{3.12}$$

Here, ρ_A denotes the reduced density matrix describing the system of Alice but similarly also the system of Bob, ρ_B, could be used instead. In contrary to the entanglement of distillation and the entanglement cost the entropy of entanglement has no operational meaning and is thus called an *abstract measure*.

3.3.2 Entanglement of Formation

Since the von Neuman entropy is only defined on pure states the convex roof construction is used to generalize the measure to mixed states. This convex roof of

the von Neuman entropy is called *entanglement of formation* [14] and is defined accordingly to eq. (3.9) as

$$E_F(\rho) = \inf_{p_i,|\varphi_i\rangle} \sum_i p_i S\Big(\mathrm{Tr}_B\big(|\varphi_i\rangle\langle\varphi_i|\big)\Big) \tag{3.13}$$

where $\rho = \sum_i p_i |\varphi_i\rangle\langle\varphi_i|$. The physical interpretation of the entanglement of formation is that it gives the minimal number of entangled states necessary to create a single copy of ρ. The main problem of the entanglement of formation is again the difficulty of the computation. To calculate the convex roof we have to optimize over all possible decompositions of the mixed state ρ.

One property of the entanglement of formation is of special interest: it is not known whether the entanglement of formation is fully additive or not. The solution of this problem is of such great interest because it has implications on, for example, the classical capacity of quantum channels [116].

3.3.3 Concurrence

The *concurrence* is a rather popular measure for entanglement and has been introduced in [67]. The main advantage of this measure is that there exists a closed form for an arbitrary mixed state ρ. This closed form is based on the complex conjugate matrix ρ^* of ρ. Further, the Pauli operator σ_y is used to perform a bit- and phase-flip on ρ^* to finally obtain the matrix

$$R = \sqrt{\sqrt{\rho}\big(\sigma_y \otimes \sigma_y\big)\rho^*\big(\sigma_y \otimes \sigma_y\big)\sqrt{\rho}} \tag{3.14}$$

The concurrence C is then defined as

$$C(\rho) = \max\big\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\big\} \tag{3.15}$$

where the λ_i are the eigenvalues of R in decreasing order.

The concurrence is also directly connected to the entanglement of formation described above, i.e. [67]

$$E_F(\rho) = h\left(\frac{1+\sqrt{1-C^2(\rho)}}{2}\right) \tag{3.16}$$

where $h(p)$ is the binary entropy function $-p\log p - (1-p)\log(1-p)$. Thus, using the concurrence there is a simple method to compute the entanglement of formation for arbitrary mixed states without the need of optimizing over all possible ensembles describing the mixed state.

3.3.4 Distant Measures

A large group of entanglement measures are the *distance measures*. These measures are based on the idea that the closer a state is to the set of separable states the less entanglement it contains (c.f also figure 3.1). This distance between the mixed state and the nearest separable state is then used as an entanglement measure. From this description we can already identify the main problem of the distance measures: it is usually not trivial to find the closest separable state to some mixed state ρ. Moreover, the minimal distance between a state ρ and all states in the set S of separable states has to be found. This results in the definition of a distance measurement

$$E_D\big(\rho\big) = \inf_{\delta \in S} D\big(\rho, \delta\big) \tag{3.17}$$

where D is some distance measure.

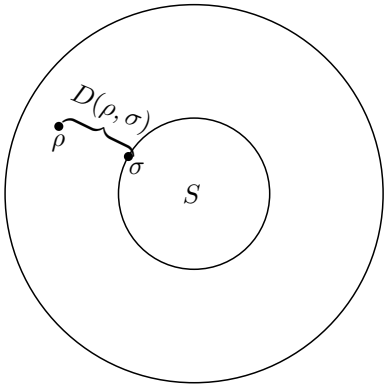

Figure 3.1: *(Distance Measure)* Graphical description of a distance measure. The inner circle represents the set S of separable states and $\delta \in S$ the closest state to the entangled state ρ. The closer the distance $D(\rho, \delta)$ the less entangled is ρ.

Since there are several possible distance measures, several individual measures arise. The most common function in this context is the relative entropy [153]

$$S\big(\rho \| \delta\big) = \mathrm{Tr}\Big(\rho\big(\log \rho - \log \delta\big)\Big) \tag{3.18}$$

giving the *relative entropy of entanglement*

$$E_R\big(\rho\big) = \inf_{\delta} S\big(\rho \| \delta\big). \tag{3.19}$$

As the name indicates, the relative entropy of entanglement is closely related to the entropy of entanglement discussed above as it reduces to the entropy of entanglement

if ρ is a pure state. We have to stress that the relative entropy of entanglement is not a metric but can be seen as a function to distinguish between quantum states. Nevertheless, it is applicable as a distance function in this special context giving an entanglement measure.

Another distance measure often found in the literature in the context of entanglement measures is the *Bures metric* [25, 153]

$$D_B\big(\rho\|\delta\big) = 2 - 2\sqrt{F(\rho,\delta)}. \tag{3.20}$$

Here, the function $F(\rho,\delta)$ is called the Uhlmann's transition probability [148] and is defined as

$$F\big(\rho,\delta\big) = \left(\mathrm{Tr}\Big(\sqrt{\sqrt{\delta}\rho\sqrt{\delta}}\Big)\right)^2 \tag{3.21}$$

resulting in the respective measure

$$E_B\big(\rho\big) = \inf_{\delta} D_B\big(\rho\|\delta\big). \tag{3.22}$$

In contrary to the relative entropy the Bures metric is a real metric but, however, has no direct relation to the entropy of entanglement. In fact, the entanglement measure based on the Bures metric is smaller than the entropy of entanglement [153].

3.3.5 Negativity

As we have already seen from the examples above most of the entanglement measures are in general rather difficult to compute. A measure that is much easier to evaluate is the *negativity* [156]. It is directly connected to the PPT separability criterion defined in section 2.1.3 and is based on the partial transpose and the trace norm. The negativity is defined as

$$\mathcal{N}\big(\rho\big) = \frac{\|\rho^{T_B}\|_1 - 1}{2} \tag{3.23}$$

or, in a similar version called *logarithmic negativity*

$$E_{\mathcal{N}}\big(\rho\big) = \log\|\rho^{T_B}\|_1 \tag{3.24}$$

Similar to all entanglement measures the negativity and the logarithmic negativity vanish for separable states but, since they are connected to the PPT criterion, these measures can not distinguish between separable states and PPT entangled states. Nevertheless, both measures can be used to quantify how much a state ρ violates the PPT criterion.

3.4 Measures for Multi-Qubit Systems

3.4.1 Distance Measures

Most of the measures as for example the distillable entanglement, the entanglement cost or the concurrence described in the previous section are strictly related to Bell states, i.e. to the bipartite case. From the definition it is not obvious how these measures can be brought to the multipartite case. One possibility to overcome this drawback is switch from a definition based on 2-qubit states (i.e. the Bell states) to a more abstract one like the CNOT gates used in the process of distillation or the number of qubits transferred in the process of creation [108]. For example, looking at the entanglement cost the number of qubits transmitted between Alice and Bob could be such an alternative quantity to measure the entanglement. In this way the extension from the bipartite to the multipartite case could be done much easier. Nevertheless, the field of entanglement measures in multi-qubit systems is much more complex than the bipartite case and has not yet been covered very well.

The main exception are the distant measures like the relative entropy of entanglement, which have no relation to the dimension of the state ρ used in their definition. Thus, they are applicable to any density matrix describing ρ regardless of the dimension. Nevertheless, the main problem of the distant measures - the identification of the closest separable state - is still valid and even more sophisticated in the multipartite case. For example, the PPT criterion discussed in section 2.1.3 can not be used to perfectly identify separable states in the multipartite case, as pointed out above.

3.4.2 Tangle

An entanglement measure defined for three qubits is the *tangle*, which has been introduced in [35]. It is defined similarly to the concurrence described in section 3.3.3 above. It also starts using the σ_y operation on both qubits of the complex conjugated state ρ, i.e.

$$\tilde{\rho} = \big(\sigma_y \otimes \sigma_y\big)\rho^*\big(\sigma_y \otimes \sigma_y\big) \tag{3.25}$$

Next, the product $\rho_{AB}\tilde{\rho}_{AB}$ is computed and the tangle is

$$\tau_{AB}\big(\rho\big) = \Big(\max\big\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\big\}\Big)^2 \tag{3.26}$$

with λ_1 to λ_4 are the square roots of the eigenvalues of $\rho_{AB}\tilde{\rho}_{AB}$ in decreasing order. This result is very similar to eq. (3.15) such that the relation of the tangle to the entanglement of formation is obvious using eq. (3.16), i.e.

$$E_F(\rho) = h\left(\frac{1}{2} + \frac{1}{2}\sqrt{1 - \tau_{AB}(\rho)}\right). \tag{3.27}$$

Because of this relation and eq. (3.26) the tangle can also be interpreted as the square of he concurrence [35]. The tangle for 2 qubits in a pure state has the convenient property that it can be computed directly. The product $\rho_{AB}\tilde{\rho}_{AB}$ has only one non-negative eigenvalue such that $\tau_{AB} = 4 \det \mathrm{Tr}_B(\rho)$. The tangle for mixed states is defined directly using the convex roof and can also be calculated for special cases [95, 53].

The definition of the tangle τ_{AB} for two qubits can be used also in a system with three qubits. For τ_{ABC} we get [35]

$$\tau_{ABC}(\rho) = \tau_{A|BC}(\rho) - \tau_{AB}(\rho) - \tau_{AC}(\rho). \tag{3.28}$$

To obtain this equation we have to start with the problem how to define the relation between two qubits in a 3-qubit system. For reasons of simplicity we focus on the case where the 3-qubit system is in a pure state. Since in any such system every 2-qubit subsystem has only 2 non-zero eigenvalues the eq. (3.26) can be rewritten as

$$\begin{aligned} \tau_{AB}(\rho) &= \Big(\max\{0, \lambda_1 - \lambda_2\}\Big)^2 = (\lambda_1 - \lambda_2)^2 \\ &= \lambda_1^2 + \lambda_2^2 - \lambda_1\lambda_2 = \mathrm{Tr}\big(\rho_{AB}\tilde{\rho}_{AB}\big) - \lambda_1\lambda_2 \\ &\leq \mathrm{Tr}\big(\rho_{AB}\tilde{\rho}_{AB}\big). \end{aligned} \tag{3.29}$$

This estimation can be done for τ_{AC} accordingly resulting in

$$\tau_{AB}(\rho) + \tau_{AC}(\rho) \leq \mathrm{Tr}\big(\rho_{AB}\tilde{\rho}_{AB}\big) + \mathrm{Tr}\big(\rho_{AC}\tilde{\rho}_{AC}\big). \tag{3.30}$$

Evaluating the term $\mathrm{Tr}\big(\rho_{AB}\tilde{\rho}_{AB}\big) + \mathrm{Tr}\big(\rho_{AC}\tilde{\rho}_{AC}\big)$ using the coefficients of the density matrix we can simplify eq. (3.30) above to [35]

$$\tau_{AB}(\rho) + \tau_{AC}(\rho) \leq 4 \det \mathrm{Tr}_B(\rho). \tag{3.31}$$

Further, the relation between two qubits and the remaining one can be described as $\tau_{A|BC}$ which is also equal to $4 \det \mathrm{Tr}_B(\rho)$ such that

$$\tau_{AB}(\rho) + \tau_{AC}(\rho) \leq \tau_{A|BC}(\rho). \tag{3.32}$$

To make this inequality an equation the difference of the two sides is of interest, which is called the *residual tangle* τ_{ABC}. This quantity can be interpreted as the amount of entanglement between qubits A and BC which can not be characterized by τ_{AB} and τ_{AC}. Therefore, $\tau_{A|BC}$ can be written as

$$\tau_{A|BC}(\rho) = \tau_{AB}(\rho) + \tau_{AC}(\rho) + \tau_{ABC}(\rho) \tag{3.33}$$

or alternatively, for the residual tangle

$$\tau_{ABC}(\rho) = \tau_{A|BC}(\rho) - \tau_{AB}(\rho) - \tau_{AC}(\rho). \tag{3.34}$$

Thus, the residual tangle characterizes the relation between all three qubits of the state ρ and also stays unchanged under permutation of the qubits.

The main advantage of the tangle is that in [35] a closed form for the residual tangle τ_{ABC} based on the coefficients of the density matrix of ρ is given, which is

$$\tau_{ABC}(\rho) = 2\Big|\sum a_{\alpha_1\alpha_2\alpha_3} a_{\beta_1\beta_2\beta_3} a_{\gamma_1\gamma_2\gamma_3} a_{\delta_1\delta_2\delta_3} \epsilon_{\alpha_1\beta_1} \epsilon_{\alpha_2\beta_2} \epsilon_{\gamma_1\delta_1} \epsilon_{\gamma_2\delta_2} \epsilon_{\alpha_3\gamma_3} \epsilon_{\beta_3\delta_3}\Big| \tag{3.35}$$

where $\rho = |\varphi\rangle\langle\varphi|$ and $|\varphi\rangle = \sum a_{i_1 i_2 i_3} |i_1 i_2 i_3\rangle$. Further, the terms $\epsilon_{01} = -\epsilon_{10} = 1$ and $\epsilon_{00} = \epsilon_{11} = 0$. Since the other coefficients of eq. (3.34) are also easy to compute this makes the tangle a very powerful tool to describe pure state entanglement between three qubits.

In their article [35] Coffman et al. suggested that the tangle can be generalized to handle a multipartite version of the W-state. Wong and Christensen defined in an article a version the tangle for higher qubit systems, called the *n-tangle* [165] where n indicates the number of qubits of the analyzed state. The closed form of the residual tangle τ_{ABC} presented in eq. (3.35) can be extended from 3 to n qubits as given in [165]

$$\begin{aligned}\tau_{1\ldots n}(\rho) = 2\Big|\sum & a_{\alpha_1\ldots\alpha_n} a_{\beta_1\ldots\beta_n} a_{\gamma_1\ldots\gamma_n} a_{\delta_1\ldots\delta_n} \\ & \epsilon_{\alpha_1\beta_1}\ldots\epsilon_{\alpha_{n-1}\beta_{n-1}} \epsilon_{\gamma_1\delta_1}\ldots\epsilon_{\gamma_{n-1}\delta_{n-1}} \epsilon_{\alpha_n\gamma_n} \epsilon_{\beta_n\delta_n}\Big|\end{aligned} \tag{3.36}$$

for all even n. Wong and Christensen showed in their article that only even n can be used since the equation is in general not invariant under permutations for odd $n > 3$ which makes it infeasible as a entanglement measure for states with an odd number of qubits.

Wong and Christensen also proposed a generalization of the n-tangle to mixed states [165]. Therefore, they used the convex roof approach resulting in

$$\tau^{\min}_{1\ldots n}(\rho) = \min \sum_i p_i \tau_{1\ldots n}(|\varphi_i\rangle) \tag{3.37}$$

where the minimum goes over all possible pure state decompositions of ρ, where $\rho = \sum p_i |\varphi_i\rangle\langle\varphi_i|$.

The versions of the n-tangle for pure and mixed states are closely related to the concurrence and further to the entanglement of formation and thus describe a good measure of entanglement for multipartite systems. Nevertheless, one drawback is that the n-tangle is in general not defined for odd $n > 3$. Additionally, the n-tangle is only defined for subsystems that are qubits.

3.4.3 Huber-Hiesmayr Measure

In an article from 2008, Huber and Hiesmayr proposed an entanglement measure for any discrete multipartite system [66] based on a generalization of the concurrence defined on two systems [67]. The authors showed that the total amount of entanglement can be described using the sum over the m-flip concurrence as defined below, in detail

$$E\big(\rho\big) = C^2_{(2)}\big(\rho\big) + C^2_{(3)}\big(\rho\big) + \cdots + C^2_{(m)}\big(\rho\big). \tag{3.38}$$

Here, $E(\rho)$ denotes the amount of entanglement of ρ. This makes it possible to separate the entanglement $E(\rho)$ into 2-, 3-, ..., m-flip entanglement. Furthermore, for special cases $E(\rho)$ can be interpreted as the sum of 2-, 3-, ... and m-partite entanglement. Looking at three qubits the amount of entanglement can be defined as

$$E\big(\rho\big) = E_{(2)}\big(\rho\big) + E_{(3)}\big(\rho\big) \tag{3.39}$$

with $E_{(n)}(\rho)$ describing the n-partite entanglement. For $n = 2$ this is defined as

$$E_{(2)}\big(\rho\big) = E_{(12)}\big(\rho\big) + E_{(23)}\big(\rho\big) + E_{(13)}\big(\rho\big). \tag{3.40}$$

To define the m-flip concurrence the authors introduce the entanglement of a state as the sum of the mixedness of all its subsystems, i.e.

$$E\big(\rho\big) = \sum_{s=1}^{n} M^2\big(\rho_s\big) = \sum_{s=1}^{n} M_s^2\big(\rho\big) \tag{3.41}$$

where ρ_s is the subsystem s given by the partial trace on ρ. Further, the squared mixedness M is defined on the one hand as

$$M^2\big(\rho\big) = \frac{d}{d-1}\Big(1 - \mathrm{Tr}\big(\rho^2\big)\Big) \tag{3.42}$$

where d is the dimension of the state, e.g. $d = 2$ for qubits. On the other hand the squared mixedness of a subsystem s can be defined by flipping, i.e. using the Pauli operation σ_x in the qubit case, in any other subsystem $s' \neq s$ of the state and in all subsystems [66]. Hence, $E(\rho)$ can be described as the sum of all terms containing two flips, all terms containing three flips and so on. These terms are then denoted by $C^2_{(m)}$ which is the definition of the *m-flip concurrence*. For pure states this is

$$C^2_{(m)}\big(|\psi\rangle\big) = \sum_{\{\alpha_j\}} \sum_{i\in\{\alpha\}} \sum_{\{i_n\}\neq\{i'_n\}} \Big|\langle\psi|\hat{O}_{\{\alpha_j\}}\big(|\{i_n\}\rangle\langle\{i_n\}| - |\{i'_n\}\rangle\langle\{i'_n\}|\big)|\psi\rangle^*\Big|^2 \tag{3.43}$$

Here, $\{\alpha_j\} = \{\alpha_1, \alpha_2, \ldots \alpha_m\}$ is the set of all possible permutations of m flips in n systems such that α_j denotes the system of the flip. Similarly, $|\{i_n\}\rangle$ denotes the state $|i_1 i_2 \ldots i_n\rangle$. For every $i \in \{\alpha_j\}$, $\{i_n\} \neq \{i'_n\}$ denotes that for all systems s where a flip takes place $i_s \neq i'_s$ and for all systems t where no flip takes place $i_t = i'_t$. The operator $\hat{O}$ is a tensor product having σ_x in the system α_j and the identity $\mathbb{1}$ everywhere else. As pointed out in [66] the flip operations are in general the d dimensional symmetric Gellman matrices and reduce to the Pauli operations for $d = 2$. In the general case there are also two additional sums over all dimensions which can be omitted in the qubit case. Using the definition of the m-flip concurrence $C^2_{(m)}$ the entanglement measure for pure states is given as

$$E\big(|\psi\rangle\big) = \sum_{m=2}^{n} C^2_{(m)}\big(|\psi\rangle\big). \tag{3.44}$$

It has to be stressed that for a system of 2 qubits this reduces to the concurrence introduced by Hill and Wootters [67] multiplied by a factor of 2.

Nevertheless, the m-flip concurrence does not describe the m-partite entanglement. As it is pointed out in [66] the m-flip concurrence is also not invariant under local operations but can be altered to gain this property and thus describe also m-partite entanglement. For the three-qubit case this leads to

$$\begin{aligned} E_{(2)}\big(|\psi\rangle\big) &= E_{(12)}\big(|\psi\rangle\big) + E_{(23)}\big(|\psi\rangle\big) + E_{(13)}\big(|\psi\rangle\big) \\ &= C^2_{(2)}\big(\mathrm{Tr}_3(|\psi\rangle\langle\psi|)\big) + C^2_{(2)}\big(\mathrm{Tr}_1(|\psi\rangle\langle\psi|)\big) + C^2_{(2)}\big(\mathrm{Tr}_2(|\psi\rangle\langle\psi|)\big) \\ E_{(m)}\big(|\psi\rangle\big) &= \max\Big[C^2_{(m)}\big(|\psi\rangle\big) + C^2_{(m-1)}\big(|\psi\rangle\big), E_{(m-1)}\big(|\psi\rangle\big)\Big] - E_{(m-1)}\big(|\psi\rangle\big) \end{aligned} \tag{3.45}$$

with $m \geq 3$. The main argument is that the amount of entanglement of any subsystem is caculated by ignoring the other subsystems.

The m-flip concurrence can also be defined for mixed states using the convex roof construction [66]

$$C^2_{(m)}\big(\rho\big) = \inf_{p_i,|\psi_i\rangle} \sum_{p_i,|\psi_i\rangle} p_i C^2_{(m)}\big(|\psi_i\rangle\big) \tag{3.46}$$

which consequently gives the entanglement measure following eq. (3.44) as

$$E\big(\rho\big) = \sum_{m=2}^{n} C^2_{(m)}\big(\rho\big). \tag{3.47}$$

The main advantage of this measure compared to e.g. the entanglement of formation is that the m-flip concurrence can be computed easily and thus the measure presented by Huber and Hiesmayr is a practicable multipartite and multidimensional entanglement measure.

Chapter 4

Entanglement Purification

In the last chapter, we presented the framework of entanglement measures, which enables us to characterize how entangled two qubits are. Nevertheless, for communication protocols it is not only necessary to detect a decrease of entanglement but also to have a method to repair the tampered states and regain the entanglement. This is achieved by *entanglement purification protocols* which enable two communication parties to recover as much entanglement as they need for their communication protocol by the use of some of the transmitted states.

4.1 Models of Quantum Channels

4.1.1 Perfect and Noisy Channels

When looking at classical communication we know that information is altered when traveling through a channel due to noise effects. There are several models representing noisy channels of which the *binary symmetric channel* is the simplest and most commonly used one. In this model the noise is described by a flip of one bit from 0 to 1 and vice versa with probability $1 - p$, cf. figure 4.1. Although it is a rather elementary model of noise in a channel it is sufficient for our further needs.

In classical communication theory there has been extensive research to overcome these errors to successfully transmit a message over a noisy channel. As a result the field of *error correction* has been established and algorithms have been developed which can detect and correct errors. One simple example for such an error correcting code is the repetition code, where a single bit is just repeated several times to create

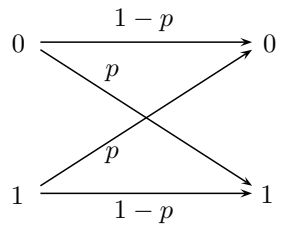

Figure 4.1: *(Binary Symmetric Channel)* Schematic depiction of the classical binary symmetric channel.

redundancy in the transmission. From this redundancy the receiving party can deduce the original bit. A good description of other codes for error correction as well as the theoretical foundations behind them are, for example, given in [161].

In the quantum world, the qubits traveling in a quantum channel are also altered due to their interaction with the environment. One severe problem is that the information stored in qubits is much more fragile than in the classical case. Therefore, immediately three major problems arise

- Qubits can not be copied unless their exact state is known, as pointed out in the *no-cloning theorem* [166]. Thus, an amplification or repetition of the quantum signal is not possible.

- The measurement of a qubit destroys the information it contains. Therefore, it is not possible to measure qubits to obtain the exact state for repetition since all information will be lost. This is another important point against amplification of a quantum signal.

- Qubits live in a continuous state space whereas classical bits only have two discrete states, 0 and 1. That means also the errors effecting the qubits are continuous. Where in the classical case only a bit flip can occur, in the quantum case the information can be altered in many different ways.

Fortunately, these drawbacks are not that severe as it may seem and communication over noisy quantum channels is also possible in the quantum world. In fact, there are two possible ways to overcome the effects of noise based on the carrier of information that is used. If just single qubits are transmitted over a channel then the information can be recovered using *quantum error correction* [136, 14]. Such algorithms use the fact that every possible error in the quantum case can be described by a linear

combination of bit flip and phase flip errors. Since we focus in this work on entangled qubits we will not go into detail on error correction but leave the interested reader with references to [139, 88, 86].

If the carrier of information is entanglement then *entanglement purification* is used to correct the error introduced by noise. The main idea is to use a number of entangled states influenced by noise and generate a fewer number of pure states out of them. Protocols for entanglement purification have been introduced by Bennett et al. [12, 14] and are described in detail in section 4.3.

4.1.2 Quantum Noisy Channel Model

Taking some quantum system S and a state ρ_S in this system, the evolution of ρ_S to ρ'_S can be described by some map $\mathcal{N}_S$, i.e.

$$\rho_S \overset{\mathcal{N}_S}{\longmapsto} \rho\prime_S. \tag{4.1}$$

In the most general case $\mathcal{N}_S$ is subject to the following constraints [131]

- $\mathcal{N}_S$ has to be linear in the density operators, i.e. for $\rho_S = p_1\sigma_S + p_2\delta_S$

$$\begin{aligned} \mathcal{N}_S\big(\rho_S\big) &= p_1\sigma'_S + p_2\delta'_S \\ &= p_1\mathcal{N}_S\big(\sigma_S\big) + p_2\mathcal{N}_S\big(\delta_S\big) \end{aligned} \tag{4.2}$$

- $\mathcal{N}_S$ has to be trace preserving, i.e. $\mathrm{Tr}\rho_S = \mathrm{Tr}\rho'_S = 1$.
- $\mathcal{N}_S$ has to be positive, i.e. if ρ_S is positive, then ρ'_S has to be positive, too.
- $\mathcal{N}_S$ has to be completely positive, i.e. for any composite system $S \otimes E$ the operator $\mathcal{N}_S \otimes \mathbb{1}_E$ is positive. That means, adjoining a system E (e.g. describing the environment) does not change the operator $\mathcal{N}_S$ up to an trivial component (the system E is left untouched).

With the first three constraints it is assured that $\mathcal{N}_S$ maps normalized density operators on normalized density operators. The fourth describes the need that $\mathcal{N}_S$ has to be positive also with respect to a larger system. In [132] a quantum information theory is described which deals with the information processing in the quantum world. Besides our explanations here we would like to refer to this article for further details.

Since the effect of noise on a quantum state ρ_S is nothing else than the evolution of ρ_S to ρ'_S it can be described by the superoperator $\mathcal{N}_S$. Especially, all unitary operations U_S of the form

$$\rho'_S = U_S \rho_S U_S^\dagger \tag{4.3}$$

fulfill the four constrains stated above. But also unitary operations that interact with an environmental system E are included. That means, assuming the environment to be in the state $|0\rangle_E$, there are unitary operations U_{SE} on the joint system which fulfill

$$\mathcal{N}_S(\rho_S) = \mathrm{Tr}_E\Big(U_{SE}(\rho_S \otimes |0\rangle\langle 0|)U_{SE}^\dagger\Big) \tag{4.4}$$

Alternatively, the superoperator describing the noise can be represented in operator-sum form, which is

$$\mathcal{N}_S(\rho_S) = \sum_i A_i \rho_S A_i^\dagger. \tag{4.5}$$

Here, the A_i are all operators acting on the system S fulfilling the condition

$$\sum_i A_i^\dagger A_i = 1 \tag{4.6}$$

Based on this representation of noise we will discuss in the following paragraphs some models of quantum channels, which are commonly used in literature.

4.1.3 One-Pauli Channel

The simplest model of a noisy channel is the *one-Pauli channel* [146]. In this model the qubit going through the noisy channel is affected by a single Pauli operation σ, i.e.

$$\rho \overset{\sigma}{\longmapsto} \rho', \tag{4.7}$$

where σ is either σ_x, σ_y or σ_z.

Taking the Pauli operator σ_x the corresponding quantum channel is called a *bit flip channel* which means the state $|0\rangle$ is flipped to $|1\rangle$ and vice versa with probability $1-p$ (cf. picture (1) in figure 4.2). The state passes the channel unchanged with probability p. Using the operator sum representation from above this can be written as

$$A_0 = \sqrt{p}\,\mathbb{1} = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad A_1 = \sqrt{1-p}\,\sigma_x = \sqrt{1-p}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{4.8}$$

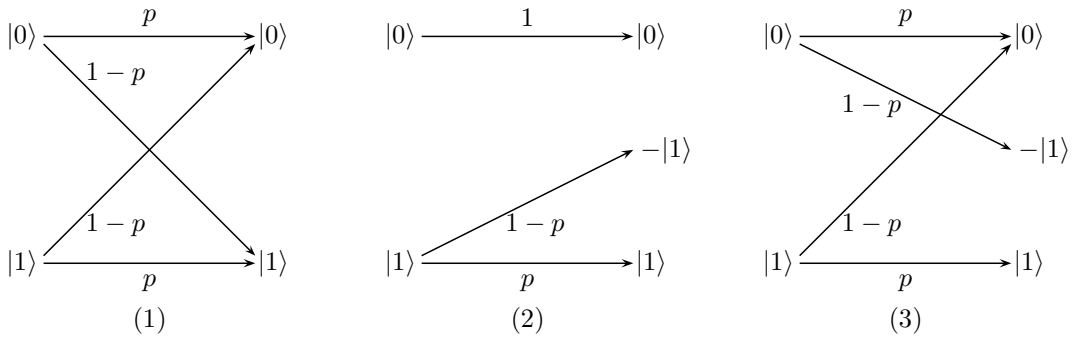

Figure 4.2: *(One-Pauli Channel)* Simplified overview of the one-Pauli channel. Picture (1) represents the σ_x operation (bit flip), picture (2) the σ_z operation (phase flip) and picture (3) the σ_y operation (combined bit and phase flip).

which leads directly to $\mathcal{N}(\rho)$ describing the noise

$$\mathcal{N}\big(\rho\big) = p\,\rho + \big(1-p\big)\,\sigma_x\rho\sigma_x \tag{4.9}$$

The quantum channel is called a *phase flip channel*, if the Pauli operation is σ_z (cf. picture (b) in figure 4.2). With probability $1-p$ this alters the phase of $|1\rangle$ to $-|1\rangle$ and of $-|1\rangle$ to $|1\rangle$. Again, the state remains unchanged with probability p. Taking the operator sum notation we have

$$A_0 = \sqrt{p}\,\mathbb{1} = \sqrt{p}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \qquad A_1 = \sqrt{1-p}\,\sigma_z = \sqrt{1-p}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \tag{4.10}$$

and for the illustration of the noise

$$\mathcal{N}\big(\rho\big) = p\,\rho + \big(1-p\big)\,\sigma_z\rho\sigma_z \tag{4.11}$$

The third possibility is a combination of the two channels mentioned above, the *bit-phase flip channel*. In this case the qubit going through the quantum channel is flipped from $|0\rangle$ to $|1\rangle$ and vice versa as well as phase flipped, i.e. from $|1\rangle$ to $-|1\rangle$ with probability $1-p$ (cf. picture (c) in figure 4.2). The state leaves the channel unchanged with probability p, respectively. Analogous from above, we get the operators

$$A_0 = \sqrt{p}\,\mathbb{1} = \sqrt{p}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \qquad A_1 = \sqrt{1-p}\,i\sigma_x\sigma_z = \sqrt{1-p}\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} \tag{4.12}$$

for the operator-sum representation of the noise induced by the channel

$$\mathcal{N}\big(\rho\big) = p\,\rho + \big(1-p\big)\,\sigma_y\rho\sigma_y \tag{4.13}$$

4.1.4 Two-Pauli channel

Similar to the One-Pauli channel the *two-Pauli channel* is characterized by the simultaneous application of two Pauli operators on the state passing the channel [145]. In detail, this is

$$A_0 = \sqrt{p}\,\mathbb{1} \qquad A_1 = \sqrt{\frac{1}{2}(1-p)}\,\sigma_1 \qquad A_2 = \sqrt{\frac{1}{2}(1-p)}\,\sigma_2 \tag{4.14}$$

where σ_1 and σ_2 are chosen from the three Pauli operators.

There are again 3 possible combinations of Pauli operations for the Two-Pauli channel. The first is where $\sigma_1 = \sigma_x$ and $\sigma_2 = \sigma_z$ which means the state passes the channel unchanged with probability p, and with probability $1/2(1-p)$ either a bit flip or a phase flip occurs. The operator representation for that is

$$A_0 = \sqrt{p}\,\mathbb{1} \qquad A_1 = \sqrt{\frac{1}{2}(1-p)}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \qquad A_2 = \sqrt{\frac{1}{2}(1-p)}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix} \tag{4.15}$$

bringing the noise $\mathcal{N}(\rho)$ to the form

$$\mathcal{N}\big(\rho\big) = p\,\rho + \frac{1-p}{2}\big(\sigma_x\rho\sigma_x + \sigma_z\rho\sigma_z\big) \tag{4.16}$$

Similarly, if $\sigma_1 = \sigma_x$ and $\sigma_2 = \sigma_y$ the state in transit is either changed by a bit flip or a combined bit and phase flip with probability $1/2(1-p)$. Therefore, we have

$$A_0 = \sqrt{p}\,\mathbb{1} \qquad A_1 = \sqrt{\frac{1}{2}(1-p)}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \qquad A_2 = \sqrt{\frac{1}{2}(1-p)}\begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} \tag{4.17}$$

describing the noise $\mathcal{N}(\rho)$ in the operator-sum form

$$\mathcal{N}\big(\rho\big) = p\,\rho + \frac{1-p}{2}\big(\sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y\big) \tag{4.18}$$

The third model where $\sigma_1 = \sigma_z$ and $\sigma_2 = \sigma_y$ representing a phase flip and a combined phase and bit flip with probability $1/2(1-p)$ is defined analog.

4.1.5 Depolarizing Channel

The most general and most important model of a quantum channel is the *depolarizing channel* [15, 144, 54]. In this model the noise of the channel depolarizes the qubit completely thus bringing it into the maximally mixed state $\mathbb{1}/2$. This brings us directly to the description of the noise $\mathcal{N}(\rho)$

$$\mathcal{N}(\rho) = p\,\rho + (1-p)\frac{\mathbb{1}}{2} \tag{4.19}$$

Obviously, this is not in the operator-sum form but it can be easily brought into this form using the representation

$$\frac{\mathbb{1}}{2} = \frac{\rho + \sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z}{4}. \tag{4.20}$$

Using this representation for $\mathbb{1}/2$ in the above equation, we get for the noise $\mathcal{N}(\rho)$

$$\mathcal{N}(\rho) = \frac{1+3p}{4}\,\rho + \frac{1-p}{4}\big(\sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z\big) \tag{4.21}$$

Usually, the depolarizing channel is parameterized in a different way, relying also on the Pauli operations. In this case the channel is described as leaving the state in transit unchanged with probability α and applying the σ_x, σ_y and σ_z operation each with probability $(1-\alpha)/3$. In detail, this means

$$\mathcal{N}(\rho) = \alpha\,\rho + \frac{1-\alpha}{3}\big(\sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z\big). \tag{4.22}$$

Comparing eq. (4.22) and eq. (4.21) we directly compute $\alpha = (1+3p)/4$. The respective operators for this representation are

$$\begin{aligned} A_0 &= \sqrt{\alpha}\,\mathbb{1} & A_1 &= \sqrt{\frac{1}{3}(1-\alpha)}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ A_2 &= \sqrt{\frac{1}{3}(1-\alpha)}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} & A_3 &= \sqrt{\frac{1}{3}(1-\alpha)}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned} \tag{4.23}$$

As we will see later on, the output of this channel is a Werner state [162], which is used heavily in the following analyses.

4.2 Building Blocks of Entanglement Purification

4.2.1 Bell-Diagonal States and Werner States

The states observed in entanglement purification protocols are mixed states since a noisy quantum channel corrupts the initially pure state as we have shortly described in section 4.1 above. Based on the models of quantum channels from above the most commonly used states are the so called *Bell-diagonal states*. Such states are a mixture of all four Bell states weighted with a certain probability, i.e.

$$W = p_1\,|\Phi^+\rangle\langle\Phi^+| + p_2\,|\Phi^-\rangle\langle\Phi^-| + p_3\,|\Psi^+\rangle\langle\Psi^+| + p_4\,|\Psi^-\rangle\langle\Psi^-| \tag{4.24}$$

where $\sum p_i = 1$ and $p_i \geq 0$. A Bell-diagonal state can be considered as coming from a very general depolarizing channel, i.e. it is affected by each of the 4 Pauli operations to a certain degree. The most studied special case of a Bell-diagonal state is the *Werner state* [162], which is heavily used in connection with entanglement purification. A Werner state is characterized only by one parameter F instead of four and is written as

$$W_F = \mathrm{F}|\Psi^-\rangle\langle\Psi^-| + \frac{1-\mathrm{F}}{3}\Big(|\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+|\Big). \tag{4.25}$$

The parameter F of the Werner state describes its fidelity $\mathrm{F} = \langle\Psi^-|W_F|\Psi^-\rangle$ relative to the initial pure state $|\Psi^-\rangle$. Also the connection to the depolarizing channel is much more obvious for a Werner state. Looking at eq. (4.22) we immediately see that a Werner state is described by a mixture of the pure state $|\Psi^-\rangle$ and some white noise

$$W_F = p\,|\Psi^-\rangle\langle\Psi^-| + \big(1-p\big)\,\frac{\mathbb{1}}{4} \tag{4.26}$$

with $p = (4\mathrm{F}-1)/3$. As already described above the identity operator $\mathbb{1}$ is just another notation for the sum of all four Bell states

$$\mathbb{1} = |\Phi^+\rangle\langle\Phi^+| + |\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|. \tag{4.27}$$

The $\mathbb{1}/4$ is the completely mixed state of two qubits, i.e. a state consisting of all four Bell states with equal probability which indicates that every information about the initial state is completely lost. As we will describe in the next section every Bell-diagonal state can be brought into a Werner form using a number of *twirl operations*.

4.2.2 Unilateral and Bilateral Operations

In the process of entanglement purification Bell states sometimes have to be mapped onto other Bell states to perform some operations correctly. This is especially the case when dealing with a Werner state, which is in a mostly $|\Psi^-\rangle\langle\Psi^-|$ form but should be brought, for example, into a mostly $|\Phi^+\rangle\langle\Phi^+|$ form to continue with the operations. This can be achieved by unilateral rotations of the angle π on one qubit of a Bell state, bilateral $\pi/2$ rotations on both qubits of a Bell state or a bilateral controlled NOT operation on two Bell states.

The simplest form of a mapping of Bell states onto Bell states are the unilateral rotations of the angle π. These rotations correspond to the Pauli operations σ_x, σ_y

and σ_z, where the σ_i describes a rotation about the i-axis. The general representation of such a rotation operator is

$$\begin{aligned} \mathrm{R}_x(\theta) &= \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \\ \mathrm{R}_y(\theta) &= \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \\ \mathrm{R}_z(\theta) &= \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix} \end{aligned} \tag{4.28}$$

which leads to the Pauli operations already defined throughout section 4.1

$$\begin{aligned} \sigma_x &= i\mathrm{R}_x(\pi) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_y &= i\mathrm{R}_y(\pi) = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ \sigma_z &= i\mathrm{R}_z(\pi) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned} \tag{4.29}$$

The Pauli operators – together with the identity matrix $\mathbb{1}$ – map the 4 Bell states onto one another when applied on one qubit. For example, giving $|\Phi^+\rangle$, σ_x applied on the first qubit changes the state into $|\Psi^+\rangle$, σ_y maps it onto $|\Psi^-\rangle$ and σ_z brings the state to $|\Phi^-\rangle$, i.e.

$$\begin{aligned} (\sigma_x \otimes \mathbb{1})|\Phi^+\rangle &= \frac{1}{\sqrt{2}}\Big((\sigma_x|0\rangle)|0\rangle + (\sigma_x|1\rangle)|1\rangle\Big) = |\Psi^+\rangle \\ (\sigma_y \otimes \mathbb{1})|\Phi^+\rangle &= \frac{1}{\sqrt{2}}\Big((\sigma_y|0\rangle)|0\rangle + (\sigma_y|1\rangle)|1\rangle\Big) = -i|\Psi^-\rangle \\ (\sigma_z \otimes \mathbb{1})|\Phi^+\rangle &= \frac{1}{\sqrt{2}}\Big((\sigma_z|0\rangle)|0\rangle + (\sigma_z|1\rangle)|1\rangle\Big) = |\Phi^-\rangle \end{aligned} \tag{4.30}$$

In some cases the resulting state has a global phase, in this case $-i$ for σ_y, which can be neglected when dealing with purification protocols. An overview of the mapping of all Bell states is given in table 4.1. As already pointed out, these mappings using Pauli operations are often used to bring a Werner state of a mostly $|\Psi^-\rangle\langle\Psi^-|$ form (c.f eq. (4.25)) into a mostly $|\Phi^+\rangle\langle\Phi^+|$ form and vice versa to correctly apply the twirl-operation as mentioned above. In detail,

$$(\sigma_y\otimes\mathbb{1})W_F(\sigma_y\otimes\mathbb{1}) = \mathrm{F}|\Phi^+\rangle\langle\Phi^+| + \frac{1-\mathrm{F}}{3}\Big(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|\Big) \tag{4.31}$$

	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
$\mathbb{1}$	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
σ_x	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$
σ_y	$\|\Psi^-\rangle$	$\|\Psi^+\rangle$	$\|\Phi^-\rangle$	$\|\Phi^+\rangle$
σ_z	$\|\Phi^-\rangle$	$\|\Phi^+\rangle$	$\|\Psi^-\rangle$	$\|\Psi^+\rangle$

Table 4.1: Mapping of Bell states onto Bell states using Pauli operations. Global phases are omitted.

A second way to realize a mapping from one Bell state onto another is a bilateral $\pi/2$ rotation, i.e. applying a rotation of an angle $\pi/2$ on both qubits of a Bell state. These operations follow directly from the general rotation operations described in eq. (4.28) and can be written as

$$B_x = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i \\ -i & 1 \end{pmatrix} \quad B_y = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \quad B_z = \frac{1}{\sqrt{2}}\begin{pmatrix} e^{3i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} \tag{4.32}$$

The effect of the $\pi/2$ rotation on the Bell state $|\Phi^+\rangle$ is then

$$\begin{aligned} \big(B_x \otimes B_x\big)|\Phi^+\rangle &= \frac{1}{\sqrt{2}}\Big(B_x|0\rangle B_x|0\rangle + B_x|1\rangle B_x|1\rangle\Big) = -i|\Psi^+\rangle \\ \big(B_y \otimes B_y\big)|\Phi^+\rangle &= \frac{1}{\sqrt{2}}\Big(B_y|0\rangle B_y|0\rangle + B_y|1\rangle B_y|1\rangle\Big) = |\Phi^+\rangle \\ \big(B_z \otimes B_z\big)|\Phi^+\rangle &= \frac{1}{\sqrt{2}}\Big(B_z|0\rangle B_z|0\rangle + B_z|1\rangle B_z|1\rangle\Big) = i|\Phi^-\rangle. \end{aligned} \tag{4.33}$$

From this equation we see that the map does not reach all four Bell states but only $|\Phi^+\rangle$, $|\Phi^-\rangle$ and $|\Psi^+\rangle$ (up to a global phase) if $|\Phi^+\rangle$ is used. In fact, each of the three operations maps one Bell state onto one of three Bell states but never onto the state $|\Psi^-\rangle$. $|\Psi^-\rangle$ is completely untouched by the operators B_x, B_y and B_z and maps only onto itself, as it can be seen in table 4.2.

An application of these rotation operators is to bring an arbitrary mixed state into a Werner form using the so called *twirl operation* [14, 12]. The twirl is a random combination of 12 SU(2) operations consisting of the B_x, B_y and B_z operators, i.e.

$$\begin{aligned} &U_1 = \mathbb{1} && U_2 = B_xB_x && U_3 = B_yB_y && U_4 = B_zB_z \\ &U_5 = B_xB_y && U_6 = B_yB_z && U_7 = B_zB_x && U_8 = B_yB_x \\ &U_9 = B_xB_yB_xB_y && U_{10} = B_yB_zB_yB_z && U_{11} = B_zB_xB_zB_x && U_{12} = B_yB_xB_yB_x \end{aligned} \tag{4.34}$$

	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
$\mathbb{1}$	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$
B_x	$\|\Psi^+\rangle$	$\|\Phi^-\rangle$	$\|\Phi^+\rangle$	$\|\Psi^-\rangle$
B_y	$\|\Phi^+\rangle$	$\|\Psi^+\rangle$	$\|\Phi^-\rangle$	$\|\Psi^-\rangle$
B_z	$\|\Phi^-\rangle$	$\|\Phi^+\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$

Table 4.2: Mapping of Bell states onto Bell states using $\pi/2$ rotations. Global phases are omitted.

such that the overall twirl operation U can be described as

$$U = \frac{1}{12}\sum_{i=1}^{12} U_i \tag{4.35}$$

The twirl has the effect of removing the off-diagonal elements of a mixed state thus bringing it into a Werner form. As it is described in the detailed purification protocols below the Werner form is needed to guarantee that the fidelity reaches 1 in the asymptotic limit.

To interchange between the Bell states as it can be done with Pauli operations is a much more difficult task using only $\pi/2$ rotations, since the state $|\Psi^-\rangle$ can't be reached. Furthermore, in contrary to the Pauli operators, both parties somehow have to agree upon which operation to perform if they want to alter a Bell state shared between them. This has a much higher complexity regarding the communication compared to one party using a Pauli operation to change the state.

4.2.3 Bilateral CNOT Operation

Another method to map between Bell states is to use *controlled NOT* (CNOT) operations on two Bell pairs. A controlled NOT is an operator of the form

$$\mathrm{CNOT}_{12} = |0\rangle\langle 0| \otimes \mathbb{1} + |1\rangle\langle 1| \otimes \sigma_x = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{4.36}$$

which takes the first qubit as source and the second qubit as target. If qubit 1 is $|1\rangle$ then qubit 2 is flipped, otherwise nothing happens. The CNOT operation has the

ability to entangle two qubits, i.e.

$$\mathrm{CNOT}_{12}\left(\frac{1}{\sqrt{2}}\big(|0\rangle_1 + |1\rangle_1\big) \otimes |0\rangle_2\right) = |\Phi^+\rangle_{12} \tag{4.37}$$

or, controversially, to disentangle a Bell state by applying a CNOT onto it. In the context of entanglement purification the CNOT is used to perform a test and generate, with a certain probability, an entangled pair of higher fidelity out of two input pairs. To achieve that a CNOT operation is performed by both parties involved in the protocol, hence the operation is called a *bilateral CNOT* (BCNOT). The operation is of the form

$$\begin{aligned} \mathrm{BCNOT} =& \mathrm{CNOT} \otimes \mathrm{CNOT} \\ =& |00\rangle\langle 00| \otimes \mathbb{1} \otimes \mathbb{1} + |01\rangle\langle 01| \otimes \mathbb{1} \otimes \sigma_x \\ &+ |10\rangle\langle 10| \otimes \sigma_x \otimes \mathbb{1} + |11\rangle\langle 11| \otimes \sigma_x \otimes \sigma_x . \end{aligned} \tag{4.38}$$

The BCNOT also maps the source and target state onto other Bell states as described in table 4.3. If both parties share a Werner state ρ in a mostly $|\Phi^+\rangle\langle\Phi^+|$ form we can

Source / Target	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$	
	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$	(source)
$\|\Phi^+\rangle$	$\|\Phi^+\rangle$	$\|\Phi^+\rangle$	$\|\Psi^+\rangle$	$\|\Psi^+\rangle$	(target)
	$\|\Phi^-\rangle$	$\|\Phi^+\rangle$	$\|\Psi^-\rangle$	$\|\Psi^+\rangle$	(source)
$\|\Phi^-\rangle$	$\|\Phi^-\rangle$	$\|\Phi^-\rangle$	$\|\Psi^-\rangle$	$\|\Psi^-\rangle$	(target)
	$\|\Phi^+\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	$\|\Psi^-\rangle$	(source)
$\|\Psi^+\rangle$	$\|\Psi^+\rangle$	$\|\Psi^+\rangle$	$\|\Phi^+\rangle$	$\|\Phi^+\rangle$	(target)
	$\|\Phi^-\rangle$	$\|\Phi^+\rangle$	$\|\Psi^-\rangle$	$\|\Psi^+\rangle$	(source)
$\|\Psi^-\rangle$	$\|\Psi^-\rangle$	$\|\Psi^-\rangle$	$\|\Phi^-\rangle$	$\|\Phi^-\rangle$	(target)

Table 4.3: Mapping of Bell states onto Bell states using BCNOT operations. Global phases are omitted.

directly compute, based on this mapping, the resulting state after they performed

the BCNOT. This is the state $\delta = \mathrm{BCNOT}(\rho \otimes \rho)\mathrm{BCNOT}$, i.e.

$$\begin{aligned}
\delta = \quad & \mathrm{F}|\Phi^+\rangle\langle\Phi^+| \otimes \big(\mathrm{F}|\Phi^+\rangle\langle\Phi^+| + \frac{(1-\mathrm{F})}{3}|\Psi^+\rangle\langle\Psi^+|\big) \\
+ \; & \frac{(1-\mathrm{F})}{3}|\Phi^-\rangle\langle\Phi^-| \otimes \big(\mathrm{F}|\Phi^-\rangle\langle\Phi^-| + \mathrm{F}|\Phi^+\rangle\langle\Phi^+| \\
+ \; & \mathrm{F}|\Psi^-\rangle\langle\Psi^-| + \frac{\mathrm{F}(1-\mathrm{F})}{3}|\Psi^+\rangle\langle\Psi^+|\big) \\
+ \; & \frac{(1-\mathrm{F})}{3}|\Psi^+\rangle\langle\Psi^+| \otimes \big(\mathrm{F}|\Psi^+\rangle\langle\Psi^+| + \frac{(1-\mathrm{F})}{3}|\Phi^+\rangle\langle\Phi^+| \\
+ \; & \frac{(1-\mathrm{F})}{3}|\Phi^-\rangle\langle\Phi^-| + \frac{(1-\mathrm{F})}{3}|\Psi^+\rangle\langle\Psi^+|\big) \\
+ \; & \frac{(1-\mathrm{F})}{3}|\Psi^-\rangle\langle\Psi^-| \otimes \big(\mathrm{F}|\Psi^+\rangle\langle\Psi^+| + \frac{(1-\mathrm{F})}{3}|\Phi^+\rangle\langle\Phi^+| \\
+ \; & \frac{(1-\mathrm{F})}{3}|\Phi^-\rangle\langle\Phi^-| + \frac{(1-\mathrm{F})}{3}|\Psi^+\rangle\langle\Psi^+|\big)
\end{aligned} \tag{4.39}$$

4.2.4 Measurement in the Computational Basis

After the application of the BCNOT both parties are able to determine whether the source qubits 1 and 2 are in an entangled state by performing a measurement on the target qubits 3 and 4 in the computational basis. The operators for this measurement are

$$\begin{aligned}
M_{00} &= \mathbb{1} \otimes \mathbb{1} \otimes |00\rangle\langle 00| \qquad M_{01} = \mathbb{1} \otimes \mathbb{1} \otimes |01\rangle\langle 01| \\
M_{10} &= \mathbb{1} \otimes \mathbb{1} \otimes |10\rangle\langle 10| \qquad M_{11} = \mathbb{1} \otimes \mathbb{1} \otimes |11\rangle\langle 11|.
\end{aligned} \tag{4.40}$$

projecting qubits 3 and 4 onto the states $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$. The state δ from eq. (4.39) above has the property that qubits 1 and 2 collapse into a mixed state ρ' if Alice and Bob obtain the same result from their measurement, i.e.

$$\begin{aligned}
\rho' &= \frac{1}{\mathrm{Tr}(M_{00}^\dagger M_{00}\delta)}\big(M_{00}\delta M_{00}^\dagger\big) = \frac{1}{\mathrm{Tr}(M_{11}^\dagger M_{11}\delta)}\big(M_{11}\delta M_{11}^\dagger\big) \\
&= \frac{1}{5 - 4\mathrm{F} + 8\mathrm{F}^2}\Big[(1 - 2\mathrm{F} + 10\mathrm{F}^2)|\Phi^+\rangle\langle\Phi^+| - 6\mathrm{F}\big(\mathrm{F}-1\big)|\Phi^-\rangle\langle\Phi^-| \\
&\qquad +2\big(\mathrm{F}-1\big)^2|\Psi^+\rangle\langle\Psi^+| + 2\big(\mathrm{F}-1\big)^2|\Psi^-\rangle\langle\Psi^-|\Big].
\end{aligned} \tag{4.41}$$

This state has a fidelity $\langle\Phi^+|\rho'|\Phi^+\rangle > \langle\Phi^+|\rho|\Phi^+\rangle$ if both parties obtain the same results. In this case the source qubits are kept to use further on. If the results of the measurement are different, the state of qubits 1 and 2 is the maximally mixed state of 2 qubits, $\mathbb{1}/4$. Thus, all entanglement is lost and the source qubits have to be discarded. The probability p_{eq} of obtaining the same result, i.e. $|00\rangle$ or $|11\rangle$, from the

measurement of qubits 3 and 4 depends fully on the initial fidelity $\mathrm{F} = \langle\Phi^+|\rho|\Phi^+\rangle$ of the Werner state $\rho = |W_F\rangle\langle W_F|$. For a better understanding we will choose $\mathrm{F} = (1+3\alpha)/4$, which describes the Werner state ρ as the effect of a depolarizing channel on the entangled state $|\Phi^+\rangle$, i.e.

$$|\Phi^+\rangle\langle\Phi^+| \longmapsto \alpha|\Phi^+\rangle\langle\Phi^+| + (1-\alpha)\mathbb{1} \tag{4.42}$$

This gives for the probability p_{eq} that both parties obtain the same result

$$p_{eq} = p_{00} + p_{11} = \mathrm{Tr}\Big(M_{00}^\dagger M_{00}\Big) + \mathrm{Tr}\Big(M_{11}^\dagger M_{11}\rho\Big) = \frac{1}{2}\big(1+\alpha^2\big) \tag{4.43}$$

and, accordingly, for the probability p_{neq} that their results are different

$$p_{neq} = p_{01} + p_{10} = \mathrm{Tr}\Big(M_{01}^\dagger M_{01}\Big) + \mathrm{Tr}\Big(M_{10}^\dagger M_{10}\rho\Big) = \frac{1}{2}\big(1-\alpha^2\big). \tag{4.44}$$

It directly shows from eq. (4.43) and figure 4.3 that it is more likely for Alice and

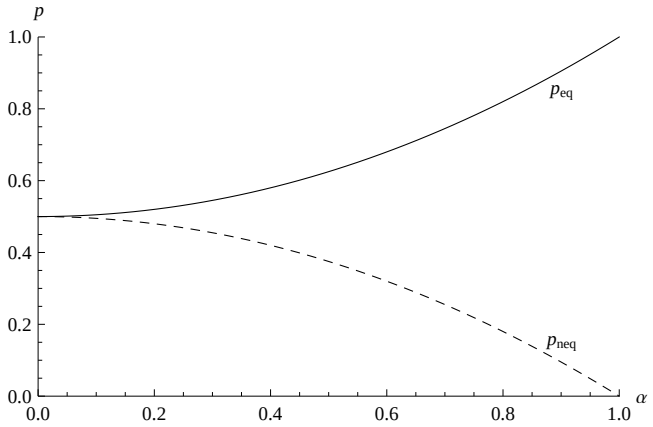

Figure 4.3: *(Probabilities in a depolarizing channel)* Alice' and Bob's probability to obtain equal (solid line) and different (dashed line) results depending on α.

Bob to obtain the same results the higher α and thus the initial fidelity F of the state ρ is. The probabilities p_{eq} and p_{neq} are the same if $\alpha = 0$ (and $\mathrm{F} = 0.25$, respectively) and the resulting state is just the completely mixed state $\mathbb{1}/4$. The fidelity $F' = \langle\Phi^+|\rho'|\Phi^+\rangle$ is higher than the fidelity $F = \langle\Phi^+|\rho|\Phi^+\rangle$ of the initial state only if $\langle\Phi^+|\rho|\Phi^+\rangle > 0.5$ which is the minimal fidelity F_{min} required for purification of Bell states. Regarding the coefficient α from the depolarizing channel model this means

$$\mathrm{F} = \frac{1+3\alpha}{4} < \frac{1+2\alpha+5\alpha^2}{4+4\alpha^2} = \mathrm{F}' \quad \longmapsto \quad \alpha < \frac{2\alpha+4\alpha^2}{3+3\alpha^2} = \alpha' \tag{4.45}$$

which is valid for $\alpha > 1/3$ (and $F > 1/2$), as it is given in figure 4.4. It has also been shown [42] that the fidelity $\langle\Phi^+|\rho'|\Phi^+\rangle$ approaches 1 in the asymptotic limit. Thus, it is possible to obtain the pure state $|\Phi^+\rangle$ out of infinitely many mixed states ρ, which are coming from a noisy channel.

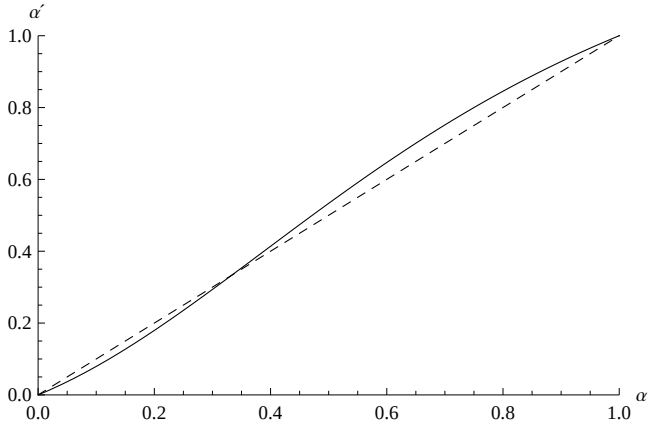

Figure 4.4: *(Fidelities in a depolarizing channel)* The coefficient after the measurement (α') in relation to the coefficient of the initial state (α). The dashed line indicates the limit $\alpha' = \alpha$ for entanglement purification.

The new state ρ' is then used in another iteration of the entanglement purification procedure and so on to generate a state arbitrarily close to the pure initial state. Alice and Bob have to be aware that the state ρ' is no longer of a Werner state form, as described in eq. (4.41). Therefore, both parties have to apply a σ_y operation to bring the state first into a mostly $|\Psi^-\rangle\langle\Psi^-|$ form and then perform the twirl operation U (c.f eq. (4.35)) which does not affect the $|\Psi^-\rangle\langle\Psi^-|$ part. Afterwards they rotate the state back to a mostly $|\Phi^+\rangle\langle\Phi^+|$ Werner form. As we will see later on it is also possible to apply a B_x operation instead of U to achieve the same effect (cf. section 4.3.1).

4.3 Entanglement Purification Protocols

In the following we will describe a number of one-way and two-way entanglement purification protocols. The terms *one-way* and *two-way* describe the way how the two parties performing the purification, Alice and Bob, communicate with each other: if they exchange information bilaterally the protocol is called two-way and

one-way otherwise. Both one- and two-way protocols start with an initial amount of n entangled states. Due to the noise coming from the channel these states are impure and in a Werner form similar to eq. (4.25),

$$\rho = \mathrm{F}|\Phi^+\rangle\langle\Phi^+| + \frac{1-\mathrm{F}}{3}\big(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|\big) \tag{4.46}$$

The general attempt is to analyze m of these pairs such that the remaining $n' = n-m$ are of a higher fidelity than the initial states. How this can be achieved is discussed in detail in the following sections.

How effective a certain purification procedure is can be measured comparing the yield of several protocols. The yield of a purification procedure is defined [14]

$$D\big(\rho\big) = \lim_{n\to\infty} \frac{n'}{n} \tag{4.47}$$

where ρ is an impure state (cf. also eq. (3.1), i.e. the definition of the entanglement of distillation). If the state is perturbed due to traveling through a quantum channel the yield $D(\rho)$ can be seen as the number of qubits that can be transmitted through this channel.

4.3.1 Recurrence Method

This purification procedure was originally described in [12] and is a two-way protocol. In this protocol Alice chooses two states at random from an ensemble of Werner states ρ. We want to remind that these states are shared between Alice and Bob and thus Alice can only act on the qubits in her possession. Both apply the BCNOT operation on their qubits which affects the corresponding qubits at Bob's side in a way described in table 4.3. After the BCNOT the two pairs are in a mixture of entangled states δ (cf. eq. (4.39)) and Alice and Bob measure the target qubits. They obtain the same results with probability

$$p_{eq} = \mathrm{Tr}\big(M_{00}\delta\big) + \mathrm{Tr}\big(M_{11}\delta\big) = \frac{1}{9}\big(5 - 4\mathrm{F} + 8\mathrm{F}^2\big) \tag{4.48}$$

similar to eq. (4.43) above and in this case keep the source pair. Otherwise they discard the two qubits from the source of the BCNOT operation. They repeat these actions for all the n initial states thus ending up with a smaller set of states ρ' (cf. eq. (4.41)) which passed their test. As pointed out in section 4.2.4 above, the fidelity $\mathrm{F}' = \langle\Phi^+|\rho'|\Phi^+\rangle$ is

$$\mathrm{F}' = \frac{1 - 2\mathrm{F} + 10\mathrm{F}^2}{5 - 4\mathrm{F} + 8\mathrm{F}^2} \tag{4.49}$$

which is, as pointed out in section 4.2.4 above, higher than the fidelity of the initial state as long as $F > F_{min} = 0.5$ but is not of a Werner form any more.

Therefore, Alice and Bob perform the bilateral *twirl operation U* from eq. (4.35) on their remaining states bringing them into Werner form again. Then, the situation is similar to the beginning and Alice and Bob start a second round of purification on the remaining n' Werner states. The fidelity of the remaining states after the second iteration increases as described in eq. (4.49). Therefore, Alice and Bob can continue their action in further iterations of the protocol to bring the fidelity arbitrarily close to 1 or until they end up with a number of states with sufficient fidelity.

As it is given in [14], there was a comment by Macchiavello regarding the twirl operation. He pointed out that the use of only the B_x operation instead of the twirl would be more efficient. Taking only the B_x operation the state is no longer of Werner form after the first iteration of the purification procedure. Nevertheless, the fidelity will not only converge to 1 in the asymptotic limit but will converge faster than in the original protocol using the twirl operation.

The recurrence method is rather inefficient since at least half of the entangled pairs have to be discarded each round because either they are measured by Alice and Bob or don't pass the test and can't be used in the next iteration. This means the yield $D_R(\rho)$ tends to 0 in the asymptotic limit, which is not a desirable case. One improvement has been described in [12] where the authors suggest that $1/\sqrt{1-F}$ states are used as source for the BCNOT operation. Using this change in the purification procedure only $(2\sqrt{1-F})/3$ pairs have to be discarded in each step and thus a positive yield can be achieved in the asymptotic limit.

4.3.2 Quantum Privacy Amplification

Another purification protocol similar to the recurrence method has been presented by Deutsch et al. [42]. They proposed a scheme called *Quantum Privacy Amplification* (QPA) referring to classical privacy amplification [13]. In their scheme Deutsch et al. start with the legitimate assumption that the Bell states shared by Alice and Bob are prepared by an adversary. Hence, both parties can not make any conjectures about their initial states, thus defining them as ρ_{12} and ρ_{34} with ρ the Bell-diagonal state

$$\rho = \alpha_1|\Phi^+\rangle\langle\Phi^+| + \alpha_2|\Phi^-\rangle\langle\Phi^-| + \alpha_3|\Psi^+\rangle\langle\Psi^+| + \alpha_4|\Psi^-\rangle\langle\Psi^-| \qquad (4.50)$$

Alice and Bob start the QPA by performing a B_x rotation (cf. eq. (4.32)), i. e. Alice applies B_x onto her qubits whereas Bob applies the inverse operation B_x^{-1}, i.e. a rotation of $-\pi/2$ about the x-axis, onto his qubits. Similar to the recurrence method described in the previous section Alice and Bob perform a bilateral CNOT operation onto $\rho_{12} \otimes \rho_{34}$ where 1 and 2 are the control qubits and 3 and 4 the target qubits. Afterwards, they measure the target qubits in the Z-basis and compare their results. If both parties obtain the same result the control qubits are kept, otherwise qubits 1 and 2 are discarded.

In detail, using the initial state $\rho \otimes \rho$ the probability for Alice and Bob to obtain coinciding results is

$$p_{eq} = \mathrm{Tr}\big(M_{00}\delta\big) + \mathrm{Tr}\big(M_{11}\delta\big) = \big(\alpha_1 + \alpha_4\big)^2 + \big(\alpha_3 + \alpha_2\big)^2 \tag{4.51}$$

In this case, Alice and Bob keep the control qubits, which have a fidelity $F' = \langle\Phi^+|\rho'|\Phi^+\rangle$ of

$$F' = \frac{\alpha_1^2 + \alpha_4^2}{(\alpha_1 + \alpha_4)^2 + (\alpha_3 + \alpha_2)^2} \tag{4.52}$$

which is larger than the original fidelity $F = \alpha_1$ if $\alpha_1 > \mathrm{F}_{min} = 1/2$. As pointed out in [42] a repeated application of the QPA on an ensemble of n qubit pairs in the state ρ increases the fidelity of the resulting state (if Alice's and Bob's result coincide) and it converges to 1.

Taking $\alpha_2 - \alpha_4$ with the same value, i.e.

$$\alpha_2 = \alpha_3 = \alpha_4 = \frac{1 - \alpha_1}{3} \tag{4.53}$$

the initial state ρ becomes a Werner state and the scheme reduces to the recurrence method. Hence, Machiavello's comment in [14] mentioned above is approved in the QPA scheme.

The scheme by Deutsch et al. [42] has been extended by Dür et al. [45] who suggested to use an auxiliary Werner state with a specific fidelity F_π as target of the BCNOT operation instead of the entangled state coming from the previous purification round. The main drawback of this alternative scheme is that it does not converge to 1 due to the fixed fidelity F_π and therefore is only applicable in scenarios where perfect entanglement is not necessary. Nevertheless, the resources needed for the purification are decreased drastically which makes it the favorable scheme for the nested purification and the quantum repeater (cf. section 4.4 below).

4.3.3 Direct Purification

Although most of the purification protocols use mixed states of a Werner form or at least of a Bell-diagonal form it is also possible to purify a state directly. This has the advantage that the entanglement is not decreased by the application of the twirling operation. Taking a mixture of an entangled state and a product state, e.g.

$$\vartheta = \frac{1}{2}|01\rangle\langle 01| + \frac{1}{2}|\Phi^+\rangle\langle\Phi^+|, \tag{4.54}$$

the state can not be purified by the recurrence method since it's fidelity $\langle\Phi^+|\vartheta|\Phi^+\rangle = 0.5$. Nevertheless, using the following procedure an ensemble of the states ϑ can be brought to $|\Phi^+\rangle$ with a certain probability. As in the recurrence method Alice and Bob randomly draw two impure pairs from the ensemble and apply a BCNOT operation on the qubits in their possession. This leads to the state

$$\begin{aligned}\vartheta' =& \mathrm{BCNOT}\Big(\vartheta \otimes \vartheta\Big) \\ =& \frac{1}{4}\Big[|01\rangle\langle 01| \otimes \big(|01\rangle\langle 01| + |\Psi^+\rangle\langle\Psi^+|\big) \\ &+ |\Phi^+\rangle\langle\Phi^+| \otimes |\Phi^+\rangle\langle\Phi^+| + |\mathrm{GHZ}_4\rangle\langle\mathrm{GHZ}_4|\Big]\end{aligned} \tag{4.55}$$

where $|\mathrm{GHZ}_4\rangle$ is the 4-qubit GHZ state $1/\sqrt{2}(|0001\rangle + |1110\rangle)$. Then they both measure their target qubits in the computational basis and publicly compare the results. It is shown from the structure of ϑ' that the source qubits will be in the entangled state $|\Phi^+\rangle$ if Alice and Bob both obtain the result $|1\rangle$ from their measurement, which happens with probability 1/8. In this case Alice and Bob will immediately end up with a pure entangled state.

This scheme can be generalized such that the initial state is

$$\vartheta = \big(1 - \mathrm{F}\big)|01\rangle\langle 01| + \mathrm{F}|\Phi^+\rangle\langle\Phi^+| \tag{4.56}$$

and the probability for Alice and Bob to obtain a pure entangled state is $\mathrm{F}^2/2$.

Since the direct purification method has only one step it is more efficient than the recurrence method. It also has to be noted that a different model of the noisy channel is used. Additionally, the procedure does not make use of the twirl operation such that no entanglement is destroyed by the bilateral rotations. Furthermore, as it is pointed out in the example, with this method Alice and Bob are able to use states with a fidelity smaller than 0.5 to generate pure states. The only drawback is that half of the qubits are useless since they are measured by Alice and Bob. This

gives an overall yield of half of the probability that Alice and Bob obtain $|11\rangle$ from their measurement, i.e. $D_D(\rho) = \mathrm{F}^2/4$.

4.3.4 Breeding Method

In the breeding method, first described in [12], Alice and Bob take advantage of a number of preshared pure entangled states to purify an ensemble of Werner states. This has the advantage that, if the fidelity of the Werner states is not too low, i.e. their von Neuman entropy is less than 1, the generation of the new entangled states will not exceed the consumption of the preshared pure states. In detail, Alice and Bob have a pool of preshared pure Bell states $|\Phi^+\rangle$ and a set of mixed state W_F. In this case the mixed states are treated as an ensemble of pure Bell states and the two parties try to bring all entangled pairs into the state $|\Phi^+\rangle$ using Pauli operations. As in the other purification procedures they make use of the BCNOT operation but this time they use the qubits coming from the quantum channel as source and one of the preshared pure states as target. As it is shown in table 4.3 if the state $|\Phi^+\rangle$ is the target of a BCNOT operation, the source stays unchanged and the target changes to $|\Psi^+\rangle$, if the source is $|\Psi^\pm\rangle$. By performing BCNOT operations on random subsets of the incoming qubit pairs Alice and Bob use this fact to apply some sort of parity check to locate all $|\Psi^\pm\rangle$ states. Then one party applies the Pauli operator σ_x on one qubit of these states to convert $|\Psi^\pm\rangle$ to $|\Phi^\pm\rangle$. Afterwards, both parties apply the bilateral B_y rotation on all qubits in their possession, which brings the states $|\Phi^-\rangle$ to $|\Psi^+\rangle$ (cf. table 4.2). Now, Alice and Bob perform another BCNOT test to identify the remaining $|\Psi^+\rangle$ states and convert them into $|\Phi^+\rangle$ using the σ_x operation.

The actions performed by Alice and Bob can also be described alternatively: The BCNOT operation applied on the Werner states together with the pure states $|\Phi^+\rangle$ as target brings the four qubits into the state

$$\begin{aligned}\rho' = \mathrm{F}|\Phi^+\Phi^+\rangle\langle\Phi^+\Phi^+| + \frac{1-\mathrm{F}}{3}\big(&|\Phi^-\Phi^+\rangle\langle\Phi^-\Phi^+| \\ &+|\Psi^+\Psi^+\rangle\langle\Psi^+\Psi^+| + |\Psi^-\Psi^+\rangle\langle\Psi^-\Psi^+|\big)\end{aligned} \tag{4.57}$$

Then, Alice and Bob use the operator

$$\begin{aligned}&\mathbb{1}\otimes\mathbb{1}\otimes|\Phi^+\rangle\langle\Phi^+| + \mathbb{1}\otimes\mathbb{1}\otimes|\Phi^+\rangle\langle\Phi^-| \\ &+\sigma_x\otimes\mathbb{1}\otimes|\Psi^+\rangle\langle\Phi^+| + \sigma_x\otimes\mathbb{1}\otimes|\Psi^-\rangle\langle\Phi^-|\end{aligned} \tag{4.58}$$

to apply the σ_x operator on the $|\Psi^{\pm}\rangle$ states exclusively. The operator in eq. (4.58) can be understood as a controlled σ_x which only acts on Alice's qubit if the target is either $|\Psi^+\rangle$ or $|\Psi^-\rangle$. This brings the state ρ' to

$$\begin{aligned}\rho'' = \mathrm{F}|\Phi^+\Phi^+\rangle\langle\Phi^+\Phi^+| + \frac{1-\mathrm{F}}{3}\big(&|\Phi^-\Phi^+\rangle\langle\Phi^-\Phi^+| \\ &+|\Phi^+\Psi^+\rangle\langle\Phi^+\Psi^+| + |\Phi^-\Psi^+\rangle\langle\Phi^-\Psi^+|\big)\end{aligned} \tag{4.59}$$

Afterwards, both parties apply the bilateral B_y operation swapping the $|\Phi^-\rangle$ to $|\Psi^+\rangle$, i.e.

$$\begin{aligned}\rho''' = \mathrm{F}|\Phi^+\Phi^+\rangle\langle\Phi^+\Phi^+| + \frac{1-\mathrm{F}}{3}\big(&|\Psi^+\Phi^+\rangle\langle\Psi^+\Phi^+| \\ &+|\Phi^+\Psi^+\rangle\langle\Phi^+\Psi^+| + |\Psi^+\Psi^+\rangle\langle\Psi^+\Psi^+|\big)\end{aligned} \tag{4.60}$$

Applying the operator from eq. (4.58) a second time switches all $|\Psi^+\rangle$ states to $|\Phi^+\rangle$ leaving the source qubits finally in the pure state $|\Phi^+\rangle$. The qubits originating from the preshared pure states have to be discarded.

We have to stress that this alternative method is just an interpretation and can not be implemented in this way. The main reason is that the operation in eq. (4.58) is acting on all four qubits, i.e. all four qubits have to be located in one place. Since Alice and Bob are separated, the implementation of this operation is not possible. Nevertheless, this alternative description gives a good hint for the idea behind the breeding method.

Regarding the efficiency of the breeding method it is stated in [12] that the yield $D_B = 1 - S(\rho)$ where S is the von Neuman entropy. As described in the article, this is based on the fact that the number of BCNOT tests to find all errors in the ensemble is $S(\rho)$ per impure pair in the asymptotic limit. For Werner states this yield can be written as

$$1 - S\big(\rho\big) = 1 + \mathrm{F}\log_2\mathrm{F} + \big(1-\mathrm{F}\big)\log_2\frac{1-\mathrm{F}}{3} \tag{4.61}$$

and becomes positive for $\mathrm{F} > 0.8107$ [12]. Using a more efficient version of the breeding protocol performing a so called partial breeding as presented in [77] the necessary fidelity for a positive yield can be reduced to $\mathrm{F} > 0.7424$.

4.4 Nested Entanglement Purification

In the description of the purification protocols above we already pointed out that the entanglement between two qubits has to be of fidelity larger than F_{min} to make

purification possible. For example, taking the recurrence method from section 4.3.1 and the quantum privacy amplification from section 4.3.2, $\mathrm{F}_{min} = 1/2$. Using an initial state with fidelity $\mathrm{F} < \mathrm{F}_{min}$ the purification procedure is going to reduce the fidelity instead of increasing it.

In a realistic environment we also have to take into account that the fidelity F of the Werner state decreases exponentially with the length l of the channel. Modeling our quantum channel as a *photonic channel* [152] it has been shown in [22] that the fidelity is given by

$$\mathrm{F} \simeq \left| \frac{1 + e^{-l/2l_c}}{2} \right|^2 \tag{4.62}$$

where l_c is the coherence length of an optical fiber. Therefore, we see from figure 4.5 that the fidelity of the initial state is below 0.5 for a channel longer than 17.62 km with a coherence length $l_c = 10$ km which means that purification is no longer possible at this distance. For a higher coherence length the maximum distance is increased accordingly.

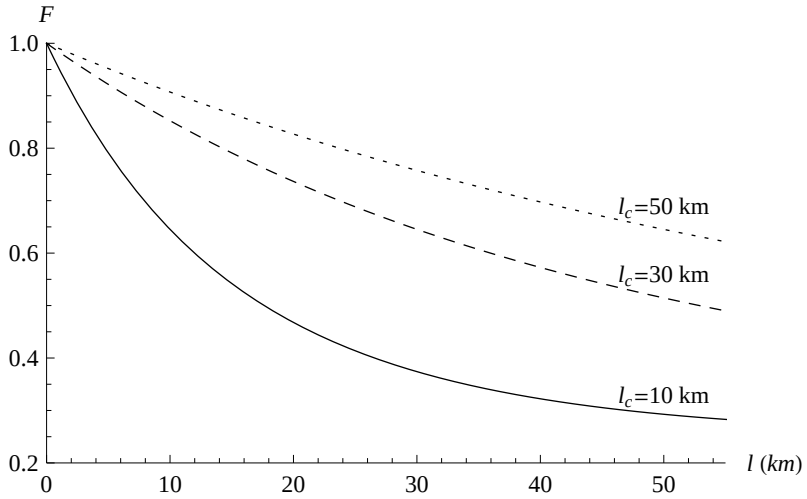

Figure 4.5: *(Noisy Channels)* Correlation between the fidelity F and the length l of a noisy quantum channel.

To overcome the distance problem Dür et al. [45] proposed a scheme for *nested purification* to establish entanglement over longer distances. The main idea is to divide the whole distance into N segments of smaller length such that an entangled state of fidelity larger than F_{min} can be created. This leads to a scheme with $N-1$ control centers $C_1 \ldots C_{N-1}$ between Alice and Bob, which establish a Bell state

between C_i and C_{i+1} (cf. figure 4.6). These N Bell states can be connected again using entanglement swapping performed at each control center C_i. Consequently, two additional problems arise: first, since the initial Bell states are not pure, the entanglement swapping is not perfect either such that the fidelity of the resulting state in the end is lower than the initial fidelity. This can be overcome by sharing M Bell states initially between Alice and C_1, C_{N-1} and Bob as well as C_i and C_{i+1} such that Alice and Bob are able to purify the resulting Bell states after the entanglement swapping. In general, and this is the second problem, the fidelity of the states resulting from the entanglement swapping performed by the C_i is below F_{min} such that purification is no longer possible.

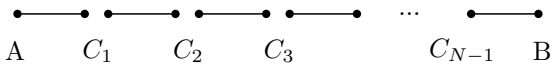

Figure 4.6: *(Nested Purification Protocol)* Illustration of the connection of N segments, i.e. N Werner states, between Alice and Bob.

Therefore, Dür et al. suggest an iteration of the connection-purification process [45]. The total number of segments, N, is divided into groups consisting of L segments (cf. figure 4.7) such that these L segments can be connected and the fidelity F_L of the resulting state is higher than F_{min}. Hence, the M Bell states between the parties can be purified to at least their initial fidelity. This scheme is repeated for every group of L segments until there are N/L of these groups. For the purification process of the next iteration a multiple of M of additional Bell states is needed. Now, the connection centers C_L, C_{2L} and so on are able to connect the Bell states using entanglement swapping and purify the resulting states.

This scheme allows Alice and Bob to share entanglement over a large distance with an arbitrarily high fidelity using the help of several control centers C_i. Dür et al. presented this scheme as a possible implementation for quantum repeaters to overcome the distance problem in quantum cryptography (cf. section 5.2.4).

One topic of major interest regarding the quantum repeater scheme is the cost, i.e. the number of entangled states required to establish one state of at least fidelity F between Alice and Bob. To describe this amount in detail we are going to use in the following paragraphs the recurrence method as purification protocol. Is has been pointed out by Dür et al. that this protocols requires a rather high number

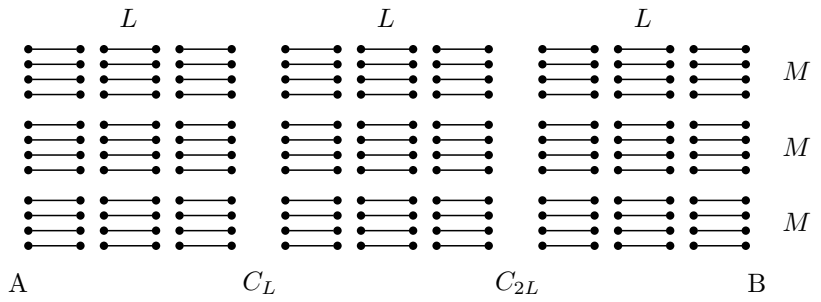

Figure 4.7: *(Nested Purification Protocol)* Schematic depiction of the nested purification by Dür et al. [45]. Here we have $N = 9$ segments, divided into $L = 3$ parts and using $M = 4$ copies of entangled states for each purification round.

of entangled states [45] but the amount of entangled states can be described very easily. We define the number of required entangled states as

$$S\big(l, N, \mathrm{F}\big) = N \times N^{\mathrm{It}(\mathrm{F}_{swap}, \mathrm{F}_{seg})} \times 2^{\mathrm{It}(\mathrm{F}_{seg}, \mathrm{F})} \tag{4.63}$$

with l the whole distance between Alice and Bob, N the number of segments into which the distance is divided and F the desired fidelity of the resulting state. The function $\mathrm{It}(\mathrm{F}_{in}, \mathrm{F}_{out})$ returns the number of iterations required using a specific purification protocol to bring a number of input states of fidelity F_{in} to a desired fidelity F_{out}. In this context the fidelities F_{seg} is the fidelity of an entangled state over the distance of a segment, i.e.

$$\mathrm{F}_{seg} = \left| \frac{1 + e^{-l/20N}}{2} \right|^2 \tag{4.64}$$

defined accordingly to eq. (4.62) above. At last, F_{swap} describes the fidelity after the entanglement swapping between states.

The number $S(l, N, \mathrm{F})$ gives a lower bound on the number of required states because only successful purification steps are considered. As already discussed, Alice and Bob could end up with different results from their measurements on the target qubits during the entanglement purification. In this case they have to discard the source qubits too and use the next states. Nevertheless, $S(l, N, \mathrm{F})$ gives a good approximation of the amount of required states for entanglement purification when using the recurrence method (cf. section 9.4). An approximation of the cost of other purification schemes has been done by Dür et al. [45].

Chapter 5

Quantum Cryptography

The main field of application for quantum mechanics is *quantum cryptography*. The idea of the combination of quantum mechanics and cryptography was introduced by Wiesner who proposed a system for counterfeit-proof money based on quantum states [163]. The special need for quantum cryptography has been addressed by Shor who described an algorithm for a quantum computer to solve the discrete logarithm and the factorization problem [137] based on the implementation of the quantum Fourier transformation [41]. These two problems are the basis of most of todays public key cryptosystems [43, 123]. Therefore, the goal was to find an alternative way to securely transmit information even in the presence of a quantum computer. One cryptographic primitive to achieve that is quantum key distribution (QKD).

5.1 The Basic Idea

In a quantum cryptographic protocol the information transmitted between the communication partners, from now on called Alice and Bob, is encoded into quantum states, mainly single qubits but also entangled qubit pairs or entangled multi-qubit states. The states are measured by both parties and they retrieve the same information only if they use the same bases in their measurements. Due to the quantum nature of the communication system there are some major differences to classical communications, which are sketched in the next few paragraphs.

The security of quantum cryptographic protocols is based on phenomena from quantum mechanics. At this, the most important phenomenon is that a measurement perturbs a quantum systems. When looking at the classical context it is always

possible to access the bits stored on a hard drive or in transit in a communication channel. Hence, an adversary, Eve, is able to gain full access to the bits sent from Alice to Bob over a classical channel. In a quantum setting Eve can not intercept and measure a qubit in transit between Alice and Bob without changing it unless she knows the exact basis. Since Alice and Bob choose their bases at random (cf. the protocols described in the following sections) it is very unlikely that Eve achieves a correct guess for every single qubit. As a consequence of Eve's measurement, the original information is lost and Eve's intervention introduces a certain error rate into the measurement results of Alice and Bob, which can be detected by them.

Another phenomenon which is counter-intuitive from a classical point of view is that a quantum state, i.e. a qubit, can not be cloned. As just pointed out for the classical case, an adversary can intercept the bits in transit between Alice and Bob and perform operations on them. Moreover, Eve is able to make a copy of classical bits to store and analyze them later on when she gains additional information, for example, about their encryption. Regarding quantum information Wooters and Zurek showed in their article [166] that qubits can not be copied in such a way, which is called the *no-cloning theorem*. This results directly from the fact that the measurement of a qubit destroys its information unless the correct basis is used. Since for a qubit in an unknown state the correct basis for a measurement can not be determined, information is lost during the attempt of copying. Thus, an adversary is not able to make a perfect copy of a qubit in transit and measure it later on to reduce the error introduced by directly measuring the qubit.

A number of quantum cryptographic protocols also make use of a third phenomenon of quantum mechanics: *entanglement*. As already described in chapter 2 one feature of an entangled state is that a measurement performed by Alice and Bob on their respective particles results in correlated measurement outcomes. Alice and Bob can use this property such that they share an entangled state and later on measure the qubits in their possession. If Eve interferes with the entangled state by measuring a qubit she destroys the entanglement. Consequently, Alice and Bob do not obtain correlated results for a large number of their measurement, i.e. Eve's intervention again introduces a certain error rate.

At this point it should be stressed that in quantum cryptography the effects of quantum mechanics do not prevent an eavesdropper from obtaining at least parts of a key. By interfering with the protocol Eve introduces a certain error rate which

can be detected by Alice and Bob. At that point Eve has already obtained some information about the key due to her intervention. If the error rate is above a certain predefined threshold Alice and Bob abort the protocol and thus Eve's information is useless. If the error rate is below the threshold Eve might have information about some parts of the key. Thus, Alice and Bob have to perform additional operations to reduce even this small amount of Eve's information. This is also rather different to classical communications where you usually do not know whether an adversary knows any part of the key.

5.2 Quantum Key Distribution

5.2.1 Single Qubit Schemes

The first QKD protocol was presented by Bennett and Brassard in 1984 [8] and is commonly known as *BB84 protocol*. In the BB84 protocol the two communication parties Alice and Bob represent the information by the polarization of single photons to generate a classical key between them. Alice is in possession of a single photon source and prepares the photons randomly according to the Z- and the X-basis (cf. figure 5.1), i.e. $\{|0\rangle, |1\rangle\}$ and $\{|x+\rangle, |x-\rangle\}$, respectively, where

$$|x+\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big) \qquad \text{and} \qquad |x-\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - |1\rangle\Big). \tag{5.1}$$

These bases are called Z- and X-basis due to their relation to the Bloch sphere. The four states can be understood as Bloch vectors pointing in the positive and negative Z and X directions of the Bloch sphere. To transfer a state from the Z basis into the X basis the *Hadamard* operation H can be used. This operation can be written as

$$H = \frac{1}{\sqrt{2}}\big(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|\big) \tag{5.2}$$

and maps the state $|0\rangle$ onto $|x+\rangle$ and $|1\rangle$ onto $|x-\rangle$.

After Alice chose the basis, the qubit is sent to Bob, who performs a measurement on it. Since Bob doesn't know which basis Alice used he will not be able to retrieve the full information for every qubit. The best strategy for him is to randomly choose between the Z- and X-basis himself. In this case Bob will choose the correct basis 1/2 of the time but until now he does not know in which cases he has guessed right.

Thus, Alice and Bob compare the choice of their bases in public after Bob measured the last qubit.

Alice and Bob eliminate their measurement results for those measurements where they used different bases (cf. figure 5.1). This step is called *sifting* [81]. The remaining measurement results are converted into classical bits. This is achieved using the mapping

$$\big\{|0\rangle, |x+\rangle\big\} \longrightarrow 0 \qquad \text{and} \qquad \big\{|1\rangle, |x-\rangle\big\} \longrightarrow 1. \tag{5.3}$$

At this stage Alice and Bob should have identical classical bit strings if the channel is perfect. Nevertheless, they have to check for errors to be sure to obtain an identical bit string. To estimate the error rate Alice and Bob publicly announce a fraction of their results. If the error rate is not too high (cf. section 5.2.3 for bounds on the error rate) they use classical error correction to eliminate the differences in their bit strings.

It is important that the announcement of the bases takes place after all qubits have been sent to minimize the possibility of a successful attack of an eavesdropper. As we already discussed in section 4.1 above a channel usually has an influence on the state of the qubits in transit between Alice and Bob. Therefore, it is possible that their results differ by a small amount. But if this error rate is above a certain predefined threshold both parties have to discard their remaining bit strings and start over because they have to assume that the error is coming from the presence of an eavesdropper. In the ideal case (noiseless channels, no eavesdropper) Alice and Bob find no error in their results and they can use the remaining bits as input for further operations.

In 1992 Charles Bennett pointed out that two non-orthogonal states instead of four would be enough to perform the BB84 protocol [5]. The idea is that two non-orthogonal states can not be perfectly distinguished but they can be distinguished without making a wrong decision using positive operator-valued measurement (POVM) [113]. That means when Bob measures the state sent by Alice he will never make a wrong decision but sometimes he will not be able to make any decision at all.

In detail, Alice prepares one of the states $|\varphi\rangle$ and $|\psi\rangle$, where $|\varphi\rangle$ codes for a classical 0 and $|\psi\rangle$ for a classical 1. She sends the qubit to Bob, who uses the operators

$$M_0 = \mathbb{1} - |\psi\rangle\langle\psi| \qquad \text{and} \qquad M_1 = \mathbb{1} - |\varphi\rangle\langle\varphi| \tag{5.4}$$

bit A	1	1	1	0	0	1	0	1	0	1	1	0
basis A	Z	Z	X	Z	X	X	Z	Z	Z	Z	X	X
qubit A	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|x+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|-\rangle$	$\|x+\rangle$
basis B	X	Z	Z	X	X	Z	Z	X	X	X	X	Z
qubit B	$\|-\rangle$	$\|1\rangle$	$\|0\rangle$	$\|x+\rangle$	$\|x+\rangle$	$\|1\rangle$	$\|0\rangle$	$\|x+\rangle$	$\|-\rangle$	$\|x+\rangle$	$\|-\rangle$	$\|1\rangle$
bit B	1	1	0	0	0	1	0	0	1	0	1	1
Raw key		1			0		0				1	

Table 5.1: Example of a BB84-protocol performed with 12 qubits.

to distinguish between $|\varphi\rangle$ and $|\psi\rangle$. From this equation we see that M_0 annihilates $|\psi\rangle$ but gives a positive result with $|\varphi\rangle$ and vice versa. That means, if Alice sent $|\varphi\rangle$ Bob's probability to measure $|\psi\rangle$ is 0 and to measure $|\varphi\rangle$ is $1 - |\langle\varphi|\psi\rangle|^2$. To describe a complete measurement a third operator M_2 is necessary such that the completeness relation $\sum M_i = \mathbb{1}$ is fulfilled, giving

$$M_2 = \mathbb{1} - M_0 - M_1 \tag{5.5}$$

If operator M_2 is the result of Bob's measurement he can not decide whether Alice sent $|\varphi\rangle$ or $|\psi\rangle$. As an example let $|\varphi\rangle = |0\rangle$ and $|\psi\rangle = |x+\rangle$ and the operators

$$\begin{aligned} M_0 &= \mathbb{1} - |x+\rangle\langle x+| = |x-\rangle\langle x-| \\ M_1 &= \mathbb{1} - |0\rangle\langle 0| = |1\rangle\langle 1| \\ M_2 &= \mathbb{1} - M_0 - M_1. \end{aligned} \tag{5.6}$$

As pointed out above, if Alice sends $|0\rangle$ Bob obtains operator M_1 with probability $p(1) = 0$ and

$$p\big(0\big) = \langle 0||x-\rangle\langle x-||0\rangle = \frac{1}{2} \qquad p\big(2\big) = \langle 0|M_2|0\rangle = \frac{1}{2}. \tag{5.7}$$

Similarly, if Alice sends $|x+\rangle$ Bob obtains operator M_0 with probability $p(0) = 0$ and operators M_1 and M_2 with equal probability of 1/2. Therefore, when Bob measures the qubit coming from Alice he obtains a correct result half of the time. For the other half he obtains an undecidable result and both have to eliminate that qubit. Both Alice's choice of the state as well as Bob's choice of the measurement operator is completely random. In the end Bob announces where his measurements had an undecidable result and they have to discard these results. For the remaining

results Alice and Bob publicly announce a fraction of them to check whether they are really correlated. If the error rate is above some predefined threshold they have to assume that it is due to the presence of an eavesdropper rather than a noisy quantum channel or imperfect devices and they restart the protocol.

A natural extension of the BB84 protocol is the *six state protocol* [24]. In this protocol additionally to the Z- and the X-basis the third complementary basis, i.e. the Y-basis is introduced, having

$$|y+\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + i|1\rangle\Big) \qquad |y-\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - i|1\rangle\Big) \tag{5.8}$$

This extension is called "natural" because in this case all three dimensions of the Bloch sphere are used. Alice chooses randomly one of the six states and sends it to Bob. Bob has to select one out of three (instead of two as in [8]) bases and performs a measurement on the received qubit. Hence, his choice will correspond to Alice's preparation only in 1/3 of the cases such that they will have to discard a greater amount of qubits when they publicly compare their measurement bases. As in the other protocols described above, Alice and Bob choose a certain fraction of the remaining measurement results and compare them in public to check if an eavesdropper is present. The major advantage of the six state protocol is that it is more sensitive to attacks and an adversary will have a smaller chance to stay undetected.

5.2.2 Entanglement Schemes

Whereas the protocols just discussed above are based on single photon sources Ekert presented a protocol in 1991 [51] which uses a source emitting maximally entangled qubit pairs, e.g. the Bell state

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle\Big). \tag{5.9}$$

This source is located between Alice and Bob and one qubit of the state is flying to Alice and the other one to Bob. It is also possible that one of the communication parties is in possession of the source, which is the case when looking at implementations of the Ekert protocol. Alice and Bob randomly measure the polarization of their qubit according to three different angles

$$a_1 = 0^\circ \qquad a_2 = +45^\circ \qquad a_3 = +22.5^\circ \tag{5.10}$$

at Alice's side and

$$b_1 = 0^\circ \qquad b_2 = -22.5^\circ \qquad b_3 = +22.5^\circ \tag{5.11}$$

at Bob's side which they choose at random. Note that these angles are non-orthogonal in contrary to the measurements discussed in connection with single photon schemes above.

After all photons have been exchanged Alice and Bob publicly compare their orientation of the measurement. If Alice chooses a_i and Bob chooses b_j they will obtain perfectly correlated results if the difference $a_i - b_j = 0^\circ$ due to the special properties of entanglement (cf. chapter 2). If $a_i - b_j = 45^\circ$ they discard the results because the error probability is maximal at this setting. All other cases where $a_i - b_j = \pm 22.5^\circ$ or $a_i - b_j = 67.5^\circ$ are used in the CHSH inequalities to check for eavesdroppers. The CHSH inequalities are violated in the quantum case, i.e. if an entangled state is present (for details on the inequalities cf. section 2.3 above and, of course, [33]). Therefore, Alice and Bob can check whether they still share an entangled state which is given if the CHSH inequalities are maximally violated (with $2\sqrt{2}$). If their result is less or equal to 2 there has been some interference and they restart the protocol.

At this point we want to stress that there is a major conceptual difference between QKD protocols using single photon sources like the BB84 protocol and protocols using entangled photons. Where in the first case Alice more or less transmits a key to Bob, in the latter the key comes into being at Alice's and Bob's side at the moment of their measurement. That means, whereas there is some information about the key in transit between Alice and Bob in the BB84 protocol, in the Ekert protocol the qubits flying to Alice and Bob contain no information at all. Thus eavesdropping on such protocols is much more difficult.

In 1992 Bennett, Brassard and David Mermin presented a variant of the Ekert protocol where they show that a test of the CHSH-inequalities [33] is not necessary for the security of the protocol [11]. Instead Alice and Bob use two complementary measurement bases and randomly apply them on the received qubits. In detail, Alice and Bob receive qubits coming from the source located in the middle of them (as pointed out above, the protocol does not change if the source is in possession of Alice or Bob). Again, the qubits are parts of the Bell state $|\Psi^-\rangle$. After receiving both randomly and independently choose either the Z- or the X-basis to measure

the qubit. Due to the entanglement of the qubits Alice's measurement completely determines the state of Bob's qubit, i.e. if Alice measures a $|1\rangle$, Bob's qubit is in the state $|0\rangle$, and vice versa (cf. section 2.3). If Bob measures in a different basis than Alice he destroys the information carried by the qubit and thus will not obtain the same result as Alice. Therefore, after the measurements are finished both parties publicly compare their measurement bases and discard their results where they used different bases. The remaining results should be perfectly correlated and the communication parties compare a randomly chosen fraction in public. If there is too much discrepancy between their results they have to assume that an adversary is present and they start over the protocol. It has also been shown by Bennett et al. in this paper that the security of this version of the protocol is equal to the security of the BB84 scheme [11].

5.2.3 Error Correction and Privacy Amplification

The protocols described in sections 5.2.1 and 5.2.2 by themselves do not provide a perfectly secure key shared between Alice and Bob. The resulting classical bit string is usually called *raw key* to indicate that it has to be further processed. Following the protocols solely as presented above the communication parties would just obtain a shared key under ideal conditions. That means they use perfect devices, a loss-free quantum channel and there is no adversary present. In reality, as already discussed in section 4.1, quantum channels are lossy and have some noise which alters the qubits in transition. Further the detectors are imperfect which means that dark counts may occur, i.e. a detector clicks although no photon is present.

Another big problem is that there exist no single photon sources but in some implementations weak coherent pulses are used instead. In this case the source emits a superposition of quantum states with 0, 1, 2, $\ldots n$ photons which gives an adversary, in principle, the opportunity to split one photon from the pulse (cf. section 6.2.2 for details). Because of these problems QKD protocols have to recover from noise and have to deal with influence from an adversary. A measure for the amount of noise in the quantum channel is the *quantum bit error rate* (QBER). The QBER is basically defined as the number of wrong detections divided by the number of total detections [106] (for more details see also [57]) and is calculated after the sifting procedure. Nevertheless, if there is too much noise involved it is not possible to obtain a key and the protocol has to be restarted.

A first step towards the final secret key has already been described in sections 5.2.1 and 5.2.2 above and is called *sifting* [81]. During this process Alice and Bob compare in public their choice of measurement bases and discard all results where they used different bases. Next, they perform *error correction* which is a classical algorithm to cancel out the discrepancies in their bit strings. To perform error correction Alice and Bob first have to estimate the QBER to check whether error correction is even possible or not. If too much information leaks to an adversary they have to restart the protocol. Therefore, they publicly compare a fraction of the remaining results to check whether they are correlated. A procedure that has been heavily used for error correction is the *CASCADE* algorithm first introduced by Charles Bennett et al. [7]. In this algorithm Alice and Bob publicly agree on a random permutation of their bits and then divide the resulting string into blocks of a certain size. The block size is chosen such that it is unlikely that there is more than one error per block. Then they compute the parity of each block and compare it in public. For blocks with equal parity they assume that they are identical and for the other blocks they subdivide them to find the error. For every block the parity is tested they discard the last bit to avoid leaking of too much information. Since there could be more than just one error per block Alice and Bob permute the resulting bit string again and start over the error correction. They stop if they do not find an error for a specific number of runs.

Due to the fact that Alice and Bob publicly compare the parity of each block an adversary is able to obtain further information about the bit string (assuming Eve's presence has not been detected during error correction). A last process called *privacy amplification* [13] performed by Alice and Bob uses hash functions to minimize the amount of Eve's information. It is shown in [13] that using a specific type of hash functions Eve's information of the resulting shared secret key can be made arbitrarily small. An example for such hash functions are the *strongly-universal$_2$ hash functions* presented in [160]. It has to be pointed out at this time that a single bit error after error correction will result in completely uncorrelated bit strings at Alice's and Bob's side after privacy amplification.

Usually, error correction as well as privacy amplification are treated as one-way communication, i.e. Alice tells Bob what to do and both alter their classical bit string accordingly. Using solely one-way communication Alice and Bob are able to obtain a secret key up to an quantum bit error rate of $\simeq 15\%$ [57]. There are protocols

called *advantage distillation* which use two-way communication to provide a secret key also for an error rate above 15%. If such protocols are applied the security of the whole system is not based on the laws of physics but on the assumptions about Eve's technology [104]. Hence, whenever error correction or privacy amplification is mentioned in the following sections we are going to limit the considerations to protocols based on one-way communication.

Furthermore, error correction reveals some information about the corrected key in public and therefore in particular to Eve. Hence, the loss of information due to the error correction and Eve's information about the key have to be subtracted from the overall information. Following this argumentation the maximal QBER such that Alice and Bob are still able to obtain a secret key is $\simeq 11\%$ [135, 87].

5.2.4 Physical Realizations

In the following we want to focus briefly on some physical realizations of photon sources and coding schemes as well as give a feeling on the evolution of experimental implementations of QKD systems. For more detailed information confer [142] and the references therein as well as the references in the following sections.

Photon Sources

There are a number of limitations when going to real-life implementations of QKD protocols. As already pointed out, there are no perfect singe-photon sources which can be used in the protocols described in section 5.2.1 above. Therefore, other sources have to be found. A simple way to realize a single photon source is to use a weak coherent pulse, i.e. a pulse from a standard telecom laser with a very low mean photon number μ. The signal from such a laser can be described by the coherent state

$$|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{5.12}$$

which can be seen as a superposition of Fock states (states with $0 \ldots n$ photons). The probability to find more than one photon in a pulse follows a Poissonian distribution [57]

$$P\big(n, \mu\big) = \frac{\mu^n}{n!} e^{-\mu} \tag{5.13}$$

and is approximately $\mu/2$, which can be made arbitrarily small. The problem is that most of the pulses from the laser will contain no photon at all and thus can not

contribute to the communication. Due to the high modulation rate of such telecom lasers the amount of pulses containing one photon is sufficiently large to keep up a adequate bit rate for communication.

Another problem in this scheme are the detectors. They have to be active for all incoming pulses, whether or not they contain a photon. Because of the large fraction of empty pulses a detector could click although no photon has been sent which is called a dark count. The number of total dark counts increases with the modulation rate of the laser and the signal to noise ratio decreases with μ. Therefore, the mean photon number can not be made really small, i.e. smaller than 0.01, because otherwise there is too much noise involved [57]. In most experiments a $\mu = 0.1$ is used giving a chance of 5% that a pulse contains more than one photon.

Another possibility to realize single photon sources is to use entangled pairs of photons. Such photon pairs are generated by spontaneous parametric down conversion in a non-linear crystal, e.g. a β-barium borate crystal (cf. [85, 22] for a good description of the down conversion). A photon coming from a laser generates inside the crystal two photons of lower energy. Taking both photons together they have the same energy as the original photon.

The main disadvantage of this scheme is that it is rather inefficient but if the generation is successful it is very unlikely that two pairs have been generated. Even if two entangled states are created occasionally at the same time it is not a big problem since they are independent of each other. Splitting off the additionally created qubit does not provide any information since Alice and Bob are using the other qubit pair in their protocol. Further, one photon of the pair is used to trigger the detector at the communication partner. That means, one photon of the pair is measured instantaneously by the communication party obtaining the source. If the detector clicks the sender knows that the other photon must be on its way and the detector at the receiver's side can be activated. Therefore, the amount of dark counts is much lower since the detector of the receiver is not active all the time.

Regarding the Ekert scheme (cf. section 5.2.2) and other protocols based on entanglement the parametric down conversion is used to create entangled photons. The application is the same as for the single photon source: the party in possession of the source pumps a laser beam into a non-linear crystal and whenever entangled photons are created they are used either for key generation or to check the CHSH inequalities.

Channels

As already pointed out in section 4.1 above quantum channels interfere with the qubits in transit and thus introduce errors in their polarization or phase. Additional to the more theoretical schemes presented in section 4.1 optical fibers, which are the most common transmission medium for quantum communications, have some special properties. As it has been shown in [106] telecom fibers working at a wavelength from 1310 nm to 1550 nm can be used for implementations based on weak coherent pulses. Most implementations with entangled photons need an optical fiber working at a different wavelength (e.g.. 810 nm [117]). The major problem arising from optical fibers are the polarization effects as birefringence and polarization mode dispersion. Although, regarding birefringence, today's optical fibers are far better than e.g. a decade ago and are very well suited for classical communication, in the quantum case any birefringence is a severe problem. Due to asymmetries in the fiber or imperfections in the fabrication of the fiber two orthogonal polarization states can propagate with two different phase velocities which may cause errors in the detection of the photons. This effect is called *polarization mode dispersion* and is present in every optical fiber [37]. The amount of photons which are influenced by this effect is rather low and depends on the quality of the fiber. But the polarization mode dispersion can not be corrected since it is a completely statistical effect.

Yet, there is a possibility to make an optical fiber polarization maintaining. In this case the core of the fiber is alternatively shaped such that one polarization orientation is preserved (e.g. the horizontal-vertical polarization). Photons in any other orientation are completely depolarized and can not be corrected. Since the security of QKD protocols relies on the application of different polarization orientations polarization maintaining fibers are of no use in quantum key distribution.

Looking at free-space links these two problems of optical fibers are mainly not given since the atmosphere is weakly dispersive and essentially non-birefringent [57]. Nevertheless, there are other influences like atmospheric conditions or daylight which result in a high error rate. For example, daylight or even moonlight can cause detections at the receiver even if no photon was sent. Further, a transmission is only manageable with clear weather. Some effect of atmospheric turbulences like arrival-time jitter can be overcome using a reference beam but in general, good atmospheric conditions are very important for a faithful transmission.

Coding Schemes

To overcome the limitations given by the photon sources and quantum channels different coding schemes have been established. To encode qubits in the polarization of photons is a very obvious solution and has already been suggested in the BB84 protocol [8] but is nevertheless rather difficult to manage. An experimental setup for polarization coding is sketched in figure 5.1 and is similar to the setup that has been used in the experiment of 1996 by Muller et al. [106].

In this scheme four laser diodes (LD) are used at Alice's place emitting pulses with the polarizations 0°, 90° and ±45°. The laser diodes are triggered randomly and one at a time for every single qubit. Using a sequence of beam splitters (BS) the pulse is guided to a set of filters (F) which reduce the number of photons below 1 and then it is sent over the quantum channel to Bob. Since the optical fiber alters the polarization of the photons as described above a number of wave plates have to be used at Bob's side to reverse the change and restore the original polarization. Next, the pulse hits a beam splitter where half of the particles are reflected and the other half is transmitted. Both reflected and transmitted photons are analyzed using a set of polarization beam splitters and photon counting detectors. Before the reflected photons hit the beam splitter they are rotated from diagonal to horizontal using a $\lambda/2$ wave plate and are analyzed afterwards.

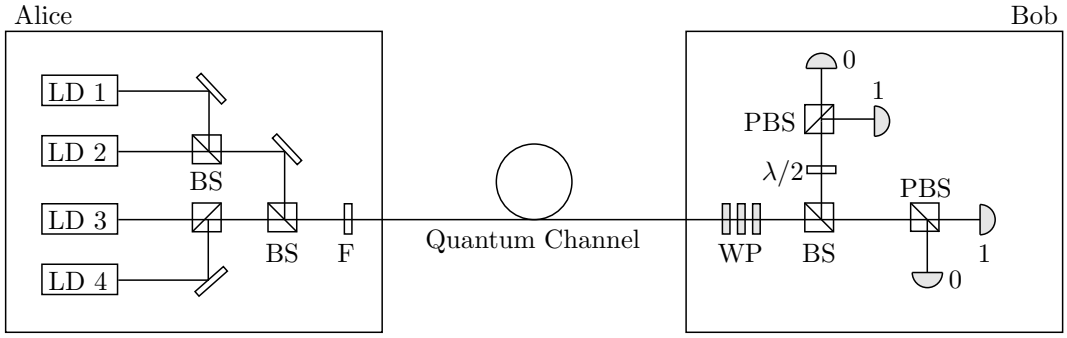

Figure 5.1: *(Polarization coding scheme)* Illustration of the polarization coding scheme used in the BB84 protocol [8]. LD: Laser Diode, (P)BS: (Polarization) Beam Splitter, F: Filter.

Another idea of coding the value of qubits is the phase of photons, which has been first proposed by Bennett in the two state protocol [5] and is depicted in figure 5.2. It is an optical fiber version of the Mach-Zehnder interferometer where

a phase modulator is placed in each arm. To implement quantum key distribution a photon source (LD 1) emitting weak coherent pulses is used at Alice's side. Alice randomly chooses the phase ϕ_A of her phase modulator (PM) to be either 0, $\pi/2$, π or $3\pi/2$, where 0 and $\pi/2$ code for 0 and π and $3\pi/2$ for 1. Similarly, Bob chooses between a phase 0 or $\pi/2$ for his modulator and his two detectors, 0 and 1, code for the respective classical bits. If the phases of Alice and Bob differ by $\pi/2$ or $3\pi/2$ destructive interference is obtained and they can not use the photon for the classical key unless it is combined with the method depicted in figure 5.1. If the difference between Alice's and Bob's phase is 0 or π one of Bob's detectors will click with certainty (for 0 detector 0 and for π detector 1) and they have secretly shared a classical bit.

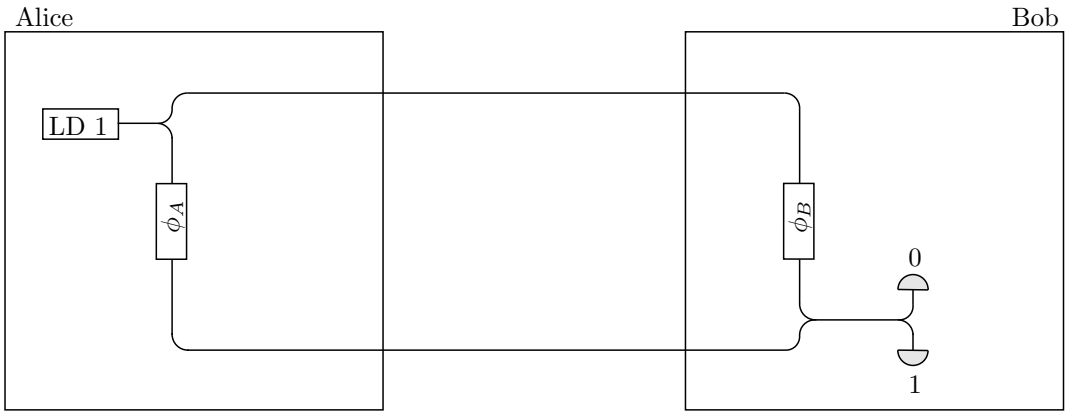

Figure 5.2: *(Phase coding scheme)* Illustration of the phase coding scheme proposed by Bennett [5]. LD: Laser Diode; ϕ_A, ϕ_B: phase modulation of Alice and Bob.

Unfortunately, the path distance becomes unstable if Alice and Bob are separated by more than a few meters [57]. Therefore another setup has been presented in [5] (cf. fig 5.3) where two interferometers are used, one at each communication party. Both interferometers have a long and a short arm, where a phase modulator (PM) is placed in the long arm. A single photon has three possibilities to pass through the interferometer: in the first two scenarios it takes either the short or the long arm at both Alice's and Bob's side. The third scenario is important because the photon takes the short arm at Alice's and the long arm at Bob's side or vice versa. In this case Bob observes interference since the path distances coincide. If Bob monitors the photon counts as a function of the time he is able to distinguish interfering from

non-interfering events, since the photons going through the short arm at both sides will arrive first whereas the photons going through the long arm at both sides will arrive last. All the other photons will arrive at the same time only if the phases at Alice's and Bob's side are equal. By choosing randomly between two phases Alice and Bob are able to secretly share a classical key.

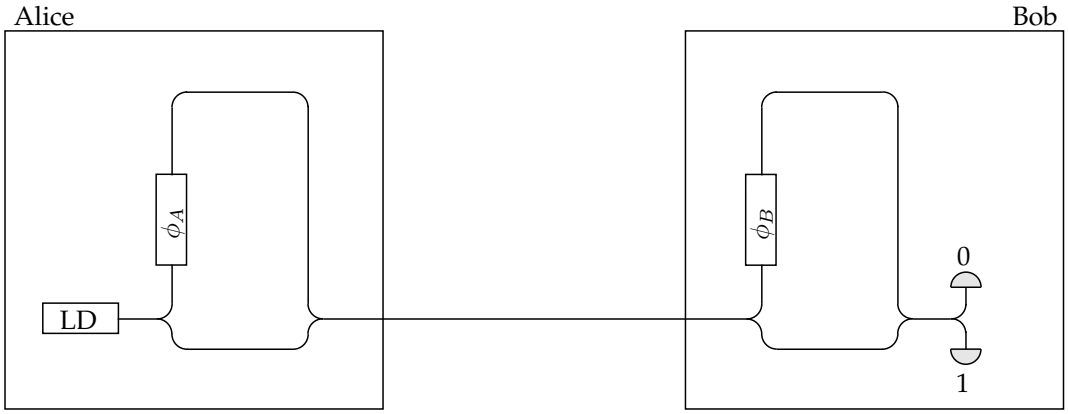

Figure 5.3: *(Double Mach-Zehnder scheme)* Illustration of the double Mach-Zehnder scheme proposed by Bennett [5]. LD: Laser Diode; ϕ_A, ϕ_B: phase modulation of Alice and Bob.

A major drawback to this scheme is, similar to the polarization coding, that the phase of a photon is altered while running through the optical fiber. Thus, a third scheme has been proposed which automatically and passively compensates all polarization fluctuations in an optical fiber [105]. The setup is similar to the double Mach-Zehnder scheme described in the previous paragraph. One major difference is that the photons are emitted by Bob and reflected at Alice's side using a Faraday mirror. A Faraday mirror is a normal mirror glued on a Faraday rotator and thus rotates the polarization of a photon by 45°, i.e. any polarization state is transformed into its orthogonal. This reflection is important to overcome the influences of the optical fiber because when the photons return to Bob the influences are reversed due to the Faraday mirror. To perform QKD the phase shifts of the modulators at Alice's side and Bob's long arm are again chosen randomly between 0 and π. Bob obtains destructive interference if Alice and Bob choose different phase shifts. Otherwise, Bob will detect a photon and can be sure that Alice sent the same bit (the coding is equivalent to the double Mach-Zehnder interferometer).

Experiments

The first major experiment implementing the BB84 protocol over a relevant distance was performed by Muller et al. in Geneva [106]. In this experiment a 23 km long standard telecom fiber installed under the Lake Geneva and connecting Geneva and Nyon is used to establish a shared secret key. Thus Muller et. al. showed that QKD is, in principle, feasible with today's technology and standardized components like telecom fibers. The experiment implements the BB84 protocol using polarization coding. Their setup is similar to the one presented in figure 5.1 and described in detail in the respective section.

After this experiment the aim was to enlarge the distance between the communication parties. In the course of the next years quantum links over huge distances where realized, such as, for example, 122 km over a standard telecom fiber [58] or even 144 km via a free-space link between the Canary Islands of La Palma and Tenerife [150]. The main problem is that the key generation rate, i.e. the amount of key material established per second, is very low. A real communication over such a long distance is therefore infeasible. Hence, research focused on smaller distances for the quantum links but very high key generation rates to be of higher practical relevance.

The first practical application of QKD was a bank transfer in Vienna which was secured by QKD [117]. The implemented QKD protocol is the variant of the Ekert protocols presented in [11]. In this experiment the distance is only 1.45 km but the key generation rate from the QKD protocol is high enough such that it can be used immediately for classical cryptography. Therefore, it has been shown that QKD is not only feasible using current technology but also is of practical use in today's communication. Based on this first result a prototype of a whole quantum network secured by QKD was build in 2008 [118, 112]. This prototype was set up in Vienna and the communication between the various users of the network was encrypted with keys coming from QKD devices. To achieve that different technologies like plug and play systems [140], weak coherent pulse systems [49], coherent one-way systems [141], continuous variable systems [61, 62] and entanglement-based systems [78] were merged together [112]. Hence, it has been shown that the application of QKD in our current communication infrastructure is possible. The main drawback of the prototype was that a high key generation rate was only maintained at distances up to 20km. From this distance problem the vision arises to establish free-space

links from earth to satellites to create a global QKD network [157].

5.3 Quantum Secret Sharing

5.3.1 The Classical Version

Suppose there are n scientist working together on a secret project. They want to lock away their results in their laboratory but, unfortunately, they do not trust each other entirely. Thus, it is impossible that they have only one key and one lock and every scientist gets the same key for the laboratory. The scientists agree that at least k of them have to come together to open the laboratory such that none of them will steal their joint results. The question is how many locks and different keys are needed to achieve that?

Such a problem is called *secret sharing* and a solution has been introduced individually by Shamir [133] and Blakley [19] in 1979. The idea is every scientist gets a *share* of the secret and any combination of k shares makes it possible to reconstruct the secret. Further, any single share or any combination of $k-1$ or less shares does not reveal any information about the secret. Shamir's solution relies on polynomial interpolation in the 2-dimensional plane which says that at least k points are necessary to identify a polynomial of order $k-1$. For any number $n \geq k$ of points the original polynomial is easy to compute, but the knowledge of only $k-1$ or fewer points gives no information about the polynomial. Such a scheme is called a (k, n) *threshold scheme*. The polynomial is of the form

$$f(x) = s + \sum_{i=1}^{k-1} a_i x^i \tag{5.14}$$

where s is the secret and the a_i are chosen at random. The Shamir secret sharing protocol is usually implemented over a finite field, therefore, the secret s as well as the a_i are elements of this finite field. n points of this polynomial, i.e. the shares, are computed and sent to the respective parties involved in the protocol. If the secret is needed, k parties have to bring their shares together and can use the Lagrange interpolation to reconstruct the polynomial and the secret s. The main advantage of this protocol is that it is information-theoretical secure, which means that an adversary has no better chance to obtain the secret than just guessing it. We want to stress that in this case, different from the key distribution described in

section 5.2 above, it is possible that there exist one or more dishonest communication parties. In fact, when dealing with the security of secret sharing protocols it is much more important to focus on dishonest parties since they are more powerful than any eavesdropper from the outside as described later on.

The scheme presented by Blakley [19] is also based on a geometric fact, i.e. that any k non-parallel k-dimensional hyperplanes intersect at one specific point. For example, in the 2-dimensional case two non-parallel lines intersect in one specific point and in the 3-dimensional case three non-parallel planes intersect in one specific point and so on. Thus, for a (k, n) threshold scheme n k-dimensional hyperplane are needed as shares and sent to the communication parties. k of them have to come together to compute the intersection point and recover the secret. The scheme by Blakley is a little less efficient than Shamir's scheme but is nevertheless information-theoretical secure.

Secret sharing is usually applied in settings where some of the parties involved are not trustworthy but a secure communication has to be established. This could be, for example, that the key for the digital signature of a company is split among the authorized signatories.

5.3.2 Sharing Classical Secrets

The first quantum versions of secret sharing were presented by Hillery, Bužek and Berthiaume [68] as well as Karlsson, Koashi and Imoto [84] in 1999, which are described in detail below. They used GHZ states and Bell states, respectively, to share a classical bit string between two parties. In the following years additional protocols were described, e.g. by Cabello [26], Guo et al [65] and Markham et al. [103]. The two main differences between these protocols and the classical secret sharing schemes described above is that the secret between the parties is created, i.e. it is not possible for Alice to share a predefined secret as in [133, 19]. Second, these protocols describe (n, n) threshold schemes. Hence, all parties have to work together to recreate the secret – it is not possible to establish a (k, n) threshold scheme with $k < n$ as in the classical case with these protocols. However, Gottesman et al. showed that a (k, n) threshold scheme is possible also using quantum secret sharing [34, 59]. They presented a $(2, 3)$ QSS protocol based on qutrits, i.e. 3-dimensional quantum states. They also showed that there is a connection between QSS and quantum error correction [34]. Nevertheless, we will focus on the (n, n) threshold

since they mostly rely on entanglement between two or more qubits.

The HBB Scheme

In their article Hillery et al. they presented a quantum secret sharing scheme based on the distribution of GHZ states [60] between three parties, Alice, Bob and Charlie [68]. Each party measures its qubit at random in one of two bases. Based on their results, Bob and Charlie together are able to determine Alice's result but individually have no information about it. In detail, Alice generates copies of the GHZ state

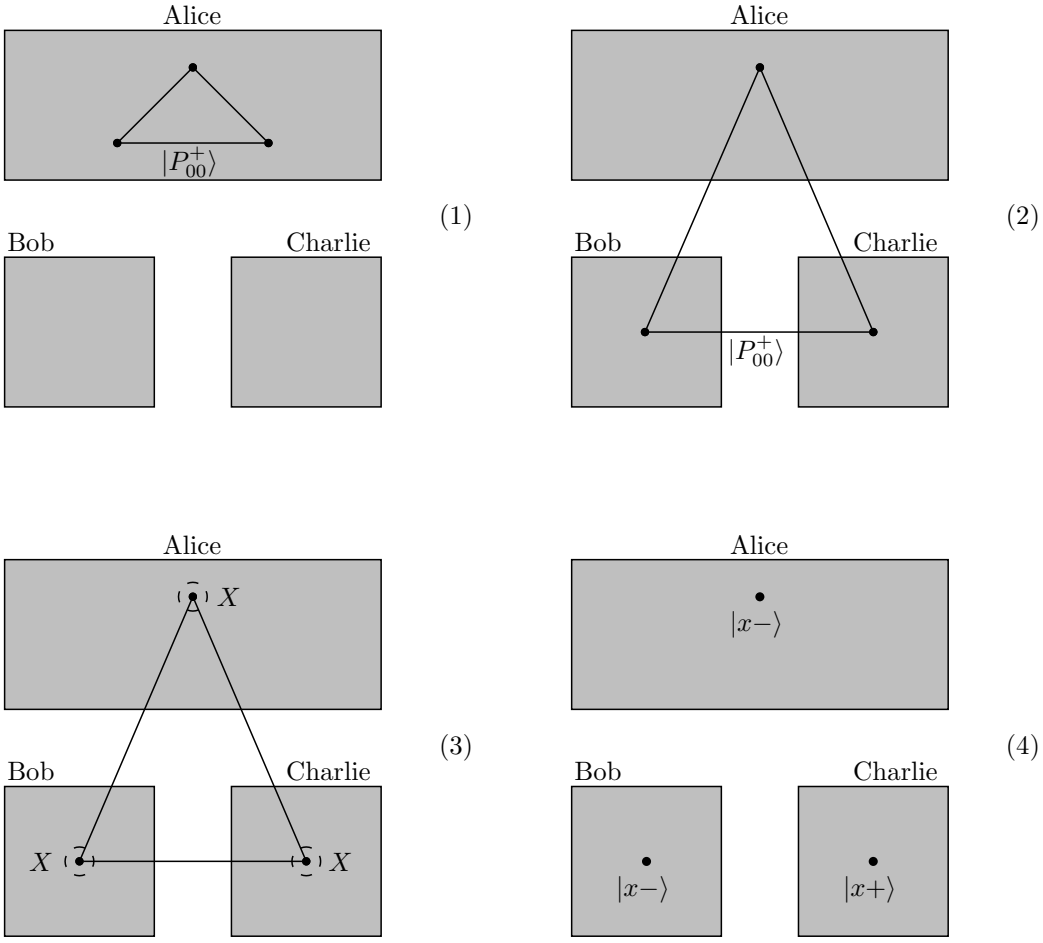

Figure 5.4: *(HBB secret sharing scheme)* Illustration of the QSS protocol by Hillery et al. [68].

$$|P_{00}^{+}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{ABC} \tag{5.15}$$

		Alice			
		$\|x^+\rangle$	$\|x^-\rangle$	$\|y^+\rangle$	$\|y^-\rangle$
Bob	$\|x^+\rangle$	$\|x^+\rangle$	$\|x^-\rangle$	$\|y^+\rangle$	$\|y^-\rangle$
	$\|x^-\rangle$	$\|x^-\rangle$	$\|x^+\rangle$	$\|y^-\rangle$	$\|y^+\rangle$
	$\|y^+\rangle$	$\|y^-\rangle$	$\|y^+\rangle$	$\|x^-\rangle$	$\|x^+\rangle$
	$\|y^-\rangle$	$\|y^+\rangle$	$\|y^-\rangle$	$\|x^+\rangle$	$\|x^-\rangle$

Table 5.2: Charlie's state depending on Alice's and Bob's measurement result.

in her laboratory (cf. picture (1) in figure 5.4) and sends qubit B to Bob and qubit C to Charlie (cf. picture (2) in figure 5.4). Then, each party randomly chooses to measure its qubit either in the X or in the Y basis. Taking the X basis the GHZ state $|P_{00}^+\rangle$ can be written as

$$\begin{aligned} |\Psi\rangle_{ABC} = \frac{1}{2}[&(|x^+\rangle_A|x^+\rangle_B + |x^-\rangle_A|x^-\rangle_B)|x^+\rangle_C \\ &+(|x^+\rangle_A|x^-\rangle_B + |x^-\rangle_A|x^+\rangle_B)|x^-\rangle_C] \end{aligned} \tag{5.16}$$

Therefore, we directly see that if both Alice and Bob perform their measurements in the X basis and obtain the same result, Charlie ends up with the state $|x^+\rangle$ (cf. pictures (3) and (4) in figure 5.4). Otherwise, if Alice and Bob obtain different results, Charlie ends up with the state $|x^-\rangle$. Regarding the case when Alice and Bob perform their measurement both in the Y basis or in different bases similar conditions can be found for Charlie's state (cf. table 5.2).

After each party performed its measurement they all announce their bases for the whole sequence sent by Alice but do not reveal the specific result. Additionally, they perform an error estimation procedure, i.e. all three parties sacrifice some of the remaining measurement results to check for eavesdroppers and dishonest parties by comparing them publicly. Based on the information about the basis choice of the remaining qubits Charlie always knows whether Alice and Bob have the same results or not, but he has no information about their exact results. Further, Bob knows that he either has the same or the opposite result of Alice and thus needs the information about Charlie's measurement result to fully determine it. Thus, Bob and Charlie have to collaborate to obtain Alice's result. Due to the random choice of the measurement bases, Charlie will measure in the wrong basis half of the

times. These cases can be identified when the three parties reveal their bases and the respective qubits have to be discarded.

The KKI Scheme

Another quantum secret sharing protocol was published also in 1999 by Karlsson, Koashi and Imoto [84]. In this scheme Alice randomly chooses a bit string and encodes it in two non-orthogonal bases (like in the BB84 protocol [8]), i.e. either as $\{0,1\} \mapsto \{|\Psi^+\rangle, |\Phi^-\rangle\}$ or $\{0,1\} \mapsto \{|\lambda^+\rangle, |\lambda^-\rangle\}$ where

$$|\lambda^{\pm}\rangle = \frac{1}{\sqrt{2}}\big(|\Phi^-\rangle \pm |\Psi^+\rangle\big). \tag{5.17}$$

Alice sends the respective qubits to Bob and Charlie who perform a measurement

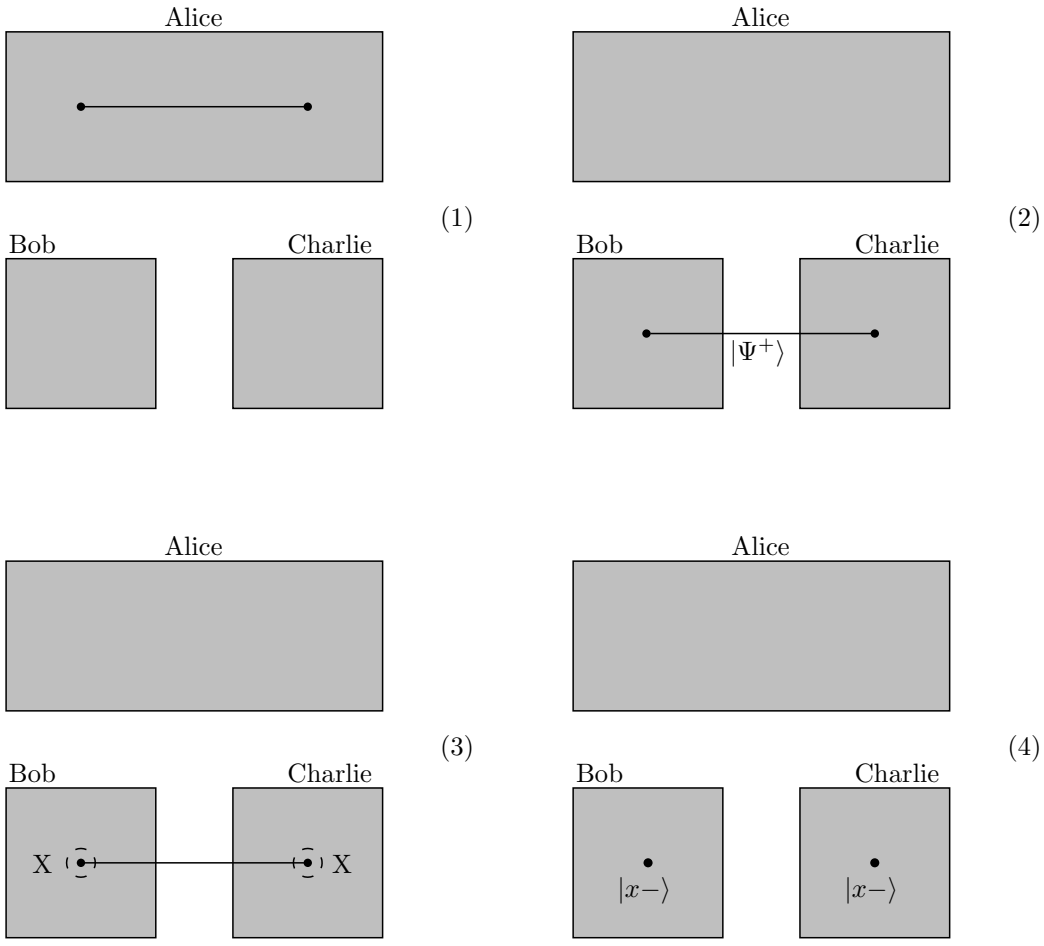

Figure 5.5: *(KKI secret sharing scheme))* Illustration of the QSS protocol by Karlsson et al. [84].

		Charlie			
		$\|0\rangle$	$\|1\rangle$	$\|x^+\rangle$	$\|x^-\rangle$
Bob	$\|0\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$	$\|\lambda^+\rangle$	$\|\lambda^-\rangle$
	$\|1\rangle$	$\|\Psi^+\rangle$	$\|\Phi^-\rangle$	$\|\lambda^-\rangle$	$\|\lambda^+\rangle$
	$\|x^+\rangle$	$\|\lambda^+\rangle$	$\|\lambda^-\rangle$	$\|\Psi^+\rangle$	$\|\Phi^-\rangle$
	$\|x^-\rangle$	$\|\lambda^-\rangle$	$\|\lambda^+\rangle$	$\|\Phi^-\rangle$	$\|\Psi^+\rangle$

Table 5.3: Bob's and Charlie's results depending on Alice's initial state.

according to the Z or X basis (cf. pictures (2) and (3) in figure 5.5). As already described in section 2.1 above, the Bell states can be described in the Z basis as

$$|\Phi^-\rangle_{BC} = \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big)_{BC} \quad |\Psi^+\rangle_{BC} = \frac{1}{\sqrt{2}}\big(|01\rangle + |10\rangle\big)_{BC} \tag{5.18}$$

and similarly for the X basis. If both Alice and Bob measure in different bases the two states are written as

$$\begin{aligned} |\lambda^+\rangle_{BC} &= \frac{1}{\sqrt{2}}\big(|0\rangle|x+\rangle + |1\rangle|x-\rangle\big)_{BC} &&= \frac{1}{\sqrt{2}}\big(|x+\rangle|0\rangle + |x-\rangle|1\rangle\big)_{BC} \\ |\lambda^-\rangle_{BC} &= \frac{1}{\sqrt{2}}\big(|0\rangle|x-\rangle + |1\rangle|x+\rangle\big)_{BC} &&= \frac{1}{\sqrt{2}}\big(|x+\rangle|1\rangle + |x-\rangle|0\rangle\big)_{BC}. \end{aligned} \tag{5.19}$$

From this results a relation between Bob's and Charlie's similar to table 5.2 above can be defined (cf. table 5.3).

Both parties publicly declare their measurement results (0 or 1) for a fraction of their bits to test for eavesdropping. After the results are announced they also declare their respective basis (Z or X) for all of their measurements. Karlsson et al. stress in their article [84] that the chronological order in which the measurement results and bases are declared is crucial for the security (see section 6.3.4 for details). The party who first declared the measurement outcomes has to be the last to declare the respective basis. When Alice and Bob revealed their bases Alice announces all the bases in which she prepared the initial state and also her exact state for the test bits. Using this information Alice and Bob are able to individually perform a check for adversaries. Further, if no adversary is present, they have to discard approximately half of their results where they chose the wrong bases according to the basis of Alice's initial state. From the other half Bob and Charlie can calculate Alice's initial state only if they combine their results.

5.3.3 Sharing Quantum Secrets

Although usually classical information, i.e. classical bits, are shared using QSS protocols there are also schemes where quantum information, i.e. a quantum state, is shared between two parties. Such protocols are called *quantum state sharing* (QSTS) schemes [89]. In contrary to a classical secret, which is located at Bob's and Charlie's laboratory at the end of the protocol, the two parties will not each end up with a copy of the secret quantum state, since that would violate the no-cloning theorem [166]. In case of quantum state sharing the two parties have to work together to recreate the secret quantum state at one of their laboratories.

A first protocol for quantum state sharing was introduced by Li et al. [92] where they present a scheme to share a qubit in an arbitrary state between two parties. Therefore, Alice shares two Bell states $|\Phi^+\rangle$, one with Bob and one with Charlie (cf. picture (1) in figure 5.6), and prepares the secret state as

$$|\phi\rangle_S = \alpha|0\rangle + \beta|1\rangle \tag{5.20}$$

with $|\alpha|^2 + |\beta|^2 = 1$. It is crucial for the security of the protocol that the Bell states are not tempered during their distribution (cf. sec 6.3 for details). The overall state of Alice, Bob and Charlie is then

$$|\phi\rangle_S \otimes |\Phi^+\rangle_{A_1B} \otimes |\Phi^+\rangle_{A_2C} \tag{5.21}$$

where Bob is in possession of qubit B and Charlie of qubit C. Alice then performs a complete GHZ measurement on all of her qubits (cf. picture (2) in figure 5.6), i.e. qubits S, A_1 and A_2 are projected onto the subspace spanned by the GHZ states (cf. eq. (2.15) in section 2.2). The overall system described in eq. (5.21) can be written in the GHZ basis as

$$\begin{aligned}\frac{1}{\sqrt{2}}\Big[&|P^+_{00}\rangle_{SA_1A_2}\big(\alpha|00\rangle + \beta|11\rangle\big)_{BC} + |P^-_{00}\rangle_{SA_1A_2}\big(\alpha|00\rangle - \beta|11\rangle\big)_{BC}\\ &+|P^+_{01}\rangle_{SA_1A_2}\big(\alpha|01\rangle + \beta|10\rangle\big)_{BC} + |P^-_{01}\rangle_{SA_1A_2}\big(\alpha|01\rangle - \beta|10\rangle\big)_{BC}\\ &+|P^+_{10}\rangle_{SA_1A_2}\big(\alpha|10\rangle + \beta|01\rangle\big)_{BC} + |P^-_{10}\rangle_{SA_1A_2}\big(\alpha|10\rangle - \beta|01\rangle\big)_{BC}\\ &+|P^+_{11}\rangle_{SA_1A_2}\big(\alpha|11\rangle + \beta|00\rangle\big)_{BC} + |P^-_{11}\rangle_{SA_1A_2}\big(\alpha|11\rangle - \beta|00\rangle\big)_{BC}\Big]\end{aligned} \tag{5.22}$$

such that after the GHZ state measurement the information of the secret qubit S is equally distributed between the qubits in Bob's and Charlie's possession. Moreover,

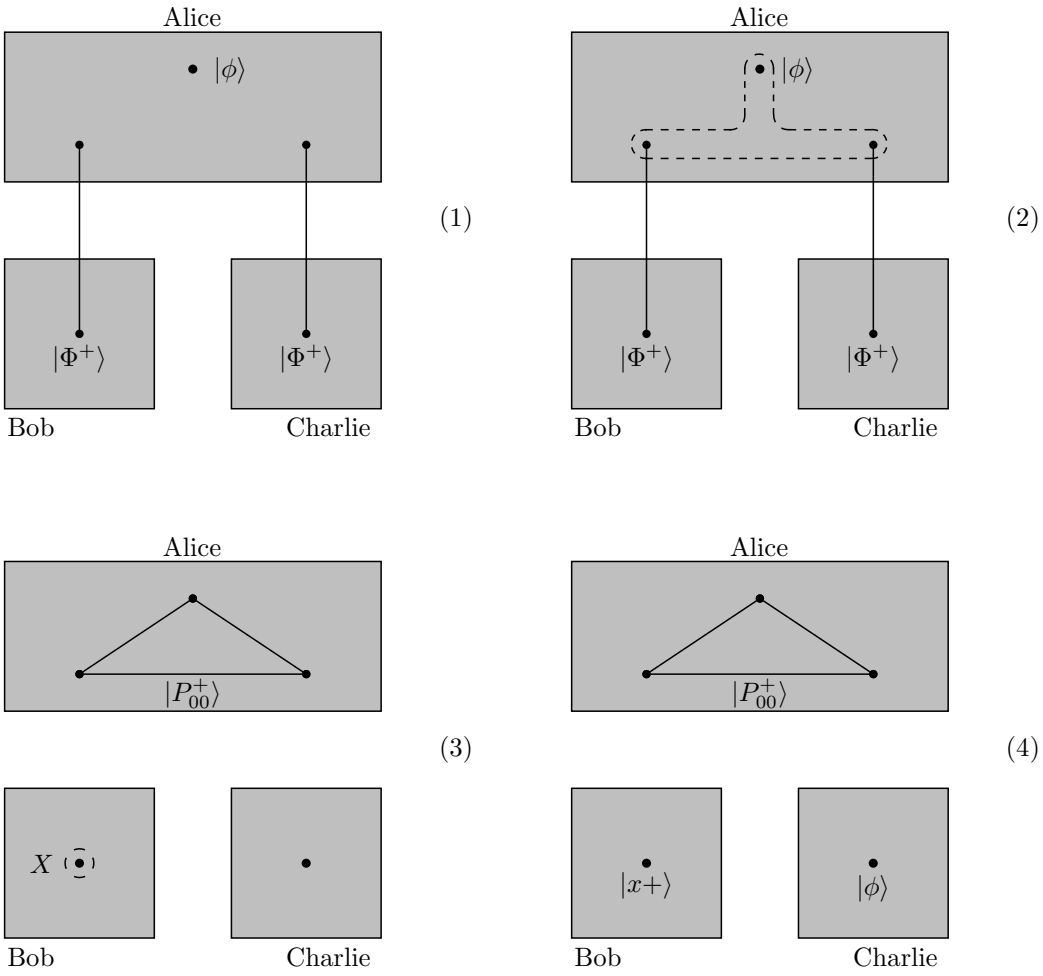

Figure 5.6: Illustration of the QSTS protocol by Li et al. [92].

the qubits B and C end up in an entangled state as given in eq. (5.22). Alice publicly reveals her measurement outcome such that Bob and Charlie are able to recover the secret qubit. To achieve that Alice specifies one party at random, say Bob, who performs a measurement in the X-basis on his qubit (cf. picture (3) in figure 5.6) and tells Charlie his result. Assuming Alice's result is $|P_{00}^+\rangle$, Bob's and Charlie's state is $\alpha|00\rangle_{BC} + \beta|11\rangle_{BC}$ and can be written in the X-basis as

$$\frac{1}{\sqrt{2}}\big[|x+\rangle_B\big(\alpha|0\rangle + \beta|1\rangle\big)_C + |x-\rangle_B\big(\alpha|0\rangle - \beta|1\rangle\big)_C\big]. \tag{5.23}$$

With the information about Bob's measurement result Charlie is able to identify an operation (in this case $\mathbb{1}$ or σ_z) to reconstruct the secret state in his laboratory. Further, eq. (5.22) and (5.23) show that neither Bob nor Charlie are able to obtain Alice's secret state from their own states.

It is also possible to share more than one qubit, as Deng et al. presented in two QSTS-schemes [38, 39]. In the scheme presented in [39] they showed how to share an arbitrary 2-qubit state between two parties as a rather straight forward extension of the above protocol [92]. In this scheme, Alice prepares four Bell states of the form

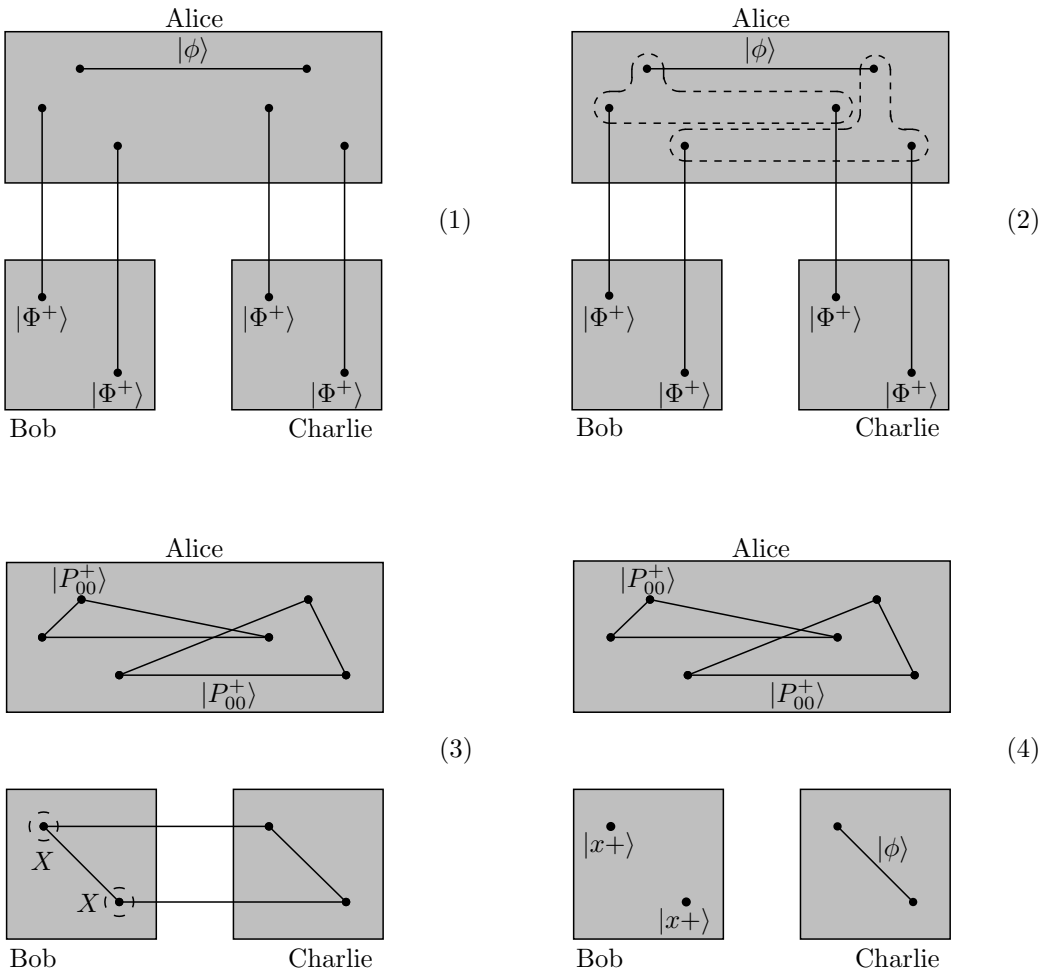

Figure 5.7: Illustration of the QSTS protocol by Deng et al. [39].

$|\Phi^+\rangle$ together with the secret 2-qubit state

$$|\phi\rangle_{S_1S_2} = \alpha|00\rangle_{S_1S_2} + \beta|01\rangle_{S_1S_2} + \gamma|10\rangle_{S_1S_2} + \delta|11\rangle_{S_1S_2} \tag{5.24}$$

with $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$. This leads to the overall state of the system (cf. picture (1) in figure 5.7)

$$|\phi\rangle_{S_1S_2} \otimes |\Phi^+\rangle_{A_1B_1} \otimes |\Phi^+\rangle_{A_2B_2} \otimes |\Phi^+\rangle_{A_3C_1} \otimes |\Phi^+\rangle_{A_4C_2}. \tag{5.25}$$

Previously to the protocol Alice sends qubit B_1 and B_2 to Bob and qubits C_1 and C_2 to Charlie. Again, it is crucial for the security of the protocol that the Bell states are not tempered during their distribution (cf. sec 6.3 for details). As her first step Alice performs two GHZ measurements, one on qubits S_1, A_1 and A_3 and the other on qubits S_2, A_2 and A_4 (cf. picture (2) in figure 5.7). Similar to eq. (5.22), this teleports the information of qubits S_1 and S_2 onto the respective qubits in Bob's and Charlie's possession. For example, if Alice obtains $|P_{00}^{+}\rangle_{S_1A_1A_3}$ and $|P_{00}^{+}\rangle_{S_2A_2A_4}$, Bob's and Charlie's state is

$$\big(\alpha|0000\rangle + \beta|0101\rangle + \gamma|1010\rangle + \delta|1111\rangle\big)_{B_1B_2C_1C_2}. \tag{5.26}$$

Alice reveals her measurement outcomes such that the other two parties are able to recover the secret state. Afterwards, Bob measures his two qubits in the X-basis (cf. picture (3) in figure 5.7). Since the state from eq. (5.26) can be rewritten as

$$\begin{aligned}\frac{1}{2}\Big[&|x+\rangle_{B_1}|x+\rangle_{B_2}\big(\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle\big)_{C_1C_2}\\ &+|x+\rangle_{B_1}|x-\rangle_{B_2}\big(\alpha|00\rangle - \beta|01\rangle + \gamma|10\rangle - \delta|11\rangle\big)_{C_1C_2}\\ &+|x-\rangle_{B_1}|x+\rangle_{B_2}\big(\alpha|00\rangle + \beta|01\rangle - \gamma|10\rangle - \delta|11\rangle\big)_{C_1C_2}\\ &+|x-\rangle_{B_1}|x-\rangle_{B_2}\big(\alpha|00\rangle - \beta|01\rangle - \gamma|10\rangle + \delta|11\rangle\big)_{C_1C_2}\Big]\end{aligned} \tag{5.27}$$

Charlie is able to reconstruct the secret state $|\phi\rangle$ from his qubits from the public information about Alice's measurement results and Bob's secret measurement results. Solely from their local information neither Bob nor Charlie is able to recover Alice's state $|\phi\rangle$, i.e. the two parties have to collaborate.

In the other QSTS-scheme by Deng et al. [38] published in the same year they used a slightly different method to share the secret two-qubit state $|\phi\rangle_{S_1S_2}$ between Bob and Charlie. In this scheme Alice prepares two GHZ-states, e.g. $|P_{00}^{+}\rangle_{A_1B_1C_1}$ and $|P_{00}^{+}\rangle_{A_2B_2C_2}$, and sends qubits B_1 and B_2 to Bob and C_1 and C_2 to Charlie, respectively. Therefore, the initial state of the overall system is (cf. picture (1) in figure 5.8)

$$|\phi\rangle_{S_1S_2} \otimes |P_{00}^{+}\rangle_{A_1B_1C_1} \otimes |P_{00}^{+}\rangle_{A_2B_2C_2} \tag{5.28}$$

Then, she again makes use of quantum teleportation to distribute the secret between the two parties. Alice performs a Bell state measurement onto one qubit of the secret state and one qubit of the GHZ state, i.e. onto qubits S_1 and A_1 as well as S_2 and A_2

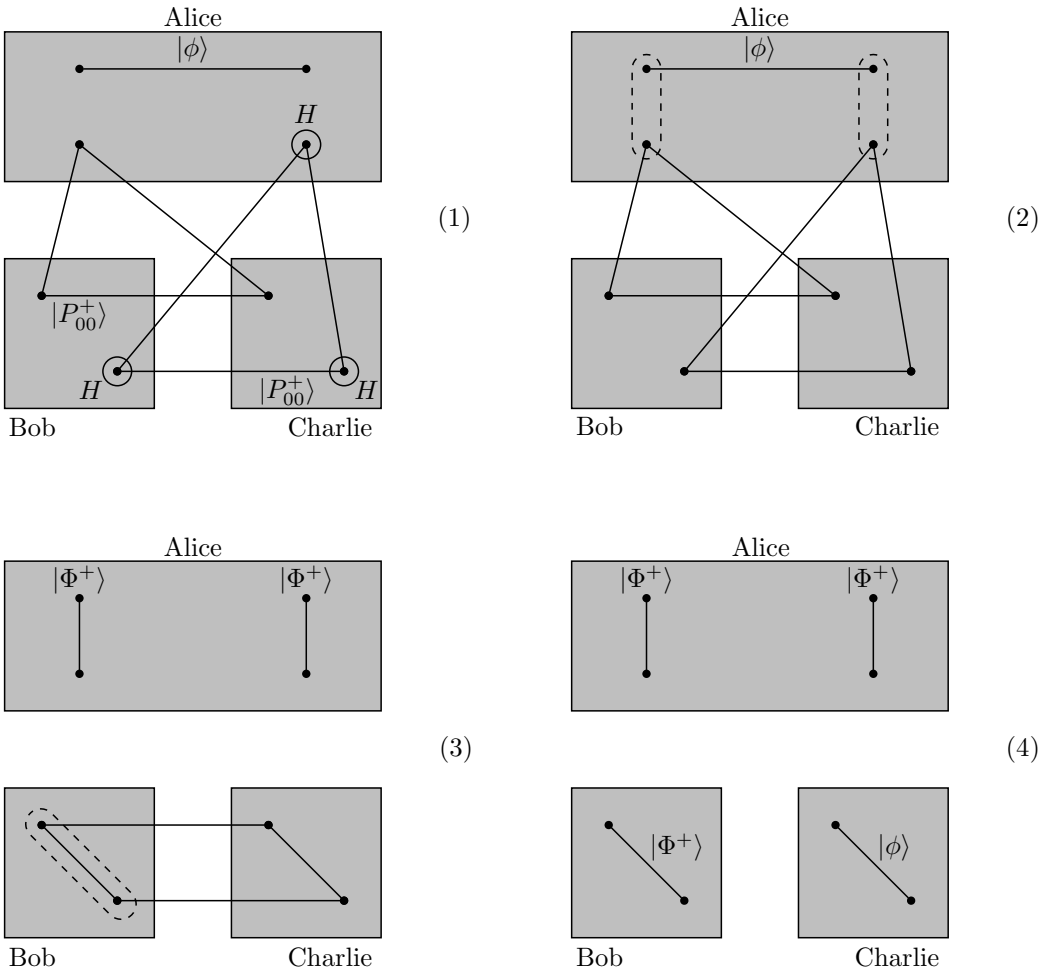

Figure 5.8: Illustration of the QSS protocol by Deng et al. [38].

(cf. picture (2) in figure 5.8). Assuming that Alice obtains $|\Phi^{+}\rangle_{S_1A_1}$ and $|\Phi^{+}\rangle_{S_2A_2}$ the state of the remaining qubits is then

$$\big(\alpha|0000\rangle + \beta|0011\rangle + \gamma|1100\rangle + \delta|1111\rangle\big)_{B_1C_1B_2C_2} \tag{5.29}$$

Hence, the remaining qubits at Bob's and Charlie's laboratory contain the full information about the secret state. Similar to the protocols described already, Bob and Charlie still need Alice's measurement result to reconstruct $|\phi\rangle_{S_1S_2}$. Thus, Alice publicly announces the results of her Bell state measurements and one of the other parties, let's say Bob, also performs a Bell state measurement and announces his result (cf. picture (3) in figure 5.8). As it is pointed out in [38], Bob's Bell state measurement destroys some of the information about the secret state. Thus, Alice has to use a trick to overcome that: she applies a Hadamard operation H on qubit

A_2, B_2 and C_2 of the second GHZ state (cf. picture (1) in figure 5.8) thus changing the state to

$$\frac{1}{2}\Big(|000\rangle + |011\rangle + |101\rangle + |110\rangle\Big)_{A_2B_2C_2}. \tag{5.30}$$

Based on this altered initial state the qubits B_1, B_2, C_1 and C_2 are then in the state

$$\begin{aligned}\big(&\alpha|0000\rangle + \alpha|0011\rangle + \gamma|1100\rangle + \gamma|1111\rangle \\ &\beta|0001\rangle + \beta|0010\rangle + \delta|1101\rangle + \delta|1110\rangle\big)_{B_1C_1B_2C_2}\end{aligned} \tag{5.31}$$

after Alice performed her measurements (assuming she obtains from her measurement $|\Phi^+\rangle_{S_1A_1}$ and $|\Phi^+\rangle_{S_2A_2}$). Hence, Charlie finally ends up with

$$\alpha|00\rangle_{C_1C_2} + \beta|01\rangle_{C_1C_2} + \gamma|11\rangle_{C_1C_2} + \delta|10\rangle_{C_1C_2} \tag{5.32}$$

after Bob's measurement (assuming Bob obtains $|\Phi^+\rangle_{B_1B_2}$). Using Bob's result Charlie is able to identify two unitary operations (in this case they are both the identity) to apply on his qubits followed by a CNOT operation on both of them to correct the state in his possession and reconstruct the secret $|\phi\rangle_{S_1S_2}$.

Both schemes [38, 39] can be extended rather straight forward to a m-qubit secret $|\phi\rangle_{S_1\cdots S_m}$, i.e.

$$|\phi\rangle_{S_1\cdots S_m} = \sum_{i=0}^{m-1} \alpha_i |i_b\rangle_{A_i} \tag{5.33}$$

where i_b is the binary form of i and $\sum |\alpha_i|^2 = 1$. Therefore, in the first scheme [39] Alice has to create 2 Bell states for every qubit of her secret state. In contrary, in the second scheme [39] Alice has to create one GHZ state for every qubit of $|\phi\rangle_{S_1\cdots S_m}$. Hence, in the first protocol Alice needs m qubits more than the second protocol to share an m-qubit secret state. As it is discussed in the general case in section 5.3.4 below, this number multiplies with the number of parties the secret is shared among. Although it uses more qubits, the main advantage of the first protocol is that it only uses Bell states as a quantum channel between the parties, which can be generated at a high rate and in a good quality rather easily with nowadays technology (cf. section 5.2.4 for implementations of sources of Bell states in QKD systems). In the second protocol 3-qubit GHZ states (and in the general case n-qubit GHZ states, see section 5.3.4 below) are needed, which are much more complex to create. Regarding the measurement in the respective schemes the second protocol is based on Bell state measurements which are easier to implement compared to the complete GHZ state measurement in the first protocol. Nevertheless, compared to the effort of preparing

GHZ states it is much easier to measure in the GHZ basis, which makes the first protocol more interesting for an actual implementation in a laboratory.

In a later article Deng et al. presented two other QSTS protocols to share an arbitrary 2-qubit state [40]. Here, Alice starts with the same overall state from eq.

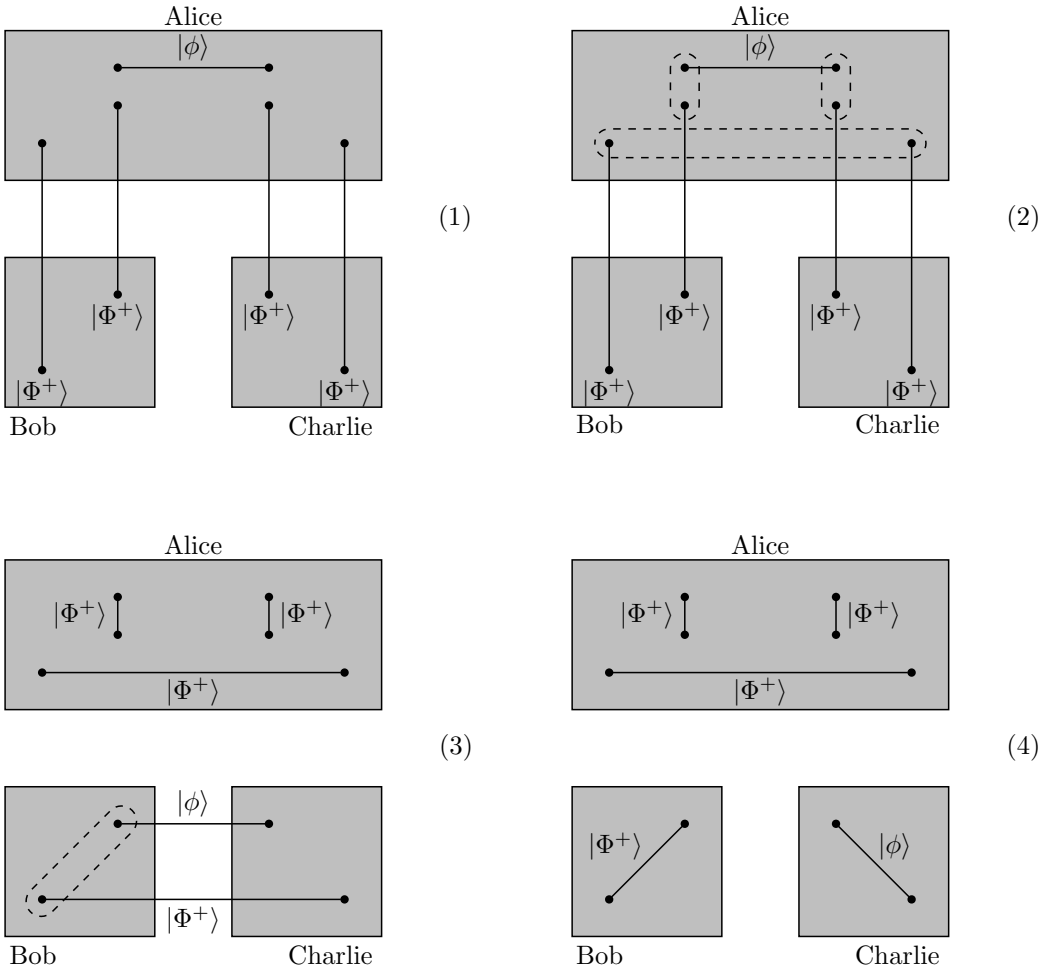

Figure 5.9: Illustration of the QSS protocol by Deng et al. [40].

(5.25) where the secret 2-qubit state $|\phi\rangle_{S_1S_2}$ is the same as in eq. (5.24) (cf. picture (1) in figure 5.9). The distribution of the qubits is also the same as in [39]: Alice is in possession of qubits S_1, S_2, A_1, A_2, A_3, and A_4, Bob is in possession of B_1 and B_2 and Charlie of qubits C_1 and C_2. In a first step Alice swaps the secret state $|\phi\rangle_{S_1S_2}$ onto the qubits B_2 and C_1 (cf. section 2.5.3 for details on entanglement swapping). She achieves that by performing a Bell-state measurement on qubits S_1 and A_2 as well as S_2 and A_3 (cf. picture (2) in figure 5.9) which leaves the remaining qubits

in the state (assuming that Alice obtains $|\Phi^+\rangle_{S_1A_2}$ and $|\Phi^+\rangle_{S_2A_3}$)

$$|\phi\rangle_{B_2C_1} \otimes |\Phi^+\rangle_{A_1B_1} \otimes |\Phi^+\rangle_{A_4C_2} \tag{5.34}$$

Afterwards, she publicly announces her results. Hence, Bob and Charlie each have one half of the secret state but can not obtain any information from their qubit. Further, Alice performs a second Bell state measurement on qubit A_1 and A_4 to entangle qubits B_1 and C_2. Let's say Alice again obtains $|\Phi^+\rangle_{A_1A_4}$ from her measurement then the qubits B_1 and C_2 are also in the Bell state $|\Phi^+\rangle_{B_1C_2}$. Now, Bob and Charlie are able to use the entangled state of qubits B_1 and C_2 to teleport the secret state into either of their laboratories (cf. picture (3) and (4) in figure 5.9). Nevertheless, to reconstruct the state after the teleportation, for example at Charlie's laboratory, Bob has to send him the outcome of his measurement. Otherwise Charlie has no chance to recover the secret by himself.

Since this scheme is very source intensive for Alice (she has to prepare 4 Bell states and distribute them between Bob and Charlie) Deng et al. also suggest a "circular" version of the protocol [40]. In this protocol the qubit pair A_1 and B_1 can be omitted and Bob and Charlie create qubits A_4 and C_2 themselves to establish a Bell state between them. The rest of the protocol is similar to the one described above. The secret state $|\phi\rangle_{S_1S_2}$ is teleported onto qubits B_2 and C_1 by Alice and later on either into Bob's or Charlie's laboratory where it is reconstructed.

5.3.4 Multiparty Secret Sharing

Sharing a secret – classical or quantum – between two parties as in the schemes described above is often not enough. Usually, more parties are involved in the communication and the secret has to be shared among all of them. Therefore, some QSS protocols can be extended to the multiparty case.

Looking at the HBB scheme an extension to n parties has been presented in [167]. Alice prepares copies of the n-partite GHZ state

$$|P^+_{0\ldots0}\rangle = \frac{1}{\sqrt{2}}(|000\ldots0\rangle + |111\ldots1\rangle)_{AB_1\ldots B_{n-1}} \tag{5.35}$$

and distributes $n-1$ qubits of every state to her communication partners, now denoted B_1 to B_{n-1} (cf. pictures (1) and (2) in figure 5.10). As in the original protocol, each party randomly chooses between the X and the Y basis and performs a measurement in the respective basis. It is stressed in [167] and also in [68] that the

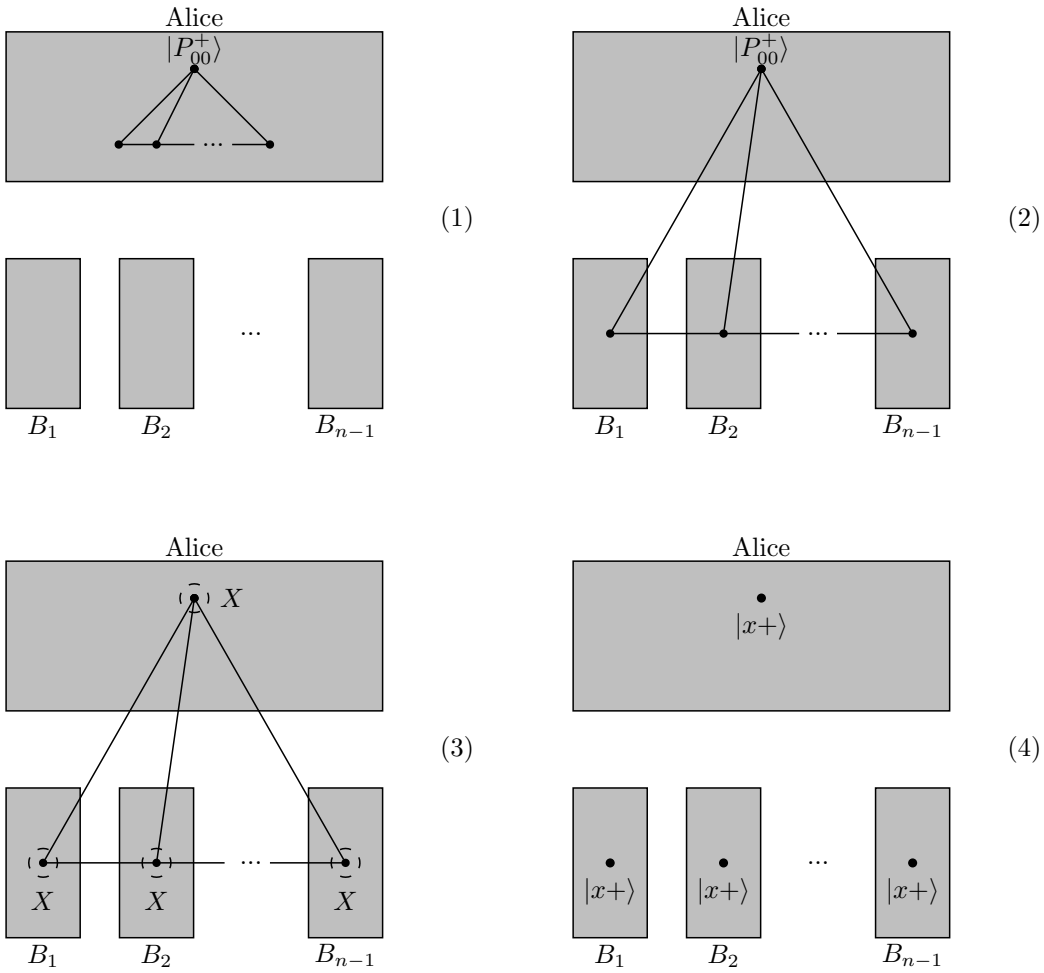

Figure 5.10: Illustration of the extension of the HBB protocol to n parties [167].

number of parties using the Y basis has to be even. The n-qubit state $|\Psi\rangle$ can also be written in the X and Y basis (similar to eq. (5.16)) such that it is – in theory – possible to generate a list of correlations like in table 5.2 for Alice's result and the result of each B_i. Since this table would be too complex for large n there is another possibility to model the correlations between the results more conveniently [167]. Assigning the value 0 to $|x^+\rangle$ and $|y^+\rangle$ and 1 to $|x^-\rangle$ and $|y^-\rangle$ Alice's measurement result can be computed using the modulo 2 sum of the results of B_1 to B_{n-1}. There are only two distinct cases to be aware of: if the number of applications of the Y basis is $4k$, with k some non-negative integer, Alice's result r_A can be computed intuitively as

$$r_A = r_{B_1} \oplus r_{B_2} \oplus \cdots \oplus r_{B_{n-1}}. \tag{5.36}$$

Otherwise, if the number of parties using the Y basis is $2(2k+1)$ Alice's result is

computed as

$$r_A = r_{B_1} \oplus r_{B_2} \oplus \cdots \oplus r_{B_{n-1}} \oplus 1, \tag{5.37}$$

i.e. the value is the inverse of the sum of the results of the B_i. After Alice distributed all qubits each of the B_i publicly announces his choice to make sure that an even number of parties has chosen the Y basis. If the number is odd, the respective qubits have to be discarded. Then Alice selects a subset of all measurements and each B_i discloses his result for the respective measurement and Alice is able to check if some parties are dishonest or if an eavesdropper is present. If no adversary is found the B_i collaborate and use their remaining measurement results to determine Alice's secret.

When looking at quantum state sharing the protocol presented by Li et al. [92] can also be generalized to n parties. In this case Alice prepares $n-1$ Bell states of the form $|\Phi^+\rangle$ and sends one qubit to each Bob $B_1 \cdots B_{n-1}$ (cf. picture (1) in figure 5.11). The secret state $|\phi\rangle_S$ Alice wants to share is the same as given in 5.20. Thus, the overall state of the system is

$$|\phi\rangle_S \otimes \left(|\Phi^+\rangle_{A_iB_i}\right)^{\otimes(n-1)} \tag{5.38}$$

where the qubits A_i are kept by Alice and the qubits B_i are sent to the respective Bobs. Similar to the 3-party protocol, Alice performs a general n-qubit GHZ measurement, i.e. a measurement projecting the system onto the basis described by the n qubit GHZ states (cf. section 5.3.3 above). This projects the state of Alice's qubits onto a n-qubit GHZ state and the secret state $|\phi\rangle_S$ is distributed onto the remaining qubits, i.e. the overall state is similar to eq. (5.22) (cf. pictures (2) and (3) in figure 5.11). To recover the secret $n-2$ of the Bob's perform a measurement in the X basis on their respective qubit. The one party, call it B_{n-1}, who does not perform the measurement will end up with a state very similar to the secret state $|\phi\rangle_S$. Using the information about Alice's result and the results of all the other Bobs it is possible for B_{n-1} to reconstruct the secret state.

In [39] Deng et al. described how to extend their scheme to n parties. Therefore, Alice prepares $2(n-1)$ Bell states and shares them with the Bobs $B_1 \cdots B_{n-1}$. The overall state of the scheme can then be written as

$$|\phi\rangle_{S_1S_2} \bigotimes_{i=1}^{n-1} \left(|\Phi^+\rangle_{A_iB_i} \otimes |\Phi^+\rangle_{A_kC_i}\right) \tag{5.39}$$

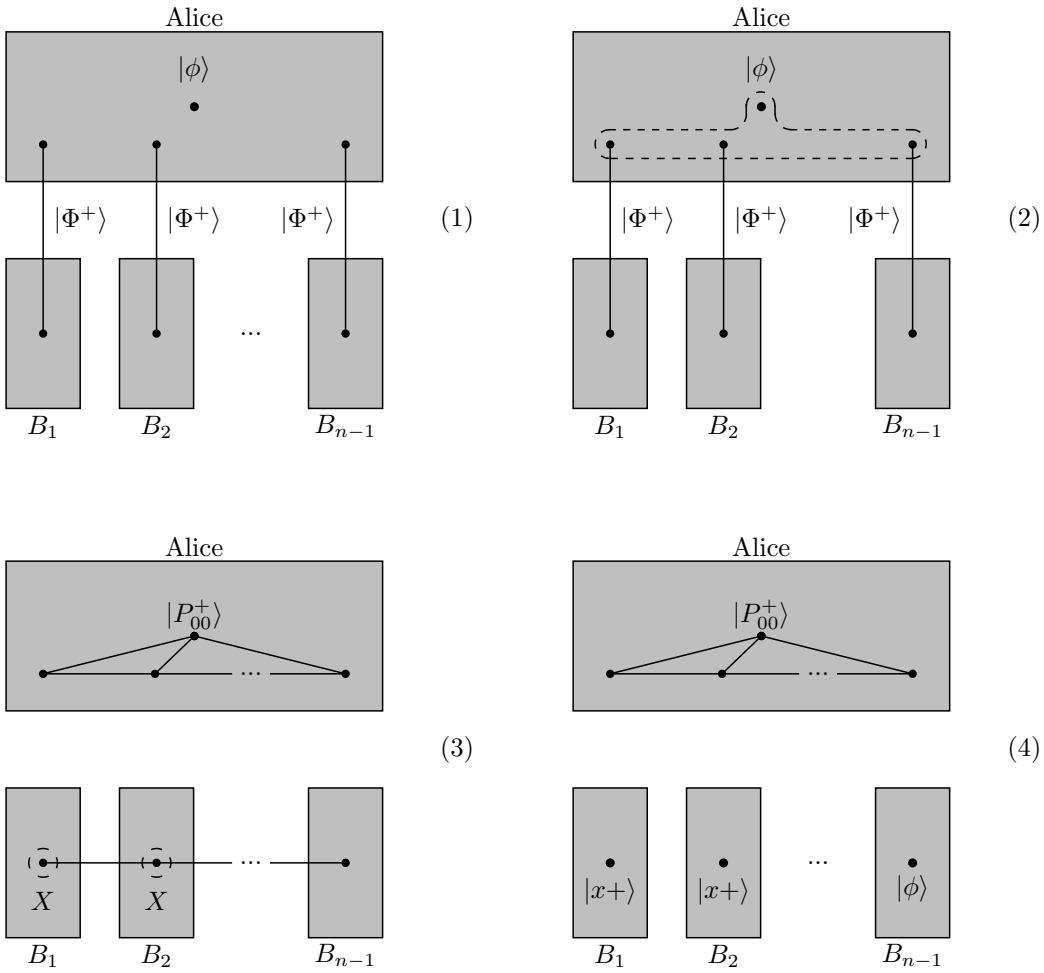

Figure 5.11: Illustration of the extension of the QSS protocol by Li et al. to n parties [92].

where $k = n - 1 + i$. Similar to the version for 3 parties described shortly in section 5.3.3 above Alice performs a complete n-qubit GHZ state measurement on qubit S_1 and the qubits $A_1 \cdots A_{n-1}$ as well as on qubit S_2 and the qubits labeled $A_n \cdots A_{2(n-1)}$ in her possession. As a result Alice obtains two n-qubit GHZ states and she announces her results publicly. Further, the Bobs $B_1 \cdots B_{n-2}$ measure the two qubits in each of their laboratories according to the X basis and reveal their results to B_{n-1} who is then able to identify a unitary operation to recover the secret state $|\phi\rangle$ from the qubits in his possession.

In the multiparty-version of the second protocol by Deng et al. [38] Alice prepares two n-qubit GHZ states of the form

$$|P_{0\cdots0}^+\rangle_{A_1B_1\cdots B_{n-1}} = \frac{1}{\sqrt{2}}\Big(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\Big)_{A_1B_1\cdots B_{n-1}} \tag{5.40}$$

and

$$|P^{+}_{0\cdots0}\rangle_{A_2C_1\cdots C_{n-1}} = \frac{1}{\sqrt{2}}\Big(|0\rangle^{\otimes n} + |1\rangle^{\otimes n}\Big)_{A_2C_1\cdots C_{n-1}} \tag{5.41}$$

to share the secret 2-qubit state $|\phi\rangle_{S_1S_2}$. Alice sends the qubits B_i and C_i to the respective Bobs and then performs Bell measurements on S_1 and A_1 and S_2 and A_2. This distributes the secret state among all the Bobs. Each one of the parties B_i except the last one performs a Bell state measurement on the two qubits B_i and C_i in his possession such that the total information about the secret is brought onto the two qubits in the laboratory of B_{n-1}. Using the information about Alice's measurement result together with the results of the other Bobs B_i, the party B_{n-1} is able to reconstruct the secret state using a specific unitary operation identified by the results. As already pointed out above it is stressed in [38] that a Hadamard operation has to be applied on every qubit of the second state $|P^{+}_{0\cdots0}\rangle_{A_2C_1\cdots C_{n-1}}$ to make a conclusive reconstruction of the secret possible.

The most general case is, of course, to share an m-qubit state $|\phi\rangle_{S_1\cdots S_m}$ between $n-1$ different parties $B_1\cdots B_n$, which can be easily achieved using the protocols just presented. Taking, for example, the protocol from [38] Alice has to prepare m copies of the n-qubit GHZ state $|P^{+}_{0\cdots0}\rangle_{A_1B_1\cdots B_{n-1}}$ and send the B_i of each state to the respective communication party. Afterwards, she performs Bell state measurements on each pair S_i of the secret state and A_i of the n-qubit GHz state to teleport the information to each party B_i. This gives every party a piece of the information about the secret state but not enough to recover it by himself. All parties have to come together to combine their information as described in the original protocol [38] such that one single party is able to reconstruct the secret. The major drawback of this scheme is, as mentioned in the previous section, the creation of n-qubit GHZ states is very complex in practice.

A multi-qubit version of the protocol in [39] is more efficient since only Bell states are used. In this case Alice has to prepare $m(n-1)$ Bell states $|\Phi^{+}\rangle$ to share the m-qubit state $|\phi\rangle_{S_1\cdots S_m}$ between $n-1$ parties. Again, the respective protocol to achieve that is generalized straight-forwardly from the original scheme: starting with the initial state

$$|\phi\rangle_{S_1\cdots S_m} \otimes \bigotimes_{j=1}^{m}\bigotimes_{i=1}^{n-1} |\Phi^{+}\rangle_{A_{ji}B_{ji}} \tag{5.42}$$

Alice sends the qubits B_{ji} to the respective Bobs. Then, for every j she performs a n-qubit GHZ state measurement on S_j and all the B_{ji}. As already described in

the original protocol this distributes the secret state between all the Bobs such that they have to bring their informations together to reconstruct the state.

We see that this protocol [39] is also easier to implement and more efficient when dealing with multi-qubit secrets. Although it consumes roughly twice as much qubits as the protocol in [38] it is much easier to generate the Bell states applied in this protocol and perform a measurement in the n-qubit GHZ basis than to generate the n-qubit GHZ states and perform Bell state measurements.

5.3.5 Physical Realizations

Physical realizations of quantum secret sharing protocols have not been of such great interest as implementations of quantum key distribution protocols. Hence, no experiment realizing a QSS protocol in a real-world environment has yet been accomplished. One major reason is that most QSS schemes make heavy use of multipartite entangled states like GHZ states. Whereas today it is rather easy to generate 2-qubit entanglement and use it for QKD protocols the generation of GHZ states and states of higher dimensions is still rather difficult.

The first implementation of a QSS protocol was performed by Tittel et al. [147] where an HBB scheme was realized. Since the generation of GHZ states was very difficult at that time, as just pointed out, a so called *pseudo GHZ state* was used instead. The main difference to a true GHZ state is that this state is based on a source creating energy-time entangled Bell states and that the three photons do not exist at the same time. Hence, it is obvious that tests for the non-locality are of no significance for this state. Nevertheless, the probability function describing the coincidences of the three photons is the same as the one coming from a true GHZ state. With this setup a rate of maximally 800 coincidences in 50 seconds was achieved [147] which shoes that QSS is in principle possible. The rate is of course far too low to perform actual communication, i.e. to share a secret of reasonable length.

An implementation using an actual GHZ state was first presented by Chen et al. [31]. In this setup a 4-qubit GHZ state

$$|\varphi\rangle = \frac{1}{\sqrt{2}}\big(|0000\rangle + |1111\rangle\big) \tag{5.43}$$

is created by basically sending two Bell states through a polarization beam splitter. The main idea is that it is not possible to distinguish from which source each photon

originated after it passed through the polarization beam splitter. The desired 3-qubit state is then obtained from the 4-qubit state using a projection of one particle onto the state $|x+\rangle$. The QSS protocol implemented in this experiment is again the HBB scheme. The experiment succeeds in sharing a key between Alice, Bob and Charlie with an average rate of a quarter bit per second [31].

A more recent experiment has been done by Gaertner et al. [56] where they succeeded in sharing a secret between four parties. Therefore, the 4-qubit GHZ state

$$|\varphi\rangle = \frac{1}{2\sqrt{3}}\big(2|0011\rangle - |0101\rangle - |0110\rangle - |1001\rangle - |1010\rangle + 2|1100\rangle\big) \tag{5.44}$$

is generated. As it is described in [56] this state perfectly fulfills the correlation function needed for the protocol. In contrary to the HBB protocol the four parties involved in this experiment perform their measurements in different bases. They either choose a set of bases similar to the BB84 protocol (cf. section 5.2.1) or similar to the Ekert protocol (cf. section 5.2.2). Thus, when checking for eavesdroppers they can use the techniques from the BB84 protocol or try to violate a Bell-like inequality like in the Ekert protocol. The rest of the protocol is rather similar to the ones previously discussed. Regarding the efficiency of the experiment 2000 raw key bits were exchanged in about 16 hours, which leads to a secret key bit rate of 100 bits per hour [56].

Chapter 6

Security of Single-Qubit Protocols

In the previous chapter it has been pointed out that the protocols described there are not secure per se since information about the secret key can leak to an adversary. Additional procedures like error correction and privacy amplification have to be applied to guarantee security. Therefore, it is important to estimate the amount of information an eavesdropper can obtain when infiltrating the protocol. The actions an eavesdropper is able to perform can be classified in different attack scenarios, which are then inspected in detail. Some passages of this chapter are closely related to [127].

The protocols discussed in this chapter are called *single-qubit* because we refer to the qubits in transit between Alice and Bob at one specific iteration of the protocol. For the BB84 protocol and similar schemes described in the last chapter this is obvious. The Ekert protocol also fits in this category, although there is an entangled qubit pair involved, since the party in possession of the source keeps one qubit at its own laboratory. In the next chapter we focus on more complex attacks on protocols where two or more qubits are involved.

6.1 Basics from Information Theory

In the discussions about the security of QKD protocols Eve's information about the secret key shared between Alice and Bob is of main interest. To provide an overview on the basic principles we want to sketch only the most important mechanisms coming from information theory and identify their connection to the security of quantum cryptography. For further information confer the excellent textbooks by

Cover and Thomas [36] as well as MacKay [99].

Every attack on a QKD protocol is characterized by the amount of information Eve is able to obtain about the secret key. Hence, Alice's and Bob's goal is to minimize Eve's information. Usually, Eve's information about the secret key consists of two parts: the information she obtains from her measurements on the signals in transit and the information about Alice's and Bob's choice of bases. The second part tells Eve whether she performed her measurement in the correct basis for the respective qubit or not. In the latter case she introduces an error since her intervention alters the state of the qubit. The probability that Eve obtains the result m from her measurement if Alice originally sent the secret classical bit s is best expressed by the *conditional probability* $p(m|s)$.

For the computation of Eve's information about Alice's classical bit s we need another conditional probability, $p(s|m)$. This is the probability that Eve obtains the classical bit s if her measurement outcome is m. The value $p(s|m)$ can be computed directly using the probabilities $p(m|s)$ by the formula based on Bayes' theorem

$$p\big(s|m\big) = \frac{p(m|s)}{\sum_{s'} p(m|s')} \tag{6.1}$$

Another interesting quantity Using the conditional probability $p(s|m)$ is the probability that Eve obtains the same classical bit s from her measurement as Alice originally prepared. This is called the *collision probability* $P_c(m)$ and it is computed as squared conditional probability $p(s|m)$ for all possible bits s, i.e.

$$P_c\big(m\big) = \sum_s p\big(s|m\big)^2 \tag{6.2}$$

Further, the collision probability can be computed over all possible measurement outcomes m of Eve giving the *expected collision probability* $\langle P_c \rangle$ which is described as

$$\big\langle P_c \big\rangle = \sum_m p\big(m\big) P_c\big(m\big) \tag{6.3}$$

The average collision probability is a central quantity when discussing the security of a protocol. It can be computed by Alice and Bob without any knowledge of Eve's actual measurement results necessary and it is needed to estimate Eve's information about the secret key. Further, the collision probability is used to define security thresholds on the acceptable error rate as described in the following sections.

To quantify Eve's amount of information on Alice's bit an estimator of the uncertainty of a probability distribution is required. This is a function quantifying the

difficulty to predict the outcome of a random event based on a probability distribution given some a-priori knowledge. In the following two such estimators are used: the *Shannon entropy* H [134] and the *Renyi entropy* R [121]. Shannon entropy and Renyi entropy are both bounded between 0, i.e. when there is no uncertainty at all, and n for a classical bit string of length n.

The Shannon entropy is the most commonly used estimator of uncertainty and is defined as

$$H\big(X\big) = -\sum_{x} p\big(x\big) \log p\big(x\big) \tag{6.4}$$

for some random variable X with values $x_1 \dots x_n$. It can also be conditioned on a random variable such that we get for a specific outcome m

$$H\big(S|M=m\big) = -\sum_{s} p\big(s|m\big) \log p\big(s|m\big) \tag{6.5}$$

with S describing all possible bits and M all possible measurement results. This is averaged over all probabilities of Eve's results m as

$$H\big(S|M\big) = \sum_{m} p\big(m\big) H\big(S|M=m\big) \tag{6.6}$$

The Shannon entropy H is an estimator of the uncertainty of a probability distribution and thus the variation of the Shannon entropy can be interpreted as the *information gain* I. For the a-priori probability distribution X and the a-posteriori distribution Y the information gain is $I = H(X) - H(Y)$. This can be used to describe the amount of information Eve obtains on Alice's key based on her measurement results, here called *mutual information* I_{AE}. In this case we have the Shannon entropy of a classical bit conditioned on Eve's measurement outcome $H(S|M)$. Eve has no a-priori information about the secret key since Alice chooses her bit string at random and thus $H(S) = 1$. Therefore, the amount of information gained by Eve for one specific value m is $I_{AE}^{m} = 1 - H(S|M=m)$. This is averaged over all possible outcomes m to obtain

$$I_{AE} = 1 - \sum_{m} p\big(m\big) H\big(S|M=m\big) = 1 - H\big(S|M\big) \tag{6.7}$$

which will be used constantly in the following sections.

The Renyi entropy is actually defined as a generalization of the Shannon entropy, i.e.

$$H_{\alpha}\big(X\big) = \frac{1}{1-\alpha} \log\Big(\sum_{x} p\big(x\big)^{\alpha}\Big) \tag{6.8}$$

for $\alpha \geq 0$ and $\alpha \neq 1$. With α approaching 1 H_α converges to the Shannon entropy such that we can say $H_1 = H$ [121]. Throughout the thesis we reduce ourselves to the second-order Renyi entropy $R = H_2$, which is conveniently defined using the collision probability, i.e.

$$R\big(X\big) = -\log \sum_x p\big(x\big)^2 = -\log P_c\big(X\big) \tag{6.9}$$

Accordingly to the Shannon entropy the Renyi entropy is conditioned for a specific measurement result m as

$$R\big(S|M=m\big) = -\log P_c\big(m\big) = -\log \sum_s p\big(s|m\big)^2. \tag{6.10}$$

with again S describing all possible bits and M all possible measurement results. To obtain the Renyi entropy $R(S|M)$ for all of Eve's results m $R(S|M=m)$ is averaged over the respective probabilities of Eve's measurement results, i.e.

$$R\big(S|M\big) = \sum_m p\big(m\big) R\big(S|M=m\big) \tag{6.11}$$

Besides Eve's information on the secret key we are interested in the amount of error Eve introduces into a protocol since this amount can be recognized by the legitimate communication parties Alice and Bob. The probability of an error is simply defined as the occurrence of an incorrect result, i.e. a result Bob would not expect from his measurement according to the additional information he has about Alice's measurement. To express that we make use of the conditional probability $p(m|s)$ which is the probability that Bob obtains the incorrect result m although Alice prepared the bit s. This directly gives the error probability P_e as

$$P_e\big(m\big) = \sum_s p\big(m|s\big) \tag{6.12}$$

for some specific message m. Accordingly to the collision probability the *expected error probability* $\big\langle P_e \big\rangle$ is defined for all possible messages as

$$\big\langle P_e \big\rangle = \sum_m p\big(m\big) P_e\big(m|s\big) \tag{6.13}$$

Another important question is how much key material has to be discarded to minimize Eve's knowledge about the key. This amount is called the *discarded fraction* τ and is computed using the expected collision probability

$$\tau = 1 + \log \big\langle P_c \big\rangle^{\frac{1}{n}} \tag{6.14}$$

Following from this equation a bit string of length n has to be reduced by $n\tau$ bits during privacy amplification to leave Eve with at most 1 Shannon bit of information on the whole secret key no matter its length [96].

6.2 Attacks on QKD Protocols

In the following we want to discuss some basic attack strategies on ideal and realistic sources. All these strategies are *individual attacks*, which means that the eavesdropper, Eve, interacts with each signal coming from Alice separately. An extension to the individual attacks are the *collective attacks*, where Eve prepares an ancilla state for each signal coming from Alice and lets it interact with the signal [52]. The benefit for Eve is that she can store the ancilla at her laboratory until she has more information about how to measure it. It has been proven that the same security bound defined for QKD protocols also holds if collective attacks are applied [18, 17].

The most general version of attacks are *coherent attacks* where Eve is allowed to perform any quantum operation on the signal in transit and use any possible ancilla state. In particular, Eve is able to collect ancilla states from all qubits sent by Alice and perform operations on a subset or all of these ancilla states. Hence, such attacks are very complex to analyze. Nevertheless, bounds for information-theoretical security against coherent attacks have been found which are equal to the bounds for collective attacks [126].

In the analysis below we want to focus mainly on individual attack strategies since we discuss collective attacks on multiple qubits in detail in the next chapter.

6.2.1 Attacks on Ideal Sources

Naive Intercept-Resend Attack

The most intuitive kind of an individual attack is the *intercept and resend* (I&R) attack [81]. The main intention for Eve is to get hold of each photon coming from Alice and measuring it in some predefined basis. According to her result Eve prepares a new photon and forwards it to the legitimate receiver, Bob. Looking at the application of the naive I&R attack on the BB84 protocol, Alice's qubit will either be in the Z- or the X-basis, explicitly one of the four states $|0\rangle$, $|1\rangle$, $|x+\rangle$ or $|x-\rangle$. As already described in section 5.2.1 if Alice sends a 0 she will either encode it into

$|0\rangle$ or $|x+\rangle$ with equal probability. Similarly, if she sends a 1 she encodes it either into $|1\rangle$ or $|-\rangle$. Eve, unaware of Alice's choice, will chose randomly between the Z- and the X-basis. Thus, she will obtain a correct result in case Alice sent $|0\rangle$ and Eve measured in the Z-basis or Alice sent $|x+\rangle$ and Eve measured in the X-basis, respectively. Any other combination will result in a completely random measurement outcome. This leads to the decision tree in figure 6.1. For now, we will also

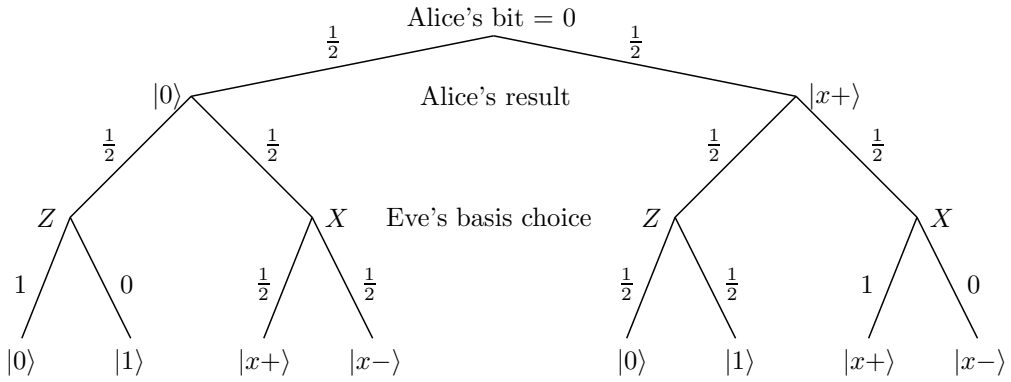

Figure 6.1: *(Naive I&R attack)* Decision tree for the naive intercept/resend attack strategy.

assume that Eve does not listen to any public communication between Alice and Bob. Therefore, she will not know in which case her measurement was wrong. As pointed out above, the best way to express the situation when Eve made a correct measurement is the conditional probability $p(m|s)$. The four possible results are then

$$\begin{aligned} p\big(m = |0\rangle|s = 0\big) = p\big(m = |x+\rangle|s = 0\big) &= \left(\frac{1}{2}\right)^3 + \left(\frac{1}{2}\right)^2 \cdot 1 = \frac{3}{8} \\ p\big(m = |1\rangle|s = 0\big) = p\big(m = |x-\rangle|s = 0\big) &= \left(\frac{1}{2}\right)^3 + \left(\frac{1}{2}\right)^2 \cdot 0 = \frac{1}{8} \end{aligned} \tag{6.15}$$

and equally for $p(m|s = 1)$. From these probabilities we can directly compute the error rate introduced by Eve's intervention. Whenever Eve choses the correct basis she does not introduce any error. Thus, we are only interested in the probabilities $p(m = |1\rangle|s = 0)$, $p(m = |x-\rangle|s = 0)$, $p(m = |0\rangle|s = 1)$ and $p(m = |x+\rangle|s = 1)$ which are all 1/8. Since $p(m) = 1/2$ for all m we obtain

$$\langle P_e \rangle = \frac{1}{2}\left(4 \cdot \frac{1}{8}\right) = \frac{1}{4} \tag{6.16}$$

For the conditional probabilities $p(s|m)$ the sum $\sum_s p(m|s) = 1/2$ and thus we get $p(s|m) = 2p(m|s)$. Looking at the collision probability we get for this naive version of the I&R attack

$$P_c\big(m = |0\rangle\big) = \left(\frac{3}{4}\right)^2 + \left(\frac{1}{4}\right)^2 = \frac{5}{8} \tag{6.17}$$

and similar values for $m = |1\rangle$, $m = |x+\rangle$ and $m = |x-\rangle$. Therefore, the average collision probability computes to

$$\big\langle P_c\big\rangle = \sum_m \frac{1}{4} P_c\big(m\big) = 4\left(\frac{1}{4}\right)\left[\left(\frac{1}{4}\right)^2 + \left(\frac{3}{4}\right)^2\right] = \frac{5}{8} \tag{6.18}$$

From the collision probability the discarded fraction can be computed which is for the naive I&R attack $\tau \simeq 0.322$. Thus, only one-third of the key has to be discarded to guarantee that Eve has less than one bit of information on the whole key.

Looking at the Renyi entropy for $m = |0\rangle$ we get

$$R\big(S|M = |0\rangle\big) = -\log P_c\big(m = |0\rangle\big) = -\log\frac{5}{8} = 3 - \log 5 \tag{6.19}$$

Since the Renyi entropy for $m = |1\rangle$, $m = |x+\rangle$ and $m = |x-\rangle$ is the same and all four results are equally probable the average Renyi entropy is

$$R\big(S|M\big) = \sum_m \frac{1}{4} R\big(S|M = m\big) = 4\left(\frac{1}{4}\right)\big(3 - \log 5\big) = 3 - \log 5 \tag{6.20}$$

For the conditional Shannon entropy $H(S|M = |0\rangle)$ we get

$$H\big(S|M = |0\rangle\big) = -\frac{3}{4}\log\frac{3}{4} - \frac{1}{4}\log\frac{1}{4} = 0.811 \tag{6.21}$$

which is equal to the other entropies $H(S|M = |1\rangle)$, $H(S|M = |x+\rangle)$, $H(S|M = |x-\rangle)$, such that

$$\begin{aligned} H\big(S|M\big) &= \sum_m \left(\frac{1}{4}\right) H\big(S|M = m\big) \\ &= 4\left(\frac{1}{4}\right)\left(-\frac{3}{4}\log\frac{3}{4} - \frac{1}{4}\log\frac{1}{4}\right) = 0.811 \end{aligned} \tag{6.22}$$

The total information Eve will have in the end about each bit is $I_{AE} = 1 - H\big(S|M\big) \simeq 0.2$, which is rather poor for Eve. Therefore, Eve will use another strategy, which gives her more information. One possibility is to use another measurement basis, e.g the *Breidbart basis* [9] and to listen to the communication between Alice and Bob. In particular, listening to the communication between Alice and Bob gives Eve more information on the raw key bits as in the naive approach, as we explain in the following paragraphs.

Full Intercept-Resend Attack

In the most successful version of the I&R attack Eve measures in the Z- and X-basis and also takes Alice's and Bob's decisions into account. In this attack Eve randomly chooses again between the Z- and the X-basis to measure the signals coming from Alice. She forwards the results she obtains to Bob and listens to the public communication between Alice and Bob during the sifting phase. If Alice sends a 0 encoded as $|0\rangle$ Eve will either measure it in the Z- or X-basis. As we have already seen above, if Eve uses the Z-basis she will obtain $|0\rangle$ with certainty and introduce no error. Otherwise, she will obtain $|x+\rangle$ or $|x-\rangle$ with equal probability (cf. figure 6.2).

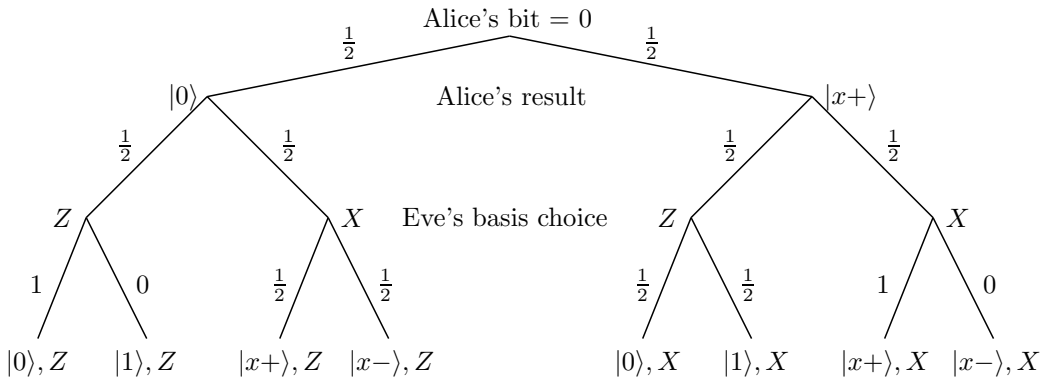

Figure 6.2: *(Full I&R attack)* Decision tree for the full I&R attack strategy.

Comparing the decision tree with the one from the naive I&R attack in figure 6.1 above we immediately see that Eve can eliminate two events for $s = 0$, i.e. if she measured $|1\rangle$ and Alice used the Z-basis and $|x-\rangle$ and Alice used the X-basis. These two events occur with probability $p = 0$ which increases Eve's information. In detail, the probabilities $p(m|s)$ are

$$\begin{aligned}
p\Big(m = \big(|0\rangle, Z\big)|s = 0\Big) &= \left(\frac{1}{2}\right)^2 \cdot 1 = \frac{1}{4} = p\Big(m = \big(|x+\rangle, X\big)|s = 0\Big) \\
p\Big(m = \big(|1\rangle, Z\big)|s = 0\Big) &= \left(\frac{1}{2}\right)^2 \cdot 0 = 0 = p\Big(m = \big(|x-\rangle, X\big)|s = 0\Big) \\
p\Big(m = \big(|x+\rangle, Z\big)|s = 0\Big) &= \left(\frac{1}{2}\right)^3 = \frac{1}{8} = p\Big(m = \big(|0\rangle, X\big)|s = 0\Big) \\
p\Big(m = \big(|x-\rangle, Z\big)|s = 0\Big) &= \left(\frac{1}{2}\right)^3 = \frac{1}{8} = p\Big(m = \big(|1\rangle, X\big)|s = 0\Big)
\end{aligned} \tag{6.23}$$

and we get similar values for $s = 1$. The expected error probability $\langle P_e \rangle$ computes conformal to the naive intercept-resend attack above such that we obtain again $\langle P_e \rangle = 1/4$. For the sum $\sum_s p(m|s)$ we obtain 1/4, such that $p(s|m) = 4p(m|s)$. This results in the collision probabilities 1 if Eve chooses the correct basis for her measurement and 1/2 if she chooses a basis different from Alice's preparation. Thus, the average collision probability is

$$\langle P_c \rangle = \frac{1}{4} + 4\frac{1}{16} + \frac{1}{4} = \frac{3}{4} \tag{6.24}$$

Calculating the discarded fraction τ we get $\tau \simeq 0.585$ which is equal to the discarded fraction when using the Breidbart basis [9].

For the Renyi entropy we obtain $R(S|M = m) = -\log 1 = 0$ whenever Eve's choice of the basis is correct and $R(S|M = m) = -\log 0.5 = 1$ otherwise. The average Renyi entropy is then

$$R\big(S|M\big) = \frac{1}{2}\big(0 + 1\big) = \frac{1}{2} \tag{6.25}$$

For the Shannon entropy we also get either 0, if Eve guessed the same basis as Alice and 1/2 otherwise. This results in a Shannon entropy of

$$H\big(S|M\big) = 4\frac{1}{8} = \frac{1}{2} \tag{6.26}$$

Accordingly, Eve's information gain from the full I&R attack is $I_{AE} = 1 - H(S|M) = 1/2$ per bit of the sifted key. This strategy gives more information to Eve than the naive approach (cf. eq. (6.22)) or the I&R attack in the Breidbart basis [9].

Intercept-Resend on the BBM Protocol

The intercept-resend attack is not only applicable on prepare and measure protocols but also on protocols using entangled states. In section 5.2.2 above we described the BBM-version of the BB84 protocol [11]. In this version a source emitting entangled pairs of qubits is used instead of a single photon source. One advantage of this scheme is that the secret key is generated at both parties using perfect randomness whereas in the BB84 protocol Alice more or less prepares the secret and sends it to Bob. Nevertheless, an eavesdropper Eve located between Alice and Bob can intercept the qubits coming from the entangled source. Following the considerations from above we want to examine how much information an eavesdropper can get when applying a full intercept-resend attack on the BBM protocol. In general, it is

not stated explicitly where the entangled source is located. Hence, it could be either in the middle of the two parties (in the laboratory of some trusted third party) or at the laboratory of one of the parties. According to these scenarios Eve has two possibilities to intervene: in the first scenario she measures both qubits before either Alice or Bob receives them. In the second scenario where we assume that Alice is in possession of the source Eve can only intercept Bob's qubit.

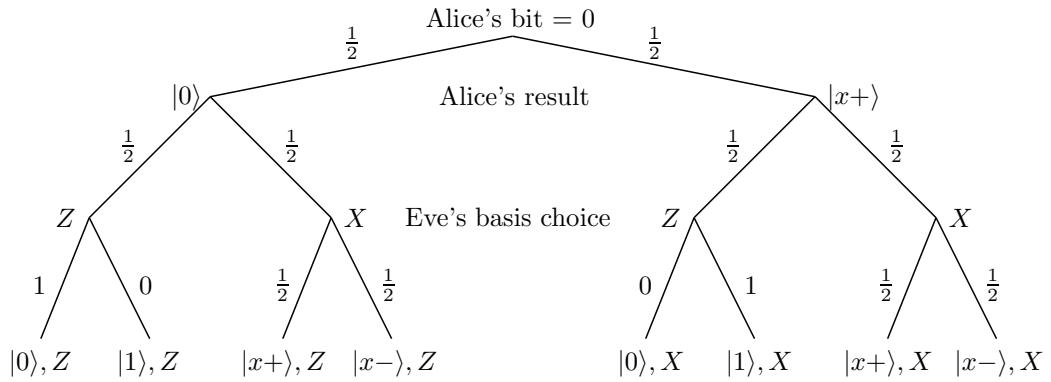

Figure 6.3: *(I&R attack on BBM)* Decision tree for the full I&R attack strategy on the BBM protocol [11].

Eve's strategy in the first scenario is to intercept both qubits while they are flying from the source to Alice and Bob. This case is somehow extraordinary because it can be understood as Eve generating the secret due to her measurement since Eve destroys the entanglement and forwards single qubits in a defined state to Alice and Bob. Nevertheless, Alice's and Bob's measurement introduces enough randomness to obtain a secure key because they choose their measurement bases at random. Eve's measurement basis coincides only for a fraction of all signals such that Eve introduces an expected error probability of 1/4 as in the QKD protocols discussed in the previous section.

In the second scenario where the source is located at Alice's lab the only strategy for Eve is to intercept Bob's qubit and measure it. This happens usually after Alice performed her measurement and thus the strategy is very similar to the full intercept-resend attack presented above in connection with prepare and measure protocols. Either Eve chooses the same basis as Alice and is able to measure the qubit perfectly or she chooses the wrong basis and destroys the information. Therefore, we get the

probabilities

$$\begin{aligned}
p\Big(m = \big(|0\rangle, Z\big)|s=0\Big) &= p\Big(m = \big(|x+\rangle, X\big)|s=0\Big) = \left(\frac{1}{2}\right)^2 \cdot 1 = \frac{1}{4} \\
p\Big(m = \big(|1\rangle, Z\big)|s=0\Big) &= p\Big(m = \big(|x-\rangle, X\big)|s=0\Big) = \left(\frac{1}{2}\right)^2 \cdot 0 = 0 \\
p\Big(m = \big(|x+\rangle, Z\big)|s=0\Big) &= p\Big(m = \big(|0\rangle, X\big)|s=0\Big) = \left(\frac{1}{2}\right)^3 = \frac{1}{8} \\
p\Big(m = \big(|x-\rangle, Z\big)|s=0\Big) &= p\Big(m = \big(|1\rangle, X\big)|s=0\Big) = \left(\frac{1}{2}\right)^3 = \frac{1}{8}
\end{aligned} \tag{6.27}$$

describing Eve's measurement results (of course, similar probabilities occur for $s = 1$). Regarding her average collision probability we get

$$\big\langle P_c \big\rangle = \frac{1}{4} + 4\frac{1}{16} + \frac{1}{4} = \frac{3}{4} \tag{6.28}$$

When looking at the probability that Bob obtains an incorrect result although both Alice and Bob measured in the same basis we get

$$\begin{aligned}
p\Big(m = \big(|1\rangle, Z\big)|s=0\Big) = \;& p\Big(m = \big(|x-\rangle, X\big)|s=0\Big) = \\
p\Big(m = \big(|0\rangle, Z\big)|s=1\Big) = \;& p\Big(m = \big(|x+\rangle, X\big)|s=1\Big) = \frac{1}{8}
\end{aligned} \tag{6.29}$$

which results in the expected error probability

$$\big\langle P_e \big\rangle = \frac{1}{2}\left(\frac{1}{4} + \frac{1}{4}\right) = \frac{1}{4}. \tag{6.30}$$

Thus, we see that the average error probability as well as the average collision probability in both scenarios is the same as for prepare and measure QKD protocols which indicates that the security is the same for single photons and entangled sources. Regarding Eve's information gain I_{AE} we compute the Shannon entropy similar to the full I&R attack above and get $H(S|M) = 1/2$ such that

$$I_{AE} = 1 - H\big(S|M\big) = \frac{1}{2}. \tag{6.31}$$

Hence, Eve has the same information on the raw key bits regardless whether she attacks the BB84 or the BBM protocol using the full intercept-resend attack.

Collective Attack

As already pointed out shortly, in a collective attack Eve uses ancilla states and entanglement to obtain information of the qubits sent by Alice. In this case Eve

prepares an ancilla state for each qubit coming from Alice, entangles the ancilla with it and then passes only the original qubit on to Bob. Later on, Eve is able to perform a measurement or any other quantum operation on the ancilla in her possession to gain information about the original signal. As pointed out in the beginning the analysis in this chapter is restricted to individual attacks only. Thus, we will just look at scenarios where Eve performs her operation on one single ancilla. An operation on a subset or even all of the ancilla states is used in coherent attacks but will not be discussed here.

Taking the BB84 protocol [8] which we also referred to in section 6.2.1 above, a rather simple strategy for Eve is to use an entangled pair, i.e. one of the Bell states from eq. (2.4), and to perform a measurement in the Bell basis on the photon coming from Alice together with one of the entangled photons. This is equal to a quantum teleportation scheme (cf. section 2.5.2 for further details) where the unknown signal state is teleported onto Eve's ancilla state.

$$\begin{aligned}\big(\alpha|0\rangle+\beta|1\rangle\big)\frac{1}{\sqrt{2}}\Big(|00\rangle+|11\rangle\Big) = \\ \frac{1}{2}\Big(|\Phi^+\rangle\Big(\alpha|0\rangle+\beta|1\rangle\Big)+|\Phi^-\rangle\Big(\alpha|0\rangle-\beta|1\rangle\Big) \\ +|\Psi^+\rangle\Big(\alpha|1\rangle+\beta|0\rangle\Big)+|\Psi^-\rangle\Big(\alpha|1\rangle-\beta|0\rangle\Big)\Big).\end{aligned} \tag{6.32}$$

Eve is able to keep her ancilla until Alice reveals her basis choice and to measure it in the correct basis to obtain full information. If we look at the average collision probability and Eve's Shannon information about Alice's bit we see that

$$\big\langle P_c\big\rangle = 1 \qquad \text{and} \qquad I_{AE} = 1 - H\big(S|M\big) = 1. \tag{6.33}$$

Hence, Eve has full information about the bit Alice sent. Nevertheless, the signal, which Eve has forwarded to Bob is now in a Bell state, i.e. it has lost every information about Alice's basis choice and is in a completely mixed state. Bob will obtain a random result upon a measurement in the Z as well as in the X-basis as it is given by Bob's average collision probability $\langle P_c\rangle = \frac{1}{2}$. Thus, Alice and Bob will detect too many errors during their sifting phase (around 50%) and therefore will abort the protocol. As we see, regarding the BB84 protocol, Eve gains full information about Alice's bit using this attack strategy but the average collision probability is the same compared to the full I&R strategy (cf. eq. (6.24)). Thus, she can gain no additional information from this strategy.

Looking at the Ekert protocol [51] a strategy for Eve in this case is to prepare her ancilla in the state $|0\rangle$ and perform a CNOT operation (cf. eq. (4.36) in section 4.2.3) on the signal and her ancilla state. The CNOT operation applied on the signal coming from Alice and Eve's ancilla will alter the state into

$$\mathrm{CNOT}_{23}|\Phi^+\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}\Big(|000\rangle + |111\rangle\Big) \tag{6.34}$$

The resulting state is a GHZ state [60] which has the special property that if one of

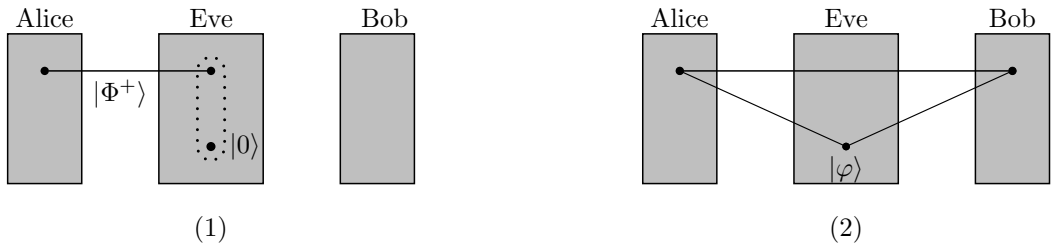

Figure 6.4: *(Collective Attack)* Illustration of a collective attack on the Ekert protocol [51]. The dotted line indicates the application of the CNOT operation.

the photons is measured the other two photons immediately collapse into a certain state depending on the measurement result (cf. section 2.2). In case of eq. (6.34) if Alice measures in the Z basis Bob and Eve will obtain the same result as Alice if they also perform their measurement in the Z basis. In case Alice uses the X-basis Bob's measurement result in the same basis will not correlate to Alice's result in 50% of the times. For the collision probability and Shannon information this means

$$\big\langle P_c \big\rangle = 1 \qquad \text{and} \qquad I_{AE} = 1 - H\big(S|M\big) = 1 \tag{6.35}$$

if Alice and Bob measure in the Z basis. For a measurement in the X-basis Bob obtains the same result as Alice with probability $\langle P_c \rangle = \frac{1}{2}$. Therefore, the overall information Eve obtains on each secret bit is $1 - H(S|M) = 0.75$, which is significantly more compared to the I&R strategies discussed in section 6.2.1 above. Nevertheless, an error is detected with probability 0.5 every time Alice and Bob use the X-basis. This unbalanced occurrence of errors makes it easier for Alice and Bob to identify the presence of Eve.

6.2.2 Attacks on Realistic Sources

We want to stress again that we were dealing in the previous section with ideal setups, which means perfect sources and channels. In a physical implementation of QKD protocols the signals going from Alice to Bob are tempered by natural noise and imperfect devices (inefficient detectors, multi-photon sources, etc.). There are various systems trying to overcome some of these errors coming from the physical limitations as we already described in section 5.2.4 above. To focus in detail on the impacts of such problems onto the security of these protocols would go beyond the scope of this thesis but we want to refer to these articles [57, 126, 118] (and the references therein) which give a great overview on this complex topic. In the following paragraphs we just want to give an idea which attack strategies are possible in an real-world environment.

Photon Number Splitting Attack

The *photon number splitting attack* (PNS) was first introduced by Huttner et al. [82] and later discussed by Brassard et al. [23] as well as Lütkenhaus [97] and is a very powerful attack strategy. It is applied on realistic photon sources emitting weak coherent pulses which generate single photons only with a certain probability. With a small probability multi-photon pulses are emitted containing 2 or more photons having the same polarization. The strategy for Eve is to intercept these pulses coming from Alice, take one photon of the multi-photon pulse and send the remaining photon(s) along to Bob. Eve waits until Alice and Bob publicly compare their measurement bases and then measures the intercepted photon in the correct basis.

In detail, according to eq. (5.13), the probability that Alice's source emits a vacuum pulse (containing zero photons) is very high and the probability of a single photon pulse is around 10%. Hence, the probability of a multi-photon pulse is very low (around 5% [57]). Because of this Eve can not split a photon off each pulse but she has to check for the multi-photon pulses. Therefore, she performs a non-demolition measurement to collapse the pulse into a state containing a fixed number of photons. This is accomplished by a projection onto Fock spaces. If Eve intercepted a multi-photon pulse, she applies an operator A_N, which destructs one

photon of the pulse and creates an appropriate auxiliary state, i.e.

$$\begin{aligned} A_N|N,0\rangle_+|\alpha\rangle &= |N-1,0\rangle_+|\varphi_1\rangle \\ A_N|0,N\rangle_+|\alpha\rangle &= |0,N-1\rangle_+|\varphi_2\rangle \\ A_N|N,0\rangle_\times|\alpha\rangle &= |N-1,0\rangle_\times|\psi_1\rangle \\ A_N|0,N\rangle_\times|\alpha\rangle &= |0,N-1\rangle_\times|\psi_2\rangle \end{aligned} \tag{6.36}$$

From her measurement on the auxiliary system together with the information about Alice's basis choice Eve is able to determine the correct value of the secret bit. Therefore, $\langle\varphi_1|\varphi_2\rangle$ and $\langle\psi_1|\psi_2\rangle$ have to be zero such that they can be distinguished by Eve. As pointed out in [23] such an operator can be described by the Jaynes-Cummings model.

Using the operator A_N Eve is able to obtain full information from multi-photon signals generated by Alice's source. But, as we already pointed out, the probability that a multi-photon signal is emitted is rather small. Only if the probability that Bob detects a signal is smaller than the probability of a multi-photon signal the attack becomes a severe problem. In this case Eve suppresses all dark counts in Bob's module and the efficiency of his detectors is increased to 100%. Further, Eve replaces the quantum channel with a perfect channel such that there are no losses due to the channel any more. It is a rather paranoid assumption to give Eve the power to do all these things, since they affect Bob's hardware directly. But, to be secure, all possible scenarios have to be considered. For each signal coming from Alice Eve acts in the following way: all signals with zero photons are ignored, since dark counts have been suppressed. All multi-photon signals are attacked using the PNS strategy. This gives Eve full information about the corresponding bit of the secret key. A fraction of the single-photon signals is suppressed and the other single-photon signals are attacked using the I&R strategy (cf. section 6.2.1 above). Eve chooses the amount of discarded signals such that they are consistent with Bob's total detection probability. With a perfect quantum channel and perfect detectors all errors in this scenario are introduced by Eve's I&R attack (the PNS attack introduces no error). Bob is not able to distinguish these errors from the ones he expects due to dark counts and the lossy channel. In this case the whole communication becomes insecure.

In [98] it has been shown that also the Poisson photon number distribution can be preserved using the PNS attack, which makes it undetectable as long as a publicly

known signal intensity is used. Therefore, the decoy states method [83, 93, 159] uses different intensities to detect the PNS attack. Another way to secure BB84-like protocols against the PNS attack was presented in [125]. Scarani et al. suggested an alternative sifting procedure such that Alice does not give away her measurement basis. Instead, she announces one of four pairs of non-orthogonal states. This leaves Bob with an inconclusive or ambiguous result and he will have to discard his result for 75% of all signals. Although the efficiency of this protocol is much lower than for standard BB84 protocols (where about 50% of the signals are discarded) it gives not enough information to an eavesdropper and the PNS attack can not be applied successfully.

Trojan Horse Attack

Another attack strategy on realistic setups of QKD systems is the *Trojan Horse attack* or *light injection attack*. It has been introduced first in [122, 16] and was discussed in more detail in [151] later on. The main idea of this attack strategy is not to interact with the photons in transit between Alice and Bob but to probe the devices in Alice's and Bob's laboratory by sending some light into them and collecting the reflected signal. In this way Eve is able to obtain information about the detectors and further on which classical bit Bob measured. In detail, Eve is in possession of a laser and a detection scheme. She sends out light pulses towards Alice's or Bob's setup, which are reflected and enter the detection scheme when returning to Eve. In [151] it is assumed that Eve uses homodyne detection for the reflected pulse and thus needs a reference pulse. This reference pulse is delayed in an arm of the optical fiber and enters the detection system together with the reflected pulse.

Eve can use the information of the reflected signal to detect which basis Alice's used for the preparation of the photon. The detection of the correct basis is based on a phase modulation occurring due to the different ways the reflected and reference beam go through [151]. If Eve is able to do this before Alice's photon reaches Bob she can perform a simple I&R attack (cf. section 6.2.1 above), i.e. intercept the photon in transit, measure it in the correct basis and send it on to Bob. This will give her full information on the secret bit string.

A counter-measure against this kind of attack strategy is implemented in the plug & play systems where the intensity of incoming light is monitored [122, 16].

The idea is that Bob sends a rather intense beam of light to Alice which is used for synchronization with a special timing detector at Alice's setup. This detector notifies the legitimate communication parties when the power of an incoming signal extends some predefined level. For protocols where light just goes one way (e.g. out of Alice's lab into Bob's lab) a strategy for preventing the attack is to add components in Alice's and Bob's laboratory to block Eve's injected pulse. This means, for example, that the laser pulses have to pass through an optical isolator and a band-pass filter [151] when leaving Alice's setup. The isolator reduces the signals coming into Alice's laboratory to make a light injection attack impossible.

Faked States Attack

The *faked states* attack is a kind of I&R attack strategy but Eve does not try to recreate the intercepted state. Instead, Eve manages to send a signal to Bob which he can only detect in a way totally controlled by Eve. This attack was first introduced in [101] and later extended in [100, 102]. In detail, Eve intercepts the signals coming from Alice using an apparatus similar to Bob's. Further, she forwards a state to Bob which can only be detected by him if he chooses the same basis as Eve. She can achieve this by exploiting the *full detector efficiency mismatch* [100]. This is a phenomenon where the signal coming into the detector has a time-shift such that it is outside the detector's sensitivity curve. Therefore, only one detector can fire and the other one is blinded out. In this way Eve can control the bit value Bob will obtain from his measurement. The second goal of the faked states attack is to eliminate the case where Bob performs a measurement in a basis incompatible to Eve's basis, thus detecting an error. Eve can achieve that by adding a relative phase to the signal such that the whole signal is deflected to the blinded detector and is lost.

For the BB84 protocol [8] the faked states attack works as follows: Eve performs an I&R attack and obtains some result from her measurement. Then she sends a signal pulse to Bob which has the opposite bit value in the opposite basis compared to what she has detected. Eve also sets the time shift of the signal such that the detector for the opposite bit value compared to what she has detected is blinded out. Thus, if Bob tries to detect the signal in a different basis than Eve he won't detect anything. Otherwise, if Bob chooses the same basis as Eve, he will either detect the same bit as Eve or nothing at all. Therefore, every time Eve measured

Alice's state in the wrong basis, also Bob will measure it in the wrong basis and the results will be discarded. If Eve has chosen the right basis, also Bob measured in the right basis and Eve has full information about this bit of the secret key.

As it is explained in [100, 102] it has to be stressed that Bob's detection efficiency is reduced by the faked states attack since all signals where Bob measured in a different basis compared to Eve and half of the signals where Bob measured in the same basis are suppressed. Eve can overcome this rather easily using faked states with a proportionally increased brightness. If Eve is not able to blind one detector completely, she can only obtain partial information about the key but, nevertheless, stays undetected [119].

Possible counter measures to prevent the attack are, for example, to actively monitor the timing of incoming pulses at Bob's side [100]. This can be achieved through a random shifting of Bob's time window or with additional detectors. Alternatively, Bob can test the characteristics of his detectors over a variety of input signals to especially check all features of the sensitivity curve. Another counter measure for Bob is to introduce random jitter into the detector synchronization to smear the curves and lower the mismatch.

Time Shift Attack

An alternative version of the faked states attack is the *time-shift attack strategy* [119]. The time-shift attack also exploits the detector efficiency mismatch, but, in contrary to the faked states attack, it is feasible with today's technology, as it has been shown in [171]. Similar to the faked states attack Eve randomly shifts the time of Alice's signal such that it arrives outside of Bob's detector's sensitivity curve. Due to her choice of the time delay Eve is able to infer the exact result of Bob's measurement. As pointed out in the previous section describing the faked state attack, if Eve is able to completely blind a detector by her time shift, she is able to obtain full information about Bob's measurement result. Otherwise, Eve will obtain only partial information about the secret key. In both cases, Eve never introduces any error, since she does not measure or otherwise interact with Alice's state in transit.

One difference to the faked states attack is that Eve has to deal with the increased loss at Bob's side in another way. Regarding the faked states attack Eve uses a brighter lases pulse to overcome the losses, as described above. With respect to the

time-shift attack Eve has to replace the quantum channel by a low-loss version to compensate Bob's additional losses.

The counter measures regarding the faked states attack described in the previous section will also work here to prevent an application of the time-shift attack. Additionally, phase shift settings can be applied to Bob's phase modulator and the detection rate and the channel loss can be checked to secure a protocol against the time-shift attack [119].

6.3 Attacks on QSS Protocols

The security analysis of QSS schemes is a little different to the analysis of QKD protocols. In general, the security of QSS protocols is rather complex to analyze since there are usually more parties involved compared to QKD and almost every protocol makes use of entanglement. Therefore, collective attacks are of much greater interest.

Some of the legal participants of a QSS protocol have to be considered dishonest which gives a second threat besides eavesdroppers from the outside. That's because the aim of QSS is to share a secret such that no single party (or no subset of parties) is able to obtain it by itself. This model of adversaries from the inside is in fact much stronger because such an adversary in general has more advantages than an eavesdropper from the outside. For example, a dishonest party is able to send authenticated classical messages to the other parties whereas an eavesdropper from the outside is not. Thus, we will especially focus on dishonest parties in the following sections. For the sake of completeness we give a short overview on strategies for an eavesdropper in the next section.

As already pointed out in section 5.3.1 above the number of dishonest parties is also important. How many dishonest parties can be handled in a QSS scheme is given by the threshold of the scheme. We pointed out that a (k, n) threshold scheme is able to deal with $k-1$ dishonest parties since $k-1$ or less shares brought together do not reveal any information about the secret. In the following we discuss (n, n) threshold schemes which means all the shares have to be combined to reconstruct the secret. With other words all but one of the receiving parties can be dishonest without compromising the security of the protocol.

6.3.1 Intercept-Resend by an Outside Adversary

An eavesdropper, Eve, is able to interfere with the qubits in transit between Alice and her communication parties Bob and Charlie (let's assume, for now, that only three parties are involved in the protocol). Similar to the intercept-resend attacks on QKD protocols Eve's aim is to measure the intercepted qubit according to some basis and generate a new qubit based on her result. Unlike in most of the QKD protocols, the qubits in a QSS protocol are usually part of an entangled state which means that an individual qubit is in a completely mixed state. Therefore, the major problem for Eve is, as we have already seen in section 6.2.1 above, that she only obtains information about the secret if her measurement basis corresponds to the bases Alice, Bob and Charlie are going to use for their respective measurements. Hence, she introduces a certain error into the protocol, which can be detected by Alice, Bob and Charlie.

Looking at the HBB scheme [68] Eve's strategy is to intercept the qubits flying to Bob and Charlie and to measure them individually either in the X- or Y-basis. Since Eve has no information about which bases Bob and Charlie are going to use she chooses her measurement basis at random. Therefore, Eve sometimes performs measurements which are compatible to the protocol, e.g. Eve uses XX or YY when Alice obtained $|x+\rangle$ from her measurement, as well as measurements which will destroy some of the information. The possible outcomes for Eve are then

$$\begin{aligned} &p\big(m = (|x+x+\rangle, X)|s=0\big) = p\big(m = (|x-x-\rangle, X)|s=0\big) = \\ &p\big(m = (|y+y-\rangle, X)|s=0\big) = p\big(m = (|y-y+\rangle, X)|s=0\big) = \frac{1}{32} \end{aligned} \tag{6.37}$$

for the measurements corresponding to the protocol (cf. also table 5.2 in section 5.3.2). The probability for the other outcomes is then

$$p\big(m = |x \pm y\pm\rangle|s=0\big) = p\big(m = |y \pm x\pm\rangle|s=0\big) = \frac{1}{64} \tag{6.38}$$

Following the computation of the collision probability as described in section 6.2.1 above we obtain the conditional probabilities

$$\begin{aligned} &p\big(s=0|m = (|x+x+\rangle, X)\big) = p\big(s=0|m = (|x-x-\rangle, X)\big) = \\ &p\big(s=0|m = (|y+y-\rangle, X)\big) = p\big(s=0|m = (|y-y+\rangle, X)\big) = \\ &p\big(s=0|m = (|x+y+\rangle, Y)\big) = p\big(s=0|m = (|x-y-\rangle, Y)\big) = \\ &p\big(s=0|m = (|y+x-\rangle, Y)\big) = p\big(s=0|m = (|y-x+\rangle, Y)\big) = 1 \end{aligned} \tag{6.39}$$

and 1/2 for the other cases. For $s = 1$ we obtain similar results and therefore the expected collision probability for Eve computes as

$$\langle P_c \rangle = 2 \times \left(8 \times \frac{1}{32} + 8 \times \frac{1}{64} \right) = \frac{3}{4}. \tag{6.40}$$

Additionally to the collision probability we want to know the probability that Eve is detected by the legitimate communication parties. As stated in section 6.2 on QKD protocols above, Alice, Bob and Charlie will detect Eve whenever they detect a wrong result during their test although they measured in the correct bases. In detail, this means we are interested in the probabilities

$$\begin{aligned} p\big(m = (|y + y-\rangle, X) | s = 0\big) = p\big(m = (|y - y+\rangle, X) | s = 0\big) = \\ p\big(m = (|x + x-\rangle, X) | s = 0\big) = p\big(m = (|x - x+\rangle, X) | s = 0\big) = \\ p\big(m = (|y + x+\rangle, Y) | s = 0\big) = p\big(m = (|y - x-\rangle, Y) | s = 0\big) = \\ p\big(m = (|x + y-\rangle, Y) | s = 0\big) = p\big(m = (|x - y+\rangle, Y) | s = 0\big) = \frac{3}{128} \end{aligned} \tag{6.41}$$

and similarly for $s = 1$. Computing the expected error probability $\langle P_e \rangle$ from all the single error probabilities from the equation above we get

$$P_e = 2 \times \left(8 \times \frac{3}{128} \right) = \frac{3}{8}. \tag{6.42}$$

As we can see, this probability is higher than, for example, in the prepare and measure protocols above (cf. section 6.2.1). If a similar strategy is pursued by a dishonest party it is much more effective, as we will show in the following section.

Looking at Eve's information about the secret key we first compute the Shannon entropy. Taking the conditional probabilities from the collision probability we get

$$H\big(S|M\big) = 2 \times \left(8 \times \frac{1}{32} \right) = \frac{1}{2} \tag{6.43}$$

which is the same as for the full intercept-resend attack on the BB84 protocol described in eq. (6.26) above. The overall information Eve obtains about Alice's secret key is then $I_{AE} = 1 - H(S|M) = 1/2$.

6.3.2 Intercept-resend by a dishonest Party

In QSS schemes the presence of one or more dishonest parties has to be considered besides an adversary from the outside. This is due to the fact that the main goal of

a QSS scheme is to distribute a secret key between several parties such that none of the parties is able to individually reconstruct the key. Such a dishonest party, let's assume it is Charlie, tries to gain knowledge about the secret from the messages in transit between Alice and Bob. Hence, in any security analysis of a QSS protocol we also have to evaluate the scenario of one or more dishonest parties. Actually, the threat by an adversary from the inside, i.e. Charlie, is much higher than by an adversary from the outside, i.e. Eve, since Charlie himself has some control over the protocol. We want to point out shortly in this section, how big this advantage is regarding the full intercept-resend attack.

Similar to Eve, Charlie's intention is also to measure the qubits coming from Alice to Bob to obtain some information about them. Therefore, he randomly chooses between a measurement in the X- and Y-basis for the intercepted qubit and forwards the qubit to Bob. Since Charlie does not know Alice's basis choice yet he also measures his qubit in the X- or Y-basis. This gives Charlie a collision probability equal to the one presented in the previous section where Eve attacked the protocol:

$$\langle P_c \rangle = 2 \times \left(8 \times \frac{1}{32} + 8 \times \frac{1}{64} \right) = \frac{3}{4}. \tag{6.44}$$

Charlie's advantage over an attack from the outside is that Alice eliminates some of the measurement results where Bob and Charlie used non-corresponding bases. For example, if Alice's outcome is $|x+\rangle$ and Charlie measured both Bob's and his own qubit in the X-basis the state of Bob's qubit is $|x+\rangle$ afterwards (cf. table 5.2). Although Bob chooses again between the X- and Y-basis only the measurement in the X-basis will count for any further step because a measurement in the Y-basis does not correspond to Alice's result $|x+\rangle$ (cf. table 5.2). Hence, the probabilities for an incorrect result during the test for adversaries are

$$\begin{aligned} &p\big(m = (|x+x-\rangle, X) | s = 0\big) = p\big(m = (|x-x+\rangle, X) | s = 0\big) = \\ &p\big(m = (|y+y+\rangle, X) | s = 0\big) = p\big(m = (|y-y-\rangle, X) | s = 0\big) = \\ &p\big(m = (|x+y-\rangle, X) | s = 0\big) = p\big(m = (|x-y+\rangle, X) | s = 0\big) = \\ &p\big(m = (|y+x+\rangle, X) | s = 0\big) = p\big(m = (|y-x-\rangle, X) | s = 0\big) = \frac{1}{64}. \end{aligned} \tag{6.45}$$

which leads to the expected error probability

$$\langle P_e \rangle = 2 \times \left(8 \times \frac{1}{64} \right) = \frac{1}{4}. \tag{6.46}$$

Hence, we can see that both attack strategies from the outside and from the inside have the same collision probability of 3/4. Nevertheless, an adversary from the outside introduces 50% more error than a dishonest party which makes an attack from the outside much easier to detect by the legitimate parties. This is the main reason why we will not focus on attacks from Eve in the next sections. Moreover, the intercept-resend attack is not the most powerful attack in this scenario. As we will present in the next sections collective attacks give a dishonest party even more advantages.

6.3.3 Attacks on the HBB Protocol

The security of the HBB protocol is mainly based on the fact that a dishonest party is detected during the test procedure of the protocol. As described in section 5.3.2 above, after Alice eliminated the uncorrelated measurements she tells Bob and Charlie to announce some of their measurement results of the remaining qubits. Using table 5.2 Alice is able to compare the results with her own and check if the desired correlation is given. If too many errors occur during this check (assuming we have ideal sources and perfect channels, no errors should occur) Alice has to believe that an adversary is present and restarts the protocol.

The security argument, as it is described in [68] has been proven to be wrong by Karlsson et al. later that year [84]. They commented that the order in which the measurement bases and the results for the test bits are revealed is crucial. They showed that the HBB scheme becomes insecure if the measurement bases are revealed before the results for the test bits. They suggested the same sequence as in their protocol (see below for details): first, Bob and Charlie publicly disclose their measurement results for the test bits and afterwards, in the reversed order, they announce the corresponding measurement bases. The reversed order is important such that none of them can gain too much information from the actions of the previous parties.

In [120] it has also been shown – using a more general approach – that the HBB scheme is insecure. The main idea is that Charlie performs a collective attack, i.e. intercepts the qubit flying to Bob and entangles it with an ancilla qubit. Later on, he uses his qubit together with the ancilla qubit to infer Alice's measurement result without Bob's assistance. Furthermore, Charlie manages to stay undetected during the test phase of the protocol since he knows which result to announce to

maintain the correlation. In detail, Charlie uses an ancilla qubit in the state $|0\rangle_E$ and entangles it with the intercepted qubit B of the GHZ state $|P_{00}^+\rangle$ of eq. (5.15). He achieves that using the Hadamard operation H on qubit B and the CNOT operation on qubits B and E. This brings the initial system $|P_{00}^+\rangle_{ABC} \otimes |0\rangle_E$ into the state

$$|\Psi\rangle = \frac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle - |1111\rangle)_{ABCE} \tag{6.47}$$

Charlie sends qubit B to Bob and waits until Bob announces his measurement basis. Since Charlie did not perform his measurement yet he announces some random basis and waits until Alice also reveals her basis choice. According to the measurement results of Alice and Bob, the qubits C and E in Charlie's possession collapse into some predefined state. In case both Alice and Bob measure in the X-basis Charlie obtains one of the states

$$\begin{aligned}
|\Psi_{x^+x^+}\rangle &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{CE} \\
|\Psi_{x^+x^-}\rangle &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)_{CE} \\
|\Psi_{x^-x^+}\rangle &= \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle)_{CE} \\
|\Psi_{x^-x^-}\rangle &= \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle - |11\rangle)_{CE}
\end{aligned} \tag{6.48}$$

Charlie uses this fact together with the information about Alice's and Bob's measurement basis and to determine the correct value he has to announce to stay undetected. This can easily be done due to the fact that the states $|\Psi_{x\pm x\pm}\rangle$ are completely distinguishable. Charlie just performs a CNOT operation on qubits C and E followed by a Hadamard operation which changes the states $|\Psi_{x\pm x\pm}\rangle$ into the Bell states. Afterwards he measures the qubits and announces 1 if he obtains either $|\Phi^\pm\rangle$ and 0 if he obtains $|\Psi^\pm\rangle$ [120]. Further, Charlie is also able to compute Alice's result for the remaining qubits without any help of Bob performing a similar procedure (application of a single Hadamard operation of qubit C), which makes the whole protocol insecure.

Besides the sequence of the announcement of their measurement bases and results, Alice, Bob and Charlie have a second opportunity to secure the HBB protocol. As presented in [128], if Alice, Bob and Charlie sacrifice some of their measurement results they can test whether they still share a genuine 3-qubit entanglement using a series of inequalities. If these inequalities are maximally violated the three parties can be sure that no eavesdropper or dishonest party entangled an additional system

as described in [120]. Of course, if the qubits are intercepted and measured in transit the 3-qubit entanglement is also destroyed and the inequalities are no longer maximally violated. This strategy to detect the presence of an eavesdropper is very powerful and therefore is discussed in further detail in section 7.3.

6.3.4 Attacks on the KKI Protocol

Regarding the protocol presented by Karlsson et al. [84] the security is also based on the fact that a dishonest party is detected during the error estimation phase of the protocol. The main result of the KKI scheme is that the sequence in which the measurement bases and results are revealed during the error estimation phase is crucial for the security. It is stressed in [84] that the measurement results have to be revealed before the measurement bases and that the party which revealed its results first should be the last to reveal the bases. This explicit order of messages makes it very unlikely for a dishonest party to stay undetected if some qubits are tempered.

Looking at the protocol in detail as described in section 5.3.2 above, Alice tells Bob and Charlie during the error estimation phase which measurement results they have to reveal. Then, Alice publicly announces her results for the respective qubits, followed by Bob. Afterwards, Bob announces his corresponding measurement bases followed by Alice announcing her bases. Due to these informations Alice is able to check the correlation of the measurement bases and results with the state she prepared using table 5.3 from above. For all measurements where Bob and Charlie used non-corresponding bases Alice discards the respective results. For all the other measurements, if the results do not correlate for a certain number of times Alice has to assume that an adversary is present and aborts the protocol.

Karlsson et al. also showed in their article [84] that the protocol does become insecure if the sequence of revealing the bases and results is changed (i.e. first the bases are declared, then the results). In this case a good strategy for a dishonest Charlie is to capture Bob's qubit coming from Alice and send qubit D from a fake state, e.g. $|\Phi^-\rangle_{DE}$, instead. Bob then performs a measurement on qubit D and announces his basis. Charlie can measure the other qubit E according to the same basis and thus obtain Bob's exact result. Further, he measures the intercepted qubit B of the original state according to the same basis and his qubit C of the original state according to some random basis, as stated in the protocol. Due to this

information Charlie is always able to announce a result which agrees to both Bob's result of his measurement on the fake state and the initial state sent by Alice thus fulfilling the correlations in table 5.3. Hence, when Alice checks for the correlation between Bob's and Charlie's result Charlie's intervention does not introduce any error and leaves him undetected. In further consequence, Charlie is able to recreate Alice's secret from the remaining measurements without Bob's help.

From this strategy we see that a strictly defined sequence of the messages can be used to secure the KKI secret sharing scheme. Furthermore, this security argument can also be used to detect a dishonest party in the HBB scheme [84]. Nevertheless, we want to stress that relying on the sequence of messages is not a very efficient way to secure a protocol since such an order of messages is not implicitly preserved by the network. Hence, there is an overhead for managing the sequence of the messages and more communication has to be done between the parties. Alice has to tell each party when to send its result and has to wait for the response. In case of three parties as in the HBB or the KKI scheme this overhead is of no big significance but it can become large when going to n parties. Therefore, the method described in [128] is much more efficient.

6.3.5 Attacks on QSTS Protocols

When looking at the QSTS schemes described in section 5.3.3 above different attack scenarios are of interest. Intercepting a qubit in transit and measuring it is no longer a good strategy since these protocols are dealing with quantum information. Moreover, they make extensive use of entanglement as we can see from the protocols described in [92, 38, 39, 40]. Hence, collective attacks and strategies involving fake states are of higher interest. Regarding the protocol presented by Li et al. [92] it can easily be shown that the scheme is insecure against a dishonest party, e.g. Charlie. A good strategy for Charlie is to intercept the qubit flying from Alice to Bob and instead send a qubit from a fake state $|\Phi^+\rangle_{DE}$. If Alice decides that the secret should be reconstructed at Charlie's laboratory, Bob performs – according to the protocol – a measurement in the X-basis on the fake qubit D obtaining, for example, $|x+\rangle$. Due to entanglement Bob's action on qubit D alters the state of qubit E in Charlie's possession such that he obtains the same result as Bob. Based on this information, Charlie is able to project qubit B he intercepted onto $|x+\rangle$ and obtain the secret $|\varphi\rangle$ without Bob's help. Otherwise, if the secret should be reconstructed at Bob's

laboratory Charlie performs a measurement in the X-basis on his qubit C. This brings the qubit B in a state similar to the secret $|\varphi\rangle$ and Charlie teleports this state to Bob using the state $|\Phi^+\rangle_{DE}$ he shares with him. In this case Charlie has to collaborate with Bob to obtain the secret but his intervention is not detected. Therefore, Charlie has full information about half of the secrets without Bob's help which is too much for a secret sharing protocol.

As already pointed out above, the scheme presented in [39] is a rather straight forward extension of the above protocol to a secret consisting of two qubits. Thus, the attack strategy can also be extended to this protocol. In this scenario Charlie sends two fake states $|\Phi^+\rangle_{D_1E_1}$ and $|\Phi^+\rangle_{D_2E_2}$ to Bob and intercepts the qubits B_1 and B_2 coming from Alice. If Bob has to perform a measurement in the X-basis on his qubits, Charlie can obtain his results from his qubits E_1 and E_2 without Bob's help and project qubits B_1 and B_2 on the corresponding states. Otherwise, Charlie performs the measurements in the X-basis and teleports the result to Bob. Hence, Charlie's actions again stay undetected and he obtains full information about half of Alice's secrets without Bob's help.

One possibility to overcome that vulnerability of these two protocols is to allow Bob to measure in either the X- or the Y-basis. This does not change the protocol significantly because Charlie only has to apply an additional σ_y operation on his qubit if Bob measured in the Y-basis. Nevertheless, a dishonest Charlie can not obtain any useful information from his fake state $|\Phi^+\rangle$ since he does not know which basis Bob used. Accordingly, Charlie can not obtain Alice's secret although he intercepted the qubit flying to Bob and therefore has to rely on Bob's help. Another possibility is to introduce another step into the protocol before Bob performs his measurement. In this step Alice, Bob and Charlie test the CHSH inequalities using some of the qubits of their entangled states to guarantee that they really do share the desired entanglement. If they can be sure that there is only entanglement between Alice and Bob as well as Alice and Charlie, respectively, they can follow the protocols as described in the original versions [92, 39].

The protocol described in [38] is a little more complex because Alice, Bob and Charlie share GHZ states (cf. section 5.3.3 and figure 5.7) but the strategy is the same for the protocols in [92, 39]. The dishonest Charlie intercepts the qubits B_1 and B_2 coming from Alice, prepares a 4-qubit state $|\psi\rangle_{E_1E_2E_3E_4}$ as

$$|\psi\rangle = \frac{1}{2}\big(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle\big)_{E_1E_2E_3E_4} \tag{6.49}$$

and sends qubits E_1 and E_2 to Bob. Following the protocol Bob performs a Bell state measurement on his qubits of the fake state which leaves the qubits at Charlie's side in the same state as Bob's result, since

$$|\psi\rangle = \frac{1}{2}\big(|\Phi^+\rangle|\Phi^+\rangle + |\Phi^-\rangle|\Phi^-\rangle + |\Psi^+\rangle|\Psi^+\rangle + |\Psi^-\rangle|\Psi^-\rangle\big). \tag{6.50}$$

Therefore, Charlie can project the qubits B_1 and B_2 onto this state and obtain the secret from his qubits C_1 and C_2 without Bob's help. Additionally, if Charlie has to perform the measurement he teleports the secret into Bob's laboratory as described above. In this way Charlie stays undetected and obtains full information on half of Alice's secret states.

Chapter 7

Security of Multi-Qubit Protocols

We have seen that quantum cryptographic protocols involving single photons have been of major interest over the last years not alone due to the fact that they can be implemented with today's physical apparatus. Nevertheless, the application of entanglement and the phenomenon of entanglement swapping is of big interest, too. These concepts have been introduced in several protocols as the main resource for generating and distributing a secret between two or more parties.

In this chapter cryptographic protocols involving entanglement and entanglement swapping are at the focus of attention. We consider systems where at least 4 qubits (2 entangled pairs) are involved and 2 qubits are in transit between Alice and Bob, thus speaking of *multi-qubit* protocols as opposed to the last chapter. The main question is to which amount the entanglement between Alice and Bob can be used by an adversary to obtain information about the secret shared between them.

7.1 The ZLG Attack

Besides the Ekert protocol [51] described in section 5.2.2 above, there are other entanglement-based protocols for quantum key distribution. A large part of them makes use of entanglement swapping (cf. section 2.5.3 for details) as a way to generate and distribute the secret. Originating from these protocols also an attack strategy based on entanglement swapping has been considered by Zhang, Li and Guo [170] as described in the following paragraphs. Protocols as well as attack strategies based on entanglement swapping are a rather theoretical approach because the realization is very complex due to current limitations of the physical apparatus.

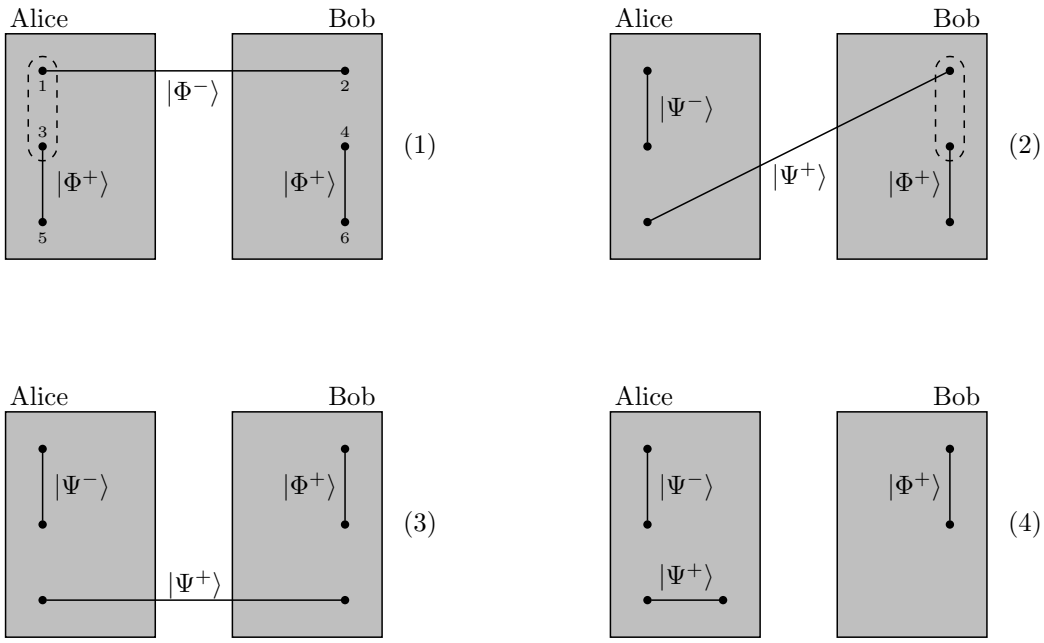

Figure 7.1: (Illustration of the protocol in [27].

Nevertheless, attack strategies based on entanglement swapping have to be considered because we have to concede Eve the possibility to hold the physical means to perform such attacks efficiently. Further, some protocols have already been shown to be insecure against them.

7.1.1 Application on a QKD Protocol

Protocol Description

An example for a QKD scheme open to an attack based on entanglement swapping is a protocol presented by Adan Cabello [27]. The main idea of this protocol is to get rid of measurement in alternative bases to avoid the loss of half of the qubits, on average, as it is the case in the prepare and measure protocols described above [8, 5, 11]. In this protocol Alice has two entangled pairs in the state $|\Phi^-\rangle_{12}$ and $|\Phi^+\rangle_{35}$ whereas Bob has one pair in the state $|\Phi^+\rangle_{46}$. Alice sends qubit 2 to Bob and performs a Bell state measurement on qubits 1 and 3 in her possession (cf. (1) in figure 7.1) which entangles qubits 2 and 5 due to entanglement swapping as

$$\begin{aligned} |\Phi^-\rangle_{12}|\Phi^+\rangle_{35} = \frac{1}{2}\Big(&|\Phi^-\rangle_{13}|\Phi^+\rangle_{25} - |\Phi^+\rangle_{13}|\Phi^-\rangle_{25} \\ &+|\Psi^-\rangle_{13}|\Psi^+\rangle_{25} - |\Psi^+\rangle_{13}|\Psi^-\rangle_{25}\Big). \end{aligned} \tag{7.1}$$

		Alice			
		$\|\Phi^+\rangle_{56}$	$\|\Phi^-\rangle_{56}$	$\|\Psi^+\rangle_{56}$	$\|\Psi^-\rangle_{56}$
Bob	$\|\Phi^+\rangle_{24}$	$\|\Phi^-\rangle_{13}$	$\|\Phi^+\rangle_{13}$	$\|\Psi^-\rangle_{13}$	$\|\Psi^+\rangle_{13}$
	$\|\Phi^-\rangle_{24}$	$\|\Phi^+\rangle_{13}$	$\|\Phi^-\rangle_{13}$	$\|\Psi^+\rangle_{13}$	$\|\Psi^-\rangle_{13}$
	$\|\Psi^+\rangle_{24}$	$\|\Psi^-\rangle_{13}$	$\|\Psi^+\rangle_{13}$	$\|\Phi^-\rangle_{13}$	$\|\Phi^+\rangle_{13}$
	$\|\Psi^-\rangle_{24}$	$\|\Psi^+\rangle_{13}$	$\|\Psi^-\rangle_{13}$	$\|\Phi^+\rangle_{13}$	$\|\Phi^-\rangle_{13}$

Table 7.1: Alice's state of qubits 1 and 3 depending on her and Bob's measurement result.

In detail, if qubits 1 and 3 are in the state $|\Psi^-\rangle_{13}$ after the Bell state measurement, Alice knows that qubits 2 and 5 are in the state $|\Psi^+\rangle_{25}$ (cf. (2) in figure 7.1). After receiving qubit 2 from Alice, Bob also performs a Bell state measurement on qubits 2 and 4 and obtains, for example, $|\Phi^+\rangle_{24}$. Now, qubits 5 and 6 are in the entangled state $|\Psi^+\rangle_{56}$ (cf. eq. (3) and (4) in figure 7.1) since

$$\begin{aligned} |\Psi^+\rangle_{25}|\Phi^+\rangle_{46} = \frac{1}{2}\Big(&|\Phi^+\rangle_{24}|\Psi^+\rangle_{56} - |\Phi^-\rangle_{24}|\Psi^-\rangle_{56} \\ &+|\Psi^+\rangle_{24}|\Phi^+\rangle_{56} - |\Psi^-\rangle_{24}|\Phi^-\rangle_{56}\Big) \end{aligned} \tag{7.2}$$

Bob sends qubit 6 to Alice, who is able to determine the state of qubits 5 and 6 by measuring them in the Bell basis. She publicly announces her result and both parties are able to calculate the state of qubits 1, 3 and 2, 4, respectively, using table 7.1. Alice and Bob use these two states to agree upon a shared secret key.

Attack Strategy and Security

In this protocol the entanglement between Alice and Bob is used to both establish and transport the secret between the two parties. The main question now is whether this entanglement, since it is the source of the information, can be misused to eavesdrop parts of the secret key. This question has been addressed in a comment on the Cabello protocol by Zhang, Li and Guo [170]. They presented an attack strategy which gives an adversary full information about the key shared between Alice and Bob (this is often referred to as the *ZLG attack*). The idea is that Eve prepares an entangled pair $|\Phi^+\rangle_{78}$ herself and uses qubit 7 to replace qubit 2 flying to Bob (cf.

(1) in figure 7.2). Due to entanglement swapping Bob's measurement on qubits 4 and 7 entangles qubits 6 and 8 shared between Bob and Eve leading to the state

$$|\Phi^+\rangle_{78}|\Phi^+\rangle_{46} = \frac{1}{2}\Big(|\Phi^+\rangle_{47}|\Phi^+\rangle_{68} + |\Phi^-\rangle_{47}|\Phi^-\rangle_{68} + |\Psi^+\rangle_{47}|\Psi^+\rangle_{68} + |\Psi^-\rangle_{47}|\Psi^-\rangle_{68}\Big). \tag{7.3}$$

Following the protocol, Bob sends qubit 6 to Alice and Eve intercepts it performing a Bell state measurement on qubits 6 and 8. As we have seen in eq. (7.1) above, qubits 2 and 5 are in the state $|\Psi^+\rangle_{25}$ according to Alice's measurement. Based on the outcome of her measurement Eve knows the exact result of Bob's measurement (cf. eq. (7.3) and (3) in figure 7.2). Moreover, she also knows how to change the state of qubits 2 and 5 such that the state of qubits 5 and 6 will correspond to Alice's and Bob's result in table 7.1. Therefore, Eve uses one of the Pauli operators onto qubit 2 to alter the state $|\Psi^+\rangle_{25}$ such that she applies $\mathbb{1}$ if she obtains $|\Phi^+\rangle_{68}$, σ_x if she obtains $|\Psi^+\rangle_{68}$, $i\sigma_y$ if she obtains $|\Psi^-\rangle_{68}$ and σ_z if she obtains $|\Phi^-\rangle_{68}$ (cf. (3) in figure 7.2). When Eve returns qubit 2 to Alice, Alice performs her measurement and will obtain a result correlated to Bob's measurement outcome, as it would be expected from table 7.1 (compare (4) in figure 7.1 and (4) in figure 7.2). Since Eve's qubits 6 and 8 are in the same state as Bob's qubits 4 and 7, Eve is able to obtain full information about the key between the two legitimate communication partners without being noticed.

Revised Protocol

As a reaction Cabello published an addendum to his protocol [28]. He described a solution to the problem, i.e. a way to secure the protocol in [27] against the ZLG attack. Cabello suggested to use the Hadamard operation H, which alters the Bell states such that

$$\begin{aligned} H|\Phi^\pm\rangle &= \frac{1}{\sqrt{2}}\Big(|\Phi^\mp\rangle \pm |\Psi^\pm\rangle\Big) = |\omega^\pm\rangle \\ H|\Psi^\pm\rangle &= \frac{1}{\sqrt{2}}\Big(|\Psi^\mp\rangle \pm |\Phi^\pm\rangle\Big) = |\chi^\pm\rangle \end{aligned} \tag{7.4}$$

In detail, Alice and Bob exchange qubits 2 and 6 as in the original protocol but they perform their Bell state measurements after they sent their respective qubits (cf. (2) and (3) in figure 7.3). Additionally, Alice decides randomly whether or not to perform a Hadamard operation on qubit 3 in her possession, which alters her Bell

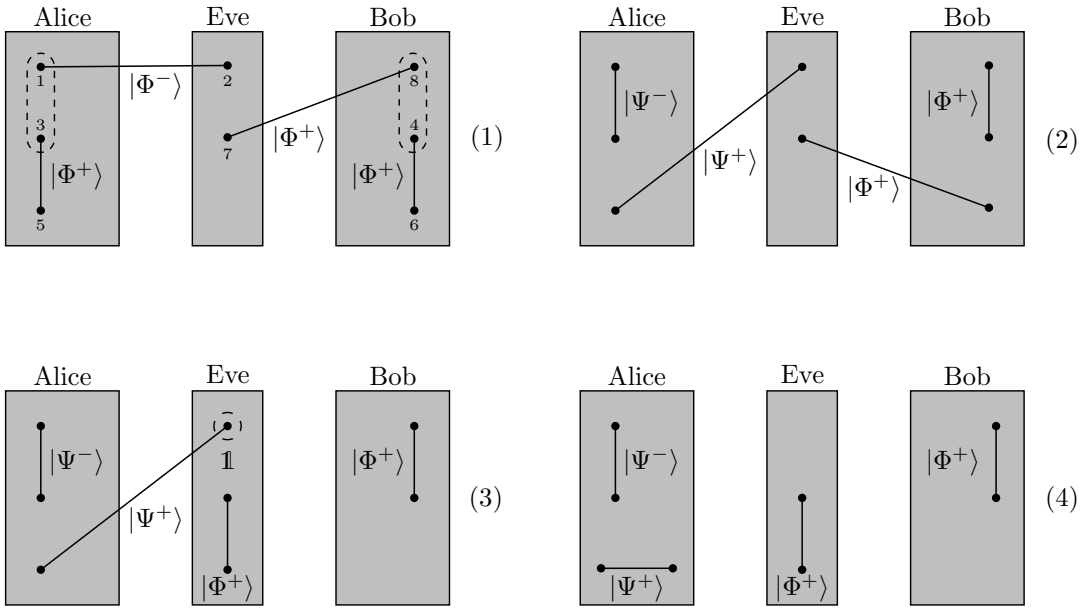

Figure 7.2: *(ZLG attack)* Illustration of the ZLG attack scenario [170].

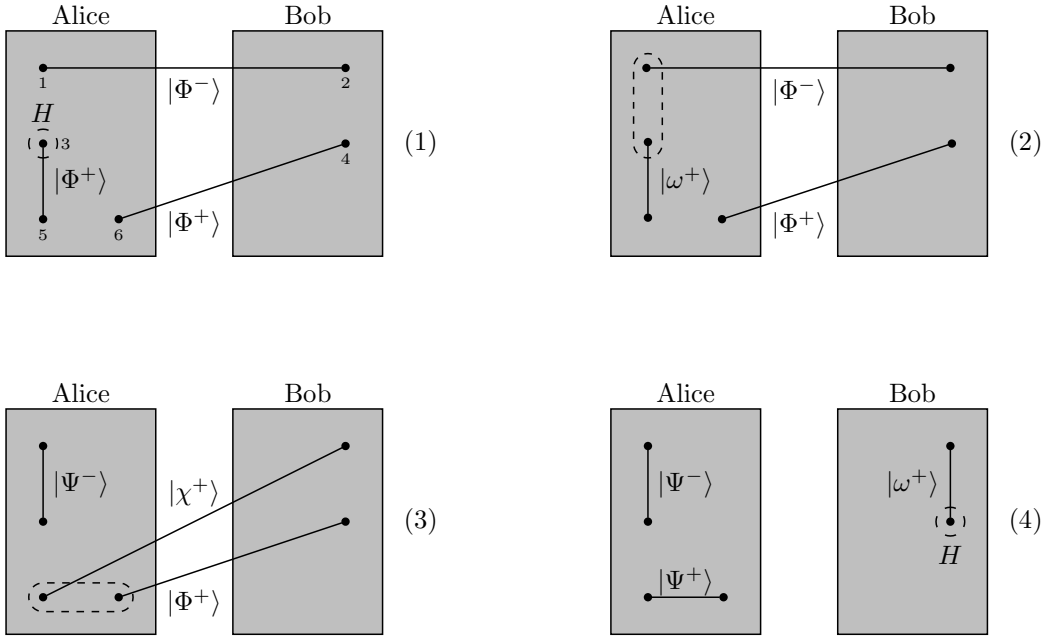

Figure 7.3: Illustration of the revised version of Cabello's QKD protocol [28].

		Alice (Secret)			
		$\|\Phi^+\rangle_{13}$	$\|\Phi^-\rangle_{13}$	$\|\Psi^+\rangle_{13}$	$\|\Psi^-\rangle_{13}$
Alice (Public)	$\|\Phi^+\rangle_{56}$	$\|\Phi^-\rangle_{24}$	$\|\Phi^+\rangle_{24}$	$\|\Psi^-\rangle_{24}$	$\|\Psi^+\rangle_{24}$
	$\|\Phi^-\rangle_{56}$	$\|\Psi^-\rangle_{24}$	$\|\Psi^+\rangle_{24}$	$\|\Phi^-\rangle_{24}$	$\|\Phi^+\rangle_{24}$
	$\|\Psi^+\rangle_{56}$	$\|\Phi^+\rangle_{24}$	$\|\Phi^-\rangle_{24}$	$\|\Psi^+\rangle_{24}$	$\|\Psi^-\rangle_{24}$
	$\|\Psi^-\rangle_{56}$	$\|\Psi^+\rangle_{24}$	$\|\Psi^-\rangle_{24}$	$\|\Phi^+\rangle_{24}$	$\|\Phi^-\rangle_{24}$

Table 7.2: Bob's state of qubits 2 and 4 depending on Alice's measurement results for the revised protocol.

state measurement accordingly to

$$|\Phi^-\rangle_{12}|\omega^+\rangle_{35} = \frac{1}{2}\Big(|\Phi^+\rangle_{13}|\omega^-\rangle_{25} + |\Phi^-\rangle_{13}|\omega^+\rangle_{25} + |\Psi^+\rangle_{13}|\chi^-\rangle_{25} + |\Psi^-\rangle_{13}|\chi^+\rangle_{25}\Big). \tag{7.5}$$

Assuming Alice obtains $|\Psi^-\rangle_{13}$ the state of qubits 2 and 5 changes into $|\chi^+\rangle_{25}$. Alice's measurement on qubits 5 and 6 can then be written as

$$|\chi^+\rangle_{25}|\Phi^+\rangle_{46} = \frac{1}{2}\Big(|\Phi^+\rangle_{56}|\chi^+\rangle_{24} + |\Phi^-\rangle_{56}|\chi^-\rangle_{24} + |\Psi^+\rangle_{56}|\omega^+\rangle_{24} + |\Psi^-\rangle_{56}|\omega^-\rangle_{24}\Big). \tag{7.6}$$

Alice announces her choice together with the result of her measurement on qubits 5 and 6, which is in our example $|\Psi^+\rangle_{56}$. If Alice does use the Hadamard operation Bob also performs a Hadamard operation on qubit 4 to undo the Alice's effects (cf. (4) in figure 7.3) otherwise he does nothing. Finally, he performs the Bell state measurement on qubits 2 and 4. It has to be stressed that the Hadamard operation, applied on the first and second qubit of a Bell state leaves only the states $|\Phi^+\rangle$ and $|\Psi^-\rangle$ invariant whereas $|\Phi^-\rangle$ changes into $|\Psi^+\rangle$ and vice versa. Therefore, table 7.1 describing the correlations has to be slightly changed into table 7.2. This fact has to be kept in mind when evaluating the key.

Attack Strategy and Security of the Revised Protocol

When looking at the ZLG attack in this alternative scenario we immediately see that the strategy in its original formulation is not really effective any more as it is

shown in [28]. If Alice does not apply the Hadamard operation the strategy works perfectly for Eve as in the original version of the protocol. If Alice does apply the Hadamard operation Eve is still able to intercept qubit 2 and send qubit 7 to Bob instead as well as intercept qubit 6 coming from Bob. By measuring qubits 6 and 8 at this time Eve determines Bob's result and alters the state of qubits 1 and 2 with her Pauli operation. For example, assuming Eve obtains $|\Psi^-\rangle_{68}$ from her result Bob's state is also $|\Psi^-\rangle_{74}$ and she applies $i\sigma_y$ onto qubit 2 which leads to $|\Psi^+\rangle_{12}$. Eve returns qubit 2 to Alice who now applies the Hadamard operation onto qubit 3 and performs a Bell state measurement on it together with qubit 1 which leads to

$$\begin{aligned}|\Psi^+\rangle_{12}|\omega^+\rangle_{35} = \frac{1}{2}\Big(&|\Phi^+\rangle_{13}|\chi^+\rangle_{52} - |\Phi^-\rangle_{13}|\chi^-\rangle_{52} \\ &+|\Psi^+\rangle_{13}|\omega^+\rangle_{52} - |\Psi^-\rangle_{13}|\omega^-\rangle_{52}\Big)\end{aligned} \tag{7.7}$$

If Alice obtains $|\Psi^-\rangle_{13}$ from her measurement as in the examples above, her measurement on qubits 5 and 2 results either in $|\Phi^+\rangle_{52}$ or in $|\Psi^-\rangle_{52}$. Alice announces the state of qubits 5 and 2 together with the fact that she performed the Hadamard operation H and Bob also applies the operation H thus changing $|\Psi^-\rangle_{74}$ to $|\chi^-\rangle_{74}$. When he performs his measurement on the two qubits he either obtains $|\Psi^+\rangle_{74}$ or $|\Phi^-\rangle_{74}$. Comparing these outcomes with table 7.2 we see that although Alice's and Bob's results are uncorrelated they will end up with valid results half of the time. Hence, for a random application of the Hadamard operation this gives an average error probability

$$\big\langle P_e\big\rangle = \frac{1}{2}\times 0 + \frac{1}{2}\times\frac{2}{4} = \frac{1}{4} \tag{7.8}$$

which is equal to the full intercept-resend attack on the BB84 protocol (cf. eq. (6.24) in section 6.2.1 above). Whenever Alice and Bob apply the Hadamard operation Eve obtains a collision only half of the time. Otherwise, she obtains full information due to her intervention. Therefore, the average collision probability for Eve is

$$\big\langle P_c\big\rangle = \frac{1}{2}\times 1 + \frac{1}{2}\times\frac{1}{2} = \frac{3}{4}. \tag{7.9}$$

Further, the Shannon entropy $H = 0$, i.e. Eve has full information about the secret bits, whenever Alice applies the $\mathbb{1}$ operation, and the entropy is maximal whenever Alice applies the Hadamard operation. With a random application of the two operations we obtain the same entropy as in the full intercept-resend attack on the BB84 protocol, i.e.

$$H\big(S|M\big) = \frac{1}{2} \tag{7.10}$$

which defines Eve's information about the secret key as $I_{AE} = 1 - H(S|M) = 1/2$.

7.1.2 Application on a QSS Protocol

Protocol Description

In the same year Adan Cabello presented another protocol [26] for quantum key distribution and quantum secret sharing which is also open to a similar kind of attack. In this protocol three parties are involved which are able to distribute a key among them or share a secret between two of them. The aim is to use the 3 qubit entanglement of the GHZ state similar to the HBB protocol [68] described above to achieve these tasks. Therefore, each party is in possession of an entangled pair, i.e. $|\Phi^+\rangle_{12}$, $|\Phi^+\rangle_{4C}$,$|\Phi^+\rangle_{5D}$, and Alice generates the GHZ state $|P_{00}^+\rangle_{3AB}$ at her side (cf. (1) in figure 7.4). She keeps qubit 3 of the GHZ state and sends the other two qubits to Bob and Charlie, respectively. Then, Alice performs a Bell state measurement on qubits 2 and 3, which alters the GHZ state as

$$\begin{aligned} |\Phi^+\rangle_{12}|P_{00}^+\rangle = \frac{1}{2}\Big(&|\Phi^+\rangle_{23}|P_{00}^+\rangle_{1AB} + |\Phi^-\rangle_{23}|P_{00}^-\rangle_{1AB} \\ &+|\Psi^+\rangle_{23}|P_{11}^+\rangle_{1AB} + |\Psi^-\rangle_{23}|P_{11}^-\rangle_{1AB}\Big). \end{aligned} \tag{7.11}$$

Bob performs his measurement on qubits 4 and A and Charlie performs his measurement on qubits 5 and B (cf. (2) in figure 7.4). As a consequence qubits 1, C and D are now in a GHZ state due to entanglement swapping as it is described in table 7.3 (there are similar tables if Alice obtains $|\Phi^-\rangle_{23}$, $|\Psi^\pm\rangle_{23}$. For example, we see from table 7.3 that if Alice, Bob and Charlie obtained $|\Phi^+\rangle$ from their respective measurements this leaves qubits 1, C and D still in the GHZ state $|P_{00}^+\rangle_{1CD}$, as presented in figure 7.4.

Bob and Charlie send their remaining qubits C and D back to Alice, who performs a GHZ state measurement and publicly announces the outcome (cf. (3) and (4) in figure 7.4). Based on this public result and the results of their own measurements the three parties can realize a QSS scheme where Bob and Charlie have to work together to recover both of Alice's secret bits. Alternatively, a QKD protocol can be realized since Bob and Charlie are always able to individually obtain one bit of information about Alice's secret from their own measurement [28].

		Bob			
		$\|\Phi^+\rangle_{4A}$	$\|\Phi^-\rangle_{4A}$	$\|\Psi^+\rangle_{4A}$	$\|\Psi^-\rangle_{4A}$
Charlie	$\|\Phi^+\rangle_{5B}$	$\|P^+_{00}\rangle_{1CD}$	$\|P^-_{00}\rangle_{1CD}$	$\|P^+_{10}\rangle_{1CD}$	$\|P^-_{10}\rangle_{1CD}$
	$\|\Phi^-\rangle_{5B}$	$\|P^-_{00}\rangle_{1CD}$	$\|P^+_{00}\rangle_{1CD}$	$\|P^-_{10}\rangle_{1CD}$	$\|P^+_{10}\rangle_{1CD}$
	$\|\Psi^+\rangle_{5B}$	$\|P^+_{01}\rangle_{1CD}$	$\|P^-_{01}\rangle_{1CD}$	$\|P^+_{11}\rangle_{1CD}$	$\|P^-_{11}\rangle_{1CD}$
	$\|\Psi^-\rangle_{5B}$	$\|P^-_{01}\rangle_{1CD}$	$\|P^+_{01}\rangle_{1CD}$	$\|P^-_{11}\rangle_{1CD}$	$\|P^+_{11}\rangle_{1CD}$

Table 7.3: Alice's GHZ state after Bob's and Charlie's measurement (assuming Alice herself obtained $|\Phi^+\rangle_{23}$).

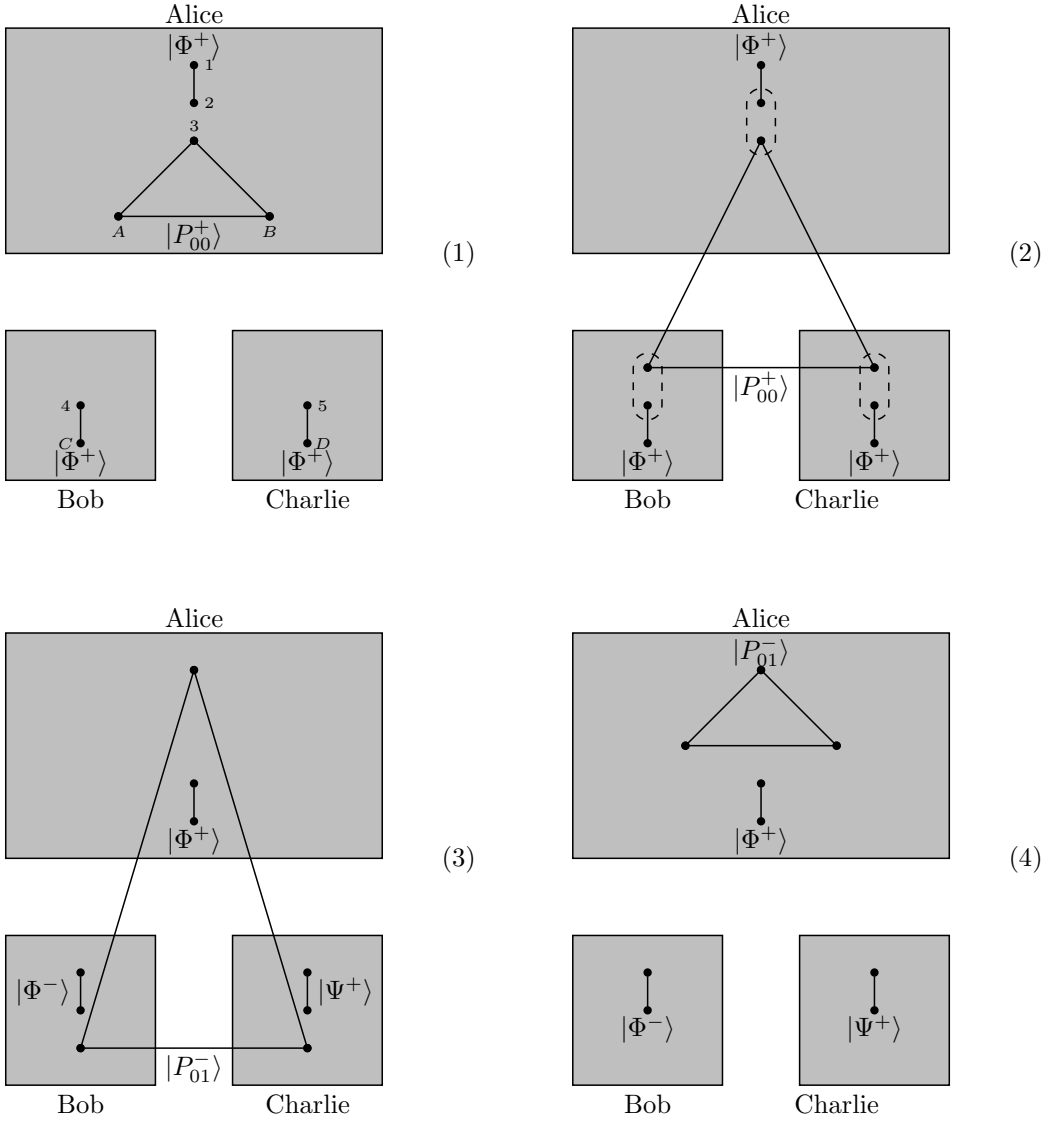

Figure 7.4: Illustration of the protocol in [26].

Attack Strategy and Security

It has been shown by Lee et al. [90] that also this protocol is open to the ZLG attack. In detail, Eve prepares two entangled pairs in the state $|\Phi^+\rangle_{PQ}$ and $|\Phi^+\rangle_{RS}$ and intercepts qubits A and B coming from Alice. She keeps the qubits P and R and forwards qubit Q and qubit S to Bob and Charlie, respectively (cf. (1) in figure 7.5). Both parties perform their measurement as described in the protocol and they return the qubits C and D. Eve intercepts also these qubits and performs a Bell measurement on the pairs P, C and R, D. Due to entanglement swapping these measurements can be described as

$$\begin{aligned} |\Phi^+\rangle_{4C}|\Phi^+\rangle_{PQ} = \frac{1}{2}\Big(&|\Phi^+\rangle_{4Q}|\Phi^+\rangle_{PC} + |\Phi^-\rangle_{4Q}|\Phi^-\rangle_{PC} \\ &+|\Psi^+\rangle_{4Q}|\Psi^+\rangle_{PC} - |\Psi^-\rangle_{4Q}|\Psi^-\rangle_{PC}\Big) \\ |\Phi^+\rangle_{5D}|\Phi^+\rangle_{RS} = \frac{1}{2}\Big(&|\Phi^+\rangle_{5S}|\Phi^+\rangle_{RD} + |\Phi^-\rangle_{5S}|\Phi^-\rangle_{RD} \\ &+|\Psi^+\rangle_{5S}|\Psi^+\rangle_{RD} - |\Psi^-\rangle_{5S}|\Psi^-\rangle_{RD}\Big). \end{aligned} \tag{7.12}$$

From eq. (7.12) we immediately see that Eve obtains the same result as Bob and Charlie, respectively, from her measurements. According to her results Eve is able to select a Pauli operator and apply it on the qubits A and B she intercepted from Alice to preserve the correlation given in table 7.3 (cf. (3) in figure 7.5). She uses the mapping

$$|\Phi^+\rangle \longmapsto \mathbb{1} \quad |\Phi^-\rangle \longmapsto \sigma_z \quad |\Psi^+\rangle \longmapsto \sigma_x \quad |\Psi^-\rangle \longmapsto \sigma_y \tag{7.13}$$

i.e. Eve applies a σ_x operation on qubit A if she obtained $|\Psi^+\rangle_{PC}$ and a σ_z operation on qubit B if she obtained $|\Phi^-\rangle_{RD}$. Since they are still in a GHZ state together with qubit 1 from Alice, these operations alter the overall state in a way such that it correlates with Alice's, Bob's and Charlie's measurement results (compare (4) in figure 7.4 with table 7.3). In the end Eve returns the two qubits to Alice, who performs a GHZ state measurement on them as described in the protocol. The three legitimate communication parties will not detect Eve since, due to her Pauli operations, she does not introduce any error in the protocol. As pointed out above Eve knows from her measurement the exact state of Bob's and Charlie's secret measurements and therefore has also full information about Alice's secret.

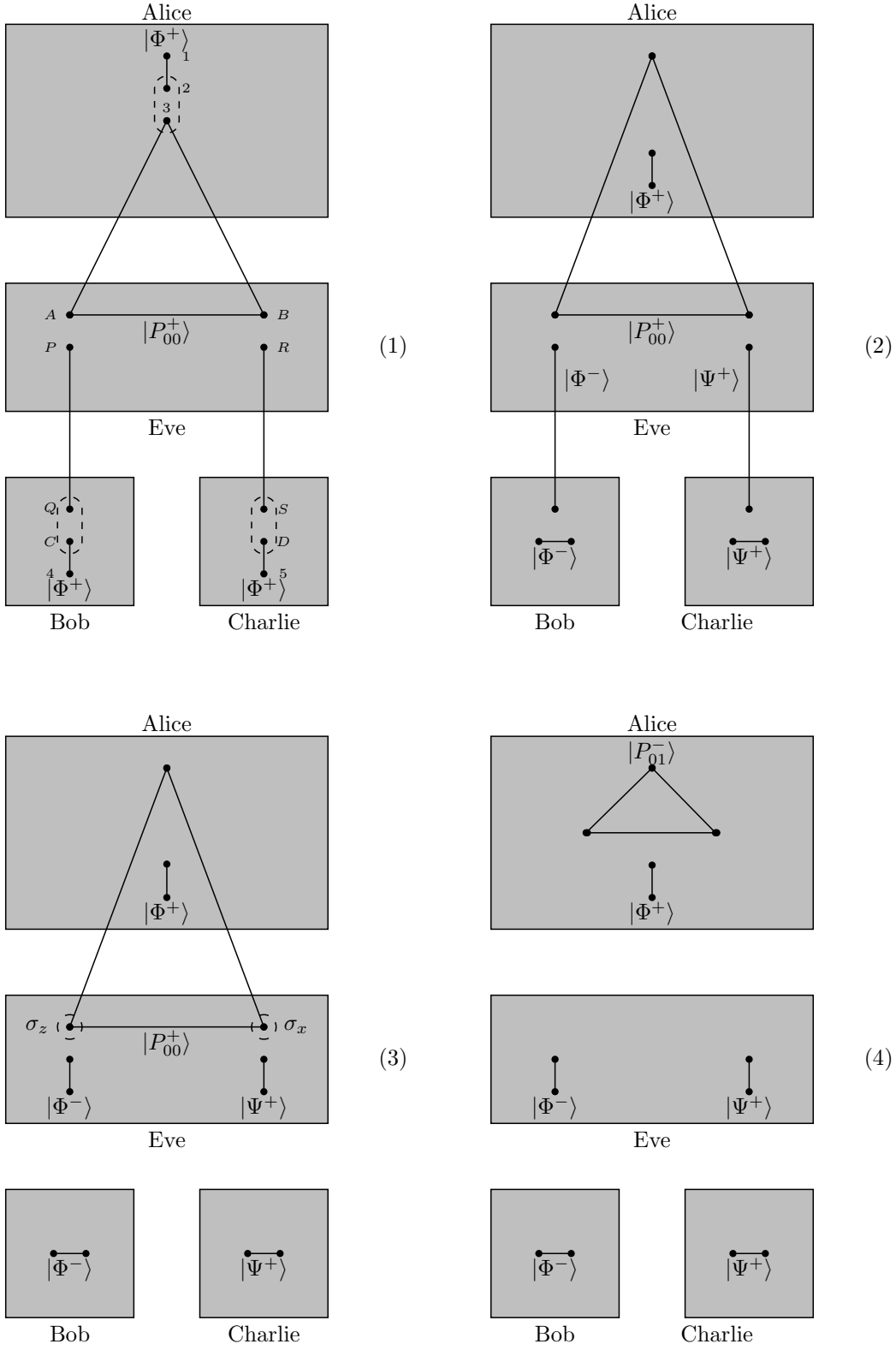

Figure 7.5: *(ZLG attack)* Illustration of the ZLG attack strategy on Cabello's QSS protocol [26] with an external adversary Eve.

Revised Protocol

In their paper [90] Lee et al. also presented a method to protect Cabello's protocol against the ZLG attack. In this case Bob and Charlie use the quantum Fourier transformation (QFT) defined as

$$|j\rangle \overset{QFT}{\longmapsto} \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\Pi ijk/N} |k\rangle \tag{7.14}$$

to secure the qubits in transit. (cf. for example [109] for details on the QFT). In this special case applying the QFT has the same effect as applying the Hadamard operation. Therefore, we will use the Hadamard operation in the following considerations. The course of the protocol is slightly different to the original one. Mainly, Alice, Bob and Charlie exchange all their qubits before performing any measurement (cf. (1) in figure 7.6). Additionally, Bob and Charlie randomly apply a Hadamard operation on the qubits in their respective laboratories. As already discussed this changes the state $|\Phi^+\rangle$ according to eq. (7.4). After Alice received the qubits from Bob and Charlie she performs a Bell state measurement on qubits 2 and 3 and Bob and Charlie act similarly on their qubits 4 and A as well as 5 and B, respectively, as described in the original protocol (cf. (2) in figure 7.6). If both Bob and Charlie do not apply the Hadamard operation the protocol is the same as in the original version. If either of them applies the Hadamard operation onto his qubit this alters the GHZ state after Bob's measurement as

$$\begin{aligned} |\omega^+\rangle_{4C}|P_{00}^+\rangle_{1AB} = \frac{1}{2}\Big(& |\Phi^+\rangle_{4A}\frac{1}{\sqrt{2}}\big(|P_{00}^-\rangle + |P_{10}^+\rangle\big)_{1CB} \\ & +|\Phi^-\rangle_{4A}\frac{1}{\sqrt{2}}\big(|P_{00}^+\rangle + |P_{10}^-\rangle\big)_{1CB} \\ & +|\Psi^+\rangle_{4A}\frac{1}{\sqrt{2}}\big(|P_{00}^-\rangle - |P_{10}^+\rangle\big)_{1CB} \\ & -|\Psi^-\rangle_{4A}\frac{1}{\sqrt{2}}\big(|P_{00}^+\rangle - |P_{10}^-\rangle\big)_{1CB}\Big) \end{aligned} \tag{7.15}$$

and similarly for Charlie's measurement (in this case Charlie obtains either $|P_{00}^{\pm}\rangle$ or $|P_{01}^{\pm}\rangle$). In case both parties apply the Hadamard operation the GHZ state changes

into

$$
\begin{aligned}
&|\omega^+\rangle_{5D}\frac{1}{\sqrt{2}}\big(|P^-_{00}\rangle + |P^+_{10}\rangle\big)_{1CB} = \\
&\quad = \frac{1}{2}\Big(|\Phi^+\rangle_{5B}\frac{1}{2}\big(|P^+_{00}\rangle + |P^-_{01}\rangle + |P^-_{10}\rangle + |P^+_{11}\rangle\big)_{1CD} \\
&\qquad +|\Phi^-\rangle_{5B}\frac{1}{2}\big(|P^-_{00}\rangle + |P^+_{01}\rangle + |P^+_{10}\rangle + |P^-_{11}\rangle\big)_{1CD} \\
&\qquad +|\Psi^+\rangle_{5B}\frac{1}{2}\big(|P^-_{00}\rangle - |P^+_{01}\rangle + |P^+_{10}\rangle - |P^-_{11}\rangle\big)_{1CD} \\
&\qquad -|\Psi^-\rangle_{5B}\frac{1}{2}\big(|P^+_{00}\rangle + |P^-_{01}\rangle - |P^-_{10}\rangle + |P^+_{11}\rangle\big)_{1CD}\Big)
\end{aligned}
\tag{7.16}
$$

if Bob obtained $|\Phi^+\rangle_{4A}$ and equivalently for $|\Phi^-\rangle_{4A}$ and $|\Psi^\pm\rangle_{4A}$. Then, Bob and Charlie publicly announce their decision and Alice performs the Hadamard operation on the qubits she received from Bob and Charlie according to their decision (cf. (3) and (4) in figure 7.6). Alice's Hadamard operation brings the GHZ state back to the state corresponding to the correlation described in table 7.3.

Attack Strategy and Security of the Revised Protocol

Similar to the addendum to Cabello's protocol [28] Eve is not able to overcome the random application of the Hadamard operation by Bob and Charlie. If Eve follows the attack strategy described in [90] she intercepts the qubits A and B coming from Alice as well as the qubits C and D coming Bob and Charlie but she can not find a Pauli operation to correct the GHZ state. In detail, Eve forwards qubits Q and S to Bob and Charlie, respectively, and measures the qubit pairs P, C and R, D. Depending on whether Bob and Charlie applied the Hadamard operation these measurements are similar to eq. (7.12) or to

$$
\begin{aligned}
|\omega^+\rangle_{4C}|\Phi^+\rangle_{PQ} &= \frac{1}{2}\Big(|\Phi^+\rangle_{PC}|\omega^+\rangle_{4Q} + |\Phi^-\rangle_{PC}|\omega^-\rangle_{4Q} \\
&\qquad +|\Psi^+\rangle_{PC}|\chi^+\rangle_{4Q} - |\Psi^-\rangle_{PC}|\chi^-\rangle_{4Q}\Big) \\
|\omega^+\rangle_{5D}|\Phi^+\rangle_{RS} &= \frac{1}{2}\Big(|\Phi^+\rangle_{RD}|\omega^+\rangle_{5S} + |\Phi^-\rangle_{RD}|\omega^-\rangle_{5S} \\
&\qquad +|\Psi^+\rangle_{RD}|\chi^+\rangle_{5S} - |\Psi^-\rangle_{RD}|\chi^-\rangle_{5S}\Big).
\end{aligned}
\tag{7.17}
$$

As we can see Eve's measurement determines the states of qubits 4, Q and 5, S, respectively, at Bob's and Charlie's laboratory. Based on her outcomes Eve performs the Pauli operations given by eq. (7.13) on qubits A and B and returns them to Alice. Upon receipt of the qubits Alice performs her Bell state measurement on

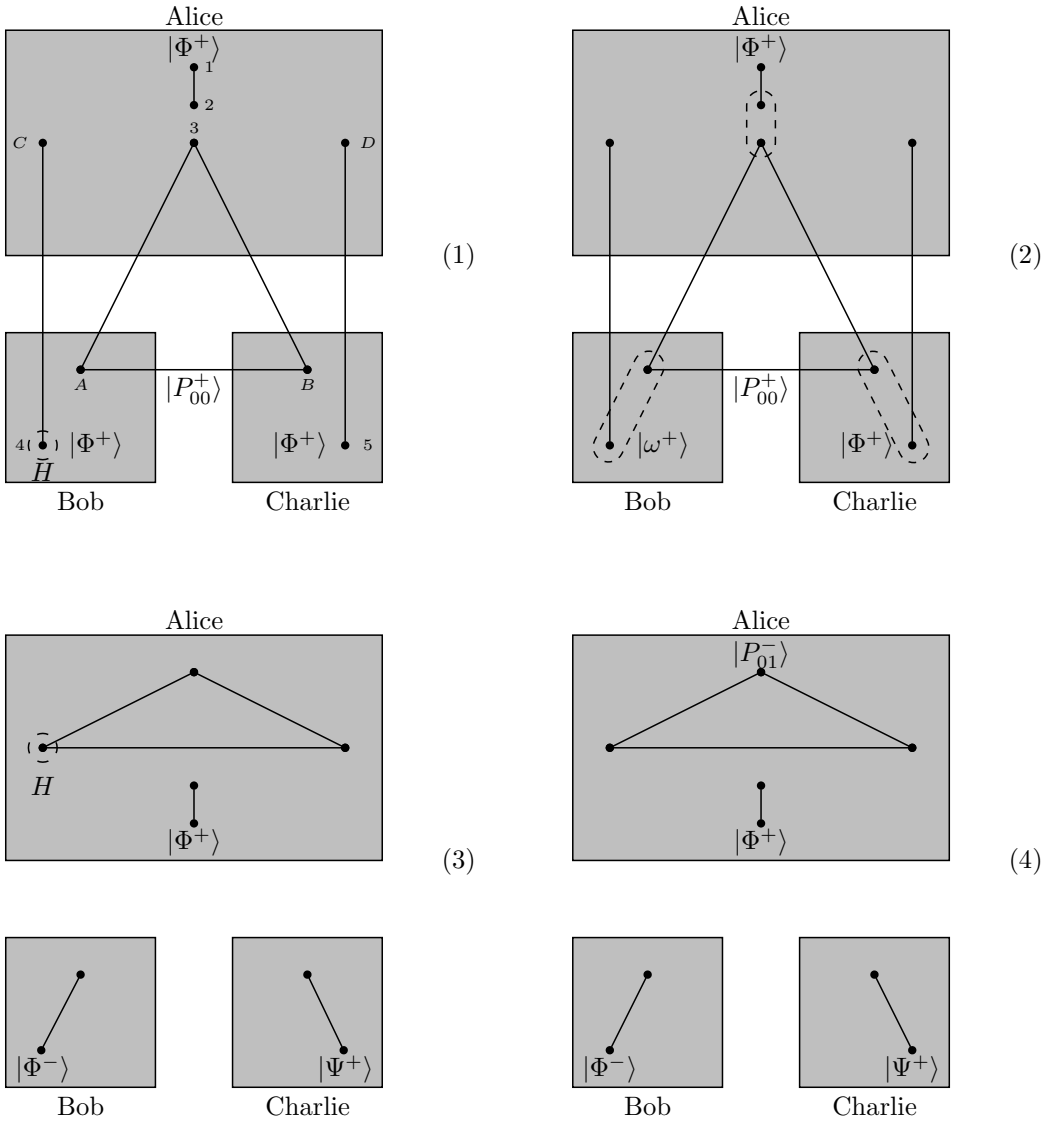

Figure 7.6: Illustration of revised version of Cabello's QSS protocol [26]. In this case only Bob applies the Hadamard operation on his qubit.

qubits 2 and 3. Simultaneously, Bob measure qubits 4, Q and 5, S, respectively. As we can see from eq. (7.17) above Bob as well as Charlie will obtain two possible results each with probability 1/2. Assuming only Bob performed the Hadamard operation and the results for Eve, Bob and Charlie are $|\Phi^+\rangle_{PC}$ and $|\Phi^+\rangle_{RD}$ as well as $|\Phi^-\rangle_{4Q}$ and $|\Phi^+\rangle_{5S}$ it is easy to compute that the GHZ state is of the form

$$\frac{1}{\sqrt{2}}\big(|P_{00}^-\rangle + |P_{10}^+\rangle\big). \tag{7.18}$$

From table 7.3 we see that only $|P_{00}^-\rangle$ is the correct state for this combination. Similarly, if both Bob and Charlie perform the Hadamard operation only 1 out of 4 possible results of Alice's measurement on the GHZ state corresponds to Bob's and Charlie's results. As already pointed out, if neither of them applies the Hadamard operation Alice will always obtain a correlated result. Therefore, the expected error probability for the revised protocol is

$$\big\langle P_e \big\rangle = \frac{1}{4}\left(0 + \frac{1}{2} + \frac{1}{2} + \frac{3}{4}\right) = \frac{7}{16} \tag{7.19}$$

which is almost twice as much as in Cabello's revised QKD protocol [28] described above (cf. eq. (7.8)) due to Bob's and Charlie's combined usage of the Hadamard operation. Nevertheless, the expected collision probability is much higher compared to Cabello's revised QKD protocol, i.e.

$$\big\langle P_c \big\rangle = \frac{7}{8} \tag{7.20}$$

which leads also to a Shannon entropy $H(S|M) = 0.25$. Thus, Eve's information about the key is in this case is

$$I_{AE} = 1 - H\big(S|M\big) = \frac{3}{4} \tag{7.21}$$

such that she knows 75% of Alice's secret bit string after her attack. Since she introduces a very high error rate it is rather easy for Alice and Bob to detect her intervention such that Eve is not able to take advantage of her information about the secret.

As pointed out in section 6.3 above regarding quantum secret sharing protocols the involved parties always have to be aware of an adversary from the inside. In this case, Lee et al. showed that a dishonest Charlie also has no chance to stay undetected when using the same strategy as Eve to interfere with the protocol.

Charlie intercepts Alice's qubit A and resends qubit Q of the state $|\Phi^+\rangle_{PQ}$. Further, he intercepts Bob's qubit C and performs a Bell measurement as described in eq. (7.12) or (7.17) depending on whether Bob applied the Hadamard operation or not. We already showed that Charlie introduces no error if Bob does not apply the Hadamard operation. In case he does apply the Hadamard operation Bob and Alice will obtain uncorrelated results half of the time (based on the same argumentation given in the paragraph above describing Eve's attack). Thus, the expected error probability is

$$\langle P_e \rangle = \frac{1}{2}\left(0 + \frac{1}{2}\right) = \frac{1}{4} \tag{7.22}$$

which is lower than in the attack from an external eavesdropper described above. It is remarkable that the expected collision probability for this scenario is

$$\langle P_c \rangle = 1 \tag{7.23}$$

which means that Charlie has full information about Alice's secret, i.e $H(S|M) = 0$ and $I_{AE} = 1$. Every combination of Charlie's measurement results together with the public information from Alice and Bob corresponds to one of the four possible secret results of Alice. Although Charlie's measurement result of the intercepted qubits does not always correspond to Bob's secret measurement result there is still a chance that Bob's secret result together with Charlie's secret result and Alice's public GHZ state is a valid correlation and Charlie's intervention is not detected. Nevertheless, Charlie is not able to reduce the error rate by any means since he can not control Bob's application of the Hadamard operation. Hence, it is in this case very obvious that a dishonest party is much more successful in eavesdropping the key because Charlie has a lot more information and introduces less error than an external adversary.

In their article [90] Lee et al. described a slightly different attack strategy on their revised version of Cabello's protocol. They showed that their revised version is secure against this attack where Eve uses entanglement swapping. As described in the article, Eve prepares 4 instead of just 2 Bell states such that the initial state of Alice, Bob, Charlie and Eve is

$$|\Phi^+\rangle_{12}|P_{00}^+\rangle_{3AB} \otimes |\Phi^+\rangle_{4C} \otimes |\Phi^+\rangle_{5D} \otimes |\Phi^+\rangle_{PQ}|\Phi^+\rangle_{RS}|\Phi^+\rangle_{TU}|\Phi^+\rangle_{VW}. \tag{7.24}$$

Eve intercepts all qubits in transit, i.e. qubits A and B coming from Alice, which she replaces by Q and S, respectively, as well as qubits C and D coming from Bob

and Charlie, which she replaces by U and W, respectively. As described above, Alice's measurement on qubits 2 and 3 alters the GHZ state in a way described in eq. (7.11). Following the protocol Bob and Charlie individually decide at random whether to apply a Hadamard operation and perform a Bell state measurement on their respective qubits. Due to entanglement swapping this alters qubits P, C and R, D in Eve's possession. When Bob and Charlie announce the decision about their operation, Eve also applies the Hadamard operation onto qubits C and D to bring the qubit pairs back into Bell states. Further, she applies Hadamard operations on qubits T and V if necessary to impersonate Bob's and Charlie's decisions. Hence, Eve obtains full information about Alice's secret from her measurement results from the qubit pairs P, C and R, D, i.e. the expected collision probability $\langle P_c \rangle = 1$. Because the qubits 3, U and W located at Alice's laboratory are not in a GHZ state Alice's measurement on them returns a random result. Hence, there is only one state such that the correlations given in table 7.3 between Alice's result from that measurement and Bob's and Charlie's result is still valid. This gives the average error probability $\langle P_e \rangle = 7/8$ which is very large compared to the QKD schemes described in the previous chapter.

Eve is also able to entangle qubits 3, U and W into a GHZ state at Alice's laboratory has not been considered in the attack described in [90]. Therefore, she first has to alter the GHZ state she still shares with Alice according to her results from the qubit pairs P, C and R, D and the mapping in eq. (7.13). Then, Eve teleports the information of qubits A and B onto qubits U and W, respectively, in Alice's possession which is achieved using entanglement swapping. Due to the teleportation of her information onto the GHZ state Eve obtains random results such that the correlations in table 7.3 are violated with probability 1/8. Hence, applying this additional step to the attack does not give Eve a better chance to succeed in her attempt to stay undetected.

7.2 The Simulation Attack

7.2.1 The Basic Idea

In the previous section we discussed in two examples how the entanglement between Alice and Bob can be exploited by an eavesdropper Eve to obtain full information

about the shared key. Now, we are going to describe a more general attack based on the same principle. In this attack strategy Eve prepares a multi-qubit state and entangles herself with the legitimate parties by the help of entanglement swapping. Due to the fact that Eve's intervention is mainly based on simulating Alice's and Bob's correlations and operations – as described in the following paragraphs – we will refer to this strategy as *simulation attack*.

As we have seen in the previous section the security check is based on the correlations between the respective measurement results of Alice and Bob coming from the entanglement swapping. If these correlations are violated Alice and Bob have to assume that an eavesdropper is present. Hence, Eve's major intention is to find a quantum state which preserves the correlation between the two legitimate parties. If she is able to find such a state Eve stays undetected during her intervention. The most intuitive candidate fulfilling these requirements is of course the state

$$|\varphi\rangle = |\Phi^+\rangle_{12}|\Phi^+\rangle_{34} = \frac{1}{2}\big(|0000\rangle + |0011\rangle + |1100\rangle + |1111\rangle\big)_{1234} \tag{7.25}$$

which comes directly from our basic definition of entanglement swapping (cf. eq. (2.41)) and hence perfectly preserves the correlation given in this equation if Alice performs a Bell state measurement on qubits 1 and 3, i.e.

$$|\varphi\rangle = \frac{1}{2}\big(|\Phi^+\rangle|\Phi^+\rangle + |\Phi^-\rangle|\Phi^-\rangle + |\Psi^+\rangle|\Psi^+\rangle + |\Psi^-\rangle|\Psi^-\rangle\big)_{1324}. \tag{7.26}$$

Nevertheless, Eve does not gain any information since the state $|\varphi\rangle$ only simulates the entanglement swapping. Therefore, she introduces 2 additional qubits to distinguish between the Alice's different measurement results. This changes the state $|\varphi\rangle$ to [129]

$$\begin{aligned}|\delta\rangle = \frac{1}{2\sqrt{2}}\Big(&|000000\rangle + |001101\rangle + |010111\rangle + |011010\rangle \\ &|100110\rangle + |101011\rangle + |110001\rangle + |111100\rangle\Big)_{123456}.\end{aligned} \tag{7.27}$$

This state preserves the correlation of Alice's and Bob's measurement results upon the entanglement swapping on qubits 1 and 3 and additionally gives Eve full information about the respective measurement results, i.e.

$$\begin{aligned}|\delta\rangle = \frac{1}{2}\Big(&|\Phi^+\rangle|\Phi^+\rangle|\Phi^+\rangle + |\Phi^-\rangle|\Phi^-\rangle|\Phi^-\rangle \\ &|\Psi^+\rangle|\Psi^+\rangle|\Psi^+\rangle + |\Psi^-\rangle|\Psi^-\rangle|\Psi^-\rangle.\Big)_{132456}\end{aligned} \tag{7.28}$$

In detail, Eve distributes qubits 1, 2, 3 and 4 between Alice and Bob such that Alice is in possession of qubits 1 and 3 and Bob is in possession of qubits 2 and 4. When Alice performs a Bell state measurement on qubits 1 and 3 the state of qubits 2 and 4 collapses into the same Bell state that Alice's obtained from her measurement as it is given by entanglement swapping (cf. eq. (2.41)). Hence, Eve stays undetected when Alice and Bob compare some of their results in public to check for eavesdroppers. Qubits 5 and 6, which remain at Eve's side, are also in the same state as Alice's and Bob's qubits. Therefore, Eve has full information about the secret measurements at Alice's and Bob's side and is able to perfectly eavesdrop the secret key later on.

We want to stress that the state $|\delta\rangle$ is generic for all protocols where 2 qubits are exchanged between Alice and Bob during one round of key generation as, for example, the QKD protocol presented by Cabello [27] (cf. section 7.1.1 above). For protocols with a higher number of qubits the state has to be extended accordingly (cf. for example section 8.4).

The distribution of the state $|\delta\rangle$ is done by entanglement swapping. Eve intercepts the qubit coming from Alice and performs a Bell state measurement on it together with the first qubit from $|\delta\rangle$. She obtains one of the four Bell states at random which changes the overall state of the other qubits a little, according to Eve's result. The measurement can be described as

$$\begin{aligned}
|\Phi^+\rangle|\delta\rangle = \frac{1}{2}\Big(&|\Phi^+\rangle\frac{1}{\sqrt{2}}\big(|000000\rangle + |001101\rangle + |010111\rangle + |011010\rangle \\
&\quad +|100110\rangle + |101011\rangle + |110001\rangle + |111100\rangle\big) \\
&+|\Phi^-\rangle\frac{1}{\sqrt{2}}\big(|000000\rangle + |001101\rangle + |010111\rangle + |011010\rangle \\
&\quad -|100110\rangle - |101011\rangle - |110001\rangle - |111100\rangle\big) \\
&+|\Psi^+\rangle\frac{1}{\sqrt{2}}\big(|000110\rangle + |001011\rangle + |010001\rangle + |011100\rangle \\
&\quad +|100000\rangle + |101101\rangle + |110111\rangle + |111010\rangle\big) \\
&+|\Psi^-\rangle\frac{1}{\sqrt{2}}\big(|000110\rangle + |001011\rangle + |010001\rangle + |011100\rangle \\
&\quad -|100000\rangle - |101101\rangle - |110111\rangle - |111010\rangle\big)\Big).
\end{aligned} \tag{7.29}$$

Based on her result Eve is able to correct the state back to its initial form $|\delta\rangle$ using the Pauli operations. Therefore, she performs a σ_z operation on qubits 4 and 6, if she obtains $|\Phi^-\rangle$, a σ_x operation onto qubits 4 and 5, if she obtains $|\Psi^+\rangle$. If she

obtains $|\Psi^-\rangle$ she combines these two actions, i.e. she first performs a σ_x on qubits 4 and 5 followed by a σ_z on qubits 4 and 6. In case Eve obtains $|\Phi^+\rangle$ she does not need to do anything. We see from eq. (7.29) above that these actions change the overall state of the 6 qubits after the entanglement swapping back into $|\delta\rangle$ although Alice is now in possession of one qubit of the state.

As pointed out above, the state $|\delta\rangle$ is applicable in all protocols where 2 qubits are exchanged between Alice and Bob during one round of key generation. Thus, we also have to discuss how the entanglement swapping between Eve and Bob works. Eve intercepts the qubit coming from Bob and performs a Bell state measurement on it together with qubit 4, which leads to

$$\begin{aligned}
|\Phi^+\rangle|\delta\rangle = \frac{1}{2}\Big(&|\Phi^+\rangle\frac{1}{\sqrt{2}}\big(|000000\rangle + |001101\rangle + |010111\rangle + |011010\rangle \\
&\quad +|100110\rangle + |101011\rangle + |110001\rangle + |111100\rangle\big) \\
&+|\Phi^-\rangle\frac{1}{\sqrt{2}}\big(|000000\rangle - |001101\rangle - |010111\rangle + |011010\rangle \\
&\quad -|100110\rangle + |101011\rangle + |110001\rangle - |111100\rangle\big) \\
&+|\Psi^+\rangle\frac{1}{\sqrt{2}}\big(|000100\rangle + |001001\rangle + |010011\rangle + |011110\rangle \\
&\quad +|100010\rangle + |101111\rangle + |110101\rangle + |111000\rangle\big) \\
&-|\Psi^-\rangle\frac{1}{\sqrt{2}}\big(|000100\rangle - |001001\rangle - |010011\rangle + |011110\rangle \\
&\quad -|100010\rangle + |101111\rangle + |110101\rangle - |111000\rangle\big)\Big).
\end{aligned} \tag{7.30}$$

Therefore, Eve is again able to correct the state back to $|\delta\rangle$ regardless of the result of her measurement. She performs the σ_z operation this time on qubits 3 and 5 if she obtains $|\Phi^-\rangle$ and the σ_x operation on qubits 3 and 6 if she obtains $|\Psi^+\rangle$. For her result $|\Psi^-\rangle$ she first applies a σ_x operation on qubits 3 and 6 and further a σ_z operation on qubits 3 and 5, whereas for the result $|\Phi^+\rangle$ she already obtained the state $|\delta\rangle$. Hence, we showed that Eve is always able to distribute her state $|\delta\rangle$ between Alice and Bob to simulate the correlations although her entanglement swapping provides random results.

The first question that may arise is whether the correlation is still preserved if Alice and Bob use different initial states than $|\Phi^+\rangle$. In this case the correlation for all possible initial states is given in table 2.1 in section 2.5.3 above. Using the state $|\delta\rangle$ the correlation is automatically preserved for every possible initial state. For

example, we suppose that Alice prepares the state $|\Psi^-\rangle_{12}$ and Bob prepares $|\Phi^-\rangle_{34}$. Alice sends the second qubit of her state to Bob but Eve intercepts this qubit and performs a Bell state measurement on it together with the first qubit of $|\delta\rangle_{P-U}$. We will assume that Eve obtains $|\Phi^-\rangle_{2P}$ from this measurement, which leaves the remaining qubits in the state

$$\begin{aligned} -\frac{1}{\sqrt{2}}\big(&|000110\rangle + |001011\rangle + |010001\rangle + |011100\rangle \\ &+|100000\rangle + |101101\rangle + |110111\rangle + |111010\rangle\big)_{1Q-U}. \end{aligned} \tag{7.31}$$

As already mentioned in the previous section Eve is able to correct the state as if she would have obtained $|\Phi^+\rangle_{2P}$ instead of $|\Phi^-\rangle_{2P}$. Therefore, she applies a σ_y operation onto qubits S and U which changes the overall state into

$$\begin{aligned} \frac{1}{\sqrt{2}}\big(&|000110\rangle + |001011\rangle + |010001\rangle + |011100\rangle \\ &-|100000\rangle - |101101\rangle - |110111\rangle - |111010\rangle\big)_{1Q-U}. \end{aligned} \tag{7.32}$$

Afterwards, Eve sends qubit Q of her state to Bob and intercepts qubit 3 of Bob's initial state $|\Phi^-\rangle_{34}$, which he intends to send to Alice. Eve again performs a Bell state measurement on the intercepted qubit and qubit S in her possession leading to the state

$$\begin{aligned} -\frac{1}{\sqrt{2}}\big(&|000010\rangle - |001111\rangle - |010101\rangle + |011000\rangle \\ &|100100\rangle - |101001\rangle - |110011\rangle + |111110\rangle\big)_{1QR4TU} \end{aligned} \tag{7.33}$$

assuming that Eve obtains $|\Psi^+\rangle_{3S}$. Based on her result she correct the state to

$$\begin{aligned} -\frac{1}{\sqrt{2}}\big(&|000110\rangle - |001011\rangle - |010001\rangle + |011100\rangle \\ &+|100000\rangle - |101101\rangle - |110111\rangle + |111010\rangle\big)_{1QR4TU}. \end{aligned} \tag{7.34}$$

performing a σ_x onto qubits R and U. Eve sends qubit R to Alice impersonating Bob's qubit. We can immediately derive from the equations above that after Alice's Bell state measurement on qubits 1 and R also Bob's qubits Q and 4 as well as Eve's qubits T and U collapse into a Bell state. Further, if Alice obtained $|\Phi^+\rangle_{1R}$ then Bob obtains $|\Psi^+\rangle_{Q4}$ and Eve obtains $|\Psi^-\rangle_{TU}$ (cf. table 7.4 for a total overview on the correlations). Hence, we see that the correlation for the initial states $|\Psi^-\rangle_{12}$ and $|\Phi^-\rangle_{34}$ as given in table 2.1 is also preserved using the state $|\delta\rangle$.

Alice	Bob	Eve
$\|\Phi^+\rangle_{1R}$	$\|\Psi^+\rangle_{Q4}$	$\|\Psi^-\rangle_{TU}$
$\|\Phi^-\rangle_{1R}$	$\|\Psi^-\rangle_{Q4}$	$\|\Psi^+\rangle_{TU}$
$\|\Psi^+\rangle_{1R}$	$\|\Phi^+\rangle_{Q4}$	$\|\Phi^-\rangle_{TU}$
$\|\Psi^-\rangle_{1R}$	$\|\Phi^-\rangle_{Q4}$	$\|\Phi^+\rangle_{TU}$

Table 7.4: Correlation between Alice's, Bob's and Eve's measurement results after entanglement swapping using the initial states $|\Psi^-\rangle_{12}$ and $|\Phi^-\rangle_{34}$.

Although Eve does no longer obtain the same result as Alice and Bob her state is nevertheless completely correlated to the states at Alice's and Bob's laboratory. Based on the initial states she is able to compute Alice's and Bob's secret results using Pauli operations. Since Alice's initial state is $|\Psi^-\rangle_{12} = \sigma_y|\Phi^+\rangle_{12}$ Eve knows that Alice's secret result is $\sigma_y|\psi\rangle$ where $|\psi\rangle \in \{|\Phi^\pm\rangle, |\Psi^\pm\rangle\}$ is the state of Eve's qubits $T$and U. Similarly, Eve knows that Bob's secret result is $\sigma_z|\psi\rangle$ since Bob prepared $|\Phi^-\rangle_{34} = \sigma_z|\Phi^+\rangle_{34}$.

An important implication from this fact is that even if Alice and Bob choose their initial states at random Eve is still able to preserve the correlations given in table 2.1 using the state $|\delta\rangle$ for eavesdropping. At some point during the protocol Alice and Bob have to announce their initial states and at this time, as pointed out in the previous paragraph, Eve also has full information about their secret measurement results based on the two qubits in Eve's possession.

In sections 8.1 to 8.4 we are going to show that this strategy is a generalization of the ZLG attack by describing the respective attack scenarios on the protocols for key distribution and secret sharing by Cabello [27, 26]. Further, we are going to present some other protocols which are also open to this attack and involve the simulation of operations at Alice's and Bob's side as they are described in the following sections.

7.2.2 Simulating Rotation Operations

Many quantum cryptographic protocols involve some operations to alter their initial states in a way only the legitimate parties are aware of. For example, in a protocol presented by Li et al. [91] Alice applies one of the four Pauli operations onto one

of her qubits to transmit more information to Bob (for details see section 8.1). As discussed in the previous section the correlations between Alice's and Bob's results are preserved by the state $|\delta\rangle$ even if the initial states are changed due to the application of a Pauli operation. Therefore, Pauli operations do not have any relevance regarding the security of the protocol.

To be more general we are looking at arbitrary rotation operations by an angle θ about the X-, Y- and Z-axis, respectively. These rotations have already been described in eq. (4.28) in section 4.2.2 above and are denoted as $R_x(\theta)$, $R_y(\theta)$ and $R_z(\theta)$. Using eq. (4.29) from above we directly see that the Pauli operations are special versions of these rotation operations for $\theta = \pi$. We are looking at first at the entanglement swapping between Alice and Bob without Eve's presence to show how the basic correlation changes. Afterwards we discuss Eve's application of $|\delta\rangle$ in detail.

The rotation operations $R_x(\theta)$, $R_y(\theta)$ and $R_z(\theta)$ change the state $|\Phi^+\rangle_{12}$ when applied onto qubit 1 (cf. (2) in figure 7.7) into

$$\begin{aligned} R_x\big(\theta\big)|\Phi^+\rangle_{12} &= \cos\frac{\theta}{2}|\Phi^+\rangle_{12} - i\sin\frac{\theta}{2}|\Psi^+\rangle_{12} \\ R_y\big(\theta\big)|\Phi^+\rangle_{12} &= \cos\frac{\theta}{2}|\Phi^+\rangle_{12} - \sin\frac{\theta}{2}|\Psi^-\rangle_{12} \\ R_z\big(\theta\big)|\Phi^+\rangle_{12} &= \cos\frac{\theta}{2}|\Phi^+\rangle_{12} - i\sin\frac{\theta}{2}|\Phi^-\rangle_{12} \end{aligned} \tag{7.35}$$

This can be understood as applying the $\mathbb{1}$ operation with probability $\cos^2\frac{\theta}{2}$ and applying the respective Pauli operation with probability $\sin^2\frac{\theta}{2}$. Assuming the rotation operations are applied only on Alice's side and Bob's state is $|\Phi^+\rangle_{34}$ the entanglement swapping between Alice and Bob changes into

$$\begin{aligned} R_x(\theta)|\Phi^+\rangle_{12}|\Phi^+\rangle_{34} = \frac{1}{2}\Bigg(& |\Phi^+\rangle_{13}\left[\cos\frac{\theta}{2}|\Phi^+\rangle_{24} - i\sin\frac{\theta}{2}|\Psi^+\rangle_{24}\right] \\ & +|\Phi^-\rangle_{13}\left[\cos\frac{\theta}{2}|\Phi^-\rangle_{24} - i\sin\frac{\theta}{2}|\Psi^-\rangle_{24}\right] \\ & +|\Psi^+\rangle_{13}\left[\cos\frac{\theta}{2}|\Psi^+\rangle_{24} - i\sin\frac{\theta}{2}|\Phi^+\rangle_{24}\right] \\ & +|\Psi^-\rangle_{13}\left[\cos\frac{\theta}{2}|\Psi^-\rangle_{24} - i\sin\frac{\theta}{2}|\Phi^-\rangle_{24}\right]\Bigg). \end{aligned} \tag{7.36}$$

if $R_x(\theta)$ is used. Similarly, if Alice applies the $R_y(\theta)$ operation the entanglement

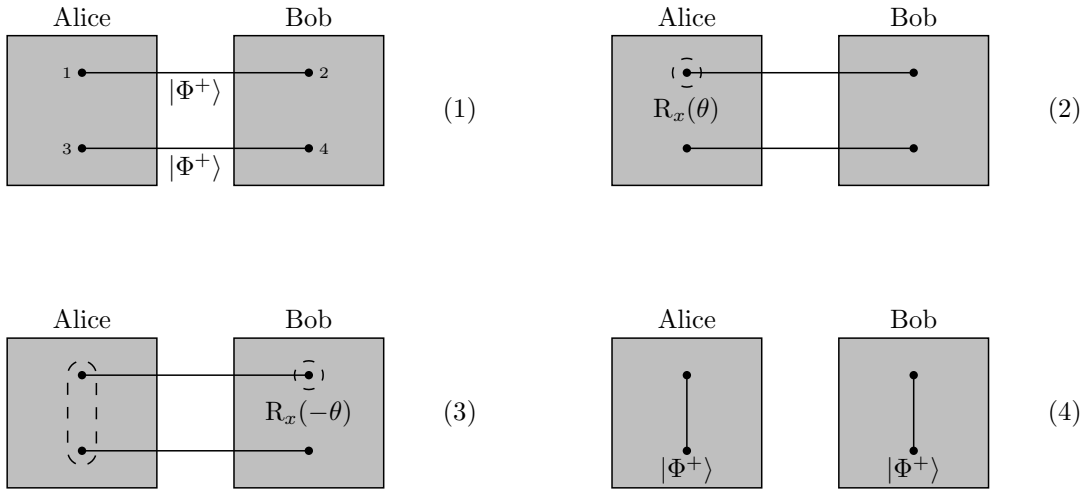

Figure 7.7: Illustration of a simple QKD protocol using a rotation by an angle θ about the X-axis.

swapping changes into

$$\begin{aligned} R_y(\theta)|\Phi^+\rangle_{12}|\Phi^+\rangle_{34} = \frac{1}{2}\Bigg(& |\Phi^+\rangle_{13}\left[\cos\frac{\theta}{2}|\Phi^+\rangle_{24} - \sin\frac{\theta}{2}|\Psi^-\rangle_{24}\right] \\ & +|\Phi^-\rangle_{13}\left[\cos\frac{\theta}{2}|\Phi^-\rangle_{24} - \sin\frac{\theta}{2}|\Psi^+\rangle_{24}\right] \\ & +|\Psi^+\rangle_{13}\left[\cos\frac{\theta}{2}|\Psi^+\rangle_{24} - \sin\frac{\theta}{2}|\Phi^-\rangle_{24}\right] \\ & +|\Psi^-\rangle_{13}\left[\cos\frac{\theta}{2}|\Psi^-\rangle_{24} - \sin\frac{\theta}{2}|\Phi^+\rangle_{24}\right]\Bigg). \end{aligned} \tag{7.37}$$

At last, using the rotation $R_z(\theta)$ about the Z axis the entanglement swapping changes into

$$\begin{aligned} R_z(\theta)|\Phi^+\rangle_{12}|\Phi^+\rangle_{34} = \frac{1}{2}\Bigg(& |\Phi^+\rangle_{13}\left[\cos\frac{\theta}{2}|\Phi^+\rangle_{24} - i\sin\frac{\theta}{2}|\Phi^-\rangle_{24}\right] \\ & +|\Phi^-\rangle_{13}\left[\cos\frac{\theta}{2}|\Phi^-\rangle_{24} - i\sin\frac{\theta}{2}|\Phi^+\rangle_{24}\right] \\ & +|\Psi^+\rangle_{13}\left[\cos\frac{\theta}{2}|\Psi^+\rangle_{24} - i\sin\frac{\theta}{2}|\Psi^-\rangle_{24}\right] \\ & +|\Psi^-\rangle_{13}\left[\cos\frac{\theta}{2}|\Psi^-\rangle_{24} - i\sin\frac{\theta}{2}|\Psi^+\rangle_{24}\right]\Bigg). \end{aligned} \tag{7.38}$$

We see that in all three cases Bob obtains a correlated result as it would be expected from table 2.1 only with probability $\cos^2\frac{\theta}{2}$. Otherwise, he obtains a result which differs from Alice's result by a σ_x, σ_y or σ_z operation, respectively, i.e Bob obtains

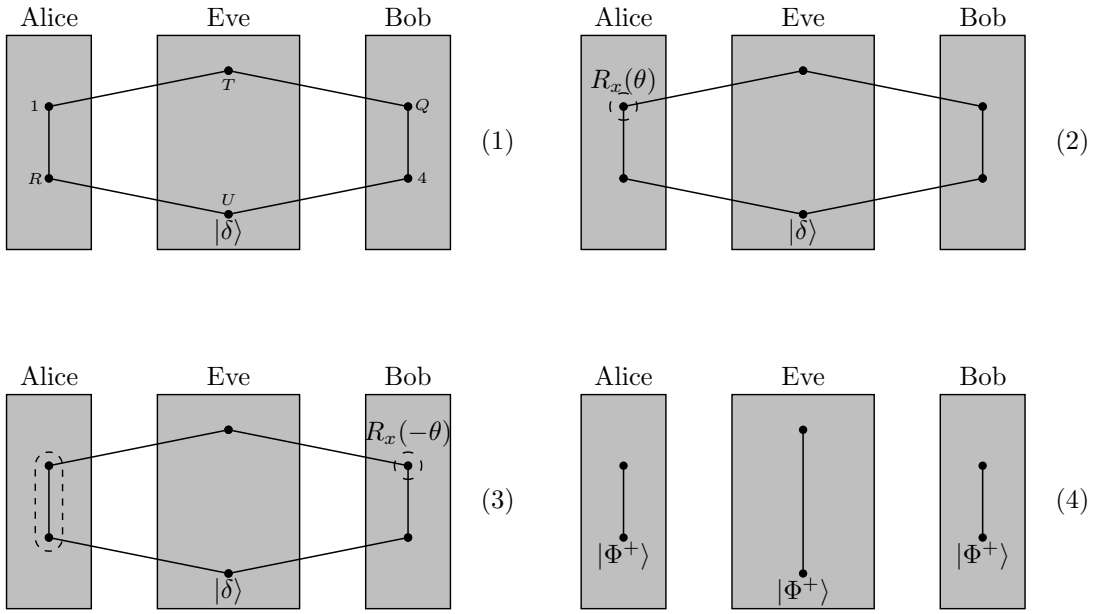

Figure 7.8: *(Simulating rotation operations)* Illustration of a successful application of the simulation attack on a simple QKD protocol using a rotation by an angle θ about the X-axis. Here, Eve already intercepted the qubits in transit and performed the entanglement swapping.

$|\Psi^+\rangle_{24}$ with probability $\sin^2\frac{\theta}{2}$ whenever Alice obtains $|\Phi^+\rangle_{13}$ after the rotation about the X-axis and so forth. That becomes a problem because Bob is no longer able to compute Alice's state based on his result and vice versa. Nevertheless, Bob can resolve this problem by rotating the state back into its original form. In the present scenario where Alice performs the rotation on qubit 1 he achieves that by applying the rotation operation $R_x(-\theta)$, $R_y(-\theta)$ or $R_z(-\theta)$, respectively, on qubit 2 of his state (cf. (3) in figure 7.7). This is a rotation by an angle $-\theta$ which leads to

$$\begin{aligned} R_x\big(-\theta\big)\left(\cos\frac{\theta}{2}|\Phi^+\rangle_{24} - i\sin\frac{\theta}{2}|\Psi^+\rangle_{24}\right) &= |\Phi^+\rangle_{24} \\ R_y\big(-\theta\big)\left(\cos\frac{\theta}{2}|\Phi^+\rangle_{24} - \sin\frac{\theta}{2}|\Psi^-\rangle_{24}\right) &= |\Phi^+\rangle_{24} \\ R_z\big(-\theta\big)\left(\cos\frac{\theta}{2}|\Phi^+\rangle_{24} - i\sin\frac{\theta}{2}|\Phi^-\rangle_{24}\right) &= |\Phi^+\rangle_{24} \end{aligned} \tag{7.39}$$

and re-establishes the perfect correlation between Alice's and Bob's measurement result in all three cases (cf. (4) in figure 7.7).

In the following paragraphs we discuss Eve's intervention in the entanglement swapping using the state $|\delta\rangle$. We will assume that Alice and Bob prepared the

initial states $|\Phi^+\rangle_{12}$ and $|\Phi^+\rangle_{34}$ as described above to make calculations easier since we already showed that different initial states do not change the effect of Eve's strategy. Further, we assume that Alice applies the $R_x(\theta)$ operation on qubit 1 (cf. (2) in figure 7.8). The calculations and argumentation for the other rotations $R_y(\theta)$ and $R_z(\theta)$ are carried out accordingly.

When performing the entanglement swapping between $|\delta\rangle_{P-U}$ and $R_x(\theta)|\Phi^+\rangle_{12}$ we realize that after Eve's corrections the qubits are in the state

$$\begin{aligned} R_x\big(\theta\big)|\delta\rangle_{1Q-U} = \frac{1}{2\sqrt{2}}\Bigg(&\cos\frac{\theta}{2}|000000\rangle - i\sin\frac{\theta}{2}|000110\rangle - i\sin\frac{\theta}{2}|001011\rangle \\ &+\cos\frac{\theta}{2}|001101\rangle - i\sin\frac{\theta}{2}|010001\rangle + \cos\frac{\theta}{2}|010111\rangle \\ &+\cos\frac{\theta}{2}|011010\rangle - i\sin\frac{\theta}{2}|011100\rangle - i\sin\frac{\theta}{2}|100000\rangle \\ &+\cos\frac{\theta}{2}|100110\rangle + \cos\frac{\theta}{2}|101011\rangle - i\sin\frac{\theta}{2}|101101\rangle \\ &+\cos\frac{\theta}{2}|110001\rangle - i\sin\frac{\theta}{2}|110111\rangle - i\sin\frac{\theta}{2}|111010\rangle \\ &+\cos\frac{\theta}{2}|111100\rangle\Bigg)_{1Q-U} \end{aligned} \tag{7.40}$$

Hence, also after the entanglement swapping between Eve's state $|\delta\rangle_{1Q-U}$ and Bob's state $|\Phi^+\rangle_{34}$ the resulting state is similar to the one in eq. (7.40) above with the only difference that qubit 4 is now part of the state (cf. eq. (7.34)). After a little algebra we get to the result that the state $R_x(\theta)|\delta\rangle_{1QR4TU}$ can be written as

$$\begin{aligned} R_x\big(\theta\big)|\delta\rangle = \frac{1}{2}\Bigg(&|\Phi^+\rangle_{1R}\left[\cos\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU} + i\sin\frac{\theta}{2}\,|\Psi^+\rangle_{Q4}|\Psi^+\rangle_{TU}\right] \\ &+|\Phi^-\rangle_{1R}\left[\cos\frac{\theta}{2}\,|\Phi^-\rangle_{Q4}|\Phi^-\rangle_{TU} - i\sin\frac{\theta}{2}\,|\Psi^-\rangle_{Q4}|\Psi^-\rangle_{TU}\right] \\ &+|\Psi^+\rangle_{1R}\left[\cos\frac{\theta}{2}\,|\Psi^+\rangle_{Q4}|\Psi^+\rangle_{TU} + i\sin\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU}\right] \\ &+|\Psi^-\rangle_{1R}\left[\cos\frac{\theta}{2}\,|\Psi^-\rangle_{Q4}|\Psi^-\rangle_{TU} - i\sin\frac{\theta}{2}\,|\Phi^-\rangle_{Q4}|\Phi^-\rangle_{TU}\right]\Bigg). \end{aligned} \tag{7.41}$$

Thus, if Alice performs a Bell state measurement on qubits 1 and R (cf. (3) in figure 7.8) she obtains each result with equal probability of 0.25 as expected. Furthermore, after the measurement qubits Q and 4 are either in the same state as Alice's result with probability $\cos^2\frac{\theta}{2}$ or in another state with probability $\sin^2\frac{\theta}{2}$. Comparing eq. (7.41) and eq. (7.36) we see that the state of qubits Q and 4 is very similar to the state of qubits 3 and 4. Nevertheless, if Bob performs the $R_x(-\theta)$ operation to

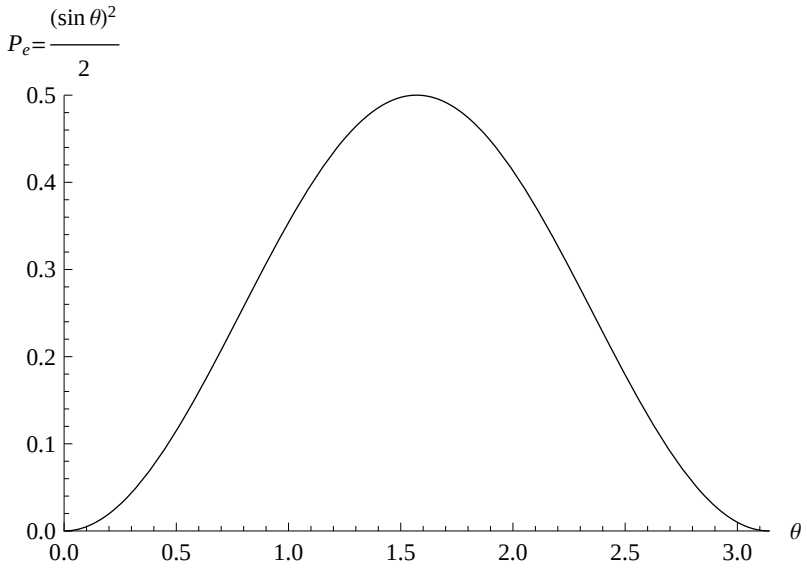

Figure 7.9: *(Error probability)* Eve's probability P_e to introduce an error depending on the angle θ.

rotate the state back into its original form (cf. (3) in figure 7.8) this brings qubits Q, 4, T and U into the state

$$\begin{aligned} R_x(-\theta)\left(\cos\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU} + i\sin\frac{\theta}{2}\,|\Psi^+\rangle_{Q4}|\Psi^+\rangle_{TU}\right) = \\ \cos^2\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU} + \sin^2\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Psi^+\rangle_{TU} \\ +\frac{i\sin\theta}{2}\,|\Psi^+\rangle_{Q4}|\Phi^+\rangle_{TU} - \frac{i\sin\theta}{2}\,|\Psi^+\rangle_{Q4}|\Psi^+\rangle_{TU} \end{aligned} \tag{7.42}$$

for Alice's result $|\Phi^+\rangle_{1R}$ and accordingly for the other results. Therefore, Bob obtains the correlated state $|\Phi^+\rangle_{Q4}$ only with probability $(3+\cos(2\theta))/4$ due to Eve's intervention. Accordingly, his measurement gives the result $|\Psi^+\rangle_{Q4}$ with probability $(\sin^2\theta)/2$. Figure 7.9 describes the error probability $P_e = (\sin^2\theta)/2$ and we can see that it is 0 for a full rotation by π, as expected, and maximal for an angle $\theta = \pi/2$. Hence, Alice and Bob will detect Eve's presence with a high probability when they choose $\theta = \pi/2$ and compare some of their measurement results as described in detail below.

Furthermore, Eve obtains the correlated result $|\Phi^+\rangle_{TU}$ with probability $(1+\cos(\theta))^2/(3+\cos(2\theta))$ from her measurement if Bob obtains $|\Phi^+\rangle_{Q4}$ and she obtains $|\Psi^+\rangle_{TU}$ otherwise. This is the collision probability P_c for Eve and it is – as we can see from figure 7.10 – larger than 0.9 for $\theta < \pi/3$ which is rather high. In contrary, if

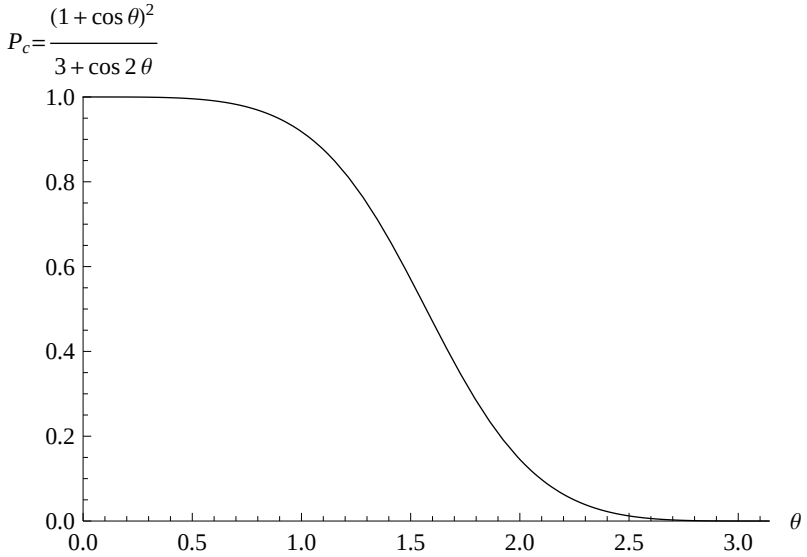

Figure 7.10: *(Collision probability)* Eve's probability P_c to obtain the same result as Bob depending on the angle θ.

Bob obtains the incorrect result $|\Psi^+\rangle_{Q4}$ Eve obtains $|\Phi^+\rangle_{TU}$ and $|\Psi^+\rangle_{TU}$ with equal probability of 1/2. This means, if Bob obtains a result correlated to Alice's outcome, Eve's information about Bob's measurement outcome is still based on the angle θ. Her information becomes larger the small the difference $|\pi - \theta|$ is. Therefore, also in this case the optimal choice for $\theta = \pi/2$. If Bob obtains the uncorrelated result, Eve has no information about Bob's measurement outcome.

When we look at the rotation about the Y- and the Z-axis we get very similar results. After Eve's Bell state measurements on qubits 2 and 3 coming from Alice and Bob, respectively, the overall state $R_y(\theta)|\delta\rangle_{1QR4TU}$ can be written as

$$\begin{aligned} R_y\big(\theta\big)|\delta\rangle = \frac{1}{2}\Bigg(& |\Phi^+\rangle_{1R}\left[\cos\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU} + \sin\frac{\theta}{2}\,|\Psi^-\rangle_{Q4}|\Psi^-\rangle_{TU}\right] \\ & +|\Phi^-\rangle_{1R}\left[\cos\frac{\theta}{2}\,|\Phi^-\rangle_{Q4}|\Phi^-\rangle_{TU} - \sin\frac{\theta}{2}\,|\Psi^+\rangle_{Q4}|\Psi^+\rangle_{TU}\right] \\ & +|\Psi^+\rangle_{1R}\left[\cos\frac{\theta}{2}\,|\Psi^+\rangle_{Q4}|\Psi^+\rangle_{TU} + \sin\frac{\theta}{2}\,|\Phi^-\rangle_{Q4}|\Phi^-\rangle_{TU}\right] \\ & +|\Psi^-\rangle_{1R}\left[\cos\frac{\theta}{2}\,|\Psi^-\rangle_{Q4}|\Psi^-\rangle_{TU} - \sin\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU}\right]\Bigg). \end{aligned} \tag{7.43}$$

If Alice applies the $R_z(\theta)$ operation on qubit 1, the overall state $R_z(\theta)|\delta\rangle_{1QR4TU}$ can

then be written as

$$\begin{aligned} R_z(\theta)|\delta\rangle = \frac{1}{2}\Big(& |\Phi^+\rangle_{1R}\left[\cos\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU} - i\sin\frac{\theta}{2}\,|\Phi^-\rangle_{Q4}|\Phi^-\rangle_{TU}\right] \\ & +|\Phi^-\rangle_{1R}\left[\cos\frac{\theta}{2}\,|\Phi^-\rangle_{Q4}|\Phi^-\rangle_{TU} - i\sin\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU}\right] \\ & +|\Psi^+\rangle_{1R}\left[\cos\frac{\theta}{2}\,|\Psi^+\rangle_{Q4}|\Psi^+\rangle_{TU} - i\sin\frac{\theta}{2}\,|\Psi^-\rangle_{Q4}|\Psi^-\rangle_{TU}\right] \\ & +|\Psi^-\rangle_{1R}\left[\cos\frac{\theta}{2}\,|\Psi^-\rangle_{Q4}|\Psi^-\rangle_{TU} - i\sin\frac{\theta}{2}\,|\Psi^+\rangle_{Q4}|\Psi^+\rangle_{TU}\right]\Big). \end{aligned} \tag{7.44}$$

Bob's application of the reverse rotation operation on qubit 4 in his possession changes the state of qubits Q, 4, T and U similar to eq. (7.42) above into either

$$\begin{aligned} R_y(-\theta)\left(\cos\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU} + \sin\frac{\theta}{2}\,|\Psi^-\rangle_{Q4}|\Psi^-\rangle_{TU}\right) = \\ \cos^2\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU} + \sin^2\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Psi^-\rangle_{TU} \\ -\frac{\sin\theta}{2}\,|\Psi^-\rangle_{Q4}|\Phi^+\rangle_{TU} + \frac{\sin\theta}{2}\,|\Psi^-\rangle_{Q4}|\Psi^-\rangle_{TU} \end{aligned} \tag{7.45}$$

for the application of $R_y(-\theta)$ and into

$$\begin{aligned} R_z(-\theta)\left(\cos\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU} + i\sin\frac{\theta}{2}\,|\Phi^-\rangle_{Q4}|\Phi^-\rangle_{TU}\right) = \\ \cos^2\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU} + \sin^2\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Phi^-\rangle_{TU} \\ +\frac{\sin\theta}{2}\,|\Phi^-\rangle_{Q4}|\Phi^+\rangle_{TU} - \frac{\sin\theta}{2}\,|\Phi^-\rangle_{Q4}|\Phi^-\rangle_{TU}. \end{aligned} \tag{7.46}$$

for the application of $R_z(-\theta)$, respectively. Therefore, Bob again obtains the correlated state $|\Phi^+\rangle_{Q4}$ also in these two cases only with probability $(3+\cos(2\theta))/4$ and with probability $(\sin^2\theta)/2$ the correlation is violated.

The main goal for Alice and Bob is to maximize Eve's probability to introduce an error and to minimize her information about their measurement results. As we have already seen in the previous section a rotation by an angle $\theta = \pi$ such that $R_x(\pi) = \sigma_x$, $R_y(\pi) = \sigma_y$ and $R_z(\pi) = \sigma_z$ leaves the protocol completely insecure. Looking at the plot of $(\sin^2\theta)/2$ in figure 7.9 we see that the error P_e is maximal if $\theta = \pi/2$. Hence, a rotation by $\pi/2$ leads to the states

$$\begin{aligned} R_x\big(\frac{\pi}{2}\big)|\Phi^+\rangle_{12} &= \frac{1}{\sqrt{2}}\big(|\Phi^+\rangle_{12} - i|\Psi^+\rangle_{12}\big) \\ R_y\big(\frac{\pi}{2}\big)|\Phi^+\rangle_{12} &= \frac{1}{\sqrt{2}}\big(|\Phi^+\rangle_{12} - |\Psi^-\rangle_{12}\big) \\ R_z\big(\frac{\pi}{2}\big)|\Phi^+\rangle_{12} &= \frac{1}{\sqrt{2}}\big(|\Phi^+\rangle_{12} - i|\Phi^-\rangle_{12}\big). \end{aligned} \tag{7.47}$$

In this case the probability P_e that Alice and Bob obtain uncorrelated results from their measurements is 0.5 (cf. figure 7.9). Additionally, Eve's probability to obtain the same result as Bob, i.e. the collision probability P_c, is also brought to 0.5 (cf. figure 7.10). Therefore, $\theta = \pi/2$ is the optimal choice for the angle of the rotation about any of the three axis in terms of the error Eve introduces into the protocol and the information she has about Alice's and Bob's measurement results.

We have to stress that a combined rotation $R_x(\theta)$ by Alice and Bob leaves the protocol again insecure against Eve performing the simulation attack strategy. If both Alice and Bob apply a rotation about the same axis and by the same angle on qubits 1 and 4, respectively, these operations neutralize each other during the entanglement swapping. The initial states $R_x^{(1)}(\theta)|\Phi^+\rangle_{12}$ and $R_x^{(4)}(\theta)|\Phi^+\rangle_{34}$ change after Eve's entanglement swapping into $R_x^{(1)}(\theta)R_x^{(4)}(\theta)|\delta\rangle_{1QR4TU}$ similar to eq. 7.40 above. Here, the superscript (α) denotes that the operation is applied on the qubit α. After receiving qubits Q and R Alice and Bob apply the operation $R_x(-\theta)$ on the received qubits which alters the overall state into

$$R_x^{(1)}\big(\theta\big)R_x^{(Q)}\big(-\theta\big)R_x^{(R)}\big(-\theta\big)R_x^{(4)}\big(\theta\big)|\delta\rangle_{1QR4TU} \tag{7.48}$$

Alice's measurement on qubits 1 and R swaps the rotation operations onto qubits Q and 4 neutralizing the effect of the previously applied operations. Hence, the correlations given by the state $|\delta\rangle$ are re-established such that Bob obtains a perfectly correlated result. Additionally, the qubits $T$and U are in the same state as Bob's qubits Q and 4 which gives Eve full information. This scenario works accordingly for rotations about the Y- and Z-axis. Therefore, this scenario has to be avoided by the legitimate parties.

As we have seen in the previous paragraphs Eve has no chance to stay undetected while using the state $|\delta\rangle$ if either Alice or Bob performs a bilateral rotation by some angle θ on one of their initial states around the X-, Y-, or Z-axis as long as $\theta \neq \pi$. Nevertheless, Eve is able to simulate the rotation on her state $|\delta\rangle$ to anticipate Alice's and Bob's actions. Therefore, she applies $R_x(-\theta)$ on qubit P and $R_x(\theta)$ on qubit S before she entangles herself with Alice and Bob. This changes Eve's initial state into

$$|\delta_x\rangle_{P-U} = R_x^{(P)}(-\theta)R_x^{(S)}(\theta)|\delta\rangle_{P-U}. \tag{7.49}$$

After Eve's Bell state measurement and her correction operations the overall state is still $|\delta_x\rangle_{1QR4TU}$. When Alice applies her rotation $R_x(\theta)$ on qubit 1 the state changes

to

$$\begin{aligned} R_x^{(1)}(\theta)|\delta_x\rangle_{1QR4TU} &= R_x^{(1)}(\theta)R_x^{(1)}(-\theta)R_x^{(4)}(\theta)|\delta\rangle_{1QR4TU} \\ &= R_x^{(4)}(\theta)|\delta\rangle_{1QR4TU} \end{aligned} \tag{7.50}$$

which means that Alice's rotation inverts Eve's initial rotation on qubit P. The same happens when Bob applies $R_x(-\theta)$ on qubit 4 and the qubits Q, 4, T, U end up in the combined state $|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU}$. Hence, Alice and Bob always obtain correlated results and Eve has full information about their secret results.

Eve is able to simulate also the rotation $R_y(\theta)$ about the Y-axis and $R_z(\theta)$ about the Z-axis in the same way as long as she knows the exact angle θ. Therefore, there remain two options for Alice and Bob to detect Eve's intervention: first, they can secretly agree upon the angle θ before the protocol starts and then alter one of the initial states in every round of the protocol. To do so they have to share this information beforehand in some way using a preshared secret. This is not a very good attempt since it depends on the fact that Alice and Bob have to meet some time in the past to agree on θ. Furthermore, if Eve somehow manages to spy out θ the whole communication becomes insecure without Alice and Bob noticing it. A better option for them is to publicly agree on some θ and some direction (X, Y or Z) of the rotation and then to choose randomly between applying the predefined rotation and doing nothing.

As we have seen in the previous paragraphs Eve is able to prepare a state for each of these events individually to obtain full information about Alice's and Bob's secret results without being detected. Nevertheless, she is not able to find a state which achieves that for a random combination of the two events as we will show in detail in the applications of the simulation attack starting with section 8.1. Therefore, the best strategy for Eve is also to randomly choose between the preparation of $|\delta\rangle$ and $|\delta_x\rangle$. Half of the time Eve obtains full information, i.e. when Eve chooses $|\delta\rangle$ and Alice does not use the rotation operation and when Eve chooses $|\delta_x\rangle$ and Alice does use the rotation operation. The remaining time Eve introduces an error $P_e = (\sin^2\theta)/2$ as described above. This leads to the expected error rate

$$\langle P_e \rangle = \frac{1}{4}\left(0 + \frac{\sin^2\theta}{2} + \frac{\sin^2\theta}{2} + 0\right) = \frac{\sin^2\theta}{4} \tag{7.51}$$

for the entire protocol. As already pointed out this term reaches its maximum of $1/4$ for $\theta = \pi/2$. Looking at the collision probability P_c, i.e. the probability that Eve obtains the same result as Bob, we have also perfect correlation between Eve's

and Bob's result whenever she prepares $|\delta\rangle$ and Alice does nothing or Eve prepares $|\delta_x\rangle$ and Alice applies $R_x(\theta)$. Otherwise, $P_c = (1+\cos(\theta))^2/(3+\cos(2\theta))$ which leads to the expected collision probability

$$\langle P_c \rangle = \frac{1}{4}\left(0 + \frac{(1+\cos(\theta))^2}{3+\cos(2\theta)} + \frac{(1+\cos(\theta))^2}{3+\cos(2\theta)} + 0\right) = \frac{(1+\cos(\theta))^2}{2(3+\cos(2\theta)} \tag{7.52}$$

for the entire protocol. Again, $\langle P_c \rangle$ reaches its maximum of 1/4 for $\theta = \pi/2$.

7.2.3 Simulating Basis Transformations

Another option for Alice and Bob to alter their initial states is to transform them into another basis. The most intuitive choice for an alternative basis is the X-basis with the states $\{|x+\rangle, |x-\rangle\}$. The transformation into this basis is done by the Hadamard operation H as already described in section 7.1.1 above and the transformation is simply described as

$$H|0\rangle = |x+\rangle \quad H|1\rangle = |x-\rangle. \tag{7.53}$$

The Hadamard operation applied on the first qubit of the Bell states $|\Phi^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$ has the effect to change them into the states $|\omega^{\pm}\rangle$ and $|\chi^{\pm}\rangle$, respectively (cf. eq. (7.4)). As in the application of rotation operations described above Alice applies the H operation onto the first qubit of her Bell state and performs the entanglement swapping. Assuming again that Alice and Bob prepare the states $|\Phi^+\rangle_{12}$ and $|\Phi^+\rangle_{34}$ the application of the H operator changes the process of entanglement swapping into

$$\begin{aligned} |\omega^+\rangle_{12}|\Phi^+\rangle_{34} = \frac{1}{2}\big(&|\Phi^+\rangle_{13}|\omega^+\rangle_{24} + |\Phi^-\rangle_{13}|\omega^-\rangle_{24} \\ &+|\Psi^+\rangle_{13}|\chi^+\rangle_{24} + |\Phi^-\rangle_{13}|\chi^-\rangle_{24}\big). \end{aligned} \tag{7.54}$$

To obtain the correct result Bob also has to apply a H operation onto qubit 2 to reverse the effect of Alice's operation. It is also possible to apply the H operation onto qubit 4 but in this case $|\omega^-\rangle_{24}$ is transformed to $|\Psi^+\rangle_{24}$ instead of $|\Phi^-\rangle_{24}$ and $|\chi^+\rangle_{24}$ is transformed into $|\Phi^-\rangle_{24}$. Bob has to be aware of that to alter his table of correlations accordingly.

In general, a transformation T from the Z-basis into the X- or Y-basis can be described as a rotation about the X- or Y-axis, respectively, by some angle θ, i.e.

$$T_x\big(\theta\big) = e^{i\phi} R_z\big(\phi\big) R_x\big(\theta\big) R_z\big(\phi\big) = \begin{pmatrix} \cos\frac{\theta}{2} & -ie^{i\phi}\sin\frac{\theta}{2} \\ -ie^{i\phi}\sin\frac{\theta}{2} & e^{2i\phi}\cos\frac{\theta}{2} \end{pmatrix} \tag{7.55}$$

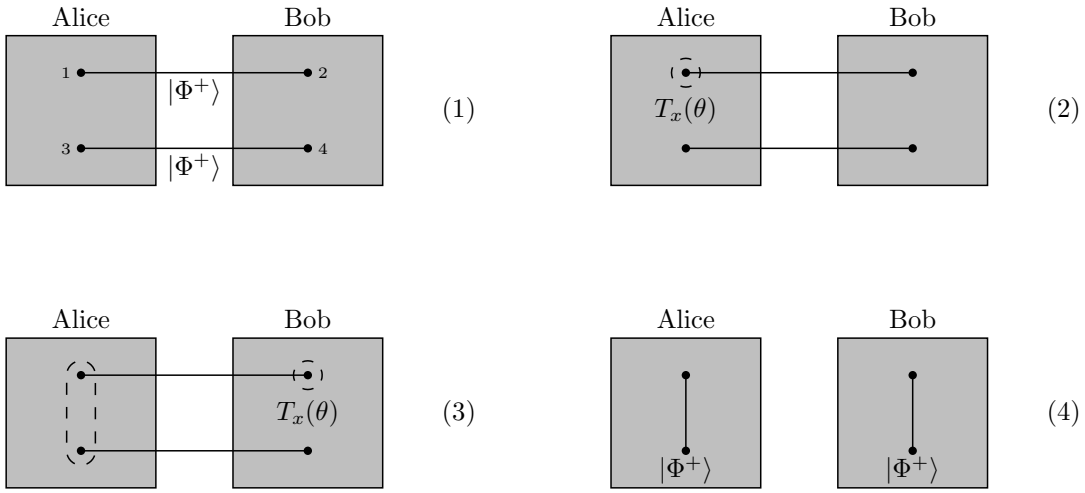

Figure 7.11: Illustration of a simple QKD protocol using a basis transformation from the Z- into the X-basis by an angle θ.

and

$$T_y(\theta) = e^{i\phi} R_z(\phi) R_y(\theta) R_z(\phi) = \begin{pmatrix} \cos\frac{\theta}{2} & -e^{i\phi}\sin\frac{\theta}{2} \\ -e^{i\phi}\sin\frac{\theta}{2} & e^{2i\phi}\cos\frac{\theta}{2} \end{pmatrix}. \tag{7.56}$$

The general transformations from the X-basis into the Z- or Y-basis as well as from the Y-basis into the X- or Z-basis are defined accordingly. For our further discussions we will limit ourselves to transformations from the Z- into the X- or Y-basis and choose $\phi = \pi/2$ since we only want to rotate the state according to the axes. This gives the matrix representation for $T_x(\theta)$ and $T_y(\theta)$ as

$$T_x(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & \sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & -\cos\frac{\theta}{2} \end{pmatrix} \quad T_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ i\sin\frac{\theta}{2} & -\cos\frac{\theta}{2} \end{pmatrix}. \tag{7.57}$$

From the equation above we immediately see that the Hadamard operation H is just the special case where $\theta = \pi/2$, which is, as we will see later on, the optimal choice for θ. Under the application of the basis transformations $T_x(\theta)$ and $T_y(\theta)$ onto qubit 1 the Bell state $|\Phi^+\rangle$ changes it into (cf. (2) in figure 7.11)

$$\begin{aligned} T_x(\theta)|\Phi^+\rangle_{12} &= \cos\frac{\theta}{2}|\Phi^-\rangle_{12} - \sin\frac{\theta}{2}|\Psi^+\rangle_{12} \\ T_y(\theta)|\Phi^+\rangle_{12} &= \cos\frac{\theta}{2}|\Phi^-\rangle_{12} - i\sin\frac{\theta}{2}|\Psi^-\rangle_{12} \end{aligned} \tag{7.58}$$

and accordingly for the other Bell states. As a consequence, the application of T_x or T_y in the entanglement swapping changes the results according to the angle θ, as

we have already seen above. In detail, we have

$$\begin{aligned} T_x(\theta)|\Phi^+\rangle_{12}|\Phi^+\rangle_{34} = \frac{1}{2}\Bigg(& |\Phi^+\rangle_{13}\left[\cos\frac{\theta}{2}|\Phi^-\rangle_{24} + \sin\frac{\theta}{2}|\Psi^+\rangle_{24}\right] \\ & +|\Phi^-\rangle_{13}\left[\cos\frac{\theta}{2}|\Phi^+\rangle_{24} - \sin\frac{\theta}{2}|\Psi^-\rangle_{24}\right] \\ & +|\Psi^+\rangle_{13}\left[\cos\frac{\theta}{2}|\Psi^-\rangle_{24} + \sin\frac{\theta}{2}|\Phi^+\rangle_{24}\right] \\ & +|\Psi^-\rangle_{13}\left[\cos\frac{\theta}{2}|\Psi^+\rangle_{24} - \sin\frac{\theta}{2}|\Phi^-\rangle_{24}\right]\Bigg) \end{aligned} \tag{7.59}$$

for a transformation into the X-basis and similarly for a transformation into the Y-basis

$$\begin{aligned} T_y(\theta)|\Phi^+\rangle_{12}|\Phi^+\rangle_{34} = \frac{1}{2}\Bigg(& |\Phi^+\rangle_{13}\left[\cos\frac{\theta}{2}|\Phi^-\rangle_{24} + i\sin\frac{\theta}{2}|\Psi^-\rangle_{24}\right] \\ & +|\Phi^-\rangle_{13}\left[\cos\frac{\theta}{2}|\Phi^+\rangle_{24} - i\sin\frac{\theta}{2}|\Psi^+\rangle_{24}\right] \\ & +|\Psi^+\rangle_{13}\left[\cos\frac{\theta}{2}|\Psi^-\rangle_{24} + i\sin\frac{\theta}{2}|\Phi^-\rangle_{24}\right] \\ & +|\Psi^-\rangle_{13}\left[\cos\frac{\theta}{2}|\Psi^+\rangle_{24} - i\sin\frac{\theta}{2}|\Phi^+\rangle_{24}\right]\Bigg) \end{aligned} \tag{7.60}$$

Comparing eq. (7.59) and eq. (7.60) with the application of $R_x(\theta)$ and $R_y(\theta)$ in eq. (7.36) and eq. (7.37) from above we see that for the basis transformation Bob never obtains a correlated result but $|\Phi^-\rangle_{24}$ with probability $\cos^2\frac{\theta}{2}$ for Alice's result $|\Phi^+\rangle_{13}$ and $|\Psi^+\rangle_{24}$ or $|\Psi^-\rangle_{24}$, otherwise, depending on the transformation $T_x(\theta)$ or $T_y(\theta)$. Therefore, Bob has to compensate the basis transformation by Alice and applies a T_x or T_y operation, respectively, by himself on the corresponding qubit in his possession. Contrary to eq. (7.39) where the reversion of rotation operations is described Bob has to choose in this case θ for his operation to transform the state of his qubits back into the desired Bell state, i.e. (cf. (3) in figure 7.11)

$$\begin{aligned} T_x(\theta)\left[\cos\frac{\theta}{2}|\Phi^-\rangle_{24} - \sin\frac{\theta}{2}|\Psi^+\rangle_{24}\right] &= |\Phi^+\rangle_{24} \\ T_y(\theta)\left[\cos\frac{\theta}{2}|\Phi^-\rangle_{24} - i\sin\frac{\theta}{2}|\Psi^-\rangle_{24}\right] &= |\Phi^+\rangle_{24}. \end{aligned} \tag{7.61}$$

Next, we are going to look at Eve's intervention using the state $|\delta\rangle$. Also in this case the application of Alice's operation alters the outcomes of the entanglement swapping similar to the scenario with the general rotation operations above. Assuming Alice uses the $T_x(\theta)$ operation to transform her state into the X-basis

this alters the state of the 6 qubits 1, Q, R, 4, T and U after Eve's entanglement swapping with Bob's qubit 3

$$\begin{aligned} T_x\big(\theta\big)|\delta\rangle_{1Q-U} = \frac{1}{2\sqrt{2}}\Big(&\cos\frac{\theta}{2}|000000\rangle + \sin\frac{\theta}{2}|000110\rangle + \sin\frac{\theta}{2}|001011\rangle \\ &+\cos\frac{\theta}{2}|001101\rangle + \sin\frac{\theta}{2}|010001\rangle + \cos\frac{\theta}{2}|010111\rangle \\ &+\cos\frac{\theta}{2}|011010\rangle + \sin\frac{\theta}{2}|011100\rangle + \sin\frac{\theta}{2}|100000\rangle \\ &-\cos\frac{\theta}{2}|100110\rangle - \cos\frac{\theta}{2}|101011\rangle + \sin\frac{\theta}{2}|101101\rangle \\ &-\cos\frac{\theta}{2}|110001\rangle + \sin\frac{\theta}{2}|110111\rangle + \sin\frac{\theta}{2}|111010\rangle \\ &-\cos\frac{\theta}{2}|111100\rangle\Big)_{1QR4TU} \end{aligned} \tag{7.62}$$

This state can be rewritten in the Bell basis as

$$\begin{aligned} T_x\big(\theta\big)|\delta\rangle = \frac{1}{2}\Big(&|\Phi^+\rangle_{1R}\Big[\cos\frac{\theta}{2}\,|\Phi^-\rangle_{Q4}|\Phi^-\rangle_{TU} + \sin\frac{\theta}{2}\,|\Psi^+\rangle_{Q4}|\Psi^+\rangle_{TU}\Big] \\ &+|\Phi^-\rangle_{1R}\Big[\cos\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU} - \sin\frac{\theta}{2}\,|\Psi^-\rangle_{Q4}|\Psi^-\rangle_{TU}\Big] \\ &+|\Psi^+\rangle_{1R}\Big[\cos\frac{\theta}{2}\,|\Psi^+\rangle_{Q4}|\Psi^-\rangle_{TU} + \sin\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU}\Big] \\ &+|\Psi^-\rangle_{1R}\Big[\cos\frac{\theta}{2}\,|\Psi^-\rangle_{Q4}|\Psi^+\rangle_{TU} - \sin\frac{\theta}{2}\,|\Phi^-\rangle_{Q4}|\Phi^-\rangle_{TU}\Big]\Big). \end{aligned} \tag{7.63}$$

Looking at eq. (7.41) we see that the state looks very similar to the equation above involving $T_x(\theta)$ which leads to the assumption that also in this case Bob's transformation back into the Z-basis does not re-establish the correlations between Alice and Bob properly. Performing the calculations we see that Bob's operation $T_x(\theta)$ brings qubits Q, 4, T and U into the form

$$\begin{aligned} T_x\big(\theta\big)\Big(\cos\frac{\theta}{2}\,|\Phi^-\rangle_{Q4}|\Phi^-\rangle_{TU} + \sin\frac{\theta}{2}\,|\Psi^+\rangle_{Q4}|\Psi^+\rangle_{TU}\Big) = \\ \cos^2\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Phi^-\rangle_{TU} + \sin^2\frac{\theta}{2}\,|\Phi^+\rangle_{Q4}|\Psi^+\rangle_{TU} \\ -\frac{\sin\theta}{2}\,|\Psi^-\rangle_{Q4}|\Phi^-\rangle_{TU} + \frac{\sin\theta}{2}\,|\Psi^-\rangle_{Q4}|\Psi^+\rangle_{TU} \end{aligned} \tag{7.64}$$

provided that Alice obtains $|\Phi^+\rangle_{1R}$. For Alice's other three possible results the state changes accordingly. From eq. (7.64) we see that Bob obtains either the correlated result $|\Phi^+\rangle_{Q4}$ with probability $(3+\cos(2\theta))/4$ or $|\Psi^-\rangle_{Q4}$, otherwise. This is the

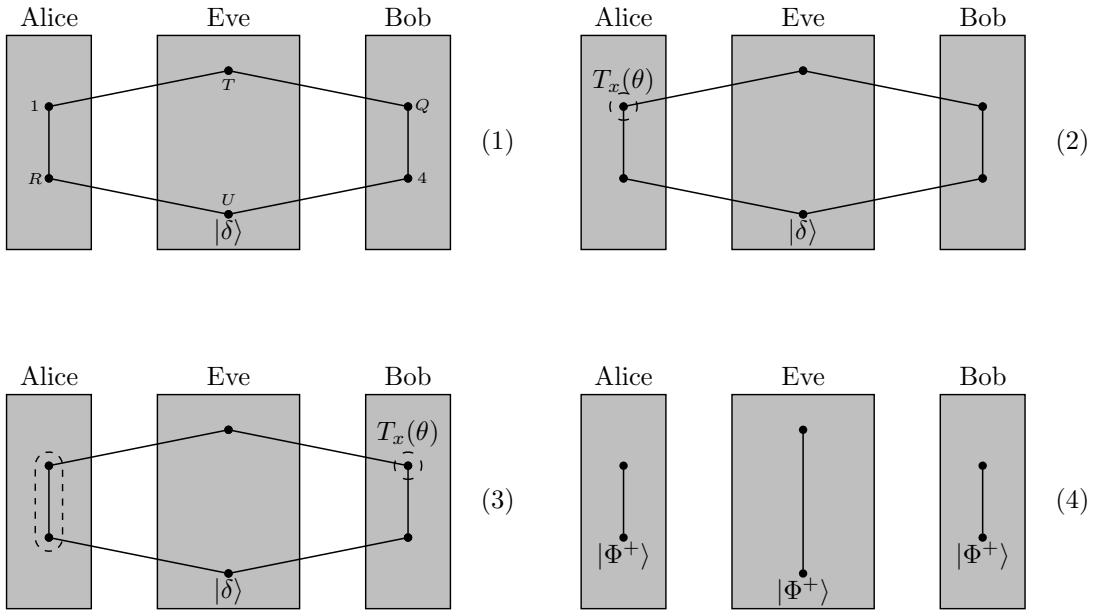

Figure 7.12: *(Simulating transformation operations)* Illustration of a successful application of the simulation attack on a simple QKD protocol using a basis transformation from the Z- into the X-basis by an angle θ. Here, Eve already intercepted the qubits in transit and performed the entanglement swapping.

same probability as above when Alice and Bob used simple rotation operations and thus Eve introduces an error with probability $P_e = (\sin^2\theta)/2$. The only difference is that Eve no longer obtains the same result as Bob but either $|\Phi^-\rangle_{TU}$ or $|\Psi^+\rangle_{TU}$. Nevertheless, the results are at least correlated as long as Bob obtains the correct result from his measurement. In this case Eve obtains $|\Phi^-\rangle_{TU}$ with probability $P_c = (1+\cos(\theta))^2/(3+\cos(2\theta))$ and knows that Bob obtained $|\Phi^+\rangle_{Q4}$. Whenever Eve obtains $|\Psi^+\rangle_{TU}$ she has no information about Bob's state. Looking at figure 7.9 and the argumentation in the previous section we see that the optimal angle for a basis transformation is also $\pi/2$ since in this case both P_e and P_c become $1/2$.

From the previous section we already know that a bilateral application of the same rotation operation gives Eve again full information about Alice's and Bob's measurement results. Accordingly, also a bilateral transformation in the same basis by Alice and Bob gives Eve again full information about their measurement results. Similar to the argumentation above the initial states $T_x^{(1)}(\theta)|\Phi^+\rangle_{12}$ and $T_x^{(4)}(\theta)|\Phi^+\rangle_{34}$ are brought into the state $T_x^{(1)}(\theta)T_x^{(4)}(\theta)|\delta\rangle_{1QR4TU}$ after Eve's entanglement swapping. Alice's and Bob's application of $T_x^{(1)}(\theta)$ onto qubits Q and R, respectively,

leaves the 6 qubits in the overall state

$$T_x^{(1)}\big(\theta\big)T_x^{(Q)}\big(\theta\big)T_x^{(R)}\big(\theta\big)T_x^{(4)}\big(\theta\big)|\delta\rangle_{1QR4TU} \tag{7.65}$$

Alice's Bells state measurement on qubits 1 and R swaps the basis transformations onto Bob's qubits Q and 4 and neutralizes the effect of the previously applied operations. Thus, Bob measurement results are perfectly correlated to Alice's results as well as to the state of Eve's qubits. Therefore, also in relation with basis transformations a bilateral application of the same transformation has to be avoided.

From our argumentation we understand that also in this case Eve in not able to stay undetected when she uses the state $|\delta\rangle$ to eavesdrop the protocol. This is also the intuitive assumption taking into account that the basis transformation can be described by a series of rotation operations as pointed out above. Nevertheless, we showed above that Eve is able to simulate rotation operations on the state $|\delta\rangle$ as long as they are performed deterministically and the angle θ is known. Therefore, Eve is also able to simulate the basis transformations $T_x(\theta)$ and $T_y(\theta)$ on $|\delta\rangle$. She has to apply $T_x(\theta)$ onto qubit P and $T_x(\theta)$ onto qubit Q which alters the initial state to

$$|\delta_x\rangle_{P-U} = T_x^{(P)}(\theta)T_x^{(Q)}(\theta)|\delta\rangle_{P-U} \tag{7.66}$$

After Eve entangled herself with Alice and Bob using entanglement swapping the overall state is $|\delta_x\rangle_{1RQ4TU}$ due to Eve's corrections. Hence, Alice's application of $T_x(\theta)$ reverses Eve's operation on qubit 1, i.e.

$$\begin{aligned} T_x^{(1)}(\theta)|\delta_x\rangle_{1QR4TU} &= T_x^{(1)}(\theta)T_x^{(1)}(\theta)T_x^{(Q)}(\theta)|\delta\rangle_{1QR4TU} \\ &= T_x^{(Q)}(\theta)|\delta\rangle_{1QR4TU} \end{aligned} \tag{7.67}$$

Similarly, Bob's application of $T_x(\theta)$ on qubit Q (which impersonates qubit 2 originally coming from Alice) reverses the effect of Eve's second operation and thus the original correlation between Alice's and Bob's results is re-established. Further, Eve has full information about Alice's and Bob's result due to the remaining two qubits in her possession.

When dealing with the rotation operations we defined two possible solutions for Alice and Bob which are of course also applicable here. The first one is to keep the angle θ of the transformation secret between Alice and Bob such that Eve can not revert its effect. The major drawback to this method is that Eve will be able to obtain full information about the secret should she somehow be able to get to know

θ. Further, Alice and Bob have to secretly distribute the angle θ between them which poses another problem. Therefore, a better solution is for Alice to randomly choose between the application of $T_x(\theta)$ and $\mathbb{1}$ before she performs her Bells state measurement. She publicly announces her choice after all the qubits are exchanged and Bob can correct the transformation where necessary. In this case Eve is not able to prepare a state that simulates the application of $\mathbb{1}$ and $T_x(\theta)$ at the same time such that she introduces a certain error rate and thus can be detected.

7.2.4 Simulating Unitary Operations

In the previous sections we focused on how Eve is able to simulate rotation operations and basis transformations with the help of $|\delta\rangle$. These two classes of operations are the most commonly used methods to secure quantum cryptographic protocols as we will see in the following sections. We also pointed out that basis transformations can be expressed by rotation operations which is intuitively understandable when looking at the Bloch sphere as a representation for quantum states. Moreover, every unitary operation U can be represented using the basis rotation about the X-, Y- and Z-axis. In detail, for an arbitrary unitary operation U there exist real numbers α, β, γ and δ such that

$$U = e^{i\alpha} R_z\big(\beta\big) \mathrm{R}_y\big(\gamma\big) \mathrm{R}_z\big(\delta\big). \tag{7.68}$$

This is called the $Z-Y$ decomposition and is described, for example, in [109], where also a proof is given. Briefly, due to the fact that U is unitary the rows and columns are orthonormal. Therefore, U can be written as

$$U = \begin{pmatrix} e^{i(\alpha-\beta/2-\delta/2)} \cos\frac{\gamma}{2} & -e^{i(\alpha-\beta/2+\delta/2)} \sin\frac{\gamma}{2} \\ e^{i(\alpha+\beta/2-\delta/2)} \sin\frac{\gamma}{2} & e^{i(\alpha+\beta/2+\delta/2)} \cos\frac{\gamma}{2} \end{pmatrix} \tag{7.69}$$

Using this representation we get, for example, the Hadamard operation for $\alpha = \beta = \gamma = \delta = \pi/2$. In general we can say that, based on the argumentation in the previous two sections Eve is able to simulate the deterministic application of an arbitrary unitary operation U using $|\delta\rangle$. Therefore, she just applies U on the respective qubits when preparing $|\delta\rangle$ such that the respective application of U at Alice's or Bob's side is neutralized. The correlation between Alice's and Bob's measurement results is then preserved by $|\delta\rangle$.

Nevertheless, a random application of a unitary U can only be compensated in special cases, as we have seen for Pauli operations. In general Eve is not able to

prepare a state that preserves the correlation between the legitimate parties although one of them makes a random choice between $\mathbb{1}$ and an arbitrary unitary operation U.

7.3 Security Arguments for Multi-Qubit Protocols

In the previous section we presented an attack strategy allowing an adversary Eve to perfectly simulate the correlations of an entanglement swapping based protocol. Hence, on the one hand Eve is able to stay undetected when Alice and Bob check their correlations to detect the presence of an eavesdropper. On the other hand she is able to obtain full information about the key shared by Alice and Bob. In sections 7.2.2, 7.2.3 and 7.2.4 we showed that the attack strategy also allows Eve simulate a rotation of an arbitrary angle θ – not necessarily known to Eve – as long as it is performed deterministically by Alice and Bob.

From these facts we can directly identify a basic strategy to secure a protocol against the simulation attack: Alice and Bob agree on some rotation or basis transformation $U(\theta)$ about some angle θ and Alice applies it on one or both of her qubits at random. After all qubits are exchanged between Alice and Bob, Alice performs the entanglement swapping and she announces whether she applied the operation U or not. Accordingly, Bob uses U^{-1} to undo Alice's rotation or transformation and performs his Bell state measurement afterwards. As pointed out above, Eve is not able to perfectly compensate a random application of U. From sections 7.2.2 and 7.2.3 we know that the amount of information Eve is able to obtain from her attack strongly depends on the angle θ. As we described in the previous sections the optimal choice for the angle is $\theta = \pi/2$ such that Eve's information is minimized.

Although Alice and Bob are able to minimize Eve's information on the secret key and detect her presence due to the error she introduces they can not be sure whether there is still an adversary entangled with them. Therefore, there is another, more rigorous way to secure such protocols: similar to the Ekert protocol [51] Alice and Bob try to violate the CHSH inequalities using some of their Bell states. As already pointed out this is a little more difficult than comparing some of their measurement results in public but it has the advantage that if the inequalities are violated Alice and Bob can be sure that no third party is entangled with them. Consequently, no

adversary can extract information from an entanglement with Alice or Bob.

In a recent paper [128] we described a generalization of this strategy to the multi-qubit case. The idea is again that an attack strategy based on auxiliary qubits like the simulation attack does not work if the parties can verify that they share a genuinely entangled n-qubit state. To achieve that a series of inequalities presented by the research group of Hiesmayr [79, 55, 80] is applied to test for genuine multipartite entanglement and for k-separability for any multipartite qudit system. These Bell-like inequalities are experimentally implementable as only local observables are needed. The intervention of an adversary changes the overall state and this can be detected by performing certain additional setups and evaluating the inequalities given in eq. (7.70) below.

In [128] we derived a new security argument for the HBB protocol [68] based on these inequalities (cf. section 5.3.2 for details on the HBB protocol). Starting from [79, 80] the inequalities can be rewritten and linearized in terms of local observable as

$$\begin{aligned} I_1: \quad & \frac{1}{8}(\sigma_x\sigma_x\sigma_x - \sigma_y\sigma_y\sigma_x - \sigma_y\sigma_x\sigma_y - \sigma_x\sigma_y\sigma_y) \\ & -\frac{1}{16}(3\times\mathbb{1}\mathbb{1}\mathbb{1} - \sigma_z\sigma_z\mathbb{1} - \sigma_z\mathbb{1}\sigma_z - \mathbb{1}\sigma_z\sigma_z) \leq 0 \\ I_2: \quad & \frac{1}{8}(\sigma_y\sigma_y\sigma_y - \sigma_x\sigma_x\sigma_y - \sigma_x\sigma_y\sigma_x - \sigma_y\sigma_x\sigma_x) \\ & -\frac{1}{16}(3\times\mathbb{1}\mathbb{1}\mathbb{1} - \sigma_z\sigma_z\mathbb{1} - \sigma_z\mathbb{1}\sigma_z - \mathbb{1}\sigma_z\sigma_z) \leq 0. \end{aligned} \tag{7.70}$$

Regarding the HBB protocol the first inequality uses combinations of local observables which are needed in the original scheme to form the secret key whereas the second inequality uses combinations which are discarded in the original protocol. Unfortunately, the latter one can only be applied if the initial state is the "imaginary" GHZ state

$$|P^+_{i00}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + i|111\rangle). \tag{7.71}$$

Nevertheless, using both inequalities Alice and Bob are able to test for genuine 3-partite entanglement. If the inequalities are maximally violated they can be sure that no additional systems are connected with them. As we will see below, there are other protocols for quantum secret sharing which use 3-qubit GHZ states, too (cf. eg. [26]). In this case the legitimate parties are also able to test for genuine 3-partite entanglement using the inequalities from eq. (7.70) to detect an adversary performing a simulation attack.

Another advantage of these inequalities is that they can be extended to the multi-qubit case, as presented in [128]. Using the framework in [79, 80] inequalities for n qubits can be derived straight forward from the 3-qubit case (eq. 7.70) and the 4-qubit case also discussed in [128]. Hence, the check for adversaries can be performed in the same way as described above for any number of qubits. Altogether, the check for genuine entanglement between two or several parties is a much stronger security argument than the random application of rotation or transformation operations described above.

Chapter 8

Applications of the Simulation Attack

In the previous chapter we introduced a new attack strategy for multi-qubit protocols – the simulation attack. We showed that using this attack it is possible to simulate not only the correlations coming from the entanglement swapping performed by Alice and Bob but also an arbitrary unitary operation applied by Alice or Bob.

In this chapter we discuss how the simulation attack works in detail on several protocols [91, 138, 28, 26]. We demonstrate in particular how an adversary is able to simulate rotations [91] as well as basis transformations [138]. Further, we show that the simulation attack is an extension to and more powerful than the ZLG attack by applying it onto Cabello's protocols [28, 26].

8.1 Application on the QKD Protocol by Li et al.

In 2006 Li et al. presented a QKD protocol [91] based on entanglement where they argued that the protocol not only produces 2 random key bits but also 2 certain key bits. This is achieved by introducing a secret Pauli operation in the entanglement swapping process. As it is shown in [91] this protocol is secure against a intercept-resend attack as well as a basic collective attack. Nevertheless, we will show how the simulation attack provides an adversary with full information about the key shared between the two parties.

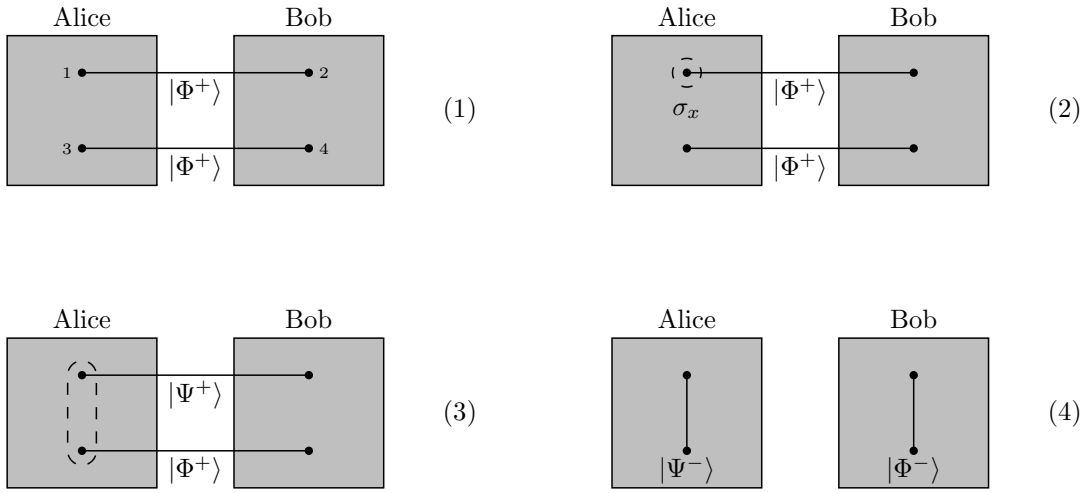

Figure 8.1: Illustration of the protocol presented in [91].

8.1.1 Protocol Description

Alice creates 2 EPR pairs each in a Bell state, e.g. $|\Phi^+\rangle_{12}$ and $|\Phi^+\rangle_{34}$ for each round of the protocol. In [91] Li et al. start the protocol with preshared entangled states which is too strong an assumption since the qubits have to be shared somehow between the two parties. Furthermore, in their security analysis an adversary Eve is granted the possibility to interact with the Bell states such that we can conclude that the qubits of the Bell states are in transit between Alice and Bob.

There are two possible ways to share the Bell states between the legitimate parties: either one party, e.g. Alice, prepares both Bell states and sends one qubit of each state to the other party or both parties prepare one Bell state and they exchange one qubit of their respective states. It is easy to show that the first scenario is insecure against a simple intercept-resend attack: If Alice prepares the Bell states $|\Phi^+\rangle_{12}$ and $|\Phi^+\rangle_{34}$ and sends qubits 2 and 4 to Bob Eve can intercept these qubits and perform a Bell state measurement on them. According to entanglement swapping this will bring qubits 1 and 3 also into a Bell state which is known to Eve. Then she forwards qubits 2 and 4 to Bob who again performs a Bell state measurement on these two qubits giving him the same result as Eve. In the meantime, Alice performed a Bell state measurement on qubits 1 and 3 and obtains the results predefined by Eve's measurement. Thus, Eve does not introduce any error into the correlation between Alice's and Bob's results and has full information about their secret measurement results.

Therefore, we will assume that Alice prepares $|\Phi^+\rangle_{12}$ and Bob prepares $|\Phi^+\rangle_{34}$ and that they exchange the qubits 2 and 3. Before Alice performs her Bell state measurement she chooses an operation $\sigma_A^{(\alpha)} \in \{I, \sigma_x, \sigma_y, \sigma_z\}$ and applies it to qubit 1 (cf. (2) in figure 8.1). Here the superscript (α) denotes again that the operation is applied on qubit α. As we already know from section 7.2.1 the application of a Pauli operation changes the initial state (cf. (3) in figure 8.1). In this case the entanglement swapping due to Alice's measurement on qubits 1 and 3 can be described as

$$\begin{aligned}\sigma_A^{(1)}|\Phi^+\rangle_{12}|\Phi^+\rangle_{34} = \frac{1}{2}\big(&|\Phi^+\rangle_{13}\sigma_A^{(2)}|\Phi^+\rangle_{24} + |\Phi^-\rangle_{13}\sigma_A^{(2)}|\Phi^-\rangle_{24} \\ &+|\Psi^+\rangle_{13}\sigma_A^{(2)}|\Psi^+\rangle_{24} + |\Psi^-\rangle_{13}\sigma_A^{(2)}|\Psi^-\rangle_{24}\big).\end{aligned} \tag{8.1}$$

Based on her result Alice can determine the state of qubits 2 and 4 in Bob's possession after her Bell state measurement, i.e. assuming Alice chose σ_x and obtained $|\Psi^-\rangle_{13}$ Bob's qubits are in the state $|\Phi^-\rangle_{24}$ (cf. (3) in figure 8.1). Additionally, Alice is also able to compute in which the state qubits 1 and 3 would be, if she did not apply any operation on qubit 1. From eq. (8.1) we can see that if Alice did nothing (i.e. performed the $\mathbb{1}$ on qubit 1) the result corresponding to $|\Phi^-\rangle_{24}$ would be $|\Phi^-\rangle_{13}$. Alice publicly announces that she made the Bell state measurement but keeps her exact result by herself.

To infer Alice's result Bob jointly measures qubits 2 and 4 in his possession. Since he does not know yet which operation Alice applied and in which state qubits 1 and 2 have been before the measurement he does not know the exact state of qubits 1 and 3. Due to the correlations in eq. (8.1) he can at least determine that qubits 1 and 3 should be in the state $|\Phi^-\rangle_{13}$ if Alice did not apply any operation on qubit 1. To get the correct state of qubits 1 and 3 Bob asks Alice about her result but keeps his own result secret. Using the information about Alice's and his own result Bob can infer the initial state before Alice's measurement and thus which Pauli operation Alice applied. Therefore, Alice and Bob share information about Alice's secret operation σ_A (the certain bits) and the result Bob obtained (the random bits). They use these two pieces of information to extract a classical raw key using some mapping of Bell states onto classical 2-bit strings, e.g.

$$|\Phi^+\rangle \longrightarrow 00 \quad |\Phi^-\rangle \longrightarrow 01 \quad |\Psi^+\rangle \longrightarrow 10 \quad |\Psi^-\rangle \longrightarrow 11 \tag{8.2}$$

as well as of Pauli operations onto classical 2-bit strings, i.e.

$$\mathbb{1} \longrightarrow 00 \quad \sigma_x \longrightarrow 01 \quad \sigma_y \longrightarrow 10 \quad \sigma_z \longrightarrow 11 \tag{8.3}$$

Alice and Bob repeat these steps for all n rounds of the protocol and thus end up with $4n$ classical raw key bits. In the end they publicly compare a certain number of these raw key bits to estimate the error rate and to detect an eavesdropper. Since Li. et al. assumed that there are perfect channels between Alice and Bob they have to restart the protocol whenever an error occurs [91].

8.1.2 Attack Strategy and Security

In their article Li et al. present an argument for the security of their protocol against an eavesdropper performing an intercept-resend attack [91]. The security against such an attack is rather obvious since Eve destroys the correlation between Alice's and Bob's result by any measurement she performs onto the qubits in transit. Even a joint measurement on both qubits does not give her any advantage because that would entangle qubits 1 and 4, both Bell state measurements at Alice's as well as Bob's side give random results. The probability that Eve stays undetected using this attack strategy can be made arbitrarily small when Alice and Bob compare a sufficiently large set of their measurement results.

Further, an attack strategy involving entanglement is described in [91] where Eve establishes separate keys with Alice and Bob at the same time. Due to the randomness of the results of the Bell measurements one bit of the key between Alice and Eve matches the corresponding bit of the key between Eve and Bob only with probability of 1/4. Hence, Eve's intervention is detected again when Alice and Bob compare some of their bits. A collective attack is described in the article where Eve intervenes with the source and entangles an auxiliary state to the Bell states of Alice and Bob. In this case Eve obtains the same result as Bob half of the time but Bob also obtains an uncorrelated result half of the time. Hence, Eve is again detected by Alice and Bob.

Nevertheless, when Eve uses the simulation attack as her strategy she is able to perfectly eavesdrop the raw key without being detected. As described in detail in the sections above, the state $|\delta\rangle$ preserves the correlation between Alice's and Bob's result even if the initial states are changed by a Pauli operation (cf. section 7.2.1). Therefore, Eve strategy is to prepare $|\delta\rangle_{P-U}$ and intercept the qubits 2 and 3 flying from Alice to Bob and vice versa. She entangles herself with Alice and Bob by the help of entanglement swapping such that qubits 1, Q, R, 4, T and U are in the state $|\delta\rangle$ (cf. (1) in figure 8.2). Then, Eve forwards qubits R to Alice and Q to Bob.

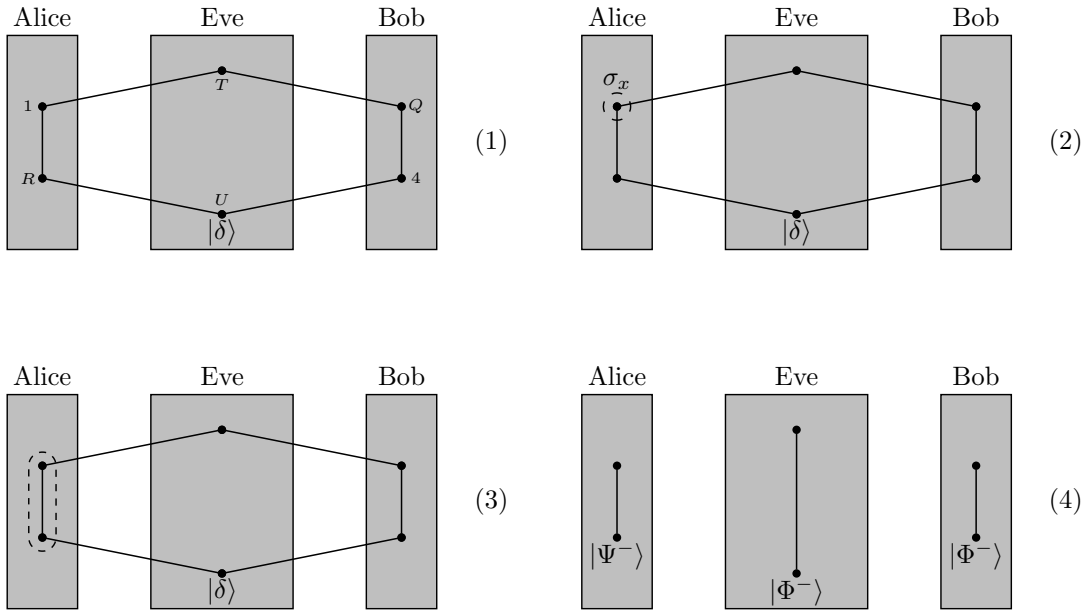

Figure 8.2: *(Simulation attack)* Illustration of the simulation attack strategy on the QKD protocol by Li et al. [91]. Here, Eve already intercepted the qubits in transit and performed the entanglement swapping.

Alice's secret Pauli operation σ_A changes the overall state into

$$\begin{aligned}\sigma_A^{(1)}|\delta\rangle = \frac{1}{2}\big(&\sigma_A^{(1)}|\Phi^+\rangle_{1R}|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU} + \sigma_A^{(1)}|\Phi^-\rangle_{1R}|\Phi^-\rangle_{Q4}|\Phi^-\rangle_{TU} \\ &+\sigma_A^{(1)}|\Psi^+\rangle_{1R}|\Psi^+\rangle_{Q4}|\Psi^+\rangle_{TU} + \sigma_A^{(1)}|\Psi^-\rangle_{1R}|\Psi^-\rangle_{Q4}|\Psi^-\rangle_{TU}\big).\end{aligned} \tag{8.4}$$

From that equation we can see that Eve's qubits T and U are always in the same state as Bob's qubits Q and 4 no matter which operation σ_A she applied. Therefore, Eve has full information about Bob's result and in further consequence about Alice's result and her secret operation σ_A.

In detail, assuming Alice chose $\sigma_A = \sigma_x$ and obtains $|\Psi^-\rangle_{1R}$ Bob's qubits are in the state $|\Phi^-\rangle_{Q4}$ as in the original protocol (cf. (4) in figure 8.2). Thus, the correlation is preserved and when Alice announces her measurement result Bob is able to determine σ_x as Alice's secret operation. But at this time also Eve's qubits T and U are in the state $|\Phi^-\rangle_{TU}$ such that also she knows the Alice's secret operation based on the public announcement of her measurement result. Hence, Eve has full information about the raw key but introduces no error since the correlation between Alice and Bob is preserved.

8.1.3 Revised Protocol

As pointed out in section 7.2.2 and 7.2.3 above a good method to secure the protocol is to randomly apply either a rotation or a basis transformation by an angle $\theta = \pi/2$ on qubit 1 before the secret Pauli operation. The rotation or transformation can not be simulated by Eve using the state $|\delta\rangle$ and Eve can not eavesdrop the secret key without introducing a certain error rate. Since it does not matter from a security point of view whether a rotation or transformation is applied we are going to use the Hadamard operation H in the following paragraphs.

Due to the use of the additional Hadamard operation it is not important any more whether Alice prepares both Bell states or each party prepares a Bell state by its own. To stay consistent with the above descriptions of the protocol and the attack we will discuss the scenario where Alice prepares the state $|\Phi^+\rangle_{12}$ and Bob prepares $|\Phi^+\rangle_{34}$ in each round of the protocol. Alice sends out qubit 2 to Bob and he sends qubit 3 to Alice. When she receives Bob's qubit she randomly applies either the identity operator I or the Hadamard operator H on qubit 1. As described in eq. (7.4) above this alters the state into $|\omega^+\rangle_{12}$. Then, Alice applies her secret Pauli operation σ_A on qubit 1 and performs a Bell state measurement on qubits 1 and 3. This Bell state measurement can be described as

$$\begin{aligned}\sigma_A^{(1)}|\omega^+\rangle_{12} \otimes |\Phi^+\rangle_{34} = \frac{1}{2}\big(&\sigma_A^{(1)}|\Phi^+\rangle_{13} \otimes |\omega^+\rangle_{24} + \sigma_A^{(1)}|\Phi^-\rangle_{13} \otimes |\omega^-\rangle_{24} \\ &+\sigma_A^{(1)}|\Psi^+\rangle_{13} \otimes |\chi^+\rangle_{24} + \sigma_A^{(1)}|\Psi^-\rangle_{13} \otimes |\chi^-\rangle_{24}\big).\end{aligned} \tag{8.5}$$

When Bob received Alice's qubit he publicly informs Alice and she announces whether she applied the Hadamard operation or not together with her measurement result. If she did so, Bob applies the H operation on qubit 2 and otherwise he does nothing. As we have see in section 7.2.3 a repeated application of the Hadamard operator eliminates the superposition and the correlation from the original Bell state measurement is re-established. In the end Bob follows the original protocol and performs a Bell measurement on qubits 2 and 4. He determines Alice's secret operation based on her actual result and computes the four classical bits of the raw key. After n rounds Alice and Bob publicly announce some of their results to estimate the error rate.

8.1.4 Attack Strategy and Security of the Revised Protocol

Since the application of the Hadamard operation is just a minor change of the original protocol, the modified version is also secure against an intercept/resend attack as well as a collective attack, as described in [91]. Therefore, we will just inspect Eve's probability to stay undetected and her information about the raw key if she follows the simulation attack strategy.

The trivial case is when Alice does not apply the Hadamard operator. As we already pointed out above Eve's attack is successful, i.e. she does not introduce any error and obtains full information about the key. If Alice performs the Hadamard operation on qubit 1 we have discussed in section 7.2.3 that Bob does obtain a correlated result only with probability $(3+\cos(2\theta))/4$. For the Hadamard operation $\theta = \pi/2$ Bob's probability to obtain the correlated result is $1/2$ or in other words Eve introduces an error with probability $1/2$ per each round. In the end the expected error probability $\langle P_e \rangle$ is $1/2$ whenever Alice applied the Hadamard operation and 0 otherwise, i.e.

$$\langle P_e \rangle = \frac{1}{2} \times 0 + \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}. \tag{8.6}$$

Accordingly, the probability of detecting Eve is $1 - \langle P_e \rangle^r$ when Alice and Bob publicly compare r of their results during sifting. Hence, the probability to detect Eve can be brought arbitrarily close to 1. Eve's collision probability is, using similar argumentation, $\langle P_c \rangle = 3/4$. Besides the error probability the most interesting value is the amount of information Eve is able to obtain from her attack. It can be easily computed that the Shannon entropy $H(S|M) = 1/2$ and thus Eve's information is

$$I_{AE} = 1 - H\big(S|M\big) = \frac{1}{2}. \tag{8.7}$$

It is also pointed out in section 7.2.3 that Eve is able to prepare a state $|\delta_x\rangle$ to simulate the application of H. Nevertheless, this introduces an error whenever Alice does not apply H such that Alice and Bob end up with the same probability to detect Eve. In both cases the error is very unbiased. If Eve uses $|\delta\rangle$ all the error occurs when Alice applies the Hadamard operation. If Eve uses $|\delta_x\rangle$ all the error occurs when Alice applies $\mathbb{1}$, i.e. when she does nothing. To overcome this fact Eve randomly chooses between preparing $|\delta\rangle$ and $|\delta_x\rangle$. Half of the time Eve uses the correct state and is able to eavesdrop perfectly. The other time she chooses $|\delta\rangle$ when Alice applies H and $|\delta_x\rangle$ when Alice applies $\mathbb{1}$, such that the expected error

probability is the same

$$\langle P_e \rangle = \frac{1}{2} \times \frac{1}{4} + \frac{1}{2} \times \frac{1}{4} = \frac{1}{4}. \tag{8.8}$$

Accordingly, the collision probability and Shannon entropy are the same as described in the previous paragraph.

8.2 Application on the QKD Protocol by Song

In 2004 Song published a QKD scheme based on entanglement swapping which is also supposed to spare alternative measurements [138]. In this scheme Song uses a rather unusual basis transformation with $\theta = 2\pi/3$ whereas in most protocols the basis transformation is the Hadamard operation. This makes this protocol a good example to evaluate how the simulation attack works on such protocols and how much information can be extracted by Eve

8.2.1 Protocol Description

In each round of the protocol Alice and Bob prepare two qubits in their laboratories which are either in the Bell basis or in a transformed basis. The transformation is done by the operation $T = T_x(2\pi/3)$ which is denoted in matrix form as

$$T = \frac{1}{2} \begin{pmatrix} 1 & \sqrt{3} \\ \sqrt{3} & -1 \end{pmatrix} \tag{8.9}$$

Alice and Bob prepare random Bell states and then randomly choose between applying $\mathbb{1}$ or T onto qubit 2 and 4, respectively, in their possession. The application of T changes $|\Phi^{\pm}\rangle$ to $|\eta^{\pm}\rangle$ and $|\Psi^{\pm}\rangle$ to $|\nu^{\pm}\rangle$ where the state in the alternative basis are denoted as

$$|\eta^{\pm}\rangle = \frac{1}{2}|\Phi^{\mp}\rangle + \frac{\sqrt{3}}{2}|\Psi^{\pm}\rangle \quad |\nu^{\pm}\rangle = \frac{\sqrt{3}}{2}|\Phi^{\pm}\rangle - \frac{1}{2}|\Psi^{\mp}\rangle. \tag{8.10}$$

For our further discussion suppose that Alice prepares $|\Psi^{+}\rangle_{12}$ and Bob prepares $|\Phi^{-}\rangle_{34}$. Additionally, Bob applies T onto qubit 4 such that $|\Phi^{-}\rangle_{34}$ is changed into $|\eta^{-}\rangle_{34}$ (cf. (1) and (2) in figure 8.3). The two parties exchange qubits 2 and 4 and publicly confirm the arrival of the respective qubit. Before measuring, Alice and Bob announce publicly whether they applied the basis transformation T or

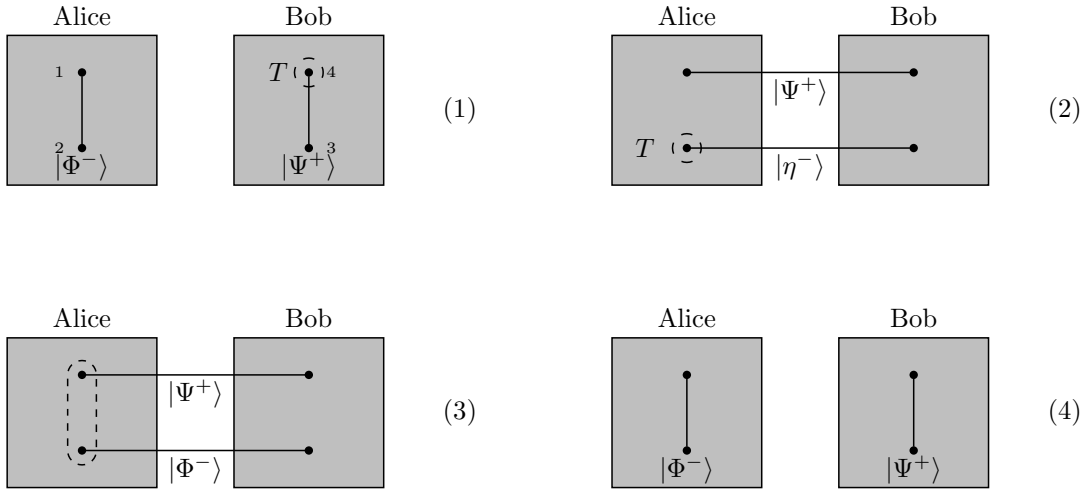

Figure 8.3: Illustration of the protocol presented in [138]. Here, only Bob applies the basis transformation onto his qubit.

not. If one party performed the basis transformation the other party reverses the transformation by applying T on the received qubit again. In our case Alice applies T on qubit 4 because Bob prepared $|\Phi^-\rangle_{34}$ in the alternative basis (cf. (2) in figure 8.3). Then, both parties perform Bell state measurements on the qubits in their possession. Although Alice performs her Bell state measurement onto qubit 1 and 4 instead of 1 and 3 the correlation is still the same as in table 2.1 (up to a global phase). Hence, both parties can compute each other's result based on their own outcome of the Bell state measurement and agree upon two classical bits. Following our example, if Alice obtains $|\Phi^-\rangle_{14}$ Bob obtains $|\Psi^+\rangle_{23}$ and they agree on the classical bit string 01 (cf. table 8.1).

These steps are repeated for all n rounds of the protocol such that Alice and Bob end up with a classical raw key of $2n$ bits. They publicly compare some of their measurement results and the corresponding initial states to estimate the error rate. Furthermore, in this protocol the channels between Alice and Bob are assumed to be perfect such that any error indicates the presence of an eavesdropper and Alice and Bob have to restart the protocol whenever they detect any error.

8.2.2 Attack Strategy and Security

Song discussed a basic version of the ZLG attack in his article [138] and showed in principle that the protocol is secure against this kind of attack. Nevertheless, he

	$\mathbb{1}$	σ_z	σ_x	σ_y
00	$\|\Phi^+\rangle_{14}\|\Phi^+\rangle_{23}$	$\|\Psi^-\rangle_{14}\|\Psi^+\rangle_{23}$	$\|\Phi^-\rangle_{14}\|\Psi^-\rangle_{23}$	$\|\Psi^+\rangle_{14}\|\Phi^-\rangle_{23}$
01	$\|\Psi^-\rangle_{14}\|\Psi^-\rangle_{23}$	$\|\Phi^+\rangle_{14}\|\Phi^-\rangle_{23}$	$\|\Psi^+\rangle_{14}\|\Phi^+\rangle_{23}$	$\|\Phi^-\rangle_{14}\|\Psi^+\rangle_{23}$
10	$\|\Psi^+\rangle_{14}\|\Psi^+\rangle_{23}$	$\|\Phi^-\rangle_{14}\|\Phi^+\rangle_{23}$	$\|\Psi^-\rangle_{14}\|\Phi^-\rangle_{23}$	$\|\Phi^+\rangle_{14}\|\Psi^-\rangle_{23}$
11	$\|\Phi^-\rangle_{14}\|\Phi^-\rangle_{23}$	$\|\Psi^+\rangle_{14}\|\Psi^-\rangle_{23}$	$\|\Phi^+\rangle_{14}\|\Psi^+\rangle_{23}$	$\|\Psi^-\rangle_{14}\|\Phi^+\rangle_{23}$

Table 8.1: Mapping from measurement results onto classical bits (adapted from [138]). The Pauli operations denote the relation between the initial states.

gave no expected error rate or collision probability for Eve which is of great interest since the operation T is a basis transformation by an angle of $2\pi/3$ and not $\pi/2$ as, for example, in the revised Cabello protocol [28]. Hence, we are going to look at it in detail in the next paragraph. Previously, we just want to point out that the protocol is also secure against an intercept-resend attack as well as a collective attack based on the same argumentation as in the revised Cabello protocol [28].

We can immediately show that Song's protocol is completely open to the simulation attack when Alice does not apply the transformation T. In this case Alice and Bob just perform the entanglement swapping and Eve can intercept qubits 2 and 4 in transit. As it is described in detail above Eve entangles herself with Alice and Bob using $|\delta\rangle$ using entanglement swapping and sends qubits Q to Bob and S to Alice, respectively (cf. (1) in figure 8.4). When Alice and Bob perform their Bell state measurements the correlation between their results is preserved by the state $|\delta\rangle$ although both parties kept their initial state secret (cf. the remark at the end of section 7.2.2). When Alice and Bob publicly announce their initial states Eve is able to obtain full information about Alice's and Bob's secret measurement based on the state of qubits T and U in her possession.

When either Alice or Bob performs the transformation T we have the scenario described in section 7.2.3. Eve is not able to compensate the random application of the transformation while still preserving the correlation when T is not applied. Hence, Eve's intervention introduces an error, i.e. the parties do not obtain correlated results all of the time. Taking the example from above, Bob applies T onto qubit 4 and therefore Alice also applies T onto qubit S she receives from Eve (cf. (2) in figure 8.4). When Alice obtains $|\Phi^-\rangle_{1S}$ from her measurement Bob obtains the

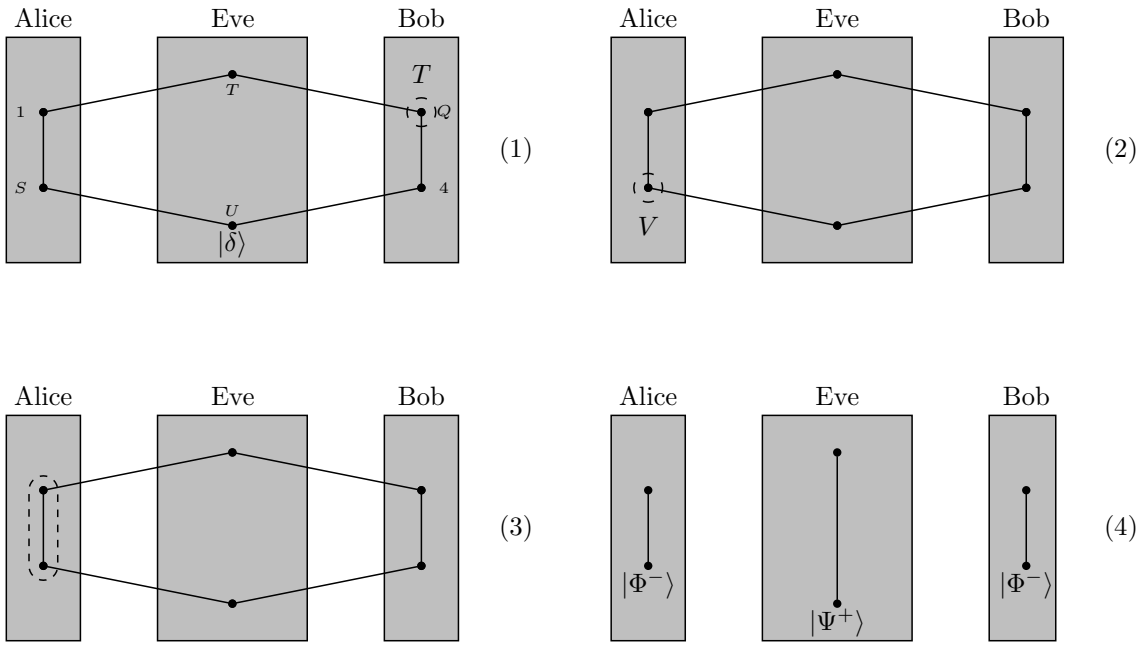

Figure 8.4: *(Simulation attack)* Illustration of the simulation attack strategy on the protocol presented in [138]. Here, only Bob applies the basis transformation onto his qubit.

correlated result $|\Psi^+\rangle_{23}$ only with probability 5/8. In other words, Eve introduces an error with probability 3/8 which leads to an expected error probability for this scenario of

$$\langle P_e \rangle = \frac{1}{2} \times 0 + \frac{1}{2} \times \frac{3}{8} = \frac{3}{16} \tag{8.11}$$

which is significantly lower than 1/4. Hence, Eve has a better opportunity to eavesdrop the key in this protocol than, for example, in the revised version of the Cabello protocol [28] or the protocol by Li et al [91]. Due to the fact that the transformation T maps onto an unbiased superposition of states (cf. eq. (8.10) above) Eve is able to extract more information than usual from her attack strategy. The Shannon entropy for the simulation attack on Song's protocol is $H(S|M) \simeq 0.406$ which leads to

$$I_{AE} = 1 - H\big(S|M\big) \simeq 0.594 \tag{8.12}$$

Assuming that both parties perform the basis transformation T the protocol becomes insecure again. Due to Eve's entanglement swapping the operation T is brought from qubits 2 and 4 onto qubits 1 and 3, which leads to the state

$$T^{(1)}T^{(3)}|\delta\rangle_{1Q3STU} \tag{8.13}$$

When Alice and Bob apply the basis transformation T on qubits Q and S they receive from Eve, the state changes again into

$$T^{(1)}T^{(Q)}T^{(3)}T^{(S)}|\delta\rangle_{1Q3STU} \tag{8.14}$$

When Alice performs her Bell state measurement onto qubits 1 and S it has the effect that the operations $T^{(1)}$ and $T^{(S)}$ are swapped onto qubits Q and 3 thus reverting the effect of T at Bob's side and re-establishing the state $|\delta\rangle$. Hence, Bob's measurement on qubits Q and 3 results into a state completely correlated to Alice's result. Further, Eve's qubits T and U are also correlated to Bob's result such that she has full information about the key when Alice and Bob announce their initial states.

As already pointed out in the previous section Eve's attempt to eavesdrop can be identified rather easily if she only uses $|\delta\rangle$. In this case the occurrence of errors is unbiased, i.e. error appear only if one of the two parties applies the operation T. Therefore, Eve prepares another state $|\delta_v\rangle$ where she applies T onto qubits P and Q to simulate Alice's actions (cf. $|\delta_x\rangle$ in section 7.2.3). When Alice chooses to use the transformation, Bob and herself perform T on qubits Q and 1, respectively, such that the effect of Eve's operations is reversed and the original correlations are re-established. If Bob chooses to use the transformation, T is applied on qubits S and 3 due to entanglement swapping. Thus, T effects all four qubits 1, Q, 3 and S which brings us to the scenario just discussed in the previous paragraph. The four instances of T neutralize each other and the original correlations are no longer violated. Hence, Eve randomly chooses between $|\delta\rangle$ and $|\delta_v\rangle$ to distribute her error over all possible cases. The expected error $\langle P_e \rangle$ in this case is again

$$\langle P_e \rangle = \frac{1}{4} \times 0 + \frac{1}{4} \times \frac{3}{8} + \frac{1}{4} \times \frac{3}{8} + \frac{1}{4} \times 0 = \frac{3}{16}. \tag{8.15}$$

8.2.3 Revised Protocol

We have just showed that the protocol presented by Song [138] per se is secure against the simulation attack. The main reason for security is the random application of the basis transformation T which can not be simulated by Eve using $|\delta\rangle$. Nevertheless, we suggest to replace T by the Hadamard operation H as an improvement to security. We are going to explain in detail why this is an advantage in the next section.

The replacement by the Hadamard operation does not change the overall process of the protocol. Alice and Bob still choose at random their initial states and individually choose whether to apply H onto qubit 2 and 4, respectively. Then, they exchange qubits 2 and 4 and upon notice of arrival at the communication partner they announce publicly their choice regarding the application of H. If necessary, Alice and Bob reverse the effect of the Hadamard operation by applying it again on the received qubits. Afterwards, Alice performs the Bell state measurement on qubits 1 and 4 and Bob does the same on qubits 2 and 3 in his possession. They publicly announce their measurement bases and based on that information are able to share two classical raw key bits according to table 8.1.

8.2.4 Attack Strategy and Security of the Revised Protocol

The reason to replace the transformation T by the Hadamard operation is the choice of the angle θ defining T. As pointed out at the beginning of the protocol description $T = T_x(2\pi/3)$, i.e. $\theta = 2\pi/3$. This transforms

$$|0\rangle \longmapsto \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle \quad \text{and} \quad |1\rangle \longmapsto \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle \tag{8.16}$$

which is an unbiased superposition of the basis states $|0\rangle$ and $|1\rangle$. In other words a measurement of $T|0\rangle$ in the Z-basis is more likely to result in $|1\rangle$ than in $|0\rangle$. This is also true for the states $|\eta^{\pm}\rangle$ and $|\nu^{\pm}\rangle$ which are superpositions of Bell states where one state is always in favor. Hence, the optimal choice of the angle θ is $\pi/2$ such that T becomes the Hadamard operation H and both states in the superposition are equally likely.

With the Hadamard operation instead of T the sequence of Eve's attack using the simulation approach is completely the same. Using the state $|\delta\rangle$ she is able to perfectly eavesdrop whenever nobody or both parties apply H. Further, Eve is able to perfectly eavesdrop if she uses the state $|\delta_x\rangle$ from section 7.2.3 above whenever either Alice or Bob chooses to apply H on the initial state. In every other case the probability for Eve to introduce an error is 1/2. Thus, the optimal strategy for Eve is to randomly choose between $|\delta\rangle$ and $|\delta_x\rangle$ for her attack to distribute the error she introduces equally as pointed out above. This leads to an expected error probability of

$$\langle P_e \rangle = \frac{1}{4} \times 0 + \frac{1}{4} \times \frac{1}{2} + \frac{1}{4} \times \frac{1}{2} + \frac{1}{4} \times 0 = \frac{1}{4}. \tag{8.17}$$

Comparing eq. (8.15) and eq. (8.17) we see that due to the application of H Eve introduces a much higher error rate and therefore is more likely to be detected. Additionally, also the Shannon entropy increases from $H(S|M) = 0.406$ in the original version to $H(S|M) = 0.5$ in the revised version such that Eve's information decreases to

$$I_{AE} = 1 - H\big(S|M\big) = \frac{1}{2} \tag{8.18}$$

for the revised version.

8.3 Application on the Cabello QKD Protocol

As already presented in section 7.1.1 Cabello published a QKD protocol based on entanglement swapping in 2000 [27]. His idea was also to spear the additional measurement in another basis to increase the efficiency of the protocol. It has been shown by Zhang et al. [170] that the protocol is open to a special kind of attack where Eve entangles herself with the legitimate parties. The detailed protocol description as well as the description of the ZLG attack can be found in section 7.1.1 above. In the following paragraphs we are going to show how the simulation attack works on the protocol by Cabello and the revised protocol [28]. We want to demonstrate that the simulation attack is a generalized version of the ZLG attack since it is as powerful as the ZLG attack but is also applicable on other protocols, as we have already seen.

8.3.1 Attack Strategy and Security

It has been shown in [170] that the protocol by Cabello is not secure. We can observe the same result when applying the simulation attack strategy onto the protocol. In this case, Eve prepares the state $|\delta\rangle_{P-U}$ and intercepts qubit 2 of the state $|\Phi^-\rangle_{12}$ coming from Alice. Eve performs a Bell state measurement on qubits 2 and P and afterwards her state changes to $\sigma_z^{(1)}|\delta\rangle_{1Q-U}$. Then, Eve sends qubit Q to Bob impersonating the qubit coming from Alice. Meanwhile, Alice performs her Bell state measurement on qubits 1 and 3 in her possession leaving qubits 5, $Q-U$ in the state $\sigma_A^{(5)}\sigma_z^{(5)}|\delta\rangle_{5Q-U}$ where $\sigma_A|\Phi^+\rangle$ is Alice's secret result. If we take $|\Psi^-\rangle_{13}$ as

Alice's secret result (cf. (1) and (2) in figure 8.5) qubits 5, $Q-U$ are in the state

$$\begin{aligned}|\delta'\rangle_{5Q-U} = \frac{1}{2}\big(&|\Phi^+\rangle_{5R}|\Psi^+\rangle_{QS}|\Psi^+\rangle_{TU} + |\Phi^-\rangle_{5R}|\Psi^-\rangle_{QS}|\Psi^-\rangle_{TU} \\ &+|\Psi^+\rangle_{5R}|\Phi^+\rangle_{QS}|\Phi^+\rangle_{TU} + |\Psi^-\rangle_{5R}|\Phi^-\rangle_{QS}|\Phi^-\rangle_{TU}\big)\end{aligned} \tag{8.19}$$

When Bob receives qubit Q he performs his Bell state measurement on qubits Q and 4 thus entangling qubit 6 with Eve. Hence, the overall state changes into $\sigma_A^{(5)}\sigma_z^{(5)}\sigma_B^{(6)}|\delta\rangle_{56R-U}$ with $\sigma_B|\Phi^+\rangle$ Bob's secret result (cf. (1) and (2) in figure 8.5). Assuming Bob obtains $|\Phi^+\rangle_{Q4}$ the state $|\delta'\rangle_{5Q-U}$ does not change at all. Afterwards Bob sends qubit 6 to Alice and Eve intercepts it. Eve then performs a Bell state measurement on qubits T and U giving her a random result as it is described in eq. (8.19). Further, she measures qubits 6 and S and compares the outcome with the state of qubits T and U. It is shown in eq. (8.19) that these two results differ only by a Pauli operation – in this case $\mathbb{1}$ – describing Bob's secret result (cf. (3) in figure 8.5). Therefore, Eve has full information about Bob's result and the information to correct the state of qubits 5 and R to preserve the correlation given in table 7.1. Next, Eve sends qubit R to Alice who performs her measurement on qubits 5 and R and publicly announces the result, in this case $|\Psi^+\rangle_{5R}$ (cf. (4) in figure 8.5). Due to Eve's Pauli operation both parties always have a valid correlation of their results and they have no chance to detect Eve. Further, Eve obtains full information about Alice's and Bob's result from the state of her qubits 6 and S (cf. (4) in figure 8.5).

There is a little overhead when using the simulation attack since the qubits T and U are of minor interest for the attack on this special protocol since the initial states are publicly known. Eve is still able to obtain full information about Bob's secret result if these two qubits are excluded. But, as we have presented in the previous section, they are of essential value when looking at other protocols [91, 138] where they give full information about Bob's result.

8.3.2 Attack Strategy and Security of the Revised Protocol

Cabello published an addendum to his protocol where he introduced a version which is secure against the ZLG attack [28]. This is achieved by the random application of a Hadamard operation on qubit 3 in Alice's possession (cf. section 7.1.1 for details). In this case the correlation between Alice's and Bob's measurement is violated with probability 1/2. This error introduced by Eve's intervention can be detected with an arbitrary high probability.

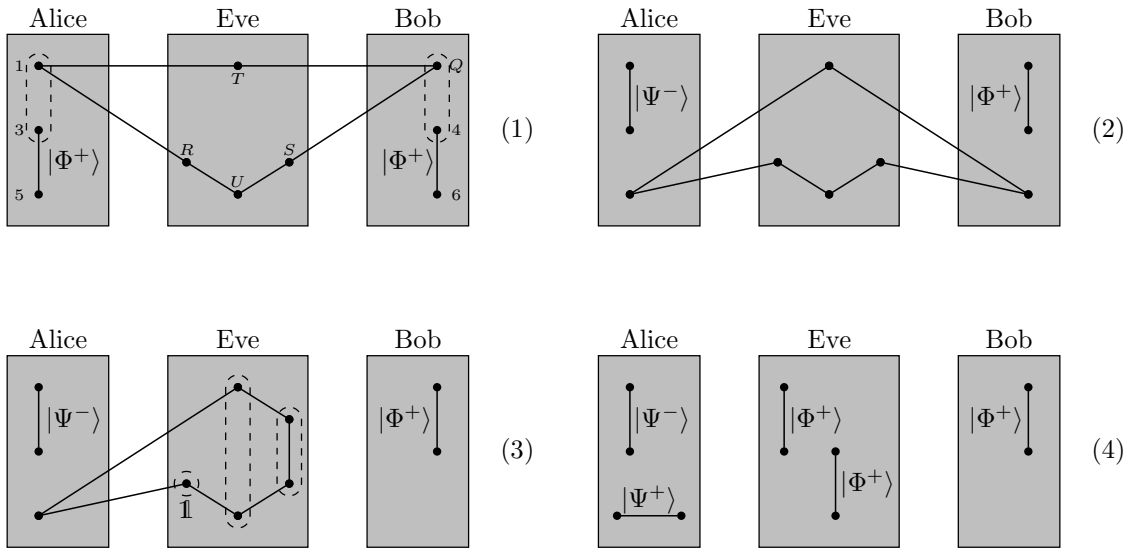

Figure 8.5: *(Simulation attack)* Illustration of the simulation attack strategy on the protocol presented in [27].

As pointed out in section 7.2.3 a random application of the Hadamard operation is also the optimal strategy to secure a protocol against the simulation attack. Eve is not able to prepare a state which preserves the correlation between Alice's and Bob's results for the application of $\mathbb{1}$ and H, simultaneously. Nevertheless, Eve has an advantage using the simulation attack compared to the ZLG attack. As we have seen above, when performing the ZLG attack the expected error probability $\langle P_e \rangle = 1/2$ but an error occurs only when Alice uses the Hadamard operation. Otherwise, Eve does not introduce any error. This fact makes it even easier to detect Eve's presence because a natural error is very unlikely to occur only on specific occasions.

Using $|\delta\rangle$ on the revised protocol, Eve intercepts qubits 2 and 6 coming from Alice and Bob, respectively, and performs Bell state measurements on them together with qubits P and S. Due to her corrections Eve obtains the state $\sigma_z^{(1)}|\delta\rangle_{1QR4TU}$ after her measurements with σ_z coming from Alice's initial state $|\Phi^-\rangle_{12}$. Then, Eve sends qubits Q to Bob and R to Alice. In the meantime, Alice applies the Hadamard operation on qubit 3 and performs a Bell state measurement on qubits 1 and 3 which swaps the Hadamard operation onto qubit 5. Let's assume for our further discussion that Alice obtains $|\Psi^-\rangle_{13}$ as in the original protocol which brings the

remaining qubits into the state

$$\begin{aligned}|\delta'\rangle_{5QR4TU} = \frac{1}{2}\big(&|\omega^+\rangle_{5R}|\Psi^+\rangle_{Q4}|\Psi^+\rangle_{TU} \\ &+|\omega^-\rangle_{5R}|\Psi^-\rangle_{Q4}|\Psi^-\rangle_{TU} \\ &+|\chi^+\rangle_{5R}|\Phi^+\rangle_{Q4}|\Phi^+\rangle_{TU} \\ &+|\chi^-\rangle_{5R}|\Phi^-\rangle_{Q4}|\Phi^-\rangle_{TU}\big)\end{aligned} \tag{8.20}$$

Further, Alice performs a Bell state measurement on qubits 5 and R bringing qubits Q, 4, T and U in the state

$$\frac{1}{\sqrt{2}}\big(|\Psi^+\rangle_{Q4}|\Psi^+\rangle_{TU} - |\Phi^-\rangle_{Q4}|\Phi^-\rangle_{TU}\big) \tag{8.21}$$

for Alice's result $|\Psi^+\rangle_{53}$. She announces her result and whether she used the Hadamard operation or not. On the other side, Bob applies the Hadamard operation onto qubit 4 and his measurement on qubits Q and 4 results either in $|\Phi^+\rangle_{Q4}$ or $|\Psi^-\rangle_{Q4}$. It follows from table 7.2 that only $|\Psi^-\rangle_{Q4}$ correlates with Alice's secret and public result and that Bob identifies an error whenever he measures $|\Phi^+\rangle_{Q4}$. Thus, Alice and Bob detect an error when publicly comparing some of their results with probability 1/2 for each result they compare.

Eve's qubits T and U are in the state $|\omega^+\rangle_{TU}$ for Bob's result $|\Psi^-\rangle_{Q4}$ and $|\chi^-\rangle_{TU}$ for Bob's result $|\Phi^+\rangle_{Q4}$. Therefore, Eve applies a Hadamard operation on qubit T to rotate the state back into the Z basis and performs a Bell state measurement afterwards. In general, whenever Bob obtains a correct result, Eve's qubits T and U are in the same state as qubits Q and 4 such that Eve has full information about Bob's result with probability 1/2. Otherwise Eve has no information about the outcome of Bob's measurement. Nevertheless, if Eve obtains either $|\Phi^-\rangle_{TU}$ or $|\Psi^-\rangle_{TU}$ she knows that Bob's result is not correlated to Alice's results.

As already discussed in section 7.2.3 the optimal strategy for Eve using the simulation attack is to randomly prepare either the state $|\delta\rangle$ or $|\delta_v\rangle$ where she applied the Hadamard operation on qubits P and Q. This gives Eve full information about Alice's and Bob's results whenever she chooses $|\delta\rangle$ and Alice uses $\mathbb{1}$ as well as when she chooses $|\delta_v\rangle$ and Alice uses H. For the other cases Eve introduces an error with probability 1/2 which gives us the expected error probability

$$\big\langle P_e\big\rangle = \frac{1}{4}\times 0 + \frac{1}{4}\times\frac{1}{2} + \frac{1}{4}\times\frac{1}{2} + \frac{1}{4}\times 0 = \frac{1}{4} \tag{8.22}$$

As pointed out, this is equal to the expected error probability using the ZLG attack but the error is equally distributed over all possible cases. Regarding the collision probability the simulation attack is equal to the ZLG attack since Eve also has no information about Bob's secret whenever she prepares the incorrect state. That gives for $\langle P_c \rangle$ the equation

$$\langle P_c \rangle = \frac{1}{4} \times 1 + \frac{1}{4} \times \frac{1}{2} + \frac{1}{4} \times \frac{1}{2} + \frac{1}{4} \times 1 = \frac{3}{4}. \tag{8.23}$$

For the overall scenario the Shannon entropy $H(S|M) = 1/2$ such that Eve's information about the secret is then

$$I_{AE} = 1 - H\big(S|M\big) = \frac{1}{2} \tag{8.24}$$

which is equal to the information Eve obtains when using the ZLG attack (cf. eq. (7.10) above). Hence, Eve obtains the same amount of information when using the simulation attack but introduces a smaller error rate such that it is more difficult to detect her.

8.4 Application on the Cabello QSS Protocol

In section 7.1.2 another protocol by Cabello is described where he presents a quantum secret sharing protocol based on entanglement swapping [26]. The idea is to share a key between two parties, Bob and Charlie, such that they can communicate with Alice only if they collaborate and bring their shares together. The entanglement between the three parties is realized using a GHZ state. We have already pointed out that the protocol is open to a kind of ZLG attack [90] where Eve entangles herself with Alice, Bob and Charlie and is able to eavesdrop the secret. In the following paragraphs we are going to describe how the simulation attack works on this protocol to stress the fact that it is a generalization of the ZLG attack and as an example that it is also applicable on QSS protocols.

8.4.1 Attack Strategy and Security

As discussed in [90] the protocol by Cabello [26] is not secure against a ZLG-type attack strategy. The idea is that Eve has to find a state which simulates the correlations given in table 7.3 and provides her with additional information about Bob's

measurement results. The version of the state $|\delta\rangle$ given in eq. (7.28) would be a possible choice, but not a very good one. A better version for $|\delta\rangle$ is

$$\begin{aligned}
|\delta\rangle = \frac{1}{2}\Big(& |\Phi^+\rangle|\Phi^+\rangle \otimes \frac{1}{2}\big(|\Phi^+\rangle|\Phi^+\rangle|P_{00}^+\rangle + |\Phi^-\rangle|\Phi^-\rangle|P_{00}^-\rangle \\
& \qquad + |\Psi^+\rangle|\Psi^+\rangle|P_{01}^+\rangle + |\Psi^-\rangle|\Psi^-\rangle|P_{01}^-\rangle\big) \\
& + |\Phi^-\rangle|\Phi^-\rangle \otimes \frac{1}{2}\big(|\Phi^+\rangle|\Phi^+\rangle|P_{00}^-\rangle + |\Phi^-\rangle|\Phi^-\rangle|P_{00}^+\rangle \\
& \qquad + |\Psi^+\rangle|\Psi^+\rangle|P_{01}^-\rangle + |\Psi^-\rangle|\Psi^-\rangle|P_{01}^+\rangle\big) \\
& + |\Psi^+\rangle|\Psi^+\rangle \otimes \frac{1}{2}\big(|\Phi^+\rangle|\Phi^+\rangle|P_{10}^+\rangle + |\Phi^-\rangle|\Phi^-\rangle|P_{10}^-\rangle \\
& \qquad + |\Psi^+\rangle|\Psi^+\rangle|P_{11}^+\rangle + |\Psi^-\rangle|\Psi^-\rangle|P_{11}^-\rangle\big) \\
& + |\Psi^-\rangle|\Psi^-\rangle \otimes \frac{1}{2}\big(|\Phi^+\rangle|\Phi^+\rangle|P_{10}^-\rangle + |\Phi^-\rangle|\Phi^-\rangle|P_{10}^+\rangle \\
& \qquad + |\Psi^+\rangle|\Psi^+\rangle|P_{11}^-\rangle + |\Psi^-\rangle|\Psi^-\rangle|P_{11}^+\rangle\big)\Big)_{E_1-E_{11}}
\end{aligned} \tag{8.25}$$

It can be immediately verified that this state simulates all possible correlations from table 7.3 and that the qubit pairs E_3, E_4 and E_7, E_8 can be used to obtain full information about Bob's and Charlie's measurement results. We already showed that an adversary from the inside is much more powerful than an eavesdropper from the outside. Hence, we are going to focus first on the scenario of an external adversary Eve and then on a dishonest Charlie both using the simulation attack to get as much information about the secret as possible.

In the first scenario the adversary Eve intercepts the qubits A and B coming from Alice and performs a GHZ state measurement on them together with qubit E_9 of the state $|\delta\rangle$. As we have already seen in the general description of the simulation attack in section 7.2 above Eve is able to correct the resulting state such that she now shares $|\delta\rangle$ with Alice. Eve sends qubits E_2 to Bob and E_6 to Charlie impersonating qubits A and B (cf. (1) in figure 8.6). Following the protocol both parties perform their respective Bell state measurements and return qubits C and D to Alice. In the meantime, Alice performed her Bell state measurement on qubits 2 and 3 which entangles qubit 1 with the state $|\delta\rangle$. Eve intercepts the qubits coming from Bob and Charlie and performs Bell state measurements on the pairs E_1, C and E_3, E_4 (cf. (2) in figure 8.6). From the definition of the state $|\delta\rangle$ we see that the result of Eve's first measurement is random but the result of the second measurement gives her a reference to determine Bob's secret result. In detail, if Bob obtained

$|\Phi^-\rangle_{4E_2}$ and Eve's first result is $|\Phi^-\rangle_{E_1C}$ the state of qubits E_3 and E_4 is $|\Phi^+\rangle_{E_3E_4}$. The difference between these two states is a σ_z operation which defines Bob's secret result. Similarly, Eve measures the qubit pairs E_5, D and E_7E_8 which gives her full information about Charlie's secret result. Further, she knows from eq. (8.25) in which state the last three qubits 1, E_{10} and E_{11} are and based on her results from the measurements on qubits E_1, C and E_5, D which Pauli operations to apply on qubits E_{10} and E_{11} to preserve the correlations between the legitimate parties. Assuming Eve obtained $|\Phi^+\rangle_{E_5D}$ and $|\Psi^+\rangle_{E_7E_8}$ from her remaining measurements she applies a σ_x on qubit E_{11}. In the end, Eve sends qubits E_{10} and E_{11} to Alice who performs a GHZ state measurement on them and publicly announces the result. Due to Eve's Pauli operations Alice's result of the GHZ state measurement always corresponds to Bob's and Charlie's results as given in table 7.3 and Eve's presence is not detected.

If we are dealing with a dishonest Charlie the process of the attack is almost the same as just described for an external adversary Eve. Charlie prepares the state $|\delta\rangle$ from eq. (8.25) above instead of $|\Phi^+\rangle_{5D}$ and intercepts the qubit flying from Alice to Bob. Charlie forwards qubit E_2 to Bob and performs his Bell state measurement on qubits E_5 and E_6. As described in the attack in the previous paragraph Bob's Bell state measurement on qubits 4 and E_2 entangles qubit C with $|\delta\rangle$. Charlie intercepts qubit C coming from Bob and measures it together with qubit E_1. The result of this measurement compared with the result of the measurement on qubits E_3 and E_4 gives him full information about Bob's secret result and also defines the Pauli operation he has to apply on qubit E_{10}. In detail, if Charlie obtained $|\Phi^-\rangle_{E_1C}$ and $|\Psi^-\rangle_{E_3E_4}$ he can infer that Bob's secret result is $|\Psi^+\rangle_{4E_2}$. Regarding the state of the remaining 3 qubits Charlie knows that he has to apply in this case a σ_x operation onto qubit E_{10} to reestablish the correlation between the legitimate parties. When he returns qubits E_{10} and E_{11} to Alice she performs a GHZ state measurement on these two qubits together with qubit 1 and announce her result. Since the correlation is still valid, Alice and Bob do not discover Charlie's intervention and he is able to obtain Alice's secret without Bob's help.

A small remark on the application of the simulation attack in this scenario is that it seems like an overkill because it uses much more qubits than the ZLG attack. But we will show in the next paragraphs that the simulation attack using the state $|\delta\rangle$ is more effective than the ZLG attack when looking at the revised version of Cabello's

protocol [90].

8.4.2 Attack Strategy and Security of the Revised Protocol

In the revised version of this protocol [90] presented by Lee et al. it is suggested that Alice, Bob and Charlie make use of the quantum Fourier transformation (QFT). The QFT simplifies in our case to the Hadamard operation as described in detail in section 7.1.2 above. First, Bob and Charlie randomly choose whether to apply the Hadamard operation or the identity $\mathbb{1}$ on their qubits 4 and 5, respectively. Additionally, Alice, Bob and Charlie exchange all necessary qubits before performing any measurement. As we have seen above, this forces an external adversary Eve as well as a dishonest Charlie to introduce a rather large error rate into the protocol since in both cases the actions of the legitimate parties can not be anticipated. When using the simulation attack in either scenario the error rate is lower compared to the ZLG attack which makes it more effective for an eavesdropper.

In the first scenario where Eve interferes with the protocol she is able to fully entangle herself with all three parties since they exchange all qubits before performing any measurements. This means, Eve prepares the state $|\delta\rangle$ from eq. (8.25) and intercepts qubits A and B coming from Alice and performs a GHZ state measurement on them together with qubit E_9. Further, she intercepts qubits C and D coming from Bob and Charlie, respectively, and performs Bell state measurement on the pairs E_1, C as well as E_5, D. After that Eve sends qubits E_2 to Bob, E_6 to Charlie and qubits E_{10} and E_{11} to Alice such that the state $|\delta\rangle$ is now distributed over all 4 parties. The definition of $|\delta\rangle$ indicates that Bob's and Charlie's measurements on the qubits in their possession yield random results but the respective qubits still in Eve's possession are in the same state, afterwards. Additionally, the three qubits 3, E_{10} and E_{11} at Alice's laboratory are always in a correlated state to Bob's and Charlie's results. Assuming again that Bob obtained $|\Psi^+\rangle_{4E_2}$ and Charlie obtained $|\Phi^-\rangle_{5E_6}$ then qubits 3, E_{10} and E_{11} are in the state $|P_{10}^-\rangle$ which corresponds to the state Alice expects to find if she obtains $|\Phi^+\rangle_{23}$ (cf. table 7.3). Also Alice's secret measurement on qubits 2 and 3 does not leave these three qubits in a state violating the expected correlation since her measurement changes the GHZ state accordingly.

In the revised version of Cabello's protocol Bob and Charlie randomly apply a Hadamard operation on one qubit in their possession which is not taken into account in the considerations above. Assuming that only Bob applied the Hadamard

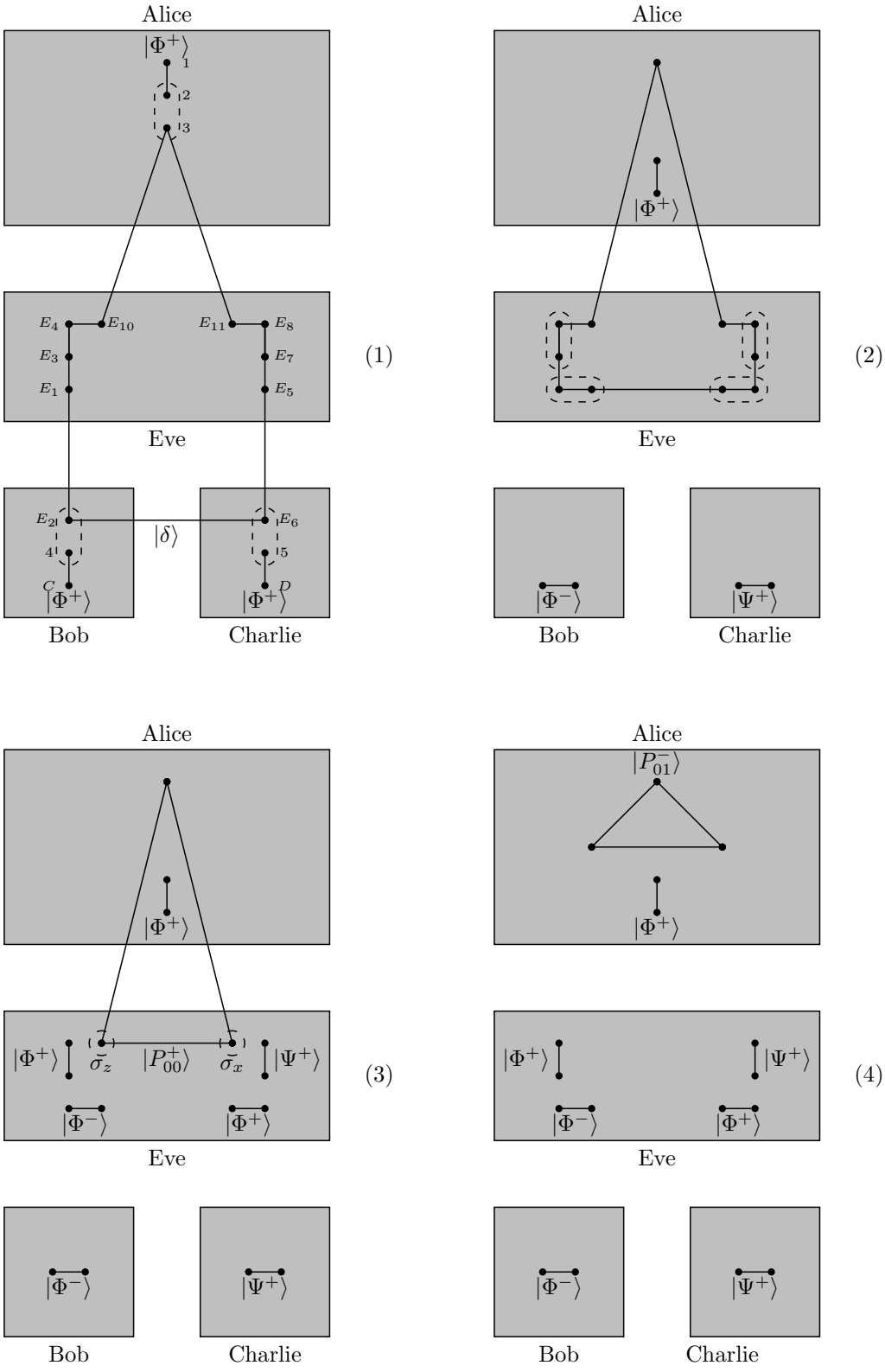

Figure 8.6: *(Simulation attack)* Illustration of the simulation attack strategy on the protocol presented in [26].

operation the overall state changes into

$$\begin{aligned}\frac{1}{\sqrt{2}}\Big(|\Phi^+\rangle \otimes \frac{1}{2}\big(&|\Phi^+\rangle|\Phi^+\rangle|P_{00}^+\rangle + |\Phi^-\rangle|\Phi^-\rangle|P_{00}^-\rangle \\ &+|\Psi^+\rangle|\Psi^+\rangle|P_{01}^+\rangle + |\Psi^-\rangle|\Psi^-\rangle|P_{01}^-\rangle\big) \\ +|\Psi^-\rangle \otimes \frac{1}{2}\big(&|\Phi^+\rangle|\Phi^+\rangle|P_{10}^-\rangle + |\Phi^-\rangle|\Phi^-\rangle|P_{10}^+\rangle \\ &+|\Psi^+\rangle|\Psi^+\rangle|P_{11}^-\rangle + |\Psi^-\rangle|\Psi^-\rangle|P_{11}^+\rangle\big)\Big)\end{aligned} \tag{8.26}$$

if Bob's result is $|\Psi^+\rangle_{4E_2}$. Hence, at this time Eve obtains from a measurement on qubits E_3 and E_4 either $|\Phi^+\rangle_{E_3E_4}$ or $|\Psi^-\rangle_{E_3E_4}$ but both do not correspond to Bob's result. Thus, the best strategy for Eve is to delay her measurement until she knows whether Bob applied the Hadamard operation or not, as described below. Similarly, if just Charlie applies the Hadamard operation the overall state is

$$\begin{aligned}|\Psi^+\rangle \otimes \frac{1}{2}\big(&|\omega^+\rangle|\Phi^+\rangle|P_{10}^+\rangle + |\omega^-\rangle|\Phi^-\rangle|P_{10}^-\rangle \\ &+|\chi^+\rangle|\Psi^+\rangle|P_{11}^+\rangle + |\chi^-\rangle|\Psi^-\rangle|P_{11}^-\rangle\big)\end{aligned} \tag{8.27}$$

after Bob's result $|\Psi^+\rangle_{4E_2}$. In this case Eve obtains the same result as Bob but further on her measurement on qubits E_7E_8 yields a result uncorrelated to Charlie's measurement outcome due to his Hadamard operation. In the last case where both Bob and Charlie apply the Hadamard operation the overall state after both measurements changes to

$$\begin{aligned}\frac{1}{\sqrt{2}}\Big(|\Phi^+\rangle \otimes \frac{1}{\sqrt{2}}\big(&|\Phi^+\rangle|P_{00}^+\rangle - |\Psi^-\rangle|P_{01}^-\rangle\big) \\ +|\Psi^-\rangle \otimes \frac{1}{\sqrt{2}}\big(&|\Phi^+\rangle|P_{10}^-\rangle - |\Psi^-\rangle|P_{11}^+\rangle\big)\Big)\end{aligned} \tag{8.28}$$

assuming Bob and Charlie obtain $|\Psi^+\rangle_{4E_2}$ and $|\Phi^-\rangle_{5E_6}$, respectively. As we can see, Eve's results are completely uncorrelated to the two secret results of Bob and Charlie. Thus, the optimal strategy for Eve is to delay her measurements on qubits E_3E_4 and E_7E_8 until Bob and Charlie publicly announce their choice regarding the application of the Hadamard operation. Having that information Eve is able to perform a Hadamard operation herself on qubits E_3 and E_7, respectively, and perform her measurement afterwards. Half of the time this gives Eve full information about Bob's result.

In all possible cases, Alice applies a Hadamard operation on qubits E_{10} and E_{11}, respectively, if Bob or Charlie tell her to do so. This changes the GHZ state similar to

eq. (7.15) and (7.16) above into a superposition of GHZ states. Hence, she obtains a GHZ state corresponding to Bob's and Charlie's secrets only half of the time. Following our example where only Bob used the Hadamard operation as described in eq. (8.26) we see after a little calculation that for Charlie's result $|\Phi^-\rangle_{5E_6}$ the state of the remaining qubits is

$$\frac{1}{\sqrt{2}}\Big(|P_{00}^+\rangle_{1E_{10}E_{11}}|\chi^+\rangle_{E_3E_4}|\Phi^-\rangle_{E_7E_8} + |P_{10}^-\rangle_{1E_{10}E_{11}}|\omega^-\rangle_{E_3E_4}|\Phi^-\rangle_{E_7E_8}\Big) \tag{8.29}$$

after Alice's application of the Hadamard operation on qubit E_{10}. Alice's measurement on qubits 1, E_{10} and E_{11} projects qubits E_3E_4 in Eve's possession into one of the two possible states. In case Alice obtains $|P_{10}^-\rangle$, which is the expected result for this combination, Eve's Hadamard operation turns $|\omega^-\rangle$ into $|\Phi^-\rangle$. In this case her result gives Eve no information about Bob's secret. Nevertheless, taking, for example, $|\Phi^+\rangle_{4E_2}$ as Bob's result and assuming Alice obtains $|P_{00}^-\rangle$ Eve's measurement always yields the perfectly correlated result $|\Phi^+\rangle_{E_3E_4}$ and thus gives her full information about Bob's state.

Further, if both parties applied the Hadamard operation, it is given in eq. (8.28) that the GHZ state in Alice's possession is either $|P_{00}^+\rangle$, $|P_{01}^-\rangle$, $|P_{10}^-\rangle$ or $|P_{11}^+\rangle$. Alice's application of the Hadamard operation on both qubit E_{10} and E_{11} alters these states accordingly into

$$\begin{aligned}
H^{(2)}H^{(3)}|P_{00}^+\rangle &= \frac{1}{2}\big(|P_{00}^+\rangle + |P_{01}^-\rangle + |P_{10}^-\rangle + |P_{11}^+\rangle\big)\\
H^{(2)}H^{(3)}|P_{01}^-\rangle &= \frac{1}{2}\big(|P_{00}^+\rangle - |P_{01}^-\rangle + |P_{10}^-\rangle - |P_{11}^+\rangle\big)\\
H^{(2)}H^{(3)}|P_{10}^-\rangle &= \frac{1}{2}\big(|P_{00}^+\rangle + |P_{01}^-\rangle - |P_{10}^-\rangle - |P_{11}^+\rangle\big)\\
H^{(2)}H^{(3)}|P_{11}^+\rangle &= \frac{1}{2}\big(|P_{00}^+\rangle - |P_{01}^-\rangle - |P_{10}^-\rangle + |P_{11}^+\rangle\big).
\end{aligned} \tag{8.30}$$

For each of these resulting superpositions of GHZ states Alice's probability to obtain $|P_{10}^-\rangle$ is only 1/4 due to the fact that the two Hadamard operations alter the initial GHZ states massively. Consequently, whenever Alice obtains a result corresponding to Bob's and Charlie's secret Eve has full information about Bob's and Charlie's respective secrets only with probability 1/4. Otherwise, she can not infer any information from her measurement results .

Taking all considerations into account this leads to an expected error probability for all four possible choices of Hadamard operations

$$\big\langle P_e\big\rangle = \frac{1}{4}\times 0 + \frac{1}{4}\times\frac{1}{2} + \frac{1}{4}\times\frac{1}{2} + \frac{1}{4}\times\frac{3}{4} = \frac{7}{16} \tag{8.31}$$

which is equal to the expected error probability of the ZLG attack (cf. eq. (7.19)). Accordingly, the expected collision probability is also equal to the one in the ZLG attack (cf. eq. (7.20)), i.e.

$$\langle P_c \rangle = \frac{7}{8} \tag{8.32}$$

due to the same reasons already discussed above. Hence, also the Shannon entropy is $H(S|M) = 1/4$ such that Eve's information is $I_{AE} = 1 - H(S|M) = 3/4$.

The second scenario dealing with an adversary from the inside, i.e. Charlie, is more important for a QSS protocol. Here, Charlie also prepares the state $|\delta\rangle$ from eq. (8.25) instead of his Bell state and intercepts the qubits coming from Alice and Bob. He performs a GHZ state measurement on A, B and E_9 as well as a Bell state measurement on E_1 and C to entangle himself with Alice and Bob. Then, he forwards qubits E_{10}, E_{11} to Alice and E_2 to Bob and jointly measures his qubits E_5 and E_6. We have to remark that in this case where the adversary comes from the inside qubits E_7 and E_8 of the state $|\delta\rangle$ can be ignored since Charlie is, of course, fully aware of his own secret measurement result. Whenever Bob does not use the Hadamard operation we have already seen that qubits E_3 and E_4 in Charlie's possession are perfectly correlated to Bob's result giving Charlie full information about Bob's result. We already showed that based on the structure of the state $|\delta\rangle$ the three qubits in Alice's possession are always in a GHZ state corresponding to Bob's and Charlie's secret results.

Whenever Bob chooses to use the Hadamard operation the exact state of the remaining qubits is of the form described in eg. (8.26) (if he obtained $|\Psi^+\rangle_{4E_2}$ the remaining qubits are exactly in the state described in that equation). As pointed out above, the best strategy for Charlie is to wait with the measurement of qubits E_3 and E_4 until Bob publicly announces that he applied the Hadamard operation. As we already showed, after Alice's application of the Hadamard operation onto qubit E_{10} the overall state of the remaining qubits is given in eq. (8.29). Therefore, her measurement projects qubits E_3 and E_4 either onto the state $|\omega^-\rangle_{E_3E_4}$ or $|\chi^+\rangle_{E_3E_4}$. In this case Charlie also applies a Hadamard operation on qubit E_3 and measures qubits E_3 and E_4. As already seen above, this measurement yields a result correlated to Bob's result only with probability 1/2. We want to stress that in case Charlie wants to perform a Hadamard operation he has to apply it on qubit E_{11} of his initial state $|\delta\rangle$ to anticipate Alice's Hadamard operation later on and preserve the correlation.

The expected error probability for both cases – Bob using the Hadamard operation or doing nothing – is then

$$\langle P_e \rangle = \frac{1}{2} \times 0 + \frac{1}{2} \times \frac{1}{2} = \frac{1}{4} \tag{8.33}$$

and the expected collision probability is

$$\langle P_c \rangle = 1 \tag{8.34}$$

Again, these are the same results as for the ZLG attack (cf. eq. (7.22) and (7.23) above). Following the same argumentation as in section 7.1.2 Eve's information about Alice's secret key is

$$I_{AE} = 1 - H\big(S|M\big) = 1 \tag{8.35}$$

because $H(S|M) = 0$ as already discussed above. Due to the fact that Charlie has full information about Bob's result, too, when he applies the simulation attack he has the opportunity to reduce the error rate to 0. Based on his measurement results Charlie is always able to tell whether Bob's and his result describe a valid combination together with Alice's secret and public result. This is trivial whenever Bob chooses not to use the Hadamard operation because in this case Alice, Bob and Charlie always obtain correlated results due to the special property of the state $|\delta\rangle$ described in eq. (8.25). Alternatively, if Bob applies the Hadamard operation we see immediately that all three parties obtain correlated results whenever Charlie obtains $|\Phi^{\pm}\rangle_{E_3E_4}$. During the error estimation phase Charlie knows Alice's public result and is able to infer Alice's and Bob's secret result based on his measurement outcomes. Looking at the valid correlations (e.g. table 7.3) Charlie figures out which state he has to announce such that no error is detected.

To give an example we assume that Alice obtains $|\Phi^+\rangle_{23}$ as her secret result and Bob as well as Charlie obtain $|\Psi^+\rangle_{4E_2}$ and $|\Psi^+\rangle_{E_5E_6}$, respectively, as their secret results. Further we assume that Bob applied the Hadamard operation and therefore Alice's public GHZ state is $|P_{01}^-\rangle_{1E_{10}E_{11}}$. From table 7.3 we see that the GHZ state does not correlate to the secret results of Alice, Bob and Charlie. As pointed out in the previous paragraph, Charlie is aware of that fact before Alice and Bob check for errors. Therefore, Charlie checks table 7.3 and recognizes that $|\Phi^-\rangle$ is the expected result. Thus, when Alice asks Bob and Charlie for their results, Charlie announces $|\Phi^-\rangle$ instead of his original result and Alice and Bob do not detect any error.

Following this argumentation we can conclude that the simulation attack is much more effective on this protocol than the ZLG attack. Although both attack strategies provide a dishonest party with the full information about Alice's secret Charlie is able to stay completely undetected when using the simulation attack due to the additional information he obtains.

Chapter 9

Security in Noisy Environments

The protocols discussed in the previous chapter are all settled in a perfect environment. The main reason for this is that most of the quantum cryptographic protocols based on multiple qubits have not been implemented due to physical limitations and thus their security has not been evaluated in a realistic environment.

In this chapter we are going to look at the security of the protocols discussed in chapter 7 in connection with a noisy quantum channel. Based on the model of a depolarizing channel introduced in chapter 8 the effect of the noise onto the basic building block of the discussed protocols – the entanglement swapping – is described. Further, threshold values on the fidelity of the entanglement are given above which a secure communication is possible.

9.1 The Noisy Channel Model

9.1.1 Depolarizing Channels and Werner States

The most common way to characterize a noisy quantum channel is to use the *depolarizing channel* [15, 54] described in section 4.1. This model takes the bit flip and phase flip errors on the qubit in transit into account and is described by the application of all three Pauli operations σ_x, σ_y and σ_z. If the qubit transmitted over the noisy channel is part of an entangled state the whole system is affected by the noisy channel. In case of a Bell state, e.g. $|\Phi^+\rangle$, the system of the two qubits after the the effect of the depolarizing channel can be described by a Werner state

$$W_F = \mathrm{F}|\Phi^+\rangle\langle\Phi^+| + \frac{1-\mathrm{F}}{3}\Big(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|\Big) \qquad (9.1)$$

with fidelity $\langle\Phi^+|W_F|\Phi^+\rangle = F$. A more common way to look at the Werner state is to describe it in connection with white noise, i.e.

$$\rho = p|\Phi^+\rangle\langle\Phi^+| + (1-p)\frac{\mathbb{1}}{4} \tag{9.2}$$

where p is the probability that the state $|\Phi^+\rangle\langle\Phi^+|$ is transmitted perfectly over the noisy channel (cf. also eq. (4.25) and eq. (4.26)). In this case the fidelity can be easily computed as $\mathrm{F} = (1+3p)/4$.

As a consequence of the transmission of qubits over a noisy channel the operations on that qubits are affected, too. In the protocols already discussed the most interesting operation is entanglement swapping. Following our previous discussions of entanglement swapping in section 2.5.3 we assume Alice prepares the Bell state $|\Phi^+\rangle\langle\Phi^+|_{12}$ and Bob prepares $|\Phi^+\rangle\langle\Phi^+|_{34}$ in their respective laboratories. They send qubits 2 and 3 to the other party over a depolarizing channel such that the overall system is described by $W_F \otimes W_F$. After Alice's Bell state measurement on qubits 1 and 3 in her possession the system of qubits 2 and 4 is (assuming Alice obtains $|\Phi^+\rangle\langle\Phi^+|_{13}$)

$$\begin{aligned}\rho_{24} =& \frac{4\mathrm{F}^2 - 2\mathrm{F} + 1}{3}|\Phi^+\rangle\langle\Phi^+|_{24} \\ &+ \frac{2\mathrm{F} - 4\mathrm{F}^2 + 2}{9}\Big(|\Phi^-\rangle\langle\Phi^-| + |\Psi^+\rangle\langle\Psi^+| + |\Psi^-\rangle\langle\Psi^-|\Big)_{24}\end{aligned} \tag{9.3}$$

which is again a Werner state. Comparing this equation with eq. (2.41) describing entanglement swapping with pure states we directly see that Alice and Bob obtain correlated results only with probability

$$P_{corr} = \frac{1 - 2\mathrm{F} + 4\mathrm{F}^2}{3} = \frac{1+3p^2}{4} \tag{9.4}$$

since $\mathrm{F} = (1+3p)/4$. Bob's measurement yields an arbitrary state not correlated to Alice's measurement with probability

$$P_{err} = \frac{2 + 2\mathrm{F} - 4\mathrm{F}^2}{3} = \frac{3(1-p^2)}{4} \tag{9.5}$$

For QKD protocols based on entanglement swapping this means that an error occurs in the communication between Alice and Bob as described in the protocols in section 9.2 below. Considering figure 9.1 we see that performing entanglement swapping over a noisy channel gives reasonable results, i.e. it is more likely to obtain correlated

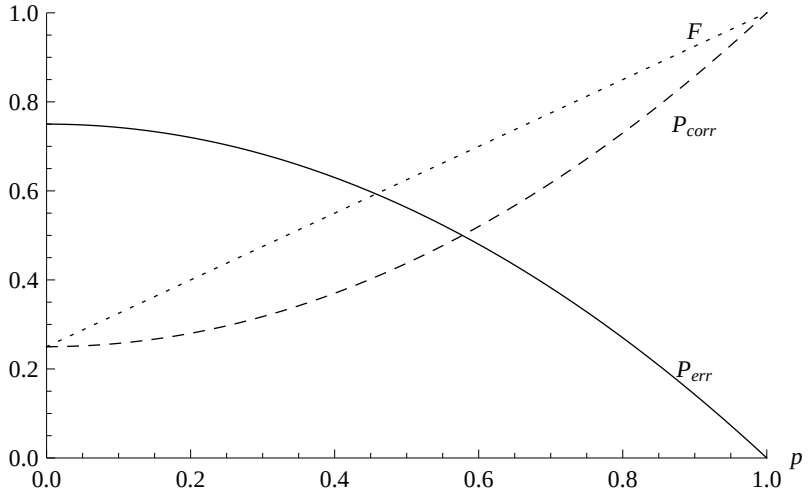

Figure 9.1: *(Noisy Channels)* The probabilities P_{corr} (dashed line) and P_{err} (solid line) from entanglement swapping in a setting with noisy channels.

results than uncorrelated, only if $p > 1/\sqrt{3}$ which corresponds to a fidelity of the initial states of $F = 0.683$.

As we have already seen there are many protocols using multi-qubit entanglement to connect three or more parties. If one or several qubits of such a multi-qubit entangled state are transmitted over a depolarizing channel the overall state is also tempered by the effect of noise. Looking, for example, at the GHZ state $|P_{00}^{+}\rangle\langle P_{00}^{+}|_{123}$, sending only qubit 1 over the depolarizing channel the state changes into

$$\begin{aligned}\vartheta_{123} &= \frac{1+3p}{4}|P_{00}^{+}\rangle\langle P_{00}^{+}| + \frac{1-p}{4}\Big(\sigma_x^{(1)}|P_{00}^{+}\rangle\langle P_{00}^{+}|\sigma_x^{(1)} \\ &\qquad + \sigma_y^{(1)}|P_{00}^{+}\rangle\langle P_{00}^{+}|\sigma_y^{(1)} + \sigma_z^{(1)}|P_{00}^{+}\rangle\langle P_{00}^{+}|\sigma_z^{(1)}\Big) \qquad (9.6) \\ &= \frac{1+3p}{4}|P_{00}^{+}\rangle\langle P_{00}^{+}| + \frac{1-p}{4}\Big(|P_{00}^{-}\rangle\langle P_{00}^{-}| + |P_{11}^{+}\rangle\langle P_{11}^{+}| - |P_{11}^{-}\rangle\langle P_{11}^{-}|\Big)\end{aligned}$$

Since the noise of the polarizing channel affects only one qubit of the GHZ state the resulting state is not a mixture of all 8 GHZ states possible but only of four states $|P_{00}^{\pm}\rangle\langle P_{00}^{\pm}|$ and $|P_{11}^{\pm}\rangle\langle P_{11}^{\pm}|$. Similarly, if only qubit 2 or qubit 3 is sent over the noisy channel the resulting state is a mixture of the states $|P_{00}^{\pm}\rangle\langle P_{00}^{\pm}|$ and $|P_{10}^{\pm}\rangle\langle P_{10}^{\pm}|$ as well as $|P_{00}^{\pm}\rangle\langle P_{00}^{\pm}|$ and $|P_{01}^{\pm}\rangle\langle P_{01}^{\pm}|$, respectively. Nevertheless, the resulting state has a fidelity $\mathrm{F} = \langle P_{00}^{+}|\vartheta|P_{00}^{+}\rangle = (1+3p)/4$, i.e. the probability to obtain the original state after the transmission of the qubit is $(1+3p)/4$ and the other 3 states are equally probable. If a second qubit, e.g qubit 2, is going through the depolarizing channel

the overall state of the three qubits changes to

$$\begin{aligned}\vartheta'_{123} =&\frac{1+3p}{4}\vartheta_{123} + \frac{1-p}{4}\left(\sigma_x^{(2)}\vartheta_{123}\sigma_x^{(2)} + \sigma_y^{(2)}\vartheta_{123}\sigma_y^{(2)} + \sigma_z^{(2)}\vartheta_{123}\sigma_z^{(2)}\right)\\ =&\frac{1+2p+5p^2}{8}|P_{00}^+\rangle\langle P_{00}^+| + \frac{1+2p-3p^2}{8}|P_{00}^-\rangle\langle P_{00}^-|\\ &+\frac{(1-p)^2}{8}|P_{01}^+\rangle\langle P_{01}^+| + \frac{(1-p)^2}{8}|P_{01}^-\rangle\langle P_{01}^-|\\ &+\frac{1-p^2}{8}|P_{10}^+\rangle\langle P_{10}^+| + \frac{1-p^2}{8}|P_{10}^-\rangle\langle P_{10}^-|\\ &+\frac{1-p^2}{8}|P_{11}^+\rangle\langle P_{11}^+| + \frac{1-p^2}{8}|P_{11}^-\rangle\langle P_{11}^-|\end{aligned} \tag{9.7}$$

In this case the resulting state is a mixture of all possible GHZ states but of a different form compared to the state in eq. (9.6). The terms not equal to the initial state $|P_{00}^+\rangle\langle P_{00}^+|$ are not equally probable any more as it is the case in eq. (9.6) above. In detail, the original state $|P_{00}^+\rangle\langle P_{00}^+|$ still has the highest probability with $P_{|P_{00}^+\rangle} = (1+2p+5p^2)/8$. Next, the state $|P_{00}^-\rangle\langle P_{00}^-|$, which differs only by a σ_z operation from the original state, occurs with probability $P_{|P_{00}^-\rangle} = (1+2p-3p^2)/8$. The remaining states have the probability $P_{|P_{01}^\pm\rangle} = (1-p)^2/8$ and $P_{|P_{10}^\pm\rangle} = P_{|P_{11}^\pm\rangle} = (1-p^2)/8$. Since the source of a GHZ state or any multi-qubit state is usually located in the laboratory of one of the communication parties it is sufficient to just look at the scenarios where one or two qubits are transmitted over a noisy channel. For the sake of completeness we will shortly describe how the GHZ state changes if all three qubits are affected by noise. The state ϑ'_{123} changes into

$$\begin{aligned}\rho_{123} =&\frac{1+3p}{4}\vartheta'_{123} + \frac{1-p}{4}\left(\sigma_x^{(3)}\vartheta'_{123}\sigma_x^{(3)} + \sigma_y^{(3)}\vartheta'_{123}\sigma_y^{(3)} + \sigma_z^{(3)}\vartheta'_{123}\sigma_z^{(3)}\right)\\ =&\frac{1+3p^2+4p^3}{8}|P_{00}^+\rangle\langle P_{00}^+| + \frac{1+3p^2-4p^3}{8}|P_{00}^-\rangle\langle P_{00}^-|\\ &+\frac{1-p^2}{8}|P_{01}^+\rangle\langle P_{01}^+| + \frac{1-p^2}{8}|P_{01}^-\rangle\langle P_{01}^-|\\ &+\frac{1-p^2}{8}|P_{10}^+\rangle\langle P_{10}^+| + \frac{1-p^2}{8}|P_{10}^-\rangle\langle P_{10}^-|\\ &+\frac{1-p^2}{8}|P_{11}^+\rangle\langle P_{11}^+| + \frac{1-p^2}{8}|P_{11}^-\rangle\langle P_{11}^-|\end{aligned} \tag{9.8}$$

if also qubit 3 is sent over a depolarizing channel. This state is already rather close to a Werner form but, as it is shown in eq. (9.8), only the states $|P_{01}^\pm\rangle\langle P_{01}^\pm|$, $|P_{10}^\pm\rangle\langle P_{10}^\pm|$ and $|P_{11}^\pm\rangle\langle P_{11}^\pm|$ occur with the same probability, i.e.

$$P_{|P_{01}^\pm\rangle} = P_{|P_{10}^\pm\rangle} = P_{|P_{11}^\pm\rangle} = \frac{1-p^2}{8} \tag{9.9}$$

The state $|P_{00}^-\rangle\langle P_{00}^-|$ has a probability of $P_{|P_{00}^-\rangle} = (1+3p^2-4p^3)/8$ and the probability to obtain the original state is $P_{|P_{00}^+\rangle} = (1+3p^2+4p^3)/8$.

In some protocols entanglement swapping not only between Bell states but also between Bell states and GHZ states is used to distribute information between several parties (cf. for example [26]). We assume Alice prepares the Bell state $|\Phi^+\rangle\langle\Phi^+|_{12}$ and Bob the GHZ state $|P_{00}^+\rangle\langle P_{00}^+|_{345}$ and they exchange qubits 2 and 3 over a depolarizing channel. This changes the initial states into ρ_{12} and ϑ_{345} as defined in the previous paragraphs. If we further assume that Alice obtains $|\Phi^+\rangle\langle\Phi^+|_{13}$ from her measurement the state of Bob's qubits after the entanglement swapping is then described as

$$\begin{aligned}\rho_{245} =& \frac{1+3p^2}{4}|P_{00}^+\rangle\langle P_{00}^+|_{245} \\ &+\frac{1-p^2}{4}\Big(|P_{00}^-\rangle\langle P_{00}^-|_{245}+|P_{11}^+\rangle\langle P_{11}^+|_{245}+|P_{11}^-\rangle\langle P_{11}^-|_{245}\Big)\end{aligned} \tag{9.10}$$

and similarly for Alice's other possible results. Hence, Bob obtains a correlated result with probability

$$P_{corr} = \frac{1+3p^2}{4} \tag{9.11}$$

and his measurement yields an arbitrary state not correlated to Alice's measurement with probability

$$P_{err} = \frac{3(1-p^2)}{4} \tag{9.12}$$

as it is the case for entanglement swapping with two Bell states (cf. eq. (9.4) and eq. (9.5) above). Looking at the case where two qubits of the GHZ state are sent over a depolarizing channel (e.g. to two different parties) and the entanglement swapping is performed afterwards Bob's probability to obtain correlated results becomes smaller since the GHZ state is more affected by the noise. Taking ϑ'_{345} as Bob's initial state and again $|\Phi^+\rangle\langle\Phi^+|_{13}$ as Alice's result the state of Bob's qubits is described as

$$\begin{aligned}\rho_{245} =& \frac{1+p+p^2+5p^3}{8}|P_{00}^+\rangle\langle P_{00}^+|_{245}+\frac{1+p+p^2-3p^3}{8}|P_{00}^-\rangle\langle P_{00}^-|_{245} \\ &+\frac{(1-p)^2(1+p)}{8}|P_{01}^+\rangle\langle P_{01}^+|_{245}+\frac{(1-p)^2(1+p)}{8}|P_{01}^-\rangle\langle P_{01}^-|_{245} \\ &+\frac{1-p+p^2-p^3}{8}|P_{10}^+\rangle\langle P_{10}^+|_{245}+\frac{1-p+p^2-p^3}{8}|P_{10}^-\rangle\langle P_{10}^-|_{245} \\ &+\frac{(1-p)(1+p)^2}{8}|P_{11}^+\rangle\langle P_{11}^+|_{245}+\frac{(1-p)(1+p)^2}{8}|P_{11}^-\rangle\langle P_{11}^-|_{245}\end{aligned} \tag{9.13}$$

In this case Bob obtains a correlated result only with probability

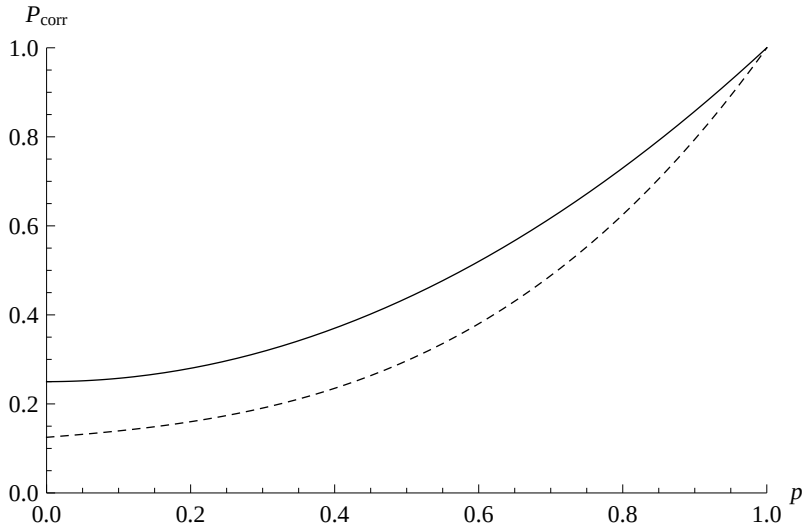

Figure 9.2: *(Correlation Probabilities)* The solid line represents P_{corr} for the scenario where only one qubit of the GHZ state is tempered (cf. eq. (9.11)) by the quantum channel. The dashed line represents P_{corr} for the scenario where two qubits of the GHZ state are transmitted over the quantum channel (cf. eq. (9.14)).

$$P_{corr} = \frac{1 + p + p^2 + 5p^3}{8} \tag{9.14}$$

which is much lower compared to the scenario where only one qubit of the GHZ state is sent over the noisy channel (cf. figure 9.2). Additionally, instead of just 4 there are 8 possible outcomes for Bob's measurement. These two facts together result in a much higher probability P_{err} for Alice and Bob to obtain an error during their measurements (cf. figure 9.3), i.e

$$P_{err} = \frac{7 - p - p^2 - 5p^3}{8} \tag{9.15}$$

9.1.2 Adaption of the Attack Strategy

To guarantee perfect security in quantum cryptography all noise – introduced naturally or by an adversary – is treated as it is caused by an eavesdropping attempt. This leads especially to the rather paranoid but very useful assumption that Eve is able to exchange the noisy channel between Alice and Bob by a perfect quantum channel, i.e. a lossless channel where the polarization and phase are preserved. Hence, Eve can use the error Alice and Bob expect to come from their noisy channel to disguise

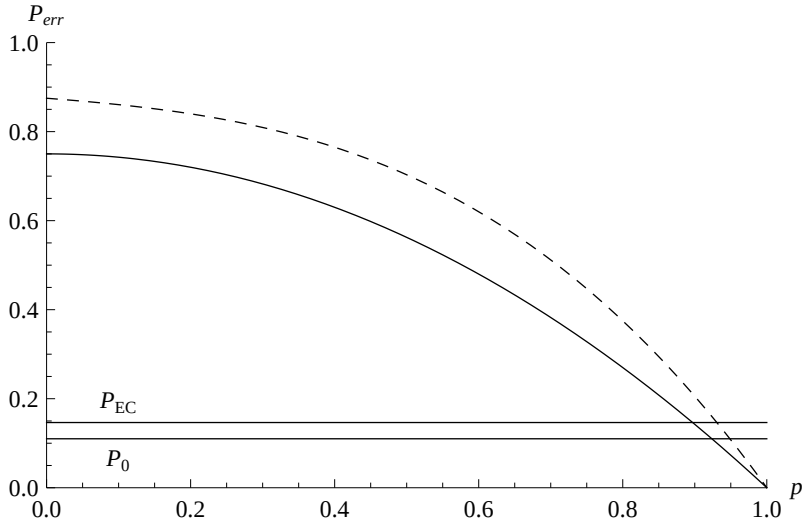

Figure 9.3: *(Error Probabilities)* The solid line represents P_{err} for the scenario where only one qubit of the GHZ state is tempered by the quantum channel (cf. eq. (9.12)). The dashed line represents P_{err} for the scenario where two qubits of the GHZ state are transmitted over the quantum channel (cf. eq. (9.15)).

her eavesdropping attempt. Such an premise is useful when dealing with the security of a protocol since no assumptions about Eve's hardware or computational power is made. As already pointed out in section 6.2.2, regarding physical implementations of QKD protocols it is also assumed that Eve is able to control characteristics of Bob's hardware like the detector efficiency, which is even a stronger assumption [126]. Since we are just dealing with a theoretical model of the noisy quantum channel we can neglect the errors coming from the physical implementations.

The first direct consequence for Alice and Bob when using noisy channels is that they can not allow an error rate larger than the error usually introduced by an adversary. For example, as we have seen in sections 6.2, 6.3, 7.1 and chapter 8 in most of the protocols the error rate due to Eve's intervention is 25%. If the natural error caused by the depolarizing channel is equal or larger than 25% Alice and Bob will not detected Eve's presence. From eq. (9.5) we know that Alice and Bob expect an error rate $P_{err} = 3(1-p^2)/4$ from entanglement swapping in a noisy channel such that at least $p > 0.8165$. This means, for a fidelity of the initial states $\mathrm{F} > 0.8624$ the natural error introduced by the noisy channel is always smaller than 25%, i.e. the error introduced by Eve.

As discussed in detail in the following paragraphs Eve has the opportunity to

attack only a fraction of all qubits in transit between Alice and Bob. This reduces the error rate coming from her intervention but leaves Eve also with a smaller amount of information about the sifted key. To react on this threat Alice and Bob perform error correction and privacy amplification. A basic idea on how these two building blocks of quantum cryptography work and which methods are involved therein has already been given in section 5.2.3. We just want to stress once more that using these two primitives Eve's information about the key can be reduced to an arbitrary small amount. Furthermore, as pointed out in section 5.2.3 to successfully perform error correction and privacy amplification based on one-way classical communication for BB84-like protocols a maximal error rate of

$$P_{EC} = \frac{1 - \frac{1}{\sqrt{2}}}{2} \simeq 0.1465 \tag{9.16}$$

is possible [126]. Since the error correction still leaks some information to an adversary the upper bound on the error rate actually used in such protocols is $\simeq 0.11$ [135, 87]. Therefore, we define lower bounds on the fidelity of the initial states for these two thresholds of the error rate.

Considering again entanglement swapping in a noisy channel, we get the corresponding lower bounds on p and F for an error rate of 0.1465 using eq. (9.5) from above (cf. also figure 9.3)

$$p_{EC} \simeq 0.8971 \qquad \mathrm{F}_{EC} \simeq 0.9228. \tag{9.17}$$

As we can see the fidelity of the initial states has to be over 92% to make one-way error correction. The final bounds p_0 and F_0 are then

$$p_0 \simeq 0.9238 \qquad \mathrm{F}_0 \simeq 0.9428. \tag{9.18}$$

i.e. the fidelity has to be an additional 2% higher compared to eq. (9.17) to achieve the maximal tolerable error rate of $\simeq 11\%$.

In the previous section not only entanglement swapping between two Bell states has been discussed but also between a Bell state and a GHZ state and it has been shown that the error rate increases in the latter case. In this context, two main scenarios are considered where one or two qubits of the GHZ state are tempered by the noisy channel. If one qubit is subject to noise we already showed in eq. (9.12) that the error rate is the same as for the entanglement swapping between two Bell states. If two qubits are affected by the noisy channel the error probability is higher

(cf. figure 9.3 and eq. (9.15) above) such that at least $p > 0.8757$ and $\mathrm{F} > 0.8912$ to achieve an error rate less than 0.25. The more interesting lower bounds are then

$$p_{EC} \simeq 0.9307 \qquad \mathrm{F}_{EC} \simeq 0.9394 \tag{9.19}$$

and

$$p_0 \simeq 0.9488 \qquad \mathrm{F}_0 \simeq 0.9552 \tag{9.20}$$

which do not differ that much from eq. (9.17) and eq. (9.18). Nevertheless, the thresholds from eq. (9.17) to (9.20) make high demands on the fidelity of the quantum channel.

Eve herself is well aware of the fidelity F of the noisy channel and the thresholds for security based on that fidelity. Her strategy is, as already mentioned, to replace the noisy channel by a perfect one and to introduce just as much error from her attack as expected by Alice and Bob. We discussed in the previous paragraphs that Alice and Bob ideally just accept a noisy channel with a fidelity $\mathrm{F} > \mathrm{F}_0$ to make sure that Eve is not able to gain too much information from her eavesdropping attempt. Therefore, Eve's approach is to attack only a fraction q of the qubits coming from Alice to stay beneath the threshold of the legitimate parties. In general, this means if Eve attacks each qubit she introduces on average an error rate of 0.25. Depending on the error P_{err} Alice and Bob are going to accept due to the noisy channel Eve attacks only the fraction $q = P_{err}/0.25 = 4P_{err}$. Going back to the scenario where Alice and Bob perform an entanglement swapping over the noisy channel Eve's fraction q is defined as

$$q = 4P_{err} = 4\,\frac{3(1-p^2)}{4} = 3\big(1-p^2\big) = \frac{8(1+\mathrm{F}-2\mathrm{F}^2)}{3} \tag{9.21}$$

using P_{err} from eq. (9.5) above. Consequently, for $\mathrm{F} = \mathrm{F}_{EC}$ – the minimal requirement for error correction – $q = 0.5858$, and for the more rigorous bound $\mathrm{F} = \mathrm{F}_0$ Eve's fraction $q = 0.44$. This means, if Eve attacks 58.58% of the qubits in transit between Alice and Bob error correction is still possible. Further, if she eavesdrops on 44% of the qubits her presence is not detected at all. Nevertheless, Eve can not gain anything from this result, because, as pointed out above, for an error rate of $\simeq$ 11% or lower Alice and Bob are able to reduce Eve's information on the final secret key to less than one bit using privacy amplification.

Looking at the other scenarios where the legitimate communication parties perform entanglement swapping between a Bell state and a GHZ state Eve's fraction q

is defined as

$$q = 4\,\frac{7-p-p^2-5p^3}{8} = \frac{7-p-p^2-5p^3}{2} = \frac{8(153-25\mathrm{F}+32\mathrm{F}^2-160\mathrm{F}^3)}{343} \tag{9.22}$$

if two qubits of the GHZ state are affected (as for example in the QSS protocol by Cabello [26]). This alternative definition of q does not change the exact values of q for F_{EC} and F_0, which are again 0.5858 and 0.44, respectively, since the lower bounds F_{EC} and F_0 on the fidelity are higher (as described in eq. (9.19) and eq. (9.20) above).

9.2 Multi-Qubit Protocols in a Noisy Environment

In the following paragraphs we want to review the security of the protocols discussed in sections 8.1 - 8.4 in connection with noisy channels. Therefore, the threshold values F_{EC} and F_0 for the fidelity of the initial states are computed for each protocol. Further, we compare the information I_{AE} Eve has on the sifted key with the results coming from sections 8.1 - 8.4.

9.2.1 The QKD Protocol by Li et al.

Li et al. presented a protocol where they used Pauli operations to obtain two additional raw key bits per round [91]. As we have shown in section 8.1 this protocol in its original version is open to the simulation attack. In the revised version Alice randomly applies a Hadamard operation on qubit 1 additionally to the Pauli operation.

The noisy channel between Alice and Bob changes the initial states $|\Phi^+\rangle_{12}$ and $|\Phi^+\rangle_{34}$ to the Werner states

$$\begin{aligned}\rho_{12} &= p|\Phi^+\rangle\langle\Phi^+| + \big(1-p\big)\mathbb{1}\\ \rho_{34} &= p|\Phi^+\rangle\langle\Phi^+| + \big(1-p\big)\mathbb{1}\end{aligned} \tag{9.23}$$

After the application of Alice's secret Pauli operation in qubit 1 – we assume that Alice chooses the σ_x operation to be consistent with section 8.1 – the state ρ_{12} changes to

$$\rho_{12} = p|\Psi^+\rangle\langle\Psi^+| + \big(1-p\big)\mathbb{1}. \tag{9.24}$$

When Alice performs her Bell state measurement she obtains one of the four Bell states with equal probability, e.g. $|\Psi^-\rangle_{13}$, but leaves the qubits 2 and 4 in Bob's laboratory in the state

$$\begin{aligned}&\frac{1}{4}\big(1+p^2\big)|00\rangle\langle 00| - \frac{p^2}{2}|00\rangle\langle 11| + \frac{1}{4}\big(1-p^2\big)|01\rangle\langle 01| \\ +&\frac{1}{4}\big(1-p^2\big)|10\rangle\langle 10| - \frac{p^2}{2}|11\rangle\langle 00| + \frac{1}{4}\big(1+p^2\big)|11\rangle\langle 11|.\end{aligned} \tag{9.25}$$

When looking at eq. (9.4) from the previous section we see that Bob obtains the correlated result $|\Phi^-\rangle_{24}$ only with probability $(1+3p^2)/4$. Thus, Bob obtains an uncorrelated result with probability $3(1-p^2)/4$ which he later on identifies as error. Hence, Alice and Bob have to be aware of this natural error rate and take it into account when checking for eavesdroppers.

The application of the Hadamard operation does not affect the error rate caused by the noisy quantum channel. Looking at the initial state ρ_{12} the application of the Hadamard operation on qubit 1 changes it into

$$H\rho_{12}H^\dagger = p|\omega^+\rangle\langle\omega^+| + \big(1-p\big)\mathbb{1}. \tag{9.26}$$

Due to entanglement swapping the H operation is swapped onto qubit 2 after Alice's measurement and its effect is reversed by Bob's application of H onto qubit 2. Hence, Bob's qubits 2 and 4 are again in the state described in eq. (9.25) and Bob obtains a correlated result with probability $(1+3p^2)/4$.

In section 8.1 we already showed that the protocol in its original version is open to the simulation attack and in the revised version an eavesdropper introduces an error rate of 1/4. Taking the noisy channel into account Alice and Bob need a fidelity of at least $\mathrm{F}_{EC} = 0.9228$ to guarantee privacy amplification and $\mathrm{F}_0 = 0.9428$ to achieve not more than 11% of natural error. As already discussed Eve attacks 58.58% and 44% of the qubits in transit, respectively, to stay undetected. Hence, her information about the secret decreases from 1/2 if she attacks each qubit (cf. eq. (8.7)) to $I_{AE} = 0.2929$ and $I_{AE} = 0.22$, respectively.

9.2.2 The QKD Protocol by Song

In the protocol presented by Song [138] Alice and Bob use a basis transformation T to secure the protocol. As already pointed out in section 8.2 T is a basis transformation of $2\pi/3$ around the X-axis and maps the Bell states $|\Phi^\pm\rangle$, $|\Psi^\pm\rangle$ onto the states $|\eta^\pm\rangle$,

$|\nu^{\pm}\rangle$ (cf. eq. (8.10)). The application of the transformation is chosen at random by Alice and Bob which is the main argument for the security of the protocol.

At first, we will look at the scenario, where Alice and Bob do not apply T onto their respective qubits. In this case the initial states $|\Phi^-\rangle_{12}$ and $|\Psi^+\rangle_{34}$ change into

$$\begin{aligned} \rho_{12} &= p|\Phi^-\rangle\langle\Phi^-| + \big(1-p\big)\mathbb{1} \\ \rho_{34} &= p|\Psi^+\rangle\langle\Psi^+| + \big(1-p\big)\mathbb{1} \end{aligned} \tag{9.27}$$

after going through the noisy channel. Assuming the result of her Bell state measurement is $|\Phi^-\rangle_{13}$ this leaves the qubits 2 and 4 at Bob's side in the state

$$\begin{aligned} &\frac{1}{4}\big(1-p^2\big)|00\rangle\langle 00| + \frac{1}{4}\big(1+p^2\big)|01\rangle\langle 01| + \frac{p^2}{2}|01\rangle\langle 10| \\ &+\frac{p^2}{2}|10\rangle\langle 01| + \frac{1}{4}\big(1+p^2\big)|10\rangle\langle 10| + \frac{1}{4}\big(1-p^2\big)|11\rangle\langle 11| \end{aligned} \tag{9.28}$$

Hence, when Bob performs his Bell state measurement on qubits 2 and 4 he obtains the correlated result $|\Psi^+\rangle_{24}$ with probability $P_{corr} = (1+3p^2)/4$ coming from eq. (9.4). Accordingly, the overall error probability is $P_{err} = 3(1-p^2)/4$ (cf. eq. (9.5)).

The random application of the basis transformation T does not effect the error probability P_{err} but nevertheless is crucial when dealing with an eavesdropper as we have already discussed in section 8.2. The transformation T applied on qubit 2 or 4, respectively, changes the initial states into $|\eta^-\rangle_{12}$ and $|\nu^+\rangle_{34}$ which leads to the states

$$\begin{aligned} T\rho_{12}T^{-1} &= p|\eta^-\rangle\langle\eta^-| + \big(1-p\big)\mathbb{1} \\ T\rho_{34}T^{-1} &= p|\nu^+\rangle\langle\nu^+| + \big(1-p\big)\mathbb{1} \end{aligned} \tag{9.29}$$

after qubits 2 and 4 are transmitted over the noisy channel. Since Alice and Bob announce whether they used the transformation T or not before their respective Bell state measurements they are able to reverse the effect of the transformation, i.e.

$$\begin{aligned} T^{-1}\big(T\rho_{12}T^{-1}\big)T &= \rho_{12} \\ T^{-1}\big(T\rho_{34}T^{-1}\big)T &= \rho_{34}. \end{aligned} \tag{9.30}$$

Therefore, Alice and Bob use the same states as described above in their Bell state measurements which leads to the same error probability P_{err}.

From the security analysis in section 8.2 we know that the protocol becomes completely insecure if the error rate is larger than 3/16. In this case Eve is able to obtain full information about the secret key using the simulation attack strategy. Hence, we can calculate that in this case $p \simeq 0.8660$ which leads to a lower bound

on fidelity $F > 0.8995$. Nevertheless, $3/16 > 0.1465$ such that F_{EC} and F_0 from eq. (9.17) and eq. (9.18) are the important lower bounds. Due to the fact that Eve introduces only an error of 3/16 in a perfect setup the fraction q of the qubits she can attack is defined as

$$q = \frac{32(1 + \mathrm{F} - 2\mathrm{F}^2)}{9}. \tag{9.31}$$

Thus, Eve is able to attack a fraction of $q \simeq 0.7810$ while introducing an error of $\simeq 0.1465$ and $q \simeq 0.58.67$ while introducing an error of $\simeq 0.11$, respectively, which is much higher than compared to the protocol by Li et al. described in the previous section. Accordingly, Eve's information about the secret decreases from 0.594 (cf. 8.12) to $I_{AE} \simeq 0.4639$ and $I_{AE} \simeq 0.3485$ for her fractions $q = 0.7810$ and $q = 0.5867$, respectively. Hence, Eve has a big advantage compared, for example, to the BB84 protocol due to the unbiased basis transformation T.

Regarding the revised version of the protocol we suggested in section 8.2 the Hadamard operation H is used instead of the transformation T to reduce Eve's chance to stay undetected. As pointed out, Eve introduces the usual error rate of 1/4 which gives the same lower bounds F_{EC} and F_0 as in the original protocol. Due to the higher error rate Eve's fraction q and her information about the secret is much lower compared to the original protocol, i.e. $I_{AE} = 0.2929$ and $I_{AE} = 0.22$ for $q \simeq 0.5858$ and $q \simeq 0.44$, respectively.

9.2.3 The Cabello QKD Protocol

In the revised version of Cabello's QKD protocol [28] Alice also uses a random application of the Hadamard operation to counter Eve's eavesdropping attempt. As described in section 8.3 they use three entangled qubit pairs instead of two as in the QKD protocols by Li et al. and Song, respectively.

When Alice and Bob exchange their qubits 2 and 6 the initial states $|\Phi^-\rangle_{12}$ and $|\Phi^+\rangle_{46}$ change into

$$\begin{aligned} \rho_{12} &= p|\Phi^-\rangle\langle\Phi^-| + \big(1-p\big)\mathbb{1} \\ \rho_{46} &= p|\Phi^+\rangle\langle\Psi^+| + \big(1-p\big)\mathbb{1} \end{aligned} \tag{9.32}$$

due to the noisy channel. In case Alice does not apply the H operation onto qubit 3 her Bell state measurement on qubits 2 and 3 of ρ_{12} and $\rho_{35} = |\Phi^+\rangle\langle\Phi^+|$ leaves

the remaining 2 qubits in the state

$$\begin{aligned}&\frac{1}{4}\big(1-p\big)|00\rangle\langle 00| + \frac{1}{4}\big(1+p\big)|01\rangle\langle 01| + \frac{p}{2}|01\rangle\langle 10| \\ +&\frac{p}{2}|10\rangle\langle 01| + \frac{1}{4}\big(1+p\big)|10\rangle\langle 10| + \frac{1}{4}\big(1-p\big)|11\rangle\langle 11|\end{aligned} \tag{9.33}$$

if Alice's result is $|\Psi^-\rangle_{23}$. Next, she measures qubits 5 and 6 to obtain her public result. Assuming she obtains $|\Psi^+\rangle$ qubits 2 and 4 at Bob's laboratory are now in the state

$$\begin{aligned}&\frac{1}{4}\big(1+p^2\big)|00\rangle\langle 00| + \frac{p^2}{2}|00\rangle\langle 11| + \frac{1}{4}\big(1-p^2\big)|01\rangle\langle 01| \\ +&\frac{1}{4}\big(1-p^2\big)|10\rangle\langle 10| + \frac{p^2}{2}|11\rangle\langle 00| + \frac{1}{4}\big(1+p^2\big)|11\rangle\langle 11|\end{aligned} \tag{9.34}$$

which is very similar to the state of Bob's qubits in Song's QKD protocol discussed in eq. (9.28) above. Hence, Bob obtains the expected result $|\Phi^+\rangle_{24}$ with the same probability given in eq. (9.4), i.e. $P_{corr} = (1+3p^2)/4$ which gives an overall error probability of $P_{err} = 3(1-p^2)/4$.

As already seen in section 9.2.2 the application of the Hadamard operation does not effect the error rate introduced by the noisy environment but it effects the correlations between Alice and Bob. Instead of using the correlations given in table 7.1 the two parties have to use table 7.2. If Alice uses the Hadamard operation previously to her Bell state measurement the state ρ_{35} changes to $|\omega^+\rangle\langle\omega^+|$. In the course of Alice's Bell state measurements the H operation is swapped onto qubit 1 and later on onto qubit 2 as discussed in section 7.1.1. Bob's application of the H operation changes $|\omega^+\rangle$ and $|\chi^-\rangle$ back to $|\Phi^+\rangle$ and $|\Psi^-\rangle$, respectively, whereas $|\omega^-\rangle$ is brought to $|\Psi^+\rangle$ and $|\chi^+\rangle$ to $|\Phi^-\rangle$. Nevertheless, the error rate P_{err} and the probability to obtain correlated results P_{corr} given above do not change.

It has been discussed in section 8.3 that the protocol in its original version [27] is open to the simulation attack and in the revised version [28] Eve introduces an error of 1/4 for a perfect environment. Considering noisy channels we again have the lower bounds F_{EC} and F_0 from eq. (9.17) and eq. (9.18) on the fidelity of the initial states. Hence, Eve attacks only 58.58% and 44%, respectively, of the qubits to stay below these bounds which reduces her information about the secret to $I_{AE} = 0.2929$ and $I_{AE} = 0.22$ (cf. eq. (8.24)).

9.2.4 The Cabello QSS Protocol

In difference to the QKD protocols discussed in the previous paragraphs the QSS scheme presented by Cabello [28] also makes use of an GHZ state. The depolarizing channel has a greater effect on the GHZ state such that a higher error rate is introduced into the protocol as it is shown in the following paragraphs.

In the beginning Bob and Charlie send qubits C and D of their respective Bell states to Alice which brings the initial states $|\Phi^+\rangle_{4C}$ and $|\Phi^+\rangle_{5D}$ into the mixed states

$$\begin{aligned} \rho_{4C} &= p|\Phi^-\rangle\langle\Phi^-| + \big(1-p\big)\mathbb{1} \\ \rho_{5D} &= p|\Phi^+\rangle\langle\Psi^+| + \big(1-p\big)\mathbb{1} \end{aligned} \tag{9.35}$$

as already seen in the previous protocol discussions. At the same time Alice sends qubits A and B of her GHZ state to Bob and Charlie, respectively. The effect of the noisy channel on the GHZ state can not be described just by adding some white noise as it is done for Bob's and Charlie's Bell state in the equation above. It has to be taken into account that the two qubits are effected individually by the depolarizing channel as pointed out in section 9.1.1. In detail, when Alice sends qubit A to Bob and qubit B to Charlie, the noisy channel changes the GHZ state into ρ_{3AB} from eq. (9.7) above. Hence, this changes the probability of Alice, Bob and Charlie to obtain correlated results. Following the protocol Alice measures qubits 2 and 3 and assuming she obtains $|\Phi^+\rangle_{23}$ the state of qubits 1, A and B is the same as in eq. (9.7). Further, Bob's and Charlie's measurements on the qubit pairs 4, A and 5, B, respectively, alter the remaining qubits 1, C and D such that

$$\begin{aligned} \rho_{1CD} =& \frac{1-p^4}{8}|000\rangle\langle 000| + \frac{1+2p^3+p^4}{8}|001\rangle\langle 001| - \frac{p^5}{2}|001\rangle\langle 110| \\ &+ \frac{1-2p^3+p^4}{8}|010\rangle\langle 010| + \frac{1-p^4}{8}|011\rangle\langle 011| + \frac{1-p^4}{8}|100\rangle\langle 100| \\ &+ \frac{1-2p^3+p^4}{8}|101\rangle\langle 101| - \frac{p^2}{2}|110\rangle\langle 001| + \frac{1+2p^3+p^4}{8}|111\rangle\langle 000| \\ &+ \frac{1-p^4}{8}|111\rangle\langle 111| \end{aligned} \tag{9.36}$$

assuming Bob obtains $|\Phi^-\rangle_{4A}$ and Charlie obtains $|\Psi^+\rangle_{5B}$ from their respective measurements (as given in the examples in section 7.1.2 and 8.4). When Alice performs a GHZ state measurement on qubits 1, C and D she obtains expected result $|P_{01}^-\rangle_{1CD}$, i.e. the result correlating with Bob's and Charlie's result as well as the result of her

secret measurement, with probability

$$P_{corr} = \frac{1}{8}\big(1 + 2p^3 + p^4 + 4p^5\big). \tag{9.37}$$

With also a rather large probability of $(1 + 2p^3 + p^4 - 4p^5)/8$ Alice's resulting state is $|P_{01}^{+}\rangle_{1CD}$. Further, she obtains $|P_{00}^{\pm}\rangle$ and $|P_{11}^{\pm}\rangle$ each with probability $(1 - p^4)/8$ which is not that significant. The most unlikely result for this scenario is $|P_{10}^{\pm}\rangle$ with a probability of $(1 - 2p^3 + p^4)/8$. The overall probability for Eve to obtain an uncorrelated result is then

$$P_{err} = \frac{1}{8}\big(7 - 2p^3 - p^4 - 4p^5\big) \tag{9.38}$$

which is much higher compared to the protocols discussed in the previous paragraphs.

In section 8.4 we already showed that the original version as well as the revised version of the protocol is completely open to the simulation attack if it is performed by a dishonest party. Therefore, we are going to look at the information of an outside adversary. The fraction q of all qubits in transit Eve can attack and still stay undetected is

$$q = 2\left(1 - \frac{7(1-8F) - 98(1-8F)^3 - 4(1-8F)^5}{7^6}\right) \tag{9.39}$$

because the error introduced by her is 7/16. Based on the error probability coming from the noisy channel the lower bounds on the fidelity are $\mathrm{F}_{EC} \simeq 0.9633$ and $\mathrm{F}_0 \simeq 0.9729$ which is much higher compared to the previously discussed protocols. Nevertheless, due to the high error rate introduced by her intervention Eve can only intercept a small amount of all qubits in transit, i.e. $q = 0.3347$ for F_{EC} and $q = 0.2514$ for F_0. This leads to Eve's overall information about the secret of $I_{AE} = 0.2510$ and $I_{AE} = 0.1885$ which is much smaller compared to the protocols presented above.

9.3 Influence of Physical Limitations

As pointed out above, a noisy quantum channel influences the fidelity of the initial states. In our model, a Bell state, e.g. $|\Phi^+\rangle$, becomes the Werner state ρ from eq. (9.1). Further, we already described in section 4.4 that in a realistic environment the fidelity decreases exponentially with the length of the channel (cf. eq. (4.62) and

Bell-States	$l_c = 10$ km	$l_c = 30$ km	$l_c = 50$ km
$F_{EC} = 0.9228$	1.64 km	4.92 km	8.20 km
$F_0 = 0.9428$	1.19 km	3.59 km	5.98 km

GHZ-States	$l_c = 10$ km	$l_c = 30$ km	$l_c = 50$ km
$F_{EC} = 0.9394$	1.27 km	3.81 km	6.35 km
$F_0 = 0.9552$	0.93 km	2.78 km	4.64 km

Table 9.1: Comparison of the distances where error correction and secure communication is still possible using different values for the coherence length l_c.

figure 4.5). This has a huge impact on the security of the QKD and QSS protocols based on entanglement swapping discussed in sections 8.1 - 8.4 above. As we showed in section 9.1.2 Alice and Bob need a fidelity of at least $F_{EC} = 0.9228$ to perform error correction and a fidelity $F_0 = 0.9428$ to reduce the error rate to 0.11 when dealing with two Bell states.

In figure 4.5 we used three different values for the coherence length l_c: 10 km, 30 km and 50 km. As we can directly see from figure 4.5 a higher coherence length results in a smaller decrease of the fidelity. Combining our results from the previous section with eq. (4.62) we can directly see that in a quantum channel with coherence length $l_c = 10$ km F_{EC} limits the length of the quantum channel to 1.64 km. Moreover, to guarantee a fidelity F_0 the length of the channel has to be at most 1.19 km (cf. table 9.1). Taking a higher coherence length of $l_c = 30$ km the distance over which error correction is still possible increases to 4.92 km and the distance for secure communication increases to 3.59 km. In the third scenario where we take $l_c = 50$ km we still get the fidelity F_{EC} at a distance of 8.20 km and the fidelity F_0 at a distance of 5.98 km.

The restrictions on the length of a channel are even stronger when we take GHZ states into account. Here, $F_{EC} = 0.9394$ and $F_0 = 0.9552$ which leads to corresponding lengths of 1.27 km and 0.93 km for $l_c = 10$ km. For a higher $l_c = 30$ km we can enlarge the distances again to 3.81 km and 2.78 km for F_{EC} and F_0, respectively. Going to a coherence length of 50 km the fidelity of the states in transit is still higher than F_{EC} and F_0 after a maximum distance of 6.35 km and 4.64 km, respectively.

These distances are still very low and of no practical value for quantum communication. Hence, Alice and Bob have to increase the fidelity of their entangled states before they can perform entanglement swapping, i.e. start the actual protocol. This is achieved using entanglement purification and nested purification protocols, as described in sections 4.3 and 4.4. How the entanglement purification affects the eavesdropping attempts of an adversary is described in further detail in section 9.5 below.

9.4 Cost of Entanglement Purification

In the previous sections we showed that the distance over which a secure communication is possible, is limited due to the exponential decrease of the fidelity in the length of the quantum channel by about 1.19 km, 3.59 km or 5.98 km depending on the coherence length (cf. also table 9.1). Such distances are of course of no practical value for real communication. To enlarge the distance entanglement purification protocols and a quantum repeater setup are used, as presented in sections 4.3 and 4.4. These protocols demand a high number of initially shared entangled states between several hops to establish an entangled state over a large distance. In the following paragraphs we will look at the cost of 2 scenarios for distances of 24 km and 128 km using the recurrence method (cf. section 4.3.1) and nested purification (cf. section 4.4). Therefore, the overall number $S(l, N, \mathrm{F})$ of states required to establish one entangled state between Alice and Bob is calculated based on eq. (4.63) for a constant $\mathrm{F} = \mathrm{F}_0 = 0.9428$. The results are lower bounds since we assume for reasons of simplicity that every purification round is perfect, i.e. no additional entangled states are discarded.

9.4.1 Scenario 1: Overcoming 24 km

In the first scenario, Alice and Bob want to overcome a distance of 24 km, which is a distance often found in a so-called "metro network" [118]. For reasons of simplicity, the number of segments are powers of 2 such that we use 8 segments of 3 km, 4 segments of 6 km and, if possible, 2 segments of 12 km. Over a distance of 3 km an entangled state with a fidelity $\mathrm{F}_{seg} \simeq 0.8656$ can be established between the respective hops using a channel with coherence length $l_c = 10$ km (cf. eq. (4.62) and figure 4.5). Following the nested purification protocol, at the first level the fidelity is

reduced due to the entanglement swapping to $F_{swap} \simeq 0.7552$. After three iterations of the recurrence method consuming 8 entangled states the fidelity is approximately brought to the initial amount F_{seg}. This is recursively done for level 2 and 3 as well until Alice and Bob share one state of at least initial fidelity F_{seg} over the whole distance of 24 km. To bring F_{seg} to F_0 three additional iterations of entanglement purification are needed such that the overall number of required states is at least

$$S_{10}\big(3,8\big) = 2^3 \times 8^3 \times 2^3 = 8^5 = 32768. \tag{9.40}$$

Using only 4 segments and two levels of nesting the fidelity F_{seg} decreases to $\simeq 0.7576$ and is further reduced by entanglement swapping to $F_{swap} \simeq 0.5936$. Therefore, 6 iterations of the recurrence method are necessary to bring the fidelity of the state to F_{seg} which consumes 64 entangled states. Due to the increased segment length Alice and Bob only need 2 nesting levels to establish a state over the whole distance of 24 km. Nevertheless, the number of required states is much higher due to the lower fidelity of each segment, i.e.

$$S_{10}\big(6,4\big) = 2^2 \times 4^6 \times 2^6 = 4^{10} = 1.04858 \times 10^6. \tag{9.41}$$

If we consider the same scenario using a quantum channel with a coherence length $l_c = 30$ km the number of required states is reduced drastically. After 3 km the fidelity $F_{seq} \simeq 0.9518$ (cf. figure 4.5) and is reduced by entanglement swapping to $F_{swap} \simeq 0.9067$. Hence, using 8 segments of length 3 km we still need 3 nesting levels but then the fidelity of the state shared by Alice and Bob is already good enough to perform secure communication since $F_{seg} > F_0$. Therefore, the number of required states is

$$S_{30}\big(3,8\big) = 2^3 \times 8^3 \times 2^0 = 8^4 = 4096. \tag{9.42}$$

When Alice and Bob reduce the number of segments by half such that each segment is 6 km long the fidelity $F_{seg} \simeq 0.9071$. After entanglement swapping this fidelity decreases to $F_{swap} = 0.8257$ and three iterations of the recurrence method are needed to bring it back to F_{seg}. In the end, Alice and Bob perform two additional iterations to bring F_{seg} to F_0. Nevertheless, the number of required states is reduced compared to $S_{30}(3,8)$, i.e.

$$S_{30}\big(6,4\big) = 2^2 \times 4^3 \times 2^2 = 4^5 = 1024. \tag{9.43}$$

With a coherence length of 10 km the longest possible segment was 6 km but with a coherence length of 30 km the whole distance can be divided into just two segments

of 12 km. The fidelity $\mathrm{F}_{seg} \simeq 0.8269$ is still rather good and is decreased due to entanglement swapping to $\mathrm{F}_{swap} \simeq 0.6938$. In contrary to the scenario with $l_c = 10$ km entanglement purification is possible at this distance such that Alice and Bob only need one level of nesting but 4 iterations of entanglement purification. This additionally reduces the number of required states to the amount

$$S_{30}\big(12, 2\big) = 2^1 \times 2^4 \times 2^4 = 2^9 = 512 \tag{9.44}$$

which is the best value so far.

Enlarging the coherence length to 50 km the number of required states can be further decreased. As already seen in the previous paragraph the fidelity after 3 km is very high, i.e. $\mathrm{F}_{seg} \simeq 0.9707$ (cf. figure 4.5), and entanglement swapping reduces the fidelity to $\mathrm{F}_{swap} \simeq 0.9424$ which is very close to $\mathrm{F}_0 = 0.9428$. Alice and Bob only have to use 2 iterations during entanglement purification such that the overall number of required states is

$$S_{50}\big(3, 8\big) = 2^3 \times 8^2 \times 2^0 = 8^3 = 512 \tag{9.45}$$

Considering segments of 6 km the fidelity for each segment $\mathrm{F}_{seg} \simeq 0.9426$ is very close to F_0 such that in the end Alice and Bob just have to perform one additional iteration of entanglement purification. To bring $\mathrm{F}_{swap} \simeq 0.8896$ to F_{seg} three iterations are required for each nesting level. This leads again to

$$S_{50}\big(6, 4\big) = 2^2 \times 4^3 \times 2^1 = 2^9 = 512 \tag{9.46}$$

such that Alice and Bob do not gain any advantage from enlarging the distance to 6 km. When going to 12 km for each segment Alice and Bob remain with only one level of nesting and the fidelities $\mathrm{F}_{seg} \simeq 0.8901$ and $\mathrm{F}_{swap} \simeq 0.7963$. Therefore, they need three iterations of entanglement purification for each level and three iterations in the end such that

$$S_{50}\big(12, 2\big) = 2^1 \times 2^3 \times 2^3 = 2^7 = 128. \tag{9.47}$$

With a coherence length of 50 km the fidelity after 24 km is $\mathrm{F}_{seq} \simeq 0.7980$ and purification is immediately possible. Hence, Alice and Bob only have to perform 5 iterations of entanglement purification which requires 32 states, i.e.

$$S_{50}\big(24, 1\big) = 2^0 \times 1^0 \times 2^5 = 2^5 = 32. \tag{9.48}$$

	$l = 3$ km	$l = 6$ km	$l = 12$ km	$l = 24$ km
$l_c = 10$ km	32768	1048576		
$l_c = 30$ km	4096	1024	512	
$l_c = 50$ km	512	512	128	32

Table 9.2: Comparison of the amount of entangled states required to overcome a distance of 24 km using different numbers of segments and different values for the coherence length l_c.

9.4.2 Scenario 2: Overcoming 128 km

In the second scenario, Alice and Bob want to communicate over a distance of 128 km which is rather large also for single-qubit QKD protocols. Again, Alice and Bob use powers of 2 for the number of segments: 64 segments of length 2 km, 32 segments of length 4 km each, 16 segments of length 8 km and, if possible 8 segments of length 16 km as well as 4 segments of length 32 km. Using a quantum channel with coherence length $l_c = 10$ km the first case is the most favorable since the fidelity after 2 km is $\mathrm{F}_{seg} \simeq 0.9071$ and is reduced by entanglement swapping to $\mathrm{F}_{swap} \simeq 0.8257$ such that three iterations of the entanglement purification are necessary for each nesting level. To bring F_{seg} to F_0 two additional steps are performed in the end. This results in

$$S_{10}\big(2, 64\big) = 2^6 \times 64^3 \times 2^2 = 6.71089 \times 10^7 \tag{9.49}$$

which is huge compared to the results in the previous section since the number scales exponentially (cf. eq. (4.63)). In this case the large number results from the high nesting level (64 segments = 6 nesting levels). Nevertheless, reducing the number of nesting levels does not improve the costs in this case because the fidelity F_{seg} decreases at larger distances. In case Alice and Bob use segments of 4 km they obtain $\mathrm{F}_{seg} \simeq 0.8269$ and $\mathrm{F}_{swap} \simeq 0.6983$ such that four iterations of purification are necessary. This leads to an amount of required states

$$S_{10}\big(4, 32\big) = 2^5 \times 32^4 \times 2^4 = 5.36871 \times 10^8. \tag{9.50}$$

This number becomes even worse when using 16 segments of length 8 km. At this length the initial fidelity of each state is $\mathrm{F}_{seg} \simeq 0.6975$ and after entanglement swapping $\mathrm{F}_{swap} \simeq 0.5170$. F_{swap} is already rather close to 0.5, i.e. the limit below

which purification with the recurrence method is not possible any more (cf. section 4.3.1) such that a large number of 14 iterations are necessary to bring F_{swap} to F_{seg} again. Hence, we obtain

$$S_{10}\big(8,16\big) = 2^4 \times 16^{14} \times 2^8 = 2.95148 \times 10^{20}. \tag{9.51}$$

With a higher coherence length the amount of required states can be decreased drastically since the fidelity of the entangled states of each segment is much higher. Considering $l_c = 30$ km we obtain the fidelities $\mathrm{F}_{seg} \simeq 0.9675$ and $\mathrm{F}_{swap} \simeq 0.9364$ for the first case (64 segments of length 2 km). Hence, only two iterations of purification are necessary and Alice and Bob need no additional purification steps in the end since $\mathrm{F}_{seq} > \mathrm{F}_0$. Therefore, the overall number of entangled states necessary is

$$S_{30}\big(2,64\big) = 2^6 \times 64^2 \times 2^0 = 2.62144 \times 10^5 \tag{9.52}$$

which is already two orders of magnitude smaller compared to $S_{10}(2,64)$. When we also compute the other values we see that for a length of 4 km for each segment the number of required states increases to

$$S_{30}\big(4,32\big) = 2^5 \times 32^3 \times 2^1 = 2.09715 \times 10^6. \tag{9.53}$$

because three iterations of the recurrence method are necessary to bring $\mathrm{F}_{swap} \simeq 0.8785$ to $\mathrm{F}_{seg} \simeq 0.9366$ and one additional purification step is needed in the end. Enlarging the length of a segment to 8 km reduces the fidelities $\mathrm{F}_{swap} \simeq 0.7776$ and $\mathrm{F}_{seg} \simeq 0.8791$ but positively affects the number of required states, i.e.

$$S_{30}\big(8,16\big) = 2^4 \times 16^3 \times 2^3 = 5.24288 \times 10^5. \tag{9.54}$$

$S_{30}(8,16) < S_{30}(4,32)$ due to the fact that the number of iterations stays the same but the number of segments is reduced. With a coherence length of 30 km Alice and Bob are able to use 8 segments of length 16 km but this gives the highest number of overall states

$$S_{30}\big(16,8\big) = 2^3 \times 8^5 \times 2^6 = 1.67772 \times 10^7 \tag{9.55}$$

because $\mathrm{F}_{seg} \simeq 0.7796$ is rather low.

In the last scenario we have a coherence length $l_c = 50$ km such that the fidelity of the entangled states is very close to 1 for small distances. Considering the first case where each segment is 2 km long the initial fidelity of the entangled states

$F_{seg} \simeq 0.9803$ is reduced to $F_{swap} \simeq 0.9611$. This gives for the amount of required states

$$S_{50}\big(2, 64\big) = 2^6 \times 64^2 \times 2^0 = 2.62144 \times 10^5. \tag{9.56}$$

Here we have the special case that F_{swap} is already larger than F_0 such that Alice and Bob are able to save the cost for the last nesting level as well such that $S_{50}(2, 64)$ can be further reduced to 65536. Choosing a segment length of 4 km is the most efficient way because Alice and Bob need the smallest amount of entangled states, i.e.

$$S_{50}\big(4, 32\big) = 2^5 \times 32^2 \times 2^0 = 3.2768 \times 10^4. \tag{9.57}$$

Here, fewer segments are needed and the fidelity $F_{seg} \simeq 0.9612$ is still larger than F_0. Compared to $S_{30}(4, 32)$ the number of required states for $l_c = 50$ km is about two orders of magnitude lower. Going to segments of length 8 km Alice and Bob have to perform additional purification steps at the end to reach at the fidelity F_0. Further, three iterations at each nesting level are required such that

$$S_{50}\big(8, 16\big) = 2^4 \times 16^3 \times 2^1 = 1.31072 \times 10^5 \tag{9.58}$$

which is 1/4 of $S_{30}(8, 16)$. When Alice and Bob further increase the length of the segments, also the number of required states grows. For segments of 16 km they need

$$S_{50}\big(16, 8\big) = 2^3 \times 8^4 \times 2^4 = 5.24288 \times 10^5 \tag{9.59}$$

entangled states, since the fidelities $F_{seg} \simeq 0.8576$ and $F_{swap} \simeq 0.7422$ are significantly lower compared to the scenario with segment length of 8 km discussed above. The coherence length of 50 km makes it possible for Alice and Bob to use also segments of 32 km resulting in fewer hops and a smaller number of nesting levels. In this case the fidelity of each state after 32 km is $F_{seg} \simeq 0.7449$ and is further decreased due to entanglement swapping to $F_{swap} \simeq 0.5766$. Hence, Alice and Bob need 7 iterations for entanglement purification for each nesting level and 7 additional iterations at the end to achieve the fidelity F_0 such that

$$S_{50}\big(32, 4\big) = 2^2 \times 4^7 \times 2^7 = 8.38861 \times 10^6. \tag{9.60}$$

9.4.3 Analysis

From the analysis of these two scenarios we see that for a small coherence length like 10 km the segment length is much more important than the number of segments.

	$l = 2$ km	$l = 4$ km	$l = 8$ km	$l = 16$ km	$l = 32$ km
$l_c = 10$ km	6.71×10^7	5.37×10^8	2.95×10^{20}		
$l_c = 30$ km	2.62×10^5	2.10×10^6	5.24×10^5	1.68×10^7	
$l_c = 50$ km	6.55×10^4	3.28×10^4	1.31×10^5	5.24×10^5	8.39×10^6

Table 9.3: Comparison of the amount of entangled states required to overcome a distance of 128 km using different numbers of segments and different values for the coherence length l_c.

Tables 9.2 and 9.3 show that in both scenarios the number of required states increases for longer segments. When looking at table 9.2 we also see that this fact is reversed in the scenario of 24 km when using a higher coherence length. For both $l_c = 30$ km and $l_c = 50$ km the number of required states decreases the longer each segment is. A higher coherence length also leaves a margin for the length of a segment, as described in table 9.3. For $l_c = 30$ km the minimal number of required states is $S_{30}(2, 64) = 2.62144 \times 10^5$, but for segment length of $l = 8$ km $S_{30}(8, 16) = 2S_{30}(2, 64)$ whereas the number of hops between Alice and Bob is reduced by 75%. We have a similar scenario for $l_c = 50$ km where a segment length of $l = 4$ km is more efficient than $l = 2$. Hence, a lot of optimization can be done here.

Comparing our results to the estimation of resources done by Dür et al. [45] we see that the amount of resources differs from our results. Nevertheless, we see that the number of copies as given by Dür et al. is given as

$$M = 2^{\mathrm{It}(\mathrm{F}_{swap}, \mathrm{F}_{seg})} \tag{9.61}$$

where $\mathrm{It}(\mathrm{F}_{in}, \mathrm{F}_{out})$ describes the number of iterations of the purification protocol (in this case the recurrence method) to bring F_{in} to F_{out} (cf. also eq. (4.63)). Further, $L = 2$ such that

$$R = N^{1+\log_2 M} = N^{\mathrm{It}(\mathrm{F}_{swap}, \mathrm{F}_{seg})+1} \tag{9.62}$$

as we already described in the definition of $S(l, N, \mathrm{F})$ in eq. (4.63). Hence, we used the same approach for calculating the resources of the recurrence method. While we focused on the overall number of entangled states required for purification, Dür et al. calculated the resources per segment, i.e.

$$R_{seg} = M^{\log_2 N} = N^{\mathrm{It}(\mathrm{F}_{swap}, \mathrm{F}_{seg})} \tag{9.63}$$

Furthermore, Dür et al. used noisy operations in addition to the noisy channel which further alters the overall number of required states. The main difference to the model by Dür et al. is that they used segments of length of 10 km and a coherence length $l_c = 10$ km. Due to our model of an photonic channel described in section 4.4 the fidelity decreases much faster such that a fidelity of 0.96 over 10 km corresponds to a coherence length $l_c \simeq 120$ km. Therefore, it is not possible in our scenarios to overcome such distances as presented in [45] with the same amount of resources. Comparing only the number of segments N we obtain similar results, as just pointed out above.

We want to stress again that the number of required states $S(l, N)$ calculated for these scenarios are lower bounds with regards to the recurrence method because the errors occurring in the purification protocol are not taken into account. Nevertheless, it gives a good approximation for the order of magnitude of $S(l, N)$. To use the recurrence method as purification protocol is not the optimal choice as discussed by Dür et al. [45] since the recurrence method is the most inefficient protocol compared to the quantum privacy amplification and the procedure introduced by Dür et al. (cf. section 4.3.2 for details). These two protocols make additional assumptions on the shape of the entangled states which makes the use of the recurrence method much more descriptive. However, we want to point out that the scheme presented by Dür et al. is the most efficient regarding the number of initially shared entangled states [45].

Overall, we see that the number of segments is essential to efficiently perform entanglement purification. There can always be found an optimal number of segments which usually becomes rather high for large distances. Besides the large amount of entangled states that have to be created this is the second major drawback to entanglement purification. Putting aside the physical limitations in an implementation of the scenarios presented here the financial and logistical overhead of running maybe a large number of control centers and establishing quantum links between them has to be considered. Nevertheless, these scenarios presented above show that it is possible to create a number of entangled states at a reasonable fidelity of at least F_0 over a practical distance to perform secure communication.

9.5 Simulating Entanglement Purification

As we have seen in section 9.2, the fidelity of the entanglement between the legitimate communication parties after the qubits passed a noisy channel is important for the security of the protocol. Additionally, the fidelity decreases exponentially in the length of the quantum channel thus resulting in maximal distances of approximately 1.19 km up to 5.98 km for secure communication. We already discussed in chapter 4 entanglement purification protocols which allow Alice and Bob to increase the fidelity of the Bell states they share by sacrificing a certain amount of those states. In the previous section we showed that a large number of initial states have to be shared to enlarge the distance of secure communication.

When Alice and Bob use entanglement purification protocols it is not that easy any more for Eve to entangle herself with them due to the additional operations coming from the purification procedure. Therefore, her goal is to overcome the effects of entanglement purification to remain undetected. To achieve that Eve uses the simulation approach presented in section 7.2 and extends the attack strategy to simulate also the purification as described in the following paragraphs.

We are going to focus on the recurrence method [12] and quantum privacy amplification [42] since these two are also the most important purification methods in the context of quantum repeaters [45].

9.5.1 Simulating a Single Purification Step

An entanglement purification protocol recurrently cited in literature is the recurrence method presented by Deutsch et al. [12], which is described in detail in section 4.3.1 and has also been used, for example, in the quantum repeater scheme by Dür et al. [45]. The idea is that Alice and Bob use bilateral CNOT and rotation operations to combine pairs of entangled states. Further, they sacrifice approximately half of their states during measurements to bring the remaining states into an entangled state of higher fidelity (cf. section 4.3.1 for further details).

As pointed out above, although Alice and Bob perform the entanglement purification an adversary Eve has the possibility to connect a system to the shared qubit pairs and keep it entangled during the purification procedure by simulating all operations of the purification. In detail, Eve starts with the basic state from the

simulation attack strategy

$$|\delta\rangle = \frac{1}{2}\Big(|\Phi^+\rangle|\Phi^+\rangle|\Phi^+\rangle + |\Phi^-\rangle|\Phi^-\rangle|\Phi^-\rangle + |\Psi^+\rangle|\Psi^+\rangle|\Psi^+\rangle + |\Psi^-\rangle|\Psi^-\rangle|\Psi^-\rangle\Big)_{E_1-E_6}, \tag{9.64}$$

which provides – as we have seen in section 7.2 – an effective tool for an adversary to eavesdrop on the secret key established between Alice and Bob. Certainly, for other protocols a different initial state might be useful. Additionally to $|\delta\rangle_{E_1-E_6}$, Eve generates two Bell states $|\Phi^+\rangle_{E_7,E_8}$ and $|\Phi^+\rangle_{E_9,E_{10}}$ which will later on simulate the target qubits of the BCNOT operations in the QPA protocol. Thus, the qubits are in the state (c.f. also part (1) in figure 9.4)

$$|\vartheta\rangle_{E_1-E_{10}} = |\delta\rangle_{E_2,E_3,E_8,E_9,E_5,E_6} \otimes |\Phi^+\rangle_{E_1,E_7} \otimes |\Phi^+\rangle_{E_4,E_{10}} \tag{9.65}$$

As pointed out above, Eve's main intention is to simulate the actions Alice and Bob perform during the purification protocol on the state $|\vartheta\rangle$ in reverse order. Therefore, Eve first simulates the application of the twirl operation U (cf. eq. (4.35) above) and it's inverse performed by Alice and Bob at the end of the purification procedure. Eve knows exactly on which qubits the twirl operation is applied, i.e. only on the resulting qubits of a successful purification. Hence, she is able to perform the inverse rotation also on the respective qubits E_2, E_3, E_8 and E_9 of $|\vartheta\rangle$ (c.f. (1) in figure 9.4). This leads to the state

$$|\varphi'\rangle = \big(U^{-1}\big)^{(E_2)}\big(U^{-1}\big)^{(E_3)}U^{(E_8)}U^{(E_9)}|\vartheta\rangle_{E_1-E_{10}} \tag{9.66}$$

Next, Eve performs BCNOT operations on her state $|\varphi'\rangle$ to simulate the application of the BCNOT operation applied by Alice and Bob. Thus, Eve applies 2 BCNOT operations on qubits E_2, E_8, E_1, E_7 as wells as qubits E_3, E_9, E_4, E_{10} from the state $|\vartheta\rangle$ (c.f. (2) in figure 9.4). Recall from the definition of the BCNOT operation from eq. (4.38) that the first two qubits are the source qubits and the second two are the target qubits. Hence, the qubits from the state $|\delta\rangle$ are the control qubits and the two Bell states are the targets of the CNOT operations. This changes the state $|\varphi'\rangle$ to the state

$$|\varphi\rangle = \mathrm{BCNOT}_{E_3,E_9,E_4,E_{10}}\mathrm{BCNOT}_{E_2,E_8,E_1,E_7}|\varphi'\rangle \tag{9.67}$$

When performing their CNOT operations later on Alice and Bob reverse Eve's actions and they end up with the state $|\varphi'\rangle$ again. Further, based on the special

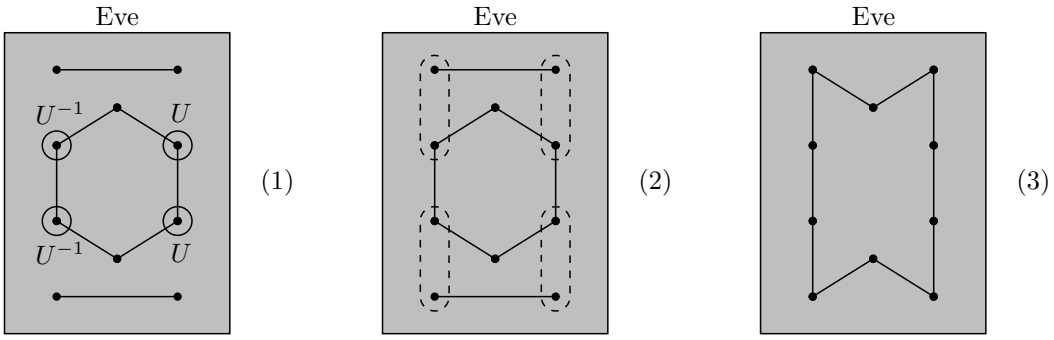

Figure 9.4: *(Eve's initial state)* Eve's preparation of the initial state for the simulation of entanglement purification. The dashed line indicates a CNOT operation.

design of the state $|\varphi'\rangle$ (and consequently $|\vartheta\rangle$) they will always obtain the same results from the measurement of their target qubits E_1 and E_7 as well as E_4 and E_{10}.

Next, Eve distributes the state $|\varphi\rangle$ between Alice and Bob (c.f. picture (1) of figure 9.5). As it is pointed out in [42] it can be assumed that Eve is able to prepare all the states for Alice and Bob, which in that case will be qubits of the state $|\varphi\rangle$. On the other hand Eve is also able to distribute $|\varphi\rangle$ by interacting with the qubits in transit between Alice and Bob using entanglement swapping. Following the protocol Alice and Bob perform the bilateral CNOT operations on their qubits changing the state $|\varphi\rangle$ back to $|\varphi'\rangle$ (c.f. picture (1) in figure 9.5). Then, both parties perform local measurements in the computational basis on qubits E_1, E_7 and E_4, E_{10}, respectively, (c.f. picture (2) in figure 9.5) which always leaves them with correlated results since the qubits are part of the Bell state $|\Phi^+\rangle$. In the end Alice and Bob apply the twirl operation U and U^{-1} on the qubits E_2, E_3 and E_8, E_9 of $|\varphi'\rangle$, respectively (c.f. picture (3) in figure 9.5). This cancels out the rotations from eq. (9.66) and brings $|\varphi'\rangle$ back to $|\delta\rangle$ (c.f. picture (4) in figure 9.5). Hence, Eve's state $|\varphi\rangle$ perfectly simulates the entanglement purification procedure such that Alice and Bob always obtain positive results from their measurements on qubits E_1 and E_7 as well as E_4 and E_{10}, respectively. Further, they share Eve's initial state $|\delta\rangle$ instead of two Bell states after they executed the entanglement purification.

When looking at the quantum privacy amplification [42] described in further detail in section 4.3.2 we see that it is very similar to the recurrence method. The main difference is that Alice and Bob use the B_x instead of the U operation. Hence, Eve follows the same strategy as defined in the previous paragraphs to simulate

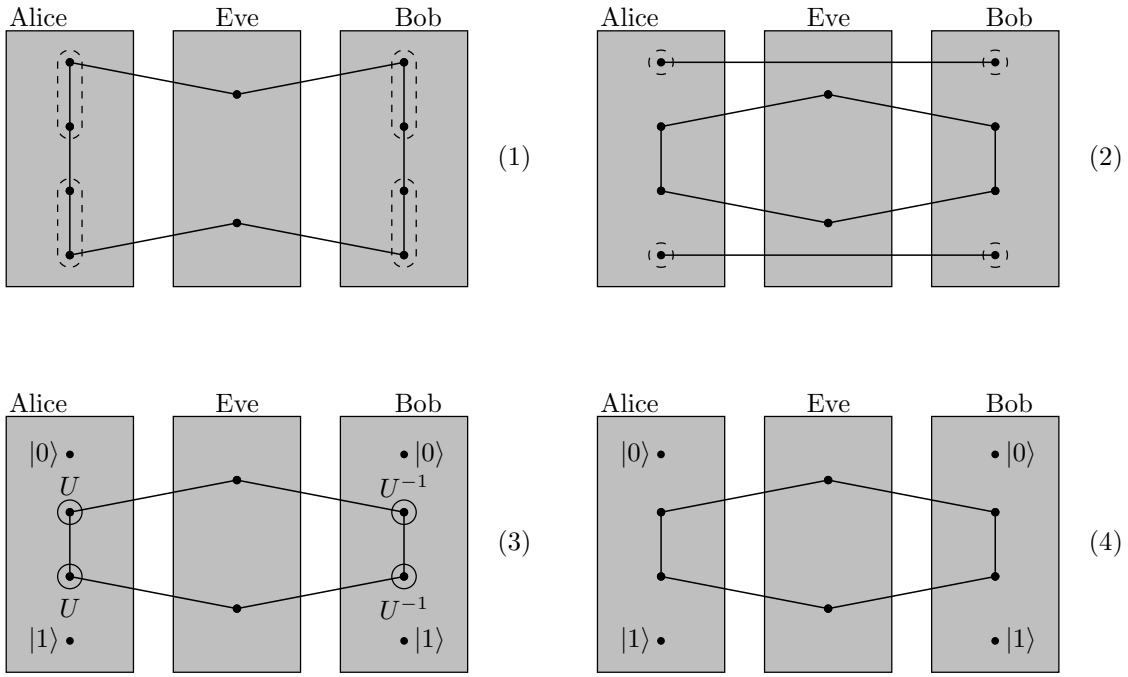

Figure 9.5: *(Simulating entanglement purification)* Eve's simulation of the entanglement purification using her initial state.

the quantum privacy amplification. Regarding the preparation she only exchanges the application of U with the application of B_x (cf. picture (1) in figure 9.4). The actions performed by Alice and Bob cancel out Eve's operations performed during the operation such that Alice and Bob end up with the state $|\delta\rangle$.

9.5.2 Simulating the Entire Purification Protocol

Taking the state $|\varphi\rangle$ Eve can simulate the purification protocol from [12] only for the case where Alice and Bob obtain the same results from their measurement of the target qubits. In fact, these are the important cases, since Alice and Bob will use only these qubits for further computations (c.f. section 4.3.1). Nevertheless, sometimes they also obtain different results from their measurements of the target qubits due to the BCNOT operations. This makes it necessary for Eve to simulate also the case where Alice and Bob obtain different results from their measurement to stay undetected. This is rather easy to accomplish with Eve preparing the state

$$|\psi'\rangle = |\Phi^+\rangle_{E_1,E_2}|\Psi^-\rangle_{E_3,E_4}. \tag{9.68}$$

Contrary to the previous paragraphs she just has to apply the BCNOT operation on $|\psi'\rangle$, resulting in the state

$$|\psi\rangle = \text{BCNOT}_{E_1,E_2,E_3,E_4}|\psi'\rangle_{E_1-E_4} \tag{9.69}$$

using the state $|\Psi^-\rangle_{3,4}$ as the target for the BCNOT operation. Afterwards, Eve distributes the state $|\psi\rangle$ between Alice and Bob. Hence, when Alice and Bob reverse Eve's action by applying their own BCNOT operation on qubits E_1 - E_4 they always obtain different results from their measurements on the target qubits E_3 and E_4 and therefore discard qubits E_1 and E_2. Thus, an error introduced by the channel is simulated using the state $|\psi\rangle_{1-4}$. We can immediately see that the state of qubits E_1 and E_2 is not relevant and Eve does not need to keep any qubits entangled with $|\psi\rangle$ for any further steps since these qubits are discarded. The state of qubits E_1 and E_2 is assumed to be $|\Phi^+\rangle_{E_1,E_2}$ for reasons of simplicity.

To simulate the full process of the entanglement purification protocol in a noisy channel Eve prepares the states $|\varphi\rangle$ and $|\psi\rangle$, alternatively. Therefore, she uses an unbiased coin which lands heads with probability F and tails with probability $1-\text{F}$. Here, F is the fidelity of the noisy channel, i.e. the probability that a state is not affected by noise (cf. also eq. (9.1)). Whenever Eve obtains a tail, she prepares the state $|\psi\rangle$ and whenever she obtains two heads in a row, she prepares $|\varphi\rangle$, i.e.

$$|\text{hh}\rangle_{1-10} = |\varphi\rangle_{E_1-E_{10}} \qquad \text{and} \qquad |\text{t}\rangle_{1-4} = |\psi\rangle_{E_1-E_4}. \tag{9.70}$$

We take the two consecutive heads, i.e. the state $|\text{hh}\rangle_{1-10}$, as the important scenario because our focus lies on protocols based on entanglement swapping two Bell states (cf. the protocols described in sections 8.1, 8.2 and 8.3). For other protocols the scenario might be different.

Of course, Eve does not always obtain two consecutive heads and therefore has to prepare additional states for the other cases of her coin toss. In case she obtains {heads, tails, heads} from her unbiased coin Eve prepares a combination of $|\varphi\rangle$ and $|\psi\rangle$, i.e.

$$|\text{hth}\rangle_{1,2,11,13,3-8,12,14,9,10} = |\varphi\rangle_{1-10}|\psi\rangle_{11-14}. \tag{9.71}$$

She distributes qubits 1-4, 11 and 13 to Alice and qubits 7-10, 12 and 14 to Bob such that Alice and Bob perform BCNOT operations on qubits 2, 8, 1, 7 as well as 11, 12, 13, 14 and 3, 9, 4, 10. Hence, they obtain a positive result from their first target pair 1, 7, a negative result from 13, 14 (based on which qubits 11 and

12 are discarded) and again a positive result from the pair 4 and 10 such that they end up again with the state $|\delta\rangle$. In general, Eve has to prepare states $|\mathrm{ht}^n\mathrm{h}\rangle$ for the sequences {heads,(tails)^n,heads} similarly to $|\mathrm{hth}\rangle$. It is easy to see that the larger n the more unlikely the state $|\mathrm{ht}^n\mathrm{h}\rangle$ becomes. For example, the state $|\mathrm{hth}\rangle$ occurs with probability $F^2(1-F)$ and in general $|\mathrm{ht}^n\mathrm{h}\rangle$ occurs with probability $F^2(1-F)^n$. Following this mechanism Eve is able to prepare a state for every possible case simulating the purification protocol over a noisy channel. Due to the fact that Eve prepared the state $|hh\rangle$ such that Alice and Bob always detect the same result and included also the error rate using the state $|\mathrm{t}\rangle$ she does not introduce any irregularity in the error rate of the protocol and thus the legitimate communication parties can not detect her intervention.

As pointed out above, the differences between the quantum privacy amplification and the recurrence method are very small (application of B_x instead of U). Hence, simulating the iterations of the purification protocol is not affected by these differences. Therefore, Eve is able to simulate the whole quantum privacy amplification protocol by the strategy described in this section, too.

Chapter 10

Conclusion

Summary

In this thesis we discussed the security of quantum key distribution and quantum secret sharing protocols based on entanglement swapping. Above all we focused primarily on collective attacks where an adversary Eve entangles herself with the states shared between the legitimate communication parties, Alice and Bob. For this scenario a specific attack strategy was presented, the *simulation attack*. Using this attack strategy the amount of information an adversary is able to obtain was analyzed. Additionally, we also addressed the information gain of an adversary in a noisy environment.

To introduce entanglement, which is the main resource of the quantum cryptographic protocols discussed in this thesis, we described in detail in chapters 2 and 3 the basic definitions of entanglement in the 2-qubit and multi qubit case as well as basic applications like entanglement swapping. Further, we sketched some methods to quantify the amount of entanglement between two or more particles. In chapter 4 we identified entanglement purification as the process to establish entanglement between two or more parties over large distances. The protocols discussed in this chapter are of major interest when looking at noisy channels later on in chapter 9.

The basic protocols for quantum key distribution and quantum secret sharing were addressed in detail in chapter 5. In the course of that we presented the central ideas of quantum cryptography and which special properties of quantum mechanics are used to secure the communication between two or several parties. The fundamental security arguments of these protocols are discussed in chapter 6. We focused

especially on the security of the sifted key and skipped the detailed analysis of the error correction and the finite key because this would go beyond the scope of this thesis. Nevertheless, we identified error rates of ∼15% and 11% as two important boundaries on the quantum bit error rate to successfully perform error correction and to guarantee the security of the protocol, respectively. These two boundaries are subsequently used in the security discussions in chapters 8 and 9 as well.

In chapter 7 the main idea of the simulation attack was introduced, which is – as its name implies – to simulate the correlations between Alice and Bob coming from the results of the entanglement swapping on the respective qubits. These correlations are used to identify the presence of an adversary which makes it important for Eve to preserve these correlations to stay undetected. We defined a state consisting of 6 qubits which implements this property for all protocols based on entanglement swapping between two Bell states. Further, the 6-qubit state allows Eve to simulate all unitary operations performed deterministically by Alice and Bob on their respective qubits.

Results

The basis of the simulation attack was originally inspired by the attack strategy presented by Zhang et al. [170]. In their article the authors showed that the entanglement swapping between two parties leaks information to an adversary. Based on that our main question is whether an adversary can find a state to extract as much information as possible from the communication between two or more parties. The ZLG attack is very specific and just defined on two protocols [27, 28]. However, we showed that the simulation attack is not only a generalization of the ZLG attack but also an extension to it. For one thing the simulation attack is applicable on a larger group of protocols and for another thing it provides Eve with more information than the ZLG attack on some specific protocols.

Contrary to the ZLG attack we demonstrate in section 7.2 how the adversary is able to overcome the deterministic application of rotation operations and basis transformations by the legitimate communication parties using the simulation attack. Moreover, we show that the random application of a rotation or basis transformation, respectively, by an angle of $\pi/2$ is the optimal choice for Alice and Bob to counter the simulation attack. Whereas Eve is able to prepare another initial

	LWWS06	Son04	Cab01	Cab00 (Ex)	Cab00 (Int)
$\langle P_e \rangle$	0.25	0.25	0.25	0.4375	0.25
$\langle P_c \rangle$	0.75	0.75	0.75	0.875	1
I_{AE}	0.5	0.5	0.5	0.75	1

Table 10.1: Comparison of the error probability and information gain using the simulation attack on the revised versions of the discussed protocols [91, 138, 27, 26].

state to overcome a deterministic application of the respective operations she is not able to overcome a random application.

Further, we describe how much information Eve has about the sifted key if Alice and Bob use the random application of a rotation or basis transformation. We find that Eve is able to obtain the same amount of information as in the individual attacks on single qubit QKD protocols. The simulation attack is applied on four different protocols [91, 138, 27, 26] in section 8 and the results are compared to an application of the ZLG attack where possible.

As a result from this analysis we showed that an adversary is able to gain a significant advantage when using the simulation attack. For three out of the four discussed protocols the simulation attack gives full information about the sifted key. We presented revised versions for all four protocols where the adversary introduces the same error rate and obtains the same amount of information compared to a single-qubit QKD scheme (cf. table 10.1). Only the revised version of the quantum secret sharing protocol [26] is still completely open to a simulation attack applied by a dishonest party.

A major topic not addressed in any protocol involving entanglement swapping are noisy channels. Usually, the protocols discussed in the literature do not take noisy channels into account although entanglement swapping needs perfect quantum channels to provide perfect correlations. Therefore, we discussed this topic in chapter 9 and analyzed the security of the protocols discussed in section 8 in a noisy environment. To model the noisy channel we used the depolarizing channel and further combined it with the exponential decrease of the fidelity over the length of the channel. This results in different threshold values for the fidelity and consequently for the length of the quantum channel above which the security is guaranteed.

	LWWS06	Son04	Cab01	Cab00 (Ex)
F_{EC}	0.9228	0.9228	0.9228	0.9633
l_{EC}	1.64 km	1.64 km	1.64 km	1.27 km
I_{AE}	0.2929	0.2929	0.2929	0.2510
q	0.5858	0.5858	0.5858	0.3347

	LWWS06	Son04	Cab01	Cab00 (Ex)
F_0	0.9428	0.9428	0.9428	0.9729
l_0	1.2 km	1.2 km	1.2 km	0.93 km
I_{AE}	0.22	0.22	0.22	0.1885
q	0.44	0.44	0.44	0.2514

Table 10.2: Comparison of the threshold values for the revised versions of the discussed protocols [91, 138, 27, 28].

For protocols using two Bell states we obtained $F_{EC} = 0.9228$ as a lower bound on the fidelity to make error correction possible. To achieve an error rate of $\sim 11\%$ as in the individual attacks the lower bound on the fidelity is $F_0 = 0.9428$. In table 10.2 the threshold values coming from section 9.2 for revised versions of all the protocols discussed in chapter 8 are given. I_{AE} is Eve's information on the sifted key if she attacks only the fraction q of the signals to stay below the respective error rate.

In section 9.3 we analyzed the decrease of the fidelity over the length of the quantum channel and found upper bounds for the fidelities F_{EC} and F_0. In table 9.1 we showed that depending on the coherence length l_c the upper bounds on the length of the channel to successfully perform error correction are $l_{EC} = 1.64$ km for $l_c = 10$ km, $l_{EC} = 4.92$ km for $l_c = 30$ km and $l_{EC} = 8.20$ km for $l_c = 50$ km. Considering secure communication, i.e. a maximal error rate of $\sim 11\%$, the upper bounds reduce to $l_0 = 1.19$ km for a coherence length of 10 km, $l_0 = 3.59$ km for a coherence length of 30 km and $l_0 = 5.98$ km for a coherence length of 50 km. Since the requirements on the fidelity are much higher for protocols using GHZ states, also the respective upper bounds on the length of a quantum channel are more restrictive as presented in table 9.1.

To extend these upper bounds entanglement purification protocols and quantum repeaters can be used as described in section 9.4. A drawback of the application of a nested purification scheme is the large number of entangled states that is required. We discussed two scenarios, for distances of 24 km and 128 km, where a nested purification scheme as suggested by Dür et al. [45] is applied. Here we showed that between 10^5 and 10^4 entangled states are required for a coherence length of 30 km and 50 km, respectively, to establish one entangled state at a fidelity larger than $F_0 = 0.9428$ over 128 km.

The results obtained from chapter 9 can be brought even closer to a realistic setup when taking imperfect local operations and measurements into account, which would go beyond the scope of this thesis. Nevertheless, as pointed out, for example, in [45] the unitary operations performed by the various parties involved in the protocols can be noisy, too. This affects entanglement swapping and consequently the security thresholds as well as the efficiency of the entanglement purification protocols. Hence, this is a possible starting point for further research.

Appendix A

Curriculum Vitae

Personal Information	
Name	**Stefan Schauer**
Address	**Heimgasse 6, A-9131 Grafenstein**
Telephone	**+43 (0) 680 24 52 787**
E-mail	**stefanschauer@gmx.at**
Nationality	Austria
Date of Birth	22.04.1981
Work Experience	
Dates (from – to)	February 2007 – present
Name and address of employer	AIT Austrian Institute of Technology GmbH Techgate Vienna Donau-City-Straße 1 1220 Wien
Type of business	Research, Quantum Technologies
Occupation or position held	Research Assistant, PhD Student
Main activities and responsibilities	Research in the field of Quantum Cryptography (security of Quantum Key Distribution protocols) and classical security (IT-Infrastructures, ISO 2700x), involved in the EU-project SECOQC

Dates (from – to)	March 2006 – January 2007
Name and address of employer	Austrian Research Centers GmbH – ARC Techgate Vienna Donau-City-Straße 1 1220 Wien
Type of business	Research, Quantum Technologies
Occupation or position held	Research Assistant, Diploma Student
Main activities and responsibilities	Research in the field of Quantum Cryptography (security of Quantum Key Distribution protocols), involved in the EU-project SECOQC

Dates (from – to)	October 2005 – January 2006
Name and address of employer	Austrian Research Centers GmbH – ARC Techgate Vienna Donau-City-Straße 1 1220 Wien
Type of business	Research, Quantum Technologies
Occupation or position held	Internship
Main activities and responsibilities	Research in the field of quantum authentication protocols

Dates (from – to)	Summers 2001 – 2005
Name and address of employer	KELAG – Kärntner Elektrizitäts-Aktiengesellschaft Arnulfplatz 2 9020 Klagenfurt am Wörthersee
Type of business	Energy provider, GIS
Occupation or position held	Internship
Main activities and responsibilities	Database administration and programming, development of small software solutions

Education

Dates (from – to)	February 2007 – present
Name and type of organization	Technical University of Vienna
Principal subjects covered	Theoretical Physics, Quantum Information
Title of qualification awarded	

Dates (from – to)	October 2000 – January 2007
Name and type of organization	University of Klagenfurt
Principal subjects covered	Computer science
Title of qualification awarded	Dipl. Ing.

Dates (from – to)	October 2002 – July 2003
Name and type of organization	ETH Zürich
Principal subjects covered	Computer science
Title of qualification awarded	

Personal Skills and Competences	
Mother tongue	**German**
Other Languages	
	English
Reading skills	Fluent
Writing skills	Fluent
Verbal skills	Fluent
	Italian
Reading skills	Basic
Writing skills	Basic
Verbal skills	Basic
Social skills and competences	Capacity for teamwork, leadership, convey of knowledge/skills (acquired as player, captain, trainer/coach in a sports club)
Organizational skills and competences	Coordination of finances (acquired as treasurer in a sports club)
Technical skills and competences	Security of computer systems and communication (classical cryptography), development of software (Java, C#), functionality of networks (acquired during the studies of computer science) Windows/Linux (as a user), Office, LaTeX, Mathematica

Bibliography

[1] A. Aspect, P. Grangier, and G. Roger. Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell's Inequalities. *Phys. Rev. Lett.*, 49(2):91–94, 1982.

[2] J. Bell. On the Einstein Podolsky Rosen Paradox. *Physics*, 1:403–408, 1964.

[3] I. Bengtsson and K. Zyczkowski. *Geometry of Quantum States*. Cambridge University Press, 2006.

[4] C. Bennett and S. Wiesner. Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States. *Phys. Rev. Lett.*, 69(20):2881–2884, 1992.

[5] C. H. Bennett. Quantum Cryptography using any Two Nonorthogonal States. *Phys. Rev. Lett.*, 68(21):3121–3124, 1992.

[6] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher. Concentrating Partial Entanglement by Local Operations. *Phys. Rev. A*, 53(4):2046–2052, 1996.

[7] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental Quantum Cryptography. *J. Crypt.*, 5(1):3–28, 1992.

[8] C. H. Bennett and G. Brassard. Public Key Distribution and Coin Tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179. IEEE Press, 1984.

[9] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner. Quantum Cryptography, or Unforgeable Subway Tokens. *Advances in Cryptology: Proceedings of the Crypto '82*, pages 267–275, 1982.

[10] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an Unknown Quantum State via Dual Classical and EPR Channels. *Phys. Rev. Lett.*, 70(13):1895–1899, 1993.

[11] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum Cryptography without Bell's Theorem. *Phys. Rev. Lett.*, 68(5):557–559, 1992.

[12] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. K. Wootters. Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. *Phys. Rev. Lett.*, 76(5):722–725, 1996.

[13] C. H. Bennett, G. Brassard, and J. M. Robert. Privacy Amplification by Public Discussion. *SIAM Journal of Computing*, 17(2):210–229, 1988.

[14] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state Entanglement and Quantum Error Correction. *Phys. Rev. A*, 54(5):3824–3851, 1996.

[15] C. H. Bennett, C. A. Fuchs, and J. A. Smolin. Entanglement-Enhanced Classical Communication on a Noisy Quantum Channel. *quant-ph/9611006 v1*, 1996.

[16] D. S. Bethune and W. P. Risk. An Autocompensating Fiber-optic Quantum Cryptography System based on Polarization Splitting of Light. *IEEE Journal of Quantum Electronics*, 36(3):340–347, 2000.

[17] E. Biham, M. Boyer, G. Brassard, J. van de Graf, and T. Mor. Security of Quantum Key Distribution Against All Collective Attacks. *Algorithmica*, 34(4):372–388, 2002.

[18] E. Biham and T. Mor. Security of Quantum Cryptography Against Collective Attacks. *Phys. Rev. Lett.*, 78(11):2256–2259, 1997.

[19] G. R. Blakley. Safeguarding Cryptographic Keys. In *Proceedings of the National Computer Conference*, volume 48, pages 313–317. AFIPS Press, 1979.

[20] S. Bose, V. Vedral, and P. L. Knight. Multiparticle Generalization of Entanglement Swapping. *Phys. Rev. A*, 57(2):822–829, 1998.

[21] J. Bouda and V. Bužek. Entanglement Swapping between Multi-Qudit Systems. *J Phys A-Math Gen*, 34(20):4301–4312, 2001.

[22] D. Bouwmeester, A. Ekert, and A. Zeilinger. *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*. Springer, 3 edition, 2001.

[23] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders. Limitations on Practical Quantum Cryptography. *Phys. Rev. Lett.*, 85(6):1330–1333, 2000.

[24] D. Bruss. Optimal Eavesdropping in Quantum Cryptography with Six States. *Phys. Rev. Lett*, 81(14):3018–3021, 1998.

[25] D. Bures. An Extension of Kakutani's Theorem on Infinite Product Measures to the Tensor Product of Semifinite ω^*-Algebras. *Trans. Am. Math. Soc.*, 135:199–212, 1969.

[26] A. Cabello. Multiparty Key Distribution and Secret Sharing Based on Entanglement Swapping. *quant-ph/0009025 v1*, 2000.

[27] A. Cabello. Quantum Key Distribution without Alternative Measurements. *Phys. Rev. A*, 61(5):052312, 2000.

[28] A. Cabello. Reply to "Comment on "Quantum Key Distribution without Alternative Measurements"". *Phys. Rev. A*, 63(3):036302, 2001.

[29] N. J. Cerf, C. Adami, and R. M. Gingrich. Reduction Criterion for Separability. *Phys. Rev. A*, 60(2):898–909, 1999.

[30] K. Chen and L.-A. Wu. A Matrix Realignment Method for Recognizing Entanglement. *Quantum Inf. Comp.*, 3(3):193–202, 2003.

[31] Y.-A. Chen, A.-N. Zhang, Z. Zhao, X.-Q. Zhou, C.-Y. Lu, T. Peng, C.-Z. andYang, and J.-W. Pan. Experimental Quantum Secret Sharing and Third-Man Quantum Cryptography. *Phys. Rev. Lett.*, 95(20):200502, 2005.

[32] L. Clarisse and P. Wocjan. On independent permutation separability criteria. *Quantum Inf. Comp.*, 6(3):277–288, 2006.

[33] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed Experiment to Test Local Hidden-Variable Theories. *Phys. Rev. Lett.*, 23(15):880–884, 1969.

[34] R. Cleve, D. Gottesman, and H.-K. Lo. How to Share a Quantum Secret. *Phys. Rev. Lett.*, 83(3):648–651, 1999.

[35] V. Coffman, J. Kundu, and W. Wootters. Distributed Entanglement. *Phys. Rev. A*, 61(5):052306, 2000.

[36] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley Inc., 2 edition, 2006.

[37] J. N. Damask. *Polarization Optics in Telecommunication*. Springer, 2005.

[38] F.-G. Deng, C.-Y. Li, Y.-S. Li, H.-Y. Zhou, and Y. Wang. Symmetric Multiparty-Controlled Teleportation of an Arbitrary Two-Particle Entanglement. *Phys. Rev. A*, 72(2):022338, 2005.

[39] F.-G. Deng, X.-H. Li, C.-Y. Li, P. Zhou, and H.-Y. Zhou. Multiparty Quantum State Sharing of an Arbitrary Two-Particle State with Einstein-Podolsky-Rosen Pairs. *Phys. Rev. A*, 72(4):044301, 2005.

[40] F.-G. Deng, X.-H. Li, C.-Y. Li, P. Zhou, and H.-Y. Zhou. Quantum State Sharing of an Arbitrary Two-Qubit State with Two-Photon Entanglements and Bell-State Measurements. *Europ. Phys. Journal D*, 39(2):459–464, 2006.

[41] D. Deutsch. Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer. *Proceedings of the Royal Society of London A*, 400(1818):97–117, 1985.

[42] D. Deutsch, A. Ekert, R. Josza, C. Machiavello, S. Popescu, and A. Sanpera. Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels. *Phys. Rev. Lett.*, 77(13):2818–2821, 1996.

[43] W. Diffie and M. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory*, (22):644–654, 1976.

[44] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller. Long Distance Quantum Communication with Atomic Ensembles and Linear Optics. *Nature*, 414(6861):413–418, 2001.

[45] W. Dür, H.-J. Briegel, J. I. Cirac, and P. Zoller. Quantum Repeaters Based on Entanglement Purification. *Phys. Rev. A*, 59(1):169–181, 1999.

[46] W. Dür, J. I. Cirac, M. Lewenstein, and D. Bruss. Distillability and Partial Transposition in Bipartite Systems. *Phys. Rev. A*, 61(6):062313, 2000.

[47] W. Dür, G. Vidal, and J. I. Cirac. Three Qubits can be Entangled in Two Inequivalent Ways. *Phys. Rev. A*, 62(6):062314, 2000.

[48] M. Dusek, N. Lütkenhaus, and M. Hendrych. Quantum Cryptography. *Progress in Optics*, 49, 2006.

[49] J. Dynes, Z. Yuan, A. Sharpe, and A. Shields. Practical Quantum Key Distribution over 60 hours at an Optical Fiber Distance of 20km Using Weak and Vacuum Decoy Pulses for Enhanced Security. *Opt. Express*, 15(13):8465–8471, 2007.

[50] A. Einstein, B. Podolsky, and N. Rosen. Can Quantum-Mechanical Description of Physical Reality be Considered Complete? *Phys. Rev.*, 47:777–780, 1935.

[51] A. Ekert. Quantum Cryptography Based on Bell's Theorem. *Phys. Rev. Lett.*, 67(6):661–663, 1991.

[52] A. Ekert, B. Huttner, G. M. Palma, and A. Peres. Eavesdropping on Quantum-Cryptographical Systems. *Phys. Rev. A*, 50(2):1047–1056, 1994.

[53] H. Fan, Y.-C. Ou, and V. Roychowdhury. Entangled Multi-qubit States Without Higher-tangle. *quant-ph/0707.1578*, 2007.

[54] D. G. Fischer, M. Mack, M. A. Cirone, and M. Freyberger. Enhanced Estimation of a Noisy Quantum Channel Using Entanglement. *Phys. Rev. A*, 64(2):022309, 2001.

[55] A. Gabriel, B. C. Hiesmayr, and M. Huber. Criterion for k-separability in Mixed Multipartite States. *Quant. Inf. Comp.*, 10(10):0829–0836, 2010.

[56] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter. Experimental Demonstration of Four-Party Quantum Secret Sharing. *Phys. Rev. Lett.*, 98(2):020503, 2007.

[57] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum Cryptography. *Rev. Mod. Phys.*, 74(1):145, 2002.

[58] C. Gobby, Z. L. Yuan, and A. J. Shields. Quantum Key Distribution over 122km of Standard Telecom Fiber. *Appl. Phys. Lett.*, 84(8):3762–3764, 2004.

[59] D. Gottesman. Theory of Quantum Secret Sharing. *Phys. Rev. A*, 61(4):042311, 2000.

[60] D. Greenberger, M. A. Horne, and A. Zeilinger. Going beyond Bell's Theorem. In M. Kafatos, editor, *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, pages 69–72. Kluwer, 1989.

[61] F. Grosshans and P. Grangier. Continuous Variable Quantum Cryptography using Coherent States. *Phys. Rev. Lett.*, 88(5):057902, 2002.

[62] F. Grosshans, G. van Ascha, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier. Quantum Key Distribution using Gaussian-Modulated Coherent States. *Nature*, 421(6920):238, 2003.

[63] O. Gühne, F. Bodoky, and M. Blaauboer. Multiparticle Entanglement under the Influence of Decoherence. *Phys. Rev. A*, 78(6):060301, 2008.

[64] O. Gühne and G. Toth. Entanglement Dtection. *Phys. Rep.*, 474(1):1–75, 2009.

[65] G.-P. Guo and G.-C. Guo. Quantum Secret Sharing Without Entanglement. *Phys. Lett. A*, 310(4):247–251, 2003.

[66] B. C. Hiesmayr and M. Huber. Multipartite Entanglement Measure for all Discrete Systems. *Phys. Rev. A*, 78(1):012342, 2008.

[67] S. Hill and W. Wootters. Entanglement of a Pair of Qubits. *Phys. Rev. Lett.*, 78(26):5022–5025, 1997.

[68] M. Hillery, V. Buzek, and A. Berthiaume. Quantum Secret Sharing. *Phys. Rev. A*, 59(3):1829–1834, 1999.

[69] A. S. Holevo. Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel. *Probl. Inf. Trans.*, 9(3):3–11, 1973.

[70] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of Mixed States: Necessary and Sufficient Conditions. *Phys. Lett. A*, 223(1-2):1–8, 1996.

[71] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-State Entanglement and Distillation: Is There a "Bound" Entanglement in Nature? *Phys. Rev. Lett.*, 80(24):5239–5242, 1998.

[72] M. Horodecki, P. Horodecki, and R. Horodecki. Limits for Entanglement Measures. *Phys. Rev. Lett.*, 84(9):2014–2017, 2000.

[73] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of Mixed quantum States: Linear Contractions Approach. *Open Syst. Inf. Dyn.*, 13(1):103–111, 2006.

[74] P. Horodecki. Separability Criterion and Inseparable Mixed States with Positive Partial Transposition. *Phys. Lett. A*, 232(5):333–339, 1997.

[75] R. Horodecki and P. Horodecki. Reduction Criterion of Seperability and Limits for a Class of Distillation Protocols. *Phys. Rev. A*, 59(6):4206–4212, 1999.

[76] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum Entanglement. *Rev. Mod. Phys*, 81(2):865–942, 2009.

[77] E. Hostens, J. Dehaene, and B. de Moor. Asymptotic Adaptive Bipartite Entanglement Distillation Protocol. *Phys. Rev. A*, 73(6):062337, 2006.

[78] H. Hübel, M. Vanner, T. Lederer, B. Blauensteiner, T. Lorünser, A. Poppe, and A. Zeilinger. High-Fidelity Transmission of Polarization Encoded Qubits from an Entangled Source over 100 km of Fiber. *Opt. Express*, 15(12):7853–7862, 2007.

[79] M. Huber, F. Mintert, A. Gabriel, and B. C. Hiesmayr. Detection of High-Dimensional Genuine Multipartite Entanglement of Mixed States. *Phys. Rev. Lett*, 104(21):210501, 2010.

[80] M. Huber, H. Schimpf, Ch. Spengler, A. Gabriel, B.C. Hiesmayr, and D. Bruss. to appear. 2010.

[81] B. Huttner and A. Ekert. Information Gain in Quantum Eavesdropping. *J. Mod. Opt.*, 41(12):2455–2466, 1994.

[82] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum Cryptography with Coherent States. *Phys. Rev. A*, 51(3):1863–1869, 1995.

[83] W.-Y. Hwang. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.*, 91(5):057901, 2003.

[84] A. Karlsson, M. Koashi, and N. Imoto. Quantum Entanglement for Secret Sharing and Secret Splitting. *Phys. Rev. A*, 59(1):162–168, 1999.

[85] Y.-H. Kim, S. Kulik, and Y. Shih. Quantum Teleportation of a Polarization State with Complete Bell State Measurement. *Physical Review Letters*, 86(7):1370–1373, 2001.

[86] E. Knill and R. Laflamme. A Theory of Quantum Error Correctiong Codes. *Phys. Rev. A*, 55(2):900–911, 1997.

[87] B. Kraus, N. Gisin, and R. Renner. Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication. *Phys. Rev. Lett.*, 95(8):080501, 2005.

[88] R. Laflamme, C. Miquel, J.-P. Paz, and W. H. Zurek. Perfect Quantum Error Correcting Code. *Phys. Rev. Lett.*, 77(1):198–201, 1996.

[89] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, T. Tyc, T. C. Ralph, and P. K. Lam. Continuous-Variable Quantum-State Sharing via Quantum Disentanglement. *Phys. Rev. A*, 71(3):033814, 2004.

[90] J. Lee, S. Lee, J. Kim, and S. D. Oh. Entanglement Swapping Secures Multiparty Quantum Communication. *Phys. Rev. A*, 70(3):032305, 2004.

[91] C. Li, Z. Wang, C.-F. Wu, H.-S. Song, and L. Zhou. Certain Quantum Key Distribution achieved by using Bell States. *International Journal of Quantum Information*, 4(6):899–906, 2006.

[92] Y. Li, K. Zhang, and K. Peng. Multiparty Secret Sharing of Quantum Information based on Entanglement Swapping. *Phys. Lett. A*, 324(4):420–424, 2004.

[93] H.-K. Lo, X. Ma, and K. Chen. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.*, 94(23):230504, 2005.

[94] Zhao Y. Lo, H.-K. Quantum Cryptography. *quant-ph/0803.2507*, 2008.

[95] R. Lohmayer, A. Osterloh, J. Siewert, and A. Uhlmann. Entangled Three-qubit States Without Concurrence and Three-tangle. *Phys. Rev. Lett.*, 97(26):260502, 2006.

[96] N. Lütkenhaus. Security Against Eavesdropping Attacks in Quantum Cryptography. *Phys. Rev. A*, 54(1):97–111, 1996.

[97] N. Lütkenhaus. Security Against Individual Attacks for Realistic Quantum Key Distribution. *Phys. Rev. A*, 61(5):052304, 2000.

[98] N. Lütkenhaus and M. Jahma. Quantum Key Distribution With Realistic States: Photon-number Statistics in the Photon-number Splitting Attack. *New J. Phys.*, 4:44.1–44.9, 2002.

[99] D. J. C. MacKeay. *Information Theory, Inference and Learning Algorithms.* cambridge University Press, 2003.

[100] V. Makarov, A. Anisimov, and J. Skaar. Effects of Detector Efficiency Mismatch on Security of Quantum Cryptosystems. *Phys. Rev. A*, 74(2):022313, 2006.

[101] V. Makarov and D. R. Hjelme. Faked States Attack on Quantum Cryptosystems. *J. of Mod. Opt.*, 52(5):691–705, 2005.

[102] V. Makarov and J. Skaar. Faked States Attack Using Detector Efficiency Mismatch on SARG04, Phase-time, DPSK and Ekert Protcols. *Quant. Inf. Comp.*, 8(6&7):622–635, 2008.

[103] D. Markham and B. C. Sanders. Graph States for Quantum Secret sharing. *Phys. Rev. A*, 78(4):042309, 2008.

[104] U. Maurer. Secret Key Agreement by Public Discussion from Common Information, journal = IEEE Trans. Inf. Theory, volume = 39, pages = 733–742, year = 1993.

[105] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin. "Plug and Play" Systems for Quantum Cryptography. *Appl. Phys. Lett.*, 70(7):793–795, 1997.

[106] A. Muller, H. Zbinden, and N. Gisin. Quantum Cryptography over 23 km in Installed Under-Lake Telecom Fibre. *Europhys. Lett.*, 33(5):335–339, 1996.

[107] G. O. Myhr. Measures of Entanglement in Quantum Mechanics. Master's thesis, Norwegien University of Science and Technology, 2004.

[108] M. A. Nielsen. On the Units of Bipartite Entanglement: Is Sixteen Ounces of Entanglement Always Equal to One Pound? *J. Phys. A*, 34(35):6987–6995, 2001.

[109] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[110] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger. Experimental Entanglement Swapping: Photons That Never Interacted. *Phys. Rev. Lett.*, 80(18):3891–3894, 1998.

[111] J.-W. Pan, M. Daniell, S. Gasparoni, G. Weihs, and A. Zeilinger. Experimental Demonstration of Four-photon Entanglement and High-fidelity Teleportation. *Phys. Rev. Lett.*, 86(20):4435–4438, 2001.

[112] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger. The SECOQC Quantum Key Distribution Network in Vienna. *New Journal of Physics*, 11(7):075001, 2009.

[113] A. Peres. How to Differentiate Between Non-orthogonal States. *Phys. Lett. A*, 128(1-2):19, 1988.

[114] A. Peres. Separability Criterion for Density Matrices. *Phys. Rev. Lett.*, 77(8):1413–1415, 1996.

[115] M. B. Plenio. Logarithmic Negativity: A Full Entanglement Monotone That is not Convex. *Phys. Rev. Lett.*, 95(9):090503, 2005.

[116] M. B. Plenio and S. Virmani. An Introduction to, Entanglement Measures. *Quant. Inf. Comp.*, 7(1):001–051, 2007.

[117] A. Poppe, A. Fedrizzi, R. Usin, H. R. Böhm, T. Lorünser, O. Maurhardt, M. Peev, M. Suda, C. Kurtsiefer, H. Weinfurter, T. Jennewein, and A. Zeilinger. Practical Quantum Key Distribution with Polarization Entangled Photons. *Optics Express*, 12(16):3865–3871, 2004.

[118] A. Poppe, M. Peev, and O. Maurhart. Outline of the SECOQC Quantum-Key-Distribution Network in Vienna. *Int. J. of Quant. Inf.*, 6(2):209–218, 2008.

[119] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma. Time-shift Attack in Practical Quantum Cryptosystems. *Quant. Inf. Comp.*, 7(1&2):73–82, 2007.

[120] S.-J. Qin, F. Gao, Q.-Y. Wen, and F.-C. Zhu. Cryptanalysis of the Hillery-Bužek-Berthiaume Quantum Secret-Sharing Protocol. *Phys. Rev. A*, 76(6):062324, 2007.

[121] A. Renyi. On Measures of Entropy and Information. In *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probobability*, pages 547–561. University of California Press, 1961.

[122] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, and H. Zbinden. Fast and User-friendly Quantum Key Distribution. *J. Mod. Optics*, 47(2&3):517–531, 2000.

[123] R.L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[124] O. Rudolph. Further Results on the Cross Norm Criterion for Separability. *Quantum Inf. Process.*, 4(3):219–239, 2005.

[125] V. Scarani, A. Acin, G. Ribordy, and N. Gisin. Quantum Cryptography Protocols Robust Against Photon Number Splitting Attacks for Weak Laser Pulses Implementations. *Phy. Rev. Lett.*, 92(5):057901, 2004.

[126] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev. The Security of Practical Quantum Key Distribution. *Rev. Mod. Phys.*, 81(3):1301–1350, 2009.

[127] S. Schauer. Attack Strategies on QKD protocols. *Lect. Notes Phys.*, 797:71–95, 2010.

[128] S. Schauer, M. Huber, and Hiesmayr. Experimentally Feasible Security Check for n-qubit Quantum Secret Sharing. *Phys. Rev. A*, 82(6):062311, 2010.

[129] S. Schauer and M. Suda. A Novel Attack Strategy on Entanglement Swapping QKD Protocols. *Int. J. of Quant. Inf.*, 6(4):841–858, 2008.

[130] E. Schrödinger. Die gegenwärtge Situation in der Quantenmechanik. *Naturwissenschaften*, 23(48):807–812, 1935.

[131] B. Schumacher. Sending Entanglement Through Noisy Quantum Channels. *Phys. Rev. A*, 54(4):2614–2628, 1996.

[132] B. Schumacher and M. A. Nielsen. Quantum Data Processing and Error Correction. *Phys. Rev. A*, 54(4):2629–2635, 1996.

[133] A. Shamir. How to Share a Secret. *Comm. of the ACM*, 22(11):612–613, 1979.

[134] C. E. Shannon. A mathematical theory of communication. *The Bell System Tech. Journal*, 27:379–423,623–656, 1948.

[135] P. Shor and J. Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.*, 85(2):441–444, 2000.

[136] P. W. Shor. Scheme for Reducing Decoherence in Quantum Computer Memory. *Phys. Rev. A*, 52(4):R2493–2496, 1995.

[137] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1996.

[138] D. Song. Secure Key Distribution by Swapping Quantum Entanglement. *Phys. Rev. A*, 69(3):034301, 2004.

[139] A. M. Steane. Error Correction Codes in Quantum Theory. *Phys. Rev. Lett.*, 77(5):793–797, 1996.

[140] D. Strucki, O. Gisin, N. Guinnard, G. Ribordy, and H. Zbinden. Quantum Key Distribution over 67km with a Plug & Play System. *New J. of Phys.*, 4:41.1–41.8, 2002.

[141] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and Zbinden. H. Fast and Simple One-Way Quantum Key Distribution. *Appl. Phys. Lett.*, 87(19):194108, 2005.

[142] M. Suda. QKD Systems. *Lect. Notes Phys.*, 797:97–121, 2010.

[143] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, H. Toshimori, K. Tamaki, and Y Yamamoto. Quantum Key Distribution over 40db Channel Loss using Superconduction Single Photon Detectors. *Nature Photonics*, 1(6):343–348, 2007.

[144] J. J.-L. Ting. Noise Effects of the Depolarizing Channel. *Phys. Lett. A*, 259(5):349–354, 1999.

[145] J. J.-L. Ting. Stochastic Resonance for Quantum Channels. *Phys. Rev. E*, 59(3):2801–2803, 1999.

[146] J. J.-L. Ting. Noise Effects on One-Pauli Channels. *Eur. Phys. J. B*, 13(3):527–530, 2000.

[147] W. Tittel, H. Zbinden, and N. Gisin. Experimental Demonstration of Quantum Secret Sharing. *Phys. Rev. A*, 63(4):042301, 2001.

[148] A. Uhlmann. The "transition probability" in the state space of a $*$-algebra. *Rep. Math. Phys*, 9(2):273–279, 1976.

[149] A. Uhlmann. Entropy and Optimal Decompositions of States Relative to a Maximal Commutative Subalgebra. *Open Systems & Information Dynamics*, 5:209–227, 1998.

[150] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger. Free-Space Distribution of Entanglement and Single Photons over 144 km. *Nature Physics*, 3(7):481–486, 2007.

[151] A. Vakahitov, V. Makarov, and D. R. Hjelme. Large Pulse Attack as a Method of Conventional Optical Eavesdropping in Quantum Cryptography. *J. Mod. Opt.*, 48(13):2023–2038, 2001.

[152] S. J. van Enk, J. I. Cirac, and P. Zoller. Photonic Channels for Quantum Communication. *Science*, 279(5348):205–208, 1998.

[153] V. Vedral and M. B. Plenio. Entanglement Measures and Purification Procedures. *Phys. Rev. A*, 57(3):1619–1633, 1998.

[154] F. Verstraete, J. Dehaene, B. de Moor, and H. Verschelde. Four Qubits can be Entangled in Nine Different Ways. *Phys. Rev. A*, 65(5):052112, 2002.

[155] G. Vidal. Entanglement Monotones. *J. Mod. Opt.*, 47(2&3):355–376, 2000.

[156] G. Vidal and R. F. Werner. Computable Measure of Entanglement. *Phys. Rev. A*, 65(3):032314, 2002.

[157] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri. Experimental Verification of the Feasibility of a Quantum Channel Between Space and Earth. *New J. of Phys.*, 10(3):033038, 2008.

[158] J. von Neumann. Mathematische Grundlagen der Quantenmechanik. In *Grundlehren der Mathematischen Wissenschaften. Bd. 38*. Springer, 1932.

[159] X.-B. Wang. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Phys. Rev. Lett.*, 94(23):230503, 2005.

[160] M. N. Wegman and J. L. Carter. New Hash Functions and their Use in Authentication and Set Equality. *Journal of Computer and System Science*, 22:265–279, 1981.

[161] D. J. A. Welsh. *Codes and Cryptography*. Oxford University Press, 1988.

[162] R. F. Werner. Quantum States with Einstein-Podolsky-Rosen Correlations Admitting a Hidden-Variable Model. *Phys. Rev. A*, 40(8):4277, 1989.

[163] S. Wiesner. Conjugate Coding. *SIGACT News*, 15(1):78–88, 1983.

[164] P. Wocjan and M. Horodecki. Characterization of Combinatorially Independent Permutation Separability Criteria. *Open Syst. Inf. Dyn*, 12(4):331–345, 2005.

[165] A. Wong and N. Christensen. Potential Multiparticle Entanglement Measure. *Phys. Rev. A*, 63(4):044301, 2001.

[166] W. K. Wootters and W. H. Zurek. A Single Quantum Cannot Be Cloned. *Nature*, 299(5886):802–803, 1982.

[167] L. Xiao, G. L. Long, F.-G. Deng, and J. W. Pan. Efficient Multiparty Quantum-secret-sharing Schemes. *Phys. Rev. A*, 69(5):052307, 2004.

[168] Z.-S. Yuan, Y.-A. Chen, B. Zhao, S. Chen, J. Schmiedmayer, and J. W. Pan. Experimental Demonstration of a BDCZ Quantum Repeater Node. *Nature*, 454(7208):1098–1101, 2008.

[169] B. Yurke and D. Stoler. Einstein-Podolsky-Rosen Effects from Independent Particle Sources. *Phys. Rev. Lett.*, 68(9):1251–1254, 1992.

[170] Y.-S. Zhang, C.-F. Li, and G.-C. Guo. Comment on "Quantum Key Distribution without Alternative Measurements". *Phys. Rev. A*, 63(3):036301, 2001.

[171] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo. Quantum Hacking: Experimental Demonstration of Time-shift Attack Against Practical Quantum Key Distribution Systems. *Phys. Rev. A*, 78(4):042333, 2008.

[172] M. Zukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert. "Event-Ready-Detectors" Bell State Measurement via Entanglement Swapping. *Phys. Rev. Lett.*, 71(26):4287–4290, 1993.