Security proof methods for quantum key distribution protocols

by

Agnes Ferenczi

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Physics

Waterloo, Ontario, Canada, 2013

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

A. Ferenczi

Abstract

In this thesis we develop practical tools for quantum key distribution (QKD) security proofs. We apply the tools to provide security proofs for several protocols, ranging from discrete variable protocols in high dimensions, protocols with realistic implementations, measurement device independent QKD and continuous-variable QKD. The security proofs are based on the Devetak-Winter security framework [31, 57].

In the key rate calculation, it is often convenient to assume that the optimal attack is symmetric. Under the assumption that the parameter estimation is based on coarse-grained observations, we show that the optimal attack is symmetric, if the protocol and the postselection have sufficient symmetries. As an example we calculate the key rates of protocols using 2, d and $d+1$ mutually unbiased bases in d-dimensional Hilbert spaces.

We investigate the connection between the optimal collective eavesdropping attack and the optimal cloning attack, in which the eavesdropper employs an optimal cloner to attack the protocol. We find that, in general, it does not hold that the optimal attack is an optimal cloner. However, there are classes of protocols, for which we can identify the optimal attack by an optimal cloner. We analyze protocols with mutually unbiased bases in d dimensions, and show that for the protocols with 2 and $d+1$ mutually unbiased bases the optimal attack is an optimal cloner, but for the protocols with d mutually unbiased bases, it is not.

In optical implementations of the phase-encoded BB84 protocol, the bit information is usually encoded in the phase of two consecutive photon pulses generated in a Mach-Zehnder interferometer. In the actual experimental realization, the loss in the arms of the Mach-Zehnder interferometer is not balanced, for example because only one arm contains a lossy phase modulator. Since the imbalance changes the structure of the signals states and measurements, the BB84 security analysis no longer applies in this scenario. We provide a security proof for the unbalanced phase-encoded BB84. The loss does lower the key rate compared to a protocol without loss. However, for a realistic parameter regime, the same key rate is found by applying the original BB84 security analysis.

Recently, the security of a measurement device-independent QKD setup with BB84 signal states was proven in Refs. [61, 14]. In this setup Alice and Bob send quantum states to an intermediate node, which performs the measurement, and is assumed to be controlled by Eve. We analyze the security of a measurement device-independent QKD protocol with B92 signal states, and calculate the key rates numerically for a realistic implementation. Based on our security proof we were able to prove the security of the strong reference pulse B92 protocol.

We analyze the security of continuous-variable protocols using the entropic uncertainty relations established in Ref. [11] to provide an estimate of the key rate based on the observed first and second moments. We analyze a protocol with squeezed coherent states and the 2-state protocol with two coherent states with opposite phases.

Acknowledgements

First and foremost, I want to thank my supervisor Norbert Lütkenhaus, who gave me the opportunity to complete my Ph.D. thesis at the Institute for Quantum Computing. I especially want to thank for his support, advice and guidance that made this project possible. I am grateful for the opportunities he provided to visit international conferences and to spend a term abroad at the Max Planck Institute for the Science of Light in Erlangen. I would also like to thank the members of my advisory committee, Raymond Laflamme, Michele Mosca and David Kribs, for the thought-provoking questions during my advisory committee meetings, and to Mark Hillery for agreeing to be my external examiner.

Thanks to my colleagues in the OQCT research group for their helpful discussions and their friendship: Razieh Annabestani, Juan Miguel Arrazola, Normand Beaudry, Oleg Gittsovich, Hauke Häseler, Matthias Heid, Nathan Killoran, Xiongfeng Ma, Will Matthews, Sergei Mikheev, Tobias Moroder, Geir Ove Myhr, Varun Narasimhachar, Marco Piani, David Pitkänen, Mohsen Razavi and William Stacey.

Waterloo has become my new home, because of the many great friends who were a source of laughter, joy and support. Thanks to Varun and Razieh for sharing jokes that made me laugh so hard it hurt. Thanks to Jean-Luc, who has been a great roommate and friend. Thanks to my training partner, Florian, for the rides to triathlon and running races. Thanks to Jonathan for the scotch and beers. Thanks to Norm for the countless board game nights. Thanks to my office mates, Gina and Peter, for the interesting discussions.

Thanks to my friends at the runner's choice marathon group, the Health and Performance group and the UW triathlon club for sharing the pain of countless training hours and for the encouragements to "never give up".

Finally, I want to thank my family for their love, their constant encouragement and support.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

The field of quantum cryptography including the subfield quantum key distribution emerged through the need to provide unconditionally secure communication protocols. The security of commonly used classical cryptography systems relies on concepts such as computational hardness of mathematical problems. Factoring a large number into the prime components is one such example, which is also the underlying security assumption of the classical cryptographic system RSA. With the emergence of Shor's factoring algorithms, such classical cryptographic systems are threatened to be broken in reasonably short time. Although the practical implementation of Shor's algorithm using a quantum computer is still in its infancy, it is necessary to start to build a defence system based on QKD before a quantum computer is ready to break existing cryptographic systems.

The goal of QKD is to enable two distant parties to generate a *secret key* by means of quantum mechanical principles. A secret key is a string of random bits known to both parties, but unknown to any third party. The secure key is later used to enable secure communication, message authentication or other cryptographic applications. QKD does not impose any computational limitations on an eavesdropper. If we accept quantum mechanics as a valid description of nature, then, in principle, unconditional security of the secret key can be guaranteed by QKD.

The process that generates the key, called *protocol*, is a predefined series of steps executed by the two parties. In a QKD protocol, the sender, Alice, encodes random bits into nonorthogonal quantum states in her laboratory. She sends the states one by one through a quantum channel to the receiving party, Bob, who performs a measurement in his laboratory to obtain the encoded data. Finally, by means of classical communication protocols over an authenticated classical channel, Alice and Bob extract the secret key

from their data. Typically it is assumed that Alice and Bob's laboratories are private, but the quantum channel and the classical channel are not. While the quantum states travel through the quantum channel, they are vulnerable to any interaction by a third party, the eavesdropper, Eve, whose aim is to learn about the key. Eve can also listen to all classical messages exchanged between Alice and Bob, but she can not change them.

A fundamental question is how to guarantee that in the end of the protocol the key is really safe to use in later applications. The basic intuition behind the security of a QKD protocol is based on the no cloning theorem, which states that it is not possible to make perfect copies of unknown quantum states. This theorem excludes the possibility that Eve intercepts the quantum channel, makes a perfect copy of the quantum states for herself, and forwards the original copies to Bob. Such a strategy would provide Eve with some knowledge about the encoded bit, without Alice and Bob noticing. Instead, Eve's interaction (attack) with the signals does not go unnoticed by Alice and Bob. There is a trade-off between the amount of information that leaks to Eve and the amount of disturbance she causes to the signal states. This disturbance is observed by Alice and Bob in their data, which allows them to infer that an eavesdropper interacted with the signals.

The main goal of a security proofs is to quantify the amount of information Eve obtains in the trade-off. Security proofs were given based on information-theoretic arguments by Devetak and Winter [31] or Renner, Kraus and Gisin [80, 57]. These proofs basically provide a bound on the amount of data that must be sacrificed in order to cut out Eve's knowledge in the classical communication protocols. Furthermore, it is also necessary for Alice and Bob to make their classical data strings uniformly distributed and correct errors. The cost of this task also shortens the length of the final key.

Alice and Bob's observations rarely identify the eavesdropping attack unambiguously. For most protocols (including the BB84 protocol) there is an entire class of eavesdropping strategies that can lead to the observed data. For each of the possible eavesdropping strategies, the Devetak-Winter security proof predicts a key rate. In order for Alice and Bob to be safe, they must protect themselves against the most powerful eavesdropping strategy. They must pick the smallest of the key rates, which is essentially the result of an optimization of the key rate over all possible attack strategies. The optimal eavesdropping strategy is therefore defined as the strategy that creates the smallest key rate among the class of strategies that fit to the observed data.

The primary goal of this thesis to advance the practical techniques used in the key rate optimization based on the Devetak-Winter security proof. In particular, we show how to exploit the underlying symmetries of a protocol in order to make the optimization problem simpler. This motivates us to provide explicit key rate calculations for a range of protocols

and scenarios: from highly theoretical protocols, such as the protocols using mutually unbiased bases in d-dimensional Hilbert spaces, to experimentally implemented protocols, such as the phase-encoded BB84 with realistic devices, to rather unusual setups, such as measurement device independent QKD with two senders and one adversary receiver.

Furthermore, we investigate the connection between the optimal eavesdropping strategy and the optimal cloning strategy. One type of eavesdropping strategy for Eve is to use an optimal quantum cloner, which makes the best possible copy of the signal states for her, while limiting the amount of disturbance in Bob's copy to match his observations. It is known that for the BB84 and the 6-state protocol the optimal cloning strategy is the optimal eavesdropping strategy, but for other protocols this connection is not established. We investigate under what conditions and for which protocols the optimal eavesdropping strategy is identical with the optimal cloning strategy.

Finally, we explore new tools with the aim to tackle protocols, for which optimal security solutions have not been derived so far. These tools are based on measurement device-independent QKD and the entropic uncertainty relation.

This thesis is organized as follows: In Chapter 2 we review the basic elements of quantum mechanics and representation theory that will be used later in the thesis. Chapter 3 is a summary of theoretical aspects of QKD: we describe the eavesdropping attacks in the source-replacement scheme, the Devetak-Winter key rate formalism under postselection, and the key rate optimization problem. Chapters 4 to 8 contain the results of our research. In Chapter 4 we show that, under certain conditions, the optimal attack carries a certain symmetry inherent to the protocol. The symmetries are helpful for the practical calculation of the key rates. In Chapter 5 we analyze the connection between the optimal eavesdropping and the optimal cloning transformation. Chapter 6 is devoted to proving the security of the unbalanced phase-encoded BB84 protocol taking into account the lossy phase modulator. This protocol differs from the BB84 protocol, because the effect of a lossy phase modulator changes the signal and measurement structure. In Chapter 7 we provide a security proof for a measurement device-independent QKD setup with B92 signal states, where Alice and Bob are both senders of quantum signals, and Eve is the receiver. This security proof acts as a new security proof technique for the strong reference pulse B92. In Chapter 8, we use an entropic uncertainty relation with the aim to prove the security of continuous-variable protocols. Finally, in Chapter 9 we draw the conclusions.

Chapter 2

Background

2.1 Postulates of quantum mechanics

In this section we review the postulates of quantum mechanics with a focus on information theory [76, 73, 84].

2.1.1 Quantum states

A *pure* quantum state is defined as normalized vector Ψ on a d-dimensional Hilbert space $\mathcal{H}$. In the Dirac notation the vector is represented by the symbol $|\Psi\rangle$, which is called a *ket*. The dual Hilbert space carries the vectors $\langle\Psi| = |\Psi\rangle^\dagger$ where the symbol $\dagger$ denotes the Hermitian conjugate. The inner product $\langle\Psi|\Phi\rangle$ of two vectors $|\Psi\rangle, |\Phi\rangle \in \mathcal{H}$ is identified with a scalar in $\mathbb{C}$. The outer product $|\Psi\rangle\langle\Phi|$ of two vectors $|\Psi\rangle, |\Phi\rangle \in \mathcal{H}$ defines a linear mapping from $\mathcal{H}$ to itself, i.e. an endomorphism on $\mathcal{H}$. We denote the set of all endomorphisms on $\mathcal{H}$ by $\mathcal{B}(\mathcal{H})$.

Definition 1 *A density operator $\rho \in \mathcal{B}(\mathcal{H})$ is a Hermitian, normalized and positive semidefinite operator, i.e. $\rho^\dagger = \rho$, $\operatorname{tr}\rho = 1$ and $\rho \geq 0$. The set of all density operators on $\mathcal{H}$ are defined as $\mathcal{D}(\mathcal{H})$.*

Not all quantum states are pure states. For example, we might be interested in a statistical mixture of pure states $|\Psi_x\rangle$ with probability $p(x)$, called an ensemble, or we might consider only the subsystem of a bigger system. The quantum states in these situations

are generally not pure. The first postulate of quantum mechanics defines general quantum states:

Postulate 1 *Density operators provide a general mathematical description of quantum states. Pure states are represented by projectors* $\rho = |\Psi\rangle\langle\Psi|$. *Quantum states that are not pure are called mixed states.*

The density operator of the ensemble mentioned above is given by

$$\rho = \sum_x p(x)|\Psi_x\rangle\langle\Psi_x|. \tag{2.1}$$

Since a density operator ρ is Hermitian, there is an eigenvalue decomposition

$$\rho = \sum_{i=1}^{d} \lambda_i |\phi_i\rangle\langle\phi_i| \tag{2.2}$$

with eigenvalues λ_i and eigenvectors $|\phi_i\rangle$.

If we define an orthonormal basis $\{|i\rangle, i = 0, ..., d\}$ of a finite-dimensional Hilbert space, a quantum state $\rho \in \mathcal{D}(\mathcal{H})$ can be expressed in that basis by

$$\rho = \sum_{i,j} a_{i,j} |i\rangle\langle j| \tag{2.3}$$

with complex coefficients $a_{i,j} = \langle i|\rho|j\rangle$. If the quantum state is pure, then $|\Psi\rangle = \sum_i c_i|i\rangle$ with complex coefficients $c_i = \langle i|\Psi\rangle$.

Qubits and Pauli operators

A *qubit* is a quantum state defined on a two-dimensional Hilbert space $\mathcal{H}_2$. The word qubit is a concatenation of the words 'quantum' and 'bit'. Qubits are the most suitable choice to represent a quantum analogue of the classical 'bit'. Therefore, the *canonical basis* (also called computational basis or standard basis) is typically denoted by the two normalized vectors $|0\rangle$ and $|1\rangle$ in analogy to the classical bits 0 and 1.

An important set of operators on $\mathcal{H}_2$ are the Pauli operators $\hat{\sigma}_x$, $\hat{\sigma}_y$ and $\hat{\sigma}_z$, or sometimes denoted by X, Y and Z. Together with the identity operator $\hat{\sigma}_0 \equiv \mathbb{1}$, they span an operator basis of the Hermitian operators on $\mathcal{H}_2$.

Definition 2 *The Pauli operators are Hermitian, positive and unitary. In the computational basis* $\{|0\rangle, |1\rangle\}$*, they are expressed by*

$$\hat{\sigma}_x = |0\rangle\langle 1| + |1\rangle\langle 0| \tag{2.4}$$
$$\hat{\sigma}_y = -i|0\rangle\langle 1| + i|1\rangle\langle 0| \tag{2.5}$$
$$\hat{\sigma}_z = |0\rangle\langle 0| - |1\rangle\langle 1|. \tag{2.6}$$

Any state ρ on the qubit Hilbert space is conveniently represented in the Bloch representation

$$\rho = \frac{1}{2}\left(\mathbb{1} + \vec{s}\cdot\vec{\sigma}\right) \tag{2.7}$$

where $\vec{\sigma} = (\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z)$ is a vector of Pauli operators. The vector $\vec{s} = (s_x, s_y, s_z)$ is called *Bloch vector* with real coefficients s_i with the property $|\vec{s}|^2 = s_x^2 + s_y^2 + s_z^2 \leq 1$. The vector $\vec{s}$ defines a representation of a qubit on the three-dimensional real sphere known as Bloch sphere. All pure states lie on the surface of the sphere with $|\vec{s}|^2 = 1$.

2.1.2 Composite systems

Individual quantum systems can be joined to form a composite quantum system. The second postulate of quantum mechanics defines joint systems.

Postulate 2 *Let us denote the Hilbert spaces corresponding to the systems A and B by* $\mathcal{H}_A$ *and* $\mathcal{H}_B$*. Then the joint space is given by the tensor product Hilbert space* $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$*. Quantum states of joint systems are denoted by density operators* ρ_{AB} *in* $\mathcal{D}(\mathcal{H}_{AB})$*.*

Perhaps we are only interested in one subsystem of a joint state ρ_{AB}. The state reduced to one subsystem is defined as follows.

Definition 3 *Let* $\rho_{AB} \in \mathcal{D}(\mathcal{H}_{AB})$*. The reduced state* ρ_A *of* ρ_{AB} *on the subsystem A is obtained by taking the partial trace over the system B*

$$\rho_A = \mathrm{tr}_B\{\rho_{AB}\}. \tag{2.8}$$

Similarly, the the partial trace over A results in a reduced state $\rho_B = \mathrm{tr}_A\,\rho_{AB}$ *on the subsystem B.*

If the individual subsystems of a joint state ρ_{AB} are independent, the state is said to be a product state.

Definition 4 *A state ρ_{AB} is said to be a product state if it is of the form $\rho_{AB} = \rho_A \otimes \rho_B$. A pure state $|\Psi\rangle_{AB}$ is said to be a product state if it is of the form $|\Psi\rangle_{AB} = |\Psi\rangle_A \otimes |\Psi\rangle_B$.*

For example, suppose $\{|i_A\rangle\}_i$ and $\{|j_B\rangle\}_j$ are two orthonormal bases of the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. One choice of a basis for the joint system $\mathcal{H}_{AB}$ is a product basis with the basis vectors $|i_A\rangle \otimes |j_B\rangle \equiv |i_A, j_B\rangle$.

A unique quantum mechanical feature of composite systems is *entanglement*. Entanglement is a resource that plays a fundamental role in quantum communication and quantum computation.

Definition 5 *A state is called separable, if it is a convex combination of product states*

$$\rho_{sep} = \sum_x p(x)\rho_A^x \otimes \rho_B^x. \tag{2.9}$$

Definition 6 *A state is called entangled if it is not separable.*

An important example of two-qubit entangled states are the four *Bell states*.

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \tag{2.10}$$

The Bell states are maximally entangled and form a basis of a two-qubit Hilbert space. They are also commonly referred to as EPR states.

We introduce two useful theorems for composite systems:

Theorem 1 ***Schmidt decomposition.*** *Let $|\Psi\rangle_{AB}$ be a pure state on the composite system AB. Then there exist orthonormal bases $\{|i_A\rangle\}_i$ and $\{|i_B\rangle\}_i$ of systems A and B, and non-negative real numbers λ_i with the property that*

$$|\Psi\rangle_{AB} = \sum_i \lambda_i |i_A\rangle|i_B\rangle. \tag{2.11}$$

The bases are called Schmidt bases, and the coefficients λ_i are called Schmidt coefficients.

This theorem implies that the eigenvalue spectra of the reduced states ρ_A and ρ_B are identical, namely $\{\lambda_i^2\}_i$.

Theorem 2 ***Purification*** *Suppose the state ρ_A on system A has a spectral decomposition $\rho_A = \sum_i p_i |i_A\rangle\langle i_A|$. Then there exists an additional system R and a pure state $|\Psi\rangle_{AR}$ on the joint system AR such that $\rho_A = \mathrm{tr}_R |\Psi\rangle\langle\Psi|_{AR}$. The pure state $|\Psi\rangle_{AR}$ is called a purification of ρ_A. If we introduce an orthonormal basis $\{|i_R\rangle\}_i$ on the system R, then the purification can be constructed as follows*

$$|\Psi\rangle_{AR} = \sum_i \sqrt{p_i} |i_A\rangle|i_R\rangle. \tag{2.12}$$

2.1.3 Measurements

In a measurement process, the quantum state ρ interacts with a measurement device, which then reveals some information about the quantum state. The description of the measurement is the third postulate of quantum mechanics:

Postulate 3 *A measurement is a set of measurement operators (Kraus operators) $\{\hat{K}_x\}_x$ acting on a Hilbert space $\mathcal{H}$. Each measurement operator $\hat{K}_x$ is associated to a measurement outcome x. The measurement operators satisfy the completeness relation $\sum_x \hat{K}_x^\dagger \hat{K}_x = \mathbb{1}$. If we measure a state $\rho \in \mathcal{D}(\mathcal{H})$, the probability to obtain the outcome x is*

$$p(x) = \mathrm{tr}\{\hat{K}_x \rho \hat{K}_x^\dagger\}. \tag{2.13}$$

The post-measurement state is

$$\rho_x = \frac{\hat{K}_x \rho \hat{K}_x^\dagger}{p(x)}. \tag{2.14}$$

If the state after the measurement is not of interest, the *positive operator valued measure* (POVM) formalism is a convenient mathematical tool to describe the measurement.

Definition 7 *A POVM* $\mathbf{M}$ *is a set of positive semidefinite operators* $\hat{F}_x \in \mathcal{B}(\mathcal{H})$*, called POVM elements. The POVM elements satisfy* $\sum_x \hat{F}_x = \mathbb{1}$*. In terms of the Kraus operators the POVM elements are given by* $\hat{F}_x = \hat{K}_x^\dagger \hat{K}_x$*.*

A special case of a measurement is the *projective measurement* or *von Neumann* measurement. The measurement operators of a von Neumann measurement are orthogonal projectors $\hat{K}_x = |\phi_x\rangle\langle\phi_x|$. They are Hermitian $\hat{K}_x^\dagger = \hat{K}_x$ and satisfy $\hat{K}_x\hat{K}_y = K_x\delta_{x,y}$. A projective measurement defines an *observable* $\hat{X}$, which is a Hermitian operator with a spectral decomposition

$$\hat{X} = \sum_x x|\phi_x\rangle\langle\phi_x|. \tag{2.15}$$

When we say we measure the observable $\hat{X}$, it means that a state ρ is measured with respect to the projective measurement that defines the observable. The expectation value of an observable $\hat{X}$ is

$$\langle\hat{X}\rangle_\rho = \mathrm{tr}\{\rho\hat{X}\}. \tag{2.16}$$

2.1.4 Quantum evolution

Postulate 4 *The time evolution of a closed quantum system is a unitary evolution, facilitated by the time evolution operator* $\hat{U}(t,t_0)$*. A pure state* $|\Psi(t_0)\rangle$ *at time* t_0 *evolves to a state* $|\Psi(t)\rangle = \hat{U}(t,t_0)|\Psi(t_0)\rangle$ *at time* t*. Mixed states evolve according to* $\rho(t) = \hat{U}(t,t_0)\rho(t_0)\hat{U}(t,t_0)^\dagger$*.*

The time evolution operator is governed by the Schrödinger equation:

$$i\hbar\frac{d}{dt}\hat{U}(t,t_0) = \hat{H}\ \hat{U}(t,t_0) \tag{2.17}$$

In this equation $\hat{H}$ is a Hermitian operator called Hamiltonian, and the constant $\hbar$ is Planck's constant. We choose here the convention where $\hbar = 1$. In case of a time independent Hamiltonian, the time evolution operator obtained by solving the Schrödinger equation is

$$\hat{U}(t,t_0) = e^{i\hat{H}(t-t_0)/\hbar}. \tag{2.18}$$

The Schrödinger equation for the time evolution operator implies the Schrödinger equation for pure states $|\Psi(t)\rangle$

$$i\hbar\frac{d|\Psi(t)\rangle}{dt} = \hat{H}|\Psi(t)\rangle, \tag{2.19}$$

and the von Neumann equation for mixed states $\rho(t)$

$$i\hbar\frac{d\rho(t)}{dt} = [\hat{H}, \rho(t)]. \tag{2.20}$$

In this equation the bracket $[\hat{X}, \hat{Y}] := \hat{X}\hat{Y} - \hat{Y}\hat{X}$ is the commutator.

The evolution of an *open* quantum system refers to the evolution of a subsystem A that is in contact with an environment E. The joint system AE evolves like a closed system. An open evolution also refers to the evolution of a system A to another system B.

The evolution of an open system is described by a *completely positive and trace preserving* (CPTP) map, or *quantum map*. The important feature of a CPTP map is that density operators are mapped onto density operators. First, let us define a positive map:

Definition 8 *A positive map $\mathcal{E} : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ takes positive semidefinite operators to positive semidefinite operators.*

If a positive map $\mathcal{E}$ acts only on a subsystem A of a composite system AB, we must ensure that the result is again a positive semidefinite operator. Surprisingly, though, the tensor product of two positive maps is not necessarily positive. The completely positive maps, which are a subset of the positive maps, have a stronger requirement on positivity, that guarantees the positivity of tensor products:

Definition 9 ***Completely positive (CP) maps*** *A completely positive map $\mathcal{E} : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$ is a linear map with the property that for any Hilbert space $\mathcal{H}_R$, the map $\mathcal{E} \otimes \mathbb{1}_R$ is positive.*

Finally, the map must be trace preserving, meaning that $\operatorname{tr}\mathcal{E}(\rho) = \operatorname{tr}(\rho)$.

The Choi-Jamiolkowski isomorphism and the Stinespring dilation

The Choi-Jamiolkowski isomorphism links quantum maps to density operators. It is a useful tool in that it reduces the study of quantum maps to the study of density operators.

Let $\mathcal{H}_A$ be isomorphic to $\mathcal{H}_{A'}$ with orthonormal bases $\{|i_A\rangle\}$ and $\{|i_{A'}\rangle\}$ for $i = 1, ..., d$. We define the maximally entangled state on the joint Hilbert space $\mathcal{H}_{AA'}$ by

$$|\Phi^+\rangle_{AA'} = \frac{1}{\sqrt{d}} \sum_i |i_A\rangle|i_{A'}\rangle. \tag{2.21}$$

Theorem 3 *The Choi-Jamiolkowski isomorphism relates the CPTP map $\mathcal{E} : \mathcal{B}(\mathcal{H}_{A'}) \to \mathcal{B}(\mathcal{H}_B)$ to a density operator σ_{AB} on $\mathcal{D}(\mathcal{H}_{AB})$ by the rule*

$$\sigma_{AB} = (\mathbb{1}_A \otimes \mathcal{E})|\Phi^+\rangle\langle\Phi^+|_{AA'} \tag{2.22}$$

The map $\mathcal{E}$ is recovered from σ_{AB} by the reverse transformation

$$\mathcal{E}(\rho_A) = d \operatorname{tr}_A\{\rho_A^T \otimes \mathbb{1}_B \sigma_{AB}\}. \tag{2.23}$$

The symbol T stands for transposition with respect to the basis $\{|i_A\rangle\}$.

The Stinespring dilation theorem relates every CPTP map to a unitary map on a dilated Hilbert space.

Theorem 4 *Let $\mathcal{E} : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_A)$ be a CPTP map. Then there exists a an environment $\mathcal{H}_E$ and a unitary map U on $\mathcal{B}(\mathcal{H}_{AE})$ such that*

$$\mathcal{E}(\rho_A) = \operatorname{tr}_E\{U(\rho_A \otimes |0\rangle\langle 0|_E)U^\dagger\}. \tag{2.24}$$

The Stinespring theorem also applies if the quantum map takes a system A to a different system B.

2.2 Basic quantum optics

Quantum communication protocols use light as a preferred carrier of information. We review in this section the fundamentals of quantum optics that are relevant for the further chapters of this thesis [84, 73, 13, 94].

2.2.1 Quantum harmonic oscillator

The classical electromagnetic field is composed of independent modes which are solutions to Maxwell's equations. When we quantize the electromagnetic field, a single mode is described by a quantum harmonic oscillator governed by the Hamiltonian

$$\hat{H} = \hbar\omega(\hat{a}^\dagger\hat{a} + 1/2). \tag{2.25}$$

In this equation, ω is the frequency of the harmonic oscillator. The operators $\hat{a}$ and $\hat{a}^\dagger$ are not Hermitian and they satisfy the commutation relation $[\hat{a}, \hat{a}^\dagger] = 1$. Their product defines the Hermitian number operator $\hat{n} = \hat{a}^\dagger\hat{a}$. The number operator has a discrete eigenbasis $|n\rangle$ with eigenvalues n which denote the number of excitations in the mode. These eigenstates are called the *Fock states* or photon number states. Each excitation corresponds to a photon in the mode, for example $|n\rangle$ denotes n photons in the mode.

The operators $\hat{a}$ and $\hat{a}^\dagger$ annihilate and create mode excitations according to the rule

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle, \tag{2.26}$$

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle. \tag{2.27}$$

They are commonly referred to as *annihilation and creation operators*.

Quadrature operators

The annihilation and creation operators are related to the *quadrature operators*

$$\hat{x} = \frac{1}{\sqrt{2}}(\hat{a}^\dagger + \hat{a}), \tag{2.28}$$

$$\hat{p} = \frac{i}{\sqrt{2}}(\hat{a}^\dagger - \hat{a}). \tag{2.29}$$

The $\hat{x}$ and $\hat{p}$ operators are the analogue of the position and momentum operators. They satisfy the commutator $[\hat{x}, \hat{p}] = i$. An $\hat{x}$ or $\hat{p}$ quadrature measurement is referred to as a *homodyne measurement*. Since $\hat{x}$ and $\hat{p}$ are Hermitian operators, they give rise to a complete basis with eigenvectors $|x\rangle$ and $|p\rangle$ and continuous spectra $x, p \in \mathbb{R}$

$$\hat{x} = \int dx\ x\ |x\rangle\langle x|, \tag{2.30}$$

$$\hat{p} = \int dp\ p\ |p\rangle\langle p|. \tag{2.31}$$

Every quantum state ρ must satisfy the Heisenberg uncertainty relation

$$\mathrm{Var}_x(\rho)\mathrm{Var}_p(\rho) \geq \frac{1}{4}, \tag{2.32}$$

where $\mathrm{Var}_x(\rho) = \langle \hat{x}^2 \rangle_\rho - \langle \hat{x} \rangle_\rho^2$ and $\mathrm{Var}_p(\rho) = \langle \hat{p}^2 \rangle_\rho - \langle \hat{p} \rangle_\rho^2$. States, for which the '=' sign holds, are called minimum uncertainty states.

2.2.2 Coherent states and squeezed states

A *coherent state* $|\alpha\rangle$ is a particular state of the quantum harmonic oscillator. It is an eigenstate of the annihilation operator $\hat{a}$ with a complex eigenvalue $\alpha = \mathrm{e}^{i\phi}|\alpha|$. The coherent state corresponding to the eigenvalue α is

$$|\alpha\rangle = e^{|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n}} |n\rangle. \tag{2.33}$$

If we perform a quadrature measurement on $|\alpha\rangle$, the distribution of the measurement outcomes x follows a Gaussian distribution

$$p_\alpha(x) = |\langle x|\alpha\rangle|^2 = \frac{1}{\sqrt{2\pi \mathrm{Var}_x(|\alpha\rangle)}} \exp\left(-\frac{(x - \langle x \rangle_{|\alpha\rangle})^2}{2\mathrm{Var}_x(|\alpha\rangle)} \right), \tag{2.34}$$

with mean $\langle \hat{x} \rangle_\alpha = \langle \alpha|\hat{x}|\alpha\rangle = \sqrt{2}\mathrm{Re}[\alpha]$ and variance $\mathrm{Var}_x(|\alpha\rangle) = \frac{1}{2}$. A measurement of the $\hat{p}$ quadrature also results in a Gaussian profile with mean $\langle \hat{p} \rangle_\alpha = \langle \alpha|\hat{p}|\alpha\rangle = \sqrt{2}\mathrm{Im}[\alpha]$ and $\mathrm{Var}_p(|\alpha\rangle) = \frac{1}{2}$. Since coherent states satisfy the equality in the Heisenberg uncertainty relation, thus they are minimum uncertainty states.

Coherent states are important because they describe the light that exits a laser. A phase randomized laser source emits a mixture of coherent states

$$\rho_{\mathrm{laser}} = \int \frac{d\phi}{2\pi} |\mathrm{e}^{i\phi}|\alpha|\rangle\langle \mathrm{e}^{i\phi}|\alpha||. \tag{2.35}$$

This mixed state is diagonal in the Fock basis

$$\rho_{\mathrm{laser}} = \sum_{n=0}^{\infty} e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!} |n\rangle\langle n|. \tag{2.36}$$

The probability to observe an n-photon state follows a Poisson distribution $p(n) = e^{-|\alpha|^2} \frac{|\alpha|^{2n}}{n!}$.

Another interesting quantum state of the quantum harmonic oscillator is a squeezed coherent state. A squeezed coherent state

$$|\alpha, r\rangle = \hat{S}(r)|\alpha\rangle \tag{2.37}$$

is obtained by applying the squeezing operator $\hat{S}(r) = \exp(r(\hat{a}^2 - \hat{a}^{\dagger 2})/2)$ to the coherent state $|\alpha\rangle$. The coefficient $r \in \mathbb{R}$ is called the squeezing parameter. If we perform an $\hat{x}$ or $\hat{p}$ quadrature measurement on $|\alpha, r\rangle$, the outcomes are distributed according to a Gaussian distribution. The expectation values are $\langle\hat{x}\rangle_{|\alpha,r\rangle} = \sqrt{2}\ \mathrm{Re}[\alpha]$ and $\langle\hat{p}\rangle_{|\alpha,r\rangle} = \sqrt{2}\ \mathrm{Im}[\alpha]$. Furthermore, the states $|\alpha, r\rangle$ are minimum uncertainty states with a squeezed variance in one quadrature and an anti-squeezed variance in the other quadrature:

$$\mathrm{Var}_x(|\alpha, r\rangle) = \frac{1}{2}e^{-2r}, \quad \mathrm{Var}_p(|\alpha, r\rangle) = \frac{1}{2}e^{2r}. \tag{2.38}$$

2.2.3 Two-mode squeezed state

The counterpart to the maximally entangled state $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ on a two-qubit Hilbert space is the two-mode squeezed state. In the Fock basis of two systems A and B, it is given by

$$|\Psi_{\mathrm{TMSS}}\rangle_{AB} = \sqrt{1-\lambda^2}\sum_n \lambda^n |n\rangle_A |n\rangle_B, \tag{2.39}$$

where $\lambda = \tanh r$. Let $\hat{x}_A$, $\hat{x}_B$ and $\hat{p}_A$, $\hat{p}_B$ be the quadrature operators of the systems A and B. The wave functions of the two-mode squeezed state expressed in the quadrature operator bases are

$$\langle x_A, x_B|\Psi_{\mathrm{TMSS}}\rangle = \frac{1}{\sqrt{\pi}}\exp\left[-\mathrm{e}^{-2r}\frac{(x_A + x_B)^2}{4} - \mathrm{e}^{2r}\frac{(x_A - x_B)^2}{4}\right] \tag{2.40}$$

$$\langle p_A, p_B|\Psi_{\mathrm{TMSS}}\rangle = \frac{1}{\sqrt{\pi}}\exp\left[-\mathrm{e}^{-2r}\frac{(p_A - p_B)^2}{4} - \mathrm{e}^{2r}\frac{(p_A + p_B)^2}{4}\right] \tag{2.41}$$

If we measure the $\hat{x}_A$ quadrature on system A, we effectively prepare on B a squeezed coherent state $|\alpha', r'\rangle_B = \langle x_A|\Psi_{\mathrm{TMSS}}\rangle$ with variance $\mathrm{Var}_{x_B}(|\alpha', r'\rangle) = \frac{1}{2\cosh 2r}$ and mean $\langle x_B\rangle_{|\alpha',r'\rangle} = \tanh 2r\ x_A$. Furthermore, the probability distribution to obtain the outcome x_A on system A follows a Gaussian distribution

$$p(x_A) = \frac{1}{\sqrt{2\pi\mathrm{Var}_{x_A}}}\exp\left[-\frac{x_A^2}{2\mathrm{Var}_{x_A}}\right] \tag{2.42}$$

centred around zero with variance $\mathrm{Var}_{x_A} = \frac{\cosh 2r}{2}$.

2.3 Quantum information theory

In this section we give a short introduction to quantum information theory according to Ref. [73].

2.3.1 Notation

Let X be a random variable that takes on values x and has a probability distribution $p(x)$. In the language of quantum mechanics, the classical random variable X can be represented by a (classical) state

$$\rho_X = \sum_x p(x)|x\rangle\langle x|_X. \tag{2.43}$$

on a system X, which we denote by the same letter as the random variable. In the following, we denote quantum systems by letters from the beginning of the alphabet, such as A, B or E, and classical systems by letters from the end of the alphabet, such as X and Y.

If there are two random variables X and Y with a joint probability distribution $p(x, y)$ and values (x, y), the classical state

$$\rho_{XY} = \sum_{x,y} p(x, y)|x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y \tag{2.44}$$

representing these random variables lives on two classical subsystems X and Y. This notation is suitable to describe hybrid systems, where one subsystem is quantum, and the other subsystem is classical, such as the classical-quantum (cq) state

$$\rho_{XB} = \sum_x p(x)|x\rangle\langle x|_X \otimes \rho_B^x. \tag{2.45}$$

This state could be obtained, for example, by partial measurement of the subsystem A of a bipartite quantum state ρ_{AB} with respect to a POVM. If the outcome of the measurement is x, which happens with probability $p(x)$, the remaining conditional state on system B is ρ_B^x.

2.3.2 Classical entropy and mutual information

Consider we inquire the value of a random variable X. The *Shannon entropy*

$$H(X) \equiv H(p_x) = -\sum_x p(x) \log_2 p(x). \tag{2.46}$$

is a measure of uncertainty that we have about the outcome of the inquiry. If the logarithm is taken to the basis 2, the entropy is in units of bits.

The entropy of a joint probability distribution $p(x, y)$ is captured in the *joint entropy*

$$H(X, Y) = -\sum_{x,y} p(x, y) \log_2 p(x, y). \tag{2.47}$$

If we ignore the system X, we can recover the probability distribution on the system Y alone by taking the marginal of $p(x, y)$, which is defined by $p(y) = \sum_x p(x, y)$.

We define the conditional entropy of X with respect to Y by

$$H(X|Y) = H(X, Y) - H(Y). \tag{2.48}$$

The conditional entropy is a measure of the uncertainty in X, provided we know Y. Furthermore, it follows from this definition that $H(X|Y) + H(Y) = H(Y|X) + H(X)$.

We define the mutual information, which is a measure of the correlations between two classical systems by

$$I(X : Y) = H(X) + H(Y) - H(X, Y). \tag{2.49}$$

2.3.3 Quantum entropy and quantum mutual information

The entropy of a quantum state ρ_A on the system A is called *von Neumann entropy* and is defined by

$$S(A) \equiv S(\rho_A) = -\operatorname{tr}\{\rho_A \log_2 \rho_A\} \tag{2.50}$$

If the eigenvalues of ρ_A are $\{\lambda_i\}_i$, the von Neumann entropy can be calculated straightforwardly

$$S(\rho_A) = -\sum_i \lambda_i \log_2 \lambda_i. \tag{2.51}$$

For a composite state ρ_{AB}, the joint von Neumann entropy is defined by

$$S(A, B) = -\operatorname{tr}_{AB}\{\rho_{AB} \log_2 \rho_{AB}\}. \tag{2.52}$$

We define the quantum conditional entropy and the quantum mutual information analogously to the classical case in Eqs. (2.48) and (2.49).

In the following we are interested in the correlations between a classical system X and a quantum system B described by the classical-quantum state ρ_{XB} in Eq. 2.45. The joint entropy of this state can be explicitly calculated

$$S(X,B) = S(\rho_{XB}) = H(X) + \sum_x p(x) S(\rho_B^x). \tag{2.53}$$

In analogy to the classical conditional entropy, the uncertainty about the quantum system B, given full access to the classical system X, is captured in the conditional entropy

$$S(B|X) = \sum_x p(x) S(\rho_B^x). \tag{2.54}$$

Finally, the mutual information between X and B

$$I(X:B) = S(\rho_B) - \sum_x p(x) S(\rho_B^x) \tag{2.55}$$

is given a special name, the *Holevo quantity*, and is denoted by $\chi(X:B)$.

Lastly, quantum operations $\mathcal{E}$ never increase the mutual information [see, for example, Ref. [73], page 522]:

Theorem 5 *Let AB be a composite system, and let $\mathcal{E} : \mathcal{B}(\mathcal{B}) \to \mathcal{B}(\mathcal{B}')$ be a quantum operation. The mutual information never increases under quantum operations on one subsystme, i.e.,*

$$I(A:B) \geq I(A:B'). \tag{2.56}$$

2.4 Representation theory

The concept of symmetries occurs very commonly in nature. The tools to analyze symmetries with mathematical rigour are provided in group and representation theory. In this section we give a short introduction to representation theory of finite groups with emphasis on applications to the topics in later chapters. See also Refs. [3, 70].

2.4.1 Groups

A group represents the concept of symmetry in a mathematical sense.

Definition 10 *A group G is a (finite or infinite) set of elements $(g_1, g_2, ...)$ and an operation called group multiplication, which associates to any two elements g_1 and g_2 a third element $g_1 g_2$. The following axioms define the group structure:*

1. *There exists an identity element e in G that satisfies: $eg = ge = g$ for all $g \in G$.*
2. *There exists an inverse element g^{-1} for each $g \in G$ that satisfies: $gg^{-1} = g^{-1}g = e$.*
3. *The group multiplication is associative: $(g_1 g_2)g_3 = g_1(g_2 g_3)$ for all $g_1, g_2, g_3 \in G$.*

The group elements are divided into conjugacy classes. Each group element belongs to exactly one conjugacy class.

Definition 11 *The conjugacy class K_g contain all group elements $g' = hgh^{-1}$ for all $h \in G$. For finite groups the number of group elements n_{K_g} in the conjugacy class K_g defines the order of the class.*

2.4.2 Representations

The idea of representation theory is to assign to each abstract group element a unitary operator which acts on a real or complex vector space. To make things fit the language of quantum mechanics, let the vector space be a the Hilbert space $\mathcal{H}$ with dimension n. We define the abstract group of all n-dimensional unitary operators acting on $\mathcal{H}$ by $U(n, \mathcal{H})$. Every group element g is now identified with an n-dimensional unitary operator U_g in $U(n, \mathcal{H})$. The homomorphism $\mathbf{U}$ that takes the group elements g to the unitary operators U_g is called a *unitary representation* of G on $U(n, \mathcal{H})$:

$$\mathbf{U} : G \to U(n, \mathcal{H}), \tag{2.57}$$

$$g \mapsto U_g. \tag{2.58}$$

The representation conserves the group structure on $U(n, \mathcal{H})$, but with the group multiplication replaced by multiplication between operators: $U_{g_1} U_{g_2} = U_{g_1 g_2}$, $U_g^{-1} = U_{g^{-1}}$ and $U_e = \mathbb{1}_n$, where $\mathbb{1}_n$ is the identity operator on the n-dimensional Hilbert space. Since the operators are unitary, $U_g^{-1} = U_g^\dagger$.

The operators U_g of a group representation act as transformations on $\mathcal{H}$ and are suitable to describe the symmetries of objects on $\mathcal{H}$. In the forthcoming chapters, these objects are sets of quantum states.

Definition 12 *Let* $\mathbf{S}$ *be a set containing* $|\mathbf{S}|$ *quantum states* $\{|\varphi_1\rangle, |\varphi_2\rangle, ..., |\varphi_{|\mathbf{S}|}\rangle\}$ *defined on* $\mathcal{D}(\mathcal{H})$*, and let* U_g *be a unitary representation of the group* G *on* $U(n, \mathcal{H})$*. The set* $\mathbf{S}$ *is called* G*-invariant, if*

$$U_g \, |\varphi_x\rangle \in \mathbf{S} \tag{2.59}$$

for all $|\varphi_x\rangle \in \mathbf{S}$*, and all* $g \in G$*. A* G*-invariant set is essentially mapped onto itself by the action of the group* G*.*

2.4.3 Irreducible representations

There are many representations of the group G on a finite-dimensional Hilbert space $\mathcal{H}$. Two representations $\mathbf{R}$ and $\mathbf{U}$ are said to be equivalent ($\mathbf{R} \cong \mathbf{U}$), if there exists a unitary transformation S in $U(n, \mathcal{H})$ such that

$$R_g = S U_g S^\dagger \quad \forall g \in G. \tag{2.60}$$

This transformation corresponds to a basis transformation. The equivalent representations define an equivalence class of representations. In order to characterize all representations of the group G, it is sufficient to determine one representation in each equivalence class.

One goals of representation theory is to characterized all representations of a group.

Definition 13 *A subspace* $\mathcal{H}'$ *of* $\mathcal{H}$ *is called invariant under* $\mathbf{U}$*, or* $\mathbf{U}$*-invariant, if for all* U_g *and all vectors* $|v\rangle \in \mathcal{H}'$*,* $U_g|v\rangle \in \mathcal{H}'$*.*

Definition 14 *A representation is called irreducible, if the only invariant subspaces are the null-space and* $\mathcal{H}$ *itself. Otherwise (if there exists a proper subspace), the representation it is called reducible.*

A Hilbert space $\mathcal{H}$ carrying a reducible representation $\mathbf{U}$ can be decomposed into a direct sum of subspaces $\mathcal{H}_i$, each carrying irreducible representations $\mathbf{U}_i$:

$$\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2 \oplus ... \mathcal{H}_k \tag{2.61}$$

$$\mathbf{U} = \mathbf{U}_1 \oplus \mathbf{U}_2 \oplus ... \mathbf{U}_k. \tag{2.62}$$

Since this decomposition is unique, the irreducible representations form the fundamental building blocks of the representation of a group.

2.4.4 Characters

In order to decompose reducible representation into irreducible representations (irreps) $\mathbf{U}^\mu$, we must first identify all irreps of the group. For many groups the irreps can be found in tables, such as in Refs. [56, 17] for the crystallographic groups. Each irrep is identified by the character, which is defined as follows:

Definition 15 *Let $\mathbf{U}^\mu$ be a representation that takes the group elements g of a group G to the operators U_g on $U(n, \mathcal{H})$. The character χ^μ of the irrep $\mathbf{U}^\mu$ is a vector with entries $\chi^\mu(g) = \mathrm{tr}\{U_g^\mu\}$ for each $g \in G$.*

The character of representation is an important quantity. Some useful properties of the characters are listed here.

1. The character $\chi^\mu\chi^\nu$ of the tensor product $\mathbf{U}^\mu \otimes \mathbf{U}^\nu$ is given by

$$\chi^\mu\chi^\nu(g) = \chi^\mu(g)\chi^\nu(g). \tag{2.63}$$

   This is a simple consequence of the trace of tensor products.

2. All group elements in the same conjugacy class K_g have the same character entry $\chi(g)$. This is a consequence of the cyclic property of the trace: $\chi(hgh^{-1}) = \mathrm{tr}\{U_h U_g U_h^{-1}\} = \mathrm{tr}\{U_g\} = \chi(g)$.

3. The number of different irreps of a group G is equal to the number of conjugacy classes. If a group has a finite number of conjugacy classes, the number of irreps is also finite.

4. Two representations $\mathbf{U}^\mu$ and $\mathbf{U}^\nu$ of a group G are equivalent $\mathbf{U}^\mu \cong \mathbf{U}^\nu$, if and only if they have the same character.

5. The characters of two irreps $\mathbf{U}^\mu$ and $\mathbf{U}^\nu$ of a group G satisfy the orthonormality conditions $\langle\chi^\mu, \chi^\nu\rangle = \delta_{\mu,\nu}$. The inner product is defined by

$$\langle\chi^\mu, \chi^\nu\rangle = \frac{1}{|G|}\sum_g (\chi^\mu(g))^* \chi^\nu(g), \tag{2.64}$$

   where the $*$ stands for complex conjugation.

Table 2.1: The character table of the Dihedral Group D_4. The horizontal line divides the real irreps ($\mathbf{U}^1$ to $\mathbf{U}^5$) from the symplectic irreps ($\mathbf{U}^6$ and $\mathbf{U}^7$).

D_4	(1) e	(2) C_{4z}	(2) C_{2z}	(4) C_{2y}	(4) C_{2xy}	(1) $\bar{e}$	(2) $\bar{C}_{4z}$
$\mathbf{U}^1$	1	1	1	1	1	1	1
$\mathbf{U}^2$	1	1	1	-1	-1	1	1
$\mathbf{U}^3$	1	-1	1	1	-1	1	-1
$\mathbf{U}^4$	1	-1	1	-1	1	1	-1
$\mathbf{U}^5$	2	0	-2	0	0	2	0
$\mathbf{U}^6$	2	$\sqrt{2}$	0	0	0	-2	$-\sqrt{2}$
$\mathbf{U}^7$	2	$-\sqrt{2}$	0	0	0	-2	$\sqrt{2}$

As an illustration, the character tables of the groups D_4 and C_4 are shown in Tables 2.1 and 2.2. Each row of a character table corresponds to a group irrep $\mathbf{U}^\mu$. The irrep in the first row is always the trivial irrep, where all group elements are identified on a one-dimensional space by the identity operator 1. The characters of this representation are trivially all equal to 1. The columns denote the conjugacy classes, e.g. e, C_{4z}, etc. and the number of elements in the conjugacy class, e.g. (1), (2), etc. The first column always shows the character of the identity element e, and is equal to the dimension n of the representation.

The symmetry group D_4 plays an important role in QKD, as it is the symmetry group of the signal states of the BB84 protocol. The group has 16 elements, divided into 7 conjugacy classes. Therefore, there are also 7 different irreps. The symmetry group C_4 is the symmetry group of the unbalanced phase-encoded BB84 protocol in Chapter 6. The group has 8 elements, 8 conjugacy classes, and 8 different irreps.

2.4.5 The complex conjugate irrep

Let $\mathbf{U}$ be an irrep of the group G with unitary operators U_g. The operators U_g can be represented by $n \times n$ matrices with complex matrix elements. We can construct a new irrep of the group G by taking the complex conjugate of the matrices with respect to a basis. The complex conjugate matrices then define the complex conjugate irrep $\mathbf{U}^*$ [see

Table 2.2: The character table of the Cyclic Group C_4. The order of each conjugacy class is one, and all irreps are one-dimensional. We define $\omega = e^{-i\pi/4}$. The horizontal line divides the real irreps ($\mathbf{U}^1$ and $\mathbf{U}^2$) from the complex irreps ($\mathbf{U}^3$ to $\mathbf{U}^8$).

C_4	e	C_{4z}	C_{2z}	C_{4z}^{-1}	$\bar{e}$	$\bar{C}_{4z}$	$\bar{C}_{2z}$	$\bar{C}_{4z}^{-1}$
$\mathbf{U}^1$	1	1	1	1	1	1	1	1
$\mathbf{U}^2$	1	-1	1	-1	1	-1	1	-1
$\mathbf{U}^3$	1	$-i$	-1	i	1	$-i$	-1	i
$\mathbf{U}^4$	1	i	-1	$-i$	1	i	-1	$-i$
$\mathbf{U}^5$	1	ω	$-i$	ω^7	-1	ω^5	i	ω^3
$\mathbf{U}^6$	1	ω^7	i	ω	-1	ω^3	$-i$	ω^5
$\mathbf{U}^7$	1	ω^5	$-i$	ω^3	-1	ω	i	ω^7
$\mathbf{U}^8$	1	ω^3	i	ω^5	-1	ω^7	$-i$	ω

for example Refs. [56, 17]]. Although complex conjugation depends on the choice of basis, the complex conjugate irreps defined in this way are all equivalent up to unitary rotations.

There is a relationship between the irreps $\mathbf{U}$ and $\mathbf{U}^*$. If the irrep $\mathbf{U}$ is real, then $\mathbf{U}^*$ is necessarily also real, and therefore, $\mathbf{U}^* \cong \mathbf{U}$. If the vector space is complex, there are two cases: (i) The matrices of the irrep $\mathbf{U}$ have complex entries, but the characters $\chi(g)$ are real (symplectic irrep). Due to the uniqueness of the characters, it follows that $\mathbf{U} \cong \mathbf{U}^*$. (ii) The matrices of the irrep $\mathbf{U}$ have complex entries and the characters $\chi(g)$ are complex (complex irrep). Then, $\mathbf{U}^*$ is necessarily different from $\mathbf{U}$.

In the character table of the Dihedral Group D_4 in Table 2.1, the irreps $\mathbf{U}^1$ through $\mathbf{U}^5$ are real, and $\mathbf{U}^6$ and $\mathbf{U}^7$ are symplectic. For the Cyclic Group C_4 in Table 2.2, the irreps $\mathbf{U}^1$ and $\mathbf{U}^2$ are real, and the rest are complex.

2.4.6 Tensor products of irreps

Direct sum decomposition

The tensor product of two irreps $\mathbf{U}^\mu \otimes \mathbf{U}^\nu$ on $\mathcal{H}^\mu \otimes \mathcal{H}^\nu$ is normally a reducible representation and can be decomposed into a direct sum of irreps $\mathbf{U}^\omega$ on Hilbert spaces $\mathcal{H}_i^\omega$:

$$\mathcal{H}^\mu \otimes \mathcal{H}^\nu = \bigoplus_\omega \bigoplus_{i=1}^{m_\omega} \mathcal{H}_i^\omega. \tag{2.65}$$

In this decomposition, the index i runs over $1, ..., m_\omega$, and the irrep $\mathbf{U}^\omega$ occurs m_ω times in the decomposition.

Which irreps $\mathbf{U}^\omega$ appear in the direct sum decomposition? What are their multiplicities m_ω? Once the character table of a group G has been established there is a systematic method to answer these questions based on character theory. The multiplicities m_μ are uniquely determined in the following theorem:

Theorem 6 *The multiplicity m_ω of the irrep $\mathbf{U}^\omega$ in the direct sum decomposition (**??**) is*

$$m_\omega = \langle \chi^\mu \chi^\nu, \chi^\omega \rangle. \tag{2.66}$$

The inner product between the characters is defined in Eq. (2.64), and $\chi^\mu \chi^\nu$ is the character of the tensor product representation $\mathbf{U}^\mu \otimes \mathbf{U}^\nu$.

In Chapter 4, we are interested in the decomposition of tensor product representations of the form $(\mathbf{U}^\mu)^* \otimes \mathbf{U}^\mu$. The irreps $\mathbf{U}^\mu$ describe transformations of the signal states of a QKD protocol. We calculate the decomposition for two examples.

Example 1 *Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two isomorphic qubit Hilbert spaces carrying the two-dimensional irreps $(\mathbf{U}^6)^*$ and $(\mathbf{U}^6)$. We are interested in the decomposition of the tensor product*

$$(\mathbf{U}^6)^* \otimes \mathbf{U}^6 := \mathbf{U}_{\mathrm{BB84}} \tag{2.67}$$

on the composite space $\mathcal{H}_A \otimes \mathcal{H}_B$. Since $\mathbf{U}^6$ is a symplectic irrep, it holds that $(\mathbf{U}^6)^* \cong \mathbf{U}^6$. The character of the tensor product according to Eq. (2.63) is given by

	e	C_{4z}	C_{2z}	C_{2y}	C_{2xy}	$\bar{e}$	$\bar{C}_{4z}$
$\mathbf{U}^6 \otimes \mathbf{U}^6$	4	2	0	0	0	4	2

(2.68)

The multiplicities m_ω for each irrep $\mathbf{U}^\mu$ are given according to Eq. (2.66) by $m_1 = m_2 = m_5 = 1$ and $m_3 = m_4 = m_6 = m_7 = 0$. Therefore, the tensor product decomposes into three irreps: two one-dimensional irreps $\mathbf{U}^1$ and $\mathbf{U}^2$, and one two-dimensional irrep $\mathbf{U}^5$

$$\mathbf{U}_{\mathrm{BB84}} \cong \mathbf{U}^1 \oplus \mathbf{U}^5 \oplus \mathbf{U}^2. \tag{2.69}$$

Example 2 *We define the sum of two one-dimensional irreps $\mathbf{U}^1 \oplus \mathbf{U}^4$ of the group C_4. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be two isomorphic qubit Hilbert spaces carrying the representations $(\mathbf{U}^1 \oplus \mathbf{U}^4)^*$ and $\mathbf{U}^1 \oplus \mathbf{U}^4$. We are interested in the decomposition of the representation*

$$\begin{aligned} \mathbf{U}_{\mathrm{UPE}} &= (\mathbf{U}^1 \oplus \mathbf{U}^4)^* \otimes (\mathbf{U}^1 \oplus \mathbf{U}^4) && (2.70)\\ &= ((\mathbf{U}^1)^* \otimes \mathbf{U}^1) \oplus ((\mathbf{U}^1)^* \otimes \mathbf{U}^4) \oplus ((\mathbf{U}^4)^* \otimes \mathbf{U}^1) \oplus ((\mathbf{U}^4)^* \otimes \mathbf{U}^4) && (2.71) \end{aligned}$$

on $\mathcal{H}_A \otimes \mathcal{H}_B$. From the uniqueness of the characters we determine that $(\mathbf{U}^1)^* \cong \mathbf{U}^1$ and $(\mathbf{U}^4)^* \cong \mathbf{U}^3$. Furthermore, any product with the trivial irrep satisfies $\mathbf{U}^1 \otimes \mathbf{U}^\mu = \mathbf{U}^\mu$. It remains to compute the direct sum decomposition of the product $\mathbf{U}^3 \otimes \mathbf{U}^4$, which is easy because all irreps of C_4 are one-dimensional. It follows that $\chi^3\chi^4 = \chi^1$, which uniquely determines the decomposition

$$\mathbf{U}_{\mathrm{UPE}} = \mathbf{U}^1 \oplus \mathbf{U}^4 \oplus \mathbf{U}^3 \oplus \mathbf{U}^1. \tag{2.72}$$

Clebsch-Gordan coefficients

Let $\mathbf{U}^\mu$ and $\mathbf{U}^\nu$ be two irreps of G on $\mathcal{H}^\mu$ and $\mathcal{H}^\nu$. We denote the bases of $\mathcal{H}^\mu$ and $\mathcal{H}^\nu$ by $\{|i_\mu\rangle\}_i$ and $\{|j_\nu\rangle\}_j$. The canonical basis on $\mathcal{H}^\mu \otimes \mathcal{H}^\nu$ is the tensor product basis $\{|i_\mu, j_\nu\rangle\}_{i,j}$. There exists a basis $\{|\phi_k\rangle\}_k$ on $\mathcal{H}^\mu \otimes \mathcal{H}^\nu$ in which the direct sum decomposition of $\mathbf{U}^\mu \otimes \mathbf{U}^\nu$ is block diagonal in the matrix representation, namely

$$U_g^\mu \otimes U_g^\nu \to \left(\begin{array}{c|cc|c} U_g^{\omega_1} & 0 & 0 & 0 \\ \hline 0 & \multicolumn{2}{c|}{\multirow{2}{*}{$U_g^{\omega_2}$}} & 0 \\ 0 & & & 0 \\ \hline 0 & 0 & 0 & \ddots \end{array}\right). \tag{2.73}$$

This new basis is related to the tensor product basis by the *Clebsch-Gordan coefficients*:

Definition 16 *The coefficients $\langle i_\mu, j_\nu | \phi_k \rangle$ in the expansion $|\phi_k\rangle = \sum_{i,j} \langle i_\mu, j_\nu | \phi_k \rangle |i_\mu, j_\nu\rangle$ are called Clebsch-Gordan coefficients.*

The Clebsch-Gordan coefficients for tensor products of crystallographic groups representations can be found in Ref. [17]

Continuing Example 1, we define the canonical basis of the isomorphic spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ by $\{|0\rangle, |1\rangle\}$. Then, the Clebsch-Gordan coefficients found in Ref [17] tell us that the matrix representation of $\mathbf{U}_{\text{BB84}} \cong (\mathbf{U}^6)^* \otimes \mathbf{U}^6$ is block diagonal in the Bell basis defined in Eq. (2.10). Each irrep appearing in the direct sum decomposition of $\mathbf{U}_{\text{BB84}}$ lives on a subspace spanned by the basis vectors of the Bell basis

$$\mathbf{U}^1 \to \{|\Phi^+\rangle\} \tag{2.74}$$
$$\mathbf{U}^5 \to \{|\Phi^-\rangle, |\Psi^+\rangle\} \tag{2.75}$$
$$\mathbf{U}^2 \to \{|\Psi^-\rangle\}. \tag{2.76}$$

Note that $\mathbf{U}^5$ is a two-dimensional irrep, while $\mathbf{U}^1$ and $\mathbf{U}^2$ are both one-dimensional.

2.4.7 Schur's lemma

Schur's lemma is a simple but powerful lemma.

Lemma 1 ***(Schur's lemma)***. *Let $\mathbf{U}^\mu$ and $\mathbf{U}^\nu$ be irreducible representations of a group G on Hilbert spaces $\mathcal{H}^\mu$ and $\mathcal{H}^\nu$, and let A be a linear map from $\mathcal{H}^\mu \to \mathcal{H}^\nu$. If the linear map and the irreps commute,*

$$A\, U_g^\mu = U_g^\nu\, A, \tag{2.77}$$

for all $g \in G$, then A satisfies one of the two cases:

(i) if $\mathbf{U}^\mu \cong \mathbf{U}^\nu$, $A = c\ \mathbb{1}_n$, where $c \in \mathbb{C}$ is a scalar and $\mathbb{1}_n$ is the identity operator mapping $\mathcal{H}^\mu \to \mathcal{H}^\nu$.

(ii) if $\mathbf{U}^\mu \ncong \mathbf{U}^\nu$, then A is equal to zero.

We continue Example 1. Suppose a density operator $\rho_A \in \mathcal{D}(\mathcal{H}_A)$ commutes with all group elements of $\mathbf{U}^6$:

$$[\rho_A,\ U_g^6] = 0, \quad \forall g \in G. \tag{2.78}$$

It follows from (i) in Schur's lemma that ρ_A is proportional to the identity $\mathbb{1}_2$. In the matrix formulation with the proper normalization $\operatorname{tr}\rho_A = 1$ this amounts to

$$\rho_A = \frac{1}{2}\mathbb{1}_2 = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{2.79}$$

Let ρ_{AB} be a composite density operator on $\mathcal{D}(\mathcal{H}_{AB})$. Suppose ρ_{AB} commutes with the representation $\mathbf{U}_{\mathrm{BB84}} = (\mathbf{U}^6)^* \otimes \mathbf{U}^6$ of the group D_4 on $\mathcal{H}_{AB}$:

$$[\rho_{AB},\ U_g^6 \otimes U_g^6] = 0, \quad \forall g \in G. \tag{2.80}$$

Since we know that the direct sum decomposition of $\mathbf{U}_{\mathrm{BB84}}$ is block-diagonal in the Bell basis, let us parametrize ρ_{AB} in the Bell basis by

$$\rho_{AB} = \left(\begin{array}{c|ccc|c} \rho_{11} & \rho_{12} & \rho_{13} & \rho_{14} \\ \hline \rho_{12}^* & \rho_{22} & \rho_{23} & \rho_{24} \\ \rho_{13}^* & \rho_{23}^* & \rho_{33} & \rho_{34} \\ \hline \rho_{14}^* & \rho_{24}^* & \rho_{34}^* & \rho_{44} \end{array}\right). \tag{2.81}$$

Then, the diagonal blocks of ρ_{AB} satisfy the following commutation relations

$$\rho_{11}\, U_g^1 = U_g^1\, \rho_{11}, \tag{2.82}$$

$$\begin{pmatrix} \rho_{22} & \rho_{23} \\ \rho_{23}^* & \rho_{33} \end{pmatrix} U_g^5 = U_g^5 \begin{pmatrix} \rho_{22} & \rho_{23} \\ \rho_{23}^* & \rho_{33} \end{pmatrix}, \tag{2.83}$$

$$\rho_{44}\, U_g^2 = U_g^2\, \rho_{44}. \tag{2.84}$$

The commutation relation of the off-diagonal blocks of ρ_{AB} is given by

$$\begin{pmatrix} \rho_{12} & \rho_{13} \end{pmatrix} U_g^5 = U_g^1 \begin{pmatrix} \rho_{12} & \rho_{13} \end{pmatrix}, \tag{2.85}$$

$$\rho_{14}\, U_g^2 = U_g^1\, \rho_{14}, \tag{2.86}$$

$$\begin{pmatrix} \rho_{24} \\ \rho_{34} \end{pmatrix} U_g^2 = U_g^5 \begin{pmatrix} \rho_{24} \\ \rho_{34} \end{pmatrix}. \tag{2.87}$$

We apply Schur's lemma to each of the blocks individually. All diagonal blocks satisfy (i) in Schur's lemma, while all off-diagonal blocks satisfy (ii). Hence,

$$\rho_{11} = a\ \mathbb{1}_1, \tag{2.88}$$

$$\begin{pmatrix} \rho_{22} & \rho_{23} \\ \rho_{32} & \rho_{33} \end{pmatrix} = b\ \mathbb{1}_2, \tag{2.89}$$

$$\rho_{44} = c\ \mathbb{1}_1, \tag{2.90}$$

where a, b and c are constants. All other entries are zero. Thus,

$$\rho_{AB} = \left(\begin{array}{c|cc|c} a & 0 & 0 & 0 \\ \hline 0 & b & 0 & 0 \\ 0 & 0 & b & 0 \\ \hline 0 & 0 & 0 & c \end{array}\right) \tag{2.91}$$

in the Bell basis with the normalization $a + 2b + c = 1$.

Chapter 3

Quantum key distribution background

This chapter is a background chapter about quantum key distribution. References can be found in [86, 39, 77].

3.1 QKD protocols

The objective of QKD is to establish a secret key between two legitimate parties, Alice and Bob. The secret key can be used later in classical cryptographic applications, for example to facilitate secure communication.

A secret key is a string k of independent and uniformly distributed random variables, that is known to Alice and Bob, but unknown to any eavesdropper, Eve. In order to generate a secret key, Alice and Bob follow a protocol with well-defined steps. Typically, the protocol has a quantum phase and the classical phase. In the quantum phase, Alice and Bob exchange quantum signals over a quantum channel. In the classical phase, they communicate over an authenticated classical channel and extract a secret key using classical communication protocols. During the whole process, the goal of the eavesdropper is to learn about the key by launching an *attack* on the protocol.

First, we describe the steps of a protocol in the *prepare-and-measure scheme*.

Quantum phase:

1. *Preparation.* Let $\mathbf{S} = \{|\varphi_x\rangle, x = 1, 2, ..., |\mathbf{S}|\}$ be a set of $|\mathbf{S}|$ quantum states $|\varphi_x\rangle$ defined on a d-dimensional Hilbert space $\mathcal{H}_S$. Alice chooses n states (signal states) with probability $p(x)$ from the set $\mathbf{S}$ in her laboratory. The quantum states encode the random variables of the key. Alice keeps a record of the chosen sequence of quantum states before sending them over a quantum channel to Bob.

2. *Measurement.* Bob measures the quantum states in his laboratory by means of a POVM $\mathbf{M}_B = \{F_B^y\}_y$. He records the measurement outcomes, which results in correlated data (raw data) according to the conditional probability distribution $p(y|x)$, shared between Alice and Bob.

Classical phase:

1. *Parameter estimation.* Alice and Bob publicly announce a small amount of their data to determine the statistics of the remaining data. If the statistics indicate that the remaining data is suitable to generate a key, the protocol continues, otherwise it aborts.

2. *Postprocessing.* Alice and Bob can process their data to their advantage. For example, they can discard data that they identify to be unsuitable for the key. Then they agree how to map their data to the actual key values.

3. *Error correction.* If the key strings are not perfectly correlated Alice and Bob perform error correction (sometimes called *reconciliation*), to generate a pair of perfectly correlated, but shorter strings. A typical choice for the error correction is one-way error correction, in which the data of one party is set as a reference key. The party with the reference key sends error correction information to the other party, who then must correct her or his noisy data to match the reference key. We speak of *direct/reverse* reconciliation, if Alice's/Bob's data serves as the reference key. If the error correction is successful, Alice and Bob share two identical strings. There is also the possibility that the error correction fails, and the protocol aborts.

4. *Privacy amplification.* In the last step, Alice and Bob eliminate Eve's information about their strings through privacy amplificaion. They obtain two shorter strings $k_A = k_B \equiv k$ of length $\ell \leq n$ on which Eve has no information. For this to succeed, Alice and Bob need to be able to upper bound the amount of information Eve knows about the correlated data. If the privacy amplification is successful, Alice and Bob generate a secret key, otherwise, the protocol aborts.

3.1.1 Source-replacement scheme

The preparation step of the quantum phase is equivalently described in the *source-replacement scheme*, which is convenient scheme to analyze the security of a protocol. The source-replacement scheme is a thought setup, in which Alice creates a hypothetical bipartite entangled state (source state)

$$|\Phi\rangle = \sum_x \sqrt{p(x)}|x\rangle_X|\varphi_x\rangle_S \tag{3.1}$$

in her laboratory, keeps the first half for herself and sends the other half to Bob. The states $|x\rangle$ form an orthonormal basis $\mathcal{X} = \{|x\rangle, x = 0, ..., |\mathbf{S}| - 1\}$ of an $|\mathbf{S}|$-dimensional Hilbert space $\mathcal{H}_X$. In order to prepare the state $|\varphi_x\rangle$ on Bob's side, Alice performs a projective measurement in the basis $\mathcal{X}$, which triggers the source state to collapse onto the conditional state $|\varphi_x\rangle$ with probability $p(x)$.

If the signal states are linearly dependent, the source state assumes a more compact form. We define a d-dimensional subsystem A of the system X, and express the source state on the "compact" Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_S$

$$|\Phi\rangle_{AS} = \sum_{i=0}^{d-1} \sqrt{\kappa_i}|\bar{i}\rangle_A|i\rangle_S. \tag{3.2}$$

In this expression, the basis $\mathcal{B} = \{|i\rangle_S; i = 0, ..., d-1\}$ is the Schmidt basis, and the coefficients $\sqrt{\kappa_i}$ are the Schmidt coefficients. They are the eigenbasis and the square roots of the eigenvalues of the reduced operator $\phi_S = \mathrm{tr}_X\{|\Phi\rangle_{XS}\langle\Phi|\}$. The Schmidt basis $\mathcal{A} = \{|\bar{i}\rangle_A; i = 0, ..., d-1\}$ of the system A can be explicitly given by the orthonormal vectors $|\bar{i}\rangle = \sum_x \sqrt{p(x)}\alpha_i^{(x)}|x\rangle/\sqrt{\kappa_i}$, where $\alpha_i^{(x)} = \langle i|\varphi_x\rangle$ are the coefficients of the signal states in the Schmidt basis $\mathcal{B}$. In the following, we omit the bar in $|\bar{i}\rangle$.

Alice's projective measurement in the basis $\mathcal{X}$ on $\mathcal{H}_X$ is equal to a measurement $\mathbf{M}_A = \{F_A^x\}_x$ with respect to rank-one POVM elements F_A^x on the smaller space $\mathcal{H}_A$ given by

$$F_A^x = p(x)\sqrt{\rho_A}^{-1}|\varphi_x^*\rangle\langle\varphi_x^*|\sqrt{\rho_A}^{-1}. \tag{3.3}$$

Here we define the density matrix of Alice's reduced state as

$$\rho_A = \mathrm{tr}_S\{|\Phi\rangle_{AS}\langle\Phi|\}, \tag{3.4}$$

and the states

$$|\varphi_x^*\rangle = \sum_i \langle\varphi_x|i\rangle\ |i\rangle = \sum_i (\alpha_i^{(x)})^*\ |i\rangle, \tag{3.5}$$

where the symbol $*$ denotes the complex conjugate with respect to the Schmidt basis $\mathcal{A}$. The operators F_A^x are positive, sum up to the identity, and satisfy the property $\mathrm{tr}_A\{F_A^x \otimes \mathbb{1}|\Phi\rangle\langle\Phi|\} = p(x)|\varphi_x\rangle\langle\varphi_x|$.

3.2 Eavesdropping attacks

Quantum key distribution promises unconditional security. This means that the security of the key is established without limitations imposed on the computational or a technological power of the eavesdropper. However, unconditional security only holds within a certain framework. Outside of the framework, we are not able to claim unconditional security. The requirements of the framework are the following:

(i) Eve has no access to any device inside Alice and Bob's laboratories.

(ii) Eve can tamper with the quantum channel at will, but she is limited by the laws of quantum mechanics.

(iii) Eve can listen to all the messages sent over the classical channel, but the authentication prevents her from changing the messages. Authentication, which is a well-known problem in the field of classical cryptography, can be achieved by means of secure classical authentication algorithms requiring only a short pre-shared secret key.

In this framework, Eve's most general attack is on the quantum signals. She attaches a fresh quantum system E' (ancilla) to the second half of the source states $|\Phi\rangle_{AS}^{\otimes n}$ followed by a unitary transformation, that takes the joint systems $S^n E'$ to $B^n E$. She then keeps the transformed ancilla E for herself, and resends the remaining systems B^n to Bob. After Eve's interaction with the signals, but prior to Alice and Bob's measurements, the state held by Alice and Bob is described by an unknown (mixed) state ρ_{AB}^n, instead of n perfect copies of the source state $|\Phi\rangle_{AS}$.

Historically, Eve's attack strategy is divided into three classes.

1. In the *individual attack* Eve interacts with each of the signals sent by Alice individually. She attaches a fresh quantum system E' to each source state $|\Phi\rangle_{AS}$ and uses the same unitary U_E each time. The unitary takes the composite system SE' to BE. Eve sends B to Bob (see Fig. 3.1), keeps E for herself, and performs a measurement on each individual system E in order to extract information about the key. Some protocols have been analyzed under this assumption in Refs. [15, 6, 22]. However,

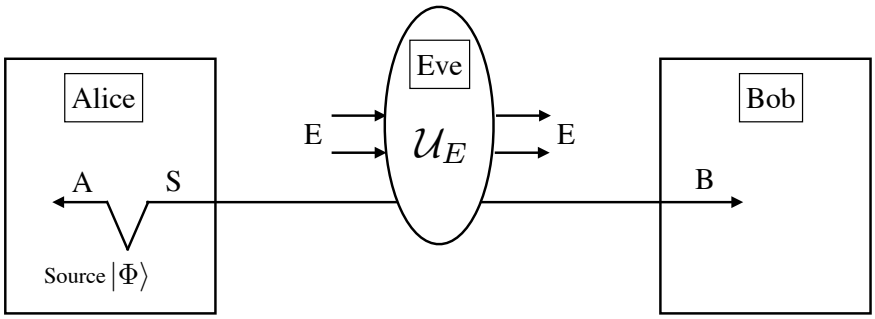


Figure 3.1: In the source-replacement scheme, Alice prepares the entangled state $|\Phi\rangle$. The system A is kept by Alice, while the system S is sent through the quantum channel to Bob. Eve attaches ancillas to the signal states and performs a unitary transformation on the joint system SE, transforming it to BE. She resends the system B to Bob. After Eve's interaction, Alice and Bob no longer share a perfect copy of $|\Phi\rangle$, but a bipartite state ρ_{AB}, which is only partially characterized by their observations.

individual attacks are no longer analyzed in the QKD community, not only because they are less powerful than other attacks (e.g. collective attacks), but also because the calculation of the key rate involves an optimization over Eve's measurement, which is generally difficult to perform, and does not lead to a composable security proof (see Sec. 3.3 for the definition of composability).

2. The second type of attack is the *collective attack*. While in the collective attack the interaction with the signals is the same as in the individual attack, Eve is allowed to do a collective measurement on all signals jointly at the end of the protocol. She can also use all information revealed to her during the classical phase of the protocol. In particular, under the assumption of collective attacks, ρ_{AB}^n assumes a product form: $\rho_{AB}^n = \rho_{AB}^{\otimes n}$.

3. Finally, in the most general attack, the *coherent attack*, Eve interacts with all the signals coherently using one large ancilla on all n systems. Under this type of attack no simplification of ρ_{AB}^n can be given.

3.2.1 Collective attacks in the source-replacement scheme

For collective attacks, Eve's interaction is completely determined by the unitary U_E between each signal and the ancilla. According to the Choi-Jamiolkowski isomorphism, the transformation U_E is equivalently characterized by the purification $|\Psi\rangle_{ABE}$ of ρ_{AB} on the dilated space $\mathcal{H}_{ABE}$. The dimension of the purifying system E is the same as the dimension of AB. In order to guarantee unconditional security, we must assume that Eve can exploit everything allowed by quantum mechanics for her attack, which is realized by giving her full control over $|\Psi\rangle_{ABE}$. Note that to each ρ_{AB} an entire class of purifications $|\Psi\rangle^W_{ABE} = \mathbb{1}_{AB} \otimes W_E|\Psi\rangle_{ABE}$ can be constructed, where W is local unitary transformation on Eve's system. However, such local transformations on Eve's system are irrelevant when quantifying Eve's knowledge on the key.

After Alice and Bob measure the systems AB of $|\Psi\rangle_{ABE}$ with respect to the POVMs $\mathbf{M}_A = \{F^x_A\}$ and $\mathbf{M}_B = \{F^y_B\}$, the resulting state shared between Alice, Bob and Eve is a tripartite classical-classical-quantum (ccq) state [31]

$$\rho_{XYE} = \sum_{x,y} p(x,y)|x\rangle\langle x|_X \otimes |y\rangle\langle y|_Y \otimes \rho^{xy}_E \tag{3.6}$$

where $|x\rangle$ and $|y\rangle$ are two sets of orthonormal bases,

$$p(x,y) = \mathrm{tr}\{F^x_A \otimes F^y_B\, \rho_{AB}\} \tag{3.7}$$

is the probability distribution of the measurement outcomes, and

$$\rho^{xy}_E = \mathrm{tr}_{AB}\{F^x_A \otimes F^y_B \otimes \mathbb{1}_E|\Psi\rangle\langle\Psi|\}/p(x,y) \tag{3.8}$$

are Eve's quantum states conditioned on the event that Alice and Bob's outcomes were x and y.

3.3 Key rate formalism

The security proof presented in Refs. [31, 80, 57] provides a bound on the rate at which Alice and Bob can extract a secret key in the infinite key limit $n \to \infty$. The proof is valid for collective attacks and for one-way classical communication, but can also be extended to coherent attacks for discrete and continuous-variable schemes via the de Finetti theorems, and two-way communication [78, 77, 79, 26].

3.3.1 Security definition

In the classical phase of the protocol, Alice and Bob transform their data into a pair of shorter key strings $k_A = k_B \equiv k$, provided that the protocol did not abort. If we describe the key k on the classical system K, and Eve's knowledge about the key at the end of the protocol by a quantum system E_k, the output of the protocol is a joint classical-quantum state ρ_{KE_k} describing the key and Eve's knowledge.

Ultimately, the security of the key k is defined as its deviation ϵ from an ideal key, which is a uniformly distributed string about which Eve has no information. For a given state ρ_{E_k} held by Eve, a key is defined to be ϵ-secure [81], if $\frac{1}{2}|\rho_{KE_k} - \mathbb{1}_K \otimes \rho_{E_k}|_1 \leq \epsilon$, where $|A|_1 = \mathrm{tr}\sqrt{A^\dagger A}$ is the trace norm and $\mathbb{1}_K$ is the completely mixed state on the system K representing the ideal key. The trace norm in the criterion ensures that the protocol fails to output a key that is identical to the ideal key at most with probability ϵ. This security definition also ensures composability, which means that the key can be securely used in other applications.

In the asymptotic limit $n \to \infty$ (infinite key limit), the security parameter ϵ can go to zero. If one considers a non-asymptotic scenario with a finite number of signals, then ϵ remains finite in general. Finite-size effects is another branch of research in the field of QKD found for example in Ref. [85].

3.3.2 The Devetak-Winter security proof

At the end of a successful protocol, a secret key of length $\ell \leq n$ is generated. The quantity of interest for all QKD protocols is the secret key rate

$$r = \lim_{n\to\infty} \frac{\ell}{n}. \tag{3.9}$$

In the infinite key limit, this rate was established by Devetak and Winter in Ref. [31], and Renner et al. in Refs. [57, 80] against collective attacks by the formula

$$r(\rho_{XYE}) = I(X:Y) - \chi(X:E). \tag{3.10}$$

The first term is the mutual information $I(X:Y) = H(X) - H(X|Y)$ between Alice and Bob's data and quantifies the amount of bits that need to be sacrificed for the error correction. According to Shannon's coding theorem, the fraction of error-free bits that can be extracted from data distributed according to a probability distribution $p(x,y)$ is given by $I(X:Y)$. The amount of privacy amplification necessary to eliminate Eve's information

is given by the Holevo quantity, or quantum mutual information, between Alice and Eve $\chi(X:E) = H(X) + S(E) - S(X,E)$. The Holevo quantity is explicitly given by

$$\chi(X:E) = S(\rho_E) - \sum_x p(x) S(\rho_E^x), \tag{3.11}$$

where ρ_E^x is Eve's state conditioned on x, and $\rho_E = \sum_x p(x)\rho_E^x$. For the practical calculation of the Holevo quantity, often an explicit reference to the system E can be eliminated, because the entropies $S(\rho_E)$ and $S(\rho_E^x)$ can be expressed in terms of quantities on the systems AB: If the state $|\Psi\rangle$ is pure, then $S(\rho_{AB}) = S(\rho_E)$. Furthermore, if Alice uses rank-one POVM elements, then the conditional states $\rho_{BE}^x = \mathrm{tr}_A\{F_A^x \otimes \mathbb{1}_{BE}|\Psi\rangle\langle\Psi|\}/p(x)$ are pure, and therefore $S(\rho_E^x) = S(\rho_B^x)$. Thus, the Holevo quantity simplifies to

$$\chi(X:E) = S(\rho_{AB}) - \sum_x p(x) S(\rho_B^x). \tag{3.12}$$

3.4 Properties of mutual information and Holevo quantity

In this section we give three properties of the classical mutual information and the Holevo quantity, that were shown in Ref. [34]. At first, we introduce the same notation for the mutual information and the Holevo quantity as in Ref. [34]. This new notation is more convenient for our purposes throughout the rest of this thesis.

Let Alice and Bob share a quantum state ρ_{AB}, which they measure with respect to the POVM $\mathbf{M}_{AB} = \{F_A^x \otimes F_B^y : F_A^x \in \mathbf{M}_A, F_B^y \in \mathbf{M}_B\}$. We always assume that Eve holds the purification $|\Psi\rangle$ of ρ_{AB}. Instead of denoting the mutual information $I(X:Y)$ in dependence of the registers XY of the measured state ρ_{XY}, we rather specify the mutual information in dependence of the quantum state ρ_{AB} and the POVM $\mathbf{M}_{AB}$,

$$I(\rho_{AB}, \mathbf{M}_{AB}) := I(X:Y). \tag{3.13}$$

On the other hand, the Holevo quantity can be calculated from the cq-state ρ_{XE} which is the result of Alice's measurement of $\rho_{AE} = \mathrm{tr}_B |\Psi\rangle\langle\Psi|$. Therefore, we denote the Holevo quantity

$$\chi(\rho_{AB}, \mathbf{M}_A) := \chi(X:E) \tag{3.14}$$

as a function of ρ_{AB} and the measurement $\mathbf{M}_A$. In the new notation the key rate $r(\rho_{XYE})$ in Eq. (3.10) is a function of the quantum state ρ_{AB}

$$r(\rho_{AB}) = I(\rho_{AB}, \mathbf{M}_{AB}) - \chi(\rho_{AB}, \mathbf{M}_A), \tag{3.15}$$

The first property in this section deals with the convexity of the classical mutual information. We show that $I(\rho_{AB}, \mathbf{M}_{AB})$ is convex in the argument ρ_{AB}, if the *a priori* probability distribution $p(x) = \mathrm{tr}\{F_A^x \, \rho_A\}$ is fixed. We call this feature "weak convexity" to indicate that convexity only holds with the restriction on $p(x)$.

Theorem 7 ***(Weak convexity).*** *Consider the states ρ_{AB}, σ_{AB} and the convex sum $\bar{\rho}_{AB} = \lambda\rho_{AB} + (1-\lambda)\sigma_{AB}$ for $\lambda \in [0,1]$ with measurement outcomes distributed according to the probability distributions $p(x,y) = \mathrm{tr}\{F_A^x \otimes F_B^y \, \rho_{AB}\}$, $q(x,y) = \mathrm{tr}\{F_A^x \otimes F_B^y \, \sigma_{AB}\}$ and $\bar{p}(x,y) = \lambda p(x,y) + (1-\lambda)q(x,y)$. If the probability distributions satisfy $p(x) = q(x)$ for all x, then the mutual information is convex in the sense that*

$$I(\bar{\rho}_{AB}, \mathbf{M}_{AB}) \leq \lambda I(\rho_{AB}, \mathbf{M}_{AB}) + (1-\lambda) I(\sigma_{AB}, \mathbf{M}_{AB}). \tag{3.16}$$

The proof of this theorem is given in Appendix A.1.

The second property is about the concavity of the Holevo quantity $\chi(\rho_{AB}, \mathbf{M}_A)$ as a function of ρ_{AB}.

Theorem 8 ***(Concavity).*** *Consider the states ρ_{AB}, σ_{AB} and the convex sum $\bar{\rho}_{AB} = \lambda\rho_{AB} + (1-\lambda)\sigma_{AB}$ for $\lambda \in [0,1]$. Then, the Holevo quantity is concave:*

$$\chi(\bar{\rho}_{AB}, \mathbf{M}_A) \geq \lambda \chi(\rho_{AB}, \mathbf{M}_A) + (1-\lambda)\chi(\sigma_{AB}, \mathbf{M}_A). \tag{3.17}$$

The proof of this theorem is in Appendix A.2.

The third property deals with unitary transformations of the input state ρ_{AB}.

Lemma 2 *Consider the states ρ_{AB} and $\sigma_{AB} = U \otimes V \rho_{AB} U^\dagger \otimes V^\dagger$, where U and V are unitaries on the systems A and B. The mutual information and the Holevo quantity transform as follows:*

$$I(\sigma_{AB}, \mathbf{M}_{AB}) = I(\rho_{AB}, U^\dagger \otimes V^\dagger \mathbf{M}_{AB} U \otimes V), \tag{3.18}$$

$$\chi(\sigma_{AB}, \mathbf{M}_A) = \chi(\rho_{AB}, U^\dagger \mathbf{M}_A U). \tag{3.19}$$

In these expressions the transformed measurements are defined by

$$U^\dagger \mathbf{M}_A U := \{U^\dagger F_A^x U\} \tag{3.20}$$

$$V^\dagger \mathbf{M}_B V := \{V^\dagger F_B^y V\} \tag{3.21}$$

$$U^\dagger \otimes V^\dagger \, \mathbf{M}_{AB} \, U \otimes V := \{U^\dagger \otimes V^\dagger (F_A^x \otimes F_B^y) \, U \otimes V\}. \tag{3.22}$$

The proof of this lemma is based on the cyclic property of the trace, and that the von Neumann entropy is unitarily invariant: $S(U\rho U^\dagger) = S(\rho)$.

3.5 Postselection

This section describes the postselection step similar to Refs. [34, 35]. Usually, the key is not directly extracted from the state ρ_{XYE}, because the data might be only weakly correlated. Alice and Bob typically postselect on highly correlated data before proceeding with the protocol. A typical example is the *basis sifting*. In many QKD protocols Alice encodes the values of the key into quantum states in various bases, and Bob randomly chooses to measure in one of those bases. If they measured in the same basis, their data is typically strongly correlated, but if they measure in different bases, the data is only weakly correlated. In this case, they need to be able to identify where their basis choice matched, so that they can keep those signals with matching basis, and discard the others. Another possible postselection is to discard those events, where Bob did not record a detection event, because the signal got lost.

Let us first examine the classical version of the postselection step, which starts with the ccq state ρ_{XYE}. Alice and Bob calculate to each measurement outcome x and y some values $f(x) = v$ and $f(y) = w$, and announcing v and w publicly. Typically, the announcements v and w do not reveal any information about the key. Based on the announcements, Alice and Bob decide if they want to keep the data or discard it (*filtering*). For example, they only keep data with matching announcements, $v = w \equiv u$. In the case of sifting, v and w plays the role of a basis announcement.

By identifying the values v and w, Alice and Bob effectively partition their original POVMs $\mathbf{M}_A$ and $\mathbf{M}_B$ into subsets $\mathbf{m}_A^v = \{F_A^x : f(x) = v\}$ and $\mathbf{m}_B^w = \{F_B^y : f(y) = w\}$, each containing the POVM elements labeled by the value v or w of the announcement.

3.5.1 Quantum description of postselection

The quantum version of the postselection procedure is described by a two-step process: in the first step, the announcement is described by a coarse-grained measurement, represented by a quantum map $\mathcal{E}$, with the classical outcomes u or "discard". In the second step, a refined measurement yields the final data.

The quantum map $\mathcal{E}$ is described by the Kraus operators $K_A^u \otimes K_B^u$ that are acting on the state ρ_{AB}. Since only events with $w = v \equiv u$ are kept, the Kraus operators come in pairs with the same index u. There is also a Kraus operator corresponding to the discarded events. The Kraus operators with index u satisfy $\sum_u K_A^{u\dagger} K_A^u \otimes K_B^{u\dagger} K_B^u \leq \mathbb{1}$, and are related to the POVM elements in the sets $\mathbf{m}_A^u$ and $\mathbf{m}_B^u$ by the rule $K_A^u = \sqrt{\sum_{\mathbf{m}_A^u} F_A^x}$ and $K_B^u = \sqrt{\sum_{\mathbf{m}_B^u} F_B^y}$. For each Kraus operator, the outcome u is announced to all parties and stored in three classical registers $\bar{A}$, $\bar{B}$ and $\bar{E}$ held by Alice, Bob and Eve, respectively. The action of the quantum map on ρ_{AB} results thus in a state

$$\mathcal{E}(\rho_{AB}) = \sum_u p(u) \mathcal{K}^u[\rho_{AB}] \otimes |u\rangle\langle u|_{\bar{A}\bar{B}\bar{E}}, \tag{3.23}$$

with normalized conditional states

$$\mathcal{K}^u[\rho_{AB}] = K_A^u \otimes K_B^u \rho_{AB} (K_A^u \otimes K_B^u)^\dagger / \tilde{p}(u) \tag{3.24}$$

$$\tilde{p}(u) = \mathrm{tr}\{K_A^u \otimes K_B^u \rho_{AB} (K_A^u \otimes K_B^u)^\dagger\}. \tag{3.25}$$

each appearing with probability $p(u) = \frac{\tilde{p}(u)}{p_{\mathrm{kept}}}$. The probability that the state ρ_{AB} is kept during the postselection is $p_{\mathrm{kept}} = \sum_u \tilde{p}(u)$.

The announcement and filtering step is followed by the refined measurement. Each $\mathcal{K}^u[\rho_{AB}]$ is measured with respect to a new (normalized) joint POVM $\mathbf{M}_{AB}^u = \{F_A^{x,u} \otimes F_B^{y,u} : F_A^{x,u} \in \mathbf{M}_A^u, F_B^{y,u} \in \mathbf{M}_B^u\}$ conditioned on u. The POVMs

$$\mathbf{M}_A^u = \{F_A^{x,u}\} = \{(K_A^u)^{-1} F_A^x (K_A^{u\dagger})^{-1} : F_A^x \in \mathbf{m}_A^u\}, \tag{3.26}$$

$$\mathbf{M}_B^u = \{F_B^{y,u}\} = \{(K_B^u)^{-1} F_B^y (K_B^{u\dagger})^{-1} : F_B^y \in \mathbf{m}_B^u\}, \tag{3.27}$$

are constructed by renormalizing the sets $\mathbf{m}_A^u$ and $\mathbf{m}_B^u$. The inverses $(K_A^u)^{-1}$ and $(K_B^u)^{-1}$ are pseudo-inverses, which means they are only defined on the non-zero subspace of K_A^u and K_B^u. The new measurement guarantees that measuring $\mathcal{K}^u[\rho_{AB}]$ with respect to $\mathbf{M}_{AB}^u$ results in the same distribution as measuring ρ_{AB} with respect to $\mathbf{M}_A \otimes \mathbf{M}_B$ followed by classical postselection.

3.5.2 Key rate formula with postselection

We choose to calculate the key rate for each coinciding announcement u independently (alternatively, one could also merge the data from the different subsets u, and extract a key from the joint data string). Thus, Eve is given the purification $|\Psi^u\rangle$ of the state $\mathcal{K}^u[\rho_{AB}]$. If we denote the state after the measurement by ρ^u_{XYE}, the key rate including postselection is

$$\bar{r}(\mathcal{E}(\rho_{AB})) = \sum_u p(u) r(\rho^u_{XYE}). \tag{3.28}$$

Each individual rate $r(\rho^u_{XYE}) = I(\mathcal{K}^u[\rho_{AB}], \mathbf{M}^u_{AB}) - \chi(\mathcal{K}^u[\rho_{AB}], \mathbf{M}^u_A)$ is calculated according Eq. (3.10). We denote in the following the mutual information and Holevo quantity including postselection by

$$\bar{I}(\mathcal{E}(\rho_{AB})) := \sum_u p(u)\ I(\mathcal{K}^u[\rho_{AB}], \mathbf{M}^u_{AB}), \tag{3.29}$$

$$\bar{\chi}(\mathcal{E}(\rho_{AB})) := \sum_u p(u)\ \chi(\mathcal{K}^u[\rho_{AB}], \mathbf{M}^u_A). \tag{3.30}$$

3.6 Key rate optimization problem

If Alice and Bob knew Eve's attack strategy, the calculation of the key rate would be straightforward. They would know ρ_{AB} exactly and could estimate the necessary amount of privacy amplification and error correction. Typically, though, Alice and Bob do not know Eve's attack and hold only partial information about ρ_{AB}, which they acquired during the parameter estimation. In addition, since the system A never leaves Alice's lab (see Fig. 3.1), Alice and Bob know that the reduced density matrix $\rho_A = \mathrm{tr}_B\, \rho_{AB}$ remains unchanged, as already anticipated in equation (3.4). However, unless Alice and Bob's measurements are sufficient to obtain a complete (tomographic) parametrization of ρ_{AB}, there could be many states ρ_{AB} that are compatible with $p(x, y)$ and ρ_A. For what follows, it is useful to make the following definition

Definition 17 *The set* $\mathbf{\Gamma}$ *contains all bipartite states* ρ_{AB} *that are compatible with the measurement outcomes* $p(x, y)$ *and that have a given reduced state* ρ_A*.*

In order to be on the safe side, we must give Eve the freedom to chose any attack that is compatible with the states ρ_{AB} in $\mathbf{\Gamma}$. Among all these possible attacks, the one that

generates the lowest key rate,

$$r_{\min} = \inf_{\rho_{AB} \in \mathbf{\Gamma}} \bar{r}(\mathcal{E}(\rho_{AB})) = \inf_{\rho_{AB} \in \mathbf{\Gamma}} \left\{ \bar{I}_{\text{obs}} - \bar{\chi}(\mathcal{E}(\rho_{AB})) \right\}, \tag{3.31}$$

is defined as the optimal attack. In this expression, we wrote $\bar{I}_{\text{obs}}$ for the mutual information, because it is determined from actual measurement data and is independent of ρ_{AB}. Since all density matrices $\rho_{AB} \in \mathbf{\Gamma}$ yield the same measurement data, we can introduce $\bar{I}_{\text{obs}} = \bar{I}(\mathcal{E}(\rho_{AB}))$. Only the amount of privacy amplification, $\bar{\chi}(\mathcal{E}(\rho_{AB}))$, depends on ρ_{AB}.

If Alice and Bob want to guarantee that their protocol is secure, they must assume that Eve performed the optimal attack. Hence, they cannot generate a secret key at a rate higher than $r_{\min}$ for the given protocol. We define the state associated to the optimal attack by ρ_{AB}^{opt}.

Chapter 4

Symmetries in quantum key distribution

4.1 Introduction

In the previous chapter we introduced the key rate optimization problem under collective attacks, but without an explicit recipe how to actually calculate the optimal attack. In this chapter we calculate the key rates of several protocols and provide a simplification of the optimization problem by exploiting the inherent symmetries of the protocols.

The key rate optimization problem is greatly simplified if we can make the assumption that the optimal attack carries a certain symmetry. In previous publications [80, 57], it was typically assumed that the observations $p(x, y)$ are only compatible with symmetric attacks in order to simplify the calculations. In this chapter we analyze protocols in a scenario where the parameter estimation is based on a coarse-grained version of $p(x, y)$. In this scenario we show that the optimal attack can always be assumed to be a symmetric attack, if the protocol and the postselection exhibit sufficient symmetries. Protocols with orthonormal bases as signal states and sifting, for example, exhibit enough symmetries to support the claim of a symmetric optimal attack.

We calculate the optimal attack for qubit-based protocols (e.g. the BB84 [10] and the 6-state protocol [15]) and for protocols in d-dimensional Hilbert spaces using mutually unbiased bases (MUBs) (e.g. protocols with 2 MUBs, d+1 MUBs [22] or d MUBs). The security of these protocols has been studied previously in Refs. [15, 6, 36, 16, 22, 33] for individual attacks. In Ref. [87], the security was proven for protocols with 2 and $d + 1$ MUBs using the security proof methods of Refs. [31, 57].

Additionally, we observe that some classes of QKD protocols, which share some common symmetry features, can be proven to have the same optimal attack, despite having different sets of signal states. As an example, we present qubit protocols which have the same optimal attack as the BB84 protocol or the 6-state protocol, and we give criteria to identify these protocols.

All the results of this chapter have been published in Ref. [34].

4.2 Symmetries in protocols

In this section we show that the density operator ρ_{AB}^{opt} corresponding to the optimal attack lies in a "symmetrized" set $\bar{\mathbf{\Gamma}}$, instead of $\mathbf{\Gamma}$. If ρ_{AB}^{opt} lies in $\bar{\mathbf{\Gamma}}$, we call the optimal attack a *symmetric optimal attack*. The symmetric states in the set $\bar{\mathbf{\Gamma}}$ are easily characterized using representation theory and Schur's lemma shown in Sec. 2.4.

4.2.1 Symmetries of signal states and measurements

Let G be a group with a unitary representation $\{U_g; g \in G\}$ on the Hilbert space $\mathcal{H}$ of the signal states $\mathbf{S} = \{|\varphi_x\rangle\}_x$ of a protocol. The group is said to be the *symmetry group* of the signal states, if $\mathbf{S}$ is G-invariant, namely, if for all $|\varphi_x\rangle \in \mathbf{S}$, the transformed states

$$|\varphi_{g(x)}\rangle := U_g|\varphi_x\rangle \tag{4.1}$$

are again in the set $\mathbf{S}$ for all $g \in G$ and all $|\varphi_x\rangle \in \mathbf{S}$. Here the index $g(x)$ denotes the index of the state $U_g|\varphi_x\rangle$.

If the set of signal states of a protocol is G-invariant, the POVM elements F_A^x and the reduced state ρ_A appearing the source-replacement scheme in Eqs. (3.3) and (3.4) also have certain symmetry properties.

Lemma 3 *If the initial probability distribution $p(x)$ is uniform ($p(x) = 1/|\mathbf{S}|$ for all x) and the set of signal states is G-invariant, then the POVM $\mathbf{M}_A = \{F_A^x\}_x$ and the reduced state ρ_A are G^*-invariant, namely*

$$U_g^* F_A^x U_g^T = F_A^{g(x)} \in \mathbf{M}_A, \tag{4.2}$$

$$U_g^* \rho_A U_g^T = \rho_A, \tag{4.3}$$

for all $g \in G$. The symbols $*$ and T denote the complex conjugate and the transpose with respect to the fixed Schmidt basis $\mathcal{B}$.

We prove Lemma 3 in Appendix A.3. Note that, with our particular definition of $*$ and T with respect to the Schmidt basis, the operators U_g^* and U_g^T are well-defined.

In the following, we only consider protocols in which Bob's POVM $\mathbf{M}_B = \{F_B^y\}_y$ is equipped with the G-invariance

$$U_g F_B^y U_g^\dagger = F_B^{g(y)} \in \mathbf{M}_B. \tag{4.4}$$

4.2.2 Coarse-grained parameter estimation

In many cases, the parameter estimation is based on a set of *coarse-grained* or *averaged* quantities, instead of the more detailed distribution $p(x, y)$. Often there is only one coarse-grained quantity, Q, for example, the quantum bit error rate (QBER) averaged over all signal states.

The coarse-grained quantity Q is defined as a linear function of the probability distribution $p(x, y)$ with the invariance property

$$Q[\{p(x, y)\}] = Q[\{p_g(x, y)\}] \quad \forall g \in G. \tag{4.5}$$

In this expression, the distribution

$$p_g(x, y) = \mathrm{tr}\{F_A^{g(x)} \otimes F_B^{g(y)} \rho_{AB}\} \tag{4.6}$$

is generated by relabelling the POVM elements $F_A^x \otimes F_B^y$ by $F_A^{g(x)} \otimes F_B^{g(y)}$.

In a coarse-grained parameter estimation scenario, the set of states that are compatible with Q and ρ_A is given by $\mathbf{\Gamma}_{\text{ave}}$. This new set is a superset of the previously defined set $\mathbf{\Gamma}$, because for each $\rho_{AB} \in \mathbf{\Gamma}$, an entire equivalence class of states $\{\mathcal{U}_g[\rho_{AB}] : g \in G\}$ of the form

$$\mathcal{U}_g[\rho_{AB}] = U_g^* \otimes U_g \rho_{AB} U_g^T \otimes U_g^\dagger, \tag{4.7}$$

are found in $\mathbf{\Gamma}_{\text{ave}}$. These states are (i) compatible with Q, because of the invariance property of Q, and (ii) have a reduced state $\mathrm{tr}_B\{\mathcal{U}_g[\rho_{AB}]\} = \rho_A$ because of the G^*-invariance of ρ_A. Furthermore, for all $\rho_{AB} \in \mathbf{\Gamma}$, the set $\mathbf{\Gamma}_{\text{ave}}$ contains all *symmetrized* states

$$\mathcal{T}^G[\rho_{AB}] \equiv \bar{\rho}_{AB} = \frac{1}{|G|} \sum_{g \in G} \rho_{AB}^{(U_g)}, \tag{4.8}$$

because of the linearity of Q. In this definition $|G|$ is the number of group elements in G. The map $\mathcal{T}^G$ is commonly known as the twirling map in the literature. The symmetrized

states form a subset $\bar{\mathbf{\Gamma}}$ of the set $\mathbf{\Gamma}_{\text{ave}}$. The subset $\bar{\mathbf{\Gamma}}$ is obtained by applying the twirling map to all density operators ρ_{AB} in $\mathbf{\Gamma}_{\text{ave}}$.

The symmetrized states have some nice properties: they commute with all tensor products $U_g^* \otimes U_g$,

$$\left[\bar{\rho}_{AB}, U_g^* \otimes U_g\right] = 0 \quad \forall g \in G. \tag{4.9}$$

Furthermore, a purification of $\bar{\rho}_{AB}$ can be chosen to satisfy the invariance

$$U_g^* \otimes U_g \otimes U_g \otimes U_g^* |\Psi\rangle = |\Psi\rangle \quad \forall g \in G. \tag{4.10}$$

The existence of this particular choice of the purification has been proven in Ref. [25] for permutation groups, but the same proof holds for arbitrary groups as well.

In the coarse-grained parameter estimation scenario, the optimization of the key rate is changed. Since the set $\mathbf{\Gamma}_{\text{ave}}$ is a superset of $\mathbf{\Gamma}$, we can safely evaluate the key rate $\bar{r}(\mathcal{E}(\rho_{AB}))$ over the enlarged set without running the risk of underestimating Eve. Therefore, we can bound the key rate by

$$r_{\min} = \inf_{\rho_{AB} \in \mathbf{\Gamma}} \bar{r}(\mathcal{E}(\rho_{AB})) \geq \inf_{\rho_{AB} \in \mathbf{\Gamma}_{\text{ave}}} \bar{r}(\mathcal{E}(\rho_{AB})). \tag{4.11}$$

4.2.3 Symmetric optimal attack

We show here that for any state $\rho_{AB} \in \mathbf{\Gamma}_{\text{ave}}$, the key rate is bounded by

$$r(\bar{\rho}_{AB}) \leq r(\rho_{AB}). \tag{4.12}$$

Proof. Recall that the key rate is defined as the difference $r(\bar{\rho}_{AB}) = I(\rho_{AB}, \mathbf{M}_{AB}) - \chi(\rho_{AB}, \mathbf{M}_A)$. Since the POVMs $\mathbf{M}_A$ and $\mathbf{M}_B$ are G^*- and G-invariant (see Eqs. (4.2) and (4.4)), we apply Lemma 2 to I and χ, which shows that all states in the equivalence class $\{\mathcal{U}_g[\rho_{AB}] : g \in G\}$ in $\mathbf{\Gamma}_{\text{ave}}$ yield equivalent key rates

$$r(\mathcal{U}_g[\rho_{AB}]) = r(\rho_{AB}) \tag{4.13}$$

Moreover, because the reduced state ρ_A of each state in $\mathbf{\Gamma}_{\text{ave}}$ is invariant by definition, the *a priori* probability distribution $p(x) = \text{tr}_A\{F_A^x \rho_A\}$ is fixed throughout the entire set $\mathbf{\Gamma}_{\text{ave}}$. Using the theorems about the convexity and concavity of I and χ (Theorems 7 and 8), it

follows that the key rate of the symmetrized state $\bar{\rho}_{AB}$ is bounded by

$$r(\bar{\rho}_{AB}) = I(\bar{\rho}_{AB}, \mathbf{M}_{AB}) - \chi(\bar{\rho}_{AB}, \mathbf{M}_A) \tag{4.14}$$

$$\leq \frac{1}{|G|} \sum_g I(\mathcal{U}_g[\rho_{AB}], \mathbf{M}_{AB}) - \chi(\mathcal{U}_g[\rho_{AB}], \mathbf{M}_A) \tag{4.15}$$

$$= \frac{1}{|G|} \sum_g r(\mathcal{U}_g[\rho_{AB}]). \tag{4.16}$$

We can now use the equivalence property in Eq. (4.13) to show that

$$\frac{1}{|G|} \sum_g r(\mathcal{U}_g[\rho_{AB}]) = r(\rho_{AB}). \tag{4.17}$$

This last equation together with Eq. (4.16) implies the desired result. ■

If there is a postselection step in a protocol, we need to extend the *equivalence property* in Eq. (4.13) and the *convexity property* in Eq. (4.16) to the key rate $\bar{r}(\mathcal{E}(\rho_{AB}))$, namely,

$$\bar{r}(\mathcal{E}(\rho_{AB})) = \bar{r}(\mathcal{E}(\mathcal{U}_g[\rho_{AB}])), \tag{4.18}$$

$$\bar{r}(\mathcal{E}(\bar{\rho}_{AB})) \leq \frac{1}{|G|} \sum_g \bar{r}(\mathcal{E}(\mathcal{U}_g[\rho_{AB}])). \tag{4.19}$$

These properties do not necessarily hold in general. For example, under certain postselection strategies, the restriction on $p(x)$ that is needed in Theorem 7 may be violated. We will later analyze a family of protocols with a special postselection where the convexity and equivalence properties of key rate $\bar{r}(\mathcal{E}(\rho_{AB}))$ always holds.

However, if Eqs. (4.19) and (4.18) hold, then for any state $\rho_{AB} \in \mathbf{\Gamma}_{\text{ave}}$, the key rate is bounded by

$$r(\mathcal{E}(\rho_{AB})) \geq r(\mathcal{E}(\bar{\rho}_{AB})). \tag{4.20}$$

This implies that the optimization can be carried out over the symmetric set $\bar{\mathbf{\Gamma}}$

$$\inf_{\rho_{AB} \in \mathbf{\Gamma}_{\text{ave}}} \bar{r}(\mathcal{E}(\rho_{AB})) \geq \inf_{\bar{\rho}_{AB} \in \bar{\mathbf{\Gamma}}} \bar{r}(\mathcal{E}(\bar{\rho}_{AB})). \tag{4.21}$$

Therefore, we can continue the estimation of the key rate in Eq. (4.11) and restrict the search for the optimal attack to a search over the set $\bar{\mathbf{\Gamma}}$:

$$r_{\min} \geq \inf_{\bar{\rho}_{AB} \in \bar{\mathbf{\Gamma}}} \bar{r}(\mathcal{E}(\bar{\rho}_{AB})). \tag{4.22}$$

In Fig. 4.1 we represent the transition from $\mathbf{\Gamma}$ to $\bar{\mathbf{\Gamma}}$ schematically. The symmetrized states $\bar{\rho}_{AB}$ can be characterized using representation theory, as shown for two examples in Sec. 2.4.

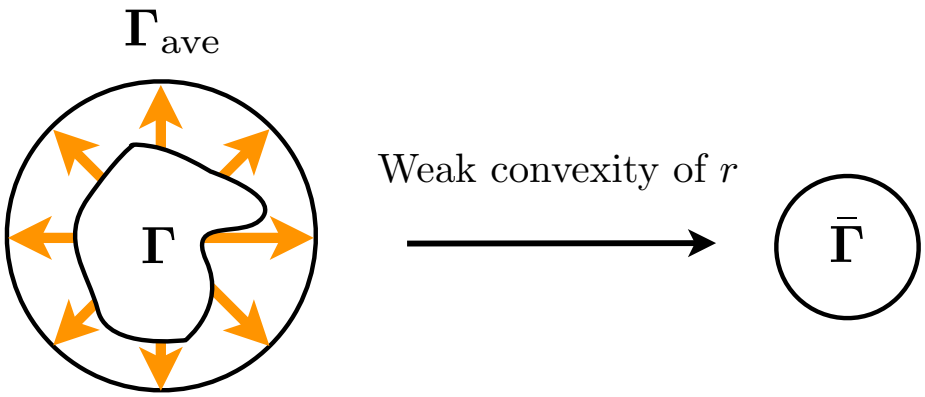


Figure 4.1: By only using coarse-grained quantities Q for parameter estimation, the set $\mathbf{\Gamma}$ is replaced by a bigger set $\mathbf{\Gamma}_{\text{ave}}$. Using the weak convexity of the key rate, the optimal attack can be chosen from a symmetrized set $\bar{\mathbf{\Gamma}}$.

4.3 A family of protocols with symmetric optimal attack

We construct a family of protocols, where the set $\mathbf{S}$ contains only complete sets of orthonormal bases (ONB), and where Alice and Bob postselect on data that they measured in the same basis (sifting). We call this family of protocols *ONB protocols*, and show that the convexity (4.19) and equivalence (4.18) properties of the key rate $\bar{r}(\mathcal{E}(\rho_{AB}))$ hold. Therefore, by choosing to do a coarse-grained parameter estimation, the optimal attack can always be assumed to be symmetric for ONB protocols.

4.3.1 Protocols with orthonormal bases (ONB)

Let us denote a basis of a d-dimensional Hilbert space by $\mathcal{B}_\beta = \{|\varphi_{(\beta,k)}\rangle : k = 0, ..., d-1\}$, where β is the basis index. Note that in the following the states $|\varphi_{(\beta,k)}\rangle$ carry two independent indices (β, k) instead of only one. We identify the set of signal states of an ONB protocol by

$$\mathbf{S}_{\mathcal{L}} = \{\mathcal{B}_\beta : \beta \in \mathcal{L}\}, \tag{4.23}$$

where $\mathcal{L}$ is the set from which the bases β are drawn. For each protocol the set $\mathcal{L}$ is fixed and contains $|\mathcal{L}|$ elements.

Each signal state $|\varphi_{(\beta,k)}\rangle$ is chosen with equal *a priori* probability $p(\beta,k) = 1/(d \cdot |\mathcal{L}|)$. This implies that Alice's reduced state ρ_A is proportional to the identity $\rho_A = \mathbb{1}/d$. Thus, Alice's POVM elements in Eq. (3.3) reduce to the projectors

$$F_A^{(\beta,k)} = \frac{1}{|\mathcal{L}|} |\varphi^*_{(\beta,k)}\rangle\langle\varphi^*_{(\beta,k)}| \tag{4.24}$$

with $|\varphi^*_{(\beta,k)}\rangle = \sum_i |i\rangle\langle\varphi_{(\beta,k)}|i\rangle$ defined in Eq. (3.5). On Bob's side, we construct a POVM that is isomorphic to Alice's POVM:

$$F_B^{(\beta,k)} = \frac{1}{|\mathcal{L}|} |\varphi_{(\beta,k)}\rangle\langle\varphi_{(\beta,k)}|. \tag{4.25}$$

4.3.2 Postselection on the same basis

Alice and Bob postselect on those measurement outcomes, which they performed in the same basis. In this particular case, Alice and Bob's announcement u is the basis β. This announcement partitions the POVMs $\mathbf{M}_A$ and $\mathbf{M}_B$ into $|\mathcal{L}|$ disjoint sets $\mathbf{m}_A^v = \{F_A^{(\beta,k)} : \beta = v\}$ and $\mathbf{m}_B^w = \{F_B^{(\beta,k)} : \beta = w\}$. Alice and Bob then decide to keep only those events which were measured and announced the the same basis $v = w \equiv u$. Because the POVM elements in each $\mathbf{m}_A^v$ and $\mathbf{m}_B^w$ add up the the identity, each Krauss operator $K_A^u = K_B^u = \mathbb{1}/\sqrt{|\mathcal{L}|}$, is proportional to the identity for all u. Consequently,

$$\mathcal{K}^u[\rho_{AB}] = \rho_{AB}$$

and the new POVMs

$$\mathbf{M}_A^u = \{|\mathcal{L}|\ F_A^{(\beta,k)} : \beta = u\} \tag{4.26}$$

$$\mathbf{M}_B^u = \{|\mathcal{L}|\ F_B^{(\beta,k)} : \beta = u\} \tag{4.27}$$

are simply rescaled versions of the old POVMs. Furthermore, each basis is kept with equal probability $p(u) = \frac{1}{|\mathcal{L}|}$.

4.3.3 Convexity and equivalence property for ONB protocols

The parameter estimation for many QKD protocols is typically based on the average error rate Q, defined as follows.

Definition 18 *The average error rate is the probability that Alice sent the signal state $|\varphi_{(\beta,k)}\rangle$, but Bob received an orthogonal state $|\varphi_{(\beta,k')}\rangle$ $(k' \neq k)$, averaged over all k and all bases β*

$$Q = \frac{1}{|\mathcal{L}|} \sum_{\beta \in \mathcal{L}} Q^{\beta}, \tag{4.28}$$

where $Q^{\beta} = \sum_{\substack{k,k' \\ k' \neq k}} \mathrm{tr}\left\{ |\varphi^{*}_{(\beta,k)}\rangle\langle\varphi^{*}_{(\beta,k)}| \otimes |\varphi_{(\beta,k')}\rangle\langle\varphi_{(\beta,k')}| \rho_{AB} \right\}$ is the average error rate found in each basis, and $|\mathcal{L}|$ is the number of bases in the set $\mathcal{L}$.

We now prove the following theorem for ONB protocols.

Theorem 9 *For ONB protocols with sifting on matching bases, the key rate $\bar{r}(\mathcal{E}(\rho_{AB}))$ satisfies the convexity and the equivalence properties in Eqs. (4.19) and (4.18).*

Using this theorem we can conclude that the optimal attack is symmetric for all ONB protocols, if the parameter estimation is coarse-grained. The key rate is therefore given by $r_{\min}$ in Eq. 4.22.

Proof. Recall that the key rate is define as

$$\bar{r}(\mathcal{E}(\rho_{AB})) = \frac{1}{|\mathcal{L}|} \sum_{u} \Big(I(\rho_{AB}, \mathbf{M}^{u}_{AB}) - \chi(\rho_{AB}, \mathbf{M}^{u}_{A}) \Big). \tag{4.29}$$

The *a priori* probability distribution is fixed for each ρ_{AB}, because ρ_A is the identity. Therefore, we use Theorems 7 and 8 to show that each term I and χ in the sum satisfies the convexity and concavity property, respectively:

$$I(\bar{\rho}_{AB}, \mathbf{M}^{u}_{AB}) \leq \frac{1}{|G|} \sum_{g} I(\mathcal{U}_g[\rho_{AB}], , \mathbf{M}^{u}_{AB}), \tag{4.30}$$

$$\chi(\bar{\rho}_{AB}, \mathbf{M}^{u}_{A}) \geq \frac{1}{|G|} \sum_{g} \chi(\mathcal{U}_g[\rho_{AB}], , \mathbf{M}^{u}_{A}). \tag{4.31}$$

From these two properties, it follows directly that the key rate is convex as a function of ρ_{AB}:

$$\bar{r}(\mathcal{E}(\bar{\rho}_{AB})) = \frac{1}{|\mathcal{L}|}\sum_u \Big(I(\bar{\rho}_{AB}, \mathbf{M}^u_{AB}) - \chi(\bar{\rho}_{AB}, \mathbf{M}^u_A)\Big) \tag{4.32}$$

$$\leq \frac{1}{|\mathcal{L}|}\sum_u \Big(\frac{1}{|G|}\sum_g I(\mathcal{U}_g[\rho_{AB}], \mathbf{M}^u_{AB}) - \frac{1}{|G|}\sum_g \chi(\mathcal{U}_g[\rho_{AB}], \mathbf{M}^u_A)\Big) \tag{4.33}$$

$$= \frac{1}{|G|}\sum_g \bar{r}(\mathcal{E}(\mathcal{U}_g[\rho_{AB}])). \tag{4.34}$$

Next, we show the equivalence property of $\bar{r}(\mathcal{E}(\rho_{AB}))$ under the symmetry group G of the signal states. Since any unitary acts like a basis transformation, the sets $\mathbf{M}^u_A$ and $\mathbf{M}^u_B$ effectively inherit the G^*- and G-invariance from the individual POVM elements $F^{(\beta,k)}_A$ and $F^{(\beta,k)}_B$. More precisely, the sets

$$\mathbf{M}^{g(u)}_A := U_g^* \mathbf{M}^u_A U_g^T, \tag{4.35}$$

$$\mathbf{M}^{g(u)}_B := U_g \mathbf{M}^u_B U_g^\dagger, \tag{4.36}$$

are again POVMs corresponding to the announcement with index $g(u)$ in the protocol. Using Eqs. (4.35) and (4.36), and applying Lemma 2, each term I and χ transforms as follows under group unitaries:

$$I(\mathcal{U}_g[\rho_{AB}], \mathbf{M}^u_{AB}) = I(\rho_{AB}, \mathbf{M}^{g^{-1}(u)}_{AB}) \tag{4.37}$$

$$\chi(\mathcal{U}_g[\rho_{AB}], \mathbf{M}^u_A) = \chi(\rho_{AB}, \mathbf{M}^{g^{-1}(u)}_A). \tag{4.38}$$

From these two equations it follows that for each $\mathcal{U}_g[\rho_{AB}]$

$$\bar{r}(\mathcal{E}(\mathcal{U}_g[\rho_{AB}])) = \frac{1}{|\mathcal{L}|}\sum_u \Big(I(\mathcal{U}_g[\rho_{AB}], \mathbf{M}^u_{AB}) - \chi(\mathcal{U}_g[\rho_{AB}], \mathbf{M}^u_A)\Big) \tag{4.39}$$

$$= \frac{1}{|\mathcal{L}|}\sum_u \Big(I(\rho_{AB}, \mathbf{M}^{g^{-1}(u)}_{AB}) - \chi(\rho_{AB}, \mathbf{M}^{g^{-1}(u)}_A)\Big) \tag{4.40}$$

$$= \frac{1}{|\mathcal{L}|}\sum_{g(u')} \Big(I(\rho_{AB}, \mathbf{M}^{u'}_{AB}) - \chi(\rho_{AB}, \mathbf{M}^{u'}_A)\Big) \tag{4.41}$$

$$= \frac{1}{|\mathcal{L}|}\sum_{u'} \Big(I(\rho_{AB}, \mathbf{M}^{u'}_{AB}) - \chi(\rho_{AB}, \mathbf{M}^{u'}_A)\Big) \tag{4.42}$$

$$= \bar{r}(\mathcal{E}(\rho_{AB})). \tag{4.43}$$

In the third last line, we made a index transformation $u' = g^{-1}(u)$. In the second last line we used the fact that $\sum_{g(u)} = \sum_u$ for any $g \in G$, because $g(u)$ is just a permutation of the index u. ■

4.4 Classes of protocols with the same optimal attack and key rate

We observe that for certain protocols with different signal states, the same attack ρ_{AB}^{opt} is found to be optimal. In this section we analyze under what conditions two protocols P and P' from the ONB family have the same optimal attack and same key rate.

Let the sets of signal states $\mathbf{S}$ and $\mathbf{S}'$ be G- and G'-invariant, respectively. We denote the average error rate for each protocol by Q and Q'. Let us denote Alice and Bob's POVM elements by F_A^x and F_B^y for the protocol P and by ${F'_A}^{x'}$ and ${F'_B}^{y'}$ for the protocol P'. The POVMs conditioned on the basis announcement u given in Eqs. (4.35) and (4.36) are denoted by $\mathbf{M}_A^u$ and $\mathbf{M}_B^u$ for protocol P and ${\mathbf{M}'}_A^{u'}$ and ${\mathbf{M}'}_B^{u'}$ for protocol P'. The sets characterizing the possible symmetric attacks are denoted by $\bar{\mathbf{\Gamma}}$ and $\bar{\mathbf{\Gamma}}'$. We also define the set of twirled states as follows

Definition 19 *The sets of all twirled bipartite states $\bar{\rho}_{AB}$ with respect to the group G is*

$$\mathbf{T}_G = \{\mathcal{T}^G[\rho_{AB}] | \rho_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B\}.$$

The following theorem states the criteria under which two protocols have the same optimal attack and the same key rate.

Theorem 10 *If the following three conditions are satisfied, the protocols P and P' have the same optimal attack and the same key rate*

(I) $\mathbf{T}_G = \mathbf{T}_{G'}$.

(II) The subset of $\mathbf{T}_G$ with fixed Q is the same as the subset of $\mathbf{T}_{G'}$ with fixed Q'.

(III) There exists a third group H with a representation $\{W_h; h \in H\}$, such that G and G' are subgroups of H, with the following properties:

(a) $\mathbf{T}_H = \mathbf{T}_G = \mathbf{T}_{G'}$, *and*

(b) for all POVM elements $F_A^x \in \mathbf{M}_A$ and ${F'_A}^{x'} \in \mathbf{M'}_A$ there exists a $W_{h(x,x')}$ in H such that

$$|\mathcal{L}|^2 W^*_{h(x,x')} F_A^x W^T_{h(x,x')} = |\mathcal{L}'|^2 {F'_A}^{x'}. \tag{4.44}$$

Note that IIIb also implies the relation $|\mathcal{L}|^2 W_{h(x,x')} F_B^x W^\dagger_{h(x,x')} = |\mathcal{L}'|^2 {F'_B}^{x'}$ for Bob's measurement operators defined in equation (4.25).

Proof. We show that the optimization of the key rate in Eq. (4.22) leads to the same optimal ρ_{AB}^{opt} and the same key rate for both protocols. There are two parts to the proof. First, from (I) and (II) it follows that $\bar{\mathbf{\Gamma}} = \bar{\mathbf{\Gamma}}'$ by definition. Therefore, the set over which the key rate is optimized is identical for the two protocols. Second, we show that the mutual information and the Holevo quantity

$$\bar{I}(\mathcal{E}(\rho_{AB})) = \frac{1}{|\mathcal{L}|} \sum_u I(\rho_{AB}, \mathbf{M}^u_{AB}), \tag{4.45}$$

$$\bar{\chi}(\mathcal{E}(\rho_{AB})) = \frac{1}{|\mathcal{L}|} \sum_u \chi(\rho_{AB}, \mathbf{M}^u_{A}). \tag{4.46}$$

are identical for both protocols for all states in the set $\bar{\mathbf{\Gamma}}$. We show this for the example of the mutual information, but the same arguments apply to the Holevo quantity as well.

For ONB protocols it is possible to uniquely relabel the unitaries $W_{h(x,x')}$ by $W_{h(u,u')}$, where u and u' are the basis announcements of the protocols P and P', respectively. We can now restate (IIIb) as a condition on the POVMs $\mathbf{M}^u_A$ and $\mathbf{M}^u_B$. For each pair (u, u') there exists unitaries $W_{h(u,u')}$, such that

$$W^*_{h(u,u')} \mathbf{M}^u_A W^T_{h(u,u')} = {\mathbf{M}'}^{u'}_A \tag{4.47}$$

$$W_{h(u,u')} \mathbf{M}^u_B W^\dagger_{h(u,u')} = {\mathbf{M}'}^{u'}_B. \tag{4.48}$$

Furthermore, for a fixed u_0 in P, there exist unitaries $W_{h(u,u_0)} = W_{h(u',u_0)} W_{h(u,u')}$, connecting all u in P to the fixed u_0. Similarly, there exist unitaries $W_{h(u',u'_0)}$ connecting all u' in P' to a fixed u'_0. Using the invariance $\bar{\rho}_{AB} = W^*_h \otimes W_h \bar{\rho}_{AB} (W^*_h \otimes W_h)^\dagger$ and Lemma 2, the mutual information $\bar{I}(\mathcal{E}(\bar{\rho}_{AB}))$ of P and $\bar{I}(\mathcal{E}'(\bar{\rho}_{AB}))$ of P' satisfy that

$$\bar{I}(\mathcal{E}(\bar{\rho}_{AB})) = \frac{1}{|\mathcal{L}|} \sum_{u=1}^{|\mathcal{L}|} I(\bar{\rho}_{AB}, \mathbf{M}^u_{AB}) = I(\bar{\rho}_{AB}, \mathbf{M}^{u_0}_{AB}),$$

$$\bar{I}(\mathcal{E}'(\bar{\rho}_{AB})) = \frac{1}{|\mathcal{L}'|} \sum_{u'=1}^{|\mathcal{L}'|} I(\bar{\rho}_{AB}, {\mathbf{M}'}^{u'}_{AB}) = I(\bar{\rho}_{AB}, {\mathbf{M}'}^{u'_0}_{AB}).$$

Furthermore, since there exists also a unitary $W_{h(u_0,u_0')}$ that connects u_0 to u_0', the same argumentation implies that $I(\bar{\rho}_{AB}, \mathbf{M}_{AB}^{u_0}) = I(\bar{\rho}_{AB}, \mathbf{M}'^{u_0'}_{AB})$ and thus,

$$\bar{I}(\mathcal{E}(\bar{\rho}_{AB})) = \bar{I}(\mathcal{E}'(\bar{\rho}_{AB})).$$

A similar argumentation also holds for the Holevo quantity.

It follows now that the same function $\bar{r}(\mathcal{E}(\rho_{AB})) = \bar{r}(\mathcal{E}'(\rho_{AB}))$ appears in the optimization of protocols P and P'. Since these are now identical optimization problems, they must have the same solution, and therefore the same optimal attack and same key rate. ■

In the next section we will give some examples of protocols with the same optimal attack. We analyze qubit protocols, where we can make use of the point group symmetries, which are commonly used and well studied in the field of crystallography.

4.5 Examples

4.5.1 Generalized Pauli group symmetry

We analyze protocols from the ONB family with signal states that are invariant under the generalized Pauli Π_d group in d dimensions. This group is very well studied, and the symmetrized states $\bar{\rho}_{AB}$ have a particularly simple from. Furthermore, this group will also appear in the next chapter of this thesis (Chapter 5).

Definition 20 *The generalized Pauli group Π_d in d dimensions has d^2 elements. The set of unitaries*

$$U_{r,s} = \sum_{k=0}^{d-1} \omega^{ks} |k+r\rangle\langle k|, \quad \omega = \mathrm{e}^{2\pi i/d}, \tag{4.49}$$

for $r, s = 0, ..., d-1$ form an irreducible unitary representation of Π_d on a d-dimensional Hilbert space. The group has two generators $Z := U_{0,1}$ and $X := U_{1,0}$, from which the entire group is generated by the relation $U_{r,s} = X^r Z^s$.

A nice property of the generalized Pauli group is that twirling map $\mathcal{T}^{\text{Pauli}}$ generates *Bell-diagonal* states

$$\mathcal{T}^{\text{Pauli}}[\rho_{AB}] = \rho_{AB}^{\text{Bell}} = \sum_{r,s=0}^{d-1} u_{r,s} |U_{r,s}\rangle\langle U_{r,s}|, \tag{4.50}$$

with eigenvalues $u_{r,s} \geq 0$ that satisfy $\sum_{r,s} u_{r,s} = 1$. The eigenvectors $|U_{r,s}\rangle = \frac{1}{\sqrt{d}} \sum_k \omega^{ks} |k+r\rangle|k\rangle$ are called Bell states and form a maximally entangled basis of $\mathcal{H}^{\otimes 2}$. We show this property by first expanding an arbitrary state ρ_{AB} in the Bell basis with coefficients $u_{m,n,m,',n'}$,

$$\rho_{AB} = \sum_{m,n} \sum_{m',n'} u_{m,n,m',n'} |U_{m,n}\rangle\langle U_{m',n'}|. \tag{4.51}$$

If we apply the twirling map $\mathcal{T}^{\text{Pauli}}$ to ρ_{AB}, and use the relation that $U^*_{r,s} \otimes U_{r,s} |U_{m,n}\rangle = \omega^{-sm+rn} |U_{m,n}\rangle$, we find that the diagonal elements remain unchanged,

$$\frac{1}{d^2} u_{m,n,m,n} \sum_{r,s} U^*_{r,s} \otimes U_{r,s} |U_{m,n}\rangle\langle U_{m,n}| (U^*_{r,s} \otimes U_{r,s})^\dagger \tag{4.52}$$

$$= \frac{1}{d^2} u_{m,n,m,n} \sum_{r,s} |U_{m,n}\rangle\langle U_{m,n}| \tag{4.53}$$

$$= u_{m,n,m,n} \equiv u_{m,n}, \tag{4.54}$$

and the off-diagonal elements disappear,

$$\frac{1}{d^2} u_{m,n,m',n'} \sum_{r,s} U^*_{r,s} \otimes U_{r,s} |U_{m,n}\rangle\langle U_{m',n'}| (U^*_{r,s} \otimes U_{r,s})^\dagger \tag{4.55}$$

$$= \frac{1}{d^2} u_{m,n,m',n'} \sum_{r,s} \omega^{-s(m-m')} \omega^{r(n-n')} |U_{m,n}\rangle\langle U_{m',n'}| \tag{4.56}$$

$$= 0. \tag{4.57}$$

As shown in Refs. [22, 24], the general form of the purification of ρ^{Bell}_{AB} is given by $|\Psi^{\text{Bell}}\rangle = \sum_{r,s} \sqrt{u_{r,s}} |U_{r,s}\rangle|U_{r,d-s}\rangle$. The representation $U_{r,s}$ is irreducible. Because the complex conjugate representation with the unitaries $U^*_{r,s}$ is also irreducible on $\mathcal{H}_d$, it follows from Schur's lemma that the reduced state $\rho^{\text{Bell}}_A = \frac{\mathbb{1}}{d}$ is proportional to the identity.

4.5.2 Protocols with mutually unbiased bases

Mutually unbiased bases (MUBs), which were first introduced in Refs. [53, 52], are a common choice for the signal states of QKD protocols. For example, in the qubit space, the BB84 and the 6-state protocol use 2 and 3 MUBs, respectively. In higher-dimensional Hilbert spaces, MUB protocols have been studied in Refs. [7, 16, 22, 32, 33, 19].

MUBs are orthonormal bases $\mathcal{B}_\alpha = \{|\psi_1^\alpha\rangle, |\psi_2^\alpha\rangle, ..., |\psi_{d-1}^\alpha\rangle\}$ on d-dimensional Hilbert spaces with the property $|\langle\psi_k^\alpha|\psi_{k'}^{\alpha'}\rangle| = \frac{1}{\sqrt{d}}$ for all $k, k' = 0, ..., d-1$ and $\alpha \neq \alpha'$.

The eigenbases of two generalized Pauli operators (for example Z and X) form two MUBs in any dimension d. It was shown in Ref. [95] that there exist at most $d+1$ MUBs for a d-dimensional Hilbert space. Up to now, no explicite construction of the $d+1$ MUBs is known for an arbitrary dimensions d. If, however, d is a prime number, the existence of exactly $d+1$ MUBs was proven in Ref. [95], and a construction of these $d+1$ MUBs was given in Ref. [4] based on the eigenbases of the $d+1$ generalized Pauli operators Z, ZX, ZX^2, ... , ZX^{d-2}, and ZX^{d-1}. The eigenbasis of the operator Z is denoted by the standard basis with the index Z,

$$\mathcal{B}_Z = \{|\psi_1^Z\rangle, |\psi_2^Z\rangle, ..., |\psi_{d-1}^Z\rangle\}, \tag{4.58}$$

$$|\psi_k^Z\rangle = |k\rangle, \tag{4.59}$$

and the eigenbases of the operators XZ^β with indices $\beta = 0, ..., d-1$ by

$$\mathcal{B}_\beta = \{|\psi_1^\beta\rangle, |\psi_2^\beta\rangle, ..., |\psi_{d-1}^\beta\rangle\}, \tag{4.60}$$

$$|\psi_k^\beta\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{-kj} \omega^{-\beta s_j} |j\rangle, \tag{4.61}$$

where $s_j = \frac{1}{2}(d-j)(d+j-1)$, $\omega = e^{2\pi i/d}$, and where $|j\rangle$ are the basis vectors of the standard basis $\mathcal{B}_Z$.

Let us consider protocols, where the set of signal states $\mathbf{S}_\mathcal{L}$ contains a selection of the Pauli-MUBs. We call these protocols *Pauli-MUB protocols*. In a slight generalization of the result of theorem 2.2 in Ref. [4], we can show that the action of any Pauli operator $U_{r,s}$ on the eigenstates of the Pauli eigenbasis $\mathcal{B}_\alpha$ for $\alpha \in \{Z, 0, 1, ..., d-1\}$ permutes the eigenstates without changing the basis index α. Using this invariance, the set of signal states $\mathbf{S}_\mathcal{L}$ is invariant under the generalized Pauli group (Pauli-invariant).

The key rate of Pauli-MUB protocols

Unfortunately, the full symmetry group of a set $\mathbf{S}_\mathcal{L}$ of Pauli-MUBs is not known explicitly. Thus, one cannot simply write down the general form of the symmetrized states $\bar{\rho}_{AB}$. However, in a first step, we can exploit the invariance of the set $\mathbf{S}_\mathcal{L}$ with respect to the generalized Pauli group. This partial symmetry implies that the optimal attack ρ_{AB}^{opt} must lie in the subset $\mathbf{\Gamma}_{\text{Bell}}$ containing only Bell-diagonal states defined in Eq. (4.50).

Since the Pauli-MUB protocols belong to the ONB family, Eqs. (4.45) and (4.46) can be used to calculate the mutual information $\bar{I}$ and the Holevo quantity $\bar{\chi}$, as well as Eqs. (4.26) and (4.27) to calculate the conditional POVMs $\mathbf{M}_A^\alpha = \{|\psi_k^{*\alpha}\rangle\langle\psi_k^{*\alpha}|\}_k$ and $\mathbf{M}_B^\alpha = \{|\psi_k^\alpha\rangle\langle\psi_k^\alpha|\}_k$. Knowing these formulas, we calculate the conditional states on Bob's side

$$\rho_B^{(\alpha,k)} = \sum_{r,s} u_{r,s}\langle\psi_k^{*\alpha}|U_{r,s}\rangle\langle U_{r,s}|\psi_k^{*\alpha}\rangle/N. \tag{4.62}$$

up to a normalization constant N for each $\alpha \in \{Z, 0, 1, ..., d-1\}$, and for Bell-diagonal states ρ_{AB}^{Bell}. In the following calculations, all operations are done modulo d, and in particular, the indices are to be understood modulo d. The overlaps in $\rho_B^{(\alpha,k)}$ are found to be

$$\langle\psi_k^{*Z}|U_{r,s}\rangle = \frac{1}{\sqrt{d}}\omega^{(k-r)s}|k-r\rangle, \tag{4.63}$$

$$\langle\psi_k^{*\beta}|U_{r,s}\rangle = \frac{1}{\sqrt{d}}\omega^{-kr-\frac{\beta}{2}(r-r^2)}|\psi_{k-(s+\beta r)}^{\beta}\rangle, \tag{4.64}$$

for Z and for $\beta \in \{0, ..., d-1\}$, respectively. After reinserting the overlaps into $\rho_B^{(\alpha,k)}$ and using $N = \frac{1}{d}$, we do an index substitution $y = s + \beta r$ in Eq. (4.64) to obtain the eigenvalue decomposition of the conditional states for $\alpha \in \{Z, 0, 1, ..., d-1\}$

$$\rho_B^{(\alpha,k)} = \sum_y \lambda_y^\alpha |\psi_{k-y}^\alpha\rangle\langle\psi_{k-y}^\alpha|, \tag{4.65}$$

with eigenvalues

$$\lambda_y^Z = \sum_{r=0}^{d-1} u_{y,r}, \tag{4.66}$$

$$\lambda_y^\beta = \sum_{r=0}^{d-1} u_{r,y-\beta r}, \tag{4.67}$$

for Z and $\beta \in \{0, ..., d-1\}$, respectively. The eigenvalue spectrum $\mathbf{\Lambda}^\alpha = \{\lambda_0^\alpha, \lambda_1^\alpha, ..., \lambda_{d-1}^\alpha\}$ for each $\rho_B^{(\alpha,k)}$ is independent of the index k.

Using this notation, the average error rate, the mutual information and the Holevo

quantity turn out to be

$$Q = 1 - \frac{1}{|\mathcal{L}|}\sum_{\alpha\in\mathcal{L}} \lambda_0^\alpha, \tag{4.68}$$

$$\bar{I}(\mathcal{E}(\rho_{AB})) = \log_2 d - \frac{1}{|\mathcal{L}|}\sum_{\alpha\in\mathcal{L}} H(\mathbf{\Lambda}^\alpha), \tag{4.69}$$

$$\bar{\chi}(\mathcal{E}(\rho_{AB})) = S(\rho_{AB}) - \frac{1}{|\mathcal{L}|}\sum_{\alpha\in\mathcal{L}} H(\mathbf{\Lambda}^\alpha), \tag{4.70}$$

where $H(\mathbf{\Lambda}^\alpha) = -\sum_y \lambda_y^\alpha \log(\lambda_y^\alpha)$. Therefore, the key rate for Pauli-MUB protocols is given by the simple formula

$$\bar{r}(\mathcal{E}(\rho_{AB})) = \log d - S(\rho_{AB}). \tag{4.71}$$

For the special protocols with 2, d and $d+1$ Pauli MUBs, we further confine our search for the optimal attack to smaller subsets $\tilde{\mathbf{\Gamma}} \subset \mathbf{\Gamma}_{\text{Bell}}$. The procedure is essentially the same as the one we used in Sec. 4.2 to go from the set $\mathbf{\Gamma}_{\text{ave}}$ to the subset $\bar{\mathbf{\Gamma}}$: for each state ρ_{AB}^{Bell} in $\mathbf{\Gamma}_{\text{Bell}}$, we generate an equivalence class of Bell-diagonal states $\{\rho_{AB}^{(P_i)}; i = 1, ..., n\}$ by applying permutations P_i to the eigenvalues of ρ_{AB}^{Bell}. In contrast to the states $\rho_{AB}^{(U_g)}$ in Eq. (4.7), the states $\rho_{AB}^{(P_i)}$ are not generated using the symmetry group of the signal states. However, since the key rate $\bar{r}(\mathcal{E}(\rho_{AB})) = \log d - S(\rho_{AB})$ is proportional to $S(\rho_{AB})$, all permuted states satisfy the invariance property $\bar{r}(\mathcal{E}(\rho_{AB}^{\text{Bell}})) = \bar{r}(\mathcal{E}(\rho_{AB}^{(P_i)}))$. Furthermore, we choose the permutations in such a way, that the states $\rho_{AB}^{(P_i)}$ give the same error rate as ρ_{AB}. This ensures that the $\rho_{AB}^{(P_i)}$ are again in $\mathbf{\Gamma}_{\text{Bell}}$. Using the convexity property of the key rate, we can conclude that the optimal attack is found in the subset $\tilde{\mathbf{\Gamma}} \subset \mathbf{\Gamma}_{\text{Bell}}$ containing only convex combinations,

$$\tilde{\rho}_{AB} = \frac{1}{n}\sum_i \rho_{AB}^{(P_i)} \in \tilde{\mathbf{\Gamma}}.$$

Note that it suffices to check that the states $\rho_{AB}^{(P_i)}$ have the same average error rate Q as ρ_{AB} in order to be in the set $\mathbf{\Gamma}_{\text{Bell}}$. We do not need to monitor the condition on ρ_A, because $\rho_A^{\text{Bell}} = \mathbb{1}/d$ is automatically satisfied for any Bell-diagonal state.

Protocols with 2 Pauli-MUBs

We show how to obtain the states $\tilde{\rho}_{AB} \in \tilde{\mathbf{\Gamma}}$ on the example of the 2 Pauli-MUB protocols with signal states $\mathbf{S}_{\mathcal{L}} = \{\mathcal{B}_0, \mathcal{B}_Z\}$. The results in this subsection are also valid for any

dimension d, because the construction of two Pauli-MUBs is possible in any dimension, and the set $\mathbf{S}_{\mathcal{L}}$ is invariant under the generalized Pauli group.

We start with a Bell-diagonal state parametrized by $\rho_{AB}^{\text{Bell}} = \sum_{r,s} u_{r,s}|U_{r,s}\rangle\langle U_{r,s}|$. As mentioned above, we generate the (Bell-diagonal) permuted states $\rho_{AB}^{(P_i)}$ by keeping the error rate [see Eq. (4.68) for Bell-diagonal states]

$$Q = 1 - \frac{1}{2}\left(\lambda_0^0 + \lambda_0^Z\right) = 1 - \frac{1}{2}\left(2u_{0,0} + \sum_{r=1}^{d-1}(u_{r,0} + u_{0,r})\right), \tag{4.72}$$

invariant. The invariance of Q is guaranteed if the permutations P_i leave the sets $\mathbf{U}_a = \{u_{0,0}\}$, $\mathbf{U}_b = \{u_{0,r}, u_{r,0}; r = 1, ..., d-1\}$ and $\mathbf{U}_c = \{u_{r,s}; r, s = 1, ..., d-1\}$ invariant. Such permutations P_i are, for example, independent permutations of the eigenvalues in each set. Therefore, the average over all eigenvalues in each set will appear in the convex combination $\tilde{\rho}_{AB}$. In this particular example, the state $\tilde{\rho}_{AB}$ will have three different types of independent eigenvalues a, b and c corresponding to the three sets $\mathbf{U}_a$, $\mathbf{U}_b$ and $\mathbf{U}_c$:

$$\tilde{\rho}_{AB} = a|U_{0,0}\rangle\langle U_{0,0}| + c\sum_{r,s=1}^{d-1}|U_{r,s}\rangle\langle U_{r,s}| + b\sum_{r=1}^{d-1}\left(|U_{r,0}\rangle\langle U_{r,0}| + |U_{0,r}\rangle|U_{0,r}\rangle\right). \tag{4.73}$$

The error rate of $\tilde{\rho}_{AB}$ reads $Q = (d-1)b + (d-1)^2 c$ and the normalization condition is $a + 2(d-1)b + d^2 c = 1$. From these two extra conditions, we are able to eliminate two of the three coefficients a and b. Afterwards, we optimize the key rate over the remaining coefficient c analytically. The optimum is found at

$$a = (1-Q)^2, \quad b = \frac{Q(1-Q)}{d-1}, \quad c = \frac{Q^2}{(d-1)}, \tag{4.74}$$

and the minimum key rate, which was independently obtained in Ref. [87], is given by

$$r_{\min} = \log d + 2(1-Q)\log(1-Q) + 2Q\log\left(\frac{Q}{d-1}\right). \tag{4.75}$$

We plot the key rates for $d = 2, 3, 5, 7, 11, 13$ in Fig. 4.2 in dependence of the average error rate. This plot compares the performance of the protocols in dependence of the error rate. For a fair comparaison, we must specify the channel model and the corresponding error model. Then, we can compare the key rates in dependence of channel parameters, for example, the distance between Alice and Bob.

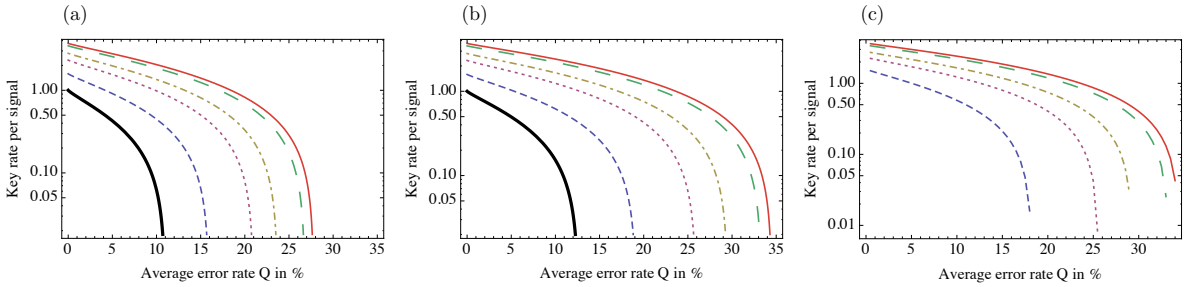


Figure 4.2: Key rates of protocols with (a) 2, (b) $d+1$ and (c) d Pauli-MUBs for $d = 2$ (thick (bottom) line, black), $d = 3$ (dashed line, blue), $d = 5$ (dotted line, purple) , $d = 7$ (dash-dotted line, yellow) , $d = 11$ (large dashed line, green) and $d = 13$ (solid (top) line, red). These plots do not serve as a comparison of the performance of the different protocols. For a fair comparaison, we must specify the channel model, and plot the key rates in dependence of channel parameters.

Protocols with $d+1$ Pauli-MUBs

Consider protocols with $d+1$ MUBs $\mathbf{S}_{\mathcal{L}} = \{\mathcal{B}_Z, \mathcal{B}_0, \mathcal{B}_1, ...\mathcal{B}_{d-1}\}$. This construction of MUBs is only valid when d is a prime number. In contrast to the protocols with 2 Pauli-MUBs, the protocols with $d+1$ Pauli-MUBs are tomographically complete, which means that ρ_{AB} can be uniquely determined. Using the strategy described in the previous section, we construct the set $\tilde{\mathbf{\Gamma}}$ for $d+1$ Pauli-MUB protocols. We choose a Bell-diagonal state ρ_{AB}^{Bell} and calculate the error rate

$$Q = 1 - \frac{1}{d+1}\left((d+1)u_{0,0} + \sum_{(r,s)\neq(0,0)} u_{r,s}\right). \tag{4.76}$$

In this formula we used that $\sum_{\beta=0}^{d-1} u_{r,-\beta r} = \sum_{\gamma=0}^{d-1} u_{r,\gamma}$ for $r \neq 0$. The error rate defines the sets $\mathbf{U}_a = \{u_{0,0}\}$ with one eigenvalue, and $\mathbf{U}_b = \{u_{r,s}; (r,s) \neq (0,0)\}$ with the remaining d^2-1 eigenvalues. By averaging over all permutations P_i, which leave the sets $\mathbf{U}_a$ and $\mathbf{U}_b$ unchanged, we determine the form of the states

$$\tilde{\rho}_{AB} \quad = a|U_{0,0}\rangle\langle U_{0,0}| + b \sum_{(r,s)\neq(0,0)} |U_{r,s}\rangle\langle U_{r,s}|, \tag{4.77}$$

The average error rate $Q = d(d-1)b$ and the normalization condition $a + (d^2-1)b = 1$ uniquely define the coefficients a and b:

$$a = 1 - \frac{d+1}{d}Q, \quad b = \frac{Q}{d(d-1)}. \tag{4.78}$$

Since there are no free parameters, there is only one state in the set $\tilde{\mathbf{\Gamma}}$, and, therefore, the optimization of the key rate is trivial. The key rate reads

$$r_{\min} = \log d + \frac{d+1}{d}Q \log\left(\frac{Q}{d(d-1)}\right) + \left(1 - \frac{d+1}{d}Q\right)\log\left(1 - \frac{d+1}{d}Q\right), \tag{4.79}$$

which was independently found in Ref. [87]. We plot the key rates for $d = 2, 3, 5, 7, 11, 13$ in Fig. 4.2. Again, the plot is not intended to compare the performance of the protocols.

Protocols with d Pauli-MUBs

The signal states of protocols using d Pauli-MUBs are $\mathbf{S}_{\mathcal{L}} = \{\mathcal{B}_0, \mathcal{B}_1, ...\mathcal{B}_{d-1}\}$. The construction of d MUBs is valid for prime dimensions. Unlike the protocols with $d+1$ Pauli-MUBs, the protocols analyzed here are not tomographically complete. The error rate

$$Q = 1 - \frac{1}{d}\left(d\, u_{0,0} + \sum_{r=0}^{d-1}\sum_{s=1}^{d-1} u_{r,s}\right) \tag{4.80}$$

defines three sets $\mathbf{U}_a = \{u_{0,0}\}$, $\mathbf{U}_b = \{u_{r,s}; r = 0, ..., d-1, s = 1, ..., d-1\}$ and $\mathbf{U}_c = \{u_{0,s}; s = 1, ..., d-1\}$, which determine the states in $\tilde{\mathbf{\Gamma}}$ by

$$\tilde{\rho}_{AB} = a|U_{0,0}\rangle\langle U_{0,0}| + c\sum_{s=1}^{d-1}|U_{0,s}\rangle\langle U_{0,s}| + b\sum_{r=0}^{d-1}\sum_{s=1}^{d-1}|U_{r,s}\rangle\langle U_{r,s}|. \tag{4.81}$$

The parameters a, b and c are further constricted by the normalization condition $a + d(d-1)b + (d-1)c = 1$, and the error rate condition $Q = (d-1)^2 b + (d-1)c$. We can express two of the three eigenvalues by

$$a = 1 + c - \frac{dQ}{d-1} \quad b = \frac{Q - (d-1)c}{(d-1)^2}. \tag{4.82}$$

We optimize the key rate over the free parameter c, and plot the numerically obtained key rates $r_{\min}$ in Fig. 4.2 for different dimensions.

4.5.3 Qubit protocols

In this section we show examples of protocols with the same optimal attack as the BB84 protocol and the 6-state protocol. We analyze qubit protocols, because we can make use of the point group symmetries, which are well studied groups.

Protocols with the same optimal attack as the 6-state protocol

The 6-state protocol is a Pauli-MUB protocol with 3 MUBs on a qubit Hilbert space. The key rate and the states $\bar{\rho}_{AB}$ in the set $\bar{\mathbf{\Gamma}}$ were already calculated in Sec. 4.5.2.

The signal states of the 6-state protocol form a regular octahedron in the Bloch sphere representation, as shown in Fig. 4.3 (b). The symmetry group of the octahedron is the discrete group O with a unitary irreducible representation on the qubit space. A symmetry group G' that satisfies condition (I) in Theorem 10 is for example the icosahedron group I [56, 17]. We can now construct protocols with signal states that are invariant under O- or I-symmetry. There are many sets of signal states that are invariant under these symmetries. Our choices are sets of signal states that form a cube (O-symmetry), a dodecahedron (I-symmetry) or an icosahedron (again I-symmetry) on the Bloch sphere, consisting of 8, 20 and 12 states, respectively. For each state there exists an orthogonal state on the opposite side of the Bloch sphere, which together form a basis of the qubit space. See Fig. 4.3 for a representation of the signal states of the 6-state and the cube protocol.

The average error rate adopts the same form for our chosen protocols, namely, $Q = 2b$, where b is defined in Eq. (4.77). Therefore, condition (II) in Theorem 10 is also satisfied, and we conclude that the sets $\bar{\mathbf{\Gamma}}$ for these protocols are identical to the set given in the case of the 6-state protocol. Since there is only one state in $\bar{\mathbf{\Gamma}}$ for the 6-state protocol, we can already conclude that the optimal attack of the 6-state, the cube, the icosahedron and the dodecahedron protocols is the same.

Protocols with the same optimal attack as the BB84 protocol

We analyze protocols with $2n$ ($n \geq 2$) signal states $\mathbf{S}\{|\varphi_x\rangle, x = 0, ..., 2n-1\}$, that are distributed equally in the equatorial plane of the Bloch sphere, represented by the Bloch vectors

$$\vec{s}_x^{(2n)} = (\sin(\pi x/n), 0, \cos(\pi x/n)) \quad x = 0, ..., 2n-1. \tag{4.83}$$

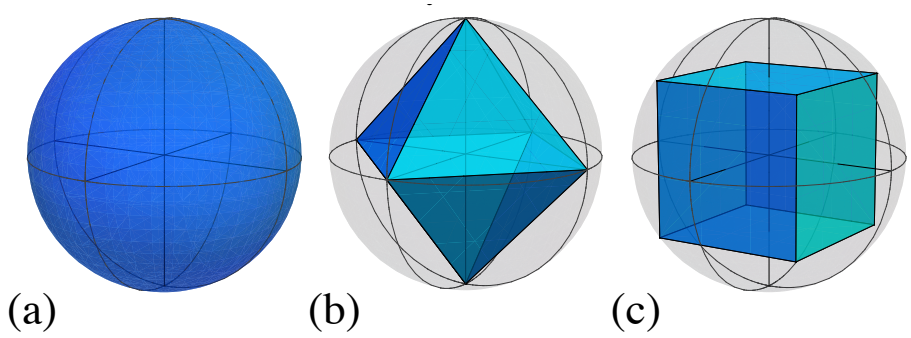


Figure 4.3: Representation of sets of signal states on the Bloch sphere related to the 6-state protocol. (a) States that are invariant under $SU(2)$ (b) States of the 6-state protocol (Octahedron), invariant under O-symmetry, (c) States of the cube protocol, invariant under O-symmetry. The octahedron protocol has the same optimal attack and the same key rate as the 6-state protocol.

For each state $|\varphi_x\rangle$ there exists an orthogonal state on the opposite side of the Bloch sphere, which together form a basis. For $n = 2$, we recover the signal states of the BB84 protocol. In Fig. 4.4 the signal states of the $2n$ protocols for $n = 2, 3$ are represented on the Bloch sphere.

The symmetry group of the signal states of the $2n$-protocol is called the Dihedral group denoted by D_{2n}. In the character tables of Refs. [56, 17], we find the form of the set $\mathbf{T}_{D_{2n}}$ for $n = 2, 3$. It turns out that $\mathbf{T}_{D_6} = \mathbf{T}_{D_4}$, where $\mathbf{T}_{D_4}$ contains the symmetrized states $\bar{\rho}_{AB}$ of the BB84 protocol [see Eq. (4.73) for $d = 2$, and Example 1 in Sec. 2.4.7]. The error rate $Q = b + c$ of the $2n$-protocol with $n = 3$ is the same as for the BB84 protocol, where b and c are defined in Eq. (4.73). Thus we can conclude that $\bar{\mathbf{\Gamma}}_6 = \bar{\mathbf{\Gamma}}_4 \equiv \bar{\mathbf{\Gamma}}_{\text{BB84}}$.

Let us define Alice's POVM elements of the BB84 and the $2n$-protocol by $F_A^{(BB84),x}$ for $x = 1, ...4$ and $F_A^{(2n),x'}$ for $x' = 1, ..., 2n$. In both cases, the POVM elements are projectors onto the signal states. We can identify the group H in Theorem 10 by the phase-covariant symmetry group $D_\infty = U(1) \times \Pi_2$, where Π_2 is the Pauli group of dimension 2 and $U(1)$ is the unitary group. In the tables of Ref. [17], we find that the set $\mathbf{T}_{D_\infty}$ is identical to $\mathbf{T}_{D_4}$ and $\mathbf{T}_{D_6}$. The phase-covariant group contains all rotations about the axis $(0, 1, 0)$ on the Bloch sphere, as well as rotations by π about all axes lying in the (x, z)-plane. Thus, it also contains group elements that satisfy Eq. (4.44) in Theorem 10 for any pair $F_A^{(BB84),x}$ and $F_A^{(2n),x}$. Therefore, we conclude that the optimal attack for the $2n$-protocol for $n = 3$ can be identified by the same as the optimal attack of the BB84 protocol.

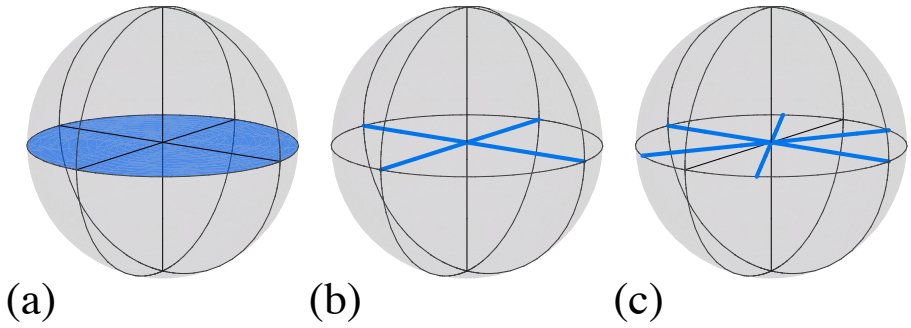


Figure 4.4: Representation of signal states on the Bloch sphere for protocols related to the BB84 protocol. (a) States that are invariant under D_∞ (b) States of the BB84 protocol, D_4-symmetry (c) States of the $2n$-protocol for $n = 3$, D_6-symmetry. The $2n$-protocol for $n = 3$ has the same optimal attack and the same key rate as the BB84 protocol.

The cuboid protocol

For some protocols with tomographically complete measurement settings the set $\bar{\mathbf{\Gamma}}$ contains more than one state. This has to do with loss of information during the symmetrization process. Recall that Alice and Bob only keep the averaged quantity Q, but otherwise ignore the measurement outcomes completely. This means that introducing symmetries to a problem can come at the expense of increasing the number of states in $\bar{\mathbf{\Gamma}}$.

As an example consider a qubit protocol where the signal states lie on the corners of a rectangular cuboid. The 8 signal states form 4 bases defined by the Bloch vectors

$$\vec{s}_1 = (\pm \sin\theta, \pm \cos\theta, 0), \tag{4.84}$$
$$\vec{s}_2 = (\pm \sin\theta, \mp \cos\theta, 0), \tag{4.85}$$
$$\vec{s}_3 = (0, \pm \cos\theta, \pm \sin\theta), \tag{4.86}$$
$$\vec{s}_4 = (0, \pm \cos\theta, \mp \sin\theta), \tag{4.87}$$

where θ describes the angle between the y-axis of the Bloch sphere and the corners of the cuboid. This protocol is composed of four bases.

The symmetry group of this protocol is the same as of the BB84 protocol (D_4). Although condition (I) in Theorem 10 is satisfied, the error rate of the cuboid protocol is given by $Q = \frac{1}{2}(3b + c + (b - c)\cos(2\theta))$, which is different from the BB84 error definition. Moreover, we could not find a group H to satisfy the condition (III). We performed numerical optimizations and found that the optimal attack of the cuboid protocol is different from the optimal attack on the BB84 protocol.

Note that for $\theta = \frac{\pi}{2}$, we recover the BB84 protocol. For $\theta = \frac{\pi}{4}$ the signal states span a cube, which we already discussed in Sec. 4.5.3.

4.6 Conclusion

We analyze the conditions under which a symmetric optimal attack can be assumed on a QKD protocol. If the parameter estimation is based on coarse-grained quantities, we prove that the optimal attack is without loss of generality a symmetric attack, if the protocol and the postselection exhibit sufficient symmetries. In particular, we show that for protocols with signal states that are orthonormal bases, and postselection on matching bases, the optimal attack is always symmetric. Furthermore, we identify classes of protocols which are characterized by a common optimal attack.

We calculate the key rate of protocols where the signal states are eigenbases of the generalized Pauli operators for 2, d and $d+1$ bases in a d-dimensional Hilbert space. We also give examples of protocols that have the same optimal attack as the BB84 and the 6-state protocols

Throughout the subsequent chapters of this thesis, we will use the tools developed in this chapter to claim symmetric optimal attacks for other protocols.

Chapter 5

Connection between optimal cloning and optimal eavesdropping

5.1 Introduction

In the previous chapter the objective was to find the optimal attack in order to calculate the key rate for a protocol. In this chapter we want to investigate about the optimal interaction U_E^{opt} between Eve and the signals.

One specific type of interaction that Eve can use to attack a QKD protocol is an optimal quantum cloner [18]. An optimal cloner is a unitary transformation U_C^{opt} that acts on the signal states (and some ancilla states), with the objective of producing two copies of the signal states. The optimal cloner has the property that the copies emerge with the highest fidelity (with respect to the original signal states) allowed by quantum mechanics. An optimal cloner is called symmetric if the fidelities of the two copies are the same, and asymmetric if the fidelities are different. Consider now the following eavesdropping attack: Eve uses an optimal asymmetric cloner to copy the signal states sent by Alice, forwards one copy to Bob, and keeps the other copy for herself. She choses the optimal cloner in such a way that the fidelity of Bob's copy is in agreement with Bob's measurement outcomes.

A cloning attack is optimal if it coincides with the optimal eavesdropping strategy, namely if $U_E^{\text{opt}} = U_C^{\text{opt}}$. In Refs. [22, 32, 33] cloning attacks were used to model Eve's attack, but optimality was only conjectured. Indeed, for some protocols (e.g. the BB84 or the 6-state protocol), the optimal attack is known to be an optimal cloner, for example, by comparing the optimal attacks in Ref. [80] to the optimal cloners in Ref. [24]. However, in general the relationship between optimal cloning and optimal eavesdropping is unknown.

The goal in the present chapter is to establish the connection between optimal eavesdropping on QKD protocols and optimal cloning in the context of the Devetak-Winter security proof for protocols with direct, one-way reconciliation. We consider protocols with enough symmetries so that, without loss of generality, the optimal attack is symmetric. In this scenario, it turns out that a necessary condition for an optimal cloner to be a candidate for an optimal attack is the strong covariance condition defined in Ref. [24]. This condition ensures that the optimal cloner and the optimal attack are drawn from the same set, and that the optimal cloner uses the same number of ancilla states as the optimal eavesdropping attack. If strong covariance does not hold for the optimal cloner, we can already conclude that the optimal attack on the QKD protocol is not an optimal cloner.

We have already calculated the optimal attack for qubit-based protocols (e.g. the BB84 and the 6-state protocol) and for protocols in d-dimensional Hilbert spaces using mutually unbiased bases (MUBs) (e.g. protocols with 2 MUBs, $d+1$ MUBs or d MUBs) in the previous chapter. Here we will compare these attacks to the optimal cloner. The results of this chapter are published in Ref. [34].

5.2 Optimal quantum Cloners

In this section we summarize quantum cloners along the lines of Refs. [24, 30]. A quantum cloner $\mathcal{C}$ is a map that creates two copies of quantum states $\varphi_x = |\varphi_x\rangle\langle\varphi_x|$ drawn from a set $\mathbf{S}$. Let us define three isomorphic Hilbert spaces $\mathcal{H}_A$, $\mathcal{H}_B$ and $\mathcal{H}_C$ each with dimension d. A cloner $\mathcal{C}$ is a completely positive and trace preserving map $\mathcal{C} : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_C$ that takes a state $\varphi_x \in \mathcal{H}_A$ to $\mathcal{C}(\varphi_x) \in \mathcal{H}_B \otimes \mathcal{H}_C$.

The quality of each copy k ($k = B, C$) is determined by the single-clone Uhlmann fidelity $f_k(\varphi_x, \mathcal{C}(\varphi_x))$ of the copy with respect to the original state φ_x. If the states φ_x are pure, the Uhlmann fidelity reads

$$f_B(\varphi_x, \mathcal{C}(\varphi_x)) = \mathrm{tr}\{|\varphi_x\rangle\langle\varphi_x|_B \otimes \mathbb{1}_C \cdot \mathcal{C}(\varphi_x)\} \tag{5.1}$$

$$f_C(\varphi_x, \mathcal{C}(\varphi_x)) = \mathrm{tr}\{\mathbb{1}_B \otimes |\varphi_x\rangle\langle\varphi_x|_C \cdot \mathcal{C}(\varphi_x)\} \tag{5.2}$$

Instead of the single-clone fidelity $f_k(\varphi_x, C(\varphi_x))$, it is often assumed that only the average fidelity over all signal states

$$F_k = \frac{1}{|\mathbf{S}|} \sum_{\varphi_x \in \mathbf{S}} f_k(\varphi_x, \mathcal{C}(\varphi_x)) \tag{5.3}$$

is of interest. The cloner is called optimal if copy C emerges with maximal average fidelity (F_C), while the fidelity F_B of the copy B has a fixed value.

The cloning transformation can also be described using the Choi-Jamiolkowski isomorphism [54, 8] with a non-maximally entangled state. For this purpose, let $\mathcal{C}$ act on the second half of a source state $|\Phi\rangle$ defined in Eq. (3.1) for the set of signal states $\mathbf{S}$. This relates $\mathcal{C}$ to a positive operator $\sigma_{ABC} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ via the rule

$$\sigma_{ABC} = (\mathbb{1} \otimes \mathcal{C})|\Phi\rangle\langle\Phi|. \tag{5.4}$$

The trace-preserving property of $\mathcal{C}$ translates to $\sigma_A = \mathrm{tr}_{BC}\, \sigma_{ABC} = \rho_A$, where ρ_A is the reduced state of the source state $|\Phi\rangle$. The map $\mathcal{C}$ can be recovered trom σ_{ABC} via the reverse transformation realized by

$$\mathcal{C}(\varphi_x) = \frac{1}{p(x)} \mathrm{tr}_A[F_A^x \otimes \mathbb{1}_B \otimes \mathbb{1}_C \cdot \sigma_{ABC}]. \tag{5.5}$$

where the F_A^x are the POVM elements defined in Eq. (3.3). The reverse transformation effectively corresponds to preparing the states $|\varphi_x\rangle$ in the source-replacement scheme for the cloner. In this language, the optimal cloning map described by a state $\sigma_{ABC}^{\mathrm{opt}}$.

5.2.1 Covariant cloners

Let the set of quantum states $\mathbf{S}$ be G-invariant. If the figure of merit of the cloning transformation is the average fidelity, then for every cloning map σ_{ABC}, the equivalence class of maps $\{U_g^* \otimes U_g \otimes U_g \sigma_{ABC} (U_g^* \otimes U_g \otimes U_g)^\dagger; \forall g \in G\}$ yields the same average fidelity F_k. Furthermore, due to the linearity of the trace, there exists a covariant cloning map

$$\bar{\sigma}_{ABC} = \sum_{g \in G} U_g^* \otimes U_g \otimes U_g \sigma_{ABC} (U_g^* \otimes U_g \otimes U_g)^\dagger \tag{5.6}$$

with the same average fidelity F_k as σ_{ABC}. As a consequence, the optimal cloning map, $\sigma_{ABC}^{\mathrm{opt}}$, can always be chosen as a covariant map, without loss of generality [30]. The covariant state in Eq. (5.6) satisfies the commutation relation

$$[\bar{\sigma}_{ABC}, U_g^* \otimes U_g \otimes U_g] = 0. \tag{5.7}$$

5.2.2 Strong covariant cloner

The unitary realization U_C of the map $\mathcal{C}$ can be uniquely described by the purification of $\bar{\sigma}_{ABC}$. In the canonical formulation, the purification of such a state lives on the extended Hilbert space $\mathcal{H}^{\otimes 6}$. Some cloners, however, can be realized with a purification on a smaller Hilbert space $\mathcal{H}^{\otimes 4}$ composed of four systems $H_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \otimes \mathcal{H}_D$, each system having the same dimension. In Ref. [24], cloners with such a purification are called strong covariant cloners and are defined as follows:

Definition 21 *A cloner is called strong covariant if it has a purification $|\Sigma\rangle_{ABCD}$ on $\mathcal{H}_{ABCD}$ with the property*

$$U_g^* \otimes U_g \otimes U_g \otimes U_g^* |\Sigma\rangle_{ABCD} = |\Sigma\rangle_{ABCD} \; \forall g \in G. \tag{5.8}$$

The strong covariant cloners are a subset of the covariant cloners, because for every strong covariant cloner $|\Sigma\rangle$, the trace over the fourth system D returns a covariant state $\bar{\sigma}_{ABC}$.

In Ref. [24], it is shown that determining the optimal cloner is a convex optimization problem. That means, the optimal cloner is an extremal point of the convex set of covariant cloning maps. Two theorems about extremal maps are proven in Ref. [24].

Theorem 11 *(Chiribella et al. [24]). Let the unitaries U_g be an irreducible representation of the group G, and let $K = \{\bar{\sigma}_{ABC}\}$ denote the set of covariant cloning maps defined in Eq. (5.7). Then, every cloning map $\bar{\sigma}_{ABC}$, which allows a strong covariant purification is an extremal point of the convex set K.*

This theorem states that the strong covariant maps are a subset of the extremal maps. The converse - that the extremal maps are a subset of the strong covariant maps - is not true in general. The next theorem, however, describes a special case in which the set of extremal maps and the set of strong covariant maps coincide:

Theorem 12 *(Chiribella et al. [24]). If the set of states $\mathbf{S}$ to be cloned is G-invariant under the generalized Pauli group Π_d, then the set of strong covariant cloning maps is equal to the set of extremal maps. The generalized Pauli group is defined in Def. 20 in Sec. 4.5.1.*

Using this Theorem, the optimal cloner $\sigma_{ABC}^{\text{opt}}$ is found in the set of strong covariant maps, if the signals in $\mathbf{S}$ are invariant under the generalized Pauli group. This means that the purification of $\sigma_{ABC}^{\text{opt}}$ is described by a four-partite state $|\Sigma\rangle_{ABCD}^{\text{opt}}$ with the property (5.8).

5.3 Connection between optimal cloners and optimal attacks

Recall that the optimal attack $\bar{\rho}_{AB}^{\text{opt}}$ was found by optimizing the key rate over the set of symmetrized states $\bar{\mathbf{\Gamma}}$. In Eq. (4.10), we showed that the purification $|\Psi\rangle$ of a symmetrized state $\bar{\rho}_{AB} \in \bar{\mathbf{\Gamma}}$ has the property $U_g^* \otimes U_g \otimes U_g \otimes U_g^* |\Psi\rangle = |\Psi\rangle$ for all $g \in G$. We define the set of all such purifications as follows:

Definition 22 *The set $\mathbf{\Delta}$ contains the purifications $|\Psi\rangle$ of the symmetrized states in $\bar{\mathbf{\Gamma}}$. All states in $\mathbf{\Delta}$ satisfy the symmetry condition $U_g^* \otimes U_g \otimes U_g \otimes U_g^* |\Psi\rangle = |\Psi\rangle$ for all $g \in G$, and are compatible with the averaged quantity Q and fixed ρ_A.*

We identify the optimal attack on a QKD protocol with an optimal cloner if Eve's interaction U_E^{opt} coincides with the optimal cloning transformation U_C^{opt}, or, in terms of the purifications, if $|\Psi\rangle^{\text{opt}} = |\Sigma\rangle^{\text{opt}}$. Comparing the purifications in the set $\mathbf{\Delta}$ to the cloning interactions, it turns out that all eavesdropping attacks described in the set $\mathbf{\Delta}$ correspond to representations of strong covariant cloners. We can therefore make the following conclusion:

Observation 1 *The optimal cloner can only be the optimal attack, if it is strong covariant. Otherwise, one can already conclude that $|\Psi\rangle^{opt} \neq |\Sigma\rangle^{opt}$.*

At this point, the strong covariance property alone does not uniquely determine if the optimal attack is an optimal cloner. Even if the optimal cloner is strong covariant, we can only conclude that the optimal attack is an optimal cloner if the set $\mathbf{\Delta}$ contains exactly one state. Otherwise, in order to compare the optimal attack with the optimal cloner, we must perform the optimization.

5.3.1 Examples with Pauli-invariant signal states

As mentioned in Theorem 12, a sufficient requirement for a cloning map to allow a strong covariant realization is the Pauli-invariance of the set of states to be cloned. Hence, if the signal states of a QKD protocol are Pauli-invariant, the corresponding cloning attack on that protocol is certainly realized by a strong covariant cloner. Therefore, we compare the optimal attack of protocols with Pauli-invariant signal states to the corresponding optimal cloners. In this section, we analyse protocols with 2, d and $d+1$ Pauli-MUBs, which have

Pauli-invariant signal states. These protocols already appeared in Sec. 4.5.2. For protocols with d and $d+1$ Pauli-MUBs, the dimension d is prime, while for 2 Pauli-MUBs the results hold for any dimension.

For ONB protocols the average error rate Q in Def. 18 is related to the average fidelity F_B of Bob's clone by the simple relation $F_B = 1 - Q$. The average fidelity for ONB protocols is given by

$$F_B = \frac{1}{|\mathcal{L}|} \sum_{\beta \in \mathcal{L}} \sum_{k} \operatorname{tr} \left\{ |\varphi^*_{(\beta,k)}\rangle\langle\varphi^*_{(\beta,k)}| \otimes |\varphi_{(\beta,k)}\rangle\langle\varphi_{(\beta,k)}| \rho_{AB} \right\}. \tag{5.9}$$

2 **Pauli-MUBs**

The optimal attack on a protocol with 2 Pauli-MUBs calculated in Eq. (4.74) is exactly the same as the optimal phase-covariant cloner in d dimensions found in Ref. [22]. This can be seen by comparing the state ρ^{opt}_{AB} to the cloner in Ref. [22].The connection between optimal cloning and the optimal attack for 2 MUBs was already conjectured in [22].

When $d = 2$ we recover the BB84 protocol. Furthermore, since we showed Sec. 4.5.3 that the $2n$ protocol for $n = 3$ has the same optimal attack as the BB84 protocol, the optimal attack on the $2n$ protocol is also the optimal phase-covariant cloner.

We also analyze the cuboid protocol, for which we know from Sec. 4.5.3 that the optimal attack is different from the optimal attack on the BB84. Numerical optimizations show that the optimal attack on the cuboid protocol is not an optimal cloner.

$d+1$ **Pauli-MUBs**

As shown in Sec. 4.5.2, there is only one state state in the set $\bar{\mathbf{\Gamma}}$ for protocols with $d+1$ Pauli-MUBs. Therefore, we can already conclude that the optimal cloner and the optimal attack are equal. This connection was already conjectured in [22]. The cloner in this case is the optimal universal cloner in d dimensions [21, 20].

For $d = 2$, we recover the the 6-state protocol. The optimal attack on the 6-state protocol is the universal cloner [18, 38] that clones all the states on the Bloch sphere equally well. Since we know from Sec. 4.5.3 that the optimal attack on the cube, the icosahedron and the dodecahedron protocol is the same as the optimal attack on the 6-state protocol, we can conclude that it is also the optimal universal cloner.

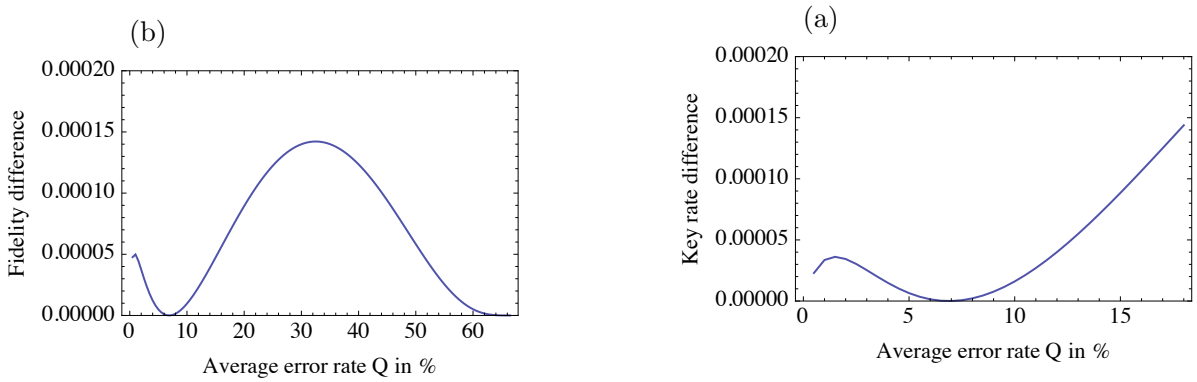


Figure 5.1: (a) A plot of the difference of the key rates $\delta r = r_{\mathrm{MPC}} - r_{\min}$ for the scenarios where Eve uses the optimal cloner (r_{MPC}), and where she uses the optimal attack ($r_{\min}$) for $d = 3$. (b) A plot of the difference of the fidelities $\delta F_E = F_E^{\mathrm{MPC}} - F_E^{\mathrm{attack}}$ for the scenarios where Eve uses the optimal MPC cloner (F_E^{MPC}) and where she uses the optimal attack (F_E^{attack}) for $d = 3$.

d Paul-MUBs

For the protocol with d Pauli-MUBs, we compare the optimal attack to the optimal multiple phase-covariant (MPC) cloner U_{MPC} given in Ref. [59]. This cloner copies all states of the form $|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{i\phi_j} |j\rangle$ for $\phi_j \in [0, 2\pi)$ optimally. If it is known that the eavesdropper performed an attack based on the optimal MPC cloner, Alice and Bob can expect some key rate r_{MPC}. Numerical optimizations for $d = 3, 5, 7, 11$ and 13 show that r_{MPC} is always bigger or equal than the key rate $r_{\min}$ in Eq. (4.22) that results from the optimal attack. Therefore, the optimal MPC cloner is not the optimal attack: $U_{\mathrm{MPC}} \neq U_E^{\mathrm{opt}}$. In Fig. 5.1 we plot the difference between the key rates $r_{\mathrm{MPC}} - r_{\min}$. We denote Eve's average fidelity of the optimal MPC cloner by F_E^{MPC} calculated according to equation (5.3). Since each of Eve's attacks U_E can be viewed as a (non-optimal) cloner, we can calculate the average clone fidelity of the transformation corresponding to the optimal attack U_E^{opt}. We call this fidelity F_E^{attack}, and plot the difference $F_E^{\mathrm{MPC}} - F_E^{\mathrm{attack}}$ for $d = 3$ in Fig. 5.1.

We would like to remark that the U_{MPC} produces optimal copies of more than just the necessary d Pauli MUBs. It is possible that there exists a cloner U_d that provides copies of the d Pauli-MUBs with a higher fidelity F_E^d for a fixed error rate, than U_{MPC}: $F_E^d \geq F_E^{\mathrm{MPC}}$. This raises the question, if the cloner U_d could be the optimal attack U_E^{opt}. To answer this, we turn the question around and ask from the cloning point of view, whether the optimal attack U_E^{opt} can play the role of the optimal cloner U_d. For this purpose, we compare Eve's

fidelity F_E^{attack} to the fidelity F_E^d. We know from our numerical optimization how F_E^{attack} compares to F_E^{MPC}: we plotted the difference $F_E^{\text{MPC}} - F_E^{\text{attack}}$ in Fig. 5.1. From this plot we see that, in general, $F_E^{\text{MPC}} > F_E^{\text{attack}}$. However, we know by construction of U_d that the fidelity $F_E^d \geq F_E^{\text{MPC}}$. By transitivity it follows that $F_E^d > F_E^{\text{attack}}$, which proves that the optimal attack is not equivalent to the optimal cloner U_d either.

5.4 Conclusion

We analyze the connection between the optimal attack on a QKD protocol and the optimal cloning attack, in which the eavesdropper uses an optimal cloner to attack the protocol. We analyze protocols that are from the ONB family with Pauli group symmetries in the signal states and compare the optimal symmetric attack to optimal covariant cloners.

It turns out that a necessary condition for the cloning transformation to be an optimal attack is the strong covariance condition, which guarantees that the optimal attack and the optimal cloner are chosen from the same set. However, this condition is not sufficient to uniquely identify the optimal attack with the optimal cloner, except in the case where only one state is found in the set from which the optimal attack and the optimal cloner are chosen. Protocols which use the $d+1$ mutually unbiased eigenbases of the generalized Pauli group fall into this category.

We analyze the optimal attack of protocols using 2, d and $d+1$ Pauli-MUBs in d-dimensional Hilbert spaces. Intuitively, one expects that the optimal attack can always be identified with an optimal cloner. We prove that this intuition is correct in the case of 2 and $d+1$ Pauli-MUBs, but for protocols using d Pauli-MUBs, the connection between optimal attack and optimal cloner fails.

Chapter 6

Unbalanced phase-encoded BB84 protocol

6.1 Introduction

Perhaps the BB84 protocol [10] is the most well-known QKD protocol. In the BB84 protocol, the bit values of the key are encoded in orthogonal quantum states of two conjugate bases. Next to the theoretical security analysis of the BB84 protocol [88, 57, 67, 68], there have been numerous experimental implementations of this protocol, both using optical fibre [40] and free space links [48, 58] as the quantum channel. Furthermore, the bit information is usually encoded in a photonic degree of freedom, either in the polarization of photons, or the phase of two consecutive photon pulses [40].

In the phase-encoded implementation of the BB84 protocol, the phase between two consecutive pulses prepared by Alice determines the bit and the basis value of the sent signal. In the actual experimental realization of the phase-encoded BB84 protocol with Mach-Zehnder interferometers (see Fig. 6.1), the phase modulator, which is in one arm of the interferometer, introduces loss. While this does not change the observed error rate in the data, it changes the signal states and the measurements of the protocol. Since this is now a different protocol, the security proofs tailored to the BB84 protocol no longer apply in this scenario.

In this chapter, we provide a security proof of the phase-encoded BB84 in the infinite key limit where we take into account the loss in the phase modulator (*unbalanced phase-encoded protocol*). We use the Devetak-Winter security proof [31, 57] to calculate the key rate.

In the limit where the phase reference is a strong pulse corresponding to the extreme case of an unbalanced interferometer, the security has been analyzed in Ref. [63]. Furthermore, a first rough security proof approach linking the unbalanced phase-encoded protocol to the BB84 protocol at the cost of key rate has been presented in Ref. [60].

We provide a qubit-based security proof, that we later extend to optical modes. On the source side, we extend the validity of the qubit-based security proof to optical modes using the tagging approach [41, 51] in the decoy framework [49, 62, 93]. On the other hand, the squashing model [5, 92, 71] justifies the assumption of a qubit-based security proof on the receiver's side. The results in this chapter were published in Ref. [35].

6.2 Protocol setup

6.2.1 Unbalanced phase-encoded (UPE) protocol

A scheme of the protocol setup is depicted in Fig. 6.1. Alice sends photon pulses through a Mach-Zehnder interferometer with a long arm and a short arm, to create the signal states $|\varphi_x\rangle$. In the long arm, Alice changes the relative phase φ_x of the two pulses with a phase modulator to imprint the basis and bit information on the signal. Alice chooses the phases $\varphi_x = \frac{\pi}{2}x$ for $x \in \{0, 1, 2, 3\}$ with equal probability for the four signal states. The phases $\varphi_x \in \{0, \pi\}$ and $\varphi_x \in \{\pi/2, 3\pi/2\}$ correspond to the bit values $\{0, 1\}$ in the "even" and "odd" basis, respectively. Likewise, the receiver, Bob, detects the signals by means of a Mach-Zehnder interferometer. Bob chooses the phase $\varphi_B \in \{0, \pi/2\}$, which determines the basis ("even" or "odd") of his measurement. Bob chooses each measurement setting with probability 1/2.

The pulses arrive at Bob's detectors in three different time slots, either in the top output port (slots c_1, c_2, and c_3 in Fig. 6.1) or in the bottom output port (slots d_1, d_2, and d_3 in Fig. 6.1). Only the middle clicks (slots c_2 and d_2) are used for the key generation. The outside clicks (slots c_1, c_3, d_1, and d_3) are pulses that did not interfere at Bob's second beam splitter. If the signal produces interference (i. e., if the detectors click in the middle time slot), then Bob determines the bit value of the incoming signal based on his phase setting.

To obtain the raw data for the key generation, Alice and Bob first execute a sifting step, in which they announce the basis ("even" or "odd") for each signal publicly and discard all data points where their basis choices did not match.

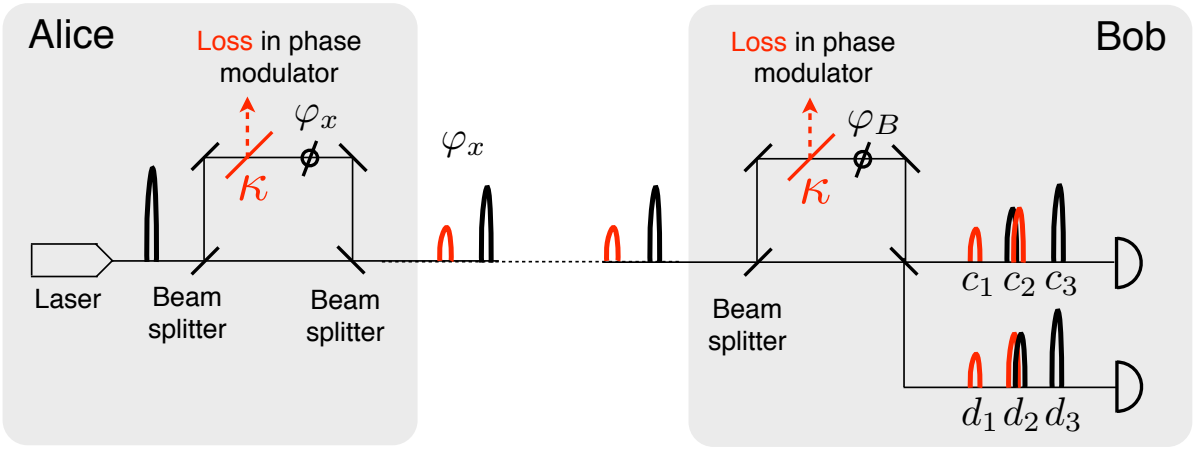


Figure 6.1: Alice and Bob use a Mach-Zehnder interferometer to prepare and detect the signal pulses. Only the interfering pulses, which produce clicks in the time slots c_2 and d_2 (black-red and red-black overlapping pulses) are used for the key generation.

The lossy phase modulator typically introduces a loss in one of the arms of the interferometer, producing pulses with different amplitudes. We model the lossy phase modulator by a perfect (lossless) phase modulator followed by a beamsplitter with transmissivity $\kappa \leq 1$ that simulates the loss.

We will refer to this protocol with three different detection time slots as the unbalanced phase-encoded (UPE) protocol.

6.2.2 Polarizing beam splitter (PBS) protocol

As a slight variation of the protocol, consider Alice encoding her outgoing pulses in different polarizations, and Bob replacing his first beamsplitter by a polarizing beamsplitter (see Fig. 6.2). This causes the two pulses to arrive simultaneously at Bob's second (interfering) beamsplitter. If he also rotates the polarization of the signal in one arm, all signals will interfere. We analyze the security proof of this protocol as well. Throughout this chapter we will call this protocol the PBS protocol.

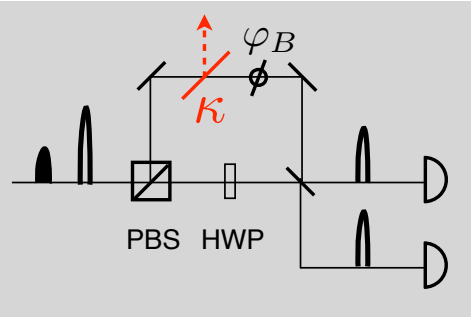


Figure 6.2: A variation of the protocol with the pulses encoded in different polarization. Bob places a polarizing beam splitter (PBS) at the entrance of his interferometer, and rotates the polarization in one arm of the interferometer, for example by using a half wave plate (HWP) to cause the desired interference.

6.3 Security proof framework

6.3.1 Lossless interferometer picture

It is generally difficult to provide a security proof for a scenario with a lossy measurement. Therefore, in the case of the UPE protocol we construct a picture where a lossy beamsplitter with transmissivity $\frac{1}{2\xi}$ is placed into the quantum channel followed by a lossless interferometer with an uneven first beamsplitter with transmissivity

$$\xi = \frac{1}{1+\kappa}. \tag{6.1}$$

This *lossless interferometer* picture is equivalent to the original picture with the lossy phase modulator in the long arm of the interferometer, as it yields the same measurement outcomes. The two pictures are shown in Fig. 6.3. However, in the lossless interferometer picture we can deal with the loss (that has now been outsourced to the channel) by giving Eve control over it and treating it like regular channel loss in the security proof.

In the case of the PBS protocol, we allot the control over the polarizing beam splitter and the lossy beamsplitter with transmissivity κ in the long arm to Eve, leaving Bob with a lossless detector.

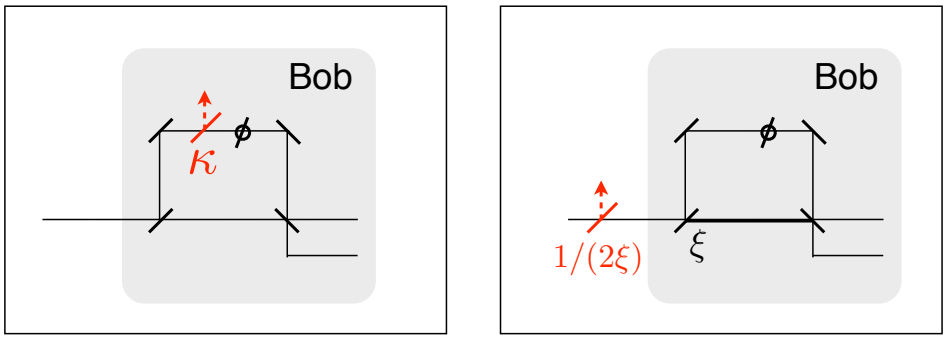


Figure 6.3: a) Original picture of the unbalanced phase-encoded protocol with the loss in Bob's interferometer. b) Equivalent lossless interferometer picture with a loss $1/(2\xi)$ in the channel followed by lossless interferometer with an uneven beam splitter with transmissivity ξ.

6.3.2 Hardware fix

One simple way to recover the original BB84 scenario is by manually introducing a beamsplitter with the same transmissivity κ in the shorter arm of each of the interferometers to compensate for the loss due to the phase modulator. Alternatively, one can replace the first beamsplitter in the interferometer by a biased beamsplitter with transmissivity $1-\xi$. A schematic of these alternatives is shown in Figs. 6.4 a) and 6.5 a).

The BB84 signal states and measurements are recovered in the equivalent lossless interferometer pictures, which are shown in Figs. 6.4 b) and 6.5 b) for the two hardware fix possibilities. Under the assumption that the loss in Bob's detector is attributed to Eve, the security proof reduces to the known BB84 security proof. The loss in Alice's device, however, is not attributed to Eve, because the intensity of the outgoing signal is calibrated at the output of Alice's lab.

6.4 Qubit-to-qubit scenario

In the following, we study the case where Alice sends a single photon and Bob obtains a single photon (qubit-to-qubit scenario). We analyze the signal structure and the measurements of the UPE protocol and the PBS protocol and provide a security proof (*qubit*

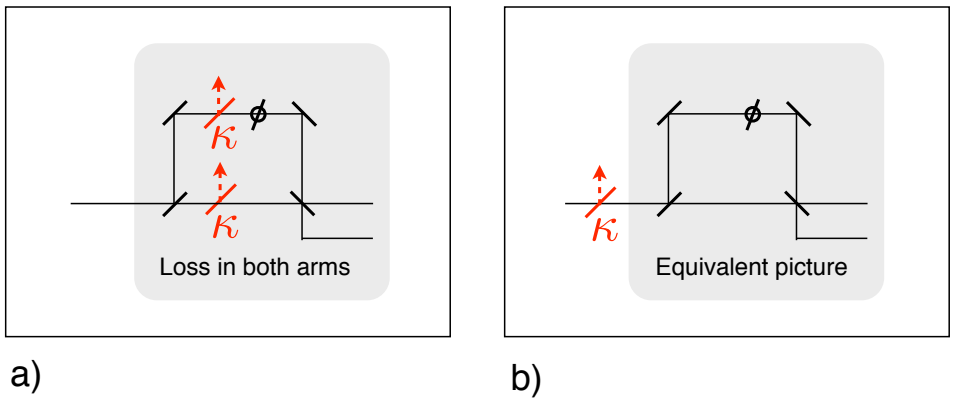


Figure 6.4: a) Hardware fix with the same amount of loss introduced in the short arm of the interferometer to compensate for the loss due to the phase modulator. b) Equivalent lossless interferometer picture.

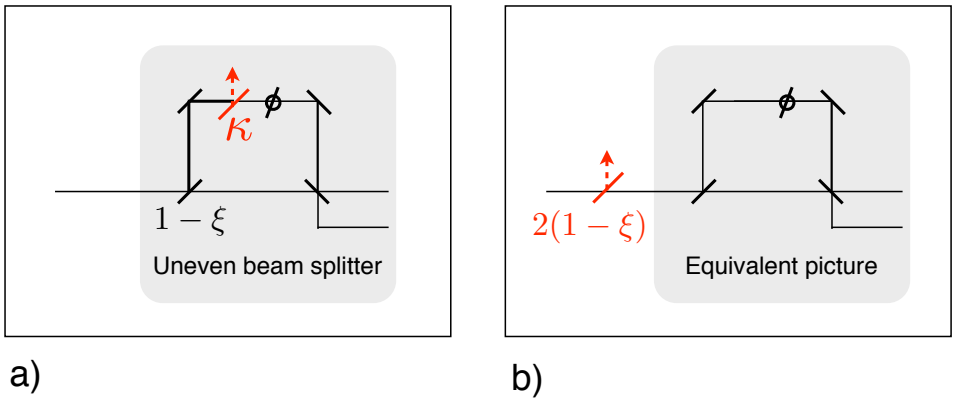


Figure 6.5: Hardware fix with a biased beamsplitter in the interferometer to compensate for the loss due to the phase modulator. b) Equivalent lossless interferometer picture.

security proof). Later, in Sec. 6.6, we embed the qubit security proof into the more realistic scenario with optical modes in infinite-dimensional Hilbert spaces using decoy states [62], tagging [41, 51] and squashing [5, 92, 71].

6.4.1 Alice's signal states

If a single photon is distributed over the two time modes (pulses) that are emerging from Alice's device, the resulting Hilbert space of the signal states ($\mathcal{H}_S$) is a qubit space. We denote the creation operators of the two time modes by $a_0^\dagger$ and $a_1^\dagger$, and define the two canonical basis vectors $|0\rangle = a_0^\dagger|\text{vac}\rangle$ and $|1\rangle = a_1^\dagger|\text{vac}\rangle$ of $\mathcal{H}_S$. After Alice has imprinted her phase choice onto the pulses, the signal leaving her apparatus can be in any of the four possible states

$$|\varphi_x\rangle = \sqrt{\xi}|0\rangle + \sqrt{1-\xi}e^{i\pi x/2}|1\rangle \tag{6.2}$$

for $x \in \{0,1,2,3\}$. Recall Eq. (6.1) that $\xi = \frac{1}{1+\kappa}$. In Fig. 6.6 we show a representation of the signal state on the Bloch sphere in comparison to the signal states of the BB84 protocol. Alice then sends the signal states, each prepared in one of the above four forms with equal probability, through a quantum channel to Bob.

We describe the signal preparation in the source-replacement scheme. In our case, the entangled source state is $|\Phi\rangle_{AS} = \sqrt{\xi}|00\rangle + \sqrt{1-\xi}|11\rangle$ with a reduced density matrix

$$\rho_A = \xi|0\rangle\langle 0| + (1-\xi)|1\rangle\langle 1|. \tag{6.3}$$

Alice's POVM elements on the system A are then essentially BB84 measurements

$$F_A^x = \frac{1}{2}P\left[\frac{|0\rangle + e^{-i\pi x/2}|1\rangle}{\sqrt{2}}\right]. \tag{6.4}$$

for $x \in \{0,1,2,3\}$. We use the notation $P\big[|\alpha\rangle\big] = |\alpha\rangle\langle\alpha|$.

6.4.2 Bob's detection in the case of the UPE protocol

The modes $a_0^\dagger$ and $a_1^\dagger$ arrive at Bob's detector after Eve has interacted with the signals. The output of Bob's detectors carries six modes in total, two in each of the three time slots. We denote the modes of the top (bottom) detector by $c_i^\dagger$ ($d_i^\dagger$) for $i = 1,2,3$, respectively.

For a fixed phase $\varphi_B \in \{0, \pi/2\}$, the transformation of the $a_i^\dagger$ to the modes in the top and bottom detectors yields (up to global phases):

$$
\begin{aligned}
c_1^\dagger &= \frac{1}{\sqrt{2}}\sqrt{\xi}a_0^\dagger, \\
c_2^\dagger &= \frac{1}{\sqrt{2}}(\sqrt{1-\xi}a_0^\dagger + e^{i\varphi_B}\sqrt{\xi}a_1^\dagger), \\
c_3^\dagger &= \frac{1}{\sqrt{2}}\sqrt{1-\xi}a_1^\dagger, \\
d_1^\dagger &= \frac{1}{\sqrt{2}}\sqrt{\xi}a_0^\dagger, \\
d_2^\dagger &= \frac{1}{\sqrt{2}}(\sqrt{1-\xi}a_0^\dagger - e^{i\varphi_B}\sqrt{\xi}a_1^\dagger), \\
d_3^\dagger &= \frac{1}{\sqrt{2}}\sqrt{1-\xi}a_1^\dagger.
\end{aligned}
$$

We choose to combine several outputs into one POVM element of Bob's measurement. In terms of the incoming modes $|0\rangle$ and $|1\rangle$, Bob's POVM elements are

$$
\begin{aligned}
F_B^y &= \frac{1}{4}P[\sqrt{1-\xi}|0\rangle + \sqrt{\xi}e^{i\pi y/2}|1\rangle)], \\
F_B^{\text{out}} &= \xi|0\rangle\langle 0| + (1-\xi)|1\rangle\langle 1|,
\end{aligned}
\tag{6.5}
$$

where y runs over $\{0, 1, 2, 3\}$. The four POVM elements F_B^y correspond to inside clicks (time slot 2) in the two bases, while F_B^{out} denotes the POVM element of the outside clicks (time slots 1 and 3).

6.4.3 Bob's detection in the case of the PBS protocol

In a similar manner, the modes in the output ports of Bob's interferometer in the PBS protocol are found to be

$$
\begin{aligned}
c^\dagger &= \frac{1}{\sqrt{2}}(e^{-i\varphi_B}a_0^\dagger - ia_1^\dagger), \\
d^\dagger &= \frac{1}{\sqrt{2}}(-ie^{-i\varphi_B}a_0^\dagger + a_1^\dagger).
\end{aligned}
$$

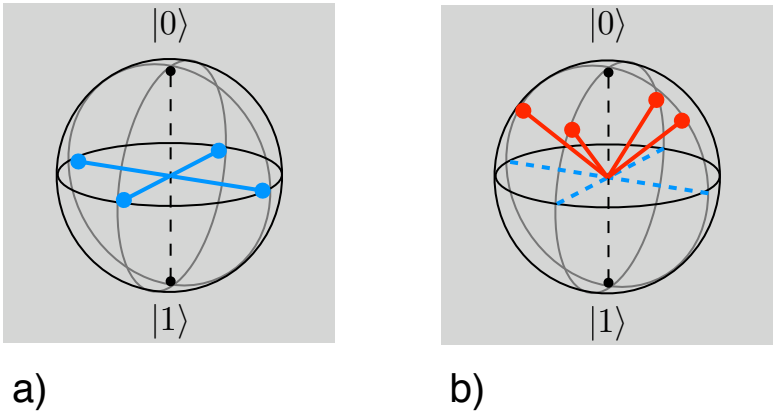


Figure 6.6: Comparison of the qubit signal states on the Bloch sphere. a) The signal states of the BB84 protocol, b) the signal states of the protocol with a lossy phase modulator.

There are only two output modes, since there are no outside clicks in this protocol. Bob's corresponding POVM on the input system has four elements for $y \in \{0, 1, 2, 3\}$

$$F_B'^{\,y} = \frac{1}{2} P\left[\frac{(|0\rangle + e^{i\pi y/2}|1\rangle}{\sqrt{2}}\right], \tag{6.6}$$

which is essentially a BB84 measurement.

Remark: Indeed, in the PBS scenario, both Alice's and Bob's measurements are BB84 measurements. However, the difference between the PBS protocol and the BB84 protocol is found in the reduced density matrix ρ_A in Eq. (6.3), which contains the information about the modified signal structure.

6.4.4 Postselection

In order to filter out uncorrelated data, Alice announces the basis of her outcome ("even" or "odd"), and Bob announces the basis of his outcome ("even" or "odd") if he saw an inside click. If he saw an outside click, Bob announces "out". Based on the announcements, they keep the events where both announced "even" or both announced "odd", and discard the rest. We denote the events where they had the same announcement by $u =$ "even" or $u =$ "odd". The identification of the announcements effectively defines the subsets $\mathbf{m}_A^{\text{even}} = \{F_A^0, F_A^2\}$, $\mathbf{m}_A^{\text{odd}} = \{F_A^1, F_A^3\}$, $\mathbf{m}_B^{\text{even}} = \{F_B^0, F_B^2\}$ and $\mathbf{m}_B^{\text{odd}} = \{F_B^1, F_B^3\}$ of the POVMs $\mathbf{M}_A$

and $\mathbf{M}_B$, which contain the POVM elements corresponding to the announcement $u =$ "even" or $u =$ "odd".

The Kraus operators on Alice's side for this kind of postselection are

$$K_A := K_A^{\text{odd}} = K_A^{\text{even}} = \mathbb{1}/\sqrt{2}. \tag{6.7}$$

The new, renormalized POVM elements in $\mathbf{M}_A^u$ conditioned on u are related to the original POVM elements in $\mathbf{m}_A^u$ simply by a factor of 2:

$$\begin{aligned} \mathbf{M}_A^{\text{even}} &= \{2F_A^0, 2F_A^2\}, \\ \mathbf{M}_A^{\text{odd}} &= \{2F_A^1, 2F_A^3\}. \end{aligned} \tag{6.8}$$

We also calculate the Kraus operators on Bob's side for "odd" and "even" announcements. There is now a dependence on the imbalance ξ in Bob's Kraus operators, but the Kraus operators are again equal for the "even" and "odd" bases

$$K_B := K_B^{\text{even}} = K_B^{\text{odd}} = \frac{1}{\sqrt{2}} \begin{pmatrix} \sqrt{1-\xi} & 0 \\ 0 & \sqrt{\xi} \end{pmatrix}. \tag{6.9}$$

Here the Kraus operators are presented in the basis $\{|0\rangle, |1\rangle\}$. It is straightforward to find Bob's new POVMs after postselection

$$\begin{aligned} \mathbf{M}_B^{\text{even}} &= \{F_B^{y,\text{even}}\} = \{2{F'_B}^0, 2{F'_B}^2\}, \\ \mathbf{M}_B^{\text{odd}} &= \{{F_B}^{y,\text{odd}}\} = \{2{F'_B}^1, 2{F'_B}^3\}, \end{aligned} \tag{6.10}$$

expressed in terms of the BB84-type measurements ${F'_B}^y$ in Eq. (6.6).

Since the Kraus operators for "even" and "odd" announcements are equal, we obtain the conditional density operators

$$\mathcal{K}[\rho_{AB}] := \mathcal{K}^{\text{even}}[\rho_{AB}] = \mathcal{K}^{\text{odd}}[\rho_{AB}], \tag{6.11}$$

where

$$\mathcal{K}[\rho_{AB}] = \frac{K_A \otimes K_B \, \rho_{AB} K_A^\dagger \otimes K_B^\dagger}{\tilde{p}}, \tag{6.12}$$

$$\tilde{p} = \text{tr}\{K_A \otimes K_B \, \rho_{AB} K_A^\dagger \otimes K_B^\dagger\}. \tag{6.13}$$

Alice and Bob extract a key from the data sets with coinciding basis independently. According to Eq. (3.28), the key rate extracted from a ρ_{AB} with postselection on $u \in \{\text{even}, \text{odd}\}$ is given by

$$\bar{r}(\mathcal{E}(\rho_{AB})) = \sum_u p(u) \Big(I(\mathcal{K}[\rho_{AB}], \mathbf{M}_{AB}^u) - \chi(\mathcal{K}[\rho_{AB}], \mathbf{M}_A^u) \Big) \tag{6.14}$$

While the normalization $\tilde{p}$ depends on the density matrix ρ_{AB}, the normalized probability distribution $p(u)$ appearing in the key rate does not, and is given by $p(\text{odd}) = p(\text{even}) = \frac{1}{2}$.

6.4.5 The key rate optimization problem

Optimizing the key rate $\bar{r}(\mathcal{E}(\rho_{AB}))$ over the set $\mathbf{\Gamma}$ gives the minimum key rate (see also Eq. (3.31)):

$$r_{\min} = \bar{I}_{\text{obs}} - \sup_{\rho_{AB} \in \mathbf{\Gamma}} \bar{\chi}(\mathcal{E}(\rho_{AB})). \tag{6.15}$$

In this expression, $\bar{I}_{\text{obs}}$ is fixed for all $\rho_{AB} \in \mathbf{\Gamma}$, and thus does not enter the optimization. The Holevo quantity is $\bar{\chi}(\mathcal{E}(\rho_{AB})) = \frac{1}{2}\sum_u \chi(\mathcal{K}[\rho_{AB}], \mathbf{M}_A^u)$ for $u \in \{\text{even}, \text{odd}\}$.

6.5 Symmetric optimal attack

6.5.1 Symmetries of signal states

The symmetry group G of the set of signal states is the cyclic group C_4 with four elements. A reducible representation of C_4 in the canonical basis of the signal states is given by

$$U_g = \begin{pmatrix} 1 & 0 \\ 0 & e^{ig\pi/2} \end{pmatrix} \quad g \in \{0, 1, 2, 3\}. \tag{6.16}$$

While Alice and Bob's POVMs F_A^x, F_B^y and $F_B'^y$ satisfy the symmetry relations

$$U_g^* F_A^x U_g^T = F_A^{x+g}, \tag{6.17}$$
$$U_g F_B^y U_g^\dagger = F_B^{y+g}, \tag{6.18}$$
$$U_g F_B'^y U_g^\dagger = F_B'^{y+g}, \tag{6.19}$$

where addition is taken modulo 4, the reduced density operator ρ_A and the POVM element of the outside clicks F_B^{out} remain invariant under the action of U_g

$$\rho_A = U_g^* \rho_A U_g^T, \tag{6.20}$$
$$F_B^{\text{out}} = U_g F_B^{\text{out}} U_g^\dagger. \tag{6.21}$$

Note that complex conjugation in the canonical basis and Hermitian conjugation are equivalent operations for all unitaries U_g, because they are simultaneously diagonal in this basis.

Not only are the POVMs $\mathbf{M}_A$ and $\mathbf{M}_B$ C_4-invariant, but also the postselected POVMs $\mathbf{M}_A^u$ and $\mathbf{M}_B^u$ for $u \in \{\text{even}, \text{odd}\}$ satisfy a certain symmetry relation with respect to C_4:

$$\begin{aligned} U_g^* \mathbf{M}_A^u U_g^T &= \mathbf{M}_A^{g(u)}, \\ U_g \mathbf{M}_B^u U_g^\dagger &= \mathbf{M}_B^{g(u)}. \end{aligned} \tag{6.22}$$

For this particular example $g(u) = u \oplus \text{parity}(g)$ with $\text{parity}(g) \in \{\text{even}, \text{odd}\}$. The addition is defined by the rules: even$\oplus$even = odd$\oplus$odd = even and odd$\oplus$even = even$\oplus$odd = odd.

6.5.2 Coarse-grained parameter estimation

We show now that the optimal attack is symmetric with respect to the symmetry group of the signal states. We assume that Alice and Bob perform the parameter estimation based on the average error rate

$$Q[\{p(x,y)\}] = \frac{p(0,2) + p(2,0) + p(1,3) + p(3,1)}{2\tilde{p}}, \tag{6.23}$$

which is calculated from the detailed probability distribution $p(x,y)$ and the normalization $\tilde{p}$ in Eq. (6.13). The average error rate satisfies the invariance property $Q[\{p(x,y)\}] = Q[\{p_g(x,y)\}]$ in Eq. (4.5). In this scenario, the key rate is optimized over the larger set $\mathbf{\Gamma}_{\text{ave}}$, which contains all state ρ_{AB} with fixed Q and ρ_A in Eq. (6.3).

In order to restrict the optimization to the subset $\bar{\mathbf{\Gamma}}$ containing only symmetric states, $\bar{\rho}_{AB}$, it suffices to show that

$$-\sup_{\rho_{AB} \in \mathbf{\Gamma}_{\text{ave}}} \bar{\chi}(\mathcal{E}(\rho_{AB})) \geq -\sup_{\bar{\rho}_{AB} \in \bar{\mathbf{\Gamma}}} \bar{\chi}(\mathcal{E}(\bar{\rho}_{AB})), \tag{6.24}$$

because the Holevo quantity is the only term that depends on ρ_{AB}. In fact, we do not use the weak convexity of the terms $I(\mathcal{K}[\rho_{AB}], \mathbf{M}_{AB}^u)$ (Theorem 7) for this protocol, because the restriction on the *a priori* probability distribution is violated for states of the form $\mathcal{K}[\rho_{AB}]$ and $\mathcal{K}[\mathcal{U}_g[\rho_{AB}]]$. If Eq. (6.24) holds, we can assume a symmetric optimal attack and bound the key rate by

$$r_{\min} \geq \bar{I}_{\text{obs}} - \sup_{\bar{\rho}_{AB} \in \bar{\mathbf{\Gamma}}} \bar{\chi}(\mathcal{E}(\bar{\rho}_{AB})). \tag{6.25}$$

6.5.3 Concavity and equivalence properties of the Holevo quantity

In this section the goal is to prove the inequality (6.24) for both the UPE and the PBS protocol. To prove this inequality, we need to show the following two properties of the Holevo quantity: the concavity property,

$$\bar{\chi}(\mathcal{E}(\bar{\rho}_{AB})) \geq \frac{1}{|G|}\sum_g \bar{\chi}(\mathcal{E}(\mathcal{U}_g[\rho_{AB}])), \tag{6.26}$$

and equivalence property,

$$\bar{\chi}(\mathcal{E}(\rho_{AB})) = \bar{\chi}(\mathcal{E}(\mathcal{U}_g[\rho_{AB}])). \tag{6.27}$$

UPE protocol

First, we show the concavity and equivalence properties of $\bar{\chi}$ in case of the UPE protocol. As a consequence of the commutation relation of the Kraus operators K_A and K_B with all unitaries U_g,

$$[K_A, U_g] = [K_B, U_g] = 0, \tag{6.28}$$

the map $\mathcal{K}$ also commutes with the symmetry group:

$$\mathcal{K}[\mathcal{U}_g[\rho_{AB}]] = \mathcal{U}_g[\mathcal{K}[\rho_{AB}]]. \tag{6.29}$$

Moreover, $\mathcal{K}$ acts linearly on any convex combination of states of the form $\mathcal{U}_g[\rho_{AB}]$, for example on the symmetrized state $\bar{\rho}_{AB}$

$$\mathcal{K}[\bar{\rho}_{AB}] = \frac{1}{|G|}\sum_g \mathcal{K}[\mathcal{U}_g[\rho_{AB}]]. \tag{6.30}$$

We have now all ingredients to show the concavity and the equivalence property of $\bar{\chi}$. Using Eq. (6.30) and the concavity property of χ (Theorem 8), the concavity of $\bar{\chi}$ follows:

$$\begin{aligned}
\bar{\chi}(\mathcal{E}(\bar{\rho}_{AB})) &= \frac{1}{2}\sum_u \chi\left(\mathcal{K}[\bar{\rho}_{AB}], \mathbf{M}_A^u\right) \\
&\geq \frac{1}{2}\sum_u \frac{1}{|G|}\sum_g \chi\left(\mathcal{K}[\mathcal{U}_g[\rho_{AB}]], \mathbf{M}_A^u\right) \\
&= \frac{1}{|G|}\sum_g \bar{\chi}(\mathcal{E}(\mathcal{U}_g[\rho_{AB}]).
\end{aligned} \tag{6.31}$$

To show the equivalence property (6.27), we first use Lemma 2, and apply it to each term

$$\chi(\mathcal{U}_g[\rho_{AB}], \mathbf{M}_A) = \chi(\rho_{AB}, U_g^T \mathbf{M}_A U_g^*). \tag{6.32}$$

Because of the commutation rule in Eq. (6.29) and the G-invariance of the $\mathbf{M}_A^u$ in Eq. (6.22), it also holds that

$$\begin{aligned}
\chi\left(\mathcal{K}[\mathcal{U}_g[\rho_{AB}]], \mathbf{M}_A^{g(u)}\right) &= \chi\left(\mathcal{U}_g[\mathcal{K}[\rho_{AB}]], \mathbf{M}_A^{g(u)}\right) && (6.33)\\
&= \chi\left(\mathcal{U}_g[\mathcal{K}[\rho_{AB}]], U_g^T \mathbf{M}_A^{g(u)} U_g^*\right) && (6.34)\\
&= \chi\left(\mathcal{K}[\rho_{AB}], \mathbf{M}_A^u\right). && (6.35)
\end{aligned}$$

The equivalence transfers to $\bar{\chi}$ by means of Eqs. (6.35) and (6.11):

$$\begin{aligned}
\bar{\chi}(\mathcal{E}(\rho_{AB})) &= \frac{1}{2}\sum_u \chi(\mathcal{K}[\rho_{AB}], \mathbf{M}_A^u)\\
&= \frac{1}{2}\sum_u \chi(\mathcal{K}[\mathcal{U}_g[\rho_{AB}]], \mathbf{M}_A^{g(u)}) \qquad (6.36)\\
&= \frac{1}{2}\sum_{g(u)} \chi(\mathcal{K}[\mathcal{U}_g[\rho_{AB}]], \mathbf{M}_A^u) = \bar{\chi}(\mathcal{E}(\mathcal{U}_g[\rho_{AB}])).
\end{aligned}$$

Having showed concavity and equivalence, we can assume without loss of generality that the optimal attack is chosen from the set $\bar{\Gamma}$. The main properties used to prove the equivalence and concavity were essentially Eqs. (6.7), (6.9) and (6.28).

PBS protocol

The PBS protocol differs from the UPE protocol only in the measurements on Bob's side. Bob's filters for the PBS protocol,

$$K_{B'} := K_{B'}^{\text{even}} = K_{B'}^{\text{odd}} = \mathbb{1}/\sqrt{2} \tag{6.37}$$

also satisfy the properties in Eqs. (6.7), (6.9) and (6.28). As these were the two properties needed to show concavity and equivalence of $\bar{\chi}$, a similar proof goes through for the PBS case, and so we can again assume a symmetric optimal attack of the form (6.38).

6.5.4 Numerical results

We now calculate the key rate of the unbalanced phase-encoded protocol in the qubit-to-qubit scenario. The most general symmetric state $\bar{\rho}_{AB}$ with respect to the C_4 symmetry group is described by the density matrix

$$\bar{\rho}_{AB} = \begin{pmatrix} a & & & f^* \\ & b & & \\ & & c & \\ f & & & d \end{pmatrix} \tag{6.38}$$

with open parameters a, b, c, d and f that satisfy the trace condition $\mathrm{tr}\,\bar{\rho}_{AB} = 1$. The matrix representation of $\bar{\rho}_{AB}$ is with respect to the canonical basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. This density operator was obtained using representation theory and Schur's lemma in Sec. 2.4.

The states in the set $\bar{\mathbf{\Gamma}}$ are further constrained by the fixed reduced density operator ρ_A and the error rate Q. For a symmetric state $\bar{\rho}_{AB}$ the reduced density matrix and the error rate are given by

$$\mathrm{tr}_B(\bar{\rho}_{AB}) = \begin{pmatrix} a+b & \\ & c+d \end{pmatrix}, \tag{6.39}$$

and

$$Q = \frac{\tilde{p} - \frac{1}{2}\Re[f]\sqrt{\xi(1-\xi)}}{2\tilde{p}}, \tag{6.40}$$

with the normalization $\tilde{p} = \frac{1}{4}((1-\xi)(a+c) + \xi(b+d))$, where $\Re[f]$ denotes the real part of f.

We calculate the Holevo quantity $\bar{\chi}$ and use MATLAB, calling the optimization function *fmincon* to perform a numerical optimization of $\bar{\chi}(\mathcal{E}(\bar{\rho}_{AB}))$ over the states $\bar{\rho}_{AB} \in \bar{\Gamma}$. The symmetry arguments so far only concerned the Holevo quantity. In order to simulate the classical data, which is used for the calculation of the mutual information, we assume a typical scenario with symmetric observations. The mutual information $\bar{I}_{\mathrm{obs}} = 1 - h(Q)$ is then a function of the average error rate Q only.

In Fig. 6.7 we show a plot of the key rates renormalized on matching bases and clicks in the middle time slot for different values of κ in the case of a lossless channel. In particular, observe that as κ increases, the key rate, renormalized to clicks in the middle

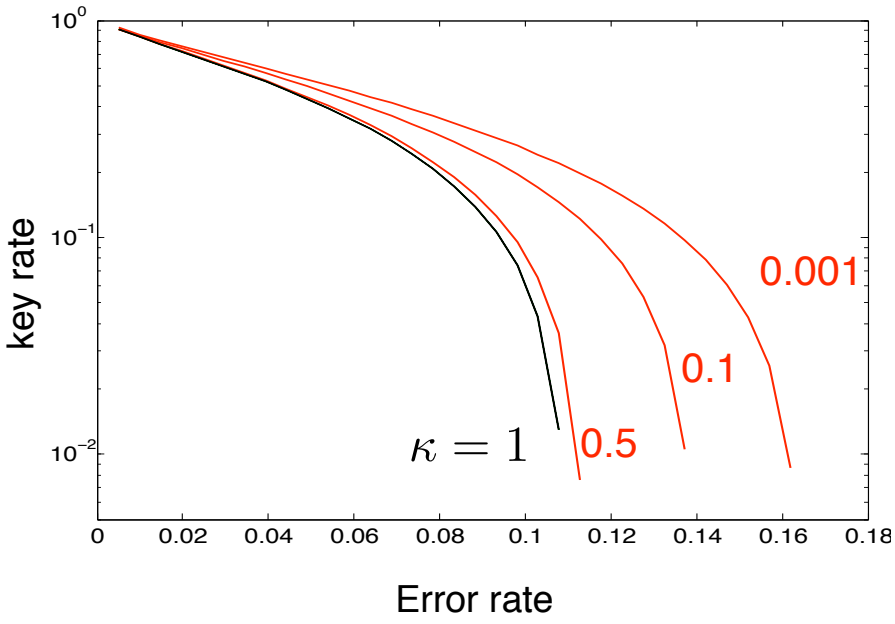


Figure 6.7: Key rates per postselected signal in the middle time slot for unbalanced phase-encoded protocol in dependence on the error rate Q for different values of κ in the phase modulator. The case $\kappa = 1$ corresponds to the lossless phase modulator. Decreasing values of κ mean more loss in the phase modulator.

slot, increases as well. This behaviour originates from the signal state structure: as the signals become more non-orthogonal with increasing κ, the eavesdropper has more difficulty in distinguishing them. In the limit of $\kappa \to 0$, we find a tolerable error rate of about 22% through numerical optimization. In a simple intercept-resend attack, where Eve does the same measurement as Bob and resends the states based on her measurement outcomes, an error rate of $Q_{\mathrm{intercept-resend}} = \frac{1}{4} + \frac{1}{4}p_{\mathrm{out}}$ is expected, where p_{out} is the probability to find an outside click corresponding to Bob's POVM F_B^{out}. In the limit of $\kappa \to 0$, p_{out} tends to 1, and thus the error rate associated to the intercept-resend attack goes to $\frac{1}{2}$.

The advantage of the high asymmetry in the signal states in terms of error rate disappears quickly, once loss is added to the channel. For a fair comparison of the performances of the different protocols, we must specify an error model for an optical channel, and compare the protocols in dependence of channel parameters, such as the distance between Alice and Bob.

6.6 Security proof for realistic devices

The qubit security proof is tailored to the situation where Alice and Bob use perfect qubits (e.g. single photons). The actual experimental implementations, however, are performed with optical modes in an infinite-dimensional Hilbert space. In particular, Alice's device can send vacuum and multi-photon states into the channel, and Bob's detector can receive vacuum and multi-photon states from the channel. In order to achieve a complete security proof, we need to include the deviation from the ideal qubit-to-qubit scenario.

Recently, several powerful tools in Refs. [62, 41, 51, 5, 92, 71] have been developed to bridge the gap between theory and experiment, with the aim to extend the validity of qubit-based security proofs to the more realistic scenario of optical modes. On Alice's side, the multi-photon components are taken care of by using decoy states [62], supported by tagging [41, 51]. This essentially permits us to estimate the fraction of the single photon contributions in the data. On the other hand, the multi-photon states entering Bob's detector are taken care of by the squashing method in Refs. [5, 92, 71]. If a squashing map exists for a certain measurement setup, then the detection pattern resulting from an arbitrary input state into Bob's detector can be interpreted as if it were coming from a single photon or a vacuum input. These tools require that the states leaving Alice's lab and entering Bob's lab are diagonal in the Fock basis. On the source side, this assumption is justified, because Alice prepares a phase-randomized laser pulse, which was shown to be Fock-diagonal in the Eq. (2.35). On the receiver's side, the assumption is justified because the POVM elements of Bob's threshold detectors are Block diagonal in the Fock basis. Therefore, for any state ρ_B entering Bob's detector generates the same detection pattern as the corresponding Fock-diagonal state $\rho_B^{\text{Fock}-\text{diag}}$.

Note that the security proof approach presented here for the UPE protocol gives a provable secure key rate. However, higher key rates may be achievable with a refined analysis. The starting point for the refined analysis is the observation that, in contrast to the general squashing and tagging assumption, a photon number splitting attack on multi-photon signals in the case of the UPE protocol does not leak the information in the signal states with certainty to Eve, even after the basis announcement. However, such an analysis will be more involved. It is expected that for strong asymmetries in the signal states a similar performance could be expected as the strong reference pulse schemes analyzed in [55, 90].

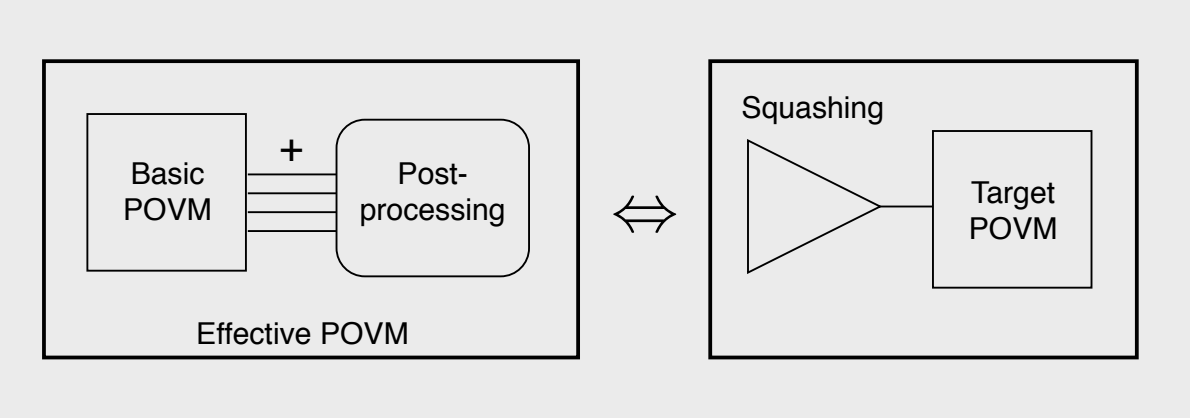


Figure 6.8: The basic POVM combined with classical post-processing forms the effective POVM, which is mapped to the target (qubit) POVM by the squashing map.

6.6.1 Security proof for UPE protocol with realistic devices

For the unbalanced phase-encoded detector setup, a valid squashing map has been proven to exist, in Ref. [71]. In the proof it is assumed that Bob's detectors can resolve the three different time slots shown in Fig. 6.1.

A schematic of the squashing idea is shown in Fig. 6.8: a general incoming optical mode can trigger any possible click pattern in the six detection slots. A POVM is associated to this measurement, called the basic POVM. Through classical post-processing, several basic POVM elements are combined to form the effective (single-click) POVM elements. The effective POVM has five elements $\{F_B^{\text{eff},y} : y = 0, ..., 3\}$ and $F_B^{\text{eff,out}}$, which reflects the single-click structure of the real qubit POVM given in Eq. (6.5). The function of the squashing map is to map the effective POVM to the real POVM. If such a squashing map exists, we can assume that all detection events on Bob's side are single-photon events, whereas Alice's source can either send a vacuum signal (v), a single photon (s) or multiple photons (m).

In the error correction step, Alice and Bob must correct all errors in their data. Therefore, the error correction term, which is the mutual information, depends on the total observed error rate Q_{tot}: $\bar{I}_{\text{obs}} = 1 - h(Q_{\text{tot}})$. Due to the decoy states and the tagging method, however, the privacy amplification term, which is the Holevo quantity, splits into the individual contributions from vacuum, single-photon and multi-photon signals ($\bar{\chi}_v$, $\bar{\chi}_s$ and $\bar{\chi}_m$). Let us define by $p_{\text{mid}}(a)$ the frequency with which the signal $a \in \{v, s, m\}$ sent

by Alice produces a click in a middle time slot in Bob's detector, and the total frequency of a middle click by $p_{\text{mid}} = \sum_{a\in\{v,s,m\}} p_{\text{mid}}(a)$. Then the total key rate is given by

$$R = \frac{1}{2}\left(p_{\text{mid}}\bar{I}_{\text{obs}} - \sum_{a\in\{v,s,m\}} p_{\text{mid}}(a)\ \bar{\chi}_a \right). \tag{6.41}$$

A factor 1/2 was introduced for the sifting.

Typically, we assume that Eve has full knowledge about the vacuum and the multi-photon signals (tagging), therefore $\bar{\chi}_v = \bar{\chi}_m = 1$. Only the term $\bar{\chi}_s$ enters the optimization. Due to the decoy and tagging methods, Alice and Bob have an estimate of the error rate within the single photon events (q). The error rate q is the quantity appearing in the optimization and is generally different from Q_{tot}.

When we are no longer dealing with the strict qubit-to-qubit scenario, we must make some modifications to the constraint on ρ_A in order to adapt to the realistic scenario. We can no longer use the full information ρ_A in Eq. (6.3) to constrain the reduced density matrix $\text{tr}_B(\bar{\rho}_{AB})$ in Eq. (6.39). Recall that the fixed reduced density matrix ρ_A describes the reduced density matrix of all single-photon states exiting the source. These photons are each lost in the channel with probability p_{lost}, and arrive in Bob's detector with probability $1 - p_{\text{lost}}$. The reduced density operator ρ_A is conserved in this process

$$\rho_A = (1 - p_{\text{lost}})\,\text{tr}_B(\bar{\rho}_{AB}) + p_{\text{lost}}\rho_A^{\text{lost}}. \tag{6.42}$$

In this equation, ρ_A^{lost} is an unknown density operator corresponding to the lost photons. We use this weaker version to constrain $\text{tr}_B(\bar{\rho}_{AB})$ in the optimization of the Holevo quantity $\bar{\chi}_s$.

We optimize the Holevo quantity $\bar{\chi}_s$ over the set of symmetric states $\bar{\rho}_{AB}$ (Eq. (6.38)) with the error rate constrain q and the relaxed constraint in Eq. (6.42) on the reduced density matrix. The dependence of the optimized Holevo quantity on q, p_{lost} and κ is denoted in square brackets $\bar{\chi}_s^{\max}[q, p_{\text{lost}}, \kappa]$. The total optimized key rate for the unbalanced phase-encoded protocol is then given by

$$R = \frac{1}{2}\Big(- p_{\text{mid}}h(Q_{\text{tot}}) + p_{\text{mid}}(s)(1 - \bar{\chi}_s^{\max}[q, p_{\text{lost}}, \kappa])\Big). \tag{6.43}$$

In Figs. 6.9 and 6.10 we plot the key rates of the unbalanced phase-encoded protocol and the hardware fixes for different values of κ. We simulate Bob's observations using the experimental values in Ref. [40] for channel loss, dark counts, detector efficiency, alignment

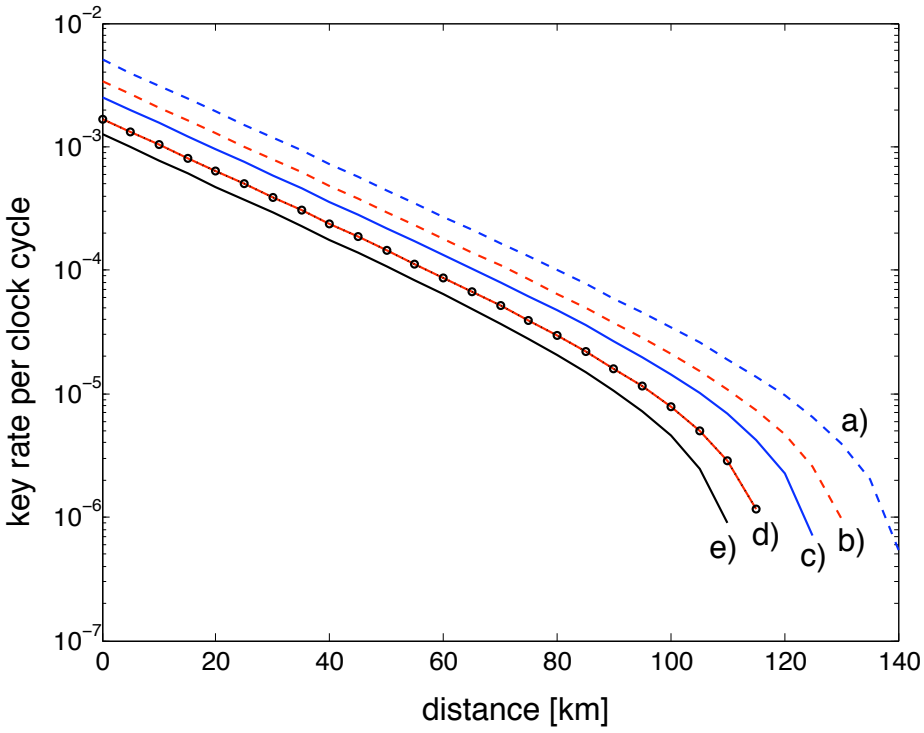


Figure 6.9: Plot of the key rates in the realistic scenario. a) Key rate of the PBS protocol with no loss (dashed blue line). b) Key rate of the PBS protocol with $\kappa = 0.5$ (dashed red line). c) Key rate of the unbalanced phase-encoded protocol with no loss ($\kappa = 1$) (solid blue line). d) Key rate of the unbalanced phase-encoded protocol with $\kappa = 0.5$ (solid red line) coinciding with the key rate of the hardware fix with an uneven beamsplitter (black circles). e) Key rate of the hardware fix with additional loss in the short arm (black line).

error and error correction efficiency. We assume that the detector efficiency is symmetric in the two detectors, so that we can equivalently treat this efficiency as an overall loss in the channel. Furthermore, we assume that no double clicks were observed. We also optimize over the mean photon number of the signal pulses leaving Alice's device.

We compare the performance of different UPE protocols depending on the value of κ to each other: generally, we see that the smaller κ, the more the key rate decreases. Furthermore, for any κ, the performance of the UPE protocol coincides with the performance of the corresponding hardware fix with an uneven beamsplitter, providing a choice between the hardware fix (requiring a special unsymmetrical beam splitter), and the improved security proof analysis presented here. Both of these scenarios, however, outperform the

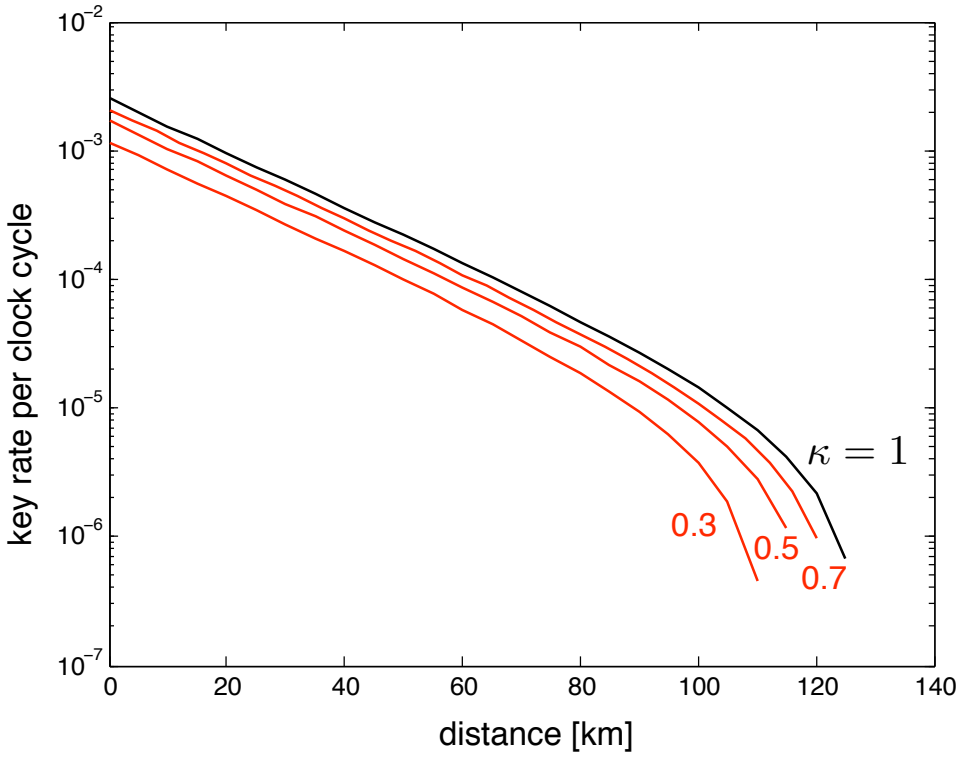


Figure 6.10: Plot of the key rates of the unbalanced phase-encoded protocol for different values of κ.

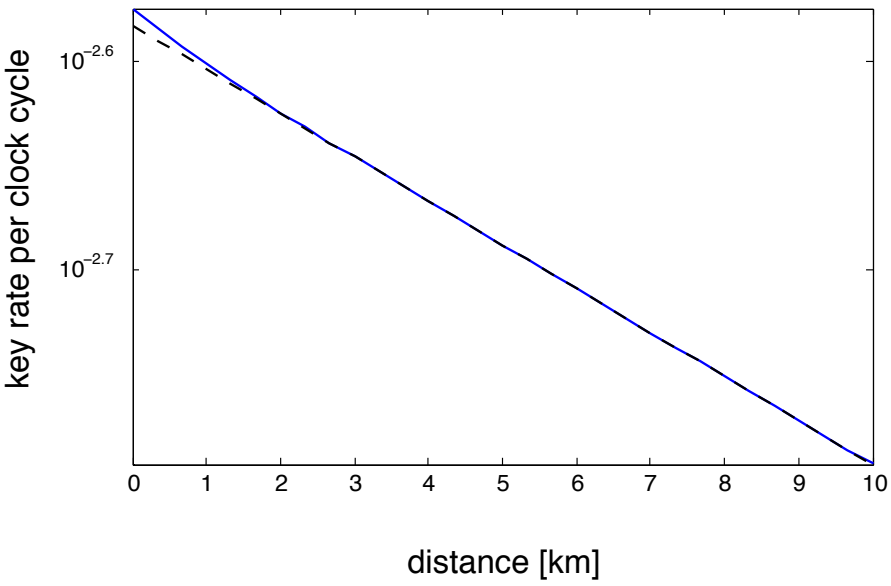


Figure 6.11: Comparison of different security proof methods: the key rate obtained using our improved security proof analysis (solid line) and the key rate obtained using the BB84 security analysis (dashed line) for the same protocol with $\kappa = 0.1$, perfect detection efficiency, and a high alignment error $e_{\text{align}} = 6\%$. In the range of low channel loss (up to a distance of approximately 2 km), the improved security analysis for the UPE protocol gives higher key rates than the BB84 security analysis.

second hardware fix with an additional loss in the short arm.

We also compare different security proof methods: we applied our improved security proof analysis and the BB84 security analysis to the same simulated observations for the UPE protocol for a fixed κ, and compared the resulting key rates. It turns out that both approaches yield the same key rate for the typical range of observations. However, if the error rate is high, the channel loss is low and κ is small enough, then our improved security proof analysis yields a higher key rate than the BB84 analysis. In Fig. 6.11 we compare the key rates using our improved security proof analysis and the BB84 security analysis for a protocol with $\kappa = 0.1$, perfect detection efficiency, and a high alignment error ($e_{\text{align}} = 6\%$ defined like in Ref. [40]). In the range where the loss is low (approximately up to a distance of 2 km), our security analysis gives a higher key rate than the BB84 analysis.

6.6.2 Security proof for PBS protocol with realistic devices

For the PBS protocol detector setup the squashing map is shown to exist in Refs. [5, 92]. Since all pulses interfere, we can drop the specification on middle clicks in the key rate. We call the frequency with which Alice sent a single photon and Bob detected it by $p_{\text{det}}(s)$ and the total detection frequency $p_{\text{det}} = \sum_{a\in\{v,s,m\}} p_{\text{det}}(a)$. The key rate in the PBS scenario is then

$$R = \frac{1}{2}\Big(- p_{\text{det}} h(Q_{\text{tot}}) + p_{\text{det}}(s)(1 - \bar{\chi}_s^{\max}[q, p_{\text{lost}}, \kappa])\Big). \tag{6.44}$$

We plot the key rates of the PBS protocol in Fig. 6.9 for different values of κ. The key rates of the PBS protocol are higher than the key rates of the UPE protocol for the same loss in the phase modulator, because no signal is lost due to outside clicks. Nevertheless, the loss in the phase modulator decreases the key rates of the PBS protocol compared to a protocol without loss.

6.7 Conclusion

We analyzed the security of the phase-encoded BB84 protocol with a lossy phase modulator in one arm of the Mach-Zehnder interferometer. We consider two protocols, the UPE and the PBS protocol. We provide a qubit-based security proof, which we embed in the more general framework of optical modes using the decoy states method, tagging and squashing.

In general, it turns out that the proven secure key rates are lowered by the unbalanced loss in the Mach-Zehnder interferometer compared to a protocol without loss in the phase modulator. The standard BB84 security analysis provides the same result as our refined analysis for the typical range of observations. For hight error rate and low channel loss, though, our refined security analysis outperforms the BB84 analysis in terms of key rate.

The implementation with additional polarization encoding of the pulses (PBS protocol) performs better than the one with no additional polarization encoding (unbalanced phase-encoded protocol), because all signals forcedly interfere in Bob's interferometer. A comparison of the key rates of the unbalanced phase-encoded protocol to the key rates of the two suggested hardware fixes shows that an experimental remedy is not necessary and does not contribute to an improvement of the key rate.

Chapter 7

Measurement-device-independent QKD

7.1 Introduction

The security proofs for QKD protocols guarantee unconditional security. This statement is based on idealized models of the devices used in experiments. The actual experimental implementations often diverge from the models under which the security proofs hold. This leaves an open window (loophole) for the eavesdropper to launch an attack on the components not covered by the theoretical security proof. A particular weak spot in this respect are detector imperfections. Attacks have been demonstrated exploiting detector loopholes for example in Ref. [65].

Since a full characterization of all devices is hardly realizable, one needs to invent other methods to guarantee security. One solution is to use *device-independent* QKD (DI-QKD) security proofs proposed in Refs. [69, 1]. The idea of DI-QKD is to prove security based on violations of Bell-type inequalities. As a consequence, the security proof is independent of the internal workings of the devices. However, there are also loopholes for Bell tests themselves, for example photon loss. Therefore, DI-QKD security proofs based on Bell-type inequalities are rather demanding on the experimental implementation, and therefore, a rather impractical attempt to apply to realistic QKD implementations.

Recently, a variation of a DI-QKD has been proposed in Refs. [61, 14], where only the measurement apparatus is device-independent. In a *measurement-device independent* (MDI) setup, the two honest parties (Alice and Bob) are both senders of quantum signals,

while an intermediate node acts as the receiver of the signals, and performs a measurement [50]. The intermediate node is typically not trusted, and can even be controlled by the eavesdropper Eve. For each signal sent by Alice and Bob the intermediate node makes a measurement and announces a classical message to the honest parties. Based on that message, Alice and Bob are able to effectively generate correlated data. An experimental implementation of this setup has recently been realized in Ref. [83].

MDI-QKD is immune against all detector loopholes, because all assumptions about the workings of the detectors can be dropped. In a way, all detector imperfections are outsourced to Eve and included in the description of her attack. The only assumption are on Alice and Bob's signal preparation.

In this chapter we provide a security proof for an MDI-QKD setup based on the Devetak-Winter security proof [31, 57]. We do this on the example of an MDI setup with B92 signal states (MDI-B92). Using the symmetry techniques of Chapter 4, we establish that the optimal attack for MDI-B92 is symmetric, and calculate the key rate numerically for a realistic channel model. We also analyze two special attacks, the minimum error discrimination (MED) attack, and the unambiguous state discrimination (USD) attack on the MDI-B92 protocol. In case of the MED attack, no secret key can be established, because the MED attack always results in a separable state between Alice and Bob. Furthermore, we apply the MDI-B92 security proof to prove the security of the B92 protocol using a strong reference pulse [9].

7.2 Measurement-device-independent B92 protocol

In this section, we describe a protocol with B92 signal states in an MDI setup (MDI-B92).

In the original B92 protocol [9] Alice chooses one of two nonorthogonal quantum states with *a priori* probability $\frac{1}{2}$. The two states encode the bits 0 and 1, respectively. in the original B92 protocol, the nonorthogonal states are encoded into two weak coherent states $|\pm\alpha\rangle$ for $\alpha \in \mathbb{R}$, which are accompanied by a strong reference pulse. Another possibility is to encode the states into a polarisation degee of freedom [90, 89]. The B92 protocol follows the traditional steps of a QKD protocol, with a quantum phase and a classical phase.

In the MDI-B92 protocol, both Alice and Bob are senders of quantum states, and an intermediate node acts as the receiver and performs the measurements [see Fig. 7.1]. Alice and Bob send the states $|\pm\alpha\rangle$ to the node. If the implementation is done with coherent states, we assume that the node has a common phase reference with Alice and with Bob.

This can be achieved, for example, if the signal states coming from Alice and bob are accompanied by a strong reference pulse.

We now give the detailed steps of the MDI-B92 setup. In particular, the quantum phase of the MDI-B92 protocol differs from the quantum phase of a traditional QKD protocol.

Quantum phase:

1. *Preparation.* Alice chooses a coherent state with equal probability from the set $S_A = \{|\alpha\rangle, |-\alpha\rangle\}$ on the Hilbert space $\mathcal{H}_{A'}$, and Bob from the set $S_B = \{|\beta\rangle, |-\beta\rangle\}$ on the Hilbert space $\mathcal{H}_{B'}$. The signal state with the positive (negative) phase corresponds to a bit value 0 (1). Alice and Bob send their chosen signal state through the quantum channels l_A and l_B that connect them to an intermediate node. They choose the timing such that the signals arrive at the same time at the node. They also calibrate the amplitudes of their coherent states (α and β) so that the states, after travelling through the channels of length l_A or l_B, have the same amplitude (α') when arriving at the node. As already mentioned above, the coherent states are accompanied by a strong reference pulse, from which the node can determine a common reference system with Alice and Bob, and the phase difference between the reference systems.

2. *Joint quantum operation by the node.* Upon arrival of a pair of signals, the intermediate node performs a joint quantum operation. The goal of the quantum operation is to distinguish whether Alice and Bob sent a correlated pair of states ($|\alpha, \beta\rangle$ or $|-\alpha, -\beta\rangle$) or an anti-correlated pair of states ($|\alpha, -\beta\rangle$ or $|-\alpha, \beta\rangle$). It is also possible that the quantum operation has an inconclusive outcome. the joint quantum operation is for exampel, a joint measurement of the signal states. In order to achieve this joint measurement, the node uses the knowledge of the phase difference between the reference systems. A classical feedforward of the phase difference allows the node to align Alice and Bob's reference systems, and then perform the joint measurement.

3. *Announcement by the node.* For each signal, the outcome (γ) of the quantum operation is broadcast to all parties. If the node detected a correlated pair of states, it announces $\gamma =$ " $+$ "; if it detected an anti-correlated pair it announces $\gamma =$ " $-$ ", and when the outcome was inconclusive, the node announces $\gamma =$ "?". This divides the data collected by Alice and Bob into subsets indexed by γ. The probability that the outcome γ is announced is $p(\gamma)$.

4. *Postprocessing.* Based on the announcement, Alice and Bob do the following postprocessing of their data:

   - $\gamma =$ " $+$ ": Alice and Bob do nothing to their data bits.

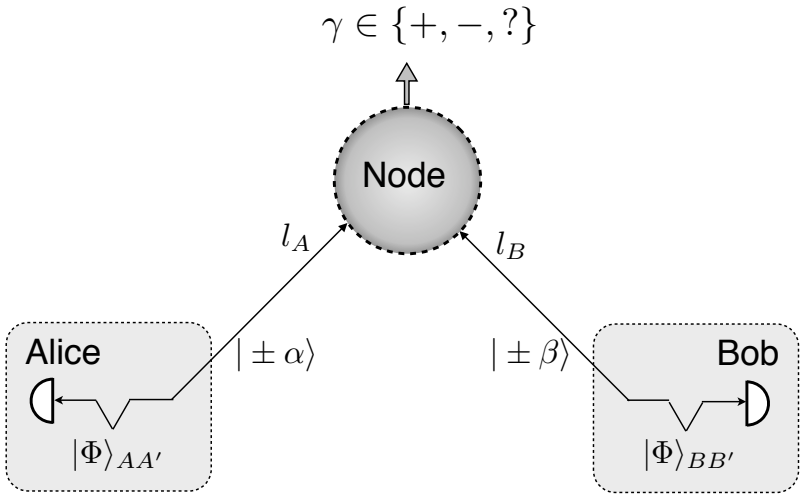


Figure 7.1: MDI-B92 setup in the two-party source-replacement scheme.

- $\gamma =$ " $-$ ": Bob performs a bit flip to his bit value.
- $\gamma =$ "?": Alice and Bob discard the data point.

The classical phase of the MDI-B92 protocol remains the same: Alice and Bob perform error correction and privacy amplification on their data sets $\gamma =$ " $\pm$ " independently, in order to extract a secret key. We choose here to calculate the key for a direct reconciliation protocol, but reverse reconciliation would yield the same results.

7.3 Two special attacks on MDI-B92 protocol

In the following we investigate two special eavesdropping attacks on the MDI-B92 protocol, which have analytical solutions. These special cases give limits to the performance of the protocol, but they are only valid if Alice and Bob observe particular values in their collected data.

In order to prove the security, we assume that Eve is in control of the node and both channels l_A and l_B. We assume that Eve implements the quantum operation in the node and is responsible for making the announcement γ. Effectively, Eve must distinguish

between the correlated and the anti-correlated joint states

$$\rho_+ = \frac{1}{2}(|\alpha,\beta\rangle\langle\alpha,\beta| + |-\alpha,-\beta\rangle\langle-\alpha,-\beta|) \tag{7.1}$$

$$\rho_- = \frac{1}{2}(|\alpha,-\beta\rangle\langle\alpha,-\beta| + |-\alpha,\beta\rangle\langle-\alpha,\beta|). \tag{7.2}$$

7.3.1 Minimum error discrimination attack

For the first special case, assume Alice and Bob observe the following values:

Observed values: There are no inconclusive announcements, namely, $p(\text{“?”}) = 0$.

If Alice and Bob make this observation, Eve must have made a conclusive announcement $\gamma = \text{“}\pm\text{”}$ for each signal. However, it is not possible to distinguish the two states ρ_+ and ρ_- without errors, because these two states are not orthogonal. Therefore, Eve will sometimes make a wrong announcement, e.g. she will announce “+” (“-”) when the state was actually ρ_- (ρ_+). The strategy with the lowest amount of wrong announcements is the *minimum error discrimination* strategy. The minimum error caused by this strategy is [45]

$$Q_{\min} = \frac{1}{2}\left(1 - |\frac{1}{2}(\rho_- - \rho_+)|_1\right). \tag{7.3}$$

Let us first look at the signal states before calculating $Q_{\min}$. Although the states $|\pm\alpha\rangle$ are in principle defined on the infinite-dimensional Fock space, they actually span a 2-dimensional subspace. We define the canonical basis of this space by $\{|\phi_A^0\rangle, |\phi_A^1\rangle\}$, and parametrize the signal states in this basis:

$$|\pm\alpha\rangle = c_0|\phi_A^0\rangle \pm c_1|\phi_A^1\rangle. \tag{7.4}$$

The coefficients c_0 and c_1 follow the normalization condition $|c_0|^2+|c_1|^2$, and are determined from the overlap condition $\langle\alpha|-\alpha\rangle = |c_0|^2 - |c_1|^2$:

$$|c_0|^2 = \frac{1}{2}(1 + \langle\alpha|-\alpha\rangle) \tag{7.5}$$

$$|c_1|^2 = \frac{1}{2}(1 - \langle\alpha|-\alpha\rangle) \tag{7.6}$$

Similar formula hold for Bob's signal states $|\pm\beta\rangle$.

For the calculation of the term $|\frac{1}{2}(\rho_- - \rho_+)|$ we expand ρ_+ and ρ_- in the canonical basis of the tensor product space $\{|\phi_A^0,\phi_B^0\rangle, |\phi_A^0,\phi_B^1\rangle, |\phi_A^1,\phi_B^0\rangle, |\phi_A^1,\phi_B^1\rangle\}$. In this parametrization,

the density matrices of ρ_+ and ρ_- are represented by 4-by-4 matrices, for which the trace norm is straightforward to calculate. The minimum error to distinguish the state ρ_+ from ρ_- is

$$Q_{\min}^{\text{joint}} = \frac{1}{2}\left(1 - \sqrt{1 - \langle\alpha| - \alpha\rangle^2}\sqrt{1 - \langle\beta| - \beta\rangle^2}\right). \tag{7.7}$$

We show now that the joint MED strategy is effectively equivalent to a separable strategy, where Eve does a MED on Alice's and Bob's link l_A and l_B independently, and combines the outcomes classically. The minimum error made in discriminating between $|\alpha\rangle$ and $|-\alpha\rangle$ on the link l_A is $Q_{\min}^A = \frac{1}{2}\left(1 - \sqrt{1 - \langle\alpha| - \alpha\rangle^2}\right)$ (a similar expression holds for $|\pm\beta\rangle$). Having discriminated the states in each link separately, the error made to discriminate the correlated and anti-correlated states is

$$Q_{\min}^{\text{sep}} = (1 - Q_{\min}^A)Q_{\min}^B + (1 - Q_{\min}^B)Q_{\min}^A \equiv Q_{\min}^{\text{joint}}. \tag{7.8}$$

Therefore, the data resulting from the joint MED strategy can be equivalently described as resulting from a separable MED strategy. The separable MED strategy is an intercept-resend strategy [29] on each link, which can be described by an entanglement breaking channel (see Ref. [47]). It was shown in Ref. [28] that no secret key can be generated over an entanglement breaking channel. In fact, any attack where Eve is forced to make an announcement for every signal will ultimately result in a separable attack, because there is no quantum operation that would introduce less error than the joint MED.

7.3.2 Unambiguous state discrimination attack

For the second special case, we make the following assumption on the observations:

Observed values: There are no errors in Alice and Bob's data, but there are inconclusive announcements, $p(\text{“?”}) > 0$.

These observations imply that Eve is allowed to make inconclusive announcements, but she must distinguish the joint states at the source, ρ_+ and ρ_-, with certainty, and never output a wrong announcement. This type of strategy is an *unambiguous state discrimination* (USD) between ρ_+ and ρ_- with the possibility to output $\gamma =$ “?” whenever the discrimination failed.

A USD is a measurement that is described by three POVM elements $\{F_{\text{USD}}^+, F_{\text{USD}}^-, F_{\text{USD}}^?\}$ corresponding to the three possible outcomes. The POVM elements satisfy $\text{tr}\{\rho_+ F_{\text{USD}}^-\} =$

$\mathrm{tr}\{\rho_- F^+_{\mathrm{USD}}\} = 0$. If the USD is also optimal, the failure probability $p(\text{“?”})$ corresponding to $F^?_{\mathrm{USD}}$ is minimal.

Theorem 2 in Ref. [75] provides at method to calculate the POVM elements of a measurement that implements the optimal joint USD. We calculate the POVM elements $F^\pm_{\mathrm{USD}}$ and $F^?_{\mathrm{USD}}$ for the symmetric case $\alpha = \beta$. By defining $k = c_1^2/c_0^2$ as the ratio between the coefficients in Eq. (7.4), the POVM elements in the canonical basis of the tensor product space are given by

$$F^\pm_{\mathrm{USD}} = \frac{1}{2}\begin{pmatrix} |k|^2 & 0 & 0 & \pm k^* \\ 0 & 1 & \pm 1 & 0 \\ 0 & \pm 1 & 1 & 0 \\ \pm k & 0 & 0 & 1 \end{pmatrix}, \quad F^?_{\mathrm{USD}} = \begin{pmatrix} 1-|k|^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{7.9}$$

The minimum failure probability $p(\text{“?”})$ of the optimal joint USD attack is

$$p(\text{“?”})_{\mathrm{joint}} = \frac{1}{2}\left(\mathrm{tr}\{F^?_{\mathrm{USD}}\rho_+\} + \mathrm{tr}\{F^?_{\mathrm{USD}}\rho_-\}\right) = |\langle\alpha| - \alpha\rangle|. \tag{7.10}$$

From the POVM elements, we deduce the Kraus operators $K^\gamma_{\mathrm{USD}} = \sqrt{F^\gamma_{\mathrm{USD}}}$ of the optimal joint USD

$$K^\pm_{\mathrm{USD}} = \frac{1}{2}\begin{pmatrix} \frac{\sqrt{2}|k|^2}{\sqrt{|k|^2+1}} & 0 & 0 & \pm\frac{\sqrt{2}k^*}{\sqrt{|k|^2+1}} \\ 0 & 1 & \pm 1 & 0 \\ 0 & \pm 1 & 1 & 0 \\ \pm\frac{\sqrt{2}k}{\sqrt{|k|^2+1}} & 0 & 0 & \frac{\sqrt{2}}{\sqrt{|k|^2+1}} \end{pmatrix}, \quad K^?_{\mathrm{USD}} = \begin{pmatrix} \sqrt{1-|k|^2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{7.11}$$

The Kraus operators allow us to calculate Eve's states $|\psi^\gamma_i\rangle_E$ conditioned on Alice's bit value $i = 0, 1$, and Eve's total state $\rho^\gamma_E = \frac{1}{2}(|\psi^\gamma_0\rangle\langle\psi^\gamma_0| + |\psi^\gamma_1\rangle\langle\psi^\gamma_1|)$. Using these states and that the von Neumann entropy of pure states is zero, we compute Eve's information $\chi(X:E)^\pm$ about Alice's bit values for $\gamma = \text{“}\pm\text{”}$,

$$\chi(X:E)^\pm = S(\rho^\pm_E) - \sum_i p(i) S(|\psi^\pm_0\rangle\langle\psi^\pm_0|) = S(\rho^\pm_E) = h\left(\frac{1 + \langle\alpha| - \alpha\rangle}{2}\right). \tag{7.12}$$

The function h denotes the binary entropy function. Since Alice and Bob observe no errors, they do not need to perform error correction. Therefore, the key rate under the optimal joint USD attack is

$$r_{\mathrm{USD}} = 1 - \frac{1}{2}\Big(\chi(X:E)^+ + \chi(X:E)^-\Big) = 1 - h\left(\frac{1 + \langle\alpha| - \alpha\rangle}{2}\right). \tag{7.13}$$

7.3.3 Implementation of the optimal joint USD

The measurement that implements the optimal joint USD between ρ_+ and ρ_- for the symmetric case $\alpha = \beta$ is shown in Fig. 7.2. The joint state arriving at the node is one of the four product states $|\alpha, \alpha\rangle_{AB}$, $|\alpha, -\alpha\rangle_{AB}$, $|-\alpha, \alpha\rangle_{AB}$ or $|-\alpha, -\alpha\rangle_{AB}$ with probability $\frac{1}{4}$. After arriving at the node, the joint state enters the input ports A and B of a balanced beamsplitter, and exits from the output ports "$+$" and "$-$". The relation between input and output state is

$$\begin{aligned} |\alpha, \alpha\rangle_{AB} &\rightarrow |\sqrt{2}\alpha, \text{vac}\rangle_{+-}, \\ |\alpha, -\alpha\rangle_{AB} &\rightarrow |\text{vac}, \sqrt{2}\alpha\rangle_{+-}, \\ |-\alpha, \alpha\rangle_{AB} &\rightarrow |\text{vac}, -\sqrt{2}\alpha\rangle_{+-}, \\ |-\alpha, -\alpha\rangle_{AB} &\rightarrow |-\sqrt{2}\alpha, \text{vac}\rangle_{+-}. \end{aligned} \tag{7.14}$$

The output states are then measured using the threshold detectors D_+ and D_-. These detectors are "click/no click" detectors, which means they don't fire ("no click") in the absence of a photon, and they fire (they produce a "click") whenever one or more photons hit the detector. The POVM elements of this measurement in the Fock basis are projections onto the vacuum $F_{\text{vac}} = |\text{vac}\rangle\langle\text{vac}|$ and onto the remaining orthogonal space $F_{\text{click}} = \mathbb{1} - |\text{vac}\rangle\langle\text{vac}|$.

The measurement outcomes of the threshold detectors is summarized in table 7.1: if the detector D_+ fires, the pair of states were correlated, and the node announces $\gamma =$ "+"; if the detector D_- fires, the states were anti-correlated and the node announces $\gamma =$ "$-$"; with probability $p(\text{"?"}) = \langle\alpha| - \alpha\rangle = e^{-2|\alpha|^2}$ none of the detectors fire, which is an inconclusive announcement and the node announces $\gamma =$ "?".

7.4 Security proof of the MDI-B92 protocol

Typically, both errors and inconclusive announcements are part of the observations, so the two special cases described in the previous section do not apply. We provide a security proof for general measurements for the MDI-B92 protocol in the present section.

7.4.1 Two-party source-replacement scheme

The preparation of the signal states of Alice and Bob is cast in a source-replacement scheme on each side, which we will refer to as the *two-party source-replacement*. The source states

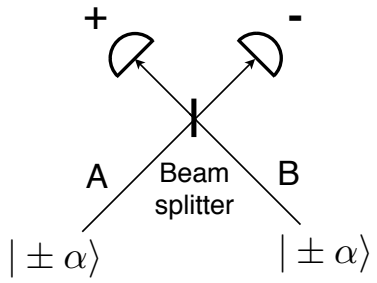


Figure 7.2: Implementation of the optimal joint USD between correlated and anti-correlated states ρ_+ and ρ_- for the symmetric case $\alpha = \beta$. The input states on the systems A and B are combined at a balanced beamsplitter. The output states on the systems $+$ and $-$ are measured by threshold detectors. If the detector in the output port $+/-$ fires, the input state was $\rho_{+/-}$ and the result of the USD is $\gamma =$ "$+/-$". If none of the detectors fires, the outcome is inconclusive, $\gamma =$ "?".

Table 7.1: The measurement outcomes of the optimal joint unambiguous state discrimination between the states ρ_+ and ρ_-.

	$p(+)$	$p(-)$	$p(?)$
$\|\alpha,\alpha\rangle$	$1-e^{-2\|\alpha\|^2}$	0	$e^{-2\|\alpha\|^2}$
$\|\alpha,-\alpha\rangle$	0	$1-e^{-2\|\alpha\|^2}$	$e^{-2\|\alpha\|^2}$
$\|-\alpha,\alpha\rangle$	0	$1-e^{-2\|\alpha\|^2}$	$e^{-2\|\alpha\|^2}$
$\|-\alpha,-\alpha\rangle$	$1-e^{-2\|\alpha\|^2}$	0	$e^{-2\|\alpha\|^2}$

in the two-party source-replacement scheme are the entangled states

$$|\Phi\rangle_{AA'} = \frac{1}{\sqrt{2}}(|0\rangle|\alpha\rangle + |1\rangle|-\alpha\rangle), \tag{7.15}$$

$$|\Phi\rangle_{BB'} = \frac{1}{\sqrt{2}}(|0\rangle|\beta\rangle + |1\rangle|-\beta\rangle), \tag{7.16}$$

respectively. The systems A and B are 2-dimensional qubit spaces with a canonical basis $\{|0\rangle, |1\rangle\}$. The systems A' and B' carry the signal states. The two-party source-replacement scheme is shown in Fig. 7.1.

Alice and Bob send the systems A' and B' of the source states to the node. The node then performs the joint quantum operation and the announcement γ, which effectively creates entanglement between Alice and Bob, and is commonly referred to as entanglement swapping. The entanglement between Alice and Bob is formally captured by introducing a bipartite quantum state ρ_{AB}^{γ} on the systems A and B for each announcement γ. The dimensions of the systems A and B depend on the number of signal states. In particular, for the MDI-B92 protocol, the dimension is two. The total state held by Alice and Bob including the classical announcements is described by a convex combination

$$\rho_{ABC} = \sum_{\gamma} p(\gamma)\rho_{AB}^{\gamma} \otimes |\gamma\rangle\langle\gamma|_C. \tag{7.17}$$

where the classical system C holds a description of the announcement γ, and $p(\gamma)$ is the probability that the announcement γ was made by the node. The classical system C is public and accessible to all parties, including Eve.

In the two-party source-replacement scheme the reduced state $\rho_{AB} = \mathrm{tr}_C\, \rho_{ABC}$ is a fixed quantity and equal to the reduced state of the source

$$\rho_{AB} = \mathrm{tr}_{A'B'}\{|\Phi\rangle\langle\Phi|_{AA'} \otimes |\Phi\rangle\langle\Phi|_{BB'}\} = \rho_A \otimes \rho_B. \tag{7.18}$$

In the canonical basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ the density matrix ρ_{AB} is given by

$$\rho_{AB} = \frac{1}{4}\begin{pmatrix} 1 & B_0 & A_0 & A_0B_0 \\ B_0 & 1 & A_0B_0 & A_0 \\ A_0 & A_0B_0 & 1 & B_0 \\ A_0B_0 & A_0 & B_0 & 1 \end{pmatrix} \tag{7.19}$$

and where $A_0 = \langle\alpha| - \alpha\rangle = \exp(-2\alpha^2)$ and $B_0 = \langle\beta| - \beta\rangle = \exp(-2\beta^2)$.

Alice and Bob perform measurements $\mathbf{M}_K = \{F_K^x\}$ for $K \in \{A, B\}$ with POVM elements $F_K^0 = |0\rangle\langle 0|$ and $F_K^1 = |1\rangle\langle 1|$ on the systems A and B, followed by the classical postprocessing of their data.

Instead of specifying the postprocessing on the classical data after the measurement, we can equivalently describe it on the quantum level before the measurement.

Postprocessing on the quantum level:

- If $\gamma =$ " $+$ ", Alice and Bob do nothing to ρ_{AB}^{+}.
- If $\gamma =$ " $-$ ", Bob applies the Pauli operator σ_X (bit flip operator) to his part of ρ_{AB}^{-}, and Alice does nothing.
- If $\gamma =$ "?", Alice and Bob do nothing to $\rho_{AB}^{?}$.

This postprocessing is described by the quantum map

$$\mathcal{V}_\gamma[\rho_{AB}^\gamma] := \mathbb{1} \otimes V_\gamma \, \rho_{AB}^\gamma \, \mathbb{1} \otimes V_\gamma^\dagger := \sigma_{AB}^\gamma. \tag{7.20}$$

where the V_γ are unitary transformations on Bob's system B defined by

$$V_+ = \mathbb{1}_2, \tag{7.21}$$
$$V_- = \sigma_X, \tag{7.22}$$
$$V_? = \mathbb{1}_2. \tag{7.23}$$

Finally, Alice and Bob measure each $\mathcal{V}_\gamma[\rho_{AB}^\gamma]$ with respect to the POVMs $\mathbf{M}_K = \{F_K^x\}$ for $K \in \{A, B\}$. If $\gamma =$ "?", they discard the data point. Otherwise, from the probability distribution of the measurement outcomes $p_\pm(x, y) = \mathrm{tr}\{F_A^x \otimes F_B^y \, V_\pm[\rho_{AB}^\pm]\}$, they determine the average error rate

$$Q_\pm = p_\pm(0, 1) + p_\pm(1, 0) \tag{7.24}$$

in each data subset $\gamma =$ " $\pm$ ". They perform parameter estimation based on the average error rates and a known probability $p($"?"$)$ in order to constrain the form of the density operators ρ_{ABC}. The set of density operators ρ_{ABC} compatible with the observations are defined as follows:

Definition 23 *The set* $\mathbf{\Gamma}$ *contains all density operators* ρ_{ABC}*, which are compatible with*

1. *The density operator* $\rho_{AB} = \rho_A \otimes \rho_B$.

2. *The averaged error rates* $Q_{\pm}$.

3. *The probability* $p(\text{“?”})$.

Eve's control over the node and the channel is described by giving her the power to generate the density operators ρ_{AB}^{γ} at her will, of which she holds the purification $|\Psi^{\gamma}\rangle_{ABE}$. Therefore, each $\rho_{ABC} \in \mathbf{\Gamma}$ corresponds to a possible eavesdropping attack.

Remark: we fix the value of $p(\text{“?”})$ in the parameter estimation, but not the values of $p(\text{“}+\text{”})$ and $p(\text{“}-\text{”})$. This allows us later to prove that the optimal attack has a symmetry with respect to the “ $+$ ” and “ $-$ ” terms.

7.4.2 Key rate optimization problem

We assume that Alice and Bob choose to extract the key from each $\mathcal{V}[\rho_{AB}^{\pm}]$ individually. Consequently, the key rate is given by

$$r = \bar{I}_{\text{obs}} - \max_{\rho_{ABC} \in \mathbf{\Gamma}} \bar{\chi}_{\text{tot}}(\rho_{ABC}), \tag{7.25}$$

where the maximum is taken over the set $\mathbf{\Gamma}$ of states ρ_{ABC} established in the parameter estimation. The mutual information, I_{obs}, depends only on observations, while the total Holevo quantity,

$$\bar{\chi}_{\text{tot}}(\rho_{ABC}) = \sum_{\gamma=\pm} p(\gamma)\ \chi(\mathcal{V}_{\gamma}[\rho_{AB}^{\gamma}], \mathbf{M}_A), \tag{7.26}$$

depends on the choice of ρ_{ABC}.

7.4.3 Symmetric optimal attack for the MDI-B92 protocol

In this technical section we show that the optimal attack on the MDI-B92 protocol lies in a symmetric subset $\bar{\mathbf{\Gamma}}$ of the set $\mathbf{\Gamma}$ using the techniques established in Chapter 4.

The signal states $\mathbf{S}_{A'} = \{|\pm\alpha\rangle_{A'}\}$ and $\mathbf{S}_{B'} = \{|\pm\beta\rangle_{B'}\}$ are invariant under a group G with two group elements

$$U_1 = \mathbb{1}_2, \tag{7.27}$$

$$U_2 = \sigma_X. \tag{7.28}$$

in the basis $\{|\phi^0_{K'}\rangle, |\phi^1_{K'}\rangle\}$ for $K' \in \{A', B'\}$. It is important to note that the group elements are the same as the unitaries V_γ.

First, we define a subset $\bar{\mathbf{\Gamma}}$ of $\mathbf{\Gamma}$, that contains only symmetrized states:

Definition 24 *The set $\bar{\mathbf{\Gamma}}$ contains all symmetrized states*

$$\bar{\rho}_{ABC} = \sum_\gamma p(\gamma) \bar{\rho}^\gamma_{AB} \otimes |\gamma\rangle\langle\gamma|_C, \tag{7.29}$$

which are compatible with the error rates $Q_\pm$, the probability $p(\text{“?”})$ and the reduced state ρ_{AB}. The symmetrized states $\bar{\rho}^\gamma_{AB}$ are defined by

$$\bar{\rho}^\gamma_{AB} = \frac{1}{|G|} \sum_g \mathcal{U}_g[\rho^\gamma_{AB}], \tag{7.30}$$

$$\mathcal{U}_g[\rho^\gamma_{AB}] = (U_g \otimes U_g)\ \rho^\gamma_{AB}\ (U_g^\dagger \otimes U_g^\dagger). \tag{7.31}$$

The unitary transformations $U_g \in \{\mathbb{1}, \sigma_X\}$ are defined in the canonical basis $\{|0\rangle, |1\rangle\}$ of the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. We stick to the general notation $\mathcal{U}_g$ for the transformations, even though our group G only has two elements.

The main result of this section is summarized in the following theorem.

Theorem 13 *For all states ρ_{ABC} in $\mathbf{\Gamma}$, it holds that*

$$\bar{\chi}_{\text{tot}}(\rho_{ABC}) \leq \bar{\chi}_{\text{tot}}(\bar{\rho}_{ABC}), \tag{7.32}$$

where $\bar{\rho}_{ABC}$ is in $\bar{\mathbf{\Gamma}}$. This implies that the optimal attack of the MDI-B92 protocol lies in the subset $\bar{\mathbf{\Gamma}}$ of $\mathbf{\Gamma}$.

We show two lemmas, which together prove the result of Theorem 13.

Lemma 4 *For each ρ_{ABC} in $\mathbf{\Gamma}$, the symmetrically transformed state*

$$\rho^g_{ABC} = \sum_\gamma p(\gamma)\ \mathcal{U}_g[\rho^\gamma_{AB}] \otimes |\gamma\rangle\langle\gamma|_C, \tag{7.33}$$

for all $g \in G$ also lies in $\mathbf{\Gamma}$.

Proof. From the commutator $[U_g \otimes U_g, \mathbb{1} \otimes V_\gamma] = 0$ for all $g \in G$ and $\gamma \in \{+, -, ?\}$ it follows that

$$\mathcal{V}_\gamma[\mathcal{U}_g[\rho_{AB}^\gamma]] = \mathcal{U}_g[\mathcal{V}_\gamma[\rho_{AB}^\gamma]]. \tag{7.34}$$

The POVMs $\mathbf{M}_{A/B} = \{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ are invariant under the unitaries U_g. Let us define the POVM element associated with the error rate by $F_Q = |01\rangle\langle 01| + |10\rangle\langle 10|$. With this notation, the error rates are $Q_\pm = \mathrm{tr}\{F_Q\ \rho_{AB}^\pm\}$. The operator F_Q satisfies the invariance $F_Q = \mathcal{U}_g[F_Q]$ for all $g \in G$. If we calculate the error rates $Q_\pm^g$ of ρ_{ABC}^g, we obtain

$$Q_\pm^g = \mathrm{tr}\{F_Q\, \mathcal{U}_g[\rho_{AB}^\pm]\} = \mathrm{tr}\{\mathcal{U}_g[F_Q]\rho_{AB}^\pm\} = Q_\pm. \tag{7.35}$$

Here we used that $U_g^\dagger = U_g$ for all $g \in G$. Furthermore, the reduced state ρ_{AB} also satisfies the invariance $\rho_{AB} = \mathcal{U}_g[\rho_{AB}]$ for all $g \in G$. From this invariance and the linearity of $\mathcal{U}_g$ it follows that the reduced state ρ_{AB}^g of ρ_{ABC}^g is

$$\rho_{AB}^g = \sum_\gamma p(\gamma)\, \mathcal{U}_g[\rho_{AB}^\gamma] = \mathcal{U}_g[\rho_{AB}] = \rho_{AB}. \tag{7.36}$$

Finally, ρ_{ABC}^g satisfies the constraint on $p(\text{“?”})$ trivially by definition. Therefore, ρ_{ABC}^g satisfies all constraints imposed by the set $\mathbf{\Gamma}$. ■

Now we show that the Holevo quantity $\bar{\chi}_{\mathrm{tot}}$ satisfies the concavity and equivalence property.

Lemma 5 *The Holevo quantity satisfies the concavity and equivalence property*

$$\bar{\chi}_{\mathrm{tot}}(\rho_{ABC}^g) = \bar{\chi}_{\mathrm{tot}}(\rho_{ABC}), \tag{7.37}$$

$$\bar{\chi}_{\mathrm{tot}}(\bar{\rho}_{ABC}) \geq \frac{1}{|G|} \sum_g \bar{\chi}_{\mathrm{tot}}(\rho_{ABC}^g). \tag{7.38}$$

Proof. Using the concavity of χ in Theorem 8 and the definition of $\bar{\rho}_{AB}^\gamma$, we deduce that

$$\chi(\mathcal{V}_\gamma[\bar{\rho}_{AB}^\gamma], \mathbf{M}_A) \geq \frac{1}{|G|} \sum_g \chi\left(\mathcal{V}_\gamma[\mathcal{U}_g[\rho_{AB}^\gamma]], \mathbf{M}_A\right). \tag{7.39}$$

Using this property, it follows that the total Holevo quantity is concave:

$$\bar{\chi}_{\text{tot}}(\bar{\rho}_{ABC}) = \sum_{\gamma=\text{“}\pm\text{”}} p(\gamma)\ \chi(\mathcal{V}_\gamma[\bar{\rho}^\gamma_{AB}], \mathbf{M}_A) \tag{7.40}$$

$$\geq \sum_{\gamma=\text{“}\pm\text{”}} p(\gamma) \left[\frac{1}{|G|} \sum_g \chi\left(\mathcal{V}_\gamma[\mathcal{U}_g[\rho^\gamma_{AB}]], \mathbf{M}_A\right) \right] \tag{7.41}$$

$$= \frac{1}{|G|} \sum_g \bar{\chi}_{\text{tot}}(\rho^g_{ABC}). \tag{7.42}$$

From the invariance property of the Holevo quantity in Lemma 2 and the commutation relation in Eq. (7.34), it follows that

$$\chi(\mathcal{V}_\gamma[\mathcal{U}_g[\rho^\gamma_{AB}]], \mathbf{M}_A) = \chi(\mathcal{V}_\gamma[\rho^\gamma_{AB}], \mathbf{M}_A). \tag{7.43}$$

From this equation, if follows that the Holevo quantity satisfies the equivalence property

$$\bar{\chi}_{\text{tot}}(\rho^g_{ABC}) = \sum_{\gamma=\text{“}\pm\text{”}} p(\gamma)\ \chi(\mathcal{V}_\gamma[\mathcal{U}_g[\rho^\gamma_{AB}]], \mathbf{M}_A) \tag{7.44}$$

$$= \sum_{\gamma=\text{“}\pm\text{”}} p(\gamma)\ \chi(\mathcal{V}_\gamma[\rho^\gamma_{AB}], \mathbf{M}_A) \tag{7.45}$$

$$= \bar{\chi}_{\text{tot}}(\rho_{ABC}). \tag{7.46}$$

■

Form the concavity and equivalence property of $\bar{\chi}_{\text{tot}}$, the result of Theorem 13 follows.

Further symmetrization

We perform a second symmetrization step using again the concavity and equivalence of $\bar{\chi}_{\text{tot}}$ to confine the optimal attack to a set of states with a symmetry in the $\gamma = \text{“}+\text{”}$ and $\gamma = \text{“}-\text{”}$ terms. For this to succeed, we define a superset $\mathbf{\Gamma}_Q$ of $\bar{\mathbf{\Gamma}}$ and optimize $\bar{\chi}_{\text{tot}}$ over the larger set $\mathbf{\Gamma}_Q$. The optimization over the larger set can only decrease the key rate.

Definition 25 *The set $\mathbf{\Gamma}_Q$ contains all symmetrized states $\bar{\rho}_{ABC}$, which are compatible with the average error rate, $Q = \frac{1}{1-p(\text{“?”})}\Big(p(\text{“}+\text{”})Q_+ + p(\text{“}-\text{”})Q_- \Big)$, the probability $p(\text{“?”})$ and the reduced density operator ρ_{AB}.*

For every $\bar{\rho}_{ABC} \in \mathbf{\Gamma}_Q$ we construct a state

$$\bar{\tau}_{ABC} = p(\text{“}-\text{”})\, \bar{\tau}^{+}_{AB} \otimes |+\rangle\langle+|_C + p(\text{“}+\text{”})\, \bar{\tau}^{-}_{AB} \otimes |-\rangle\langle-|_C + p(\text{“?”})\, \bar{\tau}^{?}_{AB} \otimes |?\rangle\langle?|_C,$$

with interchanged roles of $p(\text{“}+\text{”})$ and $p(\text{“}-\text{”})$, and transformed states $\bar{\tau}^{+}_{AB} = \mathcal{V}_-[\bar{\rho}^{-}_{AB}]$, $\bar{\tau}^{-}_{AB} = \mathcal{V}_-[\bar{\rho}^{+}_{AB}]$ and $\bar{\tau}^{?}_{AB} = \mathcal{V}_-[\bar{\rho}^{?}_{AB}]$.

The state $\bar{\tau}_{ABC}$ lies in the set $\mathbf{\Gamma}_Q$, because it is compatible with Q, $p(\text{“?”})$ and the reduced state ρ_{AB}. Furthermore, for states $\bar{\rho}_{ABC}$ and $\bar{\tau}_{ABC}$, the Holevo quantity satisfies the equivalence property

$$\begin{aligned}
\bar{\chi}_{\text{tot}}(\bar{\tau}_{ABC}) &= p(\text{“}-\text{”})\chi(\mathcal{V}_+[\bar{\tau}^{+}_{AB}], \mathbf{M}_A) + p(\text{“}+\text{”})\chi(\mathcal{V}_-[\bar{\tau}^{-}_{AB}], \mathbf{M}_A) && (7.47)\\
&= p(\text{“}-\text{”})\chi(\bar{\rho}^{-}_{AB}, \mathbf{M}_A) + p(\text{“}+\text{”})\chi(\bar{\rho}^{+}_{AB}, \mathbf{M}_A) && (7.48)\\
&= \bar{\chi}_{\text{tot}}(\bar{\rho}_{ABC}). && (7.49)
\end{aligned}$$

Using the concavity of the Holevo quantity in Eq. (7.38) and the just established equivalence, it follows that

$$\bar{\chi}_{\text{tot}}\left(\frac{\bar{\rho}_{ABC} + \bar{\tau}_{ABC}}{2}\right) \geq \bar{\chi}_{\text{tot}}(\bar{\rho}_{ABC}) \tag{7.50}$$

for all $\bar{\rho}_{ABC} \in \mathbf{\Gamma}_Q$. Therefore, the optimal attack $\bar{\rho}^{\text{opt}}_{ABC}$ lies in a subset $\bar{\mathbf{\Gamma}}_Q$ of $\mathbf{\Gamma}_Q$, containing only states of the form $\bar{\sigma}_{ABC} = \frac{\bar{\rho}_{ABC} + \bar{\tau}_{ABC}}{2}$.

The states $\bar{\sigma}_{ABC} \in \bar{\mathbf{\Gamma}}_Q$ have the properties that $p(\text{“}+\text{”}) = p(\text{“}-\text{”}) = \frac{1-p(\text{“?”})}{2}$ are defined in terms the fixed quantity $p(\text{“?”})$, and that there is a symmetry in the “$+$” and “$-$” terms: $\mathcal{V}_+[\bar{\sigma}^{+}_{AB}] = \mathcal{V}_-[\bar{\sigma}^{-}_{AB}]$.

7.4.4 Parametrization of the symmetric optimal attack

The parametrization of the states in $\bar{\mathbf{\Gamma}}_Q$ in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ are given by the density operators

$$\mathcal{V}_+[\bar{\sigma}^{+}_{AB}] = \mathcal{V}_-[\bar{\sigma}^{-}_{AB}] = \begin{pmatrix} x & a & b & c \\ a^* & y & d & b^* \\ b^* & d & y & a^* \\ c & b & a & x \end{pmatrix} \tag{7.51}$$

$$\bar{\sigma}^{?}_{AB} = \begin{pmatrix} x_? & a_? & b_? & c_? \\ a^*_? & y_? & d_? & b^*_? \\ b^*_? & d_? & y_? & a^*_? \\ c_? & b_? & a_? & x_? \end{pmatrix} \tag{7.52}$$

By concavity, the coefficients a and b can be chosen real. Two more parameters are eliminated by imposing the equality constraint Q and the normalization of the trace: $x = \frac{1-Q}{2}$ and $y = \frac{Q}{2}$. Finally, the equality constrain ρ_{AB} eliminates several parameters in $\rho^{?}_{AB}$: $x_? = y_? = \frac{1}{4}$, $d_? = c_?$ and $a_?, b_? \in \mathbb{R}$, while the remaining parameters ($a_?, b_?$ and $c_?$) are expressed in dependence of a, b, c and d:

$$a_? = \frac{1}{p(\text{“?”})}\left(\frac{B_0}{4} - (1 - p(\text{“?”}))a\right) \tag{7.53}$$

$$b_? = \frac{1}{p(\text{“?”})}\left(\frac{A_0}{4} - (1 - p(\text{“?”}))b\right) \tag{7.54}$$

$$c_? = \frac{1}{p(\text{“?”})}\left(\frac{A_0 B_0}{4} - (1 - p(\text{“?”}))\frac{c+d}{2}\right) \tag{7.55}$$

We are now left with four parameters, a, b, c and d. Additionally, $\bar{\sigma}^{+}_{AB}$, $\bar{\sigma}^{-}_{AB}$ and $\bar{\sigma}^{?}_{AB}$ must be chosen positive.

7.5 Implementations with realistic devices

In this section we simulate the expected observations (Q and $p(\text{“?”})$) for a realistic implementation in the node. We choose the implementation of the optimal USD in Sec. 7.3.3, and use the experimental values (channel loss ξ, the dark counts d_c, and alignment errors Q_{align}) in Refs. [61, 91] for our simulation. Then, using a subgradient method [12], we optimize χ_{tot} numerically over the set $\bar{\mathbf{\Gamma}}_Q$ in MATLAB with the simulated observations.

The channels l_A and l_B are characterized by transmissivity coefficients $\eta_A = 10^{-l_A\xi/10}$ and $\eta_B = 10^{-l_B\xi/10}$, where the channel loss ξ is in units of dB/km. If Alice sends coherent states $|\pm\alpha\rangle$, and Bob sends coherent states $|\pm\sqrt{\frac{\eta_A}{\eta_B}}\alpha\rangle$, the states arriving at the node are coherent states $|\pm\alpha'\rangle$ with equal magnitude $\alpha' = \sqrt{\eta_A}\alpha$. We treat detector inefficiencies as a lossy element (a beamsplitter with transmissivity η_{det}) followed by a perfect lossless detector, and assume that the detector losses are symmetric over the detectors D_+ and D_-. Two types of events cause the detectors to click: (i) an incoming state, (ii) a dark count d_c or an alignment error Q_{align}. We assume the limit of a negligable dark count rate and a negligable double click rate in the detectors.

The plots the key rates in dependence of the total distance between Alice and Bob $L = l_A + l_B$ are shown in Figs. 7.4 and 7.3. Since the amplitude α is under Alice's control, we maximize the key rate over α in order to obtain the best key rate for a given distance.

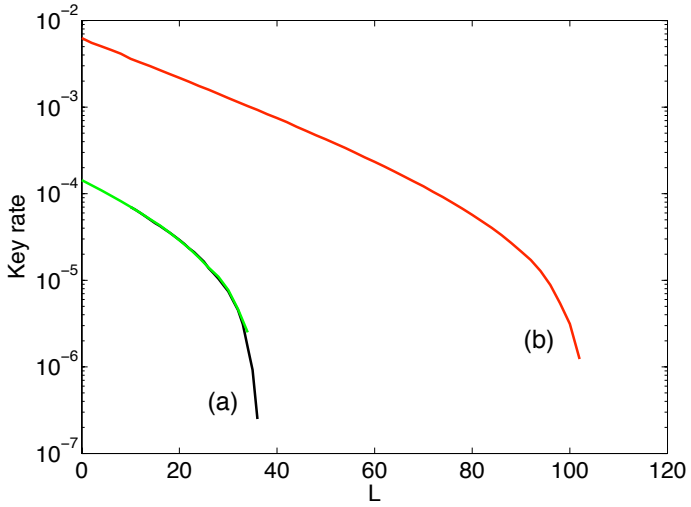


Figure 7.3: Plot of key rates for the different settings for experimental values from Ref. [91]. (a) Asymmetric MDI scenario $l_B = 0$ (green line), overlapping with symmetric MDI scenario $l_A = l_B$ (black line). (b) Strong reference pulse scenario ($l_B = 0$).

We plot two scenarios: (i) $l_A = l_B$, a symmetric placement of the node between Alice and Bob (black line), and (ii) $l_B = 0$ and $l_A = L$, an asymmetric placement of the node next to Bob (green line).

The black and the green line lie on top of each other, suggesting that the placement of the node has little importance on the performance of the protocol. However, it turns out that the distance, for which a secure key rate can be obtained, is rather low, because the MDI-B92 protocol is not very robust against loss. For the experimental parameters in Ref. [91] and [61], the maximal distance is approximately 48 km and 38 km, respectively. In comparison, the maximal distance of the MDI protocol with BB84 states in Ref. [61] is more than 200 km.

7.5.1 Homodyne measurement and postselection

Another possible strategy for the node is to do homodyne measurements instead of using threshold detectors. For example, the node could measure the quadrature $\hat{x}$ on the "+" output port, and the quadrature $\hat{p}$ on the "-" output port. The probability distribution of the outcomes (x, p) for coherent state inputs [Eq. (7.14)] is shown in Fig. 7.5. The

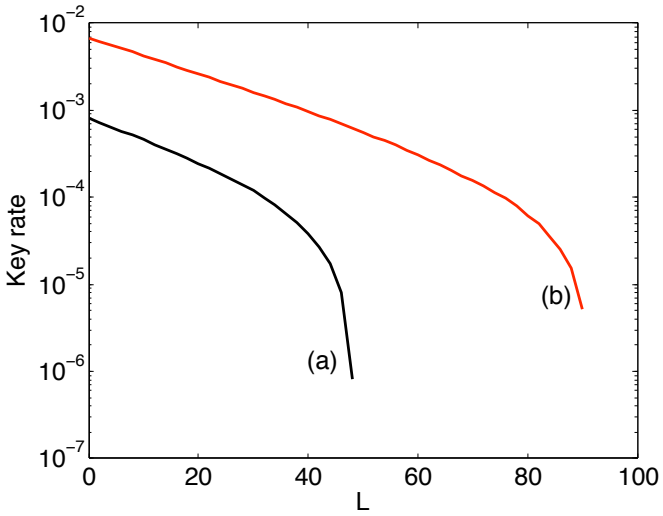


Figure 7.4: Plot of key rates for the different settings for for experimental values from Ref. [61]. (a) Symmetric MDI scenario $l_A = l_B$ (black line). (b) Strong reference pulse scenario $l_B = 0$.

colour-coding represents the regions of outcomes (x, p) which are predominantly triggered by correlated (anti-correlated) input states.

The homodyne measurements always yield a conclusive outcome ($p(\text{“?”}) = 0$), for which we have already shown in Sec. 7.3.1 that no key can be generated. However, we allow the node to postselect on the “good” measurement outcomes and make a inconclusive announcement for “bad” measurement outcomes. At the border of the regions in Fig. 7.5 we expect a high error rate, because it is equally likely that the input state was correlated and an anti-correlated. Therefore, we identify the points close to the border as “bad” and assign to them an inconclusive announcement $\gamma = \text{“?”}$. The amount of inconclusive announcements must not exceed the failure probability $p(\text{“?”})^{\text{sep}}_{\text{USD}} = \langle\alpha| - \alpha\rangle(2 - \langle\alpha| - \alpha\rangle)$, which is the failure probability of a separable USD attack, otherwise the protocol is insecure.

We computed the effective error rate after the postselection on “good” outcomes for several values of α, and compared it to the tolerable error rate obtained from our numerical calculations of the key rate. It turns out that the effective error rate was too high in order to generate a secure key.

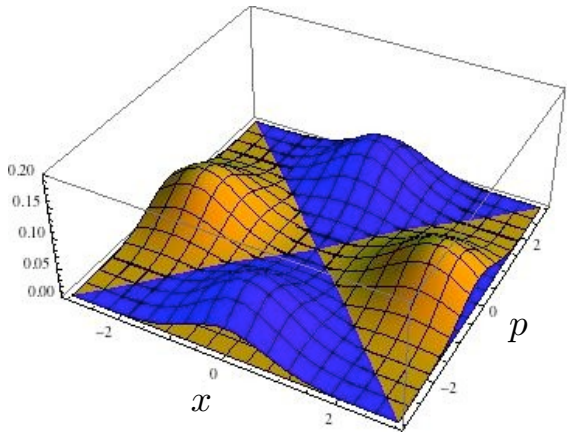


Figure 7.5: Probability distribution of measurement outcomes after a homodyne detection in the measurement values x and p. The yellow and blue regions correspond the data points (x, p) where the correlated and anti-correlated pairs are identified.

7.6 Security proof of the strong reference pulse B92 protocol

7.6.1 Strong reference pulse B92 protocol

In the original B92 protocol the signal states are accompanied by a strong reference pulse (SRP), which must be detected at Bob's side for every signal [2]. The strong reference pulse does not carry any information about the key bits, but it is important for the security. If the protocol is implemented without a strong reference pulse, the protocol becomes insecure under channel loss, because Eve can do a USD attack on the signal states. This result was shown in Refs. [89, 90].

The setup of the SRP-B92 scheme is shown in Fig. 7.6. The strong reference pulse is generated in Alice's laboratory by a source that emits coherent states. Alice splits the coherent states into a weak pulse (the signal pulse), and a strong pulse (the reference pulse). She applies a phase shift of 0 or π to the signal pulse, which prepares one of the two weak coherent states $|\pm\alpha\rangle$. The phases $+$ or $-$ of the coherent states denote the bit values 0 or 1, respectively. Finally, Alice sends the signal and the reference pulse through a quantum channel to Bob. Before performing his measurement, Bob attenuates the strong

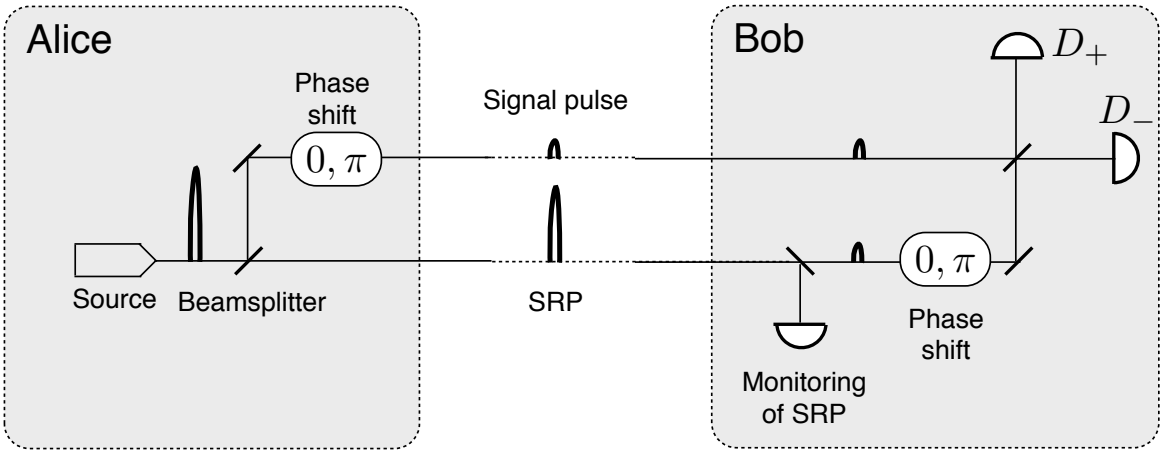


Figure 7.6: Setup of the strong reference pulse scheme.

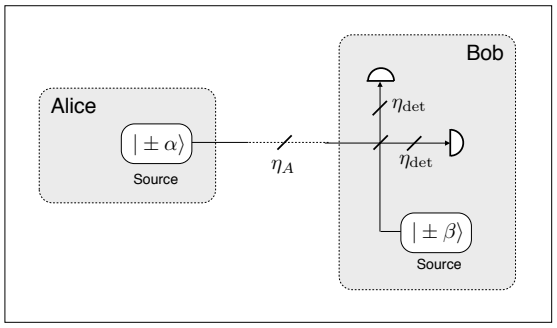
reference pulse to match the intensity of the signal pulse. He applies a phase shift 0 or π to the reference pulse before recombining the signal and the attenuated reference pulse at a balanced beamsplitter. The beams exiting from the output ports of the beamsplitter are measured using threshold detectors D_+ and D_-. Bob also monitors the intensity of the incoming strong reference pulse at all times to ensure that it was not blocked.

The security proof for the strong reference pulse scheme has been developed in Refs. [91, 55]. In the security proof in Ref. [91], two photon-number-resolving detectors are required at Bob's side.

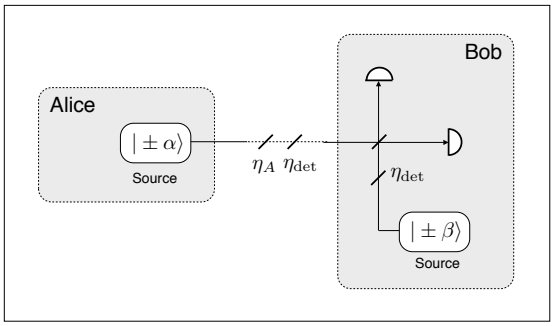
7.6.2 Adaptation of the MDI-B92 security proof to the SRP-B92 protocol

We derive a security proof for the SRP-B92 protocol from the security proof that we developed for the MDI-B92 protocol in the previous sections. The main idea is to show that the security proof that holds in the MDI scenario also holds for the SRP scenario. There are several steps between the initial SRP scenario and the final MDI scenario, that we describe here.

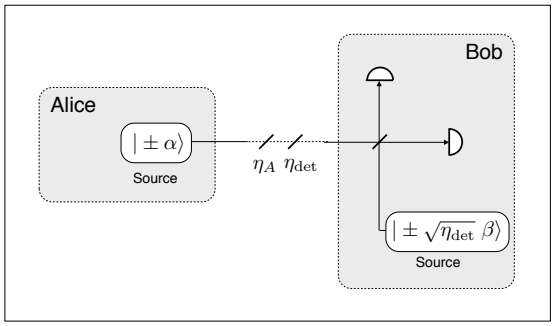
(a) We start with the original SRP scenario. If we assume that Bob can generate a reference pulse in his own laboratory, the original SRP scenario is equivalent to the scenario in



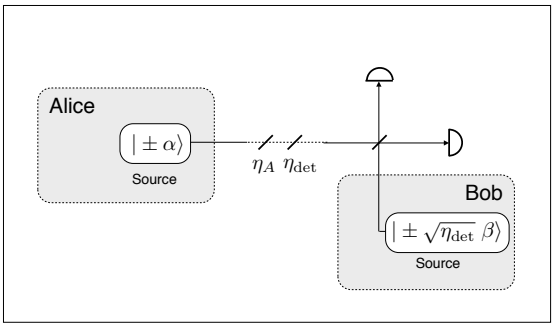
(a) The SRP is generated locally in Bob's laboratory. The detector loss is modeled by beamsplitters with transmissitivity η_{det}.



(b) Equivalent scenario with the detector loss in the channels.



(c) The detector loss is absorbed in Bob's source. His signal states are now described by $|\sqrt{\eta_{\text{det}}}\beta\rangle$.



(d) Eve's domain is extended to the beamsplitter and the two threshold detectors.

Figure 7.7: Steps leading from the SRP scenario to the MDI scenario.

Fig. 7.7 (a), where Bob generates the reference pulse locally. This assumption is justified in Ref. [55] provided that Bob is able to transfer the phase of Alice's reference pulse to his local pulse. Moreover, in classical telecommunication protocols with high detection rates it is already common practice to generate the phase reference locally.

(b) We describe the detector inefficiencies in the threshold detectors by beamsplitters with transmissivity $\eta_{\text{det}} \leq 1$ followed by perfect lossless detectors. If we place the beamsplitters η_{det} into the links l_A and l_B, the security is not compromised. In this equivalent scenario, we are able to treat the losses like channel losses [see Fig. 7.7 (b)]. The assumption that went into this step is that the losses in D_+ and D_- are symmetric.

(c) In the scenario in Fig. 7.7 (b), Bob's source emits $|\beta\rangle$ followed by an attenuation in the link by η_{det}. This scenario is equivalent to the scenario in Fig. 7.7 (c), where Bob's source emits a coherent state $|\sqrt{\eta_{\text{det}}}\beta\rangle$ into a lossless link. Therefore, we absorb the loss in the link l_B into Bob's source by recalibrating the intensity of the emitted coherent state $|\beta\rangle$ by a factor of η_{det}.

(d) Finally, in Fig. 7.7 (d) we extend Eve's domain to the balanced beamsplitter and the detectors $D_\pm$. We are now the MDI scenario, except that Eve does not have access to one of the loss η_{det} that was absorbed in Bob's source.

In the simulation we assume that the link l_B carries no channel loss because the node is placed at zero distance from Bob ($l_B = 0$). To obtain the optimal key rates, we maximize over the amplitude α. We plot the key rates in red in Figs. 7.4 and 7.3 for different experimental parameters. The key rate of the SRP-B92 beats the key rate of the MDI-B92 scenario, because on of the losses η_{det} is absorbed in Bob's source, is not accessible to Eve. However, our key rate for the SRP-B92 is low in comparison to the key rates in Ref. [91, 55]. This can be understood because we give Eve more power that she actually has. In reality Eve does not have access to the entire measurement apparatus.

7.7 Conclusion

In this chapter we analyze the performance of a MDI protocol with B92 signal states. Alice and Bob are both senders, while a node in the middle acts as the receiver and performs the measurement. To each measurement outcome the node makes an announcement that is used by Alice and Bob to postprocess their data in order to generate correlated strings of bits.

We provide a security proof for the protocol under the assumption of an MED attack and a USD attack. The assumption of these specific attacks is only valid for certain observations. If the observations indicate an MED attack, we find that no key can be generated, because the joint attack MED is equivalent to the separable MED attack, which yields no positive key rate. In fact, any strategy where the node is forced to make an announcement for each signal is equivalent to a separable strategy and yields no key. On the other hand, if the observations indicate a USD attack, a positive key rate is possible, because the joint and the separable eavesdropping strategy is different.

We also provide a security proof for the MDI-B92 protocol for general observations. The MDI-B92 protocol exhibits enough symmetries in order to justify a symmetric optimal attack. We simulate the measurement outcomes for the optimal joint USD setup in the node, including channel loss, detector efficiency, dark counts and misalignment errors. Although we obtain positive key rates, it turns out that the MDI-B92 protocol is vulnerable to channel loss. In terms of distance, the MDI-B92 protocol is outperformed by the MDI protocol with BB84 signal states and Decoy states.

Finally, we apply the established MDI-B92 security proof to generate a security proof for the B92 protocol with a strong reference pulse. Our method yields positive key rates, but it is not an improvement over already existing security proofs.

It would be interesting to apply the methods developed in this chapter to analyze MDI protocols with other sets of signal states that are less vulnerable to channel loss or to MED attacks.

Chapter 8

Application of the entropic uncertainty relation to security proofs of continuous-variable QKD

As an alternative to the discrete-variable encoding schemes, protocols with continuous-variable encoding schemes have been suggested, for example, in Refs. [46, 74]. Instead of photon counters, continuous-variable (CV) schemes employ homodyne or heterodyne quadrature measurements on the receiver's side, which provide a continuous spectrum of outcomes. While homodyne measurements are fast and have high efficiencies, the data processing is more involved, because of the continuous nature of the outcomes. Moreover, in the source replacement scheme, Bob's system is infinite-dimensional which can pose difficulties for the security proof.

In this chapter we analyze the 2-state protocol with discrete modulation and homodyne measurements. This protocol is actually rather simple to implement experimentally. Alice has the choice between two coherent states with opposite phases $|\pm\alpha\rangle$, where α is real. Bob does a homodyne measurement of the $\hat{x}$ quadrature half of the time, and if his outcome is positive/negative, he identifies the bit value by 0/1. He also measures the $\hat{p}$ quadrature half of the time in order to check for Eve's presence.

For this protocol, the quantum state ρ_{AB} in the source-replacement scheme is infinite-dimensional on system B. In the parameter estimation the state ρ_{AB} is typically characterized in terms of Bob's observed first and second moments of the $\hat{x}$ and $\hat{p}$ quadrature. For general observations, this characterization of ρ_{AB} still leaves infinitely many eavesdropping attacks, and therefore, the optimization of the key rate is difficult. However, for some spe-

cial observations, the eavesdropping attacks can be constructed analytically. For example, if Bob can verify from his observations that he receives pure states, the attack must have been a beamsplitter attack, for which a security proof is analytically given in Ref. [44]. Furthermore, for observations with very small excess noise, numerical security proofs were found in Ref. [96].

Recently, a new entropic uncertainty relation under assumption of a quantum memory was proven in Ref. [11]. Using this relation it was possible to provide a new security proof for the BB84 protocol based on Alice and Bob's observations, without having to specify the exact structure of ρ_{AB}. The security proof reproduced the exact BB84 key rates [11].

The goal of this chapter is to use the new uncertainty relation to provide an alternative approach to prove the security of CV QKD protocols with reverse reconciliation and homodyne measurements on Bob's side. On the one hand, we analyze the continuous-variable counterpart of the BB84 protocol with squeezed coherent states and Gaussian modulation. We find that the key rate is only positive, if Bob can verify a minimum amount of squeezing in his observations. On the other hand, we analyze the 2-state protocol. We hoped that the method based on the uncertainty relation would be successful, but unfortunately, it did not yield positive key rates. The reason is that there is not enough information in the observations in order to make a sufficiently good estimate of Eve's knowlegde.

8.1 Entropic uncertainty relations

We demonstrate the entropic uncertainty relation in a similar fashion as in Ref. [11]. Alice prepares the state ρ_B and sends it to Bob. Bob chooses to measure one of the non-commuting observables $\hat{x}$ or $\hat{p}$ and announces the choice of the observable publicly. Alice's task is to guess Bob's measurement outcome knowing which observable he measured. We allow Alice to keep a description of ρ_B in a memory, represented by an initial quantum state ρ_{AB} between Alice and Bob with the property $\mathrm{tr}_A\,\rho_{AB} = \rho_B$. The correlations between the systems A and B can range from basic classical correlations (classical memory) to entanglement (quantum memory).

For practical calculations we write the measurement outcomes in a classical system X_B or P_B. The joint state between Alice and Bob after the measurement is a cq state

$$\rho_{AX_B} = \sum_x p(x)\rho_A^x \otimes |x\rangle\langle x|_{X_B}, \tag{8.1}$$

$$\rho_{AP_B} = \sum_p p(p)\rho_A^p \otimes |p\rangle\langle p|_{P_B}, \tag{8.2}$$

where $p(x)$ and $p(p)$ denote the continuous probability density functions of the measurement outcomes, and the states ρ_A^x and ρ_A^p are the conditional states held by Alice. Alice's uncertainty about Bob's measurement outcome is captured in the *conditional differential entropy* $H(X_B|A)$ and $H(P_B|A)$ defined as

$$H(X_B|A) = H(X_B) + \sum_x p(x) S(\rho_A^x) - S(\rho_A). \tag{8.3}$$

In this expression, the Shannon entropy of a continuous probability density function $p(x)$ is called *differential entropy* or *continuous entropy*. It is given by $H(X_B) = -\int dx\ p(x) \log p(x)$.

The first entropic uncertainty relation, which was introduced in Ref. [66], characterize how much uncertainty Alice has about Bob's outcome if her memory is purely classical. The entropic uncertainty principle recently proven in Ref. [11] characterizes Alice's uncertainty about Bob's measurement outcomes also for quantum memories. The entropic uncertainty relation reads:

$$H(X_B|A) + H(P_B|A) \geq \log_2 \frac{1}{c} + S(B|A). \tag{8.4}$$

In this relation, the term c represents the complementarity between $\hat{x}$ and $\hat{p}$. If $\hat{x}$ and $\hat{p}$ are two non-degenerate observables with eigenvectors $\{|\phi_x\rangle\}$ and $\{|\psi_p\rangle\}$, $c = \max_{x,p} |\langle\phi_x|\psi_p\rangle|^2$. The conditional entropy $S(B|A)$ quantifies the initial entanglement in the state ρ_{AB} between Alice and Bob. In fact, this term can be negative and can cancel out the term $\log_2 \frac{1}{c}$. For example, let Alice and Bob's initial state be the perfectly entangled two-qubit state $|\phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, and let Bob measure either in the Pauli X or Z eigenbasis. Then, $c = 1/2$, $S(B|A) = -\log_2 2 = -1$ [11], and the right hand side of Eq. (8.4) cancels out. In this case, Alice is able to predict Bob's measurement outcomes perfectly, because the entropic uncertainty relations implies that $H(X_B|A) = H(P_B|A) = 0$.

If the initial state ρ_{AB} is mixed, we can construct a tripartite purification $|\Psi\rangle_{ABE}$ on an additional system E, and the entropic uncertainty relation can be written involving the system E. Due to the Schmidt decomposition it follows that $S(\rho_E) = S(\rho_{AB})$ and $S(\rho_{AX_B}) = S(\rho_{X_BE})$. From these identities, it follows that

$$\begin{aligned} H(X_B|A) - S(B|A) &= S(\rho_{AX_B}) - S(\rho_A) - S(\rho_{AB}) + S(\rho_A) && (8.5)\\ &= S(\rho_{X_BE}) - S(\rho_E) && (8.6)\\ &= H(X_B|E) && (8.7) \end{aligned}$$

Inserting this into the entropic uncertainty relation in Eq. (8.4), we obtain

$$H(X_B|E) + H(P_B|A) \geq \log_2 \frac{1}{c}. \tag{8.8}$$

Furthermore, the entropic uncertainty is valid for generalized measurements with POVM elements $\{F_x\}_x$ and $\{F_p\}_p$. The generalized version of the term c is given by

$$c = \max_p ||\sum_x F_x F_p F_x||_\infty, \tag{8.9}$$

where the infinity norm $||C||_\infty$ (or operator norm) is defined as $||C||_\infty = \max_{|\Psi\rangle} \sqrt{\langle\Psi|C^\dagger C|\Psi\rangle}$. If C is Hermitian, the operator norm is equal to the largest eigenvalue of C.

8.2 Entropic uncertainty relations in QKD

8.2.1 Key rate with reverse reconciliation

In this section we use the entropic uncertainty relation to provide a security proof for continuous-variable protocols with reverse reconciliation. Reverse reconciliation in CV QKD protocols allows to find a positive secret key rate even beyond the 3dB loss limit [43, 72].

As usually, we work in the source-replacement scheme, and describe the state between Alice and Bob by a bipartite state ρ_{AB}, of which Eve holds the purification $|\Psi\rangle_{ABE}$. We call Alice's generic measurements M with outcomes i and probabilities $p(i)$. There are no assumptions on the spectrum of Alice's measurement outcomes i, which can be discrete or continuous at this point. Bob does a homodyne measurement on the system B with respect to one of the quadratures $\hat{x}$ or $\hat{p}$. The key is build from the data that Bob obtained by measuring $\hat{x}$, while the other measurement ($\hat{p}$) is used to check for Eve's presence. The key generated using reverse reconciliation is given by the Devetak-Winter formula

$$r_{\mathrm{RR}} = I(M_A : X_B) - \chi(X_B : E) = H(X_B|E) - H(X_B|M_A). \tag{8.10}$$

If we use the entropic uncertainty relation in Eq. (8.4) to estimate Eve's uncertainty by $H(X_B|E) \geq \log_2 \frac{1}{c} - H(P_B|A)$, we obtain a bound for the key rate

$$r_{\mathrm{RR}} \geq \log_2 \frac{1}{c} - H(P_B|A) - H(X_B|M_A), \tag{8.11}$$

that depends only on Alice and Bob's systems, and not on Eve.

8.2.2 Entropic uncertainty relation and homodyne measurements

In this section we calculate the constant c for homodyne measurements [82]. We first define the coarse-grained homodyne measurements with POVM elements that are projectors onto finite intervals $(x_i - \frac{\Delta}{2}, x_i + \frac{\Delta}{2})$ of width Δ:

$$F_{x_i} = \int_{x_i-\Delta/2}^{x_i+\Delta/2} |x\rangle\langle x| dx \tag{8.12}$$

$$F_{p_j} = \int_{p_j-\Delta/2}^{p_j+\Delta/2} |p\rangle\langle p| dp. \tag{8.13}$$

If a state ρ is measured with respect to the coarse-grained measurement, the probability distribution of the outcomes is discretized $p(x_i) = \mathrm{tr}\{\rho F_{x_i}\} = \int_{x_i-\Delta/2}^{x_i+\Delta/2} p(x)dx$. We write the outcomes of the coarse-grained measurements into classical systems X^Δ and P^Δ.

For the coarse-grained homodye measurement we can calculate the constant c according to the definition in Eq. (8.9). In the limit $\Delta \to 0$, we then obtain the value of c for a homodyne measurement.

Lemma 6 *The constant c for the coarse-grained homodyne measurement is lower bounded by*

$$c \leq \frac{\Delta^2}{2\pi}. \tag{8.14}$$

In the limit of small Δ, this result is tight. The same result was independently found in Ref. [37].

Proof. The term $\sum_i F_{x_i} F_{p_j} F_{x_i}$ is a Hermitian operator, and thus the operator norm is simply the maximal eigenvalue. Since the POVM elements F_{p_j} are projectors onto disjoint subspaces $\mathcal{H}_i$, each block $F_{x_i} F_{p_j} F_{x_i}$ lives on the operator space $\mathcal{B}(\mathcal{H}_i)$. Consequently, the maximum eigenvalue of the sum $\sum_i F_{x_i} F_{p_j} F_{x_i}$ is found on one of the blocks with index i. This means that $||\sum_i F_{x_i} F_{p_j} F_{x_i}||_\infty = \max_i ||F_{x_i} F_{p_j} F_{x_i}||_\infty$. Therefore, the constant that we need to approximate is

$$c = \max_{i,j} ||F_{x_i} F_{p_j} F_{x_i}||_\infty. \tag{8.15}$$

We expand the product $F_{x_i}F_{p_j}F_{x_i}$ using the overlaps $\langle x|p\rangle = \frac{1}{\sqrt{2\pi}}e^{-ipx}$, and compute the integral over p:

$$F_{x_i}F_{p_j}F_{x_i} = \int_{x_i-\Delta/2}^{x_i+\Delta/2}\int_{p_j-\Delta/2}^{p_j+\Delta/2}\int_{x_i-\Delta/2}^{x_i+\Delta/2} dx\ dp\ dx'|x\rangle\langle x|p\rangle\langle p|x'\rangle\langle x'| \tag{8.16}$$

$$= \frac{1}{2\pi}\int_{x_i-\Delta/2}^{x_i+\Delta/2}\int_{x_i-\Delta/2}^{x_i+\Delta/2} dx\ dx'|x\rangle\langle x'|\left(\int_{p_j-\Delta/2}^{p_j+\Delta/2} dp\ e^{-ip(x-x')}\right) \tag{8.17}$$

$$= \frac{1}{2\pi}\int_{x_i-\Delta/2}^{x_i+\Delta/2}\int_{x_i-\Delta/2}^{x_i+\Delta/2} dx\ dx'|x\rangle\langle x'|\left(e^{-ip_j(x-x')}\frac{e^{-i(x-x')\Delta/2}-e^{i(x-x')\Delta/2}}{-i(x-x')}\right) \tag{8.18}$$

$$= \frac{\Delta}{2\pi}\int_{x_i+\Delta/2}^{x_i-\Delta/2}\int_{x_i+\Delta/2}^{x_i-\Delta/2} dx\ dx'|x\rangle\langle x'|\ e^{-ip_j(x-x')}\,\mathrm{sinc}\left(\frac{\Delta}{2}(x-x')\right), \tag{8.19}$$

where the sinus cardinalis is defined by $\mathrm{sinc}(x) = \sin(x)/x$.

Let $|\psi_{x_i}\rangle$ be a normalized state on $\mathcal{D}(\mathcal{H}_i)$. We estimate the operator norm of $F_{x_i}F_{p_j}F_{x_i}$ as follows:

$$\begin{aligned}
||F_{x_i}F_{p_j}F_{x_i}||_\infty &= \max_{|\psi_{x_i}\rangle}\ \langle\psi_{x_i}|F_{x_i}F_{p_j}F_{x_i}|\psi_{x_i}\rangle \\
&\leq \max_{|\psi_{x_i}\rangle}\ |\langle\psi_{x_i}|F_{x_i}F_{p_j}F_{x_i}|\psi_{x_i}\rangle| \\
&\leq \max_{|\psi_{x_i}\rangle}\frac{\Delta}{2\pi}\int\int dx\ dx'\,|\langle\psi_{x_i}|x\rangle\langle x'|\psi_{x_i}\rangle|\ \left|e^{ip(x-x')}\right|\ \left|\mathrm{sinc}\left(\frac{\Delta}{2}(x-x')\right)\right| \\
&\leq \max_{|\psi_{x_i}\rangle}\frac{\Delta}{2\pi}\int\int dx\ dx'|\langle\psi_{x_i}|x\rangle\langle x'|\psi_{x_i}\rangle| \qquad (8.20)
\end{aligned}$$

In the second line we used that $\max_y f(y) \leq \max_y |f(y)|$, and in the last line we lower-bounded $|\mathrm{sinc}(x)| \leq 1$. If we choose $|\psi_{x_i}\rangle$ such that the overlap $\langle\psi_{x_i}|x\rangle \geq 0$ and real for all x, we can drop the absolute values in line (8.20). Furthermore, we define the normalized uniform superposition state on $\mathcal{D}(\mathcal{H}_i)$ by $|\Phi_{x_i}\rangle = \frac{1}{\sqrt{\Delta}}\int_{x_i-\Delta/2}^{x_i+\Delta/2}|x\rangle$. Then Eq. (8.20) becomes

$$\max_{|\psi_{x_i}\rangle}\frac{\Delta}{2\pi}\int\int dx\ dx'\langle\psi_{x_i}|x\rangle\langle x'|\psi_{x_i}\rangle = \max_{|\psi_{x_i}\rangle}\frac{\Delta^2}{2\pi}\langle\psi_{x_i}|\Phi_{x_i}\rangle\langle\Phi_{x_i}|\psi_{x_i}\rangle = \frac{\Delta^2}{2\pi}. \tag{8.21}$$

In the last equality we chose $|\psi_{x_i}\rangle = |\Phi_{x_i}\rangle$. ■

The limit of small Δ

In the limit of small Δ, the conditional entropy $H(X_B^\Delta|E)$ of the coarse-grained random variable X^Δ is approximated by the conditional differential entropy $H(X_B|E)$ defined in Eq. (8.3) of the continuous random variable X. For the Shannon entropy and the conditional von Neumann entropy the following approximations hold:

Lemma 7 *The discrete entropies are approximated by the continuous entropies:*

$$H(X_B^\Delta) \simeq H(X_B) - \log_2 \Delta, \tag{8.22}$$

$$H(X_B^\Delta|E) \simeq H(X_B|E) - \log_2 \Delta.. \tag{8.23}$$

Using Eq. (8.23) we are able to approximate the classical conditional entropy $H(X_B^\Delta|M_A) \simeq H(X_B|M_A) - \log_2 \Delta$. Furthermore, if we substitute these approximations into the key rate together with $c \leq \Delta^2/2\pi$, all terms Δ cancel out

$$r_{\mathrm{RR}} \geq \log_2(2\pi) - H(P_B|A) - H(X_B|M_A). \tag{8.24}$$

Proof. Eq. (8.22) is proved using the mean value theorem, which states that for a continuous function $f(x)$ there exists a $\bar{x}_i$ in the interval $(x_i - \frac{\Delta}{2}, x_i + \frac{\Delta}{2})$ such that

$$\int_{x_i - \Delta x/2}^{x_i + \Delta x/2} f(x)dx = f(\bar{x}_i)\Delta. \tag{8.25}$$

We identify $f(x)$ with the probability density function $p(x)$ of measurement outcomes of X. Using the mean value theorem, we expand the Shannon entropy

$$H(X_B^\Delta) = -\sum_i p(x_i) \log_2 p(x_i) \tag{8.26}$$

$$= -\sum_i \Delta p(\bar{x}_i) \log_2(\Delta p(\bar{x}_i)) \tag{8.27}$$

$$= -\sum_i \Delta p(\bar{x}_i) \log_2(p(\bar{x}_i)) - \left(\sum_i \Delta p(\bar{x}_i)\right) \log_2 \Delta \tag{8.28}$$

In the limit of small Δ, the first term tends to $-\int p(x) \log_2 p(x)dx$, while the second term is $-\log_2 \Delta$ because of the identity $\sum_i \Delta p(\bar{x}_i) = \int p(x)dx = 1$ according to the mean value theorem. This proves the first approximation in Eq. (8.22).

In order to prove Eq. (8.23), we expand $H(X_B^\Delta|E) = H(X_B^\Delta) + S(E|X_B^\Delta) - S(E)$. The only unknown term is $S(E|X_B^\Delta) = \sum_i p(x_i) S(\rho_E^{x_i})$ with conditional states

$$\rho_E^{x_i} = \frac{\int_{x_i-\Delta x/2}^{x_i+\Delta x/2} p(x)\rho_E^x dx}{p(x_i)} = \frac{\Delta f(\bar{x}_i)}{p(x_i)} \tag{8.29}$$

We identified $f(x) = p(x)\rho_E^x$ and used the mean value theorem in the last equation. We get rid of denominator $p(x_i)$ using the identity $S(\rho/p) = S(\rho)/p + \log_2 p$ in $S(E|X_B^\Delta)$ and regroup the terms

$$H(X_B^\Delta|E) = H(X_B^\Delta) + \sum_i p(x_i) S\left(\frac{\Delta f(\bar{x}_i)}{p(x_i)}\right) - S(E) \tag{8.30}$$

$$= \sum_i S\left(\Delta f(\bar{x}_i)\right) - S(E) \tag{8.31}$$

$$= -\sum_i \Delta \operatorname{tr}\{f(\bar{x}_i)\log_2 f(\bar{x}_i)\} - \operatorname{tr}\left\{\sum_i \Delta f(\bar{x}_i)\right\}\log_2\Delta - S(E) \tag{8.32}$$

$$\simeq -\int dx\ \operatorname{tr}\{f(x)\log_2 f(x)\} - \log_2\Delta - S(E). \tag{8.33}$$

In the last line we used that, in the limit of small Δ, the first term approaches the integral $-\int dx\ \operatorname{tr}\{f(x)\log_2 f(x)\}$. The second term in (8.32) is equal to $-\log_2\Delta$ because $\operatorname{tr}\{\sum_i \Delta f(\bar{x}_i)\} = \operatorname{tr}\{\int dx\ p(x)\rho_E^x\} = 1$. If we substitute $f(x) = p(x)\rho_E^x$ we obtain

$$-\int dx\ \operatorname{tr}\{f(x)\log_2 f(x)\} = -\int dx\ p(x)\log_2 p(x) - \int dx\ p(x)\operatorname{tr}\{\rho_E^x \log_2 \rho_E^x\} \tag{8.34}$$

$$= H(X_B) + S(E|X_B). \tag{8.35}$$

Finally, substituting this result into $H(X_B^\Delta|E)$, we obtain Eq. (8.23). ■

8.3 CV QKD protocol examples

In this section we calculate the key rates of two continuous-variable protocols using the entropic uncertainty principle.

8.3.1 Protocol with Gaussian modulation and squeezed states

First we analyze a protocol with Gaussian modulated squeezed states and homodyne detection. This protocol is generally seen as the continuous-variable counterpart of the BB84 protocol. It was proposed in Ref. [23], and unconditional security was proven in Refs. [42]. We use the entropic uncertainty relation to calculate the key rate of this protocol, which was also done in Ref. [37].

Alice chooses with probability 1/2 to prepare a squeezed vacuum state in either the $\hat{x}$ or the $\hat{p}$ quadrature. If she chose $\hat{x}$ ($\hat{p}$), she modulates the squeezed state according to a Gaussian probability density function $p(x_A)$ ($p(p_A)$) along the $\hat{x}$- ($\hat{p}$) -quadrature. She then sends the squeezed state to Bob, who does a homodyne measurement of either the $\hat{x}$ or the $\hat{p}$ quadrature, with continuous outcomes x_B or p_B. Finally, Alice and Bob postselect on the data where both chose the same quadrature, which is equivalent to the basis sifting step in the BB84 protocol. After the postselection on matching quadratures, the data is divided into two sets, one set where both chose the $\hat{x}$ quadrature, and one where both chose the $\hat{p}$ quadrature, with conditional probability density functions $p(x_B|x_A)$ and $p(p_B|p_A)$ describing each set.

In the source-replacement scheme Alice prepares a two-mode squeezed state $|\Psi_{\text{TMSS}}\rangle_{AB}$ defined in Eq. (2.39) in her laboratory, and sends the second half to Bob. Alice randomly chooses to measure her part with respect to one of the two homodyne measurements $\hat{x}$ or $\hat{p}$, with continuous outcomes x_A or p_A according to a Gaussian distribution. This measurement effectively prepares a squeezed coherent state $|\alpha, r\rangle$ for Bob.

In the quantum description of the postselection, the Kraus operators $K_A^x \otimes K_B^x$ and $K_A^p \otimes K_B^p$ associated to the matching quadratures are proportional to the identity, because the measurement $\hat{x}$ and $\hat{p}$ are complete von Neumann measurements [see Sec. 3.5.1]. If we denote the state between Alice and Bob by ρ_{AB}, the conditional states after the postselection remain unchanged:

$$\rho_{AB}^{xx} = K_A^x \otimes K_B^x \rho_{AB} (K_A^x \otimes K_B^x)^\dagger = \rho_{AB}, \tag{8.36}$$

$$\rho_{AB}^{pp} = K_A^x \otimes K_B^x \rho_{AB} (K_A^x \otimes K_B^x)^\dagger = \rho_{AB}. \tag{8.37}$$

If we choose to extract the key from the data where the $\hat{x}$ quadrature was matching, the key rate is

$$r_{\text{RR}} = H(X_B|E)_{xx} - H(X_B|X_A)_{xx} \tag{8.38}$$

$$\geq \log_2(2\pi) - H(P_B|A)_{xx} - H(X_B|X_A)_{xx}. \tag{8.39}$$

In this expression we do not know the conditional entropy $H(P_B|A)_{xx}$, because the state ρ_{AB}^{xx} is never actually measured with respect to the $\hat{p}$ quadrature on Bob's side. However, since $\rho_{AB}^{xx} = \rho_{AB}^{pp}$, we can estimate the conditional entropy $H(P_B|A)_{xx}$ from the $\hat{p}$ quadrature measurement of ρ_{AB}^{pp} by $H(P_B|A)_{xx} = H(P_B|A)_{pp}$. Finally, since Alice actually performs a measurement on her system, we use the bound $H(P_B|A)_{xx} \leq H(P_B|P_A)_{xx}$ to estimate he remaining term. We are now able to express the key rate in terms of measured quantities only

$$r_{\mathrm{RR}} \geq \log_2(2\pi) - H(P_B|P_A)_{pp} - H(X_B|X_A)_{xx}. \tag{8.40}$$

Now we evaluate the key rate for a typical setup. We model Bob's measurement outcomes by Gaussian distributions. This is reasonable to expect in an experiment where Alice sends squeezed vacuum states through a lossy channel. We define Bob's first and second moments in each set of matching measurements by $(\langle x_B \rangle, \mathrm{Var}_x)$ and $(\langle p_B \rangle, \mathrm{Var}_p)$. Furthermore, we assume that the variances are independent of Alice's values x_A and p_A. Since the entropy

$$H(p_G(x)) = -\int dx\; p_G(x) \log_2 p_G(x) = \log_2 \sqrt{2\pi \mathrm{Var}_x\, e}, \tag{8.41}$$

of a Gaussian probability density function $p_G(x)$ with first and second moments $(\langle x \rangle, \mathrm{Var}_x)$ is independent of the first moment, it follows that the Bob's conditional entropies are given by

$$H(X_B|X_A)_{xx} = \log_2 \sqrt{2\pi \mathrm{Var}_x e}, \tag{8.42}$$

$$H(P_B|P_A)_{pp} = \log_2 \sqrt{2\pi \mathrm{Var}_p e}. \tag{8.43}$$

We substitute these results into the key rate and obtain

$$r_{\mathrm{RR}} \geq \log_2 \left(\frac{1}{e\sqrt{\mathrm{Var}_x \mathrm{Var}_p}} \right). \tag{8.44}$$

It turns out that this expression is only positive if the states arriving at Bob's side have a minimum amount of squeezing. In terms of the Bob's observed data, the variances must satisfy at least $\sqrt{\mathrm{Var}_x \mathrm{Var}_p} \leq \frac{1}{e}$, otherwise the key rate is zero. For example, if Bob receives coherent states, then $\mathrm{Var}_x = \mathrm{Var}_p = \frac{1}{2}$, and thus the key rate is zero. The squeezing can be expressed in terms of the squeezing parameter r (see Sec. 2.2.2), which must exceed $r > 0.15$ for a positive key rate.

Remark: Recall that the variances do not need to satisfy $\mathrm{Var}_x \mathrm{Var}_p \geq \frac{1}{4}$, because Var_x is obtained from measuring ρ_{AB}^{xx} and Var_p from measuring ρ_{AB}^{pp} after the postselection on matching bases.

In Ref. [42], unconditional security was proven for this protocol in connection with error corrections codes for a squeezing parameter $r > 0.28$.

8.3.2 The 2-state protocol

The 2-state protocol is the simplest CV protocol. In contrast to the previous protocol, Alice sends only two states to Bob. In a sense this is a "hybrid" protocol with a discrete modulation in a continuous-variable setting.

Alice chooses randomly one of two coherent states with opposite phases $|\pm\alpha\rangle$. The phases of the coherent states represent the two bit values 0 and 1. The coherent states are chosen with *a priori* probability $p(i) = 1/2$ for $i = 0, 1$. While travelling through the quantum channel, the states are typically attenuated by the loss and experience a broadening in phase space (excess noise) [64]. After traveling through the channel, Bob obtains conditional states ρ_B^i for $i = 0, 1$. He does either an $\hat{x}$ or a $\hat{p}$ quadrature measurement, and identifies the bit value from the sign of his $\hat{x}$ measurement outcome. The $\hat{p}$ measurement is used to check for Eve's presence. We assume that Bob's probability probability density functions $p(x_B|i)$ and $p(p_B|i)$ are Gaussian with variances Var_x and Var_p.

In the source-replacement scheme, the source state is entangled between a qubit system A and a infinite-dimensional system B,

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle|\alpha\rangle + |1\rangle|-\alpha\rangle), \tag{8.45}$$

Alice's measurement M is a von Neumann measurement with projectors $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$, which prepares the two coherent signal states on Bob's side. Since there is only one measurement on Alice's side, the key rate

$$r \geq \log_2(2\pi) - H(P_B|A) - H(X_B|M_A) \tag{8.46}$$

in Eq. (8.24) applies here.

Estimation of $H(P_B|A)$ for the 2-state protocol

In order to give a lower bound on the key rate, we make an estimate of the term $H(P_B|A)$. In a first step, we use the bound $H(P_B|A) \leq H(P_B|M_A)$ to make all quantities that

appear in the key rate dependent on measured quantities. For a Gaussian distribution, the conditional entropies were given in Eqs. (8.42) and (8.43). However, in contrast to the CV protocol with squeezed states and postselection, the variances in case of the 2-state protocol must satisfy the Heisenberg uncertainty relation $\mathrm{Var}_x \mathrm{Var}_p \geq 1/4$. If we calculate the key rate, we obtain

$$r_{\mathrm{RR}} \geq \log_2(2\pi) - H(P_B|M_A) - H(X_B|M_A) = \log_2 \left(\frac{1}{e\sqrt{\mathrm{Var}_x \mathrm{Var}_p}} \right) \geq \log_2 \left(\frac{2}{e} \right). \quad (8.47)$$

The term $\log_2 \frac{2}{e}$ is negative. This shows that our first estimate of $H(P_B|A)$ needs to be improved for a positive key rate.

In a second step, we tried to estimate $H(P_B|A)$ directly. Unfortunately, though, we did not succeed in finding a better bound in this case either. In the remaining part of this section, we show the steps that we tried to obtain an estimate of $H(P_B|A)$.

Let Alice, Bob and Eve share a pure tripartite state $|\Psi\rangle_{ABE}$. We would like to find an upper bound for the conditional entropy

$$H(P_B|A) = S(A|P_B) - S(A) + H(P_B), \quad (8.48)$$

after Bob did a $\hat{p}$ quadrature measurement. The term $H(P_B)$ is known from Bob's the observations. Here we assume again that Bob sees a Gaussian distribution in the $\hat{p}$-quadrature, so that $H(P_B) = \log_2 \sqrt{2\pi \mathrm{Var}_p e}$. The term $S(A) = S(\rho_A) = h(\mu_+)$ is computed from the eigenvalues $\mu_\pm = \frac{1}{2}(1 \pm e^{-2|\alpha|^2})$ of the known reduced density operators

$$\rho_A = \mathrm{tr}_B |\Phi\rangle\langle\Phi| = \frac{1}{2} \begin{pmatrix} 1 & \langle -\alpha|\alpha\rangle \\ \langle\alpha| - \alpha\rangle & 1 \end{pmatrix} \quad (8.49)$$

given here in the canonical basis $\{|0\rangle, |1\rangle\}$. In order to calculate $S(A|P_B) = \int dp_B \, p(p_B) \, S(\rho_A^{p_B})$ we parametrize Alice's conditional states $\rho_A^{p_B}$ in the canonical basis by density matrices

$$\rho_A^{p_B} = \begin{pmatrix} p(0|p_B) & t(p_B) \\ t(p_B)^* & p(1|p_B) \end{pmatrix} = \begin{pmatrix} 1/2 & t(p_B) \\ t(p_B)^* & 1/2 \end{pmatrix} \quad (8.50)$$

with unknown off-diagonal coefficients $t(p_B)$. The coefficients $t(p_B)$ are not arbitrary, since the states $\rho_A^{p_B}$ must the following constraints:

(i) The states $\rho_A^{p_B}$ are positive.

(ii) The integral $\int dp_B\, p(p_B)\rho_A^{p_B}$ must be equal to the reduced state ρ_A.

(iii) The first and second moments of Bob's measurement outcomes are fixed.

If we drop the third constraint, a solution is $t(p_B) = \frac{1}{2}\langle -\alpha|\alpha\rangle$. This implies that $\rho_A^{p_B} = \rho_A$ for all p_B, and it follows that $H(P_B|A) = H(P_B) = \log_2 \sqrt{2\pi \mathrm{Var}_p e}$. We already know that this estimate does not yield any positive key rate. Therefore, the bound on $H(P_B|A)$ obtained from constraints (i) and (ii) alone is not strong enough

We tried to incorporate the third constraint into the estimation, but we had no success. One would need to have an estimate of the entropies $S(\rho_A^{p_B})$ depending on Bob's first and second moments.

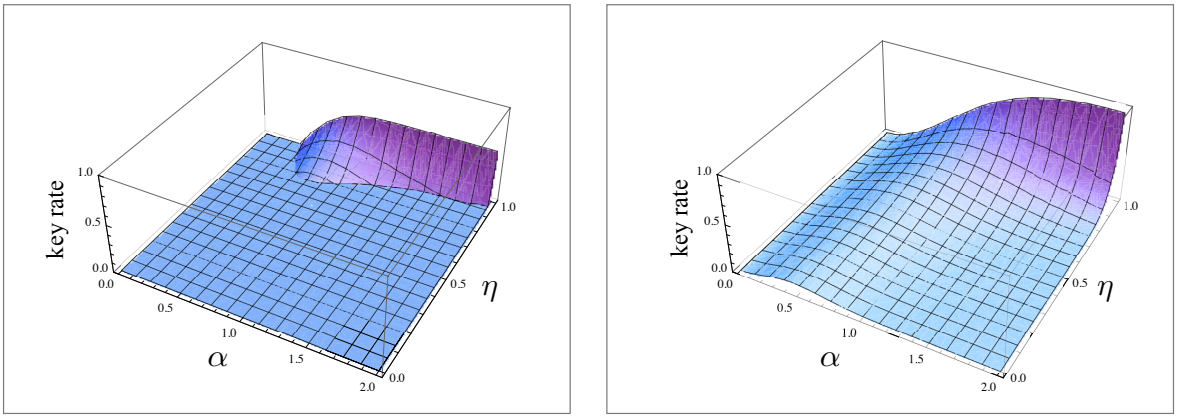
Beamsplitter attack on the 2-state protocol

The estimate of the key rate using the entropic uncertainty relation (Eq. 8.11) is a lower bound of the Devetak-Winter key rate in Eq. (8.10). Since there is a " $\geq$ " sign in the entropic uncertainty relation, it is possible that this bound is not tight in all cases. In this section, we investigate the size of the gap between the bound using the entropic uncertainty relation and the Devetak-Winter formula on an example, where we model Eve's interaction by a beamsplitter.

The security proof of the 2-state protocol under the assumption of a beamsplitter attack using the Devetak-Winter proof is found in Ref. [44]. Eve's interaction with the signal states $|\pm\alpha\rangle$ is modelled by a beamsplitter with transmissivity η that transforms $|\pm\alpha\rangle \to |\pm\sqrt{\eta}\alpha\rangle_B \otimes |\pm\sqrt{\eta}\alpha\rangle_E$. Eve keeps system E for herself, and sends system B to Bob. After this interaction, in the source-replacement scheme, the state shared between Alice, Bob and Eve is the pure state

$$|\Psi\rangle_{ABE} = \frac{1}{\sqrt{2}}\Big(|0\rangle_A \otimes |\sqrt{\eta}\alpha\rangle_B \otimes |\sqrt{1-\eta}\alpha\rangle_E + |1\rangle_A \otimes |-\sqrt{\eta}\alpha\rangle_B \otimes |-\sqrt{1-\eta}\alpha\rangle_E\Big). \tag{8.51}$$

We calculate the bound on the key rate using the entropic uncertainty relation in Eq. (8.46) and compare it to the Devetak-Winter key rate obtained in Ref. [44]. To obtain the bound, we compute the entropy $H(P_B|A)$ using the decomposition in Eq. (8.48) for a given state $|\Psi\rangle_{ABE}$. The only term missing in the decomposition is the entropy $S(A|P_B)$, which is given in terms of the eigenvalues $\lambda_\pm = \frac{1}{2}(1 \pm e^{-2(1-\eta)|\alpha|^2})$ of the conditional states



(a) (b)

Figure 8.1: Two bounds on the key rate of the 2-state protocol under the assumption of a beamsplitter attack for different values of α and η. (a) The bound obtained using the entropic uncertainty relation. (b) The bound obtained using the Devetak-Winter key rate formula.

$\rho_A^{p_B}$ by

$$S(A|P_B) = \int dp_B \; p(p_B) \; h(\lambda_+) = h(\lambda_+). \tag{8.52}$$

The bound on the key rate using the uncertainty relation,

$$r_{\text{uncert}} = \log_2(2\pi) - H(P_B|A) - H(X_B|M_A) \tag{8.53}$$

$$= \log_2(2\pi) - \left(\frac{1}{e\sqrt{\text{Var}_x \text{Var}_p}} \right) + h(\mu_+) - h(\lambda_+), \tag{8.54}$$

and the key rate r_{DW} obtained with the Devetak-Winter key rate formula in Ref. [44] are plotted in Fig. 8.1 for different values of α and η. As expected, the difference $r_{DW} - r_{\text{uncert}} \geq 0$ at each point, which can be seen in Fig. 8.2. In certain regions, the gap between r_{DW} and r_{uncert} is as large as 0.4 bits per signal.

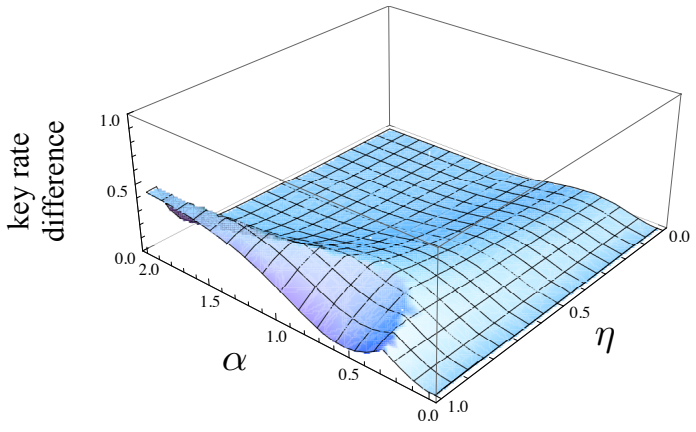


Figure 8.2: A plot of the difference $r_{DW} - r_{\text{uncert}}$ for different values of α and η.

8.4 Conclusion

In this chapter, we used the entropic uncertainty principle as a tool to calculate key rates of continuous-variable QKD protocols with reverse reconciliation. We demonstrated the performance of the new tool on the example of two protocols: first, we analyzed a Gaussian protocol with squeezed coherent states, which is the continuous-variable counterpart of the BB84 protocol, and second we analyzed the 2-state protocol, which uses two coherent states with opposite phases as signal states. For the former protocol it turns out that a minimum amount of squeezing must be observed in order to obtain a positive key rate, if following a proof using the uncertainty principle. For the latter protocol the estimation of Eve's information was not sufficient to prove a positive key rate. The reasons that no positive key could be established are

1. The key rate was found to be negative when we estimated the entropy $H(P_B|A)$ by $H(P_B|M_A)$.

2. One would need an estimate of $H(P_B|A)$ based on Bob's fist and second moments. To our knowledge there is no such estimate.

Chapter 9

Concluding remarks

In this thesis we analyzed the security of different protocols. We were able to prove the security and analyze the performance in realistic implementations for a number of protocols. For others, we explored new security proof methods and compared them to existing methods.

In order to simplify key rate calculations, it is beneficial to know if the optimal attack carries the symmetry of the the signal states of the underlying protocol. We answer the question under what conditions this claim is true in the Devetak-Winter security proof framework in Chapter 4. We work in the scenario where the parameter estimation is based on coarse-grained quantities, typically the error rate. Not only the measurements, but also the postselection needs to exhibit a certain symmetry in order to prove a symmetric optimal attack. Protocols with sets of orthonormal bases as signal states and a postselection on matching bases satisfy these conditions. Using these tools we were able to analyze the security of protocols with mutually unbiased bases on d-dimensional Hilbert spaces, and identify qubit protocols which have the same optimal attack as the BB84 or 6-state protocol.

In Chapter 5, we study the question if the optimal eavesdropping and the optimal cloning transformation coincide in the Devetak-Winter framework. We restrict our study to protocols where the optimal attack can be proven to be symmetric, such as protocols with orthonormal bases. We found that the optimal cloning transformation is drawn from the same set of symmetric transformations as the optimal eavesdropping transformation, if the optimal cloner has a strong covariant realization. However, this condition alone does not guarantee that the transformations are equivalent, unless the set of symmetric transformations contains only one transformation. Moreover, no general rule was found

to determine the answer to our question. Specific examples of protocols with n mutually unbiased bases in d dimensions demonstrate that for some cases the optimal attack is an optimal cloner ($n = 2, d + 1$), and for other cases it is not ($n = d$).

We prove the security of the unbalanced phase-encoded BB84 protocol with a lossy phase modulator under implementation of Decoy states in Chapter 6. The typical BB84 signal states and measurements are no longer guaranteed if the phase modulator is lossy. We propose two experimental remedies that restore conditions for which the BB84 security proof holds, but also provide a refined security proof taking into account the modified signal and measurement structure. Our security proof is a qubit-to-qubit security proof embedded into the more general framework of realistic devices using standard techniques. The unbalanced phase-encoded protocol exhibits enough symmetries in order to support the claim of a symmetric optimal attack for the qubit-to-qubit part. Using our security proof, we compare the performance of different protocols, which we characterize by the amount of loss in the phase modulator. We find that, as the loss increases, the performance of the protocols decreases. Therefore, the loss should not be ignored. Our results also suggest that the experimental remedies are not necessary to implement, because the refined analysis guarantees equal or better key rates. Comparing different security proof methods, we found that, for the typical range of observations, the standard BB84 security analysis yields the same result as our refined analysis. However, for protocols with a high loss in the phase modulator, in the range of hight error rates and low channel loss, our security analysis outperforms the BB84 analysis in terms of key rate.

Using the symmetry tools in Chapter 4, we were able to provide a security proof for a measurement-device-independent QKD setup with B92 signal states in Chapter 7. In the measurement-device-independent setup, Alice and Bob send quantum states to an adversary intermediate node held by Eve, that acts as the receiver. By making announcements for each obtained signal, Eve effectively prepares entanglement between Alice and Bob, who then extract a secret key using traditional QKD methods. If Eve must make a conclusive announcement for every signal, Alice and Bob can not establish a key, because the eavesdropping strategy can always be explained by a separable eavesdropping strategy. On the other hand, if Eve announces inconclusive results as well, the eavesdropping strategy is not forcedly a separable strategy. Therefore, a positive key rate can be achieved. However, the key rate of the MDI-B92 protocol is low, because the protocol is sensitive to channel loss, like the the B92 protocol with polarization encoding. Furthermore, the established MDI security proof acts as a new security proof technique for the strong reference pulse B92 protocol. Using the MDI security proof, we were able to outsource the measurement involving the strong reference pulse to Eve, making it part of the eavesdropping attack. Although we obtain positive key rates for the strong reference pulse B92 protocol, already existing

security proofs beat our results. Nevertheless, the MDI security proof is a promising new tool to provide security proofs for other protocols.

Finally, in Chapter 8, we establish security proofs based on the entropic uncertainty relation for continuous-variable protocols with reverse reconciliation. We demonstrate the new security proof method on two examples. In the example of a protocol with squeezed states and Gaussian modulation, a minimum amount of squeezing must be observed by Bob in order to obtain a positive key rate. In the second example of the discrete modulated 2-state protocol with coherent states, we were not able to establish positive key rates. The method failed because it was not possible to incorporate all observations into the estimation of Eve's knowledge, in particular, the second moments of Bob's observations. For known attacks, such as the beamsplitter attack, the security proof based on the entropic uncertainty relation leads to lower key rates than using the traditional Devetak-Winter security proof. Therefore, it is possible that the new method is not the optimal tool to prove the security of the 2-state protocol.

APPENDIX

Appendix A

Proofs of theorems and lemmas in Chapters 3 and 4

A.1 Proof of the weak convexity of the classical mutual information

In this appendix we prove Theorem 7 in Sec. 3.4.

Proof. The mutual information $I(\rho_{AB}, \mathbf{M}_{AB})$ depends only on the probability distribution $p(x, y)$. For $\bar{\rho}_{AB}$ the mutual information is explicitly given by $I(\bar{\rho}_{AB}, \mathbf{M}_{AB}) = H(\bar{p}(x)) - H(X|Y)_{\bar{p}}$, where $H(p(x)) = -\sum_x p(x) \log p(x)$ is the Shannon entropy, and $H(X|Y)_{\bar{p}} = \sum_{x,y} \bar{p}(x, y) \log \left(\frac{\bar{p}(x,y)}{\bar{p}(y)} \right)$ is the conditional entropy. The first term satisfies

$$H(\bar{p}(x)) = H(p(x)) = H(q(x)), \tag{A.1}$$

because $p(x) = q(x) = \bar{p}(x)$. The second term, the conditional entropy, is concave, namely

$$H(X|Y)_{\bar{p}} \leq \lambda H(X|Y)_p + (1 - \lambda) H(X|Y)_q, \tag{A.2}$$

where $H(X|Y)_p = -\sum_{x,y} p(x, y) \log \left(\frac{p(x,y)}{p(y)} \right)$ and similarly for $H(X|Y)_q$. The concavity of the conditional entropy is shown by applying the log sum inequality [27],

$$\left(\sum_i a_i \right) \log \left(\frac{\sum_j a_j}{\sum_k b_k} \right) \leq \sum_i a_i \log \left(\frac{a_i}{b_i} \right), \tag{A.3}$$

to $H(X|Y)_{\bar{p}}$. Eqs. (A.1) and (A.2) together imply the weak convexity of the classical mutual information.

■

A.2 Proof of the concavity of the Holevo quantity

In this appendix we prove Theorem 8 in Sec. 3.4. We will use the traditional notation

$$\chi(X:E)_{\rho_{XE}} := \sum_x p(x) S(\rho_E^x)$$

to denote the Holevo quantity of the cq state $\rho_{XE} = \sum_x p(x)|x\rangle\langle x| \otimes \rho_E^x$.

Proof. Given the states ρ_{AB} and σ_{AB} with purifications $|\Psi\rangle_{ABE'}$ and $|\Sigma\rangle_{ABE'}$ on the system $E = E'$. Alice measures the states with respect to the POVM elements A_x and stores the result in the system X. The cq states describing the situation for Alice and Eve after the measurement are

$$|\Psi\rangle \quad \to \rho_{XE'} = \sum_x p(x)|x\rangle\langle x| \otimes \rho_{E'}^x, \tag{A.4}$$

$$|\Sigma\rangle \quad \to \sigma_{XE'} = \sum_x q(x)|x\rangle\langle x| \otimes \sigma_{E'}^x, \tag{A.5}$$

with Eve's conditional states $\rho_{E'}^x = \mathrm{tr}_{AB}\{A_x \otimes \mathbb{1}|\Psi\rangle\langle\Psi|\}/p(x)$ and $\sigma_{E'}^x = \mathrm{tr}_{AB}\{A_x \otimes \mathbb{1}|\Sigma\rangle\langle\Sigma|\}/q(x)$. The Holevo quantity of $\rho_{XE'}$ and $\sigma_{XE'}$ is given by

$$\begin{aligned} \chi(\rho_{AB}, \mathbf{M}_A)) &= \chi(X:E')_{\rho_{XE'}}, \\ \chi(\sigma_{AB}, \mathbf{M}_A)) &= \chi(X:E')_{\sigma_{XE'}}. \end{aligned} \tag{A.6}$$

We construct a particular purification on the joint system $E = E'F$ for the convex sum $\bar{\rho}_{AB} = \lambda\rho_{AB} + (1-\lambda)\sigma_{AB}$:

$$|\bar{\Psi}\rangle_{ABE'F} = \sqrt{\lambda}|\Psi\rangle|0\rangle_F + \sqrt{1-\lambda}|\Sigma\rangle|1\rangle_F. \tag{A.7}$$

After measuring $|\bar{\Psi}\rangle_{ABE'F}$ with respect to A_x, the state shared by Alice and Eve is

$$\bar{\rho}_{XE'F} = \sum_x \bar{p}(x)|x\rangle\langle x| \otimes \bar{\rho}_{E'F}^x \tag{A.8}$$

with Eve's conditional states $\bar{\rho}^x_{E'F} = \mathrm{tr}_{AB}\{A_x \otimes \mathbb{1}_{BE'F}|\bar{\Psi}\rangle\langle\bar{\Psi}|\}/\bar{p}(x)$ and $\bar{p}(x) = \lambda p(x) + (1-\lambda)q(x)$. The Holevo quantity of $\bar{\rho}_{XE'F}$ is

$$\chi(\bar{\rho}_{AB}, \mathbf{M}_A)) = \chi(X : E'F)_{\rho_{XE'F}}.$$

Let $\mathcal{M} : F \to F'$ be a trace-preserving quantum operation. For our purposes, we identify $\mathcal{M}$ with a measurement on F in the standard basis $\{|0\rangle, |1\rangle\}$ and write the outcome in a new register F'. By defining $\lambda_x = \lambda\frac{p(x)}{\bar{p}(x)}$, the state after the measurement is given by

$$\rho_{XE'F'} = \sum_x \bar{p}(x)|x\rangle\langle x| \otimes [\lambda_x \rho^x_{E'} \otimes |0\rangle\langle 0|_{F'} + (1-\lambda_x)\sigma^x_{E'} \otimes |1\rangle\langle 1|_{F'}]. \tag{A.9}$$

Let us state a lemma about the Holevo quantity extracted from a state of the form $\rho_{XE'F'}$:

Lemma 8 *The Holevo quantity extracted from $\rho_{XE'F'}$ satisfies*

$$\chi(X : E'F')_{\rho_{XE'F'}} \geq \lambda\chi(X : E')_{\rho_{XE'}} + (1-\lambda)\chi(X : E')_{\sigma_{XE'}},$$

with $\chi(X : E')_{\rho_{XE'}}$ and $\chi(X : E')_{\sigma_{XE'}}$ given in Eq. (A.6). Equality holds, if the probabilities λ_x are independent of x, $\lambda_x = \lambda$.

Proof. From $\rho_{XE'F'}$ we calculate the Holevo quantity using the joint entropy theorem of the von Neuman entropy [73]

$$\chi(X : EF') = \lambda\chi(X : E')_{\rho_{XE'}} + (1-\lambda)\chi(X : E')_{\sigma_{XE'}} + h(\lambda) - \sum_x \bar{p}(x)h(\lambda_x),$$

with the binary entropy function $h(x) = -x\log(x) - (1-x)\log(1-x)$, and where $\chi(X : E')_{\rho_{XE'}}$ and $\chi(X : E')_{\sigma_{XE'}}$ are given in Eq. (A.6). From the concavity of the Shannon entropy it follows that $h(\lambda) - \sum_x \bar{p}(x)h(\lambda_x) \geq 0$, and in particular, if $\lambda = \lambda_x$ for all x, the equality holds. ■

According to Ref. [73], a map of the form $\mathcal{M} : F \to F'$ can only decrease the Holevo quantity:

$$\chi(X : E'F)_{\rho_{XE'F}} \geq \chi(X : E'F')_{\rho_{XE'F'}}. \tag{A.10}$$

Equation (A.10) together with Eq. (A.10), show that the desired result. ■

A.3 Proof of Lemma 3

In this appendix we prove Lemma 3 in Sec. 4.2.

Proof. We trace out system S from the source state $|\Phi\rangle_{AS}$ in equation (3.2) and identify Alice's reduced state ρ_A by

$$\rho_A = \sum_i \kappa_i |i\rangle\langle i| = \sum_x p(x)|\varphi_x\rangle\langle\varphi_x|. \tag{A.11}$$

From the G-invariance of the signal states and the uniform distribution of $p(x)$, it follows that ρ_A is also G-invariant. Since ρ_A is diagonal in the Schmidt basis $\mathcal{B}$ with real eigenvalues κ_i, it holds that

$$\rho_A^* = \rho_A.$$

Therefore, ρ_A is also G^*-invariance (where the complex conjugate is taken with respect to the Schmidt basis) as can be easily seen from $U_g^* \rho_A U_g^T = (U_g \rho_A U_g^\dagger)^* = \rho_A$.

Due to the positivity of the coefficients κ_i and the full rank of ρ_A, the square root $\sqrt{\rho_A}$ and the inverse ρ_A^{-1} are well-defined. The G- and G^*-invariance of ρ_A^{-1} can be straightforwardly verified: $U_g \rho_A^{-1} U_g^\dagger = (U_g \rho_A U_g^\dagger)^{-1} = \rho_A^{-1}$, and similarly for the G^*-invariance.

In Ref. [25], it is shown for permutation groups, that for every positive G-invariant operator ρ_A, $\sqrt{\rho_A}$ is also G-invariant. The same proof applies also here, and thus, the G- and G^*-invariance of ρ_A also implies the G- and G^*-invariance of $\sqrt{\rho_A}$.

By using the G-invariance of the signals states, and the G^*-invariance of $\sqrt{\rho_A}$ and ρ_A^{-1}, the G^*-invariance of A_x follows directly from the definition in Eq. (3.3).

References

[1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, 2007.

[2] A. Acín, N. Gisin, and V. Scarani. Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks. *Phys. Rev. A*, 69:012309, 2004.

[3] Michael Artin. *Algebra*. Prentice Hall Inc., 1991.

[4] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, and F. Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34(4):512–528, 2008.

[5] Normand J. Beaudry, Tobias Moroder, and Norbert Lütkenhaus. Squashing models for optical measurements in quantum communication. *Phys. Rev. Lett.*, 101:093601, 2008.

[6] H. Bechmann-Pasquinucci and N. Gisin. Incoherent and coherent eavesdropping in the 6-state protocol of quantum cryptography. *Phys. Rev. A*, 59:4238–4248, 1999.

[7] H. Bechmann-Pasquinucci and A. Peres. Quantum cryptography with 3-state systems. *Phys. Rev. Lett*, 85(15):3313–3316, 2000.

[8] Bengtsson and Życzkowski. *Geometry of Quantum States*. Cambridge University Press, 2006.

[9] C. H. Bennett, F. Bessette, L. Salvail, G. Brassard, and J. Smolin. Experimental quantum cryptography. *J. Cryptology*, 5:3–28, 1992.

[10] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India*, pages 175–179, New York, dec 1984. IEEE.

[11] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M. Renes, and Renato Renner. The uncertainty principle in the presence of quantum memory. *Nature Physics*, 6:659–662, 2010.

[12] Stephen Boyd and Lieven Vandenberghe. *Convex Optimization*. Cambridge University Press, Cambridge, 2004.

[13] S. Braunstein and P. van Loock. Quantum information with continuous variables. *Reviews of Modern Physics*, 77(2):513–577, 2005.

[14] S. L. Braunstein and S. Pirandola. Side-channel-free quantum key distribution. *Physical Review Letters*, 108(13), 2012.

[15] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81:3018–3021, 1998.

[16] D. Bruß. Optimal eavesdropping in cryptography with three-dimensional quantum states. *Phys. Rev. Lett.*, 88(12), 2002.

[17] P.H. Butler. *Point group symmetry applications: methods and tables*. Plenum Press New York, London, 1981.

[18] V. Bužek and M. Hillery. Quantum copying: Beyond the no-cloning theorem. *Phys. Rev. A*, 54:1844–1852, 1996.

[19] F. Caruso, H. Bechmann-Pasquinucci, and C. Macchiavello. Robustness of a quantum key distribution with two and three mutually unbiased bases. *Phys. Rev. A*, 72(3):32340, 2005.

[20] N. J. Cerf. Asymmetric quantum cloning in any dimension. *Mod. Opt. J.*, 47:187, 2000.

[21] N. J. Cerf. Pauli cloning of a quantum bit. *Phys. Rev. Lett.*, 84:4497, 2000.

[22] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.*, 88:1279902, 2002.

[23] N. J. Cerf, M. Levy, and G. Van Assche. Quantum distribution of gaussian keys using squeezed states. *Phys. Rev. A*, 63:052311, 2001.

[24] G. Chiribella, G. M. D'Ariano, P. Perinotti, and N. J. Cerf. Extremal quantum cloning machines. *Phys. Rev. A*, 72(4):42336, 2005.

[25] M. Christandl, R. König, G. Mitchison, and R. Renner. One-and-a-half quantum de Finetti theorems. *Communications in Mathematical Physics*, 273(2):473–498, 2007.

[26] M. Christandl, R. König, and R. Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Physical Review Letters*, 102(2), 2009.

[27] T.M. Cover and J.A. Thomas. *Elements of information theory*. John Wiley and sons, 2006.

[28] M. Curty, M. Lewenstein, and N. Lütkenhaus. Entanglement as precondition for secure quantum key distribution. *Phys. Rev. Lett.*, 92:217903, 2004.

[29] Marcos Curty and Norbert Lütkenhaus. Intercept-resend attacks in the bennett-brassard 1984 quantum-key-distribution protocol with weak coherent pulses. *Phys. Rev. A*, 71:062301, Jun 2005.

[30] G. M. D'Ariano and P. Lo Presti. Optimal nonuniversally covariant cloning. *Phys. Rev. A*, 64(4):042308, 2001.

[31] I. Devetak and A. Winter. Distillation of secret key entanglement from quantum states. *Proc. of the Roy. Soc. of London Series A*, 461(2053):207–235, 2005.

[32] T. Durt, N. J. Cerf, N. Gisin, and M. Żukowski. Security of quantum key distribution with entangled qutrits. *Phys. Rev. A*, 67(1):012311, 2003.

[33] T. Durt, D. Kaszlikowski, J.-L. Chen, and L. C. Kwek. Security of quantum key distributions with entangled qudits. *Phys. Rev. A*, 69(3):032313, 2004.

[34] A. Ferenczi and N. Lütkenhaus. Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning. *Phys. Rev. A*, 85(5):052310, 2012.

[35] A. Ferenczi, V. Narasimhachar, and N. Lütkenhaus. Security proof of the unbalanced phase-encoded bennett-brassard 1984 protocol. *Physical Review A*, 86(4), 2012.

[36] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres. Optimal eavesdropping in quantum cryptography. *Phys. Rev. A*, 56(2):1163–1176, 1997.

[37] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Physical Review Letters*, 109(10):100502, 2012.

[38] N. Gisin and S. Massar. Optimal quantum cloning machines. *Phys. Rev. Lett.*, 79:2153–2156, 1997.

[39] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145, 2002.

[40] C. Gobby, Z.L. Yuan, and A.J. Shields. Quantum key distribution over 122km of standard telecom fiber. *Appl. Phys. Lett.*, 84:3762–3764, 2004.

[41] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quant. Inf. Comp.*, 4(5):325, 2004.

[42] D. Gottesman and J. Preskill. Secure quantum key distribution using squeezed states. *Phys. Rev. A*, 63:022309, 2001.

[43] F. Grosshans. Collective attacks and unconditional security in continuous variable quantum key distribution. *Phys. Rev. Lett.*, 94(020504):020504, 2005.

[44] M. Heid and N. Lütkenhaus. Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction. *Phys. Rev. A*, 73:052316, 2006.

[45] C. W. Helstrom. *Quantum detection and estimation theory.* Academic Press, New York, 1976.

[46] M. Hillery. Quantum cryptography with squeezed states. *Phys. Rev. A*, 61:022309, 2000.

[47] M. Horodecki, P. W. Shor, and M. B. Ruskai. Entanglement breaking channels. *Rev. Mod. Phys.*, 15:629, 2003.

[48] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson. Practical free-space quantum key distribution over 10 km in daylight and at night. *New J. Phys.*, 4:43, 2002.

[49] W.-Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett*, 91:57901, 2003.

[50] H. Inamori. Security of practical time-reversed EPR quantum key distribution. *Algorithmica*, 34:340–365, 2002.

[51] H. Inamori, N. Lütkenhaus, and D. Mayers. Unconditional security of practical quantum key distribution. *Eur. Phys. J. D*, 2007.

[52] I. D. Ivanovic. Geometrical description of quantal state determination. *Journal of Physics A: Mathematical and General*, 14(12):3241–3245, 1981.

[53] I. D. Ivanovic. Unbiased projector basis over c3. *Phys. Lett. A*, 228(6):329–334, 1997.

[54] A. Jamiołkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Math. Phys.*, 3(4):275–278, 1972.

[55] Masato Koashi. Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse. *Physical Review Letters*, 93(12):120501, 2004.

[56] G.F. Koster, J.O. Dimmock, R.G. Wheeler, and H. Statz. *The Properties of the Thirty-Two Point Groups*. M.I.T. Press, Cambridge, Massachusetts, 1963.

[57] 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, Aug 2005.

[58] C. Kurtsiefer, P. Zarda, M. Halder, Weinfurter H., P. M. Gorman, P. R. Tapster, and J. G. Rarity. Quantum cryptography: A step towards global key distribution. *Nature*, 419:450, 2002.

[59] L.-P. Lamoureux and N. J. Cerf. Asymmetric phase-covariant d-dimensional cloning. *Quantum Inf. Comput.*, 5:32, 2005.

[60] H. Li, Z. Yin, Z. Han, W. Bao, and G. Guo. Security of practical phase-encoding quantum key distribution. *Quantum Information and Computation*, 10(9 & 10):771 – 779, 2010.

[61] H.-K. Lo, M. Curty, and B. Qi. Measurement-device-independent quantum key distribution. *Physical Review Letters*, 108(13), 2012.

[62] H.-K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, 2005.

[63] H.-K. Lo and J. Preskill. Security of quantum key distribution using weak coherent states with nonrandom phases. *Quant. Inf. and Comp.*, 7:431–458, 2007.

[64] S. Lorenz, J. Rigas, M. Heid, U. L. Andersen, N. Lütkenhaus, and G. Leuchs. Witnessing effective entanglement in a continuous variable prepare-and-measure setup and application to a quantum key distribution scheme using postselection. *Phys. Rev. A*, 74(4):042326, Oct 2006.

[65] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4:686, 2010.

[66] J. B. Maassen, H. Uffink. Generalized entropic uncertainty relations. *Physical Review Letters*, 60(12):1103–1106, 1988.

[67] D. Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In *Advances in Cryptology — Proceedings of Crypto '96*, pages 343–357, Berlin, 1996. Springer. Available as quant-ph/9606003.

[68] D. Mayers. Unconditional security in quantum cryptography. *JACM*, 48(3):351–406, May 2001.

[69] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. quant-ph/9809039, 1998.

[70] Willard Miller. *Symmetry groups and their applications.* Academic Press, New York, 1972.

[71] Varun Narasimhachar. Study of realistic devices for quantum key-distribution. Master's thesis, University of Waterloo, 200 University Ave. W., Waterloo, Ontario, Canada, N2L 3G1, 2011.

[72] Miguel Navascués and Antonio Acín. Security bounds for continuous variables quantum key distribution. *Phys. Rev. Lett.*, 94:020505, 2005.

[73] M. A. Nielsen and I. L Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[74] T. C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61:010303, 2000.

[75] Philippe Raynal and Norbert Lütkenhaus. Optimal unambiguous state discrimination of two density matrices: Lower bound and class of exact solutions. *Phys. Rev. A*, 72:022342, Aug 2005.

[76] R. Renner. Lecture notes on quantum information theory. http://www.itp.phys.ethz.ch/education/lectures_fs09/QIT/script_05.08.2009.pdf.

[77] R. Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zürich, 2005.

[78] R. Renner. Symmentry of large physical sysytems implies independance of subsystems. *Nature Physics*, 3:645–649, 2007.

[79] R. Renner and J. I. Cirac. de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Physical Review Letters*, 102(11), 2009.

[80] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72:012332, 2005.

[81] R. Renner and R. Konig. Universally composable privacy amplification against quantum adversaries. 3378:407–425, 2005.

[82] R. Renner and N. Lütkenhaus. Private discussion.

[83] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel. A quantum key distribution system immune to detector attacks. 04 2012.

[84] J. J. Sakurai. *Advanced quantum mechanics*. Pearson Education India, 2006.

[85] V. Scarani and R. Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical Review Letters*, 100(20), 2008.

[86] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81(3):1301–1350, Sep 2009.

[87] Lana Sheridan and Valerio Scarani. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A; Physical Review A*, 82(3), 2010.

[88] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, 2000.

[89] K. Tamaki, M. Koashi, and N. Imoto. Unconditionally secure key distribution based on two nonorthogonal states. *Phys. Rev. Lett.*, 90:167904, 2003.

[90] K. Tamaki and N. Lütkenhaus. Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel. *Phys. Rev. A*, 69:032316, 2004.

[91] K. Tamaki, N Lütkenhaus, M. Koashi, and J. Batuwantdawe. Unconditional security of the bennett 1992 quantum-key-distribution scheme with a strong reference pulse. *Physical Review A*, 80(3), 2009.

[92] Toyohiro Tsurumaru and Kiyoshi Tamaki. Security proof for quantum-key-distribution systems with threshold detectors. *Phys. Rev. A*, 78:032302, 2008.

[93] X. B. Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.*, 94:230503, 2005.

[94] Christian Weedbrook, Stefano Pirandola, Raul Garcia-Patron, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621–669, May 2012.

[95] W.K. Wootters and B.D. Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191(2):363–381, 1989.

[96] Y. B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus. Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. *Phys. Rev. A*, 79:012307, 2009.