Quantum key distribution with finite resources: Improving secret key rates

Inaugural-Dissertation

zur Erlangung des Doktorgrades
der Mathematisch-Naturwissenschaftlichen Fakultät
der Heinrich-Heine-Universität Düsseldorf

vorgelegt von

Markus Mertz
aus Merzig

Düsseldorf, Juli 2012

Aus dem Institut für Theoretische Physik, Lehrstuhl III
der Heinrich-Heine-Universität Düsseldorf

Gedruckt mit der Genehmigung der
Mathematisch-Naturwissenschaftlichen Fakultät der
Heinrich-Heine-Universität Düsseldorf

Referent: Prof. Dr. D. Bruß

Koreferent: Prof. Dr. J. Rothe

Tag der mündlichen Prüfung: 18. September 2012

Acknowledgement

I would like to use the opportunity to thank the following persons:

- *Prof. Dr. Dagmar Bruß* for her presence, advice and helpful critics.
- *Dr. Hermann Kampermann* for his permanent addressability and unerring oracle abilities.
- *Silvestre Abruzzo* and *Sylvia Bratzik* for their support in cryptographic questions.
- *Matteo Rossi*, *Dr. Zahra Shadman*, *Alexander Streltsov*, *Dr. Colin Wilmott*, *Junyi Wu* and all other group members for an excellent social climate.
- *Jens Bremer* for the immediate help concerning computer problems.
- *Cornelia Glowacki* for the help in administrative questions.
- My *family* for the help in all areas.

Abstract

Quantum key distribution (QKD) aims at the establishment of a shared secret key between two parties Alice and Bob, who are connected via a quantum channel and an authenticated classical channel. Traditionally, secure key rates were mainly calculated in the non-realistic case of infinitely many signals. Recently, QKD scenarios have been analyzed, where the number of signals sent through the channel is finite and the eavesdropper is not restricted to a specific attack. The challenge of this thesis is to develop strategies to optimize the secret key rate for finite quantum key distribution scenarios. We present two types of optimization methods.

First we modify the protocol by adding a pre-processing step, which may have beneficial effects on the secret key rate. More precisely, we investigate the effect of different noise scenarios on the achievable rate of an ε-secure key for the BB84 and six-state protocol under the assumption of collective attacks. We show that, on the one hand adding quantum noise deliberately may increase the secret key rate, and that on the other hand, under the realistic assumption that some noise is introduced by a real channel and is not dedicated to the eavesdropper, the secret key rate will increase significantly.

The second approach considers optimizations in the mathematical security analysis. Different types of entropy measures play a role in the analysis of finite QKD protocols. For example, the smooth min-entropy and Rényi entropies can be used to calculate the secret key rate for a finite QKD scenario. Since these entropies are very hard, or even impossible, to calculate for large dimensional systems, computable bounds on these entropies become very important. Besides the von Neumann entropy bound derived for tensor-product states, which leads for experimentally accessible situations to pessimistic secret key rates, and besides a very specific approach for the BB84 protocol, no further bounds are known. This thesis fills this gap: We calculate an achievable secret key rate for quantum key distribution with a finite number of signals, by bounding the smooth min-entropy by the min-entropy of a single-copy state. By an explicit evaluation of the min-entropy using its connecting to the guessing probability, we find non-zero key rates for a smaller number of signals in comparison to the von Neumann entropy approach. Another bound on the secret key rate is derived, which is expressed as an optimization problem over Rényi entropies. Under the assumption of collective attacks we develop a computable bound for the six-state protocol, which leads to improved secret key rates in comparison to previous results. Additionally, we develop a new method to quantify the secret key rate for permutation-invariant protocols for coherent attacks for finite

resources. By comparing the results to the well-known post-selection technique for the BB84 and six-state protocol, we show the high relevance of this method. Since the restriction to the class of permutation-invariant protocols is fairly weak, this underlines the wide importance of the results. In addition to the confirmation of the known equivalence of coherent and collective attacks for permutation-invariant protocols in the limit of infinitely many quantum signals, the results of this work may also give a hint that this equivalence might not hold in the regime of finite resources.

Zusammenfassung

Das Ziel der Quantenschlüsselverteilung ist die Erstellung eines sicheren Schlüssels, verteilt zwischen zwei Parteien Alice und Bob, die durch einen Quantenkanal und einen authentifizierten klassischen Kanal verbunden sind. Für gewöhnlich wurden sichere Schlüsselraten hauptsächlich in dem unrealistischen Fall von unendlich vielen Signalen berechnet. Erst kürzlich wurden Szenarien der Quantenschlüsselverteilung analysiert, die eine finite Anzahl an durch den Kanal versendeten Signalen betrachten und den Lauscher nicht auf eine spezifische Attacke einschränken. Die Herausforderung dieser Doktorarbeit ist es, Strategien zur Optimierung geheimer Schlüsselraten für die finite Quantenschlüsselverteilung zu entwickeln. Wir präsentieren zwei Arten von Optimierungsmethoden.

Zunächst modifizieren wir das Protokoll, indem wir einen vorbehandelnden Schritt hinzufügen, der nützliche Effekte auf die sichere Schlüsselrate haben kann. Genauer gesagt untersuchen wir den Effekt unterschiedlicher Rauschszenarien auf die erreichbare Rate eines ε-sicheren Schlüssels für das BB84- und 6-Zustand-Protokoll unter der Annahme von kollektiven Attacken. Wir zeigen, dass, auf der einen Seite absichtliches Hinzufügen von Rauschen zu einer Erhöhung der sicheren Schlüsselrate führen kann, und auf der anderen Seite erhöht sich die geheime Schlüsselrate deutlich unter der realistischen Annahme, dass ein realer Kanal Rauschen erzeugt, das nicht einem Lauscher zugesprochen werden muss.

Die zweite Vorgehensweise beinhaltet die Optimierung der mathematischen Sicherheitsanalyse. Unterschiedliche Arten von Entropien spielen bei der Analyse von finiter Quantenschlüsselverteilung eine Rolle. Zum Beispiel können die glatte Min-Entropie und die Rényi-Entropien zur Berechnung sicherer Schlüsselraten für finite Quantenschlüsselverteilung verwendet werden. Da diese Entropien aber für hochdimensionale Systeme sehr schwierig oder sogar unmöglich zu berechnen sind, werden berechenbare Abschätzungen für diese Entropien sehr wichtig. Neben der für Tensorproduktzustände hergeleiteten von-Neumann-Entropie-Abschätzung, die für experimentell zugängliche Situationen pessimistische geheime Schlüsselraten liefert, und neben einer sehr spezifischen Verfahrensweise für das BB84-Protokoll, sind keine weiteren Abschätzungen bekannt. Diese Lücke wird durch diese Doktorarbeit geschlossen: Wir berechnen eine erreichbare geheime Schlüsselrate für die Quantenschlüsselverteilung mit finiter Anzahl an Signalen, indem wir die glatte Min-Entropie durch die Min-Entropie eines Einzelkopiezustands abschätzen. Durch explizite Auswertung der Min-Entropie unter der Verwendung ihrer Verbindung zur Ratewahrscheinlichkeit finden wir nichtverschwindende Schlüsselraten schon für

weniger Signale als im Vergleich zum von-Neumann-Entropie-Ansatz. Eine weitere Abschätzung an die sichere Schlüsselrate wird hergeleitet, die sich als Optimierungsproblem über Rényi-Entropien darstellt. Unter der Annahme von kollektiven Attacken entwickeln wir eine berechenbare Abschätzung für das 6-Zustand-Protokoll, die zu verbesserten geheimen Schlüsselraten im Vergleich zu vorhergehenden Resultaten führt. Zusätzlich entwickeln wir eine neue Methode, geheime Schlüsselraten für pemutationsinvariante Protokolle für kohärente Attacken und finite Ressourcen zu quantifizieren. Durch einen Vergleich der Resultate mit der bekannten Post-selection-Technik für das BB84- und 6-Zustand-Protokoll wird die hohe Relevanz dieser Methode deutlich. Da die Einschränkung auf die Klasse der permutationsinvarianten Protokolle recht schwach ist, hebt dies die breite Wichtigkeit dieser Resultate hervor. Zusätzlich zu der Bestätigung der bekannten Äquivalenz zwischen kohärenten und kollektiven Attacken für permutationsinvariante Protokolle im Grenzfall unendlich vieler Quantensignale, geben die Resultate dieser Arbeit möglicherweise Hinweise darauf, dass diese Äquivalenz für den Fall finiter Ressourcen nicht mehr gewährleistet ist.

List of included publications

[A] Mertz, M., Kampermann, H., Shadman, Z., and Bruß, D. (submitted in May 2012). Quantum key distribution with finite resources: Taking advantage of quantum noise. *Physical Review A*.

[B] Mertz, M., Kampermann, H., Bratzik, S., and Bruß, D. (submitted in June 2012). Secret key rates for coherent attacks. *Physical Review A*.

[C] Bratzik, S., Mertz, M., Kampermann, H., and Bruß, D. (2011). Min-entropy and quantum key distribution: Nonzero key rates for "small" numbers of signals. *Physical Review A* 83, 022330.

[D] Abruzzo, S., Kampermann, H., Mertz, M., and Bruß, D. (2011). Quantum key distribution with finite resources: Secret key rates via Rényi entropies. *Physical Review A* 84, 032321.

Contents

Chapter 1.

Introduction

The need of private communication became very important in modern society. Cryptography is the science of secret communication. Secret communication is the private communication between a sender (usually called Alice) and a receiver (usually called Bob), without revealing any information to a spy or an eavesdropper (mostly called Eve).

A main criterion of cryptographic protocols is the security they can achieve. Here, security means the safeness of the communication between Alice and Bob with respect to a spy-attack of a third party. We distinguish between two kinds of security. The first one is called *computational* security. This relies on the computational power and the time which is needed to break the encryption code. That means, if the eavesdropper's computational power is high enough, she/he will be able to break the code after a certain time. The second type of security is called *unconditional* or *information-theoretic* security. As the name already implies, in contrast to the first type, this security is independent on computational power, times or memories. Unconditional security is also not conditioned on any assumptions about the eavesdropper's abilities.

A cryptographic protocol, which is unconditionally secure, has been found by Vernam [1] which is called "one-time pad". Alice transforms the original message, the so-called plain text, into an encrypted message, the so-called cipher text, by adding a key bitwise to the original message. After sending, Bob recovers the original message by an analogous addition of the identical key to his received ciphertext (see Figure 1.1 for an example). It has been shown by Shannon in [2] that this cryptographic protocol is unconditionally secure under the following assumptions: First, the key has to be completely random, second, the length of the key and the plaintext have to be equal and last, the key can only be used once. That means, once there is

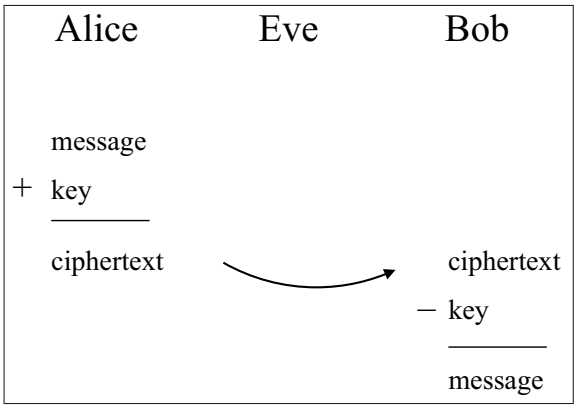

Figure 1.1.: Vernam's one-time pad: Alice encrypts her message by addition modulo two of the plaintext and the key. After sending to Bob, he decrypts the original message by addition modulo two of the ciphertext and the key.

a completely random shared key with the right length available, an unconditionally secure communication can be performed.

These important results of Vernam and Shannon shift the problem of classical cryptography to the secret-key generation. This is where quantum cryptography or more precisely quantum key distribution comes into play. Quantum key distribution is part of quantum information theory and aims at the generation of a completely random and shared secret key between two parties. In such a scenario (see Figure 1.2) Alice and Bob use a quantum channel (e.g. optical fiber or free space) and an authenticated classical channel. Authenticated means that Alice's and Bob's identity is confirmed and an eavesdropper can only listen to the information sent through the channel. The quantum channel is not restricted at all, i.e. in principle an eavesdropper can have full control of the channel. In a typical protocol Alice prepares a quantum state (e.g. photons) according to a randomly chosen bit and sends it to Bob, who measures the state and uses the outcome as a his bit. After many repetitions of this procedure, Alice and Bob have a long correlated bit-string each. During the transmission of the state, an eavesdropper can interfere to get information about the quantum state and consequently of the possible key. The easiest and most intuitive attack of an eavesdropper one might think of, is to intercept Alice's state, to copy the state and send the copy to Bob. In such a scenario, Eve would have the same information as Bob in the end. As a consequence the key would be completely insecure. This scheme is forbidden by the so-called no-cloning theorem [3], which states that non-orthogonal quantum states (this is provided by the protocol) cannot be copied or cloned perfectly. As a consequence, any interference of an eavesdropper

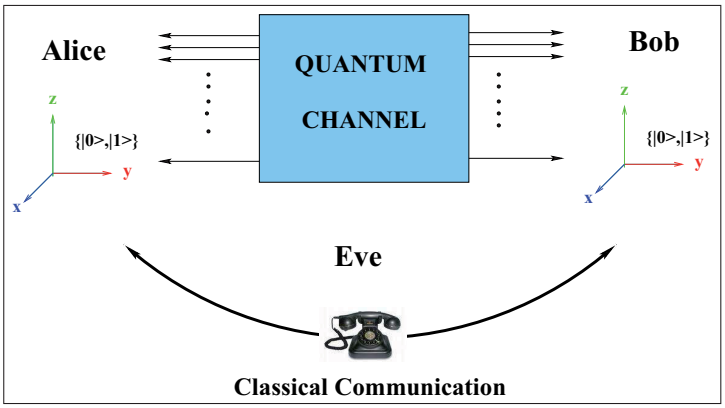

Figure 1.2.: Typical QKD setup.

on the non-orthogonal quantum states sent through the channel causes a disturbance on the state. This disturbance can be estimated by the two parties, Alice and Bob. If the disturbance is too high - which corresponds to a high gain of information for Eve and a low correlation in Alice's and Bob's bit-string- they abort the protocol and start a new trial. But if the amount of noise introduced by Eve is low, they can generate the desired secret key by a classical post-processing , with the use of classical communication.

In the year 1984 Bennett and Brassard invented the first protocol for QKD, the BB84 protocol [4]. The BB84 protocol is a prepare and measure protocol, as described above.A public comparison of a random sample of the bit-string enables them to estimate the error, which corresponds to the eavesdropper's gain of information. Nine years later Ekert presents a protocol that is based on entanglement [5]. Here Alice and Bob share an entangled state and they estimate the number of errors in their bit-strings by the violation of a Bell-inequality [6]. Already one year later the equivalence of these protocols has been proven in [7]. Up to now, the existing protocols used two bases for measurement. A generalization to a three-bases protocol appeared in [8, 9] by the invention of the six-state protocol. Many other protocols followed and many different security proofs came up in the literature [10, 11, 12, 13]. These works mostly consider the case of infinitely many signals, which are sent through the quantum channel to generate the secret key. Since this assumption is not realistic in experimental situations, security proofs for finite resources became necessary. It took until the year 2005 until Renner developed a complete framework for the security-analysis of QKD protocols for finite resources [14, 15]. Explicit calculations of secret-key rates followed for specific protocols [16, 17, 18, 19]. As a main result it turned out that the estimate of the secret key rate requires a minimal

number of signals of around 10^6 [20]. Since the aim is to transfer QKD schemes to real experimental setups, this number is rather high. The necessity to improve the bound on the secret-key rate for small initial number of signals becomes very important. Some recent works already treated this problem [21, 22] with significant success.

The aim of this work is to find methods that improve bounds on the secret key rate. More precisely, we want to decrease the minimal number of signals, which are necessary to generate a non-zero secret-key rate. There are two different ways for achieving it:

- Invent a new protocol that performs better than existing protocols or add new steps to known protocols, which are beneficial for the key generation.
- Improve the mathematical tools used for the security proofs and calculation of key rates. Since a main ingredient for security proofs is to find appropriate bounds on the maximal achievable secret key rate, there is space for improving secret key rates by finding better bounds or different proof strategies.

This thesis considers both methods. The first point is treated in Pub. A, where we investigate the influence on the secret-key rate by introducing different kinds of quantum noise to the quantum states. Pub. B, Pub. C and Pub. D are examples of the second item, where we develop formulas for the secret-key rates, which perform significantly better than previous bounds in specific scenarios.

The thesis is structured as follows: Chapter 2 introduces the mathematical framework, which is crucial for the analysis of quantum key distribution. Chapter 3 provides an introduction in quantum key distribution and shows how the previously presented mathematical tools apply to the analysis of secret key rates. A summary of the results of the thesis is given in Chapter 4 followed by an outlook in Chapter 5. After a list of main results in Chapter 6 and Appendix A the publications are attached in Publication A-D.

Chapter 2.

Mathematical framework

This chapter provides an introduction into the main mathematical tools needed for the analysis of the security of quantum key distribution presented in Chapter 3. It is inspired by standard introductory textbooks like for example [23] and [24].

2.1. Quantum states

In this thesis, in order to describe physical systems we use the density-operator formalism in finite Hilbert spaces. A density operator denoted by ρ is a positive semi-definite operator, which is normalized, i.e. $\mathrm{tr}\,(\rho) = 1$. We denote the set of density operators, also called quantum states, living in a Hilbert space $\mathcal{H}$ by $\mathcal{S}(\mathcal{H})$.

This formalism can be seen as a generalization of discrete probability theory. The correspondence of a discrete probability distribution in the density-operator formalism is called classical state and can be defined in the following way:

Definition 1. *Let $P_{\mathcal{Z}} : \mathcal{Z} \mapsto [0,1]$ be a probability distribution on $\mathcal{Z}$. Then we call the density operator $\rho_Z \in \mathcal{S}(\mathcal{H}^Z)$ defined by*

$$\rho_Z := \sum_{z \in \mathcal{Z}} P_Z(z) \left|z\right\rangle \left\langle z\right| \tag{2.1}$$

with an orthonormal basis $\{|z\rangle\}$ a classical state. Here a specific basis vector $|z\rangle$ in the density-operator language corresponds to the random variable z in the probability distribution.

Note that the fact that ρ_Z is a density operator directly follows from the normalization and positivity of the probabilities $P_Z(z)$.

Analogously we can define a classical quantum state, as a combination of classical state and quantum state:

Definition 2. *Let $P_{\mathcal{X}} : \mathcal{X} \mapsto [0,1]$ be a probability distribution on $\mathcal{X}$ and the $\rho_E^x \in \mathcal{S}(\mathcal{H}^E)$ be a quantum state, depending on the random variable x, $\forall x \in \mathcal{X}$. Then we call the density operator $\rho_{XE} \in \mathcal{S}(\mathcal{H}^X \otimes \mathcal{H}^E)$ defined by*

$$\rho_{XE} := \sum_{x \in \mathcal{X}} P_X(x) \left|x\right\rangle \left\langle x\right| \otimes \rho_E^x \tag{2.2}$$

a classical-quantum (cq-) state.

A specific case of such a cq-state is of course a classical-classical state, e.g.

$$\rho_{XY} := \sum_{x,y} P_{XY}(x,y) \left|x\right\rangle \left\langle x\right| \otimes \left|y\right\rangle \left\langle y\right|, \tag{2.3}$$

obtained for assuming a classical state on the second Hilbert space. These definitions are not restricted to the number of Hilbert spaces. One might think of an analogous definition to get for example ccq - states.

Extensions of quantum states to quantum states of larger systems occur quite frequently in quantum information theory. A specific extension is called purification.

2.2. Purification and partial trace

A possibility to categorize a density operator is given by its purity. We say a density operator $\rho \in \mathcal{H}$ is pure if and only if $\mathrm{tr}\left(\rho^2\right) = 1$. For $\mathrm{tr}\left(\rho^2\right) < 1$ we call the quantum state mixed. While an ideal quantum state, which describes an isolated and complete system, can be seen as a pure quantum state, any interaction with another quantum system leads to a mixed quantum state.

A very useful technique in quantum information theory is called purification and describes the purely mathematical transformation of a given state to a pure state in an extended Hilbert space:

Definition 3. *Let $\rho_A \in \mathcal{S}(\mathcal{H}^A)$ be a quantum state. Then we can find a pure quantum state ρ_{AB} on an extended Hilbert space $\mathcal{H}^A \otimes \mathcal{H}^B$, such that*

$$\mathrm{tr}_B\left(\rho_{AB}\right) = \rho_A. \tag{2.4}$$

We call the quantum state ρ_{AB} then a purification of ρ_A.

In other words, any mixed operator can be seen as a result from a partial-trace operation on a pure quantum state on an extended Hilbert space.

The process of purification is an unphysical process, i.e. it has no correspondence in reality. Any physical process can be described in quantum information theory by a trace-preserving completely positive map (TP-CPM).

2.3. Trace-preserving completely positive map (TP-CPM)

The evolution of quantum states in the quantum world can be described by channels, which map density operators from a Hilbert space $\mathcal{H}^A$ to density operators on a Hilbert space $\mathcal{H}^B$. As a consequence, these linear maps have to be restricted to properties, that guarantee the occurrence of a density operator after the application of the linear map, i.e. they have to be trace-preserving and preserve positivity. Additionally, since a quantum system can be seen as part of a larger joint quantum system, the map should, to be physical, also preserve positivity for any density operator on an extended Hilbert space:

Definition 4. *Let $\mathcal{H}^A, \mathcal{H}^B$ be Hilbert spaces. A linear map $\mathcal{M} : \mathcal{S}(\mathcal{H}^A) \mapsto \mathcal{S}(\mathcal{H}^B)$ is called trace-preserving completely positive (TP-CP) if for any auxiliary Hilbert space $\mathcal{H}^B$ the following properties are satisfied:*

- $\mathrm{tr}\left(\mathcal{M}(\rho_A)\right) = 1$ *with* $\rho_A \in \mathcal{S}(\mathcal{H}^A)$ *(Trace-preserving)*
- $\mathcal{M}(\rho_{AB}) \geq 0$ *with* $\rho_{AB} \in \mathcal{S}(\mathcal{H}^A \otimes \mathcal{H}^B)$ *(Complete positivity)*

Note that the positivity of the map, i.e. $\mathcal{M}(\rho_A) \geq 0$ is a direct consequence of the complete positivity.

A very useful and general way of representing any kind of TP-CP map has been developed in [25, 26] and is known as the Kraus-operator representation.

Lemma 1. *Let $\mathcal{H}^A, \mathcal{H}^B$ be Hilbert spaces and let $\mathcal{M} : \mathcal{S}(\mathcal{H}^A) \mapsto \mathcal{S}(\mathcal{H}^B)$ be a linear trace-preserving completely positive map. Then there exists a set of linear operators $\{M_k\}$ with $M_k : \mathcal{S}(\mathcal{H}^A) \mapsto \mathcal{S}(\mathcal{H}^B)\ \forall k$ and $\sum_k M_k^\dagger M_k = \mathbb{1}$, such that*

$$\mathcal{M}(\rho) = \sum_k M_k \rho M_k^\dagger \tag{2.5}$$

$\forall\ \rho \in \mathcal{S}(\mathcal{H}^A)$.

This kind of representation can give us a helpful intuition about the action of the channel. A well known example of a specific Kraus-operator representation is the so-called depolarizing channel, defined by:

Definition 5. *The action of a depolarizing channel $\mathcal{N}^p(\rho)$ is given by*

$$\mathcal{N}^p(\rho) := \sum_{i=1}^{4} A_i \rho A_i^\dagger \tag{2.6}$$

with the Kraus operators $A_1 = \sqrt{1-\frac{3}{4}p}\mathbb{1}, A_2 = \sqrt{\frac{p}{4}}\sigma_x, A_3 = \sqrt{\frac{p}{4}}\sigma_y, and A_4 = \sqrt{\frac{p}{4}}\sigma_z$. Here, σ_i are the Pauli-operators for $i \in \{x, y, z\}$.

A very important subset of TP-CP maps are the maps which represent the important measurement process, described by a positive operator-valued measurement ($POVM$).

2.4. Positive operator-valued measurement (POVM)

A measurement describes the interaction of an apparatus with the quantum system under study. It builds a bridge from the quantum states on the one side to the classical measurement outcomes observed by the apparatus on the other side. A measurement process can be seen as a specific trace-preserving completely positive map (see Definition 4). We denote this map as a positive operator-valued measurement, which is defined by:

Definition 6. *[27] A positive operator-valued measurement (POVM) on a Hilbert-space $\mathcal{H}^A$ is a set of positive measurement operators $\{M_x\}$, called $POVM$ elements with $\sum_x M_x = \mathbb{1}$. The corresponding measurement TP-CPM $\mathcal{M} : \mathcal{H}^A \mapsto \mathcal{H}^x$ is given by*

$$\mathcal{M}(\rho) := \sum_x \mathrm{tr}\left(M_x \rho\right) |x\rangle \langle x| . \tag{2.7}$$

The probability of the outcome belonging to the $POVM$ element M_x is given by $\mathrm{tr}\left(M_x \rho\right)$.

Theoretically, we can easily reduce the $POVM$ elements without changing the measurement by "grouping" some $POVM$ elements together and adjusting the probabilities.

Another key element in quantum information theory is the estimation of the distance between density operators. An appropriate distance is given by the trace distance.

2.5. Trace distance

In security proofs distance measures play a crucial role. In this thesis we use the trace distance as measure for the distance between two quantum states:

Definition 7. *Let ρ, σ be quantum states. Then we define the trace distance between ρ and σ as*

$$d(\rho, \sigma) := \frac{1}{2} ||\rho - \sigma||_1 \tag{2.8}$$

with $||A||_1 := \mathrm{tr}\left(\sqrt{AA^\dagger}\right)$.

For classical states $\rho_X := \sum_x P_X(x) |x\rangle \langle x|$ and $\sigma_X := \sum_x Q_X(x) |x\rangle \langle x|$ the distance is defined by

$$d(\rho_X, \sigma_X) := \frac{1}{2} \sum_x |P_X(x) - Q_X(x)|. \tag{2.9}$$

The exceptional position of the trace distance in comparison to other distance measures is due to a reasonable operational meaning: The trace distance between two quantum states can be interpreted as the maximal probability to distinguish the two quantum states by an arbitrary chosen measurement. More precisely:

Theorem 1. *[23] Let ρ, σ be quantum states and let the set $\{M_x\}$ be a $POVM$. Then*

$$d(\rho, \sigma) = \max_{\{\mathcal{M}_x\}} d\left(\mathrm{tr}\left(M_x \rho\right), \mathrm{tr}\left(M_x \sigma\right)\right) \tag{2.10}$$

Another useful property is that the trace distance cannot increase under quantum operations:

Lemma 2. *[23] Let ρ, σ be quantum states and let $\mathcal{M}$ be a TP-CP map, then*

$$d(\rho, \sigma) \geq d(\mathcal{M}(\rho), \mathcal{M}(\sigma)). \tag{2.11}$$

A main issue of the thesis is the optimization of quantities over quantum states having a distance ε to a reference quantum state:

Definition 8. *Let $\varepsilon > 0$ and ρ be a quantum state, then we define the ε-environment (or sometimes called ε-ball) of ρ by*

$$\mathcal{B}^\varepsilon(\rho) := \left\{ \sigma \in \mathcal{S}(\mathcal{H}) : \frac{1}{2} ||\rho - \sigma||_1 \leq \varepsilon \right\}. \tag{2.12}$$

If a quantum state is in the interior of such an ε-ball, we say the quantum state is ε-close to ρ.

In the following section we present the entropies, which are crucial for security analysis of quantum key distribution.

2.6. Entropies

A key quantity in quantum information theory and quantum key distribution is the entropy. It is used as a measure of information. One of the simplest known entropies for quantum states is the so called von Neumann entropy.

2.6.1. Von Neumann entropy

The von Neumann entropy is defined for quantum states in the following way:

Definition 9. *Let $\rho_A \in \mathcal{S}(\mathcal{H}^A)$, then we define the von Neumann entropy of ρ_A by*

$$S(A) \equiv S(\rho_A) := -\mathrm{tr}\left(\rho_A \log_2 (\rho_A)\right) \tag{2.13}$$

Since the entropy is zero for pure quantum states and maximal for fully mixed states, it can be seen as a measure of distance between the considered quantum state and a pure quantum state. Quantum information theory often treats problems where a party has some prior knowledge about some quantum state and one is interested in the remaining uncertainty about the system. This question can be answered by the conditional von Neumann entropy:

Definition 10. *Let $\rho_{AB} \in \mathcal{S}(\mathcal{H}^A \otimes \mathcal{H}^B)$ and $\rho_B \in \mathcal{S}(\mathcal{H}^B)$ with $\rho_B = \mathrm{tr}_A(\rho_{AB})$, then we define the von Neumann entropy of ρ_{AB} conditioned on B by*

$$S(A|B) := S(\rho_{AB}) - S(\rho_B) \tag{2.14}$$

In the case of classical states the von Neumann entropy reduces to the purely classical Shannon entropy [2]:

Definition 11. *Let $\rho_{XY} := \sum_{x\in\mathcal{X}, y\in\mathcal{Y}} P_{XY}(x,y) |x\rangle\langle x| \otimes |y\rangle\langle y| \in \mathcal{S}(\mathcal{H}^X \otimes \mathcal{H}^Y)$ be a cc-state and $\rho_Y = \sum_{y\in\mathcal{Y}} P_Y(y) |y\rangle\langle y| \in \mathcal{S}(\mathcal{H}^y)$ with $\rho_Y = \mathrm{tr}_X(\rho_{XY})$, then we define the Shannon entropy of ρ_{XY} conditioned on Y by*

$$H(X|Y) := H(\rho_{XY}) - H(\rho_Y) \tag{2.15}$$

with $H(\rho_Y) := -\sum_{y\in\mathcal{Y}} P_Y(y)\log_2 P_Y(y)$.

The application of these entropies are mainly related to asymptotic scenarios, which means that they are repeated infinitely many times. In real experiments this assumption is not realizable. This fact demands so-called one-shot (or single-shot) entropies, which quantify uncertainties in the case of finite runs of experiments. Possible entropies of such a kind are the Rényi entropies.

2.6.2. Rényi entropies

A generalization of the von Neumann entropy is given by the Rényi entropies [28]:

Definition 12. *Let* $\alpha \in \mathbb{R}_+^0 \bigcup \{\infty\}$ *and let* $\rho \in \mathcal{S}(\mathcal{H})$ *be a quantum state. Then the generalized Rényi entropy of order* α *is defined as*

$$S_\alpha(\rho) := \frac{1}{1-\alpha}\log_2\left(\mathrm{tr}\left(\rho^\alpha\right)\right). \tag{2.16}$$

Note that for $\alpha = 1$ we obtain the von Neumann entropy:

$$\lim_{\alpha\to 1} S_\alpha(\rho) = S(\rho). \tag{2.17}$$

Other specific Rényi entropies suitable for quantum key distribution are:

$$S_0(\rho) = \log_2\left(\mathrm{rank}(\rho)\right), \tag{2.18}$$

$$S_2(\rho) = \log_2\left(\mathrm{tr}\left(\rho^2\right)\right)\text{and} \tag{2.19}$$

$$S_\infty(\rho) := \lim_{\alpha\to\infty} S_\alpha(\rho) = -\log_2\left(\lambda_{\max}(\rho)\right) \tag{2.20}$$

where $\lambda_{\max}(\rho)$ denotes the maximal eigenvalue of ρ.

Since conditional entropies for single-shot scenarios are needed we have to generalize the Rényi entropies again to a conditional one-shot entropy, called min-entropy.

2.6.3. Min-entropy

The min-entropy was introduced by Renner [14]:

Definition 13. *Let $\sigma_{AE} \in \mathcal{S}(\mathcal{H}^A \otimes \mathcal{H}^E)$ and $\rho_E \in \mathcal{S}(\mathcal{H}^E)$ be quantum states. Then the min-entropy of σ_{AE} conditioned on system E is defined by*

$$H_{\min}(\sigma_{AE}|E) := \sup_{\rho_E \in \mathcal{S}(\mathcal{H}^E)} H_{\min}(\sigma_{AE}|\rho_E) \tag{2.21}$$

with

$$H_{\min}(\sigma_{AE}|\rho_E) := \sup\left\{\lambda \in \mathbb{R} : 2^{-\lambda}\mathbb{1}_A \otimes \rho_E - \sigma_{AE} \geq 0\right\}. \tag{2.22}$$

The rather complex definition of the min-entropy becomes more convenient when considering a very intuitive operational meaning derived in [29] for classical-quantum states.

Theorem 2. *[29] Let $\sigma_{XE} := \sum_{x\in\mathcal{X}} P_X(x)\,|x\rangle\langle x| \otimes \sigma_E^x \in \mathcal{S}(\mathcal{H}^X \otimes \mathcal{H}^E)$ be a classical-quantum state and let $\left\{M_x^E\right\}$ be a POVM acting on $\mathcal{H}^E$. Then*

$$H_{\min}(\sigma_{XE}|E) := -\log_2(p_{\text{guess}}) \tag{2.23}$$

with

$$p_{\text{guess}} := \max_{M_x^E} \sum_{x\in\mathcal{X}} P_X(x)\text{tr}\left(M_x^E \sigma_E^x\right). \tag{2.24}$$

The theorem states that the min-entropy of a cq-state corresponds to the maximal probability of correctly guessing the classical bits on system X while knowing system E.

In security proofs it turns out that the optimization of single-shot entropies in a small environment of a reference quantum state can help a lot to increase the secret key rate. Such optimizations of single-shot entropies are called smooth entropies.

2.6.4. Smooth entropies

Smooth entropies are defined as an optimization of one-shot entropies over an ε-environment to a reference quantum state. This generalization can be applied to the unconditional Rényi entropies as well as to the conditional min-entropy:

Definition 14. *[30] Let $\alpha \in \mathbb{R}_+^0 \bigcup \{\infty\}$ and let $\rho \in \mathcal{S}(\mathcal{H})$ be a quantum state. Then the smooth Rényi entropy of order α is defined as*

$$S_\alpha^\varepsilon(\rho) := \frac{1}{1-\alpha}\log\left(\inf_{\sigma \in \mathcal{B}^{\frac{\varepsilon}{2}}(\rho)} \left[\text{tr}\left(\sigma^\alpha\right)\right]\right). \tag{2.25}$$

Definition 15. *[14] Let $\sigma_{AE} \in \mathcal{S}(\mathcal{H}^A \otimes \mathcal{H}^E)$ and $\rho_E \in \mathcal{S}(\mathcal{H}^E)$ be quantum states. Then the smooth min-entropy of σ_{AE} conditioned on system E is defined by*

$$H_{\min}^{\varepsilon}(\rho_{AE}|E) := \sup_{\sigma_{AE} \in \mathcal{B}^{\frac{\varepsilon}{2}}(\rho_{AE})} \sup_{\rho_E} H_{\min}(\sigma_{AE}|\rho_E). \tag{2.26}$$

The cost of the advantage of these smooth entropies on secret key rates are difficulties in computation for large Hilbert spaces. More precisely, for quantum states of large Hilbert spaces it becomes computationally hard, or even impossible to calculate in particular the smooth min-entropy for arbitrary states. But in the case of tensor-product states, it is possible to circumvent this problem by bounding the smooth min-entropy by the conditional von Neumann entropy of a single quantum state. This property is called asymptotic equipartition property (AEP) and has been proven in [14]:

Theorem 3. *[14] Let $\varepsilon > 0$ and let $\rho_{XE} \in \mathcal{S}(\mathcal{H}^X \otimes \mathcal{H}^E)$ be a classical-quantum state. Then*

$$H_{\min}^{\varepsilon}\left(\rho_{XE}^{\otimes n}|\rho_E^{\otimes n}\right) \geq n\left(S(X|E) - (2\log_2(\operatorname{rank}(\rho_X)) + 3)\sqrt{\frac{\log_2(2/\varepsilon)}{n}}\right). \tag{2.27}$$

In the following chapter we apply the presented mathematical framework to quantum key distribution and show how the secret key rate can be analyzed for finite resources.

Chapter 3.

Quantum key distribution

The aim of quantum key distribution is to generate a secret key between two parties. In this chapter we introduce two quantum cryptography protocols, the BB84 [4] and the six-state protocol [8, 9]. Then we present a general generic setup for quantum key distribution and show how the mathematical tools defined in the previous chapter can be used in the security analysis.

3.1. BB84 and six-state protocol

In the BB84 protocol two parties, Alice and Bob, are connected via a quantum channel and an authenticated classical channel. Each party has an identical set of two conjugated bases $\{x, +\}$, where $|0_+\rangle$, $|1_+\rangle$ denote the orthogonal states in the $+$-basis, and $|0_x\rangle := \frac{1}{\sqrt{2}}(|0_+\rangle + |1_+\rangle)$, $|1_x\rangle := \frac{1}{\sqrt{2}}(|0_+\rangle - |1_+\rangle)$ denote the orthogonal states in the conjugated x-basis.

Alice creates a random bit (0 or 1) and encodes it in a quantum state according to a randomly chosen measurement basis ($+$ or x) (e.q. polarization of a photon) and sends the state via the quantum channel to Bob. Bob measures the state in a randomly chosen measurement basis and keeps the outcome. This process is repeated many times until Alice and Bob have a bit-string of a preferred length. Since quantum signals measured in different bases do not have correlations, they announce their choice of basis for each measurement publicly and discard the bits, which have been measured in different bases to get the "sifted" key. A possible scenario is shown in Table 3.1.

To check for an eavesdropper Alice and Bob calculate (by addition modulo 2) the $QBER := \sum_{i=1}^{m} \frac{a_i \oplus b_i}{m}$ ($a_i \in \{0,1\}$ and $b_i \in \{0,1\}$ denotes Alice's and Bob's bit-value at position i, respectively) of a random subset of the sifted key of size m to estimate

Alice's random bit	0	0	1	0	1	1	1	0
Alice's random basis	+	x	x	+	+	+	x	x
Bob's random basis	+	+	x	x	x	+	x	+
Bob's random bit	0	1	0	0	1	1	0	1
Basis comparison								
Sifted key Alice	0		1			1	1	
Sifted key Bob	0		0			1	0	

Table 3.1.: BB84 protocol.

the $QBER$ on their remaining bit-strings. If this estimate is too large, Alice and Bob abort the protocol. If not, they create a secret key via classical error correction [31, 32] and privacy amplification [33].

The six-state protocol can be seen as a generalization of the BB84 protocol to three bases. That means, Alice and Bob can choose randomly a measurement-basis from the extended set $\{+, x, y\}$, where the additional y-basis is defined via the orthogonal states $|0_y\rangle := \frac{1}{\sqrt{2}}(|0_+\rangle + i\,|1_+\rangle)$ and $|1_y\rangle := \frac{1}{\sqrt{2}}(|0_+\rangle - i\,|1_+\rangle)$. In comparison to the BB84 protocol, where Bob uses on average in only half of the cases a different basis than Alice, the sifting procedure reduces for the six-state protocol the initial number of bits on average to a fraction of $\frac{1}{3}$. But the addition of a third basis can have a beneficial impact on the achievable secret key rate.

To analyse the security of the BB84 and the six-state protocol it is useful to treat the protocols in a more general framework. This general framework leads to a typical generic QKD protocol, which is presented in the following section.

3.2. Generic quantum key distribution protocol

A quantum key distribution protocol consists of two parts: a quantum part, which describes the quantum state distribution between the two parties Alice and Bob and a classical part, which contains processes acting on the classical bit string resulting from measurements on the quantum state. The following description of a generic quantum key distribution protocol is inspired by [34].

3.2.1. State distribution

A quantum key distribution protocol starts with the distribution of quantum signals. We consider an entanglement-based view, where Alice and Bob share N (entangled) particle pairs, whose joint state we denote by ρ_{AB}^N. We allow the most powerful interaction an eavesdropper can perform by considering the quantum state after the distribution and interaction ρ_{ABE}^N to be pure. For clearness, we focus on protocols that use two-dimensional quantum systems (qubits).

The transition from quantum states to classical data is then done by measurements.

3.2.2. Measurement

Alice and Bob perform measurements on their parts of the shared quantum state by choosing randomly a basis out of a set, which they fixed in advance. The results are correlated classical strings of N bits. We denote the resulting ccq-state by ρ_{XYE}^N.

3.2.3. Sifting

Alice and Bob announce via public communication their choice of bases in each measurement and discard the bits of their string, which have been measured in different bases. This procedure reduces the number of bits to $N - n_s$, where n_s denotes the number of discarded bits.

Due to the interaction of an eavesdropper on the quantum state, the correlation in Alice's and Bob's bits needs to be high enough to generate a secret key. This can be verified by a procedure called parameter estimation.

3.2.4. Parameter estimation

Alice and Bob determine the statistics, e.g. the quantum bit error rate ($QBER$) of $m < N - n_s$ randomly chosen bits, denoted by Q_m and compare it to a previously fixed, maximally tolerated $QBER$ Q_{tol}. If $Q_m > Q_{\text{tol}}$, the protocol will be aborted, since a high error causes insufficient correlations in Alice's and Bob's bit strings. In the other case of $Q_m \leq Q_{\text{tol}}$ we can estimate the $QBER$ Q_∞, i.e. the parameter we would get in case of an ∞-fold measurement, i.e. [34, 18]

$$Q_\infty \leq Q_m + \zeta(\varepsilon_{\text{PE}}, |\chi|, m) \tag{3.1}$$

with $\zeta(\varepsilon_{\mathrm{PE}}, |\chi|, m) := \sqrt{\frac{\ln\left(\frac{1}{\varepsilon_{\mathrm{PE}}}\right)+|\chi|\ln(m+1)}{2m}}$. Here $\varepsilon_{\mathrm{PE}}$ denotes the probability that parameter estimation fails and $|\chi|$ denotes the number of $POVM$ elements needed to measure the $QBER$.

The more appropriate approach is to estimate the $QBER$ Q_n of the remaining n signals. This can be done by the following estimation [21]:

$$Q_n \leq Q_m + \xi(\varepsilon_{\mathrm{PE}}, n, m) \tag{3.2}$$

with $\xi(\varepsilon_{\mathrm{PE}}, n, m) := \sqrt{\frac{(n+m)(m+1)\ln(1/\varepsilon_{\mathrm{PE}})}{2m^2 n}}$ and the probability of failure $\varepsilon_{\mathrm{PE}}$.

Parameter estimation restricts the remaining state ρ^n_{XE} to $QBER$s, which are bounded by Eq. (3.1) or Eq. (3.2).

The errors in the remaining $N - n_s - m$ signals, estimated by Q_∞ or Q_n, have to be removed. This can be done by classical error correction.

3.2.5. Error correction

In order to correct the errors in Alice's and Bob's classical bit-string, they have to apply an error correction procedure that forces them to communicate publicly. The information, which is leaked during the public communication is given by [17]

$$\mathrm{leak}_{\mathrm{EC}} := n f_{\mathrm{EC}} H(X|Y) + \log_2\left(\frac{2}{\varepsilon_{\mathrm{EC}}}\right) \tag{3.3}$$

where $f_{\mathrm{EC}} > 1$ denotes the efficiency of the error correction protocol and $\varepsilon_{\mathrm{EC}}$ its probability of failure.

After correction of errors it is necessary to reduce the knowledge of a possible eavesdropper about the classical bit-string. This procedure is called privacy amplification.

3.2.6. Privacy amplification

Privacy amplification aims at the establishment of a secret key from a partially secure bit-string, i.e. a bit-string where an eavesdropper might have some information about. The number of secret bits l is then bounded by the uncertainty the adversary Eve has about the classical bit string X [14]:

$$l \leq H^{\bar{\varepsilon}}_{\min}(\rho^n_{XE}|E^n) + 2\log_2(2\varepsilon_{\mathrm{PA}}) \tag{3.4}$$

where ρ_{XE}^n denotes the classical quantum state consisting of the classical bit-string X and the eavesdropper's quantum ancilla. The failure probability of privacy amplification is determined by $\bar{\varepsilon} + \varepsilon_{\mathrm{PA}}$.

Another approach to bound the number of secret bits l is given by a combination of Rényi entropies [15]:

$$l \leq \sup_{\sigma_{XE}^n \in \mathcal{B}^{\bar{\varepsilon}}\left(\rho_{XE}^n\right)} \left[S_2\left(\sigma_{XE}^n\right) - S_0\left(\sigma_E^n\right)\right]. \tag{3.5}$$

The global optimization of both Rényi entropies can be circumvented by using the following bound [15, 35]:

$$l \leq S_2^{\varepsilon'}\left(\rho_{XE}^n\right) - S_0^{\varepsilon'}\left(\rho_E^n\right). \tag{3.6}$$

This is an immediate consequence of the following theorem [35]:

Theorem 4. *Let $\bar{\varepsilon} > 0$ and ε' such that*

$$\frac{\bar{\varepsilon}}{2} = \sqrt{\frac{\varepsilon'}{2} - \frac{3}{16}\varepsilon'^2} + \frac{\varepsilon'}{2}. \tag{3.7}$$

Then there exists a cq state $\bar{\rho}_{XE}^n \in \mathcal{B}^{\frac{\bar{\varepsilon}}{2}}\left(\rho_{XE}^n\right)$ such that

$$S_2\left(\bar{\rho}_{XE}^n\right) - S_0\left(\bar{\rho}_E^n\right) \geq S_2^{\varepsilon'}\left(\rho_{XE}^n\right) - S_0^{\varepsilon'}\left(\rho_E^n\right). \tag{3.8}$$

Remark. *The proof of Theorem 4 is inspired by [15] and modified in [35]. A fundamental ingredient of the proof is the following Lemma 3, whose detailed proof was not shown in [35]. The extended proof can be found in Appendix A.*

Lemma 3. *Let $\rho_{AB} \in \mathcal{S}(\mathcal{H}^A \otimes \mathcal{H}^B)$ be a quantum state and P_B a general projector, i.e. $P_B^2 = P_B$ acting on $\mathcal{H}^B$ with the constraint $\mathrm{tr}\left(\rho_B P_B\right) = 1 - \frac{\varepsilon}{2} = \mathrm{tr}\left(\left(\mathbb{1}_A \otimes P_B\right)\rho_{AB}\right)$, then*

$$\max_{P_B} \frac{1}{2}\left|\left|\rho_{AB} - \left(\mathbb{1}_A \otimes P_B\right)\rho_{AB}\left(\mathbb{1}_A \otimes P_B\right)\right|\right|_1 = \sqrt{\frac{\varepsilon}{2} - \frac{3}{16}\varepsilon^2} \tag{3.9}$$

The run of such a typical quantum key distribution protocol in the regime of finite resources has always a non-zero probability of failure.A definition of security is provided in the following section.

3.3. Security

The definition of security for a quantum key distribution protocol has two properties [14]:

- Correctness: The generated key for Alice and Bob is the same.
- Secrecy: The generated key is uniformly distributed and independent on the knowledge of an eavesdropper.

In the regime of finite resources this perfect security cannot be maintained in general. The protocols can then only be called almost secure, which means that with a small probability it can be insecure. More precisely, we define the contributions to security for finite resources in the following way:

Definition 16. *Let $\varepsilon > 0$, let X and Y denote the keys generated for Alice and Bob, respectively with length l. Let $\rho^l_{XE} = \sum_x P_X(x) |x\rangle\langle x| \otimes \rho^x_E$ be the real cq-output state of the protocol and let $\rho^{\text{perfect}}_{XE} := \sum_x \frac{1}{2^l} |x\rangle\langle x| \otimes \rho_E$ be the output state that represents a perfectly secret key. Then the protocol is called [14]*

- *ε-correct, if*
$$Pr[X \neq Y] \leq \varepsilon. \tag{3.10}$$
- *ε-secret, if*
$$\frac{1}{2} \left|\left| \rho^l_{XE} - \rho^{\text{perfect}}_{XE} \right|\right|_1 \leq \varepsilon. \tag{3.11}$$

It is an immediate consequence that in the limit of $\varepsilon \to 0$, we achieve perfect security.

The definition of security can be used to value the quality of a generated key rate.

3.4. Secret key rate

The secret key rate of a generic quantum key distribution protocol described in Sec. 3.2 is defined as the number l of secret bits divided by the initial number of signals N, i.e. $r := \frac{l}{N}$. The secrecy of such a protocol is bounded by the sum of the probabilities of failure of each subprotocol. By using the smooth min-entropy to quantify privacy amplification (see Eq. (3.4)), we get the following bound on the secret key rate:

Theorem 5. *[14, 34] Let $\bar{\varepsilon}, \varepsilon_{\text{PE}}, \varepsilon_{\text{EC}}, \varepsilon_{\text{PA}} > 0$ as defined in the previous sections. Then the rate $r = \frac{l}{N}$ of an*
$$\varepsilon := \bar{\varepsilon} + \varepsilon_{\text{PE}} + \varepsilon_{\text{EC}} + \varepsilon_{\text{PA}} \tag{3.12}$$
- secure key is given by
$$r = \frac{1}{N} \inf_{\text{PE}} \left(H^{\bar{\varepsilon}}_{\min}(\rho^n_{XE}|E^n) - \frac{\text{leak}_{\text{EC}}}{n} \right) + \frac{2}{N} \log_2(2\varepsilon_{\text{PA}}), \tag{3.13}$$

where $\inf_{\mathrm{PE}}$ *means a restriction on the* $QBER$ *due to parameter estimation (see Sec. 3.2.4).*

Analogously, we can bound the secret key rate using the smooth Rényi entropy approach for privacy amplification (see Eq. (3.6))

Theorem 6. *[15] Let* $\bar{\varepsilon}, \varepsilon_{\mathrm{PE}}, \varepsilon_{\mathrm{EC}}, \varepsilon_{\mathrm{PA}} > 0$ *as defined in the previous sections and let* ε' *such that*

$$\frac{\bar{\varepsilon}}{2} = \sqrt{\frac{\varepsilon'}{2} - \frac{3}{16}\varepsilon'^2} + \frac{\varepsilon'}{2}. \tag{3.14}$$

Then the rate $r = \frac{l}{N}$ *of an*

$$\varepsilon := \bar{\varepsilon} + \varepsilon_{\mathrm{PE}} + \varepsilon_{\mathrm{EC}} + \varepsilon_{\mathrm{PA}} \tag{3.15}$$

- secure key is given by

$$r = \frac{1}{N} \inf_{\mathrm{PE}} \left(S_2^{\varepsilon'}\left(\rho_{XE}^n\right) - S_0^{\varepsilon'}\left(\rho_E^n\right) - \frac{\mathrm{leak}_{\mathrm{EC}}}{n} \right) + \frac{2}{N} \log_2\left(2\varepsilon_{\mathrm{PA}}\right), \tag{3.16}$$

where $\inf_{\mathrm{PE}}$ *means a restriction on the* $QBER$ *due to parameter estimation (see Sec. 3.2.4).*

In practice, the secret key is generated by applying a two-universal hash-function to the raw key, such that the length of the output key is l and given by one of the previous formulas.

The computability of this formula strongly depends on the shape of the cq-state, for which the smooth entropies have to be evaluated. The main challenge is the optimization of quantum states in a high-dimensional Hilbert space. The optimization becomes much easier by a restriction to states, which provide a certain symmetry. This can be reached by restricting the eavesdropper to reasonable attacks.

3.4.1. Eavesdropping strategies

The interaction of an eavesdropper takes place in the quantum part of a quantum key distribution protocol, i.e. during the distribution of the N quantum signals. Due to quantum mechanics any interaction an eavesdropper can perform, can be mathematically formulated as a unitary operation. We consider two main types of unitary interactions: The collective attack and the coherent attack.

Collective attack

The restriction to collective attacks forces the eavesdropper to interact identically with each of the N distributed signals. Since no dependencies among the signals

can appear, the distributed quantum state can be written as a tensor-product state [36, 37]:

$$\rho_{AB}^{N} = \rho_{AB}^{\otimes N}. \tag{3.17}$$

This tensor-product structure enables us to apply the asymptotic equipartition property of the smooth min-entropy (Eq. (2.27)) to Eq. (3.13) to end up in a calculable formula:

Theorem 7. *[14, 34] Let $\bar{\varepsilon}, \varepsilon_{\mathrm{PE}}, \varepsilon_{\mathrm{EC}}, \varepsilon_{\mathrm{PA}} > 0$. Then the rate $r = \frac{l}{N}$ of an*

$$\varepsilon := \bar{\varepsilon} + \varepsilon_{\mathrm{PE}} + \varepsilon_{\mathrm{EC}} + \varepsilon_{\mathrm{PA}} \tag{3.18}$$

- secure key is given by

$$r = \frac{n}{N} \inf_{\mathrm{PE}} \left(S(X|E) - 5\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}} - \frac{\mathrm{leak}_{\mathrm{EC}}}{n} \right) + \frac{2}{N} \log_2(2\varepsilon_{\mathrm{PA}}). \tag{3.19}$$

Coherent attack

Coherent attacks do not provide any restrictions on the eavesdropper's interaction. But the consideration of permutation-invariant protocols (permutational invariance means invariant under permutation of N qubit pairs) causes a helpful symmetry in the distributed quantum state. A The assumption of a protocol to be permutation-invariant is not a strong restriction, since many experimentally used protocols, like e.g. the BB84 protocol, can be made permutation-invariant by the addition of a step, which randomly permutes the classical bit-strings, to the initial protocol. The quantum state can be written as a convex combination of Bell-diagonal quantum states [36, 37]:

$$\rho_{AB}^{N} = \sum_{\mathbf{n} \in \Gamma^N} \mu_{\mathbf{n}} \mathcal{P}_N \left(\sigma_1^{\otimes n_1} \otimes \sigma_2^{\otimes n_2} \otimes \sigma_3^{\otimes n_3} \otimes \sigma_4^{\otimes n_4} \right) \tag{3.20}$$

with probabilities $\mu_{\mathbf{n}}$ and

$$\Gamma^N := \left\{ \mathbf{n} = (n_1, n_2, n_3, n_4) : \sum_{i=1}^{4} n_i = N \right\}. \tag{3.21}$$

The σ_i for $i = 1,..,4$ correspond to the projector onto the 4 Bell-states in $\mathcal{H}_A \otimes \mathcal{H}_B$, i.e.

$$\begin{aligned} \sigma_1 &= \left|\phi^+\right\rangle\left\langle\phi^+\right| \\ \sigma_2 &= \left|\phi^-\right\rangle\left\langle\phi^-\right| \\ \sigma_3 &= \left|\psi^+\right\rangle\left\langle\psi^+\right| \\ \sigma_4 &= \left|\psi^-\right\rangle\left\langle\psi^-\right|, \end{aligned} \tag{3.22}$$

with

$$\left|\phi^\pm\right\rangle := \frac{1}{\sqrt{2}}\left(|0,0\rangle \pm |1,1\rangle\right) \qquad \text{and} \tag{3.23}$$

$$\left|\psi^\pm\right\rangle := \frac{1}{\sqrt{2}}\left(|0,1\rangle \pm |1,0\rangle\right). \tag{3.24}$$

$\mathcal{P}_N$ denotes the completely positive map (CPM) which symmetries the state with respect to all possible distinguishable permutations of N qubit pairs.
This symmetry permits to find strategies which analyze secret key rates for coherent attacks.

In the next chapter we summarize the results of the publications A-D. There we make statements about collective as well as coherent attacks.

Chapter 4.

Summary of results

In this chapter we summarize the results of the thesis and point out their individual connection to the global aim of improving secret key rates for finite resources in quantum key distribution. The results can be categorized in two different strategies: In Sections 4.3-4.4 and 4.2 improvements in the mathematical analysis of secret key rates are presented, while Section 4.1 considers a modification of known protocols to improve the secret key rate.

4.1. The influence of quantum noise on the secret key rate for finite resources

In Pub. A the effect of different noise scenarios on the secret key rate is compared for the BB84 and six-state protocol for finite resources under the assumption of collective attacks. The noise is simulated by a depolarizing channel (see Eq. (2.6)). The noise scenarios differ in the position where the noise is added to the initial entangled state shared by Alice and Bob:

- Noise scenario 1: Alice adds depolarizing quantum noise to her part of the initial state.
- Noise scenario 2: Alice adds depolarizing quantum noise to Bob's part of the initial state.
- Noise scenario 3: Bob adds depolarizing quantum noise to his part of the state after receiving it.
- Noise scenario 4: Alice does probabilistic bit-flips on her classical bit string.

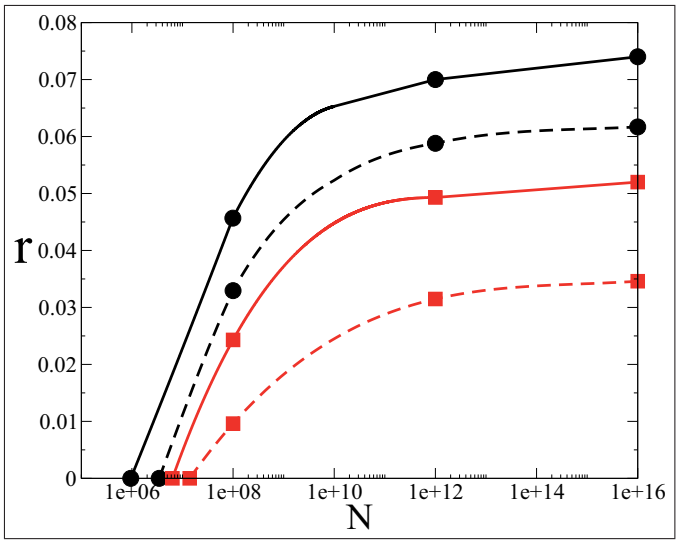

Figure 4.1.: Comparison of the finite-key rate versus signals N for a fixed $QBER$ D introduced by Eve for the BB84 protocol ($D = 0.1$) (circles (black)) and the six-state protocol ($D = 0.12$) (squares (red)); straight line: noise scenario 1 for optimal noise parameter, dashed line: no noise. Lines are drawn to guide the eye.

The equivalence of noise scenario 1, 2 and 4 is shown analytically. It turns out that, while noise scenario 3 has no benefit on the secret key rate, the other scenarios can in principle improve the key rate. More precisely, if we add noise deliberately, the secret key rate increases in comparison to the noiseless case (see Figure 4.1). The equivalence of noise scenario 1 and 2 allows us to interpret these results in another way: The noise can be seen as introduced by a given channel and not necessarily dedicated to an eavesdropper, which would be here an over-pessimistic assumption. The beneficial effect of dropping this assumption is shown in Figure 4.2. A detailed discussion of the results is provided in Pub. A.

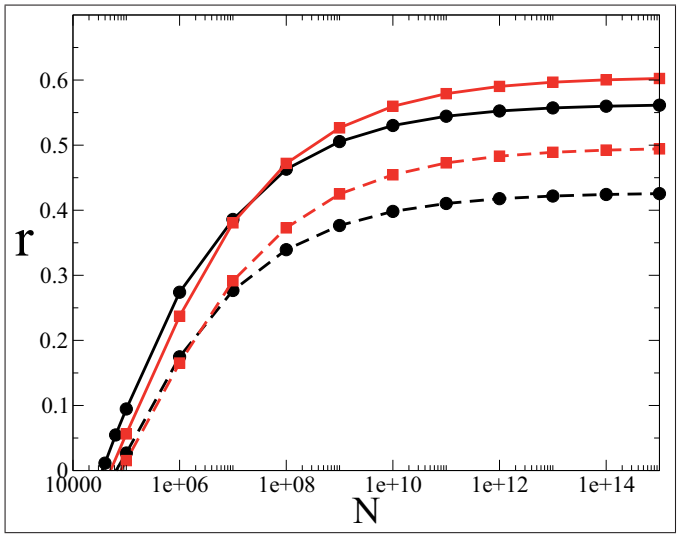

Figure 4.2.: Comparison of the finite-key rates ($\varepsilon = 10^{-9}$) versus number of signals N for various noise parameters p_b with $QBER = 5\%$ for the BB84 (circles (black)) and the six-state protocol (squares (red)); dashed lines: $p_b = 0$, straight lines: $p_b = 5\%$.

4.2. Secret key rates for coherent attacks

The main result of Pub. B is the derivation of a bound on the secret key rate for quantum key distribution with finite resources for coherent attacks. The bound considers the general class of permutation-invariant protocols and allows for coherent attacks. The new approach traces the calculation of the secret key rate for coherent attacks back to the evaluation for collective attacks, by bounding the smooth min-entropy of a permutation-invariant state (Eq. (3.20)) by the smooth min-entropy of a corresponding tensor-product state at the cost of some corrections, i.e.

$$H_{\min}^{\bar{\varepsilon}}\left(\rho_{XE}^{n}|E\right) \gtrsim H_{\min}^{\bar{\varepsilon}/n^{2}}\left(\sigma_{XE}^{\otimes n}|E\right) - 1. \tag{4.1}$$

These corrections confirm on the one hand the equivalence of collective and coherent attacks in the limit of infinitely many distributed quantum signals, but on the other hand may also give hints for their disparity in the finite case. A comparison to the post-selection technique [38], which is up to now the best known approach for treating coherent attacks for permutation-invariant protocols, shows the quality of the new bound. Figure 4.3 shows this comparison with respect to secret key rates for the BB84 protocol in reference to collective attacks. An analogous result has also been obtained in Pub. B for the six-state protocol.

A detailed derivation of the new bound and a further discussion of the results is done in Pub. B.

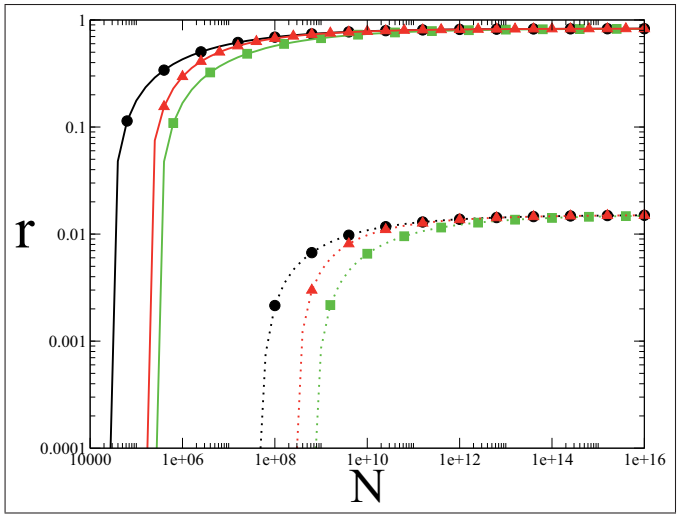

Figure 4.3.: Comparison of the secret key rates r for collective attack (black circles), the post-selection technique (green squares) and the new bound (red triangles) versus the number N of initial signals for different $QBER$s with security parameter $\varepsilon = 10^{-9}$ for the BB84 protocol in logarithmic scale; $QBER = 0.01$ (straight lines), $QBER = 0.1$ (dotted lines).

4.3. Non-zero key rates for "small" numbers of signals

As reviewed in Sec. 3.2.4, in the case of finite quantum key distribution, we have to estimate the quantum bit error rate due to the limited number of quantum signals. This estimation causes statistical fluctuations, which depend on the number of $POVM$ elements $|\chi|$ needed to measure the quantum bit error rate Q_m:

$$Q_\infty \leq Q_m + \zeta(\varepsilon_{\mathrm{PE}}, |\chi|, m) \tag{4.2}$$

with $\zeta(\varepsilon_{\mathrm{PE}}, |\chi|, m) := \sqrt{\frac{\ln\left(\frac{1}{\varepsilon_{\mathrm{PE}}}\right) + |\chi| \ln(m+1)}{2m}}$.

An established way of applying the parameter estimation procedure is to consider the $QBER$ in each measurement basis. In this case we can apply a $POVM$ with only $|\chi| = 2$ elements, which correspond to "Alice and Bob do have the same output" and "Alice and Bob do not have the same output". Let n_{PE} be the number of measurement bases, then the fluctuations of the $QBER$ for each basis can be estimated by $\zeta(\frac{\varepsilon_{\mathrm{PE}}}{n_{\mathrm{PE}}}, 2, \frac{m}{n_{\mathrm{PE}}})$. This demands that $\frac{m}{n_{\mathrm{PE}}}$ signals are used for the estimation of each $QBER$. The total probability of failure is given by $n_{\mathrm{PE}} \frac{\varepsilon_{\mathrm{PE}}}{n_{\mathrm{PE}}} = \varepsilon_{\mathrm{PE}}$. We call this approach of individual $POVM$s in the following $IPOVM$.

In Pub. C we consider one global $POVM$, which consists of $|\chi| = n_{\mathrm{PE}} + 1$ elements, where each of the n_{PE} elements corresponds to "Alice and Bob do not have the same output" for each basis and one corresponds to the completeness of the $POVM$. Using this common $POVM$, in the following denoted by $CPOVM$, the statistical fluctuations become $\zeta(\varepsilon_{\mathrm{PE}}, n_{\mathrm{PE}}, m)$.

A beneficial effect on the secret key rate r (see Eq. (3.19)) appears by considering the BB84 ($n_{\mathrm{PE}} = 2$) (see Figure 4.4). An analogous effect for the six-state protocol and a detailed discussion of the results can be found in Pub. C.

The main result of Pub. C is the derivation of a new bound on the secret key rate in Eq. (3.13) under the assumption of collective attacks. We bound the smooth min-entropy of a tensor-product state by the min-entropy of a single-signal state

$$H_{\min}^{\bar{\varepsilon}}\left(\rho_{XE}^{\otimes n} | E^n\right) \geq n H_{\min}\left(\rho_{XE} | E\right) \tag{4.3}$$

and use its relation to the guessing probability (Eq. (2.23)) to evaluate the secret key rate for the BB84 and six-state protocol. The outstanding result of this bound, in the following called min-entropy approach, leads to significantly higher secret key rates for a small number of signals in comparison to the von Neumann approach in Eq. (3.19) (the AEP-bound). In other words, by using the min-entropy approach,

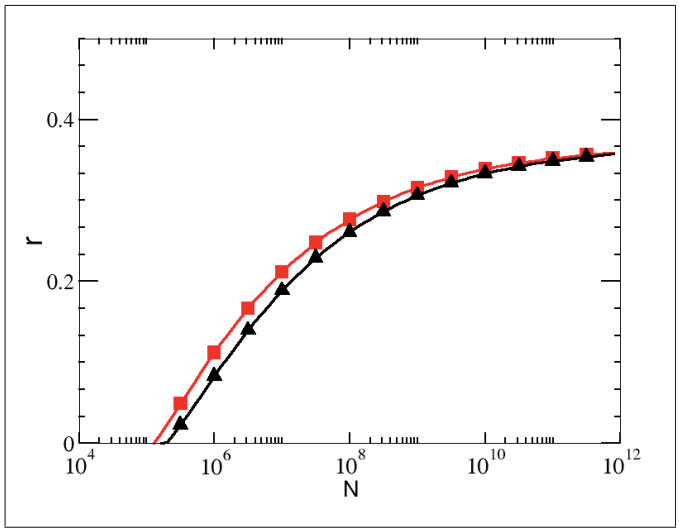

Figure 4.4.: Comparison of the key rates using different parameter estimations for BB84-protocol; $\varepsilon = 10^{-9}$, $Q := Q_m = 5\%$; squares (red): CPOVM, triangles (black): IPOVM.

you need to distribute less quantum signals N_0 to reach a non-zero key rate than with the von Neumann approach. This result is illustrated in Figure 4.5 for the BB84 and the six-state protocol. These results and a generalization to higher dimensional systems are discussed in detail in Pub. C.

An additional result concerning the minimum-error discrimination problem follows from the additivity of the min-entropy for tensor-product states [14], i.e.

$$H_{\min}\left(\rho_{XE}^{\otimes n}|E^n\right) = nH_{\min}\left(\rho_{XE}|E\right) \tag{4.4}$$

and the connection to the guessing probability (see Eq. (2.23)). It states that for a set of symmetric tensor-product states the optimal minimum-error discrimination (MED) measurement is the optimal MED measurement on each subsystem.

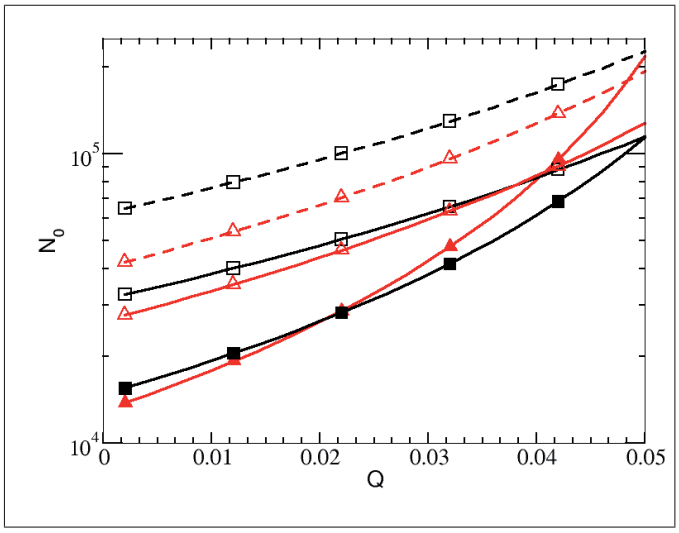

Figure 4.5.: Threshold value N_0 (number of signals, where the key rate becomes non-zero) vs $QBER\ Q := Q_m$ with $\varepsilon = 10^{-9}$; triangles (red): BB84-protocol, squares (black): six-state protocol; filled: min-entropy approach, open: von Neumann entropy approach with CPOVM, dashed line: von Neumann entropy approach with IPOVM.

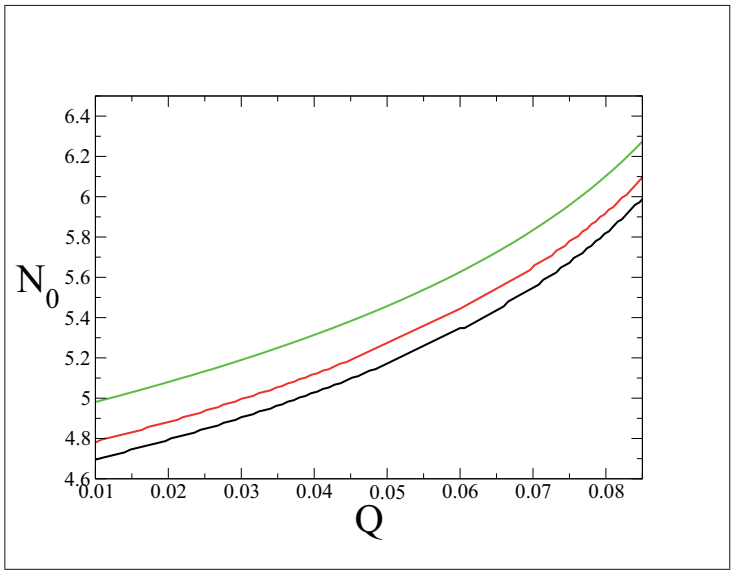

Figure 4.6.: Minimal number N_0 of signals versus $QBER$ Q permitting to extract a non-zero key rate. Comparison between the new bound (black line), the smooth Rényi entropy approach (red line) and the von Neumann entropy approach (green line).

4.4. Improved secret key rates via Rényi entropies

As presented in Eq. (3.5) we can express the rate of a secret key by a dependent optimization of Rényi entropies. The main result of Pub. D is the derivation of a new bound for the six-state protocol under the assumption of collective attacks, which only consists of independent optimizations on each of the smooth Rényi entropies. A comparison to the existing approaches, namely to the von Neumann entropy approach (see Eq. (3.5)) and to the smooth Rényi entropy approach (see Eq. (3.16)) shows a significant improvement with respect to secret key rates (see Figure 4.6 and Figure 4.7).

The main advantage of the new bound in comparison to the smooth Rényi entropy approach (see Eq. (3.16)) is that the environment for the optimization is bigger. The lack of additional correction terms as present in the von Neumann entropy approach (see Eq. (3.5)) causes the better results of the new bound in comparison to the AEP-bound.

A detailed description of the new bound and a further discussion about the results are provided in Pub. D.

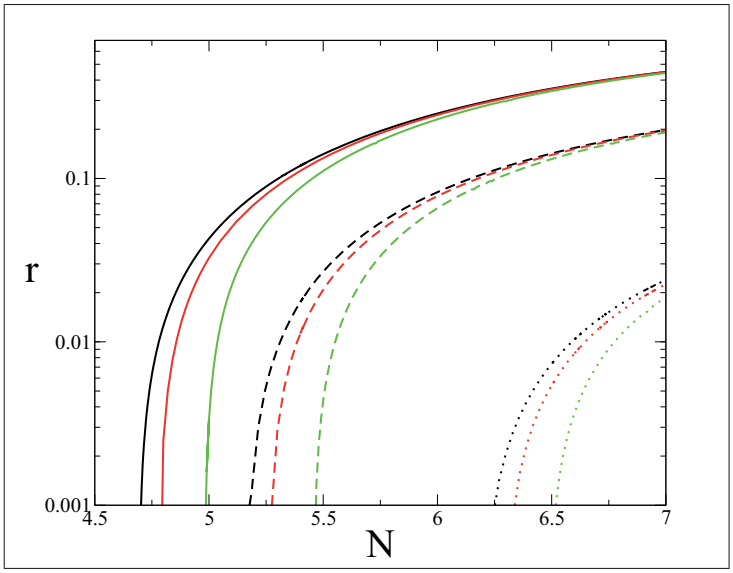

Figure 4.7.: Key rate r versus the initial number N of quantum signals in logarithmic scale. Comparison between the new bound (black lines), the smooth Rényi entropy approach (red lines) and the von Neumann entropy approach (green lines) for different $QBER$s Q: $Q = 0.01$ (straight lines), $Q = 0.05$ (dashed lines), $Q = 0.09$ (dotted lines).

Chapter 5.

Outlook

In the field of quantum key distribution there are still many open questions. In this thesis we only consider perfect protocols, i.e. experimental errors in the measurement devices are ignored. A necessary and important task is the incorporation of experimental imperfections (see e.g. [19]) in the security analysis. In practice, losses during the distribution of the quantum signals have a large influence on the distance at which quantum key distribution can be performed. The exponential decrease of entanglement with respect to the distance of distribution restricts the distance, which is suitable for QKD, to only several hundred kilometers [39]. A promising solution for establishing long-distance QKD is the concept of quantum repeaters [40]. Here, repeater stations between the parties Alice and Bob compensate the losses during the distribution by refreshing the entanglement constantly. The application of quantum repeaters to the secret key rate for finite resources may give an excellent solution to the problem of long distance [41].

Another open problem is the equivalence between coherent and collective attacks for permutation-invariant protocols in the case of finite resources. Although Pub. B gives hints for the disparity of these attacks, no proof for their disparity or for their equivalence is known. A definite statement about this problem would achieve a lot of recognition in the quantum information community.

In the analysis of pre-processing methods, like the deliberate addition of quantum noise in Pub. A, one could ask the question, whether an asymmetric version could have a bigger advantage with respect to secret key rates. For example, instead of considering the symmetric depolarizing channel, one could think of applying a more general, asymmetric Pauli-channel. The only disadvantage here could be the increasing number of parameters, which lead to a more involved optimization procedure.

Chapter 6.

List of main results

- The deliberate addition of quantum noise can be advantageous with respect to secret key rates for finite settings.
- By considering the noise introduced by the channel as not dedicated to the eavesdropper, the secret key rate can be improved significantly.
- Hints for the difference of collective and coherent attacks for finite settings are pointed out.
- A new bound on the secret key rate for permutation-invariant states for coherent attacks is derived. This bound leads to improved key rates in comparison to previous results considering the BB84 and six-state protocol.
- A common $POVM$ with $n_{\mathrm{PE}}+1$ elements can increase the secret key rate in comparison to n_{PE} individual $POVM$s, each with 2 elements. This approach has a beneficial effect for the BB84 and six-state protocol.
- Bounding the smooth min-entropy of a tensor-product state by the min-entropy of a single-signal state and calculating it exactly leads to a significant higher secret key rate for a "small" number of signals for the BB84 and six-state protocol in comparison to the von Neumann entropy approach. This result is generalizable to higher dimensional systems.
- For a set of symmetric tensor-product states the optimal minimum-error discrimination (MED) measurement is the optimal MED measurement on each subsystem.
- A new bound on the secret key rate, which is expressed as an optimization problem over Rényi entropies, is derived. This bound leads to improved key rates in comparison to previous results considering the six-state protocol for collective attacks.

Appendix A.

Proof of Lemma 3

Let $\rho_{AB} \in \mathcal{S}(\mathcal{H}^A \otimes \mathcal{H}^B)$ be a quantum state and P_B a general projector, i.e. $P_B^2 = P_B$ acting on $\mathcal{H}^B$ with the constraint $\mathrm{tr}\left(\rho_B P_B\right) = 1 - \frac{\varepsilon}{2} = \mathrm{tr}\left(\left(\mathbb{1}_A \otimes P_B\right)\rho_{AB}\right)$, then

$$\max_{P_B} \frac{1}{2}\left|\left|\rho_{AB} - \left(\mathbb{1}_A \otimes P_B\right)\rho_{AB}\left(\mathbb{1}_A \otimes P_B\right)\right|\right|_1 = \sqrt{\frac{\varepsilon}{2} - \frac{3}{16}\varepsilon^2} \tag{A.1}$$

Proof: This proof is split into three parts: Part (i) gives a quite general statement known from minimal-error discrimination (MED) [42]. Part (ii) and (iii) calculate a lower and upper bound on the quantity of interest, respectively. Because the lower and upper bound are identical, the assertion follows.

(i) Consider the problem of minimal-error discrimination (MED) [42]: Let $\gamma_1\,(\gamma_2)$ be a not necessarily normalized quantum state weighted with probability $p_1\,(p_2)$ with $p_1 + p_2 = 1$ and the constraint $\mathrm{tr}\left(\gamma_1\right) = \mathrm{tr}\left(\gamma_2\right)$. The minimum error failure probability defined by [42]

$$p_{\mathrm{fail}} = \frac{1}{2}\left|\left|\gamma_1 + \gamma_2\right|\right|_1 - \frac{1}{2}\left|\left|\gamma_1 - \gamma_2\right|\right|_1 \tag{A.2}$$

can only increase under a TP-CP map. Because the partial trace operation is such a TP-CP map, it follows that a purification leads to a higher minimum-error failure probability

$$\begin{aligned} & p_{\mathrm{fail}} \\ := \; & \frac{1}{2}\left|\left|\mathrm{tr}_{\mathrm{aux}}\left(|\gamma_1\rangle\langle\gamma_1| + |\gamma_2\rangle\langle\gamma_2|\right)\right|\right|_1 - \frac{1}{2}\left|\left|\mathrm{tr}_{\mathrm{aux}}\left(|\gamma_1\rangle\langle\gamma_1| - |\gamma_2\rangle\langle\gamma_2|\right)\right|\right|_1 \\ \geq \; & \frac{1}{2}\left|\left|\left|\gamma_1\rangle\langle\gamma_1| + |\gamma_2\rangle\langle\gamma_2|\right|\right|\right|_1 - \frac{1}{2}\left|\left|\left|\gamma_1\rangle\langle\gamma_1| - |\gamma_2\rangle\langle\gamma_2|\right|\right|\right|_1 \end{aligned} \tag{A.3}$$

Because of the fact that $\gamma_1 + \gamma_2$ is a positive operator it follows that

$$\begin{aligned} & \frac{1}{2} \left|\left| |\gamma_1\rangle\langle\gamma_1| + |\gamma_2\rangle\langle\gamma_2| \right|\right|_1 \\ = \; & \frac{1}{2} \mathrm{tr} \left(|\gamma_1\rangle\langle\gamma_1| + |\gamma_2\rangle\langle\gamma_2| \right) && \text{(A.4)} \\ = \; & \frac{1}{2} \mathrm{tr}_{12} \left(\mathrm{tr}_{\mathrm{aux}} \left(|\gamma_1\rangle\langle\gamma_1| + |\gamma_2\rangle\langle\gamma_2| \right) \right) && \text{(A.5)} \\ = \; & \frac{1}{2} \left|\left| \mathrm{tr}_{\mathrm{aux}} \left(|\gamma_1\rangle\langle\gamma_1| + |\gamma_2\rangle\langle\gamma_2| \right) \right|\right|_1 && \text{(A.6)} \end{aligned}$$

The result

$$\frac{1}{2} \left|\left| |\gamma_1\rangle\langle\gamma_1| - |\gamma_2\rangle\langle\gamma_2| \right|\right|_1 \geq \frac{1}{2} \left|\left| \gamma_1 - \gamma_2 \right|\right|_1 \qquad \text{(A.7)}$$

shows that the trace distance of the purifications of two quantum states which have the same norm, but are not necessarily normalized, is larger than the trace distance of the two quantum states.

(ii) Proof of the lower bound, i.e.,

$$\max_{P_B} \frac{1}{2} \left|\left| \rho_{AB} - \left(\mathbb{1}_A \otimes P_B \right) \rho_{AB} \left(\mathbb{1}_A \otimes P_B \right) \right|\right|_1 \geq \sqrt{\frac{\varepsilon}{2} - \frac{3}{16}\varepsilon^2} : \qquad \text{(A.8)}$$

$$\begin{aligned} & \max_{P_B} \quad \frac{1}{2} \left|\left| \rho_{AB} - \left(\mathbb{1}_A \otimes P_B \right) \rho_{AB} \left(\mathbb{1}_A \otimes P_B \right) \right|\right|_1 \\ \overset{(A.7)}{\geq} \; & \max_{P_B} \frac{1}{2} \left|\left| \rho_B - P_B \rho_B P_B \right|\right|_1 && \text{(A.9)} \end{aligned}$$

and for a specific projection P_{BD} that fulfills the constraint $\mathrm{tr}\left(P_B \rho_B\right) = \mathrm{tr}\left(P_{BD} \rho_B\right) = 1 - \frac{\varepsilon}{2}$ we get:

$$\max_{P_B} \frac{1}{2} \left|\left| \rho_B - P_B \rho_B P_B \right|\right|_1 \geq \frac{1}{2} \left|\left| \rho_B - P_{BD} \rho_B P_{BD} \right|\right|_1 \qquad \text{(A.10)}$$

For $\mathrm{rank}(\rho_B) =: r$ we can consider a $2r$-dimensional Hilbert space in a 2×2 block-diagonal basis, i.e.

$$\rho_B = \oplus_{i=1}^{r} \rho_i \qquad \text{(A.11)}$$

with $\rho_i = \lambda_i |i\rangle\langle i|$ and a block-diagonal projection

$$P_{BD} = \oplus_{i=1}^{r} P_i \qquad \text{(A.12)}$$

for $P_i = |i'\rangle\langle i'|$ with $\langle i'|j\rangle = \delta_{ij}\sqrt{1-\frac{\varepsilon}{2}}$. For $\rho_i := |\psi\rangle\langle\psi|$ and $P_i := |\phi\rangle\langle\phi|$ it follows

$$\begin{aligned}
& \frac{1}{2}\left|\left|\rho_B - P_{BD}\rho_B P_{BD}\right|\right|_1 \\
= \; & \frac{1}{2}\left|\left|\oplus_{i=1}^{r}\left(\rho_i - P_i\rho_i P_i\right)\right|\right|_1 && \text{(A.13)} \\
= \; & \sum_{i=1}^{r}\frac{1}{2}\left|\left|\rho_i - P_i\rho_i P_i\right|\right|_1 && \text{(A.14)} \\
= \; & \sum_{i=1}^{r}\frac{1}{2}\mathrm{tr}\left(\sqrt{\rho_i^2 - \rho_i P_i\rho_i P_i - P_i\rho_i P_i\rho_i + P_i\rho_i P_i P_i\rho_i P_i}\right) && \text{(A.15)} \\
= \; & \frac{1}{2}\mathrm{tr}\left(\sqrt{\left(|\psi\rangle\langle\psi| - \left(1-\frac{\varepsilon}{2}\right)|\phi\rangle\langle\phi|\right)^2}\right) && \text{(A.16)}
\end{aligned}$$

where we used $P_i\rho_i P_i = \lambda_i|\phi\rangle\langle\phi|\,|\langle\phi|\psi\rangle|^2 = \lambda_i\left(1-\frac{\varepsilon}{2}\right)|\phi\rangle\langle\phi|$ and $\sum_{i=1}^{r}\lambda_i = 1$. Moreover with $|\langle\phi|\psi\rangle|^2 = 1-\frac{\varepsilon}{2}$ and $\mathbb{1} = |\psi^c\rangle\langle\psi^c| + |\psi\rangle\langle\psi|$ it follows that

$$\begin{aligned}
|\langle\phi|\psi^c\rangle|^2 &= \langle\phi|\psi^c\rangle\langle\phi|\psi^c\rangle && \text{(A.17)} \\
&= \langle\phi|\mathbb{1} - |\psi\rangle\langle\psi||\phi\rangle && \text{(A.18)} \\
&= \langle\phi|\phi\rangle - \langle\phi|\psi\rangle\langle\psi|\phi\rangle && \text{(A.19)} \\
&= 1 - |\langle\phi|\psi\rangle|^2 && \text{(A.20)} \\
&= 1 - \left(1-\frac{\varepsilon}{2}\right) && \text{(A.21)} \\
&= \frac{\varepsilon}{2} && \text{(A.22)}
\end{aligned}$$

With this we obtain

$$
\begin{aligned}
& |\phi\rangle\langle\phi| \\
= \;& \mathbb{1}|\phi\rangle\langle\phi|\mathbb{1} && \text{(A.23)} \\
= \;& \left(|\psi^c\rangle\langle\psi^c| + |\psi\rangle\langle\psi|\right)|\phi\rangle\langle\phi|\left(|\psi^c\rangle\langle\psi^c| + |\psi\rangle\langle\psi|\right) && \text{(A.24)} \\
= \;& |\langle\phi|\psi\rangle|^2 |\psi\rangle\langle\psi| + \langle\psi|\phi\rangle\langle\phi|\psi^c\rangle|\psi\rangle\langle\psi^c| + \langle\phi|\psi\rangle\langle\psi^c|\phi\rangle|\psi^c\rangle\langle\psi| \\
& + |\langle\phi|\psi^c\rangle|^2 |\psi^c\rangle\langle\psi^c| && \text{(A.25)} \\
= \;& \left(1-\frac{\varepsilon}{2}\right)|\psi\rangle\langle\psi| + \sqrt{\left(1-\frac{\varepsilon}{2}\right)\frac{\varepsilon}{2}}|\psi\rangle\langle\psi^c| + \sqrt{\left(1-\frac{\varepsilon}{2}\right)\frac{\varepsilon}{2}}|\psi^c\rangle\langle\psi| \\
& + \frac{\varepsilon}{2}|\psi^c\rangle\langle\psi^c| && \text{(A.26)}
\end{aligned}
$$

Putting Eq. (A.26) into Eq. (A.16) the absolute values of the eigenvalues of the square-root can be determined for an orthogonal basis $\{|\psi\rangle, |\psi^c\rangle\}$ to

$$\left\{-\tfrac{1}{4}\left(\varepsilon - \sqrt{8\varepsilon - 3\varepsilon^2}\right), \tfrac{1}{4}\left(\varepsilon + \sqrt{8\varepsilon - 3\varepsilon^2}\right)\right\}.$$

Finally, this leads to

$$\max_{P_B} \frac{1}{2}\left|\left|\rho_{AB} - \left(\mathbb{1}_A \otimes P_B\right)\rho_{AB}\left(\mathbb{1}_A \otimes P_B\right)\right|\right|_1 \geq \sqrt{\frac{\varepsilon}{2} - \frac{3}{16}\varepsilon^2}. \qquad \text{(A.27)}$$

(iii) Proof of the upper bound, i.e.,

$$\max_{P_B} \frac{1}{2}\left|\left|\rho_{AB} - \left(\mathbb{1}_A \otimes P_B\right)\rho_{AB}\left(\mathbb{1}_A \otimes P_B\right)\right|\right|_1 \leq \sqrt{\frac{\varepsilon}{2} - \frac{3}{16}\varepsilon^2}. \qquad \text{(A.28)}$$

Let $\mathcal{H}^C$ be an ancilla system and P_{ABC} a general, not necessarily separable projector which acts on the joint system $\mathcal{H}^A \otimes \mathcal{H}^B \otimes \mathcal{H}^C$ with the constraint

$\mathrm{tr}\left(P_{ABC}|\rho_{AB}\rangle\langle\rho_{AB}|\right) = \mathrm{tr}\left(P_B\rho_B\right) = 1 - \frac{\varepsilon}{2}$, then it follows that

$$
\begin{aligned}
& \max_{P_B} \frac{1}{2} \left|\left|\rho_{AB} - \left(\mathbb{1}_A \otimes P_B\right) \rho_{AB} \left(\mathbb{1}_A \otimes P_B\right)\right|\right|_1 \\
\overset{(A.7)}{\leq} \quad & \max_{P_B} \frac{1}{2} \left|\left|\left|\rho_{AB}\rangle\langle\rho_{AB}\right| - \left(\mathbb{1}_A \otimes P_B \otimes \mathbb{1}_C\right) |\rho_{AB}\rangle\langle\rho_{AB}| \left(\mathbb{1}_A \otimes P_B \otimes \mathbb{1}_C\right)\right|\right|_1 \\
= \quad & \max_{P_{ABC}} \frac{1}{2} \left|\left|\left|\rho_{AB}\rangle\langle\rho_{AB}\right| - \left(\mathbb{1}_A \otimes P_B \otimes \mathbb{1}_C\right) |\rho_{AB}\rangle\langle\rho_{AB}| \left(\mathbb{1}_A \otimes P_B \otimes \mathbb{1}_C\right)\right|\right|_1 \\
= \quad & \sqrt{\frac{\varepsilon}{2} - \frac{3}{16}\varepsilon^2}
\end{aligned}
\tag{A.29}
$$

with $P_{ABC} = \mathbb{1}_A \otimes P_B \otimes \mathbb{1}_C$. The last equality follows from the exact calculation of the trace distance for pure states, which we already used in the computation of the lower bound.

□

Bibliography

[1] G. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *American Institute of Electrical Engineers, Transactions of the*, 45:295–301, 1926.

[2] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, 1949.

[3] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.

[4] 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*, volume 175. Bangalore, India, 1984.

[5] A.K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, 1991.

[6] J. S. Bell. On the einstein-podolsky-rosen paradox. *Physics*, 1(3):195–200, 1964.

[7] C.H. Bennett, G. Brassard, and N.D. Mermin. Quantum cryptography without Bell's theorem. *Physical Review Letters*, 68(5):557–559, 1992.

[8] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14):3018–3021, 1998.

[9] H. Bechmann-Pasquinucci and N. Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Physical Review A*, 59(6):4238, June 1999.

[10] H.K. Lo and H.F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050, 1999.

[11] P.W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85(2):441–444, 2000.

[12] W.Y. Hwang. Quantum key distribution with high loss: toward global secure communication. *Physical Review Letters*, 91(5):57901, 2003.

[13] V. Scarani, A. Acin, G. Ribordy, and N. Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, 92(5):57901, 2004.

[14] R. Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(1), 2008.

[15] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography Conference (TCC)*, volume 3378, pages 407–425. Springer, 2005.

[16] T. Meyer, H. Kampermann, M. Kleinmann, and D. Bruß. Finite key analysis for symmetric attacks in quantum key distribution. *Physical Review A*, 74(4):42340, 2006.

[17] V. Scarani and R. Renner. Security bounds for quantum cryptography with finite resources. *Proceedings of TQC2008, Lecture Notes in Computer Science 5106 (Springer Verlag, Berlin), pp. 83-95*, 2008.

[18] R. Y. Q. Cai and V. Scarani. Finite-key analysis for practical implementations of quantum key distribution. *New Journal of Physics*, 11(4):045024, 2009.

[19] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Review of Modern Physics*, 81(3):1301–1350, 2009.

[20] V. Scarani. QKD: a million signal task. In R. Horodecki, S. Ya. Kilin, and J. Kowalik, editors, *Quantum Cryptography and Computing*, volume 26 of *NATO Science for Peace and Security Series - D: Information and Communication Security*, pages 76–82, 2010.

[21] M. Tomamichel, C. W. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3:634, 2012.

[22] M. Hayashi and T. Tsurumaru. Simple and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths. *arXiv:quant-ph/1107.0589*, 2011.

[23] M.A. Nielsen and I.L. Chuang. *Quantum computing and quantum information*. Cambridge University Press, 2000.

[24] A. Peres. *Quantum theory: concepts and methods*. Springer, 1995.

[25] K.E. Hellwig and K. Kraus. Pure operations and measurements. *Communication of Mathematical Physics*, 11(3):214–220, 1969.

[26] K.E. Hellwig and K. Kraus. Operations and measurements ii. *Communication of Mathematical Physics*, 16(2):142–147, 1970.

[27] M. Tomamichel. *A Framework for Non-Asymptotic Quantum Information Theory*. PhD thesis, ETH Zurich, 2012.

[28] A. Rényi. On measures of information and entropy. In *Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability*, volume 1, pages 547–561, 1961.

[29] R. König, R. Renner, and C. Schaffner. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory*, 55(9), 2009.

[30] Renato Renner and Stefan Wolf. Smooth Renyi entropy and applications. In *IEEE International Symposium on Information Theory — ISIT 2004*, page 233. IEEE, June 2004.

[31] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of cryptology*, 5(1):3–28, 1992.

[32] G. Brassard and L Salvail. Secret-key reconciliation by public discussion. *In:Advances in Cryptology-EUROCRYPT '93 (T. Helleseth, ed.)*, 765:410–423, 1994.

[33] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, November 1995.

[34] V. Scarani and R. Renner. Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical Review Letters*, 100:200501, 2008.

[35] S. Abruzzo. Secret key rate in quantum key distribution using optimization on Rényi entropies. Master's thesis, Università degli studi di Torino, 2010.

[36] 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. *Physical Review Letters*, 95(8):080501, Aug 2005.

[37] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Physical Review A*, 72:012332, 2005.

[38] M. Christandl, R. König, and R. Renner. Post-selection technique for quantum channels with applications to quantum cryptography. *Physical Review Letters*, 102:020504, 2009.

[39] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New Journal of Physics*, (11):075003, 2009.

[40] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Review of Modern Physics*, (83):33–80, 2011.

[41] S. Abruzzo, S. Bratzik, N. K. Bernardes, H. Kampermann, D. Bruß, and P. van Loock. Quantum repeaters and QKD : analysis of secret key rates. *In preparation*, 2012.

[42] C.W. Helstrøm. *Quantum Detection and Estimation Theory*. Academic, New York, 1976.

Publication A

Quantum key distribution with finite resources: Taking advantage of quantum noise

Markus Mertz,* Hermann Kampermann, Zahra Shadman, and Dagmar Bruß
Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf, 40225 Düsseldorf, Germany.
(Dated: May 16, 2012)

We compare the effect of different noise scenarios on the achievable rate of an ε-secure key for the BB84 and the six-state protocol. We study the situation where quantum noise is added deliberately, and investigate the remarkable benefit for the finite key rate. We compare our results to the known case of added classical noise and the asymptotic key rate, i.e. in the limit of infinitely many signals. As a complementary interpretation we show that under the realistic assumption that the noise which is unavoidably introduced by a real channel is not fully dedicated to the eavesdropper, the secret key rate increases significantly.

I. INTRODUCTION

Quantum key distribution (QKD) aims at establishing a secret key between two parties Alice and Bob, who are connected via a quantum channel and an authenticated classical channel. In the last few years, in addition to the studies of asymptotic QKD (i.e. the unrealistic case of infinitely many signals, which is more accessible theoretically), more realistic QKD scenarios have been analyzed, where the number of signals sent through the channel is finite [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13].

A general aim in studies of security in QKD is to determine a scenario in which the secure key rate is as high as possible. It has been shown that pre-processing methods [1, 14, 15, 16, 17, 18, 19], like for example adding classical noise [1] or advantage distillation [1] can increase the secure key rate significantly. Note that those investigations have focused on pre-processing operating on the *classical* level. By the addition of *quantum noise* a beneficial effect in asymptotic QKD (on the level of mutual information) has been shown in [20] for the six-state protocol [21, 22]. However, for a finite number of signals the mutual information of Alice and Bob versus the one of the eavesdropper Eve is not a direct indicator for the secret key rate.

The purpose of this article is to investigate the effect of *quantum* noise on secret key rates with *finite* resources for the BB84 [23] and six-state protocol [21, 22]. We will analyse our results for two complementary interpretations: First, we present different quantum noise scenarios, where the noise is added on purpose, and investigate its benefit for the secret key rate. Second, we interpret the added noise as the unavoidable noise introduced by a real channel. We then show how the secret key rate can be improved if we consider the noise introduced by the channel as not fully due to the interaction of an eavesdropper. We compare the results to the known effect of classical noise and the case of infinitely many signals. For the investigation we consider the BB84 and six-state protocol in the entanglement-based scheme under the assumption of collective attacks. We use the asymptotic equipartition property (AEP) [1, 24] to bound the smooth min-entropy [1] in the high-dimensional Hilbert space, such that the ε-secure key rate can be mainly determined by the conditional von Neumann entropy of a single-signal-state. Note that here, for key rates in the finite regime, the assumption of collective attacks is necessary, since the equivalence of collective and coherent attacks for the BB84 and the six-state protocol has so far been proven only in the limit of infinitely many signals [25, 26].

The paper is structured as follows: In Section II we introduce the general framework and fix the notation. The different noise scenarios are presented and discussed in Section III. Section IV deals with the calculation and optimization of ε-secure key rates for these different noise scenarios. The results are given in Section V, followed by a conclusion in Section VI.

II. PRELIMINARIES

In the following we consider the BB84 and six-state protocol in the entanglement-based scheme, where the eavesdropper Eve can only interact with the signals (labeled by B) which are sent through the quantum channel. The most general unitary interaction U_{BE} that Eve can perform is given by [27]

$$U_{BE}\left|0\right\rangle_B\left|X\right\rangle_E = \sqrt{1-D}\left|0\right\rangle_B\left|A\right\rangle_E + \sqrt{D}\left|1\right\rangle_B\left|B\right\rangle_E \quad (1)$$

$$U_{BE}\left|1\right\rangle_B\left|X\right\rangle_E = \sqrt{1-D}\left|1\right\rangle_B\left|C\right\rangle_E + \sqrt{D}\left|0\right\rangle_B\left|D\right\rangle_E \quad (2)$$

where $\left|X\right\rangle_E$ is Eve's initial state and $\left|A\right\rangle_E$, $\left|B\right\rangle_E$, $\left|C\right\rangle_E$, $\left|D\right\rangle_E$ refer to her 4-dimensional states after the transformation. The parameter $D \in \left[0, \frac{1}{2}\right]$ corresponds to the disturbance, i.e. the quantum bit error rate ($QBER$) introduced by Eve if the quantum channel is otherwise noiseless.

Throughout our paper we will study quantum noise which is given by a depolarizing channel. (Note that our calculations could in principle be generalized to other models for quantum noise, but the lower the symmetry of the channel, the more involved the calculations will be.) The action of the depolarizing channel is described by the map $\mathcal{N}^p(\rho)$, where p is the noise parameter.

*Electronic address: mertz@thphy.uni-duesseldorf.de

Definition 1. *The action of a depolarizing channel* $\mathcal{N}^p(\rho)$ *is given by*

$$\mathcal{N}^p(\rho) := \sum_{i=1}^{4} A_i \rho A_i^\dagger \tag{3}$$

with the Kraus operators $A_1 = \sqrt{1-\frac{3}{4}p}\mathbb{1}, A_2 = \sqrt{\frac{p}{4}}\sigma_x, A_3 = \sqrt{\frac{p}{4}}\sigma_y, and A_4 = \sqrt{\frac{p}{4}}\sigma_z$. *Here,* σ_i *are the Pauli-operators for* $i \in \{x, y, z\}$.

Analogously, we define classical noise [1] via the map $\mathcal{N}^{cl,p}(\rho)$.

Definition 2. *The action of a classical noisy channel is given by*

$$\mathcal{N}^{cl,p}(\rho) := \sum_{i=1}^{2} B_i \rho B_i^\dagger \tag{4}$$

with $B_1 = \sqrt{1-\frac{p}{2}}\mathbb{1}$ *and* $B_2 = \sqrt{\frac{p}{2}}\sigma_x$.

Note that this definition is different from the usual definition of classical noise in the literature: throughout our paper the probability to flip a bit is called $\frac{p}{2}$ instead of p. This choice of p allows a fair comparison of the two different noise models (quantum versus classical) for the same parameter p, ranging from 0 to 1.

Our central figure of merit is the ε-secure key rate for a finite number of signals. We will use this quantity in the following to compare different noise scenarios. The ε-secure key rate is calculated for a typical protocol that consists of the procedures state distribution, measurement, sifting, parameter estimation (PE), one-way error correction (EC) and privacy amplification (PA). Let $\varepsilon_{\mathrm{PE}}, \varepsilon_{\mathrm{EC}}$ and $\varepsilon_{\mathrm{PA}}$ be the probability of failure for the protocol steps parameter estimation, error correction and privacy amplification, respectively. Then with a smoothing parameter $\bar{\varepsilon}$ we can bound the total security of the protocol by

$$\varepsilon := \bar{\varepsilon} + \varepsilon_{\mathrm{PE}} + \varepsilon_{\mathrm{EC}} + \varepsilon_{\mathrm{PA}}. \tag{5}$$

For such a protocol it has been shown in [1, 6] that the rate of an ε-secure key is given by

$$\begin{aligned} r \;=\; & \frac{1}{N} \min_{\rho_{AB}\in\Gamma_\zeta} \left(H_{\min}^{\bar{\varepsilon}}\left(\rho_{XE}^n|E\right) - n f_{\mathrm{EC}} H(X|Y)\right) \\ & + \frac{2}{N}\log\left(2\varepsilon_{\mathrm{PA}}\right), \end{aligned} \tag{6}$$

where the smooth min-entropy [1]

$$H_{\min}^{\varepsilon}(\rho_{AE}|E) := \sup_{\sigma_{AE}\in\mathcal{B}^{\frac{\varepsilon}{2}}(\rho_{AE})} \sup_{\rho_E\in S(\mathcal{H})} H_{\min}(\sigma_{AE}|\rho_E) \tag{7}$$

is defined as an optimization of the min-entropy

$$H_{\min}(\sigma_{AE}|\rho_E) := \sup\left\{\lambda\in\Re : 2^{-\lambda}\mathbb{1}_A\otimes\rho_E - \sigma_{AE} \geq 0\right\} \tag{8}$$

over an ε-environment given by

$$\mathcal{B}^{\varepsilon}(\rho) := \left\{\sigma : \frac{1}{2}||\sigma-\rho||_1 \leq \varepsilon\right\}, \tag{9}$$

with the 1-norm $||A||_1 = \mathrm{tr}\left(\sqrt{AA^\dagger}\right)$. Here, $S(\mathcal{H})$ denotes the set of density operators on the Hilbert space $\mathcal{H}$. The smooth min-entropy of the classical-quantum state ρ_{XE}^n shared by Alice and Eve and the correction $2\log_2(2\varepsilon_{\mathrm{PA}})$ are due to privacy amplification. It quantifies Eve's uncertainty of Alice's and Bob's perfectly correlated bitstring. The term $f_{\mathrm{EC}}H(X|Y)$ stands for the number of bits which Alice and Bob leak to the eavesdropper due to public communication during the error correction procedure. $H(X|Y)$ denotes the conditional Shannon entropy $H(X|Y) = H(\rho_{XY}) - H(\rho_Y)$ with $H(X) = -\sum_x p(x)\log(p(x))$. For simplicity we consider an ideal error correction protocol, i.e. $f_{\mathrm{EC}} = 1$. The minimization of the smooth min-entropy is due to parameter estimation, where we only except qubit-states ρ_{AB} which are contained in the set [5, 10]

$$\Gamma_\zeta := \left\{\rho : \frac{1}{2}||\lambda_m(\rho) - \lambda_\infty(\rho)||_1 \leq \zeta(\varepsilon_{\mathrm{PE}}, 2, m)\right\} \tag{10}$$

with

$$\zeta(\varepsilon_{\mathrm{PE}}, n_p, m) := \sqrt{\frac{\ln\left(\frac{1}{\varepsilon_{\mathrm{PE}}}\right) + n_p \ln(m+1)}{8m}}, \tag{11}$$

where $\lambda_m(\rho)$ ($\lambda_\infty(\rho)$) denotes the measurement statistics due to an m ($m\to\infty$)-fold independent application of a measurement.

Under the assumption of collective attacks, i.e. $\rho_{XE}^n = \rho_{XE}^{\otimes n}$ we can use the AEP [1, 24]

$$H_{\min}^{\varepsilon}\left(\rho_{XE}^{\otimes n}|E\right) \geq n\left(S(X|E) - 5\sqrt{\frac{\log(2/\varepsilon)}{n}}\right) \tag{12}$$

to bound the smooth min-entropy for product states $\rho_{XE}^{\otimes n}$ by the conditional von Neumann entropy of a single copy ρ_{XE} which is defined as $S(X|E) = S(\rho_{XE}) - S(\rho_E)$ with $S(\rho) = -\mathrm{tr}(\rho\log\rho)$. Finally, this leads to

$$\begin{aligned} r \;:=\; & \frac{n}{N} \min_{\rho_{AB}\in\Gamma_\zeta} \left(S(X|E) - 5\sqrt{\frac{\log(2/\bar{\varepsilon})}{n}} - H(X|Y)\right) \\ & + \frac{2}{N}\log\left(2\varepsilon_{\mathrm{PA}}\right). \end{aligned} \tag{13}$$

III. NOISE SCENARIOS

In this section we present four different noise scenarios which we will investigate in the following. Initially, if no noise is present, Alice holds one part of the Bell-state $|\Psi^+\rangle\langle\Psi^+|$, with

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), \tag{14}$$

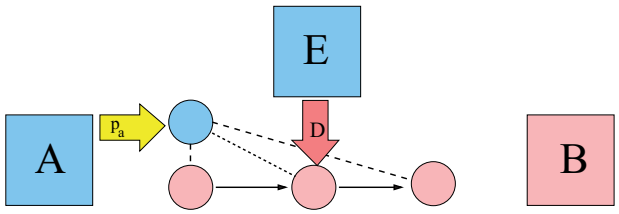

FIG. 1: (Color online) Noise scenario 1; Alice adds depolarizing quantum noise to her part of the initial state.

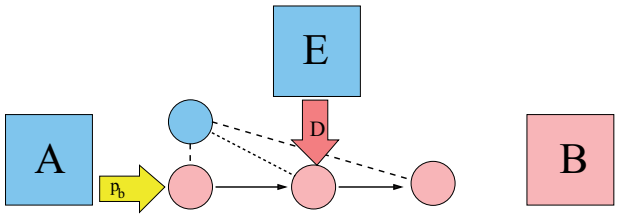

FIG. 2: (Color online) Noise scenario 2; Alice adds depolarizing quantum noise to Bob's part of the initial state.

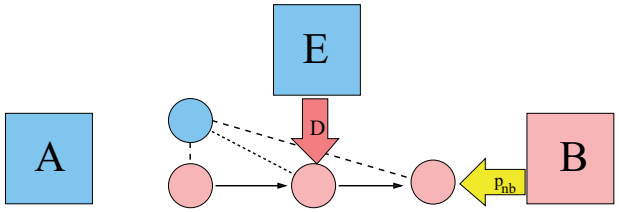

FIG. 3: (Color online) Noise scenario 3; Bob adds depolarizing quantum noise to his part of the state after receiving it.

and sends the second part to Bob, while the eavesdropper can perform a unitary interaction U_{BE} characterized by a disturbance D (see Eq. (1)) on it. Let us denote the map that corresponds to the unitary interaction U_{BE} as $\mathcal{E}_{BE}$. The total state after the action of $\mathcal{E}_{BE}$ is then given by

$$\rho_{ABE}^{(0)} = (\mathbb{1}_A \otimes \mathcal{E}_{BE}) \left(\left|\Psi^+\right\rangle \left\langle\Psi^+\right|_{AB} \otimes |X\rangle \langle X|_E \right), \quad (15)$$

where $|X\rangle \langle X|_E$ denotes Eve's initial state.

Now, four different noise scenarios are considered:

(1) Alice adds depolarizing quantum noise with noise parameter p_a to her part of the Bell-state and sends the other part to Bob (see FIG. 1). This leads to the state

$$\begin{aligned} \rho_{ABE}^{(1)} &= (\mathbb{1}_A \otimes \mathcal{E}_{BE})(\mathcal{N}_A^{p_a} \otimes \mathbb{1}_{BE}) \\ &\quad \left(\left|\Psi^+\right\rangle \left\langle\Psi^+\right|_{AB} \otimes |X\rangle \langle X|_E \right). \end{aligned} \quad (16)$$

Note that there is obviously no difference between adding Alice's noise before or after Eve's interaction, since they act on different Hilbert spaces.

(2) Alice adds depolarizing noise with noise parameter p_b to Bob's part of the Bell-state and sends it to Bob (see FIG. 2). This leads to the state

$$\begin{aligned} \rho_{ABE}^{(2)} &= (\mathbb{1}_A \otimes \mathcal{E}_{BE})(\mathbb{1}_A \otimes \mathcal{N}_B^{p_b} \otimes \mathbb{1}_E) \\ &\quad \left(\left|\Psi^+\right\rangle \left\langle\Psi^+\right|_{AB} \otimes |X\rangle \langle X|_E \right). \end{aligned} \quad (17)$$

(3) Bob adds depolarizing noise with noise parameter p_{nb} to his part of the Bell-state after Eve's interaction (see FIG. 3). This leads to the state

$$\begin{aligned} \rho_{ABE}^{(3)} &= (\mathbb{1}_A \otimes \mathcal{N}_B^{p_{nb}} \otimes \mathbb{1}_E)(\mathbb{1}_A \otimes \mathcal{E}_{BE}) \\ &\quad \left(\left|\Psi^+\right\rangle \left\langle\Psi^+\right|_{AB} \otimes |X\rangle \langle X|_E \right). \end{aligned} \quad (18)$$

(4) Alice introduces classical noise with noise parameter p_{cl} to her classical bit string after her measurement (see FIG. 4).

How do these four scenarios compare, when evaluating the ε-secure key rate?

IV. SECRET KEY RATE

The aim of this section is to investigate the effect of the various noise scenarios explained in the previous section on the finite ε-secure key rate r in Eq. (13).

From the fact that Alice and Bob share in the beginning a maximally entangled state (see Eq. (14)) we know that the action of a depolarizing channel on Alice's part or on Bob's part results in the same total state. This implies that the states $\rho_{ABE}^{(1)}$ and $\rho_{ABE}^{(2)}$ are identical for $p_a = p_b$ and the noise scenarios 1 and 2 are equivalent.

Additionally, we now show the equivalence of noise scenario 1 and 4, i.e. adding rotationally invariant quantum noise is equivalent to adding classical noise. Let us assume for noise scenario 4 that we add classical noise with probability $\frac{p_{cl}}{2}$ to flip a bit (see Definition 2) to a bit-string resulting from measurements in the z-basis. In noise scenario 1 only the Pauli-operators σ_x and σ_y from the depolarizing channel (see Definition 1) lead to a bit-flip, such that the total probability to flip a bit is given by $\frac{p_a}{4} + \frac{p_a}{4} = \frac{p_a}{2}$. Note that for the cases in scenario 4 that the bit-strings were obtained by measurements in x (y)-basis the same argument holds. Then only σ_y and σ_z (σ_x and σ_z) lead to bit-flips in scenario 1, and due to the

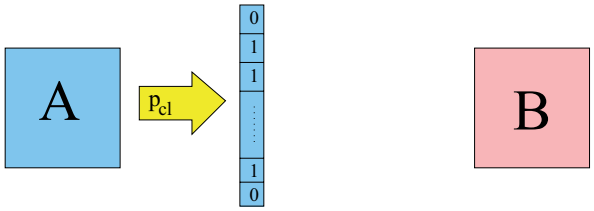

FIG. 4: (Color online) Noise scenario 4; Alice adds classical noise to her classical bit string.

symmetry of the depolarizing channel the probability to flip is also $\frac{p_a}{2}$ in both cases. This implies the equivalence of scenario 1 and scenario 4 for $p_a = p_{cl}$.

Noise scenario 3 will not lead to any benefit for the key rate as it only increases the quantum bit error rate ($QBER$). This asymmetry between noise scenario 2 and 3 is due to the underlying one-way error-correction protocol, such that adding Bob's noise after Eve's interaction only influences the key rate r by increasing $H(X|Y)$.

The equivalence of the noise scenarios 1, 2 and 4, together with the fact that scenario 3 can only be detrimental for the secret key rate, enable us to focus for the rest of this paper on a specific noise scenario, namely noise scenario 1. We start for simplicity with the investigation of the asymptotic key rate (i.e. Eq. (13) for $N \to \infty, \varepsilon \to 0$) given by [28]

$$r_{\text{asym}} = S(X|E) - H(X|Y). \tag{19}$$

Later, the effect of noise on the finite key rate (see Eq. (13)) follows by including the finite-size effects.

In order to determine Eve's unknown probes in the state $\rho^{(1)}_{ABE}$, given in Eq. (16), namely $|A\rangle_E, |B\rangle_E, |C\rangle_E, |D\rangle_E$, we expand each probe in basis vectors

$$|A\rangle_E = \alpha_a |00\rangle + \beta_a |01\rangle + \gamma_a |10\rangle + \delta_a |11\rangle \tag{20}$$

with the normalization condition

$$|\alpha_a|^2 + |\beta_a|^2 + |\gamma_a|^2 + |\delta_a|^2 = 1 \tag{21}$$

and a similar parametrization for $|B\rangle_E, |C\rangle_E, |D\rangle_E$, with indices b, c, d, respectively. A partial-trace operation on $\rho^{(1)}_{ABE}$ over Eve's part leads to the state $\rho^{(1)}_{AB}$, which corresponds to the state shared by Alice and Bob after Eve's unitary interaction. It has been shown in [25, 26] that the BB84 and the six-state protocol permit to characterize the state $\rho^{(1)}_{AB}$ as Bell-diagonal, parametrized by the quantum bit error rate Q.

$$\begin{aligned} \rho^{(1)}_{AB} &= \lambda_1 |\Psi^+\rangle\langle\Psi^+| + \lambda_2 |\Psi^-\rangle\langle\Psi^-| \\ &\quad + \lambda_3 |\Phi^+\rangle\langle\Phi^+| + \lambda_4 |\Phi^-\rangle\langle\Phi^-|, \end{aligned} \tag{22}$$

with the Bell-states

$$|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{23}$$

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \tag{24}$$

and the parameters

$$\lambda_1 = 1 - \frac{3}{2}Q, \lambda_2 = \lambda_3 = \lambda_4 = \frac{Q}{2} \tag{25}$$

for the six-state protocol, while

$$\lambda_1 = 1 - 2Q + \lambda_4, \lambda_2 = \lambda_3 = Q - \lambda_4, \lambda_4 \in [0, Q] \tag{26}$$

for the BB84 protocol. Note that the symmetry properties of $\rho^{(1)}_{AB}$ are preserved by adding symmetric depolarizing noise (see Definition 1).

We can express the $QBER$ Q as a function of the noise parameter p_a, which is introduced by the depolarizing channel, and Eve's disturbance D:

$$Q = (1 - p_a)D + \frac{p_a}{2}. \tag{27}$$

For the six-state protocol we obtain the following additional conditions on Eve's probes:

$$\langle A|B\rangle_E = \langle A|D\rangle_E = \langle B|C\rangle_E = \langle D|C\rangle_E = \langle B|D\rangle_E = 0 \tag{28}$$

and

$$\langle A|C\rangle_E = \frac{1 - 2Q}{(1 - p_a)(1 - D)}. \tag{29}$$

W.l.o.g. we can choose $|D\rangle_E = |00\rangle$ and $|B\rangle_E = |11\rangle$. It follows that

$$|A\rangle_E = \beta_a |01\rangle + \sqrt{1 - |\beta_a|^2}\,|10\rangle, \tag{30}$$

$$|C\rangle_E = \beta_c |01\rangle + \sqrt{1 - |\beta_c|^2}\,|10\rangle. \tag{31}$$

By using Eq. (29) we eliminate β_a, such that with the constraints in Eq. (28) the state $\rho^{(1)}_{ABE}$ contains only one unknown parameter, namely β_c.

Analogously, we get for the BB84 protocol the following constraints:

$$\langle A|B\rangle_E = \langle A|D\rangle_E = \langle B|C\rangle_E = \langle D|C\rangle_E = 0 \tag{32}$$

and

$$\langle B|D\rangle_E = \frac{Q - 2\lambda_4}{(1 - p_a)D}, \tag{33}$$

$$\langle A|C\rangle_E = \frac{1 - 3Q + 2\lambda_4}{(1 - p_a)(1 - D)}. \tag{34}$$

W.l.o.g. we can choose $|A\rangle_E = |11\rangle$ and $|B\rangle_E = |00\rangle$. It follows that

$$|C\rangle_E = \sqrt{1 - |\delta_c|^2}\,|10\rangle + \delta_c |11\rangle, \tag{35}$$

$$|D\rangle_E = \alpha_d |01\rangle + \sqrt{1 - |\alpha_d|^2}\,|10\rangle. \tag{36}$$

By using Eq. (33) and Eq. (34) we can reduce the unknown parameters of the state $\rho^{(1)}_{ABE}$ to the single parameter λ_4.

Remember that $\rho^{(1)}_{ABE}$ describes the quantum state shared by Alice, Bob and Eve after the state distribution step for noise scenario 1. Let us denote the classical-classical-quantum state that results from local von Neumann measurements performed by Alice and Bob by ρ_{XYE}. The states ρ_{XE} and ρ_{XY}, which are needed for the calculation of the asymptotic key rate in Eq. (19), follow directly by a partial-trace operation on Bob's part and Eve's part, respectively.

The unknown parameter β_c (λ_4) for the six-state protocol (BB84 protocol) has to be chosen in such a way that it minimizes the asymptotic key rate in Eq. (19), such that these states realize Eve's best strategy. After including the finite-key corrections (Eq. (13)) into the optimization, the key rate is now fully determined by the noise parameter p_a and the disturbance D, such that the effects of noise can be calculated, also in the regime of a finite number of signals.

V. RESULTS

In this section we present our results on the secret key rate in the noisy scenario described above. We will discuss two possible interpretations of our results: In subsection V A we consider the case that the noise is introduced deliberately by Alice. In subsection V B we analyse the case where the noise is given by the channel and did not originate from the eavesdropper. The finite-key rate r (Eq. (13)) will be calculated in both cases for a total security parameter of $\varepsilon = 10^{-9}$. The results are obtained from a numerical optimization procedure, which maximizes the key rate with respect to the parameters $m, \bar{\varepsilon}, \varepsilon_{\mathrm{PE}}, \varepsilon_{\mathrm{EC}}, \varepsilon_{\mathrm{PA}}$, while minimizing with respect to the parameters β_c (λ_4), for the six-state (BB84) protocol.

A. Introducing noise deliberately

In the following we illustrate the effect of deliberately added noise (see Section III) on the finite key rate r (see Eq. (13)).

In FIG. 5 the behaviour of N_0, the minimal number of signals that is needed to extract a non-zero key, with respect to the disturbance D is shown for an optimal noise parameter p_a (see FIG. 6) for the BB84 and the six-state protocol. In comparison to the noiseless case we obtain a beneficial effect on the finite key rate by introducing quantum noise p_a: In the six-state (BB84) protocol with $D = 0.12$ ($D = 0.1$) the improvement in the minimal number of signals N_0 is of the order of a million signals. Additionally, we find that noise enables us to extract a non-zero key for higher disturbances than in the noiseless case: We recover for our case of a finite number of signals the result of [25], which states that the maximum tolerated error rate introduced by Eve to extract a non-zero key is shifted from 12.6% to 14.1% (11.0% to 12.4%) for the six-state (BB84) protocol, in the asymptotic limit $N_0 \to \infty$.

In FIG. 6 we show the optimal noise parameter p_a that minimizes N_0 and compare it to the optimal noise parameter p_a that maximizes the asymptotic key rate (Eq. (19)) for various disturbances D for the BB84 and the six-state protocol. It turns out that the optimal noise parameter p_a for the finite case is always higher than the one for the asymptotic case. In particular, for the asymptotic key rate the optimal p_a becomes non-zero for

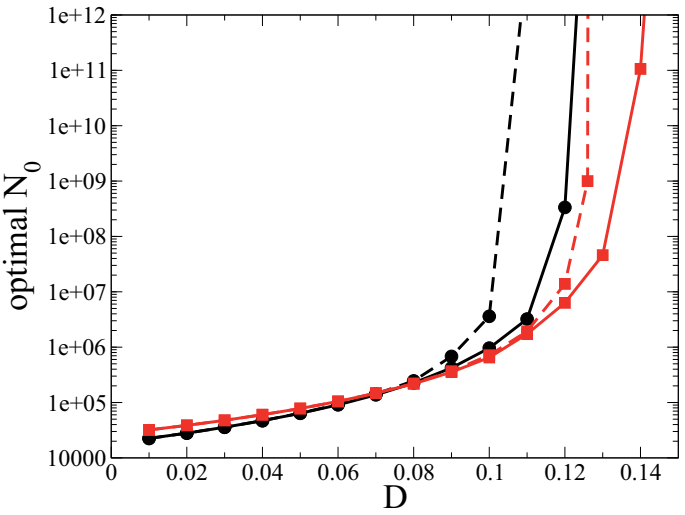

FIG. 5: (Color online) Comparison of the optimal minimal number N_0 to extract a non-zero key ($\varepsilon = 10^{-9}$) versus the QBER D introduced by Eve for the BB84 (circles (black)) and the six-state protocol (squares (red)); straight line: noise scenario 1 (see Section III), dashed line: no noise.

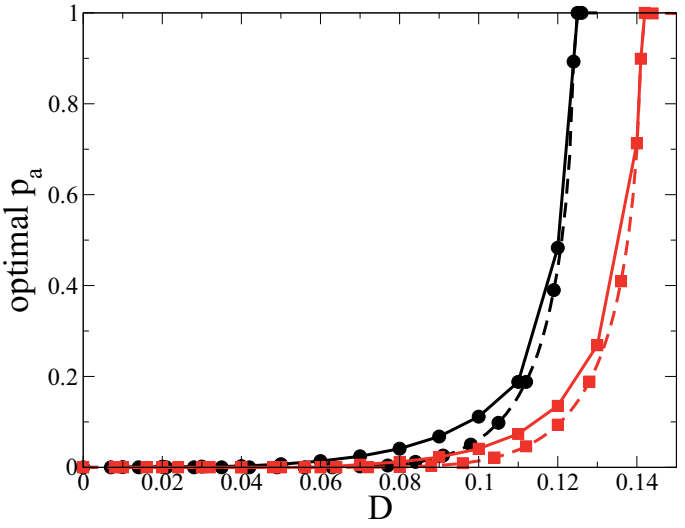

FIG. 6: (Color online) Comparison of the optimal noise parameter that minimizes N_0 (straight lines) for the finite-key rate (Eq. (13)) and the one that maximizes the asymptotic key rate (Eq. (19)) (dashed lines) versus the QBER D introduced by Eve for noise scenario 1 (see Section III); circles (black): BB84, squares (red): six-state.

around $D = 0.096$ ($D = 0.083$) for the six-state (BB84) protocol, while the benefit for the threshold N_0 in the finite scenario appears already for disturbances around 0.08 (0.06) for the six-state (BB84) protocol.

In FIG. 7 we show the optimal secret key rate r as a function of the number of signals N for a fixed disturbance $D = 0.1$ for the BB84 protocol and $D = 0.12$ for the six-state protocol, and compare it to the case without added noise. We obtain that the effect of noise on the

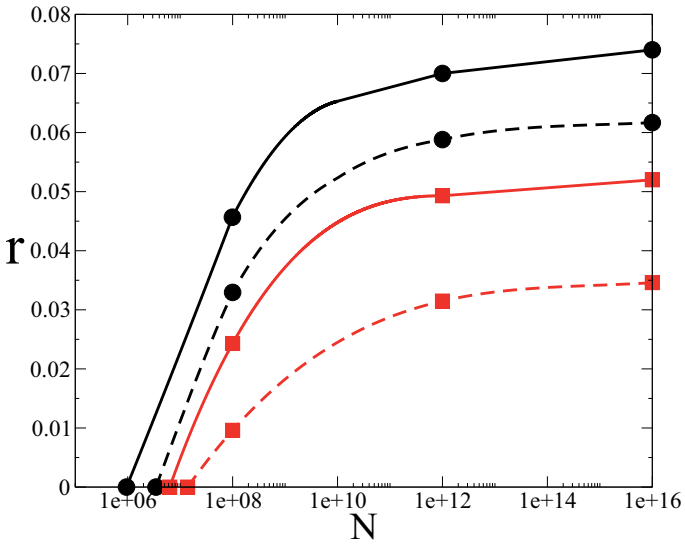

FIG. 7: (Color online) Comparison of the finite-key rate (Eq. (13)) versus signals N for a fixed disturbance D for the BB84 protocol ($D = 0.1$) (circles (black)) and the six-state protocol ($D = 0.12$) (squares (red)); straight line: noise scenario 1 (see Section III) for optimal noise parameter, dashed line: no noise. Lines are drawn to guide the eye.

finite-key rate is more beneficial than the effect on the asymptotic key rate, when taking the relative increase of the key rate as figure of merit. For example, for $N = 10^8$ signals we have an increase of 39% (153%) in the key rate, whereas the benefit for $N = 10^{16}$ is only about 20% (50%) for the BB84 (six-state) protocol.

B. Noise given by the channel

The equivalence of noise scenario 1 and 2 for $p_a = p_b$ allows us to interpret the results obtained in Section IV in another way. In contrast to adding noise deliberately the number p_b can be interpreted as the amount of noise that is introduced by the used quantum channel, which is unavoidable in real QKD settings, and not necessarily dedicated to the eavesdropper. This interpretation describes the situation in real experiments, where the assumption of unconditional security, i.e. all errors introduced by the channel have to be attributed to the eavesdropper, is over-pessimistic [7, 29]. If one makes the realistic assumption that Eve cannot replace the noisy channel by a noisefree one, the channel noise does not lead to knowledge of Eve about the key, and the key rate will thus increase. In FIG. 8 the finite-key rate (Eq. (13)) is shown as a function of the number of signals N sent through the channel for a fixed $QBER$ ($Q = 5\%$) for different values of the noise parameter p_b for the six-state and BB84 protocol. The measured $QBER$ contains both the noise p_b that we attribute to the channel and the noise D that is related to Eve's unitary interaction. For the explicit connection between these different types of noise see Eq. (27). Taking this fact into account leads to remarkably higher key rates, as shown in FIG. 8. For example, for $N = 10^8$ signals, without added noise the key rate in the six-state (BB84) protocol is 0.37 (0.34), while for channel noise of $p_b = 0.05$ it is 0.47 (0.46) for the six-state (BB84) protocol.

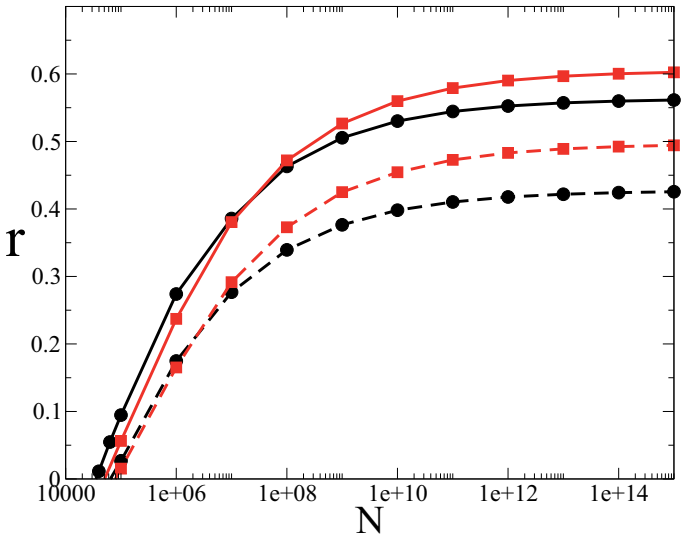

FIG. 8: (Color online) Comparison of the finite-key rates (Eq. (13)) ($\varepsilon = 10^{-9}$) versus number of signals N for various noise parameters p_b with $QBER = 5\%$ for the BB84 (circles (black)) and the six-state protocol (squares (red)); dashed lines: $p_b = 0$, straight lines: $p_b = 5\%$.

VI. CONCLUSIONS

In this article we have shown that the presence of quantum noise can improve secret key rates, in particular in the realistic scenario of a finite number of resources. We have investigated the effect of different noise scenarios on an ε-secure key rate for the BB84 and the six-state protocol in the entanglement-based scheme, for a finite number of signals. Our results can be interpreted in two ways: First, when taking the view that noise is added deliberately, it turns out that the effect of adding depolarizing noise to the state (before the state transmisson) is equal to the benefit gained by adding classical noise, i.e. when Alice performs probabilistic bit-flips on her measured bit string. We obtain that for both the BB84 and the six-state protocol the benefit (concerning the key rate) of adding noise is higher in the regime of a finite number of signals than for the asymptotic key rate. Second, under the realistic assumption that a channel itself introduces noise unavoidably, i.e. the noise is not necessarily created by the eavesdropper, the secret key rate increases significantly with respect to the "worst case", where all noise is attributed to Eve's intervention. This improvement comes from the fact that the errors from the quantum channel do not give Eve information about the key. This

approach avoids the over-pessimistic assumption of unconditional security, and is thus meaningful for realistic experiments.

Acknowledgments

We would like to thank Silvestre Abruzzo and Sylvia Bratzik for helpful discussions. This work was financially supported by Deutsche Forschungsgemeinschaft (DFG) and Bundesministerium für Bildung und Forschung (BMBF) project QuOReP.

[1] R. Renner, Int. J. Quant. Inf. **6**, 1 (2008).
[2] R. Renner and R. König, Lecture Notes in Computer Science **3378**, 407 (2005).
[3] R. Renner and S. Wolf, Lecture Notes in Computer Science **3788**, 199 (2005).
[4] T. Meyer, H. Kampermann, M. Kleinmann, and D. Bruß, Phys. Rev. A **74**, 042340 (2006).
[5] V. Scarani and R. Renner, in *Proceedings of TQC2008, Lecture Notes in Computer Science* (Springer Verlag, Berlin, 2008), vol. 5106, pp. 83–95.
[6] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).
[7] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[8] R. Cai and V. Scarani, New Journal of Physics **11**, 045024 (2009).
[9] L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301(R) (2010).
[10] S. Bratzik, M. Mertz, H. Kampermann, and D. Bruß, Phys. Rev. A **83** (2011).
[11] M. Tomamichel, C. W. Lim, N. Gisin, and R. Renner, arXiv:quant-ph/1103.4130 (2011).
[12] S. Abruzzo, M. Mertz, H. Kampermann, and D. Bruß, Phys. Rev. A **84**, 032321 (2011).
[13] M. Hayashi and T. Tsurumaru, arXiv:quant-ph/1107.0589 (2011).
[14] J. Bae and A. Acin, Phys. Rev. A **75**, 012334 (2007).
[15] J. M. Renes and G. Smith, Phys. Rev. Lett. **98**, 020502 (2007).
[16] G. Smith, J. M. Renes, and J. A. Smolin, Phys. Rev. Lett. **100**, 170502 (2008).
[17] O. Kern and J. M. Renes, Quantum Information and Computation **8**, 0756 (2008).
[18] J. M. Renes and R. Renner, arXiv:quant-ph/1008.0452 (2010).
[19] J. M. Renes and R. Renner, Information Theory, IEEE Transactions on **PP**, 1 (2010).
[20] Z. Shadman, H. Kampermann, T. Meyer, and D. Bruß, Int. J. Quant. Inform. **7**, 297 (2009).
[21] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[22] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59** (1999).
[23] C. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[24] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **55**, 5840 (2009).
[25] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[26] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[27] C. Fuchs and A. Peres, Phys. Rev. A **53**, 2038 (1996).
[28] I. Devetak and A. Winter, Proc. R. Soc. Lond. A **461**, 207 (2005).
[29] B. Qi, Y. Zhao, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. A **75**, 052304 (2007).

Quantum key distribution with finite resources: Taking advantage of quantum noise
Physical Review A (submitted in May 2012) [7 pages]
M. Mertz, H. Kampermann, Z. Shadman, and D. Bruß

Impact factor: 2.861
First author
Contribution to work by scientific work and preparation of the manuscript (90%)

Publication B

Secret key rates for coherent attacks

Markus Mertz,* Hermann Kampermann, Sylvia Bratzik, and Dagmar Bruß
Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf, 40225 Düsseldorf, Germany.
(Dated: June 30, 2012)

We develop a new method to quantify the secret key rate for permutation-invariant protocols for coherent attacks and finite resources. The method reduces the calculation of secret key rates for coherent attacks to the calculation for collective attacks by bounding the smooth min-entropy of permutation-invariant states via the smooth min-entropy of corresponding tensor-product states. The comparison of the results to the well-known post-selection technique for the BB84 and six-state protocol shows the high relevance of this method. Since our calculation of secret key rates for coherent attacks strongly depends on the way of treating collective attacks, a prospective progress in the analysis of collective attacks will immediately cause progress in our strategy.

I. INTRODUCTION

The aim of quantum key distribution (QKD) is the generation of a secret key between two authorized parties Alice and Bob in the presence of an eavesdropper Eve. In practical implementations the number of signals used to establish a secure key is finite. An essential element of the calculation of key rates for a finite number of signals is the evaluation of the smooth min-entropy [1] for high-dimensional states, which is in general hard or even impossible to compute. In the last years many results have appeared [1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11] considering the calculation of secret key rates for finite resources under the restriction of the eavesdropper's attack to a collective attack [12, 13], where Eve interacts with each signal independently and identically. This restriction leads to a state, which has tensor-product form and allows to bound the smooth min-entropy by the conditional von Neumann entropy of a single-signal state by using the asymptotic equipartition property (AEP) [1, 14].

In studies of coherent attacks [15, 16] the eavesdropper is not restricted at all, i.e. she may interact with all signals simultaneously. Already in the year 2005 it was shown in [17, 18] that for protocols, which are invariant under permutations of single-signal states, collective and coherent attacks are equivalent in the case of infinitely many signals. But for a finite number of signals this equivalence has not been proven yet. As a consequence the development of tools to compute a secret key for finite resources in the presence of coherent attacks is necessary.

Up to now direct strategies that treat coherent attacks only exist for the BB84 [19] protocol (see [10],[11]). In [10] Tomamichel et al used an uncertainty relation for smooth entropies [20] to circumvent the evaluation of the smooth min-entropy by the computation of the smooth max-entropy [1]. Since the resulting max-entropy has to be evaluated for a classical state, the calculation becomes analytically solvable.

In comparison to these direct strategies, many studies have focused on indirect approaches like post-selection [21] or the de Finetti approach [1, 22] to quantify secret key rates, where the analysis for coherent attacks is traced back to the investigation of collective attacks. In [7], these indirect approaches have been compared to each other for the BB84 protocol with the result, that the post-selection technique exceeds the de Finetti approach in terms of secure key rates.

In this paper we present a new strategy to calculate secret key rates for general permutation-invariant (i.e. the output of the protocol remains the same under permutations of the input pairs) protocols for coherent attacks. In particular, we relate the secret key rate for coherent attacks to the calculation of secret key rates for collective attacks by bounding the smooth min-entropy of a permutation-invariant state via the min-entropy of a corresponding tensor-product state "smoothed" over a reduced environment. We compare the results to the post-selection technique by applying the AEP-bound for the treatment of collective attacks. Note that most of the protocols studied in the literature already fulfill the condition of permutation-invariance or can made to be permutation-invariant, like e.g the BB84 and six-state [23, 24] protocol.

The paper is organized as follows. In Section II we explain the protocol and fix the notation. We clarify the formalism used to calculate secret key rates under the assumption of collective attacks in Section III. The formalism to analyze coherent attacks, the main result of this paper, is presented in Section IV. Section V shortly reviews the post-selection technique, which is then compared to the new strategy with respect to secret key rates for the BB84 and six-state protocol in Section VI. Finally, Section VII concludes the paper.

II. PRELIMINARIES

In this paper we consider permutation-invariant entanglement-based QKD protocols, which consist of the steps: state distribution, sifting, parameter estimation (PE), error correction (EC), error verification and privacy amplification (PA) (for a detailed description see [17, 18]). Here, permutational invariance means that for

*Electronic address: mertz@thphy.uni-duesseldorf.de

any permutation of the input pairs the output of the protocol remains unchanged. In the following we denote by ρ_{AB}^{N} the initial state of N signals shared by Alice and Bob, and by ρ_{ABE}^{N} a purification of ρ_{AB}^{N}, which describes the state shared by Alice, Bob and Eve after the state distribution. Now, let $\mathcal{N}_{AB}$ be the operation, that represents the procedures, which Alice and Bob perform on their states, i.e. measurement, sifting, parameter estimation, error correction and error verification. (Note that privacy amplification is not included here, since the output of this procedure is the final bit-string used as key.) Then we define the resulting classical-quantum state containing Alice's bit string and Eve's quantum state as $\rho_{XE}^{n} := (\mathcal{N}_{AB} \otimes \mathbb{1}_E)\, \rho_{ABE}^{N}$. As the main quantity for the calculation of secret key rates we use the smooth min-entropy [1]

$$H_{\min}^{\varepsilon}(\rho_{AE}|E) := \sup_{\sigma_{AE} \in \mathcal{B}^{\frac{\varepsilon}{2}}(\rho_{AE})} \sup_{\rho_E \in \mathcal{S}(\mathcal{H}_E)} H_{\min}(\sigma_{AE}|\rho_E), \tag{1}$$

defined as an optimization of the min-entropy

$$H_{\min}(\sigma_{AE}|\rho_E) := \sup\left\{\lambda \in \mathbb{R} : 2^{-\lambda}\mathbb{1}_A \otimes \rho_E - \sigma_{AE} \geq 0\right\} \tag{2}$$

over an $\frac{\varepsilon}{2}$-environment given by

$$\mathcal{B}^{\frac{\varepsilon}{2}}(\rho) := \left\{\sigma : \frac{1}{2}\,||\sigma - \rho||_1 \leq \frac{\varepsilon}{2}\right\}, \tag{3}$$

with the 1-norm $||A||_1 = \mathrm{tr}\left(\sqrt{AA^\dagger}\right)$. $\mathcal{S}(\mathcal{H}_E)$ denotes the set of density operators on the Hilbert space $\mathcal{H}_E$.

III. COLLECTIVE ATTACK

In contrast to coherent attacks, the assumption of collective attacks forces the eavesdropper Eve to interact with each of the signals separately. Under this restriction the distributed state can for permutation-invariant protocols be regarded as a product state $\rho_{AB}^{\otimes N}$, which is diagonal in the Bell-basis [17, 18]. We denote by m the number of randomly chosen signals used for parameter estimation and by n the remaining number of signals for privacy amplification. Then, the rate of an ε-secure key can be quantified in the following way.

Theorem 1. *[3] Let $\varepsilon_{\mathrm{PE}}, \varepsilon_{\mathrm{EC}}, \varepsilon_{\mathrm{PA}}, \bar{\varepsilon} > 0$ and let $\rho_{XE}^{\otimes n} = (\mathcal{N}_{AB} \otimes \mathbb{1}_E)\, \rho_{ABE}^{\otimes N}$ be a tensor-product state for a purification ρ_{ABE} in $\mathcal{H}_{ABE}$ of the state $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$. Then the rate of an $\varepsilon_{\mathrm{coll}} := (\varepsilon_{\mathrm{PE}} + \varepsilon_{\mathrm{EC}} + \varepsilon_{\mathrm{PA}} + \bar{\varepsilon})$-secure key is given by*

$$r := \frac{1}{N} \inf_{\rho_{AB} \in \Gamma_{\mathrm{coll}}} \left(H_{\min}^{\bar{\varepsilon}}\left(\rho_{XE}^{\otimes n}|E\right) - \mathrm{leak}_{\mathrm{EC}}\right) + \frac{2}{N}\log_2(2\varepsilon_{\mathrm{PA}}). \tag{4}$$

The smooth min-entropy of the classical-quantum state $\rho_{XE}^{\otimes n}$ shared by Alice and Eve and the correction $2\log_2(2\varepsilon_{\mathrm{PA}})$ arise from the analysis of privacy amplification. The entropy quantifies Eve's uncertainty of Alice's bit-string.

The term $\mathrm{leak}_{\mathrm{EC}}$ stands for the number of bits which Alice and Bob leak to the eavesdropper due to public communication during the error correction procedure and cost for the error verification. In total, the leakage can be estimated by [3, 10]

$$\mathrm{leak}_{\mathrm{EC}} := n1.1H(X|Y) + \log_2\left(\frac{2}{\varepsilon_{\mathrm{EC}}}\right). \tag{5}$$

Here, the factor 1.1 denotes the efficiency of a specific error-correction protocol used during the key-generation. The minimization of the smooth min-entropy is due to parameter estimation, where we only except qubit-states ρ_{AB} which are contained in the set [10]

$$\Gamma_{\mathrm{coll}} := \left\{\sigma_{AB} : \frac{1}{2}\,||P_m - P_n||_1 \leq \xi(\varepsilon_{\mathrm{PE}}, n, m)\right\} \tag{6}$$

with

$$\xi(\varepsilon_{\mathrm{PE}}, n, m) := \sqrt{\frac{(n+m)(m+1)\ln(1/\varepsilon_{\mathrm{PE}})}{8m^2 n}}. \tag{7}$$

This means, that the tolerated quantum bit error rate ($QBER$) P_m due to an m-fold independent application of a $POVM$ $\mathcal{E}$ on a tensor-product state is ξ-close to the parameter P_n, which corresponds to a virtual measurement on the remaining n signals, which are used for the key generation, except with probability $\varepsilon_{\mathrm{PE}}$ (see Lemma 6 in the Appendix). Note that this estimate has been developed in [10] for coherent attacks, i.e. Lemma 6 holds for permutation-invariant states. As tensor-product states in collective attacks are permutation-invariant, Lemma 6 can be applied.

For product states $\rho_{XE}^{\otimes n}$ we can use the asymptotic equipartition property (see Eq. (B7)) to bound the smooth min-entropy by the conditional von Neumann entropy of a single copy ρ_{XE}. Finally, we get for the rate of an $\varepsilon_{\mathrm{coll}} := (\varepsilon_{\mathrm{PE}} + \varepsilon_{\mathrm{EC}} + \varepsilon_{\mathrm{PA}} + \bar{\varepsilon})$-secure key:

$$\begin{aligned} r_{\mathrm{coll}} \;:=\; & \frac{n}{N}\left[\inf_{\rho_{AB} \in \Gamma_{\mathrm{coll}}}\left(S(X|E) - \frac{\mathrm{leak}_{\mathrm{EC}}}{n}\right)\right. \\ & \left. -\; 5\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}}\right] + \frac{2}{N}\log_2(2\varepsilon_{\mathrm{PA}}) \end{aligned} \tag{8}$$

where

$$S(X|E) = S(\rho_{XE}) - S(\rho_E) \tag{9}$$

with $S(\rho) := -\,\mathrm{tr}(\rho \log_2 \rho)$.

In the next section we present a formalism to treat coherent attacks. We will see that the analysis of secret key rates for coherent attacks can be traced back to the calculation of secret key rates under the assumption of collective attacks (see Eq. (8)).

IV. COHERENT ATTACK

A coherent attack is the most general attack an eavesdropper can perform, i.e. Eve is not restricted at all. For the investigation of secret key rates for coherent attacks, we have to consider non-product states for the evaluation of the smooth-min entropy. No changes are needed in the analysis of parameter estimation for collective attacks (see Eq. (6)), because it also holds for coherent attacks (i.e. non-product states (see Lemma 6 in the Appendix)). Since error correction and error verification are also independent of the underlying attack of the eavesdropper (they are purely classical procedures), the protocol analysis for these steps can be adopted from the one for collective attacks.

For permutation-invariant protocols it has been shown in [17] and [18] that we can assume w.l.o.g. that, after the distribution of N qubit pairs, Alice and Bob share a permutation-invariant quantum state, which is a convex combination of tensor-products of Bell-states:

$$\rho_{AB}^{N}=\mathcal{P}_{N}\left(\sum_{\mathbf{n}\in\Lambda^{N}}\mu_{\mathbf{n}}\sigma_{1}^{\otimes n_{1}}\otimes\sigma_{2}^{\otimes n_{2}}\otimes\sigma_{3}^{\otimes n_{3}}\otimes\sigma_{4}^{\otimes n_{4}}\right) \tag{10}$$

with probabilities $\mu_{\mathbf{n}}$ for the "realization" $\mathbf{n}$ and the set of realizations

$$\Lambda^{N}:=\left\{\mathbf{n}=(n_{1},n_{2},n_{3},n_{4}):\sum_{i=1}^{4}n_{i}=N\right\}. \tag{11}$$

The σ_i for $i=1,..,4$ correspond to the projector onto the 4 Bell-states in $\mathcal{H}_A\otimes\mathcal{H}_B$, i.e.

$$\begin{aligned}\sigma_{1}&=\left|\phi^{+}\right\rangle\left\langle\phi^{+}\right|,\\ \sigma_{2}&=\left|\phi^{-}\right\rangle\left\langle\phi^{-}\right|,\\ \sigma_{3}&=\left|\psi^{+}\right\rangle\left\langle\psi^{+}\right|,\\ \sigma_{4}&=\left|\psi^{-}\right\rangle\left\langle\psi^{-}\right|,\end{aligned} \tag{12}$$

with

$$\left|\phi^{\pm}\right\rangle:=\frac{1}{\sqrt{2}}\left(|00\rangle\pm|11\rangle\right)\qquad\text{and} \tag{13}$$

$$\left|\psi^{\pm}\right\rangle:=\frac{1}{\sqrt{2}}\left(|01\rangle\pm|10\rangle\right). \tag{14}$$

$\mathcal{P}_N$ denotes the completely positive map (CPM) which symmetrizes the state with respect to all possible distinguishable permutations of the N qubit pairs.

The following section explains the analysis of parameter estimation for permutation-invariant states (see Eq. (10)).

A. Parameter estimation

Let the sifting procedure now be such that $N_s=n+m$ signals remain, where m denotes the number of randomly chosen signals used for parameter estimation and n denotes the remaining number of signals for privacy amplification. Then we can adopt Lemma 6 to estimate the $QBER\ Q_n$ by the tolerated $QBER\ Q_m$ coming from a measurement on general permutation-invariant states (see also the arguments below Eq. (7)).

Theorem 2. *Let $\varepsilon_{\mathrm{PE}}>0$ and $m+n=N_s$. Let $\rho_{AB}^{N_s}\in\mathcal{S}\left(\mathcal{H}_{AB}^{\otimes N_s}\right)$ be a permutation-invariant quantum state, and let $\mathcal{E}$ be a POVM on $\mathcal{H}_{AB}$ which measures the QBER. Let $\mathbf{Q}_m$ and $\mathbf{Q}_n$ be the frequency distributions when applying the measurement $\mathcal{E}^{\otimes m}$ and $\mathcal{E}^{\otimes n}$, respectively, to different subsystems of $\rho_{AB}^{N_s}$. Then for any element Q_m and Q_n from $\mathbf{Q}_m$ and $\mathbf{Q}_n$ except with probability $\varepsilon_{\mathrm{PE}}$*

$$\frac{1}{2}\left|\left|Q_{m}-Q_{n}\right|\right|_{1}\leq\xi\left(\varepsilon_{\mathrm{PE}},n,m\right) \tag{15}$$

with $\xi(\varepsilon_{\mathrm{PE}},n,m):=\sqrt{\frac{(m+n)(m+1)\ln\left(1/\varepsilon_{\mathrm{PE}}\right)}{8m^{2}n}}$.

Proof: This follows directly from Lemma 6 in the Appendix, which is a consequence of [10]. □

Now with the definition of the set of states, which pass the parameter estimation procedure

$$\Gamma_{\varepsilon_{\mathrm{PE}}}^{n}:=\left\{\sigma_{AB}^{n}:\frac{1}{2}\left|\left|Q_{m}-Q_{n}\right|\right|_{1}\leq\xi\left(\varepsilon_{\mathrm{PE}},n,m\right)\right\}, \tag{16}$$

we are able to give an analytic expression for the rate of an ε-secure key for coherent attacks.

Corollary 1. *Let $\varepsilon_{\mathrm{PE}},\varepsilon_{\mathrm{EC}},\varepsilon_{\mathrm{PA}},\bar{\varepsilon}>0$ and let $\rho_{XE}^{n}=\left(\mathcal{N}_{AB}\otimes\mathbb{1}_{E}\right)\rho_{ABE}^{N}$ be a permutation-invariant state for a purification ρ_{ABE}^{N} in $\mathcal{H}_{ABE}^{\otimes N}$ of $\rho_{AB}^{N}\in\mathcal{S}\left(\mathcal{H}_{AB}^{\otimes N}\right)$. Then the rate of an $\varepsilon_{\mathrm{coh}}:=(\varepsilon_{\mathrm{PE}}+\varepsilon_{\mathrm{EC}}+\varepsilon_{\mathrm{PA}}+\bar{\varepsilon})$-secure key is given by*

$$r:=\frac{1}{N}\inf_{\rho_{AB}^{n}\in\Gamma_{\varepsilon_{\mathrm{PE}}}^{n}}\left(H_{\min}^{\bar{\varepsilon}}\left(\rho_{XE}^{n}|E\right)-\mathrm{leak}_{\mathrm{EC}}\right)+\frac{2}{N}\log_{2}\left(2\varepsilon_{\mathrm{PA}}\right). \tag{17}$$

In the following section we show that the smooth min-entropy for permutation-invariant states can be mainly bounded by the min-entropy for corresponding product-states "smoothed" over a reduced ε-environment.

B. Privacy amplification

In order to get a calculable formula for the key rate (Eq. (17)) we bound the smooth min-entropy for permutation-invariant states by the smooth min-entropy for tensor-product states, which then can be easily evaluated by the asymptotic equipartition property (Eq. (B7)) as explained in Section III.

We now define analogously to Eq. (10) the permutation-invariant state with n signals, which Alice

and Bob share after the parameter estimation procedure.

$$\rho_{AB}^{n} := \mathcal{P}_n \left(\sum_{\mathbf{n}\in\Lambda^n} \mu_{\mathbf{n}} \sigma_1^{\otimes n_1} \otimes \sigma_2^{\otimes n_2} \otimes \sigma_3^{\otimes n_3} \otimes \sigma_4^{\otimes n_4} \right), \tag{18}$$

where σ_i with $i = 1,..,4$ correspond to the projectors onto the 4 Bell-states in $\mathcal{H}_A \otimes \mathcal{H}_B$ and $\Lambda^n := \left\{ \mathbf{n} = (n_1, n_2, n_3, n_4) : \sum_{i=1}^4 n_i = n \right\}$ (see Eq. (10)). Additionally, we denote the single-copy state shared by Alice and Bob in the following as

$$\sigma_{AB}[\boldsymbol{\lambda}] := \sum_{i=1}^{4} \lambda_i \sigma_i \tag{19}$$

with $\boldsymbol{\lambda} := (\lambda_1, \lambda_2, \lambda_3, \lambda_4) = \left(\frac{n_1}{n}, \frac{n_2}{n}, \frac{n_3}{n}, \frac{n_4}{n}\right)$.

The next theorem is one of our central results. It gives a relation between the smooth min-entropy for permutation-invariant states and the smooth min-entropy for tensor-product states. The proof is inspired by [18] and uses the fact, that there exists a certain measurement on $\sigma_{AB}[\boldsymbol{\lambda}]^{\otimes n}$, such that the resulting state is equal to the state ρ_{AB}^n for a specific realization $\mathbf{n}$. Then, the application of some fundamental properties of the smooth min-entropy leads to the result.

Theorem 3. *Let $\bar{\varepsilon} > 0$, $\boldsymbol{\lambda} = \left(\frac{n_1}{n}, \frac{n_2}{n}, \frac{n_3}{n}, \frac{n_4}{n}\right)$ and $\mathcal{M}_{AB}$ be the quantum operation which describes the local measurements Alice and Bob perform followed by a partial-trace operation on Bob's part ($\mathcal{H}_B$). Let $\rho_{XE}^n = \left(\mathcal{M}_{AB} \otimes \mathbb{1}_E\right)^{\otimes n} \rho_{ABE}^n$ be the classical quantum state obtained after applying the quantum operation $\left(\mathcal{M}_{AB} \otimes \mathbb{1}_E\right)^{\otimes n}$ on a purification ρ_{ABE}^n in $\mathcal{H}_{ABE}^{\otimes n}$ of a permutation-invariant state $\rho_{AB}^n \in \mathcal{S}\left(\mathcal{H}_{AB}^{\otimes n}\right)$. Analogously let $\sigma_{XE}[\boldsymbol{\lambda}]^{\otimes n} = \left(\mathcal{M}_{AB} \otimes \mathbb{1}_E\right)^{\otimes n} \sigma_{ABE}[\boldsymbol{\lambda}]^{\otimes n}$ be the classical quantum state obtained after applying the quantum operation $\left(\mathcal{M}_{AB} \otimes \mathbb{1}_E\right)^{\otimes n}$ on a purification $\sigma_{ABE}[\boldsymbol{\lambda}]^{\otimes n}$ of a tensor-product state $\sigma_{AB}[\boldsymbol{\lambda}]^{\otimes n} \in \mathcal{S}\left(\mathcal{H}_{AB}^{\otimes n}\right)$. Let $\mathcal{E}$ be a POVM on $\mathcal{H}_A \otimes \mathcal{H}_B$ which measures the QBER. Let Q_n, P_n be an element of the frequency distribution $\mathbf{Q}_n$, $\mathbf{P}_n$ of the outcomes when applying the measurement $\mathcal{E}^{\otimes n}$ to ρ_{AB}^n and $\sigma_{AB}^{\otimes n}$, respectively. Then except with probability $\bar{\varepsilon}$*

$$H_{\min}^{\bar{\varepsilon}}\left(\rho_{XE}^n | E\right) \geq H_{\min}^{\bar{\varepsilon}/(2n^2)}\left(\sigma_{XE}^{\otimes n}\left[\boldsymbol{\lambda} = \frac{\mathbf{n}}{n}\right] | E\right) - 1, \tag{20}$$

where

$$\Gamma_{\text{coh}} := \left\{ \tau_{AB} : \frac{1}{2} ||Q_m - P_n||_1 \leq \xi_{\text{coh}}\left(\bar{\varepsilon}, n, m\right) \right\} \tag{21}$$

with

$$\xi_{\text{coh}}\left(\bar{\varepsilon}, n, m\right) := \frac{1}{2}\xi_{\text{att}}\left(\bar{\varepsilon}, 2, n\right) + \xi\left(\frac{\bar{\varepsilon}}{2}, n, m\right) \tag{22}$$

where

$$\xi_{\text{att}}(\bar{\varepsilon}, 2, n) := \sqrt{\frac{16\ln(2) + 8\ln\left(1/\bar{\varepsilon}\right)}{n}} \tag{23}$$

and

$$\xi\left(\frac{\bar{\varepsilon}}{2}, n, m\right) := \sqrt{\frac{(m+n)(m+1)\ln\left(2/\bar{\varepsilon}\right)}{8m^2 n}} \tag{24}$$

defines the set of tensor-product states $\tau^{\otimes n}$ which pass the parameter estimation procedure.

Proof: The state to be considered is given by ρ_{XE}^n and can be expressed as a convex combination of states for all possible realizations $\mathbf{n}$ with probability $\mu_{\mathbf{n}}$, i.e.

$$\rho_{XE}^n = \sum_{\mathbf{n}\in\Lambda^n} \mu_{\mathbf{n}} \rho_{XE}^n[\mathbf{n}]. \tag{25}$$

Note that this structure is provided in Eq. (18) and is conserved due to the linearity of $\mathcal{M}_{AB}$ and a purification of ρ_{AB}^n, which is optimal for Eve.

The first part proves the theorem for the special case, that only one $\mu_{\mathbf{n}}$ in Eq. (25) is non-zero, i.e. we consider a single realization $\mathbf{n}$. Then, part 2 extends part 1 to the general case.

Part 1:

Let $|\phi_i\rangle$ be an extension to $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ of σ_i (see Eq. (18)) with the condition, that the remaining states $\text{tr}_{AB}\left(P_{|\phi_i\rangle}\right)$ are mutually orthogonal for $i \in \{1,..,4\}$. Note that this choice of orthogonal ancillas is optimal, since it enables the eavesdropper to distinguish perfectly the reduced states shared by Alice and Bob. Let S_n be the set of distinguishable permutations π on n qubits for a fixed realization $\mathbf{n}$. Then, with

$$|\psi\rangle_{ABE}^{\mathbf{n}} := \frac{1}{\sqrt{|S_n|}} \sum_{\pi\in S_n} \pi\left(\bigotimes_{i=1}^{4} |\phi_i\rangle^{\otimes n_i}\right) \tag{26}$$

and

$$|\phi\rangle_{ABE}^{\boldsymbol{\lambda}} := \sum_{i=1}^{4} \sqrt{\lambda_i}\, |\phi_i\rangle \tag{27}$$

we define

$$\rho_{XE}^n[\mathbf{n}] := \left(\mathcal{M}_{AB} \otimes \mathbb{1}_E\right)^{\otimes n} P_{|\psi\rangle_{ABE}^{\mathbf{n}}} \tag{28}$$

$$\sigma_{XE}[\boldsymbol{\lambda}] := \left(\mathcal{M}_{AB} \otimes \mathbb{1}_E\right) P_{|\phi\rangle_{ABE}^{\boldsymbol{\lambda}}} \tag{29}$$

for an arbitrary, but fixed realization $\mathbf{n}$. For any $i \in \{1,..,4\}$ let P_i be the projector onto the support of $\left(\mathcal{M} \otimes \mathbb{1}_E\right) P_{|\phi_i\rangle}$ which by definition are orthogonal for distinct i. Let $\mathcal{F}$ be a measurement defined by

$$\mathcal{F} : \rho \to \sum_{z=0}^{1} F_z \rho F_z^\dagger \otimes |z\rangle\langle z|, \tag{30}$$

where

$$F_0 := \sum_{\pi\in S_n} \pi\left(P_1^{\otimes n_1} \otimes P_2^{\otimes n_2} \otimes P_3^{\otimes n_3} \otimes P_4^{\otimes n_4}\right) \tag{31}$$

and $F_1 := \mathbb{1} - F_0$. Then F_0 picks out a specific realization $\mathbf{n}$ from the tensor-product state $\sigma_{XE}[\boldsymbol{\lambda}]^{\otimes n}$, i.e.

$$\rho^n_{XE}[\mathbf{n}] = \frac{1}{P_Z(Z=0)} F_0 \left(\sigma_{XE}[\boldsymbol{\lambda}]^{\otimes n}\right) F_0^\dagger \tag{32}$$

with $P_Z(Z=0) = \mathrm{tr}\left(F_0 \left(\sigma^{\otimes n}_{XE}[\boldsymbol{\lambda}]\right) F_0^\dagger\right) = |S_n| \prod_{i=1}^4 \lambda_i^{n_i}$ (For a detailed proof see [18], Lemma $A.4$).

Now let $\bar{\rho}^n_{XEZ}[\mathbf{n}]$ be the resulting state after applying $\mathcal{F}$ on $\sigma^{\otimes n}_{XE}[\boldsymbol{\lambda}]$ and let Z be the classical measurement outcome, i.e.

$$\begin{aligned} \bar{\rho}^n_{XEZ}[\mathbf{n}] &= \sum_{z=0}^{1} F_z \sigma^{\otimes n}_{XE}[\boldsymbol{\lambda}] F_z^\dagger \otimes |z\rangle\langle z| &(33)\\ &=: \sum_{z=0}^{1} P_Z(Z=z) \bar{\rho}^{nZ=z}_{XE}[\mathbf{n}] \otimes |z\rangle\langle z| \,. &(34)\end{aligned}$$

Then it follows directly from Eq. (32) that

$$\rho^n_{XE}[\mathbf{n}] = \bar{\rho}^{nZ=0}_{XE}[\mathbf{n}] \tag{35}$$

and therefore

$$H^{\bar{\varepsilon}}_{\min}\left(\rho^n_{XE}[\mathbf{n}]|E\right) = H^{\bar{\varepsilon}}_{\min}\left(\bar{\rho}^{nZ=0}_{XE}[\mathbf{n}]|E\right). \tag{36}$$

With some fundamental properties of the smooth min-entropy we get

$$\begin{aligned} & H^{\bar{\varepsilon}}_{\min}\left(\bar{\rho}^{nZ=0}_{XE}[\mathbf{n}]|E\right)\\ \overset{Eq.\ (A7)}{\geq}\ & H^{p_Z(Z=0)\bar{\varepsilon}}_{\min}\left(\bar{\rho}^n_{XEZ}[\mathbf{n}]|EZ\right)\\ \overset{Eq.\ (B1)}{\geq}\ & H^{p_Z(Z=0)\bar{\varepsilon}}_{\min}\left(\bar{\rho}^n_{XEZ}[\mathbf{n}]|E\right) - \log_2\left(\mathrm{rank}(\rho_Z)\right). \end{aligned} \tag{37}$$

By definition, the orthogonality and completeness of the set $\{F_z\}$ ensures that $\mathrm{tr}_Z\left(\bar{\rho}^n_{XEZ}[\mathbf{n}]\right) = \sigma^{\otimes n}_{XE}[\boldsymbol{\lambda}]$, such that we can apply Eq. (A2) in the Appendix. This leads to

$$\begin{aligned} & H^{p_Z(Z=0)\bar{\varepsilon}}_{\min}\left(\bar{\rho}^n_{XEZ}[\mathbf{n}]|E\right) - \log_2\left(\mathrm{rank}(\rho_Z)\right)\\ \overset{Eq.\ (A2)}{\geq}\ & H^{p_Z(Z=0)\bar{\varepsilon}}_{\min}\left(\sigma^{\otimes n}_{XE}[\boldsymbol{\lambda}]|E\right) - \log_2\left(\mathrm{rank}(\rho_Z)\right)\\ \geq\ & H^{\bar{\varepsilon}/n^2}_{\min}\left(\sigma^{\otimes n}_{XE}[\boldsymbol{\lambda}]|E\right) - 1, \end{aligned} \tag{38}$$

where we used in the last step that $\mathrm{rank}(\rho_Z) \leq 2$ and from Lemma 7 in the Appendix that

$$p_Z(Z=0) = |S_n| \prod_{i=1}^4 \lambda_i^{n_i} > 1/n^2. \tag{39}$$

The following part generalizes the proof to the unrestricted case.

Part 2:

Now let $\rho^n_{ABE} := P_{|\psi\rangle}$ with

$$|\psi\rangle := \sum_{\mathbf{n}\in\Lambda^n} \sqrt{\mu_{\mathbf{n}}}\, |\psi\rangle^{\mathbf{n}}_{ABE} \tag{40}$$

be a purification of ρ^n_{AB}. For any $\mathbf{n} \in \Lambda^n$ let $\mathcal{H}^n_E$ be the smallest subspace of $\mathcal{H}^{\otimes n}_E$ containing the support of the traces $\rho^n_E[\mathbf{n}] = \mathrm{tr}_{\mathcal{H}^{\otimes n}_{AB}}\left(\rho^n_{ABE}[\mathbf{n}]\right)$. By the definition of the vectors $|\phi_i\rangle$ as in part 1, the subspaces $\mathcal{H}^n_E$ are orthogonal for distinct $\mathbf{n} \in \Lambda^n$. There exists a projective measurement $\mathcal{F}'$ onto the subspaces $\mathcal{H}^{\otimes n}_{AB} \otimes \mathcal{H}^n_E$. Now let the state $\tilde{\rho}^n_{XEZ'}$ be the resulting state from the measurement $\mathcal{F}'$ of the state ρ^n_{XE} and let $Z' \in \Lambda^n$ be the classical outcome, i.e.

$$\begin{aligned} \tilde{\rho}^n_{XEZ'} &= \sum_{\mathbf{n}\in\Lambda^n} F'_{\mathbf{n}} \rho^n_{XE} F'^\dagger_{\mathbf{n}} \otimes |\mathbf{n}\rangle\langle\mathbf{n}| &(41)\\ &=: \sum_{\mathbf{n}\in\Lambda^n} \mu_{\mathbf{n}} \rho^n_{XE}[\mathbf{n}] \otimes |\mathbf{n}\rangle\langle\mathbf{n}| \,. &(42)\end{aligned}$$

By the definition of the state ρ^n_{XE} we know that for a tolerated $QBER$ Q_m the parameter Q_n for a virtual measurement on n signals has to fulfil except with probability $\frac{\bar{\varepsilon}}{2}$ that

$$\frac{1}{2}\left|\left|Q_m - Q_n\right|\right|_1 \leq \xi\left(\frac{\bar{\varepsilon}}{2}, n, m\right). \tag{43}$$

Note that the choice of $\frac{\bar{\varepsilon}}{2}$ is arbitrary. In principle, the introduction of a new parameter could lead to better results. Now, this condition implies that realizations $\mathbf{n}$ in the permutation-invariant state $\rho^n_{AB} = \sum_{\mathbf{n}\in\Lambda^n} \mu_{\mathbf{n}} \rho^n_{AB}[\mathbf{n}]$, whose corresponding parameter Q_n does not fulfill the condition in Eq. (43), only appear with small probability, i.e. more precisely

$$\sum_{\mathbf{n}:\frac{1}{2}||Q_m - Q_n||_1 > \xi(\frac{\bar{\varepsilon}}{2},n,m)} \mu_{\mathbf{n}} \leq \frac{\bar{\varepsilon}}{2}. \tag{44}$$

This behaviour of the probabilities enables us to apply Eq. (A6) in the Appendix for probability $\varepsilon' = \frac{\bar{\varepsilon}}{2}$ to restrict the states $\rho^n_{AB}[\mathbf{n}]$ (or equivalently their corresponding realizations $\mathbf{n}$) to the set

$$\tilde{\Gamma}^n_{\bar{\varepsilon}/2} := \left\{\sigma^n_{AB}[\mathbf{n}] : \frac{1}{2}\left|\left|Q_m - Q_n\right|\right|_1 \leq \xi\left(\frac{\bar{\varepsilon}}{2}, n, m\right)\right\}. \tag{45}$$

Namely, we have

$$\begin{aligned} & H^{\bar{\varepsilon}}_{\min}\left(\rho^n_{XE}|E\right)\\ \overset{Eq.\ (A4)}{\geq}\ & H^{\bar{\varepsilon}}_{\min}\left(\tilde{\rho}^n_{XEZ'}|EZ'\right)\\ \overset{Eq.\ (A6)}{\geq}\ & \inf_{\rho^n_{AB}[\mathbf{n}]\in\tilde{\Gamma}^n_{\bar{\varepsilon}/2}} H^{\bar{\varepsilon}/2}_{\min}\left(\rho^n_{XE}[\mathbf{n}]|E\right). \end{aligned} \tag{46}$$

Then Eq. (46) becomes, together with Eq. (36), Eq. (37) and Eq. (38),

$$\begin{aligned} & \inf_{\rho^n_{AB}[\mathbf{n}]\in\tilde{\Gamma}^n_{\bar{\varepsilon}/2}} H^{\bar{\varepsilon}/2}_{\min}\left(\rho^n_{XE}[\mathbf{n}]|E\right)\\ \geq\ & \inf_{\rho^n_{AB}[\mathbf{n}]\in\tilde{\Gamma}^n_{\bar{\varepsilon}/2}} H^{\bar{\varepsilon}/(2n^2)}_{\min}\left(\sigma^{\otimes n}_{XE}[\boldsymbol{\lambda} = \frac{\mathbf{n}}{n}]|E\right) - 1 \end{aligned} \tag{47}$$

Since the min-entropy is now a function of a tensor-product state, we would like to express the restricting infimum in terms of the statistics $\mathbf{P}_n$ of this tensor-product. By definition, we have $\rho^1_{XE}[\mathbf{n}] = \sigma_{XE}[\boldsymbol{\lambda} = \frac{\mathbf{n}}{n}]$, such that we can apply Lemma 8 in the Appendix (for $k = N = n$), which states that, except with probability $\bar{\varepsilon}$, the statistics $\mathbf{P}_n$ of the tensor-product state $\sigma^{\otimes n}_{XE}[\boldsymbol{\lambda} = \frac{\mathbf{n}}{n}]$ is ξ_{att}-close to $\mathbf{Q}_n$, i.e.

$$\frac{1}{2}\left|\left|\mathbf{Q}_n - \mathbf{P}_n\right|\right|_1 \leq \xi_{\text{att}}\left(\bar{\varepsilon}, |\mathcal{E}|, n\right). \tag{48}$$

(Here the choice of $\bar{\varepsilon}$ is arbitrary. The consideration of a new parameter could in general lead to better results.) Now, we are able to bound the distance between $\mathbf{P}_n$ and the tolerated $QBER$ $\mathbf{Q}_m$ measured during parameter estimation by using the triangular inequality.

$$\begin{aligned}\frac{1}{2}\left|\left|Q_m - P_n\right|\right|_1 &\leq \frac{1}{2}\left|\left|Q_m - Q_n\right|\right|_1 + \frac{1}{2}\left|\left|Q_n - P_n\right|\right|_1 \\ &\leq \xi\left(\frac{\bar{\varepsilon}}{2}, n, m\right) + \frac{\xi_{\text{att}}\left(\bar{\varepsilon}, 2, n\right)}{2} \\ &=: \xi_{\text{coh}}\left(\bar{\varepsilon}, n, m\right),\end{aligned} \tag{49}$$

where we used that for the $POVM$ applied for parameter estimation (see Eq. (6) and Section IV A) the number of $POVM$ elements becomes 2 (see [8]) and that [8]

$$\frac{1}{2}\left|\left|Q_n - P_n\right|\right|_1 \leq \frac{1}{2}\frac{1}{2}\left|\left|\mathbf{Q}_n - \mathbf{P}_n\right|\right|_1. \tag{50}$$

Consequently we end up in

$$\begin{aligned}&\inf_{\rho^n_{AB}[\mathbf{n}] \in \tilde{\Gamma}^n_{\bar{\varepsilon}/2}} H_{\min}^{\bar{\varepsilon}/(2n^2)}\left(\sigma^{\otimes n}_{XE}[\boldsymbol{\lambda} = \frac{\mathbf{n}}{n}]|E\right) - 1 \\ \geq &\inf_{\sigma_{AB} \in \Gamma_{\xi_{\text{coh}}}} H_{\min}^{\bar{\varepsilon}/(2n^2)}\left(\sigma^{\otimes n}_{XE}\left[\boldsymbol{\lambda} = \frac{\mathbf{n}}{n}\right]|E\right) - 1.\end{aligned} \tag{51}$$

The assertion then follows by putting Eq. (51) and Eq. (47) into Eq. (46). □

Finally, we are able to formulate a calculable rate of an ε_{coh}-secure key for coherent attacks.

Theorem 4. *Let $\varepsilon_{\text{PE}}, \varepsilon_{\text{EC}}, \varepsilon_{\text{PA}}, \bar{\varepsilon} > 0$ and let $\rho^n_{XE} = (\mathcal{N}_{AB} \otimes \mathbb{1}_E)\,\rho^N_{ABE}$ be a permutation-invariant state for a purification ρ^N_{ABE} in $\mathcal{H}^{\otimes N}_{ABE}$ of $\rho^N_{AB} \in \mathcal{S}\left(\mathcal{H}^{\otimes N}_{AB}\right)$. Then the rate of an $\varepsilon_{\text{coh}} := (\varepsilon_{\text{PE}} + \varepsilon_{\text{EC}} + \varepsilon_{\text{PA}} + 2\bar{\varepsilon})$-secure key is given by*

$$\begin{aligned}r_{\text{coh}} &:= \frac{n}{N}\left[\inf_{\rho_{AB} \in \Gamma_{\text{coh}}}\left(S(X|E) - \frac{\text{leak}_{\text{EC}}}{n}\right)\right. \\ &- \left. 5\sqrt{\frac{\log_2(4n^2/\bar{\varepsilon})}{n}}\right] \\ &- \frac{1}{N} + \frac{2}{N}\log_2(2\varepsilon_{\text{PA}}),\end{aligned} \tag{52}$$

where

$$\Gamma_{\text{coh}} = \left\{\sigma_{AB} : \frac{1}{2}\left|\left|Q_m - P_n\right|\right|_1 \leq \xi_{\text{coh}}\left(\bar{\varepsilon}, n, m\right)\right\} \tag{53}$$

with

$$\xi_{\text{coh}}\left(\bar{\varepsilon}, n, m\right) := \frac{\xi_{\text{att}}\left(\bar{\varepsilon}, 2, n\right)}{2} + \xi\left(\frac{\bar{\varepsilon}}{2}, n, m\right) \tag{54}$$

for

$$\xi\left(\frac{\bar{\varepsilon}}{2}, n, m\right) := \sqrt{\frac{(m+n)(m+1)\ln\left(2/\bar{\varepsilon}\right)}{8m^2 n}}, \tag{55}$$

$$\xi_{\text{att}}(\bar{\varepsilon}, 2, n) := \sqrt{\frac{16\ln(2) + 8\ln\left(1/\bar{\varepsilon}\right)}{n}} \tag{56}$$

and

$$S(X|E) = S(\rho_{XE}) - S(\rho_E) \tag{57}$$

with $S(\rho) := -\operatorname{tr}(\rho \log_2 \rho)$.

Proof: The proof follows by inserting the result from Eq. (20) into Eq. (17) and using Eq. (B7) to express the smooth min-entropy of product states by the conditional von Neumann entropy of a single-copy state. □

A careful analysis of the proof of Eq. (20) enables us to obtain the main corrections for the secret key rate for coherent attacks (Eq. (52)) in comparison to collective attacks (Eq. (8)): First, for coherent attacks the probability to measure a single realization $\mathbf{n}$ for a given tensor-product state is rather small, which makes the ε-environment, e.g. in Eq. (51) small. Second, the statistics for the different attacks are not identical in general. Additional fluctuations have to be taken into account as done by considering ξ_{att} (see Eqs. (54) and (56)). These corrections loose their corrupting influence on the secret key rate, when considering the asymptotic limit ($N \to \infty$, $\varepsilon \to 0$). In this case ξ_{att} becomes zero and no additional fluctuations have to be added to the $QBER$, thus the corrections vanish. This confirms the equivalence of collective and coherent attacks for permutation-invariant protocols stated in [17, 18] in the asymptotic limit. But for a finite number of signals these corrections have a dramatic impact on the secret key rate. And, since these additional terms seem unavoidable, this might be a hint, that the equivalence of collective and coherent attacks might not hold for permutation-invariant states in the regime of finite resources.

The following section shortly reviews the known post-selection technique [21], which we then will compare to Eq. (52).

V. POST-SELECTION - A SHORT REVIEW

In order to determine the quality of r_{coh} (Eq. (52)) from the previous section, we have to compare it to key rates obtained by strategies existing in the literature. Up to now, there exist two main techniques to quantify secret key rates for finite resources for coherent attacks for the whole class of permutation-invariant protocols, namely the de Finetti approach [1, 22] and the post-selection technique [21]. Since Sheridan et al showed in [7] that

the latter technique leads to higher secret key rates, we only take the post-selection technique for comparison.

The post-selection technique applied to QKD estimates the deviation of the finite key rate r_{post} obtained from a permutation-invariant protocol against coherent attacks from the corresponding rate r_{coll} against collective attacks. The rate of an $\varepsilon_{\text{post}}$-secure key is given by [21]

$$r_{\text{post}} = r_{\text{coll}} - 30 \log_2 (N+1)/N \tag{58}$$

where r_{coll} is given by Eq. (8) evaluated for the security parameter $\varepsilon_{\text{coll}} = \varepsilon_{\text{post}}(N+1)^{-15}$.

VI. COMPARISON

In this section we compare our newly developed secret key rate r_{coh} (Eq. (52)) and the known rate r_{post} (Eq. (58)) for coherent attacks to the secret key rate evaluated under the assumption of collective attacks r_{coll} (Eq. (8)) for the BB84 protocol and the six-state protocol.

The finite-key rates are calculated for a total security parameter of $\varepsilon := \varepsilon_{\text{coll}} = \varepsilon_{\text{post}} = \varepsilon_{\text{coh}} = 10^{-9}$. In the following let $QBER := Q_m$ denote the tolerated $QBER$ from the POVM used for parameter estimation (see Eq. (6) and Section IV A).

The results are obtained from a numerical optimization procedure, which maximizes the key rate with respect to the parameters $m, \bar{\varepsilon}, \varepsilon_{\text{PE}}, \varepsilon_{\text{EC}}, \varepsilon_{\text{PA}}$.

In FIG. 1 the secret key rates are shown as a function of the initial number of signals N for different $QBER$s for the BB84 protocol. FIG. 2 presents an analogous calculation for the six-state protocol. Note that, as mentioned in Section IV B, in both cases we recover the known result that coherent attacks become collective attacks in the limit of infinitely many signals N. For finite N the figures show that the new rate r_{coh} is always significantly higher in comparison to the rate r_{post} obtained from the post-selection technique. This advantage of r_{coh} can be seen for a rather small $QBER = 0.01$ as well as for a high value $QBER = 0.1$. For example we obtain that the increase of r_{coh} in comparison to r_{post} is around 43% for a $QBER$ of 0.01 ($N = 10^6$) and 33% for a $QBER$ of 0.1 ($N = 10^{10}$) for the BB84 protocol. In case of the six-state protocol r_{coh} exceeds r_{post} by around 51% for a $QBER$ of 0.01 ($N = 10^6$) and 45% for a $QBER$ of 0.1 ($N = 10^8$).

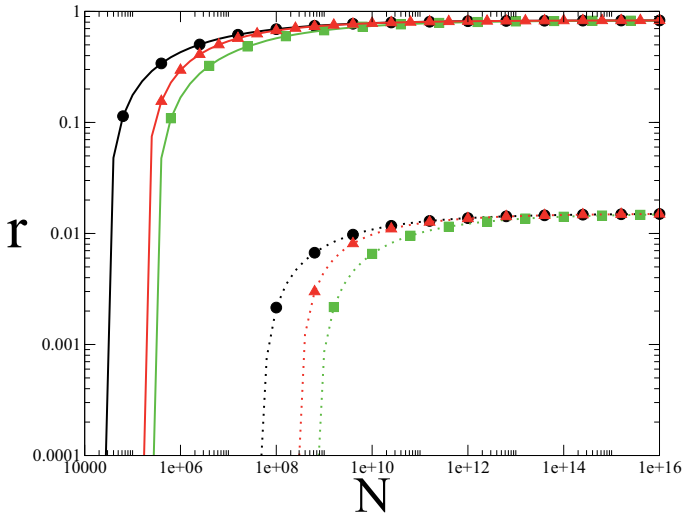

FIG. 1: (Color online) Comparison of the secret key rates r_{coll} (Eq. (8)) (black circles), r_{post} (Eq. (58)) (green squares) and r_{coh} (Eq. (52)) (red triangles) versus the number N of initial signals for different QBERs with security parameter $\varepsilon = 10^{-9}$ for the BB84 protocol in logarithmic scale; $QBER = 0.01$ (straight lines), $QBER = 0.1$ (dotted lines).

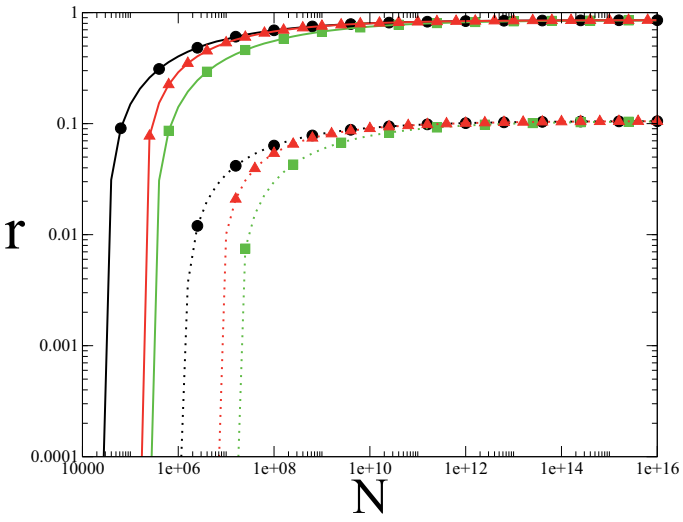

FIG. 2: (Color online) Comparison of the secret key rates r_{coll} (Eq. (8)) (black circles), r_{post} (Eq. (58)) (green squares) and r_{coh} (Eq. (52)) (red triangles) versus the number N of initial signals for different QBERs with security parameter $\varepsilon = 10^{-9}$ for the six-state protocol in logarithmic scale; $QBER = 0.01$ (straight lines), $QBER = 0.1$ (dotted lines).

VII. CONCLUSION

In this paper we presented a new method to quantify the rate of a secret key for general permutation-invariant protocols for coherent attacks. We show a technique to trace the calculation of secret key rates for coherent attacks back to the analysis of collective attacks. The high quality of this method manifests itself by a comparison to the up to now best-known strategy, the post-selection technique. For the treatment of collective attacks we applied the von Neumann entropy bound. We showed that for a finite number of initial signals the secret key rates for the BB84 and the six-state protocol obtained by our method exceed the rates coming from the post-selection technique significantly. In case of the BB84 protocol, higher secret key rates have been obtained in [10] and

[11] by a specialized method, which can, however, not be applied to the six-state protocol. Our method, in contrast, can be applied to all permutation-invariant quantum key distribution protocols for which an analysis of collective attacks is available. Since our results strongly depend on the underlying analysis of collective attacks, a prospective progress in the analysis of collective attacks will automatically cause a progress in our strategy with respect to secret key rates.

Additionally the results of our derivation confirm the known result that, in the limit of infinitely many initial signals, coherent attacks are as powerful as collective attacks. Furthermore, we point out the main impact on the corrections for the key rate against coherent attacks in comparison to collective attacks. Since this extensive impact seems unavoidable, this might give some evidence for the inequivalence of the two types of attacks for finite resources.

Since the assumption of permutation-invariance is fairly weak (most protocols used in the literature are permutation-invariant or can be made to), the results of this paper can be widely applied.

Acknowledgments

We would like to thank Silvestre Abruzzo, Renato Renner and Marco Tomamichel for helpful discussions. This work was financially supported by Deutsche Forschungsgemeinschaft (DFG) and Bundesministerium für Bildung und Forschung (BMBF), project QuOReP.

APPENDIX A

1. Properties of the (smooth) min-entropy

Lemma 1. *Let* $\rho_{ABZ} := \sum_{z\in\mathcal{Z}} P_Z(z)\rho_{AB}^z \otimes |z\rangle\langle z| \in \mathcal{S}(\mathcal{H}_A\otimes\mathcal{H}_B\otimes\mathcal{H}_Z)$ *be a classical-quantum state with* $\rho_{AB} = \mathrm{tr}_Z(\rho_{ABZ})$ *and* $\sigma_B \in \mathcal{S}(\mathcal{H}_B)$*, then*

$$H_{\min}^{\varepsilon}(\rho_{ABZ}|B) \geq H_{\min}^{\varepsilon}(\rho_{AB}|B). \tag{A1}$$

Proof: For any $\nu > 0$ there exists $\bar{\rho}_{AB} \in \mathcal{B}^{\frac{\varepsilon}{2}}(\rho_{AB})$ such that for any σ_B

$$H_{\min}(\bar{\rho}_{AB}|\sigma_B) \geq H_{\min}^{\varepsilon}(\rho_{AB}|\sigma_B) - \nu.$$

Then it follows with Eq. (B4) that

$$H_{\min}(\bar{\rho}_{ABZ}|\sigma_B) \geq H_{\min}(\bar{\rho}_{AB}|\sigma_B).$$

To conclude the proof it suffices to verify that $\bar{\rho}_{ABZ} \in \mathcal{B}^{\frac{\varepsilon}{2}}(\rho_{ABZ})$.

$$\frac{1}{2}||\bar{\rho}_{ABZ} - \rho_{ABZ}||_1 \leq \frac{1}{2}||\bar{\rho}_{AB} - \rho_{AB}||_1 \leq \frac{\varepsilon}{2},$$

where we used the fact that the trace-distance cannot increase when applying a quantum operation (see [1], Lemma $A.2.1$). The assertion then follows by choosing σ_B such that

$$H_{\min}^{\varepsilon}(\rho_{AB}|\sigma_B) = H_{\min}^{\varepsilon}(\rho_{AB}|B)$$

and the fact that

$$H_{\min}(\bar{\rho}_{ABZ}|B) \geq H_{\min}(\bar{\rho}_{ABZ}|\sigma_B).$$

□

Lemma 2. *Let* $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A\otimes\mathcal{H}_B)$*,* $\{|z\rangle\}_z$ *a family of orthogonal vectors in* $\mathcal{H}_Z$ *and* $\varepsilon > 0$*. Then for a state* $\bar{\rho}_{ABZ} := \sum_{z\in\mathcal{Z}} F_z\rho_{AB}F_z^\dagger \otimes |z\rangle\langle z|$ *with* $\sum_{z\in\mathcal{Z}} F_z^\dagger F_z = \mathbb{1}$ *and* $\mathrm{tr}_Z(\bar{\rho}_{ABZ}) = \rho_{AB}$

$$H_{\min}^{\varepsilon}(\rho_{AB}|B) \leq H_{\min}^{\varepsilon}(\bar{\rho}_{ABZ}|B). \tag{A2}$$

Proof: From the definition of $\bar{\rho}_{ABZ}$ it follows immediately that

$$H_{\min}^{\varepsilon}(\mathrm{tr}_Z(\bar{\rho}_{ABZ})|B) = H_{\min}^{\varepsilon}(\rho_{AB}|B).$$

Then the assertion follows with Lemma 1

$$H_{\min}^{\varepsilon}(\mathrm{tr}_Z(\bar{\rho}_{ABZ})|B) \leq H_{\min}^{\varepsilon}(\bar{\rho}_{ABZ}|B). \tag{A3}$$

□

Lemma 3. *Let* $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A\otimes\mathcal{H}_B)$*,* $\{|z\rangle\}_z$ *a family of orthogonal vectors in* $\mathcal{H}_Z$ *and* $\varepsilon > 0$*. Then for a state* $\bar{\rho}_{ABZ} := \sum_{z\in\mathcal{Z}} P_Z(Z=z)F'_z\rho_{AB}F'^\dagger_z \otimes |z\rangle\langle z|$ *with* $\sum_{z\in\mathcal{Z}} F'^\dagger_z F'_z = \mathbb{1}$ *and* $\mathrm{tr}_Z(\bar{\rho}_{ABZ}) = \rho_{AB}$

$$H_{\min}^{\varepsilon}(\rho_{AB}|B) \geq H_{\min}^{\varepsilon}(\bar{\rho}_{ABZ}|BZ). \tag{A4}$$

Proof: From the definition of $\bar{\rho}_{ABZ}$ it follows immediately that

$$H_{\min}^{\varepsilon}(\mathrm{tr}_Z(\bar{\rho}_{ABZ})|B) = H_{\min}^{\varepsilon}(\rho_{AB}|B).$$

Then the assertion follows from the strong subadditivity of the smooth min-entropy (see Eq. (B3)), i.e.

$$H_{\min}^{\varepsilon}(\mathrm{tr}_Z(\bar{\rho}_{ABZ})|B) \geq H_{\min}^{\varepsilon}(\bar{\rho}_{ABZ}|BZ). \tag{A5}$$

□

Lemma 4. *Let* $\rho_{ABZ} = \sum_{z\in\mathcal{Z}} P_Z(z)\rho_{AB}^z \otimes |z\rangle\langle z|$ *be a classical quantum state and* $\varepsilon, \varepsilon' > 0$*, then for any subset* $\mathcal{Z}' \subseteq \mathcal{Z}$ *such that Prob*$[z \in \mathcal{Z}'] > 1 - \varepsilon'$*,*

$$H_{\min}^{\varepsilon+\varepsilon'}(\rho_{ABZ}|BZ) \geq \inf_{z\in\mathcal{Z}'} H_{\min}^{\varepsilon}(\rho_{AB}^z|B). \tag{A6}$$

Proof: For any $\nu > 0$ and $z \in \mathcal{Z}'$ there exists $\bar{\rho}_{AB}^z \in \mathcal{B}^{\frac{\varepsilon}{2}}(\rho_{AB}^z)$ such that for any σ_B^z

$$H_{\min}(\bar{\rho}_{AB}^z|\sigma_B^z) \geq H_{\min}^{\varepsilon}(\rho_{AB}^z|\sigma_B^z) - \nu.$$

Let

$$\bar{\rho}_{ABZ} := \sum_{z\in\mathcal{Z}'} P_{Z'}(z)\bar{\rho}_{AB}^z \otimes |z\rangle\langle z|.$$

Then it follows with Eq. (B2) that

$$\begin{aligned} H_{\min}\left(\bar{\rho}_{ABZ}|\sigma_{BZ}\right) &= \inf_{z\in\mathcal{Z}'} H_{\min}\left(\bar{\rho}^z_{AB}|\sigma^z_B\right) \\ &\geq \inf_{z\in\mathcal{Z}'} H^{\varepsilon}_{\min}\left(\rho^z_{AB}|\sigma^z_B\right) - \nu. \end{aligned}$$

To conclude the proof it suffices to verify that $\bar{\rho}_{ABZ} \in \mathcal{B}^{\frac{\varepsilon+\varepsilon'}{2}}\left(\rho_{ABZ}\right)$.

$$\begin{aligned} & \frac{1}{2}\left|\left|\bar{\rho}_{ABZ} - \rho_{ABZ}\right|\right|_1 \\ \overset{Eq.\ (B6)}{=} & \sum_{z\in\mathcal{Z}'} P_{\mathrm{Z}'}(z)\frac{1}{2}\left|\left|\bar{\rho}^z_{AB} - \rho^z_{AB}\right|\right|_1 \\ & + \sum_{z\in\mathcal{Z}\setminus\mathcal{Z}'} P_{\mathrm{Z}\setminus\mathrm{Z}'}(z)\frac{1}{2}\left|\left|\rho^z_{AB}\right|\right|_1 \\ \leq & \frac{\varepsilon}{2}\sum_{z\in\mathcal{Z}'} P_{\mathrm{Z}'}(z) + \frac{1}{2}\sum_{z\in\mathcal{Z}\setminus\mathcal{Z}'} P_{\mathrm{Z}\setminus\mathrm{Z}'}(z) \\ \leq & \frac{\varepsilon+\varepsilon'}{2}. \end{aligned}$$

The assertion then follows by choosing σ^z_B such that

$$H^{\varepsilon}_{\min}\left(\rho^z_{AB}|\sigma^z_B\right) = H^{\varepsilon}_{\min}\left(\rho^z_{AB}|B\right)$$

and the fact that

$$H_{\min}\left(\bar{\rho}_{ABZ}|BZ\right) \geq H_{\min}\left(\bar{\rho}_{ABZ}|\sigma_{BZ}\right).$$

□

Lemma 5. *Let $\rho_{ABZ} = \sum_{z\in\mathcal{Z}} P_{\mathrm{Z}}(z)\rho^z_{AB}\otimes|z\rangle\langle z|$ be a classical quantum state and $\varepsilon_{\mathrm{z}} := P_{\mathrm{Z}}(z)\varepsilon$, then*

$$H^{\varepsilon_{\mathrm{z}}}_{\min}\left(\rho_{ABZ}|BZ\right) \leq H^{\varepsilon}_{\min}\left(\rho^z_{AB}|B\right). \tag{A7}$$

Proof: For any $\nu > 0$ and $z \in \mathcal{Z}$ there exists $\rho'_{ABZ} \in \mathcal{B}^{\frac{\varepsilon_{\mathrm{z}}}{2}}\left(\rho_{ABZ}\right)$ such that for any σ_{BZ}

$$H_{\min}\left(\rho'_{ABZ}|\sigma_{BZ}\right) \geq H^{\varepsilon_{\mathrm{z}}}_{\min}\left(\rho_{ABZ}|\sigma_{BZ}\right) - \nu.$$

Then it follows with Eq. (B5) that

$$H_{\min}\left(\rho'^z_{AB}|\sigma^z_B\right) \geq H^{\varepsilon_{\mathrm{z}}}_{\min}\left(\rho_{ABZ}|\sigma_{BZ}\right) - \nu.$$

To conclude the proof it suffices to verify that $\rho'^z_{AB} \in \mathcal{B}^{\frac{\varepsilon}{2}}\left(\rho^z_{AB}\right)$.

$$\begin{aligned} \frac{\varepsilon_{\mathrm{z}}}{2} \quad & \geq \quad \frac{1}{2}\left|\left|\rho'_{ABZ} - \rho_{ABZ}\right|\right|_1 \\ & \overset{Eq.\ (B6)}{=} \sum_{z\in\mathcal{Z}} P_{\mathrm{Z}}(z)\frac{1}{2}\left|\left|\rho'^z_{AB} - \rho^z_{AB}\right|\right|_1 \\ & \geq \quad P_{\mathrm{Z}}(z)\frac{1}{2}\left|\left|\rho'^z_{AB} - \rho^z_{AB}\right|\right|_1. \end{aligned}$$

The assertion then follows by choosing σ_{BZ} such that

$$H^{\varepsilon_{\mathrm{z}}}_{\min}\left(\rho_{ABZ}|\sigma_{BZ}\right) = H^{\varepsilon_{\mathrm{z}}}_{\min}\left(\rho_{ABZ}|BZ\right)$$

and the fact that

$$H_{\min}\left(\rho'^z_{AB}|B\right) \geq H_{\min}\left(\rho'^z_{AB}|\sigma^z_B\right).$$

□

2. Estimation of frequency distributions

Lemma 6. *Let $\varepsilon_{\mathrm{PE}} > 0$ and $0 \leq k \leq N$. Let $\rho^N \in \mathcal{S}\left(\mathcal{H}^{\otimes N}\right)$ be a permutation-invariant quantum state, and let $\mathcal{E}$ be a POVM on $\mathcal{H}$ which measures the quantum bit error rate (QBER). Let Q_k and Q_{N-k} be the QBERs when applying the measurement $\mathcal{E}^{\otimes k}$ and $\mathcal{E}^{\otimes N-k}$, respectively, to different subsystems of ρ^N. Then except with probability $\varepsilon_{\mathrm{PE}}$ it holds that*

$$\frac{1}{2}\left|\left|Q_{N-k} - Q_k\right|\right|_1 \leq \xi(\varepsilon_{\mathrm{PE}}, N-k, k) \tag{A8}$$

with $\xi(\varepsilon_{\mathrm{PE}}, N-k, k) := \sqrt{\frac{N(k+1)\ln\left(1/\varepsilon_{\mathrm{PE}}\right)}{8k^2(N-k)}}$.

Proof: It follows from the supplementary information (Note 2) of [10] that with $\varepsilon_{\mathrm{PE}} := e^{-\frac{2k(N-k)}{N}\frac{k}{k+1}(2\xi(\varepsilon_{\mathrm{PE}},N-k,k))^2}$

$$Prob[Q_n \geq Q_k + 2\xi(\varepsilon_{\mathrm{PE}}, N-k, k)] \leq \varepsilon_{\mathrm{PE}}. \tag{A9}$$

The assertion then follows by negation of the statement. □

3. Multinomial distribution

Lemma 7. *Let $n \in \mathbb{N}$ and $\lambda_i = \frac{n_i}{n}$ for $i = 1,..,4$ with $\sum_{i=1}^4 n_i = n$. Then*

$$\frac{n!}{n_1!n_2!n_3!n_4!}\prod_{i=1}^4 \lambda_i^{n_i} > \frac{1}{n^2} \tag{A10}$$

for $n > 500$.

Proof: After applying the logarithm we get

$$\ln\left(\frac{n!}{n_1!n_2!n_3!n_4!}\prod_{i=1}^4\lambda_i^{n_i}\right) = \ln(n!) - \sum_{i=1}^4 \ln(n_i!) + n_i\ln\left(\frac{n_i}{n}\right). \tag{A11}$$

By using the Stirling-formula

$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n < n! < \left(1+\frac{1}{11n}\right)\sqrt{2\pi n}\left(\frac{n}{e}\right)^n \tag{A12}$$

we get for $n > 0$

$$\begin{aligned} & \ln(n!) - \sum_{i=1}^4 \ln(n_i!) + n_i\ln\left(\frac{n_i}{n}\right) \\ > & \frac{1}{2}\ln(2\pi n) - \left(\sum_{i=1}^4 \frac{1}{2}\ln(2\pi n_i) + \ln\left(1+\frac{1}{11n_i}\right)\right) \\ = & -\frac{3}{2}\ln(2\pi n) - \left(\sum_{i=1}^4 \frac{1}{2}\ln\left(\frac{n_i}{n}\right) + \ln\left(1+\frac{1}{11n_i}\right)\right) \\ > & -\frac{3}{2}\ln(2\pi n) - 4\ln\left(\frac{12}{11}\right), \end{aligned} \tag{A13}$$

where we used in the last line that $\frac{1}{2}\ln\left(\frac{n_i}{n}\right) < 0$ and $\ln\left(1+\frac{1}{11n_i}\right) < \ln\left(1+\frac{1}{11}\right)$ for $n_i > 0\ \forall i = 1,..,4$. After exponentiation we end up in

$$\frac{n!}{n_1!n_2!n_3!n_4!}\prod_{i=1}^{4}\lambda_i^{n_i} > \frac{1}{(2\pi n)^{3/2}}\left(\frac{11}{12}\right)^4 > \frac{1}{n^2}, \quad \text{(A14)}$$

which holds for $n > 500$. □

APPENDIX B: KNOWN RESULTS

Here, we review known results, which are crucial for derivations in the paper.

1. Properties of the (smooth) min-entropy

- Chain rule (see [1], Theorem 3.2.12): Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ and $\varepsilon \geq 0$. Then for $\rho_C = \mathrm{tr}_{AB}(\rho_{ABC})$

$$H_{\min}^{\varepsilon}(\rho_{ABC}|B) \leq H_{\min}^{\varepsilon}(\rho_{ABC}|BC) + \log_2(\mathrm{rank}(\rho_C)). \quad \text{(B1)}$$

- Conditioning on classical information (see [1], Theorem 3.2.12): Let $\rho_{ABZ} := \sum_{z\in\mathcal{Z}} P_Z(z)\rho_{AB}^z \otimes |z\rangle\langle z| \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_Z)$ a classical-quantum state, then

$$H_{\min}(\rho_{ABZ}|BZ) = \inf_{z\in\mathcal{Z}} H_{\min}(\rho_{AB}^z|B). \quad \text{(B2)}$$

- Strong subadditivity (see [1]. Theorem 3.2.12): Let $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ and $\varepsilon \geq 0$, then

$$H_{\min}^{\varepsilon}(\rho_{ABC}|BC) \leq H_{\min}^{\varepsilon}(\rho_{AB}|B). \quad \text{(B3)}$$

- Partial-trace operation on classical subsystem can only decrease min-entropy (see [1], Lemma 3.1.9): Let $\rho_{ABZ} := \sum_{z\in\mathcal{Z}} P_Z(z)\rho_{AB}^z \otimes |z\rangle\langle z| \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_Z)$ be a classical-quantum state with $\rho_{AB} = \mathrm{tr}_Z(\rho_{ABZ})$ and $\sigma_B \in \mathcal{S}(\mathcal{H}_B)$, then

$$H_{\min}(\rho_{ABZ}|\sigma_B) \geq H_{\min}(\rho_{AB}|\sigma_B). \quad \text{(B4)}$$

- Quantum operations can only increase min-entropy (see [25], Theorem 18): Let $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and let $\mathcal{E}$ be a quantum operation such that $\bar{\rho}_{AC} = (\mathbb{1}_A \otimes \mathcal{E})\rho_{AB}$, then

$$H_{\min}^{\varepsilon}(\bar{\rho}_{AC}|C) \geq H_{\min}^{\varepsilon}(\rho_{AB}|B). \quad \text{(B5)}$$

- Trace-distance of mixtures (see [1], Lemma A.2.2): Let $\rho_{AZ} := \sum_{z\in\mathcal{Z}} P_Z(z)\rho_A^z \otimes |z\rangle\langle z| \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_Z)$ be a classical-quantum state and an analogous definition for ρ'_{AZ}, then

$$\frac{1}{2}||\rho_{AZ} - \rho'_{AZ}||_1 = \sum_{z\in\mathcal{Z}} P_Z(z)\frac{1}{2}||\rho_A^z - \rho_A'^z||_1. \quad \text{(B6)}$$

- Smooth min-entropy of quantum tensor-product states (see [1], Corollary 3.3.7): Let $\rho_{XE}^{\otimes n} \in \mathcal{S}\left((\mathcal{H}_X \otimes \mathcal{H}_E)^{\otimes n}\right)$ a classical-quantum tensor-product state and $\varepsilon \geq 0$, then

$$H_{\min}^{\varepsilon}\left(\rho_{XE}^{\otimes n}|E\right) \geq n\left(S(X|E) - 5\sqrt{\frac{\log_2(2/\varepsilon)}{n}}\right), \quad \text{(B7)}$$

where $S(X|E) = S(\rho_{XE}) - S(\rho_E)$ with $S(\rho) := -\mathrm{tr}(\rho\log_2\rho)$.

2. Estimation of frequency distributions

Lemma 8. *[18, 26] Let $\varepsilon_{\mathrm{att}} > 0$ and $0 \leq k \leq N$. Let $\rho^N \in \mathcal{S}\left(\mathcal{H}^{\otimes N}\right)$ be a permutation-invariant quantum state, and let $\mathcal{E}$ and $\mathcal{F}$ be POVMs on $\mathcal{H}$ with $|\mathcal{E}|$ and $|\mathcal{F}|$ outcomes, respectively. Let $\mathbf{Q}_k^{\mathcal{E}}$ and $\mathbf{Q}_{N-k}^{\mathcal{F}}$ be the frequency distribution of the outcomes when applying the measurement $\mathcal{E}^{\otimes k}$ and $\mathcal{F}^{\otimes N-k}$, respectively, to different subsystems of ρ^N. Finally, let Ω be any convex set of density operators such that, for any operator A on $n-1$ subsystems, the normalization of $\mathrm{tr}_{n-1}\left(\mathbb{1}\otimes A\rho^n\mathbb{1}\otimes A^\dagger\right)$ is contained in Ω. Then except with probability $\varepsilon_{\mathrm{att}}$, there exists a state $\sigma \in \Omega$ such that*

$$\frac{k}{N}\frac{1}{2}\left|\left|\mathbf{Q}_k^{\mathcal{E}} - \mathbf{P}_k^{\mathcal{E}}\right|\right|_1 + \frac{N-k}{N}\frac{1}{2}\left|\left|\mathbf{Q}_{N-k}^{\mathcal{F}} - \mathbf{P}_{N-k}^{\mathcal{F}}\right|\right|_1 \leq \xi_{\mathrm{att}}(\varepsilon_{\mathrm{att}}, |\mathcal{E}|+|\mathcal{F}|, N) \quad \text{(B8)}$$

where $\mathbf{P}_k^{\mathcal{E}}$, $\mathbf{P}_{N-k}^{\mathcal{F}}$ denote the probability distributions of the outcomes when measuring σ with respect to $\mathcal{E}$ and $\mathcal{F}$, respectively and $\xi_{\mathrm{att}}(\varepsilon_{\mathrm{att}}, |\mathcal{E}|+|\mathcal{F}|, N) := \sqrt{\frac{8\ln(2)(|\mathcal{E}|+|\mathcal{F}|)+8\ln(1/\varepsilon_{\mathrm{att}})}{N}}$.

[1] R. Renner, Int. J. Quant. Inf. **6**, 1 (2008).

[2] T. Meyer, H. Kampermann, M. Kleinmann, and D. Bruß, Phys. Rev. A **74**, 042340 (2006).

[3] V. Scarani and R. Renner, in *Theory of Quantum Computation, Communication, and Cryptography*, edited by Y. Kawano and M. Mosca (Springer Berlin / Heidelberg, 2008), vol. 5106 of *Lecture Notes in Computer Science*, pp. 83–95.

[4] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).

[5] L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301 (2010).

[6] R. Cai and V. Scarani, New Journal of Physics **11**, 045024 (2009).
[7] L. Sheridan, T. P. Le, and V. Scarani, New Journal of Physics **12**, 123019 (2010).
[8] S. Bratzik et al., Phys. Rev. A **83**, 022330 (2011).
[9] S. Abruzzo, M. Mertz, H. Kampermann, and D. Bruß, Phys. Rev. A **84**, 032321 (2011).
[10] M. Tomamichel, C. W. Lim, N. Gisin, and R. Renner, Nature Communications **3**, 634 (2012).
[11] M. Hayashi and T. Tsurumaru, arXiv:1107.0589.
[12] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, Algorithmica **34**, 372 (2002).
[13] E. Biham and T. Mor, Phys. Rev. Lett. **78**, 2256 (1997).
[14] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **55**, 5840 (2009).
[15] J. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).
[16] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[17] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[18] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[19] C. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[20] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
[21] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).
[22] R. Renner, Nature Physics **3**, 645 (2007).
[23] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[24] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[25] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **56**, 4674 (2010).
[26] M. Christandl, R. Renner, and A. Ekert, quant-ph/0402131.

Secret key rates for coherent attacks.
Physical Review A (submitted in June 2012) [11 pages]
M. Mertz, H. Kampermann, S. Bratzik, and D. Bruß

Impact Factor: 2.861
First author
Contribution to work by scientific work and preparation of the manuscript (90%)

Publication C

Min-entropy and quantum key distribution: Nonzero key rates for "small" numbers of signals

Sylvia Bratzik,* Markus Mertz, Hermann Kampermann, and Dagmar Bruß
Institute for Theoretical Physics III, Heinrich-Heine-Universität Düsseldorf, D-40225 Düsseldorf, Germany
(Received 9 November 2010; published 28 February 2011)

We calculate an achievable secret key rate for quantum key distribution with a finite number of signals by evaluating the quantum conditional min-entropy explicitly. The min-entropy for a classical random variable is the negative logarithm of the maximal value in its probability distribution. The quantum conditional min-entropy can be expressed in terms of the guessing probability, which we calculate for d-dimensional systems. We compare these key rates to previous approaches using the von Neumann entropy and find nonzero key rates for a smaller number of signals. Furthermore, we improve the secret key rates by modifying the parameter estimation step. Both improvements taken together lead to nonzero key rates for only 10^4–10^5 signals. An interesting conclusion can also be drawn from the additivity of the min-entropy and its relation to the guessing probability: for a set of symmetric tensor product states, the optimal minimum-error discrimination (MED) measurement is the optimal MED measurement on each subsystem.

DOI: 10.1103/PhysRevA.83.022330 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum key distribution (QKD) is the establishment of a random secure key between two authorized parties, Alice and Bob, which are connected with each other via a quantum and a classical channel [1]. Qubits (e.g., photons) are distributed over this quantum channel, and in practical implementations, the number of these particles is finite. Dealing with these finite resources, a new branch in QKD emerged: the finite-key analysis. It investigates secure key rates, that is, the ratio of a secure key length to the number of signals sent through the channel, in the nonasymptotic situation. The security of a finite key for a composable security definition [2–4] was proven in [5–10]. It is important to notice that composability means that the key established by QKD can be used safely in any application such as one-time-pad encryption. For a review on practical QKD and its security, see, for example, Refs. [11,12]. Calculations of finite-key rates were done in [9,13,14] and in [15] for d dimensions. The relevance of finite QKD was shown in [16]: Practical implementations of QKD lead to a dramatically lower secure key rate in comparison to asymptotic theoretical predictions.

The article is organized as follows: In Sec. II, we describe a general QKD protocol; in Sec. III, we review a bound for the statistical error in parameter estimation and show that former results on the secret key rate [9] can be improved by considering a positive operator valued measure (POVM) with two outcomes. In Sec. IV, we concentrate on quantifying the secret key length after privacy amplification. It was found in [9,10] that the conditional min-entropy [see Eq. (8)] gives an achievable upper bound on the secret key length. The calculation of the conditional min-entropy involves an optimization over a set of quantum states. A lower bound on the min-entropy by using the conditional von Neumann entropy was established in [9,10]. This bound holds under the assumption of collective attacks, that is, the state shared between Alice and Bob after Eve's interaction has tensor product structure. In Sec. V, we calculate the min-entropy explicitly by applying recent results on its operational meaning [17]. For the qubit case, we evaluate the min-entropy for the Bennett-Brassard 1984 (BB84) protocol [1] via minimum-error discrimination (MED). For d-dimensional quantum systems, we calculate it for the generalized six-state protocol [18,19] via the square-root measurement. In Sec. VI, we compare the key rates via calculation of the min-entropy to the bound with the von Neumann entropy. We show that our approach gives positive key rates for a smaller number of signals compared to the von Neumann approach. Furthermore, we compare our results in the d-dimensional case to the recent results in [15] for the mentioned bound. We conclude in Sec. VII.

II. QUANTUM KEY DISTRIBUTION PROTOCOL

We consider an entanglement-based QKD scheme. In the following, a description of the protocol will be provided.

(1) *Distribution.* Alice prepares N maximally entangled states in dimension $d \times d$, where d is the dimension of the Hilbert space of a subsystem,

$$|\Phi_{00}\rangle := \frac{1}{\sqrt{d}} \sum_{x=0}^{d-1} |xx\rangle\,, \tag{1}$$

and sends the second particle to Bob. In the case of qubits, that is, $d = 2$, the state is one of the four Bell states $|\Phi^+\rangle$. After the distribution, they share N entangled pairs, which we will denote by the state $\tilde{\rho}_{A^N B^N}$. Under the assumption of collective attacks, the state $\tilde{\rho}_{A^N B^N}$ is a tensor product state, that is, $\tilde{\rho}_{A^N B^N} = (\rho_{AB})^{\otimes N}$ [9]. Alice and Bob can symmetrize the state ρ_{AB} by applying a depolarizing map, leading to a d^2-dimensional Bell-diagonal state [6,7,15]:

$$\rho_{AB} = \sum_{j,k=0}^{d-1} \lambda_{jk} |\Phi_{jk}\rangle\langle\Phi_{jk}|, \tag{2}$$

where $|\Phi_{jk}\rangle = (1/\sqrt{d}) \sum_{s=0}^{d-1} (e^{\frac{2\pi i}{d}})^{sk} |s\rangle|(s+j) \bmod d\rangle$ are the generalized Bell states [20]. For $d = 2$, the state ρ_{AB} has the following form:

$$\rho_{AB} = \lambda_{00} P_{|\Phi^+\rangle} + \lambda_{01} P_{|\Phi^-\rangle} + \lambda_{10} P_{|\Psi^+\rangle} + \lambda_{11} P_{|\Psi^-\rangle}, \tag{3}$$

where $P_{|\psi\rangle} = |\psi\rangle\langle\psi|$, $\sum_{i,j} \lambda_{ij} = 1$, and $\{|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle\}$ is the Bell basis. For a specific depolarizing map, one can parametrize the state ρ_{AB} by one parameter Q, which,

*bratzik@thphy.uni-duesseldorf.de

in the two-dimensional case, is the quantum bit error rate (QBER). The relation between Q and λ_{jk} will be explained in Sec. V.

(2) *Encoding and measurement.* Both parties agree on an encoding, that is, each quantum state is associated with a symbol from an alphabet. They perform a projection measurement in certain bases. After this step, Alice and Bob will share N correlated pairs of $d$its (d-letter systems).

(3) *Sifting.* In this step, both parties announce for each qudit pair the encoding they have chosen. Depending on the protocol, either they discard the data when they differ, or they use them for parameter estimation. The bit string after this process has length $N - n'$, when n' bits were discarded.

(4) *Parameter estimation*. Parameter estimation serves for estimating the error in the quantum channel by using measurements, in general a POVM. The considered state is parametrized by the QBER Q for $d = 2$. To measure the QBER, a chosen POVM is used. Owing to the finite number of signals (m randomly chosen signals are used), the QBER cannot be detected perfectly. Therefore a quantification of the statistical error is needed. After parameter estimation, the number of signal states is $n = N - n' - m$.

(5) *Error correction.* In this step, Alice and Bob want to eliminate the error in their classical data, which might be there because of eavesdropping. In order to reconcile their data, they have to communicate publicly. In this article, we will use known results [9] to account for the effect of error correction on the key.

(6) *Privacy amplification.* During the key generation, information about the key might have been revealed to the eavesdropper. To reduce this information, Alice and Bob apply a randomly chosen hash function from a family of hash functions to their identical keys.

III. IMPROVED PARAMETER ESTIMATION

Parameter estimation plays an important role in finite QKD protocols. Since one has a finite number of measurement outcomes, one needs an appropriate estimate for each parameter. In this section we first remind the reader of a method for parameter estimation used in [9,14,21]. There the parameters were estimated by different two-dimensional POVMs for different bases. We will then show that we can reach a better approximation if we consider one specific POVM for the estimation of all parameters. The following theorem quantifies the unavoidable statistical errors in the estimated parameters.

Theorem 1 [*9, 14, 21*]. Let $\{B_i\}_{i=1}^{|\chi|}$ be a $|\chi|$-dimensional POVM, $\vec{\lambda}_m = (\lambda_m(1),\lambda_m(2),\ldots,\lambda_m(|\chi|))$ and $\vec{\lambda}_\infty = (\lambda_\infty(1),\lambda_\infty(2),\ldots,\lambda_\infty(|\chi|))$ the probability distributions, with $\lambda(i)$ being the probability of outcome B_i. Here the index m stands for the m-fold independent application of the POVM on identical states ρ. Let now $\lambda_m := \lambda_m(k)$, $\lambda_\infty := \lambda_\infty(k)$ denote any kth parameter. Then, except with probability $\varepsilon_{\mathrm{PE}}$,

$$\frac{1}{2}\,||\lambda_m - \lambda_\infty||_1 \leqslant \xi(\varepsilon_{\mathrm{PE}},|\chi|,m), \tag{4}$$

$$\xi(\varepsilon_{\mathrm{PE}},|\chi|,m) := \sqrt{\frac{\ln\left(\frac{1}{\varepsilon_{\mathrm{PE}}}\right) + |\chi|\ln(m+1)}{8m}}, \tag{5}$$

where $||A||_1 = \mathrm{tr}\sqrt{A^\dagger A}$ and ln denotes the natural logarithm.[1]

Proof. See the appendix.

To clarify the influence of different choices of POVMs on secure key rates, we consider a protocol where Alice and Bob share a state, which can be parametrized by n_{PE} parameters. We choose the variables of the estimation of each parameter in a symmetric way. That means $\varepsilon_{\mathrm{PE}_i} = \varepsilon_{\mathrm{PE}}/n_{\mathrm{PE}}, |\chi|_i = |\chi|$, $m_i = m/n_{\mathrm{PE}}$ for all $i \in \{1,\ldots,n_{\mathrm{PE}}\}$ such that the constraints $\sum_{i=1}^{n_{\mathrm{PE}}} \varepsilon_{\mathrm{PE}_i} = \varepsilon_{\mathrm{PE}}$ and $\sum_{i=1}^{n_{\mathrm{PE}}} m_i = m$ are fulfilled.

In previous works [9,14], each parameter is estimated by an individual two-dimensional POVM (in the following, we will use IPOVM as an abbreviation for this approach), for example, for the BB84 protocol, we have two parameters (error rates in two bases) to estimate. Then we need two POVMs, where each of them has two outcomes which correspond to "Alice and Bob *do have* the same measurement outcome" and "Alice and Bob *do not have* the same measurement outcome" in their respective measurement basis. This leads to $\xi(\varepsilon_{\mathrm{PE}}/2,2,m/2)$. Generally for states determined by n_{PE}, we get $\xi(\varepsilon_{\mathrm{PE}}/n_{\mathrm{PE}},2,m/n_{\mathrm{PE}})$ for each parameter.

Concerning secure key rates, we can improve this method by considering a common POVM with $n_{\mathrm{PE}} + 1$ measurement outcomes (CPOVM approach). This means, for example, for the BB84 protocol that we use a POVM with three outcomes, where two of them correspond to "Alice and Bob *do not have* the same measurement outcome" in each of the two bases and one corresponds to the completeness of the POVM. Then, the estimation of each parameter will be represented by $\xi(\varepsilon_{\mathrm{PE}},3,m)$. In general, for $(n_{\mathrm{PE}} + 1)$-dimensional systems, the deviation from the perfect parameter [see Eq. (4)] is given by $\xi(\varepsilon_{\mathrm{PE}},n_{\mathrm{PE}} + 1,m)$. The improvement is because of the fact that in Eq. (4), the trace distance is only bounded by $\xi(\varepsilon_{\mathrm{PE}},|\chi|,m)$ and the parameters according to the CPOVM approach lead to a smaller bound than the IPOVM approach. The results of an explicit calculation of the key rates will be provided in the last section.

IV. PRIVACY AMPLIFICATION AND THE $\bar{\varepsilon}$-SMOOTH MIN-ENTROPY

In this section, we will present some results about the min-entropy. Starting from the connection of the min-entropy to the secure key length after the privacy amplification step, we review the relation of the min-entropy to the guessing probability given in [17].

A. The $\bar{\varepsilon}$-smooth min-entropy and the secure key length ℓ

The $\bar{\varepsilon}$-smooth conditional min-entropy provides an upper bound for the secure key length ℓ after the privacy amplification step [10]:

$$\ell \lesssim H_{\min}^{\bar{\varepsilon}}\left(\rho_{XE}^{\otimes n}|E^n\right), \tag{6}$$

[1]The formula in [9,14,21] was corrected in an erratum [22]. The formula in Eq. (5) can be obtained by multiplying the corresponding formula in [22] by 1/2.

where $\rho_{XE} = \sum_{x=0}^{d-1} p_x |x\rangle\langle x| \otimes \rho_E^x$ is a classical-quantum state, which Alice and the eavesdropper Eve share after error correction. Here X is Alice's random variable with values $x \in \{0, \ldots, d-1\}$, where d is the dimension of the quantum system. The eavesdropper holds a quantum state ρ_E^x, which is correlated with the random variable X. The symbol E^n denotes the eavesdropper's system. The parameter n is the number of signals after sifting and parameter estimation, that is, $n = N - n' - m$.

In the following, we will denote the state ρ_{XE} as a single-signal state; that is, following the preceding description, both parties share one single state ($n = 1$). Otherwise, the state will be denoted by $\rho_{XE}^{\otimes n}$ if it has tensor product structure. We consider collective attacks, as the state shared between Alice and Eve has in this case tensor product structure. Collective attacks [23] are those attacks where the eavesdropper is restricted to interact with each of the signals separately, that is, by attaching an auxiliary system and performing unitary transformations. In [6,7], it was shown that it suffices to consider a convex combination of product states when analyzing the full security of QKD protocols. However, it does not follow that we can consider w.l.o.g. a product state.

We recall the definition of the $\bar{\varepsilon}$-smooth min-entropy.

Definition 1 ($\bar{\varepsilon}$-*smooth min-entropy* [10]). Let $\bar{\rho}_{XE} \in \mathcal{B}^{\bar{\varepsilon}/2}(\rho_{XE}) := \{\bar{\rho}_{XE} \geqslant 0 : \|\bar{\rho}_{XE} - \rho_{XE}\|_1 \leqslant \bar{\varepsilon}\}$. The $\bar{\varepsilon}$-smooth min-entropy is defined as

$$H_{\min}^{\bar{\varepsilon}}(\rho_{XE}|E) := \sup_{\bar{\rho}_{XE}} H_{\min}(\bar{\rho}_{XE}|E), \tag{7}$$

with

$$H_{\min}(\bar{\rho}_{XE}|E) := \sup_{\sigma_E}[-\log_2(\min\lambda : \lambda \cdot \mathbb{1}_X \otimes \sigma_E \geqslant \bar{\rho}_{XE})]. \tag{8}$$

The optimization in Eq. (7) is done over the states $\bar{\rho}_{XE}$ in the $\bar{\varepsilon}$-environment of ρ_{XE}, whereas the optimization in Eq. (8) is over all states σ_E.

B. The min-entropy and the guessing probability

The evaluation in Eq. (7) is a convex optimization problem. It was shown in [17] that the min-entropy can be rewritten as the negative logarithm of the optimal guessing probability p_{guess}:

$$H_{\min}(\rho_{XE}|E) = -\log_2 p_{\text{guess}}, \tag{9}$$

where

$$p_{\text{guess}} \equiv p_{\text{guess}}(X|E) := \max_{\{E_E^x\}} \sum_{x=0}^{d-1} p_x \operatorname{tr}\left(E_E^x \rho_E^x\right). \tag{10}$$

Here it was used that the initial state ρ_{XE} is a classical-quantum state (see earlier) which is shared between Alice and Eve, the eavesdropper. The set $\{E_E^x\}$ denotes the POVM elements of Eve, which she uses in order to distinguish her nonorthogonal ancilla states ρ_E^x. If she could perfectly discriminate them, she would know the value of Alice's random variable X and therefore the content of the secret key.

V. EVALUATION OF THE GUESSING PROBABILITY

In this section, we will present an explicit calculation of the guessing probability in Eq. (10) for d-dimensional quantum systems for the generalized six-state protocol via square-root measurement (see, e.g., [24–29]) and for qubit systems ($d = 2$) for the BB84 protocol via MED [26,30–33]. The problem of distinguishing two mixed quantum states with minimum error was solved by Helstrøm [32], but for more states, it becomes more involved. For quantum states with a certain symmetry, optimal measurements were found (see, e.g., [29]), whereas for arbitrary states, only bounds exist [34]. Finally, we draw a conclusion from the additivity of the min-entropy for tensor product states: For a set of symmetric tensor product states, the optimal MED measurement is the optimal MED measurement on the subsystems.

A. Generalized six-state protocol for d-dimensional quantum systems

In this part, we consider a $(d+1)$-basis protocol, which was introduced in [35–37]. It is a generalization of the six-state protocol [18,19]. We further assume a collective eavesdropping attack. Owing to symmetrizations [6], the eavesdropper is forced to introduce the same error in each measurement basis. This symmetrization leads to the following Bell-diagonal state shared between Alice and Bob (see Sec. II):

$$\rho_{AB} = (\beta_0 - \beta_1)|\Phi_{00}\rangle\langle\Phi_{00}| + \frac{\beta_1}{d} 1_{d^2}, \tag{11}$$

with $\beta_0 + (d-1)\beta_1 = 1$, $0 \leqslant \beta_1 < \frac{1}{d} < \beta_0 \leqslant 1$, and 1_{d^2} being the identity matrix of size d^2. Note that this form is equal to the one considered in [38,39]. The parameter β_0 can be seen as the probability that both get the same output, whereas β_1 denotes the probability that they get a particular other one. The error rate Q is given by $Q := 1 - \beta_0 = (d-1)\beta_1$; for $d = 2$, Q is the quantum bit error rate β_1. The state in Eq. (11) can be recovered from Eq. (2) by setting $\lambda_{00} = 1 - (d+1)/d(1 - \beta_0)$ and all other $\lambda_{jk} = (1-\beta_0)/[d(d-1)] = \beta_1/d$.

We assume that Eve holds a purification $|\psi_{ABE}\rangle$. Eve's reduced state is [38]

$$\rho_E = \frac{1}{d}\left(\beta_0 \sum_{x=0}^{d-1} |E_{xx}\rangle\langle E_{xx}| + \beta_1 \sum_{\substack{x,y \\ y\neq x}} |E_{xy}\rangle\langle E_{xy}|\right), \tag{12}$$

and we define the normalized states ρ_E^x as

$$\rho_E^x := \beta_0 |E_{xx}\rangle\langle E_{xx}| + \beta_1 \sum_{y\neq x} |E_{xy}\rangle\langle E_{xy}| \tag{13}$$

such that Eve's state is given by $\rho_E = (1/d)\sum_x \rho_E^x$. Eve's ancilla states $|E_{xy}\rangle$ have a specific form in order to fulfill the requirement in Eq. (11). They can be written in terms of an orthonormal basis of Eve $|f_{i,j}\rangle_E$}:

$$|E_{xy}\rangle = \begin{cases} \frac{1}{\sqrt{\beta_0}} \sum_{k=0}^{d-1} \sqrt{\lambda_{0,k}}\,\omega^{xk} |f_{0,k}\rangle_E & \text{for } x = y, \\ \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{xk} |f_{y-x,k}\rangle_E & \text{for } x \neq y, \end{cases} \tag{14}$$

with $\omega := e^{2\pi i/d}$ and $\lambda_{j,k}$ given earlier. The ancilla states with $x = y$ have a fixed angle between each other; they are called pyramid states [39]. They fulfill

$$\langle E_{xy}|E_{x'y'}\rangle = \begin{cases} 1 & \text{if } x = x' \text{ and } y = y', \\ 1 - \frac{\beta_1}{\beta_0} & \text{if } x = y \neq x' = y', \\ 0 & \text{otherwise.} \end{cases}$$

The eavesdropper would like to know Alice's and Bob's classical value x and y, respectively. For the case $x \neq y$, she knows both values with certainty, as those ancilla states are orthogonal and she can perfectly discriminate them. For the case $x = y$, Eve has to discriminate d pyramid states. Measurements for such symmetrical states exist, and it is known that the error-minimizing measurement for such states is the square-root measurement [24–29]. The following results for the tomographic protocol were derived in [39,40].

The state in Eq. (12) can be rewritten as

$$\rho_E = \beta_0 \rho^{(=)} + (1 - \beta_0)\rho^{(\neq)}, \tag{15}$$

where the density operator $\rho^{(=)} = (1/d)\sum_{x=0}^{d-1} |E_{xx}\rangle\langle E_{xx}|$ denotes the cases when Alice and Bob have the same values, whereas in the case of $\rho^{(\neq)} = 1/[d(d-1)]\sum_{y\neq x} |E_{xy}\rangle\langle E_{xy}|$, their values are different. The eavesdropper wants to find their common values, so she wants to discriminate those ancilla states for $x = y$. The POVM elements $|e_{xx}\rangle\langle e_{xx}|$ that discriminate the pyramid states with minimum error are given via

$$|e_{xx}\rangle = \frac{1}{\sqrt{d\rho^{(=)}}}\,|E_{xx}\rangle\,;$$

that is, the name square-root measurement is related to the construction of the elements. An explicit calculation for the operator $1/\sqrt{d\rho^{(=)}}$ results in [39]

$$\frac{1}{\sqrt{d\rho^{(=)}}} = \frac{(r_0 + \sqrt{r_0 r_1} + r_1)\mathbb{1} - \rho^{(=)}}{\sqrt{r_0 r_1}(\sqrt{r_0} + \sqrt{r_1})},$$

where $r_0 = 1 - (d-1)/d(\beta_1/\beta_0)$ is the eigenvalue corresponding to the eigenvector $\sum_x |E_{xx}\rangle$ and $r_1 = \beta_1/(d\beta_0)$ is the $(d-1)$-fold eigenvalue for the eigenvector $(|E_{xx}\rangle - (1/d)\sum_y |E_{yy}\rangle)$. From this, the overlap $\langle e_{xx}|E_{yy}\rangle$ can be calculated as

$$\langle e_{xx}|E_{yy}\rangle = \sqrt{\eta_0}\delta_{xy} + \sqrt{\eta_1}(1 - \delta_{xy}),$$

with $\sqrt{\eta_0} = [\sqrt{r_0} + (d-1)\sqrt{r_1}]/\sqrt{d}$, $\sqrt{\eta_1} = [\sqrt{r_0} + \sqrt{r_1}]/\sqrt{d}$, and δ_{xy} the Kronecker delta. The probability η_0 denotes the probability that Eve, when finding $|e_{xx}\rangle$, knows that Alice and Bob share the value x, and η_1 denotes the probability that they hold one of the other $d-1$ values.

The eavesdropper's probability to guess the right value of Alice consists of the following parts: the probability $(1 - \beta_0)$ that the density operator $\rho^{(\neq)}$ appears [see Eq. (15)] and the probability β_0 that $\rho^{(=)}$ appears multiplied with the probability that she guesses the right value in this case, which was η_0 (see earlier). Inserting r_0 and r_1 into η_0, we get an expression for the guessing probability depending on d and the error rate $Q = 1 - \beta_0$:

$$p_{\text{guess}}^{\text{six state}}(d, Q) = 1 - \beta_0 + \beta_0\eta_0 = Q + \frac{(1-Q)}{d}\left[1 - \frac{(d-2)Q}{d(Q-1)} + 2(d-1)\sqrt{\frac{dQ - (d+1)Q^2}{(d-1)d^2(1-Q)^2}}\right]. \tag{16}$$

B. BB84 protocol for qubit systems

A strategy to distinguish two nonorthogonal quantum states is called MED (see [26,30–33]). In MED, for each measurement, one has a conclusive result, but with probability p_{err}, the result is erroneous. It was shown by Helstrøm [32] that the maximal probability to make a correct guess when distinguishing two quantum states ρ_E^0 and ρ_E^1 that appear with the same probability $p_0 = p_1 = 1/2$ is given by

$$p_{\text{guess}}(2, Q) = 1 - p_{\text{err}}^{\min} = \tfrac{1}{2}\left(1 + \tfrac{1}{2}\left\|\rho_E^0 - \rho_E^1\right\|_1\right). \tag{17}$$

In order to calculate $\|\rho_E^0 - \rho_E^1\|_1$, we express the states ρ_E^0 and ρ_E^1 [see Eq. (13)] in terms of the computational basis of Eve.

Assuming that Eve has a purifying system of the state in Eq. (3), and that Alice and Bob perform a von Neumann measurement, one can derive an expression for $\|\rho_E^0 - \rho_E^1\|_1$ for the BB84 protocol. The operator $\rho_E^0 - \rho_E^1$ can be written as

$$\rho_E^0 - \rho_E^1 = 2\sqrt{\lambda_{00}\lambda_{01}}\,(|00\rangle\langle 01| + |01\rangle\langle 00|) + 2\sqrt{\lambda_{10}\lambda_{11}}\,(|10\rangle\langle 11| + |11\rangle\langle 01|)\,, \tag{18}$$

so

$$\left|\rho_E^0 - \rho_E^1\right| = 2\sqrt{\lambda_{00}\lambda_{01}}(P_{|00\rangle} + P_{|01\rangle}) + 2\sqrt{\lambda_{10}\lambda_{11}}(P_{|10\rangle} + P_{|11\rangle}), \tag{19}$$

with $|A| = \sqrt{A^\dagger A}$. The eigenvalues $2\sqrt{\lambda_{00}\lambda_{01}}$ and $2\sqrt{\lambda_{10}\lambda_{11}}$ occur with multiplicity 2. Thus the 1-norm is

$$\tfrac{1}{2}\left\|\rho_E^0 - \rho_E^1\right\|_1 = 2\sqrt{\lambda_{00}\lambda_{01}} + 2\sqrt{\lambda_{10}\lambda_{11}}. \tag{20}$$

The error rates in the z and x directions are $e_z = \lambda_{10} + \lambda_{11}$ and $e_x = \lambda_{01} + \lambda_{11}$ (see [10,12]). There remains one free parameter that we have to optimize to obtain the best case for Eve. We adopt the method in Appendix A of [12] to maximize the probability of correct guess in Eq. (17): According to [12], we choose $\lambda_{00} = (1-Q)(1-u)$, $\lambda_{01} = (1-Q)u$, $\lambda_{10} = Q(1-v)$, and $\lambda_{11} = Qv$, with $u, v \in [0,1]$, and the additional constraint (from $\lambda_{01} + \lambda_{11} = Q$)

$$(1-Q)u + Qv = Q. \tag{21}$$

Defining $|\Phi_{ij}\rangle$ as the corresponding Bell states to the value λ_{ij}, the purification of the state ρ_{AB} can be written as $|\psi_{ABE}\rangle = \sum_{ij}\sqrt{\lambda_{ij}}|\Phi_{ij}\rangle_{AB} \otimes |e_{ij}\rangle_E$, where $\{|e_{ij}\rangle\}$ is a four-dimensional orthonormal basis. Using Eq. (20) and the constraint given in Eq. (21), we find a function that depends on the parameter v:

$$\tfrac{1}{2}\left\|\rho_E^0 - \rho_E^1\right\|_1 = f(v) := 2\sqrt{(1-v)\;Q\;[1 + (v-2)\,Q]} + 2\sqrt{(1-v)\;v\;Q^2}. \tag{22}$$

Finding the maximum of the expression leads to the result $u = v = Q$ and finally to the expressions of λ_{ij}: $\lambda_{00} = (1 - Q)^2$, $\lambda_{01} = \lambda_{10} = (1 - Q)Q$, and $\lambda_{11} = Q^2$. This gives the guessing probability

$$p_{\text{guess}}^{\text{BB84}}(2, Q) = \tfrac{1}{2}[1 + 2\sqrt{(1 - Q)Q}]. \tag{23}$$

By using the same methods, we can derive the guessing probability for the six-state protocol, which leads to the same result as derived in Eq. (16):

$$p_{\text{guess}}^{\text{six state}}(2, Q) = \tfrac{1}{2}[1 + \sqrt{Q(2 - 3Q)} + Q]. \tag{24}$$

C. Optimal multistate MED measurement from additivity of min-entropy

We know from [10] that the min-entropy is additive; that is, for tensor product states $\rho_{XE}^{\otimes n}$, it holds that $H_{\min}(\rho_{XE}^{\otimes n}|E^n) = nH_{\min}(\rho_{XE}|E)$. The min-entropy is a function of the probability of a correct guess of Eve's states. The state $\rho_{XE}^{\otimes n}$ is of the form

$$\rho_{XE}^{\otimes n} = \left(\frac{1}{d}\sum_{x=0}^{d-1}|x\rangle\langle x| \otimes \rho_E^x\right)^{\otimes n} \tag{25}$$

$$= \frac{1}{d^n}\sum_{\mathbf{x}\in\{0,\ldots,d-1\}^n}|\mathbf{x}\rangle\langle\mathbf{x}| \otimes \rho_{E^n}^{\mathbf{x}}, \tag{26}$$

where

$$\rho_{E^n}^{\mathbf{x}} = \bigotimes_{i=0}^{n-1}\rho_E^{x_i} \tag{27}$$

and $\mathbf{x} = (x_0, \ldots, x_{n-1})$ is a vector of length n with $x_i \in \{0, \ldots, d-1\}$. Thus Eve's state is given by

$$\rho_E^{\otimes n} = \frac{1}{d^n}\sum_{\mathbf{x}}\rho_{E^n}^{\mathbf{x}} \tag{28}$$

and is a sum of tensor product states [see Eq. (27)]. The explicit MED problem is to distinguish the set of states $\{\rho_{E^n}^{\mathbf{x}}\}$ for different $\mathbf{x}$s. We can conclude from the additivity of the min-entropy that for the set of states given in Eq. (27), the optimal MED measurement consists of optimal MED measurements on the single-signal states $\rho_E^{x_i}$. This result is interesting as, in general, measurements in the total Hilbert space may lead to higher guessing probabilities than measurements in individual subspaces. To the best of our knowledge, this result is not known in the context of state discrimination.

VI. COMPARISON OF KEY RATES

In this section, we provide the results of parameter estimation with CPOVM (see Sec. III) and those of the calculation of the min-entropy (see Sec. V). We first review some results about finite-key distribution.

For a finite number of signals, the achievable secure key rate is found to be [9,14]

$$\ell_1/N = \frac{n}{N}[S_\xi(\rho_{XE}|E) + \Delta - \text{leak}_{\text{EC}}] + \frac{2}{N}\log_2(2\varepsilon_{\text{PA}}), \tag{29}$$

with $\Delta := -7\sqrt{[\log_2(2/\bar{\varepsilon})]/n}$; the total security parameter ε (see, e.g., [14,21]),

$$\varepsilon = \varepsilon_{\text{PA}} + \varepsilon_{\text{EC}} + \varepsilon_{\text{PE}} + \bar{\varepsilon}; \tag{30}$$

and $S_\xi(\rho_{XE}|E) := \min_{\bar{\rho}_{XE}\in\Gamma_\xi} S(\rho_{XE}|E)$. The set $\Gamma_\xi = \{\sigma : \frac{1}{2}|\lambda_m - \lambda_\infty(\sigma)| \leqslant \xi\}$ contains all states compatible with the statistics in parameter estimation. The conditional von Neumann entropy with the correction term Δ is a lower bound on the $\bar{\varepsilon}$-smooth min-entropy. The leakage term leak_{EC} is taken from [12] to be $\text{leak}_{\text{EC}} = 1.2h(Q)$ for $\varepsilon_{\text{EC}} = 10^{-10}$, where $h(x)$ is the binary entropy. Throughout all calculations, we assume asymmetric protocols with a symmetric attack. An asymmetric protocol means that one only keeps the measurement results of one particular basis for the key; the other results are used for parameter estimation. In the case of protocols with $(d + 1)$ bases (e.g., the six-state protocol with $d = 2$), this basis is chosen with probability $q = (1 - dp)$ and the other d bases with probability p. For protocols with two bases (e.g., the BB84 protocol with $d = 2$), $q = 1 - p$. Taking the largest deviation ξ_i from the perfect parameter in one measurement basis and equating it with the other deviations leads to a symmetric choice of parameters m_i and $\varepsilon_{\text{PE}_i}$, that is, $m_i = m/(d + 1)$ ($m_i = m/2$ for two-basis protocols) and $\varepsilon_{\text{PE}_i} = \varepsilon_{\text{PE}}/(d + 1)$ ($\varepsilon_{\text{PE}_i} = \varepsilon_{\text{PE}}/2$) (see Sec. III). This assumption gives a lower bound on the secret key rate. The number of signals used for parameter estimation is given by $m = Np^2$.

In order to calculate the key rate, we fix ε and ε_{EC} and maximize ℓ_1/N in Eq. (29) for the parameters $\varepsilon_{\text{PE}}, \varepsilon_{\text{PA}}, \bar{\varepsilon}$, and q with a computational software program (MATHEMATICA) under the constraint given in Eq. (30).

A. Key rates via von Neumann entropy for different approaches of parameter estimation

For a comparison of the approaches (IPOVM, CPOVM) explained in Sec. III, we consider the asymmetric BB84 and six-state protocols for a symmetric attack for dimension $d = 2$, as discussed in [9]. In the calculation of the key rates via the von Neumann entropy [see Eq. (29)], we use a QBER of $Q = 0.05$ and a total security parameter of $\varepsilon = 10^{-9}$ [see Eq. (30)]. The conditional von Neumann entropy for the six-state protocol is given by [9,12]

$$S^{\text{six state}}(\rho_{XE}|E) = (1 - Q)\left[1 - h\left(\frac{1 - \frac{3}{2}Q}{1 - Q}\right)\right] \tag{31}$$

and for the BB84 protocol by

$$S^{\text{BB84}}(\rho_{XE}|E) = 1 - h(Q). \tag{32}$$

The variables ξ for parameter estimation used in this comparison are summarized in Table I. Note that the symmetrized state is parametrized by only one parameter. This has no influence on the IPOVM approach, in contrast to CPOVM, where the number of POVM outcomes can be reduced from three for the BB84 protocol (four for the six-state protocol) to 2 (2).

The results are shown in Figs. 1 and 2. We point out that our CPOVM approach leads to higher key rates for the BB84 and six-state protocols. In particular, for signals $N \lesssim 10^{11}$,

TABLE I. Deviations ξ from perfect parameter [see Eq. (4) in Sec. III] for different parameter estimation approaches (IPOVM and CPOVM): BB84 and six-state protocols.

	BB84 protocol	Six-state protocol
IPOVM	$\xi(\frac{\varepsilon_{\mathrm{PE}}}{2},2,\frac{m}{2})$	$\xi(\frac{\varepsilon_{\mathrm{PE}}}{3},2,\frac{m}{3})$
CPOVM	$\xi(\varepsilon_{\mathrm{PE}},2,m)$	$\xi(\varepsilon_{\mathrm{PE}},2,m)$

the numerical analysis reveals the importance of parameter estimation. While the CPOVM approach leads for $N = 10^6$ signals to a 80% (37%) higher key rate than the IPOVM approach for the six-state (BB84) protocol, the improvement for $N = 10^{10}$ is still 4% (2%).

B. Key rates via the min-entropy for two-dimensional quantum systems

In this section, we exploit the preceding results from Sec. V regarding the min-entropy in order to compute the secret key rate and compare it to the key rate calculated with Eq. (29). We explained in Sec. IV that the achievable upper bound on the secure key length ℓ after the privacy amplification step is given by Eq. (6). We can derive a key rate by using the following bounds [10], Lemma 3.2.6]:

$$H_{\min}^{\bar{\varepsilon}}\left(\rho_{XE}^{\otimes n}|E^n\right) \geqslant nH_{\min}^{\bar{\varepsilon}/n}(\rho_{XE}|E) \geqslant nH_{\min}(\rho_{XE}|E); \quad (33)$$

the last inequality is a very good approximation as $\bar{\varepsilon}$ is in the order of 10^{-10}. Thus we arrive at the following key rate:

$$\ell_2/N = \frac{n}{N}[H_{\min,\xi}(\rho_{XE}|E) - \mathrm{leak}_{\mathrm{EC}}] + \frac{2}{N}\log_2(2\varepsilon_{\mathrm{PA}}), \quad (34)$$

where the leakage term $\mathrm{leak}_{\mathrm{EC}}$ and $\varepsilon_{\mathrm{PA}}$ are the same as in Eq. (29), and $H_{\min,\xi}(\rho_{XE}|E) := \min_{\bar{\rho}_{XE}\in\Gamma_\xi} H_{\min}(\rho_{XE}|E)$ [see Eq. (29)]. We calculate this key rate using the connection to the guessing probability, that is, $H_{\min}^{\mathrm{protocol}}(\rho_{XE}|E) = -\log_2 p_{\mathrm{guess}}^{\mathrm{protocol}}$ [see Eq. (9)], and compare it to the key rate given in Eq. (29). The guessing probability for the specific protocol is given by Eqs. (23) and (24).

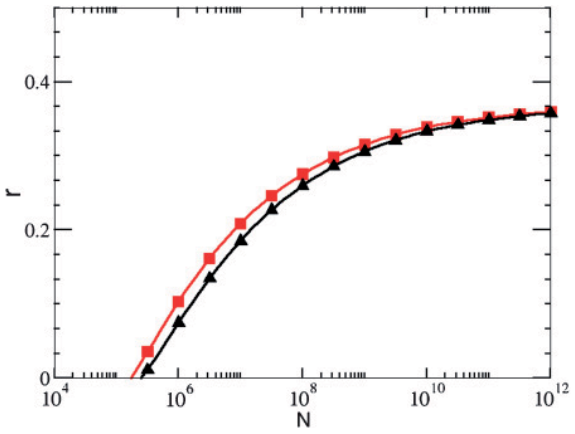

FIG. 1. (Color online) Comparison of the key rates [calculated via the von Neumann entropy; see Eqs. (29) and (32)] using different parameter estimations for asymmetric BB84 protocol; $\varepsilon = 10^{-9}$, $Q = 5\%$; squares (red), CPOVM; triangles (black), IPOVM (see Sec. III for explanations).

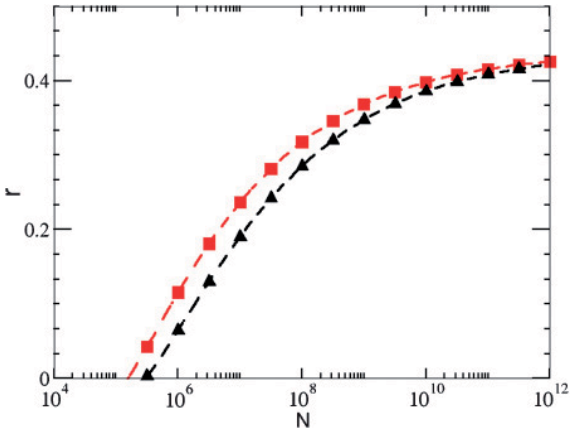

FIG. 2. (Color online) Comparison of the key rates [calculated via the von Neumann entropy; see Eqs. (29) and (31)] using different parameter estimations for asymmetric six-state protocol; $\varepsilon = 10^{-9}, Q = 5\%$; squares (red), CPOVM; triangles (black), IPOVM (see Sec. III for explanations).

In Fig. 3, the threshold number of signals N_0, where the key rate becomes nonzero is plotted as a function of the QBER Q. For parameter estimation, we have considered the CPOVM approach (see Sec. III) with the variables given in Table I. Additionally, we have plotted the key rate via the von Neumann entropy [Eq. (29)] for the IPOVM approach. In comparison to the von Neumann approximation [Eq. (29)], only 1/3 (1/2) of the number of signals is needed for nonzero key rates in the six-state protocol for $Q = 0.2\%$ ($Q = 4\%$), when using the min-entropy. For the BB84 protocol, only 1/3 (2/3) of the number of signals is needed for $Q = 0.2\%$ ($Q = 4\%$).

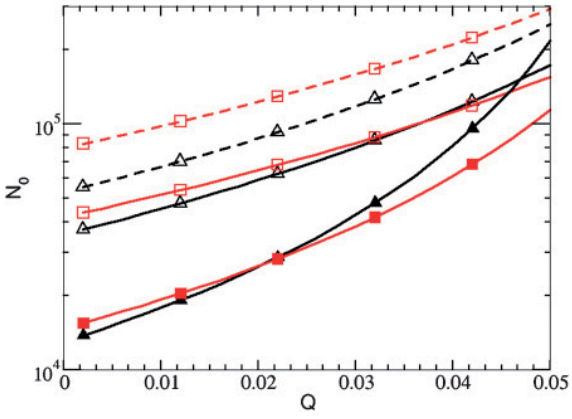

FIG. 3. (Color online) Threshold value N_0 (number of signals, where the key rate becomes nonzero) vs QBER Q with $\varepsilon = 10^{-9}$ and $\varepsilon_{\mathrm{EC}} = 10^{-10}$; triangles (red), BB84 protocol; squares (black), six-state protocol; filled, min-entropy [Eq. (34)]; open, von Neumann entropy with CPOVM approach [Eq. (29)]; dashed line, von Neumann entropy [Eq. (29)] with IPOVM approach (see Sec. III for explanations).

Thus, by calculating a key rate explicitly with the min-entropy, we get positive key rates for a smaller number of signals than via the von Neumann entropy approach. This behavior can be explained by the correction term Δ in the key rate in Eq. (29). For a small number of total signals N, this correction term is not a good approximation and has a big impact on the key rate.

We point out that for low Q, we can achieve nonzero key rates with only $O(10^4)$–$O(10^5)$ signals. Note that in [41], it was considered a "milestone" to reach nonzero key rates for significantly less than 10^5–10^6 signals.

C. Key rates via the min-entropy for d-dimensional quantum systems

In [15], the influence of the dimension on the key rate was discussed. Exploiting the results from this article, we discuss the improvement for higher dimensional quantum systems. Throughout this section, we only consider the $(d+1)$-basis protocols such as the six-state protocol for $d=2$. Furthermore, we adapt our CPOVM approach, and by using Eq. (4) from Sec. III, we get $\xi(\varepsilon_{\mathrm{PE}},2,m)$. The correction term to the d-dimensional von Neumann entropy is given in [15] as $\Delta = -(2d+3)\sqrt{[\log_2(2/\bar{\varepsilon})]/n}$, and the leakage term is characterized by $\mathrm{leak}_{\mathrm{EC}} = 1.2 h_d(Q)$ with $h_d(p) := -p\log_2[p/(d-1)] - (1-p)\log_2(1-p)$. The conditional von Neumann entropy was calculated in [15] as

$$S^d(\rho_{XE}|E) = (1-Q)\left[\log_2 d - h_d\left(\frac{1-\frac{d+1}{d}Q}{1-Q}\right)\right], \quad (35)$$

where $Q = 1-\beta_0$ denotes the error rate in the sifted key. We will compare the key rate calculated via the d-dimensional conditional von Neumann entropy with the one calculated via the d-dimensional min-entropy. The latter can be obtained by using

$$H^d_{\min}(\rho_{XE}|E) = -\log_2 p_{\mathrm{guess}}(d,Q), \quad (36)$$

where $p_{\mathrm{guess}}(d,Q)$ was given in Eq. (16).

In order to quantify the number of signals, we have scaled N_0 with $\log_2 d$, as, for example, sending one state in the dimension $d=4$ corresponds to sending two states in the dimension $d=2$. For making the key rate comparable to the two-dimensional case, it has to be divided by $\log_2 d$. The dimensions are prime numbers as complete mutually unbiased bases can be formed for primes and prime powers (see, e.g., [42]).

Figure 4 shows the behavior of the key rate calculated with Eq. (35) for different dimensions. In contrast to [15], we scaled the key rate with the dimension. It can be seen from the plot that higher dimensions are advantageous as the key rate increases. In order to obtain the behavior for a small number of signals, Fig. 5 provides a magnification of this area. The higher the dimension, the more the point where the key rate becomes nonzero is shifted to the right (apart from the case $d=2$). This might be because of the correction term, as it scales linearly with the dimension, so for higher dimension, more is subtracted from the conditional von Neumann entropy. We will see in the next paragraph that the min-entropy approach has an advantage over the von Neumann entropy approach for a small number of signals.

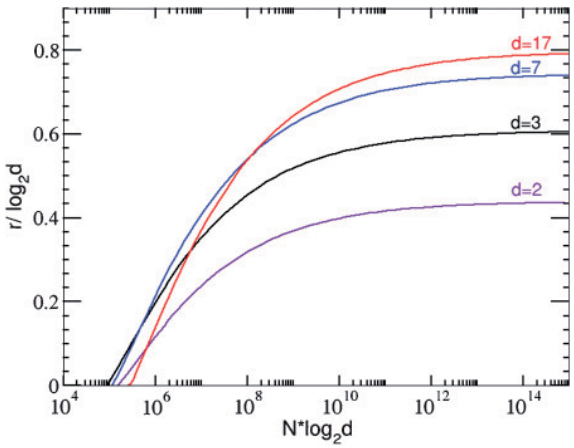

FIG. 4. (Color online) Key rates with d-dimensional conditional von Neumann entropy [Eq. (35)] plotted vs scaled total number of signals for a fixed error rate $Q = 5\%$. This is analogous to [15], where a different scale was used for the axes.

In Fig. 6, we compare the number N_0, where the key rate becomes nonzero, for key rates using the quantities given in Eqs. (35) and (36) for different dimensions. It can be seen that the min-entropy approach is better throughout the presented error rates. The advantage of the min-entropy approach [Eq. (36)] over the von Neumann approach [Eq. (35)] augments with increasing dimensions. This can be explained again with the correction term that scales linearly with the dimension. When comparing higher dimensions to the qubit case, one can see that for certain error rates, the dimensions bigger than two are advantegous. The dimension $d=3$, for example, gives a lower threshold value N_0 for nonzero key rates than the qubit case throughout all the presented error rates.

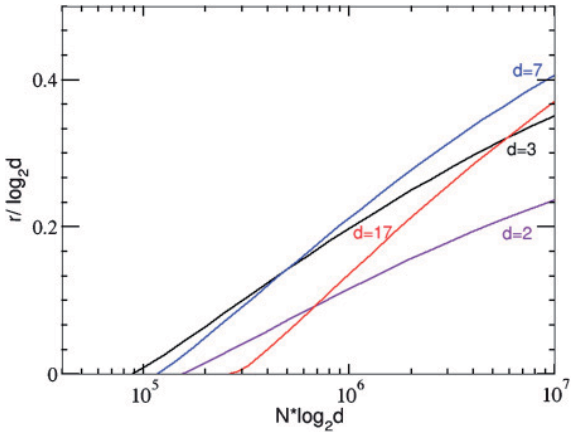

FIG. 5. (Color online) Key rates with d-dimensional conditional von Neumann entropy [Eq. (35)] plotted vs scaled total number of signals for a fixed error rate $Q = 5\%$ (magnification of Fig. 4).

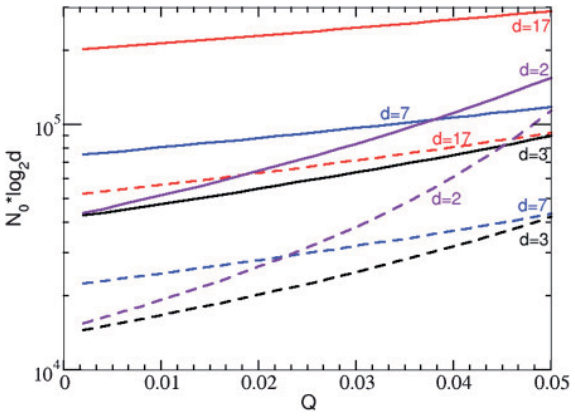

FIG. 6. (Color online) Threshold value N_0 (number of signals, where the key rate is positive) vs QBER with $\varepsilon = 10^{-9}$ and $\varepsilon_{\mathrm{EC}} = 10^{-10}$ for different dimensions $d \in \{2,3,7,17\}$. Dashed line, min-entropy [Eq. (36)]; straight line, von Neumann entropy [Eq. (35)].

VII. CONCLUSION

We have improved the secret key rates in QKD with a finite number of signals by considering parameter estimation to be implemented by a single POVM for all parameters. Additionally, we have calculated the min-entropy for a single-signal state in d dimensions explicitly by using its operational meaning via the guessing probability. We showed that using this ansatz for a small number of signals leads to computable nonzero key rates. This advantage of the min-entropy might be because of the correction term Δ in key rate calculations using the conditional von Neumann entropy [9,14,15] as this correction is big for a small number of signals. This correction term scales linearly with the dimension, so an improvement for high dimensions (up to $d = 17$) is found by calculating the min-entropy. Thus higher dimensional systems might be advantageous when resources are limited. As a spin-off, we have deduced from the additivity property of the min-entropy and its relation to the guessing probability that the optimal MED measurement for a set of tensor product states with a certain symmetry is the optimal MED measurement on each subsystem.

Considering the importance of finite-key analysis for practical implementations, we have shown that nonzero secure key rates can be achieved already with 10^4–10^5 signals per run.

ACKNOWLEDGMENTS

We would like to thank Silvio Abruzzo, Fabian Furrer, Matthias Kleinmann, and, in particular, Renato Renner for valuable and enlightening discussions. This work was financially supported in part by Deutsche Forschungsgemeinschaft (DFG).

APPENDIX: PROOF OF THEOREM 1

Proof. We first show that $\mathrm{Prob}[\frac{1}{2}||\vec{\lambda}_m - \vec{\lambda}_\infty||_1 > 2\xi] \leqslant \varepsilon_{\mathrm{PE}}$. Starting from the law of large numbers [43],

$$\mathrm{Prob}[D(\vec{\lambda}_m||\vec{\lambda}_\infty) > 2\xi'] \leqslant 2^{-m(2\xi' - |\chi| \frac{\log_2(m+1)}{m})}, \tag{A1}$$

with $D(\vec{\lambda}_m||\vec{\lambda}_\infty) := \sum_{i=1}^{|\chi|} \lambda_m(i) \log_2(\frac{\lambda_m(i)}{\lambda_\infty(i)})$ and using [43],

$$\frac{1}{2}||\vec{\lambda}_m - \vec{\lambda}_\infty||_1 \leqslant \sqrt{\frac{D(\vec{\lambda}_m||\vec{\lambda}_\infty)\ln 2}{2}}, \tag{A2}$$

we result in

$$\begin{aligned}
&\mathrm{Prob}\left[\frac{1}{2}||\vec{\lambda}_m - \vec{\lambda}_\infty||_1 > \sqrt{\frac{2\xi' \ln 2}{2}}\right] \\
&\overset{(A2)}{\leqslant} \mathrm{Prob}\left[\sqrt{\frac{D(\vec{\lambda}_m||\vec{\lambda}_\infty)\ln 2}{2}} > \sqrt{\frac{2\xi' \ln 2}{2}}\right] \\
&\overset{(A1)}{\leqslant} 2^{-m(2\xi' - |\chi| \frac{\log(m+1)}{m})}.
\end{aligned} \tag{A3}$$

For $\xi := \sqrt{\frac{2\xi' \ln 2}{2}}$ it follows that

$$\begin{aligned}
&\mathrm{Prob}\left[\frac{1}{2}||\vec{\lambda}_m - \vec{\lambda}_\infty||_1 > 2\xi\right] \\
&= \mathrm{Prob}\left[\frac{1}{2}||\vec{\lambda}_m - \vec{\lambda}_\infty||_1 > \sqrt{\frac{2(4\xi')\ln 2}{2}}\right] \\
&\overset{(A3)}{\leqslant} 2^{-m(2(4\xi') - |\chi| \frac{\log(m+1)}{m})} \\
&= 2^{-m(8\frac{\xi^2}{\ln 2} - |\chi| \frac{\log(m+1)}{m})} =: \varepsilon_{\mathrm{PE}}.
\end{aligned}$$

Then except with probability $\varepsilon_{\mathrm{PE}}$, the following holds:

$$\tfrac{1}{2}||\vec{\lambda}_m - \vec{\lambda}_\infty||_1 \leqslant 2\xi,$$

with $\xi = \sqrt{\frac{\ln(\frac{1}{\varepsilon_{\mathrm{PE}}}) + |\chi| \ln(m+1)}{8m}}$. It remains to show that

$$\tfrac{1}{2}||\lambda_m - \lambda_\infty||_1 \equiv \tfrac{1}{2}|\lambda_m - \lambda_\infty| \leqslant \tfrac{1}{2}\tfrac{1}{2}||\vec{\lambda}_m - \vec{\lambda}_\infty||_1.$$

Remember that we denote by $\lambda_m := \lambda_m(k)$ and $\lambda_\infty := \lambda_\infty(k)$ any kth parameter. The normalization conditions of the POVM $\sum_{i=1}^{|\chi|} \lambda_\infty(i) = 1 = \sum_{i=1}^{|\chi|} \lambda_m(i)$ lead to

$$\begin{aligned}
|\lambda_m - \lambda_\infty| &= \left|\sum_{i=1, i\neq k}^{|\chi|} \lambda_m(i) - \lambda_\infty(i)\right| \\
&\overset{\Delta}{\leqslant} \sum_{i=1, i\neq k}^{|\chi|} |\lambda_m(i) - \lambda_\infty(i)|
\end{aligned} \tag{A4}$$

$$\sum_{i=1}^{|\chi|} |\lambda_m(i) - \lambda_\infty(i)| \overset{(A4)}{\geqslant} 2|\lambda_m - \lambda_\infty|.$$

The assertion follows by multiplication with factor $\frac{1}{4}$.

[1] C. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[2] M. Ben-Or and D. Mayers, e-print arXiv:quant-ph/0409062.
[3] D. Unruh, e-print arXiv:quant-ph/0409125.
[4] J. Müller-Quade and R. Renner, New J. Phys. **11**, 085006 (2009).

[5] R. Renner and R. König, *Theory of Cryptography*, Lecture Notes in Computer Science, edited by J. Kilian (Springer, Berlin, 2005), Vol. 3378, p. 407.
[6] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[7] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[8] M. Hayashi, Phys. Rev. A **76**, 012329 (2007).
[9] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).
[10] R. Renner, Int. J. Quant. Inform. **6**, 1 (2008).
[11] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[12] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[13] T. Meyer, H. Kampermann, M. Kleinmann, and D. Bruß, Phys. Rev. A **74**, 042340 (2006).
[14] R. Cai and V. Scarani, New J. Phys. **11**, 045024 (2009).
[15] L. Sheridan and V. Scarani, Phys. Rev. A **82**, 030301 (2010).
[16] J. Hasegawa, M. Hayashi, T. Hiroshima, A. Tanaka, and A. Tomita, e-print arXiv:0705.3081 [quant-ph].
[17] R. König, R. Renner, and C. Schaffner, IEEE Trans. Inform. Theor. **55**, 4337 (2009).
[18] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).
[19] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).
[20] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[21] V. Scarani and R. Renner, in *Theory of Quantum Computation, Communication, and Cryptography*, Lecture Notes in Computer Science, edited by Y. Kawano and M. Mosca (Springer, Berlin, 2008), Vol. 5106, p. 83.
[22] R. Y. Q. Cai and V. Scarani, New J. Phys. **11**, 109801 (2009).
[23] E. Biham and T. Mor, Phys. Rev. Lett. **78**, 2256 (1997); E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, Algorithmica **34**, 372 (2002).
[24] A. Holevo, Theor. Probab. Appl. **23**, 411 (1978).
[25] P. Hausladen and W. Wootters, J. Mod. Opt. **41**, 2385 (1994).
[26] M. Ban, K. Kurukowa, R. Momose, and O. Hirota, Int. J. Theor. Phys. **36**, 1269 (1997).
[27] Y. Eldar and G. Forney, IEEE Trans. Inform. Theor. **47**, 858 (2001).
[28] A. Chefles, Contemp. Phys. **41**, 401 (2000).
[29] S. M. Barnett, Phys. Rev. A **64**, 030303 (2001).
[30] A. S. Holevo, J. Multivariate Anal. **3**, 337 (1973).
[31] H. Yuen, R. Kennedy, and M. Lax, IEEE Trans. Inform. Theor. **21**, 125 (1975).
[32] C. Helstrøm, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[33] U. Herzog and J. A. Bergou, Phys. Rev. A **70**, 022302 (2004).
[34] D. Qiu and L. Li, Phys. Rev. A **81**, 042329 (2010).
[35] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
[36] D. Bruß and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).
[37] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).
[38] D. Bruß, M. Christandl, A. Ekert, B. G. Englert, D. Kaszlikowski, and C. Macchiavello, Phys. Rev. Lett. **91**, 097901 (2003).
[39] Y. Liang, D. Kaszlikowski, B. G. Englert, L. C. Kwek, and C. H. Oh, Phys. Rev. A **68**, 022324 (2003).
[40] D. Kaszlikowski, A. Gopinathan, Y. C. Liang, L. C. Kwek, and B. G. Englert, Phys. Rev. A **70**, 032306 (2004).
[41] V. Scarani, in *Quantum Cryptography and Computing*, NATO Science for Peace and Security Series D: Information and Communication Security, edited by R. Horodecki, S. Y. Kilin, and J. Kowalik (IOS press, Amsterdam, 2010), Vol. 26, p. 76.
[42] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, e-print arXiv:1004.3348 [quant-ph].
[43] T. Cover and J. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).

Min-entropy and quantum key distribution: Nonzero key rates for “small” numbers of signals
Physical Review A, Vol. **83**, p. 022330 (2011) [9 pages]
S. Bratzik, M. Mertz, H. Kampermann, and D. Bruß

Impact factor: 2.861
Second author
Contribution to work by scientific work and preparation of Section III of the manuscript (35%)

Publication D

Quantum key distribution with finite resources: Secret key rates via Rényi entropies

Silvestre Abruzzo,* Hermann Kampermann, Markus Mertz, and Dagmar Bruß
Institute for Theoretical Physics III, Heinrich-Heine-universität Düsseldorf, D-40225 Düsseldorf, Germany
(Received 31 May 2011; published 16 September 2011)

A realistic quantum key distribution (QKD) protocol necessarily deals with finite resources, such as the number of signals exchanged by the two parties. We derive a bound on the secret key rate which is expressed as an optimization problem over Rényi entropies. Under the assumption of collective attacks by an eavesdropper, a computable estimate of our bound for the six-state protocol is provided. This bound leads to improved key rates in comparison to previous results.

DOI: 10.1103/PhysRevA.84.032321 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum key distribution (QKD) is a method for transmitting a secret key between two partners. Since its initial proposal [1] QKD has reached maturity through many theoretical developments and experimental realizations. Moreover, in the last few years QKD has entered the commercial market [2] and small QKD networks were realized [3,4].

A significant figure of merit in QKD is the *secret key rate* (i.e., the ratio between the length of the secret key and the initial number of signals). There is a big difference between the key rate calculated under the assumption that the key is composed of an infinite number of bits, and a key in real applications, where the number of bits is finite. In recent years a new paradigm for security in the finite-key setting was developed [5–10]. However, the complexity of the entropic quantities involved in the formalism only permits to find bounds on the optimal quantities, which leads to much lower key rates for a small number of signals with respect to the asymptotic ones.

To our knowledge the first work dealing with finite key corrections is [11]. The currently used framework for finite-key analysis was developed in [6,7,9,10]. The bound proved in [7] was used by Meyer *et al*. [12] to calculate the key rate in the finite-key scenario. In [9,10] security bounds for the BB84 and the six-state protocol were provided using an easily calculable bound for the smooth min-entropy. Recently, many efforts were done for improving the bounds on the secret key rates for a finite amount of resources (e.g., using the connection between the min-entropy and the guessing probability [13,14]). So far the secret key rates provided are only proven to be secure for collective attacks. A possible approach for providing security against coherent attacks using the results against collective attacks can be obtained by postselections techniques [15–17] or the exponential de Finetti theorem [6]. A recent technique is given by uncertainty relations for the smooth min-entropy [18,19]. This last approach is very promising because it provides an easily calculable tight bound on the key rate even for coherent attacks, however, it is not easily applicable to the six-state protocol. A step in the direction of considering more practical issues in addition to finite-key corrections (BB84 with and without decoy states and entanglement-based implementations) was provided in [20,21].

In this paper, we present a bound on the achievable key length for the six-state protocol. The presented bound is resorted from [7], Lemma 9, where it is used for bounding the key length in terms of smooth Rényi entropies. We calculate explicitly the presented bound under the assumptions of collective attacks and the depolarizing channel. The calculated secret key rates for a small number of signals lead to an improvement over the bounds derived in [10–12].

The paper is organized as follows. In Sec. II we present the protocol we are going to study. In Sec. III we introduce definitions and our notation. In Sec. IV we explain the approach developed in this paper and we show how to estimate the proposed bound for the achievable key rate. In Sec. V we compare the proposed bound with other relevant bounds present in the literature. Section VI contains the conclusions. In the Appendices we prove additional results used in the paper.

II. DESCRIPTION OF THE PROTOCOL

In this paper we consider the entanglement-based version of the *six-state protocol* [22,23]. The protocol consists of the following steps.

State preparation and distribution. Alice prepares N entangled Bell states and distributes one part of each pair to Bob. We assume that Eve performs at most a collective attack (i.e., the adversary acts on each of the signals independently and identically).

Reduction to Bell-diagonal form. Alice and Bob apply randomly and simultaneously one of the operators $\{\mathbb{1},\sigma_X,\sigma_Y,\sigma_Z\}$ and as a result they obtain a Bell-diagonal state the entries of which are directly connected with the quantum bit error rates (QBER), [24] and Appendix. C.

Sifting and Measurement. Alice and Bob measure at random one of the three Pauli operators. The Pauli operators are chosen with different probabilities. We consider that σ_X and σ_Y are chosen with the same probability and that σ_Z is chosen such that $\mathrm{Prob}(\sigma_Z) \geqslant \mathrm{Prob}(\sigma_X)$. This biased setting [25] is advantageous in terms of sifting. At the end of the measurement process, Alice and Bob broadcast the choice of the bases through the classical channel and discard the results coming from a different choice of the measurement basis. We call $n' = n'_X + n'_Y + n'_Z$ the length of the sifted key shared by Alice and Bob, where n'_i with $i = X,Y,Z$ are the remaining number of signals when both Alice and Bob measure $\sigma_X,\sigma_Y,\sigma_Z$.

*abruzzo@thphy.uni-duesseldorf.de

Parameter estimation. Parameter estimation (PE) permits to measure the amount of errors on the key, which in the security analysis are assumed to be introduced via Eve's eavesdropping. In the six-state protocol three bases are used for the measurement and therefore a QBER in each direction is calculated by Alice and Bob. Practically speaking, Alice broadcasts for each basis $m_i < n_i'$ bits of the sifted key on the classical channel. Bob compares these outcomes with his corresponding outcomes and calculates the QBERs e_m^i as the ratio between the number of discordant positions and the length of the transmitted strings. In general $e_m^X \neq e_m^Y \neq e_m^X$. For calculating explicitly the bound that we are going to propose we use the biggest QBER as measured QBER, denoted as e_m. Note that it is possible to introduce additional symmetrizations [26,27] that reduce the initial state to a state described by only one parameter: the QBER. However those symmetrizations require additional experimental means that can be difficult to implement.

The remaining $n := n' - m_X - m_Y - m_Z$ bits will be used for the extraction of the key. The QBER e is bounded by the PE developed in [11,12,14,20]. The parameter $\varepsilon_{\mathrm{PE}}$ represents the probability that we underestimated the real QBER.

The QBER of the key e with probability $1 - \varepsilon_{\mathrm{PE}}$ is such that [11,12,14,20]

$$e \leqslant e_m + 2\zeta(\varepsilon_{\mathrm{PE}}, m), \tag{1}$$

with

$$\zeta(\varepsilon_{\mathrm{PE}}, m) := \sqrt{\frac{\ln\left(\frac{1}{\varepsilon_{\mathrm{PE}}}\right) + 2\ln(m+1)}{8m}}. \tag{2}$$

Error correction. Alice and Bob hold correlated classical bit strings X^n and Y^n. The purpose of an error correction (EC) protocol is to create a fully correlated string, while leaking only a small amount of information to an adversary. In the following, we will consider realistic EC protocols. The number of bits leaked during the classical communication to an eavesdropper is given by [11,20]

$$\mathrm{leak}_{\mathrm{EC}} = f_{\mathrm{EC}} n h(e) + \log_2\left(\frac{2}{\varepsilon_{\mathrm{EC}}}\right), \tag{3}$$

where $f_{\mathrm{EC}} \gtrsim 1$ depends on the used EC protocol, $h(e)$ is the binary Shannon entropy [i.e., $h(e) = -e\log_2(e) - (1-e)\log_2(1-e)$], and e is the QBER. Here, $\varepsilon_{\mathrm{EC}}$ is the probability that Alice's and Bob's strings differ after the EC step.

Privacy amplification. Let Alice and Bob hold a perfectly correlated bit string X^n, on which Eve might have some information. The purpose of privacy amplification is to shrink the length of X^n to reduce Eve's information on the resulting string.

Practically, Alice chooses at random a two-universal hash function (Definition B.1 in Appendix B) and communicates it to Bob.

III. DEFINITIONS AND NOTATION

The set of quantum states, which are normalized positive-semidefinite bounded operators, will be represented by $S(\mathcal{H})$, where $\mathcal{H}$ stands for a finite-dimensional Hilbert space. In the following $\rho_A(\rho_B)$ belongs to the set of bounded operators which act on the Hilbert space $\mathcal{H}^A(\mathcal{H}^B)$. For a given state ρ_{AB}, the states ρ_A, ρ_B are defined via the partial trace (i.e., $\rho_A := \mathrm{tr}_B\,\rho_{AB}$ and $\rho_B := \mathrm{tr}_A\,\rho_{AB}$).

In this paper, we will consider Rényi entropies, which are a generalization of the Von Neumann entropy.

Definition III.1. (Rényi entropies [7,28]) Let $\alpha \in \mathbb{R} \cup \{\infty\}$ and $\rho, \sigma \in \mathrm{S}(\mathcal{H})$. The Rényi entropy of order α is defined as

$$S_\alpha(\rho) := \frac{1}{1-\alpha}\log_2\left[\mathrm{tr}\left(\rho^\alpha\right)\right]. \tag{4}$$

In particular, we get

$$S_0(\rho) = \log_2\left[\mathrm{rank}(\rho)\right], \tag{5}$$

$$S_2(\rho) = -\log_2\left[\mathrm{tr}(\rho^2)\right], \tag{6}$$

$$S_\infty(\rho) = -\log_2\left[\lambda_{\max}(\rho)\right], \tag{7}$$

where $\lambda_{\max}(\rho)$ is the maximal eigenvalue of ρ.

Another useful quantity is the smooth Rényi entropy, which is the Rényi entropy optimized on a set of operators which are ε-close to the operator involved in the actual computation. We define an ε-environment via the trace distance in the following way [7].

Definition III.2. (ε-environment) Let $\varepsilon \geqslant 0$ and $\rho \in S(\mathcal{H})$, then

$$\mathcal{B}^\varepsilon(\rho) := \{\sigma \in S(\mathcal{H}) : \tfrac{1}{2}||\sigma - \rho||_1 \leqslant \varepsilon\}, \tag{8}$$

where $||A||_1 = \mathrm{tr}\sqrt{AA^\dagger}$.

Definition III.3. The smooth Rényi entropy of order α is defined (following [7]) as

$$S_\alpha^\varepsilon(\rho) := \frac{1}{1-\alpha}\inf_{\sigma\in\mathcal{B}^{\frac{\varepsilon}{2}}(\rho)}\log_2\left[\mathrm{tr}\left(\sigma^\alpha\right)\right]. \tag{9}$$

The main result presented in this paper will be expressed as an optimization problem on a *classical-quantum ε-environment* of a certain operator.

Definition III.4. [Classical-quantum (cq)-state] Let $\{|x\rangle\}$ be an orthonormal basis of $\mathcal{H}^X$ and moreover let $\mathcal{H}^A$ be a generic Hilbert space. We define the state ρ_{XA} which is classical on $\mathcal{H}^X$ and quantum on $\mathcal{H}^A$ as the state

$$\rho_{XA} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho_A^x,$$

where $\rho_A^x \in \mathcal{S}(\mathcal{H}^A)$ and $P_X(x)$ is a classical probability distribution.

Finally, we define the *classical-quantum ε-environment* as the space

$$\mathcal{B}_{\mathrm{cq}}^\varepsilon(\rho_{XA}) := \left\{\sigma_{XA} \in \mathcal{B}^\varepsilon(\rho_{XA}) : \sigma_{XA} = \sum_x P_X(x)|x\rangle\langle x| \otimes \sigma_A^x\right\},$$

where $\sigma_A^x \in \mathcal{S}(\mathcal{H}^A)$ and $P_X(x)$ is a classical probability distribution. Finally, we recall the composable definition of security introduced by Renner in [7]. For additional details see [29].

Definition III.5. Let ρ_{KE} be the cq-state describing the classical key K of length ℓ, distilled at the end of a

QKD protocol, correlated with the quantum states of the eavesdropper ρ_E. The state ρ_{KE} is said to be ε-secure if

$$\tfrac{1}{2}\left\|\rho_{KE} - \tfrac{1}{2^\ell}\mathbb{1}\otimes\rho_{E'}\right\|_1 \leqslant \varepsilon, \tag{10}$$

where $\rho_{E'}$ is the quantum state of an eavesdropper not correlated with the key.

In the literature several bounds on an ε-secure key length [6,7,30] were presented.

IV. BOUND ON THE ACHIEVABLE KEY LENGTH

The following bound was inspired by [7], Theorem 4 where it was used as a bridge for providing an analogous bound in terms of smooth Rényi entropies.

Theorem IV.1. Let $\rho_{X^nE^n}$ be the cq state describing Alice's bitstring X^n as well as Eve's quantum information represented by ρ_{E^n}. Let $\overline{\varepsilon},\varepsilon_{PA} \geqslant 0$. If the length ℓ of the key is such that

$$\ell \leqslant \sup_{\sigma_{X^nE^n}\in\mathcal{B}^{\frac{\overline{\varepsilon}}{2}}_{\mathrm{cq}}(\rho_{X^nE^n})} [S_2(\sigma_{X^nE^n}) - S_0(\sigma_{E^n})] - \mathrm{leak}_{\mathrm{EC}} + 2\log_2(2\varepsilon_{PA}), \tag{11}$$

then the key is $\overline{\varepsilon}+\varepsilon_{PA}$-secure.

Sketch of Proof. In the following we give an idea of the proof which follows the lines of [6,7]. For all details see Appendix B. We first prove that ℓ can be chosen such that

$$\ell \leqslant \sup_{\sigma_{X^nE^nC}\in\mathcal{B}^{\frac{\overline{\varepsilon}}{2}}(\rho_{X^nE^nC})} [S_2(\sigma_{X^nE^nC}) - S_0(\sigma_{E^nC})] + 2\log_2(2\varepsilon_{PA}), \tag{12}$$

where the additional random variable C is associated with the probability distribution of transcripts of the EC protocol. Then we will "extract" the leakage term using the data processing inequality and the subadditivity of the Rényi entropies. ■

The bound in Eq. (11) is related to the bound calculated in [10] because it involves optimizations on Rényi entropies. However, in [10] the two Rényi entropies were optimized independently and here we have a combined optimization problem. This additional constraint is mitigated by the fact that in our bound we optimize over a bigger environment than the one used in [10], more precisely $\varepsilon' = \frac{\overline{\varepsilon}^2}{2}$ where ε' is the environment used for the smooth Rényi entropies in [10].

A. Lower bound of Theorem IV.1 using smooth Rényi entropies

In this section, we present a lower bound for the key length presented in Theorem IV.1. The optimization problem involved in Eq. (11) is exponentially complex because the dimension of the involved operators scales with n, that is, the length of the string used for extracting the key. For reducing the complexity of the problem we consider the symmetric six-state protocol. For this protocol the number of different eigenvalues in $\rho_{XE}^{\otimes n}$ scales polynomially with n [10], therefore as done in [10], it is possible to concentrate on optimizing the eigenvalue distribution of $\sigma_{X^nE^n}$. However, it is not clear how to find the eigenvalue distribution of σ_{E^n} from the one of $\sigma_{X^nE^n}$ in such a way that it is possible to perform computations for big n. In the following we present a lower bound on Theorem IV.1 expressed in terms of the smooth Rényi entropy of order zero and a *modified smooth Rényi entropy of order two* that we will denote as $\overline{S}_2^{\varepsilon}(\rho_{XE}^{\otimes n})$. This last entropy permits to bound the eigenvalues of σ_{E^n} for a given $\sigma_{X^nE^n}$. From the numerical point of view the deviation from $S_2^{\varepsilon}(\rho_{XE}^{\otimes n})$ is negligible.

1. Modified Smooth Rényi entropy of order two

Let $\rho_{XE}^{\otimes n}$ be the operator describing Alice's classical string of n bits correlated with the operator $\rho_E^{\otimes n}$ held by Eve. The operator $\rho_{XE}^{\otimes n}$ is constructed by a direct sum of 2^n blocks which have the same eigenvalues (see Appendix C for additional details).

Definition IV.2. The modified smooth Rényi entropy of order two of the operator $\rho_{XE}^{\otimes n}$ is defined by

$$\overline{S}_2^{\varepsilon}\left(\rho_{XE}^{\otimes n}\right) := S_2(\tau_{X^nE^n}), \tag{13}$$

where the operator $\tau_{X^nE^n}$ has the following properties.

(1) $\tau_{X^nE^n}$ has the following form

$$\tau_{X^nE^n} := \frac{1}{2^n}\sum_{x=0}^{2^n-1} |x\rangle\langle x| \otimes \tau_{E^n}^x, \tag{14}$$

where $\{|x\rangle\}$ is the basis in which $\rho_{XE}^{\otimes n}$ is a cq-state (Definition III.4). Moreover each of the $\{\tau_{E^n}^x\}$ has the same eigenvalues and the dependence on x is manifested only in the eigenvectors (see Eq. (D4) for a more formal statement).

(2) Let $\{\Lambda_i\}_{i=0,\ldots,n+1}$ be the set of differing eigenvalues of one block of the operator $\rho_{XE}^{\otimes n}$ in increasing order; that is, $\Lambda_i < \Lambda_{i+1}$ and let $\{m_i\}_{i=0,\ldots,n+1}$ be the set of multiplicities such that m_i is the multiplicity of Λ_i. Let $\{\mu_i\}_{i=0,\ldots,n+1}$ be the eigenvalues of one block of $\tau_{X^nE^n}$ in increasing order with respective multiplicity $\{n_i\}_{i=0,\ldots,n+1}$. Let

$$s_r^+ := \sum_{i=1}^{r} m_{n-i+2}(\Lambda_{n-i+2} - \Lambda_{n-r+1}), \tag{15}$$

(16)

for $1 \leqslant r \leqslant n+1$. The eigenvalues of $\tau_{X^nE^n}$ are defined by the following relations

$$\begin{cases} \mu_i := \begin{cases} \Lambda_+ & n+1-b^+ \leqslant i \leqslant n+1, \\ \Lambda_i & 1 \leqslant i \leqslant n-b^+, \\ \frac{\varepsilon}{2m_0} & i=0, \end{cases} \\ n_i = m_i \quad 1 \leqslant i \leqslant n+1, \end{cases} \tag{17}$$

where

$$b^+ := \max\left\{r : s_r^+ \leqslant \frac{\varepsilon}{2}\right\}, \tag{18}$$

and

$$\Lambda_+ := \Lambda_{n-b^++1} - \frac{\frac{\varepsilon}{2} - s_{b^+}^+}{\sum_{i=0}^{b^+} m_{n-i+1}}. \tag{19}$$

Since the smoothing in the smooth Rényi entropy of order two is realized by taking the maximum in the environment, it follows for any operator $\overline{\sigma}_{X^nE^n} \in \mathcal{B}^{\frac{\varepsilon}{2}}(\rho_{XE}^{\otimes n})$

$$S_2^{\varepsilon}\left(\rho_{XE}^{\otimes n}\right) \geqslant S_2(\overline{\sigma}_{X^nE^n}).$$

Therefore, if we can prove that the operator $\tau_{X^nE^n}$ introduced before is such that $\tau_{X^nE^n} \in \mathcal{B}^{\frac{\varepsilon}{2}}(\rho_{XE}^{\otimes n})$, then we have proven that

the modified smooth Rényi entropy is a lower bound for the smooth Rényi entropy.

Proposition IV.3. The operator $\tau_{X^nE^n}$ defined by its eigenvalues in Eq. (17) is such that $\frac{1}{2}\|\tau_{X^nE^n} - \rho_{XE}^{\otimes n}\| = \frac{\varepsilon}{2}$ [i.e., $\tau_{X^nE^n} \in \mathcal{B}^{\frac{\varepsilon}{2}}(\rho_{XE}^{\otimes n})$].

Proof. The proof follows by the direct calculation of the distance using the spectral decomposition of $\rho_{XE}^{\otimes n}$. ■

For the six-state protocol for $n = 10^4$, it turns out that[1] $|\overline{S}_2^{\varepsilon}(\rho_{XE}^{\otimes n}) - S_2^{\varepsilon}(\rho_{XE}^{\otimes n})|/S_2^{\varepsilon}(\rho_{XE}^{\otimes n}) \propto 10^{-5390}$ for a QBER = 5% and $\varepsilon = 10^{-16}$. Moreover, for increasing n the difference becomes smaller. The reason of this similarity is that the dimension of the kernel of $\rho_{XE}^{\otimes n}$ is much bigger than the degeneracy of the support, namely $m_0 = 2^{2n} - 2^n$ versus $\sum_{i\neq 0} m_i = 2^n$, therefore there is, practically, no difference between the eigenvalue distribution in Eq. (17) and the optimal eigenvalue distribution for $S_2^{\varepsilon}(\rho_{XE}^{\otimes n})$ presented in [10].

2. Computable lower bound for the achievable key length

The following theorem provides the bound that we are going to exploit in this paper.

Theorem IV.4. Let $\rho_{XE}^{\otimes n}$ be the cq state describing the classical string shared by Alice and Bob and the correlated quantum state of the eavesdropper. Then

$$\sup_{\sigma_{X^nE^n} \in \mathcal{B}_{\mathrm{cq}}^{\frac{\bar{\varepsilon}}{2}}\left(\rho_{XE}^{\otimes n}\right)} [S_2(\sigma_{X^nE^n}) - S_0(\sigma_{E^n})] \geqslant \overline{S}_2^{\bar{\varepsilon}-\hat{\varepsilon}}\left(\rho_{XE}^{\otimes n}\right) - S_0^{\hat{\varepsilon}}\left(\rho_E^{\otimes n} + \bar{\delta}_{E^n}\right) - \hat{\varepsilon},$$

with $\bar{\delta}_{E^n} = \frac{\hat{\varepsilon}}{2^{2n+1}}\mathbf{1}_{E^n}$ and $0 \leqslant \hat{\varepsilon} \leqslant \bar{\varepsilon}$.

Proof. To provide a lower bound, it is enough to choose an operator in $\mathcal{B}_{\mathrm{cq}}^{\frac{\bar{\varepsilon}}{2}}(\rho_{XE}^{\otimes n})$ and to calculate the difference between the Rényi entropies of the chosen operator. In Appendix D we construct an operator $\eta_{X^nE^n} \in \mathcal{B}_{\mathrm{cq}}^{\frac{\bar{\varepsilon}}{2}}(\rho_{XE}^{\otimes n})$ such that the following two inequalities hold:

$$S_2(\eta_{X^nE^n}) \geqslant \overline{S}_2^{\bar{\varepsilon}-\hat{\varepsilon}}\left(\rho_{XE}^{\otimes n}\right) - \hat{\varepsilon}, \tag{20}$$

and

$$S_0(\eta_{E^n}) \leqslant S_0^{\hat{\varepsilon}}\left(\rho_E^{\otimes n} + \bar{\delta}_{E^n}\right), \tag{21}$$

where $\bar{\delta}_{E^n} = \frac{\hat{\varepsilon}}{2^{2n+1}}\mathbf{1}_{E^n}$.

Using these two inequalities, we have

$$\sup_{\sigma_{X^nE^n} \in \mathcal{B}_{\mathrm{cq}}^{\frac{\bar{\varepsilon}}{2}}(\rho_{XE}^{\otimes n})} [S_2(\sigma_{X^nE^n}) - S_0(\sigma_{E^n})] \tag{22}$$

$$\geqslant S_2(\eta_{X^nE^n}) - S_0(\eta_{E^n}) \tag{23}$$

$$\geqslant \overline{S}_2^{\bar{\varepsilon}-\hat{\varepsilon}}\left(\rho_{XE}^{\otimes n}\right) - S_0^{\hat{\varepsilon}}\left(\rho_E^{\otimes n} + \bar{\delta}_{E^n}\right) - \hat{\varepsilon}. \tag{24}$$

■

Remark IV.5. Numerical calculations indicate that the choice $\hat{\varepsilon} = \frac{\bar{\varepsilon}}{2}$ is optimal for a wide range of used parameters.

Remark IV.6. The bound provided in Theorem IV.4 may not be asymptotically optimal. However, the emphasis is for finite-key analysis and the bound permits to improve the key rate for experimentally relevant number of signals. Note that, although we can have small differences in the asymptotic case, the bound is, from the numerical point of view, pretty tight. In fact, note that (see Definition III.3)

$$\sup_{\sigma_{X^nE^n} \in \mathcal{B}_{\mathrm{cq}}^{\frac{\bar{\varepsilon}}{2}}(\rho_{XE}^{\otimes n})} [S_2(\sigma_{X^nE^n}) - S_0(\sigma_{E^n})] \leqslant S_2^{\bar{\varepsilon}}\left(\rho_{XE}^{\otimes n}\right) - S_0^{\bar{\varepsilon}}\left(\rho_E^{\otimes n}\right).$$

Calculating the difference between the upper bound and the lower bound, it is for small n ($n \approx 10^4$) of the order of 0.1% and it decreases for larger n.

V. RESULTS

The security is characterized by the parameter ε, representing the acceptable probability of failure of the execution of the protocol. In the following we consider a standard setting with $\varepsilon = 10^{-9}$. For the simulations we assume that $n'_X = n'_Y$ and we take for PE $m_X = m_Y = m_Z = n'_X$. The length of the string used for the extraction of the key is $n = n'_Z - m_Z$ which has, at most, QBER $e = e_m + 2\zeta(\varepsilon_{\mathrm{PE}}, m_Z)$ with probability $1 - \varepsilon_{\mathrm{PE}}$ (see Eq. (1)). The EC protocol performs such that in Eq. (3) we have $f_{\mathrm{EC}} = 1.2$ and $\varepsilon_{\mathrm{EC}} = 10^{-10}$ ([12] and Eq. (3)). Finally, we optimize the free parameters $[\varepsilon_{\mathrm{PE}}, \bar{\varepsilon}, \varepsilon_{PA}, \mathrm{Prob}(\sigma_X), n]$ to maximize the secret key rate.

The algorithms for the calculations were implemented using C++. The library CNL (Class Library for Numbers) [31] was used to perform calculations with arbitrary precision. Due to the nonsmoothness of the involved functions, we used the Hybrid Optimization Parallel Search PACKage (HOPSPACK) [32], which permits to deal with all involved optimizations in an efficient way and permits to perform the calculations on a cluster.

In the following we summarize the three bounds for the achievable secret key rate that we are going to compare.

3. Bound proposed in this paper

The following proposition summarizes our results of Sec. IV.

Proposition V.1. Let $\rho_{XE}^{\otimes n}$ be the cq-state describing the classical string shared by Alice and Bob which is correlated with the quantum state of the eavesdropper. Let N be the initial number of quantum states shared by Alice and Bob, n be the length of the string used for extracting the key which has QBER $e = e_m + 2\zeta(\varepsilon_{\mathrm{PE}}, m_Z)$ with probability $1 - \varepsilon_{\mathrm{PE}}$. Then Alice and Bob can achieve the secret key rate

$$r := \frac{1}{N}\left[\overline{S}_2^{\bar{\varepsilon}}\left(\rho_{XE}^{\otimes n}\right) - S_0^{\bar{\varepsilon}}\left(\rho_E^{\otimes n} + \bar{\delta}_{E^n}\right) - \bar{\varepsilon} - \mathrm{leak}_{\mathrm{EC}}\right]_{e=e_m+2\zeta} + 2\log_2(2\varepsilon_{PA}), \tag{25}$$

where $\varepsilon = \varepsilon_{\mathrm{PE}} + \varepsilon_{PA} + \bar{\varepsilon} + \varepsilon_{\mathrm{EC}}$.

Proof. Using Theorems IV.1 and IV.4 and Remark IV.5 the result follows. ■

4. Asymptotic Equipartition Property bound

The conditional smooth min-entropy [6] characterizes the optimal secret key rate [6,18]. The asymptotic equipartition property AEP bound used in [12,14] comes from the AEP

[1]The high precision used in this calculation is obtained using an arbitrary precision computer program (see Sec. V).

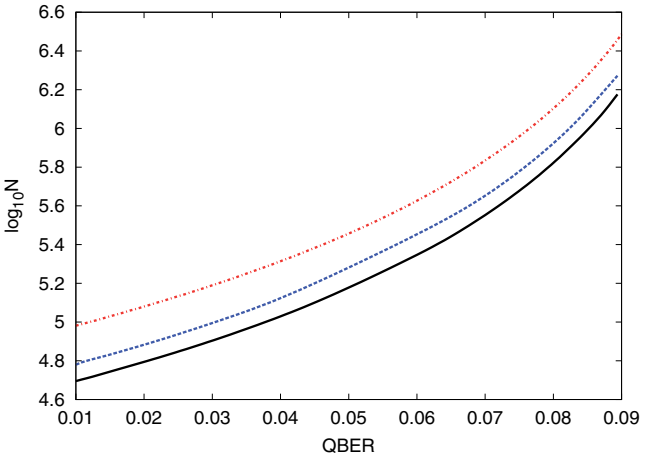

FIG. 1. (Color online) Minimal number of signals versus QBER permitting to extract a nonzero secret key rate. Comparison between the bound presented in this article r (black solid line), see Eq. (25), the smooth Rényi entropy bound r_{SRE} (blue dashed line), see Eq. (27) and the AEP bound r_{AEP} (red dot-dashed line), see Eq. (26).

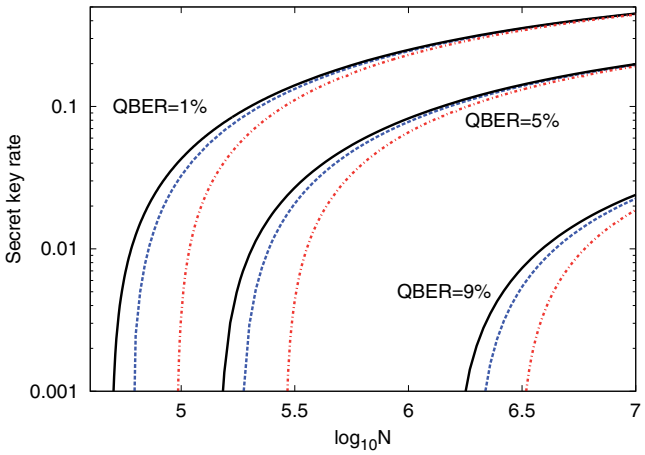

FIG. 2. (Color online) Secret key rate versus $\log_{10}(N)$ where N is the initial number of quantum systems shared by Alice and Bob. Comparison between the bound presented in this article r (black solid line), see Eq. (25), the smooth Rényi entropy bound r_{SRE} (blue dashed line), see Eq. (27) and the AEP bound r_{AEP} (red dot-dashed line), see Eq. (26).

approximation [6,33] of the conditional smooth min-entropy. Collective attacks allow us to bound the smooth min-entropy of a product state by the conditional von Neumann entropy of a single state [11,14]. The secret key rate is

$$r_{\mathrm{AEP}} := \frac{n}{N}\left[H(X|E)_\rho - 5\sqrt{\frac{\log_2(2/\bar{\varepsilon})}{n}} - \mathrm{leak}_{\mathrm{EC}}\right]_{e=e_m+2\zeta} + 2\log_2(2\varepsilon_{PA}), \tag{26}$$

with $H(X|E)_\rho = (1-e)[1-h(\frac{1-\frac{3}{2}e}{1-e})]$.

5. *Smooth Rényi entropy bound*

This bound was derived in [7] and calculated in [10] and is given by

$$r_{\mathrm{SRE}} := \frac{1}{N}\left[S_2^{\varepsilon'}\left(\rho_{XE}^{\otimes n}\right) - S_0^{\varepsilon'}\left(\rho_E^{\otimes n}\right) - \mathrm{leak}_{\mathrm{EC}}\right]_{e=e_m+2\zeta} + 2\log_2(2\varepsilon_{PA}), \tag{27}$$

where $\varepsilon' = \frac{\bar{\varepsilon}^2}{2}$.

A. Robustness of the protocol

An important figure of merit is the *threshold QBER* which characterizes the minimal N for a fixed QBER permitting to extract a positive secret key rate. As shown in Fig. 1, with the bound presented in this paper it is possible to have a positive secret key rate with 23% signals less than the smooth Rényi entropy bound and 50% signals less than the AEP approach, for a QBER of 1%.

B. Secret key rates

In Fig. 2, we compare the secret key rates calculated by the three approaches for various QBERs. The bound developed in this paper leads to significantly higher secret key rates when limited resources are used. In particular when QBER $= 1\%$ with the bound presented in this paper with $N \approx 5 \times 10^4$, it is possible to have nonzero secret key rates. Instead with the other approaches it is necessary to use $N \approx 6.5 \times 10^4$ for the smooth Rényi entropy bound and $N \approx 10^5$ for the AEP bound.

VI. CONCLUSION

Although optimal bounds for the finite-key scenario are provided in the literature they are not calculable and were, so far, only estimated by bounds coming from the asymptotic equipartition theorem (see [14,19] for two exceptions). In this paper we resumed the smooth Rényi entropy bound [10] and we proved that this bound is tighter than the AEP bound. Our main contribution is a bound on the maximal achievable secret key length which involves optimizations on Rényi entropies. With respect to [10] the main advantage is that we use a bigger environment for the optimizations and with respect to [11,12] we do not use bounds coming from corrections to the asymptotic case. As a result we were able to obtain higher secret key rates with respect to [10–12]. For calculating the quantities involved in our analysis we need the quantum channel to be symmetric. Although we do not have any guarantee that Alice and Bob share such a channel, it is possible for them to reduce to this case employing additional symmetries[2] or taking as QBER of a symmetric channel the worst one of a nonsymmetric channel.

Finally, regarding future work, note that here we considered an ideal protocol where the signals entering in Alice and Bob's laboratory are qubits and where the measurement devices are perfect. All these assumptions could be relaxed following the analysis done in [20,24].

[2]Actually, in this case it also possible to redefine the protocol removing the sifting following the construction presented in [27]. The key rate will be higher, but the relative differences between the three approaches remain the same.

ACKNOWLEDGMENTS

We would like to thank Sylvia Bratzik, Matthias Kleinmann, and in particular Renato Renner for valuable and enlightening discussions. AS thanks also Alberto Carlini for his interest, advice, and support during the early stages of this work. We acknowledge partial financial support by Deutsche Forschungsgemeinschaft (DFG) and by BMBF (project QuOReP).

APPENDIX A: PROPERTIES OF RÉNYI ENTROPIES

The following properties and their proofs can be found in [5] and [34].

Lemma A.1. (Data processing) Let $\varepsilon,\varepsilon' \geqslant 0$ and $\rho_{XBC} \in S(\mathcal{H}^X \otimes \mathcal{H}^B \otimes \mathcal{H}^C)$ be a cq state (i.e., $\rho_{XBC} = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes \rho_B^x \otimes \rho_C^x$). Then with $S_2(\rho_{XC}|X) := \inf_{x\in\mathcal{X}} S_2(\rho_{XC}|x)$, the following inequality holds

$$S_2^{\varepsilon+\varepsilon'}(\rho_{XBC}) \geqslant S_2^{\varepsilon'}(\rho_{XC}) + S_2^{\varepsilon}(\rho_{XB}|X). \tag{A1}$$

Lemma A.2. (Subadditivity) Let $\varepsilon \geqslant 0,\varepsilon' \geqslant 0$ and $\rho_{AB} \in S(\mathcal{H}^A \otimes \mathcal{H}^B)$, then

$$S_0^{\varepsilon+\varepsilon'}(\rho_{AB}) \geqslant S_0^{\varepsilon}(\rho_A) + S_0^{\varepsilon'}(\rho_B). \tag{A2}$$

APPENDIX B: PROOF OF THEOREM IV.1

Before we start with the proof, we define some quantities used in the following.

Definition B.1. (Two-universal hash functions [35]) Let $\mathcal{F}$ be a family of functions from $\mathcal{X}$ to $\mathcal{Z}$ and let P_{F} be a probability distribution on F. The pair $(\mathcal{F},P_{\mathrm{F}})$ is called two-universal if $\mathrm{P}_f[f(x) = f(x')] \leqslant \frac{1}{|\mathcal{Z}|}$ for any distinct $x,x' \in \mathcal{X}$ and f chosen at random from $\mathcal{F}$ according to the distribution P_{F}.

The following definition involves the leakage of information during the EC protocol.

Definition B.2. The number of bits leaked to an eavesdropper during the EC protocol is [6]

$$\mathrm{leak}_{\mathrm{EC}} := \log_2|\mathcal{C}| - \inf_{x^n\in\mathcal{X}} S_\infty(P_{C|X^n=x^n}), \tag{B1}$$

where $|\mathcal{C}|$ is the cardinality of the set $\mathcal{C}$ containing all possible communication transcripts and $P_{C|X^n=x^n}$ is the probability that there is a specific communication transcript when Alice has a specific x^n.

Note that in the definition Bob is missing because we consider a one-way EC protocol.

Moreover, let us recall a result proven in [7] and used in the following proof.

Theorem B.3 [7]. Let $\rho_{X^nE^nC}$ be a cq-state describing Alice's bitstring X^n, Eve's quantum system, and the distribution of EC transcripts C. Let $\mathcal{F}$ be a two-universal family of hash function from $\mathcal{X}^n \to \{0,1\}^\ell$. Then

$$\begin{aligned}&\tfrac{1}{2}\|\rho_{F(X^n)^\ell E^\ell CF} - \rho_U \otimes \rho_{E^\ell CF}\|_1\\ &\quad\leqslant \tfrac{1}{2}2^{-\frac{1}{2}[S_2(\rho_{X^nE^nC})-S_0(\rho_{E^nC})-\ell]},\end{aligned} \tag{B2}$$

where $\rho_{F(X^n)^\ell E^\ell CF} := \sum_{f\in\mathcal{F}} P_{\mathrm{F}}(f)\rho_{f(X^n)^\ell E^\ell C} \otimes |f\rangle\langle f|$ and $\rho_U = \frac{1}{2^\ell}\mathbf{1}$.

Now we are ready to prove Theorem IV.1.

Proof. (Theorem IV.1) At the end of the QKD protocol, the classical string obtained from privacy amplification correlated with Eve's information is

$$\rho_{F(X^n)^\ell E^\ell CF} := \sum_{f\in\mathcal{F}} P_{\mathrm{F}}(f)\rho_{f(X^n)^\ell E^\ell C} \otimes |f\rangle\langle f|.$$

Let $\rho'_{F(X^n)^\ell E^\ell CF} \in \mathcal{B}^{\frac{\overline{\varepsilon}}{2}}(\rho_{F(X^n)^\ell E^\ell CF})$ be the operator that maximizes the right-hand side of Eq. (B2). Because the trace distance does not increase applying the partial trace, it follows that $\rho'_{E^\ell CF} \in \mathcal{B}^{\frac{\overline{\varepsilon}}{2}}(\rho_{E^\ell CF})$. Let us define $\rho_U = \frac{1}{2^\ell}\mathbf{1}$. Then,

$$\begin{aligned}&\frac{1}{2}||\rho_{F(X^n)^\ell E^\ell CF} - \rho_U \otimes \rho_{E^\ell CF}||_1\\ &= \frac{1}{2}\|\rho_{F(X^n)^\ell E^\ell CF} - \rho'_{F(X^n)^\ell E^\ell CF}\\ &\quad + \rho'_{F(X^n)^\ell E^\ell CF} - \rho_U \otimes \rho'_{E^\ell CF}\\ &\quad - \rho_U \otimes \rho_{E^\ell CF} + \rho_U \otimes \rho'_{E^\ell CF}\|_1 \qquad \text{(B3)}\\ &\leqslant 2\frac{\overline{\varepsilon}}{2} + \frac{1}{2}||\rho'_{F(X^n)^\ell E^\ell CF} - \rho_U \otimes \rho'_{E^\ell CF}||_1\\ &\leqslant \overline{\varepsilon} + \frac{1}{2}2^{-\frac{1}{2}(\sup_{\sigma_{X^nE^nC}\in\mathcal{B}^{\frac{\overline{\varepsilon}}{2}}(\rho_{X^nE^nC})}[S_2(\sigma_{X^nE^nC})-S_0(\sigma_{E^nC})]-\ell)}. \qquad \text{(B4)}\end{aligned}$$

In the step from Eq. (B3) to Eq. (B4) we used the triangle inequality and the fact that the maximal possible distance is $\frac{\overline{\varepsilon}}{2}$. The last inequality follows from Eq. (B2) and the definition of $\rho'_{F(X^n)^\ell E^\ell CF}$. Requiring that the distilled key is $(\overline{\varepsilon}+\varepsilon_{PA})$-secure, that is,

$$\overline{\varepsilon} + \frac{1}{2}2^{-\frac{1}{2}(\sup_{\sigma_{X^nE^nC}\in\mathcal{B}^{\frac{\overline{\varepsilon}}{2}}(\rho_{X^nE^nC})}[S_2(\sigma_{X^nE^nC})-S_0(\sigma_{E^nC})]-\ell)} \overset{!}{\leqslant} \overline{\varepsilon} + \varepsilon_{PA},$$

the proof of Eq. (12) is completed.

Regarding the leakage term, note that to apply Lemma A.1 of Appendix A for bounding $S_2(\sigma_{X^nE^nC})$ we restrict the optimization space to $\mathcal{B}^{\frac{\overline{\varepsilon}}{2}}_{\mathrm{cq}}(\rho_{X^nE^nC})$. Therefore,

$$\begin{aligned}&\sup_{\sigma_{X^nE^nC}\in\mathcal{B}^{\frac{\overline{\varepsilon}}{2}}(\rho_{X^nE^nC})} [S_2(\sigma_{X^nE^nC}) - S_0(\sigma_{E^nC})]\\ &\geqslant \sup_{\sigma_{X^nE^nC}\in\mathcal{B}^{\frac{\overline{\varepsilon}}{2}}_{\mathrm{cq}}(\rho_{X^nE^nC})} [S_2(\sigma_{X^nE^nC}) - S_0(\sigma_{E^nC})].\end{aligned}$$

Using Lemma A.1 of Appendix A with $\varepsilon = \varepsilon' = 0$, it follows that

$$S_2(\sigma_{X^nE^nC}) \geqslant S_2(\sigma_{X^nE^n}) + S_2(\sigma_{X^nC}|X^n). \tag{B5}$$

By definition

$$\begin{aligned}S_2(\sigma_{X^nC}|X^n) &:= \inf_{x^n\in\mathcal{X}} S_2(P_{C|X^n=x^n}) &\text{(B6)}\\ &\geqslant \inf_{x^n\in\mathcal{X}} S_\infty(P_{C|X^n=x^n}). &\text{(B7)}\end{aligned}$$

Moreover, using Lemma A.2 with $\varepsilon = \varepsilon' = 0$ we obtain

$$S_0(\sigma_{E^nC}) \geqslant S_0(\sigma_{E^n}) + S_0(\sigma_C). \tag{B8}$$

Putting together the last four equations and Definition B.2 the proof is concluded.

APPENDIX C: THE OPERATOR ρ_{XE}

The Bell-diagonal state shared by Alice and Bob after the use of the depolarizing map is

$$\rho_{AB} = \lambda_1|\psi^+\rangle\langle\psi^+| + \lambda_2|\psi^-\rangle\langle\psi^-| + \lambda_3|\phi^+\rangle\langle\phi^+| + \lambda_4|\phi^-\rangle\langle\phi^-|,$$

where the states $\{|\psi^\pm\rangle,|\phi^\pm\rangle\}$ are the Bell states and $\sum_i \lambda_i = 1$.

For the symmetric six-state protocol

$$\lambda_0 = \frac{1}{2}(2-3e), \quad \lambda_1 = \lambda_2 = \lambda_3 = \frac{e}{2}, \tag{C1}$$

where e is the QBER.

The operator ρ_{ABE} is defined as the purification of ρ_{AB}. Tracing out Bob and measuring Alice's system, we get the operator $\rho_{XE}^{\otimes n}$ describing the classical string X^n held by Alice and Bob and Eve's quantum systems $\rho_E^{\otimes n}$. In general

$$\rho_{XE}^{\otimes n} := \left(\rho_E^0 \oplus \rho_E^1\right)^{\otimes n}, \tag{C2}$$

with

$$\rho_E^0 := \begin{pmatrix} \lambda_0 & \sqrt{\lambda_0\lambda_1} & 0 & 0 \\ \sqrt{\lambda_0\lambda_1} & \lambda_1 & 0 & 0 \\ 0 & 0 & \lambda_2 & \sqrt{\lambda_2\lambda_3} \\ 0 & 0 & \sqrt{\lambda_2\lambda_3} & \lambda_3 \end{pmatrix}, \tag{C3}$$

$$\rho_E^1 := \begin{pmatrix} \lambda_0 & -\sqrt{\lambda_0\lambda_1} & 0 & 0 \\ -\sqrt{\lambda_0\lambda_1} & \lambda_1 & 0 & 0 \\ 0 & 0 & \lambda_2 & -\sqrt{\lambda_2\lambda_3} \\ 0 & 0 & -\sqrt{\lambda_2\lambda_3} & \lambda_3 \end{pmatrix}. \tag{C4}$$

Diagonalizing the operators above, we find that they have the same eigenvalues but different eigenvectors, that is,

$$\rho_E^x := \sum_{i=0}^{3} \Gamma_i^{(1)} P_i^x, \tag{C5}$$

where the eigenvalues $\{\Gamma_i^{(1)}\}$ are

$$\Gamma_0^{(1)} = \Gamma_2^{(1)} = 0, \tag{C6a}$$

$$\Gamma_1^{(1)} = \lambda_0 + \lambda_1, \tag{C6b}$$

$$\Gamma_3^{(1)} = \lambda_2 + \lambda_3, \tag{C6c}$$

and the operators $\{P_i^x\}$ are projectors on the eigenspace of the eigenvalues $\{\Gamma_i^{(1)}\}$ obtained by diagonalizing ρ_E^x. From the diagonalization it is possible to derive explicitly the projectors[3]

$$P_0^0 = \begin{pmatrix} \frac{\lambda_1}{\lambda_0+\lambda_1} & -\frac{\sqrt{\lambda_0\lambda_1}}{\lambda_0+\lambda_1} \\ -\frac{\sqrt{\lambda_0\lambda_1}}{\lambda_0+\lambda_1} & \frac{\lambda_0}{\lambda_0+\lambda_1} \end{pmatrix} \oplus \mathbb{O}_2,$$

$$P_1^0 = \begin{pmatrix} \frac{\lambda_0}{\lambda_0+\lambda_1} & \frac{\sqrt{\lambda_0\lambda_1}}{\lambda_0+\lambda_1} \\ \frac{\sqrt{\lambda_0\lambda_1}}{\lambda_0+\lambda_1} & \frac{\lambda_1}{\lambda_0+\lambda_1} \end{pmatrix} \oplus \mathbb{O}_2,$$

$$P_2^0 = \mathbb{O}_2 \oplus \begin{pmatrix} \frac{\lambda_3}{\lambda_2+\lambda_3} & -\frac{\sqrt{\lambda_2\lambda_3}}{\lambda_2+\lambda_3} \\ -\frac{\sqrt{\lambda_2\lambda_3}}{\lambda_2+\lambda_3} & \frac{\lambda_2}{\lambda_2+\lambda_3} \end{pmatrix},$$

$$P_3^0 = \mathbb{O}_2 \oplus \begin{pmatrix} \frac{\lambda_2}{\lambda_2+\lambda_3} & \frac{\sqrt{\lambda_2\lambda_3}}{\lambda_2+\lambda_3} \\ \frac{\sqrt{\lambda_2\lambda_3}}{\lambda_2+\lambda_3} & \frac{\lambda_3}{\lambda_2+\lambda_3} \end{pmatrix},$$

$$P_0^1 = \begin{pmatrix} \frac{\lambda_1}{\lambda_0+\lambda_1} & \frac{\sqrt{\lambda_0\lambda_1}}{\lambda_0+\lambda_1} \\ \frac{\sqrt{\lambda_0\lambda_1}}{\lambda_0+\lambda_1} & \frac{\lambda_0}{\lambda_0+\lambda_1} \end{pmatrix} \oplus \mathbb{O}_2,$$

$$P_1^1 = \begin{pmatrix} \frac{\lambda_0}{\lambda_0+\lambda_1} & -\frac{\sqrt{\lambda_0\lambda_1}}{\lambda_0+\lambda_1} \\ -\frac{\sqrt{\lambda_0\lambda_1}}{\lambda_0+\lambda_1} & \frac{\lambda_1}{\lambda_0+\lambda_1} \end{pmatrix} \oplus \mathbb{O}_2,$$

$$P_2^1 = \mathbb{O}_2 \oplus \begin{pmatrix} \frac{\lambda_3}{\lambda_2+\lambda_3} & \frac{\sqrt{\lambda_2\lambda_3}}{\lambda_2+\lambda_3} \\ \frac{\sqrt{\lambda_2\lambda_3}}{\lambda_2+\lambda_3} & \frac{\lambda_2}{\lambda_2+\lambda_3} \end{pmatrix},$$

$$P_3^1 = \mathbb{O}_2 \oplus \begin{pmatrix} \frac{\lambda_2}{\lambda_2+\lambda_3} & -\frac{\sqrt{\lambda_2\lambda_3}}{\lambda_2+\lambda_3} \\ -\frac{\sqrt{\lambda_2\lambda_3}}{\lambda_2+\lambda_3} & \frac{\lambda_3}{\lambda_2+\lambda_3} \end{pmatrix}. \tag{C7}$$

For the following, it is convenient to define

$$P_i := \frac{1}{2}\sum_{x=0}^{1} P_i^x, \tag{C8}$$

with $i = 0,1,2,3$. As can be easily verified the operators $\{P_i\}$ are diagonal in the basis where the operators $\{P_i^x\}$ assume the form given above.

APPENDIX D: ADDITIONAL DETAILS OF THE PROOF OF THEOREM IV.4

Before starting, it is necessary to fix the notation for the involved operators. The operator $\rho_{XE}^{\otimes n}$ can be written as

$$\rho_{XE}^{\otimes n} = \frac{1}{2^n}\sum_{x=0}^{2^n-1} |x\rangle\langle x| \otimes \sum_{i=0}^{2^{2n}-1} \Gamma_i^{(n)} P_i^{(n)x}, \tag{D1}$$

where

$$P_i^{(n)x} := \bigotimes_{p=0}^{n-1} P_{i_p}^{x_p}, \tag{D2}$$

$$\Gamma_i^{(n)} := \prod_{p=0}^{n-1} \Gamma_{i_p}^{(1)}, \tag{D3}$$

and $i := \sum_{p=0}^{n-1} 4^p i_p$ with $i_p = 0,\ldots,3$, $x := \sum_{p=0}^{n-1} 2^p x_p$ where x_p is a binary digit.

The operator $\rho_{XE}^{\otimes n}$ is constituted of 2^n diagonal blocks labeled by the index x. Each of the blocks has 2^{2n} eigenvalues $\Gamma_i^{(n)}$ and each eigenvalue is associated to a projector $P_i^{(n)x}$ that depends on the eigenvalue (index "i") and on the block (index "x").

1. Construction of the operator $\eta_{X^nE^n}$

The operator $\eta_{X^nE^n}$ is constructed in such a way that the inequalities in Eqs. (20) and (21) are satisfied. For constructing $\eta_{X^nE^n}$ we construct first η_{E^n} using the following two steps:

(1) Find $\tau_{X^nE^n}$ such that $S_2(\tau_{X^nE^n}) = \overline{S}_2^{\bar{\varepsilon}-\hat{\varepsilon}}(\rho_{XE}^{\otimes n})$;

[3]Let us define $\mathbb{O}_2$ as the 2×2 matrix with zero entries.

(2) Find $\eta_{X^nE^n}$ such that $S_0(\eta_{E^n}) = S_0^{\hat{\varepsilon}}(\tau_{E^n})$.

By definition of smooth Rényi entropy of order two $\tau_{X^nE^n} \in \mathcal{B}_{\mathrm{cq}}^{\frac{\bar{\varepsilon}-\hat{\varepsilon}}{2}}(\rho_{XE}^{\otimes n})$ and it can be written as

$$\tau_{X^nE^n} := \frac{1}{2^n}\sum_{x=0}^{2^n-1} |x\rangle\langle x| \otimes \sum_{i=0}^{2^{2n}-1} \tau_i^{(n)} P_i^{(n)x}. \tag{D4}$$

Regarding the operator η_{E^n}, the constraint on its Rényi entropy of order zero is only a constraint on its eigenvalues. For assigning a well-defined structure of operator to $\eta_{X^nE^n}$ we use $\tau_{X^nE^n}$. Let Π be the projector that cuts out the eigenvalues of τ_{E^n} such that their sum is $\hat{\varepsilon}/2$.

The operator $\eta_{X^nE^n}$, is defined by

$$\eta_{X^nE^n} := \frac{1}{1-\frac{\hat{\varepsilon}}{2}}(\mathbf{1}_{X^n}\otimes\Pi)\tau_{X^nE^n}(\mathbf{1}_{X^n}\otimes\Pi). \tag{D5}$$

This definition is such that $\eta_{E^n} = \frac{1}{1-\frac{\hat{\varepsilon}}{2}}\Pi\tau_{E^n}\Pi$ has the eigenvalues for respecting $S_0(\eta_{E^n}) = S_0^{\hat{\varepsilon}}(\tau_{E^n})$.

Finally, note, that the construction above, although arbitrary, is legitimate because, as it is easy to verify, $\eta_{X^nE^n} \in \mathcal{B}_{\mathrm{cq}}^{\frac{\bar{\varepsilon}}{2}}(\rho_{XE}^{\otimes n})$ as required by the statement of Theorem IV.4.

2. Proof of $S_0(\eta_{E^n}) \leqslant S_0^{\hat{\varepsilon}}(\rho_E^{\otimes n} + \bar{\delta}_{E^n})$

To find the claimed bound, we need to find a bound on the eigenvalues of the operator τ_{E^n}. To do that, we exploit the definition of $\tau_{X^nE^n}$, $\rho_{XE}^{\otimes n}$ and of modified smooth Rényi entropy of order two (Defintion IV.2).

We introduce the operator $\delta_{X^nE^n}$ defined by

$$\delta_{X^nE^n} := \tau_{X^nE^n} - \rho_{XE}^{\otimes n}. \tag{D6}$$

Let $\delta_{E^n} := \mathrm{tr}_{E^n}(\delta_{X^nE^n})$, $\tau_{E^n} := \mathrm{tr}_{E^n}(\tau_{X^nE^n})$ and let $\{|l\rangle\}$ be a basis of eigenvectors of the operator τ_{E^n}. The eigenvalues of τ_{E^n} are

$$\langle l|\,\tau_{E^n}\,|l\rangle := \langle l|\,\rho_E^{\otimes n}\,|l\rangle + \langle l|\,\delta_{E^n}\,|l\rangle\,. \tag{D7}$$

The operator $\rho_E^{\otimes n}$ is fully characterized by the protocol [10]. To complete the proof, it remains to bound $\langle l|\,\delta_{E^n}\,|l\rangle$.

The following lemma permits to reduce the analysis to the eigenvalues of δ_{E^n}.

Lemma D.1. Let $\rho_{XE}^{\otimes n}, \tau_{X^nE^n}$ be the operators described by Eqs. (D1) and (D4). Then

$$\left[\tau_{E^n}, \rho_E^{\otimes n}\right] = 0.$$

Proof. By definition

$$\begin{aligned}\tau_{E^n} &= \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{i=0}^{2^{2n}-1}\tau_i^{(n)}P_i^{(n)x}\\ &= \sum_{i=0}^{2^{2n}-1}\tau_i^{(n)}\left(\frac{1}{2^n}\sum_{x=0}^{2^n-1}P_i^{(n)x}\right).\end{aligned}$$

Observe that the operator in the brackets is diagonal, in fact

$$\begin{aligned}\frac{1}{2^n}\sum_{x=0}^{2^n-1}P_i^{(n)x} &= \frac{1}{2^n}\sum_{x=0}^{2^n-1}\bigotimes_{p=0}^{n-1}P_{i_p}^{x_p}\\ &= \frac{1}{2^n}\sum_{x_0=0}^{1}\sum_{x_1=0}^{1}\cdots\sum_{x_{n-1}=0}^{1}\bigotimes_{p=0}^{n-1}P_{i_p}^{x_p}\\ &= \bigotimes_{p=0}^{n-1}\left(\frac{1}{2}\sum_{x=0}^{1}P_{i_p}^{x}\right)\\ &= \bigotimes_{p=0}^{n-1}P_{i_p}.\end{aligned}$$

Due to the diagonality of the operators $\{P_{i_p}\}_{i_p=0,\ldots,3}$ and the fact that the tensor product of diagonal operators lead to a diagonal operator, the assertion is proved.

The next lemma, permits to relate the operator δ_E to the operators P_i defined in Eq. (C8).

Lemma D.2. It holds

$$\delta_{E^n} = \frac{\bar{\varepsilon}-\hat{\varepsilon}}{2m_0}[\mathbf{1} - (P_1+P_3)^{\otimes n}] + \sum_{i\in\mathcal{V}}\delta_i P_i^{(n)},$$

where the operators P_i are defined in Eq. (C8), $P_i^{(n)} = \bigotimes_{p=0}^{n-1}P_{i_p}$ and $\mathcal{V} := \{i : \Gamma_i^{(n)} \neq 0\}$.

Proof. Using the eigenvalues in Eqs. (17) and (D6), Eq. (D4)

$$\begin{aligned}\delta_{E^n} &:= \mathrm{tr}_{X^n}(\delta_{X^nE^n})\\ &= \frac{\bar{\varepsilon}-\hat{\varepsilon}}{2m_0}\frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{i\in\mathcal{V}^\perp}P_i^{(n)x} + \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{i\in\mathcal{V}}\delta_i P_i^{(n)x}.\end{aligned}$$

The quantity $\sum_{i\in\mathcal{V}^\perp}P_i^{(n)x}$ is such that

$$\sum_{i\in\mathcal{V}^\perp}P_i^{(n)x} = \mathbf{1} - \sum_{i\in\mathcal{V}}P_i^{(n)x}.$$

From Eqs. (D3) and (C6), we see that the nonzero eigenvalues of $\rho_{XE}^{\otimes n}$ are characterized by the absence of the index $i_p = 0,2$. Therefore, it follows that

$$\begin{aligned}\sum_{i\in\mathcal{V}}P_i^{(n)x} &\overset{(D2)}{=} \sum_{i\in\mathcal{V}}\bigotimes_{p=0}^{n-1}P_{i_p}^{x_p}\\ &= \bigotimes_{p=0}^{n-1}\left(P_1^{x_p}+P_3^{x_p}\right).\end{aligned}$$

By taking the sum over all blocks and using the operator defined in Eq. (C8) the statement of the lemma follows.

Using the previous lemma we can prove the most important result of this section.

Proposition. For $\lambda_0 > \frac{1}{2}$ and $\lambda_1 = \lambda_2 = \lambda_3$ the following inequality holds:

$$\langle l|\,\delta_{E^n}\,|l\rangle \leqslant \frac{\bar{\varepsilon}-\hat{\varepsilon}}{2m_0}\left[1-\left(\frac{\lambda_1}{\lambda_1+\lambda_0}\right)^n\right], \tag{D8}$$

where $\{|l\rangle\}$ is a basis of eigenvectors for the operator $\rho_E^{\otimes n}$.

Proof.

$$\begin{aligned}\langle l|\,\delta_{E^n}\,|l\rangle &\leqslant \frac{\overline{\varepsilon}-\hat{\varepsilon}}{2m_0}\max_{\{|l\rangle\}}\langle l|\left[\mathbf{1}-(P_1+P_3)^{\otimes n}\right]|l\rangle \\ &\quad+\sum_{i\in\mathcal{V}}\delta_i\,\langle l|\,P_i^{(n)}\,|l\rangle \\ &= \frac{\overline{\varepsilon}-\hat{\varepsilon}}{2m_0}\left[1-\left(\frac{\lambda_1}{\lambda_1+\lambda_0}\right)^n\right]+\sum_{i\in\mathcal{V}}\delta_i\,\langle l|\,P_i^{(n)}\,|l\rangle\,,\end{aligned} \tag{D9}$$

where $\mathcal{V}:=\{i:\Gamma_i^{(n)}\neq 0\}$. Since the δ_i are negative or zero and the operators $P_i^{(n)}$ are such that $P_i^{(n)}\geqslant 0$, the last term in Eq. (D9) is negative and then the proposition follows.

Concluding, using Proposition D.3, it is possible to give an upper bound for $S_0^{\varepsilon}(\tau_{E^n})$, in fact

$$\begin{aligned}\langle l|\,\tau_{E^n}\,|l\rangle &= \langle l|\,\rho_E^{\otimes n}\,|l\rangle+\langle l|\,\delta_{E^n}\,|l\rangle \\ &\leqslant \langle l|\,\rho_E^{\otimes n}\,|l\rangle+\frac{\overline{\varepsilon}-\hat{\varepsilon}}{2m_0}\left[1-\left(\frac{\lambda_1}{\lambda_1+\lambda_0}\right)^n\right].\end{aligned} \tag{D10}$$

Substituting in the formula above the actual values for the symmetric six-state protocol provided in Eq. (C1) the proof is concluded.

3. Proof of $S_2(\eta_{X^nE^n})\geqslant \overline{S}_2^{\overline{\varepsilon}-\hat{\varepsilon}}(\rho_{XE}^{\otimes n})-\hat{\varepsilon}$

Using Eq. (D5), it follows that

$$\begin{aligned}S_2(\eta_{X^nE^n}) &= -\log_2\{\mathrm{tr}_{X^nE^n}\left[(\mathbf{1}\otimes\Pi)\tau_{X^nE^n}(\mathbf{1}\otimes\Pi)\right]^2\} \\ &\quad+2\log_2\left(1-\frac{\hat{\varepsilon}}{2}\right).\end{aligned}$$

Using the first requirement in Definition IV.2, the operator $\tau_{X^nE^n}$ is of the form

$$\tau_{X^nE^n}=\frac{1}{2^n}\bigoplus_{x=0}^{2^n-1}\tau_{E^n}^x.$$

We concentrate on the argument of the logarithm in the first term on the right-hand side of $S_2(\tau_{X^nE^n})$

$$\begin{aligned}&\mathrm{tr}_{X^nE^n}\{[(\mathbf{1}\otimes\Pi)\tau_{X^nE^n}(\mathbf{1}\otimes\Pi)]^2\} \\ &\quad=\mathrm{tr}_{X^nE^n}\left[\bigoplus_{x=0}^{2^n-1}\left(\frac{1}{2^n}\Pi\tau_{E^n}^x\Pi\right)^2\right] \\ &\quad=\mathrm{tr}_{E^n}\left[\sum_{x=0}^{2^n-1}\left(\frac{1}{2^n}\Pi\tau_{E^n}^x\Pi\right)^2\right] \\ &\quad=\sum_{x=0}^{2^n-1}\mathrm{tr}_{E^n}\left[\left(\frac{1}{2^n}\Pi\tau_{E^n}^x\Pi\right)^2\right] \\ &\quad\leqslant\sum_{x=0}^{2^n-1}\mathrm{tr}_{E^n}\left[\left(\frac{1}{2^n}\tau_{E^n}^x\right)^2\right] \\ &\quad=\mathrm{tr}_{X^nE^n}\left[(\tau_{X^nE^n})^2\right].\end{aligned}$$

Taking the first term of the Maclaurin expansion of $\log_2(1-\frac{\hat{\varepsilon}}{2})$ for $\hat{\varepsilon}$ small, we conclude that

$$S_2(\eta_{X^nE^n})\geqslant S_2(\tau_{X^nE^n})-\hat{\varepsilon}.$$

Using Eq. (13) the proof is concluded.

[1] C. Bennett *et al.*, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India, 1984), Vol. 175.

[2] A. Shields and Z. Yuan, Phys. World **20**, 24 (2007).

[3] [http://www.uqcc2010.org/].

[4] [http://quantum.ukzn.ac.za/quantum-city].

[5] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).

[6] R. Renner, Ph.D. thesis, Swiss Federal Institute of Technology, Zürich, 2005.

[7] R. Renner and R. König, in *Theory of Cryptography*, Lecture Notes in Computer Science, Vol. **3378**, edited by J. Kilian, (Springer, Berlin, 2005), pp. 407–425.

[8] M. Christandl, R. Renner, and A. Ekert, e-print arXiv:quant-ph/0402131.

[9] V. Scarani and R. Renner, in *Theory of Quantum Computation, Communication, and Cryptography*, Lecture Notes in Computer Science, Vol. 5106, edited by Y. Kawano and M. Mosca, (Springer, Berlin, 2008), pp. 83–95.

[10] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).

[11] D. Mayers, J. ACM **48**, 351 (2001).

[12] T. Meyer, H. Kampermann, M. Kleinmann, and D. Bruß, Phys. Rev. A **74**, 042340 (2006).

[13] R. König, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[14] S. Bratzik, M. Mertz, H. Kampermann, and D. Bruß, Phys. Rev. A **83**, 022330 (2011).

[15] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).

[16] R. Renner, in *NATO Advanced Research Workshop Quantum Cryptography and Computing: Theory and Implementation*, NATO Advanced Research Workshop Quantum Cryptography and Computing: Theory and Implementation, Vol. 26 (IOS Press, Amsterdam, 2010), pp. 66–75.

[17] L. Sheridan, T. P. Le, and V. Scarani, New J. Phys. **12**, 123019 (2010).

[18] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

[19] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, e-print arXiv:1103.4130.

[20] R. Y. Q. Cai and V. Scarani, New Journal of Physics **11**, 045024 (2009).

[21] H.-W. Li, Y.-B. Zhao, Z.-Q. Yin, S. Wang, Z.-F. Han, W.-S. Bao, and G.-C. Guo, Opt. Commun. **282**, 4162 (2009).

[22] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).

[23] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).

[24] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[25] H.-K. Lo, H. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005).
[26] H. K. Lo, Quantum Inf. Comput. **1**, 81 (2001).
[27] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[28] A. Rényi, in *Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability*, (University of California Press, Berkeley, CA, 1961), Vol. 1, pp. 547–561.
[29] J. Müller-Quade and R. Renner, New J. Phys. **11**, 085006 (2009).
[30] M. Tomamichel, R. Renner, C. Schaffner, and A. Smith, in *IEEE International Symposium on Information Theory*, IEEE International Symposium on Information Theory (IEEE, New York, 2010), pp. 2703–2707.
[31] B. Haible and R. B. Kreckel, [http://www.ginac.de/CLN/].
[32] T. D. Plantenga, HOPSPACK*2.0 User Manual*, Tech. Rep. No. SAND2009-6265 (Sandia National Laboratories, Albuquerque, NM and Livermore, CA, 2009).
[33] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. on Inf. Theory **55**, 5840 (2009).
[34] R. Renner and S. Wolf, in *IEEE International Symposium on Information Theory—ISIT 2004* (IEEE, New York, 2004), p. 233.
[35] J. L. Carter and M. N. Wegman, J. Comput. Syst. Sci. **18**, 143 (1979).

Quantum key distribution with finite resources: Secret key rates via Rényi entropies
Physical Review A, Vol. **84**, p. 032321 (2011) [10 pages]
S. Abruzzo, H. Kampermann, M. Mertz, and D. Bruß

Impact Factor: 2.861
Third author
Contribution to work by scientific work and editing the manuscript (30%)

Ich versichere an Eides statt, dass die Dissertation von mir selbständig und ohne unzulässige fremde Hilfe unter Beachtung der ,,Grundsätze zur Sicherung guter wissenschaftlicher Praxis an der Heinrich-Heine-Universität Düsseldorf" erstellt worden ist.

Düsseldorf, den 26. September 2012

(Markus Mertz)

Hiermit erkläre ich, dass ich die Dissertation keiner anderen Fakultät bereits vorgelegt habe und keinerlei vorherige erfolglose Promotionsversuche vorliegen.

Düsseldorf, den 26. September 2012

(Markus Mertz)