Lecture notes:
Security proofs of Quantum Key Distribution

Gláucia Murta

Last update: November 2023

Contents

1 Quantum key distribution

Quantum key distribution is a cryptographic task in which two honest parties, Alice and Bob, wish to establish a common secret key, i.e., a shared string of bits which is unknown to any third party, including a potential eavesdropper Eve.

As resources, Alice and Bob have access to a classical authenticated public channel and an insecure quantum channel.

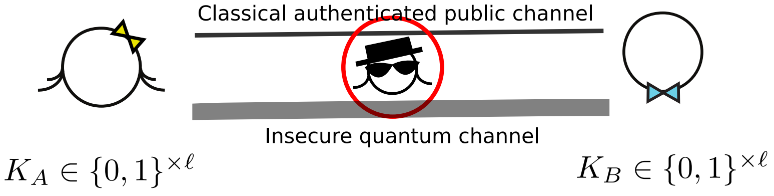
Classical authenticated public channel
Insecure quantum channel
$K_A \in \{0,1\}^{\times \ell}$
$K_B \in \{0,1\}^{\times \ell}$

Figure 1: Quantum key distribution: Alice and Bob establish a secret key using a classical authenticated public channel and an insecure quantum channel.

1.1 The BB84 protocol

The first quantum key distribution protocol, the BB84 [1], was proposed by Bennet and Brassard, building on the ideas of conjugate coding introduced by Wiesman in [2]. Indeed, the BB84 protocol makes use of two non-orthogonal bases to encode a classical bit:

$$\begin{aligned} 0 &\mapsto |0\rangle \text{ or } |+\rangle \\ 1 &\mapsto |1\rangle \text{ or } |-\rangle \end{aligned} \tag{1}$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

The BB84 protocol consists of the following steps:

BB84 Protocol

```
Distribution and measurements:
for $i = 1$ to $n$ do
    Alice chooses random bits $x$ and $a$.
    If $x = 0$, Alice uses the $Z$-basis to encode $a$ (if $a = 0$ she prepares the state $|0\rangle$, and if $a = 1$ she prepares $|1\rangle$). Similarly, if $x = 1$, Alice uses the $X$-basis to encode $a$.
    Alice sends the prepared state to Bob through the insecure quantum channel.
    Bob announces whether he received the state.
    Bob randomly chooses a bit $y$.
    If $y = 0$, Bob measures the system in the $Z$-basis. If $y = 1$, he measures in the $X$-basis.
    Bob records the outcome $b$.
end for
Sifting: Alice and Bob publicly announce their choices of basis, $x$ and $y$, and compare them. They discard the rounds in which Bob measured in a different basis than the one prepared by Alice, i.e., when $x \neq y$.
Parameter estimation: Alice and Bob use a fraction of the remaining rounds (in which both measured in the same basis) in order to estimate the quantum bit error rates (QBERs) $Q_X$ and $Q_Z$.
Information reconciliation: Alice and Bob choose a classical error correcting code and communicate over the authenticated public channel in order to correct their string of bits. At the end of this phase Alice and Bob should hold the same bit-string.
Privacy amplification: Alice and Bob use an extractor on the previously established strings to generate shorter but completely secret strings of $\ell$ bits, which is their final keys $K_A$ and $K_B$.
```

Remark 1: The “quantum part” ends after distribution and measurement. The remaining steps of a QKD protocol consist of processing classical information.

Remark 2: As shown in [3], the efficiency of these protocols can be increased, without compromising security, if one of the bases is chosen with a higher probability. Then, in the asymptotic limit, the preferred basis is used almost all the time. We can use the less frequent basis for parameter estimation and reserve the rounds measured in the frequent basis for key generation. For this reason, it is common to denote the basis respectively, test basis and key generation basis.

1.2 Entanglement-based version

The protocol described in the previous section only requires the preparation and measurement of *single qubit states*, and for this reason it is called a prepare-and-measure protocol. An equivalent entanglement-based protocol can be designed [4], which is based on the distribution of entangled states in the quantum phase:

Entanglement-based BB84 Protocol

```
Distribution and measurements:
for $i = 1$ to $n$ do
    A source distributes a two-qubit system (ideally in the maximally entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$) to Alice and Bob.
    Alice chooses a random bit $x$.
    If $x = 0$ Alice measures her part of the system in the $Z$-basis, and if $x = 1$ she measures in the $X$-basis.
    Alice records the outcome $a$.
    Similarly, Bob chooses a random bit $y$.
    If $y = 0$ Bob measures his system in the $Z$-basis, and if $y = 1$ he measures in the $X$-basis.
    Bob records the outcome $b$.
end for
```

All the other steps of the protocol are the same as the previous protocol.

Remark 1: If the source is in Alice's laboratory we have a completely analogous situation: measuring her part of the system corresponds to preparing Bob's part of the system in one of the BB84 states.

Remark 2: The entanglement-based protocol offers stronger security. The source does not have to be in Alice's laboratory and could be even in control of a malicious eavesdropper Eve.

The entanglement-based version of a QKD protocol is very useful for its security proof. In fact, the first simple proof of the BB84, presented [5], was based on entanglement purification results. In this course we will also focus on the entanglement based version to derive the security proofs. However, we will use the more general approach developed in references [6, 7] which does not rely directly on entanglement purification.

1.3 Eavesdropper's attack

We can consider three different types of attack that an eavesdropper can perform:

- **Individual attacks:** the eavesdropper can only interact (perhaps intercept and measure) with each round of the protocol individually. This is the case when the eavesdropper has no quantum memory.

- **Collective attacks:** in this case it is assumed that the system distributed to Alice and Bob is the same in every round of the protocol (i.e., the state distributed in n rounds can be described as $\rho_{AB}^{\otimes n}$, they are i.i.d.), however the eavesdropper is allowed to store and make arbitrary global operations on her quantum side information;

- **Coherent attacks:** this is the most general type of attack. Eve can perform a global operation on her quantum side information and moreover the states distributed to Alice and Bob can have arbitrary correlations ($\rho_{A_1^n B_1^n} \neq \rho_{AB}^{\otimes n}$).

1.4 Assumptions

We note several assumptions that are present in the description of the BB84 protocol.

- **Isolated labs:** no information is leaked from or enters Alice's and Bob's labs, apart from the state distribution before the measurements and the public classical information described by the protocol.

- **Local random number generators:** Alice and Bob possess independent and trusted random number generators.

- **Trusted classical post-processing:** all the public classical communication is performed using an authenticated channel and the local classical computations are trusted.

- **Trusted measurements:** the measurement devices of Alice and Bob implement the measurements specified by the protocol.

- **Trusted source for prepare-and-measure:** Alice's device prepares the state specified by the protocol. The trust in the source can be relaxed for an entanglement based implementation.

- **Quantum mechanics:** the systems of Alice, Bob and any additional party is correctly described by quantum theory.

2 Tools for the security analysis

In the following we denote the set of quantum states of a system A with Hilbert space $\mathcal{H}_A$ by $\mathcal{S}(A)$:

$$\mathcal{S}(A) = \{\rho_A \in \mathcal{L}(\mathcal{H}_A) : \rho_A \geq 0 \text{ and } \mathrm{tr}(\rho_A) = 1\}, \tag{2}$$

where $\mathcal{L}(\mathcal{H}_A)$ is the set of linear operators acting on $\mathcal{H}_A$.

2.1 Distance between quantum states

Definition 2.1 (Trace distance)**.** *Let ρ and σ be two quantum states,*

$$\|\rho-\sigma\|_{\mathrm{tr}} := \sup_{\substack{P\\ 0\le P\le I}} \mathrm{tr}(P(\rho-\sigma)). \tag{3}$$

Alternatively

$$\|\rho-\sigma\|_{\mathrm{tr}} = \frac{1}{2}\|\rho-\sigma\|_1, \tag{4}$$

where $\|X\|_1 = \mathrm{tr}(|X|) = \mathrm{tr}(\sqrt{X^\dagger X})$.

The trace distance has an operational interpretation: if $\|\rho-\sigma\|_{\mathrm{tr}} = \epsilon$, then the probability of distinguishing between ρ and σ with a single measurement is bounded by $\frac{1}{2}(1+\epsilon)$.

The trace distance can be generalized to sub-normalized states $\hat{\rho}$ and $\hat{\sigma}$, i.e., for positive operators with trace smaller or equal to 1, in the following way

$$\|\hat{\rho}-\hat{\sigma}\|_{\mathrm{tr}} = \frac{1}{2}\|\hat{\rho}-\hat{\sigma}\|_1 + \frac{1}{2}|\mathrm{tr}(\hat{\rho}-\hat{\sigma})| \tag{5}$$

For details, see [8, Chapter 3].

Another distance of interest is the purified distance, also defined for sub-normalized states.

Definition 2.2 (Purified distance)**.** *Let ρ and σ be two sub-normalized states, the purified distance is defined as*

$$D_P(\rho,\sigma) := \sqrt{1-F(\rho,\sigma)}, \tag{6}$$

where F is the generalized fidelity

$$F(\rho,\sigma) := \left(\mathrm{tr}\left(\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right) + \sqrt{(1-\mathrm{tr}\rho)(1-\mathrm{tr}\sigma)}\right)^2. \tag{7}$$

The name comes from the fact that the purified distance actually represents the minimum trace-distance of purifications of the respective states:

$$D_P(\rho,\sigma) = \min_{\phi,\varphi}\|\phi-\varphi\|_{\mathrm{tr}}, \tag{8}$$

where ϕ and φ are purifications of ρ and σ, respectively.

The purified distance is related to trace distance by [8]:

$$\|\rho-\sigma\|_{\mathrm{tr}} \le D_P(\rho,\sigma) \le \sqrt{2\|\rho-\sigma\|_{\mathrm{tr}}}. \tag{9}$$

Proposition 2.3 (Properties of distances)**.** *The trace distance and the purified distance are metrics. I.e., they satisfy:*

- *Positive-definiteness:* $\Delta(\rho,\sigma) \geq 0$ *and* $\Delta(\rho,\sigma) = 0 \Leftrightarrow \rho = \sigma$*,*
- *Symmetry:* $\Delta(\rho,\sigma) = \Delta(\sigma,\rho)$*,*
- *Triangle inequality:* $\Delta(\rho,\sigma) \leq \Delta(\rho,\eta) + \Delta(\eta,\sigma)$*.*

Moreover, they are non-increasing under trace-non-increasing completely positive maps

$$\Delta(\mathcal{M}(\rho),\mathcal{M}(\sigma)) \leq \Delta(\rho,\sigma). \tag{10}$$

Where $\Delta(\rho,\sigma)$ *stands for* $\|\rho-\sigma\|_{\mathrm{tr}}$ *or* $D_P(\rho,\sigma)$*.*

2.2 cq-states

When analysing the security of a QKD protocol we will be often interested in making statements about a classical-quantum state, or cq-state for short. These are states of the form

$$\rho_{AE} = \sum_x p(x)\, |x\rangle\langle x|_A \otimes \rho_{E|x} \tag{11}$$

where $\{|x\rangle\}$ forms an orthonormal basis for system A and can represent a classical random variable X that assumes value x with probability $p(x)$, and $\rho_{E|x}$ is a general quantum state on system E that may depend on the specific value of x.

2.3 Entropies

2.3.1 Shannon entropy

The Shannon entropy quantifies the uncertainty about a random variable. If X is a random variable that assume the value x with probability $p(x)$ then the entropy of the variable X is given by

$$H(X) = -\sum_x p(x) \log p(x). \tag{12}$$

In this text, all the logarithms are in base 2.

The conditional entropy quantifies the remaining uncertainty about a variable X given that the value of a variable Y is known

$$H(X|Y) = -\sum_{x,y} p(x,y) \log p(x|y) = H(X,Y) - H(Y). \tag{13}$$

Exercise 1. *Given random variables X and Y that assume values $x \in (0, 1, 2, 3)$ and $y \in (0, 1)$ respectively, with distribution*

$$\begin{aligned} p(x=0, y=0) = \frac{1}{4}, \, p(x=1, y=0) = \frac{1}{4} \\ p(x=2, y=1) = \frac{1}{4}, \, p(x=3, y=1) = \frac{1}{4} \end{aligned} \tag{14}$$

Compute:

a) $H(X)$

b) $H(Y)$

c) $H(X|Y)$

d) $H(Y|X)$

2.3.2 von Neumann entropy

The concept of entropy also plays an important role in quantum information theory. The von Neumann entropy can be seen as a generalization of Shannon entropy from probability distributions to positive semidefinite operators. And the von Neumann entropy of a system X in state ρ is given by

$$H(X)_\rho = -\mathrm{tr}(\rho \log \rho). \tag{15}$$

Similarly, a conditional quantum entropy can be defined.

Definition 2.4 (Conditional von Neumann entropy)**.** *The entropy of system A conditioned on system E is given by*

$$H(A|E) = H(AE) - H(E), \tag{16}$$

where $H(E) = -\mathrm{tr}(\rho_E \log \rho_E)$ is the von Neumann entropy of the quantum state ρ_E of system E, and similarly for $H(AE)$.

If X and Y are classical variables with joint probability distribution $\{p(x, y)\}$, then the conditional von Neumann entropy reduces to the conditional Shannon entropy (13).

Exercise 2. *Calculate the conditional von-Neumann entropy $H(A|E)$ for the following quantum states:*

a) $\rho_{AE} = |\Phi^+\rangle\langle\Phi^+|_{AE}$

b) $\rho_{AE} = \frac{1}{2} |0\rangle\langle 0|_A \otimes |+\rangle\langle +|_E + \frac{1}{2} |1\rangle\langle 1|_A \otimes |-\rangle\langle -|_E$

c) $\rho_{AE} = \frac{1}{2} |0\rangle\langle 0|_A \otimes \sigma_{E|0} + \frac{1}{2} |1\rangle\langle 1|_A \otimes \sigma_{E|1}$ *where*

$$\sigma_{E|0} = |f_{00}\rangle\langle f_{00}| + |f_{01}\rangle\langle f_{01}| \ , \ \sigma_{E|1} = |f_{10}\rangle\langle f_{10}| + |f_{11}\rangle\langle f_{11}|$$

and

$$\begin{aligned} |f_{00}\rangle &= \sqrt{\lambda_{00}}\, |e_{00}\rangle + \sqrt{\lambda_{01}}\, |e_{01}\rangle \\ |f_{01}\rangle &= \sqrt{\lambda_{10}}\, |e_{10}\rangle + \sqrt{\lambda_{11}}\, |e_{11}\rangle \\ |f_{10}\rangle &= \sqrt{\lambda_{10}}\, |e_{10}\rangle - \sqrt{\lambda_{11}}\, |e_{11}\rangle \\ |f_{11}\rangle &= \sqrt{\lambda_{00}}\, |e_{00}\rangle - \sqrt{\lambda_{01}}\, |e_{01}\rangle \end{aligned}$$

where $|f_{ij}\rangle$ are non-normalized states and $\{|e_{ij}\rangle\}$ forms an orthonormal basis on system E.

Proposition 2.5. *The conditional von Neumann entropy satisfies:*

1. ***Positivity for separable states*** *[8, Lem. 5.11]: If ρ_{AB} is separable then*

$$H(A|B)_\rho \geq 0 \tag{17}$$

2. ***Data processing*** *[8, Cor. 5.5]: Let $\tau_{AB'} = I_A \otimes \mathcal{E}_B(\rho_{AB})$, where $\mathcal{E}_B$ is a CPTP(B, B') channel, then*

$$H(A|B)_\rho \leq H(A|B')_\tau. \tag{18}$$

3. ***Additivity*** *[8, Cor. 5.9]: For $\rho_{AB} \otimes \tau_{A'B'}$ it holds that*

$$H(AA'|BB')_{\rho\otimes\tau} = H(A|B)_\rho + H(A'|B')_\tau. \tag{19}$$

4. ***Conditioning on classical information*** *[8, Prop. 5.4]: Let ρ_{ABX} be a cq-state, $\rho_{ABX} = \sum_x p(x) |x\rangle\langle x| \otimes \rho_{AB|x}$, then*

$$H(A|BX)_\rho \quad = \textstyle\sum_x p(x) H(A|BX = x)_\rho = \sum_x p(x) H(A|B)_{\rho_{|x}}. \tag{20}$$

5. ***Removing classical information*** *[8, Lem. 5.15]: For ρ_{ABX} classical in X,*

$$H(A|XB) \quad \geq H(A|B) - \log |X|, \tag{21}$$

where $|X|$ is the dimension of system X.

The conditional von Neumann entropy finds applications when describing the resources required to perform certain information processing tasks in the i.i.d. limit of many repetitions (e.g. data compression given quantum side information [9]). However, when it comes to consider the one-shot scenario – in which a finite number of repetitions, not necessarily i.i.d., are performed – the von Neumann entropy is insufficient. Moreover, as we will see, in cryptography we are often interested in analysing the performance of a particular task allowing for a small probability of failure. Therefore we need entropic quantities that have meaningful interpretations in these scenarios. For a discussion of one-shot information processing, we refer the reader to [10].

2.3.3 Guessing probability

Let ρ_{AE} be a cq-state

$$\rho_{AE} = \sum_a p(a) \left|a\right\rangle\!\left\langle a\right| \otimes \rho_{E|a}. \tag{22}$$

The guessing probability, $p_{\text{guess}}(A|E)$, is the optimal probability with which someone that has access to system E can correctly guess the value of the variable A:

$$p_{\text{guess}}(A|E)_\rho = \sup_{\{M_E^a\}} \sum_a p(a) \mathrm{Tr}\left(M_E^a \rho_{E|a}\right), \tag{23}$$

where the supremum is over all possible measurements, described by the set of POVMs $\{M_E^a\}_a$ on the system E.

It was shown in [11] that, similarly to the classical case, the conditional min-entropy $H_{\min}(A|E)$ of a classical variable A is directly related to the guessing probability:

$$H_{\min}(A|E)_\rho = -\log p_{\text{guess}}(A|E)_\rho. \tag{24}$$

2.3.4 More entropy

Another entropy that will appear in the security analysis is the max-entropy, that can be defined as:

$$H_{\max}(A|E)_\rho = \sup_{\sigma_E \in \mathcal{S}(E)} \log F(\rho_{AE}, I_A \otimes \sigma_E) \tag{25}$$

where F is the fidelity.

All the entropies introduced so far can be seen as particular cases of a one paremeter family of conditional entropies.

Definition 2.6 (Sandwiched α-Rényi entropies)**.** *For any density operator ρ_{AE} and for $\alpha \in [\frac{1}{2}, 1) \cup (1, \infty)$ the sandwiched α-Rényi entropy of A conditioned on E is defined as*

$$H_\alpha(A|E)_\rho := \sup_{\sigma_E \in \mathcal{S}(E)} \frac{1}{1-\alpha} \log \left(\mathrm{Tr} \left[\left(\mathrm{I}_A \otimes \sigma_E^{\frac{1-\alpha}{2\alpha}} \rho_{AE} \, \mathrm{I}_A \otimes \sigma_E^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \right] \right), \tag{26}$$

where the generalized inverse (i.e., the usual inverse evaluated on the operator's support) is used where appropriate.

The extremal cases of definition (26) correspond to the previously introduced entropies:

- $\alpha \to \infty$ defines the min-entropy $H_{\min}(A|E)$.
- $\alpha = \frac{1}{2}$ defines the max-entropy $H_{\max}(A|E)$.
- For $\alpha \to 1$, one recover $H(A|E)$.

Moreover, we have the following relation

$$H_{\min}(A|E) \leq H(A|E) \leq H_{\max}(A|E). \tag{27}$$

And in general, the sandwiched α-Rényi entropies are monotonically decreasing in α, i.e.:

$$H_\alpha(A|E)_\rho \geq H_{\alpha'}(A|E)_\rho \text{ for } \alpha \leq \alpha'. \tag{28}$$

Proposition 2.7. *The conditional α-Rényi entropies satisfy:*

1. ***Data processing** [8, Cor. 5.5]: Let $\tau_{AB'} = I_A \otimes \mathcal{E}_B(\rho_{AB})$, where $\mathcal{E}_B$ is a CPTP(B, B') channel, then*

$$H_\alpha(A|B)_\rho \leq H_\alpha(A|B')_\tau. \tag{29}$$

2. ***Additivity** [8, Cor. 5.9]: For $\rho_{AB} \otimes \tau_{A'B'}$ it holds that*

$$H_\alpha(AA'|BB')_{\rho\otimes\tau} = H_\alpha(A|B)_\rho + H_\alpha(A'|B')_\tau. \tag{30}$$

3. ***Conditioning on classical information** [8, Prop. 5.4]: Let ρ_{ABX} be a cq-state, $\rho_{ABX} = \sum_x p(x) |x\rangle\langle x| \otimes \rho_{AB|x}$, then*

$$H_\alpha(A|BX)_\rho \quad = \tfrac{\alpha}{1-\alpha} \log \left[\textstyle\sum_x p(x) 2^{\left(\frac{1-\alpha}{\alpha} H_\alpha(A|B)_{\rho_{|x}} \right)} \right], \tag{31}$$

where $\rho_{|x}$ is short for $\rho_{AB|x}$. And for the conditional von Neumann it holds that

$$H(A|BX)_\rho \quad = \textstyle\sum_x p(x) H(A|BX = x)_\rho = \sum_x p(x) H(A|B)_{\rho_{|x}}. \tag{32}$$

4. ***Removing classical information** [8, Lem. 5.15]: For ρ_{ABX} classical in X,*

$$H_\alpha(A|XB) \quad \geq H_\alpha(A|B) - \log |X|, \tag{33}$$

where $|X|$ is the dimension of system X.

2.3.5 Smooth entropies

We are now ready to define quantities that will play a crucial role in determining the key rate of a QKD protocol. The smoothed min- and max-entropies are defined as an optimization over operators that are ϵ-close, in the purified distance, to the state of interest.

$$H^{\epsilon}_{\min}(A|E)_{\rho} = \max_{\tilde{\rho}\in\mathcal{B}^{\epsilon}(\rho)} H_{\min}H(A|E)_{\tilde{\rho}}, \tag{34}$$

$$H^{\epsilon}_{\max}(A|E)_{\rho} = \min_{\tilde{\rho}\in\mathcal{B}^{\epsilon}(\rho)} H_{\max}H(A|E)_{\tilde{\rho}}. \tag{35}$$

This optimization takes into account also operators that are sub-normalized, *i.e.* positive operators with trace smaller than 1

$$\mathcal{B}^{\epsilon}(\rho) = \left\{\tilde{\rho}_{AE} \in \mathcal{L}(AE) : \tilde{\rho}_{AE} \geq 0, \mathrm{tr}(\tilde{\rho}_{AE}) \leq 1 \text{ and } D_P(\rho_{AE}, \tilde{\rho}_{AE}) \leq \epsilon\right\}. \tag{36}$$

The smoothed entropies, defined with respect to the purified distance, display many interesting properties. In particular, they satisfy a duality relation.

Proposition 2.8 (Duality of smoothed entropies)**.** *Let ρ_{ABC} be a pure quantum state, then*

$$H^{\epsilon}_{\max}(A|B)_{\rho} = -H^{\epsilon}_{\min}(A|E)_{\rho}. \tag{37}$$

Moreover, the smooth min- and max-entropies inheret some properties of the α-Rényi entropies.

Proposition 2.9. *The smoothed entropies satisfy:*

1. ***Data processing** [8, Thm. 6.19]: Let $\tau_{AB'} = I_A \otimes \mathcal{E}_B(\rho_{AB})$, where $\mathcal{E}_B$ is a CPTP(B, B') channel, then*

$$H^{\epsilon}_{\min}(A|B)_{\rho} \leq H^{\epsilon}_{\min}(A|B')_{\tau}, \tag{38}$$

$$H^{\epsilon}_{\max}(A|B)_{\rho} \leq H^{\epsilon}_{\max}(A|B')_{\tau}, \tag{39}$$

2. ***Removing classical information** [8, Lem. 6.18]: For ρ_{ABX} classical X,*

$$H^{\epsilon}_{\min}(A|XB)_{\rho} \geq H^{\epsilon}_{\min}(A|B)_{\rho} - \log|X|, \tag{40}$$

$$H^{\epsilon}_{\max}(A|XB)_{\rho} \geq H^{\epsilon}_{\max}(A|B)_{\rho} - \log|X| \tag{41}$$

where $|X|$ is the dimension of system X.

Interestingly, we will see that the smooth min- and max-entropies converge to the von Neumann entropy in the limit of several copies of a quantum state:

$$\lim_{n\to\infty}\frac{1}{n}H^{\epsilon}_{\min}(A_1^n|E_1^n)_{\rho^{\otimes n}} = \lim_{n\to\infty}\frac{1}{n}H^{\epsilon}_{\max}(A_1^n|E_1^n)_{\rho^{\otimes n}} = H(A|E)_{\rho} \tag{42}$$

This means that if a resource usage in the one-shot setting is characterized by the smooth min- or max-entropy, then in the i.i.d. limit of many repetitions the rate of resource usage is given by the von Neumann entropy.

3 Security of quantum key distribution

The security of quantum key distribution can be split into two conditions.

Definition 3.1 (Correctness)**.** *A QKD protocol is ϵ_{corr}-correct if the probability that the final key of Alice, K_A, differs from the final key of Bob, K_B, is smaller than ϵ_{corr}, i.e.*

$$P(K_A \neq K_B) \leq \epsilon_{corr}. \tag{43}$$

Definition 3.2 (Secrecy)**.** *Let Ω be the event that the QKD protocol does not abort, and $p(\Omega)$ be the probability of the event Ω. The protocol is ϵ_{sec}-secret if*

$$p(\Omega) \cdot \left\| \rho_{K_A E|\Omega} - \tau_{K_A} \otimes \rho_{E|\Omega} \right\|_{\mathrm{tr}} \leq \epsilon_{sec}, \tag{44}$$

where $\tau_{K_A} = \frac{1}{2^\ell} \sum_k |k\rangle\langle k|_A$ is the maximally mixed state in the space of strings $K_A \in \{0,1\}^\ell$.

If a protocol is ϵ_{corr}-correct and ϵ_{sec}-secret, then it is ϵ^s_{QKD}-correct-and-secret for any $\epsilon^s_{QKD} \geq \epsilon_{corr} + \epsilon_{sec}$.

Remark: a third condition, called completeness or robustness, is required from a QKD protocol. Completeness states that there should exist an honest implementation for which the probability of aborting the protocol is very small.

For a QKD protocol with n rounds of *distribution and measurement* that generates an ϵ-correct-and-secret key of ℓ bits, the secret key rate is defined as

$$r = \frac{\ell}{n} \text{ bits/round.} \tag{45}$$

The above rate is evaluated in *bits/round*, but the generation rate τ, i.e., how many rounds can be generated per second, can also be taken into account to give a rate in *bits/s*

$$r = \tau \frac{\ell}{n} \text{ bits/s.} \tag{46}$$

The goal of the security analysis of a QKD protocol is to derive the secret key rate as a function of the parameters that Alice and Bob can estimate during the execution of the protocol.

3.1 Privacy amplification

We now deal with the ‘classical’ part of a QKD protocol.

In the last step of a QKD protocol, Alice and Bob want to turn their equal string of bits, which may be partially known to an eavesdropper, into a shorter completely secure string of bits. In order to do that, they are going to make use of a 2-universal family of hash functions.

A hash function $f : \{0,1\}^n \to \{0,1\}^\ell$ is a function that maps a longer string of bits into a shorter string, $\ell \leq n$. We will be interested in particular families of hash functions that satisfy a property called 2-universality.

Definition 3.3 (2-universal hash functions)**.** *A family of hash functions $\mathcal{F} = \{f : \{0,1\}^n \to \{0,1\}^\ell\}$ is called 2-universal if for every two strings $x, x' \in \{0,1\}^n$ with $x \neq x'$ then*

$$\Pr_{f \in \mathcal{F}}(f(x) = f(x')) = \frac{1}{2^\ell}, \tag{47}$$

where f is chosen uniformly at random in $\mathcal{F}$.

The property of 2-universality ensures a good distribution of the outputs. For $\ell \leq n$ there always exist a 2-universal family of hash functions [12].

We are now ready to state a very important result that allows Alice and Bob to establish privacy amplification in the presence of a quantum eavesdropper.

Theorem 3.4 (Leftover Hashing Lemma)**.** *Let $\rho_{A_1^n E}$ be a cq-state, where the classical register A_1^n stores an n-bit string, and let $\mathcal{F}$ be a 2-universal family of hash functions, from $\{0,1\}^n$ to $\{0,1\}^\ell$, that maps A_1^n into K_A, then*

$$\|\rho_{K_A FE - \tau_{K_A} \otimes \rho_{FE}}\|_{\mathrm{tr}} \leq \frac{1}{2} 2^{-\frac{1}{2}(H_{\min}(A_1^n|E)_\rho - \ell)}, \tag{48}$$

where F is a classical register that stores the hash function f.

The Leftover Hashing Lemma establishes a relation between the size ℓ of a secret key that can be extracted and the min-entropy of the system before privacy amplification. For more details and proof of the left-over hashing lemma, we refer the reader to [7, 13].

The Leftover Hashing lemma can also be formulated in terms of the smooth min-entropy. This is important because the smooth min-entropy can be much larger than the min-entropy, and the price to pay is only a linear term in the security parameter[1].

Theorem 3.5 (Leftover Hashing Lemma with smooth min-entropy)**.** *Let $\rho_{A_1^n E}$ be a cq-state, where the classical register A_1^n stores an n-bit string, and let $\mathcal{H}$ be a 2-universal family of hash functions, from $\{0,1\}^n$ to $\{0,1\}^\ell$, that maps A_1^n into K_A, then*

$$\|\rho_{K_A FE} - \tau_{K_A} \otimes \rho_{FE}\|_{\mathrm{tr}} \leq \frac{1}{2} 2^{-\frac{1}{2}\left(H^\epsilon_{\min}(A_1^n|E)_\rho - \ell\right)} + 2\epsilon. \tag{49}$$

[1] In Ref. [7], the leftover hash lemma was formulated with the smooth min-entropy defined as a maximum over states that are ϵ-close to ρ in the trace norm. The proof of Theorem 3.5, with the smooth min-entropy defined according to eq. (34), can be found in Ref. [13]

Proof. Let $\tilde{\rho}_{A_1^n E}$ be a sub-normalized state such that $H_{\min}(A_1^n|E)_{\tilde{\rho}} = H_{\min}^{\epsilon}(A_1^n|E)_{\rho}$ and $D_P(\rho_{A_1^n E}, \tilde{\rho}_{A_1^n E}) \leq \epsilon$.

Given that the purified distance is non-increasing under CPTP maps, eq. (10), we have

$$D_P(\rho_{FE}, \tilde{\rho}_{FE}) \leq D_P(\rho_{K_A FE}, \tilde{\rho}_{K_A FE}) \leq \epsilon. \tag{50}$$

Now we make use of the triangle inequality

$$\begin{aligned}\|\rho_{K_A FE} - \tau_{K_A} \otimes \rho_{FE}\|_{\mathrm{tr}} \leq & \underbrace{\|\rho_{K_A FE} - \tilde{\rho}_{K_A FE}\|_{\mathrm{tr}}}_{\leq \epsilon} + \|\tilde{\rho}_{K_A FE} - \tau_{K_A} \otimes \tilde{\rho}_{FE}\|_{\mathrm{tr}} \\ & + \underbrace{\|\tau_{K_A} \otimes \tilde{\rho}_{FE} - \tau_{K_A} \otimes \rho_{FE}\|_{\mathrm{tr}}}_{\leq \epsilon}.\end{aligned} \tag{51}$$

The fact that the first and third term are bounded by ϵ follows from (50) and the relation with the trace distance, eq. (9). The second term can be bounded using Theorem 3.4, from which we obtain the desired relation. □

The Leftover hashing lemma gives us a tool to bound the distance of the state of the protocol after privacy amplification to an ideal state. Indeed we can use the following steps

$$p(\Omega) \cdot \left\|\rho_{K_A E_{|\Omega}} - \tau_{K_A} \otimes \rho_{E|\Omega}\right\|_{\mathrm{tr}} = \|\rho_{K_A E_{\wedge\Omega}} - \tau_{K_A} \otimes \rho_{E \wedge \Omega}\|_{\mathrm{tr}} \tag{52}$$

$$\leq \frac{1}{2} 2^{-\frac{1}{2}\left(H_{\min}^{\epsilon}(A_1^n|E)_{\rho_{\wedge\Omega}} - \ell\right)} + 2\epsilon \tag{53}$$

where $\rho_{K_A E_{\wedge\Omega}} = p(\Omega)\rho_{K_A E_{|\Omega}}$ is a subnormalized state.

We now note that by choosing

$$\ell = H_{\min}^{\epsilon}(A_1^n|E)_{\rho} - 2\log\left(\frac{1}{2\epsilon_{PA}}\right) \tag{54}$$

we obtain a ϵ_{sec}-secret key with $\epsilon_{sec} = \epsilon_{PA} + 2\epsilon$.

Remark: Eq. (54) follows from the fact that $H_{\min}^{\epsilon}(A_1^n|E)_{\rho_{\wedge\Omega}} \geq H_{\min}^{\epsilon}(A_1^n|E)_{\rho}$ as proved in [13, Lemma 10]. This is a technicality to deal with the fact that we will have an estimate of ρ instead of the conditioned state.

3.2 Information reconciliation

In the previous section we have seen that the key length is basically determined by the smooth min-entropy of Alice's string of raw bits conditioned on the information available to the eavesdropper.

The total information available to Eve, that here we denote[2] E_T, is composed by her quantum side information and all the public classical communication performed

[2] Note that, in order to avoid overloading notation, E_T was denoted simply E in the previous sections.

by Alice and Bob. We can now use Property 2.9.2 to remove the dependence on the information exchanged by Alice and Bob during information reconciliation

$$H^{\epsilon}_{\min}(A_1^n|E_T)_\rho \geq H^{\epsilon}_{\min}(A_1^n|E)_\rho - \mathrm{leak}_{\mathrm{IR}}, \tag{55}$$

where now E denotes the side information of Eve excluding the knowledge of public information exchanged during information reconciliation, and $\mathrm{leak}_{\mathrm{IR}}$ is the amount of bits communicated by Alice and Bob during information reconciliation.

We will consider a one-way information reconciliation[3] protocol based on 2-universal hashing functions which leads to the minimum possible leakage.

```
One-way Information reconciliation
1: Alice sends a syndrome $C = synd(A_1^n)$ to Bob.
2: Using his string $B_1^n$ and the syndrome $C$, Bob computes a guess $\hat{A}_1^n$ for Alice's string.
3: Alice computes a hash $f_{\mathrm{IR}}(A_1^n)$ (chosen from a two-universal family of hashing functions) of $\log\left(\frac{1}{\epsilon_{\mathrm{IR}}}\right)$ bits and sends it to Bob.
4: Bob checks if $f_{\mathrm{IR}}(\hat{A}_1^n) = f_{\mathrm{IR}}(A_1^n)$, and aborts if that is not the case.
```

The minimum leakage for a one-way information reconciliation was established in [14, 15].

Theorem 3.6. *The minimum leakage of a one-way information reconciliation protocol satisfies*

$$\mathrm{leak}_{\mathrm{IR}} \leq H_{\max}^{\frac{\epsilon'_{\mathrm{IR}}}{2}}(A_1^n|B_1^n) + \log\left(\frac{8}{{\epsilon'_{\mathrm{IR}}}^2} + \frac{2}{2-\epsilon'_{\mathrm{IR}}}\right) + \log\left(\frac{1}{\epsilon_{\mathrm{IR}}}\right). \tag{56}$$

We note that, due to step 3 of the information reconciliation protocol and the property (47) of two-universal hashing functions, if Ω is the event that Alice and Bob does not abort in the information reconciliation protocol, then

$$\begin{gathered} P(\Omega|A_1^n \neq \hat{A}_1^n) = \epsilon_{\mathrm{IR}} \\ \Downarrow \\ P(A_1^n \neq \hat{A}_1^n \wedge \Omega) \leq \epsilon_{\mathrm{IR}}. \end{gathered} \tag{57}$$

Therefore, we can calculate

$$\begin{aligned} P(K_A \neq K_B) &= P(K_A \neq K_B \wedge \Omega) \\ &\leq P(A_1^n \neq \hat{A}_1^n \wedge \Omega) \\ &\leq \epsilon_{\mathrm{IR}} \end{aligned} \tag{58}$$

[3] The term‘one-way’ stands for the fact that Alice's string is fixed and only Bob performs corrections to match Alice's string.

where the first equality follows from the fact that, when the protocol aborts, we can consider Alice and Bob to trivially share the same key of size zero.

We have, then, establish that we have an ϵ_{corr}-correct protocol with $\epsilon_{corr} = \epsilon_{\mathrm{IR}}$.

4 Security against collective attacks

The earlier proofs of QKD security were based on entanglement distillation [5]. In particular, Devetak and Winter [16], derived that the asymptotic key rate of a QKD protocol against collective attacks is given by:

$$r = H(A|E) - H(A|B). \tag{59}$$

Here we will derive the asymptotic key rate following the results of [7, 13].

So far we have established that the key is given by the conditional smooth min-entropy $H^{\epsilon}_{\min}(A_1^n|E)$.

We start by analysing the case that the eavesdropper is restricted to collective attacks. In this case, the state at the end of the protocol $\rho_{A_1^n E}$ is of the form:

$$\rho_{A_1^n E} = \rho_{AE}^{\otimes n}. \tag{60}$$

The quantum asymptotic equipartition property (AEP) [17] is the key result that allows us to break the conditional smooth min-entropy of state the total $\rho_{AE}^{\otimes n}$ into n times the conditional von Neumann entropy of a single state ρ_{AE}.

Theorem 4.1 (Asymptotic equipartition property [17]). *For $n \geq \frac{8}{5}\log\frac{2}{\epsilon^2}$:*

$$H^{\epsilon}_{\min}(A_1^n|E_1^n)_{\rho_{AE}^{\otimes n}} \geq nH(A|E)_{\rho_{AE}} - \sqrt{n}\,\delta(\epsilon, \eta_{AE}) \tag{61}$$

$$H^{\epsilon}_{\max}(A_1^n|E_1^n)_{\rho_{AE}^{\otimes n}} \leq nH(A|E)_{\rho_{AE}} + \sqrt{n}\,\delta(\epsilon, \eta_{AE}) \tag{62}$$

where $\delta(\epsilon, \eta_{AE}) = 4\log\eta_{AE}\sqrt{\log\frac{2}{\epsilon^2}}$ and $\eta_{AE} = \sqrt{2^{-H_{\min}(A|E)_\rho}} + \sqrt{2^{H_{\max}(A|E)_\rho}} + 1$.

Therefore, under the assumption of collective attacks, the quantum AEP reduces the problem of estimating the key rate of a string of n bits to the problem of bounding the one-round conditional von Neumann entropy. We remark that the AEP implies an additional term, proportional to $\sqrt{n}$, which is significant for the finite regime analyses.

We can also use the AEP to bound the information leaked during information reconciliation

$$\mathrm{leak}_{\mathrm{IR}} \leq nH(A|B)_\rho + \sqrt{n}\,\delta\left(\frac{\epsilon'_{\mathrm{IR}}}{2}, \eta_{AB}\right) + \log\left(\frac{8}{{\epsilon'_{\mathrm{IR}}}^2} + \frac{2}{2-\epsilon'_{\mathrm{IR}}}\right) + \log\left(\frac{1}{\epsilon_{\mathrm{IR}}}\right). \tag{63}$$

Putting the results together we have that the asymptotic key rate is given by

$$r_\infty = \lim_{n\to\infty} \frac{\ell}{n} = H(A|E)_\rho - H(A|B)_\rho. \tag{64}$$

Note that eqs. (61) and (63) provide a way to calculate the key rate for a real implementation with a finite number of rounds. For small n ($< 10^6$), the terms depending on $\sqrt{n}$ are significant, which implies that a secure key, $\ell > 0$, can only be obtained if a minimum number of rounds $n_{\min}$ is performed.

4.1 Asymptotic key rate of the BB84

We are ready to focus again on the BB84 protocol. In the BB84, the only information we obtain about the state are the two parameters estimated during the protocol, Q_X and Q_Z:

$$Q_X = p(a \neq b|\text{X-basis measurement}) \tag{65}$$

$$Q_Z = p(a \neq b|\text{Z-basis measurement}) \tag{66}$$

Therefore our goal is to compute:

$$r_\infty = \inf_{\rho\in\mathcal{S}_{(Q_X,Q_Z)}} \left\{H(A|E)_\rho - H(A|B)_\rho\right\}, \tag{67}$$

where $\mathcal{S}_{(Q_X,Q_Z)}$ is the set of quantum states with QBERs Q_X and Q_Z.

4.1.1 Reduction to Bell diagonal states

In fact we can restrict the analysis to Bell diagonal states only. These are states of the form

$$\tilde{\rho}_{AB} = \lambda_{00}\Phi_{00} + \lambda_{01}\Phi_{01} + \lambda_{10}\Phi_{10} + \lambda_{11}\Phi_{11} \tag{68}$$

where $\Phi_{ij} = |\Phi_{ij}\rangle\langle\Phi_{ij}|$ and $|\Phi_{ij}\rangle = X^i Z^j \otimes I\,|\Phi^+\rangle$ form the Bell basis.

To see that we first note that the state $\tilde{\rho}$ can be obtained from ρ by the following operation:

$$\tilde{\rho}_{AB} = \frac{1}{4}\left(\rho_{AB} + X\otimes X\rho_{AB}X\otimes X + Y\otimes Y\rho_{AB}Y\otimes Y + Z\otimes Z\rho_{AB}Z\otimes Z\right), \tag{69}$$

which preserves the Bell diagonal elements

$$\langle\Phi_{ij}|\,\rho_{AB}\,|\Phi_{ij}\rangle = \langle\Phi_{ij}|\,\tilde{\rho}_{AB}\,|\Phi_{ij}\rangle = \lambda_{ij}, \tag{70}$$

and also the QBERs: just note that the maps applied in each term either commute with the measurement basis or flips the outcome of Alice and Bob, which does not change the QBERs.

Moreover, it is possible to show that

$$H(A|E)_\rho \geq H(A|E)_{\tilde{\rho}}, \tag{71}$$

so without loss of generality we will restrict the analysis to Bell diagonal states.

4.1.2 Asymptotic key rate

We start with the Bell diagonal state $\tilde{\rho}$, eq. (68), and construct a purification which is held by the eavesdropper

$$|\psi\rangle_{ABE} = \sum_{i,j} \sqrt{\lambda_{ij}} \, |\Phi_{ij}\rangle \otimes |e_{ij}\rangle \tag{72}$$

$$\begin{aligned} &= |00\rangle \frac{1}{\sqrt{2}} \left(\sqrt{\lambda_{00}} \, |e_{00}\rangle + \sqrt{\lambda_{01}} \, |e_{01}\rangle \right) \\ &\quad + |11\rangle \frac{1}{\sqrt{2}} \left(\sqrt{\lambda_{00}} \, |e_{00}\rangle - \sqrt{\lambda_{01}} \, |e_{01}\rangle \right) \\ &\quad + |01\rangle \frac{1}{\sqrt{2}} \left(\sqrt{\lambda_{10}} \, |e_{10}\rangle + \sqrt{\lambda_{11}} \, |e_{11}\rangle \right) \\ &\quad + |10\rangle \frac{1}{\sqrt{2}} \left(\sqrt{\lambda_{10}} \, |e_{10}\rangle - \sqrt{\lambda_{11}} \, |e_{11}\rangle \right) . \end{aligned} \tag{73}$$

After Alice and Bob measure in the Z basis and we trace out Bob, we obtain the state

$$\rho_{AE} = \frac{1}{2} \, |0\rangle\langle 0|_A \otimes \sigma_{E|0} + \frac{1}{2} \, |1\rangle\langle 1|_A \otimes \sigma_{E|1}, \tag{74}$$

where

$$\sigma_{E|0} = |f_{00}\rangle\langle f_{00}| + |f_{01}\rangle\langle f_{01}| \ , \ \sigma_{E|1} = |f_{10}\rangle\langle f_{10}| + |f_{11}\rangle\langle f_{11}| \tag{75}$$

and

$$\begin{aligned} |f_{00}\rangle &= \sqrt{\lambda_{00}} \, |e_{00}\rangle + \sqrt{\lambda_{01}} \, |e_{01}\rangle \\ |f_{01}\rangle &= \sqrt{\lambda_{10}} \, |e_{10}\rangle + \sqrt{\lambda_{11}} \, |e_{11}\rangle \\ |f_{10}\rangle &= \sqrt{\lambda_{10}} \, |e_{10}\rangle - \sqrt{\lambda_{11}} \, |e_{11}\rangle \\ |f_{11}\rangle &= \sqrt{\lambda_{00}} \, |e_{00}\rangle - \sqrt{\lambda_{01}} \, |e_{01}\rangle \end{aligned} \tag{76}$$

From Exercise 2.c) we have that

$$H(A|E)_{\tilde{\rho}} = 1 + h(\lambda_{10} + \lambda_{11}) - H(\{\lambda_{ij}\}), \tag{77}$$

where $h(p) = -p \log p - (1-p) \log(1-p)$ is the binary entropy and $H(\{\lambda_{ij}\}) = -\sum_{ij} \lambda_{ij} \log \lambda_{ij}$.

For the information reconciliation term we get

$$H(A|B)_{\tilde{\rho}} = -\sum_{a,b} p(a,b) \log p(a|b) \tag{78}$$

$$= h(\lambda_{10} + \lambda_{11}). \tag{79}$$

And since the QBERs Q_X and Q_Z relate to the Bell coefficients by

$$Q_Z = \lambda_{10} + \lambda_{11} \tag{80}$$
$$Q_X = \lambda_{01} + \lambda_{11}, \tag{81}$$

we see that, in the asymptotic limit, the leakage in the information reconciliation is determined by the QBER on the measurement basis:

$$\text{leak}_{\text{IR}} = h(Q_Z). \tag{82}$$

Combining (77) and (79) we have that

$$r_\infty = \inf_{\{\lambda_{ij}\} \in \mathcal{S}_{(Q_X, Q_Z)}} 1 - H(\{\lambda_{ij}\}). \tag{83}$$

Minimizing the r.h.s. with respect to a single free parameter we obtain[4]

$$r_\infty = 1 - h(Q_X) - h(Q_Z). \tag{84}$$

Exercise 3. *Consider a noisy implementation where the source distributes a maximally entangled state that undergoes depolarizing noise, i.e., the state shared by Alice and Bob at each round is*

$$\rho_{AB} = (1-\nu)\Phi^+ + \nu\frac{I}{4}. \tag{85}$$

What is the maximum amount of noise ν that an implementation of the BB84 with this setup can tolerate? How does that translate to the values of QBERs Q_X and Q_Z?

[4] **Hint:** To achieve the desired expression you can use the parametrization

$$\lambda_{00} = 1 - \left(\frac{Q_X + t + Q_Z}{2}\right)$$
$$\lambda_{01} = \frac{Q_X + t - Q_Z}{2}$$
$$\lambda_{10} = \frac{-Q_X + t + Q_Z}{2}$$
$$\lambda_{11} = \frac{Q_X - t + Q_Z}{2}$$

and the fact that

$$H(\{\lambda_{ij}\}) \equiv h(\lambda_{10} + \lambda_{11}) + (\lambda_{10} + \lambda_{11})h\left(\frac{\lambda_{10}}{\lambda_{10} + \lambda_{11}}\right) + (\lambda_{00} + \lambda_{01})h\left(\frac{\lambda_{00}}{\lambda_{00} + \lambda_{01}}\right).$$

5 Security against coherent attacks

5.1 Post-selection technique

The extension of de Finetti theorems to the quantum setting establishes that if a quantum state of N parties is symmetric, i.e., invariant under the permutation of parties, then the state of a small subset of $m \ll N$ parties is of the form $\sigma^{\otimes m}$, for some unknown state σ. Improved versions of quantum de Finetti theorems and their application to quantum key distribution were explored in [7, 18]. In summary, by exploring the symmetries of a QKD protocol, we can reduce the analysis to collective attacks.

The most recent de Finetti-type result is the post-selection technique introduced in [19], which provides tighter bounds for QKD security.

Theorem 5.1. *Let $\mathcal{P}_{\mathrm{QKD}}$ be a QKD protocol that is invariant under the permutation of the input subsystems. Then if $\mathcal{P}_{\mathrm{QKD}}$ is ϵ-secure against collective attacks generating a key of size ℓ, the $\mathcal{P}_{\mathrm{QKD}}$ is ϵ'-secure against collective attacks if the key is shortened to a size ℓ' where*

$$\epsilon' = (n+1)^{d^2-1}\epsilon \tag{86}$$

and

$$\ell' = \ell - 2(d^2-1)\log(n+1), \tag{87}$$

where d is the dimension of each subsystem shared by Alice and Bob, and n the total number of rounds.

For a detailed proof of the post-selection technique we refer the reader to [20].

The post-selection technique is a general result, valid for any QKD protocol with the required symmetry. We note that the BB84 protocol is invariant under the permutation of the input states, since the protocol acts in the same way in each round of the protocol. Moreover, for the BB84 we have that $d = 4$.

5.2 Uncertainty relation

Another way of proving security of the BB84 against coherent attacks is using the uncertainty relation for smooth entropies [21].

Theorem 5.2 (Uncertainty relation for smooth entropies)**.** *Let ρ_{ABE} be a tri-partite quantum state and $\{M_X^a\}$ and $\left\{M_Z^{a'}\right\}$ be two POVMs on A. Then,*

$$H_{\min}^{\epsilon}(A_Z|E)_\rho + H_{\max}^{\epsilon}(A_X|B)_\rho \geq \log\left(\frac{1}{c}\right), \tag{88}$$

where

$$c := \max_{a,a'} \left\| \sqrt{M_X^a} \sqrt{M_Z^{a'}} \right\|_\infty^2 \tag{89}$$

and $\|X\|_\infty$ *is the operator norm that corresponds to the largest singular value of* X*.*

For the BB84 protocol we can take $\left\{M_Z^{a'}\right\}$ to be the measurement in the Z-basis of the n qubits of Alice and $\{M_X^a\}$ to be the measurement of the n qubits in the X basis, and then we have that

$$c = \max_{\vec{a}_X, \vec{a}_Z} \left\| \bigotimes_i |a_{Xi}\rangle \langle a_{Xi}|a_{Zi}\rangle \langle a_{Zi}| \right\|_\infty^2 = \left(\frac{1}{2}\right)^n, \tag{90}$$

since $\langle a_{Xi}|a_{Zi}\rangle = \frac{1}{\sqrt{2}}$, as $|a_{Xi}\rangle \in \{|+\rangle, |-\rangle\}$ and $|a_{Zi}\rangle \in \{|0\rangle, |1\rangle\}$.

Therefore we have

$$\begin{aligned} H_{\min}^\epsilon(A_1^n|E)_\rho &\geq n - H_{\max}^\epsilon({A_X}_1^n|B)_\rho & (91)\\ &\geq n - H_{\max}^\epsilon({A_X}_1^n|{B_X}_1^n)_\rho & (92)\end{aligned}$$

where in the second inequality we use the data-processing of smoothed entropies (Property 2.9.1). $H_{\max}^\epsilon({A_X}_1^n|{B_X}_1^n)_\rho$ is the conditional entropy of Alice's outcomes given Bob's outcomes, had they measured all the systems in the X-basis.

The problem is now reduced to bounding the entropy of a classical probability distribution, given the parameters estimated in the protocol.

Using classical results for sampling without replacement, the authors of [13, 22] bound $H_{\max}^\epsilon({A_X}_1^n|{B_X}_1^n)_\rho$ by a function of the estimated QBER in the X basis. In the limit of infinitely many rounds, their result states that

$$\frac{1}{n} H_{\max}^\epsilon({A_X}_1^n|{B_X}_1^n)_\rho \longrightarrow H(A_X|B_X) = h(Q_X). \tag{93}$$

The leakage in the information reconciliation can be evaluated for an honest i.i.d. implementation and therefore it is bounded by (63). Therefore, using the uncertainty relation we again obtain:

$$r_\infty = 1 - h(Q_X) - h(Q_Z). \tag{94}$$

Remark 1: Both techniques to prove security against coherent attacks, the post-selection technique and the uncertainty relation, achieve the same asymptotic key rate and show that collective attacks are optimal in the limit of infinitely many repetitions. In the finite regime, however, the security analysis based on the uncertainty relation leads to tighter results (it has smaller overhead terms and therefore better rates in the finite regime).

Remark 2: Security proof based on the uncertainty relation is restricted to protocols in which Alice performs only two possible measurements. The post-selection technique, on the other hand, can be applied to more general protocols (in particular the six-state protocol [23] in which Alice and Bob perform measurements in three basis, X, Y and Z).

6 BB84 with imperfect sources (decoy states method)

A feasible source for the implementation of the BB84 protocol consists of phase randomized weak coherent pulses (WCP) (i.e. the BB84 states are encoded in the polarization of a coherent state). The problem is that, in this case, Alice may send more than one photon per round. If Eve can intercept some of these extra photons, what is called a photon-number-splitting (PNS) attack, then she will have access to the same information as Bob and not generate any QBER in the system. Therefore Alice and Bob will not detect the attack and end up with an insecure key.

The way to overcome this problem, as proposed in [24], is to account for the fact that security is only guaranteed for the rounds in which the source emitted single photons. The asymptotic key rate of the BB84 is then modified to:

$$r_\infty = \Gamma^{(1)} \left[1 - h(q_X^{(1)})\right] - \Gamma\, h(Q_Z) \tag{95}$$

where

- Γ: is the gain of the signal state, i.e. the probability that Bob has a detection given that Alice sent a state
- $\Gamma^{(1)}$: is the gain of the single photon state, i.e. the probability that Bob has a detection of a single photon event.
- Q_Z: QBER of the signal state in the Z basis.
- $q_X^{(1)}$: QBER of single photon events in the X basis.

The problem is that $\Gamma^{(1)}$ and $q_X^{(1)}$ are not directly observed quantities.

The method of decoy states (see [25] for details) provides a way to estimate $\Gamma^{(1)}$ and $q_X^{(1)}$. The idea is that, in some of the rounds, Alice uses different intensities to prepare the so called decoy states.

A phase-randomized WCP source with mean photon number μ is described by the state:

$$\rho_\mu = \frac{1}{2\pi}\int_0^{2\pi} d\theta \left|\sqrt{\mu}e^{i\theta}\right\rangle\left\langle\sqrt{\mu}e^{i\theta}\right| = \sum_{n=0}^{\infty} e^{-\mu}\frac{\mu^n}{n!}\,|n\rangle\langle n| \tag{96}$$

where $|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$ is a coherent state. This state describes a situation in which the probability that Alice's signal has n photons is given by $p_n = e^{-\mu} \frac{\mu^n}{n!}$.

The gain of this source can be described by

$$\Gamma(\mu) = Y^{(0)} e^{-\mu} + Y^{(1)} e^{-\mu} \mu + Y^{(2)} e^{-\mu} \frac{\mu^2}{2} + \ldots + Y^{(n)} e^{-\mu} \frac{\mu^n}{n!} + \ldots, \tag{97}$$

where

$$Y^{(n)} = \Pr(\text{Bob detects a photon}|\text{Alice emitted } n \text{ photons}) \tag{98}$$

is the yield of an n-photon signal.

Similarly the QBER can depend on the photon number, and we define $q_Z^{(n)}$ ($q_X^{(n)}$) as the QBER of an n-photon signal in the $Z(X)$ basis. The total (observed) QBER is given by

$$Q_Z(\mu) = \frac{Y^{(0)} e^{-\mu} q_Z^{(0)} + Y^{(1)} e^{-\mu} \mu q_Z^{(1)} + \ldots + Y^{(n)} e^{-\mu} \frac{\mu^n}{n!} q_Z^{(n)} + \ldots}{\Gamma(\mu)} \tag{99}$$

which is the weighted average of the QBERs of different photon number. And similarly for $Q_X(\mu)$.

Since Eve cannot distinguish a decoy from a signal state, but the only information available to her is the photon number, then *the yields $Y^{(n)}$ and QBERs $q_Z^{(n)}$, are independent of the intensities* μ, i.e. it is independent of whether the photons come from a decoy state or a signal state.

By generating phase-randomized WCPs of different intensities μ in the testing rounds and measuring the observable quantities $\Gamma(\mu)$, $Q_X(\mu)$, and $Q_Z(\mu)$, Alice and Bob can estimate the values of $\Gamma^{(1)}$ and $q_X^{(1)}$ (note that equation (97) is linear on the parameters $Y^{(n)}$, and afterwards equation (99) is linear on the parameters $q_X^{(n)}$).

More precisely, we want to determine a lower bound on $\Gamma^{(1)} = Y^{(1)} e^{-\mu} \mu$, for the signal state, and an upper bound on $q_X^{(1)}$. The use of only two decoy states was shown to be sufficient to achieve almost optimal results [26].

7 Untrusted detectors: measurement device-independent quantum key-distribution (MDI-QKD)

Another big weakness of the BB84 protocol lies in the assumption that the measurement devices are performing the required measurements. Measurement device-independent QKD is a proposal to drop this assumption. For a review on MDI-QKD see [27].

In the MDI setting, Alice and Bob have *trusted* sources in which they can prepare BB84 states. They send the prepared states to an unstrusted relay (which can be controlled by the eavesdropper Eve) that performs a Bell state measurement and announces the outcome.

For the rounds in which Alice and Bob used the same basis for preparation, the outcome of the relay reveals the parity of their encoded bits (see Table 1).

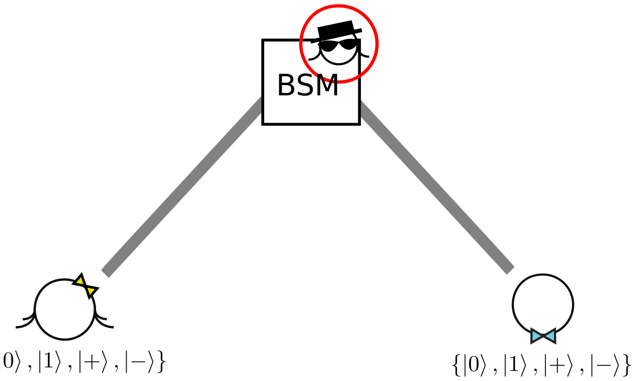
BSM
$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$
$\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$

Figure 2: MDIQKD setup: Alice and Bob prepare BB84 states and send to an untrusted relay who performs a Bell state measurement.

Relay output	Φ^+	Φ^-	Ψ^+	Ψ^-
Z-basis preparation	$a = b$	$a = b$	$a \neq b$	$a \neq b$
X-basis preparation	$a = b$	$a \neq b$	$a = b$	$a \neq b$

Table 1: Relation of Alice and Bob encoded bits given the Bell state measured by the relay, for preparation in the Z and the X bases.

The knowledge of the parity does not allow the relay to obtain information about the actual values of Alice and Bob shared bits. And by comparing the outcomes of some of the rounds and estimating the QBERs Q_X and Q_Z, Alice and Bob can ensure that the relay is behaving honestly.

Imperfect state preparation can also be accounted for in MDI-QKD by combining it with the method of decoy states [28]. The difference here is that now we have Alice and Bob preparing states. Therefore security is guaranteed only when both, Alice and Bob's sources, prepared single photons. In this case the asymptotic key rate is given by:

$$r_\infty = \Gamma^{(1,1)}\left[1 - h(q_X^{(1,1)})\right] - \Gamma\, h(Q_Z), \tag{100}$$

where Γ is the total gain of the source, and $\Gamma^{(m,n)}$, $q_X^{(m,n)}(q_Z^{(m,n)})$ are the gain and QBER in the $X(Z)$ basis, of the signal states sent by Alice and Bob, when Alice's source sends n photons and Bob sends m.

In this scenario the method of decoy states generates the set of equations

$$\Gamma(\mu,\nu) = \sum_{n,m} e^{-\mu}\frac{\mu^n}{n!}e^{-\nu}\frac{\nu^m}{m!}Y^{(n,m)}, \tag{101}$$

$$Q_X(\mu,\nu) = \frac{\sum_{n,m} e^{-\mu}\frac{\mu^n}{n!}e^{-\nu}\frac{\nu^m}{m!}Y^{(n,m)}q_X^{(n,m)}}{\Gamma(\mu,\nu)}, \tag{102}$$

and similarly for $Q_Z(\mu,\nu)$.

8 Device-independent quantum key distribution (DIQKD)

In the MDI-QKD scenario discussed in the previous section, we still need to assume that Alice and Bob's preparation device is somewhat trusted (although we can overcome some imperfections, such as multiple-photon generation, using decoy states). We are now going to relax all the assumptions about the specific workings of the systems and measurement devices. In the device-independent scenario the systems and measurement-devices are modelled as black-boxes.

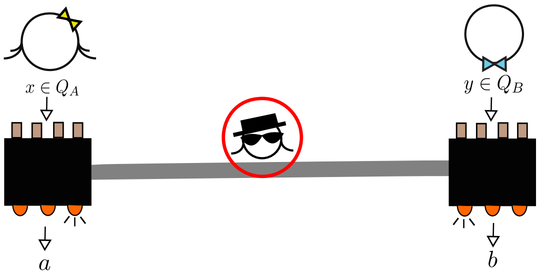

Figure 3: Device-independent scenario: the uncharacterized devices of Alice and Bob are treated as black boxes. The only relevant information is the statistics of inputs and outputs.

In the DI scenario, the only relevant information about the system is the statistics of inputs and outputs $\{p(ab|xy)\}$, without assumptions on how these statistics were generated. Security is then going to be inferred by the violation of a Bell inequality.

The simplest Bell inequality is the CHSH-inequality [29], in which Alice and Bob have each two inputs with two possible outputs. The CHSH inequality reads:

$$\beta = \langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle \leq 2 \tag{103}$$

for

$$\langle A_xB_y\rangle = p(a=b|xy) - p(a\neq b|xy). \tag{104}$$

Interestingly, quantum mechanics can violate this inequality up to the value $2\sqrt{2}$.

The idea of device-independent QKD arouse from the E91 protocol [30], which proposed to use a test of the CHSH inequality in order to check for the presence of an eavesdropper.

The simplest DIQKD protocol uses the CHSH inequality for the security test:

Protocol 1 DIQKD protocol

```
for $i = 1$ to $n$ do
    A source distributes a quantum state to Alice and Bob.
    Alice chooses $x \in \{0, 1\}$, performs the corresponding measurement, and records the outcome $a$.
    Bob chooses $y \in \{0, 1, 2\}$, performs the corresponding measurement, and records the outcome $b$.
end for
Sifting: Alice and Bob publicly announce their choices of basis, $x$ and $y$, and compare them. They discard the rounds in which Alice and Bob chose $x = 1$ and $y = 2$.
Parameter estimation: Using the rounds in $x \in \{0, 1\}$ and $y \in \{0, 1\}$, Alice and Bob estimate the Bell violation $\beta$. And using some of the rounds in which $x = 0$ and $y = 2$, they estimate the QBER $Q$. The other rounds form their raw keys.
Information reconciliation: Alice and Bob choose a classical error correcting code and communicate over the authenticated public channel in order to correct their string of bits. At the end of this phase Alice and Bob should hold the same bit-string.
Privacy amplification: Alice and Bob use an extractor on the previously established strings to generate shorter but completely secret strings of $\ell$ bits, which are their final keys $K_A$ and $K_B$.
```

8.1 DIQKD against collective attacks

If we are restricted to collective attacks, we have seen that the Asymptotic equipartition property (Theorem 4.1) reduces the problem of computing the asymptotic key rate to the problem of bounding the entropies:

$$H(A|E)_\rho \text{ and } H(A|B)_\rho. \tag{105}$$

Remark: In the DI scenario, the assumption of collective attacks also constraints the devices, who are then supposed to behave in the same way in each round of the protocol. In particular, the devices need to be memoryless.

The leakage of information reconciliation is straightforwardly determined by the estimated QBER Q:

$$H(A|B)_\rho = h(Q). \tag{106}$$

It only remains to estimate $H(A|E)_\rho$ given the observed violation β:

$$\inf_{\rho \in \mathcal{S}_\beta} H(A|E)_\rho. \tag{107}$$

The problem we face here is that in the DI scenario we don't even make a assumption about the dimension of the underlying state, which makes the optimization seemly intractable.

For the CHSH inequality this problem was solved in [31, 32]. Here we report the main result:

Theorem 8.1. *For a state ρ_{AB} that achieves a violation β for the CHSH inequality, it holds that*

$$H(A|E)_\rho \geq 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\left(\frac{\beta}{2}\right)^2 - 1}\right). \tag{108}$$

So finally we obtain the asymptotic key rate for the DIQKD protocol based on the CHSH inequality

$$r_\infty = 1 - h\left(\frac{1}{2} + \frac{1}{2}\sqrt{\left(\frac{\beta}{2}\right)^2 - 1}\right) - h(Q). \tag{109}$$

Exercise 4. *As a benchmark, consider again a noisy implementation where the source distributes a maximally entangled that undergoes depolarizing noise, see eq* (85)*. If the devices perform the measurements that maximize the CHSH violation for the maximally entangled state Φ^+, then the parameters of interest relate to the noise parameter ν by*

$$Q = \frac{\nu}{2} \quad \textit{and} \quad \beta = 2\sqrt{2}(1 - \nu). \tag{110}$$

What is the maximum amount of noise ν that an implementation of the DIQKD protocol with this setup can tolerate? How does that translate into the value of the QBER Q?

The CHSH inequality is significantly simpler than other Bell inequalities. Due to the fact that the CHSH inequality has only two binary inputs per party, a strong result [33, 34] states that the description of any realization of a CHSH experiment can be decomposed into subspaces of dimension two, where projective measurements are performed in each subspace. This significantly simplifies the optimization (107) which can then be restricted to qubit states.

For other Bell inequalities, one can in general use the relation

$$H(A|E)_\rho \geq H_{\min}(A|E)_\rho. \tag{111}$$

to obtain lower bounds. Indeed the conditional min-entropy can be computed as a function of the Bell violation by semi-definite programming [35]. The idea is that in order to estimate the min-entropy one can upper bound the guessing probability, p_{guess} (see Eq. (23)), of the eavesdropper. The problem of bounding the guessing probability can then be expressed as an optimization over probability distributions, which is exactly the information available in the device-independent scenario. As shown in Ref. [35], for any Bell inequality, an upper bound on the p_{guess} can be obtained by semidefinite programming making use of the NPA-hierarchy [36].

8.2 DIQKD against coherent attacks

In standard QKD, we have seen that the post-selection technique, Theorem 5.1, allows to extend the proofs against collective attacks to coherent attacks for protocols that present some symmetry. The price to pay is an overhead term in the security parameter that depends on the dimension of the underlying system. In the DI scenario, we do not make assumptions on the dimension of the underlying system. Moreover, symmetry of the protocol is not guaranteed, as we do not know the behaviour of the measurement devices. Therefore, de Finetti techniques cannot be used to straightforwardly extend the security proofs against collective attacks to coherent attacks in the device-independent scenario.

This problem was overcome by a recently developed technique called the entropy accumulation theorem (EAT) [37, 38]. When applied to DIQKD, the EAT theorem can be summarized as follows.

Theorem 8.2 (EAT applied to QKD)**.** *For an event Ω that happens with probability p_Ω, it holds that*

$$H^{\epsilon}_{\min}(A_1^n|E)_{\rho_{|\Omega}} > n f_{\min}(\Omega) - \mathcal{O}(\sqrt{n}), \tag{112}$$

and $f_{\min}(\Omega)$ is a convex function such that

$$f_{\min}(\Omega) \leq \inf_{\sigma \in \mathcal{S}_{(\Omega)}} H(A|E)_\sigma, \tag{113}$$

where $\mathcal{S}_{(\Omega)}$ is the set of quantum states that lead to the event Ω. Moreover the explicit form of the $\mathcal{O}(\sqrt{n})$ depends on p_Ω, ϵ,$\|\nabla f_{\min}\|_\infty$ and the dimension of classical registers A_1^n and B_1^n.

We refer the reader to [37, 38] for more formal details.

Analogous to the AEP, the entropy accumulation theorem allows us to break the entropy of the string of bits conditioned into some event Ω (e.g., a certain violation β of the CHSH inequality) into the entropy of a single round. Note, however, that this single-round entropy does not refer to the entropy of the real state of the protocol at each round. It is minimized over hypothetical states that would achieve the observed violation.

Remark: It is important to remark that a crucial assumption in the EAT [37, 38] is that some of the variables of interested satisfy what is called the Markov condition. This is the case for QKD protocols performed sequentially. For definition and discussion of the implications of the Markov condition, see [37].

References

[1] 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, 1984, pp. 175 – 179.

[2] S. Wiesner, "Conjugate coding," SIGACT News, vol. 15, no. 1, p. 78–88, Jan. 1983. [Online]. Available: https://doi.org/10.1145/1008908.1008920

[3] H.-K. Lo, H. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," Journal of Cryptology, vol. 18, no. 2, pp. 133–165, 2005. [Online]. Available: https://doi.org/10.1007/s00145-004-0142-y

[4] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," Phys. Rev. Lett., vol. 68, pp. 557–559, Feb 1992. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.68.557

[5] P. W. Shor and J. Preskill, "Simple proof of security of the bb84 quantum key distribution protocol," Phys. Rev. Lett., vol. 85, pp. 441–444, Jul 2000. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.85.441

[6] B. Kraus, N. Gisin, and R. Renner, "Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication," Phys. Rev. Lett., vol. 95, p. 080501, Aug 2005. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.95.080501

[7] R. Renner, "Security of quantum key distribution," International Journal of Quantum Information, vol. 06, no. 01, pp. 1–127, 2008.

[8] M. Tomamichel, "Quantum information processing with finite resources," SpringerBriefs in Mathematical Physics, 2016, [Theorem refs based on arXiv:1504.00233]. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-21891-5

[9] I. Devetak and A. Winter, "Classical data compression with quantum side information," Phys. Rev. A, vol. 68, p. 042301, Oct 2003. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.68.042301

[10] M. Tomamichel, "A framework for non-asymptotic quantum information theory," 2012. [Online]. Available: https://arxiv.org/abs/1203.2142

[11] R. Konig, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," IEEE Transactions on Information Theory, vol. 55, no. 9, pp. 4337–4347, Sep. 2009.

[12] J. Carter and M. N. Wegman, "Universal classes of hash functions," Journal of Computer and System Sciences, vol. 18, no. 2, pp. 143–154, 1979. [Online]. Available: https://www.sciencedirect.com/science/article/pii/0022000079900448

[13] M. Tomamichel and A. Leverrier, "A largely self-contained and complete security proof for quantum key distribution," Quantum, vol. 1, p. 14, 2017. [Online]. Available: https://doi.org/10.22331/q-2017-07-14-14

[14] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in Advances in Cryptology — EUROCRYPT '93, T. Helleseth, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 410–423.

[15] R. Renner and S. Wolf, "Simple and tight bounds for information reconciliation and privacy amplification," in Advances in Cryptology - ASIACRYPT 2005, B. Roy, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 199–216.

[16] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," Proc. R. Soc. A, vol. 461, January 2005. [Online]. Available: https://doi.org/10.1098/rspa.2004.1372

[17] M. Tomamichel, R. Colbeck, and R. Renner, "A fully quantum asymptotic equipartition property," IEEE Transactions on Information Theory, vol. 55, no. 12, pp. 5840–5847, 2009.

[18] R. Renner, "Symmetry of large physical systems implies independence of subsystems," Nature Physics, vol. 3, no. 9, p. 645–649, Jul 2007. [Online]. Available: http://dx.doi.org/10.1038/nphys684

[19] M. Christandl, R. König, and R. Renner, "Postselection technique for quantum channels with applications to quantum cryptography," Phys. Rev. Lett., vol. 102, p. 020504, Jan 2009. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.102.020504

[20] P. Belzig, "Studying stabilizer de finetti theorems and possible applications in quantum information processing," Master thesis, 2020.

[21] M. Tomamichel and R. Renner, "Uncertainty relation for smooth entropies," Phys. Rev. Lett., vol. 106, p. 110506, Mar 2011. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.106.110506

[22] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," Nature Communications, vol. 3, p. 634, 2012. [Online]. Available: https://doi.org/10.1038/ncomms1631

[23] D. Bruß, “Optimal eavesdropping in quantum cryptography with six states,” Phys. Rev. Lett., vol. 81, pp. 3018–3021, Oct 1998. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.81.3018

[24] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, “Security of quantum key distribution with imperfect devices,” Quantum Info. Comput., vol. 4, no. 5, p. 325–360, Sep. 2004.

[25] H.-K. Lo, X. Ma, and K. Chen, “Decoy state quantum key distribution,” Phys. Rev. Lett., vol. 94, p. 230504, Jun 2005. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.94.230504

[26] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, “Practical decoy state for quantum key distribution,” Phys. Rev. A, vol. 72, p. 012326, Jul 2005. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.72.012326

[27] F. Xu, M. Curty, B. Qi, and H. Lo, “Measurement-device-independent quantum cryptography,” IEEE Journal of Selected Topics in Quantum Electronics, vol. 21, no. 3, pp. 148–158, 2015.

[28] H.-K. Lo, M. Curty, and B. Qi, “Measurement-device-independent quantum key distribution,” Phys. Rev. Lett., vol. 108, p. 130503, Mar 2012. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.108.130503

[29] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, “Proposed experiment to test local hidden-variable theories,” Phys. Rev. Lett., vol. 23, pp. 880–884, Oct 1969. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.23.880

[30] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” Phys. Rev. Lett., vol. 67, pp. 661–663, 1991. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.67.661

[31] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, “Device-independent security of quantum cryptography against collective attacks,” Phys. Rev. Lett., vol. 98, p. 230501, 2007. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.98.230501

[32] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, “Device-independent quantum key distribution secure against collective attacks,” New Journal of Physics, vol. 11, no. 4, p. 045021, 2009. [Online]. Available: http://stacks.iop.org/1367-2630/11/i=4/a=045021

[33] L. Masanes, “Asymptotic violation of Bell inequalities and distillability,” Phys. Rev. Lett., vol. 97, p. 050503, 2006. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.97.050503

[34] B. Tsirelson, “Some results and problems on quantum Bell-type inequalities,” Hadronic Journal Supplement, vol. 8, pp. 329–345, 1993. [Online]. Available: http://www.tau.ac.il/~tsirel/download/hadron.html

[35] L. Masanes, S. Pironio, and A. Acín, “Secure device-independent quantum key distribution with causally independent measurement devices,” Nature Communications, vol. 2, p. 238, 2011.

[36] M. Navascues, S. Pironio, and A. Acin, “A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations,” New Journal of Physics, vol. 10, no. 7, p. 073013, jul 2008.

[37] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, “Practical device-independent quantum cryptography via entropy accumulation,” Nature Communications, vol. 9, p. 459, 2018. [Online]. Available: https://doi.org/10.1038/s41467-017-02307-4

[38] F. Dupuis, O. Fawzi, and R. Renner, “Entropy accumulation,” 2016, arXiv:quant-ph/1607.01796.