A Rigorous and Complete Proof of the Security of Quantum Key Distribution

Marco Tomamichel[*], Anthony Leverrier[†]

Introduction: Quantum Key Distribution (QKD) is a cryptographic task that allows two distant parties, Alice and Bob, to communicate securely over an untrusted channel, provided they have access to an authenticated classical channel. The first QKD protocol, BB84, appeared more than three decades ago [2] and the last 30 years have witnessed staggering experimental advances, making QKD the first quantum information technology. This parallels the development of more complete security proofs, first given in the asymptotic limit of infinitely long keys [6, 11, 7] and more recently in the composable security framework for finite keys [9]. While the former results are of great theoretical importance, only the more recent security proofs that are valid for finite keys can claim practical relevance.

Let us for the moment focus on entanglement-based QKD, as first proposed in [4]. From a mathematical point of view, an entanglement-based QKD protocol is a completely positive trace-preserving (CPTP) map composed of local operations and classical communication (LOCC) that takes a bipartite state ρ_{AB} as an input and returns to Alice and Bob two classical binary strings, the keys, ideally identical and independent of the transcript produced by the protocol. Proving the security of a such a QKD protocol therefore amounts to establishing that this map is indistinguishable from an ideal map that either outputs random identical keys or aborts, for any possible quantum input, potentially entangled with a reference system held by an eavesdropper — it is a purely mathematical question.

The Problem: Surveying the current literature on the topic, we were not able to find a security proof for any QKD protocol that satisfies the following three very stringent criteria:

1. The protocol is able to extract a composably secure key for reasonable parameters (i.e. realistic noise level, keys of a length that can be handled with state-of-the-art computer hardware).

2. The protocol is completely specified and all aspects of it are formalized, including all the randomness that is required and all the transcripts that are produced.

3. All the assumptions on the devices used in the protocol are fully formalized.

As mentioned above, the early asymptotic proofs fail with Point 1. Moreover, while Renner's analysis [9] gives bounds for finite keys, these are not sufficient to pass Point 1 either since the bounds are not good enough for realistic key lengths.[1] Furthermore, our requirements in Point 2 are very stringent and we are not aware of any security proof that has met this level of rigor, except arguably Renner's thesis [9]. More recent security proofs by one of the present authors [12] and Tsurumaru and Hayashi [5] satisfy Point 1, but they are not fully formalized and thus do not satisfy Point 2.[2] Point 3 hinges on Point 2 and can be avoided using device-independent protocols, which will not be discussed here.

[*] School of Physics, University of Sydney, NSW 2006, Australia

[†] Inria, EPI SECRET, B.P. 105, 78153 Le Chesnay Cedex, France

[1] Unfortunately, de Finetti reductions often do not provide good bounds in practice and at least 10^5 or 10^6 uses of the quantum channel are typically required for the key rate to effectively become nonzero.

[2] For example, a small flaw in the formalization of the protocol in [12] has recently been pointed out by Pfister *et al.* in unpublished work. While this does not suggest that the security proof in [12] is inherently wrong, it is a stark reminder that Point 2 is often not taken seriously enough.

It is in fact common in much of the present literature to fully formalize some aspects of a security proof while keeping other aspects vague and informal — and this has lead to various misconceptions. For example, it is often argued that collective attacks are optimal using symmetry and de-Finetti arguments [10, 3]. To get such symmetry it is at some point or another used that measurements are performed in a random basis or that a random subset of raw key bits are used for parameter estimation. However, complete security proofs also must allow for the protocol to abort in case certain thresholds are not met, and one is then left to analyze the state of the system conditioned on the fact that the protocol does not abort. However, since the abort event is dependent on the random seed used to choose the basis and subset, conditioned on not aborting these seeds are no longer independent of the state of the system. Hence, many simple arguments based on symmetry or independent randomness simply do not go trough without modification when the security proof is put under a microscope.

Our Contribution: In the present paper, we give a fully rigorous and self-contained security proof for QKD that satisfies all the above conditions. The proof is based on the security proof in [12] and uses an entropic uncertainty relation as its main ingredient, but our analysis is more rigorous and consequently a few additional technical results are needed. The resulting key rate is much better than the one achieved using the exponential de Finetti theorem in [9]. To the best our knowledge, this constitutes the most detailed and rigorous security proof of QKD so far. We also believe that our proof is more accessible than others since understanding it does not require prior knowledge of various tricks and security reductions[3], it is a purely mathematical argument that we provide in the attached technical material.

We first describe and analyze a simple entanglement-based QKD protocol, reminiscent of [1] (outlined in Table 1), before moving on to a more realistic 'prepare and measure' BB84 protocol.

Entanglement-Based Protocol: The protocol is parametrized as follows. Let $k, n \in \mathbb{N}$. Here k and n are the size (in bits) of the raw key used for parameter estimation and key extraction, respectively. Moreover, let $\delta \in (0, \frac{1}{2})$ be the tolerated error rate. Also define $m := n + k$ as the total length of the raw key, and $\Pi_{m,k} := \{\pi \subset [m] : |\pi| = k\}$, the set of subsets of $[m]$ of size k.

$(K_A, K_B, S, C, F) = \texttt{qkd\_simple}_{k,n,\delta,\mathrm{ec},\mathrm{pa}}\ (\rho_{AB})$:

Input: Alice and Bob are given a state ρ_{AB}, where $A = A_{[m]}$ and $B = B_{[m]}$ are comprised of m quantum systems.

Randomization: They agree on a random string $\Phi \in \{0,1\}^m$, a random subset $\Pi \in \Pi_{m,k}$, and random hash functions $H_{\mathrm{ec}} \in \mathcal{H}_{\mathrm{ec}}$ as well as $H_{\mathrm{pa}} \in \mathcal{H}_{\mathrm{pa}}$. The corresponding uniformly random seeds are denoted $S = (S^{\Phi}, S^{\Pi}, S^{H_{\mathrm{ec}}}, S^{H_{\mathrm{pa}}})$.

Measurement: Alice and Bob measure the m quantum systems with the setting Φ. They store the binary measurement outcomes in two strings, the *raw keys*. These are denoted (X, V) and (Y, W) for Alice and Bob, respectively. Here V, W are of length k and correspond to the indices in Π, whereas X, Y of length n correspond to indices not in Π.

Parameter Estimation: Alice sends V to Bob, the transcript is denoted C^V. Bob compares V and W. If the fraction of errors exceeds δ, Bob sets the flag $F^{\mathrm{pe}} =$ '$\perp$' and they abort. Otherwise he sets $F^{\mathrm{pe}} =$ '$\not\perp$' and they proceed.

Error Correction: Alice sends the syndrome $Z = \mathrm{synd}(X)$ to Bob, with transcript C^Z. Bob computes $\hat{X} = \mathrm{corr}(Y, Z)$. Alice computes the hash $T = H_{\mathrm{ec}}(X)$ of length t and sends it to Bob, with transcript C^T. Bob computes $H_{\mathrm{ec}}(\hat{X})$. If it differs from T, he sets the flag $F^{\mathrm{ec}} =$ '$\perp$' and they abort the protocol. Otherwise he sets $F^{\mathrm{ec}} =$ '$\not\perp$' and they proceed.

Privacy Amplification: They compute keys $K_A = H_{\mathrm{pa}}(X)$ and $K_B = H_{\mathrm{pa}}(\hat{X})$ of length ℓ.

Output: The output of the protocol consists of the keys K_A and K_B, the seeds $S = (S^{\Phi}, S^{\Pi}, S^{H_{\mathrm{ec}}}, S^{H_{\mathrm{pa}}})$, the transcript $C = (C^V, C^Z, C^H)$ and the flags $F = (F^{\mathrm{pe}}, F^{\mathrm{ec}})$. In case of abort, we assume that all registers are initialized to a predetermined value.

Table 1: Simple QKD Protocol.

Fix an error correcting scheme described by a quintuple $\mathrm{ec} = \{r, t, \mathrm{synd}, \mathrm{corr}, \mathcal{H}_{\mathrm{ec}}\}$. Here, $r \in \mathbb{N}$ is the length (in bits) of the error correction syndrome, and $t \in \mathbb{N}$ is then length (in bits) of the hash used for verification. Moreover, synd and corr are functions of the form $\mathrm{synd} : \{0,1\}^n \to \{0,1\}^r$ and $\mathrm{corr} : \{0,1\}^n \times \{0,1\}^r \to \{0,1\}^n$ used to compute the error syndrome and calculate the corrected

[3] . . . which are also sometimes proved in a different context than the one they are used in . . .

$(K_A, K_B, S, C, F) = \texttt{qkd\_ideal}_{k,n,\delta,\text{ec},\text{pa}}\ (\rho_{AB})$:

Run protocol: Set $(K_A, K_B, S, C, F) = \texttt{qkd\_simple}_{k,n,\delta,\text{ec},\text{pa}}(\rho_{AB})$.

Output: If $F^{\text{pe}} = F^{\text{ec}} =$ '$\not\perp$', then replace K_A and K_B by an independent and uniformly distributed random variable K, i.e. set $K_A = K_B = K$.

Table 2: Ideal QKD Protocol.

string, respectively. We do not need to assume anything about the structure of this code.[4] Finally, $\mathcal{H}_{\text{ec}} := \left\{h_{\text{ec}} : \{0,1\}^n \to \{0,1\}^t\right\}$ is a universal$_2$ family of hash functions.

Finally, privacy amplification is characterized by a couple $\text{pa} = \{\ell, \mathcal{H}_{\text{pa}}\}$, where $\ell \in \mathbb{N}$ with $\ell \le n$ is the length (in bits) of the extracted key and $\mathcal{H}_{\text{pa}} := \left\{h_{\text{pa}} : \{0,1\}^n \to \{0,1\}^\ell\right\}$ is a universal$_2$ family of hash functions.

Security: The security proof of the simple protocol is done in the composable security framework (see, e.g., [8]), and essentially consists of bounding the diamond distance between the protocol and an *ideal protocol* defined in Table 2. We show that the action of the map $\texttt{qkd\_simple}_{k,n,\delta,\text{ec},\text{pa}}$ is indistinguishable from the action of the map $\texttt{qkd\_ideal}_{k,n,\delta,\text{ec},\text{pa}}$ prescribed in Table 2 when the protocol parameters satisfy certain natural constraints. In the technical supplement we give an upper bound on

$$\Delta_{k,n,\delta,\text{ec},\text{pa}} := \sup_{\rho_{ABE}} \frac{1}{2}\left\|\texttt{qkd\_simple}_{k,n,\delta,\text{ec},\text{pa}}(\rho_{ABE}) - \texttt{qkd\_ideal}_{k,n,\delta,\text{ec},\text{pa}}(\rho_{ABE})\right\|_1 \tag{1}$$

in terms of the protocol parameters. This bound is our main technical contribution.

Prepare-and-Measure Protocol: We prove the security of a more realistic 'prepare and measure' protocol in the attached technical supplement by reducing it to the above entanglement-based protocol and specify all the assumptions required for this transformation.

References

[1] C. Bennett, G. Brassard, and N. Mermin. Quantum Cryptography Without Bells Theorem. *Phys. Rev. Lett.*, 68(5):557–559, 1992. DOI: 10.1103/PhysRevLett.68.557.

[2] C. H. Bennett and G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process.*, pages 175–179, Bangalore, 1984. IEEE.

[3] M. Christandl, R. König, and R. Renner. Postselection Technique for Quantum Channels with Applications to Quantum Cryptography. *Phys. Rev. Lett.*, 102(2), 2009. DOI: 10.1103/PhysRevLett.102.020504.

[4] A. K. Ekert. Quantum Cryptography Based on Bell's Theorem. *Phys. Rev. Lett.*, 67(6):661–663, 1991. DOI: 10.1103/PhysRevLett.67.661.

[5] M. Hayashi and T. Tsurumaru. Concise and Tight Security Analysis of the Bennett-Brassard 1984 Protocol with Finite Key Lengths. *New J. Phys.*, 14(9):093014, 2012. DOI: 10.1088/1367-2630/14/9/093014.

[6] H.-K. Lo and H. F. Chau. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science*, 283(5410):2050–2056, 1999. DOI: 10.1126/science.283.5410.2050.

[7] D. Mayers. Unconditional Security in Quantum Cryptography. *J. ACM*, 48(3):351–406, 2001.

[8] C. Portmann and R. Renner. Cryptographic security of quantum key distribution. 2014. arXiv: 1409.3525.

[9] R. Renner. *Security of Quantum Key Distribution.* PhD thesis, ETH Zurich, 2005. arXiv: quant-ph/0512258.

[10] R. Renner. Symmetry of Large Physical Systems Implies Independence of Subsystems. *Nat. Phys.*, 3(9):645–649, 2007. DOI: 10.1038/nphys684.

[11] P. W. Shor and J. Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.*, 85(2):441–444, 2000. DOI: 10.1103/PhysRevLett.85.441.

[12] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight Finite-Key Analysis for Quantum Cryptography. *Nat. Commun.*, 3:634, 2012. DOI: 10.1038/ncomms1631.

[4] For example, synd could be a linear code described by an $r \times n$ parity check matrix H such that $\text{synd}(x) = Hx$. Moreover, corr can be any decoder, for example the (optimal) maximum likelihood decoder, but also more practical suboptimal iterative decoders.

A Rigorous and Complete Proof of the Security of Quantum Key Distribution

Marco Tomamichel[*], Anthony Leverrier[†]

April 28, 2015

Abstract

The goal of this work is to provide a self-contained, rigorous proof of the security of quantum key distribution. Our presentation differs from previous work in that we are careful to model all the randomness that is used throughout the protocol and take care of all the transcripts of the communication over the public channel.

Contents

[*] School of Physics, University of Sydney, NSW 2006, Australia
[†] Inria, EPI SECRET, B.P. 105, 78153 Le Chesnay Cedex, France

Nomenclature

$[M]$	Set $\{1, 2, \ldots, M\}$
$\bar{c}$	Parameter quantifying the overall quality of the measurements
δ	Threshold for the parameter estimation test
ℓ	Length of the final key
$\mathcal{E}_f$	CPTP map associated to the classical function f
$\mathcal{H}_{\mathrm{ec}}$	Universal$_2$ family of hash functions used in the error correcting scheme
$\mathcal{H}_{\mathrm{pa}}$	Universal$_2$ family of hash functions used in the privacy amplification scheme
$\mathcal{N}_{A\to B}$	Quantum channel between Alice and Bob in the Prepare and Measure version
$\not\perp$	Passing symbol for the various tests
Ω	Subset of $[M]$ for which Bob obtains a conclusive measurement result
ω	Final output of the protocol
$\perp$	Abort symbol
ρ	Quantum state before any measurement took place
Σ	Subset of m indices for which Alice and Bob's settings agree, and where Bob obtained a conclusive measurement outcome
σ	Quantum state once Alice and Bob's quantum registers have been entirely measured
τ	Quantum state after the registers used for parameter estimation have been measured
A	Alice's initial quantum system
B	Bob's initial quantum system
C	Register containing all the transcripts
C^V	Transcript corresponding to register V
c_i	Parameter quantifying the quality of the measurement on register i
E	Eve's quantum memory
F	Register corresponding to all the flags: $F = (F^{\mathrm{pe}}, F^{\mathrm{ec}})$ for the idealized protocol, and $F = (F^{\mathrm{sift}}, F^{\mathrm{pe}}, F^{\mathrm{ec}})$ for the Prepare and Measure version
F^{ec}	Flag for the error correction test
F^{pe}	Flag for the parameter estimation test
F^{sift}	Flag for the sifting procedure in the Prepare and Measure version
h_{ec}	Hash function used for the error correction test
h_{pa}	Hash function used for the privacy amplification
k	Length of the raw key used for parameter estimation
K_A	Register for Alice's final key
K_B	Register for Bob's final key
M	Number of states sent by Alice in the Prepare and Measure version
m	Number of states measured by Alice and Bob in the idealized version
$M_{A_i}^{\phi,x}$	Measurement operator acting on register A_i with setting ϕ and outcome x
n	Length of the raw key used for key distillation
R	Register for Alice's raw key in the Prepare and Measure Version

r	Length of the error correction syndrome
S	Register corresponding to all the seeds $S = (S^{\Phi}, S^{\Pi}, S^{\Xi}, S^{\Theta}, S^{H_{\mathrm{pe}}}, S^{H_{\mathrm{ec}}})$ in the idealized protocol, or $S = (S^{\Phi_A}, S^{\Phi_B}, S^{\Pi}, S^{\Xi}, S^{\Theta} S^{H_{\mathrm{pe}}}, S^{H_{\mathrm{ec}}})$ in the Prepare and Measure version
S^{Φ}	Seed for the choice of the measurement bases in the idealized protocol
S^{Π}	Seed for the choice of the random subset $\pi \in \Pi_{m,k}$ used for parameter estimation
S^{Θ}	Seed for the choice of the measurement bases for the subsystems used for key distillation
S^{Ξ}	Seed for the choice of the measurement bases for the subsystems used for parameter estimation
S^{Φ_A}	Seed for the choice of Alice's measurement bases in the Prepare and Measure version
S^{Φ_B}	Seed for the choice of Bob's measurement bases in the Prepare and Measure version
$S^{H_{\mathrm{ec}}}$	Seed for the choice of the hash function used in the error correction test
$S^{H_{\mathrm{pe}}}$	Seed for the choice of the hash function used in the parameter estimation test
T	Register for Bob's measurement results in the Prepare and Measure Version
t	Length of the hash used for verification in the error correcting scheme
V	Register for Alice's classical bits used for parameter estimation
W	Register for Bob's classical bits used for parameter estimation
X	Register for Alice's classical bits used for key distillation
Y	Register for Bob's classical bits used for key distillation
Z	Register for Alice's syndrome
corr	Function that calculate the corrected string
ec	Error correcting scheme
pa	Privacy amplification scheme
pe	Test function used in the parameter estimation step
ro	Reordering map used in the randomization step
synd	Function computing the error syndrome

1 Notation

We use $[n]$ to denote the set $\{1, 2, \ldots, n\}$ and use $A_{[n]}$ to denote a collection of separate quantum systems $A_1 A_2, \ldots, A_n$. Similarly, if the subscript is a subset of $[n]$, we just refer to the subsystems in the subset. We write $\mathcal{S}(A)$ to denote normalized states (positive semi-definite operators with unit trace) on A.

We model discrete random variables by quantum systems (called registers) with a fixed orthonormal basis. For example, let $x \in \mathcal{X}$ be a random variable with probability law $x \mapsto P_X(x)$. Then we write the corresponding quantum state as

$$\rho_X = \sum_{x \in \mathcal{X}} P_X(x) \, |x\rangle\langle x|_X \, , \tag{1}$$

where $\{|x\rangle\}_{x \in \mathcal{X}}$ is an orthonormal basis of the space X. Conversely, we write $\Pr_\rho[X = x] = P_X(x)$.

More generally, the classical register might be correlated with a quantum system A, and this is modeled using *classical-quantum (cq)* states:

$$\rho_{XA} = \sum_{x \in \mathcal{X}} P_X(x) \, |x\rangle\langle x|_X \otimes \rho_{A|X=x} \, , \tag{2}$$

where we use $\rho_{A|X=x}$ to denote the quantum state on A conditioned on the register X taking the value x. We also write $\Pr_\rho[X = x] = \mathrm{tr}\{|x\rangle\langle x|_X \, \rho_{XA}\} = P_X(x)$. This convention is extended to arbitrary events defined on a classical register X, i.e. if $\Omega : \mathcal{X} \to \{0, 1\}$ is an *event*, we write

$$\Pr_\rho[\Omega] = \sum_{x \in \mathcal{X}} P_x(x)\Omega(x) \quad \text{and} \quad \rho_{XA|\Omega} = \frac{1}{\Pr_\rho[\Omega]} \sum_{x \in \mathcal{X}} P_x(x)\Omega(x) \, |x\rangle\langle x|_X \otimes \rho_{A|X=x} \, . \tag{3}$$

In some occasions we will also write $\rho_{XA,\Omega} = \Pr_\rho[\Omega]\rho_{XA|\Omega}$, a state that is not normalized.

Let $f : \mathcal{X} \to \mathcal{Y}$ be a function acting on classical registers of a classical-quantum state. Then we denote by $\mathcal{E}_f : X \to XY$ the corresponding completely positive trace-preserving map

$$\mathcal{E}_f[\cdot] = \sum_{x \in \mathcal{X}} |f(x)\rangle_Y \, |x\rangle\langle x|_X \cdot |x\rangle\langle x|_X \, \langle f(x)|_Y \ . \tag{4}$$

Note that we defined the map such that the input register is kept intact.

A *generalized measurement* on A is a set of linear operators $\{E_A^x\}_{x \in \mathcal{X}}$ such that

$$\sum_{x \in \mathcal{X}} (E_A^x)^\dagger (E_A^x) = 1_A \,, \tag{5}$$

where 1_A denotes the identity operator on A.

Part I

Entanglement-Based Protocol

2 The Entanglement-Based Protocol

We first focus on a very simple and unrealistic QKD protocol, for which we provide a complete security analysis. We first give a rough overview of the protocol in Table 1, and the detailed mathematical description follows in Section 2.3.

2.1 Overview

The protocol is parametrized as follows. Let $k, n \in \mathbb{N}$. Here k and n are the size (in bits) of the raw key used for parameter estimation and key extraction, respectively. Moreover, let $\delta \in (0, \frac{1}{2})$ be the tolerated error rate. Also define $m := n + k$ as the total length of the raw key, and $\Pi_{m,k} := \{\pi \subset [m] : |\pi| = k\}$, the set of subsets of $[m]$ of size k.

Fix an error correcting scheme described by a quintuple $\mathrm{ec} = \{r, t, \mathrm{synd}, \mathrm{corr}, \mathcal{H}_{\mathrm{ec}}\}$. Here, $r \in \mathbb{N}$ is the length (in bits) of the error correction syndrome, and $t \in \mathbb{N}$ is then length (in bits) of the hash used for verification. Moreover, synd and corr are functions of the form $\mathrm{synd} : \{0,1\}^n \to \{0,1\}^r$ and $\mathrm{corr} : \{0,1\}^n \times \{0,1\}^r \to \{0,1\}^n$ used to compute the error syndrome and calculate the corrected string, respectively. We do not need to assume anything about the structure of this code.[1] Finally, $\mathcal{H}_{\mathrm{ec}} := \left\{ h_{\mathrm{ec}} : \{0,1\}^n \to \{0,1\}^t \right\}$ is a universal$_2$ family of hash functions (see Section 4.1.3).

Finally, privacy amplification is characterized by a couple $\mathrm{pa} = \{\ell, \mathcal{H}_{\mathrm{pa}}\}$, where $\ell \in \mathbb{N}$ with $\ell \leq n$ is the length (in bits) of the extracted key and $\mathcal{H}_{\mathrm{pa}} := \left\{ h_{\mathrm{pa}} : \{0,1\}^n \to \{0,1\}^\ell \right\}$ is a universal$_2$ family of hash functions (see Section 4.1.3).

This allows us to define a family of protocols $\texttt{qkd\_simple}_{k,n,\delta,\mathrm{ec},\mathrm{pa}}$ in Table 1. We note that such a protocol is simply a completely positive trace-preserving map.

2.2 Measurement Devices

We model Alice's measurements on subsystem A_i for measurement setting $\phi \in \{0,1\}$ by a binary generalized measurement $\{M_{A_i}^{\phi,x}\}_{x \in \{0,1\}}$. Analogously, Bob's measurements on subsystem B_i is a binary generalized measurement $\{M_{B_i}^{\phi,y}\}_{y \in \{0,1\}}$.

[1] For example, ec_A could be a linear code described by an $r \times n$ parity check matrix H such that $\mathrm{ec}_A(x) = Hx$. Moreover, ec_B can be any decoder, for example the (optimal) maximum likelihood decoder, but also more practical suboptimal iterative decoders.

$(K_A, K_B, S, C, F) = \texttt{qkd\_simple}_{k,n,\delta,\mathrm{ec},\mathrm{pa}}\ (\rho_{AB})$:

Input: Alice and Bob are given a state ρ_{AB}, where $A = A_{[m]}$ and $B = B_{[m]}$ are comprised of m quantum systems.

Randomization: They agree on a random string $\Phi \in \{0,1\}^m$, a random subset $\Pi \in \Pi_{m,k}$, and random hash functions $H_{\mathrm{ec}} \in \mathcal{H}_{\mathrm{ec}}$ as well as $H_{\mathrm{pa}} \in \mathcal{H}_{\mathrm{pa}}$. The corresponding uniformly random seeds are denoted $S = (S^{\Phi}, S^{\Pi}, S^{H_{\mathrm{ec}}}, S^{H_{\mathrm{pa}}})$.

Measurement: Alice and Bob measure the m quantum systems with the setting Φ. They store the binary measurement outcomes in two strings, the *raw keys*. These are denoted (X, V) and (Y, W) for Alice and Bob, respectively. Here V, W are of length k and correspond to the indices in Π, whereas X, Y of length n correspond to indices not in Π.

Parameter Estimation: Alice sends V to Bob, the transcript is denoted C^V. Bob compares V and W. If the fraction of errors exceeds δ, Bob sets the flag $F^{\mathrm{pe}} =$ '$\perp$' and they abort. Otherwise he sets $F^{\mathrm{pe}} =$ '$\not\perp$' and they proceed.

Error Correction: Alice sends the syndrome $Z = \mathrm{synd}(X)$ to Bob, with transcript C^Z. Bob computes $\hat{X} = \mathrm{corr}(Y, Z)$.

Alice computes the hash $T = H_{\mathrm{ec}}(X)$ of length t and sends it to Bob, with transcript C^T. Bob computes $H_{\mathrm{ec}}(\hat{X})$. If it differs from T, he sets the flag $F^{\mathrm{ec}} =$ '$\perp$' and they abort the protocol. Otherwise he sets $F^{\mathrm{ec}} =$ '$\not\perp$' and they proceed.

Privacy Amplification: They compute keys $K_A = H_{\mathrm{pa}}(X)$ and $K_B = H_{\mathrm{pa}}(\hat{X})$ of length ℓ.

Output: The output of the protocol consists of the keys K_A and K_B, the seeds $S = (S^{\Phi}, S^{\Pi}, S^{H_{\mathrm{ec}}}, S^{H_{\mathrm{pa}}})$, the transcript $C = (C^V, C^Z, C^H)$ and the flags $F = (F^{\mathrm{pe}}, F^{\mathrm{ec}})$. In case of abort, we assume that all registers are initialized to a predetermined value.

Table 1: Simple QKD Protocol. The precise mathematical model is to be found in Section 2.3.

The exact description of the measurement devices will not be relevant for our derivations. However, the following parameter $\bar{c}$ of Alice's measurements is important:

$$c_i := \max_{\phi,x,z\in\{0,1\}} \left\| M_{A_i}^{\phi,x} \left(M_{A_i}^{\bar{\phi},z}\right)^{\dagger} \right\|_{\infty}^{2}, \quad \text{where} \quad \bar{\phi} = 1-\phi, \quad \text{and} \quad \bar{c} := \min_{\pi\in\Pi_{m,k}} \left(\prod_{i\in\bar{\pi}} c_i \right)^{\frac{1}{n}},$$

where the product is taking over the complement $\bar{\pi}$ of the set π in $[m]$.

2.3 Mathematical Model of the Protocol

Here we describe in detail the mathematical model underlying the protocol in Table 1.

Input: Alice and Bob are given a state ρ_{AB}, where $A = A_{[m]} = A_1 \otimes A_2 \otimes \ldots \otimes A_m$ consist of m quantum systems of arbitrary, finite dimension, $B = B_{[m]} = B_1 \otimes B_2 \otimes \ldots \otimes B_m$ consists of m quantum systems of arbitrary, finite dimension. Note that apart from the above structure, the state ρ_{AB} is fully general.

Randomization: We model the randomization by random seeds (uniform random variables), shared between Alice and Bob.

The first random variable is a random basis choice for each quantum system. This is modeled as a register S^Φ in the state

$$\rho_{S^\Phi} = \sum_{\phi \in \{0,1\}^m} \frac{1}{2^m} \, |\phi\rangle\langle\phi|_{S^\Phi} \,, \tag{6}$$

where $\{|\phi\}_{\phi\rangle \in \{0,1\}^m}$ is an orthonormal basis of the space S^Φ and $\phi = \phi_{[m]} = (\phi_1, \phi_2, \ldots, \phi_m)$ with $\phi_i \in \{0,1\}$. The total state at the beginning of the protocol is thus of the form $\rho_{ABE} \otimes \rho_{S^\Phi}$.

The seed for the choice of the random subset is denoted S^Π and is initially in the state

$$\rho_{S^\Pi} = \sum_{\pi \in \Pi_{m,k}} \frac{1}{\binom{m}{k}} \, |\pi\rangle\langle\pi|_{S^\Pi} \,, \tag{7}$$

where $\{|\pi\rangle\}_{\pi \in \Pi_{m,k}}$ is an orthonormal basis of the space S^Π. For any $\pi \in \Pi_{m,k}$, we denote its k elements by π_i, for $i \in [k]$ and we denote by $\bar{\pi}$ the complement of $\pi \in [m]$.

At this point we reorder the measurement settings in S^Φ into two parts: the settings to be used for measuring quantum systems in π will be stored in a register S^Ξ and the settings to be used for measuring the remaining n quantum systems in $\bar{\pi}$ will be stored in a register S^Θ. Formally, we consider the function

$$\mathrm{ro} : \{0,1\}^m \times \Pi_{m,k} \to \{0,1\}^k \times \{0,1\}^n, \quad (\phi, \pi) \mapsto (\phi_\pi, \phi_{\bar{\pi}}) \,. \tag{8}$$

Since S^Φ is uniformly random, the resulting state after applying this function and discarding S^Φ is of the form

$$\rho_{S^\Pi S^\Xi S^\Theta} = \mathrm{tr}_{S^\Phi} \left\{ \mathcal{E}_{\mathrm{ro}}(\rho_{S^\Phi} \otimes \rho_{S^\Pi}) \right\} = \rho_{S^\Pi} \otimes \rho_{S^\Xi} \otimes \rho_{S^\Theta} \,, \tag{9}$$

where the registers containing S^Ξ and S^Θ are again uniformly random:

$$\rho_{S^\Xi} = \sum_{\xi \in \{0,1\}^k} \frac{1}{2^k} \, |\xi\rangle\langle\xi|_{S^\Xi} \quad \text{and} \quad \rho_{S^\Theta} = \sum_{\theta \in \{0,1\}^n} \frac{1}{2^n} \, |\theta\rangle\langle\theta|_{S^\Theta} \tag{10}$$

for $\xi = \xi_{[k]} = (\xi_1, \xi_2, \ldots, \xi_k)$ and $\theta = \theta_{[n]} = (\theta_1, \theta_2, \ldots, \theta_n)$ with $\theta_i, \xi_i \in \{0,1\}$.

The choice of the hash function in the family $\mathcal{H}_{\mathrm{ec}} = \{h_{\mathrm{ec}} : \{0,1\}^n \to \{0,1\}^t\}$ and the choice of hash function in the family $\mathcal{H}_{\mathrm{pa}} = \{h_{\mathrm{pa}} : \{0,1\}^n \to \{0,1\}^t\}$ are modeled via random seeds

$$\rho_{S^{H_{\mathrm{ec}}}} = \sum_{h \in \mathcal{H}_{\mathrm{ec}}} \frac{1}{|\mathcal{H}_{\mathrm{ec}}|} |h\rangle\langle h|_{S^{H_{\mathrm{ec}}}} \qquad \text{and} \qquad \rho_{S^{H_{\mathrm{pa}}}} = \sum_{h \in \mathcal{H}_{\mathrm{pa}}} \frac{1}{|\mathcal{H}_{\mathrm{pa}}|} |h\rangle\langle h|_{S^{H_{\mathrm{pa}}}} . \tag{11}$$

Measurement: We split the measurement process into two parts, measuring the systems in the set π and $\bar{\pi}$ separately. This will be important for the security analysis later. The first measurement concerns the registers in π, which are used for parameter estimation. For any subset $\pi \in \Pi_{m,k}$, we define a completely positive trace-preserving map $\mathcal{M}^\pi_{A \to V|S^\Xi} : A_\pi S^\Xi \to V A_\pi S^\Xi$ where $V = V_{[k]} = V_1 \otimes V_2 \otimes \ldots V_k$ models k binary classical registers storing the measurement outcomes. The map is given by

$$\mathcal{M}^\pi_{A \to V|S^\Xi}(\cdot) = \sum_{\xi \in \{0,1\}^k} \sum_{v \in \{0,1\}^k} |v\rangle_V \left(M^{\xi,v}_{A_\pi} \otimes |\xi\rangle\langle\xi|_{S^\Xi} \right) \cdot \left(M^{\xi,v}_{A_\pi} \otimes |\xi\rangle\langle\xi|_{S^\Xi} \right)^\dagger \langle v|_V \,, \tag{12}$$

where $M^{\xi,v}_{A_\pi} := \bigotimes_{i \in [k]} M^{\xi_i, v_i}_{A_{\pi_i}}$. This map measures the k subsystems determined by π using the (random) measurement settings stored in the register S^Ξ. The results are stored in the classical register V, and the post-measurement state remains in the systems A_π.

Similarly, we define $\mathcal{M}^\pi_{B \to W|S^\Xi} : B_\pi S^\Xi \to W B_\pi S^\Xi$ as

$$\mathcal{M}^\pi_{B \to W|S^\Xi}(\cdot) = \sum_{\xi \in \{0,1\}^k} \sum_{w \in \{0,1\}^k} |w\rangle_W \left(M^{\xi,w}_{B_\pi} \otimes |\xi\rangle\langle\xi|_{S^\Xi} \right) \cdot \left(M^{\xi,w}_{B_\pi} \otimes |\xi\rangle\langle\xi|_{S^\Xi} \right)^\dagger \langle w|_W \,, \tag{13}$$

where $M_{B_\pi}^{\xi,w} := \bigotimes_{i\in[k]} M_{B_{\pi_i}}^{\xi_i,w_i}$. Clearly the two maps $\mathcal{M}_{A\to V|S^\Xi}^\pi$ and $\mathcal{M}_{B\to W|S^\Xi}^\pi$ commute and we write their concatenation as $\mathcal{M}_{A\to V|S^\Xi}^\pi \circ \mathcal{M}_{B\to W|S^\Xi}^\pi = \mathcal{M}_{B\to W|S^\Xi}^\pi \circ \mathcal{M}_{A\to V|S^\Xi}^\pi$.

So far we have considered π to be fixed. The full measurement for parameter estimation instead consults the register S^Π and is modeled as a map $\mathcal{M}_{AB\to VW|S^\Pi S^\Xi} : ABS^\Pi S^\Xi \to ABVWS^\Pi S^\Xi$ given by

$$\mathcal{M}_{AB\to VW|S^\Pi S^\Xi}(\cdot) = \sum_{\pi\in\Pi_{m,k}} \mathcal{M}_{A\to V|S^\Xi}^\pi \circ \mathcal{M}_{B\to W|S^\Xi}^\pi \big(|\pi\rangle\langle\pi|_{S^\Pi} \ \cdot \ |\pi\rangle\langle\pi|_{S^\Pi} \big) \tag{14}$$

The state of the total system after the measurement required for parameter estimation is thus given by

$$\begin{aligned}
\tau_{ABVWS^\Pi S^\Xi S^\Theta} &= \mathcal{M}_{AB\to VW|S^\Pi S^\Xi}(\rho_{ABS^\Pi S^\Xi S^\Theta}) && (15)\\
&= \sum_{\pi\in\Pi_{m,k}} \frac{1}{\binom{m}{k}} |\pi\rangle\langle\pi|_{S^\Pi} \otimes \rho_{S^\Theta} \otimes \mathcal{V}^\pi \circ \mathcal{W}^\pi \big[\rho_{ABS^\Xi}\big] && (16)\\
&= \sum_{\pi\in\Pi_{m,k}} \sum_{\xi\in\{0,1\}^k} \sum_{v,w\in\{0,1\}^k} \frac{1}{2^k\binom{m}{k}} |\pi,\xi\rangle\langle\pi,\xi|_{S^\Pi S^\Xi} \otimes \rho_{S^\Theta} \otimes \\
&\qquad \ldots\ |v,w\rangle\langle v,w|_{VW} \otimes \big(M_{A_\pi}^{\xi,v} \otimes M_{B_\pi}^{\xi,w}\big)\rho_{AB}\big(M_{A_\pi}^{\xi,v} \otimes M_{B_\pi}^{\xi,w}\big)^\dagger . && (17)
\end{aligned}$$

The second measurement concerns the quantum systems used for extracting the secret key. The corresponding measurement maps are defined analogously to the measurements maps above, but now act on the systems determined by $\bar\pi$, the complement of π in $[m]$. We define

$$\mathcal{M}_{A\to X|S^\Pi S^\Theta}(\cdot) = \sum_{\pi\in\Pi_{m,k}} \sum_{\theta,x\in\{0,1\}^n} |x\rangle_X \big(M_{A_{\bar\pi}}^{\theta,x} \otimes |\pi,\theta\rangle\langle\pi,\theta|_{S^\Pi S^\Theta}\big) \ \cdot \ \big(M_{A_{\bar\pi}}^{\theta,x} \otimes |\pi,\theta\rangle\langle\pi,\theta|_{S^\Pi S^\Theta}\big)^\dagger \langle x|_X \,, \tag{18}$$

$$\mathcal{M}_{B\to Y|S^\Pi S^\Theta}(\cdot) = \sum_{\pi\in\Pi_{m,k}} \sum_{\theta,y\in\{0,1\}^n} |y\rangle_Y \big(M_{B_{\bar\pi}}^{\theta,y} \otimes |\pi,\theta\rangle\langle\pi,\theta|_{S^\Pi S^\Theta}\big) \ \cdot \ \big(M_{B_{\bar\pi}}^{\theta,y} \otimes |\pi,\theta\rangle\langle\pi,\theta|_{S^\Pi S^\Theta}\big)^\dagger \langle y|_Y \tag{19}$$

as well as $\mathcal{M}_{AB\to XY|S^\Pi S^\Theta} = \mathcal{M}_{A\to X|S^\Theta S^\theta} \circ \mathcal{M}_{B\to Y|S^\Pi S^\Theta}$. It is evident that all measurements $\mathcal{M}$ defined so far mutually commute. Finally, we define the total measurement map as $\mathcal{M}_{AB\to VWXY|S^\Pi S^\Xi S^\Theta} := \mathcal{M}_{AB\to VW|S^\Pi S^\Xi} \circ \mathcal{M}_{AB\to XY|S^\Pi S^\Theta}$.

Of particular interest is the state of the system after measurement and after we discard the quantum systems. This is given by a classical state $\sigma_{VWXYS^\Pi S^\Xi S^\Theta}$. This state is of the form

$$\begin{aligned}
&\sigma_{VWXYS^\Pi S^\Xi S^\Theta} && (20)\\
&= \mathrm{tr}_{AB}\big(\mathcal{M}_{AB\to VWXY|S^\Pi S^\Xi S^\Theta}(\rho_{ABS^\Pi S^\Xi S^\Theta})\big) && (21)\\
&= \mathrm{tr}_{AB}\big(\mathcal{M}_{AB\to XY|S^\Pi S^\Theta}(\tau_{ABVWS^\Pi S^\Xi S^\Theta})\big) && (22)\\
&= \sum_{\pi\in\Pi_{m,k}} \sum_{\substack{\xi\in\{0,1\}^k\\ \theta\in\{0,1\}^n}} \sum_{\substack{v,w\in\{0,1\}^k\\ x,y\in\{0,1\}^n}} \frac{1}{2^m\binom{m}{k}} |\pi,\xi,\theta\rangle\langle\pi,\xi,\theta|_{S^\Pi S^\Xi S^\Theta} \otimes |v,w,x,y\rangle\langle v,w,x,y|_{VWXY} \otimes \\
&\qquad \ldots\ \mathrm{tr}_{AB}\Big\{\big(\widetilde{M}_{A_\pi}^{\xi,v} \otimes \widetilde{M}_{A_{\bar\pi}}^{\theta,x} \otimes \widetilde{M}_{B_\pi}^{\xi,w} \otimes \widetilde{M}_{B_\pi}^{\theta,y}\big)\rho_{AB}\Big\}\,, && (23)
\end{aligned}$$

where we write $\widetilde{M}_{A_\pi}^{\xi,v} = \big(M_{A_\pi}^{\xi,v}\big)^\dagger M_{A_\pi}^{\xi,v}$ and analogously introduce $\widetilde{M}_{A_{\bar\pi}}^{\theta,x}$, $\widetilde{M}_{B_\pi}^{\xi,w}$ and $\widetilde{M}_{B_\pi}^{\theta,y}$.

Parameter Estimation: We model parameter estimation by a test function acting on the registers V and W and creating a binary flag F^{pe} as follows:

$$\mathrm{pe} : \{0,1\}^k \otimes \{0,1\}^k \to \{\perp, \not\perp\}, \quad \mathrm{pe}(v,w) = \begin{cases} \perp & \text{if } \sum_{i\in[k]} 1\{v_i \neq w_i\} \geq k\delta \\ \not\perp & \text{otherwise} \end{cases} . \tag{24}$$

This test can be applied to the states $\tau_{ABVWS^\Pi S^\Xi S^\Theta}$ or $\sigma_{VWXYS^\Pi S^\Xi S^\Theta}$ defined previously.

Step	**Input State**		**Output State**
Input:			ρ_{AB}
Randomization:			$\rho_{S^\Phi} \otimes \rho_{S^\Pi} \otimes \rho_{S^{H_{\rm ec}}} \otimes \rho_{S^{H_{\rm pa}}}$
Measurement:	$\rho_{AB} \otimes \rho_{S^\Phi} \otimes \rho_{S^\Pi}$	$\mapsto$	$\sigma_{VWXYABS^\Phi S^\Pi}$
Parameter Estimation:	σ_{VW}	$\mapsto$	$\sigma_{C^V F^{\rm pe}}$
Error Correction:	$\sigma_{XY} \otimes \rho_{S^{H_{\rm ec}}}$	$\mapsto$	$\sigma_{X\hat{X}C^Z F^{\rm ec}}$
Privacy Amplification:	$\sigma_{X\hat{X}} \otimes \rho_{S^{H_{\rm pa}}}$	$\mapsto$	$\omega_{K_A K_B C^H}$
Output:			$\omega_{K_A K_B SCF}$

Table 2: Evolution of the registers during the execution of the simple QKD Protocol.

We are specifically interested in the state $\tau_{ABVWS^\Pi S^\Xi S^\Theta F^{\rm pe}} = \mathcal{E}_{\rm pe}\big[\tau_{ABVWS^\Pi S^\Xi S^\Theta}\big]$ and the corresponding state conditioned on the outcome $F^{\rm pe} = \not\perp$, given by

$$\tau_{ABVWS^\Pi S^\Xi S^\Theta | F^{\rm pe} = \not\perp} = \frac{1}{\Pr_\tau[F^{\rm pe} = \not\perp]} \sum_{\pi \in \Pi_{m,k}} \sum_{\xi \in \{0,1\}^k} \sum_{\substack{v,w \in \{0,1\}^k \\ \sum_{i=1}^k 1\{v_i \neq w_i\} < k\delta}} \frac{1}{2^k \binom{m}{k}} |\pi, \xi\rangle\langle\pi, \xi|_{S^\Pi S^\Xi} \otimes$$

$$\ldots \ \rho_{S^\Theta} \otimes |v,w\rangle\langle v,w|_{VW} \otimes \big(M_{A_\pi}^{\xi,v} \otimes M_{B_\pi}^{\xi,w}\big) \rho_{AB} \big(M_{A_\pi}^{\xi,v} \otimes M_{B_\pi}^{\xi,w}\big)^\dagger . \tag{25}$$

We will see that this state is crucial for the security analysis in the next section. Finally, we note that $\mathcal{M}_{XY}$ and $\mathcal{E}_{\rm pe}$ commute, and thus in particular we find that

$$\mathrm{tr}_{AB}\left(\mathcal{M}_{AB \to XY | S^\Pi S^\Theta}(\tau_{ABVWS^\Pi S^\Xi S^\Theta | F^{\rm pe} = \not\perp})\right) = \sigma_{VWXYS^\Pi S^\Xi S^\Theta | F^{\rm pe} = \not\perp}, \qquad \text{where} \tag{26}$$

$$\sigma_{VWXYS^\Pi S^\Xi S^\Theta F^{\rm pe}} = \mathcal{E}_{\rm pe}(\sigma_{VWXYS^\Pi S^\Xi S^\Theta}) . \tag{27}$$

We also relabel V to C^V and keep it around as part of the transcript, while we discard W after performing parameter estimation.

Error Correction: Alice computes the syndrome $Z = \mathrm{synd}(X)$ and sends it to Bob. Bob then computes $\hat{X} = \mathrm{corr}(Y, Z)$.

Alice and Bob then need to check that the decoding procedure succeeded. The simplest strategy is to compare hashes of their respective strings x and $\hat{x}$ and abort the protocol if they differ.

Alice computes a hash of size t (in bits) of x and sends it to Bob, who computes the corresponding hash for $\hat{x}$. If both hashes differ, Bob sends the flag '$\perp^{\rm ec}$' to Alice. Alice and Bob will then output '$\perp^{\rm ec}$' and abort the protocol. Otherwise Bob sends '$\not\perp^{\rm ec}$' to Alice and they proceed.

This test is modeled as a classical map ec acting on registers X, $\hat{X}$ and $S^{H_{\rm ec}}$ creating a transcript of the hash value C^T and a binary flag $F^{\rm ec}$ as follows:

$$\mathrm{ec} : \{0,1\}^n \times \{0,1\}^n \times \mathcal{H}_{\rm ec} \to \{0,1\}^t \times \{\perp, \not\perp\}, \quad (x, \hat{x}) \mapsto \begin{cases} (h_{\rm ec}(x), \perp) & \text{if } h_{\rm ec}(x) \neq h_{\rm ec}(\hat{x}) \\ (h_{\rm ec}(x), \not\perp) & \text{otherwise} \end{cases} . \tag{28}$$

The classical functions are modeled using CPTP maps $\mathcal{E}_{\rm synd}$, $\mathcal{E}_{\rm corr}$, as well as $\mathcal{E}_{\rm ec}$.

Applying these maps to the state $\sigma_{XYC^V S^\Pi S^\Xi S^\Theta F^{\rm pe}}$ yields

$$\sigma_{X\hat{X}C^V C^Z C^T S^\Pi S^\Xi S^\Theta S^{H_{\rm ec}} F^{\rm pe} F^{\rm ec}} = \mathrm{tr}_Y \Big(\mathcal{E}_{\rm ec} \circ \mathcal{E}_{\rm corr} \circ \mathcal{E}_{\rm synd}\left(\sigma_{XYC^V S^\Pi S^\Xi S^\Theta F^{\rm pe}} \otimes \rho_{S^{H_{\rm ec}}}\right)\Big), \tag{29}$$

where the transcript register C^Z contains the value of the syndrome and C^T the output of Alice's hash.

Privacy Amplification: Alice and Bob use the seed $H_{\rm pa}$ to choose a hash function, which they then both apply on their raw key to compute $K_A = H_{\rm pa}(X)$ and $K_B = H_{\rm pa}(\hat{X})$, their respective keys. Formally, the privacy amplification map is defined as:

$$\mathrm{pa} : \left\{ \begin{array}{ccc} \{0,1\}^n \times \{0,1\}^n \times \mathcal{H}_{\rm pa} & \to & \{0,1\}^l \times \{0,1\}^l \\ (x, \hat{x}, h_{\rm pa}) & \mapsto & (h_{\rm pa}(x), h_{\rm pa}(\hat{x})) \end{array} \right. \tag{30}$$

$(K_A, K_B, S, C, F) = \texttt{qkd\_ideal}_{k,n,\delta,\mathrm{ec},\mathrm{pa}}\ (\rho_{AB})$:

Run protocol: Set $(K_A, K_B, S, C, F) = \texttt{qkd\_simple}_{k,n,\delta,\mathrm{ec},\mathrm{pa}}(\rho_{AB})$.

Output: If $F^{\mathrm{pe}} = F^{\mathrm{ec}} =$ '$\not\perp$', then replace K_A and K_B by an independent and uniformly distributed random variable K, i.e. set $K_A = K_B = K$.

Table 3: Ideal QKD Protocol.

Denoting by K_A and K_B the respective key spaces of Alice and Bob, the final quantum state is

$$\omega_{K_A K_B ECSF} = \mathrm{tr}_{X\hat{X}}\left(\mathcal{E}_{\mathrm{pa}}(\sigma_{X\hat{X}ECSF} \otimes \rho_{S^{H_{\mathrm{pa}}}})\right). \tag{31}$$

3 Security Definition and Results

Security is defined with regards to an ideal protocol, which is defined in Table 3. Note in particular that an ideal protocol is allowed to abort, but it will always output a uniformly random shared key in case it does not.

For a detailed discussion of the security of quantum key distribution, we refer the reader to [3]. For our purposes, it suffices to show that

$$\Delta_{k,n,\delta,\mathrm{ec},\mathrm{pa}} := \frac{1}{2}\left\|\texttt{qkd\_simple}_{k,n,\delta,\mathrm{ec},\mathrm{pa}} - \texttt{qkd\_ideal}_{k,n,\delta,\mathrm{ec},\mathrm{pa}}\right\|_{\diamond} \tag{32}$$

$$= \sup_{\rho_{ABE}} \frac{1}{2}\left\|\texttt{qkd\_simple}_{k,n,\delta,\mathrm{ec},\mathrm{pa}}(\rho_{ABE}) - \texttt{qkd\_ideal}_{k,n,\delta,\mathrm{ec},\mathrm{pa}}(\rho_{ABE})\right\|_1 \tag{33}$$

is very small for certain choices of parameters k, n, δ, ec and pa. In the latter expression $\rho_{ABE} \in \mathcal{S}(ABE)$ is an arbitrary extension of ρ_{AB} to a finite-dimensional system E. (Note that the restriction to finite-dimensional E is not restrictive if AB is finite-dimensional, since the diamond norm of a trace-annihilating map is achieved by quantum states with E of the same dimension as AB.)

Let us now fix ρ_{ABE}. The trace distance in (33) can be simplified by noting that the output of `qkd_ideal` equals the output of `qkd_simple` if the protocol aborts. We find

$$\left\|\texttt{qkd\_simple}_{k,n,\delta,\mathrm{ec},\mathrm{pa}}(\rho_{ABE}) - \texttt{qkd\_ideal}_{k,n,\delta,\mathrm{ec},\mathrm{pa}}(\rho_{ABE})\right\|_1$$

$$= \left\|\omega_{K_A K_B SCFE, F^{\mathrm{pe}}=F^{\mathrm{ec}}=\text{`}\not\perp\text{'}} - \chi_{K_A K_B} \otimes \omega_{SCFE, F^{\mathrm{pe}}=F^{\mathrm{ec}}=\text{`}\not\perp\text{'}}\right\|_1 \tag{34}$$

$$= \Pr\left[F^{\mathrm{pe}} = F^{\mathrm{ec}} = \text{`}\not\perp\text{'}\right]_{\omega} \cdot \left\|\omega_{K_A K_B SCE|F^{\mathrm{pe}}=F^{\mathrm{ec}}=\text{`}\not\perp\text{'}} - \chi_{K_A K_B} \otimes \omega_{SCE|F^{\mathrm{pe}}=F^{\mathrm{ec}}=\text{`}\not\perp\text{'}}\right\|_1, \tag{35}$$

where we use $\omega_{K_A K_B SCFE} = \texttt{qkd\_simple}_{k,n,\delta,\mathrm{ec},\mathrm{pa}}(\rho_{ABE})$ and define

$$\chi_{K_A K_B} := \frac{1}{2^{\ell}} \sum_{k \in \{0,1\}^{\ell}} |k\rangle\langle k|_{K_A} \otimes |k\rangle\langle k|_{K_B}\ . \tag{36}$$

The goal of in the following is to bound (35) uniformly in ρ_{ABE}, which implies an upper bound on (33) as well. In order to do this we will employ the following lemma which allows us to split the norm into two terms corresponding to correctness and secrecy. (See Portmann et al. [3] for a proof.)

Lemma 1. *If, for every state ρ_{ABE}, we have*

$$\Pr[K_A \neq K_B \wedge F^{pe} = F^{ec} = \not\perp]_{\omega} \leq \epsilon_{ec} \qquad \textit{and} \tag{37}$$

$$\Pr\left[F = (\not\perp, \not\perp)\right]_{\omega} \cdot \frac{1}{2}\left\|\omega_{K_A SCFE|F=(\not\perp,\not\perp)} - \chi_{K_A} \otimes \omega_{SCFE|F=(\not\perp,\not\perp)}\right\|_1 \leq \epsilon_{pa}\,. \tag{38}$$

Then, $\Delta_{k,n,\delta,\mathrm{ec},\mathrm{pa}} \leq \epsilon_{\mathrm{ec}} + \epsilon_{pa}$.

The first statement of the above lemma corresponds to *correctness*, and the second one to *secrecy*. If both are satisfied, we say that the protocol is *secure*. We will show the following theorems. The first theorem establishes correctness of the protocol.

Theorem 2. *Let* $n, k, \delta, \mathrm{ec}, \mathrm{pa}$ *be defined as in Section 2.1. Then for every state* ρ_{ABE} *and* $\omega_{K_A K_B SCFE} = \texttt{qkd\_simple}_{k,n,\delta,\mathrm{ec},\mathrm{pa}}(\rho_{ABE})$ *we have*

$$\Pr[K_A \neq K_B \wedge F = (\not\perp, \not\perp)]_\omega \leq \epsilon_{\mathrm{ec}} := 2^{-t} \,. \tag{39}$$

The second theorem asserts secrecy.

Theorem 3. *Let* $n, k, \delta, \mathrm{ec}, \mathrm{pa}$ *be defined as in Section 2.1. Define*

$$\epsilon_{\mathrm{pa}}(\nu) := 2^{-\frac{1}{5}\left(n \log \frac{1}{c} - nh(\delta+\nu) - r - t - \ell\right)}, \tag{40}$$

where h *is the binary entropy function (cf. Prop. 8). If* $\varepsilon_{\mathrm{pa}}(0) < 1$*, define* ν_* *as the unique solution of the equality*

$$\epsilon_{\mathrm{pa}}(\nu) = \exp\left(-\frac{nk^2\nu^2}{2(n+k)(k+1)}\right). \tag{41}$$

If, furthermore, this solution satisfies $\epsilon_{\mathrm{pa}}(\nu_*) \leq \frac{1}{4}$*, then, for every state* ρ_{ABE} *and* $\omega_{K_A K_B SCFE} = \texttt{qkd\_simple}_{k,n,\delta,\mathrm{ec},\mathrm{pa}}(\rho_{ABE})$*, we have*

$$\Pr\left[F = (\not\perp, \not\perp)\right]_\omega \cdot \frac{1}{2}\left\|\omega_{K_A SCFE|F=(\not\perp,\not\perp)} - \chi_{K_A} \otimes \omega_{SCFE|F=(\not\perp,\not\perp)}\right\|_1 \leq \epsilon_{pa}(\nu_*) \,. \tag{42}$$

Remark 1. Note that $\epsilon_{\mathrm{pa}}(0) < 1$ is a necessary condition for security. The additional constraint, $\epsilon_{\mathrm{pa}}(\nu_*) \leq \frac{1}{4}$ was added since it allows us to simplify the presentation of the result, and it will always be satisfied in realistic settings where this term is expected to be exponentially small in n.

4 The Security Proof

The purpose of this section is to proof Theorems 2 and 3.

4.1 Technical Ingredients

Here we overview the main technical ingredients for our proof.

4.1.1 Smooth Rényi Entropies

We use the following definitions. The min- and max-entropy are natural generalization of conditional Rényi entropies [5] to the quantum setting. They were first proposed by Renner [4] and König–Renner–Schaffner [2], respectively.

Definition 1 (Min and Max-Entropy)**.** For any bipartite state $\rho_{AB} \in \mathcal{S}_\bullet(AB)$, we define

$$H_{\min}(A|B)_\rho := \sup\left\{\lambda \in \mathbb{R} : \exists\, \sigma_B \in \mathcal{S}(B) \text{ such that } \rho_{AB} \leq 2^{-\lambda} \mathrm{id}_A \otimes \sigma_B, \right\} \tag{43}$$

$$H_{\max}(A|B)_\rho := \sup_{\sigma_B \in \mathcal{S}(B)} \log\left(\mathrm{tr}\sqrt{\sqrt{\rho_{AB}}(\mathrm{id}_A \otimes \sigma_B)\sqrt{\rho_{AB}}}\right)^2, \tag{44}$$

which are called the min- and max-entropy of A conditioned on B, respectively.

The following metric is very useful when dealing with sub-normalized states [8]:

Definition 2 (Purified distance)**.** For $\rho_A, \sigma_A \in \mathcal{S}_\bullet(A)$, we define

$$F(\rho_A, \sigma_A) := \left(\operatorname{tr} \sqrt{\sqrt{\rho_A}\sigma_A\sqrt{\rho_A}} + \sqrt{1 - \operatorname{tr}(\rho_A)}\sqrt{1 - \operatorname{tr}(\sigma_A)} \right)^2, \tag{45}$$

$$P(\rho_A, \sigma_A) := \sqrt{1 - F(\rho_A, \sigma_A)}, \tag{46}$$

which are called the generalized fidelity and the purified distance, respectively.

In particular, the purified distance is a metric on sub-normalized states and satisfies [8, Lem. 2]

$$P(\rho_A, \sigma_A) \geq P\big(\mathcal{F}(\rho_A), \mathcal{F}(\sigma_A)\big) \tag{47}$$

for every trace non-increasing completely positive map $\mathcal{F}$. This means that the distance contracts when we apply a quantum channel to both states. Finally, we note that [8, Lem. 6]

$$\frac{1}{2}\big\|\rho_A - \sigma_A\big\|_1 + \frac{1}{2}\big|\operatorname{tr}(\rho_A) - \operatorname{tr}(\sigma_A)\big| \leq P(\rho_A, \sigma_A)\,. \tag{48}$$

Based on this metric, we define the smooth min- and max-entropy.

Definition 3 (Smooth Entropies)**.** For $\rho_{AB} \in \mathcal{S}_\bullet(AB)$ and $\varepsilon \in \Big[0, \sqrt{\operatorname{tr}(\rho_{AB})}\Big)$, we define

$$H_{\min}^\varepsilon(A|B)_\rho := \max_{\substack{\tilde\rho_{AB} \in \mathcal{S}_\bullet(AB),\\ P(\tilde\rho_{AB}, \rho_{AB}) \leq \varepsilon}} H_{\min}(A|B)_{\tilde\rho}, \qquad H_{\max}^\varepsilon(A|B)_\rho := \min_{\substack{\tilde\rho_{AB} \in \mathcal{S}_\bullet(AB),\\ P(\tilde\rho_{AB}, \rho_{AB}) \leq \varepsilon}} H_{\max}(A|B)_{\tilde\rho}\,. \tag{49}$$

The smooth entropies satisfy a duality relation [8]. For any pure state ρ_{ABC}, we have

$$H_{\min}^\varepsilon(A|B)_\rho = -H_{\max}^\varepsilon(A|C)_\rho\,. \tag{50}$$

They also satisfy a data-processing inequality (DPI) [8, Thm. 18]. For any state ρ_{AB} and any completely positive trace-preserving map $\mathcal{E}_{B\to C}$, we have

$$H_{\min}^\varepsilon(A|B)_\rho \leq H_{\min}^\varepsilon(A|C)_{\mathcal{E}(\rho)}, \quad \text{and} \quad H_{\max}^\varepsilon(A|B)_\rho \leq H_{\max}^\varepsilon(A|C)_{\mathcal{E}(\rho)}\,. \tag{51}$$

We also need a simple chain rule [13, Lem. 11], which states that

$$H_{\min}^\varepsilon(A|BX)_\rho \geq H_{\min}^\varepsilon(A|B)_\rho - \log|X| \tag{52}$$

where X is a (classical) register of dimension $|X|$. Finally, we note that

$$H_{\max}(X)_\rho \leq \log\Big|\{x \in X : \Pr_\rho[X = x] > 0\}\Big| \tag{53}$$

by the monotonicity of the Rényi entropies [5]. A more extensive review of the smooth entropy calculus can be found in [7] and in [?].

4.1.2 Entropic Uncertainty Relation

We state the uncertainty relation in a natural form applied to the situation at hand. This relation forms the core technical ingredient of our security proof [7, Cor. 7.4].

Theorem 4. *Let $\tau_{ABCP} \in \mathcal{S}(ABCP)$ be an arbitrary state with P a classical register. Furthermore, let $\varepsilon \in [0, 1)$ and let q be a bijective function on P that is a symmetry of ρ_{ABCP} in the sense that $\rho_{ABC,P=p} = \rho_{ABC,P=q(p)}$ for all $p \in P$. Then, we have*

$$H_{\min}^\varepsilon(X|CP)_\sigma + H_{\max}^\varepsilon(X|BP)_\sigma \geq \log\frac{1}{c_q}, \qquad \textit{where} \tag{54}$$

where $c_q = \max_{p\in P}\max_{x,z\in X}\big\|F_A^{q(p),x}\big(F_A^{p,z}\big)^\dagger\big\|_\infty^2$. Here, $\sigma_{XBCP} = \mathcal{M}_{A\to X|P}(\tau_{ABCP})$ for the map

$$\mathcal{M}_{A\to X|P}[\,\cdot\,] = \operatorname{tr}_A\left(\sum_{p\in P}\sum_{x\in X}|x\rangle_X\left(|p\rangle\!\langle p|_P \otimes F_A^{p,x}\right)\,\cdot\,\left(|p\rangle\!\langle p|_P \otimes F_A^{p,x}\right)^\dagger\langle x|_X\right). \tag{55}$$

and any set (indexed by $p \in P$) of generalized measurements $\{F_A^{p,x}\}_{x\in X}$.

This uncertainty relation was first shown in [7], based on the techniques introduced in [10]. The difference to [7, Cor. 7.4] is that we here account for general measurements, whereas previous bounds assumed that $F_A^{p,x} \geq 0$. We provide a full proof of the uncertainty relation in Appendix A for completeness.

4.1.3 Universal$_2$ Hashing and Leftover Hashing Lemma

Universal hashing is used twice in the analysis of the quantum key distribution protocol: first in the error correction step to ensure the correctness of the protocol (Theorem 2), and then in the privacy amplification procedure to guarantee the secrecy of the final key.

Definition 4 (Universal$_2$ Hashing)**.** Let $\mathcal{H} = \{h\}$ be a family of functions from $\mathcal{X}$ to $\mathcal{Z}$. The family $\mathcal{H}$ is said to be *universal*$_2$ if $\Pr\left[H(x) = H(x')\right] \leq \frac{1}{|\mathcal{Z}|}$ for any pair of distinct elements $x, x' \in \mathcal{X}$, when h is chosen uniformly at random in $\mathcal{H}$.

In this work we do not need to specify any particular family of hash functions, and it suffices to note that such families of functions always exist if $|\mathcal{X}|$ and $|\mathcal{Z}|$ are powers of 2. (See, e.g., [1, 12].)

We now state a version of the Leftover Hashing Lemma is, up to a slight change of the definition of the smooth min-entropy, due to Renner [4, Corr. 5.6.1]. The proof of this exact statement is provided in Appendix B for the convenience of the reader.

Theorem 5. *Let $\sigma_{XE'}, \tilde{\sigma}_{XE'} \in \mathcal{S}_\bullet(XE')$ be a classical-quantum state and let $\mathcal{H}$ be a universal$_2$ family of hash functions from $\{0,1\}^n$ to $\{0,1\}^\ell$. Moreover, let $\rho_{S^H} = \sum_{h\in\mathcal{H}} \frac{1}{|\mathcal{H}|} |h\rangle\langle h|_{S^H}$ be fully mixed. Then,*

$$\|\omega_{KS^HE'} - \chi_K \otimes \omega_{S^HE'}\|_1 \leq 2^{-\frac{1}{2}\left(H_{\min}(X|E')_{\tilde{\sigma}} - \ell\right)} + 2\|\sigma_{XE'} - \tilde{\sigma}_{XE'}\|_1 \tag{56}$$

where $\chi_K = \frac{1}{2^\ell}\mathrm{id}_K$ is the fully mixed state and $\omega_{KS^HE'} = \mathrm{tr}_X\left(\mathcal{E}_f(\sigma_{XE'} \otimes \rho_{S^H})\right)$ for the function $f : (x,h) \mapsto h(x)$ that acts on the registers X and S^H.

4.2 Correctness: Proof of Theorem 2

We wish to upper bound the probability of the protocol not aborting and outputting distinct final keys for Alice and Bob.

Proof of Theorem 2. We consider the following chain of inequalities:

$$\begin{aligned}
\Pr_\omega[K_A \neq K_B \wedge F^{\mathrm{pe}} = F^{\mathrm{ec}} = \not\perp] &\leq \Pr_\omega[K_A \neq K_B \wedge F^{\mathrm{ec}} = \not\perp] && (57)\\
&= \Pr_\omega[H_{\mathrm{pa}}(X) \neq H_{\mathrm{pa}}(X') \wedge H_{\mathrm{ec}}(X) = H_{\mathrm{ec}}(X')] && (58)\\
&\leq \Pr_\sigma[X \neq X' \wedge H_{\mathrm{ec}}(X) = H_{\mathrm{ec}}(X')] && (59)\\
&= \Pr_\sigma[X \neq X'] \Pr_\sigma[H_{\mathrm{ec}}(X) = H_{\mathrm{ec}}(X') \mid X \neq X'] && (60)\\
&\leq \Pr_\sigma[H_{\mathrm{ec}}(X) = H_{\mathrm{ec}}(X') \mid X \neq X'] && (61)\\
&\leq |\mathcal{H}_{\mathrm{ec}}|^{-1} = 2^{-t}. && (62)
\end{aligned}$$

The first inequality follows since we ignore the status of the flag F^{pe}. The second inequality is a consequence of the fact $X = X'$ implies $H_{\mathrm{pa}}(X) = H_{\mathrm{pa}}(X')$. The third inequality follows since $\Pr[X \neq X'] \leq 1$ and the last one by definition of universal$_2$ hashing. □

4.3 Measurement Uncertainty: Bound on Smooth Min-Entropy

The crucial bound on the smooth entropy of Alice's measurement outcomes follows by the entropic uncertainty relation, suitably applied.

Proposition 6. *Consider the state $\sigma_{XYVWS^{\Pi}S^{\Xi}S^{\Theta}F^{\mathrm{pe}}E}$ as in (27) after measurement and parameter estimation. Let $\varepsilon \in [0,1)$. Then, with $\bar{c}$ defined in (6), we have*

$$H_{\min}^{\varepsilon}(X|VWS^{\Pi}S^{\Xi}S^{\Theta}E, F^{\mathrm{pe}} = \not\perp)_{\sigma} + H_{\max}^{\varepsilon}(X|Y, F^{\mathrm{pe}} = \not\perp)_{\sigma} \geq n \log \frac{1}{\bar{c}}\,. \tag{63}$$

Proof. Consider the state $\tau_{ABVWS^{\Pi}S^{\Xi}S^{\Theta}F^{\mathrm{pe}}E|F^{\mathrm{pe}}=\not\perp}$ defined in (25) and note that it is of the form

$$\tau_{ABVWS^{\Pi}S^{\Xi}S^{\Theta}F^{\mathrm{pe}}E|F^{\mathrm{pe}}=\not\perp} = \tau_{ABVWS^{\Pi}S^{\Xi}F^{\mathrm{pe}}E|F^{\mathrm{pe}}=\not\perp} \otimes \rho_{S^{\Theta}}\,. \tag{64}$$

This is the state of the system after parameter estimation and after measuring V and W, but with the measurement of X and Y (in the basis determined by Θ) delayed.

Let us now apply Theorem 4 to this state. For this purpose we equate $C = VWEF^{\mathrm{pe}}$ and $P = S^{\Pi}S^{\Xi}S^{\Theta}$. The symmetry is determined by the map $q : \theta \mapsto \bar{\theta}$ with $\bar{\theta}_i = 1 - \theta_i$, which only acts on S^{Θ}. The measurement map is then simply $\mathcal{M}_{A\to X|S^{\Pi}S^{\Theta}}$ and we can calculate

$$c_q = \max_{\pi\in\Pi_{m,k}} \max_{\theta,x,z\in\{0,1\}^n} \left\| M_{A_{\bar{\pi}}}^{\bar{\theta},x} \big(M_{A_{\bar{\pi}}}^{\theta,z}\big)^{\dagger} \right\|_{\infty}^{2} = \max_{\pi\in\Pi_{m,k}} \left(\prod_{i\in\bar{\pi}} c_i \right) = \bar{c}^{\,n}\,. \tag{65}$$

Theorem 4 applied to our setup thus yields

$$H_{\min}^{\varepsilon}(X|VWES^{\Pi}S^{\Xi}S^{\Theta}, F^{\mathrm{pe}} = \not\perp)_{\sigma} + H_{\max}^{\varepsilon}(X|BS^{\Pi}S^{\Xi}S^{\Theta}, F^{\mathrm{pe}} = \not\perp)_{\tau} \geq n \log \frac{1}{\bar{c}} \tag{66}$$

Finally, the statement of the Proposition follows by applying the measurement map $\mathcal{M}_{B\to Y|S^{\Pi}S^{\Theta}}$ and noting that $H_{\max}^{\varepsilon}(X|BS^{\Pi}S^{\Xi}S^{\Theta}, F^{\mathrm{pe}} = \not\perp)_{\tau} \leq H_{\max}^{\varepsilon}(X|Y, F^{\mathrm{pe}} = \not\perp)_{\sigma}$ by the data-processing inequality. □

Remark 2. Observe that the right hand side of (66) can be further bounded as

$$n \log \frac{1}{\bar{c}} = \min_{\pi\in\Pi_{m,k}} \left(\sum_{i\in\bar{\pi}} \log \frac{1}{c_i} \right) \geq n \log \frac{1}{\hat{c}}, \quad \text{where} \quad \hat{c} = \max_{\pi\in\Pi_{m,k}} \left(\frac{1}{n} \sum_{i\in\bar{\pi}} c_i \right)\,. \tag{67}$$

using the concavity of the logarithm function (or the arithmetic-geometric mean inequality).

4.4 Parameter Estimation: Statistical Bounds on Smooth Max-Entropy

This section covers the necessary statistical analysis. This replicates the analysis in [9], but we are more careful in working out the details here. We will use the following tail bound.

Lemma 7. *Consider a set of binary random variables $Z = (Z_1, Z_2, \ldots, Z_m)$ with Z_i taking values in $\{0,1\}$ and $m = n + k$. Let $\Pi \in \Pi_{m,k}$ be an independent, uniformly distributed random variable. Then,*

$$\Pr\left[\sum_{i\in\Pi} Z_i \leq k\delta \;\wedge\; \sum_{i\in\bar{\Pi}} Z_i \geq n(\delta+\nu) \right] \leq \exp\left(-2\nu^2 \frac{nk^2}{(n+k)(k+1)} \right) \tag{68}$$

Remarkably this bound is valid without any assumptions on the distribution of Z.

Proof. Let $\mu(z) = \frac{1}{m}\sum_{i\in[m]} z_i$. Consider the following sequence of inequalities:

$$\begin{aligned}
\Pr\left[\frac{1}{k}\sum_{i\in\Pi} Z_i \leq \delta \;\wedge\; \frac{1}{n}\sum_{i\notin\Pi} Z_i \geq \delta+\nu \right] &\leq \Pr\left[\frac{1}{n}\sum_{i\in\bar{\Pi}} Z_i \geq \frac{1}{k}\sum_{i\in\Pi} Z_i + \nu \right] && (69)\\
&= \sum_{z\in\{0,1\}^m} \Pr[Z=z] \Pr\left[\frac{1}{n}\sum_{i\in\bar{\Pi}} z_i \geq \frac{1}{k}\sum_{i\in\Pi} z_i + \nu \right] && (70)\\
&= \sum_{z\in\{0,1\}^m} \Pr[Z=z] \Pr\left[\frac{1}{n}\sum_{i\in\bar{\Pi}} z_i \geq \mu(z) + \frac{k\nu}{m} \right]. && (71)
\end{aligned}$$

Here, the first inequality holds since $A \implies B$ implies $\Pr[A] \leq \Pr[B]$ for any events A and B. The first equality follows from the fat that Π is independent of Z. The last equality follows by substituting $\sum_{i\in\Pi} z_i = m\mu(z) - \sum_{i\in\bar{\Pi}} z_i$ and rearranging the terms appropriately.

Now note that the random sums $S_n := \sum_{i\in\bar{\Pi}} z_i$ can be seen as emanating from randomly sampling without replacement n balls labelled by $z_i \in \{0,1\}$ from a population z with mean $\mu(z)$. Serfling's bound [6, Cor. 1.1] then tells us that

$$\Pr\left[\frac{1}{n}S_n \geq \mu(z) + \frac{k\nu}{m}\right] \leq \exp\left(-2n\left(\frac{k\nu}{m}\right)^2\frac{1}{1-f_n^*}\right) = \exp\left(-2\nu^2\frac{nk^2}{(n+k)(k+1)}\right). \tag{72}$$

where we substituted $f_n^* = \frac{n-1}{m}$. It is important to note that this bound is independent of $\mu(z)$. Thus, substituting this back into (71), we conclude the proof. □

With this in hand, we wish to bound the smooth max-entropy of the state conditioned on passing the parameter estimation test.

Proposition 8. *For any $\nu \in (0,1)$, define*

$$\varepsilon(\nu) := \exp\left(-\frac{nk^2\nu^2}{(n+k)(k+1)}\right). \tag{73}$$

Consider any state $\sigma_{XYF^{\text{pe}}}$ as in (27) after measurement and parameter estimation. For any $\nu \in (0, \frac{1}{2}-\delta]$, we set $p = \Pr_\sigma[F^{\text{pe}} = \not\angle]$ and $\varepsilon' = \varepsilon(\nu)/\sqrt{p}$. Then, the following implication is true:

$$p > \varepsilon(\nu)^2 \qquad \implies \qquad H_{\max}^{\varepsilon'}(X|Y, F^{\text{pe}} = \not\angle)_\sigma \leq nh(\delta+\nu)\,, \tag{74}$$

where $h : x \mapsto -x\log x - (1-x)\log(1-x)$ is the binary entropy.

Roughly speaking, this result is a consequence of that fact that, conditioned on any particular value of Y, the support of X is restricted since the number of errors (positions where $x_i \neq y_i$) is bounded when we pass the parameter estimation test with sufficiently high probability.

Proof. We use the shorthand $\varepsilon = \varepsilon(\nu)$. We show that the second statement holds if we assume $p > \varepsilon^2$. Using Lemma 7 below, we find

$$\Pr_\sigma\left[F^{\text{pe}} = \not\angle \ \wedge \ \sum_{i\in[n]} 1\{X_i \neq Y_i\} \geq n(\delta+\nu)\right] \tag{75}$$

$$= \Pr_\sigma\left[\sum_{i\in[k]} 1\{V_i \neq W_i\} \leq k\delta \ \wedge \ \sum_{i\in[n]} 1\{X_i \neq Y_i\} \geq n(\delta+\nu)\right] \leq \varepsilon^2 \tag{76}$$

Thus, using Bayes' rule, we conclude that the event $\Omega = 1\big\{\sum_{i\in[n]} 1\{X_i \neq Y_i\} \geq n(\delta+\nu)\big\}$ satisfies

$$\Pr_\sigma\left[\Omega \,\middle|\, F^{\text{pe}} = \not\angle\,\right] \leq \frac{\varepsilon^2}{p} \tag{77}$$

Now consider the state $\tilde{\sigma}_{XYF^{\text{pe}}} = \tilde{\sigma}_{XY} \otimes |\not\angle\rangle\langle\not\angle|_{F^{\text{pe}}}$ determined by the relation

$$\Pr_{\tilde{\sigma}}[X=x, Y=y] = \begin{cases} \frac{\Pr_\sigma[X=x,Y=y|F^{\text{pe}}=\not\angle]}{1-\Pr_\sigma[\Omega|F^{\text{pe}}=\not\angle]} & \text{if } \sum_{i\in[n]} 1\{x_i \neq y_i\} < n(\delta+\nu) \\ 0 & \text{else} \end{cases}. \tag{78}$$

This state is close to $\sigma_{XYF^{\mathrm{pe}}|F^{\mathrm{pe}}=\not\perp}$ as we will see in the following. We evaluate

$$\begin{aligned}
&\sqrt{F(\sigma_{XYF^{\mathrm{pe}}|F^{\mathrm{pe}}=\not\perp}, \tilde{\sigma}_{XYF^{\mathrm{pe}}})} && (79)\\
&= \sum_{x,y\in\{0,1\}^n} \sqrt{\Pr_{\tilde{\sigma}}[X=x,Y=y]\Pr_{\sigma}[X=x,Y=y|F^{\mathrm{pe}}=\not\perp]} && (80)\\
&= \sum_{x,y\in\{0,1\}^n} 1\Big\{\sum_{i\in[n]} 1\{x_i\neq y_i\} < n(\delta+\nu)\Big\} \frac{\Pr_\sigma[X=x,Y=y\,|\,F^{\mathrm{pe}}=\not\perp]}{\sqrt{1-\Pr_\sigma[\Omega\,|\,F^{\mathrm{pe}}]}} && (81)\\
&= \sqrt{1-\Pr_{\sigma}[\Omega\,|\,F^{\mathrm{pe}}]} \geq \sqrt{1-\frac{\varepsilon^2}{p}}\,. && (82)
\end{aligned}$$

In the last step we used (77). From this we conclude that $P(\sigma_{XYF^{\mathrm{pe}}|F^{\mathrm{pe}}=\not\perp}, \tilde{\sigma}_{XYF^{\mathrm{pe}}}) \leq \varepsilon'$, and, as a consequence $H_{\max}^{\varepsilon'}(X|Y,F^{\mathrm{pe}}=\not\perp)_\sigma \leq H_{\max}(X|YF^{\mathrm{pe}})_{\tilde{\sigma}} = H_{\max}(X|Y)_{\tilde{\sigma}}$.

Finally, it remains to show that $H_{\max}(X|Y)_{\tilde{\sigma}} \leq nh(\delta+\nu)$. We have

$$\begin{aligned}
H_{\max}(X|Y)_{\tilde{\sigma}} &= \log\Bigg(\sum_{y\in\{0,1\}^n} 2^{H_{\max}(X|Y=y)_{\tilde{\sigma}}}\Bigg) && (83)\\
&\leq \max_{y\in\{0,1\}^n} \log\Big|\Big\{x\in\{0,1\}^n : \Pr_{\tilde{\sigma}}[X=x|Y=y]>0\Big\}\Big|\,. && (84)
\end{aligned}$$

Here we used that the Rényi entropy is upper bounded by the logarithm of the distribution's support [5]. The ultimate inequality, which states that

$$\log\Big|\Big\{x\in\{0,1\}^n : \Pr_{\tilde{\sigma}}[X=x|Y=y]>0\Big\}\Big| \leq nh(\delta+\nu), \qquad (85)$$

follows from a combinatoric argument in Claim 9 below. □

Claim 9. *Inequality* (85) *holds.*

Proof. Note that by definition of $\tilde{\sigma}_{XY}$, we have

$$\begin{aligned}
\Big|\Big\{x\in\{0,1\}^n : \Pr_{\tilde{\sigma}}[X=x|Y=y]>0\Big\}\Big| &\leq \sum_{x\in\{0,1\}^n} 1\Big\{\sum_{i\in[n]} 1\{x_i\neq y_i\} < n(\delta+\nu)\Big\} && (86)\\
&= \sum_{e\in\{0,1\}^n} 1\Big\{\sum_{i=1}^n e_i < n(\delta+\nu)\Big\} && (87)\\
&= \sum_{\lambda=0}^n \binom{n}{\lambda} 1\{\lambda < n(\delta+\nu)\} = \sum_{\lambda=0}^{\lfloor n(\delta+\nu)\rfloor} \binom{n}{\lambda} && (88)
\end{aligned}$$

Here, in order to derive (87) we reparametrize $e_i = x_i$ xor y_i, indicating if there is an error at the i-th position. Finally, in (88) we substitute $\lambda = \sum_{i=1}^n e_i$, the total number of errors.

The inequality $\sum_{\lambda=0}^{\lfloor n(\delta+\nu)\rfloor}\binom{n}{\lambda} \leq 2^{nh(\delta+\nu)}$ (see, e.g., [11, Sec. 1.4]) then concludes the proof. □

4.5 Secrecy: Proof of Theorem 3

Once Propositions 6 and 8 are established, the proof of Theorem 3 essentially follows by an application of the Leftover Hashing Lemma and a few technical ingredients. The following lemma allows us to bound the smooth min-entropy when conditioning on events.

Lemma 10. *Let $\varepsilon\in[0,1)$, let $\sigma_{ABXY}\in\mathcal{S}(ABXY)$ be a state that is classical on X and Y and let Ω be an event on X and Y. Then, if $p=\Pr_\sigma[\Omega]>\varepsilon$, there exists a state $\tilde{\sigma}_{ABXY}$ such that*

$$\frac{1}{2}\big\|\tilde{\sigma}_{ABXY}-\sigma_{ABXY|\Omega}\big\| \leq \frac{\varepsilon}{p} \quad \textit{and} \quad H_{\min}(AX|BY)_{\tilde{\sigma}} \geq H_{\min}^{\varepsilon}(AX|BY)_\sigma - \log\frac{1}{p-\varepsilon}\,. \qquad (89)$$

Proof. We assume that $p > \varepsilon$ and let $\lambda = H_{\min}^{\varepsilon}(AX|BY)_{\sigma}$. By the definition of the min-entropy, there exists states $\bar{\sigma}_{AXBY}$ and τ_{BY} such that $\bar{\sigma}_{AXBY} \leq 2^{-\lambda}\mathrm{id}_{AX} \otimes \tau_{BY}$ and $P(\bar{\sigma}_{AXBY}, \sigma_{AXBY}) \leq \varepsilon$. Moreover, without loss of generality [7, Prop. 5.8] we can assume that $\bar{\sigma}_{AXBY}$ is classical and X and Y.

Define $\tilde{\sigma}_{AXBY} = \bar{\sigma}_{AXBY|\Omega}$ and set $\tilde{p} = \Pr_{\bar{\sigma}}[\Omega]$. Since $\bar{\sigma}_{AXBY|\Omega} \leq \frac{1}{\tilde{p}}\bar{\sigma}_{AXBY}$ we immediately find

$$H_{\min}(AX|BY)_{\tilde{\sigma}} \geq H_{\min}^{\varepsilon}(AX|BY)_{\sigma} - \log\frac{1}{\tilde{p}} \geq H_{\min}^{\varepsilon}(AX|BY)_{\sigma} - \log\frac{1}{p-\varepsilon} \tag{90}$$

Furthermore, by the monotonicity of the purified distance under trace non-increasing maps, we have

$$\begin{aligned}
\varepsilon &\geq P(\bar{\sigma}_{AXBY}, \sigma_{AXBY}) && (91)\\
&\geq P(\tilde{p}\cdot\bar{\sigma}_{AXBY|\Omega},\, p\cdot\sigma_{AXBY|\Omega}) && (92)\\
&\geq \frac{1}{2}\big\|\tilde{p}\cdot\bar{\sigma}_{AXBY|\Omega} - p\cdot\sigma_{AXBY|\Omega}\big\|_1 + \frac{1}{2}|\tilde{p}-p| && (93)\\
&= \frac{1}{2}\big\|p(\bar{\sigma}_{AXBY|\Omega} - \sigma_{AXBY|\Omega}) - (p-\tilde{p})\bar{\sigma}_{AXBY|\Omega}\big\|_1 + \frac{1}{2}\big\|(p-\tilde{p})\bar{\sigma}_{AXBY|\Omega}\big\|_1 && (94)\\
&\geq \frac{1}{2}p\big\|\bar{\sigma}_{AXBY|\Omega} - \sigma_{AXBY|\Omega}\big\|_1, && (95)
\end{aligned}$$

where the last inequality follows by the reverse triangle inequality of the trace norm. Hence we have established that $\frac{1}{2}\big\|\tilde{\sigma}_{ABXY} - \sigma_{ABXY|\Omega}\big\| \leq \frac{\varepsilon}{p}$, concluding the proof. □

Let us first proof the following technical statement, of which Theorem 3 will be a corollary.

Proposition 11. *Define $\varepsilon(\nu)$ as in Proposition 8 with $\nu \in (0, \frac{1}{2}-\delta)$ large enough such that $\varepsilon(\nu) \leq 2^{-4}$. Then, the state $\omega_{K_A K_B SCFE} = \texttt{qkd\_simple}_{k,n,\delta,\mathrm{ec},\mathrm{pa}}(\rho_{ABE})$ satisfies*

$$\begin{aligned}
&\Pr_{\omega}\left[F = (\not\perp, \not\perp)\right]\cdot\frac{1}{2}\Big\|\omega_{K_A SCFE|F=(\not\perp,\not\perp)} - \chi_{K_A}\otimes\omega_{SCFE|F=(\not\perp,\not\perp)}\Big\|_1 && (96)\\
&\quad\leq \max\left\{\sqrt{\varepsilon(\nu)},\ \varepsilon(\nu) + \sqrt{\frac{2^{-g(\nu)}}{\varepsilon(\nu)^{\frac{1}{2}}}}\right\}, && (97)
\end{aligned}$$

where $g(\nu) := n\log\frac{1}{\bar{c}} - nh(\delta+\nu) - r - t - \ell$.

Proof. Combining Propositions 6 and 8, we have that either

$$p = \Pr_{\sigma}[F^{\mathrm{pe}} = \not\perp] \leq \sqrt{\varepsilon(\nu)} \qquad \text{or} \qquad H_{\min}^{\varepsilon'}(X|VWS^{\Pi}S^{\Xi}S^{\Theta}E, F^{\mathrm{pe}} = \not\perp)_{\sigma} \geq nq\,, \tag{98}$$

where we set $\varepsilon' = \varepsilon(\nu)/\sqrt{p}$ using the notation of , and $q = \log\frac{1}{\bar{c}} - h(\delta+\nu)$. In particular, $\varepsilon(\nu)$ is defined as in (73) with $\nu \in (0, \frac{1}{2}-\delta]$. In the first case we directly conclude that indeed

$$\Pr_{\omega}[F^{\mathrm{pe}} = F^{\mathrm{ec}} = \not\perp] \leq \sqrt{\varepsilon(\nu)}\,. \tag{99}$$

and the statement of the proposition thus holds.

In the second case, since $p > \sqrt{\varepsilon(\nu)}$, we have that $\varepsilon' \in (0, \varepsilon(\nu)^{3/4})$ and the smooth min-entropy is thus well-defined. The following chain of inequalities holds:

$$\begin{aligned}
nq &\leq H_{\min}^{\varepsilon'}(X|S^{\Pi}S^{\Xi}S^{\Theta}C^{V}E, F^{\mathrm{pe}} = \not\perp)_{\sigma} && (100)\\
&\leq H_{\min}^{\varepsilon'}(X|S^{\Pi}S^{\Xi}S^{\Theta}C^{V}C^{Z}E, F^{\mathrm{pe}} = \not\perp)_{\sigma} + r && (101)\\
&= H_{\min}^{\varepsilon'}(X|S^{\Pi}S^{\Xi}S^{\Theta}S^{H_{\mathrm{ec}}}C^{V}C^{Z}E, F^{\mathrm{pe}} = \not\perp)_{\sigma\otimes\rho} + r && (102)\\
&\leq H_{\min}^{\varepsilon'}(X|S^{\Pi}S^{\Xi}S^{\Theta}S^{H_{\mathrm{ec}}}C^{V}C^{Z}C^{T}F^{\mathrm{ec}}E, F^{\mathrm{pe}} = \not\perp)_{\sigma} + r + t + 1 && (103)
\end{aligned}$$

These inequalities cover the error correction step of the protocol. The first inequality follows by relabelling V to C^{V} and discarding W, an instance of the data-processing inequality. The transcript register C^{Z}

contains the syndrome sent from Alice to Bob and the inequality (101) follows by the chain rule in (52), and the fact that $\log|C^Z| = r$. The register $S^{H_{\text{ec}}}$ in the state $\rho_{S^{H_{\text{ec}}}}$ is independent of σ. Finally, the register C^T contains the hash of the raw key X and F^{ec} is a binary flag indicating whether the error correction step succeeded. The last inequality (103) then follows again from (52) and the fact that $\log|C^T| = t$. Summarizing $S' = (S^\Pi, S^\Xi, S^\Theta, S^{H_{\text{ec}}})$ as well as $C = (C^V, C^Z, C^T)$, and $F = (F^{\text{pe}}, F^{\text{ec}})$ as usual, we can thus write

$$H_{\min}^{\varepsilon'}(X|S'CFE, F^{\text{pe}} = \not\perp)_\sigma \geq nq - r - t - 1\,. \tag{104}$$

We now want to condition on the event $F^{\text{ec}} = \not\perp$ that the error correction step succeeds. For later convenience, let us introduce the notation $p' = \Pr[F^{\text{ec}} = \not\perp | F^{\text{pe}} = \not\perp]$. Lemma 10 now reveals that either $p' \leq \sqrt{\varepsilon(\nu)}$ and, thus, (99) and the statement of the proposition holds, or there exists a state $\tilde{\sigma}_{XS'CFE}$ such that

$$\frac{1}{2}\big\|\tilde{\sigma}_{XS'CFE} - \sigma_{XS'CFE|F=(\not\perp,\not\perp)}\big\|_1 \leq \frac{\varepsilon'}{p'} \leq \frac{\varepsilon(\nu)}{p'p} \quad \text{and} \tag{105}$$

$$H_{\min}(X|S'CFE)_{\tilde{\sigma}} \geq nq - r - t - 1 - \log\frac{1}{p' - \varepsilon'} \geq nq - r - t - 1 - \log\frac{2}{\varepsilon(\nu)^{\frac{1}{2}}}\,. \tag{106}$$

To simplify the second line, we used that $p' - \varepsilon' > \sqrt{\varepsilon(\nu)}\big(1 - \varepsilon(\nu)^{\frac{1}{4}}\big) \geq \frac{1}{2}\sqrt{\varepsilon(\nu)}$, using the assumption that $\varepsilon(\nu) \leq 2^{-4}$ in the last step.

Finally, we want to apply Theorem 5 to the state $\sigma_{XS'CFE|F=(\not\perp,\not\perp)}$ and the seed $\rho_{S^{H_{\text{pa}}}}$. This covers the final protocol step, privacy amplification. Theorem 5 reveals that

$$\frac{1}{2}\big\|\omega_{K_ASCFE|F=(\not\perp,\not\perp)} - \chi_{K_A} \otimes \omega_{SCFE|F=(\not\perp,\not\perp)}\big\|_1 \leq \frac{1}{2}2^{-\frac{1}{2}\left(H_{\min}(X|S'CFE)_{\tilde{\sigma}} - \ell\right)} + \frac{\varepsilon(\nu)}{p'p} \tag{107}$$

$$\leq \sqrt{\frac{2^{-(nq-r-t-\ell)}}{\varepsilon(\nu)^{\frac{1}{2}}}} + \frac{\varepsilon(\nu)}{p'p} \tag{108}$$

Note in particular that the map $\mathcal{E}_f$ defined in Theorem 5 exactly correspond to the privacy amplification step in Section 2.3, marginalized to Alice's system. □

Proof of Theorem 3. We use the notation of Proposition 11. Define the function $q(\nu) = \frac{5}{2}\log\frac{1}{\varepsilon(\nu)}$ which satisfies $q(0) = 0$ and is strictly monotonically increasing in ν. On the other hand, $g(\nu)$ is strictly monotonically decreasing in ν and clearly satisfies $g(\frac{1}{2} - \delta) < 0$. Hence, if $g(0) > 0$ (as in the assumption of the theorem), then there exists a point $\nu_* \in (0, \frac{1}{2} - \delta)$ such that $\varepsilon(\nu_*) = 2^{-\frac{2}{5}g(\nu_*)}$.

We now plug this solution into the statement of Proposition 11. We find

$$\Pr_\omega\big[F = (\not\perp, \not\perp)\big] \cdot \frac{1}{2}\Big\|\omega_{K_ASCFE|F=(\not\perp,\not\perp)} - \chi_{K_A} \otimes \omega_{SCFE|F=(\not\perp,\not\perp)}\Big\|_1 \leq \max\Big\{\sqrt{\varepsilon(\nu_*)},\ 2\varepsilon(\nu_*)\Big\} \tag{109}$$

$$\leq \sqrt{\varepsilon(\nu_*)}, \tag{110}$$

where in the last step we exploited the assumption that $\varepsilon(\nu_*) \leq 2^{-4}$. Hence, the statement of the theorem follows by substituting $\epsilon_{\text{sec}}(\nu) = \sqrt{\varepsilon(\nu)}$. □

Part II

Prepare-And-Measure Protocol

In this part, we discuss a more realistic prepare-and-measure (PM) version of the QKD protocol, essentially BB84 [?], and prove that its security follows from that of the idealized protocol, provided that some additional assumptions are made.

We first describe the realistic version of the protocol in Section 5 and establish its security in Section 6.

$(K_A, K_B, S, C, F) = \texttt{qkd\_PM}_{M,k,n,\delta,\mathrm{ec},\mathrm{pa}}\ (\mathcal{N}_{A\to B})$:

Input: Alice and Bob have access to a quantum channel $\mathcal{N}_{A\to B} : A \to B$ where $A = A_{[M]}$ and $B_{[M]}$ are comprised of M quantum systems.

Randomization: Alice and Bob respectively choose two random strings $\Phi_A, \Phi_B \in \{0,1\}^M$. Both parties further agree on a random subset $\Pi \in \Pi_{m,k}$, and random hash functions $H_{\mathrm{ec}} \in \mathcal{H}_{\mathrm{ec}}$ as well as $H_{\mathrm{pa}} \in \mathcal{H}_{\mathrm{pa}}$. The corresponding uniformly random seeds are denoted $S = (S^{\Phi_A}, S^{\Phi_B}, S^{\Pi}, S^{H_{\mathrm{ec}}}, S^{H_{\mathrm{pa}}})$.

State Preparation: Alice chooses a random string $r \in \{0,1\}^M$ and prepares a quantum state ρ_A^{r,ϕ_A}, encoding the string r in the measurement basis corresponding to ϕ_A.

State Distribution: Alice sends the state ρ_A^{r,ϕ_A} through the quantum channel $\mathcal{N}$ and Bob receives the output state $\rho_B^{r,\phi_A} = \mathcal{N}(\rho_A^{r,\phi_A})$.

Measurement: Bob measures the M quantum systems with the setting Φ_B, and stores his ternary measurement outcomes in a string $T \in \{0,1,\emptyset\}^M$, where $\emptyset$ denotes an inconclusive measurement result. Bob publicly announces both the value of Φ_B, with transcript C^{Φ_B} and the set $\Omega \subseteq 2^{[M]}$ of indices such that $T_\Omega \in \{0,1\}^{|\Omega|}$ and $T_{\bar{\Omega}} = \emptyset^{M-|\Omega|}$. The corresponding transcript is denoted C^{Ω}.

Sifting: If it exists, Alice publicly announces a set $\Sigma \subseteq \Omega$, with transcript C^{Σ} of cardinality m, such that Φ_A and Φ_B coincide on Σ, and sets the flag $F^{\mathrm{sift}} =\not\perp$. Otherwise, she sets $F^{\mathrm{sift}} =\perp$ and they abort. The respective binary substrings of R and T restricted to Σ become the raw keys. As in the idealized protocol, they are denoted (X, V) and (Y, W) for Alice and Bob, respectively. Here V, W are of length k and correspond to the indices in Π, whereas X, Y of length n correspond to indices not in Π.

Parameter Estimation: Alice sends V to Bob, the transcript is denoted C^V. Bob compares V and W. If the fraction of errors exceeds δ, Bob sets the flag $F^{\mathrm{pe}} =$ '$\perp$' and they abort. Otherwise he sets $F^{\mathrm{pe}} =$ '$\not\perp$' and they proceed.

Error Correction: Alice sends the syndrome $Z = \mathrm{synd}(X)$ to Bob, with transcript C^Z. Bob computes $\hat{X} = \mathrm{corr}(Y, Z)$.

Alice computes the hash $T = H_{\mathrm{ec}}(X)$ of length t and sends it to Bob, with transcript C^T. Bob computes $H_{\mathrm{ec}}(\hat{X})$. If it differs from T, he sets the flag $F^{\mathrm{ec}} =$ '$\perp$' and they abort the protocol. Otherwise he sets $F^{\mathrm{ec}} =$ '$\not\perp$' and they proceed.

Privacy Amplification: They compute keys $K_A = H_{\mathrm{pa}}(X)$ and $K_B = H_{\mathrm{pa}}(\hat{X})$ of length ℓ.

Output: The output of the protocol consists of the keys K_A and K_B, the seeds $S = (S^{\Phi_B}, S^{\Pi}, S^{H_{\mathrm{ec}}}, S^{H_{\mathrm{pa}}})$, the transcript $C = (C^{\Omega}, C^{\Sigma}, C^{V}, C^{Z}, C^{H})$ and the flags $F = (F^{\mathrm{sift}}, F^{\mathrm{pe}}, F^{\mathrm{ec}})$. In case of abort, we assume that all registers are initialized to a predetermined value.

Table 4: Realistic Prepare-and-Measure QKD Protocol. The precise mathematical model is described in Section 5. This protocol differs from the ideal version in several points: in particular, the input now corresponds to the quantum channel $\mathcal{N}$ between Alice and Bob.

5 The Prepare-And-Measure Protocol

We consider the simplest possible implementation of a Prepare and Measure version of BB84. This section provides the details of the protocol described in Table 4, for the steps where it differs from the idealized protocol.

The protocol $\texttt{qkd\_PM}_{M,k,n,\delta,\mathrm{sift},\mathrm{ec},\mathrm{pa}}$ is parametrized similarly as the simple protocol of Section 2, with two extra parameters: an integer $M \geq k+n$ counting the number of individual states prepared by Alice, and a *sifting* procedure described by a classical map $\mathrm{sift} : \{0,1\}^M \times \{0,1\}^M \times 2^{[M]} \to \Pi_{M,m} \times \{\perp, \not\perp\}$.

5.1 Preparation and Measurement Devices

Bob's measurement operators are the same as in the entanglement-based protocol, although they now need to be specified for indices in $[M]$ and have an additional outcome, '$\emptyset$', corresponding to an inconclusive result. An inconclusive result can for instance occur when no detector clicked (photon loss) or when more than 1 detector clicked (shot noise). Bob's measurement on subsystem B_i is a binary generalized measurement $\{M^{\phi,t}_{B_i}\}_{t\in\{0,1,\emptyset\}}$.

Alice's, on the other hand, is able to prepare states $\rho^{r,\phi}_{A_i}$ where $r, \phi \in \{0,1\}$ on each subsystem A_i.

5.2 Mathematical Model of the Protocol

He we describe in detail the mathematical model corresponding to the protocol in Table 4.

Input: The realistic protocol $\texttt{qkd\_PM}_{M,k,n,\delta,\mathrm{sift},\mathrm{ec},\mathrm{pa}}$ we consider is a 'prepare and measure' protocol, based on BB84, and the role of the input is now played by an (arbitrary) quantum channel $\mathcal{N}_{A\to B}$ between Alice and Bob. Here $A = A_{[M]}$ and $B = B_{[M]}$.

Randomization: The random seeds are modeled similarly as for the idealized version of the protocol. Here, the seed S^Φ corresponding to identical measurement settings is not provided directly. Instead, Alice and Bob initially choose independently two strings $\Phi_A, \Phi_B \in \{0,1\}^M$, and it will later be the role of the sifting procedure to produce a set of identical measurement settings Φ. The random choice of the strings Φ_A, Φ_B is modeled by two registers S^{Φ_A}, S^{Φ_B} in the state

$$\rho_{S^{\Phi_A}} \otimes \rho_{S^{\Phi_B}} = \frac{1}{4^M} \sum_{\phi_A,\phi_B\in\{0,1\}^M} |\phi_A\rangle\langle\phi_A|_{S^{\Phi_A}} \otimes |\phi_B\rangle\langle\phi_B|_{S^{\Phi_B}}\,, \tag{111}$$

where $\{|\phi_A\rangle\}, \{|\phi_B\rangle\}$ are orthonormal bases of S^{Φ_A} and S^{Φ_B}, respectively.

The other random seeds $\rho_{S^\Pi}, \rho_{S^{H_{\mathrm{ec}}}}, \rho_{S^{H_{\mathrm{pa}}}}$ are identical to the idealized version.

State preparation: Alice randomly chooses an M-bit strings $r \in \{0,1\}^M$. This is modeled as an extra register R in the state

$$\rho_R = \frac{1}{2^M} \sum_{r\in\{0,1\}^M} |r\rangle\langle r|_R \tag{112}$$

where $\{|r\rangle\}$ is an orthonormal basis of R.

Alice then prepares a state using the map

$$\mathcal{P}_{\emptyset\to A|RS^{\Phi_A}}(\cdot) = \sum_{r,\phi\in\{0,1\}^M} \Big(|r\rangle\langle r|_R \otimes |\phi\rangle\langle\phi|_{S^{\Phi_A}}\Big) \cdot \Big(|r\rangle\langle r|_R \otimes |\phi\rangle\langle\phi|_{S^{\Phi_A}}\Big) \otimes \rho^{r,\phi}_A \tag{113}$$

where $\rho^{r,\phi}_A = \bigotimes_{i=1}^M \rho^{r_i,\phi_i}_{A_i}$.[2] Applying this map to the seeds in registers R and S_{Φ_A} gives:

$$\rho_{RS^{\Phi_A}A} = \frac{1}{4^M} \sum_{r,\phi\in\{0,1\}^M} |r\rangle\langle r|_R \otimes |\phi\rangle\langle\phi|_{S^{\Phi_A}} \otimes \rho^{r,\phi}_A. \tag{115}$$

[2] In an ideal implementation, the states ρ^{r,ϕ^A} would be given by

$$\rho^{0,0} = |0\rangle\langle 0|\,, \quad \rho^{1,0} = |1\rangle\langle 1|\,, \quad \rho^{0,1} = |+\rangle\langle +|\,, \quad \rho^{1,1} = |-\rangle\langle -|\,. \tag{114}$$

State distribution: Alice sends her register A to Bob through the quantum channel $\mathcal{N} : A \to B$. The state shared by Alice and Bob is given by:

$$\begin{aligned}\rho_{RS^{\Phi_A}B} &= \mathcal{N}_{A\to B}(\rho_{RS^{\Phi_A}A'}) && (116)\\ &= \frac{1}{4^M}\sum_{r,\phi\in\{0,1\}^M} |r\rangle\langle r|_R \otimes |\phi\rangle\langle\phi|_{S^{\Phi_A}} \otimes \rho_B^{r,\phi}, && (117)\end{aligned}$$

where we defined $\rho_B^{r,\phi} = \mathcal{N}\left(\rho_{A'}^{r,\phi}\right)$.

Measurement: Bob measures each of his M quantum systems in the basis corresponding to Φ_B and stores his measurement outcomes, either 0, 1, or $\emptyset$ in the case of inconclusive outcomes, in a string $T \in \{0,1,\emptyset\}^M$. The measurement map $\mathcal{M}_{B\to T\Omega|S^{\Phi_B}} : BS^{\Phi_B} \to TB\Omega S^{\Phi_B}$ is defined as:

$$\mathcal{M}_{B\to T\Omega|S^{\Phi_B}}(\cdot) = \sum_{\phi\in\{0,1\}^M}\sum_{t\in\{0,1,\emptyset\}^M} |t,\omega\rangle_{TC^\Omega}\left(M_B^{\phi,t}\otimes|\phi\rangle\langle\phi|_{S^{\Phi_B}}\right)\cdot\left(M_B^{\phi,t}\otimes|\phi\rangle\langle\phi|_{S^{\Phi_B}}\right)^\dagger\langle t,\omega|_{TC^\Omega}, \tag{118}$$

where $\omega = \omega(t)$ is the subset of $[M]$ where t takes values in $\{0,1\}$, namely

$$\omega(t) = \{i\in[M] \,:\, t_i \neq \emptyset\}. \tag{119}$$

The state of the total system after Bob's measurement is given by

$$\sigma_{RTC^\Omega BS^{\Phi_A}S^{\Phi_B}} = \frac{1}{8^M}\sum_{r,\phi_A,\phi_B\in\{0,1\}^M} |r,t,\omega,\phi_A,\phi_B\rangle\langle r,t,\omega,\phi_A,\phi_B|_{RTC^\Omega S^{\Phi_A}S^{\Phi_B}} \otimes M_B^{\phi_B,t}\rho_B^{r,\phi_A}\left(M_B^{\phi_B,t}\right)^\dagger. \tag{120}$$

Sifting: Bob publicly announces the content of the register S^{Φ_B} together with the description C^Ω of the set Ω of indices corresponding to conclusive measurement results.

Alice then applies the *sifting map*, a classical map 'sift'defined as follows

$$\text{sift} : \left\{\begin{array}{ccc}\{0,1,\emptyset\}^M\times\{0,1,\emptyset\}^M\times 2^{[M]} & \to & \Pi_{M,m}\times\{\perp,\not\perp\}\\ (\Phi_A,\Phi_B,\Omega) & \mapsto & (\Sigma,F^{\text{sift}})\end{array}\right. \tag{121}$$

where Σ is either the first subset of Ω of cardinality m in the lexicographic order where Φ_A and Φ_B coincide, if such a set exists, or else σ is set to $[m]$. In the first case, the flag F^{sift} is set to $\not\perp$, otherwise it is set to $\perp$ and the protocol aborts.

This classical map is lifted to give a CPTP map $\mathcal{E}_{\text{sift}} = S^{\Phi_A}S^{\Phi_B}C^\Omega \to C^\Sigma C^\Omega F^{\text{sift}}S^{\Phi_A}S^{\Phi_B}$.

We then define an CPTP map $\mathcal{E}_{\text{ro}}$ that considers the set Σ and the subset Π and reorders the registers of $A_{[M]}, B_{[M]}, R_{[M]}, T_{[M]}$ and puts the k registers corresponding to the subset Π of Σ first, followed by the n registers of the subset $\bar{\Pi}$ of Σ, while tracing out the remaining $(M-m)$ registers, and creates a new register S^Φ containing the restriction of Φ_A to Σ:

$$\mathcal{E}_{\text{ro}} : C^\Sigma S^\Pi A_{[M]}B_{[M]}R_{[M]}T_{[M]}S^{\Phi_A}S^{\Phi_B} \to A_{\Pi\circ\Sigma}VB_{\Pi\circ\Sigma}WA_{\bar{\Pi}\circ\Sigma}XB_{\bar{\Pi}\circ\Sigma}YC^\Sigma S^\Phi S^\Pi S^{\Phi_A}S^{\Phi_B}. \tag{122}$$

We will sometimes abuse notation and denote A for $A_{\Pi\circ\Sigma}A_{\bar{\Pi}\circ\Sigma}$ (and instead for B) when it is clear that we consider a state after the map $\mathcal{E}_{\text{ro}}$ was applied.

Remaining steps: The remaining steps are as in the entanglement-based QKD protocol.

Step	Input State		Output State
Input:			$\mathcal{N}$
Randomization:			$\rho_{S^{\Phi_B}} \otimes \rho_{S^{\Phi_B}} \otimes \rho_{S^{\Pi}} \otimes \rho_{S^{H_{\text{ec}}}} \otimes \rho_{S^{H_{\text{pa}}}}$
State preparation:	$\rho_{RS^{\Phi_A}}$		$\rho_{RS^{\Phi_A}A'}$
State distribution:	$\rho_{RS^{\Phi_A}A'}$		$\rho_{RS^{\Phi_A}B}$
Measurement:	$\rho_{RS^{\Phi_A}B} \otimes \rho_{S^{\Phi_B}}$	$\mapsto$	$\sigma_{RTC^{\Omega}BS^{\Phi_A}S^{\Phi_B}}$
Sifting:	$\sigma_{RTC^{\Omega}BS^{\Phi_A}S^{\Phi_B}} \otimes \rho_{S^{\Pi}}$	$\mapsto$	$\sigma_{VWXYBS^{\Phi}S^{\Pi}C^{\Omega}C^{\Sigma}F^{\text{sift}}}$
Parameter Estimation:	σ_{VW}	$\mapsto$	$\sigma_{C^V F^{\text{pe}}}$
Error Correction:	$\sigma_{XY} \otimes \rho_{S^{H_{\text{ec}}}}$	$\mapsto$	$\sigma_{X\hat{X}C^Z F^{\text{ec}}}$
Privacy Amplification:	$\sigma_{X\hat{X}} \otimes \rho_{S^{H_{\text{pa}}}}$	$\mapsto$	$\omega_{K_A K_B C^H}$
Output:			$\omega_{K_A K_B SCF}$

Table 5: Evolution of the registers during the execution of the realistic Prepare and Measure QKD Protocol.

6 Security: Reduction to the Entanglement-Based Protocol

The security proof should establish that for any input channel $\mathcal{N}_{A\to B}$ given to $\texttt{qkd\_PM}_{M,k,n,\delta,\text{ec},\text{pa}}$, either the protocol outputs secret identical keys, or else it aborts. In the same spirit as the entanglement-based version, we define the security parameter

$$\Delta_{M,k,n,\delta,\text{ec},\text{pa}} := \sup_{\mathcal{N}_{A\to BE}} \frac{1}{2}\left\| \texttt{qkd\_PM}_{M,k,n,\delta,\text{ec},\text{pa}}(\mathcal{N}_{A\to BE}) - \texttt{qkd\_ideal}_{M,k,n,\delta,\text{ec},\text{pa}}(\mathcal{N}_{A\to BE}) \right\|_1, \tag{123}$$

where again $\texttt{qkd\_ideal}_{M,k,n,\delta,\text{ec},\text{pa}}$ is defined analogously to the entanglement-based case and simply replaces the output of $\texttt{qkd\_PM}_{M,k,n,\delta,\text{ec},\text{pa}}(\mathcal{N}_{A\to BE})$ with a perfect key in case the protocol does not abort. Here, the channels $\mathcal{N}_{A\to BE}$ have an additional output that goes to an eavesdropper, and it again suffices to consider maps where E is finite-dimensional.

Establishing security proof thus boils down to showing that this trace distance is small for all such channels. The following Lemma, along the same lines as the discussion for the entanglement-based case, gives a sufficient condition for this.

Lemma 12. *If, for every $\mathcal{N}_{A\to BE}$ as in (123), the state $\omega_{K_A K_B SCFE} = \texttt{qkd\_PM}_{M,k,n,\delta,\text{ec},\text{pa}}(\mathcal{N}_{A\to BE})$ satisfies $\frac{1}{2}\left\|\omega_{K_A K_B SCFE|F^{\text{sift}}=\not\perp} - \chi_{K_A K_B} \otimes \omega_{SCFE|F^{\text{sift}}=\not\perp}\right\|_1 \leq \epsilon$, then we have $\Delta_{M,k,n,\delta,\text{ec},\text{pa}} \leq \epsilon$.*

Our strategy is to show that the realistic protocol is equivalent to applying the idealized QKD protocol on a virtual quantum state ρ_{AB} and that the random seed S^{Φ} is uniformly distributed. For this, we need to make explicit assumptions about (i) the state preparation on Alice's side to make sure that no basis information is leaked and (ii) the measurement device on Bob's side to ensure that the invalid measurement results do not depend on the measurement basis.

6.1 Assumptions on the Devices

We need to impose strict conditions on Bob's measurement devices and Alice's states in case we want to reduce the security of the protocol to the entanglement-based protocol, and these will be discussed next.

6.1.1 Assumption 1: Alice's state:

The state $\rho_{R\Phi_A A}$ prepared by Alice should not leak any information about the basis choice Φ_A, i.e., we need that

$$\operatorname{tr}_R(\rho_{R\Phi_A A}) = \rho_{\Phi_A} \otimes \rho_A. \tag{124}$$

In other words, the marginal state $\rho_{A'}$ does not leak any information about the basis choice made by Alice. Note that Assumption 1 is equivalent to

$$\sum_{r\in\{0,1\}^M} \rho_A^{r,\phi} = \sum_{r\in\{0,1\}^M} \rho_A^{r,\phi'}, \tag{125}$$

for any pair $\phi, \phi' \in \{0,1\}^M$.

This assumption allows us to replace the state preparation by a virtual measurement.

Lemma 13 (Virtual entanglement)**.** *If Assumption 1 in* (124) *holds, then there exists a state $\rho_{AA'}$ and a measurement map $\mathcal{M}_{A'\to R|S^{\Phi_A}}$ such that*

$$\rho_{R\Phi_A A} = \mathcal{M}_{A'\to R|S^{\Phi_A}} \left(\rho_{AA'} \otimes \rho_{\Phi_A}\right). \tag{126}$$

Proof. The assumption implies that the sum

$$\rho_A = \frac{1}{2^M} \sum_{r\in\{0,1\}^M} \rho_A^{r,\phi} \tag{127}$$

is independent of the parameter ϕ. This in turn ensures the existence of an extension $\rho_{AA'}$ of ρ_A and of measurement operators $M_{A'}^{r,\phi}$ such that

$$\sum_{r\in\{0,1\}^M} \left(M_{A'}^{r,\phi}\right)^\dagger M_{A'}^{r,\phi} = \mathrm{id}_A \quad \text{and} \quad \rho_A^{r,\phi} = \mathrm{tr}_{A'}\left(M_{A'}^{r,\phi} \rho_{AA'} \left(M_{A'}^{r,\phi}\right)^\dagger\right). \tag{128}$$

Let us therefore define the measurement map $\mathcal{M}_{A'\to R|S^{\Phi_A}} : A'\Phi_A \to RA\Phi_A$:

$$\mathcal{M}_{A'\to R|S^{\Phi_A}}(\cdot) = \sum_{r\in\{0,1\}^M} \sum_{\phi\in\{0,1\}^M} |r\rangle_R \left(M_{A'}^{r,\phi} \otimes |\phi\rangle\langle\phi|_{\Phi_A}\right) \cdot \left(M_{A'}^{r,\phi} \otimes |\phi\rangle\langle\phi|_{\Phi_A}\right)^\dagger \langle r|_R. \tag{129}$$

One can easily check that $\rho_{R\Phi_A A} = \mathcal{M}_{A'\to R|S^{\Phi_A}} \left(\rho_{AA'} \otimes \rho_{\Phi_A}\right)$. □

6.1.2 Assumption 2: Bob's measurement:

Bob's measurement map can be decomposed as follows:

$$\mathcal{M}_{B\to T\Omega|S^{\Phi_B}} = \mathcal{M}_{B\to T|S^{\Phi_B}} \circ \mathcal{M}_{B\to\Omega}, \tag{130}$$

where $\mathcal{M}_{B\to\Omega} : B \to B\Omega$ is given by

$$\mathcal{M}_{B\to\Omega}(\cdot) = \sum_{s\in\{\emptyset,\bar{\emptyset}\}^M} |\omega\rangle_\Omega \left(M_B^s\right) \cdot \left(M_B^s\right)^\dagger \langle\omega|_\Omega\,. \tag{131}$$

where $\omega(s) = \{i \in [M] : s_i \neq \emptyset\}$.

This decomposition allows us to perform the sifting operation prior to the actual measurement, i.e. the sifting step and the measurement commute in the sense of the next lemma.

Lemma 14. *Assume Assumption 2 holds. For any state $\rho_{A'BE}$, define*

$$\rho_{A'BC^\Sigma C^\Omega S^\Phi EF^{\mathrm{sift}}} = \mathcal{E}_{\mathrm{ro}} \circ \mathcal{E}_{\mathrm{sift}} \circ \mathcal{M}_{B\to\Omega}(\rho_{A'BE} \otimes \rho_{S^{\Phi_A}} \otimes \rho_{S^{\Phi_B}}). \tag{132}$$

Then, the state conditioned on the sifting procedure passing satisfies:

$$\rho_{A'BS^\Phi C^\Sigma C^\Omega E|F^{\mathrm{sift}}=\not\perp} = \rho_{A'BC^\Sigma C^\Omega E|F^{\mathrm{sift}}=\not\perp} \otimes \rho_{S^\Phi}, \tag{133}$$

where $\rho_{S^\Phi} = \frac{1}{2^m}\sum_{\phi\in\{0,1\}^m} |\phi\rangle\langle\phi|_\Phi$.

Proof. Since the map $\mathcal{M}_{B\to\Omega}$ only acts on register B, independently on the value of Φ_B,

$$\mathcal{M}_{B\to\Omega}(\rho_{A'BE} \otimes \rho_{S^{\Phi_A}} \otimes \rho_{S^{\Phi_B}}) = \rho_{A'BC^\Omega E} \otimes \rho_{S^{\Phi_A}} \otimes \rho_{S^{\Phi_B}}\,, \tag{134}$$

where the state $\rho_{A'BC^\Omega E} = \mathcal{M}_{B\to\Omega}(\rho_{A'BE})$ can be expanded as:

$$\rho_{A'BC^\Omega E} = \sum_{s\in\{\emptyset,\bar{\emptyset}\}^M} |\omega\rangle_{C^\Omega} \left(M_B^s\right) \rho_{A'BE} \left(M_B^s\right)^\dagger \langle\omega|_{C^\Omega}\,. \tag{135}$$

The classical map 'sift' has the following property: for any string $\theta \in \{0,1\}^M$ and any subset $\Omega \subseteq [M]$, if the sifting succeeds, then

$$\mathrm{sift}(\phi_A + \theta, \phi_B + \theta, \Omega) = \mathrm{sift}(\phi_A, \phi_B, \Omega). \tag{136}$$

The map $\mathcal{E}_{\mathrm{ro}}$ examines the register S^{Φ_A} and puts its content (restricted to the set Σ determined by the sifting map) into register S^Φ. The above property of the sifting map ensures that the value of Φ does not depend on Ω. Moreover, it Φ_A and Φ_B are initially independent and uniformly distributed, then so is Φ.

This proves that whenever the sifting test passes, the output state takes a tensor product form: $\rho_{A'BS^\Phi C^\Sigma C^\Omega E|F^{\mathrm{sift}}=\not\perp} = \rho_{A'BC^\Sigma C^\Omega E|F^{\mathrm{sift}}=\not\perp} \otimes \rho_{S^\Phi}$. □

6.2 Security Statement and Proof

Under these assumptions, we show that the realistic QKD protocol is secure.

Theorem 15. *Under Assumptions 1 and 2, if the protocol* qkd_simple$_{k,n,\delta,\mathrm{ec,pa}}$ *is ϵ-secure with $\bar{c}$ evaluated for the measurements specified in Lemma 13, then* qkd_PM$_{M,k,n,\delta,\mathrm{sift,ec,pa}}$ *is also ϵ-secure.*

Proof. Let us consider the input state $\rho_{R\Phi_A B} \otimes \rho_{S^{\Phi_B}}$ The assumption on Alice's state preparation together with Lemma 13 proves the existence of a state $\rho_{A'BE} \otimes \rho_{S^{\Phi_B}} = \mathcal{N}_{A\to BE}(\rho_{AA'}) \otimes \rho_{S^{\Phi_B}}$ such that $\rho_{R\Phi_A B} = \mathcal{M}_{A'\to R|S^{\Phi_A}}(\rho_{A'B} \otimes \rho_{S^{\Phi_A}})$.

Define the QKD protocol qkd_modified$_{k,n,\delta,\mathrm{ec,pa}}$ similarly as the idealized version of the protocol, qkd_simple$_{k,n,\delta,\mathrm{ec,pa}}$, with the exception that the randomness for the measurement basis choice is explicitly given as an input. In particular, one has:

$$\texttt{qkd\_modified}_{k,n,\delta,\mathrm{ec,pa}}(\rho_{A'BE} \otimes \rho_{S^\Phi}) = \texttt{qkd\_simple}_{k,n,\delta,\mathrm{ec,pa}}(\rho_{A'B})\,. \tag{137}$$

The sifting map $\mathcal{E}_{\mathrm{sift}} \otimes \mathcal{M}_{B\to\Omega}$ commutes with $\mathcal{M}_{A'\to R|S^{\Phi_A}}$, which implies that

$$\begin{aligned}\mathcal{E}_{\mathrm{sift}} \otimes \mathcal{M}_{B\to\Omega}\left(\rho_{R\Phi_A B}\right) &= \mathcal{M}_{A'\to R|S^{\Phi_A}} \circ \mathcal{E}_{\mathrm{sift}} \otimes \mathcal{M}_{B\to\Omega}\big(\rho_{A'B} \otimes \rho_{S^{\Phi_A}}\big) &(138)\\ &= \mathcal{M}_{A'\to R|S^{\Phi_A}}\big(\rho_{A'BS^\Phi C^\Sigma F^{\mathrm{sift}}}\big). &(139)\end{aligned}$$

Moreover, using Lemma 14, conditioning on the sifting test passing, one obtains $\rho_{A'BS^\Phi C^\Sigma C^\Omega E|F^{\mathrm{sift}}=\not\perp} = \rho_{A'BC^\Sigma C^\Omega E} \otimes \rho_{S^\Phi}$, which means that

$$\texttt{qkd\_modified}_{k,n,\delta,\mathrm{ec,pa}}\left(\rho_{A'BS^\Phi C^\Sigma C^\Omega E|F^{\mathrm{sift}}=\not\perp}\right) = \texttt{qkd\_simple}_{k,n,\delta,\mathrm{ec,pa}}\left(\rho_{A'BC^\Sigma C^\Omega E}\right)\,. \tag{140}$$

Let us now collect $E' = C^\Sigma C^\Omega E$. Finally, if the sifting test passes, one has the following equalities:

$$\begin{aligned}\texttt{qkd\_PM}_{M,k,n,\delta,\mathrm{sift,ec,pa}}(\mathcal{N}_{A\to BE}) &= \texttt{qkd\_modified}_{k,n,\delta,\mathrm{ec,pa}}\left(\rho_{ABS^\Phi E'|F^{\mathrm{sift}}=\not\perp}\right) &(141)\\ &= \texttt{qkd\_simple}_{k,n,\delta,\mathrm{ec,pa}}\left(\rho_{A'BE'}\right), &(142)\end{aligned}$$

which, together with Lemma 12, concludes the proof. □

A Proof of Entropic Uncertainty Relation in Theorem 4

We will show that $H^{\varepsilon}_{\min}(X|BP)_\sigma + H^{\varepsilon}_{\max}(X|CP)_\sigma \geq \log \frac{1}{c_q}$ for the definitions given in Theorem 4. (Note that we have changed notation here by interchanging B and C.) For this purpose, we first introduce the Stinespring dilation isometry of the measurement map $\mathcal{M}_X$. This is the isometry $V_X : PA \to PAXX'$ given by

$$V_X := \sum_{p \in P} \sum_{x \in X} |x\rangle_X \otimes |x\rangle_{X'} \otimes |p\rangle\!\langle p|_P \otimes F^{p,x}_A \tag{143}$$

Now note that σ_{XBP} has a natural purification in

$$\sigma_{XX'ABCDPP'} = V_X \big(\tau_{ABCD} \otimes \psi_{PP'}\big) V_X^\dagger \,, \tag{144}$$

where $\psi_{PP'}$ is a maximally entangled state and τ_{ABCD} is any purification of τ_{ABC}.

The proof is now split into two parts.

- The main technical difficulty lies in Lemma 16 below, which asserts that

$$H^{\varepsilon}_{\min}(X|BP)_\sigma \geq H^{\varepsilon}_{\min}(X|X'ABP)_\sigma + \log \frac{1}{c_q} \,. \tag{145}$$

- Then, applying the duality relation in (50) to (145) yields

$$H^{\varepsilon}_{\min}(X|BP)_\sigma + H^{\varepsilon}_{\max}(X|CDP')_\sigma \geq \log \frac{1}{c_q} \,. \tag{146}$$

  The desired result then follows from the DPI in (51) applied for the CPTP map tr_D, and the fact that $\sigma_{XCP'}$ is isomorphic to σ_{XCP}.

Lemma 16. *Equation (145) holds for $\sigma_{XX'ABCDPP'}$ defined as in (143)–(144).*

Proof. Let us consider the following unitary rotations (permutation):

$$Q_P = \sum_{p \in P} |q(p)\rangle\!\langle p|_P \,. \tag{147}$$

that exchange p with its conjugate, $q(p)$. Clearly we have $Q_P(\rho_{ABCP})Q_P^\dagger = \rho_{ABCP}$ due to the symmetry condition on q. Based on this we define the isometry

$$\bar{V}_X := Q_P V_X Q_P^\dagger = \sum_{p \in P} \sum_{x \in X} |x\rangle_X \otimes |x\rangle_{X'} \otimes |p\rangle\!\langle p|_P \otimes F^{q(p),x}_A \,, \tag{148}$$

and note that

$$\bar{V}_X V_X^\dagger \sigma_{XX'ABCP} V_X \bar{V}_X^\dagger = Q_P V_X Q_P^\dagger (\rho_{ABCP}) Q_P V_X^\dagger Q_P^\dagger \tag{149}$$

$$= Q_P \sigma_{XX'ABCP} W_P^\dagger \,. \tag{150}$$

The CP trace non-increasing map $\bar{V}_X V_X^\dagger (\cdot) V_X \bar{V}_X^\dagger$ coherently undoes the measurement in the basis determined by q and then instead measures in the basis determined by $q(p)$.

By the definition of the smooth min-entropy, $H^{\varepsilon}_{\min}(X|X'ABP)_\sigma = \lambda$, there exists a state $\tilde{\sigma}_{XX'ABP}$ with $P(\sigma_{XX'ABP}, \tilde{\sigma}_{XX'ABP}) \leq \varepsilon$ and a state $\omega_{X'ABP} \in \mathcal{S}(X'ABP)$ such that

$$\tilde{\sigma}_{XX'ABP} \leq 2^{-\lambda}\, \mathrm{id}_X \otimes \omega_{X'ABP} \,. \tag{151}$$

Next we consider the CP trace non-increasing map

$$\mathcal{F}_{XX'A \to X|P}[\,\cdot\,] = \sum_{p \in P} \mathrm{tr}_{X'A} \Big(W_P^\dagger \bar{V}_X V_X^\dagger \, |p\rangle\!\langle p|_P \,\cdot\, |p\rangle\!\langle p|_P \, V_X \bar{V}_X^\dagger W_P \Big) . \tag{152}$$

From (150) we learn that $\mathcal{F}\big[\sigma_{XX'ABP}\big] = \sigma_{XBP}$. Thus, using the fact that the purified distance contracts (47) when we apply $\mathcal{F}$, we find that the state $\hat{\sigma}_{XBP} = \mathcal{F}\big[\tilde{\sigma}_{XX'ABP}\big]$ satisfies

$$P(\hat{\sigma}_{XBP}, \sigma_{XBP}) \leq P(\tilde{\sigma}_{XX'ABP}, \sigma_{XX'ABP}) \leq \varepsilon. \tag{153}$$

Furthermore, Applying $\mathcal{F}$ on both sides of (151) yields

$$\hat{\sigma}_{XBP} \leq 2^{-\lambda}\mathcal{F}\big[\mathrm{id}_X \otimes \omega_{X'ABP}\big] = 2^{-\lambda}\,\mathrm{tr}_{X'A}\Big(W_P^\dagger \bar{V}_X V_X^\dagger \big(\mathrm{id}_X \otimes \hat{\omega}_{X'ABP}\big) V_X \bar{V}_X^\dagger W_P\Big), \tag{154}$$

where $\hat{\omega}_{X'ABP} = \sum_{p\in P} |p\rangle\!\langle p|_P \otimes \hat{\omega}^p_{X'AB}$ with $\hat{\omega}^p_{X'AB} = \langle p|\,\omega_{X'ABP}\,|p\rangle_P$. Let us now simplify the right-hand side of this inequality using Claim 17 below, which asserts that

$$\mathcal{F}\big[\mathrm{id}_X \otimes \omega_{X'ABP}\big] \leq c_q \cdot \sum_{p\in P} \mathrm{id}_X \otimes |p\rangle\!\langle p|_P \otimes \hat{\omega}^p_B\,. \tag{155}$$

Combining this bound with (154) yields

$$\hat{\sigma}_{XBP} \leq 2^{-\lambda} c_q \cdot \mathrm{id}_X \otimes \sum_{p\in P} |p\rangle\!\langle p|_P \otimes \hat{\omega}^p_B\,. \tag{156}$$

Since $\sum_{p\in P} \mathrm{tr}(\hat{\omega}^p_B) = 1$ by construction and $P(\hat{\sigma}_{XBP}, \sigma_{XBP}) \leq \varepsilon$ due to (153), the definition of the smooth entropy implies that

$$H^\varepsilon_{\min}(X|BP)_\sigma \geq \lambda - \log c_q = H^\varepsilon_{\min}(X|X'ABP)_\sigma - \log c_q\,, \tag{157}$$

concluding the proof. □

Claim 17. *Equation* (155) *holds.*

Proof. First, we note that

$$W_P^\dagger \bar{V}_X V_X^\dagger = \sum_{p\in P}\sum_{x,z\in X} |z\rangle\!\langle x|_X \otimes |z\rangle\!\langle x|_{X'} \otimes \big|q(p)\big\rangle\!\big\langle p\big|_P \otimes F_A^{q(p),z}\big(F_A^{p,x}\big)^\dagger\,. \tag{158}$$

and, hence, we can simplify

$$\begin{aligned}
&\mathcal{F}\big[\mathrm{id}_X \otimes \omega_{X'ABP}\big]\\
&\quad= \sum_{p\in P}\sum_{x,z\in X} |x\rangle\!\langle x|_X \otimes |q(p)\rangle\!\langle q(p)|_P \otimes \langle z|\,\mathrm{tr}_A\Big(F_A^{q(p),z}\big(F_A^{p,x}\big)^\dagger \hat{\omega}^p_{X'AB} F_A^{p,x}\big(F_A^{q(p),z}\big)^\dagger\Big)\,|z\rangle_{X'} &(159)\\
&\quad\leq \sum_{p\in P}\sum_{x,z\in X} |x\rangle\!\langle x|_X \otimes |q(p)\rangle\!\langle q(p)|_P \otimes \Big\|F_A^{p,x}\big(F_A^{q(p),z}\big)^\dagger F_A^{q(p),z}\big(F_A^{p,x}\big)^\dagger\Big\|_\infty \langle z|\,\mathrm{tr}_A\big(\hat{\omega}^p_{X'AB}\big)\,|z\rangle_{X'} &(160)\\
&\quad= \sum_{p\in P}\sum_{x,z\in X} |x\rangle\!\langle x|_X \otimes |q(p)\rangle\!\langle q(p)|_P \otimes \Big\|F_A^{q(p),x}\big(F_A^{p,z}\big)^\dagger\Big\|_\infty^2 \langle z|\,\hat{\omega}^p_{X'B}\,|z\rangle_{X'} &(161)\\
&\quad\leq \max_{p\in P}\max_{x,z\in X}\Big\|F_A^{q(p),x}\big(F_A^{p,z}\big)^\dagger\Big\|_\infty^2 \cdot \sum_{p\in P}\sum_{x,z\in X} |x\rangle\!\langle x|_X \otimes |p\rangle\!\langle p|_P \otimes \langle z|\,\hat{\omega}^p_{X'B}\,|z\rangle_{X'} &(162)\\
&\quad= c_q \cdot \sum_{p\in P} \mathrm{id}_X \otimes |p\rangle\!\langle p|_P \otimes \hat{\omega}^p_B\,. &(163)
\end{aligned}$$

To establish (160) and (161) we used the fact that $L^\dagger L \leq \|L^\dagger L\|_\infty\,\mathrm{id} = \|L\|_\infty^2\,\mathrm{id}$ for every linear operator L by definition of the operator norm. The final equality (163) follows from the definition of c_q. □

B Proof of Leftover Hashing Lemma in Theorem 5

We will use the following Proposition due to Renner [4, Cor. 5.5.2].

Lemma 18. *Using the notation of Theorem 5, we have*

$$\|\omega_{KS^H E'} - \chi_K \otimes \omega_{S^H E'}\|_1 \leq \sqrt{\mathrm{tr}(\sigma_{XE'})} \cdot 2^{-\frac{1}{2}\left(H_{\min}(X|E')_\sigma - \ell\right)} \,. \tag{164}$$

Note that the trace term can be ignored since it is always upper-bounded by 1.

Proof of Theorem 5. We apply Lemma 18 to the state $\tilde{\sigma}_{XE'}$, which yields

$$\|\tilde{\omega}_{KS^H E'} - \chi_K \otimes \tilde{\omega}_{S^H E'}\|_1 \leq 2^{-\frac{1}{2}\left(H_{\min}(X|E')_{\tilde{\sigma}} - \ell\right)} \,. \tag{165}$$

Here, $\tilde{\omega}_{KS^H E'} = \mathrm{tr}_X \left(\mathcal{E}_f(\tilde{\sigma}_{XE'} \otimes \rho_{S^H})\right)$. Then, exploiting the triangle inequality, we find

$$\begin{aligned}
&\|\omega_{KS^H E'} - \chi_K \otimes \omega_{S^H E'}\|_1 \\
&\quad \leq \|\tilde{\omega}_{KS^H E'} - \chi_K \otimes \tilde{\omega}_{S^H E'}\|_1 + \|\tilde{\omega}_{KS^H E'} - \omega_{KS^H E'}\|_1 + \|\tilde{\omega}_{S^H E'} - \omega_{S^H E'}\|_1 && (166) \\
&\quad \leq 2^{-\frac{1}{2}\left(H_{\min}(X|E')_{\tilde{\sigma}} - \ell\right)} + 2\|\tilde{\sigma}_{XE'} - \sigma_{XE'}\|_1 \,, && (167)
\end{aligned}$$

as desired. Here we used the data-processing inequality for the trace norm, which implies that

$$\|\tilde{\omega}_{HE'} - \omega_{S^H E'}\|_1 \leq \|\tilde{\omega}_{KS^H E'} - \omega_{KHE'}\|_1 \leq \|\tilde{\sigma}_{XE'} \otimes \rho_{S^H} - \sigma_{KE'} \otimes \rho_{S^H}\|_1 = \|\tilde{\sigma}_{XE'} - \sigma_{KE'}\|_1 \,. \tag{168}$$

□

References

[1] J. L. Carter and M. N. Wegman. Universal Classes of Hash Functions. *J. Comp. Syst. Sci.*, 18(2):143–154, 1979. DOI: 10.1016/0022-0000(79)90044-8.

[2] R. König, R. Renner, and C. Schaffner. The Operational Meaning of Min- and Max-Entropy. *IEEE Trans. on Inf. Theory*, 55(9):4337–4347, 2009. DOI: 10.1109/TIT.2009.2025545.

[3] C. Portmann and R. Renner. Cryptographic security of quantum key distribution. 2014. arXiv: 1409.3525.

[4] R. Renner. *Security of Quantum Key Distribution.* PhD thesis, ETH Zurich, 2005. arXiv: quant-ph/0512258.

[5] A. Rényi. On Measures of Information and Entropy. In *Proc. Symp. on Math., Stat. and Probability*, pages 547–561, Berkeley, 1961. University of California Press.

[6] R. J. Serfling. Probability Inequalities for the Sum in Sampling without Replacement. *Ann. Stat.*, 2(1):39–48, 1974.

[7] M. Tomamichel. *A Framework for Non-Asymptotic Quantum Information Theory.* PhD thesis, ETH Zurich, 2012. arXiv: 1203.2142.

[8] M. Tomamichel, R. Colbeck, and R. Renner. Duality Between Smooth Min- and Max-Entropies. *IEEE Trans. on Inf. Theory*, 56(9):4674–4681, 2010. DOI: 10.1109/TIT.2010.2054130.

[9] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight Finite-Key Analysis for Quantum Cryptography. *Nat. Commun.*, 3:634, 2012. DOI: 10.1038/ncomms1631.

[10] M. Tomamichel and R. Renner. Uncertainty Relation for Smooth Entropies. *Phys. Rev. Lett.*, 106(11):110506, 2011. DOI: 10.1103/PhysRevLett.106.110506.

[11] J. H. van Lint. *Introduction to Coding Theory*. Graduate Texts in Mathematics. Springer, third edition, 1999.

[12] M. N. Wegman and J. L. Carter. New Hash Functions and their Use in Authentication and Set Equality. *J. Comp. Syst. Sci.*, 22(3):265–279, 1981. DOI: 10.1016/0022-0000(81)90033-7.

[13] S. Winkler, M. Tomamichel, S. Hengl, and R. Renner. Impossibility of Growing Quantum Bit Commitments. *Phys. Rev. Lett.*, 107(9), 2011. DOI: 10.1103/PhysRevLett.107.090502.