Simple and Rigorous Proof Method for Practical Security of Quantum Key Distribution in the Single-Qubit Regime Using Mismatched Basis Measurements

Michel Boyer\textsuperscript{1}, Gilles Brassard\textsuperscript{1,2}, Nicolas Godbout\textsuperscript{3}, Rotem Liss\textsuperscript{1,4}, and Stéphane Virally\textsuperscript{3}

\textsuperscript{1}Département IRO, Université de Montréal, 2920 Chemin de la Tour, Montréal (Québec) H3T 1N8, Canada
\textsuperscript{2}QuSoft, CWI Amsterdam, Science Park 123, 1098 XG Amsterdam, The Netherlands
\textsuperscript{3}Polytechnique Montréal, Department of Engineering Physics, 2500 Chemin de Polytechnique, Montréal (Québec) H3T 1J4, Canada
\textsuperscript{4}ICFO—Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, Av. Carl Friedrich Gauss 3, 08860 Castelldefels (Barcelona), Spain

Abstract

Quantum key distribution (QKD) protocols aim at allowing two parties to generate a secret shared key. While many QKD protocols have been proven unconditionally secure in theory, practical security analyses of experimental QKD implementations typically do not take into account all possible loopholes, and practical devices are still not fully characterized for obtaining tight and realistic key rates. We present a simple method of computing secure key rates for any practical implementation of discrete-variable QKD (which can also apply to measurement-device-independent QKD), initially in the single-qubit regime, and we rigorously prove its unconditional security against any possible attack. We hope our method becomes one of the standard tools used for analyzing, benchmarking, and standardizing all practical realizations of QKD.

1 Introduction

The purpose of quantum key distribution (QKD) is allowing two legitimate parties, typically named Alice and Bob, to generate an information-theoretically secure key [1]. Most QKD protocols have been proven secure even if the adversary Eve is allowed to apply any theoretical attack allowed by the laws of quantum physics. However, despite enormous progress in recent years, unconditional security of practical implementations of QKD has remained elusive.
The difficulty of achieving practical security stems from the fact that practical implementations deviate from the theoretical protocols in many important aspects. The theoretical modelings of the preparation devices, the transmitted quantum systems, the quantum channels, and the measurement devices, differ enormously from any experimental realization, and these differences open up loopholes and weaknesses that Eve may be able to exploit.

Most security weaknesses of the measurement devices can be closed using measurement-device independent (MDI) QKD \([2, 3, 4, 5]\). However, MDI QKD still requires us to trust the preparation devices of Alice and Bob, and deviations of the actually prepared quantum states from the theoretical states still pose a significant security threat. Alternatively, in (fully) device independent (DI) QKD \([6, 7, 8]\), Alice’s and Bob’s devices are completely uncharacterized, and violations of Bell’s inequality prove the secrecy of the final key. This method, while promising and theoretically solid, still achieves far worse secret key rates than standard QKD (including MDI QKD) in realistic experimental settings \([9, 10, 11]\); in addition, it still requires assumptions, including the assumption that Alice’s and Bob’s uncharacterized devices are never allowed to communicate with each other or with Eve. Therefore, while we believe that both DI QKD and standard (especially MDI) QKD are important directions that can lead to practical security (perhaps in different levels of security), in this paper we focus on standard and MDI QKD protocols, where the most pressing practical security problem is imperfectly generated quantum states.

We suggest a simple and systematic method for analyzing source imperfections and proving unconditional security of a large variety of QKD protocols. Our method (similarly to the “loss tolerant” QKD protocol \([12, 13, 14, 15]\)) assumes the quantum source can only emit three possible quantum states (instead of the four states used by BB84), and it uses a mismatched-basis analysis (see, e.g., \([16]\)) for deriving the key rate in the finite-key regime. Our analysis method is vastly simplified, rigorous, takes into account many subtle points that are often omitted in other security proofs, and gives an explicit key rate formula in the finite-key regime. We further suggest a practical step-by-step process for analyzing experimental implementations of QKD, and we verify the restriction to three states is indeed essential for practical security.

Our method currently applies only to the qubit regime (in the generalized sense: namely, we require the three emitted quantum states to be linearly dependent and lie inside a two-dimensional Hilbert subspace), and it does not support decoy states \([17, 18, 19]\). We believe the analysis of decoy states will work with our framework (see, e.g., \([20, 21, 22]\)), but we leave their rigorous and precise analysis for future research. We also believe our analysis can prove security for practical implementations of MDI QKD using the reduction techniques introduced by \([2, 4]\), but we leave a detailed analysis of this direction for future research.

In Section 2 we explain how the security of practical implementations of QKD should be rigorously analyzed and proved. In Section 3 we fully define the analyzed QKD protocol, and in Section 4 we prove its security; our final security result (the key rate) is presented as Corollary 9. In Section 5 we explain why four source states are likely too many (in the qubit and 2-basis regime), and why we must restrict our protocol to three states.

2 Step-by-Step Analysis of Practical Implementations of QKD

Nowadays, despite the enormous progress made on practical security analysis, a comprehensive method for proving security is still lacking. In many descriptions of practical implementations
of QKD, while the theoretical model suggested for analysis is close to the practical implementation, it is naturally not identical, and the reduction from the practical implementation to the theoretical protocol sometimes uses hand wavy arguments instead of fully rigorous mathematical modeling and analysis.

For rigorously proving the security of a practical implementation in the case of a measurement device independent (MDI) protocol, we suggest the following way:

1. The implementation should be evaluated and tested. In particular, the emitted quantum states must be repeatedly measured in all aspects, including determining the modes: frequency spectrum (which includes wavelengths and their relative phases), polarization, timing and location of emission, direction of propagation (wave vector), and their degrees of mutual coherence; and performing a full tomography for each mode, discovering the resulting quantum states. Each resulting quantum state (for each basis choice and data choice) must be reconstructed and explicitly written; this reconstruction is essential for the security analysis.

2. The quantum states must be given as inputs to the security proof. The security proof then gives us a key rate formula and security parameters.

3. The key rate and security parameters can now be compared to the security definition. The result of this comparison decides whether security of the practical implementation has been proved.

In particular, if this process requires any reduction between the practical implementation and the theoretical model, the reduction must be rigorous and precise, it must be included as a part of the proof, and it must be verified to work against any possible attack.

3 Definition of the QKD Protocol

The QKD protocol we analyze in this paper is a prepare-and-measure protocol which is defined as follows:

1. Alice and Bob publicly agree on the parameters of the protocol:
   - Three normalized quantum states \( \{ |\gamma_0 \rangle_{B_i}, |\gamma_1 \rangle_{B_i}, |\gamma_+ \rangle_{B_i} \} \), that can reside in any arbitrary Hilbert space, but must be linearly dependent (namely, they must span a 2-dimensional Hilbert subspace). Specifically, we denote:
     \[
     |\gamma_+ \rangle_{B_i} = a |\gamma_0 \rangle_{B_i} + b |\gamma_1 \rangle_{B_i},
     \]
     where \(a, b \in \mathbb{C}\). We require \(|a|^2 + |b|^2 > \frac{1}{2}\), or, equivalently, \(\Re(a^* b \langle \gamma_0 | \gamma_1 \rangle_{B_i}) < \frac{1}{4}\).
   - Bob’s generalized measurement operators for each round \(i\):
     (a) \( \{ M_{B_i}^{Z,i} \}_{i \in \{0,1,\emptyset\}} \), which we name “measurement in the standard basis” or “measurement in the z basis”; and
     (b) \( \{ M_{B_i}^{X,i} \}_{i \in \{0,1,\emptyset\}} \), which we name “measurement in the conjugate basis” or “measurement in the x basis”.

3
which are defined similarly to [20]. The $\emptyset$ sign corresponds to a non-definite measurement result (e.g., a loss), and we require the non-definite results of both measurement bases to coincide (see [20]):

$$\left( M^{Z,\emptyset}_{B_i} \right) \dagger \left( M^{Z,\emptyset}_{B_i} \right) = \left( M^{X,\emptyset}_{B_i} \right) \dagger \left( M^{X,\emptyset}_{B_i} \right) \quad (2)$$

We note that Bob’s measurement operators can be arbitrary and are not required to be perfectly implemented or perfectly known. However, they influence the measurement results and the error rate, which influence the protocol’s success probability and key rate.

- The number $M$ of all rounds (all quantum states sent by Alice to Bob).
- The required number $m$ of rounds where Bob gets a successful measurement result (i.e., not the non-definite measurement result “$\emptyset$”).
- The probabilities that Alice chooses each “preparation basis”: $p^A_\emptyset$ represents the probability that Alice prepares either $|\gamma_0\rangle_{B_i}$ or $|\gamma_1\rangle_{B_i}$, each of which she chooses with equal probabilities, $p^A_\emptyset$, and $p^A_\emptyset$ represents the probability that Alice prepares $|\gamma_i\rangle_{B_i}$. We require $p^A_\emptyset + p^A_\emptyset = 1$.
- The probabilities that Bob chooses to measure in each measurement basis: $p^B_\emptyset$ (for choosing to measure in the “$z$ basis”) and $p^B_\emptyset$ (for choosing to measure in the “$x$ basis”), respectively, such that $p^B_\emptyset + p^B_\emptyset = 1$.
- The numbers $k_1, k_2, k_3, k_4$ of TEST bits required for each pair of basis choices of Alice and Bob ($Z-Z$, $Z-X$, $X-Z$, and $X-X$, respectively, where the first letter ($Z$ or $X$) represents Alice’s basis choice, and the second letter represents Bob’s basis choice), and the number $n_1$ of required INFO bits corresponding to basis choices of $Z-Z$. We require $n_1 + k_1 + k_2 + k_3 + k_4 \leq m$.
- The error rate threshold $\delta$ (maximal allowed noise in TEST-Z-Z and TEST-X-X bits).
- The zero rate threshold $\delta_{\text{mismatch}}$ (maximal allowed rate of “$+$” or “$0$” results measured by Bob in TEST-Z-X and TEST-X-Z bits, respectively).

2. Alice randomly chooses a string $\Phi_A \in \{0,1\}^M$ of basis choices: she chooses each bit independently to have value 0 with probability $p^A_\emptyset$ or value 1 with probability $p^A_\emptyset$. Bob randomly chooses a string $\Phi_B \in \{0,1\}^M$ of basis choices: he chooses each bit independently to have value 0 with probability $p^B_\emptyset$ or value 1 with probability $p^B_\emptyset$. In addition, Alice chooses a uniformly random string $R \in \{0,1\}^M$ of the raw bits she prepares and sends (it is only used for rounds where Alice’s basis choice is 0).

All strings are kept secret.

3. For each round $i \in \{1,2,\ldots,M\}$ of the protocol, Alice prepares the state dictated by $(\Phi_A)_i$ and $R_i$—namely:
   - Alice prepares $|\gamma_0\rangle_{B_i}$ if $(\Phi_A)_i = 0$ and $R_i = 0$;
   - Alice prepares $|\gamma_1\rangle_{B_i}$ if $(\Phi_A)_i = 0$ and $R_i = 1$;
Alice prepares $|\gamma_+\rangle_B$ if $(\Phi_A)_i = 1$ (independently of $R_i$).

Alice sends the prepared state to Bob via the quantum channel. Bob measures each obtained state in the basis dictated by $(\Phi_B)_i$ (the “z basis” if $(\Phi_B)_i = 0$, or the “x basis” if $(\Phi_B)_i = 1$) and puts the measurement result in the string $U \in \{0, 1, \emptyset\}^M$, which is kept secret. In addition, Bob defines $\Omega \triangleq \{1 \leq i \leq M \mid U_i \neq \emptyset\}$ (the set of all rounds where Bob obtained a successful measurement result).

4. Bob publicly sends to Alice both his basis choice string $\Phi_B$ and the set $\Omega$.

5. Alice verifies that at least $m$ rounds appear in $\Omega$, in which case she sets the flag $F_{\text{sift}} = \checkmark$ and publishes the set $\Sigma \subseteq \Omega$ consisting of the first $m$ rounds appearing in $\Omega$ (namely, the first $m$ successful measurements of Bob). Otherwise (if fewer than $m$ rounds appear in $\Omega$), Alice sets the flag $F_{\text{sift}} = \not\checkmark$ and aborts the protocol.

6. Alice verifies that $\Sigma$ includes at least $n_1 + k_1$ rounds where Alice chose $z$ and Bob chose $z$ (named “Z-Z rounds”), at least $k_2$ “Z-X rounds”, at least $k_3$ “X-Z rounds”, and at least $k_4$ “X-X rounds”. If it does, Alice sets the flag $F_{\text{min}} = \checkmark$; otherwise, she sets the flag $F_{\text{min}} = \emptyset$ and aborts the protocol.

7. Alice randomly chooses four subsets $\Pi_1, \Pi_2, \Pi_3, \Pi_4 \subseteq \Sigma$ of test rounds:

- $|\Pi_1| = k_1$ is randomly chosen out of all “Z-Z rounds” in $\Sigma$, and it consists of $k_1$ rounds we define as the “TEST-Z-Z rounds”;
- $|\Pi_2| = k_2$ is randomly chosen out of all “Z-X rounds” in $\Sigma$, and it consists of $k_2$ rounds we define as the “TEST-Z-X rounds”;
- $|\Pi_3| = k_3$ is randomly chosen out of all “X-Z rounds” in $\Sigma$, and it consists of $k_3$ rounds we define as the “TEST-X-Z rounds”;
- $|\Pi_4| = k_4$ is randomly chosen out of all “X-X rounds” in $\Sigma$, and it consists of $k_4$ rounds we define as the “TEST-X-X rounds”,

and one subset $\Sigma_1 \subseteq \Sigma$ of information rounds:

- $|\Sigma_1| = n_1$ is randomly chosen out of all “Z-Z rounds” in $\Sigma \setminus \Pi_1$, and it consists of $n_1$ rounds we define as the “INFO rounds”.

She publicly sends the five disjoint sets $\Pi_1, \Pi_2, \Pi_3, \Pi_4, \Sigma_1$ to Bob.

8. Each one of Alice and Bob produces five substrings of their respective bit strings $R, U$:

- $V^1$ and $W^1$ are the substrings corresponding to $\Pi_1$ (the TEST-Z-Z rounds) of Alice and Bob, respectively;
- $V^2$ and $W^2$ are the substrings corresponding to $\Pi_2$ (the TEST-Z-X rounds) of Alice and Bob, respectively;
- $V^3$ and $W^3$ are the substrings corresponding to $\Pi_3$ (the TEST-X-Z rounds) of Alice and Bob, respectively;
- $V^4$ and $W^4$ are the substrings corresponding to $\Pi_4$ (the TEST-X-X rounds) of Alice and Bob, respectively;
• $X^1$ and $Y^1$ are the substrings corresponding to $\Sigma_1$ (the INFO rounds) of Alice and Bob, respectively.

9. Alice sends $V^1, V^4$ to Bob, and Bob compares them to his $W^1, W^4$ and computes the error rates. If the error rate in either the TEST-Z-Z rounds or the TEST-X-X rounds exceeds $\delta$, Bob sets $F_{pe} = \emptyset$ and aborts the protocol.

In addition, Bob evaluates his bit strings $W^2, W^3$ and computes their zero rates (namely, the percentages of his “+” or “0” measurement results, respectively). If the zero rate in either the TEST-Z-X rounds or the TEST-X-Z rounds exceeds $\delta_{\text{mismatch}}$, Bob sets $F_{pe} = \emptyset$ and aborts the protocol.

If both tests pass, Bob sets $F_{pe} = \checkmark$, and the protocol proceeds.

10. Alice and Bob perform error correction and privacy amplification to their secret INFO bits $X^1, Y^1$ in the standard way for BB84 protocols (described, e.g., in [20]) to obtain their final secret keys. We note that Alice and Bob generate another flag, $F_{cc}$, and they abort the protocol if $F_{cc} = \emptyset$ (see details in [20]); however, if $F_{cc} = \checkmark$, the protocol succeeds, and Alice’s and Bob’s final secret keys are denoted by $K_A, K_B \in \{0, 1\}^\ell$, respectively.

We point out that this is a very general protocol in the qubit regime, because Alice’s emitted states $\{|\gamma_0\rangle_B, |\gamma_1\rangle_B, |\gamma_+\rangle_B\}$ can be any states (assuming they are linearly dependent and satisfy $|a|^2 + |b|^2 > \frac{1}{2}$), even if they lie inside a very general Hilbert space (which may be infinite-dimensional or even continuous). Thus, for this security proof to apply, Alice and Bob must first test their devices, perform a full quantum tomography of their emitted states, and input the resulting states $|\gamma_0\rangle_B, |\gamma_1\rangle_B, |\gamma_+\rangle_B$ to the security proof, as described in Section 2.

Using pure states $|\gamma_0\rangle_B, |\gamma_1\rangle_B, |\gamma_+\rangle_B$ does not hurt generality, because if Alice sends a mixed state, we can always assume she also sends the purifying system (which Eve intercepts and uses): this assumption is only beneficial to Eve, so it makes our security proof stronger.

### 4 Security Proof

Our security proof is a generalized version of the rigorous, mostly self-contained security proof presented by [20] for BB84-based protocols. That security proof uses entropic uncertainty relations to derive a key rate formula in the finite-key regime, showing a reduction from the prepare-and-measure protocol to an entanglement-based protocol. Here we generalize this approach to apply to our practical protocol (in the qubit regime) described in Section 3.

#### 4.1 Equivalent Modified Entanglement-Based Protocol

We begin our security proof by performing a reduction to the following modified entanglement-based protocol. We point out the this protocol does not strictly adhere to standard definitions of “entanglement-based” protocols, because it requires Alice to prepare a specific entangled state, measure some portions of it, and send other portions to Bob (which Eve can attack). Therefore, it is similar to prepare-and-measure protocols. Nevertheless, this protocol is entanglement-based in the narrowest sense, because it allows Alice to delay her measurements (on some portions of her state) and relies on the resulting entanglement for proving security.

Therefore, we call it a “modified entanglement-based protocol”, and it is defined as follows:
1. Alice and Bob publicly agree on the parameters of the protocol:

- Three normalized quantum states \( \{ |\gamma_0\rangle_{B_i}, |\gamma_1\rangle_{B_i}, |\gamma_+\rangle_{B_i} \} \), that can reside in any arbitrary Hilbert space, but must be linearly dependent (namely, they must span a 2-dimensional Hilbert subspace). Specifically, we denote:

\[
|\gamma_+\rangle_{B_i} = a|\gamma_0\rangle_{B_i} + b|\gamma_1\rangle_{B_i},
\]

(3)

where \( a, b \in \mathbb{C} \). We require \( |a|^2 + |b|^2 > \frac{1}{2} \), or, equivalently, \( \Re(a^*b\langle \gamma_0 | \gamma_1 \rangle_{B_i}) < \frac{1}{4} \).

We also denote the following parameter \( T \):

\[
T \equiv |a|^2 + |b|^2
\]

(4)

(so \( T > \frac{1}{2} \), or \( 2T - 1 > 0 \)), and a resulting fourth quantum state \( |\gamma_-\rangle_{B_i} \):

\[
|\gamma_-\rangle_{B_i} = \frac{b^*|\gamma_0\rangle_{B_i} - a^*|\gamma_1\rangle_{B_i}}{\sqrt{2T - 1}}.
\]

(5)

**Lemma 1.** If \( |\gamma_0\rangle_{B_i}, |\gamma_1\rangle_{B_i}, |\gamma_+\rangle_{B_i} \) are all normalized, then \( |\gamma_-\rangle_{B_i} \) is normalized, too.

**Proof.**

\[
1 = \langle \gamma_+ | \gamma_+ \rangle_{B_i} = |a|^2 \langle \gamma_0 | \gamma_0 \rangle_{B_i} + |b|^2 \langle \gamma_1 | \gamma_1 \rangle_{B_i} + 2\Re(a^*b\langle \gamma_0 | \gamma_1 \rangle_{B_i})
\]

\[
\langle \gamma_- | \gamma_- \rangle_{B_i} = \frac{|b|^2 \langle \gamma_0 | \gamma_0 \rangle_{B_i} + |a|^2 \langle \gamma_1 | \gamma_1 \rangle_{B_i} - 2\Re(ba^*\langle \gamma_0 | \gamma_1 \rangle_{B_i})}{2T - 1}
\]

\[
= \frac{T - 2\Re(ab\langle \gamma_0 | \gamma_1 \rangle_{B_i})}{2T - 1} = \frac{T - (1 - T)}{2T - 1} = \frac{2T - 1}{2T - 1} = 1.
\]

\( \square \)

- Inside a separate qubit space \( \mathcal{H}_{A_i} \equiv \text{Span}\{ |0\rangle_{A_i}, |1\rangle_{A_i} \} \), two orthonormal quantum states (using the same \( a, b \in \mathbb{C} \) and \( T \) as above):

\[
|\xi_+\rangle_{A_i} \equiv \frac{a^*|0\rangle_{A_i} + b^*|1\rangle_{A_i}}{\sqrt{T}},
\]

(8)

\[
|\xi_-\rangle_{A_i} \equiv \frac{b|0\rangle_{A_i} - a|1\rangle_{A_i}}{\sqrt{T}},
\]

(9)

leading to two orthonormal measurement bases (representing standard, projective quantum measurements) of Alice for each round \( i \):

(a) \( \{ |0\rangle_{A_i}, |1\rangle_{A_i} \} \), which we name “the standard basis” or “the \( x \) basis”; and

(b) \( \{ |\xi_+\rangle_{A_i}, |\xi_-\rangle_{A_i} \} \), which we name “the conjugate basis” or “the \( x \) basis”.

- Bob’s generalized measurement operators for each round \( i \):

(a) \( \{ M_{B_i}^{x,0} \}_{i \in \{0,1\}} \), which we name “measurement in the standard basis” or “measurement in the \( x \) basis”; and

(b) \( \{ M_{B_i}^{x,0} \}_{i \in \{0,1\}} \), which we name “measurement in the conjugate basis” or “measurement in the \( x \) basis”. 

7
which are defined similarly to [20]. We note that Bob’s measurement operators can be arbitrary and are not required to be perfectly implemented or perfectly known. However, they influence the measurement results and the error rate, which influence the protocol’s success probability and key rate.

- The number $M'$ of all rounds (all quantum states sent by Alice to Bob).
- The required number $m$ of rounds where Alice does not tell Bob to discard (see Step 3).
- The probabilities that Alice chooses to measure in each measurement basis: $p^A_z$ (for choosing to measure in the “$z$ basis”) and $p^A_x$ (for choosing to measure in the “$x$ basis”), respectively, such that $p^A_z + p^A_x = 1$.
- The probabilities that Bob chooses to measure in each measurement basis: $p^B_z$ (for choosing to measure in the “$z$ basis”) and $p^B_x$ (for choosing to measure in the “$x$ basis”), respectively, such that $p^B_z + p^B_x = 1$.
- The numbers $k_1, k_2, k_3, k_4$ of TEST bits required for each pair of basis choices of Alice and Bob (Z-Z, Z-X, X-Z, and X-X, respectively, where the first letter (Z or X) represents Alice’s basis choice, and the second letter represents Bob’s basis choice), and the number $n_1$ of required INFO bits corresponding to basis choices of Z-Z. We require $n_1 + k_1 + k_2 + k_3 + k_4 \leq m$.
- The error rate threshold $\delta$ (maximal allowed noise in TEST-Z-Z and TEST-X-X bits).
- The zero rate threshold $\delta_{\text{mismatch}}$ (maximal allowed rate of “+” or “0” results measured by Bob in TEST-Z-X and TEST-X-Z bits, respectively).

2. Alice randomly chooses a string $\Phi_A \in \{0, 1\}^{M'}$ of basis choices: she chooses each bit independently to have value 0 with probability $p^A_z$ or value 1 with probability $p^A_x$.

Bob randomly chooses a string $\Phi_B \in \{0, 1\}^{M'}$ of basis choices: he chooses each bit independently to have value 0 with probability $p^B_z$ or value 1 with probability $p^B_x$.

Both strings are kept secret.

3. For each round $i \in \{1, 2, \ldots, M'\}$ of the protocol, Alice generates the following entangled state:

$$|\Psi\rangle_{A_i B_i} \triangleq \frac{1}{\sqrt{2}} (|A_i\rangle B_i + |1\rangle A_i |\gamma\rangle B_i) = \frac{1}{\sqrt{2T}} (|\xi_+\rangle A_i |\gamma_+\rangle B_i + |\xi_-\rangle A_i |\gamma_-\rangle B_i)$$  \hspace{1cm} (10)

(this equality between its two representations can be proved algebraically). In other words, Alice generates the state

$$\otimes_{i=1}^{M'} |\Psi\rangle_{A_i B_i}$$  \hspace{1cm} (11)

consisting of the $M'$ quantum systems $A_1, A_2, \ldots, A_{M'}$ (one system for each round $i$).

For each round $i$, if $|\Phi_A\rangle_i = 1$ (namely, if Alice will have to measure this round in the “$x$ basis”), Alice measures subsystem $A_i$ in the “$x$ basis” $\{|\xi_+\rangle A_i, |\xi_-\rangle A_i\}$. (If $|\Phi_A\rangle_i = 0$, she delays measurement to Step 6.) Alice then defines the following bit string $D_i \in \{0, 1\}^{M'}$:

$$D_i \triangleq \begin{cases} 1 & \text{if } (\Phi_A)_i = 1 \text{ and Alice measures } "\xi_-" \text{ in round } i \\ 0 & \text{otherwise (either } (\Phi_A)_i = 0, \text{ or Alice measures } "\xi_+" \text{ in round } i \end{cases}$$  \hspace{1cm} (12)
Alice publicly sends to Bob the string $D$. This means that for each round $i$, Alice tells Bob (and Eve) whether she obtained the measurement result “$\xi_-$” or not; however, if she did not obtain the measurement result “$\xi_-$”, she does not expose the measurement result (if any) or the chosen basis.

Alice and Bob discard and ignore all rounds where $D_i = 1$, which we name the “discarded rounds”. However, for all the “non-discarded rounds” (rounds where $D_i = 0$), Alice sends to Bob the subsystem $B_i$ via the quantum channel, which can be attacked by Eve.

4. Bob publicly sends to Alice his basis choice string $\Phi_B$.

5. Alice denotes the set of rounds that were not discarded by her as $\Omega \subseteq \{1, 2, \ldots, M'\}$ (namely, $\Omega \triangleq \{1 \leq i \leq M' \mid D_i = 0\}$). Alice verifies that at least $m$ rounds appear in $\Omega$, in which case she sets the flag $F_{\text{sift'}} = \checkmark$ and publishes the set $\Sigma \subseteq \Omega$ consisting of the first $m$ rounds appearing in $\Omega$ (namely, the first $m$ successful measurements of Bob). Otherwise (if fewer than $m$ rounds appear in $\Omega$), Alice sets the flag $F_{\text{sift'}} = \times 0$ and aborts the protocol.

6. Alice measures all quantum systems $A_i$ for which $(\Phi_A)_i = 0$ in the “$z$ basis” $\{|0\rangle_{A_i}, |1\rangle_{A_i}\}$. She puts all her measurement results (from both this step and Step 3) in the string $R \in \{0, 1\}^{M'}$, which is kept secret.

7. Bob measures all his non-discarded quantum systems in the bases dictated by $\Phi_B$ (the “$z$ basis” if $(\Phi_B)_i = 0$, or the “$x$ basis” if $(\Phi_B)_i = 1$) and puts his measurement results in the string $U \in \{0, 1\}^{M'}$, which is kept secret.

The rest of the protocol is completely identical to the last steps of the original prepare-and-measure protocol described in Section 3 (in its Steps 6–10):

8. Alice verifies that $\Sigma$ includes at least $n_1 + k_1$ rounds where Alice chose $z$ and Bob chose $z$ (named “Z-Z rounds”), at least $k_2$ “Z-X rounds”, at least $k_3$ “X-Z rounds”, and at least $k_4$ “X-X rounds”. If it does, Alice sets the flag $F_{\text{min}} = \checkmark$; otherwise, she sets the flag $F_{\text{min}} = \times 0$ and aborts the protocol.

9. Alice randomly chooses four subsets $\Pi_1, \Pi_2, \Pi_3, \Pi_4 \subseteq \Sigma$ of test rounds:

- $|\Pi_1| = k_1$ is randomly chosen out of all “Z-Z rounds” in $\Sigma$, and it consists of $k_1$ rounds we define as the “TEST-Z-Z rounds”;
- $|\Pi_2| = k_2$ is randomly chosen out of all “Z-X rounds” in $\Sigma$, and it consists of $k_2$ rounds we define as the “TEST-Z-X rounds”;
- $|\Pi_3| = k_3$ is randomly chosen out of all “X-Z rounds” in $\Sigma$, and it consists of $k_3$ rounds we define as the “TEST-X-Z rounds”;
- $|\Pi_4| = k_4$ is randomly chosen out of all “X-X rounds” in $\Sigma$, and it consists of $k_4$ rounds we define as the “TEST-X-X rounds”,

and one subset $\Sigma_1 \subseteq \Sigma$ of information rounds:

- $|\Sigma_1| = n_1$ is randomly chosen out of all “Z-Z rounds” in $\Sigma \setminus \Pi_1$, and it consists of $n_1$ rounds we define as the “INFO rounds”.

9
She publicly sends the five disjoint sets $\Pi_1, \Pi_2, \Pi_3, \Pi_4, \Sigma_1$ to Bob.

10. Each one of Alice and Bob produces five substrings of their respective bit strings $R, U$:

- $V^1$ and $W^1$ are the substrings corresponding to $\Pi_1$ (the TEST-Z-Z rounds) of Alice and Bob, respectively;
- $V^2$ and $W^2$ are the substrings corresponding to $\Pi_2$ (the TEST-Z-X rounds) of Alice and Bob, respectively;
- $V^3$ and $W^3$ are the substrings corresponding to $\Pi_3$ (the TEST-X-Z rounds) of Alice and Bob, respectively;
- $V^4$ and $W^4$ are the substrings corresponding to $\Pi_4$ (the TEST-X-X rounds) of Alice and Bob, respectively;
- $X^1$ and $Y^1$ are the substrings corresponding to $\Sigma_1$ (the INFO rounds) of Alice and Bob, respectively.

11. Alice sends $V^1, V^4$ to Bob, and Bob compares them to his $W^1, W^4$ and computes the error rates. If the error rate in either the TEST-Z-Z rounds or the TEST-X-X rounds exceeds $\delta$, Bob sets $F_{pe} = \emptyset$ and aborts the protocol.

In addition, Bob evaluates his bit strings $W^2, W^3$ and computes their zero rates (namely, the percentages of his “+” or “0” measurement results, respectively). If the zero rate in either the TEST-Z-X rounds or the TEST-X-Z rounds exceeds $\delta_{mismatch}$, Bob sets $F_{pe} = \emptyset$ and aborts the protocol.

If both tests pass, Bob sets $F_{pe} = \checkmark$, and the protocol proceeds.

12. Alice and Bob perform error correction and privacy amplification to their secret INFO bits $X^1, Y^1$ in the standard way for BB84 protocols (described, e.g., in [20]) to obtain their final secret keys. We note that Alice and Bob generate another flag, $F_{ec}$, and they abort the protocol if $F_{ec} = \emptyset$ (see details in [20]); however, if $F_{ec} = \checkmark$, the protocol succeeds, and Alice’s and Bob’s final secret keys are denoted by $K_A, K_B \in \{0, 1\}^\ell$, respectively.

In Subsection 4.2 we prove security of this protocol, and in Subsection 4.3 we prove the reduction to be correct—namely, we prove that security of the above protocol implies security of the original protocol.

### 4.2 Security Proof for the Modified Entanglement-Based Protocol

Our security proof is a generalization of Section 6 of [20] (which proves security of an entanglement-based version of BB84 [1, 23, 24]), requiring a few modifications of their proof.

The proof of [20] is based on an *entropic uncertainty relation* which, roughly speaking, links two quantities: the smooth min-entropy of Alice’s data conditioned on Eve’s data (denoted $H^\varepsilon_{\min}(A|E)$) and the smooth max-entropy of Alice’s data conditioned on Bob’s data (denoted $H^\varepsilon_{\max}(A|B)$). Generally speaking, these entropies are measures of uncertainty: they capture the number of bits in Alice’s system $A$ that are unknown to either Eve or Bob, respectively. Intuitively (and imprecisely), the smooth min-entropy $H^\varepsilon_{\min}(A|E)$ describes the number of secret bits that can be extracted from Alice’s system $A$ and will be completely secret even from Eve (or from anyone that has Eve’s system $E$), while the smooth max-entropy $H^\varepsilon_{\max}(A|B)$ describes
the number of extra information bits that Bob will have to get from Alice if he wants to have full information on her system A (which is roughly equivalent to asking how much information Alice would need to send to Bob during the error correction procedure).

Roughly speaking, the entropic uncertainty relation used by [20] shows a lower bound on $H^e_{\text{min}}(A|E) + H^e_{\text{max}}(A|B)$. Then, their proof upper-bounds $H^e_{\text{max}}(A|B)$ by bounding the error rate between Alice and Bob using a law of large numbers (which shows it is unlikely that the error rate on TEST bits is less than $\delta$ while the error rate on INFO bits is more than $\delta + \nu$)\(^1\). The combination of these two results implies a lower bound on $H^e_{\text{min}}(A|E)$, and this lower bound immediately gives us the protocol’s key rate using the Leftover Hashing Lemma [25] (which intuitively says that $H^e_{\text{min}}(A|E)$ bits, known to Alice and completely secret from Eve, can be extracted from Alice’s system using a standard procedure of privacy amplification).

We mainly modify the first two parts of [20]: the entropic uncertainty relation, and the use of the law of large numbers. In addition, we need to justify security of our sifting step.

4.2.1 The Sifting Step

The sifting step of our modified entanglement-based protocol does not appear in the entanglement-based protocol of [20]. Therefore, we must prove it does not hurt security, by showing it keeps Alice’s and Bob’s basis choice strings $\Phi_A, \Phi_B$ independent from the other systems.

Each bit of $\Phi_A, \Phi_B$ is chosen independently (with probabilities $p^A_\xi, p^A_x, p^B_\xi, \text{ and } p^B_x$, respectively). Moreover, the state that Alice generates for each round is:

$$|\Psi\rangle_{A,B_i} \triangleq \frac{|0\rangle_A |\gamma_0\rangle_B_i + |1\rangle_A |\gamma_1\rangle_B_i}{\sqrt{2}} = \frac{|\xi_+\rangle_A |\gamma_+\rangle_B_i + \sqrt{2T-1}|\xi_-\rangle_A |\gamma_-\rangle_B_i}{\sqrt{2T}},$$

so we observe that if $(\Phi_A)_i = 0$ (namely, if Alice chooses the “$z$ basis”), Alice obtains the “0” and “1” results with equal conditional probabilities ($\frac{1}{2}$); and if $(\Phi_A)_i = 1$ (namely, if Alice chooses the “$x$ basis”), Alice obtains the “$\xi_+$” result with conditional probability $\frac{1}{2T}$ and obtains the “$\xi_-$” result with conditional probability $\frac{2T-1}{2T}$. We conclude:

$$\Pr_{A_i}(0) = \Pr_{A_i}(1) = \frac{p^A_x}{2},$$

$$\Pr_{A_i}(\xi_+) = \frac{p^A_x}{2T} = \frac{p^A_x}{2T},$$

$$\Pr_{A_i}(\xi_-) = \frac{p^A_\xi}{2T} = \frac{p^A_\xi}{2T}.$$ 

To justify the sifting step, we notice that this probabilistic process can equivalently be described as the following two-stage process:

1. First, for each round $i$, Alice determines whether round $i$ is discarded ($D_i = 1$) or not ($D_i = 0$). The round is discarded if and only if Alice measures “$\xi_-$”; therefore:

$$\Pr_{A_i}(D_i = 1) = \Pr_{A_i}(\xi_-) = \frac{p^A_\xi(2T-1)}{2T},$$

\(^1\)Intuitively, the smoothness parameter $\varepsilon$ means we do not necessarily use the original quantum state given as an input to the entropy, but we may use any quantum state up to distance $\varepsilon$ from it. In our case, for example, $\varepsilon$ represents the maximal probability that the law of large numbers is violated—namely, the maximal probability that the error rate in the INFO bits is much larger than the error rate observed in the TEST bits. Using the smooth min- and max-entropy allows us to upper-bound the impact of this unwanted possibility.
\[ \Pr_{A_i}(D_i = 0) = \Pr_{A_i}(0) + \Pr_{A_i}(1) + \Pr_{A_i}(\xi_+) = 2 \cdot \frac{p_z^A}{2} + \frac{p_x^A}{2T} = p_z^A + \frac{p_x^A}{2T}. \quad (18) \]

Remember that we define \( \Omega \triangleq \{1 \leq i \leq M' \mid D_i = 0\} \) as the set of non-discarded rounds.

2. Then, for each round \( i \in \Omega \) (each non-discarded round), Alice determines the basis:

\[ \Pr_{A_i}((\Phi_A)_i = 0 \mid D_i = 0) = \frac{\Pr_{A_i}(0) + \Pr_{A_i}(1)}{\Pr_{A_i}(D_i = 0)} = \frac{2 \cdot \frac{p_z^A}{2} + p_x^A}{p_z^A + \frac{p_x^A}{2T}} = \frac{p_z^A}{p_z^A + \frac{p_x^A}{2T}}, \quad (19) \]

\[ \Pr_{A_i}((\Phi_A)_i = 1 \mid D_i = 0) = \frac{\Pr_{A_i}(\xi_+) + \Pr_{A_i}(D_i = 0)}{\Pr_{A_i}(D_i = 0)} = \frac{p_z^A + \frac{p_x^A}{2T}}{p_z^A + \frac{p_x^A}{2T}}. \quad (20) \]

These probabilities are independent between the rounds: namely, the basis is determined independently for each non-discarded round.

Note that this equivalence is only correct with respect to the probability distribution; the above process does not describe a physical process, but a virtual process that cannot be applied in practice and only gives the same probability distribution over \( \Phi_A \) and \( R \). (This point can be counter-intuitive: from the quantum mechanical point of view, the choice of discarded and non-discarded rounds obviously depends on the basis chosen for measurement; yet, from the probabilistic point of view, the process can be divided to the two above stages and still give us an identical probability distribution.)

We notice that both the flag \( F^{\text{sift}} \) (which notes whether there are at least \( m \) rounds in \( \Omega \)—namely, whether at least \( m \) rounds were not discarded) and the set \( \Sigma \) (which represents the first \( m \) rounds in \( \Omega \)) only depend on stage 1: namely, from the probabilistic point of view, both the passing of the sifting test \( (F^{\text{sift}}) \) and the choice of the \( m \) relevant rounds \( (\Sigma) \) depend only on the choice of discarded rounds in stage 1, and they are both completely independent of the bases \( \Phi_A \) chosen for the non-discarded rounds in stage 2. The bases of the non-discarded rounds are chosen independently with the predetermined probabilities computed in Equations (19)–(20).

For this reason, in the rest of the analysis we can treat \( \Phi_A \) and \( \Phi_B \) (more precisely, their restrictions to the \( m \) non-discarded rounds in \( \Sigma \)) to be completely independent of Eve’s attack. In other words, Eve’s attack is applied independently of Alice’s and Bob’s chosen bases (or their actually used bases), because Eve is only given access to the discarding string \( D \) which is completely independent of the bases in the non-discarded rounds. This result is crucial for the application of the laws of large numbers to hypothetical protocols in Subsubsection 4.2.3.

Furthermore, we notice that our modified entanglement-based protocol actually acts in the following way regarding the choice of bases and TEST and INFO bits inside \( \Sigma \):

1. In stage 2 (included in Step 2 of the protocol), Alice and Bob determine the bases of the \( m \) non-discarded rounds in \( \Sigma \), chosen randomly and independently for each round in \( \Sigma \).

2. In Step 8 of the protocol, Alice verifies that \( \Sigma \) has sufficient numbers of rounds corresponding to each pair of bases (namely, at least \( n_1 + k_1 \) “Z-Z rounds”, at least \( k_2 \) “Z-X rounds”, at least \( k_3 \) “X-Z rounds”, and at least \( k_4 \) “X-X rounds”). For simplicity, let us denote the “Z-Z rounds” by \( \Sigma_{Z,Z} \), the “Z-X rounds” by \( \Sigma_{Z,X} \), the “X-Z rounds” by \( \Sigma_{X,Z} \), and the “X-X rounds” by \( \Sigma_{X,X} \); here Alice verifies that \( |\Sigma_{Z,Z}| \geq n_1 + k_1, |\Sigma_{Z,X}| \geq k_2, |\Sigma_{X,Z}| \geq k_3, \) and \( |\Sigma_{X,X}| \geq k_4 \). We condition on this verification passing—namely, we evaluate the conditional probabilities on \( F^{\text{min}} = \checkmark \).
3. In Step 9 of the protocol, Alice uniformly and randomly chooses the corresponding disjoint subsets $\Sigma_1, \Pi_1 \subseteq \Sigma_{Z,Z}, \Pi_2 \subseteq \Sigma_{Z,X}, \Pi_3 \subseteq \Sigma_{X,X},$ and $\Pi_4 \subseteq \Sigma_{X,Z}$ (of sizes $n_1, k_1, k_2, k_3,$ and $k_4,$ respectively). This effectively discards the other $m - n_1 - k_1 - k_2 - k_3 - k_4$ rounds in $\Sigma \setminus (\Sigma_1 \cup \Pi_1 \cup \Pi_2 \cup \Pi_3 \cup \Pi_4),$ because their basis choices and measurement results are completely ignored by the rest of the protocol.

Combining these three steps, and conditioning on $F^{\min} = \check{\square}$ (namely, conditioning on the verification of the second step to pass), this process is equivalent from the probabilistic point of view to uniformly and randomly choosing five disjoint subsets $\Sigma_1, \Pi_1, \Pi_2, \Pi_3, \Pi_4 \subseteq \Sigma$ of sizes $n_1, k_1, k_2, k_3,$ and $k_4,$ respectively (out of the $m$-sized set $\Sigma),$ and letting this uniform choice dictate the choice of measurement probabilities ($Z-Z, Z-Z, Z-X, X-Z,$ and $X-X,$ respectively). This equivalence results from the complete symmetry of the above three steps, which have no dependence whatsoever on the identifying number of each round. This observation is, too, crucial for the application of the laws of large numbers in Subsubsection 4.2.3.

### 4.2.2 Entropic Uncertainty Relation

The security proof in [20] uses the uncertainty relation described in Proposition 4 of [20], which is equivalent to Corollary 7.4 of [26]. This uncertainty relation uses the symmetry of the BB84 protocol with respect to the chosen basis of the INFO bits: namely, it uses the fact that the INFO bits are measured in uniformly random bases, independently of the TEST bits’ results and bases. Since a similar property does not apply to our protocol (because all our INFO bits are measured in uniformly random bases, independently of the TEST bits’ results and bases). This equivalence results from the complete symmetry of the above three steps, which have no dependence whatsoever on the identifying number of each round. This observation is, too, crucial for the application of the laws of large numbers in Subsubsection 4.2.3.

**Theorem 2.** (Theorem 7.2 of [26]) Given $\epsilon \geq 0$ and a non-normalized state $\rho_{ABC}$ over the Hilbert space $\mathcal{H}_{ABC},$ and given two generalized measurement operators $M_1 = \{M_1^x\}_x, M_2 = \{M_2^x\}_x$ on $\mathcal{H}_A$ and a projective measurement $\{P^k\}_k$ on $\mathcal{H}_A,$ the two post-measurement states

\[
\sigma_{XKB} = \sum_{x,k} |x\rangle_X \langle x|_X \otimes |k\rangle_K \langle k|_K \otimes \text{tr}_{AC}(M_1^{x,k} \rho_{ABC} P_k (M_1^{x,k})^\dagger),
\]

\[
\sigma_{X'KC} = \sum_{x',k} |x'\rangle_{X'} \langle x'|_{X'} \otimes |k\rangle_K \langle k|_K \otimes \text{tr}_{AB}(M_2^{x',k} P_k \rho_{ABC} P_k (M_2^{x',k})^\dagger)
\]

satisfy the following inequality (uncertainty relation):

\[
H^e_{\min}(X|KB) + H^e_{\max}(X'|KC)\sigma \geq \log_2 \left( \frac{1}{c_K^e} \right),
\]

where:

\[
c_K^e \triangleq \max_{k,x,x'} ||M_1^{x,k} P_k (M_2^{x',k})^\dagger||_\infty.
\]

**Proof.** Proved in [26, Subsection 7.3.2] as Theorem 7.2. \square

The next proposition will give us a similar result as Corollary 5 of [20] (namely, roughly speaking, a lower bound on the sum $H^e_{\min}(A|E) + H^e_{\max}(A|B)$), with one important difference: the first term $H^e_{\min}(A|E)$ will still refer to the real QKD protocol (the modified entanglement-based protocol described in Subsection 4.1), but the second term $H^e_{\max}(A|B)$ will now refer to a
Proposition 3. For the modified entanglement-based protocol described in Subsection 4.1, for \( \varepsilon \geq 0 \), it holds that:
\[
H_{\min}^e(X^1 \land F^{pe} = \sqrt{|VW\Pi\Phi_A\Phi_BE}, F^{sift'} = F^{\min} = \sqrt{)} \sigma \\
+ H_{\max}^e(X'^1 \land F^{pe} = \sqrt{|Y'^1}, F^{sift'} = F^{\min} = \sqrt{)} \sigma \geq n_1 \log_2 \left( \frac{1}{c} \right),
\]
where we define \( V \triangleq (V^1, V^2, V^3, V^4) \), \( W \triangleq (W^1, W^2, W^3, W^4) \), \( \Pi \triangleq (\Pi_1, \Pi_2, \Pi_3, \Pi_4, \Sigma_1, \Sigma, \Omega, \Sigma) \), and \( c \triangleq \max \{ \langle |0\rangle_{\xi_+} |A_1 \rangle, \langle |0\rangle_{\xi_-} |A_1 \rangle, \langle |1\rangle_{\xi_+} |A_1 \rangle, \langle |1\rangle_{\xi_-} |A_1 \rangle \} \) (i.e., the “x basis”) and the projective measurement \( \{P_i\} \). It is easy to verify (see, e.g., [26]) that \( c_k \) of Theorem 2 is equal to \( c^{n_1} \) computed using the \( c \) of our proposition.

Then, we apply Theorem 2 to the state after Alice’s and Bob’s measurements of all TEST bits, before Alice’s and Bob’s measurements of the INFO bits (here it is important that our modified entanglement-based protocol delays Alice’s measurements in the “z basis” to Step 6, and that they can be delayed even to Step 10), conditioned on the first two tests passing (\( F^{sift'} = F^{\min} = \sqrt{) \), and requiring the third test to pass (\( F^{pe} = \sqrt{) \); (the difference between “conditioning” and “requiring” in this context is analogous to the difference between a “conditional probability” and a “joint probability”, respectively; see [20] for the precise definitions)
\[
\rho_{ABVW\Pi\Phi_A\Phi_BF^{sift'}F^{min}F^{pe}=\sqrt{F^{sift'}F^{min}}=\sqrt{}}
\]
and by choosing the parameters \( K = \Pi\Phi_A\Phi_B \), \( B = VWE \), \( C = B \) for the theorem, we get:
\[
H_{\min}^e(X^1 \land F^{pe} = \sqrt{|VW\Pi\Phi_A\Phi_BE}, F^{sift'} = F^{\min} = \sqrt{)} \sigma \\
+ H_{\max}^e(X'^1 \land F^{pe} = \sqrt{|B\Pi\Phi_A\Phi_B}, F^{sift'} = F^{\min} = \sqrt{)} \sigma \geq n_1 \log_2 \left( \frac{1}{c} \right),
\]
where \( X^1 \) and \( X'^1 \) represent the measurement results of the INFO bits in the “z basis” and in the “x basis”, respectively.

Performing a measurement of Bob’s INFO bits in subsystem B in the “x basis” (yielding the bit string \( Y'^1 \)) and discarding the classical information systems \( \Pi\Phi_A\Phi_B \) are two quantum operations (CPTP) operated exclusively on subsystems \( \Pi\Phi_A\Phi_B \). According to the data processing inequality (see, e.g., [25, 20]), such operations can only increase the max-entropy:
\[
H_{\max}^e(X'^1 \land F^{pe} = \sqrt{|B\Pi\Phi_A\Phi_B}, F^{sift'} = F^{\min} = \sqrt{)} \sigma \leq H_{\max}^e(X'^1 \land F^{pe} = \sqrt{|Y'^1}, F^{sift'} = F^{\min} = \sqrt{)} \sigma,
\]
which gives us the desired result:

\[
H_{\min}^e(X_1 \land F_{pe} = \sqrt{\text{VWE}} \Phi_A \Phi_B, \ F_{\text{sift}}' = F_{\text{min}} = \sqrt{\cdot})_\sigma \\
H_{\max}^e(X_1' \land F_{pe} = \sqrt{\text{Y}'|}, \ F_{\text{sift}}' = F_{\text{min}} = \sqrt{\cdot})_\sigma \geq n_1 \log_2 \left( \frac{1}{c} \right).
\]

(29)

4.2.3 The Law of Large Numbers

Intuitively, the proof of [20] uses a law of large numbers (Lemma 6 of [20]) to upper-bound the max-entropy \( H_{\max}^e(X|Y) \)—namely, the max-entropy of Alice’s raw key conditioned on Bob’s raw key in the real protocol. However, in our proof we need to bound \( H_{\max}^e(X_1'|Y_1') \)—namely, the max-entropy of Alice’s raw key conditioned on Bob’s raw key in a hypothetical protocol where Alice and Bob measure the INFO bits in the conjugate (“x”) basis. For obtaining this bound, we need to apply the law of large numbers twice, to two different hypothetical protocols:

1. In the \( X-X \) hypothetical protocol (where both Alice and Bob measure the INFO bits in the “x basis”), we can compare the TEST-X-X bits (where the only non-discarded rounds are those where Alice measured “\( \xi_+ \)”) to the INFO bits. This way, we can discover the error rate on the “\( \xi_+ \)” bits.

2. For finding the error rate on the “\( \xi_- \)” bits, we use the \( Z-X \) hypothetical protocol, where Alice measures the INFO bits in the “z basis” while Bob measures them in the “x basis”. The following intuitive formula will give us the needed bound:

\[
\Pr(A_i = - , B_i = +) = \Pr(A_i = 0 , B_i = +) + \Pr(A_i = 1 , B_i = +) - \Pr(A_i = + , B_i = +).
\]

(30)

This formula is intuitively trivial, because it follows from the formula:

\[
\Pr(A_i = - , B_i = +) + \Pr(A_i = + , B_i = +) = \Pr(B_i = +)
\]

(31)

Formally, it follows from the independence of Alice’s and Bob’s operations, as elaborated in the “bounding the fourth probability” portion of the proof of Proposition 6 below.

This idea can be compared with [28]’s analysis of the “loss-tolerant” protocol (improving on the usual analysis which involves matrix computations [12, 13, 14, 15]), but that analysis is more complicated and has several free parameters. Here we present a full and precise analysis leading to an explicit key rate formula in the single-qubit regime.

Formally, we use the following law of large numbers (Lemma 6 of [20]):

**Lemma 4.** (Lemma 6 of [20]) Given a set of \( N \) random variables \( Z = (Z_1, Z_2, \ldots, Z_N) \) where each \( Z_i \) takes values in \( \{0,1\} \) and \( N = a + b \), and given an independent, uniformly distributed subset \( \Pi \subseteq \{1,2,\ldots,N\} \) of size \( a \), it holds that:

\[
\Pr \left[ \sum_{i \in \Pi} Z_i \leq a\delta \land \sum_{i \in \Pi} Z_i \geq b \cdot (\delta + v) \right] \leq e^{-\frac{2b\delta^2v^2}{(a+b)(a+b+1)}}.
\]

(32)
Proof. Proved in [20, Subsection 6.3] as Lemma 6.

We also use another law of large numbers, proved by [29, Section 2, Theorem 1]:

**Lemma 5.** Let \( X_1, \ldots, X_N \) be independent random variables with finite first and second moments, such that \( 0 \leq X_i \leq 1 \) for all \( 1 \leq i \leq N \). If \( \overline{X} \triangleq \frac{X_1 + \cdots + X_N}{N} \) and \( \mu \triangleq E[\overline{X}] \) is the expected value of \( \overline{X} \), then for any \( \nu > 0 \),

\[
\Pr[\overline{X} - \mu \geq \nu] \leq e^{-2N\nu^2}.
\]

(33)

Using these Lemmas, we prove the following (a modified version of Proposition 8 from [20]):

**Proposition 6.** For the modified entanglement-based protocol described in Subsection 4.1, with error rate threshold \( \nu \) and zero rate threshold \( \delta_{\text{mismatch}} \), if we define for any \( 0 < \nu \leq \frac{1}{2} - \delta \):

\[
\delta'(\nu) \triangleq \delta_{\text{mismatch}} + \nu - \left( \frac{1}{2T} - \nu \right) \cdot (1 - 2\delta - 2\nu),
\]

(34)

\[
\epsilon(\nu) \triangleq \sqrt{e^{-2n_1\nu^2} + e^{-\frac{2n_1}{(\frac{1}{2T} - \nu)^2}\nu^2} + e^{-\frac{2n_1}{k_2}\nu^2}},
\]

(35)

then, for any \( 0 < \nu \leq \frac{1}{2} - \delta \) satisfying \( 0 < \delta'(\nu) \leq \frac{1}{2} \) and \( \epsilon(\nu)^2 < \Pr(F^\text{pe} = \checkmark | F^\text{sift'} = F^\text{min} = \checkmark) \), it holds that

\[
H^\epsilon(\nu)(X^\text{rl} \land F^\text{pe} = \checkmark | Y^\text{rl}, F^\text{sift'} = F^\text{min} = \checkmark) \leq n_1 \cdot h_2(\delta'(\nu)),
\]

(36)

where \( h_2(x) \triangleq -x \log_2(x) - (1 - x) \log_2(1 - x) \).

**Proof.** Let us define the following event:

\[
\Omega \triangleq 1 \left\{ \sum_{i=1}^{n_1} 1\{X^\text{rl}_i \neq Y^\text{rl}_i\} > n_1 \delta'(\nu) \right\}.
\]

(37)

We would like to prove the following probability to be exponentially small:

\[
\Pr[F^\text{pe} = \checkmark \land \Omega | F^\text{sift'} = F^\text{min} = \checkmark] = \Pr\left[\sum_{i=1}^{K_1} 1\{V^\text{rl}_i \neq W^\text{rl}_i\} \leq K_1 \nu \land K_2 \sum_{i=1}^{K_2} 1\{W^\text{rl}_i = 0\} \leq K_2 \delta_{\text{mismatch}} \land K_3 \sum_{i=1}^{K_3} 1\{W^\text{rl}_i^3 = 0\} \leq K_3 \delta_{\text{mismatch}} \land K_4 \sum_{i=1}^{K_4} 1\{V^\text{rl}_i^4 \neq W^\text{rl}_i^4\} \leq K_4 \delta \land \sum_{i=1}^{n_1} 1\{X^\text{rl}_i \neq Y^\text{rl}_i\} > n_1 \delta'(\nu) | F^\text{sift'} = F^\text{min} = \checkmark \right]\]

\[
\leq \Pr\left[\sum_{i=1}^{K_2} 1\{W^\text{rl}_i^2 = 0\} \leq K_2 \delta_{\text{mismatch}} \land \sum_{i=1}^{K_4} 1\{V^\text{rl}_i^4 \neq W^\text{rl}_i^4\} \leq K_4 \delta \land \sum_{i=1}^{n_1} 1\{X^\text{rl}_i \neq Y^\text{rl}_i\} > n_1 \delta'(\nu) | F^\text{sift'} = F^\text{min} = \checkmark \right].
\]

(38)
Let us remember that $V^2$ and $W^2$ are Alice’s and Bob’s substrings corresponding to $\Pi_2$ (the $k_2$ TEST-Z-X rounds); $V^4$ and $W^4$ are Alice’s and Bob’s substrings corresponding to $\Pi_4$ (the $k_4$ TEST-X-X rounds); and $X_i'$ and $Y_i'$ are Alice’s and Bob’s substrings corresponding to $\Sigma_1$ (the $n_1$ INFO rounds) in the X-X hypothetical protocol—namely, assuming that both Alice and Bob measured the INFO bits in the “$x$ basis”.

Let us also denote Alice’s “$\xi_+$ rate” (the percentage of INFO bits which Alice measures as “$\xi_+$”) in the X-X hypothetical protocol by $R'_+$—namely, $R'_+ \triangleq \frac{1}{n_1} \sum_{i=1}^{n_1} 1\{X_i' = 0\}$. Thus, the probability $\Pr \left[ F_{pe} = \checkmark \land \Omega \mid F_{sift'} = F_{min} = \checkmark \right]$ is bounded by the sum of four probabilities:

$$
\Pr \left[ F_{pe} = \checkmark \land \Omega \mid F_{sift'} = F_{min} = \checkmark \right] \leq \Pr \left[ R'_+ \leq \frac{1}{2T} - \nu \mid F_{sift'} = F_{min} = \checkmark \right] + \Pr \left[ R'_+ \geq \frac{1}{2T} - \nu \land \sum_{i=1}^{k_4} 1\{V_i^4 \neq W_i^4\} \leq k_4 \delta \right] + \Pr \left[ \sum_{i=1}^{k_2} 1\{W_i^2 = 0\} \leq k_2 \delta_{\text{mismatch}} \land \sum_{i=1}^{n_1} 1\{Y_i'^{1l} = 0\} \geq n_1 \cdot (\delta_{\text{mismatch}} + \nu) \mid F_{sift'} = F_{min} = \checkmark \right] + \Pr \left[ R'_+ \geq \frac{1}{2T} - \nu \land \sum_{i=1}^{n_1} 1\{X_i'^{1l} = 0 \land Y_i'^{1l} = 1\} \leq n_1 R'_+ \cdot (\delta + \nu) \land \sum_{i=1}^{n_1} 1\{Y_i'^{1l} = 0\} \leq n_1 \cdot (\delta_{\text{mismatch}} + \nu) \land \sum_{i=1}^{n_1} 1\{X_i'^{1l} \neq Y_i'^{1l}\} > n_1 \delta'(\nu) \mid F_{sift'} = F_{min} = \checkmark \right].
$$

We would now like to bound each of these four probabilities:

**Bounding the first probability:** We need to bound

$$
\Pr \left[ R'_+ \leq \frac{1}{2T} - \nu \mid F_{sift'} = F_{min} = \checkmark \right],
$$

where $R'_+$ is the “$\xi_+$” measurement rate of Alice among the INFO bits in the X-X hypothetical protocol. We notice that this rate is only dictated by identical quantum actions performed by Alice: because Alice measures all INFO bits in the “$x$ basis” in the hypothetical protocol, her measurement results are obtained independently for all rounds, and her probability of measuring “$\xi_+$” is always $\frac{1}{2T}$. Namely, Alice’s measurement results are $n_1$ independent random variables $\{X_i\}_{i=1}^{n_1}$ (with all probabilities conditioned on $F_{sift'} = F_{min} = \checkmark$) such that for each $i$:

$$
\Pr(X_i = 0 \mid F_{sift'} = F_{min} = \checkmark) = \frac{1}{2T}, \quad \Pr(X_i = 1 \mid F_{sift'} = F_{min} = \checkmark) = 1 - \frac{1}{2T}.
$$

Therefore, the expected value of each $X_i$ is $E[X_i] = 1 - \frac{1}{2T}$. 

17
We can thus apply Lemma 5 (which applies to $N$ independent random variables) to the random variables $\{X_i\}_{i=1}^{n_1}$ with parameters $N = n_1$ and $\mu = E[X] = 1 - \frac{1}{2T}$. We note that $X = 1 - R'_+$. Therefore, we obtain the following result:

$$
\Pr \left[ R'_+ \leq \frac{1}{2T} - \nu \mid F^{sift'} = F^{\min} = \checkmark \right] = \Pr \left[ R'_+ - \frac{1}{2T} \leq -\nu \mid F^{sift'} = F^{\min} = \checkmark \right] = \Pr \left[ \frac{1}{2T} - R'_+ \geq \nu \mid F^{sift'} = F^{\min} = \checkmark \right] = \Pr \left[ (1 - R'_+) - \left( 1 - \frac{1}{2T} \right) \geq \nu \mid F^{sift'} = F^{\min} = \checkmark \right] = \Pr \left[ X - \mu \geq \nu \mid F^{sift'} = F^{\min} = \checkmark \right] \leq e^{-2n_1\nu^2}. \quad (42)
$$

**Bounding the second probability:** We need to bound

$$
\Pr \left[ R'_+ \geq \frac{1}{2T} - \nu \wedge \sum_{i=1}^{k_4} 1\{V_i^4 \neq W_i^4\} \leq k_4\delta \wedge \sum_{i=1}^{n_1} 1\{X_i^{4l} = 0 \wedge Y_i^{4l} = 1\} \geq n_1R'_+ \cdot (\delta + \nu) \mid F^{sift'} = F^{\min} = \checkmark \right], \quad (43)
$$

where $V_i^4$ and $W_i^4$ are Alice’s and Bob’s substrings corresponding to $\Pi_4$ (the $k_4$ TEST-X-X rounds); $X_i^{4l}$ and $Y_i^{4l}$ are Alice’s and Bob’s substrings corresponding to $\Sigma_1$ (the $n_1$ INFO rounds) in the X-X hypothetical protocol; and $R'_+$ is the “$\xi_+$” measurement rate of Alice among the INFO bits in the X-X hypothetical protocol. We notice that the TEST-X-X rounds in $\Pi_4$ consist only of rounds where Alice measured “$\xi_+$” (the other rounds are discarded), so her recorded bit must be 0; therefore, the error event $V_i^4 \neq W_i^4$ is actually equivalent to $V_i^4 = 0 \wedge W_i^4 = 1$, and the probability is actually:

$$
\Pr \left[ R'_+ \geq \frac{1}{2T} - \nu \wedge \sum_{i=1}^{k_4} 1\{V_i^4 = 0 \wedge W_i^4 = 1\} \leq k_4\delta \wedge \sum_{i=1}^{n_1} 1\{X_i^{4l} = 0 \wedge Y_i^{4l} = 1\} \geq n_1R'_+ \cdot (\delta + \nu) \mid F^{sift'} = F^{\min} = \checkmark \right]. \quad (44)
$$

We notice that all rates are evaluated in the X-X hypothetical protocol; that in all rounds, both Alice and Bob measure in the “$x$ basis”; and that in all rounds taken into account, Alice gets the “$\xi_+$” result. We thus notice that the quantum behavior of Alice, Bob, and Eve is identical on all these rounds in the X-X hypothetical protocol (in particular, $D_i = 0$ for all these rounds; and while the timing of Alice’s measurements may differ, the timing is meaningless from the quantum point of view).

Therefore, we can apply Lemma 4 using the following parameters: the random variables $Z = (Z_1, Z_2, \ldots, Z_N)$ represent the condition that Alice’s bit is 0 and Bob’s bit is 1 (namely, $Z_i$ represents the evaluation of the condition $V_i^4 = 0 \wedge W_i^4 = 1$ or $X_i^{4l} = 0 \wedge Y_i^{4l} = 1$, respectively); the sampled subset $\Pi$ includes the $a = k_4$ TEST-X-X rounds in the $\Pi_4$ subset chosen by the protocol, and the rest $\tilde{\Pi}$ includes the $b = n_1R'_+\Sigma_1$ INFO rounds in the $\Sigma_1$ subset chosen by the protocol where Alice gets the “$\xi_+$” measurement result. The sampled subset $\Pi$ is completely
independent of Bob’s measurement results (that are dictated solely by Eve’s transmitted states and Alice’s results in the “x basis”), because we showed in Subsubsection 4.2.1 that \( \Sigma_1 \) and \( \Pi_4 \) can be seen as uniformly and randomly chosen subsets of \( \Sigma \), conditioning on \( F^\text{sift} = F^\text{min} = \checkmark \).

We remark that this is not a straightforward application of Lemma 4, because the number \( b = n_1 R'_+ \) of rounds in \( \bar{n}_1 \) is a random variable and not a parameter. Therefore, the computation is slightly more complicated, because all possible values of \( R'_+ = r'_+ \) need to be evaluated. Nevertheless, using the condition \( R'_+ \geq \frac{1}{2T} - \nu \) and applying Lemma 4 for any possible value of \( R'_+ \), we are able to bound this probability and prove it exponentially small.

Using the formulation of Lemma 4, we get:

\[
\Pr \left[ R'_+ \geq \frac{1}{2T} - \nu \land \sum_{i=1}^{k_4} \{ V_i^4 \neq W_i^4 \} \leq k_4 \delta \right] \\
\land \sum_{i=1}^{n_1} \{ X_i^{l1} = 0 \land Y_i^{l1} = 1 \} \geq n_1 R'_+ \cdot (\delta + \nu) \mid F^\text{sift} = F^\text{min} = \checkmark \\
= \Pr \left[ R'_+ \geq \frac{1}{2T} - \nu \land \sum_{i=1}^{k_4} \{ V_i^4 = 0 \land W_i^4 = 1 \} \leq k_4 \delta \right] \\
\land \sum_{i=1}^{n_1} \{ X_i^{l1} = 0 \land Y_i^{l1} = 1 \} \geq n_1 R'_+ \cdot (\delta + \nu) \mid F^\text{sift} = F^\text{min} = \checkmark \\
= \sum_{j=\lceil n_1 \cdot (\frac{1}{2T} - \nu) \rceil}^{n_1} \Pr \left[ R'_+ = \frac{j}{n_1} \land \sum_{i=1}^{k_4} \{ V_i^4 = 0 \land W_i^4 = 1 \} \leq k_4 \delta \right] \\
\land \sum_{i=1}^{n_1} \{ X_i^{l1} = 0 \land Y_i^{l1} = 1 \} \geq n_1 R'_+ \cdot (\delta + \nu) \mid R'_+ = \frac{j}{n_1} , F^\text{sift} = F^\text{min} = \checkmark \right].
\]

We can now bound this conditional probability, for each value of \( j \in \left[ n_1 \cdot \left( \frac{1}{2T} - \nu \right) , n_1 \right] \):

\[
\Pr \left[ \sum_{i=1}^{k_4} \{ V_i^4 = 0 \land W_i^4 = 1 \} \leq k_4 \delta \right] \\
\land \sum_{i=1}^{n_1} \{ X_i^{l1} = 0 \land Y_i^{l1} = 1 \} \geq n_1 R'_+ \cdot (\delta + \nu) \mid R'_+ = \frac{j}{n_1} , F^\text{sift} = F^\text{min} = \checkmark \\
= \Pr \left[ \sum_{i=1}^{k_4} \{ V_i^4 = 0 \land W_i^4 = 1 \} \leq k_4 \delta \right] \\
\land \sum_{i=1}^{n_1} \{ X_i^{l1} = 0 \land Y_i^{l1} = 1 \} \geq j \cdot (\delta + \nu) \mid R'_+ = \frac{j}{n_1} , F^\text{sift} = F^\text{min} = \checkmark \right].
\]
Bounding the third probability:

We need to bound

\[ \Pr \left[ \sum_{i \in \Pi} Z_i \leq k_4 \delta \land \sum_{i \in \Pi} Z_i \geq j \cdot (\delta + \nu) \mid R'_+ = \frac{j}{n_1}, F_{\text{sift}'} = F_{\min} = \checkmark \right] \]

\[ \leq e^{-\frac{2 \beta^2 \nu^2}{(k_4 + n_1)k_4 + 1}} \leq e^{-\frac{2n_1 \left(\frac{1}{T} - \nu \right) \gamma^2 \nu^2}{(k_4 + n_1) \left(\frac{1}{T} - \nu \right) \nu}} \]  

(46)

where the last inequality results from the fact that \( j \geq n_1 \cdot \left(\frac{1}{2T} - \nu \right) \).

Substituting Equation (46) into Equation (45), we get:

\[ \Pr \left[ R'_+ \geq \frac{1}{2T} - \nu \land \sum_{i = 1}^{k_4} 1 \{ V_i^d \neq W_i^d \} \leq k_4 \delta \right. \]

\[ \land \sum_{i = 1}^{n_1} 1 \{ X_i^{r_1} = 0 \land Y_i^{l_1} = 1 \} \geq n_1 R'_+ \cdot (\delta + \nu) \mid F_{\text{sift}'} = F_{\min} = \checkmark \]  

\[ = \sum_{j = [n_1 \left(\frac{1}{T} - \nu \right) \nu]}^{n_1} \Pr \left[ R'_+ = \frac{j}{n_1} \mid F_{\text{sift}'} = F_{\min} = \checkmark \right] \cdot \Pr \left[ \sum_{i = 1}^{k_4} 1 \{ V_i^d = 0 \land W_i^d = 1 \} \leq k_4 \delta \right. \]

\[ \land \sum_{i = 1}^{n_1} 1 \{ X_i^{r_1} = 0 \land Y_i^{l_1} = 1 \} \geq n_1 R'_+ \cdot (\delta + \nu) \mid R'_+ = \frac{j}{n_1}, F_{\text{sift}'} = F_{\min} = \checkmark \]  

\[ \leq \sum_{j = [n_1 \left(\frac{1}{T} - \nu \right) \nu]}^{n_1} \Pr \left[ R'_+ = \frac{j}{n_1} \mid F_{\text{sift}'} = F_{\min} = \checkmark \right] \cdot e^{-\frac{2n_1 \left(\frac{1}{T} - \nu \right) \gamma^2 \nu^2}{(k_4 + n_1) \left(\frac{1}{T} - \nu \right) \nu}} \]

\[ \leq e^{-\frac{2n_1 \left(\frac{1}{T} - \nu \right) \gamma^2 \nu^2}{(k_4 + n_1) \left(\frac{1}{T} - \nu \right) \nu}} \]  

(47)

Bounding the third probability:  We need to bound

\[ \Pr \left[ \sum_{i = 1}^{k_2} 1 \{ W_i^2 = 0 \} \leq k_2 \delta_{\text{mismatch}} \land \sum_{i = 1}^{n_1} 1 \{ Y_i^{r_1} = 0 \} \geq n_1 \cdot (\delta_{\text{mismatch}} + \nu) \mid F_{\text{sift}'} = F_{\min} = \checkmark \right] , \]

(48)

where \( W^2 \) is Bob’s substring corresponding to \( \Pi_2 \) (the \( k_2 \) TEST-Z-X rounds), and \( Y^{r_1} \) is Bob’s substring corresponding to \( \Sigma_1 \) (the \( n_1 \) INFO rounds) in the X-X hypothetical protocol. Let us now define \( X^{r_1} \) and \( Y^{r_1} \) as Alice’s and Bob’s substrings corresponding to \( \Sigma_1 \) (the \( n_1 \) INFO rounds) in the Z-X hypothetical protocol—namely, assuming that Alice measured the INFO bits in the “z basis”, and Bob measured the INFO bits in the “x basis”. We can notice that \( Y^{r_1} \) is completely identical to \( Y^{r_1} \), because Bob’s quantum operations (and Eve’s attack) are completely independent of Alice’s basis choice for the INFO bits (remembering that \( D_i = 0 \) for all INFO bits—namely, they are never discarded). Therefore, \( Y^{r_1} = Y^{r_1} \), and the probability is:

\[ = \Pr \left[ \sum_{i = 1}^{k_2} 1 \{ W_i^2 = 0 \} \leq k_2 \delta_{\text{mismatch}} \land \sum_{i = 1}^{n_1} 1 \{ Y_i^{r_1} = 0 \} \geq n_1 \cdot (\delta_{\text{mismatch}} + \nu) \mid F_{\text{sift}'} = F_{\min} = \checkmark \right] . \]

(49)

We notice that all rates are evaluated in the Z-X hypothetical protocol; that in all rounds, Bob measures in the “x basis” (and Alice measures in the “z basis”); and that Alice’s measurement results are completely unconstrained (namely, no discarding is possible, because \( D_i = 0 \) for all
rounds where Alice measures in the “\(z\) basis”). We thus notice that the quantum behavior of Alice, Bob, and Eve is identical on all these rounds in the Z-X hypothetical protocol.

Therefore, we can apply Lemma 4 using the following parameters: the random variables \(Z = (Z_1, Z_2, \ldots, Z_N)\) represent the condition that Bob’s bit is 0 (namely, \(Z_i\) is the value of \(1 - W_i^2\) or \(1 - Y_i'^{\perp 1}\), respectively); the sampled subset \(\Pi\) includes the \(a = k_2\) TEST-Z-X rounds in the \(\Pi_2\) subset chosen by the protocol, and the rest \(\Pi\) includes the \(b = n_1\) INFO rounds in the \(\Sigma_1\) subset chosen by the protocol (note that Bob measures them in the “\(x\) basis”). The sampled subset \(\Pi\) is completely independent of Bob’s measurement results (that are dictated solely by Eve’s transmitted states and Alice’s non-discarding of the rounds), because we showed in Subsubsection 4.2.1 that \(\Sigma_1\) and \(\Pi_2\) can be seen as uniformly and randomly chosen subsets of \(\Sigma\), conditioning on \(F^{\text{sift}} = F^{\text{min}} = \checkmark\). Using the formulation of Lemma 4, we get:

\[
\begin{align*}
\Pr \left[ \sum_{i=1}^{k_2} W_i^2 = 0 \right] & \leq k_2 \delta_{\text{mismatch}} \land \sum_{i=1}^{n_1} Y_i'^{\perp 1} = 0 \geq n_1 \cdot (\delta_{\text{mismatch}} + \nu) \land F^{\text{sift}} = F^{\text{min}} = \checkmark \\
\Pr \left[ \sum_{i=1}^{k_2} W_i^2 = 0 \right] & \leq k_2 \delta_{\text{mismatch}} \land \sum_{i=1}^{n_1} Y_i'^{\perp 1} = 0 \geq n_1 \cdot (\delta_{\text{mismatch}} + \nu) \land F^{\text{sift}} = F^{\text{min}} = \checkmark \\
\Pr \left[ \sum_{i \in \Pi} Z_i \leq k_2 \delta_{\text{mismatch}} \land \sum_{i \in \Pi} Z_i \geq n_1 \cdot (\delta_{\text{mismatch}} + \nu) \land F^{\text{sift}} = F^{\text{min}} = \checkmark \right] & \leq e^{-\frac{2n_1 k_2^2 \nu^2}{(k_2 + n_1)(k_2 + 1)}}.
\end{align*}
\]

Bounding the fourth probability: We need to bound

\[
\begin{align*}
\Pr \left[ R'_+ \geq \frac{1}{2T} - \nu \land \sum_{i=1}^{n_1} Y_i'^{\perp 1} = 0 \land X_i'^{\perp 1} = 1 \right] & \leq n_1 R'_+ \cdot (\delta + \nu) \land \sum_{i=1}^{n_1} Y_i'^{\perp 1} = 0 \leq n_1 \cdot (\delta_{\text{mismatch}} + \nu) \land \sum_{i=1}^{n_1} Y_i'^{\perp 1} = 1 \geq n_1 \delta'(\nu) \land F^{\text{sift}} = F^{\text{min}} = \checkmark,
\end{align*}
\]

(51)

where \(X_i'^{\perp 1}\) and \(Y_i'^{\perp 1}\) are Alice’s and Bob’s substrings corresponding to \(\Sigma_1\) (the \(n_1\) INFO rounds) in the X-X hypothetical protocol, and \(R'_+\) is the “\(\xi_+\)” measurement rate of Alice among the INFO bits in the X-X hypothetical protocol. We would like to prove this probability to be zero; namely, the combination of the above conditions must be impossible.

Indeed, assume by contradiction that all four conditions hold:

\[
\begin{align*}
R'_+ \geq \frac{1}{2T} - \nu \land \sum_{i=1}^{n_1} Y_i'^{\perp 1} = 0 \land X_i'^{\perp 1} = 1 \leq n_1 R'_+ \cdot (\delta + \nu) \land \sum_{i=1}^{n_1} Y_i'^{\perp 1} = 0 \leq n_1 \cdot (\delta_{\text{mismatch}} + \nu) \land \sum_{i=1}^{n_1} Y_i'^{\perp 1} = 1 \geq n_1 \delta'(\nu),
\end{align*}
\]

(52)

We can upper-bound \(\sum_{i=1}^{n_1} Y_i'^{\perp 1} = 1\) (which represents the total error rate on the INFO bits in the X-X hypothetical protocol) using the first three conditions, as well as the two following
definitions: \( \delta'(v) \triangleq \delta_{\text{mismatch}} + v - (\frac{1}{2T} - v) \cdot (1 - 2\delta - 2v) \) and \( R'_+ \triangleq \frac{1}{n_1} \sum_{i=1}^{n_1} 1 \{ X'_i = 0 \}. \) So:

\[
\begin{align*}
\sum_{i=1}^{n_1} 1 \{ X'_i \neq Y'_i \} &= \sum_{i=1}^{n_1} 1 \{ X'_i = 0 \land Y'_i = 1 \} + \sum_{i=1}^{n_1} 1 \{ X'_i = 1 \land Y'_i = 0 \} \\
&= \sum_{i=1}^{n_1} 1 \{ X'_i = 0 \land Y'_i = 1 \} + \sum_{i=1}^{n_1} 1 \{ Y'_i = 0 \} - \sum_{i=1}^{n_1} 1 \{ X'_i = 0 \land Y'_i = 0 \} \\
&= \sum_{i=1}^{n_1} 1 \{ X'_i = 0 \land Y'_i = 1 \} + \sum_{i=1}^{n_1} 1 \{ Y'_i = 0 \} \\
&- \left[ \sum_{i=1}^{n_1} 1 \{ X'_i = 0 \} - \sum_{i=1}^{n_1} 1 \{ X'_i = 0 \land Y'_i = 1 \} \right] \\
&= 2 \sum_{i=1}^{n_1} 1 \{ X'_i = 0 \land Y'_i = 1 \} + \sum_{i=1}^{n_1} 1 \{ Y'_i = 0 \} - \sum_{i=1}^{n_1} 1 \{ X'_i = 0 \} \\
&= 2 \sum_{i=1}^{n_1} 1 \{ X'_i = 0 \land Y'_i = 1 \} + \sum_{i=1}^{n_1} 1 \{ Y'_i = 0 \} - n_1 R'_+ \\
&\leq 2n_1 R'_+ \cdot (\delta + v) + n_1 \cdot (\delta_{\text{mismatch}} + v) - n_1 R'_+ \\
&= n_1 \cdot 2R'_+ \cdot (\delta + v) + \delta_{\text{mismatch}} + v - R'_+ \\
&= n_1 \cdot [\delta_{\text{mismatch}} + v - R'_+ \cdot (1 - 2\delta - 2v)] \\
&\leq n_1 \cdot [\delta_{\text{mismatch}} + v - (\frac{1}{2T} - v) \cdot (1 - 2\delta - 2v)] = n_1 \delta'(v), \quad (53)
\end{align*}
\]

which strictly contradicts the fourth condition. (In the last inequality we also used the condition \( v \leq \frac{1}{2} - \delta \), which means that \( 1 - 2\delta - 2v \geq 0 \).) Therefore, our probability is 0.

**Summary of the proof:** Combining our four bounds, we get the following inequality:

\[
\begin{align*}
\Pr \left[ F^{\text{pe}} = \checkmark \land \Omega \mid F^{\text{sift}}' = F^{\text{min}} = \checkmark \right] \\
&\leq \Pr \left[ R'_+ \leq \frac{1}{2T} - v \mid F^{\text{sift}}' = F^{\text{min}} = \checkmark \right] \\
&+ \Pr \left[ R'_+ \geq \frac{1}{2T} - v \land \sum_{i=1}^{k_2} 1 \{ X'_i \neq W'_i \} \leq k_4 \delta \right] \\
&\land \sum_{i=1}^{n_1} 1 \{ X'_i = 0 \land Y'_i = 1 \} \geq n_1 R'_+ \cdot (\delta + v) \mid F^{\text{sift}}' = F^{\text{min}} = \checkmark \\
&+ \Pr \left[ \sum_{i=1}^{k_2} 1 \{ W'_i = 0 \} \leq k_2 \delta_{\text{mismatch}} \land \sum_{i=1}^{n_1} 1 \{ Y'_i = 0 \} \geq n_1 \cdot (\delta_{\text{mismatch}} + v) \mid F^{\text{sift}}' = F^{\text{min}} = \checkmark \right] \\
&+ \Pr \left[ R'_+ \geq \frac{1}{2T} - v \land \sum_{i=1}^{n_1} 1 \{ X'_i = 0 \land Y'_i = 1 \} \leq n_1 R'_+ \cdot (\delta + v) \right] \\
&\land \sum_{i=1}^{n_1} 1 \{ Y'_i = 0 \} \leq n_1 \cdot (\delta_{\text{mismatch}} + v) \land \sum_{i=1}^{n_1} 1 \{ X'_i \neq Y'_i \} > n_1 \delta'(v) \mid F^{\text{sift}}' = F^{\text{min}} = \checkmark \\
\end{align*}
\]

22
\[ \begin{aligned}
\leq & \quad e^{-2n_1v^2} + e^{-\frac{2n_1(\frac{1}{T} - v)k_2^2v^2}{(k_4+n_1)(\frac{1}{T} - v)}(k_2+1)} + e^{-\frac{2n_1k_2^2v^2}{(k_2+n_1)(k_2+1)}}
= & \quad \varepsilon(v)^2.
\end{aligned} \]

The rest of the proof is identical to the proof of Proposition 8 in [20, Subsection 6.3], using our parameters \( \varepsilon(v), X^1, Y^1, n_1, \Omega, \delta'(v) \). (A small algebraic difference is that our set \( \Omega \) requires a strong inequality \((1 \approx \sum_{i=1}^{n_1} 1\{X^1_i \neq Y^1_i\} > n_1 \delta'(v)\}) while [20]'s set \( \Omega \) requires a weak inequality \((1 \approx \sum_{i=1}^{n_1} 1\{X_i \neq Y_i\} \geq n_1 \delta'(v)\}), but the proof still holds.) Therefore, we obtain:

\[ H_{\text{max}}^{\varepsilon(v)}(X^1 \land F_{\text{pe}} = \checkmark | Y^1, F_{\text{sift'}} = F_{\text{min}} = \checkmark) \leq n_1 \cdot h_2(\delta'(v)), \]

as we wanted.

\[ \square \]

4.2.4 Security Theorem for the Modified Entanglement-Based Protocol

Applying the entire proof described in [20, Section 6] to our modified entanglement-based protocol described in Subsection 4.1, with the modifications described in Subsubsections 4.2.1–4.2.3, gives the following security result:

**Corollary 7.** For the modified entanglement-based protocol described in Subsection 4.1, we denote the final state as \( \omega_{KA,KB,SCFE} \), where \( K_A \) is the final key generated by Alice and \( K_B \) is the final key generated by Bob (both consisting of \( \ell \) bits), \( E \) is Eve’s ancillary quantum system, and \( S, C, F \) consist of information published by Alice and Bob (where \( H_{ec}, H_{pa}, Z, T, F_{ec}, r, t \) are used in the error correction and privacy amplification step elaborated in [20]):

\[ S \triangleq (\Phi_A, \Phi_B, \Pi_1, \Pi_2, \Pi_3, \Pi_4, \Sigma_1, H_{ec}, H_{pa}), \]

\[ C \triangleq (\Omega, \Sigma, V^1, V^2, V^3, V^4, Z, T), \]

\[ F \triangleq (F_{\text{sift'}}, F_{\text{min}}, F_{pe}, F_{ec}). \]

We also denote \( \omega_{\Omega} \triangleq \frac{1}{2^\frac{T}{2}} \sum_{k \in \{0,1\}^T} \langle k | k_A \rangle \langle k | k_B \rangle \) (an ideal key: a uniformly random key, identical for Alice and Bob) and \( \omega_{SCFE} \triangleq I_{KA,KB} \otimes \omega_{\Omega_{KA,KB,SCFE}} \). It then holds that:

\[ \frac{1}{2} \left\| \omega_{KA,KB,SCFE} \land F_{pe} = \checkmark \land F_{\text{sift'}} = F_{\text{min}} = \checkmark \right\| - \omega_{\Omega} \otimes \omega_{SCFE} \land F_{pe} = \checkmark \land F_{\text{sift'}} = F_{\text{min}} = \checkmark \]
\[ \leq 2^{-r} + \inf_{v, \delta'(v) < \frac{1}{2}} (\varepsilon_{pa}(v) + \varepsilon_{pe}(v)), \]

where we define:

\[ \varepsilon_{pa}(v) \triangleq \frac{1}{2} \sqrt{2^{-n_1(\log_2(\frac{1}{T}) - h_2(\delta'(v))) + r + \ell}}, \]

\[ \varepsilon_{pa}(v) \triangleq 2 \varepsilon(v), \]

\[ \delta'(v) \triangleq \delta_{\text{mismatch}} + v - \left( \frac{1}{2T} - v \right) \cdot (1 - 2\delta - 2v), \]

\[ \varepsilon(v) \triangleq \sqrt{e^{-2n_1v^2} + e^{-\frac{2n_1(\frac{1}{T} - v)k_2^2v^2}{(k_4+n_1)(\frac{1}{T} - v)}(k_2+1)} + e^{-\frac{2n_1k_2^2v^2}{(k_2+n_1)(k_2+1)}}}, \]

\[ h_2(x) \triangleq -x \log_2(x) - (1 - x) \log_2(1 - x). \]
This result is similar to [20, Section 5], but has different parameters. According to standard definitions of composable security for QKD (see, e.g., [25]), this proves security of the modified entanglement-based protocol and gives a tight finite-key rate.

### 4.3 Reduction of the Original Protocol to the Modified Entanglement-Based Protocol

Intuitively, for proving the security of our original prepare-and-measure protocol from Section 3, we perform a reduction to the entanglement-based protocol: namely, we show that the modified entanglement-based protocol includes the prepare-and-measure protocol as a special case.

The proof intuitively works as follows: in the prepare-and-measure protocol, instead of generating one of the states \( \{ |\gamma_0\rangle_B, |\gamma_1\rangle_B, |\gamma_+\rangle_B \} \), Alice can instead generate the following entangled state:

\[
|\Psi\rangle_{A,B} \triangleq \frac{|0\rangle_A |\gamma_0\rangle_B + |1\rangle_A |\gamma_1\rangle_B}{\sqrt{2}} = |\xi_+\rangle_A |\gamma_+\rangle_B + \sqrt{2T-1} |\xi_{\ -}\rangle_A |\gamma_{\ -}\rangle_B,
\]

where the equality between the two expressions in Equation (65) can be shown algebraically using Equations (3)–(5) and (8)–(9). Then, Alice either measures her subsystem \( A \) in the standard ("\( \xi \)" basis \( \{ |0\rangle_A, |1\rangle_A \} \) with probability \( p^{\xi}_A \), or measures it in the conjugate ("\( \gamma \)" basis \( \{ |\xi_+\rangle_A, |\xi_{\ -}\rangle_A \} \) with probability \( p^{\gamma}_A \). Either way, she sends the resulting state in subsystem \( B \) to Bob (immediately notifying Bob and canceling the round if she measured "\( \xi_{\ -}\)" in the "\( \gamma \) basis"). This procedure is equivalent to our original prepare-and-measure protocol, but it works within the framework of the modified entanglement-based protocol (assuming Alice gets the chance to measure and discard the round before Bob gets his own state from Eve), which proves the reduction.

Formally, we use an adapted version of the reduction in Section 7 of [20]. First of all, given the parameters of the original prepare-and-measure protocol (described in its step 1), we must define all the parameters of the modified entanglement-based protocol (described in its step 1), which we do as follows:

- The parameters \( |\gamma_0\rangle_B, |\gamma_1\rangle_B, |\gamma_+\rangle_B, m, k_1, k_2, k_3, k_4, n_1, \delta, \delta_{\text{mismatch}} \) are all identical for the two protocols. (From \( |\gamma_0\rangle_B, |\gamma_1\rangle_B, |\gamma_+\rangle_B \) we infer \( a, b, \) and \( T \triangleq |a|^2 + |b|^2 \).)
- Given Bob’s measurement operators \( \{ M_{B_i}^{Z,t} \}_{t \in \{0,1\}} \) and \( \{ M_{B_i}^{X,1} \}_{t \in \{0,1\}} \) in the prepare-and-measure protocol, we choose Bob’s measurement operators \( \{ M_{B_i}^{Z,t} \}_{t \in \{0,1\}} \) and \( \{ M_{B_i}^{X,t} \}_{t \in \{0,1\}} \) of the entanglement-based protocol to be: (similarly to the proof of Lemma 16 in [20, Subsection 9.2])

\[
M_{B_i}^{Z,t} = \frac{M_{B_i}^{Z,t}}{\sqrt{M_{B_i}^{Z,t}}}, \quad M_{B_i}^{X,t} = \frac{M_{B_i}^{X,t}}{\sqrt{M_{B_i}^{X,t}}},
\]

where we first define: (these equalities result from Equation (2))

\[
\begin{align*}
\left( M_{B_i}^{\gamma} \right)^\dagger \left( M_{B_i}^{\gamma} \right) & \triangleq \sum_{t=0}^{1} \left( M_{B_i}^{Z,t} \right)^\dagger \left( M_{B_i}^{Z,t} \right) = \sum_{t=0}^{1} \left( M_{B_i}^{X,t} \right)^\dagger \left( M_{B_i}^{X,t} \right), \\
\left( M_{B_i}^{\theta} \right)^\dagger \left( M_{B_i}^{\theta} \right) & \triangleq \left( M_{B_i}^{Z,0} \right)^\dagger \left( M_{B_i}^{Z,0} \right) = \left( M_{B_i}^{X,0} \right)^\dagger \left( M_{B_i}^{X,0} \right).
\end{align*}
\]
• We choose the parameter $0 < \nu_0 < \frac{1}{2T}$ of the entanglement-based protocol freely, without any constraint, where the trade-off is between performance (number of needed rounds) and robustness (sifting success probability).

• Given the parameters $m, T, \nu_0$, we choose the parameter $M'$ of the entanglement-based protocol to be:

$$M' = \frac{m}{2T - \nu_0}.$$  \hspace{1cm} (69)

• Given the parameters $p^{A_A}_z, p^{A_A}_x$ of the prepare-and-measure protocol and the parameter $T$, we choose the parameters $p'_{zA}^{A_A}, p'_{xA}^{A_A}$ of the entanglement-based protocol to be:

$$p'_{zA}^{A_A} = \frac{p_z^{A_A}}{p_z^{A_A} + 2T p_x^{A_A}} \quad , \quad p'_{xA}^{A_A} = \frac{2T p_x^{A_A}}{p_z^{A_A} + 2T p_x^{A_A}}.$$  \hspace{1cm} (70)

• Given the parameters $p^{B_B}_z, p^{B_B}_x$ of the prepare-and-measure protocol, we choose the parameters $p'_{zB}^{B_B}, p'_{xB}^{B_B}$ of the entanglement-based protocol to be:

$$p'_{zB}^{B_B} = p_z^{B_B} \quad , \quad p'_{xB}^{B_B} = p_x^{B_B}.$$  \hspace{1cm} (71)

Using these parameters, it is easy to verify that the output of the prepare-and-measure protocol (conditioned on $F_{\text{sift}} = F_{\text{min}} = \sqrt{\cdot}$) is identical to the output of the modified entanglement-based protocol (conditioned on $F'_{\text{sift}} = F_{\text{min}} = \sqrt{\cdot}$) if Eve performs the same attack on the first $m$ non-discarded rounds in both protocols. Formally, the differences between the protocols are settled as follows:

• The prepare-and-measure protocol includes the possibility of non-definite measurement results (e.g., losses), while the modified entanglement-based protocol does not allow them. The techniques of Lemmas 16 and 17 of [20, Subsection 9.2] can be applied and easily work for our protocols, too; therefore, the sifting and discarding of rounds where Bob achieved non-definite measurement results does not hurt the reduction: it does not hurt the independent probabilities of Alice and Bob choosing each basis (because, similarly to [20], Equation (2) requires the non-definite results to be identical for each basis), and Eve’s attack on the first $m$ rounds with definite results (i.e., on $\Sigma$) can easily be deduced. Bob’s measurement process is thus divided into two parts (as in Lemma 16 of [20]): the first part, where Bob’s device “decides” whether the result is definite or not (which is independent of the basis), and the second part, where Bob’s device actually performs the measurement and gives a definite result (equivalent to Equation (66)). The first part is performed before the reduction, and the second part is identical between the two protocols.

• The modified entanglement-based protocol includes the possibility of discarded rounds (where Alice measures “$\xi^-$”) which are immediately notified to Bob and Eve, while the prepare-and-measure protocol does not allow them. For this, we use the explanation in Subsubsection 4.2.1 to divide the process into two stages (again, this division works with respect to the probability distribution, not to the actual quantum operations): stage 1, where Alice determines which rounds are discarded; and stage 2, where Alice determines the basis for measuring all the non-discarded rounds. As explained in
Subsubsection 4.2.1, stage 1 is in fact independent on the bases used for non-discarded rounds; furthermore, the results of stage 1 are promptly communicated to Eve, who can devise her attack accordingly. Meanwhile, stage 2 is completely identical between the two protocols, as shown in the next item.

- **Alice’s preparation** is different between the two protocols:

  In the prepare-and-measure protocol, Alice randomly chooses $\Phi_A \in \{0, 1\}^M$ (where each bit, independently, is 0 with probability $p_A^0$ or 1 with probability $p_A^1$) and chooses $\Phi_A, R \in \{0, 1\}^M$ uniformly at random, which lead to the preparation of $|\gamma_0\rangle_B$, $|\gamma_1\rangle_B$, or $|\gamma_+\rangle_B$, with probabilities $\frac{p_A^0}{2}$, $\frac{p_A^1}{2}$, and $p_A^x$, respectively.

  In the modified entanglement-based protocol, Alice generates the following state $|\Psi\rangle$ for each round $i$:

  $$|\Psi\rangle_{A,B_i} \triangleq \frac{|0\rangle_A |\gamma_0\rangle_B + |1\rangle_A |\gamma_1\rangle_B}{\sqrt{2}} = |\xi_i\rangle_A |\gamma_i\rangle_B + \frac{\sqrt{2T-1} |\xi_i\rangle_A |\gamma_i\rangle_B}{\sqrt{2T}} , \quad (72)$$

  randomly chooses the measurement bases $\Phi_A \in \{0, 1\}^M$ (where each bit, independently, is 0 with probability $p_z^A$ or 1 with probability $p_x^A$), performs the measurement, publicly discards the round if she gets “$\xi_z$”, and keeps the result secret otherwise. (In fact, the measurement can be delayed if the chosen basis is $z$, as described in Subsection 4.1.) As explained in Subsubsection 4.2.1 (Equations (19)–(20)), for each of the *non-discarded* rounds, the total probabilities that Alice measures “0”, “1”, or “$\xi_+$” (leading to her sending to Bob $|\xi_0\rangle_B$, $|\xi_1\rangle_B$, or $|\xi_+\rangle_B$, respectively) are:

  $$\Pr_{A_i}(0) = \Pr_{A_i}(1) = \frac{1}{2} \cdot \frac{p_z^A}{p_z^A + \frac{p_x^A}{2T}} , \quad \Pr_{A_i}(\xi_+) = \frac{1}{2T} \cdot \frac{p_x^A}{p_z^A + \frac{p_x^A}{2T}} . \quad (73)$$

  Substituting Equation (70) (and the fact $p_z^A + p_x^A = 1$), we get the following probabilities:

  $$\Pr_{A_i}(0) = \Pr_{A_i}(1) = \frac{1}{2} \cdot \frac{p_z^A}{p_z^A + \frac{2T p_x^A}{p_z^A + 2T p_x^A}} = \frac{1}{2} \cdot \frac{p_z^A}{p_z^A + p_x^A} = \frac{p_z^A}{2} , \quad (74)$$

  $$\Pr_{A_i}(\xi_+) = \frac{1}{2T} \cdot \frac{p_x^A}{p_z^A + \frac{2T p_x^A}{p_z^A + 2T p_x^A}} = \frac{1}{2T} \cdot \frac{2T p_x^A}{p_z^A + p_x^A} = p_x^A , \quad (75)$$

  which are identical to the prepare-and-measure probabilities found above. Therefore, Alice’s preparation results are identical on the non-discarded rounds of both protocols.

- **Eve’s attack** is slightly different between the two protocols: on the prepare-and-measure protocol it is applied to all $M$ rounds (including those where Bob obtains a non-definite measurement result), while on the modified entanglement-based protocol it is applied to all $M'$ rounds (including the discarded rounds), and Eve knows *ahead of time* which rounds are discarded.
We need to prove that any attack that Eve applies to the relevant rounds of the prepare-and-measure protocol (namely, the $m$ rounds in $\Sigma$, which are the first $m$ rounds where Bob gets a definite measurement result), can also be applied to the relevant rounds of the modified entanglement-based (namely, the $m$ rounds in $\Sigma$, which are the first $m$ rounds not discarded by Alice). This is indeed true, because in the modified entanglement-based protocol, Eve knows ahead of time (before she applies her attack) which rounds are discarded, and therefore she knows exactly which rounds are included in $\Sigma$ and can apply her attack only to them. This means that any attack by Eve on the $\Sigma$ rounds of the prepare-and-measure protocol, is a completely legitimate and valid attack on the $\Sigma$ rounds of the modified entanglement-based protocol.

- The rest of the steps in the prepare-and-measure protocol (Steps 6–10) are identical to the rest of the steps in the modified entanglement-based protocol (Steps 8–12).

From the above we can deduce that any attack by Eve on the prepare-and-measure protocol, can also be applied to the modified entanglement-based protocol, giving exactly the same output. This conclusion only applies when we condition on $F_{\text{sift}} = F_{\text{min}} = \sqrt{\epsilon}$ (for the prepare-and-measure protocol) and $F_{\text{sift}}' = F_{\text{min}} = \sqrt{\epsilon}$ (for the modified entanglement-based protocol), which is indeed the case in our security proof in Subsection 4.2.

We therefore obtain the following result:

**Corollary 8.** If the modified entanglement-based protocol is secure with a specific security parameter $\epsilon$, the prepare-and-measure protocol is secure with the same security parameter.

Combining Corollaries 7 and 8, we get the final security result for the prepare-and-measure protocol:

**Corollary 9.** For the prepare-and-measure protocol described in Section 3, we denote the final state as $\omega_{K_A K_B \text{SCFE}}$, where $K_A$ is the final key generated by Alice and $K_B$ is the final key generated by Bob (both consisting of $\ell$ bits), $E$ is Eve's ancillary quantum system, and $S, C, F$ consist of information published by Alice and Bob (where $H_{\text{ec}}, H_{\text{pa}}, Z, T, F_{\text{ec}}, r, t$ are used in the error correction and privacy amplification step elaborated in [20]):

\[
S \triangleq (\Phi_1, \Phi_2, \Pi_1, \Pi_2, \Pi_3, \Pi_4, \Sigma, H_{\text{ec}}, H_{\text{pa}}), \quad (76)
\]

\[
C \triangleq (\Omega, \Sigma, V^1, V^2, V^3, V^4, Z, T), \quad (77)
\]

\[
F \triangleq (F_{\text{sift}}, F_{\text{min}}, F_{\text{pe}}, F_{\text{ec}}). \quad (78)
\]

We also denote $\omega_U \triangleq \frac{1}{2^n} \sum_{k \in \{0,1\}^n} |k\rangle_{K_A} \langle k|_{K_B} \otimes |k\rangle_{K_B} \langle k|_{K_B}$ (an ideal key: a uniformly random key, identical for Alice and Bob) and $\omega_{\text{SCFE}} \triangleq \text{tr}_{K_A K_B}(\omega_{K_A K_B \text{SCFE}})$. It then holds that:

\[
\frac{1}{2} \text{tr} \left| \omega_{K_A K_B \text{SCFE}} \wedge \text{Fpe} = \text{Fec} = \sqrt{\epsilon} \right| \text{Fpe} = \text{Fmin} = \sqrt{\epsilon} - \omega_{\text{U}} \otimes \omega_{\text{SCFE}} \wedge \text{Fpe} = \text{Fec} = \sqrt{\epsilon} | \text{Fpe} = \text{Fmin} = \sqrt{\epsilon} \right| \\
\leq 2^{-t} + \inf_v (\epsilon_{\text{pa}}(v) + \epsilon_{\text{pe}}(v)), \quad (79)
\]

where we define:

\[
\epsilon_{\text{pa}}(v) \triangleq \frac{1}{2} \sqrt{2^{-n_1 - (\log_2(\frac{1}{\sqrt{2}}) - h_2(\delta'(v))) + r + t + \ell}}, \quad (80)
\]

27
We thus get the following conditions for equality between Equation (85) and Equation (87):

\[
\epsilon_{pa}(v) \triangleq 2\epsilon(v), \quad \delta'(v) \triangleq \delta_{\text{mismatch}} + v - \left(\frac{1}{2T} - v\right) \cdot (1 - 2\delta - 2v),
\]

\[
\epsilon(v) \triangleq \sqrt{e^{-2n_1v^2} + e^{-\frac{2n_1}{(4 + n_1)T}} + e^{-\frac{2n_1k_2^2v^2}{(5 + 2n_1)(k_2^2 + 1)}},
\]

\[
h_2(x) \triangleq -x\log_2(x) - (1-x)\log_2(1-x).
\]

5 Necessity of the Restriction to Three Source States

In our protocol, similarly to the “loss tolerant” protocol, only three source states are used. This restriction is necessary in the imperfect-generation regime, as we briefly explain below.

Let us assume that our protocols emits four input states (like BB84), denoted \(|\gamma_0\rangle, |\gamma_1\rangle, |\gamma_+\rangle, |\gamma_-\rangle\). For standard security analysis to work, the following conditions is required for some \(0 < p < 1\) and \(0 < q < 1\):

\[
p|\gamma_0\rangle\langle\gamma_0| + (1-p)|\gamma_1\rangle\langle\gamma_1| = q|\gamma_+\rangle\langle\gamma_+| + (1-q)|\gamma_-\rangle\langle\gamma_-|,
\]

which means that Alice sends to Bob identical mixed states in each round of the protocol, independently of the chosen basis. (Otherwise, Eve may gain information on the basis and attack differently on each basis, which refutes the crucial possibility of comparing her attack’s influence in different bases.)

For meeting the above condition, we obviously need \(|\gamma_+\rangle\) and \(|\gamma_-\rangle\) to be in the 2-dimensional Hilbert subspace spanned by \(|\gamma_0\rangle\) and \(|\gamma_1\rangle\). Therefore, we require (for some \(a, b, c, d \in \mathbb{C}\)):

\[
|\gamma_+\rangle = a|\gamma_0\rangle + b|\gamma_1\rangle, \quad |\gamma_-\rangle = c|\gamma_0\rangle + d|\gamma_1\rangle.
\]

Substituting this in Equation (85), we get:

\[
q|\gamma_+\rangle\langle\gamma_+| + (1-q)|\gamma_-\rangle\langle\gamma_-| = q \cdot [a|\gamma_0\rangle + b|\gamma_1\rangle] \cdot [a^*\langle\gamma_0| + b^*\langle\gamma_1|] + (1-q) \cdot [c|\gamma_0\rangle + d|\gamma_1\rangle] \cdot [c^*\langle\gamma_0| + d^*\langle\gamma_1|]
\]

\[
= [q \cdot |a|^2 + (1-q) \cdot |c|^2] \cdot |\gamma_0\rangle\langle\gamma_0| + [q \cdot ab^* + (1-q) \cdot cd^*] \cdot |\gamma_0\rangle\langle\gamma_1| + [q \cdot a^*b + (1-q) \cdot c^*d] \cdot |\gamma_1\rangle\langle\gamma_0| + [q \cdot |b|^2 + (1-q) \cdot |d|^2] \cdot |\gamma_1\rangle\langle\gamma_1|.
\]

We thus get the following conditions for equality between Equation (85) and Equation (87):

\[
q \cdot |a|^2 + (1-q) \cdot |c|^2 = p, \quad (88)
\]

\[
q \cdot |b|^2 + (1-q) \cdot |d|^2 = 1 - p, \quad (89)
\]

\[
q \cdot ab^* + (1-q) \cdot cd^* = 0, \quad (90)
\]

\[
q \cdot a^*b + (1-q) \cdot c^*d = 0. \quad (91)
\]

The two last equations are the complex conjugates of one another, so one of them is sufficient.

Therefore, for standard security proofs to work, we require very stringent conditions on \(a, b, c, d\). In particular, according to Equation (91), we require:

\[
q = -\frac{c^*d}{a^*b - c^*d} = \frac{c^*d}{c^*d - a^*b}, \quad (92)
\]
and for $q$ to be real (and satisfy $0 < q < 1$), the complex phases of $c \ast d$ and $a \ast b$ must be opposite.

This requirement poses severe restrictions on $|\gamma_0\rangle, |\gamma_1\rangle, |\gamma_+\rangle, |\gamma_-\rangle$. In particular, if we assume (without loss of generality) that $a$ and $c$ are real and non-negative, it requires that $b$ and $d$ have opposite phases. Namely:

$$|\gamma_+\rangle = |a||\gamma_0\rangle + |b|e^{i\phi}|\gamma_1\rangle, \quad |\gamma_-\rangle = |c||\gamma_0\rangle + |d|e^{-i\phi}|\gamma_1\rangle,$$

where $|c|$ and $|d|$ are dictated by $|a|$ and $|b|$, respectively (see Equations (88)–(89)).

The above analysis means that $|\gamma_-\rangle$ faces severe restrictions, and is, in fact, completely determined by the choice of $|\gamma_0\rangle, |\gamma_1\rangle, |\gamma_+\rangle$. From a realistic point of view, this means that a four-state protocol (measured with two bases) could be practically insecure whenever a slight deviation of $|\gamma_-\rangle$ (or of the states $|\gamma_0\rangle, |\gamma_1\rangle, |\gamma_+\rangle$ which determine it) causes the protocol to violate the conditions in Equations (88)–(91). Essentially, this means that in the presence of source imperfections, we require the use of at most three states (or, alternatively, measurement in three or more bases, which we do not explore here), as the use of four states could lead to practical security issues.

6 Conclusion

To sum up, we have found a new way for analyzing the practical security of QKD protocols. Our proof, compared to other proofs, is rigorous, careful, and simple, aiming to make it easy-to-use in the qubit regime (its extension to decoy states is left for future research). We believe our suggested tools can contribute to benchmarking and certifying the security of practical implementations of QKD.

Acknowledgments

The work of G.B. was supported in part by Canada’s Natural Sciences and Engineering Research Council (NSERC), Quèbec’s Institut transdisciplinaire d’information quantique (INTRIQ), and the Canada Research Chair Program. The work of N.G. and S.V. was supported in part by NSERC and INTRIQ. The work of R.L. was supported in part by the Canada Research Chair Program, the Technion’s Helen Diller Quantum Center (Haifa, Israel), the Government of Spain (FIS2020–TRANQI and Severo Ochoa CEX2019–000910–S), Fundació Cellex, Fundació Mir–Puig, Generalitat de Catalunya (CERCA program), and the EU NextGen Funds.

References

[1] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In International Conference on Computers, Systems & Signal Processing, Bangalore, India, 10–12 December 1984, pages 175–179, Dec 1984.

[2] Eli Biham, Bruno Huttner, and Tal Mor. Quantum cryptographic network based on quantum memories. Phys. Rev. A, 54:2651–2658, Oct 1996. doi:10.1103/PhysRevA.54.2651.
[3] Hitoshi Inamori. Security of practical time-reversed EPR quantum key distribution. *Algorithmica*, 34(4):340–365, Nov 2002. doi:10.1007/s00453-002-0983-4.

[4] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, Mar 2012. doi:10.1103/PhysRevLett.108.130503.

[5] Samuel L. Braunstein and Stefano Pirandola. Side-channel-free quantum key distribution. *Phys. Rev. Lett.*, 108:130502, Mar 2012. doi:10.1103/PhysRevLett.108.130502.

[6] Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. In *Proceedings 39th Annual Symposium on Foundations of Computer Science*, pages 503–509, Nov 1998. doi:10.1109/SFCS.1998.743501.

[7] Lluís Masanes, Antonio Acín, and Stefano Pironio. Secure device-independent quantum key distribution with causally independent measurement devices. *Nat. Commun.*, 2(238):1–7, Mar 2011. doi:10.1038/ncomms1244.

[8] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113:140501, Sep 2014. doi:10.1103/PhysRevLett.113.140501.

[9] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. Secure quantum key distribution. *Nat. Photon.*, 8(8):595–604, Jul 2014. doi:10.1038/nphoton.2014.149.

[10] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.*, 92:025002, May 2020. doi:10.1103/RevModPhys.92.025002.

[11] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Adv. Opt. Photonics*, 12(4):1012–1236, Dec 2020. doi:10.1364/AOP.361502.

[12] Kiyoshi Tamaki, Marcos Curty, Go Kato, Hoi-Kwong Lo, and Koji Azuma. Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A*, 90:052314, Nov 2014. doi:10.1103/PhysRevA.90.052314.

[13] Feihu Xu, Kejin Wei, Shihan Sajeeed, Sarah Kaiser, Shihai Sun, Zhiyuan Tang, Li Qian, Vadim Makarov, and Hoi-Kwong Lo. Experimental quantum key distribution with source flaws. *Phys. Rev. A*, 92:032305, Sep 2015. doi:10.1103/PhysRevA.92.032305.

[14] Akihiro Mizutani, Marcos Curty, Charles Ci Wen Lim, Nobuyuki Imoto, and Kiyoshi Tamaki. Finite-key security analysis of quantum key distribution with imperfect light sources. *New J. Phys.*, 17(9):093011, Sep 2015. doi:10.1088/1367-2630/17/9/093011.

[15] Margarida Pereira, Marcos Curty, and Kiyoshi Tamaki. Quantum key distribution with flawed and leaky sources. *npj Quantum Inf.*, 5(1):62, Jul 2019. doi:10.1038/s41534-019-0180-9.
[16] Walter O. Krawec. Asymptotic analysis of a three state quantum cryptographic protocol. In 2016 IEEE International Symposium on Information Theory (ISIT), pages 2489–2493, Jul 2016. doi:10.1109/ISIT.2016.7541747.

[17] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. Phys. Rev. Lett., 91:057901, Aug 2003. doi:10.1103/PhysRevLett.91.057901.

[18] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. Phys. Rev. Lett., 94:230504, Jun 2005. doi:10.1103/PhysRevLett.94.230504.

[19] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. Phys. Rev. Lett., 94:230503, Jun 2005. doi:10.1103/PhysRevLett.94.230503.

[20] Marco Tomamichel and Anthony Leverrier. A largely self-contained and complete security proof for quantum key distribution. Quantum, 1:14, Jul 2017. doi:10.22331/q-2017-07-14-14.

[21] Jun Hasegawa, Masahito Hayashi, Tohya Hiroshima, and Akihisa Tomita. Security analysis of decoy state quantum key distribution incorporating finite statistics. arXiv preprint arXiv:0707.3541, July 2007. URL: https://arxiv.org/abs/0707.3541.

[22] Charles Ci Wen Lim, Marcos Curty, Nino Walenta, Feihu Xu, and Hugo Zbinden. Concise security bounds for practical decoy-state quantum key distribution. Phys. Rev. A, 89:022307, Feb 2014. doi:10.1103/PhysRevA.89.022307.

[23] Artur K. Ekert. Quantum cryptography based on Bell’s theorem. Phys. Rev. Lett., 67:661–663, Aug 1991. doi:10.1103/PhysRevLett.67.661.

[24] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without Bell’s theorem. Phys. Rev. Lett., 68:557–559, Feb 1992. doi:10.1103/PhysRevLett.68.557.

[25] Renato Renner. Security of quantum key distribution. Int. J. Quantum Inf., 6(01):1–127, Feb 2008. doi:10.1142/S0219749908003256.

[26] Marco Tomamichel. A Framework for Non-Asymptotic Quantum Information Theory. PhD thesis, ETH Zurich, Zurich, Switzerland, Mar 2012. URL: https://arxiv.org/abs/1203.2142.

[27] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. Nat. Commun., 3(634):1–6, Jan 2012. doi:10.1038/ncomms1631.

[28] Margarida Pereira, Go Kato, Akihiro Mizutani, Marcos Curty, and Kiyoshi Tamaki. Quantum key distribution with correlated sources. Sci. Adv., 6(37):eaaz4487, Sep 2020. doi:10.1126/sciadv.aaz4487.

[29] Wassily Hoeffding. Probability inequalities for sums of bounded random variables. J. Am. Stat. Assoc., 58(301):13–30, 1963. doi:10.1080/01621459.1963.10500830.