Article

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

Michel Boyer [1], Gilles Brassard [1,2] , Nicolas Godbout [3] , Rotem Liss [1,4,*] and Stéphane Virally [3]

1   Département IRO, Université de Montréal, 2920 Chemin de la Tour, Montréal, QC H3T 1N8, Canada
2   QuSoft, CWI Amsterdam, Science Park 123, 1098 XG Amsterdam, The Netherlands
3   Polytechnique Montréal, Department of Engineering Physics, 2500 Chemin de Polytechnique,
     Montréal, QC H3T 1J4, Canada
4   ICFO—Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, Av. Carl Friedrich
     Gauss 3, 08860 Castelldefels, Barcelona, Spain
*   Correspondence: rotem.liss@icfo.eu

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 lossless regime, and we rigorously prove its unconditional security against any possible attack. We hope our method becomes one of the standard tools used for analysing, benchmarking, and standardizing all practical realizations of QKD.

Keywords: quantum key distribution; practical implementations; security; proof

1. Introduction

The purpose of quantum key distribution (QKD) is to allow 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 theory. 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 models 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 (see, e.g., [2,3]).

Most security weaknesses of the measurement devices can be closed using *measurement-device-independent* (MDI) QKD [4–7]. 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 [8–10], 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 [11–13]; 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 that has no fully available solution is imperfectly generated quantum states.

We suggest a simple and systematic method for analysing source imperfections and proving unconditional security of a large variety of QKD protocols. Our method (similarly to the "loss tolerant" QKD protocol [14–17]) assumes that 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., [18]) for deriving the key rate in the finite-key regime. Our analysis method is vastly simplified and 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 analysing experimental implementations of QKD, and we verify that 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, therefore, lie inside a two-dimensional Hilbert subspace), it does not support losses, and it does not support decoy states [19–21]. We believe that the analysis of losses and decoy states will work within our framework (see, e.g., [22–24]), but we leave their rigorous and precise analysis for future research. We also believe that our analysis can prove security for practical implementations of MDI QKD using the reduction techniques introduced by [4,6], 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 analysed and proved. In Section 3, we fully define the analysed QKD protocol, and in Section 4, we prove its security; our final security result (the key rate) is presented as Corollary 3. In Section 5, we explain why four source states are likely too many (in the qubit and two-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 modelling 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, thereby 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 analyse 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 $\{|\gamma_0\rangle_{B_i}, |\gamma_1\rangle_{B_i}, |\gamma_+\rangle_{B_i}\}$ (identical between all rounds i) that can reside in any arbitrary Hilbert space but must be linearly dependent (and, therefore, must span a two-dimensional Hilbert subspace). Specifically, we denote

     $$|\gamma_+\rangle_{B_i} = a|\gamma_0\rangle_{B_i} + b|\gamma_1\rangle_{B_i}, \tag{1}$$

     where $a, b \in \mathbb{C}$. We require $|a|^2 + |b|^2 > \frac{1}{2}$ or, equivalently, $\Re(a^\star b\langle\gamma_0|\gamma_1\rangle_{B_i}) < \frac{1}{4}$.
   - Bob's generalized measurement operators for each round i:

     (a) $\{M_{B_i}^{Z,t}\}_{t\in\{0,1\}}$, which we name "measurement in the standard basis" or "measurement in the z basis", and

     (b) $\{M_{B_i}^{X,t}\}_{t\in\{0,1\}}$, which we name "measurement in the conjugate basis" or "measurement in the x basis".

     which are defined similarly to [22]. 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 probabilities that Alice chooses each "preparation basis": p_z^A represents the probability that Alice prepares either $|\gamma_0\rangle_{B_i}$ or $|\gamma_1\rangle_{B_i}$ (each of which she chooses with an equal probability, $\frac{p_z^A}{2}$), and p_x^A represents the probability that Alice prepares $|\gamma_+\rangle_{B_i}$. We require $p_z^A + p_x^A = 1$.
   - The probabilities that Bob chooses to measure in each measurement basis: p_z^B (for choosing to measure in the "z basis") and p_x^B (for choosing to measure in the "x basis"), respectively, such that $p_z^B + p_x^B = 1$.
   - 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 δ (maximal allowed noise in TEST-Z-Z and TEST-X-X bits).
   - The zero rate threshold δ_{mismatch} (maximal allowed rate of "+" or "0" results measured by Bob in TEST-Z-X and TEST-X-Z bits, respectively).
   - The error correction and privacy amplification parameters described in [22], including, in particular, the final key length ℓ.

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_z^A or value 1 with probability p_x^A. 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_z^B or value 1 with probability p_x^B.
   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 $|\gamma_+\rangle_{B_i}$ 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 $U \in \{0,1\}^m$, which is kept secret.

4. Bob publicly sends to Alice his basis choice string Φ_B.

5. Alice verifies that the set $\Sigma \triangleq \{1, 2, \ldots, m\}$ 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 verified, Alice sets the flag $F^{\min} = \checkmark$; otherwise, she sets the flag $F^{\min} = \varnothing$ and aborts the protocol.

6. 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 Σ, 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 Σ, 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 Σ, 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 Σ, 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.

7. 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 Π_1 (the TEST-Z-Z rounds) of Alice and Bob, respectively;
- V^2 and W^2 are the substrings corresponding to Π_2 (the TEST-Z-X rounds) of Alice and Bob, respectively;
- V^3 and W^3 are the substrings corresponding to Π_3 (the TEST-X-Z rounds) of Alice and Bob, respectively;
- V^4 and W^4 are the substrings corresponding to Π_4 (the TEST-X-X rounds) of Alice and Bob, respectively;
- X^1 and Y^1 are the substrings corresponding to Σ_1 (the INFO rounds) of Alice and Bob, respectively.

8. 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 δ, Bob sets $F^{pe} = \varnothing$ 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 δ_{mismatch}, Bob sets $F^{pe} = \varnothing$ and aborts the protocol.

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

9. 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 [22]) to obtain their final secret keys. We note that Alice and Bob generate another flag, F^{ec}, and they abort the protocol if $F^{ec} = \varnothing$ (see details in [22]); 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.

We point out that this is a very general protocol in the lossless qubit regime because Alice's emitted states $\{|\gamma_0\rangle_{B_i}, |\gamma_1\rangle_{B_i}, |\gamma_+\rangle_{B_i}\}$ 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 $|\gamma_0\rangle_{B_i}, |\gamma_1\rangle_{B_i}, |\gamma_+\rangle_{B_i}$ to the security proof, as described in Section 2.

Using pure states $|\gamma_0\rangle_{B_i}, |\gamma_1\rangle_{B_i}, |\gamma_+\rangle_{B_i}$ does not hurt generality because if Alice sends a mixed state, we can always assume that 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 [22] 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 that 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 $\{|\gamma_0\rangle_{B_i}, |\gamma_1\rangle_{B_i}, |\gamma_+\rangle_{B_i}\}$ (identical between all rounds *i*) that can reside in any arbitrary Hilbert space but must be linearly dependent (and, therefore, must span a two-dimensional Hilbert subspace). Specifically, we denote

$$|\gamma_+\rangle_{B_i} = a|\gamma_0\rangle_{B_i} + b|\gamma_1\rangle_{B_i}, \tag{2}$$

where $a, b \in \mathbb{C}$. We require $|a|^2 + |b|^2 > \frac{1}{2}$ or, equivalently, $\Re(a^\star b\langle\gamma_0|\gamma_1\rangle_{B_i}) < \frac{1}{4}$. We also denote the following parameter T:

$$T \triangleq |a|^2 + |b|^2 \tag{3}$$

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

$$|\gamma_-\rangle_{B_i} \triangleq \frac{b^\star|\gamma_0\rangle_{B_i} - a^\star|\gamma_1\rangle_{B_i}}{\sqrt{2T - 1}}. \tag{4}$$

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.

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

$$= T + 2\Re(a^\star b \langle \gamma_0 | \gamma_1 \rangle_{B_i}), \tag{5}$$

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

$$= \frac{T - 2\Re(a^\star b \langle \gamma_0 | \gamma_1 \rangle_{B_i})}{2T - 1} = \frac{T - (1 - T)}{2T - 1} = \frac{2T - 1}{2T - 1} = 1 \tag{6}$$

$\square$

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

$$|\xi_+\rangle_{A_i} \triangleq \frac{a^\star |0\rangle_{A_i} + b^\star |1\rangle_{A_i}}{\sqrt{T}}, \tag{7}$$

$$|\xi_-\rangle_{A_i} \triangleq \frac{b|0\rangle_{A_i} - a|1\rangle_{A_i}}{\sqrt{T}}, \tag{8}$$

  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 z 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) $\{M_{B_i}^{Z,t}\}_{t \in \{0,1\}}$, which we name "measurement in the standard basis" or "measurement in the z basis", and
  (b) $\{M_{B_i}^{X,t}\}_{t \in \{0,1\}}$, which we name "measurement in the conjugate basis" or "measurement in the x basis".

  which are defined similarly to [22]. 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: $p_z'^A$ (for choosing to measure in the "z basis") and $p_x'^A$ (for choosing to measure in the "x basis"), respectively, such that $p_z'^A + p_x'^A = 1$.
- The probabilities that Bob chooses to measure in each measurement basis: $p_z'^B$ (for choosing to measure in the "z basis") and $p_x'^B$ (for choosing to measure in the "x basis"), respectively, such that $p_z'^B + p_x'^B = 1$.
- 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 δ (maximal allowed noise in TEST-Z-Z and TEST-X-X bits).
- The zero rate threshold $\delta_{\mathrm{mismatch}}$ (maximal allowed rate of "+" or "0" results measured by Bob in TEST-Z-X and TEST-X-Z bits, respectively).
- The error correction and privacy amplification parameters described in [22], including, in particular, the final key length ℓ.

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 $p_z'^A$ or value 1 with probability $p_x'^A$. 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 $p_z'^B$ or value 1 with probability $p_x'^B$.

Both strings are kept secret.

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

$$|\Psi\rangle_{A_i B_i} \triangleq \frac{|0\rangle_{A_i} |\gamma_0\rangle_{B_i} + |1\rangle_{A_i} |\gamma_1\rangle_{B_i}}{\sqrt{2}} = \frac{|\xi_+\rangle_{A_i} |\gamma_+\rangle_{B_i} + \sqrt{2T-1} |\xi_-\rangle_{A_i} |\gamma_-\rangle_{B_i}}{\sqrt{2T}} \quad (9)$$

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

$$\otimes_{i=1}^{M'} |\Psi\rangle_{A_i B_i} \quad (10)$$

consisting of the M' quantum systems $A_1, A_2, \ldots, A_{M'}$ (one system for each round i). For each round i, if $(\Phi_A)_i = 1$ (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 $(\Phi_A)_i = 0$, she delays measurement to Step 8.) Alice then defines the following bit string $D \in \{0,1\}^{M'}$:

$$D_i \triangleq \begin{cases} 1 & \text{If } (\Phi_A)_i = 1 \text{ and Alice measures "ξ_-" in round } i \\ 0 & \text{Otherwise, (either } (\Phi_A)_i = 0, \text{ or Alice measures "ξ_+" in round } i) \end{cases} \quad (11)$$

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 "ξ_-"; however, if she did not obtain the measurement result "ξ_-", 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 Φ_B.

5. Alice denotes the set of rounds that were not discarded by her as $\Omega \subseteq \{1, 2, \ldots, M'\}$ (namely, $\Omega \triangleq \{1 \le i \le M' \mid D_i = 0\}$). Alice verifies that at least m rounds appear in Ω, 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 Ω (which are the first m non-discarded rounds). Otherwise (if fewer than m rounds appear in Ω), Alice sets the flag $F^{\text{sift}'} = \emptyset$ and aborts the protocol.

    The two next steps are *completely identical* to Steps 5 and 6 of the original prepare-and-measure protocol described in Section 3:

6. Alice verifies that Σ 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 verified, 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 Σ, 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 Σ, 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 Σ, 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 Σ, 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. 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.

9. Bob measures all his non-discarded quantum systems in the bases dictated by Φ_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 7–9):

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 Π_1 (the TEST-Z-Z rounds) of Alice and Bob, respectively;
    - V^2 and W^2 are the substrings corresponding to Π_2 (the TEST-Z-X rounds) of Alice and Bob, respectively;
    - V^3 and W^3 are the substrings corresponding to Π_3 (the TEST-X-Z rounds) of Alice and Bob, respectively;
    - V^4 and W^4 are the substrings corresponding to Π_4 (the TEST-X-X rounds) of Alice and Bob, respectively;
    - X^1 and Y^1 are the substrings corresponding to Σ_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 δ, Bob sets $F^{pe} = \varnothing$ 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 $F^{pe} = \varnothing$ 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 [22]) to obtain their final secret keys. We note that Alice and Bob generate another flag, F^{ec}, and they abort the protocol if $F^{ec} = \varnothing$ (see details in [22]); 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 Section 4.2, we prove security of this protocol, and in Section 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 [22] (which proves security of an entanglement-based version of BB84 [1,25,26]), requiring a few modifications of their proof.

The proof of [22] 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 $H_{min}^\epsilon(A|E)$) and the smooth max-entropy of Alice's data conditioned on Bob's data (denoted $H_{max}^\epsilon(A|B)$). 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 $H_{min}^\epsilon(A|E)$ 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 $H_{max}^\epsilon(A|B)$ describes the number of *extra* information bits that Bob will have to receive 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 [22] shows a lower bound on $H^\epsilon_{\min}(A|E) + H^\epsilon_{\max}(A|B)$. Then, their proof upper-bounds $H^\epsilon_{\max}(A|B)$ 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 δ while the error rate on INFO bits is more than $\delta + \nu$. (Intuitively, the smoothness parameter ϵ means that 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 ϵ from it. In our case, for example, ϵ^2 represents the maximal probability that the law of large numbers is violated—namely, the maximal probability that the true error rate in the INFO bits is much higher 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.) The combination of these two results implies a lower bound on $H^\epsilon_{\min}(A|E)$, and this lower bound immediately gives us the protocol's key rate using the Leftover Hashing Lemma [27] (which intuitively says that roughly $H^\epsilon_{\min}(A|E)$ 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 [22]'s proof: 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 [22]. Therefore, we must prove that it does not hurt security by showing that it keeps Alice's and Bob's basis choice strings Φ_A, Φ_B independent of the other systems.

Each bit of Φ_A, Φ_B is chosen independently (with probabilities p'^A_z, p'^A_x, p'^B_z, and p'^B_x, respectively). Moreover, the state that Alice generates for each round is as follows:

$$|\Psi\rangle_{A_i B_i} \triangleq \frac{|0\rangle_{A_i}|\gamma_0\rangle_{B_i} + |1\rangle_{A_i}|\gamma_1\rangle_{B_i}}{\sqrt{2}} = \frac{|\xi_+\rangle_{A_i}|\gamma_+\rangle_{B_i} + \sqrt{2T-1}|\xi_-\rangle_{A_i}|\gamma_-\rangle_{B_i}}{\sqrt{2T}}, \quad (12)$$

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 "ξ_+" result with conditional probability $\frac{1}{2T}$ and obtains the "ξ_-" result with conditional probability $\frac{2T-1}{2T}$. We conclude the following:

$$\mathrm{Pr}_{A_i}(0) = \mathrm{Pr}_{A_i}(1) \quad = \quad p'^A_z \cdot \frac{1}{2} = \frac{p'^A_z}{2}, \quad (13)$$

$$\mathrm{Pr}_{A_i}(\xi_+) \quad = \quad p'^A_x \cdot \frac{1}{2T} = \frac{p'^A_x}{2T}, \quad (14)$$

$$\mathrm{Pr}_{A_i}(\xi_-) \quad = \quad p'^A_x \cdot \frac{2T-1}{2T} = \frac{p'^A_x(2T-1)}{2T}. \quad (15)$$

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 "ξ_-"; therefore,

$$\mathrm{Pr}_{A_i}(D_i = 1) \quad = \quad \mathrm{Pr}_{A_i}(\xi_-) = \frac{p'^A_x(2T-1)}{2T}, \quad (16)$$

$$\mathrm{Pr}_{A_i}(D_i = 0) \quad = \quad \mathrm{Pr}_{A_i}(0) + \mathrm{Pr}_{A_i}(1) + \mathrm{Pr}_{A_i}(\xi_+) = 2 \cdot \frac{p'^A_z}{2} + \frac{p'^A_x}{2T} = p'^A_z + \frac{p'^A_x}{2T}. \quad (17)$$

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 Ω (each non-discarded round), Alice determines the basis:

$$\Pr_{A_i}[(\Phi_A)_i = 0 \mid D_i = 0] \;=\; \frac{\Pr_{A_i}(0) + \Pr_{A_i}(1)}{\Pr_{A_i}(D_i = 0)} = \frac{2 \cdot \frac{p_z'^A}{2}}{p_z'^A + \frac{p_x'^A}{2T}} = \frac{p_z'^A}{p_z'^A + \frac{p_x'^A}{2T}}, \quad (18)$$

$$\Pr_{A_i}[(\Phi_A)_i = 1 \mid D_i = 0] \;=\; \frac{\Pr_{A_i}(\xi_+)}{\Pr_{A_i}(D_i = 0)} = \frac{\frac{p_x'^A}{2T}}{p_z'^A + \frac{p_x'^A}{2T}}. \quad (19)$$

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 Φ_A and R. (This point can be counter-intuitive: from a quantum theory's point of view, the choice of discarded and non-discarded rounds obviously depends on the basis chosen for measurement, yet from a 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 $F^{\mathrm{sift}'}$ (which notes whether there are at least m rounds in Ω—namely, whether at least m rounds were not discarded) and the set Σ (which represents the first m rounds in Ω) *only* depend on stage 1: namely, from the probabilistic point of view, both the passing of the sifting test ($F^{\mathrm{sift}'}$) and the choice of the m relevant rounds (Σ) depend only on the choice of discarded rounds in stage 1, and they are both completely independent of the bases Φ_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 (18) and (19).

For this reason, in the rest of the analysis, we can treat Φ_A and Φ_B (more precisely, their restrictions to the m non-discarded rounds in Σ) as *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 law of large numbers to hypothetical protocols in Section 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 Σ:

1. In stage 2 (included in Step 2 of the protocol), Alice and Bob determine the bases of the m non-discarded rounds in Σ, chosen randomly and independently for each round in Σ.
2. In Step 6 of the protocol, Alice verifies that Σ 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 passing this verification—namely, we evaluate the conditional probabilities on $F^{\min} = \checkmark$.
3. In Step 7 of the protocol, Alice uniformly and randomly chooses the corresponding disjoint subsets $\Sigma_1, \Pi_1 \subseteq \Sigma_{Z,Z}$, $\Pi_2 \subseteq \Sigma_{Z,X}$, $\Pi_3 \subseteq \Sigma_{X,Z}$, and $\Pi_4 \subseteq \Sigma_{X,X}$ (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 $F^{\min} = \checkmark$ (namely, conditioning on passing the verification of the second step), 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 Σ),

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 inside Σ. This observation, too, is crucial for the application of the law of large numbers in Section 4.2.3.

4.2.2. Entropic Uncertainty Relation

The security proof in [22] uses the uncertainty relation described in Proposition 4 of [22], which is equivalent to Corollary 7.4 of [28]. This uncertainty relation uses the symmetry of the BB84 protocol with respect to the chosen basis of the INFO bits: namely, it uses the property that each INFO bit in BB84 is measured in a uniformly random basis, 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 the "z basis"), we must use a different uncertainty relation.

Adopting an approach similar to [29], we use Theorem 7.2 of [28] as the generalized entropic uncertainty relation (using slightly different notations compared to [28]):

Theorem 1. *(Theorem 7.2 of [28]) Given $\epsilon \geq 0$ and a non-normalized state ρ_{ARS} over the Hilbert space $\mathcal{H}_{\mathrm{ARS}}$, and given two generalized measurement operators $M_1 = \{M_1^x\}_x$, $M_2 = \{M_2^{x'}\}_{x'}$ on $\mathcal{H}_\mathrm{A}$ and a projective measurement $\{P^p\}_p$ on $\mathcal{H}_\mathrm{A}$, the two post-measurement states*

$$\sigma_{\mathrm{XPR}} = \sum_{x,p} |x\rangle_\mathrm{X}\langle x|_\mathrm{X} \otimes |p\rangle_\mathrm{P}\langle p|_\mathrm{P} \otimes \mathrm{tr}_{\mathrm{AS}}\left(M_1^x P^p \rho_{\mathrm{ARS}} P^p (M_1^x)^\dagger\right), \tag{20}$$

$$\sigma'_{\mathrm{X'PS}} = \sum_{x',p} |x'\rangle_{\mathrm{X'}}\langle x'|_{\mathrm{X'}} \otimes |p\rangle_\mathrm{P}\langle p|_\mathrm{P} \otimes \mathrm{tr}_{\mathrm{AR}}\left(M_2^{x'} P^p \rho_{\mathrm{ARS}} P^p (M_2^{x'})^\dagger\right) \tag{21}$$

satisfy the following inequality (uncertainty relation):

$$H_{\min}^\epsilon(\mathrm{X|PR})_\sigma + H_{\max}^\epsilon(\mathrm{X'|PS})_{\sigma'} \geq \log_2\left(\frac{1}{c_\mathrm{P}}\right), \tag{22}$$

where:

$$c_\mathrm{P} \triangleq \max_{p,x,x'}\left|\left|M_1^x P^p (M_2^{x'})^\dagger\right|\right|_\infty^2. \tag{23}$$

Proof. Proved in Section 7.3.2 of [28] as Theorem 7.2. $\square$

The next proposition will give us a similar result to Corollary 5 of [22] (namely, roughly speaking, a lower bound on the sum $H_{\min}^\epsilon(\mathrm{A|E}) + H_{\max}^\epsilon(\mathrm{A|B})$), with one important difference: the first term $H_{\min}^\epsilon(\mathrm{A|E})$ will still refer to the real QKD protocol (the modified entanglement-based protocol described in Section 4.1), but the second term $H_{\max}^\epsilon(\mathrm{A|B})$ will now refer to a hypothetical QKD protocol (still entanglement-based) where both Alice and Bob measure the INFO bits in the conjugate ("x") basis. Formally:

Proposition 1. *For the modified entanglement-based protocol described in Section 4.1, for $\epsilon \geq 0$, the state $\sigma_{\mathrm{X^1 Y^1 VW\Pi\Phi_A\Phi_B F^{sift'} F^{min} F^{pe} E}}$ held by Alice, Bob, and Eve after Step 11 of the real protocol, and the state $\sigma'_{\mathrm{X'^1 Y'^1 VW\Pi\Phi_A\Phi_B F^{sift'} F^{min} F^{pe} E}}$ held by Alice, Bob, and Eve after Step 11 of the hypothetical protocol defined below, it holds that*

$$H_{\min}^\epsilon(\mathrm{X^1 \wedge F^{pe}} = \checkmark|\mathrm{VW\Pi\Phi_A\Phi_B E} , \mathrm{F^{sift'}} = \mathrm{F^{min}} = \checkmark)_\sigma$$

$$+ \quad H_{\max}^\epsilon(\mathrm{X'^1 \wedge F^{pe}} = \checkmark|\mathrm{Y'^1} , \mathrm{F^{sift'}} = \mathrm{F^{min}} = \checkmark)_{\sigma'} \geq n_1 \log_2\left(\frac{1}{c}\right), \tag{24}$$

where we define $\mathrm{V} \triangleq (V^1, V^2, V^3, V^4)$, $\mathrm{W} \triangleq (W^1, W^2, W^3, W^4)$, $\Pi \triangleq (\Pi_1, \Pi_2, \Pi_3, \Pi_4, \Sigma_1, D, \Sigma)$, *and* $c \triangleq \max\left(|\langle 0|\xi_+\rangle_{\mathrm{A}_i}|^2, |\langle 0|\xi_-\rangle_{\mathrm{A}_i}|^2, |\langle 1|\xi_+\rangle_{\mathrm{A}_i}|^2, |\langle 1|\xi_-\rangle_{\mathrm{A}_i}|^2\right)$, *using the protocol's notations;*

subsystem E *represents Eve's ancilla (including her quantum data); and* X'^1, Y'^1 *are the substrings corresponding to the n_1 INFO rounds (namely, the Z-Z rounds in Σ_1) in the hypothetical protocol where both Alice and Bob measure the INFO bits in the conjugate ("x") basis.*

(The hypothetical protocol only changes the actual measurements performed by Alice and Bob in Steps 8 and 9 of the modified entanglement-based protocol. It does not change any other part of the protocol: in particular, Alice neither discards INFO rounds where she measured "ξ_-" in the hypothetical protocol nor notifies Bob about them.)

Proof. This proof combines modified versions of the proofs of Corollary 7.4 in Section 7.4.2 of [28] and Corollary 5 in Section 6.2 of [22].

We choose the measurement operators $M_1 = \{|j\rangle_A \langle j|_A \mid j \in \{0,1\}^{n_1}\}$ (i.e., the tensor product of n_1 copies of the "z basis") and $M_2 = \{|j\rangle_A \langle j|_A \mid j \in \{\xi_+, \xi_-\}^{n_1}\}$ (i.e., the tensor product of n_1 copies of the "x basis") and the projective measurement $\{P^p\}_p = \{|\Pi\Phi_A\Phi_B\rangle\langle\Pi\Phi_A\Phi_B|\}_{\Pi\Phi_A\Phi_B}$. It is easy to verify (see, e.g., [28]) that c_P of Theorem 1 is equal to c^{n_1}, where c was defined in our proposition ($c \triangleq \max(|\langle 0|\xi_+\rangle_{A_i}|^2, |\langle 0|\xi_-\rangle_{A_i}|^2, |\langle 1|\xi_+\rangle_{A_i}|^2, |\langle 1|\xi_-\rangle_{A_i}|^2)$).

Then, we apply Theorem 1 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 to its Step 8 all Alice's measurements in the "z basis", which include all measurements of the INFO bits), *conditioned* on the first two tests passing ($F^{sift'} = F^{min} = \checkmark$), and *requiring* the third test to pass ($F^{pe} = \checkmark$): (the difference between "conditioning" and "requiring" in this context is analogous to the difference between a "conditional probability" and a "joint probability", respectively; see [22] for the precise definitions)

$$\rho_{ABVW\Pi\Phi_A\Phi_B F^{sift'} F^{min} F^{pe} E \wedge F^{pe} = \checkmark \mid F^{sift'} = F^{min} = \checkmark}, \tag{25}$$

and by choosing the systems $P = \Pi\Phi_A\Phi_B$, $R = VWE$, $S = B$ for Theorem 1, we obtain the following:

$$H_{min}^\epsilon(X^1 \wedge F^{pe} = \checkmark \mid VWE\Pi\Phi_A\Phi_B, F^{sift'} = F^{min} = \checkmark)_\sigma$$
$$+ \quad H_{max}^\epsilon(X'^1 \wedge F^{pe} = \checkmark \mid B\Pi\Phi_A\Phi_B, F^{sift'} = F^{min} = \checkmark)_{\sigma'} \geq n_1 \log_2\left(\frac{1}{c}\right), \tag{26}$$

where X^1 and X'^1 represent the measurement results of Alice's 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 $B\Pi\Phi_A\Phi_B$. According to the data processing inequality (see, e.g., [22,27]), such operations can only increase the max-entropy:

$$H_{max}^\epsilon(X'^1 \wedge F^{pe} = \checkmark \mid B\Pi\Phi_A\Phi_B, F^{sift'} = F^{min} = \checkmark)_{\sigma'} \leq H_{max}^\epsilon(X'^1 \wedge F^{pe} = \checkmark \mid Y'^1, F^{sift'} = F^{min} = \checkmark)_{\sigma'}, \tag{27}$$

which gives us the desired result:

$$H_{min}^\epsilon(X^1 \wedge F^{pe} = \checkmark \mid VWE\Pi\Phi_A\Phi_B, F^{sift'} = F^{min} = \checkmark)_\sigma$$
$$+ \quad H_{max}^\epsilon(X'^1 \wedge F^{pe} = \checkmark \mid Y'^1, F^{sift'} = F^{min} = \checkmark)_{\sigma'} \geq n_1 \log_2\left(\frac{1}{c}\right). \tag{28}$$

$\square$

4.2.3. The Law of Large Numbers

Intuitively, the proof of [22] uses a law of large numbers (Lemma 6 of [22]) to upper-bound the max-entropy $H_{max}^\epsilon(X|Y)$—namely, the max-entropy of Alice's raw key condi-

tioned on Bob's raw key in the *real* protocol. However, in our proof, we need to bound $H_{\max}^\epsilon(X'^1|Y'^1)$—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 "ξ_+") to the INFO bits. This way, we can discover the error rate on the "ξ_+" bits.

2. For finding the error rate on the "ξ_-" 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:

$$\Pr(A_i = - \, , \, B_i = +) \ = \ \Pr(A_i = 0 \, , \, B_i = +) + \Pr(A_i = 1 \, , \, B_i = +) - \Pr(A_i = + \, , \, B_i = +). \quad (29)$$

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

$$\begin{aligned} \Pr(A_i = - \, , \, B_i = +) + \Pr(A_i = + \, , \, B_i = +) \ &= \ \Pr(B_i = +) \\ = \ \Pr(A_i = 0 \, , \, B_i = +) &+ \Pr(A_i = 1 \, , \, B_i = +). \end{aligned} \quad (30)$$

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 2 below.

This idea can be compared with [30]'s analysis of the "loss tolerant" protocol (improving on the usual analysis which involves matrix computations [14–17]), but their 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 [22]):

Lemma 2. *(Lemma 6 of [22]) 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, *a uniformly distributed subset $\Pi \subseteq \{1, 2, \ldots, N\}$ of size a, it holds that*

$$\Pr\left[\sum_{i \in \Pi} Z_i \leq a\delta \ \wedge \ \sum_{i \in \overline{\Pi}} Z_i \geq b \cdot (\delta + \nu)\right] \leq e^{-\frac{2ba^2\nu^2}{(a+b)(a+1)}}. \quad (31)$$

Proof. Proved in Section 6.3 of [22] as Lemma 6. □

We also use another law of large numbers, proved in Section 2 of [31] as Theorem 1:

Lemma 3. *Let $Z_1, \ldots, Z_N$ be independent random variables with finite first and second moments, such that $0 \leq Z_i \leq 1$ for all $1 \leq i \leq N$. If $\overline{Z} \triangleq \frac{Z_1 + \ldots + Z_N}{N}$ is their average and $\mu \triangleq E[\overline{Z}]$ is the expected value of $\overline{Z}$, then for any $\nu > 0$,*

$$\Pr\left[\overline{Z} - \mu \geq \nu\right] \leq e^{-2N\nu^2}. \quad (32)$$

Using these Lemmas, we prove the following (a modified version of Proposition 8 of [22]):

Proposition 2. *For the modified entanglement-based protocol described in Section 4.1, for the state $\sigma'_{X'^1 Y'^1 V W \Pi \Phi_A \Phi_B F^{sift'} F^{min} F^{pe} E}$ defined in Proposition 1, and for error rate threshold δ and zero rate threshold δ_{mismatch}, if we define for any $0 < \nu \leq \frac{1}{2} - \delta$:*

$$\delta'(\nu) \ \triangleq \ \delta_{\text{mismatch}} + \nu - \left(\frac{1}{2T} - \nu\right) \cdot (1 - 2\delta - 2\nu), \quad (33)$$

$$\epsilon(\nu) \triangleq \sqrt{e^{-2n_1\nu^2} + e^{-\frac{2n_1\cdot\left(\frac{1}{2T}-\nu\right)k_4^2\nu^2}{\left(k_4+n_1\cdot\left(\frac{1}{2T}-\nu\right)\right)(k_4+1)}} + e^{-\frac{2n_1k_2^2\nu^2}{(k_2+n_1)(k_2+1)}}}, \tag{34}$$

then, for any $0 < \nu \le \frac{1}{2} - \delta$ *satisfying* $0 < \delta'(\nu) \le \frac{1}{2}$ *and* $\epsilon(\nu)^2 < \Pr\left[F^{\mathrm{pe}} = \checkmark \mid F^{\mathrm{sift}'} = F^{\min} = \checkmark\right]$, *it holds that*

$$H_{\max}^{\epsilon(\nu)}(X'^1 \wedge F^{\mathrm{pe}} = \checkmark \mid Y'^1, F^{\mathrm{sift}'} = F^{\min} = \checkmark)_{\sigma'} \le n_1 \cdot h_2(\delta'(\nu)), \tag{35}$$

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

Proof. Let us define the following event:

$$\Omega_0 \triangleq 1\left\{\sum_{i=1}^{n_1} 1\{X_i'^1 \ne Y_i'^1\} > n_1\delta'(\nu)\right\}. \tag{36}$$

We need to prove the following probability to be exponentially small:

$$\begin{aligned}
&\Pr\left[F^{\mathrm{pe}} = \checkmark \wedge \Omega_0 \mid F^{\mathrm{sift}'} = F^{\min} = \checkmark\right] \\
&= \Pr\Bigg[\sum_{i=1}^{k_1} 1\{V_i^1 \ne W_i^1\} \le k_1\delta \wedge \sum_{i=1}^{k_2} 1\{W_i^2 = 0\} \le k_2\delta_{\mathrm{mismatch}} \\
&\quad \wedge \sum_{i=1}^{k_3} 1\{W_i^3 = 0\} \le k_3\delta_{\mathrm{mismatch}} \wedge \sum_{i=1}^{k_4} 1\{V_i^4 \ne W_i^4\} \le k_4\delta \\
&\quad \wedge \sum_{i=1}^{n_1} 1\{X_i'^1 \ne Y_i'^1\} > n_1\delta'(\nu) \mid F^{\mathrm{sift}'} = F^{\min} = \checkmark\Bigg] \\
&\le \Pr\Bigg[\sum_{i=1}^{k_2} 1\{W_i^2 = 0\} \le k_2\delta_{\mathrm{mismatch}} \wedge \sum_{i=1}^{k_4} 1\{V_i^4 \ne W_i^4\} \le k_4\delta \\
&\quad \wedge \sum_{i=1}^{n_1} 1\{X_i'^1 \ne Y_i'^1\} > n_1\delta'(\nu) \mid F^{\mathrm{sift}'} = F^{\min} = \checkmark\Bigg]. \tag{37}
\end{aligned}$$

Let us remember that V^2 and W^2 are Alice's and Bob's substrings corresponding to Π_2 (the k_2 TEST-Z-X rounds); V^4 and W^4 are Alice's and Bob's substrings corresponding to Π_4 (the k_4 TEST-X-X rounds); and X'^1 and Y'^1 are Alice's and Bob's substrings corresponding to Σ_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" in Steps 8 and 9 of the protocol, respectively.*

Let us also denote Alice's "ξ_+ rate" (the percentage of INFO bits which Alice measures as "ξ_+") in the X-X hypothetical protocol by R'_+—namely, $R'_+ \triangleq \frac{1}{n_1}\sum_{i=1}^{n_1} 1\{X_i'^1 = 0\}$. Thus, the probability $\Pr\left[F^{\mathrm{pe}} = \checkmark \wedge \Omega_0 \mid F^{\mathrm{sift}'} = F^{\min} = \checkmark\right]$ is bounded by the sum of four probabilities:

$$\Pr\left[F^{\text{pe}} = \checkmark \,\wedge\, \Omega_0 \mid F^{\text{sift}'} = F^{\min} = \checkmark\right]$$

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

$$+ \Pr\left[R'_+ \geq \frac{1}{2T} - \nu \,\wedge\, \sum_{i=1}^{k_4} 1\{V_i^4 \neq W_i^4\} \leq k_4\delta\right.$$

$$\wedge \,\, \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \,\wedge\, Y_i'^1 = 1\} \geq n_1 R'_+ \cdot (\delta + \nu) \mid F^{\text{sift}'} = F^{\min} = \checkmark\right]$$

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

$$+ \Pr\left[R'_+ \geq \frac{1}{2T} - \nu \,\wedge\, \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \,\wedge\, Y_i'^1 = 1\} \leq n_1 R'_+ \cdot (\delta + \nu)\right.$$

$$\wedge \,\, \sum_{i=1}^{n_1} 1\{Y_i'^1 = 0\} \leq n_1 \cdot (\delta_{\text{mismatch}} + \nu) \,\wedge\, \sum_{i=1}^{n_1} 1\{X_i'^1 \neq Y_i'^1\} > n_1\delta'(\nu) \mid F^{\text{sift}'} = F^{\min} = \checkmark\right]. \quad (38)$$

We now bound each of these four probabilities:

Bounding the first probability:

We need to bound

$$\Pr\left[R'_+ \leq \frac{1}{2T} - \nu \mid F^{\text{sift}'} = F^{\min} = \checkmark\right], \quad (39)$$

where R'_+ is the "ξ_+" 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 "ξ_+" is always $\frac{1}{2T}$. Namely, Alice's measurement results are n_1 independent random variables $\{Z_i\}_{i=1}^{n_1}$ (with all probabilities conditioned on $F^{\text{sift}'} = F^{\min} = \checkmark$) such that for each i:

$$\Pr(Z_i = 0 \mid F^{\text{sift}'} = F^{\min} = \checkmark) = \frac{1}{2T} \quad, \quad \Pr(Z_i = 1 \mid F^{\text{sift}'} = F^{\min} = \checkmark) = 1 - \frac{1}{2T} \quad. \quad (40)$$

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

We can thus apply Lemma 3 (which applies to N independent random variables) to the random variables $\{Z_i\}_{i=1}^{n_1}$ with parameters $N = n_1$ and $\mu = E[\overline{Z}] = 1 - \frac{1}{2T}$. We note that $\overline{Z} = 1 - R'_+$. Therefore, we obtain the following result:

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

$$= \Pr\left[\frac{1}{2T} - R'_+ \geq \nu \mid F^{\text{sift}'} = F^{\min} = \checkmark\right]$$

$$= \Pr\left[(1 - R'_+) - \left(1 - \frac{1}{2T}\right) \geq \nu \mid F^{\text{sift}'} = F^{\min} = \checkmark\right]$$

$$= \Pr\left[\overline{Z} - \mu \geq \nu \mid F^{\text{sift}'} = F^{\min} = \checkmark\right] \leq e^{-2n_1\nu^2}. \quad (41)$$

Bounding the second probability:

We need to bound

$$\Pr\left[R'_+ \geq \frac{1}{2T} - \nu \ \wedge \ \sum_{i=1}^{k_4} 1\{V_i^4 \neq W_i^4\} \leq k_4 \delta \right.$$
$$\left. \wedge \ \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \wedge Y_i'^1 = 1\} \geq n_1 R'_+ \cdot (\delta + \nu) \ | \ F^{\text{sift}'} = F^{\min} = \checkmark \right], \quad (42)$$

where V^4 and W^4 are Alice's and Bob's substrings corresponding to Π_4 (the k_4 TEST-X-X rounds); X'^1 and Y'^1 are Alice's and Bob's substrings corresponding to Σ_1 (the n_1 INFO rounds) in the X-X hypothetical protocol; and R'_+ is the "ξ_+" measurement rate of Alice among the INFO bits in the X-X hypothetical protocol. We notice that the TEST-X-X rounds in Π_4 consist *only* of rounds where Alice measured "ξ_+" (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

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

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 obtains the "ξ_+" result. We thus notice that the quantum behaviour 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 between the rounds, this timing is meaningless from the quantum point of view).

Therefore, we can apply Lemma 2 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 $X_i'^1 = 0 \wedge Y_i'^1 = 1$, respectively); the sampled subset Π includes the $a = k_4$ TEST-X-X rounds in the Π_4 subset chosen by the protocol, and the rest $\overline{\Pi}$ includes the $b = n_1 R'_+$ INFO rounds in the Σ_1 subset chosen by the protocol where Alice obtains the "ξ_+" measurement result. The sampled susbet Π 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 Section 4.2.1 that Σ_1 and Π_4 can be seen as uniformly and randomly chosen subsets of Σ, conditioning on $F^{\text{sift}'} = F^{\min} = \checkmark$.

We remark that this is not a straightforward application of Lemma 2 because the number $b = n_1 R'_+$ of rounds in $\overline{\Pi}$ 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 2 for any possible value of R'_+, we are able to bound this probability and prove it exponentially small.

Using the formulation of Lemma 2, we obtain

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

$$\wedge \quad \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \ \wedge \ Y_i'^1 = 1\} \ge n_1 R_+' \cdot (\delta + \nu) \ \mid \ F^{\text{sift}'} = F^{\min} = \checkmark \Big]$$

$$= \sum_{j = \lceil n_1 \cdot \left(\frac{1}{2T} - \nu\right) \rceil}^{n_1} \Pr \Big[R_+' = \frac{j}{n_1} \ \wedge \ \sum_{i=1}^{k_4} 1\{V_i^4 = 0 \ \wedge \ W_i^4 = 1\} \le k_4 \delta$$

$$\wedge \quad \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \ \wedge \ Y_i'^1 = 1\} \ge n_1 R_+' \cdot (\delta + \nu) \ \mid \ F^{\text{sift}'} = F^{\min} = \checkmark \Big]$$

$$= \sum_{j = \lceil n_1 \cdot \left(\frac{1}{2T} - \nu\right) \rceil}^{n_1} \Pr \Big[R_+' = \frac{j}{n_1} \ \mid \ F^{\text{sift}'} = F^{\min} = \checkmark \Big] \cdot \Pr \Big[\sum_{i=1}^{k_4} 1\{V_i^4 = 0 \ \wedge \ W_i^4 = 1\} \le k_4 \delta$$

$$\wedge \quad \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \ \wedge \ Y_i'^1 = 1\} \ge n_1 R_+' \cdot (\delta + \nu) \ \mid \ R_+' = \frac{j}{n_1} \ , \ F^{\text{sift}'} = F^{\min} = \checkmark \Big]. \tag{44}$$

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

$$\Pr \Big[\sum_{i=1}^{k_4} 1\{V_i^4 = 0 \ \wedge \ W_i^4 = 1\} \le k_4 \delta$$

$$\wedge \quad \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \ \wedge \ Y_i'^1 = 1\} \ge n_1 R_+' \cdot (\delta + \nu) \ \mid \ R_+' = \frac{j}{n_1} \ , \ F^{\text{sift}'} = F^{\min} = \checkmark \Big]$$

$$= \Pr \Big[\sum_{i=1}^{k_4} 1\{V_i^4 = 0 \ \wedge \ W_i^4 = 1\} \le k_4 \delta$$

$$\wedge \quad \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \ \wedge \ Y_i'^1 = 1\} \ge j \cdot (\delta + \nu) \ \mid \ R_+' = \frac{j}{n_1} \ , \ F^{\text{sift}'} = F^{\min} = \checkmark \Big]$$

$$= \Pr \Big[\sum_{i \in \Pi} Z_i \le k_4 \delta \ \wedge \ \sum_{i \in \overline{\Pi}} Z_i \ge j \cdot (\delta + \nu) \ \mid \ R_+' = \frac{j}{n_1} \ , \ F^{\text{sift}'} = F^{\min} = \checkmark \Big]$$

$$\le \ e^{- \frac{2j k_4^2 \nu^2}{(k_4 + j)(k_4 + 1)}} \le e^{- \frac{2 n_1 \cdot \left(\frac{1}{2T} - \nu\right) k_4^2 \nu^2}{\left(k_4 + n_1 \cdot \left(\frac{1}{2T} - \nu\right)\right)(k_4 + 1)}} , \tag{45}$$

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

Substituting Equation (45) into Equation (44), we have

$$\Pr \Big[R_+' \ge \frac{1}{2T} - \nu \ \wedge \ \sum_{i=1}^{k_4} 1\{V_i^4 \ne W_i^4\} \le k_4 \delta$$

$$\wedge \quad \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \ \wedge \ Y_i'^1 = 1\} \ge n_1 R_+' \cdot (\delta + \nu) \ \mid \ F^{\text{sift}'} = F^{\min} = \checkmark \Big]$$

$$= \sum_{j = \lceil n_1 \cdot \left(\frac{1}{2T} - \nu\right) \rceil}^{n_1} \Pr \Big[R_+' = \frac{j}{n_1} \ \mid \ F^{\text{sift}'} = F^{\min} = \checkmark \Big] \cdot \Pr \Big[\sum_{i=1}^{k_4} 1\{V_i^4 = 0 \ \wedge \ W_i^4 = 1\} \le k_4 \delta$$

$$\wedge \quad \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \ \wedge \ Y_i'^1 = 1\} \ge n_1 R_+' \cdot (\delta + \nu) \ \mid \ R_+' = \frac{j}{n_1} \ , \ F^{\text{sift}'} = F^{\min} = \checkmark \Big]$$

$$\le \sum_{j = \lceil n_1 \cdot \left(\frac{1}{2T} - \nu\right) \rceil}^{n_1} \Pr \Big[R_+' = \frac{j}{n_1} \ \mid \ F^{\text{sift}'} = F^{\min} = \checkmark \Big] \cdot e^{- \frac{2 n_1 \cdot \left(\frac{1}{2T} - \nu\right) k_4^2 \nu^2}{\left(k_4 + n_1 \cdot \left(\frac{1}{2T} - \nu\right)\right)(k_4 + 1)}}$$

$$\leq \quad e^{-\dfrac{2n_1 \cdot \left(\frac{1}{2T} - v\right) k_4^2 v^2}{\left(k_4 + n_1 \cdot \left(\frac{1}{2T} - v\right)\right)(k_4 + 1)}}. \tag{46}$$

Bounding the third probability:

We need to bound

$$\Pr\left[\sum_{i=1}^{k_2} 1\{W_i^2 = 0\} \leq k_2 \delta_{\text{mismatch}} \ \wedge \ \sum_{i=1}^{n_1} 1\{Y_i'^1 = 0\} \geq n_1 \cdot (\delta_{\text{mismatch}} + v) \ \mid \ F^{\text{sift}'} = F^{\min} = \checkmark\right], \tag{47}$$

where W^2 is Bob's substring corresponding to Π_2 (the k_2 TEST-Z-X rounds) and Y'^1 is Bob's substring corresponding to Σ_1 (the n_1 INFO rounds) in the X-X hypothetical protocol. Let us now define X''^1 and Y''^1 as Alice's and Bob's substrings corresponding to Σ_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'^1 is completely identical to Y''^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, $Y'^1 = Y''^1$, and the probability is

$$= \Pr\left[\sum_{i=1}^{k_2} 1\{W_i^2 = 0\} \leq k_2 \delta_{\text{mismatch}} \ \wedge \ \sum_{i=1}^{n_1} 1\{Y_i''^1 = 0\} \geq n_1 \cdot (\delta_{\text{mismatch}} + v) \ \mid \ F^{\text{sift}'} = F^{\min} = \checkmark\right]. \tag{48}$$

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 behaviour of Alice, Bob, and Eve is *identical* on all these rounds in the Z-X hypothetical protocol.

Therefore, we can apply Lemma 2 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 $1 - Y_i''^1$, respectively); the sampled subset Π includes the $a = k_2$ TEST-Z-X rounds in the Π_2 subset chosen by the protocol, and the rest $\overline{\Pi}$ includes the $b = n_1$ INFO rounds in the Σ_1 subset chosen by the protocol (note that Bob measures them in the "x basis"). The sampled susbet Π 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 Section 4.2.1 that Σ_1 and Π_2 can be seen as uniformly and randomly chosen subsets of Σ, conditioning on $F^{\text{sift}'} = F^{\min} = \checkmark$. Using the formulation of Lemma 2, we obtain the following:

$$\Pr\left[\sum_{i=1}^{k_2} 1\{W_i^2 = 0\} \leq k_2 \delta_{\text{mismatch}} \ \wedge \ \sum_{i=1}^{n_1} 1\{Y_i'^1 = 0\} \geq n_1 \cdot (\delta_{\text{mismatch}} + v) \ \mid \ F^{\text{sift}'} = F^{\min} = \checkmark\right]$$

$$= \ \Pr\left[\sum_{i=1}^{k_2} 1\{W_i^2 = 0\} \leq k_2 \delta_{\text{mismatch}} \ \wedge \ \sum_{i=1}^{n_1} 1\{Y_i''^1 = 0\} \geq n_1 \cdot (\delta_{\text{mismatch}} + v) \ \mid \ F^{\text{sift}'} = F^{\min} = \checkmark\right]$$

$$= \ \Pr\left[\sum_{i \in \Pi} Z_i \leq k_2 \delta_{\text{mismatch}} \ \wedge \ \sum_{i \in \overline{\Pi}} Z_i \geq n_1 \cdot (\delta_{\text{mismatch}} + v) \ \mid \ F^{\text{sift}'} = F^{\min} = \checkmark\right]$$

$$\leq \ e^{-\dfrac{2n_1 k_2^2 v^2}{(k_2 + n_1)(k_2 + 1)}}. \tag{49}$$

Bounding the fourth probability:

We need to bound

$$\Pr\left[R'_+ \geq \frac{1}{2T} - v \ \wedge \ \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \ \wedge \ Y_i'^1 = 1\} \leq n_1 R'_+ \cdot (\delta + v)\right.$$

$$\wedge \ \sum_{i=1}^{n_1} 1\{Y_i'^1 = 0\} \le n_1 \cdot (\delta_{\text{mismatch}} + \nu) \ \wedge \ \sum_{i=1}^{n_1} 1\{X_i'^1 \ne Y_i'^1\} > n_1 \delta'(\nu) \ | \ F^{\text{sift}'} = F^{\min} = \checkmark \bigg], \tag{50}$$

where X'^1 and Y'^1 are Alice's and Bob's substrings corresponding to Σ_1 (the n_1 INFO rounds) in the X-X hypothetical protocol, and R'_+ is the "ξ_+" measurement rate of Alice among the INFO bits in the X-X hypothetical protocol. We prove this probability to be *zero*; namely, we prove that these four conditions contradict each other and cannot be all true.

Indeed, assume by contradiction that all four conditions hold:

$$R'_+ \ge \frac{1}{2T} - \nu \ \wedge \ \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \ \wedge \ Y_i'^1 = 1\} \le n_1 R'_+ \cdot (\delta + \nu)$$

$$\wedge \ \sum_{i=1}^{n_1} 1\{Y_i'^1 = 0\} \le n_1 \cdot (\delta_{\text{mismatch}} + \nu) \ \wedge \ \sum_{i=1}^{n_1} 1\{X_i'^1 \ne Y_i'^1\} > n_1 \delta'(\nu). \tag{51}$$

We can upper-bound $\sum_{i=1}^{n_1} 1\{X_i'^1 \ne Y_i'^1\}$ (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: $\delta'(\nu) \triangleq \delta_{\text{mismatch}} + \nu - \left(\frac{1}{2T} - \nu\right) \cdot (1 - 2\delta - 2\nu)$ and $R'_+ \triangleq \frac{1}{n_1} \sum_{i=1}^{n_1} 1\{X_i'^1 = 0\}$. So:

$$
\begin{aligned}
\sum_{i=1}^{n_1} 1\{X_i'^1 \ne Y_i'^1\} &= \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \ \wedge \ Y_i'^1 = 1\} + \sum_{i=1}^{n_1} 1\{X_i'^1 = 1 \ \wedge \ Y_i'^1 = 0\} \\
&= \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \ \wedge \ Y_i'^1 = 1\} + \sum_{i=1}^{n_1} 1\{Y_i'^1 = 0\} - \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \ \wedge \ Y_i'^1 = 0\} \\
&= \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \ \wedge \ Y_i'^1 = 1\} + \sum_{i=1}^{n_1} 1\{Y_i'^1 = 0\} \\
&\quad - \left[\sum_{i=1}^{n_1} 1\{X_i'^1 = 0\} - \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \ \wedge \ Y_i'^1 = 1\}\right] \\
&= 2\sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \ \wedge \ Y_i'^1 = 1\} + \sum_{i=1}^{n_1} 1\{Y_i'^1 = 0\} - \sum_{i=1}^{n_1} 1\{X_i'^1 = 0\} \\
&= 2\sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \ \wedge \ Y_i'^1 = 1\} + \sum_{i=1}^{n_1} 1\{Y_i'^1 = 0\} - n_1 R'_+ \\
&\le 2n_1 R'_+ \cdot (\delta + \nu) + n_1 \cdot (\delta_{\text{mismatch}} + \nu) - n_1 R'_+ \\
&= n_1 \cdot [2R'_+ \cdot (\delta + \nu) + \delta_{\text{mismatch}} + \nu - R'_+] \\
&= n_1 \cdot [\delta_{\text{mismatch}} + \nu - R'_+ \cdot (1 - 2\delta - 2\nu)] \\
&\le n_1 \cdot \left[\delta_{\text{mismatch}} + \nu - \left(\frac{1}{2T} - \nu\right) \cdot (1 - 2\delta - 2\nu)\right] = n_1 \delta'(\nu),
\end{aligned} \tag{52}
$$

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

Summary of the proof:

Combining our four bounds, we obtain the following inequality:

$$
\begin{aligned}
&\Pr\left[F^{\text{pe}} = \checkmark \ \wedge \ \Omega_0 \ | \ F^{\text{sift}'} = F^{\min} = \checkmark\right] \\
\le \ &\Pr\left[R'_+ \le \frac{1}{2T} - \nu \ | \ F^{\text{sift}'} = F^{\min} = \checkmark\right] \\
+ \ &\Pr\left[R'_+ \ge \frac{1}{2T} - \nu \ \wedge \ \sum_{i=1}^{k_4} 1\{V_i^4 \ne W_i^4\} \le k_4 \delta\right.
\end{aligned}
$$

$$\wedge \quad \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \wedge Y_i'^1 = 1\} \geq n_1 R_+' \cdot (\delta + \nu) \mid F^{\text{sift}'} = F^{\min} = \checkmark \Bigg]$$

$$+ \quad \Pr\Bigg[\sum_{i=1}^{k_2} 1\{W_i^2 = 0\} \leq k_2 \delta_{\text{mismatch}} \wedge \sum_{i=1}^{n_1} 1\{Y_i'^1 = 0\} \geq n_1 \cdot (\delta_{\text{mismatch}} + \nu) \mid F^{\text{sift}'} = F^{\min} = \checkmark \Bigg]$$

$$+ \quad \Pr\Bigg[R_+' \geq \frac{1}{2T} - \nu \wedge \sum_{i=1}^{n_1} 1\{X_i'^1 = 0 \wedge Y_i'^1 = 1\} \leq n_1 R_+' \cdot (\delta + \nu)$$

$$\wedge \quad \sum_{i=1}^{n_1} 1\{Y_i'^1 = 0\} \leq n_1 \cdot (\delta_{\text{mismatch}} + \nu) \wedge \sum_{i=1}^{n_1} 1\{X_i'^1 \neq Y_i'^1\} > n_1 \delta'(\nu) \mid F^{\text{sift}'} = F^{\min} = \checkmark \Bigg]$$

$$\leq \quad e^{-2n_1\nu^2} + e^{-\frac{2n_1 \cdot \left(\frac{1}{2T} - \nu\right)k_4^2\nu^2}{\left(k_4 + n_1 \cdot \left(\frac{1}{2T} - \nu\right)\right)(k_4+1)}} + e^{-\frac{2n_1 k_2^2 \nu^2}{(k_2+n_1)(k_2+1)}} + 0$$

$$= \quad \epsilon(\nu)^2. \tag{53}$$

The rest of the proof is identical to the proof of Proposition 8 in Section 6.3 of [22], using our parameters $\epsilon(\nu), X'^1, Y'^1, n_1, \Omega_0, \delta'(\nu)$ and conditioning all probabilities and entropies on $F^{\text{sift}'} = F^{\min} = \checkmark$. (A small algebraic difference is that our set Ω_0 requires the strong inequality $1\{\sum_{i=1}^{n_1} 1\{X_i'^1 \neq Y_i'^1\} > n_1 \delta'(\nu)\}$, while Ω's definition in [22] only requires a weak inequality $(1\{\sum_{i=1}^{n} 1\{X_i \neq Y_i\} \geq n \cdot (\delta + \nu)\})$, but the proof still holds.) Therefore, we obtain the following:

$$H_{\max}^{\epsilon(\nu)}(X'^1 \wedge F^{\text{pe}} = \checkmark \mid Y'^1 , F^{\text{sift}'} = F^{\min} = \checkmark)_{\sigma'} \leq n_1 \cdot h_2(\delta'(\nu)), \tag{54}$$

as we wanted. $\square$

4.2.4. Security Theorem for the Modified Entanglement-Based Protocol

Applying the entire proof described in Section 6 of [22] to our modified entanglement-based protocol described in Section 4.1, with the modifications described in Sections 4.2.1–4.2.3, yields the following security result:

Corollary 1. *For the modified entanglement-based protocol described in Section 4.1, we denote the final state as $\omega_{\text{K}_A \text{K}_B \text{SCFE}}$, where K_A is the final key generated by Alice and K_B is the final key generated by Bob (both consisting of ℓ 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 steps elaborated in [22]):*

$$\text{S} \triangleq (\Phi_A, \Phi_B, \Pi_1, \Pi_2, \Pi_3, \Pi_4, \Sigma_1, H_{\text{ec}}, H_{\text{pa}}), \tag{55}$$

$$\text{C} \triangleq (D, \Sigma, V^1, V^2, V^3, V^4, Z, T), \tag{56}$$

$$\text{F} \triangleq (F^{\text{sift}'}, F^{\min}, F^{\text{pe}}, F^{\text{ec}}). \tag{57}$$

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

$$\frac{1}{2} \text{tr} \Big| \omega_{\text{K}_A \text{K}_B \text{SCFE} \wedge F^{\text{pe}} = F^{\text{ec}} = \checkmark \mid F^{\text{sift}'} = F^{\min} = \checkmark} - \omega_U \otimes \omega_{\text{SCFE} \wedge F^{\text{pe}} = F^{\text{ec}} = \checkmark \mid F^{\text{sift}'} = F^{\min} = \checkmark} \Big|$$

$$\leq 2^{-t} + \inf_{\nu \mid 0 < \nu < \frac{1}{2} - \delta, \, 0 < \delta'(\nu) < \frac{1}{2}} (\epsilon_{\text{pa}}(\nu) + \epsilon_{\text{pe}}(\nu)), \tag{58}$$

for any possible attack by Eve, where we define

$$\epsilon_{\text{pa}}(\nu) \triangleq \frac{1}{2} \sqrt{2^{-n_1 \cdot \left[\log_2\left(\frac{1}{c}\right) - h_2(\delta'(\nu))\right] + r + t + \ell}}, \tag{59}$$

$$\epsilon_{\text{pe}}(\nu) \triangleq 2\epsilon(\nu), \tag{60}$$

$$\delta'(\nu) \triangleq \delta_{\text{mismatch}} + \nu - \left(\frac{1}{2T} - \nu\right) \cdot (1 - 2\delta - 2\nu), \tag{61}$$

$$c \triangleq \max\left(|\langle 0|\xi_+\rangle_{A_i}|^2, |\langle 0|\xi_-\rangle_{A_i}|^2, |\langle 1|\xi_+\rangle_{A_i}|^2, |\langle 1|\xi_-\rangle_{A_i}|^2\right), \tag{62}$$

$$\epsilon(\nu) \triangleq \sqrt{e^{-2n_1\nu^2} + e^{-\frac{2n_1 \cdot \left(\frac{1}{2T} - \nu\right)k_4^2\nu^2}{\left(k_4 + n_1 \cdot \left(\frac{1}{2T} - \nu\right)\right)(k_4 + 1)}} + e^{-\frac{2n_1 k_2^2\nu^2}{(k_2 + n_1)(k_2 + 1)}}}, \tag{63}$$

$$h_2(x) \triangleq -x\log_2(x) - (1 - x)\log_2(1 - x). \tag{64}$$

This result is similar to Theorems 2–3 in Section 5 of [22] but has different parameters. According to standard definitions of composable security for QKD (e.g., [27]), 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, to prove 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. More precisely, for any possible attack of Eve on the prepare-and-measure protocol, we need to show that there exists an equivalent attack on the modified entanglement-based protocol leading to the same output for both protocols.

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

$$|\Psi\rangle_{A_iB_i} \triangleq \frac{|0\rangle_{A_i}|\gamma_0\rangle_{B_i} + |1\rangle_{A_i}|\gamma_1\rangle_{B_i}}{\sqrt{2}} = \frac{|\xi_+\rangle_{A_i}|\gamma_+\rangle_{B_i} + \sqrt{2T-1}|\xi_-\rangle_{A_i}|\gamma_-\rangle_{B_i}}{\sqrt{2T}}, \tag{65}$$

where the equality between the two expressions in Equation (65) can be shown algebraically using Equations (2)–(4) and (7)–(8). Then, Alice either measures her subsystem A_i in the standard ("z") basis $\{|0\rangle_{A_i}, |1\rangle_{A_i}\}$ with probability $p_z'^{A}$, or measures it in the conjugate ("x") basis $\{|\xi_+\rangle_{A_i}, |\xi_-\rangle_{A_i}\}$ with probability $p_x'^{A}$. Either way, she sends the resulting state in subsystem B_i to Bob (immediately notifying Bob and cancelling the round if she measured "ξ_-" in the "x 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 measures and discards the round *before* she sends Bob his part of the state), which proves the reduction.

Formally, we use an adapted version of the reduction in Section 9 of [22]. First, 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), as follows:

- The parameters $|\gamma_0\rangle_{B_i}, |\gamma_1\rangle_{B_i}, |\gamma_+\rangle_{B_i}, \{M_{B_i}^{Z,t}\}_{t\in\{0,1\}}, \{M_{B_i}^{X,t}\}_{t\in\{0,1\}}, m, k_1, k_2, k_3, k_4, n_1, \delta,$ and δ_{mismatch} are all identical for the two protocols. (From $|\gamma_0\rangle_{B_i}, |\gamma_1\rangle_{B_i}, |\gamma_+\rangle_{B_i}$ we can infer a, b, and $T \triangleq |a|^2 + |b|^2$.) The error correction and privacy amplification parameters (from [22]) are also identical in both protocols.
- Given the parameters m, T, we choose the parameter M' of the modified entanglement-based protocol to be

$$M' = \frac{m}{\frac{1}{2T} - \nu_0}, \tag{66}$$

where $0 < \nu_0 < \frac{1}{2T}$ is chosen *freely*, without any constraint, to reach the desired trade-off between performance (number of needed rounds) and robustness (success probability of the sifting procedure).

- Given the parameters p_z^A, p_x^A of the prepare-and-measure protocol and the parameter T, we choose the parameters $p_z'^A$, $p_x'^A$ of the modified entanglement-based protocol to be

$$p_z'^A = \frac{p_z^A}{p_z^A + 2Tp_x^A} \quad , \quad p_x'^A = \frac{2Tp_x^A}{p_z^A + 2Tp_x^A} \quad . \tag{67}$$

- Given the parameters p_z^B, p_x^B of the prepare-and-measure protocol, we choose the parameters $p_z'^B$, $p_x'^B$ of the modified entanglement-based protocol to be

$$p_z'^B = p_z^B \quad , \quad p_x'^B = p_x^B \quad . \tag{68}$$

Using these parameters, it is easy to verify that the output of the prepare-and-measure protocol (conditioned on $F^{\min} = \checkmark$) is identical to the output of the modified entanglement-based protocol (conditioned on $F^{\text{sift}'} = F^{\min} = \checkmark$) 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 modified entanglement-based protocol includes the possibility of *discarded rounds* (where Alice measures "ξ_-") 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 Section 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 Section 4.2.1, stage 1 is in fact independent of the bases used for the 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_z^A or 1 with probability p_x^A) and chooses $R \in \{0,1\}^m$ uniformly at random, which lead to the preparation of $|\gamma_0\rangle_{B_i}$, $|\gamma_1\rangle_{B_i}$, or $|\gamma_+\rangle_{B_i}$ with probabilities $\frac{p_z^A}{2}$, $\frac{p_z^A}{2}$, and p_x^A, respectively. These probabilities are independent between the rounds.
  In the modified entanglement-based protocol, Alice generates the following state $|\Psi\rangle_{A_iB_i}$ for each round i:

$$|\Psi\rangle_{A_iB_i} \triangleq \frac{|0\rangle_{A_i}|\gamma_0\rangle_{B_i} + |1\rangle_{A_i}|\gamma_1\rangle_{B_i}}{\sqrt{2}} = \frac{|\xi_+\rangle_{A_i}|\gamma_+\rangle_{B_i} + \sqrt{2T-1}|\xi_-\rangle_{A_i}|\gamma_-\rangle_{B_i}}{\sqrt{2T}}, \tag{69}$$

  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 obtains "ξ_-", and keeps the result secret otherwise. (In fact, Alice's measurement is delayed to Step 8 if the chosen basis is the "z basis", as described in Section 4.1.)
  As explained in Section 4.2.1 (Equations (18) and (19)), for each *non-discarded* round in the modified entanglement-based protocol, the probabilities that Alice measures "0", "1", or "ξ_+" (leading to her sending to Bob $|\gamma_0\rangle_{B_i}$, $|\gamma_1\rangle_{B_i}$, or $|\gamma_+\rangle_{B_i}$, respectively) are

$$\Pr_{A_i}(0) = \Pr_{A_i}(1) = \frac{1}{2} \cdot \frac{p_z'^A}{p_z'^A + \frac{p_x'^A}{2T}} \quad , \quad \Pr_{A_i}(\xi_+) = \frac{1}{2T} \cdot \frac{p_x'^A}{p_z'^A + \frac{p_x'^A}{2T}} \quad . \tag{70}$$

Substituting Equation (67) (and the fact $p_z^A + p_x^A = 1$), we obtain the following probabilities:

$$\mathrm{Pr}_{A_i}(0) = \mathrm{Pr}_{A_i}(1) = \frac{1}{2} \cdot \frac{\frac{p_z^A}{p_z^A + 2Tp_x^A}}{\frac{p_z^A}{p_z^A + 2Tp_x^A} + \frac{\frac{2Tp_x^A}{p_z^A + 2Tp_x^A}}{2T}} = \frac{1}{2} \cdot \frac{p_z^A}{p_z^A + p_x^A} = \frac{p_z^A}{2}, \quad (71)$$

$$\mathrm{Pr}_{A_i}(\xi_+) = \frac{1}{2T} \cdot \frac{\frac{\frac{2Tp_x^A}{p_z^A + 2Tp_x^A}}{2T}}{\frac{p_z^A}{p_z^A + 2Tp_x^A} + \frac{\frac{2Tp_x^A}{p_z^A + 2Tp_x^A}}{2T}} = \frac{1}{2T} \cdot \frac{2Tp_x^A}{p_z^A + p_x^A} = p_x^A, \quad (72)$$

which are independent between the rounds and identical to the prepare-and-measure probabilities found above. Therefore, Alice's preparation results are *identical* on the (non-discarded) rounds of both protocols, even when conditioning on $F^{\mathrm{sift}'} = \checkmark$ in the modified entanglement-based protocol.

- *Eve's attack* is slightly different between the two protocols: on the prepare-and-measure protocol, it is applied to the m rounds which are all relevant, while on the modified entanglement-based protocol, it is applied to all M' rounds (including the discarded rounds) when Eve knows *ahead of time* which rounds are discarded.

  We need to prove that any attack that Eve applies to the m rounds of the prepare-and-measure protocol can also be applied to the relevant rounds of the modified entanglement-based (namely, to the m rounds in Σ, 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 Σ and can apply her attack only to them. This means that any attack by Eve on the m rounds of the prepare-and-measure protocol is a completely legitimate and valid attack on the m rounds in Σ of the modified entanglement-based protocol, and it gives the same outputs in both protocols.

- The rest of the steps in the prepare-and-measure protocol (Steps 5–9) are identical to the rest of the steps in the modified entanglement-based protocol (Steps 6–12), except the delayed measurement in Steps 8 and 9 of the modified entanglement-based protocol.

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 $F^{\mathrm{min}} = \checkmark$ (for the prepare-and-measure protocol) and $F^{\mathrm{sift}'} = F^{\mathrm{min}} = \checkmark$ (for the modified entanglement-based protocol), which is indeed the case in our security proof in Section 4.2.

We therefore obtain the following result:

Corollary 2. *If the modified entanglement-based protocol is secure with a specific security parameter ϵ, the prepare-and-measure protocol is secure with the same security parameter.*

Combining Corollaries 1 and 2, we obtain the final security result for the prepare-and-measure protocol:

Corollary 3. *For the prepare-and-measure protocol described in Section 3, we denote the final state as $\omega_{K_A K_B SCFE}$, where K_A is the final key generated by Alice and K_B is the final key generated by Bob (both consisting of ℓ bits), E is Eve's ancillary quantum system, and S, C, F consist of information published by Alice and Bob (where $H_{\mathrm{ec}}, H_{\mathrm{pa}}, Z, T, F^{\mathrm{ec}}, r, t$ are used in the error correction and privacy amplification steps elaborated in [22]):*

$$S \triangleq (\Phi_A, \Phi_B, \Pi_1, \Pi_2, \Pi_3, \Pi_4, \Sigma_1, H_{\mathrm{ec}}, H_{\mathrm{pa}}), \quad (73)$$

$$C \triangleq (V^1, V^2, V^3, V^4, Z, T), \quad (74)$$

$$\text{F} \quad \triangleq \quad (F^{\min}, F^{\text{pe}}, F^{\text{ec}}). \tag{75}$$

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

$$\frac{1}{2}\,\text{tr}\left|\omega_{\text{K}_\text{A}\text{K}_\text{B}\text{SCFE} \wedge \text{F}^{\text{pe}}=\text{F}^{\text{ec}}=\checkmark \mid \text{F}^{\min}=\checkmark} - \omega_{\text{U}} \otimes \omega_{\text{SCFE} \wedge \text{F}^{\text{pe}}=\text{F}^{\text{ec}}=\checkmark \mid \text{F}^{\min}=\checkmark}\right|$$
$$\leq \quad 2^{-t} + \inf_{\nu \mid 0<\nu<\frac{1}{2}-\delta\,,\,0<\delta'(\nu)<\frac{1}{2}} (\epsilon_{\text{pa}}(\nu) + \epsilon_{\text{pe}}(\nu)), \tag{76}$$

for any possible attack by Eve, where we define

$$\epsilon_{\text{pa}}(\nu) \quad \triangleq \quad \frac{1}{2}\sqrt{2^{-n_1 \cdot \left[\log_2\left(\frac{1}{c}\right) - h_2(\delta'(\nu))\right] + r + t + \ell}}, \tag{77}$$

$$\epsilon_{\text{pe}}(\nu) \quad \triangleq \quad 2\epsilon(\nu), \tag{78}$$

$$\delta'(\nu) \quad \triangleq \quad \delta_{\text{mismatch}} + \nu - \left(\frac{1}{2T} - \nu\right) \cdot (1 - 2\delta - 2\nu), \tag{79}$$

$$c \quad \triangleq \quad \max\left(|\langle 0|\xi_+\rangle_{\text{A}_i}|^2, |\langle 0|\xi_-\rangle_{\text{A}_i}|^2, |\langle 1|\xi_+\rangle_{\text{A}_i}|^2, |\langle 1|\xi_-\rangle_{\text{A}_i}|^2\right), \tag{80}$$

$$\epsilon(\nu) \quad \triangleq \quad \sqrt{e^{-2n_1\nu^2} + e^{-\frac{2n_1 \cdot \left(\frac{1}{2T}-\nu\right)k_4^2\nu^2}{\left(k_4+n_1 \cdot \left(\frac{1}{2T}-\nu\right)\right)(k_4+1)}} + e^{-\frac{2n_1k_2^2\nu^2}{(k_2+n_1)(k_2+1)}}}, \tag{81}$$

$$h_2(x) \quad \triangleq \quad -x\log_2(x) - (1-x)\log_2(1-x). \tag{82}$$

5. Necessity of the Restriction to Three Source States

In our protocol, similarly to the "loss tolerant" protocol [14–17], 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 protocol emits *four* input states (similarly to 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 $0 < q < 1$:

$$p|\gamma_0\rangle\langle\gamma_0| + (1-p)|\gamma_1\rangle\langle\gamma_1| = q|\gamma_+\rangle\langle\gamma_+| + (1-q)|\gamma_-\rangle\langle\gamma_-|, \tag{83}$$

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 on different bases.)

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

$$|\gamma_+\rangle = a|\gamma_0\rangle + b|\gamma_1\rangle \quad, \quad |\gamma_-\rangle = c|\gamma_0\rangle + d|\gamma_1\rangle. \tag{84}$$

Substituting this into Equation (83), we obtain the following:

$$\begin{aligned}
q|\gamma_+\rangle\langle\gamma_+| + (1-q)|\gamma_-\rangle\langle\gamma_-| \quad &= \quad q \cdot [a|\gamma_0\rangle + b|\gamma_1\rangle] \cdot [a^\star\langle\gamma_0| + b^\star\langle\gamma_1|] \\
&+ \quad (1-q) \cdot [c|\gamma_0\rangle + d|\gamma_1\rangle] \cdot [c^\star\langle\gamma_0| + d^\star\langle\gamma_1|] \\
&= \quad [q \cdot |a|^2 + (1-q) \cdot |c|^2] \cdot |\gamma_0\rangle\langle\gamma_0| + [q \cdot ab^\star + (1-q) \cdot cd^\star] \cdot |\gamma_0\rangle\langle\gamma_1| \\
&+ \quad [q \cdot a^\star b + (1-q) \cdot c^\star d] \cdot |\gamma_1\rangle\langle\gamma_0| + [q \cdot |b|^2 + (1-q) \cdot |d|^2] \cdot |\gamma_1\rangle\langle\gamma_1|. \tag{85}
\end{aligned}$$

We thus obtain the following conditions for equality between Equations (83) and (85):

$$q \cdot |a|^2 + (1-q) \cdot |c|^2 \quad = \quad p, \tag{86}$$

$$q \cdot |b|^2 + (1-q) \cdot |d|^2 \quad = \quad 1-p, \tag{87}$$

$$q \cdot ab^\star + (1-q) \cdot cd^\star \quad = \quad 0, \tag{88}$$

$$q \cdot a^\star b + (1 - q) \cdot c^\star d \;\; = \;\; 0. \tag{89}$$

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 (89), we require

$$q = -\frac{c^\star d}{a^\star b - c^\star d} = \frac{c^\star d}{c^\star d - a^\star b}, \tag{90}$$

and for q to be real (and satisfy $0 < q < 1$), the complex phases of $c^\star d$ and $a^\star b$ must be *opposite* (namely, they must differ by $\pm\pi$, which is equivalent to having opposite signs).

This requirement seriously restricts the possible values 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 b and d to have opposite phases. Namely,

$$|\gamma_+\rangle = |a||\gamma_0\rangle + |b|e^{i\phi}|\gamma_1\rangle \;\;,\;\; |\gamma_-\rangle = |c||\gamma_0\rangle - |d|e^{i\phi}|\gamma_1\rangle, \tag{91}$$

where $|c|$ and $|d|$ are dictated by $|a|$ and $|b|$, respectively (see Equations (86) and (87)).

The above analysis means that $|\gamma_-\rangle$ is, in fact, completely determined by the choice of $|\gamma_0\rangle, |\gamma_1\rangle, |\gamma_+\rangle$ (because $|c|, |d|,$ and ϕ can all be inferred from $|\gamma_+\rangle$). 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 of Equations (86)–(89). Essentially, this means that in the presence of source imperfections, the use of at most three states (or, alternatively, measurements in three or more bases, which we do not explore here) is *required* for practical security, and the use of four states could lead to practical security issues.

6. Conclusions

To sum up, we have found a new way to analyse the security of practical QKD protocols by generalizing the results of [22] to more practical protocols (using a modified entropic uncertainty relation and a refined analysis of finite-key statistics). Our proof, compared with other proofs, is rigorous, careful, and simple, aiming to make it easy-to-use in the lossless qubit regime (its extension to losses and decoy states is left for future research because they present specific hurdles in this analysis regime: in particular, losses would need to be declared by Eve in the modified entanglement-based protocol, which could complicate the analysis). We believe that our suggested tools can contribute to benchmarking and certifying the security of practical implementations of QKD.

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the International Conference on Computers, Systems & Signal Processing, Bangalore, India, 10–12 December 1984; pp. 175–179.
2. Brassard, G.; Lütkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **2000**, *85*, 1330–1333. [CrossRef] [PubMed]
3. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.* **2010**, *4*, 686–689. [CrossRef]
4. Biham, E.; Huttner, B.; Mor, T. Quantum cryptographic network based on quantum memories. *Phys. Rev. A* **1996**, *54*, 2651–2658. [CrossRef]
5. Inamori, H. Security of practical time-reversed EPR quantum key distribution. *Algorithmica* **2002**, *34*, 340–365. [CrossRef]
6. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
7. Braunstein, S.L.; Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502. [CrossRef]
8. Mayers, D.; Yao, A. Quantum cryptography with imperfect apparatus. In Proceedings of the 39th Annual Symposium on Foundations of Computer Science, Palo Alto, CA, USA, 8–11 November 1998; pp. 503–509. [CrossRef]
9. Masanes, L.; Pironio, S.; Acín, A. Secure device-independent quantum key distribution with causally independent measurement devices. *Nat. Commun.* **2011**, *2*, 238. [CrossRef]
10. Vazirani, U.; Vidick, T. Fully device-independent quantum key distribution. *Phys. Rev. Lett.* **2014**, *113*, 140501. [CrossRef]
11. Lo, H.K.; Curty, M.; Tamaki, K. Secure quantum key distribution. *Nat. Photon.* **2014**, *8*, 595–604. [CrossRef]
12. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [CrossRef]
13. Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **2020**, *12*, 1012–1236. [CrossRef]
14. Tamaki, K.; Curty, M.; Kato, G.; Lo, H.K.; Azuma, K. Loss-tolerant quantum cryptography with imperfect sources. *Phys. Rev. A* **2014**, *90*, 052314. [CrossRef]
15. Xu, F.; Wei, K.; Sajeed, S.; Kaiser, S.; Sun, S.; Tang, Z.; Qian, L.; Makarov, V.; Lo, H.K. Experimental quantum key distribution with source flaws. *Phys. Rev. A* **2015**, *92*, 032305. [CrossRef]
16. Mizutani, A.; Curty, M.; Lim, C.C.W.; Imoto, N.; Tamaki, K. Finite-key security analysis of quantum key distribution with imperfect light sources. *New J. Phys.* **2015**, *17*, 093011. [CrossRef]
17. Pereira, M.; Curty, M.; Tamaki, K. Quantum key distribution with flawed and leaky sources. *npj Quantum Inf.* **2019**, *5*, 62. [CrossRef]
18. Krawec, W.O. Asymptotic analysis of a three state quantum cryptographic protocol. In Proceedings of the 2016 IEEE International Symposium on Information Theory (ISIT), Barcelona, Spain, 10–15 July 2016; pp. 2489–2493. [CrossRef]
19. Hwang, W.Y. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef]
20. Lo, H.K.; Ma, X.; Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef]
21. Wang, X.B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef]
22. Tomamichel, M.; Leverrier, A. A largely self-contained and complete security proof for quantum key distribution. *Quantum* **2017**, *1*, 14. [CrossRef]
23. Hasegawa, J.; Hayashi, M.; Hiroshima, T.; Tomita, A. Security analysis of decoy state quantum key distribution incorporating finite statistics. *arXiv* **2007**, arXiv:0707.3541.
24. Lim, C.C.W.; Curty, M.; Walenta, N.; Xu, F.; Zbinden, H. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A* **2014**, *89*, 022307. [CrossRef]
25. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
26. Bennett, C.H.; Brassard, G.; Mermin, N.D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **1992**, *68*, 557–559. [CrossRef]
27. Renner, R. Security of quantum key distribution. *Int. J. Quantum Inf.* **2008**, *6*, 1–127. [CrossRef]
28. Tomamichel, M. A framework for non-asymptotic quantum information theory. Ph.D. Thesis, ETH Zurich, Zurich, Switzerland, 2012.
29. Tomamichel, M.; Lim, C.C.W.; Gisin, N.; Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **2012**, *3*, 634. [CrossRef]
30. Pereira, M.; Kato, G.; Mizutani, A.; Curty, M.; Tamaki, K. Quantum key distribution with correlated sources. *Sci. Adv.* **2020**, *6*, eaaz4487. [CrossRef]
31. Hoeffding, W. Probability inequalities for sums of bounded random variables. *J. Am. Stat. Assoc.* **1963**, *58*, 13–30. [CrossRef]