Security loophole in error verification in quantum key distribution

Toyohiro Tsurumaru *,[1] Akihiro Mizutani †,[2] and Toshihiko Sasaki ‡[3]

[1] *Mitsubishi Electric Corporation, Information Technology R&D Center, 5-1-1 Ofuna, Kamakura-shi, Kanagawa 247-8501, Japan*

[2] *Faculty of Engineering, University of Toyama, Gofuku 3190, Toyama 930-8555, Japan*

[3] *Quantinuum K.K. Otemachi Financial City Grand Cube 3F, Global Business Hub Tokyo 1-9-2 Otemachi, Chiyoda-ku, Tokyo 100-0004 Japan*

The security of quantum key distribution (QKD) is evaluated based on the secrecy of Alice's key and the correctness of the keys held by Alice and Bob. A practical method for ensuring correctness is known as error verification, in which Alice and Bob reveal a portion of their reconciled keys and check whether the revealed information matches. In this paper, we argue that when the verification is executed in QKD protocols, it must be assumed that its outcome is leaked to Eve. However, we observe that some existing security proofs for QKD protocols that abort based on this outcome do not explicitly take into account the information leakage associated with this outcome. To address this problem, we present a simple and practical method that builds on Renner's approach using the leftover hash lemma. Specifically, we show that even if verification's outcome is leaked to Eve, the security can still be guaranteed by increasing the number of bits reduced in privacy amplification by just one bit. This result, presenting a method to incorporate a key step in practical QKD protocols into security proofs, is expected to play an important role in future standardization and formal certification of QKD protocols.

I. INTRODUCTION

The standard goal of security proofs of quantum key distribution (QKD) [1–3] is to derive the security parameter defined based on the universal composable security framework [4–6]. The security parameter is, roughly speaking, defined as the trace distance between the ideal secret keys and the actual keys (see Sec. II for its definition). Toward this goal, it is customary and convenient first to split the security parameter into the secrecy and the correctness parameters, and then to derive each of them separately [7–10]. One of them, the correctness parameter is defined by the probability that Alice's and Bob's secret keys are not identical. The prevalent method for deriving this parameter is called *error verification* (see, for example, Ref. [11] for details), wherein Alice and Bob publicly compare hash values of their reconciled keys (i.e., the keys obtained after completing bit error correction) to check the identicalness of these keys. While other methods may in principle be able to serve for the same purpose [37], error verification widely used [9, 10, 12–18] because it is by far the simplest and most reliable method in practice. In this respect, it is an essential part of practical QKD implementations.

Our goals in this paper are first to point out a possible problem - namely, that most of the literature on the security proof of QKD (e.g., Refs. [9, 12, 19]) does not seem to treat the effect of error verification properly, and then to present a simple solution to it.

The issue described above seems to originate from an unclear or inconsistent treatment of the outcome V of error verification: By a simple observation, it can be shown that V must be announced publicly (see Sec. III A for detail). Once one accepts this public nature of V, one can readily conclude that the secrecy parameter must be defined for the state *after* error verification (see Sec. III B for detail). However, most of the literature seems to inappropriately treat V as secret information and define the secrecy for the state *without* error verification. This is the core of the problem regarding the treatment of the outcome of error verification, which we refer to as the *verification problem*.

In order to demonstrate the serious consequences of this inappropriate definition of secrecy, we present a counterexample where a false claim of the security can be made according to such definition, even though it does not hold in reality (see Sec. III C for detail). This situation occurs because in a certain type of protocol, the one bit of information V may become correlated with the secret key, thereby compromising the security.

Fortunately, we can also provide a simple solution to the verification problem: Security proofs based on the appropriate definition of secrecy can always be repaired by shortening the final key length by one bit (see Sec. IV for detail). The basic idea here is conceptually simple, although the actual proof entails nontrivial technical work. It is known that the effect of any newly announced information, represented by a random variable $X \in \{0,1\}^m$, can be compensated by shortening the privacy amplification output by m bits [9]. Hence, the effect of announcing the outcome V, which discloses one bit of information, can be canceled by shortening the final key by one bit.

From a future perspective, the widespread adoption of QKD in society requires the standardization of a compre-

*Tsurumaru.Toyohiro@da.MitsubishiElectric.co.jp
†mizutani@eng.u-toyama.ac.jp
‡Toshihiko.Sasaki@quantinuum.com

hensive framework for certifying its security. Our work represents an important contribution in this direction, as it clearly demonstrates the importance of rigorously incorporating error verification into the security proof and provides a practical method to address this challenge.

II. CONVENTIONAL ARGUMENT OF THE SEPARATION

We begin by summarizing the notation adopted throughout this paper.

1. $[b]$ denotes the projector $|b\rangle\langle b|$, with $\{|b\rangle\}_b$ being the computational basis.
2. For a composite system described by a density operator $\rho_{AB\cdots}$ over multiple systems $(AB\cdots)$, the state of a particular system (e.g., ρ_A) is defined by taking the partial trace over the remaining systems.
3. Given a quantum classical (sub normalized) state ρ_{AB} of systems AB, $\rho_A^{B=b}$ is defined by $\mathrm{tr}_B[\rho_{AB}(\mathbb{I}_A \otimes [b]_B)]$.
4. Given a density matrix σ, its trace norm is defined by [20]

$$\|\sigma\|_1 := \frac{1}{2}\mathrm{tr}\sqrt{\sigma\sigma^\dagger}. \tag{1}$$

In this section, we revisit the conventional argument for decomposing QKD's security parameter into those of secrecy and correctness based on Ref. [7]. This argument states that if Alice's final key is $\varepsilon_{\mathrm{sec}}$-secret and Alice's and Bob's final keys are $\varepsilon_{\mathrm{cor}}$-correct, then their pair of final keys as a whole satisfies $\varepsilon_{\mathrm{sec}} + \varepsilon_{\mathrm{cor}}$-security.

The more precise explanation would be as follows. In this section, we restrict ourselves to the types of QKD protocols where decisions of continuing or aborting the protocol are made solely based on public information and do not depend on the contents of the sifted, reconciled, or secret keys. This situation typically arises in certain types of the BB84 protocol, where Alice and Bob abort the protocol if the estimated quantum bit error rate (QBER) during the sampling and parameter estimation phases exceeds a predetermined threshold. However, once the key distillation process—including error correction and privacy amplification—has commenced, they never abort the protocol.

In such cases, the security of a QKD protocol is defined as follows. Let K_A, K_B be the states of Alice's and Bob's secret keys and E Eve's quantum system. Also, let $\rho_{K_AK_BE}$ be the marginal (thus possibly sub-normalized) state corresponding to the event where the protocol is continued. Then we say that the QKD protocol is ε-secure if

$$\left\|\rho_{K_AK_BE} - \rho^{\mathrm{ideal}}_{K_AK_BE}\right\|_1 \leq \varepsilon, \tag{2}$$

is satisfied, with the ideal state being

$$\rho^{\mathrm{ideal}}_{K_AK_BE} = \sum_{k\in\{0,1\}^\ell} 2^{-\ell}[k]_{K_A} \otimes [k]_{K_B} \otimes \rho_E, \tag{3}$$

and ℓ the length of the secret key. To prove Eq. (2), it is common to decompose the trace distance into two parameters (secrecy and correctness) and evaluate each separately. Specifically, the $\varepsilon_{\mathrm{sec}}$-secrecy of Alice's secret key K_A is defined by

$$d(\rho_{K_AE}|E) \leq \varepsilon_{\mathrm{sec}}, \tag{4}$$

where

$$d(\rho_{K_AE}|E) := \left\|\rho_{K_AE} - \rho^{\mathrm{ideal}}_{K_AE}\right\|_1, \tag{5}$$

$$\rho^{\mathrm{ideal}}_{K_AE} = 2^{-\ell}\mathbb{I}_{K_A} \otimes \rho_E. \tag{6}$$

Furthermore, the protocol satisfies $\varepsilon_{\mathrm{cor}}$-correctness if the probability that Alice's and Bob's secret keys do not match is upper-bounded by $\varepsilon_{\mathrm{cor}}$, i.e.,

$$\Pr[K_A \neq K_B] \leq \varepsilon_{\mathrm{cor}}. \tag{7}$$

Under these conditions, the following lemma [7] holds.

Lemma 1. *(Separation lemma without error verification) For QKD protocols without error verification, the trace distance is bounded as*

$$\left\|\rho_{K_AK_BE} - \rho^{\mathrm{ideal}}_{K_AK_BE}\right\|_1 \leq d(\rho_{K_AE}|E) + \Pr[K_A \neq K_B]. \tag{8}$$

That is, the security parameter ε can be bounded as $\varepsilon \leq \varepsilon_{\mathrm{sec}} + \varepsilon_{\mathrm{cor}}$.

Intuitively, this lemma means that if Alice's key is secret to Eve and matches Bob's key, then both Alice and Bob share a secret key. We remark that due to Eve's attacks, the bit error rate can be increased at will. Therefore, in practice, it is impossible to ensure that $\Pr[K_A \neq K_B]$ in Eq. (8) is a small value.

III. SEPARATION LEMMA FOR QKD PROTOCOLS WITH ERROR VERIFICATION

In Sec. II, we restricted ourselves to the case where decisions of continuing or aborting the protocol are made solely based on public information. In practical QKD protocols, however, this restriction is often violated due to error verification.

A. Error verification's outcome must be announced

We first note that, in light of actual operations performed in QKD systems, it is unrealistic to assume that the outcome of error verification — denoted by $v = 0$ or

1 for continuing or aborting the protocol — can be kept permanently hidden from Eve. Therefore, it must be assumed that this information v is always publicly available to Eve. This situation can be justified by the fact that the following scenario frequently occurs.

Inevitable leakage of error verification's outcome Suppose, for example, that Alice and Bob execute a QKD protocol, and immediately after its completion, they use the generated secret key for secure communication with the one-time pad. In such a case, Eve can determine that the QKD protocol did not abort by observing a large volume of encrypted messages transmitted over the public channel. This implies that the outcome of error verification $v \in \{0,1\}$ is effectively leaked to Eve.

In other words, even if Alice and Bob attempt to conceal $v \in \{0,1\}$ through encryption or other means, it is easy to construct scenarios in which the value of v is leaked to Eve. Therefore, it is not reasonable to assume that v remains concealed from Eve indefinitely, and it must instead be treated as publicly known.

B. Separation lemma with error verification

In order to describe variable V properly, we use the following notation. We treat V as part of the public information accessible to Eve. As in Sec. II, we continue to let $\rho_{K_AK_BVE}$ denote the marginal state corresponding to the event where Alice and Bob decided to continue the protocol based solely on the public information. In addition, we express the event where they decided to continue (or abort) due to error verification by $\rho^{V=0}_{K_AK_BVE}$ (or $\rho^{V=1}_{K_AK_BVE}$), which is a marginal state of $\rho_{K_AK_BVE}$. The final key state $\rho_{K_AK_BVE}$ then takes the form

$$\rho_{K_AK_BVE} = \sum_{v\in\{0,1\}} \rho^{V=v}_{K_AK_BE} \otimes [v]_V, \tag{9}$$

$$\rho^{V=1}_{K_AK_BE} = [\perp]_{K_A} \otimes [\perp]_{K_B} \otimes \rho^{V=1}_E, \tag{10}$$

with the symbol '$\perp$' denoting the situation where no key is generated since the verification failed.

In this notation, our observation of Sec. III A claims that it is inappropriate to evaluate the security using the left-hand side (LHS) of Eq. (2), where V is not included as public information accessible to Eve. The security should rather be evaluated by the trace distance

$$\left\|\rho_{K_AK_BVE} - \rho^{\text{ideal}}_{K_AK_BVE}\right\|_1,$$

for which the following separation lemma (a variant of Lemma 1) holds.

Lemma 2. *(Separation lemma with or without error verification) For QKD protocols in general, with or without error verification, the security parameter can be upper-bounded as*

$$\left\|\rho_{K_AK_BVE} - \rho^{\text{ideal}}_{K_AK_BVE}\right\|_1 \le d\left(\rho^{V=0}_{K_AE}|E\right) + \Pr[K_A \neq K_B]. \tag{11}$$

Proof. By using Eqs. (9) and (10), the trace distance with the ideal case can be bounded as

$$\begin{aligned}
&\left\|\rho_{K_AK_BVE} - \rho^{\text{ideal}}_{K_AK_BVE}\right\|_1 \\
&= \sum_{v\in\{0,1\}} \left\|\rho^{V=v}_{K_AK_BE} - \left(\rho^{V=v}_{K_AK_BE}\right)^{\text{ideal}}\right\|_1 \\
&= \left\|\rho^{V=0}_{K_AK_BE} - \left(\rho^{V=0}_{K_AK_BE}\right)^{\text{ideal}}\right\|_1 \\
&\le d\left(\rho^{V=0}_{K_AE}|E\right) + \Pr[K_A \neq K_B \wedge V = 0] \\
&= d\left(\rho^{V=0}_{K_AE}|E\right) + \Pr[K_A \neq K_B].
\end{aligned} \tag{12}$$

The first equality holds since the random variable V is public. The second equality follows by the fact that $\rho^{V=1}_{K_AK_BE}$ is ideal, namely, $\rho^{V=1}_{K_AK_BE} = (\rho^{V=1}_{K_AK_BE})^{\text{ideal}}$ (because no information is leaked to Eve when no key is generated), which can be seen from Eq. (10). The inequality follows by applying Lemma 1 to $\rho^{V=0}_{K_AK_BE}$. The last equality holds since $\Pr[K_A \neq K_B \wedge V = 1] = 0$ due to Eq. (10).

Note that there is a practical method to upper-bound the second term $\Pr[K_A \neq K_B]$; see Appendix A for the detail. □

Comparing Lemmas 1 and 2, we observe that the quantity used to evaluate secrecy is replaced from $d(\rho_{K_AE}|E)$ to $d(\rho^{V=0}_{K_AE}|E)$. In other words, if we prove the security of QKD protocols with error verification, secrecy must be evaluated only with respect to the event conditioned on the success of error verification (i.e., $V = 0$).

Secrecy condition with error verification The ε_{sec}-secrecy, conditioned on the event that the verification succeeds (i.e., $V = 0$), is expressed by

$$d\left(\rho^{V=0}_{K_AE}|E\right) \le \varepsilon_{\text{sec}}. \tag{13}$$

Although many existing works consider QKD protocols with error verification, they often adopt the LHS of Eq. (8) as the secrecy criterion [9, 12, 19], rather than that of Eq. (11), which should be used to properly bound the trace distance in the presence of error verification [38]. This indicates that the adopted definition is, in general, inadequate for QKD protocols with error verification. One might expect that the LHS of Eq. (11) can still be upper-bounded by the right-hand side (RHS) of Eq. (8). However, we will show in the next Sec. III C that this is not the case. Specifically, we demonstrate that, when error verification is present, there exists a situation in which the LHS of Eq. (11) cannot be bounded by the RHS of Eq. (8) [39].

C. Counterexample to bounding Eq. (11) by Eq. (8)

In this section, we show by example that the LHS of Eq. (11) cannot, in general, be upper-bounded by the RHS of Eq. (8).

In the following, the outcome of error verification is represented by a variable $V \in \{0,1\}$, which must be assumed known to Eve. More precisely, V should be regarded not as a variable of Alice or Bob, but as the one accessible to Eve.

a. Protocol without error verification We assume that the reconciled key consists of two bits, with

$$\rho_{ABE} = \frac{1}{8} \sum_{x,y,z\in\{0,1\}} [xy]_A \otimes [zx]_B \otimes [z]_E. \tag{14}$$

This corresponds, for example, to a situation in the BB84 protocol where Eve leaves the first qubit sent by Alice intact, performs the intercept-and-resend attack on the second qubit, swaps the two qubits, and then sends them to Bob.

Privacy amplification (PA) Alice and Bob set the first bit of the reconciled key as the secret keys k_A, k_B, namely, $k_A = a_1(= x)$, $k_B = b_1(= z)$.

In this case, the joint state of Alice's secret key and Eve's system is already the ideal state, as

$$\rho_{K_AE} = \left(\frac{1}{2}\mathbb{I}_2\right)_{K_A} \otimes \left(\frac{1}{2}\mathbb{I}_2\right)_E \tag{15}$$

holds. This means that 0-secrecy ($\varepsilon_{\rm sec} = 0$) is satisfied, that is

$$d(\rho_{K_AE}|E) = 0. \tag{16}$$

b. Protocol with error verification added Suppose we add the following step to the above protocol.

Error verification Bob compares his two reconciled key bits. If they match, the protocol proceeds; otherwise, Bob aborts the protocol.

This verification succeeds with probability 1/2, and the resulting (sub-normalized) state satisfies

$$\begin{aligned}\rho_{K_AK_BEV} =& \frac{1}{4}\left(\sum_{k\in\{0,1\}} [k]_{K_A} \otimes [k]_{K_B} \otimes [k]_E \otimes [0]_V\right) \\ &+ \frac{1}{4}[\perp]_{K_A} \otimes [\perp]_{K_B} \otimes \mathbb{I}_E \otimes [1]_V. \end{aligned}\tag{17}$$

Clearly,

$$\Pr[K_A \neq K_B] = 0 \tag{18}$$

holds, and the secret keys satisfy 0-correctness.

To summarize, Eq. (16) shows that $\varepsilon_{\rm sec} = 0$, and as stated in Eq. (18), $\varepsilon_{\rm cor} = 0$ also holds. Naively, one might therefore expect that combining these with Lemma 1 would imply 0-security—that is,

$$\begin{aligned}&\left\|\rho_{K_AK_BEV} - (\rho_{K_AK_BEV})^{\rm ideal}\right\|_1 \\ &\leq d(\rho_{K_AE}|E) + \Pr[K_A \neq K_B] = 0. \end{aligned}\tag{19}$$

However, this is incorrect. In fact, a direct calculation shows that

$$\left\|\rho_{K_AK_BEV} - (\rho_{K_AK_BEV})^{\rm ideal}\right\|_1 = \frac{1}{4}, \tag{20}$$

indicating that the actual situation is far from achieving 0-security.

D. Analysis of the counterexample

This section provides an analysis of the counterexample given in Sec. III C. If we evaluate secrecy using the inappropriate definition [Eq. (4)]—which should not be used for QKD protocols involving error verification—then, as shown in Eq. (16), 0-secrecy appears to hold. However, when secrecy is assessed based on the correct definition [Eq. (13)], we have

$$d\left(\rho^{V=0}_{K_AE}|E\right) = \frac{1}{4}, \tag{21}$$

which indicates that the state is far from satisfying 0-secrecy. We note that substituting Eqs. (18) and (21) into Lemma 2 yields a result consistent with Eq. (20). The fundamental reason for this discrepancy is that Eve gains additional information about Alice's secret key upon learning that the protocol has not been aborted (i.e., $V = 0$). A more detailed explanation is given below.

- According to Eq. (14) and the verification procedure, the protocol ensures $k_A = E$ if $V = 0$, and $k_A \neq E$ when $V = 1$.
- In a protocol without error verification (i.e., where v is not disclosed to Eve and the protocol is not aborted), Eve only has the information averaged over the above correlated ($k_A = E$) and anti-correlated events ($k_A \neq E$). As a result, the variable k_A appears uniformly distributed, and 0-secrecy holds, as shown in Eq. (16).
- In contrast, for a protocol with error verification, the verification step succeeds with probability 1/2, and its outcome is disclosed to Eve. In this case, Eq. (17) implies that Alice's secret key is fully leaked to Eve, and secrecy can no longer be guaranteed.

The counterexample above is a toy example indicative of what might happen in a real QKD protocol without error correction. It illustrates an important point that the intuitive relation given by Eq. (19) does not hold in general.

IV. SIMPLE METHOD FOR BOUNDING SECRECY WITH ERROR VERIFICATION BY MIN-ENTROPY OF RECONCILED KEY

The counterexample in Sec. III C demonstrates that the variable V can be correlated with the secret key. Consequently, even if secrecy were guaranteed in a situation where the key is generated without revealing V (i.e., in a protocol without error verification), this does not necessarily imply security in the case where V is made public. This discrepancy lies at the heart of the verification problem.

To address this issue—namely, to guarantee the secrecy of a protocol with error verification, we adopt Renner's approach [12], in which the bit of information V is explicitly treated as part of the public information. The applicability of this approach within Koashi's approach is discussed in Sec. V. In this case, the disclosure of V results in a decrease in the min-entropy [12] of the reconciled key, leading to a shorter secret key. Equivalently, this can be interpreted as requiring privacy amplification with an overhead of one additional bit. This can be formally stated as the following lemma.

Lemma 3. *Suppose that the conditional min-entropy of the (possibly sub-normalized) classical-quantum state ρ of Alice's reconciled key and Eve's system satisfies*

$$H_{\min}(A|E)_\rho \geq \ell + 2\log(1/\varepsilon_{\sec}) \tag{22}$$

with $\varepsilon_{\sec}, \ell > 0$. Suppose also that, in order to generate secret keys, Alice and Bob perform

- *error verification, and she newly announces the hash value information H,*
- *privacy amplification on their reconciled keys with the output bit length $\ell - |H| - 1$, where $|H|$ denotes the bit length of H.*

Alice's secret key K'_A thus generated (of $\ell - |H| - 1$ bits) is $\varepsilon_{\sec}$-secret; i.e., it holds that

$$d(\rho^{V=0}_{K'_A EHF}|EHF) \leq \varepsilon_{\sec}, \tag{23}$$

where F denotes the choice of a hash function used for privacy amplification.

The meaning of this lemma can also be explained as follows. As one can easily imagine, by a straightforward application of the chain rule for the conditional min-entropy, it can readily be shown that $d(\rho_{K_A EHF}|EHF) \leq \varepsilon_{\sec}$ holds for $(\ell - |H|)$-bit key K_A. This inequality, however, turned out to be inappropriate in the previous section for guaranteeing the security of the protocols with error verification. The above lemma claims that there is still a simple method for ensuring the correct inequality, $d(\rho^{V=0}_{K'_A EHF}|EHF) \leq \varepsilon_{\sec}$, by shortening the secret keys by only one bits.

Proof. Recall that in the actual protocol, Alice and Bob generate the $(\ell - |H| - 1)$-bit secret key (by applying privacy amplification with just one extra bit compared to the case without error verification) if $V = 0$, and they abort the protocol if $V = 1$.

In order to prove

$$d(\rho^{V=0}_{K'_A EHF}|EHF) = \left\| \rho^{V=0}_{K'_A EHF} - (\rho^{V=0}_{K'_A EHF})^{\mathrm{ideal}} \right\|_1 \leq \varepsilon_{\sec}, \tag{24}$$

consider a virtual scenario where Alice and Bob do not abort the protocol even when $v = 1$. In this scenario, the state $\bar{\rho}_{K'_A EHVF}$ of systems $K'_A EHVF$ is written as

$$\bar{\rho}_{K'_A EHVF} = \sum_{\substack{k'_A \in \{0,1\}^{\ell-1}, \\ v\in\{0,1\}, h, f}} [k'_A]_{K'_A} \otimes \left(\sum_{a \in f^{-1}(k'_A)} \rho_E^{(A,H,V)=(a,h,v)} \right) \otimes [h]_H \otimes [v]_V \otimes \Pr[F = f][f]_F. \tag{25}$$

Here, A denotes Alice's reconciled key. For this state, we have

$$\left\| \bar{\rho}_{K'_A EHVF} - (\bar{\rho}_{K'_A EHVF})^{\mathrm{ideal}} \right\|_1 = \sum_{v\in\{0,1\}} \left\| \bar{\rho}^{V=v}_{K'_A EHF} - \left(\bar{\rho}^{V=v}_{K'_A EHF}\right)^{\mathrm{ideal}} \right\|_1 . \tag{26}$$

Note that the states for $v = 0$ are the same in both the actual and virtual scenarios, i.e.,

$$\bar{\rho}^{V=0}_{K'_A EHF} = \rho^{V=0}_{K'_A EHF}. \tag{27}$$

If we can prove that

$$\left\| \bar{\rho}_{K'_A EHVF} - (\bar{\rho}_{K'_A EHVF})^{\mathrm{ideal}} \right\|_1 \leq \varepsilon_{\sec}, \tag{28}$$

then we have Eq. (24) from Eqs. (26) and (27) and the non-negativity of trace distance. Hence, our remaining task is to prove Eq. (28).

The LHS of Eq. (28) is the secrecy when Alice always generates $(\ell - |H| - 1)$-bit secret key K'_A (i.e., without aborting the protocol) and Eve possesses systems EHV. To evaluate this, it suffices to lower-bound the min-entropy $H_{\min}(A|EHV)_\rho$ as

$$\begin{aligned} H_{\min}(A|EHV)_\rho &\geq H_{\min}(A|E)_\rho - H_{\max}(HV)_\rho \\ &\geq H_{\min}(A|E)_\rho - (|H| + 1) \\ &\geq \ell + 2\log(1/\varepsilon_{\sec}) - (|H| + 1). \end{aligned} \tag{29}$$

The first inequality follows by Eq. (3.21) in [12], the chain rule of the conditional min-entropy. The second inequality follows from the fact that the max-entropy [12] is upper-bounded as $H_{\max}(HV)_\rho \leq |H| + 1$, where V is a one-bit variable and $|H|$ denotes the bit length of H. The last inequality comes from Eq. (22). Then, the leftover hash lemma [10, 12, 21] guarantees that the resulting trace distance can be upper-bounded by $\varepsilon_{\rm sec}$ by performing privacy amplification using the hash function F. □

V. DISCUSSION

In our proof of Lemma 3, we employed a method based on the leftover hash lemma (referred to as Renner's approach [12] or the LHL-based approach). We note, however, that the result of Lemma 3 can also be used in security proofs based on the phase error correction method (referred to as the PEC-based approach, also known as Koashi's approach [7, 22]). This is because the LHL-based and the PEC-based approaches have been proven to be equivalent [23, 24].

More precisely, the security proof based on Koashi's approach can be interpreted as (i) considering a virtual protocol where Alice prepares qubits entangled with the systems sent to Bob, and then measures these qubits in the X-basis (the basis complementary to the key generation basis), yielding outcomes denoted by X^A, and then (ii) upper-bounding the max-entropy $H_{\max}(X^A|B)$ [23, 24]. By applying an entropic uncertainty relation [25] to $H_{\max}(X^A|B)$, one obtains a lower bound on the min-entropy $H_{\min}(A|E)$. If this lower bound is identified with Eq. (22), then Lemma 3 can be proven accordingly.

The verification problem identified in this paper originates from the fact that the verification's outcome V can, in general, be correlated with the sifted, reconciled or final keys. On the other hand, it should be noted that if one can somehow prove that V is uncorrelated with the keys, then this issue does not arise. As already discussed in Sec. II, such a situation occurs, for example, when the decisions to continue or abort the protocol are made solely based on the public information.

We also note that there is another typical situation where V can be shown uncorrelated with the keys. That is where one can apply a Shor–Preskill-type security proof [26], and thus regard the error verification step as part of the syndrome measurement for bit error correction (or, equivalently, if it is incorporated into the choice of a sufficiently large code C_1 for Z-basis error correction). This is true, for example, when Alice and Bob can be assumed to possess qubits in the virtual protocol (as in the PEC-based approach) and perform error verification using a linear hash function [40]. In such cases, the secrecy of Alice's (or Bob's) final key can be discussed independently of error verification, and thus the verification problem no longer occurs [41].

Acknowledgements

We thank Kiyoshi Tamaki, Go Kato and Shun Kawakami for helpful discussions. A. Mizutani is partially supported by JSPS KAKENHI Grant Number JP24K16977.

Appendix A: Practical method for bounding $\Pr[K_A \neq K_B]$

There is a practical method for bounding the probability $\Pr[K_A \neq K_B]$ appearing, e.g., in Eqs. (7) and (11) [10]. This is the probability of an undesirable event in which the secret keys do not match despite the error verification being successful. This probability can be upper-bounded as

$$\begin{aligned}\Pr[K_A \neq K_B] &= \Pr[K_A \neq K_B \wedge V = 0] \\ &\leq \Pr[A \neq B \wedge V = 0] = \Pr[V = 0 \,|\, A \neq B]\Pr[A \neq B] \\ &\leq \Pr[V = 0 \,|\, A \neq B]. \end{aligned} \tag{A1}$$

Here, A and B denote Alice's and Bob's reconciled keys, respectively. The quantity on the last line (and thus also $\Pr[K_A \neq K_B]$) can be upper-bounded by $\varepsilon_{\rm cor}$ as follows. Suppose that Alice announces the hash value $h(a)$ of her reconciled key a, using a randomly chosen element h of the universal hash function H with the output length $\lceil \log(1/\varepsilon_{\rm cor}) \rceil$. Also, suppose that Bob announces that the protocol is aborted ($v = 1$) if and only if the hash values of the reconciled keys differ, i.e., $h(a) \neq h(b)$. Then, we have

$$\Pr[V = 0 \,|\, A \neq B] = \Pr[H(A) = H(B) \,|\, A \neq B] \leq \varepsilon_{\rm cor}. \tag{A2}$$

[1] H.-K. Lo, M. Curty, and K. Tamaki, Nature Photonics **8**, 595 (2014), ISSN 1749-4893, URL https://doi.org/10.1038/nphoton.2014.149.

[2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Rev. Mod. Phys. **92**, 025002 (2020), URL https://link.aps.org/doi/10.1103/RevModPhys.92.025002.

[3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, et al., Adv. Opt. Photon. **12**, 1012 (2020), URL https://opg.optica.org/aop/abstract.cfm?URI=aop-12-4-1012.

[4] C. Portmann and R. Renner, Rev. Mod. Phys. **94**, 025008 (2022), URL https://link.aps.org/doi/10.1103/RevModPhys.94.025008.

[5] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, *The universal composable security of quantum key distribution* (2004), quant-ph/0409078, URL https://arxiv.org/abs/quant-ph/0409078.

[6] J. Müller-Quade and R. Renner, New Journal of Physics **11**, 085006 (2009), URL https://dx.doi.org/10.1088/1367-2630/11/8/085006.

[7] M. Koashi, New Journal of Physics **11**, 045018 (2009), URL https://dx.doi.org/10.1088/1367-2630/11/4/045018.

[8] M. Hayashi and T. Tsurumaru, New Journal of Physics **14**, 093014 (2012), URL https://dx.doi.org/10.1088/1367-2630/14/9/093014.

[9] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nature Communications **3** (2012), ISSN 2041-1723, URL http://dx.doi.org/10.1038/ncomms1631.

[10] M. Tomamichel and A. Leverrier, Quantum **1**, 14 (2017), ISSN 2521-327X, URL https://doi.org/10.22331/q-2017-07-14-14.

[11] D. Tupkary, E. Y. Z. Tan, S. Nahar, L. Kamin, and N. Lütkenhaus, *Qkd security proofs for decoy-state bb84: protocol variations, proof techniques, gaps and limitations* (2025), 2502.10340, URL https://arxiv.org/abs/2502.10340.

[12] R. Renner, *Security of quantum key distribution* (2006), quant-ph/0512258, URL https://arxiv.org/abs/quant-ph/0512258.

[13] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nature Communications **5**, 3732 (2014), ISSN 2041-1723, URL https://doi.org/10.1038/ncomms4732.

[14] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Phys. Rev. A **89**, 022307 (2014), URL https://link.aps.org/doi/10.1103/PhysRevA.89.022307.

[15] K. Maeda, T. Sasaki, and M. Koashi, Nature Communications **10**, 3140 (2019), ISSN 2041-1723, URL https://doi.org/10.1038/s41467-019-11008-z.

[16] M. Sandfuchs, M. Haberland, V. Vilasini, and R. Wolf, Quantum **9**, 1611 (2025), ISSN 2521-327X, URL https://doi.org/10.22331/q-2025-01-27-1611.

[17] A. Mizutani, T. Sasaki, and G. Kato, *Protocol-level description and self-contained security proof of decoy-state bb84 qkd protocol* (2025), 2504.20417, URL https://arxiv.org/abs/2504.20417.

[18] L. Kamin, J. Burniston, and E. Y. Z. Tan, *Rényi security framework against coherent attacks applied to decoy-state qkd* (2025), 2504.12248, URL https://arxiv.org/abs/2504.12248.

[19] D. Tupkary, E. Y.-Z. Tan, and N. Lütkenhaus, Physical Review Research **6** (2024), ISSN 2643-1564, URL http://dx.doi.org/10.1103/PhysRevResearch.6.023002.

[20] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, 2010).

[21] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Transactions on Information Theory **57**, 5524 (2011).

[22] M. Koashi, *Simple security proof of quantum key distribution via uncertainty principle* (2005), quant-ph/0505108, URL https://arxiv.org/abs/quant-ph/0505108.

[23] T. Tsurumaru, IEEE Transactions on Information Theory **66**, 3465 (2020), ISSN 1557-9654, URL http://dx.doi.org/10.1109/TIT.2020.2969656.

[24] T. Tsurumaru, IEEE Transactions on Information Theory **68**, 1016 (2022).

[25] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011), URL https://link.aps.org/doi/10.1103/PhysRevLett.106.110506.

[26] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000), URL https://link.aps.org/doi/10.1103/PhysRevLett.85.441.

[27] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)* (Wiley-Interscience, USA, 2006), ISBN 0471241954.

[28] T. Richardson and R. Urbanke, *Modern Coding Theory* (Cambridge University Press, 2008).

[29] A. Mizutani, Y. Takeuchi, and K. Tamaki, Phys. Rev. Res. **5**, 023132 (2023), URL https://link.aps.org/doi/10.1103/PhysRevResearch.5.023132.

[30] M. Pereira, G. Currás-Lorenzo, A. Navarrete, A. Mizutani, G. Kato, M. Curty, and K. Tamaki, Phys. Rev. Res. **5**, 023065 (2023), URL https://link.aps.org/doi/10.1103/PhysRevResearch.5.023065.

[31] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, New Journal of Physics **17**, 093011 (2015), URL https://doi.org/10.1088/1367-2630/17/9/093011.

[32] K. Tamaki, H.-K. Lo, A. Mizutani, G. Kato, C. C. W. Lim, K. Azuma, and M. Curty, Quantum Science and Technology **3**, 014002 (2017), URL https://dx.doi.org/10.1088/2058-9565/aa89bd.

[33] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Nature Photonics **9**, 827 (2015), ISSN 1749-4893, URL https://doi.org/10.1038/nphoton.2015.173.

[34] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008), URL https://link.aps.org/doi/10.1103/PhysRevLett.101.093601.

[35] C.-H. F. Fung, H. F. Chau, and H.-K. Lo, Phys. Rev. A **84**, 020303 (2011), URL https://link.aps.org/doi/10.1103/PhysRevA.84.020303.

[36] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus, Phys. Rev. A **89**, 012325 (2014), URL https://link.aps.org/doi/10.1103/PhysRevA.89.012325.

[37] Some theoretical methods are known to bound the decoding failure probability, which equals the correctness parameter; see. e.g., Refs. [27, 28]. However, such methods are not feasible in practical QKD systems, because computationally efficient methods cannot achieve both a high coding rate and a rigorous bound on the decoding failure probability simultaneously, and also because in practical QKD systems, it is almost impossible to precisely characterize the probability distribution of bit errors under arbitrary Eve's attacks.

[38] For example, in Remark 6.3.2 of Ref. [12], the author essentially presents Lemma 1 of the present paper. However, this appears to lead to a logical flaw, as Section 6.3.2 of the same chapter discusses a protocol that uses error verification without making the outcome V public. These papers [29–33] by the present authors also exhibit a similar logical flaw. However, all of them can be corrected by subtracting one extra bit in privacy amplification, as justified by Lemma 3 in this paper.

[39] Footnote [22] of Ref. [19] seems to state that disclosing V does not affect the security of QKD, but it seems to contradict our counterexample given in Sec. III C.

[40] For example, Bob's measurement can be effectively modeled as acting on qubits due to the existence of a squash operator [34–36]. In this case, the effect of the verification can be explicitly incorporated into the security proof. Indeed, a recent security proof of the decoy-state BB84 protocol [17] rigorously addresses this issue using the PEC approach.

[41] Reference [8] fits this situation if one restricts that the universal hash function used for error verification, mentioned at the end of Section 2.2, to be linear (though we failed to say that it should be linear).