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*

(Received 4 August 2025; accepted 10 November 2025; published 2 December 2025)

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 point out that when error verification is performed in a QKD protocol, the definition of secrecy must be revised accordingly. We illustrate the necessity of this revision with a counterexample, showing that neglecting it can lead to an incorrect security claim. In particular, we observe that in the case of the security proof method based on phase error correction, which is one of the mainstream approaches and also known as Koashi's approach, no explicit method has been established to properly incorporate the revised secrecy definition. To resolve this issue, we present a way to translate the phase error correction-based approach into another mainstream approach, called the leftover hash lemma-based approach, also known as Renner's approach, where a solution has already been formulated. As a consequence, security proofs under the phase error correction-based approach automatically remain valid without any change in the secret key length, even if they implicitly consider error verification without revising the secrecy definition.

DOI: 10.1103/3vms-bx5d

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 [14], error verification is widely used [9,10,15–21] 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.

When considering the use of the secret key generated by QKD in subsequent cryptographic applications, we point out that the outcome of error verification, denoted by V, must be publicly announced (see Sec. III A for details). Once this public nature of V is accepted, one can readily conclude that the secrecy parameter must be defined for the state *after* error verification (see Sec. III B for details).

However, security proofs based on the phase-error-correction (PEC) approach [7,22], also known as Koashi's approach, appear to inappropriately treat V as secret information and instead define secrecy for the state *without* error verification [23–29]. This is the core of the problem concerning the treatment of the outcome of error verification, which we identify as the central problem of this paper and refer to as the *verification problem*.

As one of the main contributions of this paper, we demonstrate the serious consequences of this inappropriate definition of secrecy by presenting a counterexample. In this example, a false claim of security can be made under this definition for a state without error verification, even though the claim 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.

It should be noted that Koashi's approach (as summarized in Sec. IV B 1) has been the mainstream method for security proofs (see, for example, Sec. II B 3 of Ref. [2] and Sec. 6.2 of Ref. [30]) and has been applied to a wide variety of QKD protocols, such as round-robin differential-phase-shift (DPS) protocol [27,29,31,32], decoy-state BB84 [33,34], BB84 with an uncharacterized source [35], six-state protocol [36], twin field protocol [18], loss-tolerant protocol [37], DPS protocol

*Contact author: Tsurumaru.toyohiro@da.mitsubishielectric.co.jp
†Contact author: mizutani@eng.u-toyama.ac.jp
‡Contact author: Toshihiko.Sasaki@quantinuum.com

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

[38], and continuous variable protocols [39,40]. Nevertheless, the verification problem persists and leads to a security flaw [23–29]. We also explain in Sec. IV B 1 why this problem is difficult to resolve within the framework of Koashi's approach. Note that even if a protocol does not explicitly describe a verification step, there is no practical way to guarantee correctness other than by employing error verification. Consequently, as long as the security proof relies on Koashi's approach, the verification problem inevitably arises.

Fortunately, in Renner's approach [15], which is another mainstream method for QKD security proofs, the verification problem has already been solved [10]. We discuss this in Sec. IV A. Here, Renner's approach is based on the leftover hash lemma (LHL) [15] for min-entropy, and we can relate the min-entropy of the quantum state after error verification to that without error verification (specifically, by using Lemma 10 in Ref. [10]). As a result, even when the outcome of error verification is publicly revealed, secrecy can still be guaranteed without shortening the key length by even a single bit.

Another main contribution of this paper, in addition to clarifying the verification problem, is that we provide a simple solution to the problem in Koashi's approach. Specifically, we prove that security proofs based on Koashi's approach can always be repaired without reducing the final key length (see Sec. IV B 2 for details). The basic idea is to translate Koashi's approach into Renner's approach by exploiting their equivalence established in Refs. [41,42], thereby resolving the problem within the framework of Renner's approach.

From a future perspective, the widespread adoption of QKD in society requires the standardization of a comprehensive 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.

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 (subnormalized) 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 [43]

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

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 is 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 (PA)—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 subnormalized) state corresponding to the event where the protocol is continued. Then, we say that the QKD protocol is ε-secure if

$$\tfrac{1}{2}\left\|\rho_{K_AK_BE} - \rho^{\mathrm{ideal}}_{K_AK_BE}\right\|_1 \leqslant \varepsilon \tag{2}$$

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

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

where

$$d(\rho_{K_AE}|E) := \tfrac{1}{2}\left\|\rho_{K_AE} - \rho^{\mathrm{ideal}}_{K_AE}\right\|_1, \tag{5}$$

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

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.,

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

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

$$\tfrac{1}{2}\left\|\rho_{K_AK_BE} - \rho^{\mathrm{ideal}}_{K_AK_BE}\right\|_1 \leqslant d(\rho_{K_AE}|E) + \Pr[K_A \neq K_B]. \tag{8}$$

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

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 [44].

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 $\rho^{V=0}_{K_AK_BE}$ (or $\rho^{V=1}_{K_AK_BE}$), 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

$$\tfrac{1}{2}\left\|\rho_{K_AK_BVE} - \rho^{\text{ideal}}_{K_AK_BVE}\right\|_1,$$

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

$$\tfrac{1}{2}\left\|\rho_{K_AK_BVE} - \rho^{\text{ideal}}_{K_AK_BVE}\right\|_1 \leqslant d\left(\rho^{V=0}_{K_AE}|E\right) + \Pr[K_A \neq K_B]. \tag{11}$$

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

$$\begin{aligned}
&\tfrac{1}{2}\left\|\rho_{K_AK_BVE} - \rho^{\text{ideal}}_{K_AK_BVE}\right\|_1 \\
&= \tfrac{1}{2}\sum_{v\in\{0,1\}} \left\|\rho^{V=v}_{K_AK_BE} - \left(\rho^{V=v}_{K_AK_BE}\right)^{\text{ideal}}\right\|_1 \\
&= \tfrac{1}{2}\left\|\rho^{V=0}_{K_AK_BE} - \left(\rho^{V=0}_{K_AK_BE}\right)^{\text{ideal}}\right\|_1 \\
&\leqslant d\left(\rho^{V=0}_{K_AE}|E\right) + \Pr[K_A \neq K_B \wedge V = 0] \\
&= d\left(\rho^{V=0}_{K_AE}|E\right) + \Pr[K_A \neq K_B].
\end{aligned} \tag{12}$$

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 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

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

Although many existing works based on Koashi's approach consider QKD protocols with error verification, they often adopt the LHS of Eq. (8) as the secrecy criterion [23–28], rather than that of Eq. (11), which should be used to properly bound the trace distance in the presence of error verification [45]. 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 Sec. III C that this is not the case in general. 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).

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. 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

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

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

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

(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 (subnormalized) state satisfies

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

Clearly,

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

holds, and the secret keys satisfy 0-correctness.

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

$$\tfrac{1}{2}\|\rho_{K_A K_B E V} - (\rho_{K_A K_B E V})^{\mathrm{ideal}}\|_1 \leqslant d(\rho_{K_A E}|E) + \Pr[K_A \neq K_B] = 0. \tag{19}$$

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

$$\tfrac{1}{2}\|\rho_{K_A K_B E V} - (\rho_{K_A K_B E V})^{\mathrm{ideal}}\|_1 = \tfrac{1}{4}, \tag{20}$$

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

$$d\left(\rho_{K_A E}^{V=0}|E\right) = \tfrac{1}{4}, \tag{21}$$

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.

(1) According to Eq. (14) and the verification procedure, the protocol ensures $k_A = E$ if $V = 0$, and $k_A \neq E$ when $V = 1$.

(2) 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 anticorrelated events ($k_A \neq E$). As a result, the variable k_A appears uniformly distributed, and 0-secrecy holds, as shown in Eq. (16).

(3) 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 PARAMETER WITH ERROR VERIFICATION

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.

However, for both mainstream methods of QKD security proofs, namely Renner's approach and Koashi's approach, we show in Secs. IV A and IV B, respectively, that the verification problem can be resolved. In other words, in both approaches, if secrecy without revealing V, i.e., Eq. (4), is guaranteed, then secrecy with the announcement of V, namely Eq. (13), can also be derived.

For simplicity of presentation, we will describe the case without smoothing. However, the same principles apply straightforwardly when smoothing is included.

A. Solution in Renner's approach

When employing Renner's approach for the security proof, Tomamichel and Leverrier have resolved the verification problem in Ref. [10].

1. Setups and claims

We begin by explaining the setups.

First, in this section, we limit ourselves to the following type of error verification method: After bit error correction, Alice and Bob publicly announce classical information H, which is determined from their reconciled keys A and B. Next, either Alice or Bob decides whether to continue or abort, disclosing the decision variable $V \in \{0, 1\}$, based on H and her (or his) reconciled key (A or B). In other words, the public information H and V can be expressed by some functions f and g as $H = f(A, B)$ and $V = g(H, A)$ or $V = g(H, B)$.

Second, in this paper, by "Renner's approach" [15] we always refer to the situation where (1) the protocol employs a universal$_2$ hash function (or more generally, the almost dual universal$_2$ function [46,47]) for privacy amplification and (2) the leftover hash lemma is used to prove the secrecy of the final key.

Under these setups, if the secrecy without revealing V, as in Eq. (4), has been proven, then the secrecy with V revealed, as in Eq. (13), automatically holds. In other words, among the two secrecy conditions [Eqs. (4) and (13)], it suffices to prove only one of them.

2. Mathematical details

Recall that, within Renner's approach, to prove the secrecy condition in Eq. (4) without revealing V as considered in Sec. II, one usually discusses as follows. After bit error correction, only the public information H is revealed, while V remains hidden, and we consider the state ρ_{ABEH}. Based on the data obtained in the parameter estimation phase, one then proves that the conditional min-entropy satisfies

$$H_{\min}(A|EH)_\rho \geqslant \ell + 2\log_2(1/\varepsilon_{\sec}). \tag{22}$$

The secret key K_A is obtained by applying privacy amplification to the reconciled key A. The state ρ_{K_AEH} of this secret key can then be shown, by the LHL together with Eq. (22), to satisfy

$$d(\rho_{K_AEH}|EH) \leqslant 2^{\frac{1}{2}\left(\ell - H_{\min}(A|EH)_\rho\right)}. \tag{23}$$

Thus, Eq. (4) is established.

Next, we evaluate the secrecy condition in Eq. (13) when V is revealed. This corresponds, by definition, to deriving an upper bound on $d(\rho^{V=0}_{K_AEH}|EH)$.

To this end, let us first note the following. After the state ρ_{ABEH} is generated as described two paragraphs earlier, Alice and Bob compute and reveal $V \in \{0, 1\}$, and denote the resulting state by ρ_{ABEHV}. In this case, the following statements hold.

(1) If Alice applies privacy amplification to the reconciled key A of $\rho_{ABEH} = \mathrm{tr}_V(\rho_{ABEHV})$, one can reproduce the subnormalized state ρ_{K_AEH}, which is employed in the evaluation of the secrecy considered without revealing V, in Eq. (4).

(2) Consider the subnormalized state $\rho^{V=0}_{ABEH}$ obtained by projecting ρ_{ABEHV} onto the case $V = 0$, i.e., $\rho^{V=0}_{ABEH} = \mathrm{tr}_V(\rho_{ABEHV}[0]_V)$. If one then applies privacy amplification to the reconciled key A, the resulting state coincides with the subnormalized state $\rho^{V=0}_{K_AEH}$ used in the evaluation of the secrecy condition in Eq. (13).

In summary, to evaluate the secrecy condition without revealing V, it suffices to apply the LHL using the conditional min-entropy $H_{\min}(A|EH)_\rho$ of ρ_{ABEH}. On the other hand, to evaluate the secrecy condition when V is revealed, one should use the conditional min-entropy $H_{\min}(A|EH)_{\rho^{V=0}}$ of $\rho^{V=0}_{ABEH}$. It is known that the following relation holds between these two conditional min-entropies.

Lemma 3 (Ref. [10], Lemma 10). The conditional min-entropy of (possibly subnormalized) state ρ does not decrease when marginalized by the condition $V = 0$, i.e.,

$$H_{\min}(A|EH)_\rho \leqslant H_{\min}(A|EH)_{\rho^{V=0}}. \tag{24}$$

Thanks to this lemma, as long as Eq. (22) holds,

$$H_{\min}(A|EH)_{\rho^{V=0}} \geqslant \ell + 2\log_2(1/\varepsilon_{\sec}) \tag{25}$$

is satisfied. By applying the LHL to $\rho^{V=0}$, we obtain

$$d\left(\rho^{V=0}_{K_AEH}|EH\right) \leqslant 2^{\frac{1}{2}\left(\ell - H_{\min}(A|EH)_{\rho^{V=0}}\right)}, \tag{26}$$

which shows that Eq. (13) is fulfilled.

3. Proof of Lemma 3

The proof of Lemma 3 is given in Ref. [10], but for the reader's convenience, we provide it here.

Since the projection $[0]_V$ on the space V is a quantum operation,

$$[0]_V \rho_{ABEHV} [0]_V \leqslant \rho_{ABEHV}$$

holds. By tracing out subsystems B and V, we obtain

$$\rho^{V=0}_{AEH} \leqslant \rho_{AEH}. \tag{27}$$

Also note that, by the definition of the conditional min-entropy (see, e.g., Definition 3.1.1 of Ref. [15]), there exists a state σ_{EH} satisfying

$$\rho_{AEH} \leqslant 2^{-H_{\min}(A|EH)_\rho} \mathbb{I}_A \otimes \sigma_{EH}. \tag{28}$$

By combining inequalities (27) and (28), we have

$$\rho^{V=0}_{AEH} \leqslant 2^{-H_{\min}(A|EH)_\rho} \mathbb{I}_A \otimes \sigma_{EH}, \tag{29}$$

which guarantees Eq. (24), again by the definition of the conditional min-entropy.

B. Solution in Koashi's approach

While security proofs based on the phase-error-correction method (PEC-based approach, also known as Koashi's approach [7,22]) have not yet provided a general solution to this verification problem, we describe here a way to address it.

1. Summary of Koashi's approach and the challenge of addressing the verification problem within this framework

Security proofs based on Koashi's approach (in the absence of error verification) typically proceed as follows (see, e.g., Refs. [41,42]).

(1) Let ρ_{AE} denote the sifted key state; that is, the joint state of Alice's sifted key and Eve's system immediately after parameter estimation. Define a virtual pure state $|\rho\rangle_{ABE}$ that equals ρ_{AE} when subsystem A is measured in the bit basis (usually chosen to be the Z basis) and B is traced out [48].

(2) Let ρ_{X^AB} be the *virtual* state, obtained by measuring subsystem A of $|\rho\rangle_{ABE}$ in the phase basis (usually chosen to be the X basis) and tracing out E. Upper-bound the conditional max-entropy $H_{\max}(X^A|B)_\rho$, using the data obtained in the parameter estimation phase.

(3) Suppose that one performs error correction on subsystem X^A in the phase basis, using B as side information. Use $H_{\max}(X^A|B)_\rho$ to obtain an upper bound Q^{EC} on the failure probability of the above phase error correction [50]. Then, the secrecy of Alice's secret key K_A can be given as $d(\rho_{K_AE}|E) \leqslant 2\sqrt{2}\sqrt{Q^{\mathrm{EC}}}$; see, e.g., Refs. [8,41,42]. In other words, the secrecy parameter can be bounded as $\varepsilon_{\sec} \leqslant 2\sqrt{2}\sqrt{Q^{\mathrm{EC}}}$.

As described above, in Koashi's approach, the target state of the security proof is not the state ρ_{ABE} corresponding to the actual QKD protocol, but rather the virtual state $\rho_{X^A B}$ that is mathematically defined from ρ_{ABE}. In this framework, Alice's sifted key A is not defined; instead, the state obtained after measuring in the phase basis is considered. Consequently, the description of the public information H and V is not straightforward (in contrast, in Renner's approach discussed in Sec. IV A, the reconciled keys A and B appear explicitly as classical variables in the state ρ_{ABE} after error correction but before the calculation of H and V, so that the state ρ_{ABEHV} including H and V can be described straightforwardly). This has made it difficult to address the verification problem in Koashi's approach. For example, within this approach it is not clear whether a lemma analogous to Lemma 3 exists. For these reasons, when adopting a security proof based on Koashi's approach, a general solution to the verification problem has not yet been established.

2. Proposed solution

The idea of the solution is to exploit the fact that Step (3) in Sec. IV B 1 is equivalent to the LHL in Renner's approach [41,42]. Using this equivalence, we translate the situation of Step (3) into Renner's approach, and then apply the solution described in Sec. IV A for Renner's approach.

We begin by stating the conclusion, and the mathematical details will be given in the next section.

Our conclusion is the following: Suppose Koashi's approach is applied to a protocol without aborting due to error verification, in the same sense as in Sec. II. Further assume that in Step (2) we obtain the following upper bound on the conditional max-entropy:

$$H_{\max}(X^A|B)_\rho \leqslant H_{\max}^{\mathrm{th}}, \tag{30}$$

where $H_{\max}^{\mathrm{th}}$ is a constant once the parameter estimation phase is completed. If we then add the error-verification procedure of Sec. IV A 1 to the protocol, the secrecy condition with aborting due to error verification

$$d\left(\rho_{K_A EH}^{V=0}\right) \leqslant 2^{\frac{1}{2}(\ell - n + H_{\max}^{\mathrm{th}} + |H|)} \tag{31}$$

holds. Here, $|H|$ denotes the bit length of H.

3. Mathematical details

Once Eq. (30) holds, by an entropic uncertainty relation [51], we obtain a lower bound on the min-entropy $H_{\min}(A|E)_\rho \geqslant n - H_{\max}^{\mathrm{th}}$, and by the chain rule of the conditional min-entropy, Eq. (3.21) in Ref. [15], we have

$$H_{\min}(A|EH)_\rho \geqslant n - H_{\max}^{\mathrm{th}} - |H|. \tag{32}$$

This lower bound can be identified with Eq. (22), by letting $\ell = n - H_{\max}^{\mathrm{th}} - |H| - 2\log_2(1/\varepsilon_{\mathrm{sec}})$. With this, we have completed the translation of Koashi's approach into Renner's approach in Sec. IV A 2. By applying a solution analogous to that in Sec. IV A 2, Eq. (31) can then be established.

V. DISCUSSION

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 [52], 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 [58]. 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 [59].

ACKNOWLEDGMENTS

We thank Kiyoshi Tamaki, Go Kato, and Shun Kawakami for helpful discussions. Also, we are deeply grateful to the anonymous referee for pointing out that, in Renner's approach, the situation where the outcome of error verification is disclosed to Eve has already been incorporated into the security proof in Ref. [10]. A.M. was partially supported by JSPS KAKENHI Grant No. JP24K16977.

DATA AVAILABILITY

No data were created or analyzed in this study.

APPENDIX: 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

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

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 $\varepsilon_{\mathrm{cor}}$ 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 $\lceil \log_2(1/\varepsilon_{\mathrm{cor}}) \rceil$. 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

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

[1] H.-K. Lo, M. Curty, and K. Tamaki, Secure quantum key distribution, Nat. Photon. **8**, 595 (2014).

[2] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, Secure quantum key distribution with realistic devices, Rev. Mod. Phys. **92**, 025002 (2020).

[3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, Advances in quantum cryptography, Adv. Opt. Photon. **12**, 1012 (2020).

[4] C. Portmann and R. Renner, Security in quantum cryptography, Rev. Mod. Phys. **94**, 025008 (2022).

[5] M. Ben-Or, M. Horodecki, D. W. Leung, D. Mayers, and J. Oppenheim, The universal composable security of quantum key distribution, in *Theory of Cryptography*, edited by J. Kilian (Springer, Berlin, 2005), pp. 386–406.

[6] J. Müller-Quade and R. Renner, Composability in quantum cryptography, New J. Phys. **11**, 085006 (2009).

[7] M. Koashi, Simple security proof of quantum key distribution based on complementarity, New J. Phys. **11**, 045018 (2009).

[8] M. Hayashi and T. Tsurumaru, Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths, New J. Phys. **14**, 093014 (2012).

[9] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).

[10] M. Tomamichel and A. Leverrier, A largely self-contained and complete security proof for quantum key distribution, Quantum **1**, 14 (2017).

[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, arXiv:2502.10340.

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

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

[14] Some theoretical methods are known to bound the decoding failure probability, which equals the correctness parameter; see, e.g., Refs. [12,13]. 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.

[15] R. Renner, Security of quantum key distribution, arXiv:quant-ph/0512258.

[16] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Finite-key analysis for measurement-device-independent quantum key distribution, Nat. Commun. **5**, 3732 (2014).

[17] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Concise security bounds for practical decoy-state quantum key distribution, Phys. Rev. A **89**, 022307 (2014).

[18] K. Maeda, T. Sasaki, and M. Koashi, Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit, Nat. Commun. **10**, 3140 (2019).

[19] M. Sandfuchs, M. Haberland, V. Vilasini, and R. Wolf, Security of differential phase shift QKD from relativistic principles, Quantum **9**, 1611 (2025).

[20] A. Mizutani, T. Sasaki, and G. Kato, Protocol-level description and self-contained security proof of decoy-state BB84 QKD protocol, arXiv:2504.20417.

[21] L. Kamin, J. Burniston, and E. Y. Z. Tan, Rényi security framework against coherent attacks applied to decoy-state QKD, arXiv:2504.12248.

[22] M. Koashi, Simple security proof of quantum key distribution via uncertainty principle, arXiv:quant-ph/0505108.

[23] A. Mizutani, Y. Takeuchi, and K. Tamaki, Finite-key security analysis of differential-phase-shift quantum key distribution, Phys. Rev. Res. **5**, 023132 (2023).

[24] M. Pereira, G. Currás-Lorenzo, A. Navarrete, A. Mizutani, G. Kato, M. Curty, and K. Tamaki, Modified BB84 quantum key distribution protocol robust to source imperfections, Phys. Rev. Res. **5**, 023065 (2023).

[25] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, Finite-key security analysis of quantum key distribution with imperfect light sources, New J. Phys. **17**, 093011 (2015).

[26] K. Tamaki, H.-K. Lo, A. Mizutani, G. Kato, C. C. W. Lim, K. Azuma, and M. Curty, Security of quantum key distribution with iterative sifting, Quantum Sci. Technol. **3**, 014002 (2018).

[27] H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, Experimental quantum key distribution without monitoring signal disturbance, Nat. Photon. **9**, 827 (2015).

[28] G. Currás-Lorenzo, A. Navarrete, M. Pereira, and K. Tamaki, Finite-key analysis of loss-tolerant QKD based on random sampling theory, Phys. Rev. A **104**, 012406 (2021).

[29] T. Sasaki, Y. Yamamoto, and M. Koashi, Practical quantum key distribution protocol without monitoring signal disturbance, Nature (London) **509**, 475 (2014).

[30] 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, arXiv:2502.10340.

[31] J.-Y. Guan *et al.*, Experimental passive round-robin differential phase-shift quantum key distribution, Phys. Rev. Lett. **114**, 180502 (2015).

[32] S. Wang *et al.*, Experimental demonstration of a quantum key distribution without signal disturbance monitoring, Nat. Photon. **9**, 832 (2015).

[33] M. Koashi, Efficient quantum key distribution with practical sources and detectors, arXiv:quant-ph/0609180.

[34] M. Hayashi and R. Nakayama, Security analysis of the decoy method with the Bennett-Brassard 1984 protocol for finite key lengths, New J. Phys. **16**, 063009 (2014).

[35] M. Koashi and J. Preskill, Secure quantum key distribution with an uncharacterized source, Phys. Rev. Lett. **90**, 057902 (2003).

[36] G. Kato and K. Tamaki, Security of six-state quantum key distribution protocol with threshold detectors, Sci. Rep. **6**, 30044 (2016).

[37] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Loss-tolerant quantum cryptography with imperfect sources, Phys. Rev. A **90**, 052314 (2014).

[38] A. Mizutani, T. Sasaki, Y. Takeuchi, K. Tamaki, and M. Koashi, Quantum key distribution with simply characterized light sources, npj Quantum Inf. **5**, 87 (2019).

[39] T. Matsuura, K. Maeda, T. Sasaki, and M. Koashi, Finite-size security of continuous-variable quantum key distribution with digital signal processing, Nat. Commun. **12**, 252 (2021).

[40] T. Matsuura, S. Yamano, Y. Kuramochi, T. Sasaki, and M. Koashi, Refined finite-size analysis of binary-modulation continuous-variable quantum key distribution, Quantum **7**, 1095 (2023).

[41] T. Tsurumaru, Leftover hashing from quantum error correction: Unifying the two approaches to the security proof of quantum key distribution, IEEE Trans. Inf. Theory **66**, 3465 (2020).

[42] T. Tsurumaru, Equivalence of three classical algorithms with quantum side information: Privacy amplification, error correction, and data compression, IEEE Trans. Inf. Theory **68**, 1016 (2022).

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

[44] Note that, as mentioned in Sec. II, when the abort decision is determined solely from the public information (for example, when the QBER is disclosed and the protocol is aborted whenever it exceeds a predetermined threshold), then even if the abort/nonabort outcome is publicly announced, no additional sacrifice in privacy amplification is required. In contrast, in the error-verification procedure considered from Sec. III, Alice announces a hash value whereas Bob does not; instead, Bob checks consistency and announces the verification outcome. In this case, the abort decision is not determined solely from the public information, and in principle one must consider the possibility of further shortening the key during privacy amplification. Nevertheless, as explained in Sec. IV, within the security proof based on the leftover hash lemma, no additional sacrifice is required.

[45] We note, however, that all of them can be corrected without increasing the amount of privacy amplification, as justified in Sec. IV B of this paper.

[46] T. Tsurumaru and M. Hayashi, Dual universality of hash functions and its applications to quantum cryptography, IEEE Trans. Inf. Theory **59**, 4700 (2013).

[47] M. Hayashi and T. Tsurumaru, More efficient privacy amplification with less random seeds via dual universal hash function, IEEE Trans. Inf. Theory **62**, 2213 (2016).

[48] Note that subsystem B does not only consist of Bob's system, but also includes any system accessible to Alice. For example, it includes subsystems other than the qubits possessed by Alice, such as the shield system (i.e., the system that purifies Alice's emitted states).

[49] R. Koenig, R. Renner, and C. Schaffner, The operational meaning of min- and max-entropy, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[50] For example, Refs. [42,49] state that $Q^{\mathrm{EC}} \leqslant 2^{H_{\max}(X^A|B)_\rho - (n-\ell)}$ is possible on average.

[51] M. Tomamichel and R. Renner, Uncertainty relation for smooth entropies, Phys. Rev. Lett. **106**, 110506 (2011).

[52] P. W. Shor and J. Preskill, Simple proof of security of the BB84 quantum key distribution protocol, Phys. Rev. Lett. **85**, 441 (2000).

[53] T. Tsurumaru and K. Tamaki, Security proof for QKD systems with threshold detectors, Phys. Rev. A **78**, 032302 (2008).

[54] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Squashing models for optical measurements in quantum communication, Phys. Rev. Lett. **101**, 093601 (2008).

[55] T. Tsurumaru, Squash operator and symmetry, Phys. Rev. A **81**, 012328 (2010).

[56] C.-H. F. Fung, H. F. Chau, and H.-K. Lo, Universal squash model for optical communications using linear optics and threshold detectors, Phys. Rev. A **84**, 020303(R) (2011).

[57] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus, Squashing model for detectors and applications to quantum-key-distribution protocols, Phys. Rev. A **89**, 012325 (2014).

[58] For example, Bob's measurement can be effectively modeled as acting on qubits due to the existence of a squash operator [53–57]. 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 [20] rigorously addresses this issue using the PEC approach.

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