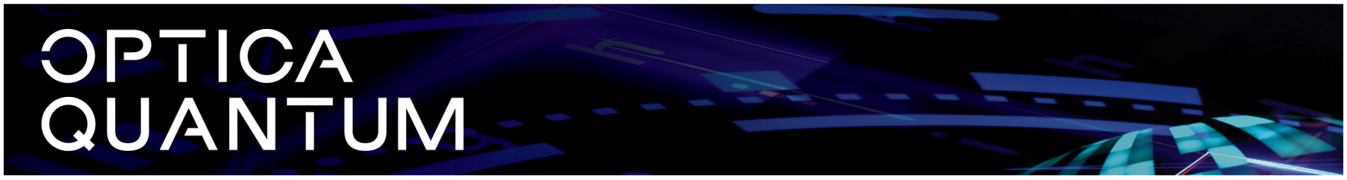
Research Article Vol. 3, No. 6 / 25 December 2025 / Optica Quantum 525



Security framework for quantum key distribution with imperfect sources

Guillermo Currás-Lorenzo,[1,2,3,4,*] Margarida Pereira,[1,2,3,4] Go Kato,[5] Marcos Curty,[2,3,4] and Kiyoshi Tamaki[1]

[1]Faculty of Engineering, University of Toyama, Gofuku 3190, Toyama 930-8555, Japan
[2]Vigo Quantum Communication Center, University of Vigo, Vigo E-36310, Spain
[3]Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain
[4]atlanTTic Research Center, University of Vigo, Vigo E-36310, Spain
[5]National Institute of Information and Communications Technology, Nukui-kita, Koganei, Tokyo 184-8795, Japan
*gcurras@vqcc.uvigo.es

Received 2 June 2025; revised 26 October 2025; accepted 27 October 2025; published 17 November 2025

Imperfect bit-and-basis encoders compromise the security of quantum key distribution (QKD) systems via modulation flaws, side channels, and inter-pulse correlations, which invalidate standard security proofs. Existing results addressing such imperfections suffer from critical limitations: they either consider only specific flaws, offer an unreasonably poor performance, or require the protocol to be run very slowly. Here, we present a finite-key security proof approach against coherent attacks that incorporates general bit-and-basis encoding imperfections (including modulation flaws, side channels, and inter-pulse correlations) while achieving significantly better performances than previous approaches and requiring only partial characterization.

https://doi.org/10.1364/OPTICAQ.569424

1. INTRODUCTION

Quantum key distribution (QKD) can theoretically achieve the Holy Grail of cryptography, unconditional security against eavesdropping. However, in practice, discrepancies between the mathematical models assumed in security proofs and the actual functioning of the devices used in implementations prevent it from reaching this goal. Device-independent QKD [1–3] is currently not a satisfactory solution to this problem, as its performance is extremely poor [4–7] and, in any case, its security proofs assume that the user devices leak absolutely no information to the outside [8,9]. On the other hand, measurement-device-independent (MDI) QKD [10] provides a practical approach to guarantee security with arbitrarily flawed receivers while achieving high performance. Thus, the remaining challenge is ensuring the security of QKD with imperfect sources, such as sources that suffer from imperfections and side channels in the encoding of bit-and-basis information.

So far, all efforts in this regard [11–16] have come at a price; some proofs are suitable only for particular encoding imperfections such as qubit flaws [14], while others severely compromise the system's performance, i.e., its repetition rate [15–18] and maximum achievable distance [11–13] (see Section 3). Here, we overcome these crucial problems by presenting a security proof in the finite-key regime against coherent attacks that can incorporate bit-and-basis encoding imperfections and side channels while achieving much higher performances than previous approaches. Our approach unifies ideas from the quantum coin [11–13] and loss-tolerant [14] security analyses in a way that naturally preserves their respective advantages—including their validity against the most general attacks allowed by quantum mechanics without any sequential restrictions—while overcoming their respective limitations. Moreover, our proof requires only partial state characterization, which facilitates its application to real-life implementations.

2. RESULTS

2.1. Partial State Characterization Assumption

For ease of discussion, in the main text, we present our security proof approach by considering its application to an imperfect BB84 [19] protocol; in Supplement 1, we provide a general description of our approach and explicitly show how to apply it to other schemes. More precisely, here we consider that, in each round k, the sender (Alice) probabilistically selects a setting $j \in \{0_Z, 1_Z, 0_X, 1_X\}$ and sends a signal in the state $\rho_j^{(k)}$ to the receiver (Bob). The states $\rho_j^{(k)}$ are partially characterized: they are known to be ϵ-close (in terms of fidelity) to some characterized states $\{|\phi_j\rangle_B\}_j$, i.e.,

$$\langle\phi_j|\,\rho_j^{(k)}\,|\phi_j\rangle_B \geq 1-\epsilon, \tag{1}$$

for known $0 \leq \epsilon \leq 1$, which could more generally depend on j. In this discussion, for concreteness, we will assume that $\{|\phi_j\rangle_B\}_j$ is

any set of qubit states, including flawed versions of the eigenstates $|j\rangle_B$ of the Pauli operators. We remark, however, that $\{|\phi_j\rangle_B\}_j$ could more generally be *any* set of characterized states (see Section 4 of Appendix A).

We refer to the deviation between $|\phi_j\rangle_B$ and $|j\rangle_B$ as the qubit flaw, and to the deviation between $\rho_j^{(k)}$ and $|\phi_j\rangle_B$ as the side channel. Equation (1) is general in that it is not necessary to specify the cause for a non-zero ϵ; it can cover *any* kind of practical passive information leakage, such as those due to mode dependencies [20–22], electromagnetic or acoustic radiation [23], or power consumption [24]; and *any* kind of practical active information leakage, such as those due to Trojan-horse attacks (THAs) [15,16,25–27]. The partial state characterization assumed by our security proof is useful because some imperfections could in principle live in arbitrarily high-dimensional spaces, making it extremely challenging to fully characterize them in practice.

In our main text discussion, for concreteness, we will consider that the emitted states are pure, and we will not mark their possible dependence on the round k, i.e., we will assume that $\rho_j^{(k)} = |\psi_j\rangle\langle\psi_j|_B$. However, we remark that our security proof is directly applicable even if the emitted states are mixed and/or different for different rounds k, as long as Eq. (1) holds (see Section 1 of Appendix A). We also remark that our security proof is applicable even if the emitted states are correlated, although in this case, one needs to consider a modification to Eq. (1) and to the post-processing step of the protocol (see Section 3 of Appendix A).

Due to Eq. (1), the emitted states $|\psi_j\rangle_B$, which we denote by $|\psi_j(\epsilon_j)\rangle_B$ hereafter, can be expressed as [15]:

$$|\psi_j(\epsilon_j)\rangle_B = \sqrt{1-\epsilon_j}\,|\phi_j\rangle_B + \sqrt{\epsilon_j}\,|\phi_j^{\perp}\rangle_B, \tag{2}$$

which is simply a state expansion in the basis $\{|\phi_j\rangle_B, |\phi_j^{\perp}\rangle_B\}$. Here, $0 \le \epsilon_j \le \epsilon$, and $|\phi_j^{\perp}\rangle_B$ could be *any* state orthogonal to $|\phi_j\rangle_B$, which implies that $\{|\psi_j(\epsilon_j)\rangle_B\}_j$ could be linearly independent when $\epsilon \neq 0$. Importantly, this fact makes the system inherently vulnerable to channel loss, as Eve could exploit it to enhance the distinguishability of the emitted states caused by the side channels. For example, she could perform an unambiguous state discrimination (USD) [28] measurement and ensure that conclusive (inconclusive) events result (do not result) in detections. This implies that, if ϵ and the observed channel loss are high enough, Eve could have learned Alice's setting choices for all detected rounds without introducing any errors, and no security proof can provide a positive key rate. On the other hand, qubit flaws do not cause this vulnerability, as in their presence $\{|\psi_j(0)\rangle_B\}_j$ remain linearly dependent, and there is no USD measurement for linearly dependent qubit states.

Side channels and qubit flaws are thus qualitatively different, and to achieve the best possible performance, security proofs should treat them differently. However, so far, no security proof achieves this satisfactorily. The loss-tolerant (LT) analysis [14] deals with qubit flaws tightly, and in fact shows that they have almost no impact on the secret-key rate, but cannot be applied in the presence of side channels, i.e., when $\epsilon > 0$. Conversely, the quantum coin analysis [11–13] can be applied in the presence of both qubit flaws and side channels, but does not take into account their qualitative difference, and thus offers an extremely pessimistic performance for the former. Meanwhile, recent attempts to combine the strengths of both analyses, such as the reference technique (RT) [16] (see also [15]), require an additional sequential assumption [17,25,29] that restricts the repetition rate at which the protocol can be run, severely reducing the secret-key rate obtainable in practice.

2.2. Security Analysis

Here, we introduce a security proof approach that solves all these drawbacks. To illustrate how, in this discussion, we consider a particular instance in which the qubit components can be expressed as:

$$|\psi_j(0)\rangle_B = |\phi_j\rangle_B = \cos(\theta_j)\,|0_Z\rangle_B + \sin(\theta_j)\,|1_Z\rangle_B, \tag{3}$$

where $\theta_j = (1+\delta/\pi)\varphi_j/2$, $\varphi_j \in \{0, \pi, \pi/2, 3\pi/2\}$ for $j \in \{0_Z, 1_Z, 0_X, 1_X\}$, and $\delta \in [0, \pi)$ represents the magnitude of the qubit flaws. We emphasize that this is just a specific example for illustration purposes, and that our general security proof, presented in Supplement 1, can be applied regardless of the specific form of the states $\{|\phi_j\rangle_B\}_j$. Moreover, without loss of generality (see Supplement 1), we consider that $\epsilon_j = \epsilon$ for all j. The sifted key is generated from the detected key rounds, i.e., the rounds in which both Alice and Bob select the Z basis and Bob obtains a bit value. In these rounds, instead of emitting $|\psi_{0_Z}(\epsilon)\rangle_B$ and $|\psi_{1_Z}(\epsilon)\rangle_B$ randomly, Alice could have generated the entangled state,

$$|\Psi_Z(\epsilon)\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0_Z\rangle_A\,|\psi_{0_Z}(\epsilon)\rangle_B + |1_Z\rangle_A\,|\psi_{1_Z}(\epsilon)\rangle_B\right), \tag{4}$$

and measured the ancillary system A in the Z basis. The amount of privacy amplification that needs to be applied to turn the sifted key into a secret key is directly related to the phase-error rate e_{ph}, which is defined as the error rate that Alice and Bob would have observed if, in the detected key rounds, Alice had measured system A in the X basis (X_A), complementary to the Z basis, and Bob had used his actual X-basis measurement (X_B). This is the case for security proofs based on the leftover hashing lemma with the entropic uncertainty relation [30–34], and for those based on phase-error correction [13,35–37], which have been shown to be essentially equivalent [38].

The phase-error rate cannot be observed directly, and the goal of the security proof is to estimate it using the data obtained in the experiment. A common approach is to use the observed X-basis bit-error rate e_X. By noting that Alice could have replaced her X-basis emissions by the generation of

$$|\Psi_X(\epsilon)\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0_X\rangle_A\,|\psi_{0_X}(\epsilon)\rangle_B - |1_X\rangle_A\,|\psi_{1_X}(\epsilon)\rangle_B\right), \tag{5}$$

one can define e_{ph} and e_X as the error rates associated to the measurement of X_A and X_B on the detected rounds in which Alice prepares $|\Psi_Z(\epsilon)\rangle_{AB}$ and $|\Psi_X(\epsilon)\rangle_{AB}$, respectively. If δ and ϵ are close to zero, $|\Psi_Z(\epsilon)\rangle_{AB}$ and $|\Psi_X(\epsilon)\rangle_{AB}$ are close to each other, implying that e_{ph} and e_X should also be relatively similar. This intuition was formalized in [11–13] by introducing the quantum coin state,

$$\frac{1}{\sqrt{2}}\left(|0_Z\rangle_C\,|\Psi_Z(\epsilon)\rangle_{AB} + |1_Z\rangle_C\,|\Psi_X(\epsilon)\rangle_{AB}\right), \tag{6}$$

and then considering that Alice probabilistically selects one of the complementary bases Z_C or X_C to measure the coin C. In particular, these works showed that the deviation between e_{ph} and e_X can be bounded by a function of the fraction of events in which Alice obtained $X_C = 1$ amongst the detected events in which she selected X_C. Of course, since in the real protocol Alice's coin is actually classical, this fraction cannot be observed. Instead, it can be upper bounded by considering the a priori probability that Alice obtains $X_C = 1$, given by $\frac{1}{2}(1 - \text{Re}\langle\Psi_Z(\epsilon)|\Psi_X(\epsilon)\rangle_{AB})$, and assuming the worst-case scenario in which all events such that $X_C = 1$ are detected. However, the need to assume this scenario leads to a bound on e_{ph} whose tightness deteriorates as the channel loss increases. The speed at which this occurs depends on the probability to obtain $X_C = 1$, which grows with both δ and ϵ. In the case of ϵ, this behavior is expected, as the effect of the side channels can be enhanced by Eve in the presence of loss. However, as previously discussed, this is not the case for qubit flaws, leading to a very loose bound when $\delta > 0$. The solution to this limitation is the key to our security proof, and to understand it, it is helpful to first review the LT analysis, which is tight for $\delta > 0$ but only valid when $\epsilon = 0$.

The main idea of the LT analysis is to consider the state resulting from the measurement of X_A on $|\Psi_Z(0)\rangle_{AB}$ by re-expressing $|\Psi_Z(0)\rangle_{AB} = \sqrt{1-q_0}\,|0_X\rangle_A\,|\psi_{\text{vir}0}(0)\rangle_B + \sqrt{q_0}\,|1_X\rangle_A\,|\psi_{\text{vir}1}(0)\rangle_B$ with $q_0 = \frac{1}{2}(1 - \text{Re}\langle\psi_{0_Z}(0)|\psi_{1_Z}(0)\rangle_B)$; we call $|\psi_{\text{vir}\beta}(0)\rangle_B$ ($\beta \in \{0,1\}$) the virtual states. That is, Alice emits $|\psi_{\text{vir}0}(0)\rangle_B$ ($|\psi_{\text{vir}1}(0)\rangle_B$) with probability $1-q_0$ (q_0), and the estimation of the phase-error rate is reduced to the task of estimating the X_B detection statistics of these virtual states. By using the fact that when $\epsilon = 0$ the emitted states are qubit states, one can always find an operator form a linear relationship between the actual states and the virtual states. We remark that these linear relationships can always be derived regardless of the form of the qubit states $\{|\psi_j(0)\rangle_B\}_j$; the general procedure to do so can be found in [39, Appendix B] and is discussed in our Supplement 1. When the qubit states have the particular form in Eq. (3), one such linear relationship is given by:

$$|\psi_{\text{vir}0}(0)\rangle\langle\psi_{\text{vir}0}(0)|_B = |\psi_{0_X}(0)\rangle\langle\psi_{0_X}(0)|_B, \tag{7}$$

$$\begin{aligned} &c_1\,|\psi_{0_Z}(0)\rangle\langle\psi_{0_Z}(0)|_B + |\psi_{\text{vir}1}(0)\rangle\langle\psi_{\text{vir}1}(0)|_B \\ &= c_2\,|\psi_{1_Z}(0)\rangle\langle\psi_{1_Z}(0)|_B + c_3\,|\psi_{1_X}(0)\rangle\langle\psi_{1_X}(0)|_B, \end{aligned} \tag{8}$$

where

$$\begin{aligned} c_1 &:= \frac{\cos(\kappa\pi/2)}{\cos(\kappa\pi) - \cos(\kappa\pi/2)}, \\ c_2 &:= \frac{\cos(\kappa\pi/2)}{\cos(\kappa\pi/2) - 1}, \\ c_3 &:= \frac{1 + \cos(\kappa\pi/2)}{\cos(\kappa\pi/2) - \cos(\kappa\pi)}, \end{aligned} \tag{9}$$

with $\kappa = 1 + \delta/\pi$. The existence of such linear relationships implies that the X_B detection statistics of the virtual states can be determined *exactly* using the observed X_B detection statistics of the actual states, including basis-mismatched events. As a result, the LT analysis allows a tight estimation of e_{ph} even in the presence of high loss, and offers a key rate that is almost independent of δ when $\epsilon = 0$.

The key idea of our proof to extend this behavior to the case $\epsilon > 0$ is to combine the quantum coin analysis and the LT analysis through the notion of the target and reference states introduced by the RT [16]. Note that, when $\epsilon > 0$, the relationships in Eqs. (7) and (8) do not hold exactly, but do still hold approximately if $\epsilon \approx 0$, irrespectively of the value of δ. We use this fact to construct a quantum coin state for which the probability to obtain $X_C = 1$ is almost independent of δ.

First of all, rather than considering $|\Psi_Z(\epsilon)\rangle_{AB}$, which is a purification of a convex combination of $|\psi_{\text{vir}0}(\epsilon)\rangle\langle\psi_{\text{vir}0}(\epsilon)|_B$ and $|\psi_{\text{vir}1}(\epsilon)\rangle\langle\psi_{\text{vir}1}(\epsilon)|_B$ taken according to the probabilities $1-q_\epsilon$ and $q_\epsilon = \frac{1}{2}(1 - \text{Re}\langle\psi_{0_Z}(\epsilon)|\psi_{1_Z}(\epsilon)\rangle_B)$; we consider instead a purification of a convex combination of the LHS of Eqs. (7) and (8) taken according to these probabilities (followed by normalization), i.e.,

$$\begin{aligned} |\Psi_{\text{Tar}}(\epsilon)\rangle_{DAB} = \frac{1}{\sqrt{1+c_1 q_\epsilon}}\Big[&\sqrt{1-q_\epsilon}\,|0\rangle_D\,|0\rangle_A\,|\psi_{\text{vir}0}(\epsilon)\rangle_B \\ &+ \sqrt{q_\epsilon}\,|1\rangle_D\,(\sqrt{c_1}\,|0\rangle_A\,|\psi_{0_Z}(\epsilon)\rangle_B + |1\rangle_A\,|\psi_{\text{vir}1}(\epsilon)\rangle_B)\Big]. \end{aligned} \tag{10}$$

Then, we define the target statistics as the error rate associated to the measurement $\{|0\rangle_D, |1\rangle_D\}$ and X_B on the detected rounds after Eve's attack, i.e., the statistics of the outcomes $(|0\rangle_D, X_B = 1)$ and $(|1\rangle_D, X_B = 0)$. Note that, since this measurement commutes with the measurement $\{|0\rangle_A, |1\rangle_A\}$, the target statistics can be regarded as a mixture of the phase-error statistics and the statistics of the events in which Alice emits $|\psi_{0_Z}(\epsilon)\rangle_B$ and Bob obtains $X_B = 0$, with the latter being observed in the actual protocol. Therefore, if we can estimate the overall target statistics, we can estimate the phase-error rate.

To do so, we consider a purification of a similar convex combination of the RHS of Eqs. (7) and (8), i.e.,

$$\begin{aligned} |\Psi_{\text{Ref}}(\epsilon)\rangle_{DAB} = \frac{1}{\sqrt{1+c_1 q_\epsilon}}\Big[&\sqrt{1-q_\epsilon}\,|0\rangle_D\,|0\rangle_A\,|\psi_{0_X}(\epsilon)\rangle_B \\ &+ \sqrt{q_\epsilon}\,|1\rangle_D\,(\sqrt{c_2}\,|0'\rangle_A\,|\psi_{1_Z}(\epsilon)\rangle_B + \sqrt{c_3}\,|1'\rangle_A\,|\psi_{1_X}(\epsilon)\rangle_B)\Big], \end{aligned} \tag{11}$$

where the orthonormal basis $\{|0'\rangle_A, |1'\rangle_A\}$ has been chosen such that $|\Psi_{\text{Tar}}(0)\rangle_{DAB} = |\Psi_{\text{Ref}}(0)\rangle_{DAB}$, which is always possible due to the equality in Eq. (8). As before, we define the reference statistics as the error rate of the measurement $\{|0\rangle_D, |1\rangle_D\}$ and X_B on the detected rounds after Eve's attack. Since this measurement commutes with the measurement $\{|0'\rangle_A, |1'\rangle_A\}$, the reference statistics can be regarded as a mixture of the statistics of the events in which Alice emits $|\psi_{0_X}(\epsilon)\rangle_B$ and Bob obtains $X_B = 1$, and the events in which Alice emits $|\psi_{1_Z}(\epsilon)\rangle_B$ or $|\psi_{1_X}(\epsilon)\rangle_B$ and Bob obtains $X_B = 0$, all of which are observed. In other words, the reference statistics can be determined using the data acquired in the actual protocol.

Finally, we define the loss-tolerant quantum coin state as:

$$\begin{aligned} &|\Psi_{\text{LTcoin}}(\epsilon)\rangle_{CDAB} \\ &= \frac{1}{\sqrt{2}}(\,|0_Z\rangle_C\,|\Psi_{\text{Tar}}(\epsilon)\rangle_{DAB} + |1_Z\rangle_C\,|\Psi_{\text{Ref}}(\epsilon)\rangle_{DAB}\,), \end{aligned} \tag{12}$$

and bound the deviation between the target and reference statistics by considering the probability to obtain $X_C = 1$, given by $\frac{1}{2}(1 - \text{Re}\langle\Psi_{\text{Tar}}(\epsilon)|\Psi_{\text{Ref}}(\epsilon)\rangle_{DAB})$. When $\delta > 0$, the resulting bound on the phase-error rate is much tighter than in the original quantum coin analysis, since $\text{Re}\langle\Psi_{\text{Tar}}(\epsilon)|\Psi_{\text{Ref}}(\epsilon)\rangle_{DAB}$ is almost independent of δ, while $\text{Re}\langle\Psi_Z(\epsilon)|\Psi_X(\epsilon)\rangle_{DAB}$ decreases rapidly as δ increases.

To turn the above argument into a full security proof against general attacks, there remains a loose end to tie up. Unlike in the original quantum coin analysis, it is not possible to assume here that Alice replaces her actual source by the generation of Eq. (12) in all rounds, since the statistics of Alice's source differ in general from those of Eq. (12). Instead, we consider that Alice randomly samples her emissions, where the sampling probabilities depend on her emitted state and are chosen such that a sampled emission is equivalent to that originating from Eq. (12). As shown in Supplement 1, this allows us to apply the above analysis to estimate the number of phase errors within the sampled rounds, and then extend this estimate to all rounds via known statistical results, thus obtaining a bound on the overall phase-error rate that is valid even in the finite-key regime. We note that the proof merely relies on the idea that Alice *could* in principle sample her emissions; in the actual experiment, however, Alice does not actually need to perform this sampling step, nor to decide which sampled rounds correspond to measuring the quantum coin in the Z_C or X_C bases. The latter is another improvement over the original quantum coin analysis, which requires Alice to actually assign each round of the protocol to either the Z_C or X_C basis, and discard the data of the rounds assigned to X_C [40].

A critical advantage of our security proof is that it allows the protocol to be run at high repetition rates, unlike some previous approaches that address source imperfections. In particular, the RT [16], while sharing many of the advantages of our approach (including the ability to incorporate side channels and resilience to qubit flaws), requires the assumption that the probability that Alice selects a particular bit-and-basis choice in round k must be independent of Bob's previous $k-1$ measurement outcomes. This independence condition can only be guaranteed if Eve's attack is sequential, that is, if she is prevented from correlating Bob's measurement outcomes with Alice's setting choices in later rounds. In practice, enforcing this sequential condition requires running the protocol slowly such that Alice's emitted pulses could not possibly have influenced Bob's previous outcomes, even if Eve wanted to correlate them.

In contrast, our security proof directly guarantees security against the most general attacks allowed by quantum mechanics without any sequential restrictions, thus enabling high-speed operation. The key technical insight is that our proof is based on bounding the deviation between the reference and target statistics by considering that Alice generates the quantum coin state in Eq. (12), and then deriving a quantum coin inequality through the application of the Bloch sphere bound to each coin system C. To derive this inequality, we consider that Eve performs a coherent attack on all rounds simultaneously, after which Bob performs basis-independent quantum non-demolition measurements to determine which rounds are detected, and then Alice and Bob measure the systems corresponding to the detected rounds. Crucially, the coin system C corresponding to any particular detected round k always remains a qubit system, even when conditioning on Eve's global attack, on Bob's detection outcomes for all rounds, and on all of Alice's and Bob's previous measurement outcomes in detected rounds 1 through $k-1$. As a result, we obtain a quantum coin inequality that relates the expectation values for the outcomes on round k conditional on any outcomes in rounds 1 through $k-1$. We then apply concentration inequalities such as Azuma's inequality or Kato's inequality [41] to relate the conditional expectations to the actual statistics observed in the protocol. Importantly, all our proof steps hold regardless of any correlations Eve might introduce between rounds.

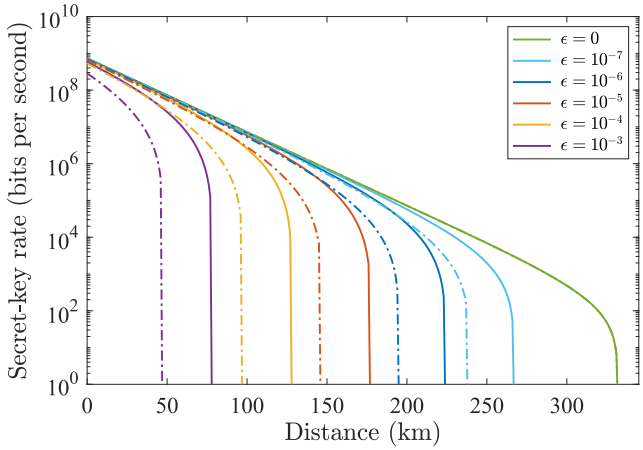


Fig. 1. Asymptotic secret-key rate obtainable using our proof as a function of the distance (km) for the BB84 (solid lines) and three-state (dashed-dotted lines) protocols. We assume $\delta = 0.063$ [21,44] and consider several values of ϵ.

We remark that, while in this section we have focused on the prepare-and-measure BB84 protocol for clarity, our security proof approach is broadly applicable to other QKD protocols as well. For example, it can be directly extended to standard MDI-QKD [10]. Since MDI-QKD eliminates all detector side channels while our proof addresses transmitter imperfections, combining these approaches enables security against both source and measurement-device imperfections. The extension to MDI-QKD follows naturally because the bit-and-basis encoding imperfections at each transmitter can be incorporated using the same loss-tolerant quantum coin technique described above. Furthermore, our approach can be applied to other protocols, including three-state protocols and even an MDI-type protocol in which the users send non-phase-randomized coherent states [26], demonstrating the versatility of our techniques. For the full analysis of these scenarios, see Supplement 1.

3. DISCUSSION

Now, we apply our loss-tolerant quantum coin analysis to evaluate the secret-key rate obtainable for BB84-type protocols in the presence of both qubit flaws and side channels, and discuss our findings by drawing a comparison with previous analyses. For the simulations, we assume the following parameters: error correction inefficiency $f = 1.16$, detector dark count probability $p_d = 10^{-8}$ [9,42], detector efficiency $\eta_d = 0.73$ [42], and a repetition rate of 2.5 GHz [43].

In Fig. 1, we plot the achievable secret-key rate in bits per second for both the BB84 and three-state protocols when using our analysis. We consider $\delta = 0.063$, following the experimental results reported in [21,44], and several values of ϵ. For both protocols, the key rate is sensitive to the value of ϵ, which is expected, as higher values of ϵ make it easier for Eve to discriminate the emitted states in the presence of channel loss. When $\epsilon = 0$, both protocols offer the same secret-key rate, as already known [14]. However, consistently with previous results [25], we find that, for $\epsilon > 0$, the additional state emitted in the BB84 protocol results in a tighter phase-error rate estimation, which translates to higher key rates.

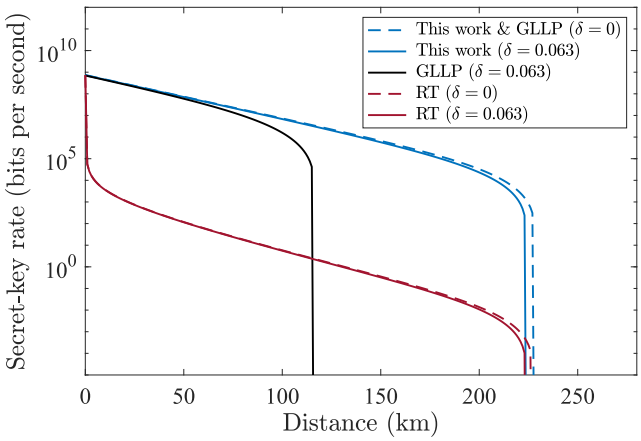


Fig. 2. Asymptotic secret-key rate obtainable using our proof as a function of the distance (km) for the BB84 protocol, compared with that of the original quantum coin (GLLP) [11–13] and reference technique (RT) [16,25] analyses. We consider the values $\epsilon = 10^{-6}$ and $\delta \in \{0, 0.063\}$.

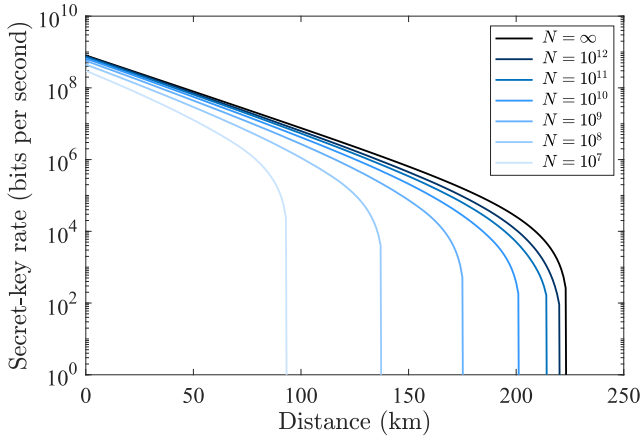


Fig. 3. Finite-size secret-key rate against general attacks obtainable using our proof as a function of the total number of emitted pulses N. We consider the BB84 protocol, $\epsilon = 10^{-6}$, $\delta = 0.063$, and we set the correctness and secrecy parameters of the final key to $\epsilon_{\text{corr}} = \epsilon_{\text{secr}} = 10^{-10}$.

In Fig. 2, we compare the secret-key rate obtainable using our proof with that of the original quantum coin analysis [11–13] and the RT analysis [16,25]. We consider the BB84 protocol, since the original quantum coin analysis cannot provide any key for the three-state protocol. Also, we fix $\epsilon = 10^{-6}$, and consider the presence ($\delta = 0.063$) and absence ($\delta = 0$) of qubit flaws. When there are no qubit flaws, our proof converges to the original quantum coin analysis. However, in their presence, the secret-key rate offered by our proof decreases only very slightly, while that of the original quantum coin analysis decreases dramatically. As already mentioned, applying the RT requires running the protocol sequentially, which limits the repetition rate. Therefore, for the RT, rather than using 2.5 GHz, we determine the maximum repetition rate under the restriction that Alice only emits a pulse after Bob has finished his measurement of the previous pulse. For this calculation, we assume a standard fiber in which photons travel at about 2/3 of the speed of light [45]. As can be seen in Fig. 2, this significantly restricts the secret-key rate achievable using the RT after the first few kilometers. We note that this sequential condition, which is also imposed by security proofs based on the generalized entropy accumulation theorem [17,29], is not required by our security proof, as discussed in Section II.B. In Supplement 1, we explain at length why this is the case.

In Figs. 1 and 2, we have assumed the asymptotic regime in which the total number of emitted pulses, N, approaches infinity. However, our security proof can be applied to secure practical QKD implementations with a finite N. In Fig. 3, we show the achievable secret-key rate for several values of this parameter. For large N, the performance approaches that of the asymptotic regime.

4. CONCLUSION

We have introduced a security proof approach that can ensure the finite-key security of QKD protocols against the most general attacks allowed by quantum mechanics (i.e., coherent attacks) in the presence of bit-and-basis encoding imperfections. As Fig. 2 demonstrates, our analysis achieves significantly higher secret-key rates than previous results in the presence of both side channels and qubit flaws, guaranteeing the security of practical QKD setups without compromising their performance. Moreover, it does not need any characterization of the side channels, other than an upper bound on their overall magnitude. Importantly, when applied to the BB84 protocol, the asymptotic performance of our security proof is essentially optimal given its partial characterization assumptions [46].

While our security proof represents a significant advance in addressing implementation imperfections while relaxing the need for full characterization, several important challenges remain for achieving truly secure QKD in practice. On the experimental front, accurately determining the parameter ϵ that bounds the magnitude of side channels remains a difficult task. Real QKD systems may suffer from multiple side channels simultaneously—including mode dependencies, setting-dependent correlations, electromagnetic radiation, acoustic emissions, power consumption variations, and susceptibility to Trojan-horse attacks—each requiring careful characterization, and new unexpected side channels are still being discovered [22]. The total ϵ must account for all these leakage channels combined, and obtaining tight bounds requires sophisticated measurement techniques with very high accuracy and extremely low noise. Furthermore, as we have shown, if ϵ is too large, the system becomes vulnerable to USD attacks that can completely compromise security. This places stringent requirements on experimental implementations to minimize side-channel leakage through careful engineering, shielding, and isolation techniques. Modulator-free [47] and passive QKD [48,49] represent a promising approach to eliminate the side channels introduced by active components, and our techniques have been adapted to incorporate residual side channels in such setups [50].

On the theoretical front, while our proof addresses bit-and-basis encoding imperfections, extending it to simultaneously handle imperfections in decoy-state implementations remains an open challenge. Decoy-state QKD is crucial for practical implementations using weak coherent pulses, but decoy-state modulators can introduce their own side channels (including correlations in intensity modulation and phase randomization) that are not fully covered by our current analysis. Although we

discuss in Supplement 1 how our techniques could potentially be extended to address some of these issues, and simple imperfections like intensity fluctuations can be readily incorporated, a comprehensive treatment of general decoy-state imperfections—particularly in the finite-key regime—requires further theoretical development.

Despite these challenges, the techniques we have developed demonstrate considerable flexibility and broad applicability. While we have focused on the prepare-and-measure BB84 protocol for clarity in the main text, our security proof approach can be extended to many other QKD protocols. For example, it can be applied to MDI-QKD [10]. Since MDI-QKD eliminates all detector side channels while our proof addresses transmitter imperfections, combining these approaches enables security against both source and measurement-device imperfections. The extension to MDI-QKD follows naturally because the bit-and-basis encoding imperfections at each transmitter can be incorporated using the same loss-tolerant quantum coin technique. Furthermore, our approach can be applied to other protocols, including three-state protocols and even an MDI-type protocol in which the users send non-phase-randomized coherent states [26], demonstrating the versatility of our techniques (see Appendix A and Supplement 1 for detailed analyses of these scenarios). Moreover, as shown in [51], our security proof can be combined with the result in [34] to incorporate also detection efficiency mismatches in Bob's setup, going beyond previous attempts at simultaneously addressing source and detector imperfections [52,53] in terms of generality and applicability in the finite-key regime. Beyond QKD, our techniques may also prove useful for other information-theoretic tasks in which information leakage must be addressed.

In short, we believe this work represents an important step toward bridging the gap between the theoretical promise of unconditional security and the practical reality of QKD implementations.

APPENDIX A: METHODS

1. Mixed and Non-Identically Distributed States

Our analysis directly applies even if the emitted states ρ_j are mixed. To see why, note that, if Eq. (1) holds, by Uhlmann's theorem, there must exist a purification $|\psi_j\rangle_{BS}$ of ρ_j such that

$$|\langle\phi_j|\psi_j\rangle_{BS}|^2 = \langle\phi_j|\,\rho_j\,|\phi_j\rangle_B \geq 1-\epsilon, \tag{A1}$$

where we have defined $|\phi_j\rangle_{BS} := |\phi_j\rangle_B|0\rangle_S$. This implies that our analysis for pure states can be directly applied to the mixed state case simply by substituting $|\psi_j\rangle_B \to |\psi_j\rangle_{BS}$ and $|\phi_j\rangle_B \to |\phi_j\rangle_{BS}$ throughout.

Also, our security proof can be applied without any modification even if the emitted states $\rho_j^{(k)}$ are different for different rounds k, as long as Eq. (1) holds for all rounds. Note that, in this case, the target and reference states $|\Psi_{\mathrm{Tar}}^{(k)}(\epsilon)\rangle$ and $|\Psi_{\mathrm{Ref}}^{(k)}(\epsilon)\rangle$, and thus also the quantum coin state $|\Psi_{\mathrm{LTcoin}}^{(k)}(\epsilon)\rangle$, depend on the round k. However, this is not a problem since one can use exactly the same procedure as in the case of identically distributed states to find a lower bound on $\mathrm{Re}\langle\Psi_{\mathrm{Ref}}^{(k)}(\epsilon)|\Psi_{\mathrm{Tar}}^{(k)}(\epsilon)\rangle$ that holds for all rounds k, and apply our security proof as is.

2. Determining the Value of ϵ

Any device used in a communication system can leak partial information about its internal settings to the channel. This means that any cryptosystem, including device-independent QKD [1–3], necessarily requires a degree of characterization of such potential side channels to guarantee security. For this characterization, our security proof requires only a bound on the overall combined magnitude of all side channels — the parameter ϵ. That is, unlike other security proofs (e.g., [54]), we do not need any state characterization of the side channels, which might be impossible to obtain in practice. Remarkably, this means that our proof could serve as a guideline to secure the source while significantly relaxing the need for detailed characterization. While obtaining a rigorous bound on ϵ for a given implementation is a non-trivial experimental problem that is outside the scope of this work, here, we discuss how one could combine information about various side channels in order to obtain a value for ϵ.

One critical side channel is that caused by a THA, in which Eve injects light into Alice's source and then measures the back-reflected light to learn information about Alice's setting choice. The amount of leaked information can be related to the intensity of the back-reflected light, $\mu_{\mathrm{out}} = \gamma\,\mu_{\mathrm{in}}$, where μ_{in} is the intensity of the injected light, and γ represents the optical isolation of the transmitting unit. In particular, it is straightforward to show that the back-reflected light can be expressed as:

$$|\xi_j\rangle_E = \sqrt{1-\epsilon_j}\,|v\rangle_E + \sqrt{\epsilon_j}\,|\Omega_j\rangle_E, \tag{A2}$$

where $\epsilon_j \leq \mu_{\mathrm{out}}$ [25]. Here, $|v\rangle_E$ is a vacuum state independent of Alice's setting j, and $|\Omega_j\rangle_E$ is a non-vacuum state that can in general depend on j. It has been argued [54] that, for any given implementation, one can determine a threshold $\mu_{\mathrm{in}}^{\mathrm{U}}$ above which the injected light is very likely to damage the optical components of Alice's source and be detected. Based on this, one can obtain a bound $\mu_{\mathrm{out}}^{\mathrm{U}} := \gamma\,\mu_{\mathrm{in}}^{\mathrm{U}}$ that can be reduced by adjusting the optical isolation γ. If Eve's THA is the only side channel present, the emitted states are $\{|\phi_j\rangle_B \otimes |\xi_j\rangle_E\}_j$, where $\{|\phi_j\rangle_B\}_j$ are qubit states. Therefore, we can apply our proof by considering the set of qubit states $\{|\phi_j\rangle_B \otimes |v\rangle_E\}_j$ and setting $\epsilon = \epsilon_{\mathrm{THA}} := \mu_{\mathrm{out}}^{\mathrm{U}}$. Note that, unlike other analyses [54], our proof does not need any assumption on Eve's injected light, such as it being a coherent state, other than a bound on its intensity.

Beyond THAs, Alice's source may also passively leak information through unwanted modes. For example, consider polarization mode dependencies in phase-encoding setups. While the encoded pulses should ideally maintain constant polarization (e.g., horizontal), imperfect alignment between laser and phase modulator can cause the polarization to depend slightly on the setting choice j. The generated pulse then becomes,

$$|\psi_j\rangle_B = \sqrt{1-\epsilon_j'}\,|\phi_j\rangle_{B_h}|v\rangle_{B_v} + \sqrt{\epsilon_j'}\,|v\rangle_{B_h}|\phi_j\rangle_{B_v}, \tag{A3}$$

where B_h (B_v) denotes the horizontally (vertically) polarized mode. While the exact values of $\{\epsilon_j'\}_j$ may fluctuate, obtaining an upper bound $\epsilon_j' \leq \epsilon_{\mathrm{MD}}$ should be experimentally feasible. If necessary, its value may be reduced using countermeasures such as polarizing beam splitters. In the presence of both the THA and the polarization mode dependencies, the emitted states are $\{|\psi_j\rangle_B|\xi_j\rangle_E\}_j$, and one can apply our analysis by defining the

qubit states $\{|\phi_j\rangle_{B_h}|\nu\rangle_{B_v}|\nu\rangle_E\}_j$, which satisfy,

$$\left|{}_{B_h}\langle\phi_j|\,{}_{B_v}\langle\nu|\,{}_E\langle\nu|\,|\psi_j\rangle_B|\xi_j\rangle_E\right|^2 \le \epsilon, \tag{A4}$$

where $\epsilon := 1-(1-\epsilon_{\mathrm{THA}})(1-\epsilon_{\mathrm{MD}}) \le \epsilon_{\mathrm{THA}}+\epsilon_{\mathrm{MD}}$. That is, the magnitudes of the side channels simply combine additively. Other forms of information leakage, such as electromagnetic/acoustic radiation, or temporal/spectral/spatial mode dependencies, can also be written in the form of Eqs. (A2) and (A3), and thus their individual magnitudes also contribute additively towards the overall ϵ. Pulse correlations can also be essentially regarded as a form of information leakage and incorporated into ϵ in this way (see below).

Based on all the above, we consider the following to be a promising approach: (1) identify the principal source side channels affecting a particular implementation; (2) obtain an upper bound on their magnitude; (3) if necessary, apply countermeasures to reduce this magnitude; and (4) sum all the individual upper bounds. Side channels that are too small to be precisely quantified could be accounted for by conservatively increasing ϵ.

3. Pulse Correlations

Pulse correlations are a special type of side channel that occurs when the state emitted in the k-th round, denoted as $|\psi_{j_k|j_{k-1},j_{k-2},\ldots,j_{k-l_c}}\rangle_{B_k}$, depends not only on the k-th setting choice j_k, but also on the previous l_c setting choices $j_{k-1},j_{k-2},\ldots,j_{k-l_c}$, where l_c denotes the maximum correlation length. In this case, these states should satisfy,

$$\left|\left\langle\phi_{j_k}\middle|\psi_{j_k|j_{k-1},j_{k-2},\ldots,j_{k-l_c}}\right\rangle_{B_k}\right|^2 \ge 1-\epsilon_{\mathrm{qubit}}, \tag{A5}$$

and

$$\left|\left\langle\psi_{j_k|j_{k-1},\ldots,\tilde{j}_{k-l},\ldots,j_{k-l_c}}\middle|\psi_{j_k|j_{k-1},\ldots,j_{k-l},\ldots,j_{k-l_c}}\right\rangle_{B_k}\right|^2 \ge 1-\epsilon_l, \tag{A6}$$

where $\{|\phi_j\rangle_{B_k}\}_j$ is a set of known qubit states, $l\in\{1,\ldots,l_c\}$, and $\tilde{j}_{k-l}$ is a setting choice that differs from j_{k-l}. Then, one can apply our security proof by setting:

$$\epsilon = 1-(1-\epsilon_{\mathrm{qubit}})(1-\epsilon_{\mathrm{correl}}) \le \epsilon_{\mathrm{qubit}}+\epsilon_{\mathrm{correl}} \tag{A7}$$

where

$$\epsilon_{\mathrm{correl}} := 1-\prod_{l=1}^{l_c}(1-\epsilon_l) \le \sum_{l=1}^{l_c}\epsilon_l. \tag{A8}$$

Also, one needs to divide the protocol rounds into (l_c+1) groups according to the value of $k(l_c+1)$, and apply post-processing separately for each group [16,25,27]. While this does not affect the asymptotic key rate, it can have an impact in the finite-key regime, as the blocksize is effectively reduced from N to $N/(l_c+1)$ rounds. Also, although this discussion implicitly assumes a finite maximum correlation length l_c, our security proof can also be applied when the correlations have an unbounded length, as recently shown in [55] (see also [56]). For more details, see Supplement 1.

4. A More General Form of Eq. (1)

In the main text, we have assumed that the emitted states $\rho_j^{(k)}$ are close in fidelity to some known qubit states $\{|\phi_j\rangle_B\}_j$, see Eq. (1). However, our security proof can be applied under a more general assumption; namely,

$$\langle\tilde{\phi}_j|\rho_j^{(k)}|\tilde{\phi}_j\rangle_B \ge 1-\epsilon, \tag{A9}$$

where $\{|\tilde{\phi}_j\rangle_B\}_j$ are *any* characterized states, not necessarily qubits. This is because, in our analysis, the fictitious qubit states $\{|\phi_j\rangle_B\}_j$ only serve as a blueprint to appropriately define the states $|\Psi_{\mathrm{Tar}}\rangle_{DAB}$ and $|\Psi_{\mathrm{Ref}}\rangle_{DAB}$. The secret-key rate obtainable primarily depends on $\mathrm{Re}\langle\Psi_{\mathrm{Tar}}|\Psi_{\mathrm{Ref}}\rangle_{DAB}$, which is a linear combination of the inner products $\mathrm{Re}\langle\psi_{j'}|\psi_j\rangle_B\ \forall j,j'$. Although these inner products are not known precisely, in Supplement 1, we show that, for any $\{|\tilde{\phi}_j\rangle_B\}_j$, the problem of finding the minimum value of $\mathrm{Re}\langle\Psi_{\mathrm{Tar}}|\Psi_{\mathrm{Ref}}\rangle_{DAB}$ that is consistent with Eq. (A9) reduces to a numerically solvable semidefinite program. Our numerical simulations focus on the case $|\tilde{\phi}_j\rangle_B = |\phi_j\rangle_B$, for which Eq. (9) becomes Eq. (1). As explained in Section 2 of Appendix A, this corresponds to minimal side-channel characterization, in which one knows only the overall magnitude of the side channels, but has no information on their specific form. While this minimal requirement is a key strength of our proof, given the experimental challenges of obtaining precise side-channel characterization, our proof is not *only* applicable in this scenario. Namely, if one is able to obtain a partial characterization of some side channels, one could include this information into the definition of the states $\{|\tilde{\phi}_j\rangle_B\}_j$. This would generally improve the bound on $\mathrm{Re}\langle\Psi_{\mathrm{Tar}}|\Psi_{\mathrm{Ref}}\rangle_{DAB}$, potentially resulting in a significant performance improvement for many practical side channels.

5. Characterizing Qubit Flaws

In addition to ϵ, the proof also requires knowledge of the qubit states $\{|\phi_j\rangle\}_j$, which can be acquired by testing the source. Methods to characterize this imperfection have been proposed and implemented, see e.g., [21,57]. In practice, these characterization tests could be subject to small inaccuracies. The simplest way to take these into account would be to incorporate any deviation between the estimated $\{|\phi_j\rangle\}_j$ and the actual qubit components of the emitted states into the parameter ϵ. However, this is in general pessimistic, since Eve cannot enhance the effect of this deviation in the presence of loss.

A tighter approach would be to define $\{|\phi_j\rangle\}_j$ as the actual qubit components of the emitted states. This requires a slight modification to our security proof, as the states $\{|\phi_j\rangle\}_j$ would no longer be fully characterized. Consequently, the coefficients in Eqs. (7) and (8), which appear in the definition of the target and reference states in Eqs. (10) and (11), are no longer known precisely. However, as shown in [25], one can calculate the maximum possible range for these coefficients and find the worst-case scenario within those ranges. For more information on this approach, we refer the reader to [25].

6. Protection against Detector Imperfections Side Channels

Our security proof is designed to protect QKD implementations from source imperfections. When applied to BB84—or other prepare-and-measure (PM) scenarios—our security proof's only

requirement for Bob's measurement is that it satisfies the basis-independent detection efficiency condition, i.e., that the probability that he obtains a successful bit outcome is independent of his choice of basis. While this requirement relaxes the need for an exact characterization of Bob's setup and can tolerate certain imperfections (such as the measurement bases not being mutually unbiased), it is still a stringent condition that is only met in practice if all of Bob's detectors have the same efficiency. However, we remark that, as recently shown in [51], our security proof can be readily combined with the result in [34] to incorporate detection efficiency mismatches.

Still, detector control attacks [58–61] constitute a significant threat to the security of BB84 and other PM protocols, and no solution at the security proof level is known to comprehensively deal with these [8,9]. That being said, our approach is compatible with MDI-QKD [10], which eliminates all detector-related security vulnerabilities by delegating measurements to an untrusted intermediary node. When applied to MDI protocols, our analysis secures both Alice's and Bob's sources against general imperfections, providing robust protection against both source and detector side channels. For details on applying our security proof to MDI-type protocols, see Supplement 1.

7. Weak Coherent Sources

Our security proof can also be applied when the users emit intensity-modulated phase-randomized weak coherent pulses, rather than single photons. In this case, assuming ideal intensity modulation and phase randomization, the emitted signals can be regarded as a statistical mixture of photon-number states, and our proof is directly applicable to obtain a bound on the number of phase errors within the single-photon events. The quantities needed to evaluate this bound are not directly observable, since the users do not know which events correspond to single photons. Nevertheless, one can simply obtain bounds for these quantities using the decoy-state method [62–64].

For decoy-state QKD protocols, our security proof can directly incorporate general imperfections and side-channels in the bit-and-basis encoder, which addresses a major practical security concern. Our proof can also straightforwardly incorporate fluctuations in the intensity modulation, since in their presence the emitted states can still be regarded as a mixture of photon-number states. For scenarios with imperfect intensity modulation (beyond simple fluctuations) and/or imperfect phase randomization, additional considerations are needed since the emitted signals may no longer be perfectly described as a statistical mixture of photon-number states independent of the intensity choice. As explained in Supplement 1, the techniques introduced in our work could find applications in incorporating such decoy imperfections into security proofs while considering the finite-key regime and general attacks. This represents a promising research avenue, since previous works addressing such imperfections [65–71] have considered the asymptotic regime and/or collective attacks.

An alternative approach to circumvent the security vulnerabilities associated with these imperfections is the MDI-type protocol proposed in [26], which employs coherent light but requires neither intensity modulation nor phase randomization. Our security analysis is directly compatible with this protocol and offers significant enhancements in both security and performance compared with its original security proof [26] based on the RT [16]. In particular, while the original proof is only valid against sequential attacks, ours can defend against the most general attacks allowed by quantum mechanics. The combination of our approach with this protocol constitutes a practical solution that offers an unprecedented level of implementation security and performance. For more details, including a comprehensive security analysis and numerical results, see Supplement 1.

8. Choice of Target and Reference States

We note that Eqs. (10) and (11) are not the only possible choice for $|\Psi_{\mathrm{Tar}}(\epsilon)\rangle_{DAB}$ and $|\Psi_{\mathrm{Ref}}(\epsilon)\rangle_{DAB}$. Essentially, these states need to satisfy two conditions: (1) when $\epsilon = 0$, $|\Psi_{\mathrm{Tar}}(0)\rangle_{DAB} = |\Psi_{\mathrm{Ref}}(0)\rangle_{DAB}$, as this ensures the resilience of the phase-error rate bound against qubit flaws; (2) the coefficient of the state $|\psi_{\mathrm{vir0}}(\epsilon)\rangle_B$ ($|\psi_{\mathrm{vir1}}(\epsilon)\rangle_B$) inside $|\Psi_{\mathrm{Tar}}(\epsilon)\rangle_{DAB}$ should be proportional to $\sqrt{1-q_\epsilon}$ ($\sqrt{q_\epsilon}$), as in $|\Psi_Z(\epsilon)\rangle_{AB}$, which is needed to ensure that phase errors are correctly defined. To compute the results in Figs. 1, 2 and 3, we have used a slightly different choice of target and reference states than that in Eqs. (10) and (11). The reason why this different choice is advantageous is explained in Supplement 1.

9. Comparison with Side-Channel-Secure QKD

Both our work and side-channel-secure (SCS) QKD [72] aim to address source imperfections in QKD systems, but they take fundamentally different approaches. The main idea behind SCS-QKD is to design a variant of twin-field QKD [73] that is inherently immune to mode dependencies by having each user send only two states: a vacuum state and a non-vacuum state. Since the vacuum state is "mode independent," the protocol becomes immune to mode dependencies in the sense that, regardless of which mode the non-vacuum state occupies, this does not allow Eve to better distinguish between the two states. However, despite its name, SCS-QKD is not immune to other side channels that leak key information through systems different from the intended signal, such as unintended electromagnetic radiation, back-reflected light due to Trojan-horse attacks, or correlations between consecutive pulses.

Recently, a refined version of the protocol was proposed [74] to address a limitation of the original proposal—the requirement to generate perfect vacuum states—by demanding only a lower bound on the fidelity between the two emitted states. Although this is not discussed in [74], we believe this new assumption could be exploited to incorporate side channels beyond mode dependencies (including pulse correlations through the approach described in Section 3 of Appendix A) after bounding their overall magnitude, by introducing a parameter ϵ as in our work. Thus, certain aspects of our work, such as our state characterization (see Section 2 of Appendix A), may be relevant for SCS-QKD as well.

A limitation of SCS-QKD is that its key idea is fundamentally restricted to protocol designs where each user sends only two different states. In contrast, our work develops general techniques to incorporate source imperfections into security proofs of QKD and is thus broader in scope. Our state characterization can incorporate general imperfections directly into the state used in the security proof, making it highly useful for the security analysis of the QKD protocol in general. Although we focus mainly on BB84-type protocols, in Supplement 1, we demonstrate the versatility of our techniques by applying them

to an MDI-type scenario in which the users send non-phase-randomized coherent states [26]. This latter scenario differs from SCS-QKD mainly in that three states are emitted rather than two, and thus the approach we take to prove security is necessarily different.

Funding. Japan Society for the Promotion of Science (JSPS) KAKENHI (23K25793, 23H01096); Galician Regional Government (consolidation of Research Units: AtlantTIC); Spanish Ministry of Economy and Competitiveness (MINECO); Fondo Europeo de Desarrollo Regional (FEDER) (2024-162270OB-I00); Ministerio de Ciencia e Innovación (MICIN) with funding from European Union NextGenerationEU (PRTR-C17.I1) and the Galician Regional Government with own funding through the "Planes Complementarios de I+D+I con las Comunidades Autónomas" in Quantum Communication; "Hub Nacional de Excelencia en Comunicaciones Cuanticas" funded by the Spanish Ministry for Digital Transformation and the Public Service and the European Union NextGenerationEU; European Union Horizon Europe Framework Programme under Marie Skłodowska-Curie (101072637, Project QSI); Quantum Secure Networks Partnership (QSNP) Project (101114043); European Union via the European Health and Digital Executive Agency (HADEA) under the Project QuTechSpace (101135225); European Union's Horizon Europe research and innovation programme under the Marie Skłodowska-Curie Postdoctoral Fellowship grant agreement (101149523).

Acknowledgment. We thank Koji Azuma, Akihiro Mizutani, Álvaro Navarrete, and Víctor Zapatero for valuable discussions.

G.C.-L. and M.P. acknowledge support from JSPS Postdoctoral Fellowships for Research in Japan. G.K. acknowledges support from JSPS Kakenhi (C) No.20K03779 and 21K03388. K.T. acknowledges support from JSPS KAKENHI grant numbers JP18H05237 and JST-CREST JPMJCR 1671.

G.C.-L. identified the need for the research project, and K.T. conceived the fundamental idea behind the security proof, with help from all the authors. K.T., G.C.-L., and M.P. developed the majority of the security proof, with contributions from G.K. and M.C. M.P., and G.C.-L. performed the calculations and the numerical simulations. G.C.-L., M.P., and K.T. wrote the manuscript, and all the authors contributed towards improving it and checking the validity of the results.

Disclosures. The authors declare no competing interests.

Data availability. All data generated and analyzed during this study are available from the corresponding author on reasonable request.

Supplemental document. See Supplement 1 for supporting content.

REFERENCES

1. D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," in *39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)* (1998), pp. 503–509.
2. J. Barrett, L. Hardy, and A. Kent, "No signaling and quantum key distribution," Phys. Rev. Lett. **95**, 010503 (2005).
3. A. Acín, N. Brunner, N. Gisin, *et al.*, "Device-independent security of quantum cryptography against collective attacks," Phys. Rev. Lett. **98**, 230501 (2007).
4. D. P. Nadlinger, P. Drmota, B. C. Nichol, *et al.*, "Experimental quantum key distribution certified by bell's theorem," Nature **607**, 682–686 (2022).
5. W. Zhang, T. van Leent, K. Redeker, *et al.*, "A device-independent quantum key distribution system for distant users," Nature **607**, 687–691 (2022).
6. W.-Z. Liu, Y.-Z. Zhang, Y.-Z. Zhen, *et al.*, "Toward a photonic demonstration of device-independent quantum key distribution," Phys. Rev. Lett. **129**, 050502 (2022).
7. V. Zapatero, T. van Leent, R. Arnon-Friedman, *et al.*, "Advances in device-independent quantum key distribution," NPJ Quantum Inf. **9**, 1 (2023).
8. V. Zapatero, Á. Navarrete, and M. Curty, "Implementation security in quantum key distribution," Adv. Quantum Technol. **7**, 2300380 (2023).
9. F. Xu, X. Ma, Q. Zhang, *et al.*, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. **92**, 025002 (2020).
10. H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. **108**, 130503 (2012).
11. D. Gottesman, H.-K. Lo, N. Lütkenhaus, *et al.*, "Security of quantum key distribution with imperfect devices," Quantum Inf. Comput. **4**, 325–360 (2004).
12. H.-K. Lo and J. Preskill, "Security of quantum key distribution using weak coherent states with nonrandom phases, quantum," Quantum Inform. Comput. **7**, 431–458 (2007).
13. M. Koashi, "Simple security proof of quantum key distribution based on complementarity," New J. Phys. **11**, 045018 (2009).
14. K. Tamaki, M. Curty, G. Kato, *et al.*, "Loss-tolerant quantum cryptography with imperfect sources," Phys. Rev. A **90**, 052314 (2014).
15. M. Pereira, M. Curty, and K. Tamaki, "Quantum key distribution with flawed and leaky sources," NPJ Quantum Inf. **5**, 62 (2019).
16. M. Pereira, G. Kato, A. Mizutani, *et al.*, "Quantum key distribution with correlated sources," Sci. Adv. **6**, eaaz4487 (2020).
17. T. Metger and R. Renner, "Security of quantum key distribution from generalised entropy accumulation," Nat Commun. **14**, 5272 (2023).
18. M. Sandfuchs, M. Haberland, V. Vilasini, *et al.*, "Security of differential phase shift QKD from relativistic principles," Quantum **9**, 1611 (2025).
19. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (1984), pp. 175–179.
20. S. Nauerth, M. Fürst, T. Schmitt-Manderbach, *et al.*, "Information leakage via side channels in freespace BB84 quantum cryptography," New J. Phys. **11**, 065001 (2009).
21. F. Xu, K. Wei, S. Sajeed, *et al.*, "Experimental quantum key distribution with source flaws," Phys. Rev. A **92**, 032305 (2015).
22. A. Gnanapandithan, L. Qian, and H.-K. Lo, "Hidden multidimensional modulation side channels in quantum protocols," Phys. Rev. Lett. **134**, 130802 (2025).
23. K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in *Cryptographic Hardware and Embedded Systems—CHES 2001*, Lecture Notes in Computer Science, Ç. K. Koç, D. Naccache, and C. Paar, eds. (Springer, 2001), pp. 251–261.
24. P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology—CRYPTO '99*, Lecture Notes in Computer Science, M. Wiener, ed. (Springer, 1999), pp. 388–397.
25. M. Pereira, G. Currás-Lorenzo, Á. Navarrete, *et al.*, "Modified BB84 quantum key distribution protocol robust to source imperfections," Phys. Rev. Res. **5**, 023065 (2023).
26. Á. Navarrete, M. Pereira, M. Curty, *et al.*, "Practical quantum key distribution that is secure against side channels," Phys. Rev. Appl. **15**, 034072 (2021).
27. A. Mizutani and G. Kato, "Security of round-robin differential-phase-shift quantum-key-distribution protocol with correlated light sources," Phys. Rev. A **104**, 062611 (2021).
28. I. D. Ivanovic, "How to differentiate between non-orthogonal states," Phys. Lett. A **123**, 257–259 (1987).
29. M. Sandfuchs, M. Haberland, V. Vilasini, *et al.*, "Security of differential phase shift QKD from relativistic principles," arXiv (2023).
30. R. Renner, "Security of quantum key distribution," Ph.D. thesis (ETH Zurich, 2005).
31. M. Tomamichel and R. Renner, "Uncertainty relation for smooth entropies," Phys. Rev. Lett. **106**, 110506 (2011).
32. M. Tomamichel, C. C. W. Lim, N. Gisin, *et al.*, "Tight finite-key analysis for quantum cryptography," Nat Commun. **3**, 634 (2012).
33. G. Currás-Lorenzo, Á. Navarrete, K. Azuma, *et al.*, "Tight finite-key security for twin-field quantum key distribution," NPJ Quantum Inf. **7**, 22 (2021).
34. D. Tupkary, S. Nahar, P. Sinha, *et al.*, "Phase error rate estimation in QKD with imperfect detectors," arXiv (2024).

35. D. Mayers, "Quantum key distribution and string oblivious transfer in noisy channels," in *Advances in Cryptology—CRYPTO '96*, N. Koblitz, ed. (Springer, 1996), pp. 343–357.
36. P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. **85**, 441–444 (2000).
37. 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).
38. 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).
39. G. Currás-Lorenzo, Á. Navarrete, M. Pereira, *et al.*, "Finite-key analysis of loss-tolerant quantum key distribution based on random sampling theory," Phys. Rev. A **104**, 012406 (2021b).
40. W. Wang, K. Tamaki, and M. Curty, "Finite-key security analysis for quantum key distribution with leaky sources," New J. Phys. **20**, 083027 (2018).
41. G. Kato, "Concentration inequality using unconfirmed knowledge," arXiv (2020).
42. M. Pittaluga, M. Minder, M. Lucamarini, *et al.*, "600-km repeater-like quantum communications with dual-band stabilization," Nat. Photon. **15**, 530–535 (2021).
43. A. Boaron, G. Boso, D. Rusca, *et al.*, "Secure quantum key distribution over 421 km of optical fiber," Phys. Rev. Lett. **121**, 190502 (2018).
44. T. Honjo, K. Inoue, and H. Takahashi, "Differential-phase-shift quantum key distribution experiment with a planar light-wave circuit Mach–Zehnder interferometer," Opt. Lett. **29**, 2797–2799 (2004).
45. G. P. Agrawal, *Fiber-Optic Communication Systems* (John Wiley Sons, 2021).
46. G. Currás-Lorenzo, Á. Navarrete, J. Núñez-Bon, *et al.*, "Numerical security analysis for quantum key distribution with partial state characterization," Quantum Sci. Technol. **10**, 035031 (2025).
47. T. K. Paraïso, I. De Marco, T. Roger, *et al.*, "A modulator-free quantum key distribution transmitter chip," NPJ Quantum Inf. **5**, 42 (2019).
48. W. Wang, R. Wang, C. Hu, *et al.*, "Fully passive quantum key distribution," Phys. Rev. Lett. **130**, 220801 (2023).
49. V. Zapatero, W. Wang, and M. Curty, "A fully passive transmitter for decoy-state quantum key distribution," Quantum Sci. Technol. **8**, 025014 (2023).
50. Á. Navarrete, V. Zapatero, and M. Curty, "Security of practical modulator-free quantum key distribution," arXiv (2024).
51. G. Currás-Lorenzo, M. Pereira, S. Nahar, *et al.*, "Security of quantum key distribution with source and detector imperfections through phase-error estimation," arXiv (2025).
52. S. Sun and F. Xu, "Security of quantum key distribution with source and detection imperfections," New J. Phys. **23**, 023011 (2021).
53. A. Marcomini, A. Mizutani, F. Grünenfelder, *et al.*, "Loss-tolerant quantum key distribution with detection efficiency mismatch," arXiv (2024).
54. M. Lucamarini, I. Choi, M. B. Ward, *et al.*, "Practical security bounds against the Trojan-Horse attack in quantum key distribution," Phys. Rev. X **5**, 031030 (2015).
55. M. Pereira, G. Currás-Lorenzo, A. Mizutani, *et al.*, "Quantum key distribution with unbounded pulse correlations," Quantum Sci. Technol. **10**, 015001 (2025).
56. A. Agulleiro, F. Grünenfelder, M. Pereira, *et al.*, "Modeling and characterization of arbitrary order pulse correlations for quantum key distribution," arXiv (2025).
57. A. Huang, A. Mizutani, H.-K. Lo, *et al.*, "Characterization of state-preparation uncertainty in quantum key distribution," Phys. Rev. Appl. **19**, 014048 (2023).
58. L. Lydersen, C. Wiechers, C. Wittmann, *et al.*, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nature Photon. **4**, 686–689 (2010).
59. I. Gerhardt, Q. Liu, A. Lamas-Linares, *et al.*, "Full-field implementation of a perfect eavesdropper on a quantum cryptography system," Nat Commun. **2**, 349 (2011).
60. V. Makarov, "Controlling passively quenched single photon detectors by bright light," New J. Phys. **11**, 065003 (2009).
61. C. Wiechers, L. Lydersen, C. Wittmann, *et al.*, "After-gate attack on a quantum cryptosystem," New J. Phys. **13**, 013043 (2011).
62. W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," Phys. Rev. Lett. **91**, 057901 (2003).
63. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
64. X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
65. K. Tamaki, M. Curty, and M. Lucamarini, "Decoy-state quantum key distribution with a leaky source," New J. Phys. **18**, 065008 (2016).
66. V. Zapatero, Á. Navarrete, K. Tamaki, *et al.*, "Security of quantum key distribution with intensity correlations," Quantum **5**, 602 (2021).
67. X. Sixto, V. Zapatero, and M. Curty, "Security of Decoy-state quantum key distribution with correlated intensity fluctuations," Phys. Rev. Appl. **18**, 044069 (2022).
68. G. Currás-Lorenzo, S. Nahar, N. Lütkenhaus, *et al.*, "Security of quantum key distribution with imperfect phase randomisation," Quantum Sci. Technol. **9**, 015025 (2024).
69. S. Nahar, T. Upadhyaya, and N. Lütkenhaus, "Imperfect phase randomization and generalized decoy-state quantum key distribution," Phys. Rev. Appl. **20**, 064031 (2023).
70. X. Sixto, G. Currás-Lorenzo, K. Tamaki, *et al.*, "Secret key rate bounds for quantum key distribution with faulty active phase randomization," EPJ Quantum Technol. **10**, 53 (2023).
71. X. Sixto, Á. Navarrete, M. Pereira, *et al.*, "Quantum key distribution with imperfectly isolated devices," Quantum Sci. Technol. **10**, 035034 (2025).
72. X.-B. Wang, X.-L. Hu, and Z.-W. Yu, "Practical long-distance side-channel-free quantum key distribution," Phys. Rev. Appl. **12**, 054034 (2019).
73. M. Lucamarini, Z. Yuan, J. Dynes, *et al.*, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400–403 (2018).
74. C. Jiang, X.-L. Hu, Z.-W. Yu, *et al.*, "Side-channel security of practical quantum key distribution," Phys. Rev. Res. **6**, 013266 (2024).