Letter

Phase-error-estimation security framework for quantum key distribution with correlated sources

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

[1] *Vigo Quantum Communication Center, University of Vigo, E-36310 Vigo, Spain*

[2] *Escuela de Ingeniería de Telecomunicación, Department of Signal Theory and Communications, University of Vigo, E-36310 Vigo, Spain*

[3] *atlanTTic Research Center, University of Vigo, E-36310 Vigo, Spain*

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

(Received 15 January 2026; accepted 10 August 2026; published 15 September 2026)

Practical quantum key distribution (QKD) modulators introduce correlations between consecutively emitted pulses due to bandwidth limitations, violating key assumptions underlying many security proof techniques. Here, we address this problem by introducing a simple yet powerful mathematical framework to directly extend phase-error-estimation-based security proofs for imperfect but uncorrelated sources to also incorporate encoding correlations. Our framework overcomes important limitations of previous approaches in terms of generality and rigor, significantly narrowing the gap between theoretical security guarantees and real-world QKD implementations.

DOI: 10.1103/tkx1-23xz

Introduction. Quantum key distribution (QKD) promises information-theoretically secure communications by exploiting fundamental quantum mechanical principles. However, a central challenge in practical QKD is rigorously accounting for device imperfections that inevitably arise in real systems. While security proofs have been developed to handle various imperfections [1–11], encoding correlations—which arise naturally from the limited bandwidth of optical modulators [12,13] and cause each emitted quantum state to depend on setting choices from previous rounds—remain particularly challenging to incorporate within existing security frameworks. These correlations fundamentally violate key assumptions underlying several popular security proof techniques such as the Postselection Technique [14,15], Quantum de Finetti approaches [16], and the marginal-constrained entropy accumulation theorem (MEAT) [9,17], invalidating their application to realistic QKD setups that inevitably suffer from such correlations [18].

On the other hand, security proofs based on phase-error estimation—including both proofs based on entropic uncertainty relations (EUR) with the leftover hashing lemma (LHL) [19–21] and proofs based on phase-error correction (PEC) [22]—face no fundamental barriers to incorporating encoding correlations, as we rigorously establish in this work. Nevertheless, such correlations significantly complicate the phase-error-estimation task and were largely overlooked until a key conceptual breakthrough was introduced by Ref. [5]. To illustrate the key idea, consider the simplest case of nearest-neighbor correlations. From the perspective of the kth pulse, these correlations manifest in two ways: (1) the photonic system of round k depends on the setting choice made in round $(k-1)$ and (2) the setting choice in round k affects the encoding of the photonic pulse in round $(k+1)$. The crucial insight of Ref. [5] is that effect (1) resembles an encoding flaw, while effect (2) is analogous to information leakage through a side-channel system.

Building on this insight, Ref. [5] (see also Refs. [6,23,24]) shows how security proofs capable of handling encoding flaws and side-channel leakage can be adapted to incorporate encoding correlations. The approach partitions rounds into (l_c+1) groups according to k mod (l_c+1), where l_c is the maximum correlation length, and treats each group as an independent subprotocol. For instance, with nearest-neighbor correlations $(l_c=1)$, rounds are split into even and odd groups, and a phase-error-rate bound for the odd-rounds key is established by conditioning on fixed values of the even-rounds' settings. Then, these works argue that, since this bound holds for any fixed values of the even-rounds' settings, the resulting security proof for the odd-rounds key remains valid regardless of the value of the even-rounds key. Applying the same argument to the even-rounds key, the security of the full key then follows from composing the two individual proofs.

While this approach represents the only known method to incorporate encoding correlations into phase-error-estimation-based proofs to date, it suffers from several limitations that reduce its practical usefulness:

(1) *Privacy amplification complexity*. It requires that privacy amplification is performed separately for the (l_c+1) subkeys. This increases implementation complexity and introduces potential failure points.

(2) *Composability concerns*. Despite attempts to formalize the composability arguments needed to combine the security proofs for the individual subprotocols [23], the validity of this composition remains contested, with a recent work

*Contact author: gcurras@vqcc.uvigo.es

explicitly labeling it a "conjecture" [9]. This concern is also reflected in a recent review paper that classifies phase-error-estimation-based proofs as robust only against independent device imperfections (see Table III of Ref. [25]).

(3) *Protocol specificity.* Previous works consider specific protocols and security proofs on a case-by-case basis, without providing a fully general mathematical framework to address correlations across protocols.

In this work, we overcome these challenges by constructing a rigorous and general framework to extend phase-error-estimation-based security proofs to correlated sources in a systematic way, addressing Limitation (3). In doing so, we rigorously establish that phase-error-rate bounds for individual partitions can be directly combined into a single bound on the overall phase-error rate of the full sifted key. Thus, by applying our framework, one can achieve security through a single privacy amplification step on the full key, eliminating Limitation (1) and circumventing the composability arguments of Limitation (2).

For concreteness, we focus our presentation on prepare-and-measure protocols, i.e., protocols in which Alice sends states to Bob. However, our framework can also be applied to address encoding correlations in interference-based protocols, i.e., protocols in which Alice and Bob send states to an untrusted middle node Charlie. To simulate the resulting key rate, we consider, as a particular example, a BB84 phase modulator modeled as a linear time-invariant (LTI) system, although our framework is general and not restricted to any specific device model.

Source replacement scheme with correlated sources. Consider a general prepare-and-measure QKD protocol where, in round $k \in \{1, \ldots, N\}$, Alice selects setting $j_k \in \mathcal{J}$ with probability p_{j_k}, where $\mathcal{J}$ denotes the alphabet of all her possible setting choices (e.g., in BB84, this includes all combinations of her basis and bit choices, i.e., $\mathcal{J} = \{(Z,0),(Z,1),(X,0),(X,1)\}$). Then, she emits a state $|\psi^{(k)}_{j_1^k}\rangle_{T_k}$, where $j_1^k := j_1, \ldots, j_k$. Due to encoding correlations, this state depends not only on the current setting j_k, but also on the history of previous settings j_1^{k-1}. Alice's state preparation is equivalent to generating the global source-replacement state

$$|\Psi_N\rangle_{A_1^N T_1^N} = \sum_{j_1^N} \bigotimes_k \sqrt{p_{j_k}} |j_k\rangle_{A_k} \big|\psi^{(k)}_{j_1^k}\big\rangle_{T_k} \tag{1}$$

and then measuring systems $A_1^N := A_1, \ldots, A_N$ in the computational basis $\{|j_k\rangle_{A_k}\}_{j_k \in \mathcal{J}}$, while sending systems T_1^N through the channel.

Uncorrelated sources correspond to the special case where $|\psi^{(k)}_{j_1^k}\rangle_{T_k} \equiv |\psi^{(k)}_{j_k}\rangle_{T_k}$. In this case, the global state factorizes as

$$|\Psi_N\rangle_{A_1^N T_1^N} = \bigotimes_k \sum_{j_k} \sqrt{p_{j_k}} |j_k\rangle_{A_k} \big|\psi^{(k)}_{j_k}\big\rangle_{T_k}. \tag{2}$$

Phase-error estimation with correlated sources. Security proofs based on phase-error estimation follow a specific approach. Using the source-replacement state, one first defines a scenario equivalent to the actual protocol in which Alice and Bob initially determine *which* rounds will be used to generate the sifted key, and only later extract the actual key bits. In this extraction phase, Alice measures qubit systems in the computational basis $\{|0\rangle, |1\rangle\}$, while Bob performs a two-outcome positive operator-valued measure (POVM) $\{G_0, G_1\}$ on his sifted-key systems.

Then, one considers a fictitious *phase-error-estimation protocol* in which Alice instead measures her qubits in the $\{|+\rangle, |-\rangle\}$ basis, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, and Bob uses his side information to attempt to predict her outcomes. The phase-error rate $\boldsymbol{e}_{\mathbf{ph}}$ is defined as the fraction of incorrect predictions, and bounding this quantity is the key to establishing security of the actual protocol. Specifically, one must prove that

$$\Pr[\boldsymbol{e}_{\mathbf{ph}} > \mathcal{E}_{\mathrm{ph}}(\vec{\boldsymbol{n}}; N, \epsilon)] \leqslant \epsilon, \tag{3}$$

where $\vec{\boldsymbol{n}}$ is a random vector representing the announced data (before postprocessing), ϵ is the bound's failure probability, $\mathcal{E}_{\mathrm{ph}}$ is a function relating these quantities, and the bound is established for any value of the total number of transmitted rounds N. Note that we use the convention that bold variables represent random variables.

For uncorrelated sources, it is well established that such a bound is enough to guarantee security either via EUR + LHL [19–21] or by using PEC arguments [22], even when the final key is of variable length [7,26–28]. In particular, under the EUR + LHL framework, one obtains a final key of length [7]

$$\begin{aligned}\boldsymbol{l} = \boldsymbol{n}_{\boldsymbol{K}}[1 - h(\mathcal{E}_{\mathrm{ph}}(\vec{\boldsymbol{n}}; N, \epsilon))] - \lambda_{\mathrm{EC}}(\vec{\boldsymbol{n}}) \\ - 2\log_2(1/(2\varepsilon_{\mathrm{PA}})) - \log_2(2/\varepsilon_{\mathrm{EV}}),\end{aligned} \tag{4}$$

with security parameter $(\varepsilon_{\mathrm{corr}} + \varepsilon_{\mathrm{sec}})$, where

$$\varepsilon_{\mathrm{corr}} = \varepsilon_{\mathrm{EV}} \quad \text{and} \quad \varepsilon_{\mathrm{sec}} = 2\sqrt{\epsilon} + \varepsilon_{\mathrm{PA}}. \tag{5}$$

Here, $\boldsymbol{n}_{\boldsymbol{K}}$ is the sifted key length, $\varepsilon_{\mathrm{EV}}$ is the error verification failure probability, $\varepsilon_{\mathrm{PA}} > 0$ is freely chosen, and λ_{EC} is a function of $\vec{\boldsymbol{n}}$ that determines the number of bits leaked during error correction.

In this work, we rigorously establish that a *phase-error-estimation protocol* defined for the uncorrelated source-replacement state in Eq. (2) remains equally valid when considering the correlated source-replacement state in Eq. (1). Consequently, proving a bound of the form in Eq. (3) suffices to guarantee security even with correlated sources (see the Supplemental Material [29] for the detailed construction and proof). This is significant because it demonstrates that the fundamental security framework—deriving secure key lengths from phase-error-rate bounds via EUR + LHL or PEC—applies naturally to correlated sources. The challenge thus reduces to deriving phase-error-rate upper bounds that account for correlations. Our main contribution below addresses this challenge by providing a general method to extend phase-error-rate upper bounds from uncorrelated to correlated sources. For the proof of the technical results below, as well as the full statement of our framework, see the Supplemental Material [29].

Corollary 1. Consider a prepare-and-measure QKD protocol with an uncorrelated source. In each round k, the source is characterized by a family of states $\{|\psi^{(k)}_{j_k}\rangle_{T_k}\}_{j_k \in \mathcal{J}}$ indexed by the setting $j_k \in \mathcal{J}$. Suppose there exists an admissibility set $\mathcal{S}$ of families of single-round states such that the phase-error bound in Eq. (3) is guaranteed to hold as long as the source

satisfies

$$\left\{\left|\psi_{j_k}^{(k)}\right\rangle_{T_k}\right\}_{j_k\in\mathcal{J}} \in \mathcal{S}, \quad \forall k. \tag{6}$$

Now consider the analogous protocol with a source exhibiting correlations up to length l_c, where in round k Alice emits a state $|\psi_{j_{k-l_c}^{k}}^{(k)}\rangle_{T_k}$ that depends on the setting history up to l_c rounds ago. For any sequence of settings $j_{k-l_c}^{k+l_c}$ (with the convention that indices outside $\{1,\ldots,N\}$ are truncated appropriately), define the joint state emitted in rounds k to $k+l_c$ as

$$\left|\Psi_{j_{k-l_c}^{k+l_c}}^{(k)}\right\rangle_{T_k^{k+l_c}} = \bigotimes_{m=k}^{k+l_c} \left|\psi_{j_{m-l_c}^{m}}^{(m)}\right\rangle_{T_m}. \tag{7}$$

Suppose that, for every round k and every fixed choice of past and future settings $(j_{k-l_c}^{k-1}, j_{k+1}^{k+l_c})$, the family $\{|\Psi_{j_{k-l_c}^{k+l_c}}^{(k)}\rangle_{T_k^{k+l_c}}\}_{j_k\in\mathcal{J}}$ obtained by varying j_k is isometrically equivalent to (i.e., has the same Gram matrix as) an acceptable family of single-round states $\{|\varphi_j^{(j_{k-l_c}^{k-1}, j_{k+1}^{k+l_c})}\rangle_{T_k}\}_{j\in\mathcal{J}} \in \mathcal{S}$.

Then, partitioning the rounds $k \in \{1,\ldots,N\}$ into (l_c+1) sets $I_w = \{k : k \equiv w \bmod (l_c+1)\}$ with $w = 0,\ldots,l_c$, the phase-error rate in the correlated scenario satisfies

$$\Pr[\boldsymbol{e}_{\mathrm{ph}} > \mathcal{E}'_{\mathrm{ph}}(\vec{\boldsymbol{n}}; N, \epsilon, l_c)] \leqslant \epsilon, \tag{8}$$

with

$$\mathcal{E}'_{\mathrm{ph}}(\vec{\boldsymbol{n}}; N, \epsilon, l_c) = \frac{\sum_{w=0}^{l_c} \boldsymbol{n}_{\boldsymbol{K}}^{(\boldsymbol{w})} \mathcal{E}_{\mathrm{ph}}\left(\vec{\boldsymbol{n}}^{(\boldsymbol{w})}; N^{(w)}, \frac{\epsilon}{l_c+1}\right)}{\boldsymbol{n}_{\boldsymbol{K}}}, \tag{9}$$

where $\vec{\boldsymbol{n}}^{(\boldsymbol{w})}$ is the restriction of the announced data vector $\vec{\boldsymbol{n}}$ to rounds in I_w, $N^{(w)} = |I_w|$, $\boldsymbol{n}_{\boldsymbol{K}}^{(\boldsymbol{w})}$ is the number of sifted key bits from rounds in I_w, and $\boldsymbol{n}_{\boldsymbol{K}} = \sum_{w=0}^{l_c} \boldsymbol{n}_{\boldsymbol{K}}^{(\boldsymbol{w})}$.

Interpretation. Corollary 1 essentially says that, as long as the family of multiround correlated states $\{|\Psi_{j_{k-l_c}^{k+l_c}}^{(k)}\rangle_{T_k^{k+l_c}}\}_{j_k\in\mathcal{J}}$ satisfies the single-round conditions of the original uncorrelated proof (up to an isometry), then one can divide the protocol rounds into (l_c+1) partitions, apply the uncorrelated phase-error-estimation formula to upper bound the phase-error rate of each partition, and take the weighted average to obtain an upper bound on the overall phase-error rate. Then, the secret-key length of the final key is given by Eq. (4) after substituting $\mathcal{E}_{\mathrm{ph}}(\vec{\boldsymbol{n}}; N, \epsilon)$ by $\mathcal{E}'_{\mathrm{ph}}(\vec{\boldsymbol{n}}; N, \epsilon, l_c)$.

This implies that the asymptotic secret-key rate obtainable with a correlated source whose multiround states satisfy the admissibility conditions in $\mathcal{S}$ is the same as that of an uncorrelated source whose single-round states are in $\mathcal{S}$. However, the correlated scenario incurs a larger finite-key penalty, which manifests in two ways: (1) The failure probability entering each application of the uncorrelated phase-error estimator $\mathcal{E}_{\mathrm{ph}}$ is reduced from ϵ to $\epsilon/(l_c+1)$ [see Eq. (9)] and (2) the effective block size to which this estimator is applied is reduced from N to $N/(l_c+1)$, since rounds are divided into (l_c+1) partitions. In practice, effect (2) dominates, since finite-key deviation bounds typically depend only logarithmically on the failure probability, making effect (1) comparatively mild. Thus, to achieve similar finite-key performance as in the uncorrelated case, the total block size N should be increased by a factor of roughly (l_c+1).

Note that, for some correlation models, the Gram matrix of the family $\{|\Psi_{j_{k-l_c}^{k+l_c}}^{(k)}\rangle_{T_k^{k+l_c}}\}_{j_k\in\mathcal{J}}$ may depend on $(j_{k-l_c}^{k-1}, j_{k+1}^{k+l_c})$ and/or the round k. For such models, the admissibility set $\mathcal{S}$ cannot consist of a single family $\{|\varphi_j\rangle\}_{j\in\mathcal{J}}$; i.e., the original security proof should consider some form of partial state characterization. A common approach, employed in Refs. [5,6,24,30,31], is to require fidelity bounds to reference states, a condition originally developed to handle information leakage through hard-to-characterize degrees of freedom such as mode dependencies or Trojan-horse attacks. In the following corollary, we show how our framework extends such security proofs to also incorporate encoding correlations. For other examples of admissibility sets and protocols to which our results apply, see Appendices A and B.

Corollary 2 (Fidelity bound to reference states). Consider a prepare-and-measure QKD protocol with an uncorrelated source, and suppose there exists a set of reference states $\{|\phi_j\rangle\}_{j\in\mathcal{J}}$ such that the phase-error bound in Eq. (3) holds as long as

$$\left|\left\langle\phi_{j_k}\middle|\psi_{j_k}^{(k)}\right\rangle_{T_k}\right|^2 \geqslant 1-\xi_{j_k}, \quad \forall k, \quad \forall j_k \in \mathcal{J}. \tag{10}$$

For an analogous protocol with a source with correlations up to length l_c, fix, for every round k and every choice of past and future settings $(j_{k-l_c}^{k-1}, j_{k+1}^{k+l_c})$, an arbitrary family of states $\{|\phi_{j_{k-l_c}^{k+l_c}}^{(k)}\rangle_{T_k}\}_{j_k\in\mathcal{J}}$ with the same Gram matrix as the family of reference states $\{|\phi_j\rangle\}_j$, and an arbitrary state $|\lambda_{j_{k-l_c}^{k-1}, j_{k+1}^{k+l_c}}^{(k)}\rangle_{T_{k+1}^{k+l_c}}$ independent of j_k, such that

$$\left|\left\langle\phi_{j_{k-l_c}^{k+l_c}}^{(k)}\right|_{T_k} \otimes \left\langle\lambda_{j_{k-l_c}^{k-1}, j_{k+1}^{k+l_c}}^{(k)}\right|_{T_{k+1}^{k+l_c}} \left|\Psi_{j_{k-l_c}^{k+l_c}}^{(k)}\right\rangle_{T_k^{k+l_c}}\right|^2 \geqslant 1-\xi_{j_k}, \quad \forall j_k. \tag{11}$$

Then, the phase-error-rate bound in Eq. (8) holds for this correlated scenario.

Note that Corollary 2 places no structural assumption on the correlated source (beyond a finite correlation length l_c, which can be lifted by applying Lemma 1). In particular, valid choices for the states $|\phi_{j_{k-l_c}^{k+l_c}}^{(k)}\rangle_{T_k}$ and $|\lambda_{j_{k-l_c}^{k-1}, j_{k+1}^{k+l_c}}^{(k)}\rangle_{T_{k+1}^{k+l_c}}$ always exist (e.g., one may take $|\phi_{j_{k-l_c}^{k+l_c}}^{(k)}\rangle_{T_k} = |\phi_{j_k}\rangle_{T_k}$ and any fixed state for $|\lambda_{j_{k-l_c}^{k-1}, j_{k+1}^{k+l_c}}^{(k)}\rangle_{T_{k+1}^{k+l_c}}$), and once these are fixed, the fidelities in Eq. (11) are always well defined. Since ξ_{j_k} are free parameters of the uncorrelated security proof, Eq. (11) can then always be satisfied by simply setting ξ_{j_k} to the worst-case fidelity over all rounds and setting histories. Consequently, Corollary 2 can be applied to *any* source with correlations of length l_c; the choice of $|\phi_{j_{k-l_c}^{k+l_c}}^{(k)}\rangle_{T_k}$ and $|\lambda_{j_{k-l_c}^{k-1}, j_{k+1}^{k+l_c}}^{(k)}\rangle_{T_{k+1}^{k+l_c}}$ merely determines the achievable values of ξ_{j_k}, and hence the tightness of the resulting key-rate bound. This motivates optimizing this choice to maximize the fidelities in Eq. (11); in the example below, we show how to do this for a correlations model of particular experimental interest.

Example: LTI correlations. As a concrete application of our framework, we consider correlations arising from modeling a BB84 phase modulator as an LTI system [13]. Due to linearity, the encoding phase for the kth pulse conditioned on the full

setting history j_1^k decomposes as

$$\theta_{j_1^k} = \hat{\theta}_{j_k} + \sum_{l=1}^{k-1} \delta^{(l)}_{j_{k-l}}. \tag{12}$$

Here, $\hat{\theta}_{j_k}$ is the phase that would be encoded if the system had been in its baseline state prior to the encoding (which may still deviate from the ideal BB84 phase due to the imperfect response of the modulator) and $\delta^{(l)}_{j_{k-l}}$ represents the residual contribution from setting j_{k-l} chosen l rounds earlier. Assuming for simplicity no encoding side channels beyond correlations (though our framework can also incorporate them), the emitted state in round k is

$$|\psi^{(k)}_{j_1^k}\rangle_{T_k} = \cos\left(\theta_{j_1^k}\right)|0\rangle_{T_k} + \sin\left(\theta_{j_1^k}\right)|1\rangle_{T_k}. \tag{13}$$

As shown in Appendix D of Ref. [13], one can experimentally obtain an exponential bound on the correlation strength, i.e.,

$$\left|\delta^{(l)}_j - \delta^{(l)}_{j'}\right| \leqslant \sqrt{\xi_l}, \quad \text{with} \quad \xi_l = \xi_1 e^{-C(l-1)}, \tag{14}$$

where $j, j' \in \mathcal{J}$, ξ_1 is the nearest-neighbor correlation strength, and $C > 0$ is a decay constant determined by the modulator's impulse response.

As a first step, consider for now an idealized scenario where correlations vanish beyond some length l_c, i.e., $\xi_l = 0$ for $l > l_c$. The family of correlated states $\{|\psi^{(k)}_{j^k_{k-l_c}}\rangle_{T_k}\}_{j_k}$ has a Gram matrix independent of both k and the past settings $j_{k-l_c}^{k-1}$, matching that of the reference family $\{|\phi_j\rangle\}_j$, with

$$|\phi_j\rangle = \cos(\hat{\theta}_j)|0\rangle + \sin(\hat{\theta}_j)|1\rangle. \tag{15}$$

To apply Corollary 2, we identify $|\phi^{(k)}_{j^{k+l_c}_{k-l_c}}\rangle_{T_k} \mapsto |\psi^{(k)}_{j^k_{k-l_c}}\rangle_{T_k}$ and

$$\left|\lambda^{(k)}_{j^{k-1}_{k-l_c}, j^{k+l_c}_{k+1}}\right\rangle_{T_{k+1}^{k+l_c}} \mapsto \bigotimes_{m=k+1}^{k+l_c} \left|\psi^{(m)}_{j^{k-1}_{m-l_c}, j^*, j^m_{k+1}}\right\rangle_{T_m}, \tag{16}$$

where $j^* \in \mathcal{J}$ is an arbitrary fixed setting for the kth pulse. A straightforward calculation (see Appendix C) then shows that Eq. (11) holds with $\xi_{j_k} = \xi, \forall j_k$, where

$$\xi := \sum_{l=1}^{l_c} \xi_l = \frac{\xi_1(1 - e^{-Cl_c})}{1 - e^{-C}}. \tag{17}$$

Thus, for finite-length correlations, one could directly apply Corollary 2 to extend an uncorrelated proof that accommodates fidelity bounds of the form in Eq. (10) to the reference states in Eq. (15), such as the proof in Ref. [6].

Of course, real sources may exhibit correlations of unbounded length, even if their strength may decay exponentially. To handle this, we introduce a freely chosen truncation length l_c^{eff} and account for the neglected long-range correlations beyond that length by slightly increasing the failure probability of the phase-error-rate bound. Note that, unlike the previous approach of Ref. [32], where the truncation argument and trace-distance correction are applied as a separate step outside the phase-error proof, our framework incorporates this correction directly into the phase-error-rate bound, yielding a single self-contained statement that can be used to directly prove security.

Lemma 1. Let $|\Psi_N^{(\infty)}\rangle_{A_1^N T_1^N}$ be the source-replacement state for a source with unbounded correlations, and let $|\Psi_N^{(l_c^{\text{eff}})}\rangle_{A_1^N T_1^N}$ be the corresponding state for a fictitious source with correlations truncated at length l_c^{eff}. If the trace distance between these two states satisfies

$$T\left(\left|\Psi_N^{(\infty)}\right\rangle\!\left\langle\Psi_N^{(\infty)}\right|, \left|\Psi_N^{(l_c^{\text{eff}})}\right\rangle\!\left\langle\Psi_N^{(l_c^{\text{eff}})}\right|\right) \leqslant d, \tag{18}$$

and the phase-error bound in Eq. (3) holds for the truncated source with failure probability ϵ, then the same bound holds for the actual source with failure probability $\epsilon + d$.

To apply this result, we bound the trace distance d between the actual and truncated source-replacement states. For the exponential model in Eq. (14), a straightforward calculation (see Appendix D) shows that

$$d \leqslant \sqrt{N} \sum_{l=l_c^{\text{eff}}+1}^{\infty} \sqrt{\xi_l} = \frac{\sqrt{N\xi_1} e^{-Cl_c^{\text{eff}}/2}}{1 - e^{-C/2}}. \tag{19}$$

Inverting this relation, to achieve a target d, one should choose the effective correlation length as

$$l_c^{\text{eff}} = \left\lceil \frac{1}{C} \ln\left(\frac{N\xi_1}{d^2(1 - e^{-C/2})^2}\right)\right\rceil. \tag{20}$$

Note that, once d is selected, l_c^{eff} can be deterministically calculated using Eq. (20), since C, N, and ξ_1 are known parameters. Then, applying Corollary 2 to the fictitious source with correlations truncated at length l_c^{eff}, and then applying Lemma 1, one obtains a secret key of length

$$\begin{aligned} \boldsymbol{l} = \boldsymbol{n_K}\left[1 - h\left(\mathcal{E}'_{\text{ph}}(\vec{\boldsymbol{n}}; N, \epsilon, l_c^{\text{eff}})\right)\right] - \lambda_{\text{EC}}(\vec{\boldsymbol{n}}) \\ - 2\log_2(1/(2\varepsilon_{\text{PA}})) - \log_2(2/\varepsilon_{\text{EV}}), \end{aligned} \tag{21}$$

with security parameter $(\varepsilon_{\text{corr}} + \varepsilon_{\text{sec}})$, where $\varepsilon_{\text{corr}} = \varepsilon_{\text{EV}}$ and $\varepsilon_{\text{sec}} = 2\sqrt{\epsilon + d} + \varepsilon_{\text{PA}}$.

We have focused on exponential decay because it arises naturally for bandwidth-limited optical modulators under the LTI model, which is supported by the experimental results in Ref. [13]. However, the approach above is not restricted to exponential decay: Lemma 1 applies to any correlation model, and the truncation is effective whenever the tail sum $\sum_{l>l_c^{\text{eff}}} \sqrt{\xi_l}$ converges fast enough to make d negligible for moderate values of l_c^{eff}. For exponential decay, $l_c^{\text{eff}} \sim \frac{1}{C} \ln N$, which grows only logarithmically with the block size N. For slower decay models, the scaling of l_c^{eff} with N may be worse, which would reduce the usefulness of the truncation approach. While we are not aware of realistic QKD modulator models exhibiting such slowly decaying correlations, determining whether secure key distribution remains possible under such models is an interesting open question.

Moreover, practical sources operating at very high clock rates may exhibit nonlinear pattern-dependent effects beyond the LTI description. Our framework is fully compatible with such nonlinear correlation models: The theoretical results (Corollaries 1 and 2 and Lemma 1) place no restrictions on the functional form of the history dependence and apply whenever the multiround correlated states can be experimentally characterized sufficiently to verify the relevant admissibility conditions. Once a validated model for such nonlinearities is

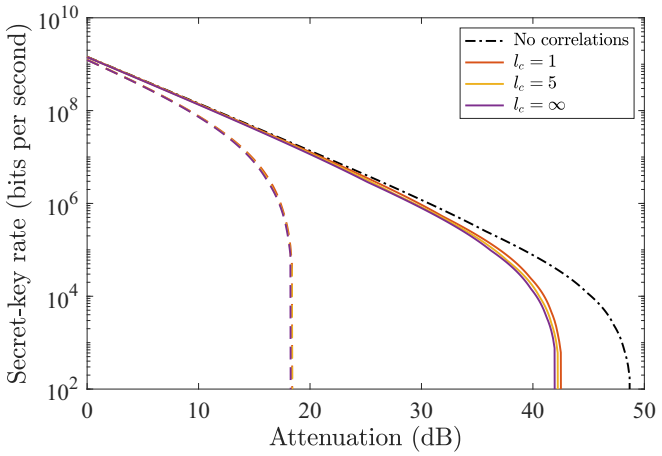

FIG. 1. Secret-key rate vs channel attenuation for a BB84 protocol with a source suffering from LTI correlations, assuming the exponential decay model in Eq. (14). The secret-key rates are obtained by combining Corollary 2 with the uncorrelated security analysis of Ref. [6]. The solid lines correspond to $\xi_1 = 10^{-6}$ and the dashed lines correspond to $\xi_1 = 10^{-3}$. The lines labeled by $l_c = 1$ and $l_c = 5$ consider correlations truncated artificially at length l_c (i.e., $\xi_l = 0$ for $l > l_c$), while $l_c = \infty$ corresponds to unbounded correlations handled via Lemma 1. The dash-dotted line corresponds to the ideal case of no correlations.

available, one can directly apply our framework to obtain the corresponding key rates without any modification.

Key-rate simulations for BB84. We now demonstrate our framework by simulating the achievable secret-key rate for a BB84 protocol with a source suffering from LTI correlations, combining Corollary 2 and Lemma 1 with the uncorrelated security proof in Refs. [6, 33]. We consider a source that emits states of the form in Eq. (13) with baseline phases $\hat{\theta}_j = (1 + \delta_{\mathrm{SPF}}/\pi)\varphi_j$, where $\varphi_j \in \{0, \pi/4, \pi/2, 3\pi/4\}$ is the ideal BB84 phase for setting $j \in \{0_Z, 0_X, 1_Z, 1_X\}$ and δ_{SPF} parametrizes state-preparation flaws arising from the imperfect modulator response. The correlations $\delta^{(l)}_{j_{k-l}}$ are assumed to satisfy the exponential bound in Eq. (14). We use the standard BB84 channel model in Ref. [34] with parameters: error-correction inefficiency $f = 1.16$, dark-count probability $p_d = 10^{-6}$, detector efficiency $\eta_d = 0.73$, and $N = 10^{12}$ transmitted signals. The state-preparation flaw is set to $\delta_{\mathrm{SPF}} = 0.068$ [35,36], and for the correlations model, we consider $\xi_1 \in \{10^{-3}, 10^{-6}\}$ and $C = 12.7$ [13]. The correctness and secrecy parameters of the final key are set to $\varepsilon_{\mathrm{corr}} = \varepsilon_{\mathrm{sec}} = 10^{-10}$. The results are shown in Fig. 1. As expected, the secret-key rate drops as ξ_1 increases. Moreover, for the exponential decay model, the impact of the correlations is dominated by the first few correlation terms, since ξ_l quickly becomes negligible with l. Thus, incorporating correlations of unbounded length results in almost no penalty compared to the finite-length case.

Conclusion. We have established a rigorous mathematical framework for extending phase-error-rate bounds to scenarios with encoding correlations, which can then be directly used to prove the security of QKD protocols in their presence. Our framework resolves key limitations of previous approaches: It eliminates the need for multiple privacy amplification steps, circumvents contested composability arguments, handles unbounded correlation lengths naturally, and applies systematically to any existing phase-error-estimation-based analysis that considers appropriate admissibility conditions on the emitted states. We anticipate that our framework will prove valuable for the security analysis of practical QKD implementations where such correlations are unavoidable and may extend to other scenarios beyond QKD involving temporally correlated sources.

Acknowledgments. We thank Devashish Tupkary, Shlok Nahar, and Víctor Zapatero for valuable discussions, and Davide Rusca for insights on LTI correlations. This work was supported by the Galician Regional Government (consolidation of research units: atlanTTic), the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through Grant No. PID2024-162270OB-I00, MICIN with funding from the European Union NextGenerationEU (PRTRC17.I1) and the Galician Regional Government with own funding through the "Planes Complementarios de I + D + I con las Comunidades Autonomas" in Quantum Communication, the "Hub Nacional de Excelencia en Comunicaciones Cuanticas" funded by the Spanish Ministry for Digital Transformation and the Public Service and the European Union NextGenerationEU, the European Union's Horizon Europe Framework Programme under the Marie Sklodowska-Curie Grant No. 101072637 (Project QSI), the project "Quantum Secure Networks Partnership" (QSNP, Grant Agreement No. 101114043), and the European Union via the European Health and Digital Executive Agency (HADEA) under the Project QuTechSpace (Grant No. 101135225) and the Project IberianQCI (Grant No. 101249593), as well as the Programa de Cooperación Interreg VI-A España–Portugal (POCTEP) 2021–2027 through the project QUANTUM_IBER_IA. G.C.-L. acknowledges funding from the European Union's Horizon Europe research and innovation program under the Marie Skłodowska-Curie Postdoctoral Fellowship Grant Agreement No. 101149523. K.T. acknowledges support from JSPS KAKENHI Grants No. 23K25793 and No. 23H01096.

Data availability. The data that support the findings of this article are available from the authors upon reasonable request.

Appendix A: Application to B92. Consider a security proof for the B92 protocol, such as Ref. [37], that assumes Alice emits some characterized states $|\phi_0\rangle$ and $|\phi_1\rangle$, and suppose that these states satisfy

$$|\langle\phi_1|\phi_0\rangle|^2 = c. \tag{A1}$$

Now consider a practical implementation in which Alice has a flawed but uncorrelated source emitting states $|\psi_0^{(k)}\rangle_{T_k}$ and $|\psi_1^{(k)}\rangle_{T_k}$ in round k that satisfy

$$\left|\langle\psi_1^{(k)}|\psi_0^{(k)}\rangle_{T_k}\right|^2 \geqslant c. \tag{A2}$$

Then, there exists a completely positive trace-preserving map $\mathcal{M}_k$ such that $|\psi_j^{(k)}\rangle\langle\psi_j^{(k)}|_{T_k} = \mathcal{M}_k(|\phi_j\rangle\langle\phi_j|_{T_k})$ for $j \in \{0, 1\}$ [38]. Since this map can be absorbed into Eve's attack channel, the proof applies under the general admissibility set

$$\mathcal{S} = \{\{|\psi_j\rangle\}_{j\in\{0,1\}} : |\langle\psi_1|\psi_0\rangle|^2 \geqslant c\}. \tag{A3}$$

To directly extend the proof to correlated sources via Corollary 1, the requirement is that the multiround correlated states defined in Eq. (7) satisfy

$$\left|\langle\Psi_{j_{k-l_c}^{k-1},1,j_{k+1}^{k+l_c}}|\Psi_{j_{k-l_c}^{k-1},0,j_{k+1}^{k+l_c}}\rangle_{T_k^{k+l_c}}\right|^2 \geqslant c, \tag{A4}$$

for all fixed past settings $j_{k-l_c}^{k-1}$ and future settings $j_{k+1}^{k+l_c}$. This condition ensures that the correlated states $\{|\Psi_{j_{k-l_c}^{k+l_c}}\rangle_{T_k^{k+l_c}}\}_{j_k\in\{0,1\}}$ are isometrically equivalent to an acceptable family $\{|\psi_0\rangle, |\psi_1\rangle\} \in \mathcal{S}$, since both families share the same inner product structure by construction.

Appendix B: Application to side-channel-secure QKD. In side-channel-secure QKD protocols [38,39], since Alice and Bob send only two states each, one can also apply the same argument to trivially extend an uncorrelated security proof to the acceptability set in Eq. (A4) for the states emitted by each user. Our results are not directly applicable to the existing security proofs in Refs. [38,39], however, since these are not based on obtaining a phase-error bound of the form in Eq. (3) that holds for general eavesdropping attacks, but are based on the application of the Postselection Technique to extend the proof from collective to general attacks. Still, a recently proposed variant of the protocol [40] performs better in some contexts and its security proof is based on obtaining a phase-error-rate bound as in Eq. (3), and thus the security proof in Ref. [40] can be extended directly to correlated sources via Corollary 1, with the condition that the multiround correlated states emitted by Alice and Bob satisfy a bound as in Eq. (A4).

Appendix C: Proof of Eq. (17). After identifying $|\phi_{j_{k-l_c}^{k+l_c}}^{(k)}\rangle_{T_k} \mapsto |\psi_{j_{k-l_c}^{k}}^{(k)}\rangle_{T_k}$ and Eq. (16), the inner product squared in Eq. (11) becomes

$$\begin{aligned}
&\left|\langle\psi_{j_{k-l_c}^{k}}^{(k)}|_{T_k}\bigotimes_{m=k+1}^{k+l_c}\langle\psi_{j_{m-l_c}^{k-1},\,j^*,\,j_{k+1}^{m}}^{(m)}|_{T_m}|\Psi_{j_{k-l_c}^{k+l_c}}^{(k)}\rangle_{T_k^{k+l_c}}\right|^2\\
&=\prod_{m=k+1}^{k+l_c}\left|\langle\psi_{j_{m-l_c}^{k-1},\,j^*,\,j_{k+1}^{m}}^{(m)}|\psi_{j_{m-l_c}^{k-1},\,j_k,\,j_{k+1}^{m}}^{(m)}\rangle_{T_m}\right|^2\\
&=\prod_{l=1}^{l_c}\cos^2\left(\delta_{j_k}^{(l)}-\delta_{j^*}^{(l)}\right)=\prod_{l=1}^{l_c}\left(1-\sin^2\left(\delta_{j_k}^{(l)}-\delta_{j^*}^{(l)}\right)\right)\\
&\geqslant\prod_{l=1}^{l_c}\left(1-\left(\delta_{j_k}^{(l)}-\delta_{j^*}^{(l)}\right)^2\right)\geqslant\prod_{l=1}^{l_c}(1-\xi_l)\\
&\geqslant 1-\sum_{l=1}^{l_c}\xi_l =: 1-\xi.
\end{aligned}\tag{C1}$$

Then, by substituting the exponential model in Eq. (14) into Eq. (C1), we obtain Eq. (17).

Appendix D: Proof of Eq. (19). Let

$$|\Psi_N^{(l_c^{\rm eff})}\rangle_{A_1^N T_1^N}=\sum_{j_1^N}\bigotimes_k\sqrt{p_{j_k}}|j_k\rangle_{A_k}|\psi_{j_{k-l_c^{\rm eff}}^{k}}^{(k)}\rangle_{T_k},\tag{D1}$$

where we have defined

$$|\psi_{j_{k-l_c^{\rm eff}}^{k}}^{(k)}\rangle_{T_k}=|\psi_{j_1^k}^{(k)}\rangle_{T_k}\Big|_{j_1=j_2=\cdots=j_{k-l_c^{\rm eff}-1}=j^*},\tag{D2}$$

with $j^*\in\mathcal{J}$ being an arbitrary fixed setting. Using similar derivations as in Appendix B of Ref. [32], we have that

$$\left|\langle\psi_{j_{k-l_c^{\rm eff}}^{k}}^{(k)}|\psi_{j_1^k}^{(k)}\rangle_{T_k}\right|^2\geqslant 1-\left(\sum_{l=l_c^{\rm eff}+1}^{\infty}\sqrt{\xi_l}\right)^2.\tag{D3}$$

Therefore,

$$\left|\langle\Psi_N^{(l_c^{\rm eff})}|\Psi_N^{(\infty)}\rangle_{A_1^N T_1^N}\right|^2\geqslant\left[1-\left(\sum_{l=l_c^{\rm eff}+1}^{\infty}\sqrt{\xi_l}\right)^2\right]^N.\tag{D4}$$

Thus, using the fact that for $x\in[0,1]$, $1-(1-x)^N\leqslant Nx$,

$$d=\sqrt{1-\left|\langle\Psi_N^{(l_c^{\rm eff})}|\Psi_N^{(\infty)}\rangle_{A_1^N T_1^N}\right|^2}\leqslant\sqrt{N}\sum_{l=l_c^{\rm eff}+1}^{\infty}\sqrt{\xi_l}.\tag{D5}$$

Then, by substituting the exponential model in Eq. (14) into Eq. (D5) and evaluating the resulting convergent series, we obtain Eq. (19).

[1] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, Quantum Inf. Comput. **4**, 325 (2004).

[2] C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, Security proof of quantum key distribution with detection efficiency mismatch, Quantum Inf. Comput. **9**, 131 (2009).

[3] Ø. Marøy, L. Lydersen, and J. Skaar, Security of quantum key distribution with arbitrary individual imperfections, Phys. Rev. A **82**, 032337 (2010).

[4] 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).

[5] M. Pereira, G. Kato, A. Mizutani, M. Curty, and K. Tamaki, Quantum key distribution with correlated sources, Sci. Adv. **6**, eaaz4487 (2020).

[6] G. Currás-Lorenzo, M. Pereira, G. Kato, M. Curty, and K. Tamaki, Security framework for quantum key distribution with imperfect sources, Opt. Quantum **3**, 525 (2025).

[7] D. Tupkary, S. Nahar, P. Sinha, and N. Lütkenhaus, Phase error rate estimation in QKD with imperfect detectors, Quantum **9**, 1937 (2025).

[8] X. Sixto, Á. Navarrete, M. Pereira, G. Currás-Lorenzo, K. Tamaki, and M. Curty, Quantum key distribution with imperfectly isolated devices, Quantum Sci. Technol. **10**, 035034 (2025).

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

[10] A. Marwah and F. Dupuis, Proving security of BB84 under source correlations, arXiv:2402.12346.

[11] G. Currás-Lorenzo, M. Pereira, S. Nahar, and D. Tupkary, Security of quantum key distribution with source and detector imperfections through phase-error estimation, npj Quantum Inf. **12**, 129 (2026).

[12] F. Grünenfelder, A. Boaron, D. Rusca, A. Martin, and H. Zbinden, Performance and security of 5 GHz repetition rate polarization-based quantum key distribution, Appl. Phys. Lett. **117**, 144003 (2020).

[13] A. Agulleiro, F. Grünenfelder, M. Pereira, G. Currás-Lorenzo, H. Zbinden, M. Curty, and D. Rusca, Modeling and characterization of arbitrary order pulse correlations for quantum key distribution, arXiv:2506.18684.

[14] M. Christandl, R. König, and R. Renner, Postselection technique for quantum channels with applications to quantum cryptography, Phys. Rev. Lett. **102**, 020504 (2009).

[15] S. Nahar, D. Tupkary, Y. Zhao, N. Lütkenhaus, and E. Y.-Z. Tan, Postselection technique for optical quantum key distribution with improved de Finetti reductions, PRX Quantum **5**, 040315 (2024).

[16] R. Renner, Symmetry of large physical systems implies independence of subsystems, Nat. Phys. **3**, 645 (2007).

[17] A. Arqand and E. Y.-Z. Tan, Marginal-constrained entropy accumulation theorem, arXiv:2502.02563.

[18] The Postselection Technique [14,15] and approaches based on the Quantum de Finetti theorem [16] require the global protocol state to be permutation-invariant, enabling a reduction from general attacks to collective attacks. However, with encoding correlations, the temporal ordering of settings affects the physical state, breaking this symmetry. Similarly, the MEAT [17] models the protocol state as produced by a sequence of channels, each acting on an input state satisfying a fixed marginal constraint. With correlations, Alice's source state in round k depends on all previous settings j_1^{k-1}, violating the required factorization structure of the source-replacement state.

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

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

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

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

[23] 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).

[24] M. Pereira, G. Currás-Lorenzo, Á. 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] D. Tupkary, E. Y.-Z. Tan, S. Nahar, L. Kamin, and N. Lütkenhaus, Security proofs for practical QKD: Variations, techniques, gaps, and limitations, Rev. Mod. Phys. **98**, 035003 (2026).

[26] G. Currás-Lorenzo, Á. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, Tight finite-key security for twin-field quantum key distribution, npj Quantum Inf. **7**, 22 (2021).

[27] 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).

[28] S. Kawakami, Security of quantum key distribution with weak coherent pulses, Ph.D. thesis, University of Tokyo, 2017.

[29] See Supplemental Material at http://link.aps.org/supplemental/10.1103/tkx1-23xz for the general statement of our framework and the detailed proofs of all results, which includes Refs. [41–43].

[30] M. Pereira, M. Curty, and K. Tamaki, Quantum key distribution with flawed and leaky sources, npj Quantum Inf. **5**, 62 (2019).

[31] Á. Navarrete, M. Pereira, M. Curty, and K. Tamaki, Practical quantum key distribution that is secure against side channels, Phys. Rev. Appl. **15**, 034072 (2021).

[32] M. Pereira, G. Currás-Lorenzo, A. Mizutani, D. Rusca, M. Curty, and K. Tamaki, Quantum key distribution with unbounded pulse correlations, Quantum Sci. Technol. **10**, 015001 (2025).

[33] Note that, while the core security proof proposed by Ref. [6] assumes uncorrelated sources, this work then argues that the proof could be extended to correlated sources using the approach of Ref. [5]. However, this extension suffers from the limitations identified in our introduction, and by applying our framework directly to the uncorrelated proof, we overcome these limitations.

[34] M. Pereira, G. Currás-Lorenzo, and M. Araújo, Optimal key rates for quantum key distribution with partial source characterization, arXiv:2510.13085.

[35] T. Honjo, K. Inoue, and H. Takahashi, Differential-phase-shift quantum key distribution experiment with a planar lightwave circuit Mach–Zehnder interferometer, Opt. Lett. **29**, 2797 (2004).

[36] F. Xu, K. Wei, S. Sajeed, S. Kaiser, S. Sun, Z. Tang, L. Qian, V. Makarov, and H.-K. Lo, Experimental quantum key distribution with source flaws, Phys. Rev. A **92**, 032305 (2015).

[37] K. Tamaki and N. Lütkenhaus, Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel, Phys. Rev. A **69**, 032316 (2004).

[38] C. Jiang, X.-L. Hu, Z.-W. Yu, and X.-B. Wang, Side-channel security of practical quantum key distribution, Phys. Rev. Res. **6**, 013266 (2024).

[39] 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).

[40] Y.-G. Shan, Z.-Q. Yin, S. Wang, W. Chen, D.-Y. He, G.-C. Guo, and Z.-F. Han, Practical phase-coding side-channel-secure quantum key distribution, arXiv:2305.13861.

[41] H. Zhou, T. Sasaki, and M. Koashi, Numerical method for finite-size security analysis of quantum key distribution, Phys. Rev. Res. **4**, 033126 (2022).

[42] Z. Wang, D. Tupkary, and S. Nahar, Phase error estimation for passive detection setups with imperfections and memory effects, arXiv:2508.21486.

[43] A. Marcomini, A. Mizutani, F. Grünenfelder, M. Curty, and K. Tamaki, Loss-tolerant quantum key distribution with detection efficiency mismatch, Quantum Sci. Technol. **10**, 035002 (2025).