

Surpassing the loss-noise robustness trade-off in quantum key distribution

Hannah Seabrook^{1,2,*}, Emilien Lavie,¹ Teodor Strömberg³, Matthew P. Stafford^{1,2} and Giulia Rubino^{1,4,†}

¹*Quantum Engineering Technology Labs, H. H. Wills Physics Laboratory and School of Electrical, Electronic, and Mechanical Engineering, University of Bristol, BS8 1FD, United Kingdom*

²*Quantum Engineering Centre for Doctoral Training, Centre for Nanoscience and Quantum Information, University of Bristol, United Kingdom*

³*Institute of Science and Technology Austria, Klosterneuburg, Austria*

⁴*H. H. Wills Physics Laboratory, University of Bristol, Tyndall Avenue, Bristol BS8 1TL, United Kingdom*

 (Received 17 February 2025; revised 21 July 2025; accepted 23 July 2025; published 29 August 2025)

Quantum key distribution (QKD) offers a theoretically secure method to share secret keys, yet practical implementations face challenges due to noise and loss over long-distance channels. Traditional QKD protocols require extensive noise compensation, hindering their industrial scalability and lowering the achievable key rates. Alternative protocols encode logical qubits in noise-resilient states but at the cost of using many physical qubits, increasing susceptibility to loss and limiting transmission distance. In this work, we introduce a logical-qubit encoding that uses antisymmetric Bell states in the continuous photonic degrees of freedom, frequency and time. By leveraging the continuous space, we overcome this noise-loss robustness trade-off by minimizing the number of photons per logical qubit while optimizing the encoding resilience over noise fluctuations. We analyze the security of our encoding and demonstrate its robustness compared to existing state-of-the-art protocols. This approach provides a path toward scalable, efficient QKD implementations under realistic noise conditions.

DOI: [10.1103/xq2l-r4r7](https://doi.org/10.1103/xq2l-r4r7)

I. INTRODUCTION

Quantum information theory reached key milestones with the establishment of early protocols such as BB84 [1] and advancements such as Shor's algorithm [2], which showcased its transformative potential for real-world applications. These developments solidified the field's focus on practical challenges, laying the foundations for quantum technologies today [3]. Among these technologies, quantum key distribution (QKD) stands out as a leading candidate for near-term applications and commercialization due to its potential for fundamentally secure communication [4,5]; however, transitioning QKD from theoretical models to scalable, industrial implementations remains a significant challenge [6]. Achieving high key rates across a large-scale QKD network requires extensive stabilization and compensation techniques to overcome the

noise experienced by qubits in transmission [7–9]. For example, while twin-field QKD (TF-QKD) enables state-of-the-art key rates, it also requires the stabilization of two lasers' frequencies, polarizations, and field phases across long-distance noisy channels [10–12]. Impressive systems have been demonstrated experimentally that actively stabilize these elements [9,13–16]. Nonetheless, this raises the question of whether an alternative approach to implementing QKD could offer a path forward without the substantial overheads required for compensated QKD.

Here, we investigate such an alternative solution: devising a QKD protocol that encodes information into inherently noise-resilient states. Such protocols have previously been proposed, e.g., for resilience against collective unitary noise channels [17–21], and they typically encode logical qubits in the subspace of a higher-dimensional space formed from many photonic qubits; however, these approaches inherently involve a trade-off between loss robustness and noise robustness (see Table I). On the one hand, increasing the number of qubits improves the noise robustness of the logical subspace, and beyond a minimum qubit threshold, the logical states can be made perfectly noise robust. On the other hand, if even one photon is lost in transmission, the whole logical state is compromised. Thus, increasing the number of photons in the logical state

*Contact author: hannah.seabrook@bristol.ac.uk

†Contact author: giulia.rubino@bristol.ac.uk

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

TABLE I. Comparison of commonly employed protocols and existing noise-robust protocols in terms of loss robustness and noise robustness. The table illustrates the trade-off between loss robustness and noise robustness in QKD protocols, which we further analyze in Appendix A, and it highlights how our protocol improves upon existing approaches. Protocols are listed with increasing susceptibility to photon loss down the table, where $\eta = 10^{-\text{loss(dB)}/10}$ is the channel transmissivity—larger powers of η correspond to greater degradation with loss. Twin-field QKD (TF-QKD) [10] and BB84 [1] are not robust to noise fluctuations, and they require extensive stabilization techniques for their effective operation. As we show in Sec. IV A, Ref. [17] demonstrates better robustness to collective unitary noise than BB84; however, its key rate vanishes under time-varying noise parameters, thus necessitating noise-compensation methods. As our protocol uses both frequency-bin and time-bin qubits, in Sec. III B, we outline the model used to assess the robustness of our protocol on conjugate qubits, represented as a unitary on frequency-bin qubits.

Protocol	Loss scaling	No stabilization needed?	Robust to collective unitary noise?	Robust to randomly varying unitary noise parameters?
TF-QKD [10]	$\eta^{1/2}$	✗	✗	✗
BB84 [1]	η	✗	✗	✗
Wang (2005) [17]	η^2	✗	✓	✗
This work	η^2	✓	✓	✓
Boileau <i>et al.</i> (2004) three photon [18]	η^3	✓	✓	✓
Boileau <i>et al.</i> (2004) four photon [18]	η^4	✓	✓	✓
Li <i>et al.</i> (2008) [19]	η^4	✓	✓	✓

makes it exponentially more susceptible to photon loss, severely limiting the distance over which the secret key can be shared.

In this work, we introduce an encoding scheme that reduces the number of photons in a logical qubit state, thereby minimizing the impact of loss while increasing the robustness of the logical state to noise. Inspired loosely by bosonic codes—a field of quantum error correction that uses the redundancy of infinite-dimensional Hilbert spaces to encode logical qubits and mitigate physical errors [22]—we exploit similar redundancies in a continuous photonic degree of freedom (DOF) to achieve noise resilience. Specifically, our encoding represents logical qubit states in superpositions across two-photon antisymmetric Bell states defined over frequency bins and time bins. The antisymmetric structure of the states ensures intrinsic robustness to noise. At the same time, by using superpositions of excitations across modes of a continuous photonic DOF, our encoding reduces the number of photons required for a logical qubit, thus offering a low-loss alternative to noise-robust QKD protocols.

We illustrate the robustness of our protocol under two continuous channel-noise models: one experimentally motivated (chromatic dispersion) and the other motivated to enable a comparison with existing discrete-variable (DV)-encoded protocols (a unitary applied to frequency-bin qubits). Additionally, we demonstrate that the parameters of our encoding can be optimized over fluctuations in noise parameters.

Finally, we perform a rigorous and unified key-rate analysis of our protocol under the noise models and loss channel, and we compare the key rates to those of existing noise-robust protocols [17–19]. We show that our protocol surpasses the noise-resilience of two-photon protocols [17] and the loss robustness of perfectly noise-canceling protocols [18,19]. These results highlight how encoding

in continuous DOFs can enhance the robustness of secure communication protocols.

In the next section, we present our encoding. In Sec. III, we demonstrate the noise-robust properties of our encoding. In Sec. IV, we analyze and discuss the security of our protocol and existing protocols in lossy and collective unitary noise channels. We conclude by discussing our findings and their implications and suggesting possible directions for future work.

II. PROTOCOL

Our protocol follows the BB84 scheme [1], with single-photon states replaced by two-photon logical qubit states encoded in a continuous DOF for noise resilience, as illustrated in Fig. 1. In the protocol, a sender (Alice) prepares states randomly in either the logical Z (which we label Z_L) basis $\{|0_L\rangle, |1_L\rangle\}$, or the logical X (X_L) basis $\{|\pm_L\rangle = (|0_L\rangle \pm |1_L\rangle)/\sqrt{2}\}$. Similarly, a receiver (Bob) measures randomly in either Z_L or X_L . Bob’s projectors are given by $\{|0_L\rangle\langle 0_L|, |1_L\rangle\langle 1_L|, |+_L\rangle\langle +_L|, |-_L\rangle\langle -_L|, |\perp_L\rangle\langle \perp_L|\}$, where $|\perp_L\rangle$ corresponds to an inconclusive measurement due to loss or the measurement of a state outside the logical subspace.

To describe our encoding, we simply need to establish the encoding of the Z_L basis states $\{|0_L\rangle, |1_L\rangle\}$, as the X_L basis states and the measurement operators follow trivially. We use antisymmetric Bell states to encode $|0_L\rangle$ and $|1_L\rangle$ in such a way that they are naturally robust to noise, as in the existing DV protocols [17–19] (reviewed in Sec. S.I of the Supplemental Material (SM) [23]). These states are invariant under local collective unitary operations; i.e., $(U \otimes U) |\Psi^-\rangle = e^{i\Delta} |\Psi^-\rangle$, where $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$ and Δ is some U -dependent global phase factor [24] (see Appendix A). To minimize the number of photons per logical state, we encode the Z_L

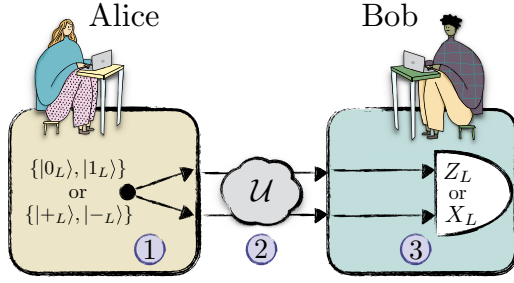


FIG. 1. Depiction of the BB84 protocol using logical noise-robust qubit states. We propose a BB84 protocol using logical noise-robust states to improve key rates in noisy channels. Alice prepares a logical qubit in either the Z_L or X_L basis, randomly, encoding the bit value 0 in $|0_L\rangle$ or $|+_L\rangle$ and the bit value 1 in $|1_L\rangle$ or $|-_L\rangle$. She sends the state to Bob, who measures randomly in either the Z_L or X_L basis. After transmission, Alice and Bob discard cases with mismatched bases and measurement outcomes outside the logical subspace, and they check for errors due to an eavesdropper on a subset of the remaining bits. If the error rate is below a certain threshold, they proceed with error correction and privacy amplification; otherwise, they abort the protocol. We assume that the channel induces “collective noise,” applying the same unknown transformation $\mathcal{U}$ to each photon in the logical state.

basis states as two-photon antisymmetric Bell states in the conjugate variables, frequency and time.

Our encoding is built in two layers. The first layer is formed of single-photon physical qubits. In this layer, we define single-photon physical qubit states in conjugate variables: the single-photon frequency-bin qubit states that we label by $\{|0_f\rangle, |1_f\rangle\}$, and the single-photon time-bin qubit states that we label as $\{|0_t\rangle, |1_t\rangle\}$. The second layer is the logical encoding layer (labeled by the subscript L). In the logical layer, we construct two two-photon antisymmetric Bell states, one from the frequency-bin qubits of the first layer and the other from the time-bin qubits. These two antisymmetric Bell states act as the building blocks of our logical qubit space $\{|0_L\rangle, |1_L\rangle\}$.

We start by defining the first layer of the encoding using bosonic creation operators on the vacuum state $|\emptyset\rangle$. We define the creation operator for a photon occupying a frequency-bin mode as

$$\hat{a}_{\Omega_i, M}^\dagger = \int d\omega f_{\Omega_i, \sigma_\omega}(\omega) \hat{a}_M^\dagger(\omega), \quad (1)$$

where $\hat{a}_M^\dagger(\omega)$ is the creation operator for a photon in some mode M (for example, a polarization mode or a spatial mode) with frequency ω , and $f_{\Omega_i, \sigma_\omega}(\omega)$ is the frequency-bin mode amplitude function, which is a sharply peaked function centered around Ω_i with width σ_ω .

Similarly, we define the creation operator for a photon occupying a time-bin mode as

$$\hat{a}_{\tau_i, M}^\dagger = \int dt f_{\tau_i, \sigma_t}(t) \hat{a}_M^\dagger(t) = \int d\omega F_{\tau_i, \sigma_t}(\omega) \hat{a}_M^\dagger(\omega), \quad (2)$$

where $\hat{a}_M^\dagger(t)$ is the creation operator for a photon in some mode M at time t and $f_{\tau_i, \sigma_t}(t)$ is the time-bin mode amplitude function, sharply peaked in time, centered around τ_i with width σ_t . The second equality shows that this can be expressed as a creation operator on frequency modes by applying the Fourier transform between frequency and time. In this context, $F_{\tau_i, \sigma_t}(\omega)$ is the Fourier transform of $f_{\tau_i, \sigma_t}(t)$ and ω is now defined relative to the central frequency of the states.

Defining two frequency bins centered at frequencies Ω_0 and Ω_1 and two time bins centered at times τ_0 and τ_1 , we can now define single-photon frequency-bin qubit and time-bin qubit states as

$$|i_x\rangle_M = \hat{a}_{\mu_i, M}^\dagger |\emptyset\rangle, \quad (3)$$

where $i \in \{0, 1\}$ and $x \in \{f, t\}$, in which f indicates the frequency-bin states and t indicates the time-bin states, and μ_i is Ω_i or τ_i , respectively. This assumes that Ω_0 and Ω_1 , and τ_0 and τ_1 are sufficiently well separated such that $\langle 0_x | 1_x \rangle_M \approx 0$. For brevity, we label the parameters of the frequency-bin and time-bin qubits by $\bar{\Omega} = (\Omega_0, \Omega_1, \sigma_\omega)$ and $\bar{\tau} = (\tau_0, \tau_1, \sigma_t)$, respectively.

We now establish the logical encoding layer, formed from biphoton antisymmetric Bell states in frequency bins and time bins. We define these as

$$|\Psi_x^-\rangle = \frac{|0_x\rangle_M |1_x\rangle_N - |1_x\rangle_M |0_x\rangle_N}{\sqrt{2}}, \quad (4)$$

where the labels M and N signify that the two photons are distinguished by some extra mode (e.g., spatial mode or polarization). The states $|\Psi_f^-\rangle$ in the frequency domain and $|\Psi_t^-\rangle$ in the time domain are depicted in Fig. 2, with Gaussian amplitude functions used as an illustrative example. Here, $|\Psi_f^-\rangle$ and $|\Psi_t^-\rangle$ define a two-dimensional logical Hilbert space. The logical states in the Z_L basis are given by

$$|0_L\rangle = |\Psi_f^-\rangle \quad |1_L\rangle = |\Psi_{\perp f}^-\rangle, \quad (5)$$

where $|\Psi_{\perp f}^-\rangle$ is a state orthogonal to $|\Psi_f^-\rangle$, defined according to

$$|\Psi_{\perp f}^-\rangle = \frac{(|\Psi_t^-\rangle - a |\Psi_f^-\rangle)}{\sqrt{1 - |a|^2}}, \quad (6)$$

in which a is the overlap of the frequency-bin and time-bin Bell states, $\langle \Psi_f^- | \Psi_t^- \rangle$. Typical experimental parameters

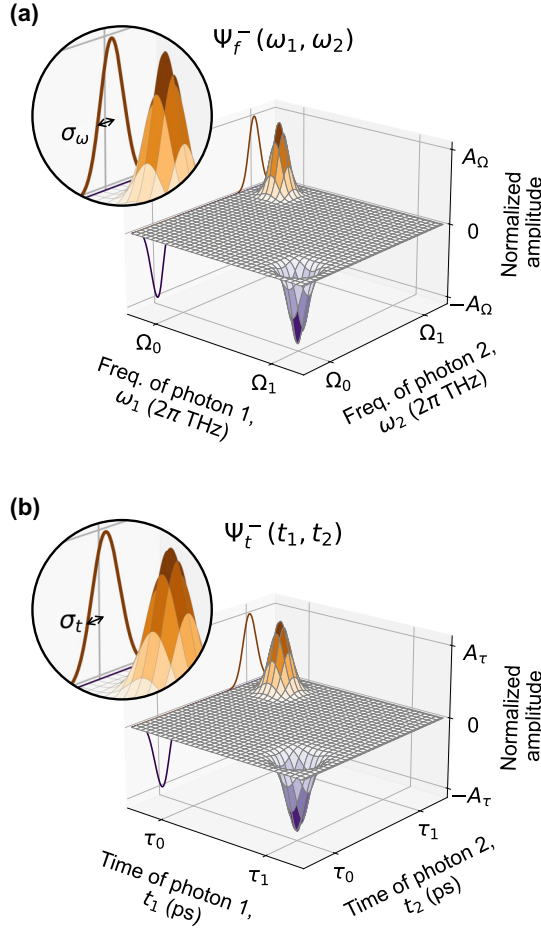


FIG. 2. Two-dimensional joint frequency and temporal spectra of the frequency- and time-bin-encoded antisymmetric Bell states used to form the logical states $|0_L\rangle$ and $|1_L\rangle$. (a) Normalized biphoton wavefunction amplitude of the antisymmetric frequency-bin-encoded Bell state $|\Psi_f^-\rangle$ visualized in the frequency domain and (b) the normalized biphoton wavefunction amplitude of the antisymmetric time-bin-encoded Bell state $|\Psi_t^-\rangle$ visualized in the time domain, for amplitude functions modeled as state-normalized Gaussians. Here, A_Ω and A_τ are the peak amplitudes of the wavefunctions (set by the normalization conditions and the encoding parameters $\vec{\Omega}$ and $\vec{\tau}$, respectively; see Sec. S.II of the SM [23]). The insets highlight the widths, σ_ω and σ_t , of the one-dimensional frequency bins and time bins.

give a negligible value for a . In fact, we show that $|\Psi_f^-\rangle$ and $|\Psi_t^-\rangle$ can be made perfectly distinguishable (i.e., $a = 0$) for both Gaussian and Lorentzian amplitude functions by tuning $\vec{\Omega}$ and $\vec{\tau}$ (see Sec. S.II of the SM [23]). In Appendix B, we propose one possible method for preparing these states and measuring in the two bases, using domain-engineered nonlinear crystals.

In the next section, we demonstrate the robustness of this encoding to different noise channels and their parameter fluctuations.

III. NOISE ROBUSTNESS OF ENCODING

We now showcase the resilience of our encoding against two example channel-noise models, for state amplitudes modeled as Gaussian functions. (As justified in Sec. S.III of the SM [23], using more general peaked amplitude functions should yield results analogous to those of Gaussian states.) First, we briefly demonstrate the robustness of our encoding under a common experimental noise model (dispersion), illustrating the applicability of our encoding to typical experimental scenarios. This initial analysis is heuristic, with a detailed quantitative study and figures provided in Sec. S.IV of the SM [23]. The remainder of this section is dedicated to in-depth analysis of our encoding's resilience to a theoretically motivated noise model (the “frequency beamsplitter”; FBS). This model enables us to compare the efficacy of our encoding's noise robustness to that of the existing protocols in Refs. [17–19], which we subsequently present in Sec. IV.

A. Dispersion noise

Chromatic dispersion is an optical property of transparent media in which the phase velocity and group velocity of light traversing the medium are frequency dependent [25] (typical in optical fibers, for example [26]). In this subsection, we present the analytical noise model of chromatic dispersion and summarize the effect of this noise on our encoding and its key rates.

By expanding the frequency-dependent wave vector of light in a dispersive medium about some frequency ω_0 , the effect of n th-order dispersion on the photon's spectral amplitude can be written as

$$g(\omega) \mapsto e^{i\alpha_n(\omega-\omega_0)^n} g(\omega), \quad (7)$$

where α_n is the corresponding dispersion coefficient (as derived in Sec. S.IV of the SM [23]). Typical materials only need consideration of the group delay dispersion (GDD; the $n = 1$ term) and the group velocity dispersion (GVD; the $n = 2$ term). When higher-order terms have to be considered, it is often more convenient to use direct numerical modeling [25].

The GDD ($n = 1$) physically corresponds to a simple time delay of the pulses sent by Alice, as understood by the time-shift property of the Fourier transform. Both our protocol and current QKD experiments can cancel this using common synchronization techniques based on the arrival time of a reference signal from Alice at Bob [27–30]. Synchronization ensures that Alice and Bob assign the same sequence number to each event [31] and that the time-bin basis-state labels of Alice's encoding align with those of Bob's measurement for time-bin-encoded QKD; however, our encoding relaxes the synchronization requirements needed for typical time-bin-encoded QKD.

Only synchronizing the events' sequence numbers is necessary, as an offset between Alice and Bob's time-bin labels results in an incurred loss rather than a quantum bit error rate (QBER) for our protocol (see Sec. S.IV B of the SM [23]).

The GVD ($n = 2$) instead changes the shape of the temporal probability amplitude by broadening it. For single-qubit time-bin-encoded QKD, this broadening effect compromises the security of the protocol over intermediate distances (around 50 km of fiber), unless appropriate compensation is employed [29]. This occurs due to the QBER rapidly increasing as the pulses spread into the neighboring time bins. In contrast, for our encoding, GVD increases the effective loss. This is due to an increasing rate of inconclusive outcomes as the photons' probability density "leaks" outside Bob's logical measurement subspace; however, this does not increase the QBER, allowing our protocol to maintain security under this noise at long distances.

Overall, the effect of chromatic dispersion on our encoding results in decaying oscillations of key rate as a function of $|\alpha_n|$. The decay rate is due to the increased inconclusive outcomes and depends on the encoding parameters $\vec{\Omega}$ and $\vec{\tau}$. The oscillations arise from an α_n -dependent decoherence phase imparted on the single-qubit frequency-bin states, due to the difference in dispersive phase between the two central frequencies. This corresponds to a decoherence phase at the logical layer of our encoding, resulting in an oscillating phase error rate with a period depending again on $\vec{\Omega}$ and $\vec{\tau}$. The encoding parameters can be optimized to maintain significant key rates across the channel by ensuring the key-rate oscillation period is large compared to the variation of the dispersion parameters, α_n , (e.g., due to varying temperature [32]). This allows the key rate to remain close to a maximum within the fluctuation range of α_n . Figures, further mathematical analysis, and the consideration of realistic noise and nonoptimal experimental parameters are presented in Sec. S.IV of the SM [23].

B. Frequency beamsplitter noise

To compare the noise resilience of our protocol against existing protocols that leverage antisymmetric Bell states (Refs. [17–19]), we now consider an alternative noise model based on frequency-bin qubits. While the physical encoding of Refs. [17–19] can be expressed in a discrete Hilbert space, our logical qubit encoding uses two distinct physical qubit types defined in conjugate variables, requiring representation in a continuous space. To address this, we define the FBS noise model, which applies a unitary operation on frequency-bin qubits, enabling a direct comparison of the noise robustness of these protocols and ours (assuming that the former are encoded in frequency-bin qubits). Although rooted in theoretical considerations, this noise model has potential experimental relevance, for

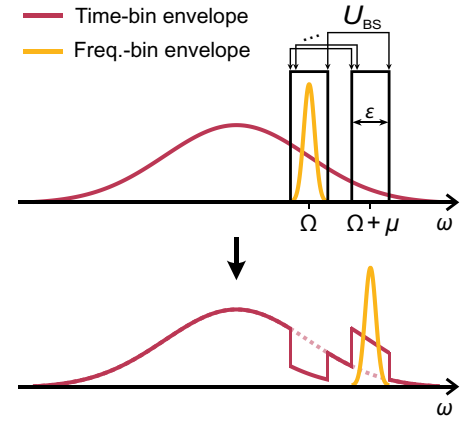


FIG. 3. Schematic of the frequency beamsplitter (FBS) noise model. The FBS model applies a beamsplitter unitary (U_{BS}) across pairs of frequency modes separated by μ over continuous frequency intervals of width ϵ , as shown in the top diagram. For the example of a bit-flip (X) operation on single-photon time-bin and frequency-bin states, this operation transforms the pink and yellow states in the top diagram to the corresponding states in the bottom diagram. The pink curve represents the broad spectral amplitude envelope of time-bin states, while the orange curve depicts a frequency-bin state.

example, in processes such as Bragg-scattering four-wave mixing [33].

1. Frequency beamsplitter model

We first define a single-frequency beamsplitter (BS) operation. A single-frequency BS acts on pairs of single-frequency creation operators $\hat{a}^\dagger(\omega)$ to apply a BS unitary operation, U_{BS} , on the frequency modes in the form $\hat{a}^\dagger(\omega_1) \mapsto \cos \theta \hat{a}^\dagger(\omega_1) + e^{i\phi} \sin \theta \hat{a}^\dagger(\omega_2)$ and $\hat{a}^\dagger(\omega_2) \mapsto -e^{-i\phi} \sin \theta \hat{a}^\dagger(\omega_1) + \cos \theta \hat{a}^\dagger(\omega_2)$. This applies a unitary operation between a pair of single-frequency modes, with rotation noise parameter θ and dephasing noise parameter ϕ .

We now generalize the single-frequency BS to define the general FBS noise model, illustrated in Fig. 3. In the general FBS model, the same (but unknown) single-frequency BS operations act between pairs of frequencies, separated by μ , over continuous frequency intervals of width ϵ . The first interval is centered on frequency Ω and, correspondingly, the second interval is centered on the frequency $\Omega + \mu$. For brevity, we label the FBS noise parameters by $\vec{\epsilon} = (\Omega, \mu, \epsilon)$. The action of this model in the frequency domain is made mathematically explicit in Sec. S.III of the SM and further extended in Sec. S.V of the SM [23].

Before analyzing the impact of the FBS noise model on our encoding, it is helpful to summarize the key parameters introduced so far. The frequency-bin qubit states are parameterized by frequencies Ω_0 and Ω_1 , and Gaussian width σ_ω . The time-bin qubit states are parameterized by

times τ_0 and τ_1 , and Gaussian width σ_t . We then parameterize the FBS noise model as a unitary operation across frequency modes with rotation angle θ and dephasing angle ϕ . This FBS noise acts on frequency bins centered around Ω and $\Omega + \mu$, with a top-hat filter shape of width ϵ .

2. Effect of frequency beamsplitter noise

To analyze the effect of the FBS on our encoding, we must first make assumptions about the relationship of parameters $\vec{\epsilon}$ to $\vec{\Omega}$. We assume that the FBS acts exactly across the frequency-bin states of Alice's encoding (i.e., $\Omega = \Omega_0$ and $\Omega + \mu = \Omega_1$) and that the noise bands are sufficiently wide to capture the frequency-bin amplitude function, as in Fig. 3 (requiring $\epsilon \gtrsim 6\sigma_\omega$ to contain all but a negligible fraction of a Gaussian function). Under these assumptions, the FBS applies a unitary operation on the frequency-bin qubit states $\{|0_f\rangle, |1_f\rangle\}$. Thus, $|0_L\rangle = |\Psi_f^-\rangle$ is unaffected by this noise.

In contrast, the $|1_L\rangle$ state will be affected under the FBS. Due to the broad nature of the time bins in the frequency domain, both $|0_t\rangle$ and $|1_t\rangle$ span both of the FBS bins (pink curve in Fig. 3). Therefore, the FBS does not apply a logical unitary to the time-bin qubit states, but it does change the shape of their distribution (with a dependence on $\vec{\epsilon}, \theta, \phi$), as depicted in Fig. 3 and Fig. S2 of the SM [23]. As with the GVD, the changing time-bin state distribution increases the rate of inconclusive measurement outcomes at Bob due to the probability amplitude “leaking” outside the logical subspace.

To quantitatively analyze the effect this has on the key rate, we consider the states measured by Bob ($|\Psi_t^-\rangle$ and $|\Psi_f^-\rangle$) and the time-bin state arriving at Bob after traversing the FBS noise, which we call $|\Psi_t'^-\rangle$. As a is typically small, we set $a = 0$ here to provide a clearer, more intuitive picture of the scheme's robustness; however, the security analysis in the following section fully accounts for the true, nonzero (albeit small) value of a determined by the chosen encoding parameters. We calculate the fidelities $\mathcal{F}(\Psi_t'^-, \Psi_t^-) = |\langle \Psi_t'^- | \Psi_t^- \rangle|^2$ and $\mathcal{F}(\Psi_t'^-, \Psi_f^-) = |\langle \Psi_t'^- | \Psi_f^- \rangle|^2$, and any phase accumulated by $|\Psi_t'^-\rangle$, as a function of $\vec{\epsilon}, \theta, \phi$, and the encoding parameters $\vec{\tau}$ and $\vec{\Omega}$. In the aforementioned simplified case ($a = 0$), the sum of these fidelities is equal to the probability of Bob measuring a conclusive outcome given that $|\Psi_t'^-\rangle$ arrived. Here, $\mathcal{F}(\Psi_t'^-, \Psi_f^-)$ gives the bit error rate in the logical encoding, and the phase accumulated by $|\Psi_t'^-\rangle$ relative to $|\Psi_t^-\rangle$ and $|\Psi_f^-\rangle$ gives rise to a phase error rate.

The bit error is negligible here and thus has a negligible effect on the key rate. For example, for the experimentally reported parameters used in Fig. 4, $\mathcal{F}(\Psi_t'^-, \Psi_f^-)$ is numerically found to be of the order of 10^{-4} when varying θ and ϕ (giving a reduction in key rate of less than 0.3%). Further, for typical parameters (such as those used in Fig. 4),

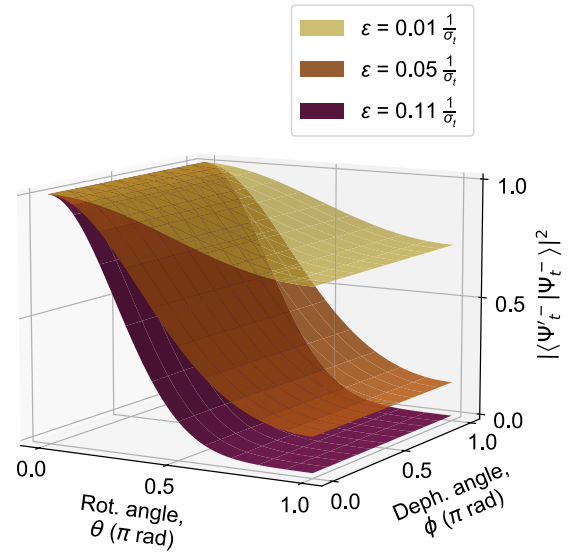


FIG. 4. Robustness of time-bin Bell states under the FBS noise model for varying frequency-noise bin widths, showing the fidelity between the arriving state $|\Psi_t'^-\rangle$ sent by Alice through the FBS channel and the state $|\Psi_t^-\rangle$ measured by Bob. The fidelity is plotted as a function of the FBS channel parameters θ and ϕ . For the simulation, we use a Gaussian time-bin state with parameters $\tau_0 = 0$ ps, $\tau_1 = 220$ ps, and $\sigma_t = 17$ ps (values experimentally reported in Ref. [34]) and FBS noise parameters $\Omega = 195.860$ THz and $\Omega + \mu = 195.879$ THz, with varying width $\epsilon = 0.6, 3.0$, and 6.6 GHz (close to experimentally reported values for a frequency-bin Bell-state encoding in Ref. [35], with $\epsilon = 6\sigma_\omega$). In the legend, we express ϵ as a fraction of the time-bin state's width in the frequency domain ($\propto 1/\sigma_t$). We take the central frequency of the time-bin state to equal Ω .

the accumulated relative phase is small and has minimal effect on the key rate. Therefore, the effect of the FBS on the key rate is dominated by $\mathcal{F}(\Psi_t'^-, \Psi_t^-)$. Further details about the accumulated phase and bit error can be found in Secs. S.III B 2 and S.III C of the SM [23], respectively.

Figure 4 shows the fidelity $\mathcal{F}(\Psi_t'^-, \Psi_t^-)$ of a time-bin Bell state under an FBS, using experimentally reported values, for various noise bin widths ϵ , as a function of θ and ϕ . We observe that the state fidelity is approximately independent of the FBS dephasing angle ϕ , and it reduces with FBS rotation angle θ . As ϵ decreases, the fidelity is higher for a given θ and ϕ . If the time-bin states are sufficiently wide in the frequency domain ($\propto 1/\sigma_t$) compared to ϵ , the effect of the noise on the time-bin states is small. Thus, our encoding will show a high rate of conclusive outcomes at Bob, giving high key rates, for any values of the noise parameters θ and ϕ . The detailed analytical expression for $\mathcal{F}(\Psi_t'^-, \Psi_t^-)$ using Gaussian amplitude functions and the study of further parameter dependence is presented in Sec. S.III B of the SM [23].

In this analysis, we demonstrated the robustness of our encoding against variations in noise parameters using fixed

settings. Alternatively, our protocol can be adapted by optimizing the encoding parameters to enhance robustness when noise fluctuations can be characterized, as detailed in Appendix C. The fixed-parameter approach is ideal when noise characterization is impractical, while the second strategy enables fine-tuned performance in scenarios where detailed noise characterization is possible.

Overall, the effect of the FBS noise channel can be effectively understood as an amplitude damping and decoherence channel on our logical states, where the damping probability and decoherence phase are dependent on the channel noise parameters $\vec{\epsilon}$, θ , and ϕ .

In Appendix D, we highlight the advantages of our proposed encoding compared to alternative continuous-DOF encodings with only two photons. Specifically, we demonstrate how our use of both time-bin and frequency-bin qubits allows us to make fewer assumptions about the channel-noise model.

IV. SECURITY ANALYSIS

In this section, we present a comparative security analysis of our protocol against existing ones that are robust against collective unitary noise [17,18] and the standard BB84 protocol [1] under the FBS model introduced above. We extend this model to analyze the security under experimentally realistic noise fluctuations by using a probabilistic value for the noise parameter θ . Subsequently, we compare these schemes under a lossy channel, additionally including TF-QKD in the analysis. Despite its alternative setup—featuring two senders and a central measuring device, unlike the prepare-and-measure BB84-type scheme used by the others—the inclusion of TF-QKD allows for a rigorous comparison of our protocol with state-of-the-art approaches. We conclude by discussing how the stabilization techniques required for TF-QKD and BB84 affect their key rates and implementation overheads. We leave the analysis of Ref. [19] to Sec. S.VI B of the SM [23], as it does not contribute further insights to the main discussion.

It is worth noting that the protocols in Refs. [17–19] were developed during the early years of QKD, when robustness against specific individual attacks was the primary focus. Here, we harness more recent developments in numerical techniques for QKD security analysis to provide asymptotic secure key rates that are valid against any collective attack. More precisely, we use the framework developed in Ref. [36] to compute an asymptotic lower bound on the secure key rates for each of the protocols listed above, as well as our proposed implementation. We provide an explanation and full details of the analysis methods used in Sec. S.VII of the SM [23].

A. Noise-robust protocols under the FBS channel

In this subsection, we consider Refs. [1,17–19] implemented using frequency-bin qubits (with a width less

than the noise-bin widths, i.e., $\epsilon \gtrsim 6\sigma_\omega$). With this encoding, their security can be analyzed by examining the effects of a collective unitary operation (Appendix A) on the physical qubit states, as described in the previous section.

By contrast, the FBS channel affects our logical encoding differently, causing amplitude damping and decoherence at the logical level (see Sec. III B 2). To evaluate the key rate while accounting for the two-photon nature of our states, we reformulate the continuous-DOF single-photon frequency-bin and time-bin qubit states of Eq. (3) into a discrete orthonormal ququart basis (see Sec. S.VII B 2 of the SM [23]). By inverting this mapping, we can express our logical states in a two-ququart basis. Then, using the overlaps between the single-photon states comprising Bob’s measurement projectors and the noise-transformed single-photon states arriving at him, we construct a channel acting on this ququart basis (as detailed in Sec. S.VII C 1 of the SM [23]).

The resulting key rates are close to those of BB84 subject to an amplitude damping and decoherence channel, where the fidelities of our encoding under the FBS (Fig. 4) determine the amplitude damping, while the accumulated phases correspond to the decoherence phase for each set of noise parameters $(\vec{\epsilon}, \theta, \phi)$ (see Sec. S.VII C 2 of the SM [23]). This confirms that considering the channel’s action on the states at the logical level in the previous section (i.e., without explicitly introducing the full ququart basis) provides a meaningful intuition, as it suffices to capture the impact of the noise on the key rate. Indeed, although a more detailed treatment is necessary for the completeness of the security analysis, this yields results that are effectively equivalent.

Figure 5 shows the secure key rates of the different protocols in a lossless FBS channel as a function of the unitary rotation angle θ , with other parameters fixed. The FBS noise and the encoding parameters match those of the surfaces in Fig. 4. The key rate is symmetric in θ about $\theta = \pi$ for all protocols due to the symmetry of the FBS operation under θ . In Secs. S.VI A and S.VIII of the SM [23], we provide an additional analysis showing the key rate’s ϕ dependence (which is small for all protocols presented).

The three- and four-photon protocols in Ref. [18] perfectly cancel collective unitary noise; therefore, their key rates are maximal for both unitary parameters (θ, ϕ) in a lossless channel. We illustrate this with the flat-line reference plot in Fig. 5, and we need not consider the noise robustness further here.

We now analyze the one- and two-photon protocols. Our protocol shows a substantial improvement in key rate compared to Refs. [1,17] for $0 < \theta \lesssim 0.4\pi$. As the noise width reduces relative to the time-bin width in the frequency domain, the key-rate robustness to θ increases (blue curves in Fig. 5). With sufficiently narrow FBS noise bins or optimized σ_t of our states, the key rate of our protocol remains nonzero for all unitary parameters (θ, ϕ) , unlike

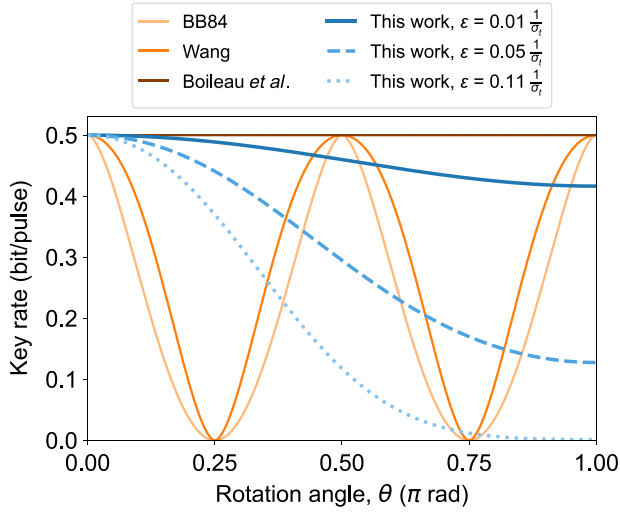


FIG. 5. Comparison of key rates as a function of FBS noise parameter θ (with $\phi = 0$) for collective-unitary-noise-robust protocols. Key rate in an FBS channel with unitary parameter θ of BB84, Wang (2005) [17], Boileau *et al.* (2004) [18], and our protocol for the states and noise outlined in Fig. 4 (Gaussian states with $\tau_0 = 0$ ps, $\tau_1 = 220$ ps, $\sigma_t = 17$ ps, and noise parameters $\Omega = 195.860$ THz, $\Omega + \mu = \Omega_1 = 195.879$ THz, and $\epsilon = 6\sigma_\omega = 0.6, 3$, and 6.6 GHz). The action of the FBS on the DV protocols is analyzed as a collective unitary operation on frequency-bin qubits. BB84 and Ref. [17] show less robustness to the FBS noise than our approach. Unlike our scheme, the key rates of BB84 and Ref. [17] vanish when θ varies with time due to their key rate oscillating with θ [see model in Eq. (8)]. Reference [18] exhibits the highest key rate and robustness under FBS noise; however, it has the worst scaling with loss of the examined protocols (see Sec. IV B).

Refs. [1,17]. This, combined with preventing the accumulation of a bit error rate, is advantageous for our encoding when experimental time variations of noise parameters are accounted for.

We demonstrate this by updating the FBS channel model to instead consider random mixtures of parameters. We now model the channel as an FBS with fixed parameter values θ_i with probabilities p_i , so that the channel map becomes

$$\rho_N \rightarrow \sum_i p_i \hat{F}_{\theta_i}^{\otimes N} \rho_N \hat{F}_{\theta_i}^{\dagger \otimes N}, \quad (8)$$

where we define $\hat{F}_\theta$ as the action of the FBS with parameter θ and all the other unspecified parameters $\vec{\epsilon}$ and ϕ kept fixed. In our simulation, we consider points of θ_i uniformly sampled between 0 and 2π .

Under Eq. (8), we find that the key rates for both Ref. [1] and Ref. [17] vanish. Indeed, while a positive key can be obtained in both the regimes $\theta < \pi/4$ and $\theta > \pi/4$, these two regimes correspond to Alice's and Bob's bit values being correlated and anticorrelated, respectively. As a

result, under a random mixture of θ , no correlation can be established. In contrast, our protocol can maintain a positive key rate since the bit values remain correlated throughout the parameter range. The dotted, dashed, and solid blue lines in Fig. 5 achieve rates of 0.124, 0.278, and 0.457 bit/pulse, respectively. This also shows that a significant key rate can be achieved even with nonoptimal encoding parameters (e.g., due to only partial channel characterization) provided that an upper-bound estimate on ϵ is available.

B. Noise-robust protocols in lossy channels

We now present the analysis of different DV-QKD protocols across a loss-only channel. Figure 6 shows the key-rate dependence of our protocol, noise-robust protocols with a varying number of photons per logical state [17,18], BB84 [1], and TF-QKD [10]. These results highlight quantitatively the loss-noise robustness trade-off discussed earlier and presented in Table I (and Appendix A). From Fig. 6 we confirm that, for a given channel loss, the key rate scales exponentially with the number of photons in a protocol; however, as seen in Fig. 5, reducing the number of photons in a logical state decreases the protocol's robustness to noise, underscoring the trade-off.

Our scheme requires only two photons per logical state, and it thus scales better with loss than other noise-robust protocols. Meanwhile, by exploiting nontrivial encodings in continuous DOFs, it leads to an increased parameter robustness compared to the existing methods with two or fewer qubits (Fig. 5). Therefore, by optimizing the encoding parameters to expected noise fluctuations (Fig. 4 and Appendix C), our approach can surpass the key rates of previously proposed noise-robust schemes.

In Sec. S.VI of the SM [23], we present further discussion of the observed key rates for Refs. [17–19], and we compare the rates to the security predicted in their works. In Sec. S.IX of the SM [23], we also address security considerations that are relevant for realistic implementations that use photon-pair sources with imperfect photon-number purity. We justify that decoy-state methods can be applied within our scheme, ensuring security against photon-number-splitting (PNS) attacks.

C. Compensation techniques for BB84 and TF-QKD

By construction, the BB84 [1] and TF-QKD [10] schemes scale better with loss than the noise-robust protocols, achieving higher key rates over longer distances; however, implementing these protocols in practice relies on extensive compensation and stabilization techniques to mitigate the effects of channel fluctuations (discussed further in Appendix A) [9,11,13–15,38–40]. These methods require allocating a portion of the pulses to estimating the noise, reducing the fraction available for establishing a shared secret key [38–40].

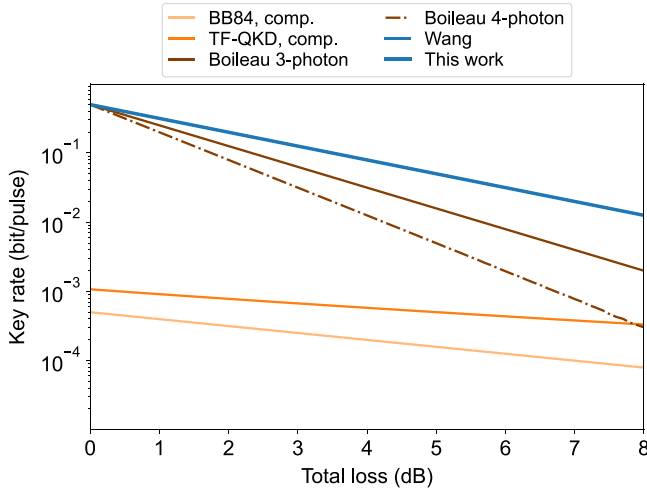


FIG. 6. Key rate as a function of channel loss in dB for collective-unitary-noise-robust protocols and commonly implemented QKD protocols. Comparison of the key-rate scaling with loss for various protocols in a lossy channel. Our scheme and the existing collective-unitary-noise-robust approaches [17,18] show a BB84 scaling (scaling as η) with loss. For these, the key rate for a given loss scales exponentially with the number of photons in the logical qubit state. Our protocol and that of Ref. [17] use the same number of photons per logical state, and they thus show the same loss dependence (thick blue line); however, the protocol of Ref. [17] shows worse performance than our scheme under channel noise (Sec. IV A, cf. Fig. 5). For comparison, we also show the key rate for BB84 [1] (simulated) and TF-QKD [10] (analytically calculated in Ref. [37], with $\mu = \mu_{\text{opt}} = 0.1146$), accounting for noise-compensation techniques that are necessary for the operation these protocols, unlike the noise-robust schemes.

To account for compensation, in Fig. 6, we present key rates for BB84 and TF-QKD as experimentally reported using these techniques. For BB84 with polarization compensation, Ref. [38] presents a secret-key rate of 80 bit/s with 40-dB loss and a transmission rate of 50 MHz. Converting this to a key rate in bits per pulse, and accounting for detection losses, this corresponds to an order 10^3 reduction in key rate. For TF-QKD, Ref. [14] reports a secret-key rate of 9.22×10^{-10} bit/pulse at 106-dB loss. Accounting for detection and component losses, this corresponds to an order 10^2 reduction in key rate. We note that experiments employing different stabilization methods will result in slight variations of the key-rate reduction factor. An exhaustive analysis of the experimentally achieved key rates would require a more open discussion of experimental downtimes, duty cycles, and other factors affecting the total average key rate; however, detailed data in this area are currently limited. In Appendix E, we include the theoretical key rates of BB84 and TF-QKD for a complete comparison. Additionally, we present the key rate in bits

per second (another important figure of merit for assessing real-world practicality), based on the estimated rate at which our logical states can be generated experimentally.

V. DISCUSSION

In this work, we introduced an approach to encoding logical qubits for QKD, where they are represented within subspaces of continuous photonic DOFs. Specifically, we define a nontrivial orthonormal basis in the frequency domain from superpositions of antisymmetric Bell states defined in frequency-bin and time-bin qubits. Antisymmetry is employed for its noise-resilient properties, while the use of a continuous DOF enhances loss robustness by reducing the number of photons per logical state. Our analysis demonstrates that this scheme offers superior resilience to loss and noise compared to existing methods under realistic noise fluctuations. Furthermore, it eliminates the need for the extensive stabilization typically required in state-of-the-art protocols, which often entails significant operational complexity and imposes limited duty cycles. This passive robustness may be especially advantageous in environments where active compensation is impractical or unstable, such as channels with rapidly varying noise. We also outlined a viable experimental implementation of our protocol, showcasing the near-term applicability of these findings for scalable QKD networks. More broadly, our work highlights the importance of considering industrial scalability—not just loss scaling or one-off implementation overhead—when evaluating QKD protocols. By avoiding active compensation and relying on compact, replicable components, our approach is well positioned for deployment at scale.

Recent works have explored architectures for quantum repeaters based on concatenated bosonic error-correcting codes, leveraging Gottesman-Kitaev-Preskill (GKP) qubits for their inherent loss-resilient properties [41–44]. While our protocol does not rely on error correction, it shares a conceptual connection with these approaches by exploiting redundancies in continuous photonic DOFs to achieve resilience against noise. Practical realization of GKP states, however, remains a significant experimental challenge, particularly in optical implementations, with only recent progress reported [45]. Alternative strategies, such as that proposed in Ref. [46] for optical quantum computing, address these challenges by encoding GKP qubits in a fixed number of excitations superposed across frequency and time modes, rather than the typical bosonic codes, which encode qubits in superpositions of the number of excitations within a single mode. This approach provides a more experimentally feasible route to the implementation of optical bosonic error-correcting codes.

Similar to the method presented in Ref. [46], our approach employs a fixed number of excitations in a superposition across modes of a continuous photonic DOF to

improve the practical feasibility; however, the encoding we propose is specifically tailored for QKD applications, enabling the use of simpler states since only noise robustness, rather than full error correction, is required. Our approach opens promising directions for exploring alternative encodings in continuous photonic DOFs for quantum information tasks, extending beyond the scope of QKD.

A natural extension of this research would be to adapt our encoding strategy to develop a general methodology for designing implementation-specific encodings. Such a framework could be optimized for robustness against experimentally characterized noise channels and their expected noise fluctuations, while minimizing the impact of loss. For example, by modeling and parameterizing the noise channel, and characterizing the expected fluctuations of its parameters, it could be possible to develop tools that output optimal encoding spectral functions and their parameters for a given implementation. Additionally, while our encoding is not compatible with some widely used protocols like TF-QKD, it could hold promise for other QKD protocols, such as device-independent QKD [47].

Beyond these immediate extensions, our work reveals a counterintuitive result: antisymmetric Bell states in frequency-bin and time-bin modes, despite their conjugate nature, can be made perfectly orthogonal. This property may have deeper connections to foundational topics in quantum mechanics, such as the nature of Einstein-Podolsky-Rosen steering [48]. While our results clearly establish the utility of this encoding for QKD, they also suggest broader implications for leveraging foundational principles in practical quantum technologies. We envision that these ideas could inspire approaches across the field of quantum information, bridging foundational insights with real-world applications.

ACKNOWLEDGMENTS

We thank B. Baragiola, A. Boubriak, M. Clark, M. Jones, and P. Skrzypczyk for useful discussions. H.S. acknowledges financial support from EPSRC Quantum Engineering Centre for Doctoral Training Grant No. EP/SO23607/1. E.L. acknowledges support from the Engineering and Physical Sciences Research Council (EPSRC) Hub in Quantum Computing and Simulation (EP/T001062/1). T.S. acknowledges that they received no funding in support of this research. M.P.S. acknowledges support from the EPSRC Quantum Engineering Centre for Doctoral Training EP/SO23607/1 and the European Commission through Starting Grant No. ERC-2018-STG803665 (PEQEM). G.R. acknowledges support from the Royal Commission for the Exhibition of 1851 through a Research Fellowship, from the European Commission through Starting Grant No. ERC-2018-STG803665 (PEQEM) and Advanced Grant No.

ERC-2020-ADG101021085 (FLQuant), and from EPSRC through Standard Proposal Grant No. EP/X016218/1 (Mono-Squeeze).

The conceptualization and methodology for this project were developed by G.R. and H.S. All authors contributed to the validation and interpretation of this work. E.L. and H.S. carried out the formal analysis. Visualization was conducted by G.R. and H.S. G.R. supervised the work. All the authors contributed to scientific discussion, reviewed the draft, and approved the final manuscript.

The authors declare that they have no competing interests.

DATA AVAILABILITY

The data that support the findings of this article are openly available [49,50].

APPENDIX A: FUNDAMENTAL TRADE-OFF BETWEEN LOSS-ROBUST AND NOISE-ROBUST QKD

In this appendix, we outline the collective unitary noise channel and the loss channel models considered for the analysis of Refs. [17–19]. We then discuss the overheads of employing compensation techniques to mitigate noise fluctuations and the limitations these present for the industrial scalability of QKD implementations. Finally, we explain the loss-noise robustness trade-off in more detail. We highlight this with the specific example of protocols that exploit antisymmetry for robustness to collective unitary noise, such as those in Refs. [17–19].

1. Collective unitary noise channel

A collective unitary noise channel applies the same unknown unitary U to all qubits in a given N -qubit state, ρ_N , transforming the state as

$$\rho_N \rightarrow U^{\otimes N} \rho_N U^{\dagger \otimes N}. \quad (\text{A1})$$

2. Loss channel

A lossy channel absorbs or loses a photon in transmission with probability p . All N photons in a logical qubit state must arrive at the receiver for the state to be successfully transmitted. Under a lossy channel, the state transforms as

$$\rho_N \rightarrow p^N \rho_N + (1 - p^N) \rho_{\perp}. \quad (\text{A2})$$

We define $\rho_{\perp}$ as a state in the subspace in which one or more photons are lost to the channel, and this will result in an inconclusive measurement outcome due to loss.

3. Compensation techniques

Compensation techniques are required by protocols that do not have inherent noise resilience, such as BB84 (including decoy-BB84) and TF-QKD. Without stabilization against channel fluctuations, noise leads to an overwhelming error rate, rapidly rendering key sharing insecure. Compensating noise results in a large resource cost (such as long servo channels and active feedback loops [13]), which limits the practical scalability of real-world implementations of QKD. For example, TF-QKD experiments require stabilizing the phase, frequency, and polarization of two sources arriving at a central node from separate locations. These stabilization tasks have been addressed in various ways, although each introduces its own level of complexity. Frequency locking can be achieved using common laser sources [14,15], while polarization stabilization was demonstrated using active feedback from the central detectors [9,11–15]. Phase stabilization typically relies on techniques such as time and wavelength multiplexing to track phase fluctuations via reference signals [9,13], or postprocessing approaches that estimate and correct phase drift using reference-frame time blocks [12]; however, all these methods come at the cost of increased system complexity, requiring multiple active control loops and tightly coordinated reference frames. While feasible in well-controlled, point-to-point links, as noted in Ref. [7], such schemes pose serious challenges for scalability, particularly in dynamic or multiuser network settings, where the overhead of independent stabilizing controllers quickly becomes prohibitive.

In addition to the physical resources required, stabilization techniques require continuous monitoring of channel fluctuations. Typical methods involve interleaving data and reference pulses in time [12,13,15], or monitoring the QBER using a significant fraction of the sifted shared key [38–40]. These methods inevitably reduce the protocol's effective duty cycle, as a fraction of pulses must be reserved for stabilization rather than key generation. Specifically, once a channel's stability degrades, reference pulses must be sent (in place of signal pulses) to estimate the current noise parameters of the channel and inform adjustments to the stabilizing components (e.g., motorized waveplates for polarization compensation). Consequently, only a fraction of operational time contributes to secret-key generation, with the remainder consumed by channel monitoring and correction. As discussed in Sec. IV C of the main text, this leads to orders-of-magnitude reductions in the effective key rate in state-of-the-art decoy-state BB84 and TF-QKD implementations.

While a complete survey of the compensation burdens across all QKD architectures is beyond the scope of this manuscript, it is well supported in the literature that such requirements—in terms of both hardware complexity and active control overhead—are a persistent challenge for large-scale and cost-effective deployment.

4. Loss-noise robustness trade-off

To circumvent the extensive overheads associated with compensating noise fluctuations, encoding inherently noise-resilient states can be considered. Designing a secure QKD scheme requires at least two nonorthogonal states and measurements in their respective bases [51]. Collective-unitary-noise-robust protocols proposed to date [17–20] use the invariant property of the antisymmetric Bell state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$ under local unitary transformations, i.e., $(U \otimes U)|\Psi^-\rangle = e^{i\Delta}|\Psi^-\rangle$, where Δ is some unobservable U -dependent global phase factor [24]; however, $|\Psi^-\rangle$ is the only two-qubit state satisfying invariance under the action of a collective unitary [52]. Thus, two perfectly noise-canceling nonorthogonal bases using only two qubits cannot be found. By introducing more qubits into a logical state, noise-robust subspaces of at least dimension 2 can be found. A QKD protocol that is perfectly noise-canceling against collective unitary noise can be devised when the logical state contains three or four qubits, as in Ref. [18].

Qubits in QKD are typically encoded in photonic degrees of freedom, since photons are natural information carriers [53,54]. QKD protocols devised with higher noise robustness thus use more photons per logical state; however, the key rate scales exponentially with the channel loss probability of a logical qubit, and the loss probability itself scales exponentially with the number of photons (i.e., physical qubits) in the logical state [Eq. (A2)]. Therefore, we arrive at a trade-off between loss robustness and noise robustness: increasing the number of physical qubits (i.e., photons) per logical qubit state for the purpose of noise cancelation leads to an exponential decrease in the key rate for a given transmission distance. We qualitatively illustrate this trade-off in Table I. To overcome this trade-off, we encode a fixed number of photons in a continuous DOF, rather than the tensor-product space of many qubit Hilbert spaces, in a conceptually similar manner to bosonic codes [41,46].

APPENDIX B: STATE GENERATION AND MEASUREMENT

Implementing our protocol requires generating antisymmetric Bell states in frequency bins and time bins, and superpositions of these. Antisymmetric Bell states in frequency bins can be produced through spontaneous parametric down-conversion (SPDC) [55] or spontaneous four-wave mixing [35], i.e., processes that involve pumping nonlinear crystals. Entangled time-bin qubit states can be created using optical switches [56]; however, similarly to frequency-bin states, time-bin Bell states can also be generated by pumping a domain-engineered nonlinear crystal [57,58] (or by performing quantum optical synthesis in two-dimensional time-frequency space [59]). By producing the antisymmetric time-bin Bell state in

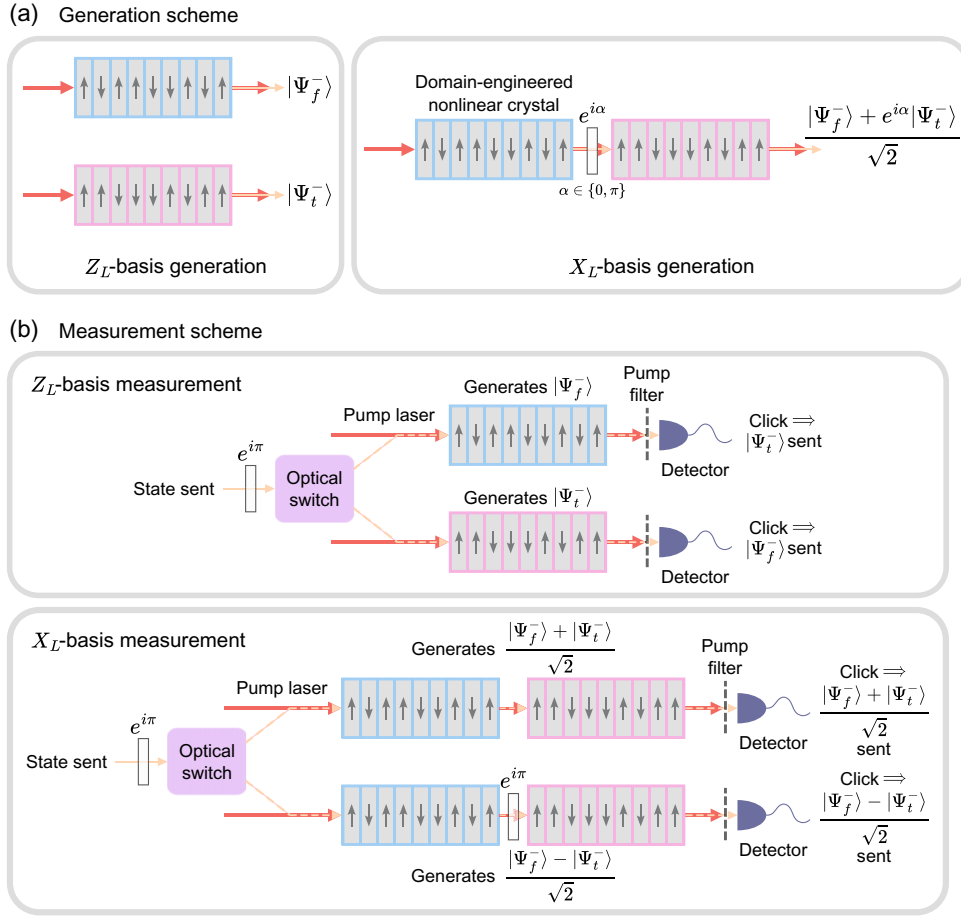


FIG. 7. Illustration of the proposed measurement and generation schemes for the logical Z and X basis states. (a) Antisymmetric frequency-bin and time-bin Bell states can be generated through domain engineering nonlinear crystals and pump engineering. Superpositions of the frequency-bin and time-bin antisymmetric Bell states can be generated by precisely tuning the phase difference α of the pump between the two domain-engineered crystals for the time-bin and frequency-bin state. (b) A logical Z -basis measurement and logical X -basis measurement can be made with a 50% incurred loss by destructively interfering the incoming states with one of the basis states. An optical switch is used to randomly measure for either the $|0_L\rangle$ or the $|1_L\rangle$ states in the Z_L basis or randomly measure for either the $|+_L\rangle$ or the $|-_L\rangle$ states in the X_L basis. If the incoming state is in the same state as the photon pair being generated, there will be no click at the detector (this cannot be distinguished from channel loss). Conversely, if there is a click at the detector, Bob infers that the state sent by Alice is opposite to the state generated by the detector's associated setup. (In this figure, we have assumed $\langle \Psi_f^- | \Psi_t^- \rangle \approx 0$.)

this way, superpositions of the frequency-bin and time-bin states can be made by coherently pumping crystals with different domain engineering and implementing a set phase relationship between these crystals [60,61] [see Fig. 7(a)]. It should be noted that this state-generation method uses a probabilistic process that can produce multipair emissions, introducing a vulnerability to PNS attacks, where an eavesdropper could exploit extra photon pairs to gain information; however, in Sec. S.IX of the SM [23], we clarify how a decoy-state extension of our scheme can mitigate this risk, ensuring security in such implementations.

To estimate the state-generation rates for our scheme, we extrapolate from existing experimental work on

photon-pair generation using SPDC. Specifically, we model a type-0 SPDC process in periodically poled lithium niobate and normalize our photon rates to the values reported for such a source in Ref. [62]. Using a 5-cm-long crystal with a poling period of 19.1 μm , we find that antisymmetric frequency states with 1-nm bandwidth could be generated at a rate of 10^9 pairs/s [50]. Our simulation assumes lossless spectral filtering of both photons using 1-nm broad filters with a Gaussian shape, which in a real source would be replaced by domain engineering in the crystals, a technique that has been demonstrated in Ref. [63]. This would simultaneously allow for the generation of the time-bin states.

Performing measurements in the logical Z_L and X_L bases is a harder challenge to tackle. Here, we outline one possible method for performing the measurements, based on reverse engineering the state-generation process. For example, consider making a measurement to distinguish $|-_L\rangle = 1/\sqrt{2}(|\Psi_f^-\rangle - |\Psi_{\perp f}^-\rangle)$ from $|+_L\rangle = 1/\sqrt{2}(|\Psi_f^-\rangle + |\Psi_{\perp f}^-\rangle)$. To do this, Bob generates the state $|+_L\rangle$ by coherently pumping domain-engineered crystals with the correct relative phase (as proposed above for state preparation). This setup is aligned such that it has the opposite phase to the incoming signal and thus destructively interferes with the incoming state. If the state $|+_L\rangle$ has been sent by Alice, the two states will destructively interfere [60] and a loss will be measured. If, instead, the state $|-_L\rangle$ is sent on the setup generating state $|+_L\rangle$, then part of the amplitude will constructively interfere and photons will be measured at the detector. Therefore, if photons are detected out of the setup generating the state $|+_L\rangle$, Bob concludes that the state sent was $|-_L\rangle$, whereas if a loss is measured, the result is inconclusive. To make this a balanced measurement, Bob should generate $|+_L\rangle$ only 50% of the time. The other 50% of the time, Bob generates $|-_L\rangle$ to infer whether the state $|+_L\rangle$ was sent. Identically, this process could be used to perform the Z_L basis measurement. This measurement process works with an incurred 50% loss; thus, the key rate is reduced by a factor of 0.5, but the scaling of the key rate with the channel loss is identical (scaling as η^2). This measurement scheme is illustrated in Fig. 7(b).

The proposed scheme requires a simple experimental setup, though it is not perfectly faithful to our theoretical model. Specifically, it allows Z_L - and X_L -basis measurements to be made, but it does not distinguish inconclusive outcomes (i.e., the projector $|\perp_L\rangle\langle\perp_L|$), which instead manifest as bit errors for this implementation.

This setup underscores the experimental feasibility of our protocol. Its simplicity highlights the practical potential for near-term applications. Optimizing this measurement scheme to account for inconclusive outcomes due to noise is beyond the present scope and would merit a dedicated study. This proposal provides a valuable foundation for further progress toward this goal.

APPENDIX C: OPTIMIZATION OF ENCODING PARAMETERS OF FBS NOISE FLUCTUATIONS

In Fig. 8, we present the fidelity $\mathcal{F}(\Psi_t^-, \Psi_t^-)$ of a time-bin Bell state with varying widths, σ_t , under the FBS for a range of noise-bin widths ϵ and rotation angles θ . By finding the fidelity over a range of FBS variables and varying the Bell-state parameters, this highlights how the encoding can be optimized for robustness to characterized fluctuations in the noise parameters. Here, we observe increasing fidelity over the range of FBS variables given as σ_t decreases. Therefore, for noise that fluctuates over

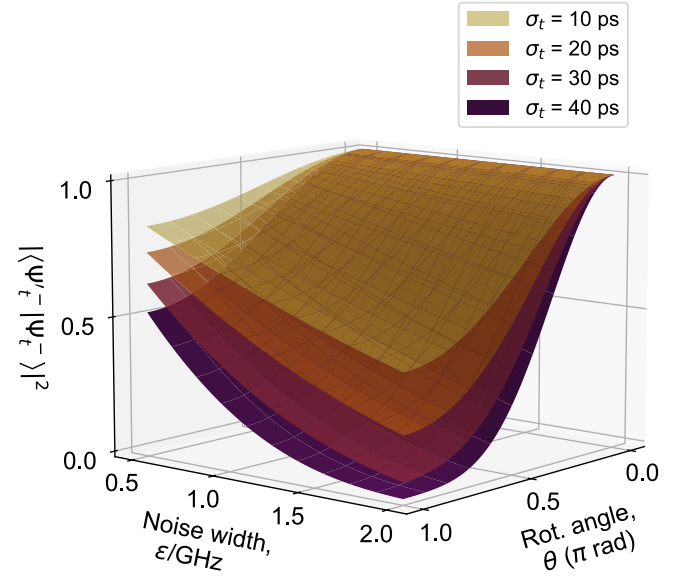


FIG. 8. Robustness of time-bin Bell states with varying bin width under the FBS noise model, as a function of noise-bin width and rotation angle, showing the fidelity between the arriving state $|\Psi_t^-\rangle$ sent by Alice through the FBS channel and the state $|\Psi_t^-\rangle$ measured by Bob. The fidelity is plotted as a function of the FBS channel parameters ϵ and θ . For the simulation, we use Gaussian time bins with parameters $\tau_0 = 0$ ps, $\tau_1 = 220$ ps, and values experimentally reported in Ref. [34], with a central frequency assumed at 195.860 THz and varying $\sigma_t = 10, 20, 30$, and 40 ps. The fixed FBS noise parameters are $\Omega = 195.860$ THz, $\Omega + \mu = 195.879$ THz, and $\phi = 0$, and varying width $\epsilon = 0.6, 3.0$, and 6.6 GHz (close to experimentally reported values for a frequency-bin Bell-state encoding in Ref. [35], with $\epsilon = 6\sigma_\omega$). The key rate can be optimized by reducing σ_t .

the ranges given for ϵ and θ in Fig. 8, σ_t is optimized when it is sufficiently small to ensure that the fidelity never falls to zero, giving nonzero key rates without compensation.

APPENDIX D: COMPARISON OF OUR ENCODING TO ALTERNATIVE CONTINUOUS-DOF ENCODING SCHEMES

Given that the time-bin states are not perfectly robust against the FBS noise model, it is worth comparing our encoding scheme to alternative but similar encodings in the continuous space. The advantage of our protocol is that fewer assumption on the noise model are needed compared to other continuous-DOF encodings while still achieving a robust key rate. We highlight this with a couple of example cases.

First, let us consider instead encoding purely in Bell states of two pairs of frequency bins, such that $|0_L\rangle = |\Psi_f^-\rangle_{01,MN}$ and $|1_L\rangle = |\Psi_f^-\rangle_{23,MN}$, where $|\Psi_f^-\rangle_{ab,MN} = (|a_f\rangle_M |b_f\rangle_N - |b_f\rangle_M |a_f\rangle_N)/\sqrt{2}$. Thus, $|0_L\rangle$ is the anti-symmetric frequency-bin Bell state on modes M and N

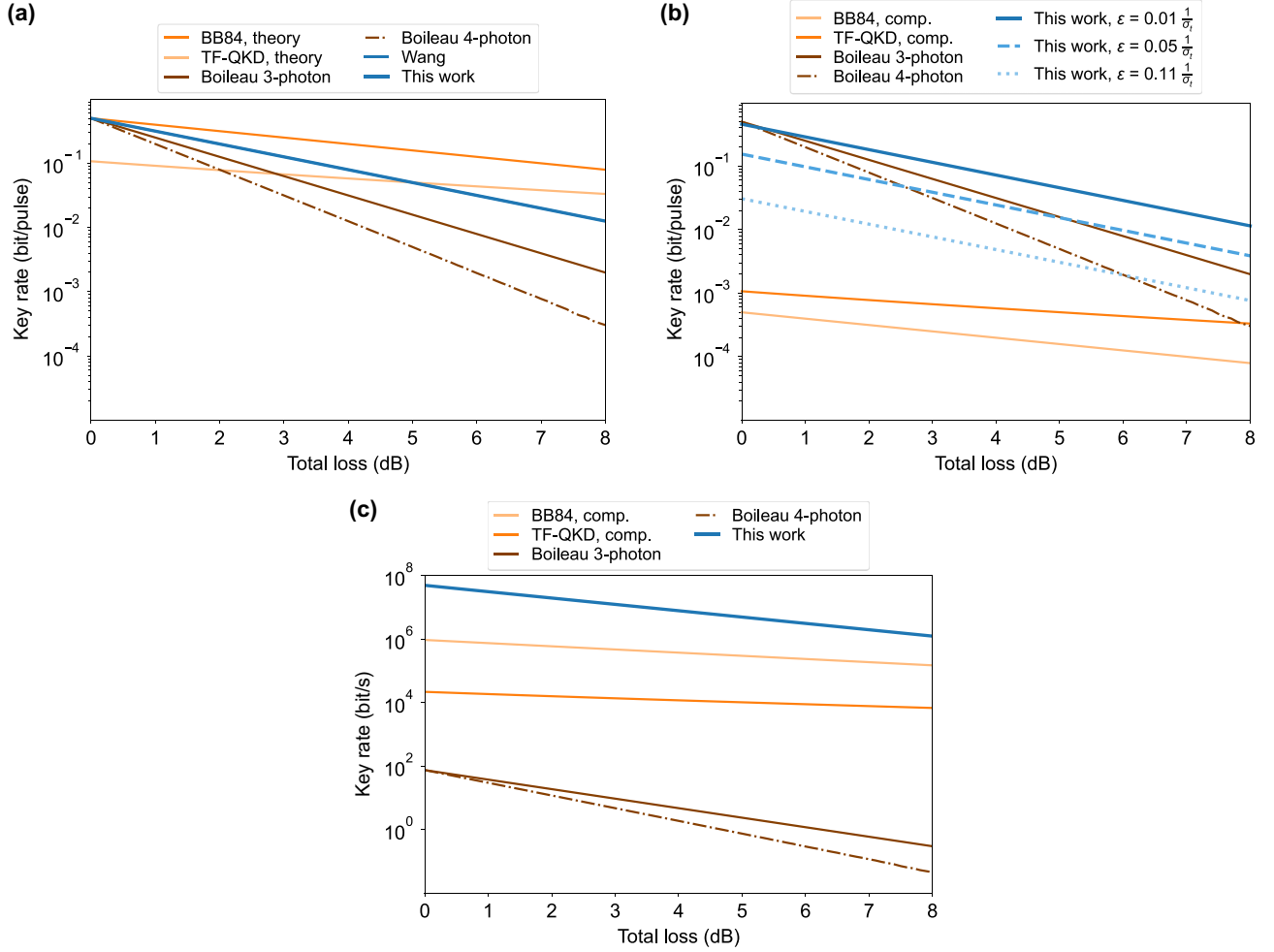


FIG. 9. Key rate as a function of channel loss for collective-unitary-noise-robust and commonly implemented QKD protocols under theoretical and experimental conditions. (a) Comparison of the key rate in a lossy but otherwise ideal channel. TF-QKD and BB84 perform efficiently due to using low numbers of photons per shared bit; however, under experimental noise conditions, BB84, TF-QKD, and Ref. [17] require extensive stabilization techniques to mitigate the effects of noise. These lower the shared key rates and come with substantial overheads, as shown in (b). In contrast, our protocol and those in Ref. [18] do not require noise compensation. (b) Comparison of the key rate in a lossy channel when the effects of noise are accounted for. Noise scales the key rate of our noise-optimized protocol by only an order of 1 (see Sec. IV A). Conversely, the compensation techniques required for BB84, TF-QKD, and Ref. [17] lower the key rates by orders of magnitude. (c) Comparison of the key rates in bits per second in a lossy but otherwise ideal channel. Rates for BB84 and TF-QKD are extracted from experimental literature, while those for our protocol and Ref. [18] are estimated based on simulations informed by experimental data. Our protocol achieves significantly higher key rates than existing approaches under realistic assumptions, maintaining competitive performance even when considering experimentally feasible generation rates of our time- and frequency-entangled two-photon states.

over frequency-bin states $|0_f\rangle = |\Omega_0\rangle$ and $|1_f\rangle = |\Omega_1\rangle$, and $|1_L\rangle$ is the antisymmetric frequency-bin Bell state on modes M and N over new frequency-bin states $|2_f\rangle = |\Omega_2\rangle$ and $|3_f\rangle = |\Omega_3\rangle$. To have no logical bit error rate on this basis, this encoding makes the assumption that the FBS acts between states $|0_f\rangle$ and $|1_f\rangle$ and between $|2_f\rangle$ and $|3_f\rangle$ only (or outside this subspace). If we instead allow the noise to act across these the two frequency-bin Bell states (e.g., between states $|0_f\rangle$ and $|2_f\rangle$ and between states $|1_f\rangle$ and $|3_f\rangle$), the protocol accrues a bit error rate and an incurred loss at the measurement stage. In contrast,

if we allow this model of unitary noise on our proposed encoding (i.e., the FBS noise acting between the encoded frequency bins and frequency bins outside that space), negligible bit error rate and only an extra loss at measurement is incurred. We quantify this in Sec. S.X A of the SM [23].

Our chosen encoding also allows us to alleviate another assumption on the noise channel. We assumed in Sec. III B that the noise acts between frequency bins. By encoding one basis state in frequency bins and one basis state in time bins, we allow the possibility that the noise instead acts between time bins while maintaining the robustness of the

encoding. In contrast, the fidelity of the above encoding would degrade more than our proposed encoding. Thus, our encoding is more robust under fewer noise constraints.

If the channel takes the states $|0_f\rangle$ to $|0_r\rangle$ and $|1_f\rangle$ to $|1_r\rangle$, our encoding is no longer robust. In this case, however, a simple change in measurement choice at Bob allows for a perfectly noise-robust single-qubit encoding to be appropriate. Designing an encoding that is robust against such a model is beyond the scope considered in this paper.

APPENDIX E: KEY RATE UNDER LOSSY CHANNELS—THEORETICAL AND EXPERIMENTAL COMPARISONS

In this Appendix, we present the key rates of all protocols in Fig. 6 under loss in both an ideal theoretical case and under experimental considerations. We show these in Figs. 9(a)–9(c).

Under ideal conditions (loss-only channel), Fig. 9(a) reveals that TF-QKD and BB84 perform well because they use fewer photons per bit shared by Alice and Bob; however, under experimental noise conditions, extensive noise-compensation techniques are required. Not only do these methods require complex feedback systems that reduce the industrial scalability of the protocols, but they also require a significant portion of the pulses to be used for estimating and stabilizing against the channel noise fluctuations. This greatly lowers the overall rate of establishing a key between Alice and Bob (by orders of magnitude), as shown in Fig. 9(b). In contrast, our scheme does not require stabilization mechanisms due to its inherent noise resilience. By optimizing the encoding parameters for the expected noise fluctuations, our protocol will see only an order of 1 reduction in key rate under channel noise without employing any compensation methods [e.g., as seen for the channel model in Eq. (8)].

In addition to Figs. 9(a) and 9(b), which present key rates in units of bits per pulse, it is also important to evaluate performance in terms of bits per second, which is a critical figure of merit for practical implementations. Accordingly, in Fig. 9(c), we compare the key rates of the discussed protocols in bits per second as a function of channel loss.

To facilitate a comparison, we first consider all protocols at 0-dB loss and then apply the appropriate loss-dependent scaling. For BB84 and TF-QKD, we extract key rates from Ref. [38] and Ref. [14], respectively. Reference [38] reports 80 bit/s at 40-dB loss for BB84, which corresponds to approximately 9.5×10^5 bit/s at 0 dB after accounting for detection and transmission losses. Similarly, Ref. [14] reports a rate of 0.092 bit/s at 106-dB loss for TF-QKD, which scales to roughly 2.2×10^4 bit/s at 0 dB.

By contrast, to our knowledge, the existing noise-canceling schemes in Ref. [18] are yet to be realized experimentally. Nonetheless, we can estimate their performance

by considering the generation of the four-photon entangled states needed by the protocol. These states remain experimentally challenging to produce, with recent demonstrations reporting generation rates of approximately 150 Hz for four-photon Greenberger-Horne-Zeilinger states [64], corresponding to a key rate of around 75 bit/s at 0 dB.

To estimate the key rate in bits per second for our protocol, we use the methods described in Appendix B, drawing on experimental parameters from Ref. [62]. Under optimized conditions, our protocol can achieve generation rates of the order of 10^9 logical states per second at 0-dB loss, enabled by domain-engineered nonlinear crystals. To account for further experimental constraints (such as limitations due to multiphoton emissions), in Fig. 9(c), we consider a more conservative generation rate of 10^8 pairs/s. Multiplying this rate by the bits per pulse obtained from the previous figures also yields key rates of the order of 10^8 pairs/s.

This comparison highlights that our protocol is competitive with state-of-the-art approaches both in terms of bits per pulse and bits per second.

-
- [1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Theor. Comput. Sci.* **560**, 7 (2014), Theoretical Aspects of Quantum Cryptography—celebrating 30 years of BB84.
 - [2] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM J. Comput.* **26**, 1484 (1997).
 - [3] A. Acín, I. Bloch, H. Buhrman, T. Calarco, C. Eichler, J. Eisert, D. Esteve, N. Gisin, S. J. Glaser, F. Jelezko, S. Kuhr, M. Lewenstein, M. F. Riedel, P. O. Schmidt, R. Thew, A. Wallraff, I. Walmsley, and F. K. Wilhelm, The quantum technologies roadmap: A European Community view, *New J. Phys.* **20**, 080201 (2018).
 - [4] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, *Science* **283**, 2050 (1999).
 - [5] D. Mayers, Unconditional security in quantum cryptography, *J. ACM* **48**, 351 (2001).
 - [6] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Practical challenges in quantum key distribution, *npj Quantum Inf.* **2**, 16025 (2016).
 - [7] M. Peranić, M. Clark, R. Wang, S. Bahrani, O. Alia, S. Wengerowsky, A. Radman, M. Lončarić, M. Stipčević, J. Rarity, R. Nejabati, and S. K. Joshi, A study of polarization compensation for quantum networks, *EPJ Quantum Technol.* **10**, 30 (2023).
 - [8] J.-Y. Liu, X. Liu, W. Zhang, and Y.-D. Huang, Impact of fiber dispersion on the performance of entanglement-based dispersive optics quantum key distribution, *J. Electron. Sci. Technol.* **19**, 100119 (2021).
 - [9] L. Zhou, J. Lin, Y. Jing, and Z. Yuan, Twin-field quantum key distribution without optical frequency dissemination, *Nat. Commun.* **14**, 928 (2023).
 - [10] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum

- key distribution without quantum repeaters, *Nature* **557**, 400 (2018).
- [11] C. Clivati, A. Meda, S. Donadello, S. Virzi, M. Genovese, F. Levi, A. Mura, M. Pittaluga, Z. Yuan, A. J. Shields, M. Lucamarini, I. P. Degiovanni, and D. Calonico, Coherent phase transfer for real-world twin-field quantum key distribution, *Nat. Commun.* **13**, 157 (2022).
- [12] W. Li, L. Zhang, Y. Lu, Z.-P. Li, C. Jiang, Y. Liu, J. Huang, H. Li, Z. Wang, X.-B. Wang, Q. Zhang, L. You, F. Xu, and J.-W. Pan, Twin-field quantum key distribution without phase locking, *Phys. Rev. Lett.* **130**, 250802 (2023).
- [13] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, 600-km repeater-like quantum communications with dual-band stabilization, *Nat. Photonics* **15**, 530 (2021).
- [14] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, D.-F. Zhao, W.-J. Zhang, F.-X. Chen, H. Li, L.-X. You, Z. Wang, Y. Chen, X.-B. Wang, Q. Zhang, and J.-W. Pan, Quantum key distribution over 658 km fiber with distributed vibration sensing, *Phys. Rev. Lett.* **128**, 180502 (2022).
- [15] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution over 830-km fibre, *Nat. Photonics* **16**, 154 (2022).
- [16] J.-P. Chen, F. Zhou, C. Zhang, C. Jiang, F.-X. Chen, J. Huang, H. Li, L.-X. You, X.-B. Wang, Y. Liu, Q. Zhang, and J.-W. Pan, Twin-field quantum key distribution with local frequency reference, *Phys. Rev. Lett.* **132**, 260802 (2024).
- [17] X.-B. Wang, Fault tolerant quantum key distribution protocol with collective random unitary noise, *Phys. Rev. A* **72**, 050304 (2005).
- [18] J.-C. Boileau, D. Gottesman, R. Laflamme, D. Poulin, and R. W. Spekkens, Robust polarization-based quantum key distribution over a collective-noise channel, *Phys. Rev. Lett.* **92**, 017901 (2004).
- [19] X.-H. Li, F.-G. Deng, and H.-Y. Zhou, Efficient quantum key distribution over a collective noise channel, *Phys. Rev. A* **78**, 022321 (2008).
- [20] P.-L. Guo, C. Dong, Y. He, F. Jing, W.-T. He, B.-C. Ren, C.-Y. Li, and F.-G. Deng, Efficient quantum key distribution against collective noise using polarization and transverse spatial mode of photons, *Opt. Express* **28**, 4611 (2020).
- [21] Y. Sun, Q.-Y. Wen, F. Gao, and F.-C. Zhu, Robust variations of the Bennett-Brassard 1984 protocol against collective noise, *Phys. Rev. A* **80**, 032321 (2009).
- [22] L. Berent, T. Hillmann, J. Eisert, R. Wille, and J. Roffe, Analog information decoding of bosonic quantum low-density parity-check codes, *PRX Quantum* **5**, 020349 (2024).
- [23] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/xq2l-r4r7> for details of the mathematical models of the states and noise channels used, a full description of the security analysis method, full key-rate simulation plots, and experimental parameter considerations.
- [24] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010), p. 113.
- [25] R. Paschotta, Chromatic dispersion, RP Photonics Encyclopedia (2024), available online at https://www.rp-photonics.com/chromatic_dispersion.html.
- [26] A. Willner, Y.-W. Song, J. McGehean, Z. Pan, and B. Hoanca, in *Encyclopedia of Modern Optics*, edited by R. D. Guenther (Elsevier, Oxford, 2005), p. 353.
- [27] J. C. Bienfang, A. J. Gross, A. Mink, B. J. Hershman, A. Nakassis, X. Tang, R. Lu, D. H. Su, C. W. Clark, C. J. Williams, E. W. Hagley, and J. Wen, Quantum key distribution with 1.25 Gbps clock synchronization, *Opt. Express* **12**, 2011 (2004).
- [28] I. Vagniluca, B. Da Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenløwe, and D. Bacco, Efficient time-bin encoding for practical high-dimensional quantum key distribution, *Phys. Rev. Appl.* **14**, 014051 (2020).
- [29] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Simple 2.5 GHz time-bin quantum key distribution, *Appl. Phys. Lett.* **112**, 171108 (2018).
- [30] C.-Z. Wang, Y. Li, W.-Q. Cai, W.-Y. Liu, S.-K. Liao, and C.-Z. Peng, Synchronization using quantum photons for satellite-to-ground quantum key distribution, *Opt. Express* **29**, 29595 (2021).
- [31] A. V. Miller, Time synchronization in satellite quantum key distribution, *Probl. Inf. Transm.* **59**, 225 (2023).
- [32] P. S. André and A. N. Pinto, Chromatic dispersion fluctuations in optical fibers due to temperature and its effects in high-speed optical communication systems, *Opt. Commun.* **246**, 303 (2005).
- [33] D. Lee, W. Shin, S. Park, J. Kim, and H. Shin, Noon-state interference in the frequency domain, *Light: Sci. Appl.* **13**, 90 (2024).
- [34] G. Finco, F. Miserocchi, A. Maeder, J. Kellner, A. Sabatti, R. J. Chapman, and R. Grange, Time-bin entangled Bell state generation and tomography on thin-film lithium niobate, *npj Quantum Inf.* **10**, 135 (2024).
- [35] M. Clementi, F. A. Sabbatoli, M. Borghi, L. Gianini, N. Tagliavacche, H. El Dirani, L. Youssef, N. Bergamasco, C. Petit-Etienne, E. Pargon, J. E. Sipe, M. Liscidini, C. Sciancalepore, M. Galli, and D. Bajoni, Programmable frequency-bin quantum states in a nano-engineered silicon device, *Nat. Commun.* **14**, 176 (2023).
- [36] A. Winick, N. Lütkenhaus, and P. J. Coles, Reliable numerical key rates for quantum key distribution, *Quantum* **2**, 77 (2018).
- [37] J. Lin and N. Lütkenhaus, Simple security analysis of phase-matching measurement-device-independent quantum key distribution, *Phys. Rev. A* **98**, 042332 (2018).
- [38] C. Agnesi, M. Avesani, L. Calderaro, A. Stanco, G. Foletto, M. Zahidy, A. Scriminich, F. Vedovato, G. Vallone, and P. Villoresi, Simple quantum key distribution with qubit-based synchronization and a self-compensating polarization encoder, *Optica* **7**, 284 (2020).
- [39] Y.-Y. Ding, W. Chen, H. Chen, C. Wang, Y.-P. Li, S. Wang, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Polarization-basis tracking scheme for quantum key distribution using revealed sifted key bits, *Opt. Lett.* **42**, 1023 (2017).

- [40] Y. Du, X. Zhu, X. Hua, Z. Zhao, X. Hu, Y. Qian, X. Xiao, and K. Wei, Silicon-based decoder for polarization-encoding quantum key distribution, *Chip* **2**, 100039 (2023).
- [41] F. Rozpędek, K. Noh, Q. Xu, S. Guha, and L. Jiang, Quantum repeaters based on concatenated bosonic and discrete-variable quantum codes, *npj Quantum Inf.* **7**, 102 (2021).
- [42] F. Schmidt, D. Miller, and P. van Loock, Error-corrected quantum repeaters with Gottesman-Kitaev-Preskill qudits, *Phys. Rev. A* **109**, 042427 (2024).
- [43] K. Fukui, R. N. Alexander, and P. van Loock, All-optical long-distance quantum communication with Gottesman-Kitaev-Preskill qubits, *Phys. Rev. Res.* **3**, 033118 (2021).
- [44] F. Rozpędek, K. P. Seshadreesan, P. Polakos, L. Jiang, and S. Guha, All-photonic Gottesman-Kitaev-Preskill-qubit repeater using analog-information-assisted multiplexed entanglement ranking, *Phys. Rev. Res.* **5**, 043056 (2023).
- [45] S. Konno, W. Asavanant, F. Hanamura, H. Nagayoshi, K. Fukui, A. Sakaguchi, R. Ide, F. China, M. Yabuno, S. Miki, H. Terai, K. Takase, M. Endo, P. Marek, R. Filip, P. van Loock, and A. Furusawa, Logical states for fault-tolerant quantum computation with propagating light, *Science* **383**, 289 (2024).
- [46] E. Descamps, A. Keller, and P. Milman, Gottesman-Kitaev-Preskill encoding in continuous modal variables of single photons, *Phys. Rev. Lett.* **132**, 170601 (2024).
- [47] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, and M. Curty, Advances in device-independent quantum key distribution, *npj Quantum Inf.* **9**, 10 (2023).
- [48] M. D. Reid, P. D. Drummond, W. P. Bowen, E. G. Cavalcanti, P. K. Lam, H. A. Bachor, U. L. Andersen, and G. Leuchs, Colloquium: The Einstein-Podolsky-Rosen paradox: From concepts to applications, *Rev. Mod. Phys.* **81**, 1727 (2009).
- [49] H. Seabrook, SurpassingLNTradeOffQKD, GitHub repository, <https://github.com/hmis4/SurpassingLNTradeOffQKD> (2025).
- [50] H. Seabrook, SurpassingLNTradeOffQKD, GitHub repository, <https://github.com/hmis4/SurpassingLNTradeOffQKD/tree/main/DomainEngineering> (2025).
- [51] C. H. Bennett, Quantum cryptography using any two nonorthogonal states, *Phys. Rev. Lett.* **68**, 3121 (1992).
- [52] A. Cabello, Six-qubit permutation-based decoherence-free orthogonal basis, *Phys. Rev. A* **75**, 020301 (2007).
- [53] A. Al-Juboori, H. Z. J. Zeng, M. A. P. Nguyen, X. Ai, A. Laucht, A. Solntsev, M. Toth, R. Malaney, and I. Aharonovich, Quantum key distribution using a quantum emitter in hexagonal boron nitride, *Adv. Quantum Technol.* **6**, 2300038 (2023).
- [54] S. Slussarenko and G. J. Pryde, Photonic quantum information processing: A concise review, *Appl. Phys. Rev.* **6**, 041303 (2019).
- [55] S. Seshadri, H.-H. Lu, D. E. Leaird, A. M. Weiner, and J. M. Lukens, Complete frequency-bin basis synthesizer, *Phys. Rev. Lett.* **129**, 230505 (2022).
- [56] H.-P. Lo, T. Ikuta, K. Azuma, T. Honjo, W. J. Munro, and H. Takesue, Generation of a time-bin Greenberger-Horne-Zeilinger state with an optical switch, *Quantum Sci. Technol.* **8**, 035003 (2023).
- [57] A. Dosseva, L. Cincio, and A. M. Brańczyk, Shaping the joint spectrum of down-converted photons through optimized custom poling, *Phys. Rev. A* **93**, 013801 (2016).
- [58] F. Graffitti, D. Kundys, D. T. Reid, A. M. Brańczyk, and A. Fedrizzi, Pure down-conversion photons through sub-coherence-length domain engineering, *Quantum Sci. Technol.* **2**, 035001 (2017).
- [59] R.-B. Jin, K. Tazawa, N. Asamura, M. Yabuno, S. Miki, F. China, H. Terai, K. Minoshima, and R. Shimizu, Quantum optical synthesis in 2D time-frequency space, *APL Photonics* **6**, 086104 (2021).
- [60] T. J. Herzog, J. G. Rarity, H. Weinfurter, and A. Zeilinger, Frustrated two-photon creation via interference, *Phys. Rev. Lett.* **72**, 629 (1994).
- [61] A. Hochrainer, M. Lahiri, M. Erhard, M. Krenn, and A. Zeilinger, Quantum indistinguishability by path identity and with undetected photons, *Rev. Mod. Phys.* **94**, 025007 (2022).
- [62] S. P. Neumann, M. Selimovic, M. Bohmann, and R. Ursin, Experimental entanglement generation for quantum key distribution beyond 1 Gbit/s, *Quantum* **6**, 822 (2022).
- [63] C. Chen, C. Bo, M. Y. Niu, F. Xu, Z. Zhang, J. H. Shapiro, and F. N. Wong, Efficient generation and characterization of spectrally factorable biphotons, *Opt. Express* **25**, 7300 (2017).
- [64] M. Pont, G. Corrielli, A. Fyrrillas, I. Agresti, G. Carvacho, N. Maring, P.-E. Emeriau, F. Ceccarelli, R. Albiero, P. H. Dias Ferreira, N. Somaschi, J. Senellart, I. Sagnes, M. Morassi, A. Lemaître, P. Senellart, F. Sciarrino, M. Liscidini, N. Belabas, and R. Osellame, High-fidelity four-photon GHz states on chip, *npj Quantum Inf.* **10**, 50 (2024).