Floodlight quantum key distribution: A practical route to gigabit-per-second secret-key rates

Quntao Zhuang, Zheshen Zhang, Justin Dove, Franco N. C. Wong, and Jeffrey H. Shapiro

Phys. Rev. A **94**, 012322 — Published 14 July 2016

DOI: 10.1103/PhysRevA.94.012322

Floodlight quantum key distribution: A practical route to Gbps secret-key rates

Quntao Zhuang,* Zheshen Zhang, Justin Dove, Franco N. C. Wong, and Jeffrey H. Shapiro

Research Laboratory of Electronics, Massachusetts Institute of Technology,

77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA

Abstract

The channel loss incurred in long-distance transmission places a significant burden on quantum key distribution (QKD) systems: they must defeat a passive eavesdropper who detects all the light lost in the quantum channel and does so without disturbing the light that reaches the intended destination. The current QKD implementation with the highest long-distance secret-key rate meets this challenge by transmitting no more than one photon per bit [Opt. Express **21,** 24550–24565 (2013)]. As a result, it cannot achieve the Gbps secret-key rate needed for one-time pad encryption of large data files unless an impractically large amount of multiplexing is employed. We introduce floodlight QKD (FL-QKD), which floods the quantum channel with a high number of photons per bit distributed over a much greater number of optical modes. FL-QKD offers security against the optimum frequency-domain collective attack by transmitting less than one photon per mode and using photon-coincidence channel monitoring, and it is completely immune to passive eavesdropping. More importantly, FL-QKD is capable of a 2 Gbps secret-key rate over a 50 km fiber link, *without* any multiplexing, using available equipment, i.e., no new technology need be developed. FL-QKD achieves this extraordinary secret-key rate by virtue of its unprecedented secret-key efficiency, in bits per channel use, which exceeds those of state-of-the-art systems by two orders of magnitude.

PACS numbers: 03.67.Hk, 03.67.Dd, 42.50.Lc

*Electronic address: quntao@mit.edu

I. INTRODUCTION

One-time pad (OTP) encryption provides information-theoretically secure message transmission [1], but key distribution is its Achilles' heel. Quantum key distribution (QKD) permits remote parties (Alice and Bob) to share a random bit string—the key needed for OTP encryption—with security vouchsafed by quantum mechanics [2–5]. Unfortunately, the demonstrated secret-key rates of long-distance QKD systems fall far short of the Gbps rates needed for OTP encryption of large data files, as seen from the following state-of-the-art achievements. In discrete-variable QKD (DV-QKD), the best result to date is Lucamarini *et al.*'s decoy state Bennett-Brassard 1984 (BB84) system, which used a 1 Gbps source rate but only realized a 1 Mbps secret-key rate over a 50-km-long fiber [6]. In continuous-variable QKD (CV-QKD), the best result to date is from Huang *et al.*, who reported a 1 Mbps secret-key rate at 25 km path length using a 50 Mbaud source rate [7], with 90 kbps expected at 50 km in the asymptotic (infinite block-length) regime.

Focusing, for the moment, on DV-QKD systems—owing to their greater demonstrated capability over long distances—it is easy to identify why Gbps rates are beyond their state-of-the-art grasp: they transmit no more than $\sim$1 photon/bit. One justification for this self-imposed limit is that these systems must defeat the undetectable passive eavesdropper. QKD security analyses afford the eavesdropper (Eve) all things consistent with the laws of physics. In particular, a passive Eve could replace the transmissivity $\kappa \ll 1$ optical fiber connecting Alice and Bob with a lossless long-distance coupler that allows her to capture and measure a fraction $1-\kappa$ of Alice's transmitted light while routing the remaining fraction κ to Bob without disturbance. With no disturbance of the light that Bob receives, Eve does not create the telltale errors that reveal her eavesdropping. In principle, such a coupler could be constructed to mimic—insofar as Alice and Bob are concerned—the propagation characteristics of the fiber that it replaced. Thus Alice and Bob could not detect Eve's presence via channel monitoring, e.g., with an optical time-domain reflectometer. So, were Alice to ignore the potential presence of the undetectable passive eavesdropper and make a many-photons-per-bit BB84 transmission to Bob through this lossy quantum channel, then Eve could easily obtain a near-perfect measurement of *all* of Alice's bits.

We regard secret-key rate, in bits per second, as QKD systems' preeminent figure of merit: unless Gbps rates over metropolitan-area spans can be realized, OTP-encrypted transmission

of large data files will not reach widespread usage. Existing QKD systems operating over long–distance connections *might* be pushed to Gbps secret-key rates, but doing so would require impractically large amounts of wavelength-division multiplexing (WDM). Consider scaling Lucamarini *et al.*'s BB84 system [6] to a 10 Gbps source rate achieving a 10 Mbps secret-key rate over a 50 km fiber link. That system would require 100 WDM channels to yield a 1 Gbps secret-key rate—while 1000 such channels would be needed at the original source rate—each with its own single-photon detection setup. A similar scaling of Huang *et al.*'s CV-QKD system [7]—to a 10 Gbaud source rate that achieves 18 Mbps secret-key rate over a 50 km fiber link in the asymptotic regime—implies that more than 50 WDM channels would be needed to obtain a 1 Gbps secret-key rate.

In this paper we introduce floodlight quantum key distribution (FL-QKD), and show that it offers a practical route to Gbps secret-key rates over metropolitan-area distances with security against the optimum frequency-domain collective attack and without the need for multiplexing. How does FL-QKD realize this extraordinary secret-key rate? It derives from FL-QKD's secret-key efficiency, in bits per channel use, being two order of magnitude higher than those of state-of-the-art systems. In particular, FL-QKD floods the Alice-to-Bob channel with broadband light—whose bandwidth is much greater than the modulation rate—containing many photons per bit. Its immunity to the undetectable passive-eavesdropping attack then comes from that high number of transmitted photons per bit being distributed over a much greater number of optical modes to make that transmission have low brightness, i.e., less than one photon per mode. FL-QKD also employs photon-coincidence channel monitoring on the Alice-to-Bob channel, to ensure security against the active component of a frequency-domain collective attack, in which Eve can inject her own light into Bob's terminal and tries to obtain his bit string from the modulated version of that light which is contained in what she taps from the Bob-to-Alice channel. More importantly, we show that FL-QKD can support a 2 Gbps secret-key rate over a 50-km-long fiber link against the optimum frequency-domain collective attack, and that it can be implemented with available equipment, i.e., no new technology need be developed. In short, FL-QKD opens the possibility for OTP encryption of large data files for secure transmission over metropolitan-area distances at Gbps rates.

The remainder of the paper is organized as follows. Sections II through V present, in succession, a description of the FL-QKD protocol, its security analysis, its secret-key rate

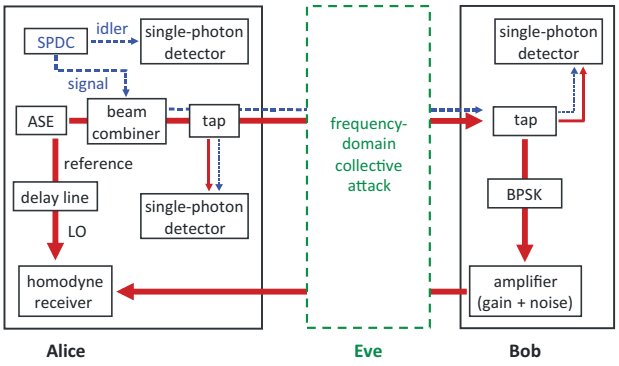

FIG. 1: (color online). Quantum channel setup for FL-QKD under frequency-domain collective attack. ASE: amplified spontaneous emission source. SPDC: spontaneous parametric downconverter. BPSK: binary phase-shift keying. LO: local oscillator.

behavior, and some concluding discussion. For the sake of readability, we have relegated all detailed analysis to a series of appendices.

II. PROTOCOL DESCRIPTION

Figure 1 shows FL-QKD's quantum channel setup in the presence of a frequency-domain collective attack. Alice and Bob use this setup to generate their raw key and to bound Eve's Holevo information. Not shown in this figure is the tamper-proof classical channel that Alice and Bob use for reconciliation. Neither that procedure nor FL-QKD's subsequent privacy amplification step will be described herein, because they are merely higher rate versions of standard practice in QKD.

Raw key generation in FL-QKD occurs as follows. Alice sends unmodulated, continuous-wave (cw) light over optical fiber to Bob, who imposes a random bit string on that light by means of binary phase-shift keying (BPSK), amplifies the modulated light (to overcome return-path loss), and returns it to Alice over optical fiber. FL-QKD's security against a frequency-domain collective attack, and its high secret-key rate, come from the composite nature of Alice's source plus the data that Alice and Bob obtain from their channel monitors, which are used to ensure the integrity of the Alice-to-Bob channel, i.e, the near-perfect correlation between the light reaching Bob and the reference retained by Alice. So, to complete our protocol description, we will characterize Alice's source and Alice and Bob's channel monitors.

Alice uses an optical amplifier to produce a high-brightness (many photons/sec-Hz) single spatial-mode beam of amplified spontaneous emission (ASE) noise with a W-Hz-bandwidth flat spectrum. She uses a cw spontaneous parametric downconverter (SPDC) to produce quadrature-entangled, single spatial-mode signal and idler beams that have bandwidth W flat spectra, with the former having the same center frequency as her ASE source. Alice directs the idler beam to a single-photon detector that is part of her channel monitor. She uses a beam combiner to merge a low-brightness ($\ll 1$ photon/sec-Hz) portion of her ASE light with her SPDC's signal light resulting in an n:1 ASE-to-SPDC-ratio output with $n \gg 1$. She sends a small fraction of her combined ASE-SPDC light to another single-photon detector (also part of her channel monitor), and transmits the remaining portion of her ASE-SPDC light to Bob. Alice stores the high-brightness portion of her initial ASE light in an optical delay-line fiber (whose delay matches that of the Alice-to-Bob-to-Alice roundtrip) for use as the local oscillator (LO) in a broadband homodyne receiver. She employs optical amplification, as needed, so that her LO retains its high-brightness character without appreciable degradation, see App. A.3 for details. Prior to BPSK modulation, Bob routes a small fraction of the light he receives to the single-photon detector that is his channel monitor.

Alice and Bob use their channel monitors to measure the singles rates, S_I for Alice's idler beam, S_A for Alice's tap on her transmitted beam, and S_B for Bob's tap on his received beam. They also use their monitors to obtain C_{IA} and $\widetilde{C}_{IA}$, the time-aligned and time-shifted coincidence rates between Alice's idler and the tap on her transmitted beam, and C_{IB} and $\widetilde{C}_{IB}$, the time-aligned and time-shifted coincidence rates between Alice's idler and Bob's tap on his received beam, in both cases employing a T_g-duration coincidence gate and accounting for the relevant propagation delays in the appropriate manners. From these rates they compute

$$f_E = 1 - \frac{[C_{IB} - \widetilde{C}_{IB}]/S_B}{[C_{IA} - \widetilde{C}_{IA}]/S_A}, \tag{1}$$

which will be shown below to quantify the integrity of the Alice-to-Bob channel.

III. SECURITY ANALYSIS

As detailed in App. B, Eve's general frequency-domain collective attack is as follows. Eve first establishes lossless connections between her equipment and the communicating parties

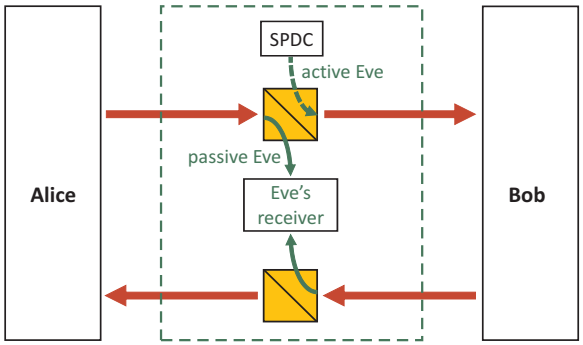

FIG. 2: (color online). Realization of Eve's optimum frequency-domain collective attack. SPDC: spontaneous parametric downconverter. Eve's SPDC signal beam (shown) is coupled to Bob through a beam splitter, while her SPDC idler beam (not shown) is retained for use in her receiver.

in both the forward (Alice-to-Bob) and backward (Bob-to-Alice) channels. In the forward path, she performs a general unitary transformation that, during each of Bob's bit intervals, acts in an independent, identically distributed manner on the $M = W/R$ frequency modes of Alice's transmitted light. In particular, the inputs to that unitary transformation are Alice's transmitted field and Eve's K vacuum-state ancilla fields. Eve retains the K ancilla fields that emerge from this unitary operation and sends the remaining field to Bob. She completes her attack with a collective measurement on her stored ancilla fields and the light she taps from the Bob-to-Alice channel. Here we note, see App. E, that f_E is an intrusion parameter that quantifies Eve's degradation of the phase-sensitive cross-covariance between Alice's idler and Bob's received light from what it would be were Eve only mounting a passive attack. Furthermore, we show in App. C.2 that Eve's optimum frequency-domain collective attack—one that maximizes her Holevo information for a given photon flux and f_E value—is in fact Gaussian and can be realized by her using an SPDC source, injecting its signal light into Bob through a beam splitter in the Alice-to-Bob fiber, while retaining her idler for a collective measurement with the light she taps from the Alice-to-Bob and Bob-to-Alice fibers, see Fig. 2. For this optimum attack, f_E equals Eve's injection fraction, viz., the fraction of light entering Bob's terminal that is due to her [8]. Hence that configuration will be employed throughout the security analysis below. (Interestingly, this SPDC beam-splitter attack has the same structure as the entangling-cloner attack on CV-QKD [9].)

We will be concerned with optimized performance for Alice and Bob against Eve's op-

timum frequency-domain collective attack without regard for finite-key effects. (For FL-QKD's ∼Gbps secret-key rates, finite-key effects become inconsequential for key-generation sessions as short as a few seconds.) Thus, following standard practice for assessing security against collective attacks (see, e.g., [10, 11]), we will find $\Delta I_{AB}^{\rm LB}$, a lower bound on Alice and Bob's secret-key rate, from

$$\Delta I_{AB}^{\rm LB} = \beta I_{AB} - \chi_{EB}^{\rm UB}, \tag{2}$$

where I_{AB} is Alice and Bob's Shannon-information rate, β is Alice and Bob's reconciliation efficiency, and $\chi_{EB}^{\rm UB}$ is an upper bound on Eve's Holevo-information rate for her optimum frequency-domain collective attack. Before doing so, let us provide some simple intuition about how FL-QKD can be secure against individual passive or active attacks.

We will limit our consideration of these individual attacks to low-brightness operation (the ASE-SPDC light Alice sends to Bob has $N_S \ll 1$ photon/sec-Hz) in a lossy scenario (channel transmissivity $\kappa_S \ll 1$) with Alice's source bandwidth W greatly exceeding Bob's BPSK modulation rate R. For Eve's passive attack, we neglect the small amount of SPDC light in Alice's transmission and the small amounts tapped by Alice and Bob for their channel monitors. Alice's homodyne receiver and Eve's optimum quantum receiver then have error probabilities satisfying $\Pr(e)_{\rm Alice}^{\rm hom} \sim \exp(-W\kappa_S N_S G_B/RN_B)/2$ [12] and $\Pr(e)_{\rm Eve}^{\rm pass} \sim \exp(-4W\kappa_S N_S^2 G_B/RN_B)/2$ [13], where $G_B \gg 1$ and $N_B \geq G_B - 1$ are the gain and ASE output-noise brightness of Bob's optical amplifier. Because $\ln[\Pr(e)_{\rm Alice}^{\rm hom}]/\ln[\Pr(e)_{\rm Eve}^{\rm pass}] \sim 1/4N_S$, we see that low-brightness ($N_S \ll 1$) operation affords Alice and Bob a considerable advantage over Eve. Physically, this advantage is due to the $N_S \ll 1$ low-brightness condition's making Eve unable to obtain a high-brightness reference—from the light she taps from the Alice-to-Bob fiber—with which to detect Bob's BPSK modulation. Later, we will see that this low-brightness condition ensures that Eve's Holevo information rate for her undetectable passive-eavesdropping attack falls far below Alice and Bob's Shannon information rate. In other words, as claimed earlier, FL-QKD's transmitting less than one photon per mode makes it immune to the attack that has driven the highest-rate, long-distance QKD system to limit its transmissions to ∼1 photon/bit.

For Eve's active attack, we employ the conditions applied above and, in addition, presume that Alice and Bob's channel monitors constrain their adversary's light injection to a small fraction, $f_E \ll 1$, of the light entering Bob's terminal. The error probability of Alice's homodyne receiver will then obey $\Pr(e)_{\rm Alice}^{\rm hom} \sim \exp(-W(1-f_E)\kappa_S N_S G_B/RN_B)/2$. Eve's

optimum quantum receiver—for an individual attack in the Fig. 2 setup using her optimum SPDC-injection strategy in conjunction with a tap on just the Bob-to-Alice channel—then has error probability $\Pr(e)^{\rm act}_{\rm Eve} \sim \exp(-4Wf_E\kappa_S N_S G_B/RN_B)/2$. Now we find that $\ln[\Pr(e)^{\rm hom}_{\rm Alice}]/\ln[\Pr(e)^{\rm act}_{\rm Eve}] \sim (1-f_E)/4f_E$, which is highly favorable to Alice and Bob when their channel monitors limit Eve to $f_E \ll 1$.

Having provided some individual-attack insights into FL-QKD's security, we return to the task of assessing our protocol's security analysis when Eve mounts her optimum frequency-domain collective attack. To evaluate Alice's error probability under that attack, we note the number of independent modes that contribute to the light Alice receives from Bob being much greater than one—for $W = 2\,\text{THz}$ with $R \leq 10\,\text{Gbps}$, as we will assume below, we get $M = W/R \geq 200$—justifies a central limit theorem argument that makes Alice's error probability satisfy [14]

$$\Pr(e)^{\rm hom}_{\rm Alice} = Q\left(\frac{\mu_0 - \mu_1}{\sigma_0 + \sigma_1}\right), \tag{3}$$

where μ_b and σ_b for $b = 0, 1$ are the means and standard deviations of Alice's homodyne measurement when Bob's bit values (phase modulations) are equally likely to be 0 (0 rad phase shift) or 1 (π rad phase shift), and $Q(x) = \int_x^\infty \mathrm{d}t\, e^{-t^2/2}/\sqrt{2\pi}$. See App. D for the $\{\mu_b\}$ and $\{\sigma_b\}$ with all losses included. With Alice's error probability in hand, Alice and Bob's Shannon-information rate is found from

$$\begin{aligned} I_{AB} = R\big[1 &+ \Pr(e)^{\rm hom}_{\rm Alice} \log_2(\Pr(e)^{\rm hom}_{\rm Alice}) \\ &+ (1 - \Pr(e)^{\rm hom}_{\rm Alice}) \log_2(1 - \Pr(e)^{\rm hom}_{\rm Alice})\big]\,. \end{aligned} \tag{4}$$

Eve's Holevo-information rate about Bob's bit string for her optimum collective attack is

$$\chi_{EB} = R\left[S(\boldsymbol{\rho}_E) - \sum_{b=0}^{1} S(\boldsymbol{\rho}_E^{(b)})/2\right], \tag{5}$$

where $S(\cdot)$ denotes von Neumann entropy. Here, $\boldsymbol{\rho}_E^{(b)}$ is Eve's conditional joint density operator—when Bob transmits a single bit with value $b = 0$ or 1—for the $3M$ modes available to her that are associated with that bit, viz., M modes each from her retained idler, the light she collects from the Alice-to-Bob fiber, and the light she collects from the Bob-to-Alice fiber. Her unconditional joint density operator for those $3M$ modes is then $\boldsymbol{\rho}_E = \sum_{b=0}^{1} \boldsymbol{\rho}_E^{(b)}/2$. The $\boldsymbol{\rho}_E^{(b)}$ are zero-mean Gaussian states whose von Neumann entropies are easily found by symplectic diagonalization [15], as explained in App. C. The unconditional

state, $\boldsymbol{\rho}_E$ is zero mean but *not* Gaussian, making its von Neumann entropy quite difficult to evaluate. However, that state's covariance matrix is easily found [16], and we know that $S(\boldsymbol{\rho}_E) \leq S(\boldsymbol{\rho}_E^{\text{Gauss}})$, where $\boldsymbol{\rho}_E^{\text{Gauss}}$ is a zero-mean Gaussian state with the same covariance matrix as $\boldsymbol{\rho}_E$. We can find $S(\boldsymbol{\rho}_E^{\text{Gauss}})$ by another symplectic diagonalization and so obtain

$$\chi_{EB} \leq \chi_{EB}^{\text{UB}} = R \min \left[S(\boldsymbol{\rho}_E^{\text{Gauss}}) - \sum_{b=0}^{1} S(\boldsymbol{\rho}_E^{(b)})/2, 1 \right], \tag{6}$$

where we have used $S(\boldsymbol{\rho}_E) - \sum_{b=0}^{1} S(\boldsymbol{\rho}_E^{(b)})/2 \leq 1$, which follows from that term's being Eve's Holevo information about a single-bit transmission from Bob.

IV. SECRET-KEY RATES

We are now ready to demonstrate the power of FL-QKD. Figure 3(a) plots the lower bound from Eq. (2) on Alice and Bob's secret-key rate versus one-way path length when Eve mounts her optimum collective attack, but Alice and Bob's channel monitoring ensures that Eve's injection fraction into Bob's terminal is $f_E = 0.01$. Also shown in that figure is a brightness versus path length plot for the light Alice sends to Bob. These curves were obtained assuming that: (1) Alice's ASE source and her SPDC signal light have flat spectra with the same center frequency and $W = 2\,\text{THz}$ bandwidth, and are combined in an n:1 ratio with $n = 99$; (2) the brightness of the light Alice sends to Bob and Bob's bit rate $R \leq 10\,\text{Gbps}$ are chosen to maximize their secret-key rate subject to the constraint that $\Pr(e)_{\text{Alice}} \leq 0.1$ to ensure the availability of a high-efficiency code for reconciliation [17]; (3) Bob's amplifier has $G_B = N_B = 10^4$; (4) Eve has replaced the L-km-long, 0.2 dB/km fibers in the Alice-to-Bob and Bob-to-Alice channels with lossless fibers and $(1 - f_E)\kappa_S$ and κ_S transmissivity beam splitters, respectively, with $\kappa_S = 10^{-0.02L}$; (5) Alice taps 1% of her combined ASE-SPDC light, and Bob taps 1% of his received light, for channel monitoring; (6) Alice's homodyne receiver has an undegraded local oscillator with brightness $N_{\text{LO}} = 10^4$ and efficiency 0.9; (7) $\beta = 0.94$; and (8) the system is otherwise ideal.

We see from Fig. 3(a) that 2 Gbps QKD is possible at 50 km one-way path length when $f_E = 0.01$, and that this secret-key rate is obtained with $N_S = 0.043$. (Figure 3(b) shows how this rate degrades as Eve's injection fraction increases.) Thus, as suggested at the outset, security against a collective attack has been ensured by a combination of low-brightness transmission and coincidence-based channel monitoring. That FL-QKD has such a high

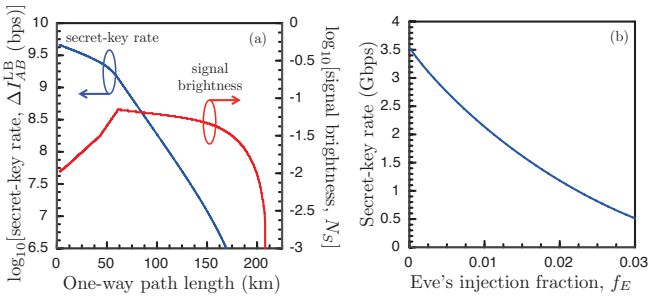

FIG. 3: (color online). (a) Lower bound on Alice and Bob's secret-key rate and Alice's optimum signal brightness when Eve mounts her optimum frequency-domain collective attack with injection fraction $f_E = 0.01$. (b) Lower bound on Alice and Bob's secret-key rate versus f_E for a 50-km fiber link with all other parameters as in (a).

rate after the 10 dB of one-way propagation loss incurred at 50 km is then due to its use of an optical bandwidth far in excess of its modulation rate, which enables Alice to transmit many photons per bit (ppb) without affording Eve very much information. This follows from Fig. 4(a), which plots the ppb that Alice transmits to Bob and the ppb that Bob receives from Alice. We see that FL-QKD maintains a near-unity ppb received by Bob for all path lengths less than 200 km [18]. The highest rate, long-distance, DV-QKD demonstration—Lucamarini *et al.*'s BB84 system [6]—employs ∼1 *transmitted* ppb. Hence it cannot match FL-QKD's loss-independent ∼1 *received* ppb performance. Thus its long-distance secret-key rate is vastly inferior to FL-QKD's. Moreover, as noted earlier, an impractically large amount of WDM would be needed for that BB84 system to match FL-QKD's single-channel Gbps secret-key rate capability over 50 km of fiber.

The story for Huang *et al.*'s CV-QKD demonstration [7] is a little different. CV-QKD transmissions are better quantified in terms of photons per channel use rather than photons per bit, quantities that are identical for BB84 systems and for FL-QKD but typically different for CV-QKD systems. Moreover, CV-QKD systems do not limit themselves to ∼1 photon/use. Nevertheless, even scaling it up to a 10 Gbaud source rate, Huang *et al.*'s system would still require more than 50 WDM channels to realize a 1 Gbps secret-key rate on a 50-km-long link.

We will close our secret-key rate assessment with some additional comments on its underlying security analysis. Consider first the optimality of Eve's using SPDC light injection in

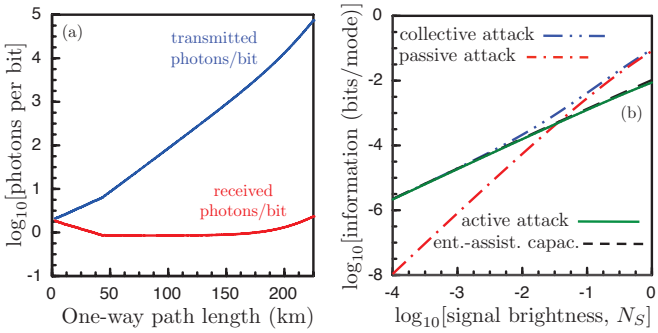

FIG. 4: (color online). (a) Alice's transmitted photons per bit (ppb) and Bob's received ppb when Eve mounts her optimum frequency-domain collective attack with injection fraction $f_E = 0.01$. (b) Upper bounds on Eve's optimum frequency-domain collective attack, passive attack, and active attack Holevo informations per mode—along with her entanglement-assisted capacity—as a function of Alice's signal brightness, N_S, for a 50 km one-way path length assuming $f_E = 0.01$.

the Fig. 2 setup. For a given value of her injection fraction, f_E, Eve's use of an SPDC source in an active attack yields a Holevo information that saturates the entanglement-assisted capacity for the channel created by her injection, Bob's BPSK modulation and optical amplification, and her tap of the Bob-to-Alice channel. Hence this confirms that no non-Gaussian active attack with the same f_E can do any better. This behavior is illustrated in Fig. 4(b), for a 50 km one-way path length and $f_E = 0.01$, where we have plotted our upper bound on Eve's active-attack Holevo information per mode versus Alice's signal brightness, N_S, along with Eve's entanglement-assisted capacity [19]. Further insights from Fig. 4(b) come from its display of Eve's passive-attack and optimum frequency-domain collective attack Holevo informations per mode [20]. When $N_S \leq 10^{-3}$, the active attack is almost as powerful as the optimum frequency-domain collective attack, but at $N_S \geq 0.1$ the passive attack makes the dominant contribution to the optimum frequency-domain collective attack [21]. These characteristics are easily understood from the simple, individual-attack error probabilities we presented earlier. For both passive and fixed-f_E active attacks, Eve's error probability decreases with increasing N_S, but her passive-attack error exponent is proportional to N_S^2 at low brightness, whereas her fixed-f_E active-attack error exponent is proportional to N_S. In future work we will pursue security analysis for coherent attacks. Because FL-QKD can be regarded as a two-way CV-QKD protocol that uses discrete modulation, coherent-attack security analyses for one-way CV-QKD [22–24] may provide a useful starting point.

V. DISCUSSION

We have argued that a QKD system's secret-key rate, in bits per second, is its preeminent figure of merit, and we have shown that single-channel FL-QKD vastly outperforms its state-of-the-art competition for long-distance OTP distribution. To elaborate on why that is so, let us compare FL-QKD's secret-key *efficiency*, in bits per channel use, with those of the highest-rate, long-distance DV-QKD and CV-QKD systems. The secret-key efficiency of Lucamarini *et al.*'s DV-QKD system at 50 km is 1 Mbps/10 Gbps = 10^{-3} bits/use, while the extrapolated secret-key efficiency for Huang *et al.*'s CV-QKD system is 90 kbps/50 Mbaud = 1.8×10^{-3} bits/use at that distance. FL-QKD, however, is predicted to have a secret-key efficiency of 0.2 bits/use at 50 km, two orders of magnitude better than state-of-the-art performance. Pirandola *et al.* [25, 26] have shown that the ultimate limit for any QKD protocol's secret-key efficiency, in bits per *mode*, is $-\log_2(1-\kappa_S) = 0.152$ bits per mode for a 50-km-long fiber with 0.2 dB/km loss. Because CV-QKD must mode-match its LO to its signal, CV-QKD's secret-key efficiencies in bits per channel use and bits per mode will coincide. Ideal DV-QKD systems also use single-mode transmission, in which case their secret-key efficiencies in bits per channel use and bits per mode will coincide. FL-QKD, on the other hand, employs many modes per channel use: at 50 km, our 10 Gbps modulation rate and 2 THz ASE bandwidth imply there are 200 modes per channel use, making FL-QKD's secret-key efficiency in bits per mode 0.2 bits/use $\div$ 200 modes/use = 10^{-3} bits/mode, i.e., on par with Huang *et al.*'s and Lucamarini *et al.*'s.

Before closing, two additional points need some attention. Both are related to our use of coincidence-based channel monitoring—the first concerns what information that monitoring might reveal to Eve and the second has to do with preventing Eve from eluding that monitoring with an intercept-resend attack—and both will be part of our continuing security analysis for FL-QKD.

In their channel monitoring, Alice and Bob will record the times at which their monitors have detected photons. Bob will transmit his detection times to Alice—over their tamper-proof classical connection—and Alice, in turn, will merge that data with her own to find the singles and coincidence rates she needs to determine the value of Eve's intrusion parameter, f_E. As part of her frequency-domain collective attack, Eve can listen to Alice and Bob's classical channel, and use Bob's photon-detection information to help her decode Bob's

transmission. The security analysis we have presented thus far does not account for that possibility. We show, however, in App. G, that Eve's Holevo information rate increases by an inconsequential amount when she pays attention to Bob's detection-time data. Indeed, the resolution of the secret-key rate plot in Fig. 3(a) is insufficient to show the effect.

Although Eve's frequency-domain collective attack derives no appreciable benefit from learning the photon-detection times of Bob's channel monitor, she could take an altogether different approach to breaking FL-QKD: an intercept-resend attack. By detecting the photons that Alice sends to Bob, Eve could transmit her own light—with photons concentrated at those detection times—in the hope that Bob's channel-monitor data will be indistinguishable from what he would get were she not present. Whether Eve could do so without changing Alice and Bob's f_E measurement is unclear, as is whether Eve could do so while simultaneously being able to retain a suitable reference beam for decoding Bob's message, but it is important to note that intercept-resend is *not* a frequency-domain collective attack, although security against it would be included were we able to prove FL-QKD's security against a general coherent attack. Even without that coherent-attack analysis, Alice and Bob's can augment their channel monitors to at least *detect* an intercept-resend attack—and hence turn it into a denial-of-service attack—by exploiting the entanglement between the signal and idler outputs of Alice's SPDC source. Alice and Bob's coincidence-based channel monitoring only relies on the photon-paired nature of those signal and idler beams, which is why Eve could potentially duplicate that pairing. Entanglement, on the other hand, cannot be spoofed. So, if Alice and Bob add either dispersive-optics (frequency-domain coincidence) measurements (as in [27]), or a Franson interferometer (as in [10]), to their channel monitors, it will be impossible for Eve to mount an intercept-resend attack without being detected.

In conclusion, existing single-channel QKD systems' secret-key rates at 50 km are so low that their Gbps WDM versions have overwhelming implementation and cost issues. With Gbps FL-QKD, however, OTP encryption of large files becomes practical over metropolitan-area networks using only a single channel. In this regard we emphasize that FL-QKD needs *no* new technology: erbium-doped fiber amplifiers suffice for Alice's ASE source and Bob's amplifier; high-quality SPDC's are capable of the brightness that Alice requires; BPSK modulators capable of 10 Gbps rates are readily available; Alice's receiver can use commercially available balanced mixers and need *not* be shot-noise limited [28]; and Alice and Bob's channel monitors can employ available superconducting nanowire detectors.

We acknowledge support from ONR grant number N00014-13-1-0774, AFOSR grant number FA9550-14-1-0052, and the DARPA Quiness Program through ARO Grant number W31P4Q-12-1-0019. We also acknowledge the anonymous reviewer who directed us to address the information that Eve might gain from knowing the photon-detection times from Bob's channel monitor.

Appendix A: Alice and Bob's Terminals

In this section we will detail the equipment that Alice and Bob use in the FL-QKD setup shown in Fig. 1.

1. Alice's Transmitter

Alice uses both a spontaneous parametric downconverter (SPDC) and an amplified spontaneous emission (ASE) source. For each bit interval, the SPDC source produces $M = TW \gg 1$ signal-idler mode pairs—where $T = 1/R$ gives the bit duration in terms of Bob's modulation rate R, and W is the SPDC's phase-matching bandwidth—with annihilation operators $\{\, (\hat{a}_{S_m}^{\rm SPDC}, \hat{a}_{I_m}^{\rm SPDC}) : 1 \leq m \leq M \,\}$. These SPDC mode pairs are in independent, identically-distributed, zero-mean Gaussian pure states that are characterized by the Wigner covariance matrix

$$\mathbf{\Lambda}_{SI}^{\rm SPDC} = \frac{1}{4} \begin{bmatrix} \mathbf{A}_{\rm SPDC} & \mathbf{C}_{\rm SPDC} \\ \mathbf{C}_{\rm SPDC} & \mathbf{A}_{\rm SPDC} \end{bmatrix}, \tag{A1}$$

where $\mathbf{A}_{\rm SPDC} = (2N_{\rm SPDC} + 1)\mathbf{I}_2$, with $\mathbf{I}_2$ being the 2×2 identity matrix, and

$$\mathbf{C}_{\rm SPDC} = \begin{bmatrix} C_{\rm SPDC} & 0 \\ 0 & -C_{\rm SPDC} \end{bmatrix}, \tag{A2}$$

with $N_{\rm SPDC} \ll 1$ and $C_{\rm SPDC} = 2\sqrt{N_{\rm SPDC}(N_{\rm SPDC} + 1)}$. For each bit interval, the ASE source—whose W Hz bandwidth and center frequency match those of the SPDC's signal beam—produces M signal-reference mode pairs, with annihilation operators $\{\, (\hat{a}_{S_m}^{\rm ASE}, \hat{a}_{R_m}^{\rm ASE}) : 1 \leq m \leq M \,\}$. These ASE mode pairs are in independent, identically-distributed,

completely-correlated thermal states that are characterized by the Wigner covariance matrix,

$$\mathbf{\Lambda}_{SR}^{\rm ASE} = \frac{1}{4}\left[\begin{array}{cc} \mathbf{A}_{\rm ASE} & \mathbf{C}_{\rm ASE} \\ \mathbf{C}_{\rm ASE} & \mathbf{A}_{\rm LO} \end{array}\right], \tag{A3}$$

where $\mathbf{A}_{\rm ASE} = (2N_{\rm ASE}+1)\mathbf{I}_2$, $\mathbf{C}_{\rm ASE} = 2\sqrt{N_{\rm ASE}N_{\rm LO}}\,\mathbf{I}_2$, and $\mathbf{A}_{\rm LO} = (2N_{\rm LO}+1)\mathbf{I}_2$, with $N_{\rm ASE} = 1 \ll N_{\rm LO}$,

Alice sends her SPDC's idler beam to a channel monitor, and combines her SPDC and ASE source's signal beams on an asymmetric beam splitter obtaining output modes,

$$\hat{a}_{A_m} = \sqrt{\kappa_C}\,\hat{a}_{S_m}^{\rm SPDC} + \sqrt{1-\kappa_C}\,\hat{a}_{S_m}^{\rm ASE}. \tag{A4}$$

Because she wants each of these modes to have average photon number $N_A \ll 1$, and she wants their ASE-to-SPDC ratio to be n:1 with $n \gg 1$, Alice uses $\kappa_C = 1 - nN_A/(n+1)$, and adjusts her downconverter's pump power to obtain $N_{\rm SPDC} = N_A/[n(1-N_A)+1]$. Note that for $N_A \leq 0.1$ and $n = 99$, these choices imply $\kappa_C \geq 0.9$.

Alice now directs a fraction κ_A of her ASE-SPDC signal light to a channel monitor and sends the remaining portion to Bob; the latter's M modes are governed by annihilation operators

$$\hat{a}_{S_m} = \sqrt{1-\kappa_A}\,\hat{a}_{A_m} + \sqrt{\kappa_A}\,\hat{v}_{A_m}, \tag{A5}$$

where the noise modes $\{\hat{v}_{A_m}\}$ are in their vacuum states. It follows that the signal modes Alice sends to Bob, her SPDC idler modes, and her ASE reference modes—i.e., the $\{\,(\hat{a}_{S_m}, \hat{a}_{I_m}^{\rm SPDC}, \hat{a}_{R_m}^{\rm ASE}) : 1 \leq m \leq M\,\}$—are independent, identically-distributed mode triples. Each such mode triple is in a zero-mean Gaussian state that is completely characterized by the Wigner covariance matrix

$$\mathbf{\Lambda}_{SIR} = \frac{1}{4}\left[\begin{array}{ccc} \mathbf{A}_S & \mathbf{C}'_{\rm SPDC} & \mathbf{C}'_{\rm ASE} \\ \mathbf{C}'_{\rm SPDC} & \mathbf{A}_{\rm SPDC} & \mathbf{0} \\ \mathbf{C}'_{ASE} & \mathbf{0} & \mathbf{A}_{\rm LO} \end{array}\right], \tag{A6}$$

where $\mathbf{A}_S = (2N_S+1)\mathbf{I}_2$, $N_S = (1-\kappa_A)N_A$, $\mathbf{C}'_{\rm SPDC} = \sqrt{(1-\kappa_A)\kappa_C}\,\mathbf{C}_{\rm SPDC}$, and $\mathbf{C}'_{\rm ASE} = \sqrt{(1-\kappa_A)(1-\kappa_C)}\,\mathbf{C}_{\rm ASE}$.

2. Bob's Terminal

For each bit interval, Bob receives a collection of independent, identically-distributed modes with annihilation operators $\{\,\hat{a}'_{S_m} : 1 \leq m \leq M\}$. He first diverts a fraction κ_B of each mode to his channel monitor before sending the remaining light—with annihilation operators

$$\hat{a}''_{S_m} = \sqrt{1-\kappa_B}\,\hat{a}'_{S_m} + \sqrt{\kappa_B}\,\hat{v}_{B_m}, \tag{A7}$$

where the noise modes $\{\hat{v}_{B_m}\}$ are in their vacuum states—to his binary phase-shift keying (BPSK) modulator. Bob then amplifies the modulated modes with an erbium-doped fiber amplifier (EDFA) with gain G_B and output ASE $N_B \geq G_B - 1$. The modes that Bob transmits to Alice therefore have photon annihilation operators

$$\hat{a}_{B_m} = (-1)^b\sqrt{G_B}\,\hat{a}''_{S_m} + \sqrt{G_B-1}\,\hat{n}^\dagger_{B_m}, \tag{A8}$$

where $b = 0$ or 1 is Bob's bit value and the noise modes $\{\hat{n}_{B_m}\}$ are in independent, identically-distributed thermal states with $\langle \hat{n}_{B_m}\hat{n}^\dagger_{B_m}\rangle = N_B/(G_B-1) \geq 1$.

3. Alice's Receiver

For a bit interval in which Bob has transmitted the value b, Alice receives a collection of independent, identically-distributed modes with annihilation operators $\{\,\hat{a}'_{B_m} : 1 \leq m \leq M\,\}$. Alice detects them using a balanced-homodyne arrangement and decides on the value of Bob's bit by comparing the outcome of that

$$\hat{N}_{\rm hom} = \sum_{m=1}^{M}\left(\hat{a}'^\dagger_{+m}\hat{a}'_{+m} - \hat{a}'^\dagger_{-m}\hat{a}'_{-m}\right) \tag{A9}$$

measurement with zero. She decides that Bob sent $b = 0$ if the measurement outcome exceeds zero, and she decides $b = 1$ otherwise [29]. In this expression,

$$\hat{a}'_{\pm m} = \sqrt{\eta}\left(\frac{\hat{a}'_{B_m} \pm \hat{a}'_{R_m}}{\sqrt{2}}\right) + \sqrt{1-\eta}\,\hat{v}_{\pm_m}, \tag{A10}$$

where η is the homodyne detector's efficiency, i.e., the product of its mode-mixing and quantum efficiencies, and the noise modes $\{\hat{v}_{\pm_m}\}$ are in their vacuum states.

The reference modes, $\{\hat{a}_{R_m}\}$, undergo optical amplification, with gain G_R and output ASE $N_R = G_R$, prior to being stored in a transmissivity-κ_I fiber spool—whose length is chosen

so that its output will be delay matched to the light Alice receives from Bob—resulting in

$$\hat{a}'_{R_m} = \sqrt{\kappa_I}\left(\sqrt{G_R}\hat{a}_{R_m} + \sqrt{G_R - 1}\,\hat{n}^\dagger_{R_m}\right) + \sqrt{1-\kappa_I}\,\hat{v}_{R_m}, \tag{A11}$$

with the amplifier-noise modes $\{\hat{n}_{R_m}\}$ being in independent, identically-distributed thermal states with $\langle \hat{n}_{R_m}\hat{n}^\dagger_{R_m}\rangle = N_R/(G_R-1)$ and the loss-noise modes $\{\hat{v}_{R_m}\}$ being in their vacuum states. For $N_{\rm LO} \gg 1$ and $G_R = 1/\kappa_I$, this amplify-then-store procedure leaves the average photon number of the reference almost unchanged and it preserves nearly-complete correlation between the stored reference and the signal beam that Alice sent to Bob. In particular, before storage we have that

$$\langle \hat{a}^\dagger_{R_m}\hat{a}_{R_m}\rangle = N_{\rm LO}, \tag{A12}$$

and

$$\begin{aligned}\frac{|\langle \hat{a}^\dagger_{S_m}\hat{a}_{R_m}\rangle|^2}{\langle \hat{a}^\dagger_{S_m}\hat{a}_{S_m}\rangle\langle \hat{a}^\dagger_{R_m}\hat{a}_{R_m}\rangle} &= \frac{(1-\kappa_C)N_{\rm ASE}}{\kappa_C N_{\rm SPDC} + (1-\kappa_C)N_{\rm ASE}} \\ &= n/(n+1),\end{aligned} \tag{A13}$$

while after storage we find that

$$\begin{aligned}\langle \hat{a}'^\dagger_{R_m}\hat{a}'_{R_m}\rangle &= \kappa_I G_R N_{\rm LO} + \kappa_I N_R \\ &= N_{\rm LO} + 1 \approx N_{\rm LO},\end{aligned} \tag{A14}$$

and

$$\begin{aligned}&\frac{|\langle \hat{a}^\dagger_{S_m}\hat{a}'_{R_m}\rangle|^2}{\langle \hat{a}^\dagger_{S_m}\hat{a}_{S_m}\rangle\langle \hat{a}'^\dagger_{R_m}\hat{a}'_{R_m}\rangle} \\ &= \frac{(1-\kappa_C)N_{\rm ASE}N_{\rm LO}}{(\kappa_C N_{\rm SPDC} + (1-\kappa_C)N_{\rm ASE})(N_{\rm LO}+1)} \\ &\approx n/(n+1),\end{aligned} \tag{A15}$$

when $N_{\rm LO} \gg 1$ [30]. For $n = 99$, as assumed in the paper's secret key-rate calculations, we see that Alice's reference suffers almost no degradation.

Appendix B: Eve's Frequency-Domain Collective Attack

Figure 5 shows the structure of Eve's general frequency-domain collective attack that we will use to place an upper bound on her Holevo information rate. Eve has replaced

the low-loss (0.2 dB/km) fibers that Alice and Bob presume are connecting their terminals with lossless fibers. For each of Alice's M transmitted modes, $\{\,\hat{a}_{S_m} : 1 \le m \le M\,\}$, in a bit interval, Eve then performs the same general unitary operation on K ancilla modes, $\{\,\hat{e}_{V_m}^{(k)} : 1 \le k \le K\,\}$, and Alice's $\hat{a}_{S_m}$, resulting in Bob's receiving the $\hat{a}'_{S_m}$ mode. Here, without loss of generality, we will assume that the $\{\hat{e}_{V_m}^{(k)}\}$ are in their vacuum states.

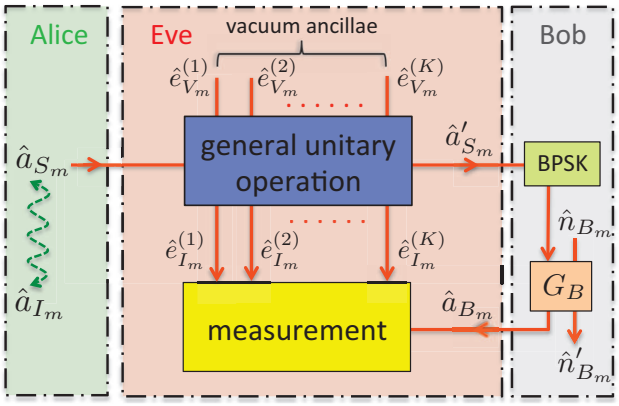

FIG. 5: (color online). Schematic of Eve's K-mode collective attack used to upper bound her Holevo information rate. BPSK: binary phase-shift keying. G_B amplifier gain. The dashed wavy line represents an entanglement that purifies the state of the $\hat{a}_{S_m}$ mode.

For each bit interval, Eve retains the KM ancilla output modes, $\{\,\hat{e}_{I_m}^{(k)} : 1 \le k \le K, 1 \le m \le M\,\}$, from her unitary operation and the light she taps from the Bob-to-Alice channel in a quantum memory. At the end of the key distribution session she then makes a collective measurement in her attempt to capture all of Bob's bit values. Because we will derive only an upper bound on Eve's Holevo information rate from this procedure, Fig. 5 shows Eve as taking *all* the light Bob sends to Alice. Other concessions to Eve that will be used in obtaining our upper bound are: (1) Bob will not divert any light to his channel monitor, i.e., $\kappa_B = 0$; and (2) Bob's amplifier will have quantum-limited ASE, viz., $N_B = G_B - 1$. All of these conditions increase Eve's Holevo information rate. That said, in practice Eve will *not* collect all the light that Bob sends to Alice, Bob *will* do channel monitoring ($\kappa_B > 0$), and Bob's amplifier may *not* be quantum limited ($N_B > G_B - 1$). Furthermore, in order to minimize Alice's ability to detect Eve's presence by simple photon-flux and spectrum monitoring, Eve will not inject any of her own light into Alice's receiver and she will arrange that the Bob-to-Alice channel still has transmissivity $\kappa_S = 10^{-0.02L}$ that Alice and Bob expect.

Appendix C: Upper Bound on Eve's Holevo Information Rate

Let $\hat{\mathbf{e}}_I$ denote $\{\, \hat{e}_{I_m}^{(k)} : 1 \leq k \leq K, 1 \leq m \leq M \,\}$ and $\hat{\boldsymbol{a}}_B$ denote $\{\, \hat{a}_{B_m} : 1 \leq m \leq M \,\}$. Eve's Holevo information rate for her general frequency-domain collective attack is bounded above by

$$\chi_{EB} = R \left[S(\hat{\rho}_{\hat{\mathbf{e}}_I, \hat{\boldsymbol{a}}_B}) - \sum_{b=0}^{1} S(\hat{\rho}^{(b)}_{\hat{\mathbf{e}}_I, \hat{\boldsymbol{a}}_B})/2 \right], \tag{C1}$$

where $S(\cdot)$ denotes von Neumann entropy, $\hat{\rho}^{(b)}_{\hat{\mathbf{e}}_I, \hat{\boldsymbol{a}}_B}$ is the conditional joint density operator for the $\hat{\mathbf{e}}_I$ and $\hat{\boldsymbol{a}}_B$ modes given Bob's bit value, $\hat{\rho}_{\hat{\mathbf{e}}_I, \hat{\boldsymbol{a}}_B} = \sum_{b=0}^{1} \hat{\rho}^{(b)}_{\hat{\mathbf{e}}_I, \hat{\boldsymbol{a}}_B}/2$ is their unconditional joint density operator, and the bound is due to our assuming that Eve captures all the light Bob sends to Alice.

Before going into details, we place two constraints on Eve's attack. First, we assume that Eve precludes her presence being detected from simple photon-flux and spectrum monitoring at Bob's terminal by requiring her attack to satisfy

$$\langle \hat{a}'^{\dagger}_{S_m} \hat{a}'_{S_m} \rangle = \kappa_S N_S, \tag{C2}$$

where $\kappa_S = 10^{-0.02L}$ is the transmissivity of the L-km-long connection Alice and Bob believe they have and N_S is the brightness of the light Alice sends to Bob. Second, Alice and Bob's channel monitors allow them to measure Eve's intrusion parameter, f_E, that, as shown in App. E, measures Eve's degradation of the phase-sensitive cross-covariance between Alice's $\hat{a}_{I_m}$ mode and Bob's $\hat{a}'_{S_m}$ mode, i.e., we have that

$$|\, \langle \hat{a}'_{S_m} \hat{a}_{I_m} \rangle \,|^2 = (1 - f_E) \kappa_S |\, \langle \hat{a}_{S_m} \hat{a}_{I_m} \rangle \,|^2. \tag{C3}$$

Equations (C2) and (C3) both constrain what Eve's general frequency-domain collective attack does to the Wigner covariance matrix of the $(\hat{a}'_{S_m}, \hat{a}_{I_m})$ mode pair.

To proceed further, we first introduce $\hat{\boldsymbol{a}}_I = \{\, \hat{a}_{I_m} : 1 \leq m \leq M \}$ that purifies $\hat{\boldsymbol{a}}_S = \{\, \hat{a}_{S_m} : 1 \leq m \leq M \}$, i.e., the mode pairs $\{\, (\hat{a}_{S_m}, \hat{a}_{I_m}) : 1 \leq m \leq M \,\}$ are in independent, identically-distributed, zero-mean Gaussian pure states that are characterized by the Wigner covariance matrix

$$\boldsymbol{\Lambda}_{SI} = \frac{1}{4} \begin{bmatrix} \mathbf{A}_S & \mathbf{C}_S \\ \mathbf{C}_S & \mathbf{A}_S \end{bmatrix}, \tag{C4}$$

where

$$\mathbf{C}_S = \begin{bmatrix} 2\sqrt{N_S(N_S+1)} & 0 \\ 0 & -2\sqrt{N_S(N_S+1)} \end{bmatrix}. \tag{C5}$$

After Eve's unitary operation, however, the $\{\hat{a}'_{S_m}\}$ modes will, in general, be in non-Gaussian states. Next, we introduce the complement to the Eq. (A8) input-output relation for Bob's amplifier, i.e.,

$$\hat{n}'_{B_m} = \sqrt{G_B}\,\hat{n}_{B_m} + (-1)^b\sqrt{G_B - 1}\,\hat{a}''_{S_m}, \tag{C6}$$

with $\hat{a}''_{S_m} = \hat{a}'_{S_m}$ because our upper bound will be found using $\kappa_B = 0$, and $\hat{n}_{B_m}$ in its vacuum state because that bound will presume Bob's amplifier is quantum limited. With these assumptions, we have that the $\{\,\hat{\boldsymbol{a}}_I, \hat{\boldsymbol{a}}_S, \hat{\mathbf{e}}_V, \hat{\mathbf{n}}_B\,\}$ modes—where $\hat{\mathbf{e}}_V = \{\,\hat{e}^{(k)}_{V_m} : 1 \leq k \leq K, 1 \leq m \leq M\}$, and $\hat{\mathbf{n}}_B = \{\,\hat{n}_{B_m} : 1 \leq m \leq M\}$—are in a zero-mean Gaussian pure state. It then follows that the $\{\,\hat{\boldsymbol{a}}_I, \hat{\boldsymbol{a}}_B, \hat{\mathbf{e}}_I, \hat{\mathbf{n}}'_B\,\}$ modes—where $\hat{\mathbf{n}}'_B = \{\,\hat{n}'_{B_m} : 1 \leq m \leq M\}$—are in a (not necessarily zero-mean Gaussian) pure state given Bob's bit value, because Eve and Bob's operations are unitary. An immediate consequence of this purity is

$$S(\hat{\rho}^{(b)}_{\hat{\mathbf{e}}_I, \hat{\boldsymbol{a}}_B}) = S(\hat{\rho}^{(b)}_{\hat{\boldsymbol{a}}_I, \hat{\mathbf{n}}'_B}). \tag{C7}$$

Moreover, the unitarity of the phase modulation that Bob performs, given his bit value, implies that these conditional entropies are independent of b. So, because the mode pairs $\{\,\hat{a}_{I_m}, \hat{n}'_{B_m} : 1 \leq m \leq M\,\}$ are in independent, identically-distributed states given Bob's bit value, we have that

$$\sum_{b=0}^{1} S(\hat{\rho}^{(b)}_{\hat{\boldsymbol{a}}_I, \hat{\mathbf{n}}'_B})/2 = MS(\hat{\rho}^{(0)}_{\hat{a}_{I_m}, \hat{n}'_{B_m}}). \tag{C8}$$

Having obtained a simplified expression for the second entropy term on the right in (C1), we use the subadditivity of von Neumann entropy to get

$$\chi_{EB} \leq R\left[S(\hat{\rho}_{\hat{\mathbf{e}}_I}) + S(\hat{\rho}_{\hat{\boldsymbol{a}}_B}) - MS(\hat{\rho}^{(0)}_{\hat{a}_{I_m}, \hat{n}'_{B_m}})\right], \tag{C9}$$

with equality when $\hat{\rho}_{\hat{\mathbf{e}}_I \hat{\boldsymbol{a}}_B} = \hat{\rho}_{\hat{\mathbf{e}}_I} \otimes \hat{\rho}_{\hat{\boldsymbol{a}}_B}$. The $\{\hat{\mathbf{e}}_I\}$ modes are independent of Bob's bit value. Grouping them by mode index m, i.e., writing $\{\hat{\mathbf{e}}_I\} = \{\,\hat{\mathbf{e}}_{I_m} : 1 \leq m \leq M\,\}$ where $\hat{\mathbf{e}}_{I_m} = \{\,\hat{e}^{(k)}_{I_m} : 1 \leq k \leq K\,\}$, we have that the $\{\hat{\mathbf{e}}_{I_m}\}$ modes are independent and identically distributed, so

$$S(\hat{\rho}_{\hat{\mathbf{e}}_I}) = MS(\hat{\rho}_{\hat{\mathbf{e}}_{I_m}}). \tag{C10}$$

Moreover, because Eve's operation is unitary, the $\{\hat{\mathbf{e}}_{I_m}, \hat{a}_{I_m}, \hat{a}'_{S_m}\}$ modes are in a pure state, so we have

$$S(\hat{\rho}_{\hat{\mathbf{e}}_{I_m}}) = S(\hat{\rho}_{\hat{a}_{I_m}, \hat{a}'_{S_m}}). \tag{C11}$$

Finally, since we are considering Eve's frequency-domain collective attack, the $\{\hat{a}_{B_m}\}$ modes are independent and identically distributed, thus subadditivity gives us

$$S(\hat{\rho}_{\hat{\boldsymbol{a}}_B}) \leq MS(\hat{\rho}_{\hat{a}_{B_m}}). \tag{C12}$$

Putting the preceding results together gives us an upper bound on Eve's Holevo information rate:

$$\chi_{EB} \leq R \min\Big\{M\Big[S(\hat{\rho}_{\hat{a}_{B_m}}) - [S(\hat{\rho}^{(0)}_{\hat{a}_{I_m},\hat{n}'_{B_m}}) - S(\hat{\rho}_{\hat{a}_{I_m},\hat{a}'_{S_m}})]\Big], 1\Big\}, \tag{C13}$$

where we have used the fact that Eve's maximum Holevo information per bit interval is one. Our next step is to place a lower bound on $S(\hat{\rho}^{(0)}_{\hat{a}_{I_m},\hat{n}'_{B_m}}) - S(\hat{\rho}_{\hat{a}_{I_m},\hat{a}'_{S_m}})$ by recognizing that term as the entropy output of a tensor-product quantum channel.

Definition: Entropy output

Let $\phi(\cdot)$ be a quantum channel that maps states in $\mathcal{H}_1$ to states in $\mathcal{H}_2$. The entropy-output function $E_\phi(\cdot)$ of that channel quantifies the difference between the von Neumann entropies of its output and input states, i.e., for input-state $\hat{\rho}$ we have that

$$E_\phi(\hat{\rho}) = S[\phi(\hat{\rho})] - S(\hat{\rho}). \tag{C14}$$

Using this definition (C13) can be rewritten as

$$\chi_{EB} \leq R \min\Big\{M[S(\hat{\rho}_{\hat{a}_{B_m}}) - E_\phi(\hat{\rho}_{\hat{a}_{I_m},\hat{a}'_{S_m}})], 1\Big\}. \tag{C15}$$

Next, we prove that entropy output is superadditive for the quantum channel $\phi(\cdot) = \phi_S(\cdot) \otimes I_I(\cdot)$ that maps the $\{\hat{a}'_{S_m}, \hat{a}_{I_m}\}$ modes into the $\{\hat{n}'_{B_m}, \hat{a}_{I_m}\}$ modes, where $I_I(\cdot)$ is the identity channel.

Theorem: Superadditivity of entropy output

Let A_{12} and B_{12} be bipartite quantum systems on $\mathcal{H}_A^{\otimes 2}$ and $\mathcal{H}_B^{\otimes 2}$ with components $\{A_1, A_2\}$ and $\{B_1, B_2\}$, respectively. For an arbitrary input state $\hat{\rho}_{A_{12},B_{12}}$ in $\mathcal{H}_A^{\otimes 2} \otimes \mathcal{H}_B^{\otimes 2}$, and an arbitrary quantum channel $\phi(\cdot)$ that maps states in $\mathcal{H}_A \otimes \mathcal{H}_B$ into states in $\mathcal{H}'_A \otimes \mathcal{H}'_B$ we have that

$$E_{\phi\otimes\phi}(\hat{\rho}_{A_{12},B_{12}}) \geq E_\phi(\hat{\rho}_{A_1,B_1}) + E_\phi(\hat{\rho}_{A_2,B_2}), \tag{C16}$$

with equality when $\hat{\rho}_{A_{12},B_{12}} = \hat{\rho}_{A_1B_1} \otimes \hat{\rho}_{A_2B_2}$*, i.e., entropy output is superadditive.*
From entropy output's definition, Ineq. (C16) is equivalent to

$$S[\phi \otimes \phi\,(\hat{\rho}_{A_{12},B_{12}}) - S(\hat{\rho}_{A_{12},B_{12}}) \geq S[\phi(\hat{\rho}_{A_1,B_1})] \\ - S(\hat{\rho}_{A_1,B_1}) + S[\phi(\hat{\rho}_{A_2,B_2})] - S(\hat{\rho}_{A_2,B_2}). \tag{C17}$$

This inequality can be rewritten as

$$I(A_1B_1 : A_2B_2) \geq I[\phi(A_1B_1) : \phi(A_2B_2)], \tag{C18}$$

where $I(A:B) = S(\hat{\rho}_A) + S(\hat{\rho}_B) - S(\hat{\rho}_{A,B})$ is the quantum mutual information. The validity of Ineq. (C18) follows from the quantum data-processing inequality [31], because $\phi(\cdot)$ acts independently on (A_1, B_1) and (A_2, B_2).

The subadditivity of von Neumann entropy and the superadditivity of entropy output imply that $S(\hat{\rho}_{\hat{a}_{B_m}}) - E_\phi(\hat{\rho}_{\hat{a}_{I_m},\hat{a}'_{S_m}})$ is subadditive. Moreover, von Neumann entropy is continuous. So, if we can show that entropy output for Gaussian channels is invariant under passive symplectic operations then we could apply Gaussian extremality [32] and obtain

$$S(\hat{\rho}_{\hat{a}_{B_m}}) - E_\phi(\hat{\rho}_{\hat{a}_{I_m},\hat{a}'_{S_m}}) \leq \\ S_G(\mathbf{\Lambda}_B) - [S_G(\mathbf{\Lambda}^{(0)}_{IB'}) - S_G(\mathbf{\Lambda}_{IS'})], \tag{C19}$$

where $S_G(\mathbf{\Lambda})$ denotes the von Neumann entropy of a Gaussian state with Wigner covariance matrix $\mathbf{\Lambda}$, and $\mathbf{\Lambda}_B$, $\mathbf{\Lambda}^{(0)}_{IB'}$, and $\mathbf{\Lambda}_{IS'}$ are the Wigner covariance matrices of $\hat{\rho}_{\hat{a}_{B_m}}$, $\hat{\rho}^{(0)}_{\hat{a}_{I_m},\hat{n}'_{B_m}}$, and $\hat{\rho}_{\hat{a}_{I_m},\hat{a}'_{S_m}}$, respectively. It would then follow that, Eve's Holevo information rate for her general frequency-domain collective attack satisfies

$$\chi_{EB} \leq R \min\Big\{ M[S_G(\mathbf{\Lambda}_B) + S_G(\mathbf{\Lambda}_{IS'}) - S_G(\mathbf{\Lambda}^{(0)}_{IB'})], 1 \Big\}, \tag{C20}$$

which means that we only need to maximize this rate when Eve makes a collective frequency-domain Gaussian attack. Note that $\mathbf{\Lambda}_B$ and $\mathbf{\Lambda}^{(0)}_{IB'}$ are obtained from $\mathbf{\Lambda}_{IS'}$ by applying Bob's modulator and amplifier transformations, and that Eqs. (C2) and (C3) place constraints on $\mathbf{\Lambda}_{IS'}$ when Eve mounts her frequency-domain collective attack. The rest of this section is devoted to: (1) proving that entropy output for Gaussian channels is invariant under passive symplectic transformations; and (2) placing an explicit upper bound on Eve's Holevo information rate for her optimum frequency-domain collective Gaussian attack under the preceding covariance constraints.

To show that entropy output for Gaussian channels is invariant under passive symplectic transformations, we rely on the fact that Gaussian channels and symplectic transformations are both linear Bogoliubov mode transformations. Also, because the $\{\hat{a}_{I_m}\}$ modes are in Gaussian states, we only need to consider symplectic transformations of the $\{\hat{a}'_{S_m}\}$ modes. Consider a Gaussian channel $\phi_G(\cdot)$ whose input modes are $\hat{a}_1$ and $\hat{a}_2$ and whose output modes satisfy

$$\hat{b}_1 = c_1\hat{a}_1 + c_2\hat{a}_1^\dagger + c_3\hat{n}_1 + c_4\hat{n}_1^\dagger, \tag{C21}$$

$$\hat{b}_2 = c_1\hat{a}_2 + c_2\hat{a}_2^\dagger + c_3\hat{n}_2 + c_4\hat{n}_2^\dagger, \tag{C22}$$

where the $\{c_k\}$ are complex-valued coefficients associated with $\phi_G(\cdot)$ and the $\{\hat{n}_k\}$ are vacuum-state ancilla modes. Now suppose that the input modes are applied to the input ports of a 50–50 beam splitter whose outputs,

$$\hat{a}_\pm = (\hat{a}_1 \pm \hat{a}_2)/\sqrt{2}, \tag{C23}$$

become the inputs to $\phi_G(\cdot)$. Now the output modes will be

$$\hat{b}_+ = c_1\hat{a}_+ + c_2\hat{a}_+^\dagger + c_3\hat{n}_1 + c_4\hat{n}_1^\dagger, \tag{C24}$$

$$\hat{b}_- = c_1\hat{a}_- + c_2\hat{a}_-^\dagger + c_3\hat{n}_2 + c_4\hat{n}_2^\dagger. \tag{C25}$$

Because unitary operations do not change von Neumann entropy, we can apply another 50–50 beam splitter to these output modes and obtain

$$\hat{b}'_1 = (\hat{b}_+ + \hat{b}_-)/\sqrt{2}, \tag{C26}$$

$$\hat{b}'_2 = (\hat{b}_+ - \hat{b}_-)/\sqrt{2} \tag{C27}$$

whose von Neumann entropy will be the same as that of the $\{\hat{b}_+, \hat{b}_-\}$ modes. With some algebra, we can verify that

$$\hat{b}'_1 = c_1\hat{a}_1 + c_2\hat{a}_1^\dagger + c_3\hat{n}_+ + c_4\hat{n}_+^\dagger, \tag{C28}$$

$$\hat{b}'_2 = c_1\hat{a}_2 + c_2\hat{a}_2^\dagger + c_3\hat{n}_- + c_4\hat{n}_-^\dagger, \tag{C29}$$

where the $\hat{n}_\pm = (\hat{n}_1 \pm \hat{n}_2)/\sqrt{2}$ are in their vacuum states. Hence the $\{\hat{b}'_1, \hat{b}'_2\}$ modes have the same von Neumann entropy as $\{\hat{b}_1, \hat{b}_2\}$ modes. A similar analysis will demonstrate entropy

invariance for waveplate transformations, completing the proof that the entropy output for Gaussian channels is invariant under passive symplectic transformations.

Having shown the last condition we needed for Gaussian extremality to hold, we turn our attention to Eve's collective frequency-domain Gaussian attack. In such an attack, Eve's unitary operation in Fig. 5 is a $K+1$-mode Bogoliubov transformation [33], resulting in

$$\hat{a}'_{S_m} = u_0 \hat{a}_{S_m} + v_0^* \hat{a}^\dagger_{S_m} + \sum_{k=1}^{K} (u_k \hat{e}^{(k)}_{V_m} + v_k^* \hat{e}^{(k)\dagger}_{V_m}) + \alpha. \tag{C30}$$

A direct consequence of Gaussian extremality is that the optimum displacement is $\alpha = 0$, because only when $\alpha = 0$ will the unconditional state $\hat{\rho}_{\hat{a}_{B_m}}$ be Gaussian. So, setting $\alpha = 0$, we need to maximize the right-hand side of Ineq. (C20) over the parameters $\{\, u_k, v_k : 1 \leq k \leq K\}$ and α, subject to the following constraints.

First, so that Eq. (C30) yields a proper free-field commutator bracket for $\hat{a}'_{S_m}$, we require that the coefficients $\{\, u_k, v_k : 0 \leq k \leq K \,\}$ satisfy

$$\sum_{k=0}^{K} (|u_k|^2 - |v_k|^2) = 1. \tag{C31}$$

Second, the security-monitoring constraint in Eq. (C2) implies that Eve's attack parameters $\{\, u_k, v_k : 0 \leq k \leq K \,\}$ must obey

$$(|u_0|^2 + |v_0|^2) N_S + \sum_{k=0}^{K} |v_k|^2 = \kappa_S N_S. \tag{C32}$$

Because the first term on the left is Alice's light injection into Bob while the second terms is due to Eve, the constraint in Eq. (C3) can be rewritten as

$$f_E = \frac{\sum_{k=0}^{K} |v_k|^2}{\kappa_S N_S}, \tag{C33}$$

which shows that under Eve's collective frequency-domain Gaussian attack the intrusion parameter f_E equals the fraction of light entering Bob's terminal that is due to Eve. In App. E we will show that Alice and Bob's photon-coincidence channel monitoring can measure f_E. Hence Eve will constrain her attack parameters to yield an f_E value that Alice and Bob will tolerate in the FL-QKD protocol. (Eve's using an f_E value that exceeds what Alice and Bob will tolerate would constitute a denial-of-service attack.)

1. Evaluating Eve's Holevo Information Rate Upper Bound

We can evaluate the bound in (C20) by symplectic diagonalization of the Wigner covariance matrices of $\{\hat{a}_{I_m}, \hat{n}'_{B_m}\}$, $\{\hat{a}_{I_m}, \hat{a}'_{S_m}\}$, and $\hat{a}_{B_m}$ conditioned on the value of Bob's bit. From App. B we can easily show that

$$\mathbf{\Lambda}_{IS'} = \frac{1}{4}\begin{bmatrix} \mathbf{A}_S & \mathbf{C}_{IS'} \\ \mathbf{C}_{IS'} & \mathbf{B}_{IS'} \end{bmatrix}, \tag{C34}$$

where

$$\mathbf{B}_{IS'} = 2\begin{bmatrix} B + \mathrm{Re}(w) & \mathrm{Im}(w) \\ \mathrm{Im}(w) & B - \mathrm{Re}(w) \end{bmatrix}, \tag{C35}$$

and

$$\mathbf{C}_{IS'} = 2\sqrt{N_S(N_S+1)}\begin{bmatrix} \mathrm{Re}(u_0 + v_0) & \mathrm{Im}(u_0 - v_0) \\ \mathrm{Im}(u_0 + v_0) & -\mathrm{Re}(u_0 - v_0) \end{bmatrix}, \tag{C36}$$

with $B = 1/2 + \kappa_S N_S$, $w = \mathbf{v}^\dagger \mathbf{u} + (2N_S + 1)v_0^* u_0$, $\mathbf{v}^\dagger \equiv \begin{bmatrix} v_1^* & v_2^* & \cdots & v_K^* \end{bmatrix}$ and $\mathbf{u} = \begin{bmatrix} u_1 & u_2 & \cdots & u_K \end{bmatrix}^T$ and ^{T} denoting transpose. We also find that

$$\mathbf{\Lambda}^{(b)}_{IB'} = \frac{1}{4}\begin{bmatrix} \mathbf{A}_S & \mathbf{C}^{(b)}_{IB'} \\ \mathbf{C}^{(b)}_{IB'} & \mathbf{B}_{IB'} \end{bmatrix}, \tag{C37}$$

where

$$\mathbf{B}_{IB'} = \begin{bmatrix} B' + \mathrm{Re}(x) & -\mathrm{Im}(x) \\ -\mathrm{Im}(x) & B' - \mathrm{Re}(x) \end{bmatrix}, \tag{C38}$$

$$\mathbf{C}^{(b)}_{IB'} = (-1)^b 2\sqrt{(G_B - 1)N_S(N_S+1)} \times \begin{bmatrix} \mathrm{Re}(u_0 + v_0) & -\mathrm{Im}(u_0 - v_0) \\ \mathrm{Im}(u_0 + v_0) & \mathrm{Re}(u_0 - v_0) \end{bmatrix}, \tag{C39}$$

with $B' = 1 + 2(G_B - 1)(\kappa_S N_S + 1)$ and $x = 2(G_B - 1)w$. The last Wigner covariance that we need is

$$\mathbf{\Lambda}^{(b)}_B = \frac{1}{4}\begin{bmatrix} B'' + 2G_B\mathrm{Re}(w) & 2G_B\mathrm{Im}(w) \\ 2G_B\mathrm{Im}(w) & B'' - 2G_B\mathrm{Re}(w) \end{bmatrix}, \tag{C40}$$

where $B'' = -1 + 2G_B(\kappa_S N_S + 1)$. Because this covariance matrix is independent of b, we have $\mathbf{\Lambda}_B = \mathbf{\Lambda}^{(b)}_B$ and the unconditional state of $\hat{a}_{B_m}$ is Gaussian.

After evaluating all the symplectic eigenvalues of the preceding Wigner covariances, we have that

$$\begin{aligned}\chi_{EB} \;\leq\; & R\min\Bigg\{M\left[g\left(\frac{4\xi_{IS'+}-1}{2}\right)+g\left(\frac{4\xi_{IS'-}-1}{2}\right)\right.\\ & +\; g\left(\frac{4\xi_B-1}{2}\right)-g\left(\frac{4\xi_{IB'+}-1}{2}\right)\\ & -\; \left.g\left(\frac{4\xi_{IB'-}-1}{2}\right)\right],1\Bigg\},\end{aligned} \tag{C41}$$

where $g(x)=(x+1)\log_2(x+1)-x\log_2(x)$ is the von Neumann entropy of a thermal state with average photon number x. Here $\xi_{IS'+}\geq\xi_{IS'-}$ and $\xi_{IB'+}\geq\xi_{IB'-}$ are, respectively, the symplectic eigenvalues of $\mathbf{\Lambda}_{IS'}$ and $\mathbf{\Lambda}^{(b)}_{IB'}$, and ξ_B is the symplectic eigenvalue of $\mathbf{\Lambda}_B$.

Because FL-QKD operates with $N_B\gg 1$, we shall replace (C41) with its leading-order expansion in that regime, namely

$$\begin{aligned}\chi_{EB} \;\leq\; & R\min\{M\left[g(2\xi_{IS'+}-1/2)+g(2\xi_{IS'-}-1/2)\right.\\ & -\; \left.g(2\tilde{\xi}_{IB'-}-1/2)+O(N_B^{-1/2})\right],1\Big\},\end{aligned} \tag{C42}$$

where $\xi_{IS'\pm}$ is independent of N_B and $\tilde{\xi}_{IB'-}$ is the $N_B\gg 1$ leading-order, $O(1)$, approximation to $\xi_{IB'-}$. Our next task is to maximize the right-hand side of (C42) over all possible values of Eve's attack parameters, $\{\,u_k,v_k\,:\,0\leq k\leq K\,\}$, subject to the commutator-preservation constraint (C31), the photon-flux constraint (C32), and the injection-fraction constraint (C33). The first of these constraints is an absolute requirement on frequency-domain collective Gaussian attacks, the second is set by Eve's desire to elude Bob's detecting her by simple photon-flux and spectrum monitoring, and the third is a consequence of Alice and Bob's photon-coincidence monitoring.

The preceding attack-parameter optimization can be accomplished more readily by sat-

isfying (C31), (C32), and (C33) by means of

$$|v_0| = \sqrt{(1-f_E)\kappa_S}\,\cos(\gamma_v),$$
$$\text{with } \gamma_v \in [0,\pi/2] \text{ and } \cos^2(\gamma_v) \leq f_E N_S/(1-f_E) \tag{C43}$$

$$|u_0| = \sqrt{(1-f_E)\kappa_S}\,\sin(\gamma_v) \tag{C44}$$

$$\mathbf{v}^\dagger\mathbf{v} = [f_E\kappa_S N_S - (1-f_E)\kappa_S\cos^2(\gamma_v)] \tag{C45}$$

$$\mathbf{u}^\dagger\mathbf{u} = f_E\kappa_S N_S + 1 - (1-f_E)\kappa_S + (1-f_E)\kappa_S\cos^2(\gamma_v), \tag{C46}$$

$$|\mathbf{v}^\dagger\mathbf{u}| = \sqrt{(\mathbf{v}^\dagger\mathbf{v})(\mathbf{u}^\dagger\mathbf{u})}\,\cos(\delta), \text{ with } \delta \in [0,\pi/2]. \tag{C47}$$

Next, we further simplify (C42) by restricting it to FL-QKD's desired long-distance operating regime, wherein $\kappa_S \ll 1$. Here we find that

$$\begin{aligned}\chi_{EB} \leq R\min\Big(M\big\{&\kappa_S[f_E N_S - (1-f_E)\cos^2(\gamma_v)]\sin^2(\delta)\\ &\times\{1/\ln(2) - \log_2[\sin^2(\delta)\kappa_S[f_E N_S - (1-f_E)\cos^2(\gamma_v)]]\}\\ &+ (1-f_E)\kappa_S\log_2(1+1/N_S)[(2N_S+1)\cos^2(\gamma_v) + N_S^2]\\ &+ O(\kappa_S^{3/2}) + O(N_B^{-1/2})\big\}, 1\Big).\end{aligned} \tag{C48}$$

Neglecting the $O(\cdot)$ terms, we find that the derivative of the right-hand side of (C48) with respect to $\sin^2(\delta)$ will be positive if $\ln[2f_E\kappa_S N_S] < 0$, a condition that will always be satisfied when $\kappa_S N_S \ll 1$. Thus we conclude that $\delta = \pi/2$ is Eve's best choice. Next, using $\delta = \pi/2$ in (C48), neglecting the $O(\cdot)$ terms, and differentiating (C48)'s right-hand side with respect to $\cos^2(\gamma_v)$, we find that it will be negative if

$$\begin{aligned}\ln(2f_E\kappa_S) &< -\max_{N_S\leq 1}[\ln(N_S) + (1+2N_S)\ln(1+1/N_S)]\\ &\approx -2,\end{aligned} \tag{C49}$$

where the N_S constraint is due to FL-QKD's operating at low brightness. Alice and Bob's constraining Eve to $f_E \ll 1$ combined with $\kappa_S \ll 1$ ensures that (C49) is obeyed, making $\gamma_v = \pi/2$ optimum.

At this point, using $\delta = \gamma_v = \pi/2$ in Eqs. (C44)–(C47), we have that Eve's optimum

frequency-domain collective Gaussian attack is to use the Fig. 5 setup with

$$v_0 = 0 \tag{C50}$$

$$|u_0| = \sqrt{(1 - f_E)\kappa_S} \tag{C51}$$

$$\alpha = 0 \tag{C52}$$

$$\mathbf{v}^\dagger \mathbf{v} = f_E \kappa_S N_S \tag{C53}$$

$$\mathbf{u}^\dagger \mathbf{u} = f_E \kappa_S N_S + 1 - (1 - f_E)\kappa_S \tag{C54}$$

$$\mathbf{v}^\dagger \mathbf{u} = 0. \tag{C55}$$

Her Holevo information rate for this optimum frequency-domain collective Gaussian attack obeys

$$\begin{aligned} \chi_{EB} \leq \chi_{EB}^{\mathrm{UB}} = \\ R \min[M(\kappa_S N_S \{ f_E [1/\ln(2) - \log_2(f_E \kappa_S N_S)] + \\ (1 - f_E) N_S \log_2(1 + 1/N_S) \}), 1], \end{aligned} \tag{C56}$$

This result omits the $O(\kappa_S^{3/2})$ and $O(N_B^{-1/2})$ terms in (C48), so it is important to note that: (1) in computing the paper's secret-key rate results we used the *exact* form from (C41) with the attack parameters from Eqs. (C50)–(C55); and (2) numerically maximizing the right-hand side of (C42) over Eve's attack parameters for the path lengths considered in the paper yielded $\delta = \gamma_v = \pi/2$ [34].

2. Physical Realization of Eve's Optimum Frequency-Domain Collective Attack

At this juncture it is instructive to exhibit a physical implementation for Eve's optimum frequency-domain collective attack, namely her Fig. 5 Gaussian attack with attack parameters given by Eqs. (C50)–(C55). That attack can be realized with Eve's using only two ancilla and choosing $u_1 = \sqrt{f_E \kappa_S N_S + 1 - (1 - f_E)\kappa_S}$, $v_1 = 0$, $u_2 = 0$, and $v_2 = \sqrt{f_E \kappa_S N_S}$. Then, because Alice and Bob must do phase tracking—FL-QKD is an interferometric protocol—no loss of generality ensues from setting $u_0 = \sqrt{(1 - f_E)\kappa_S}$. With these parameter values, Eve's optimum frequency-domain collective Gaussian attack becomes the SPDC beam-splitter attack, shown in Fig. 2. Here, Eve uses an SPDC source identical to Alice's with the exception

of its brightness being $N_E = f_E \kappa_S N_S / [1 - (1 - f_E)\kappa_S]$. She retains her idler and injects her signal into the Alice-to-Bob channel through a beam splitter with Alice-to-Bob transmissivity $\sqrt{(1 - f_E)\kappa_S}$. Eve then performs a collective measurement on the light she collects from that beam splitter's other output port, her retained idler, and the light she taps from the Bob-to-Alice channel in which she has inserted a beam splitter with Bob-to-Alice transmissivity κ_S. To see that this identification is correct, we exhibit its three-mode Bogoliubov transformation,

$$\begin{aligned} \hat{a}'_{S_m} &= \sqrt{(1 - f_E)\kappa_S}\, \hat{a}_{S_m} \\ &+ \sqrt{f_E \kappa_S N_S + 1 - (1 - f_E)\kappa_S}\, \hat{e}^{(1)}_{V_m} \\ &+ \sqrt{f_E \kappa_S N_S}\, \hat{e}^{(2)\dagger}_{V_m} \end{aligned} \tag{C57}$$

$$\begin{aligned} \hat{e}^{(1)}_{I_m} &= \sqrt{\frac{f_E \kappa_S N_S}{1 - (1 - f_E)\kappa_S}}\, \hat{e}^{(1)\dagger}_{V_m} \\ &+ \sqrt{\frac{f_E \kappa_S N_S + 1 - (1 - f_E)\kappa_S}{1 - (1 - f_E)\kappa_S}}\, \hat{e}^{(2)}_{V_m} \end{aligned} \tag{C58}$$

$$\begin{aligned} \hat{e}^{(2)}_{I_m} &= \sqrt{1 - (1 - f_E)\kappa_S}\, \hat{a}_{S_m} \\ &+ \sqrt{\frac{(1 - f_E)\kappa_S (f_E \kappa_S N_S + 1 - (1 - f_E)\kappa_S)}{1 - (1 - f_E)\kappa_S}}\, \hat{e}^{(1)}_{V_m} \\ &+ \sqrt{\frac{(1 - f_E)\kappa_S (f_E \kappa_S N_S)}{1 - (1 - f_E)\kappa_S}}\, \hat{e}^{(2)\dagger}_{V_m}. \end{aligned} \tag{C59}$$

and recognize $\hat{a}'_{S_m}$ and $\hat{e}^{(2)}_{I_m}$ as the beam splitter outputs in Fig. 2 and $\hat{e}^{(1)}_{I_m}$ as Eve's retained idler.

In the paper, we not only report our upper bound on the Holevo information rate for Eve's optimum frequency-domain collective Gaussian attack, as realized by the SPDC beam-splitter arrangement, but also upper bounds on her Holevo information rates for her collective passive and collective active attacks with that arrangement. The upper bound on the Holevo information rate of Eve's collective passive attack is trivially obtained from the development presented earlier in this section: her optimum collective frequency-domain Gaussian attack becomes her collective passive attack when $f_E = 0$. Eve's optimum collective active attack is realized, in the Fig. 2 setup, by her only making a collective measurement on her retained

idler and the light she taps from the Bob-to-Alice channel. That rate bound, which can be derived by a procedure similar to what we have just presented, is as follows:

$$\chi_{EB}^{\text{UBact}} = R \min\left\{ M \left[S_G(\mathbf{\Lambda}_{IB}) - \sum_{b=0}^{1} S_G(\mathbf{\Lambda}_{IB}^{(b)}) \right], 1 \right\}, \tag{C60}$$

where

$$\mathbf{\Lambda}_{IB}^{(b)} = \frac{1}{4} \begin{bmatrix} \mathbf{A}_E & \mathbf{C}_{IB}^{\text{act(b)}} \\ \mathbf{C}_{IB}^{\text{act(b)}} & \mathbf{A}_B \end{bmatrix}, \tag{C61}$$

with $\mathbf{A}_E = (2N_E + 1)\mathbf{I}_2$, $\mathbf{A}_B = [2(G_B N_S + N_B) + 1]\mathbf{I}_2$, and

$$\mathbf{C}_{IB}^{\text{act(b)}} = \begin{bmatrix} (-1)^b C_{IB}^{\text{act}} & 0 \\ 0 & (-1)^{b+1} C_{IB}^{\text{act}} \end{bmatrix}, \tag{C62}$$

with $C_{IB}^{\text{act}} = 2\sqrt{G_B(1 - f_E \kappa_S) N_E (N_E + 1)}$, is the conditional Wigner covariance matrix of the $\{\hat{e}_{I_m}^{(1)}, \hat{a}_{B_m}\}$ mode pair given Bob's bit value. That mode pair's unconditional Wigner covariance matrix is then

$$\mathbf{\Lambda}_{IB} = \sum_{b=0}^{1} \mathbf{\Lambda}_{IB}^{(b)}/2. \tag{C63}$$

As before, the von Neumann entropies in this bound can be found in terms of thermal-state von Neumann entropies via symplectic diagonalization of the Wigner covariances.

Appendix D: Alice's Error Probabilities and Alice and Bob's Shannon Information Rates

Because $M \geq 200$ for all the performance evaluations presented in the paper, we can use the Central Limit Theorem to justify the following Gaussian-approximation formula for Alice's error probability [14] when Bob's bit value is equally likely to be 0 or 1 and Eve mounts her optimum frequency-domain collective Gaussian attack using the Fig. 2 setup:

$$\Pr(e)_{\text{Alice}}^{\text{hom}} = Q\left(\frac{\mu_0 - \mu_1}{\sigma_0 + \sigma_1} \right), \tag{D1}$$

where

$$Q(x) = \int_x^\infty \mathrm{d}t \, \frac{e^{-t^2/2}}{\sqrt{2\pi}}. \tag{D2}$$

Here, μ_b and σ_b are the conditional mean and conditional standard deviation of the $\hat{N}_{\text{hom}}$ measurement given the value of Bob's message bit, b. Once Alice's error probability is found,

Alice and Bob's Shannon-information rate follows immediately from

$$I_{AB} = R\big[1 + \Pr(e)^{\rm hom}_{\rm Alice} \log_2(\Pr(e)^{\rm hom}_{\rm Alice}) + (1 - \Pr(e)^{\rm hom}_{\rm Alice}) \log_2(1 - \Pr(e)^{\rm hom}_{\rm Alice})\big], \tag{D3}$$

hence all that remains is to determine the conditional means and standard deviations needed to instantiate our error-probability formula.

The conditional moments we require are easily calculated from the Fig. 2 setup and its associated state characterizations, so we will merely present the results. We have that

$$\mu_b = 2(-1)^b M\eta\kappa_S\sqrt{G_B N'_{\rm ASE} N_{\rm LO}}, \tag{D4}$$

and

$$\sigma_b = \sqrt{M\{\eta N_1 + 2\eta^2[N_R^{\rm Alice} N_{\rm LO} + \kappa_S^2 G_B N'_{\rm ASE} N_{\rm LO}]\}}, \tag{D5}$$

where $N'_{\rm ASE} = (1-\kappa_B)(1-f_E)(1-\kappa_A)(1-\kappa_C)N_{\rm ASE}$, $N_1 = N_R^{\rm Alice} + N_{\rm LO}$, $N_R^{\rm Alice} = \kappa_S G_B(1-\kappa_B)\kappa_S N_S + \kappa_S N_B$, and perfect reference storage has been assumed [35]. At this point we can obtain the asymptotic ($N_B \gg 1, N_{\rm LO} \gg 1$) form of $\Pr(e)^{\rm hom}_{\rm Alice}$ that was used for illustrative purposes in the paper, albeit not in the performance-evaluation figures. In this asymptotic regime we have that

$$\sigma_K \to \sqrt{2M\eta^2\kappa_S N_B N_{\rm LO}}, \tag{D6}$$

whence

$$\Pr(e)^{\rm hom}_{\rm Alice} \to Q\left(\sqrt{2M\kappa_S G_B N'_{\rm ASE}/N_B}\right). \tag{D7}$$

Neglecting the small amount of SPDC light that Alice sent to Bob, we can replace $(1-\kappa_A)(1-\kappa_C)N_{\rm ASE}$ with N_S. Using $M = TW = W/R$, and replacing $(1-\kappa_B)$ with 1 because Bob's channel monitor will withdraw only a small amount of the light he receives from Alice, we then get

$$\begin{aligned}\Pr(e)^{\rm hom}_{\rm Alice} &\to Q\Big(\sqrt{2M\kappa_S G_B(1-f_E)N_S/N_B}\Big) \\ &\le \exp(-WG_B(1-f_E)N_S/RN_B)/2,\end{aligned} \tag{D8}$$

in the $N_B \gg 1$, $N_{\rm LO} \gg 1$ regime, where we have used the well-known bound $Q(x) \le \exp(-x^2/2)/2$. In the paper, this expression was quoted for ideal equipment, which presumes unity homodyne efficiency ($\eta = 1$). The derivation we have just given verifies that in this

asymptotic regime $\Pr(e)^{\rm hom}_{\rm Alice}$ is not sensitive to the homodyne efficiency. Thus the $\eta = 0.9$ homodyne efficiency assumed in the paper is *not* a critical value.

We have now obtained upper bounds on the Holevo information rates of Eve's optimum frequency-domain collective attack, her collective passive attack, and her collective active attack, all of which are realizable with the beam-splitter arrangement shown in Fig. 2. In the paper we plot upper bounds for these attacks' Holevo informations in bits per mode, rather than bits per second. The bits per mode bounds are trivially obtained by dividing the bits per second bounds by the illumination bandwidth W, which specifies the number of modes per second that are being employed on the Alice-to-Bob and Bob-to-Alice channels.

Appendix E: Channel monitoring for general states

Alice and Bob measure the singles rates at their channel monitors, i.e., S_I for Alice's idler beam, S_A for Alice's tap on her transmitted beam, and S_B for Bob's tap on his received beam. They also measure C_{IA} and $\widetilde{C}_{IA}$, the time-aligned and time-shifted coincidence rates between Alice's idler and the tap on her transmitted beam, and C_{IB} and $\widetilde{C}_{IB}$, the time-aligned and time-shifted coincidence rates between Alice's idler and Bob's tap on his received beam, in both cases after accounting for the relevant propagation delays as described below. Their monitors will be assumed to have detectors with quantum efficiencies η_I, η_A and η_B, respectively, and identical jitter-limited coincidence-gate durations, $T_g \sim 100\,\text{ps}$. When the average number of photons illuminating each monitor in a gate time is much smaller than one—as will be the case for our performance evaluation—the average values of the preceding rates can be taken to be [36]

$$S_K = \frac{\eta_K}{T_R} \int_{-T_R/2}^{T_R/2} \mathrm{d}t \, \langle \hat{E}_K^{\rm mon\dagger}(t) \hat{E}_K^{\rm mon}(t) \rangle, \tag{E1}$$

for $K = I, A, B$, and

$$\begin{aligned} C_{IK} = \frac{\eta_I \eta_K}{T_R} & \int_{-T_R/2}^{T_R/2} \mathrm{d}t \int_{t-T_g/2}^{t+T_g/2} \mathrm{d}u \\ & \times \langle \hat{E}_I^{\rm mon\dagger}(t) \hat{E}_I^{\rm mon}(t) \hat{E}_K^{\rm mon\dagger}(u) \hat{E}_K^{\rm mon}(u) \rangle, \end{aligned} \tag{E2}$$

$$\begin{aligned} \widetilde{C}_{IK} = \frac{\eta_I \eta_K}{T_R} & \int_{-T_R/2}^{T_R/2} \mathrm{d}t \int_{t+T_s-T_g/2}^{t+T_s+T_g/2} \mathrm{d}u \\ & \times \langle \hat{E}_I^{\rm mon\dagger}(t) \hat{E}_I^{\rm mon}(t) \hat{E}_K^{\rm mon\dagger}(u) \hat{E}_K^{\rm mon}(u) \rangle, \end{aligned} \tag{E3}$$

for $K = A, B$, where $\hat{E}_K^{\rm mon}(t)$, for $K = I, A, B$, are the positive-frequency, $\sqrt{\text{photons/s}}$-units field operators entering Alice's idler and transmitter tap monitors and Bob's monitor, respectively. Here, the time-origins for the $\{\hat{E}_K^{\rm mon}(t)\}$ have been chosen to ensure that true coincidences *and* accidental coincidences will be counted in the time-aligned coincidences C_{IK}, but *only* accidental coincidences will be counted in the time-shifted coincidences $\widetilde{C}_{IK}$. The latter condition is ensured by taking the time shift T_s to satisfy $WT_s \gg 1$, $T_s \gg T_g$, and $T_s \ll T_R$, where W is Alice's source bandwidth and $t \in [-T_R/2, T_R/2]$ is the duration of the FL-QKD protocol's quantum communication. In practice, $T_s \sim 10\,\text{ns}$ will suffice for $W = 2\,\text{THz}$ and $T_g = 100\,\text{ps}$.

If we assume that Eve mounts a collective frequency-domain Gaussian attack, then all of the fields appearing in our singles and coincidence rates are in a zero-mean, jointly-Gaussian state and we can evaluate these rates by means of Gaussian moment factoring [37]. However, because we seek security against the general frequency-domain collective attack, we will show that Alice and Bob's channel monitors can determine Eve's intrusion parameter, f_E, even when her attack in *not* Gaussian. Toward that end it is convenient to introduce Fourier-series decompositions for the field operators $\{\, \hat{E}_K^{\rm mon}(t) : K = I, A, B \,\}$ over the entire duration of FL-QKD's quantum communication, viz.,

$$\hat{E}_I^{\rm mon}(t) = \frac{e^{-i\omega_I t}}{\sqrt{T_R}} \sum_{m=-WT_R/2}^{WT_R/2} \hat{a}_{I_m}^{\rm mon} e^{-i2\pi m t/T_R}, \tag{E4}$$

$$\hat{E}_K^{\rm mon}(t) = \frac{e^{-i\omega_S t}}{\sqrt{T_R}} \sum_{m=-WT_R/2}^{WT_R/2} \hat{a}_{K_m}^{\rm mon} e^{i2\pi m t/T_R}, \tag{E5}$$

for $K = A, B$, where ω_S and ω_I are the center frequencies of Alice's signal and idler beams and we have limited the series to Alice's source bandwidth, i.e., to the frequency modes that are in non-vacuum states. The behaviors of the modes appearing in these Fourier series can be gotten from App. A by presuming that the Fourier expansions in that appendix were made on the $[-T_R/2, T_R/2]$ interval and making the following identifications:

$$\hat{a}_{I_m}^{\rm mon} = \hat{a}_{I_m} \tag{E6}$$

$$\hat{a}_{A_m}^{\rm mon} = \sqrt{\kappa_A}\, \hat{a}_{A_m} - \sqrt{1-\kappa_A}\, \hat{v}_{A_m} \tag{E7}$$

$$\hat{a}_{B_m}^{\rm mon} = \sqrt{\kappa_B}\, \hat{a}'_{S_m} - \sqrt{1-\kappa_B}\, \hat{v}_{B_m}. \tag{E8}$$

Note that Eve's mounting a frequency-domain collective attack makes the mode triples

$\{\,(\hat{a}^{\rm mon}_{I_m}, \hat{a}^{\rm mon}_{A_m}, \hat{a}^{\rm mon}_{B_m}) \,:\, -WT_R/2 \,\leq\, m \,\leq\, WT_R/2\,\}$ independent and identically distributed with the $\{\hat{a}_{I_m}\}$ modes being in zero-mean states.

For the singles rates we find that

$$\begin{aligned} S_K \;&=\; \frac{\eta_K}{T_R} \sum_{n=-WT_R/2}^{WT_R/2} \sum_{m=-WT_R/2}^{WT_R/2} \langle \hat{a}^{\rm mon\dagger}_{K_n} \hat{a}^{\rm mon}_{K_m} \rangle \\ &\times\; \frac{\sin[\pi(n-m)]}{\pi(n-m)} \qquad \text{(E9)} \\ &=\; \frac{\eta_K}{T_R} \sum_{n=-WT_R/2}^{WT_R/2} \langle \hat{a}^{\rm mon\dagger}_{K_n} \hat{a}^{\rm mon}_{K_n} \rangle \qquad \text{(E10)} \\ &=\; \eta_K W \langle \hat{a}^{\rm mon\dagger}_{K_n} \hat{a}^{\rm mon}_{K_n} \rangle, \qquad \text{(E11)} \end{aligned}$$

for $K = I, A, B$. Using this result in conjunction with Eqs. (E6)–(E8) then gives us

$$S_I = \eta_I N_{\rm SPDC} W, \qquad \text{(E12)}$$

$$S_A = \eta_A \kappa_A N_A W, \qquad \text{(E13)}$$

$$S_B = \eta_B \kappa_B \kappa_S N_S W. \qquad \text{(E14)}$$

Finding the time-aligned and time-shifted coincidence rates is more complicated than what we have just done for the singles rates. We start from the photon-flux cross-correlation function,

$$R_{IK}(t,u) = \langle \hat{E}^{\rm mon\dagger}_I(t) \hat{E}^{\rm mon}_I(t) \hat{E}^{\rm mon\dagger}_K(u) \hat{E}^{\rm mon}_K(u) \rangle, \qquad \text{(E15)}$$

for $K = A, B$, which, employing the Fourier series given earlier and grouping terms, can be reduced to

$$R_{IK}(t,u) = \sum_{k=1}^{3} R^{(k)}_{IK}(t,u), \qquad \text{(E16)}$$

where

$$\begin{aligned} R^{(1)}_{IK}(t,u) \;&=\; \frac{1}{T_R^2} \Bigg[\sum_{n,m} \langle \hat{a}^{\rm mon\dagger}_{I_n} \hat{a}^{\rm mon\dagger}_{K_n} \rangle \langle \hat{a}^{\rm mon}_{I_m} \hat{a}^{\rm mon}_{K_m} \rangle \\ &\times\; e^{i2\pi(n-m)(t-u)/T_R} \Big] , \qquad \text{(E17)} \\ R^{(2)}_{IK} &= \frac{1}{T_R^2} \Bigg[\sum_{n,m} \langle \hat{a}^{\rm mon\dagger}_{I_n} \hat{a}^{\rm mon}_{I_n} \rangle \langle \hat{a}^{\rm mon\dagger}_{K_m} \hat{a}^{\rm mon}_{K_m} \rangle \Bigg] , \qquad \text{(E18)} \end{aligned}$$

and

$$R^{(3)}_{IK}(t,u) = \frac{1}{T_R^2}\Bigg\{\sum_n \Big[\langle \hat{a}^{\rm mon\dagger}_{I_n}\hat{a}^{\rm mon\dagger}_{K_n}\hat{a}^{\rm mon}_{I_n}\hat{a}^{\rm mon}_{K_n}\rangle - |\langle \hat{a}^{\rm mon}_{I_n}\hat{a}^{\rm mon}_{K_n}\rangle|^2 - \langle \hat{a}^{\rm mon\dagger}_{I_n}\hat{a}^{\rm mon}_{I_n}\rangle\langle \hat{a}^{\rm mon\dagger}_{K_n}\hat{a}^{\rm mon}_{K_n}\rangle\Big]\Bigg\}, \tag{E19}$$

because of the independence of the mode triples and the zero-mean nature of the $\{\hat{a}^{\rm mon}_{I_m}\}$ modes, with all indices are summed from $-WT_R/2$ to $WT_R/2$.

The time-independence of $R^{(2)}_{IK}(t,u)$ and $R^{(3)}_{IK}(t,u)$ implies that these terms will not contribute to $C_{IK} - \widetilde{C}_{IK}$. Moreover the independence and identical distribution of the mode pairs $\{\hat{a}^{\rm mon}_{I_m}, \hat{a}^{\rm mon}_{A_m}\hat{a}^{\rm mon}_{B_m}\}$ makes $R^{(1)}_{IK})(t,u)$ vanish when $|t-u| \gg 1/W$. Hence we find that

$$\begin{aligned} C_{IK} - \widetilde{C}_{IK} &= \frac{\eta_I\eta_K}{T_R}|\langle \hat{a}^{\rm mon}_{I_m}\hat{a}^{\rm mon}_{K_m}\rangle|^2 \\ &\quad\times \sum_{n,m}\frac{T_g}{T_R}\frac{\sin[\pi(n-m)T_g/T_R]}{\pi(n-m)T_g/T_R}. \end{aligned} \tag{E20}$$

In the main text we claimed that Alice and Bob's channel monitors will enable them to measure Eve's intrusion parameter,

$$f_E \equiv 1 - \frac{|\langle \hat{a}'_{S_m}\hat{a}_{I_m}\rangle|^2}{\kappa_S|\langle \hat{a}_{S_m}\hat{a}_{I_m}\rangle|^2}, \tag{E21}$$

via

$$f_E = 1 - \frac{[C_{IB} - \widetilde{C}_{IB}]/S_B}{[C_{IA} - \widetilde{C}_{IA}]/S_A}. \tag{E22}$$

Using Eqs. (E13), (E14), and (E20) we get

$$\frac{[C_{IB} - \widetilde{C}_{IB}]/S_B}{[C_{IA} - \widetilde{C}_{IA}]/S_A} = \frac{|\langle \hat{a}^{\rm mon}_{I_m}\hat{a}^{\rm mon}_{B_m}\rangle|^2}{|\langle \hat{a}^{\rm mon}_{I_m}\hat{a}^{\rm mon}_{A_m}\rangle|^2}\frac{\langle \hat{a}^{\rm mon\dagger}_{A_m}\hat{a}^{\rm mon}_{A_m}\rangle}{\langle \hat{a}^{\rm mon\dagger}_{B_m}\hat{a}^{\rm mon}_{B_m}\rangle}. \tag{E23}$$

From Eqs. (E6)–(E8) we can reduce this result to

$$\frac{[C_{IB} - \widetilde{C}_{IB}]/S_B}{[C_{IA} - \widetilde{C}_{IA}]/S_A} = \frac{|\langle \hat{a}_{I_m}\hat{a}'_{S_m}\rangle|^2}{|\langle \hat{a}_{I_m}\hat{a}_{A_m}\rangle|^2}\frac{\langle \hat{a}^\dagger_{A_m}\hat{a}_{A_m}\rangle}{\langle \hat{a}'^\dagger_{S_m}\hat{a}'_{S_m}\rangle}. \tag{E24}$$

Use of Eqs. (A5) and (C2) then yields

$$\frac{[C_{IB} - \widetilde{C}_{IB}]/S_B}{[C_{IA} - \widetilde{C}_{IA}]/S_A} = \frac{|\langle \hat{a}'_{S_m}\hat{a}_{I_m}\rangle|^2}{\kappa_S|\langle \hat{a}_{S_m}\hat{a}_{I_m}\rangle|^2}. \tag{E25}$$

Although this result appears to verify the agreement of Eqs. (E21) and (E22), there is an issue with that identification. The modes appearing in Eq. (E21) were obtained from Fourier-series decompositions of the relevant continuous-time field operators on a duration-$1/R$ s interval, whereas those in Eq. (E25) come from Fourier-series decompositions of those field operators on a duration-T_R s interval. Because of the independent, identical distribution of the mode operators, however, their second moments—which are all that appears in Eqs. (E21) and (E22)—will be the same regardless of whether the Fourier series' time interval has duration $1/R$ or T_R.

Appendix F: Eve's Entanglement-Assisted Capacity

When Eve mounts a collective active attack, we can regard her use of the SPDC's idler beam she has retained and the modulated, amplified, noisy version of her SPDC's signal beam she collects from her tap on the Bob-to-Alice fiber as an entanglement-assisted communication channel from Bob to her. Consequently, her collective active attack's Holevo information per mode cannot exceed the single-mode entanglement-assisted capacity for that channel, C_E [38, 39], because entanglement-assisted capacity is known to be additive. From [38, 39] we have that

$$\begin{aligned} C_E \;=\; & g[(1-\kappa_B)[1-(1-f_E)\kappa_S]N_E] \\ & +\; g[G_B(1-\kappa_B)[1-(1-f_E)\kappa_S]N_E + N_B] \\ & -\; g[(1+(1-\kappa_B)[1-(1-f_E)\kappa_S]N_E N_B]. \end{aligned} \tag{F1}$$

We have been somewhat conservative in Eq. (F1) in that this result assumes that Alice does not inject any light into Bob and that Eve collects all the light that Bob sends on the Bob-to-Alice fiber. Neither of these assumptions is of great consequence, but they make it easier to obtain the result in Eq. (F1). In particular, Alice's injection into Bob acts as noise for Eve's active attack. Moreover, because Alice's injection into Bob has low brightness, it is dwarfed by the ASE from Bob's amplifier. Finally, because Fig. 4(b) plots C_E for a 50-km-long path, Eve is already getting 90% of the light Bob sends to Alice. Hence increasing that value to 100% is not a major change, especially since Bob's amplifier gain is sufficient to overcome return-path loss.

Appendix G: Bounding Eve's information gain from knowing the output of Bob's channel monitor

Bob sends Alice the times at which his channel monitor has detected photons so that she can use that data to estimate Eve's intrusion parameter. To do so he uses a tamper-proof classical channel that Eve can monitor. So far, we have not included the information that Eve could glean from that classical transmission in bounding her Holevo information rate. Here we will show that the extra information that Eve might gain from knowing those detection times is inconsequential.

The mean photon-number per bit at Bob's monitor detector is $M\kappa_B\kappa_S N_S \simeq \kappa_B \ll 1$, owing to FL-QKD's operating with $M\kappa_S N_S \sim 1$ ($\sim$1 ppb at Bob's terminal), we will only consider two leading-order possibilities: no photon is detected (probability of occurrence = p_0) or one photon is detected (probability of occurrence = $p_1 = 1 - p_0$).

Let us use $\chi^{\rm UB}_{EB|n}$, for $n = 0, 1$, to denote an upper bound on Eve's Holevo information rate given that Bob's monitor has detected n photons *and*, if there has been a detection, that Eve knows from which frequency mode it came. (This frequency-mode knowledge is not available to Eve from her eavesdropping on Bob's classical-channel transmission, so assuming she has this knowledge increases her Holevo information rate.) Then, averaged over Bob's monitor result, the upper bound on Eve's Holevo information rate for her optimum frequency-domain collective attack is

$$\bar{\chi}^{\rm UB}_{EB} = p_0\chi^{\rm UB}_{EB|0} + p_1\chi^{\rm UB}_{EB|1}. \tag{G1}$$

Because all M modes are independent, we have that $\chi^{\rm UB}_{EB|0} = M\chi_0$, where χ_0 is the per-mode upper bound on Eve's Holevo information rate when Bob's monitor failed to detect a photon [40]. When Bob's monitor does detect a photon, and Eve knows which frequency mode has lost a photon to that detection, the upper bound on her conditional Holevo information rate will be

$$\chi^{\rm UB}_{EB|1} = (M-1)\chi_0 + \chi_1, \tag{G2}$$

where χ_1 is the per-mode upper bound when Bob's monitor detected a photon in that mode. We now have that

$$\bar{\chi}^{\rm UB}_{EB} = M\chi_0 + p_1(\chi_1 - \chi_0), \tag{G3}$$

which we need to compare to our upper bound from App. C, which neglected any information Eve might gain from learning the times at which Bob's channel monitor made photon

detections.

For $\chi_{EB}^{\rm UB}$ being the App. C upper bound we will use $\chi \equiv \chi_{EB}^{UB}/M$,to denote its per-mode contribution. We now have that

$$\frac{\bar{\chi}_{EB}^{\rm UB}}{\chi_{EB}^{\rm UB}} = \frac{\chi_0}{\chi} + p_1 \frac{(\chi_1 - \chi_0)}{M\chi}. \tag{G4}$$

Figure 4(a) shows that Bob will receive $\sim$1 ppb for one-way path lengths less than 200 km, and our secret-key rate calculations assume that Bob's monitor taps 1% of that light. Together these conditions imply that $p_1 \approx 0.01$. Figure 4(a) also implies that $M\chi \approx 0.8$ for a 50 km one-way path length. So, taking the *very* conservative upper limit of unity for $\chi_1 - \chi_0$, we have that the second term on the right in Eq. (G4) is at most 0.013. Thus it only remains for us to address the first term on the right in that equation. We will do so within the App. C.2 framework, i.e., for Eve' frequency-domain collective Gaussian attack.

Eve gains her information from measuring the mode triples $\{\hat{e}_{I_m}^{(1)}, \hat{e}_{I_m}^{(2)}, \hat{a}_{B_m}\}$. To assess the impact of Eve's having Bob's channel-monitor data, we focus our attention on what that data implies about conditional state of the $\{\hat{a}''_{S_m}\}$ modes, viz., the modes that enter Bob's BSPK modulator and, after modulation and subsequent amplification, become the $\{\hat{a}_{B_m}\}$ modes. Moreover, to do so we will presume that the $\{\hat{a}'_{S_m}\}$ modes that arrive at Bob's terminal are in independent, identically-distributed thermal states with average photon number $\kappa_S N_S$, as is the case in Eve's optimum frequency-domain Gaussian collective attack. Using the beam-splitter relation that converts these modes and the vacuum-state $\{\hat{v}_{B_m}\}$ modes into the $\{\hat{a}_{B_m}^{\rm mon}, \hat{a}''_{S_m}\}$ mode pairs, we find that those mode pairs are in independent, identically-distributed Gaussian states whose coherent-state decomposition is

$$\begin{aligned} \hat{\rho}_{\hat{a}_{B_m}^{\rm mon}, \hat{a}''_{S_m}} &= \int \frac{{\rm d}^2\alpha}{\pi\kappa_S N_S} e^{-|\alpha|^2/\kappa_S N_S} \, |\sqrt{\kappa_B}\,\alpha\rangle_{BB}\langle\sqrt{\kappa_B}\,\alpha| \\ &\quad \otimes \, |\sqrt{1-\kappa_B}\,\alpha\rangle_{SS}\langle\sqrt{1-\kappa_B}\,\alpha| \, . \end{aligned} \tag{G5}$$

Given that Bob's monitor did not detect a photon, the $\{\hat{a}''_{S_m}\}$ modes are still independent and identically distributed, with conditional density operator

$$\hat{\rho}_{\hat{a}''_{S_m}|0} = \frac{{}_B\langle 0|\, \hat{\rho}_{\hat{a}_{B_m}^{\rm mon}, \hat{a}''_{S_m}} \, |0\rangle_B}{{\rm Tr}\Big({}_B\langle 0|\, \hat{\rho}_{\hat{a}_{B_m}^{\rm mon}, \hat{a}''_{S_m}} \, |0\rangle_B \Big)}. \tag{G6}$$

After some algebra, we have the $\hat{\rho}_{\hat{a}''_{S_m}|0}$ is a thermal state whose mean photon number, $(1-\kappa_B)\kappa_S N_S/(1+\kappa_B\kappa_S N_S)$, is less than that mode's unconditional photon number, $(1-$

$\kappa_B)\kappa_S N_S$. Thus we conclude conditioning on Bob getting no count, the mean photon number in the return mode decreases, but the quantum state is still Gaussian. Similar results hold for Eve's $\{\hat{e}_{I_m}^{(1)}, \hat{e}_{I_m}^{(2)}\}$ modes, and we conclude that $\chi_0/\chi < 1$, hence $\bar{\chi}_{EB}^{\mathrm{UB}}/\chi_{EB}^{\mathrm{UB}} < 1.013$ at 50 km one-way path length.

---

[1] C. E. Shannon, Bell Syst. Tech. J. **28,** 656-715 (1949).

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing,"Proc. IEEE International Conf. on Computers, Systems, and Signal Processing, Bangalaore, pp. 175–179 (1984).

[3] A. K. Ekert, Phys. Rev. Lett. **67,** 661–663 (1991).

[4] N. Gisin, G. G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74,** 145–195 (2002).

[5] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88,** 057902 (2002).

[6] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Frölich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, Opt. Express **21,** 24550–24565 (2013).

[7] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, Opt. Express **23,** 17511–17519 (2015).

[8] A passive attack therefore has $f_E = 0$ while an active attack has $f_E > 0$.

[9] M. Navascués and A. Acín, Phys. Rev. Lett. **94,** 020505 (2005).

[10] Z. Zhang, J. Mower, D. Englund, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. Lett. **112,** 120506 (2014).

[11] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook. S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nature Photon. **9,** 397–402 (2015).

[12] See App. D for details.

[13] J. H. Shapiro, Phys. Rev. A **80,** 022320 (2009).

[14] Z. Zhang, M. Tengner, T. Zhong, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. Lett. **111,** 010501 (2013).

[15] S. Pirandola and S. Lloyd, Phys. Rev. A **78,** 012331 (2008).

[16] See App. C for details.

[17] T. J. Richardson, A. Shokrollah, and R. L. Urbanke, IEEE Trans. Inform. Theory **47,** 619–637 (2001).

[18] Bob's receiving ∼1 ppb keeps $\Pr(e)^{\rm hom}_{\rm Alice} = 0.1$ when his amplifier's gain is sufficient to make return-path loss inconsequential. The increase in Bob's received ppb seen in Fig. 4(a) as the path length decreases from 50 km is due to our $R \leq 10$ Gbps constraint, which leads to $\Pr(e)^{\rm hom}_{\rm Alice}$ appreciably lower than 0.1 at such short distances when Alice and Bob optimize their secret-key rate. On the other hand, the increase in Bob's received ppb as the path length increases beyond 150 km occurs because $G_B = 10^4$ is becoming insufficient to overcome return-path loss at these distances, so that Bob must receive more ppb to ensure $\Pr(e)^{\rm hom}_{\rm Alice} \leq 0.1$.

[19] See Apps. C.2 and F for details.

[20] See App. C.2 for details.

[21] It follows from Eve's passive-attack Holevo information rate versus Alice's signal brightness, shown in Fig. 4(b), and Alice source brightness versus path length, shown in Fig. 3(a), that Alice and Bob can realize a 2 Gbps secret-key rate over a 50-km-long fiber link with complete immunity to the undetectable passive-eavesdropping attack. In this regard we note that because a passive eavesdropper does *not* interact with the light going to Bob, the collective passive-eavesdropping attack is its most powerful form, i.e., there is no coherent passive-eavesdropping attack.

[22] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102,** 180504 (2009).

[23] A. Leverrier and P. Grangier, Phys. Rev. A **83,** 042312 (2011).

[24] A. Leverrier and P. Grangier, Phys. Rev. Lett. **106,** 259902(E) (2011).

[25] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, arXiv:1510.08863 [quant-ph].

[26] Pirandola *et al.* [25] quote this limit in bits per channel use, but their channel uses are implicitly single mode.

[27] J. Mower, Z. Zhang, P. Desjardins, C. Lee, J. H. Shapiro, and D. Englund, Phys. Rev. A **87,** 062322 (2013).

[28] The strong ASE contributed by Bob's amplifier to the light he returns to Alice provides the dominant noise in Alice's homodyne receiver, see App. D.

[29] This threshold value minimizes Alice's error probability.

[30] If κ_I is so small that amplifiers with gain $G_R = 1/\kappa_I$ are unavailable, then the fiber spool can be divided into a series connection of shorter-length spools—that together provide the required overall delay–with a loss-compensating amplifier employed at the input to each of them. Such an arrangement can achieve the same goal of near-perfect reference storage.

[31] R. Ahlswede and P. Lober, IEEE Trans. Inform. Theory **47,**, 474-478 (2001).

[32] M. M. Wolf, G. Giedke, and J. I. Cirac, Phys. Rev. Lett. **96,** 080502 (2006).

[33] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84,** 621–669 (2012).

[34] Q. Zhuang, Z. Zhang, and J. H. Shapiro, in preparation.

[35] Because $\sigma_0 = \sigma_1$, Alice's setting her homodyne receiver's decision threshold to $(\mu_0 + \mu_1)/2 = 0$ minimizes $\Pr(e)^{\text{hom}}_{\text{Alice}}$, and does so with equal false-alarm and miss probabilities.

[36] J. H. Shapiro, IEEE J. Sel. Top. Quantum Electron. **15,** 1547 (2009).

[37] J. H. Shapiro, J. Opt. Soc. Am. B **11,** 1130 (1994).

[38] A. S. Holevo and R. F. Werner, Phys. Rev. A **63,** 032312 (2001).

[39] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, IEEE Trans. Inform. Theory **48,**, 2637-2655 (2002).

[40] Here, and in the rest of App. G, we shall ignore the upper limit of R bps on Eve's Holevo information rate.