This is the accepted manuscript made available via CHORUS. The article has been published as:

Security-proof framework for two-way Gaussian quantum-key-distribution protocols

Quntao Zhuang, Zheshen Zhang, Norbert Lütkenhaus, and Jeffrey H. Shapiro

Phys. Rev. A **98**, 032332 — Published 28 September 2018

DOI: 10.1103/PhysRevA.98.032332

Security proof framework for two-way Gaussian quantum key distribution protocols

Quntao Zhuang[1,2],* Zheshen Zhang[1,3], Norbert Lütkenhaus[4,5], and Jeffrey H. Shapiro[1]
[1] *Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*
[2] *Department of Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*
[3] *Department of Materials Science and Engineering, University of Arizona, Tucson, Arizona 85721, USA*
[4] *Perimeter Institute for Theoretical Physics, 31 Caroline St N, Waterloo, Ontario N2L 2Y5, Canada*
[5] *Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada*
(Dated: August 8, 2018)

Two-way Gaussian protocols have the potential to increase quantum key distribution (QKD) protocols' secret-key rates by orders of magnitudes [Phys. Rev. A **94**, 012322 (2016)]. Security proofs for two-way protocols, however, are underdeveloped at present. In this paper, we establish a security proof framework for the general coherent attack on two-way Gaussian protocols in the asymptotic regime. We first prove that coherent-attack security can be reduced to collective-attack security for all two-way QKD protocols. Next, we identify two different constraints that each provide intrusion parameters which bound an eavesdropper's coherent-attack information gain for any two-way Gaussian QKD protocol. Finally, we apply our results to two such protocols.

I. INTRODUCTION

The continuing improvement of classical computational power [1] and the emergence of quantum computers [2–4], are increasing the likelihood that complexity-based classical cryptographic algorithms—such as Rivest-Shamir-Adleman encryption [5] and elliptic-curve cryptography [6, 7]—will be broken. Two distinct approaches have emerged for countering this vulnerability: post-quantum cryptography [8], which seeks new public-key cryptography algorithms that are immune to the threat posed by a quantum computer running Shor's algorithm [9]; and quantum key distribution [10] (QKD), which provides protocol security based on physical laws rather than computational complexity.

In QKD, Alice and Bob establish a raw key by quantum-channel transmission and detection of photons. They use security testing and classical communication to quantify Eve's intrusion on the quantum channel. With these intrusion parameters they can place an upper bound on Eve's information gain. Then, they complete the QKD protocol by reconciling their raw keys, to eliminate errors, and distilling a final key via privacy amplification, to ensure its unconditional protocol security.

QKD's principal advantage is its provable protocol security. Its ultimate benefit would be enabling Alice and Bob to transmit messages using one-time-pad encryption, which would afford them information-theoretic security for their communications. QKD systems using the decoy-state BB84 or conventional continuous-variable (CV) protocols, however, have state-of-the-art secret key rates (SKRs) [11–13] of $\sim$1 Mbit/s at metropolitan-area distances, which is far below the Gbit/s rates needed for Internet-speed secure communications. These systems' SKRs could be pushed to Gbit/s with massive combinations of space-division and wavelength-division multiplexing, but that approach comes with a major equipment burden in cost and complexity. Recently, floodlight QKD (FL-QKD) [14–17] has been proposed as a means to realize Gbit/s SKRs at metropolitan-area distances over single-mode fiber (no space-division multiplexing), in a single-wavelength channel (no wavelength-division multiplexing), and without the need to develop any new technology. It does so by encoding each transmitted symbol over multiple temporal modes, whereas decoy-state BB84 makes no use of multimode encoding and conventional CV-QKD requires single-mode encoding. As a result, FL-QKD's SKR is less constrained by the PLOB bound [18, 19], which sets the ultimate limit on secret bits per mode, than those protocols. That said, decoy-state BB84 and conventional CV-QKD have the advantage of being one-way (OW) protocols, whereas FL-QKD is a two-way (TW) protocol, so that the former have much stronger security guarantees—e.g., decoy-state BB84 has coherent-attack security with finite-key analysis—while the latter's security to date is only against the frequency-domain collective attack in the asymptotic regime [14]. On the other hand, unlike other TW-QKD protocols [21–29], FL-QKD uses an optical amplifier in Bob's terminal to overcome the Bob-to-Alice channel's loss, making FL-QKD's channel loss equivalent to that of OW-QKD protocols.

The limited nature of FL-QKD's security proof is characteristic of the situation for other TW-QKD protocol's [14–17, 21–29]. In part, this is because proof techniques for OW-QKD [30–34] do not readily cope with simultaneous attacks on both the Alice-to-Bob and Bob-to-Alice channels of a TW-QKD protocol. Thus, for a long time only special attacks [21, 24–26, 28, 29, 35], or general attacks in the absence of loss and/or noise [22, 23, 27], have been considered for TW-QKD.

At this point it should be clear that a coherent-

* zhuangquntao@gmail.com

attack security proof, with finite-key analysis [36], for FL-QKD would be an enormous step toward its widespread employment, given that protocol's potential for Gbit/s SKRs. More generally, such security proofs for other TW-QKD protocols could also be valuable. In this paper, we take a first step in that direction by establishing TW-QKD's coherent-attack security in the asymptotic regime wherein there are an infinite number of channel uses. Because we want to include protocols like FL-QKD that encode over multiple modes, we cannot entirely rely on raw-key post-processing by Alice and Bob that permutes or otherwise independently manipulates measurements made on individual optical modes. Moreover, at high modulation rates, manipulation of each encoded symbol is difficult, even if single-mode encoding is employed. Hence, de Finetti theorem arguments [32, 33] are not directly applicable for the reduction from coherent attack to collective attack on a mode-by-mode basis; Instead, it reduces the general coherent attack to a block-wise coherent attack, in which Eve performs the same but arbitrary operations on blocks of modes that may comprise one or more symbols, i.e., one or more of Alice and Bob's channel uses.

The asymptotic SKR for the block-wise coherent attack is given by the block-wise Devetak-Winter formula [37, 38], which reduces the problem to bounding the information leaked to Eve during the raw-key generation process, as constrained by intrusion-parameter estimates made by Alice and Bob using local operations and classical communication (LOCC) [39]. Note that in a block-wise coherent attack [36], Eve can entangle signals sent in different channel uses within a block, which makes bounding Eve's information gain a difficult multi-letter maximization involving Eve's operations over multiple channel uses. A crucial task for us is therefore reducing the maximization to a single-letter (single channel-use) form from which computing an upper bound on Eve's information gain is tractable.

We will use the recently developed noisy-entanglement-assisted classical capacity formula [14, 40] to resolve the preceding single-letterization dilemma for Gaussian TW-QKD protocols, i.e., protocols that employ Gaussian-state sources and Gaussian operations [41]. We consider two different constraints—the pair-wise sum constraints and the permutation-invariant sum constraints—that provide intrusion parameters which suffice to establish tractable (single-letter) upper bounds on Eve's coherent-attack information gain.

The remainder of the paper is organized as follows. In Sec. II, we introduce Gaussian TW-QKD protocols. In Sec. III, we prove that the capacity formula in Ref. [40] provides an upper bound on Eve's information gain from her most general coherent attack. There, we also describe the pair-wise sum constraints and permutation-invariant sum constraints that lead to efficiently calculable bounds on Eve's coherent-attack information gain, and we show that the resulting upper bound can be achieved by a collective attack. In Sec. IV, we evaluate the secret-key efficiencies (in bits/symbol) of two Gaussian TW-QKD protocols: the two-mode squeezed-vacuum (TMSV) protocol from Refs. [21, 26, 28, 29] and FL-QKD. We conclude, in Sec. V, with a summary and some discussion.

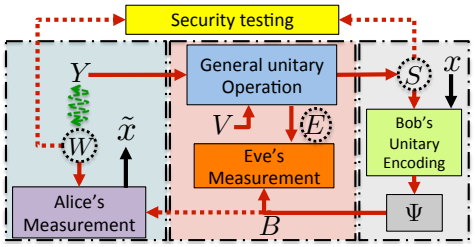

FIG. 1. General schematic for a Gaussian TW-QKD protocol.

II. GAUSSIAN TWO-WAY PROTOCOLS

Figure 1 shows a general schematic for how a Gaussian TW-QKD protocol generates raw key [42]. First, Alice prepares a signal-reference mode pair (Y, W) in a maximally entangled bipartite Gaussian pure state, i.e., the two-mode squeezed vacuum (TMSV), with average photon number N_S and Wigner covariance matrix

$$\mathbf{\Lambda}_{YW} = \frac{1}{4}\begin{bmatrix} \mathbf{A}_Y & \mathbf{C}_{YW} \\ \mathbf{C}_{YW} & \mathbf{A}_W \end{bmatrix}, \tag{1}$$

where $\mathbf{A}_Y = \mathbf{A}_W = (2N_S+1)\mathbf{I}_2$, and $\mathbf{C}_{YW} = 2C_S\,\mathbf{Z}_2$, with $\mathbf{I}_2 = \mathrm{Diag}[1,1]$, $\mathbf{Z}_2 = \mathrm{Diag}[1,-1]$, and $C_S = \sqrt{N_S(N_S+1)}$. As explained below, Alice will use part of W for security testing [43], but Eve is unable to access any of W. Next, Alice sends Y to Bob through a quantum channel that Eve controls. In general, Eve performs a unitary operation on Y and some pure-state modes V of her own, producing her ancilla E, which can be multi-mode, and the single-mode signal S that she transmits to Bob. Because Eve can mount a coherent attack, her unitary operation can act on the entire sequence of signals that Alice transmits during a QKD session.

Bob takes a small portion of the S mode he receives from Eve and uses it for security testing. After that, he encodes a random symbol X on the remainder of the S mode to produce his encoded mode S'. He does so, when $X = x$, by means of a unitary U_x that imparts a deterministic, complex-valued displacement d_x, and a deterministic phase shift θ_x. The S' mode's photon annihilation operator is therefore $\hat{a}'_S = e^{i\theta_X}\hat{a}_S + d_X$, where $\hat{a}_S$ is the S mode's annihilation operator, and we have not accounted for the small portion of S that is consumed by Bob's security testing.

We will assume that d_X is a zero-mean, circulo-complex, Gaussian random variable. Thus, if no phase encoding is applied, then S' will be in a thermal state with average photon number

$$\langle \hat{a}'^{\dagger}_S \hat{a}'_S \rangle = \int \mathrm{d}x\, p_X(x)\, \langle \hat{a}'^{\dagger}_S \hat{a}'_S \rangle_x = \langle \hat{a}^{\dagger}_S \hat{a}_S \rangle + E_X, \tag{2}$$

where $\langle\cdot\rangle_x$ denotes averaging conditioned on $X = x$, and $E_X \equiv \int \mathrm{d}x\, p_X(x)|d_x|^2$ with $p_X(x)$ being X's probability density function. Our security analysis will presume encoding symmetry, i.e., that the S' mode's unconditional state has zero mean, which is guaranteed by assuming that $\int \mathrm{d}x\, p_X(x) e^{i\theta_x} = 0$. Note that the S' mode's average photon number is unaffected by the phase shift θ_X, making Eq. (2) applicable when Bob encodes in both displacement and phase.

The preceding encoding scheme, while not the most general, includes the random-displacement encoding employed in Ref. [21], and the phase encoding used in FL-QKD [14–17]. Here we note that the average state of (S', W) is, in general, non-Gaussian owing to the action of Eve's unitary operation and/or Bob's phase modulation.

After completing his encoding, Bob sends S' through a quantum channel, Ψ, within his terminal that models the characterizable part of the Bob-to-Alice return path that is not controlled by Eve. This channel produces an output mode B that Bob sends to Alice through a quantum channel that is under Eve's control. Alice makes a joint measurement of the mode she receives and W to obtain her raw-key symbol $\tilde{x}$ that results from Bob's having sent x, with the nature of Alice's measurement depending on Bob's choice of his encoding operation U_X. Alice and Bob also perform security testing, which is an LOCC parameter-estimation scheme based on Alice's measuring part of W and Bob's measuring part of S. That scheme allows them to evaluate some bipartite functions of the joint state ρ_{SW} that constitute intrusion parameters which they use to compute an upper bound on Eve's information gain.

Alice and Bob distill their secret key by the following two-step procedure. Starting from his transmitted-symbol sequence and Alice's raw-key sequence, Bob performs the key-map operation [36, 44] and sends error-correction information to Alice on an authenticated classical channel. At that point, Alice and Bob share a common key, but its security is not assured because of the information Eve has gained. Thus they use their upper bound on Eve's information gain to determine and perform a sufficient amount of privacy amplification to ensure their final key's security.

To complete our explanation of Fig. 1, we conclude this section with some remarks about Ψ, the quantum channel within Bob's terminal. For single-mode encoding, we take Ψ to be a single-mode Gaussian channel with no excess noise, which can be represented as a unitary operation on the encoded signal mode S' and a vacuum-state environment mode N that produces the return mode B and a transformed environment mode N'. If multi-mode encoding over $M_E > 1$ modes is employed, the channel internal to Bob's terminal is $\Psi^{\otimes M_E}$, which applies, e.g., to FL-QKD with Ψ being a quantum-limited amplifier channel, $\mathcal{A}^0_{G_B}$, whose output modes B and N' are characterized by $\hat{a}_B = \sqrt{G_B}\,\hat{a}'_S + \sqrt{G_B - 1}\,\hat{a}^\dagger_N$, and $\hat{a}'_N = \sqrt{G_B - 1}\,\hat{a}'^\dagger_S + \sqrt{G_B}\,\hat{a}_N$, where $G_B \geq 1$. The Ψ channel can also model loss in Bob's terminal by means of a pure-loss channel, $\mathcal{L}^0_{\eta_B}$, whose output modes satisfy $\hat{a}_B = \sqrt{\eta_B}\,\hat{a}'_S + \sqrt{1-\eta_B}\,\hat{a}_N$, and $\hat{a}'_N = \sqrt{1-\eta_B}\,\hat{a}'_S - \sqrt{\eta_B}\,\hat{a}_N$, where $0 \leq \eta_B \leq 1$. For completeness, we will also consider the complement of $\mathcal{A}^0_{G_B}$—the contravariant quantum-limited amplifier channel $\tilde{\mathcal{A}}^0_{G_B}$—whose outputs obey $\hat{a}_B = \sqrt{G_B - 1}\,\hat{a}'^\dagger_S + \sqrt{G_B}\,\hat{a}_N$ and $\hat{a}'_N = \sqrt{G_B}\,\hat{a}'_S + \sqrt{G_B - 1}\,\hat{a}^\dagger_N$. From these input-output relations the B mode's average photon number, $\langle\hat{a}^\dagger_B\hat{a}_B\rangle$, can be found to be

$$N_B = \begin{cases} G_B(\langle\hat{a}'^\dagger_S\hat{a}'_S\rangle + E_X) + G_B - 1, & \text{for } \mathcal{A}^0_{G_B}, \\ \eta_B(\langle\hat{a}'^\dagger_S\hat{a}'_S\rangle + E_X), & \text{for } \mathcal{L}^0_{\eta_B}, \\ (G_B - 1)(\langle\hat{a}'^\dagger_S\hat{a}'_S\rangle + E_X + 1), & \text{for } \tilde{\mathcal{A}}^0_{G_B}. \end{cases} \tag{3}$$

In deriving an upper bound on Eve's information gain we can (and will) assume that Eve collects *all* the B modes, because Bob performs the key-map operation.

As a final note on Ψ, we point out that no loss of generality is entailed by our assumption that $\hat{a}_N$ is in its vacuum state. This is because Eve gains less information when $\hat{a}_N$ is in a thermal state than when that mode is in its vacuum state, as is easily demonstrated by a channel decomposition [45, 46] argument. In particular, let an N_0 superscript on our channel models' symbols denote the average photon number of that channel's thermal-state environment. The thermal-environment amplifier channel can be expressed as

$$\mathcal{A}^{N_0}_{G_B} = \mathcal{L}^{N'_0}_{1/G'} \circ \mathcal{A}^0_{G'} \circ \mathcal{A}^0_{G_B}, \tag{4}$$

where $G' = \sqrt{1 + N'_0}/\sqrt{1 + N'_0 - N_0(G_B^2 - 1)} > 1$ with $N'_0 > N_0(G_B^2 - 1)$. Likewise, the thermal-environment loss channel can be written as

$$\mathcal{L}^{N_0}_{\eta_B} = \mathcal{A}^0_{1/\eta'} \circ \mathcal{L}^0_{\eta'} \circ \mathcal{L}^0_{\eta_B}, \tag{5}$$

where $\eta' = 1/\sqrt{1 + N_0(1 - \eta_B^2)} < 1$. (A similar relation holds for the complementary channel, but we shall omit it). The data-processing inequality [47] now guarantees that the upper bound on Eve's information gain for the $N_0 = 0$ version of each of our Gaussian Ψ channels is also an upper bound on the information Eve gains from the $N_0 > 0$ version of that Gaussian channel.

III. BOUNDING EVE'S INFORMATION GAIN

For protocols that encode multiple modes per symbol, post-processing cannot independently manipulate each mode within a raw-key symbol. In particular, permutation of the raw keys only permutes multiple-mode blocks. Hence, the de Finetti theorem [32, 33] can be used to reduce the coherent attack to a block-wise coherent attack, but not to reduce it further to a single-mode attack. In a block-wise coherent attack, Eve performs the same arbitrary attack on each size $M_B \gg 1$ symbol block of Alice

and Bob's transmissions. To accomplish the reduction, we will make use of the tools from Ref. [40].

Consider a multiple-block QKD session in which Alice and Bob spend some small amount of pre-shared key to randomly discard some of the size-M_B blocks, during post-processing of their raw keys. By de Finetti theorem, we only need to bound Eve's information gain by analyzing, see Sec. III A, the block-wise coherent attack. Note that because $M_B \gg 1$, the amount of key consumption for determining the blocks being discarded is very small compared to the keys being generated. It is worth emphasizing that there is hope that the reduction from the general coherent attack to the block-wise coherent attack may be accomplished without relying on de Finetti argument, see Sec. III B.

Alice and Bob's secret-key efficiency (SKE), in bits/symbol, for an asymptotic-regime block-coherent attack is given by the Devetak-Winter formula [37, 38, 48]

$$\text{SKE} = \max(\beta I_{AB} - M_E \chi_E, 0). \tag{6}$$

Here: I_{AB} is the Shannon information (in bits/symbol) between Bob's key map $\{X\}$ and Alice's measurement data $\{\tilde{X}\}$; β is Alice and Bob's reconciliation efficiency; χ_E is Eve's bits/mode Holevo-information gain; and M_E is the number of modes per encoded symbol. Alice and Bob can calculate I_{AB} from error-probability measurements, and they know the efficiency of their error-correction procedure, but they need to maximize χ_E over all block-wise coherent attacks that are consistent with their security-testing results. That maximization—obtaining an upper bound on χ_E—is therefore the heart of the asymptotic-regime security proof for TW-QKD protocols. In what follows, we show that the structure of TW-QKD protocols leads to an additive upper bound on χ_E that, in turn, results in an SKE lower bound.

A. Bounding the block-wise coherent attack

Reference [40] developed a way to bound Eve's information gain for a TW-QKD protocol, but that reference focused on a rigorous formulation for noisy entanglement-assisted classical capacity, and did not present in full detail a security proof for TW-QKD protocols. Here we present a detailed proof that Ref. [40]'s capacity formula provides an upper bound on the the most general block-wise coherent attack's information gain. Our proof applies to *all* TW-QKD protocols in which Bob performs the key map, not just to the Gaussian special case. As shown in Fig. 2, Alice transmits the M_B-symbol block $\boldsymbol{Y} \equiv Y_1 \cdots Y_{M_B}$, where the $\{Y_m\}$ each have M_E modes and we are using the Fig. 1 notation with a subscript to identify the symbol's place within the M_B-symbol block. Alice has access to the purifications $\boldsymbol{W} \equiv W_1 \cdots W_{M_B}$, i.e., each $(Y_m W_m)$ pair is in the tensor product of M_E TMSV states.

We shall allow Eve to perform the most general attack on this block—shown schematically in Fig. 2—by

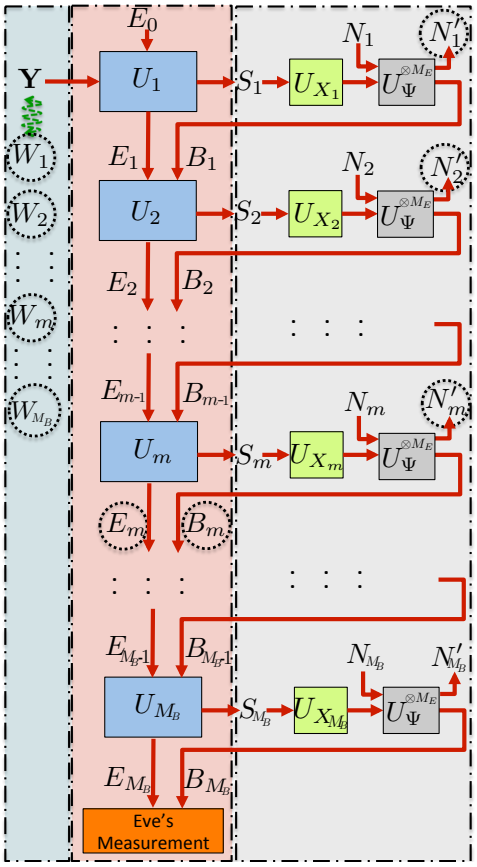

FIG. 2. Schematic of the most general coherent attack on an M_B-symbol block. Dotted circles enclose the modes present after the mth attack round.

supposing that Alice sends all of $\boldsymbol{Y}$ simultaneously on the forward channel, and that Eve performs the following M_B-round interactive process with Bob. In the mth round, Eve sends an M_E-mode signal S_m [49] to Bob who responds by transmitting his M_E-mode encoded symbol B_m [50]. We assume that Eve captures B_m in its entirety, because doing so will aid our security analysis and full capture affords Eve more information than she would get from partial capture. In addition, we will give Eve an ideal quantum memory, so that she can postpone her quantum measurement until after the M_Bth interaction round. Furthermore, we grant Eve the power to create an arbitrarily entangled multi-mode ancilla E_0 for use in her first round, and the ability to perform an arbitrary multi-mode unitary, U_m, in the mth round. Her first round's unitary acts on $\boldsymbol{Y}$ and produces the outputs S_1, which Eve sends to Bob, and E_1, which is an ancilla that Eve retains for use in the second round. In the next $M_B - 2$ rounds, Eve's unitary acts on $(E_m B_m)$ and produces the output E_{m+1}. Eve makes her quantum measurement on $(E_{M_B} B_{M_B})$, the outputs from her M_Bth interaction round.

Bob's operations in Fig. 2 are the following. Upon receipt of S_m from Eve, he encodes a randomly-chosen

classical symbol X_m by means of the unitary U_{X_m} which he then passes through the channel $\Psi^{\otimes M_E}$, whose Stinespring-dilation unitary $U_\Psi^{\otimes M_E}$ has ancilla input N_m and produces the return B_m and the ancilla output N'_m. (Note that Fig. 2 has omitted Bob's use of a small portion of each S_m for security testing.)

We assume that Eve can neither access the $\boldsymbol{W}$ that are in Alice's lab nor the $\boldsymbol{N} \equiv N_1 \cdots N_{M_B}$ and the $\boldsymbol{N}' \equiv N'_1 \cdots N'_{M_B}$ that are in Bob's lab. Thus her Holevo-information gain satisfies

$$\chi_E^{(M)} \equiv I(E_{M_B} B_{M_B} : X_{M_B} \cdots X_1) \tag{7}$$

$$= \sum_{m=1}^{M_B} I(E_{M_B} B_{M_B} : X_m \mid X_{m-1} \cdots X_1) \tag{8}$$

$$\leq \sum_{m=1}^{M_B} I(E_m B_m : X_m \mid X_{m-1} \cdots X_1), \tag{9}$$

where the superscript $M = M_B M_E$ denotes the total number of modes from which Eve has gained information. The first equality is because the Holevo information obtainable from a quantum system A, in state ρ_A^x with probability density function $p_X(x)$, about a classical register X can be written as the Shannon information $I(A:X)$ between A and X for the classical-quantum state $\rho_{AX} \equiv \int \mathrm{d}x\, p_X(x) \rho_A^x \otimes |x\rangle_X \langle x|$ [47]. The second equality is due to the chain rule for Shannon information, with $I(A : C \mid B)$ being the conditional Shannon information between A and C given B [51]. The inequality follows from the data processing inequality [47], because key distribution after the mth round is a quantum operation that generates $E_{M_B} B_{M_B}$ from $E_m B_m$ with assistance from ancilla that are independent of X_m, and hence do not increase the Shannon information.

Now let us focus on the system after mth round, which consists of $E_m B_m W_1 \cdots W_{M_B} N'_1 \cdots N'_m$. These modes, which are contained in Fig. 2's dotted circles, are in a joint pure state with Eve only having access to $E_m B_m$. Nevertheless, it is convenient to *increase* Eve's information gain by pretending that she can access B_m and $\tilde{E}_m \equiv E_m W_1 \cdots W_{m-1} W_{m+1} W_{M_B} N'_1 \cdots N'_{m-1}$, i.e., we have that

$$I(E_m B_m : X_m \mid X_{m-1} \cdots X_1)$$
$$\leq I(\tilde{E}_m B_m : X_m \mid X_{m-1} \cdots X_1). \tag{10}$$

The term on the right in (10) is bounded above by the noisy entanglement-assisted capacity formula from Ref. [40], with $\tilde{E}_m$ as the ancilla generated by Eve and $W_m \tilde{E}_m S_m$ in a pure state. Thus we have $\chi_E^{(M)}$ from (9) has an upper bound given by M_B times a multi-letter capacity formula over M_E modes, where we emphasize that this result applies to *all* TW-QKD protocols in which Bob performs the key map.

B. Optimality of the block-wise coherent attack

Despite the de Finetti theorem sufficing to reduce the coherent attack to the block-wise coherent attack, here we provide an analysis that the block-wise coherent attack is the optimum coherent attack in the asymptotic regime. Note that the analysis is not entirely rigorous yet, however, there is good hope that with some future generalization of quantum asymptotic-equipartition property (QAEP) [52], the analysis will be fully rigorous. This approach is desirable, not only because it is more elegant, but also since we expect it will lead to tighter finite-key bounds. Consider K blocks of M_B symbols that are indexed by $1 \leq k \leq K$. The schematic for Eve's coherent attack on these K blocks is similar to the single-block attack from Fig. 2, except that now all of Alice's signal modes, $\mathbb{Y} \equiv \boldsymbol{Y}^{(1)} \cdots \boldsymbol{Y}^{(K)}$, are supplied to Eve simultaneously. To proceed expeditiously, we introduce some new notation. In the kth block, we let $\boldsymbol{E}_k \equiv E_{M_B}^{(k)} B_{M_B}^{(k)}$, $\boldsymbol{N}_k \equiv N_1^{(k)} \cdots N_{M_B}^{(k)}$, $\boldsymbol{N}'_k \equiv N_1'^{(k)} \cdots N_{M_B}'^{(k)}$, and $\boldsymbol{W}_k \equiv W_1^{(k)} \cdots W_{M_B}^{(k)}$, where, except for the superscript denoting the block index, the right-hand sides of each definition have the same meanings as in Fig. 2. In a similar manner, we use $\boldsymbol{X}_k \equiv X_1^{(k)} \cdots X_{M_B}^{(k)}$ to denote Bob's random classical messages for the kth block.

With the preceding notation, Fig. 3 shows the schematic for Eve's K-block coherent attack, in which the kth block can be considered a unitary from input $\boldsymbol{E}_{k-1} \boldsymbol{N}_k$ to output $\boldsymbol{E}_k \boldsymbol{N}'_k$, conditioned on the classical messages $\boldsymbol{X}_k$. For a K-block QKD session, the $\epsilon_{\mathrm{EC}} + \epsilon_{\mathrm{PA}} + \epsilon$-secure SKE, in bits/symbol, is given by [36]

$$\mathrm{SKE}(K, M_B) = \left[H_{\min}^{\epsilon} (\boldsymbol{X}_1 \cdots \boldsymbol{X}_K \mid \boldsymbol{E}_K) - \mathrm{leak}_{\mathrm{IR}} + \log\left(\epsilon_{\mathrm{PA}}^2\right) \right] / K M_B, \tag{11}$$

where $\mathrm{leak}_{\mathrm{IR}}$ is the information leaked to Eve in the information reconciliation protocol with ϵ_{EC}-secure error correction and ϵ_{PA}-secure privacy amplification, and $H_{\min}^{\epsilon}(A \mid B)$ is the smooth min-entropy of A conditioned on B. Note that $\mathrm{leak}_{\mathrm{IR}}$ can be determined by Alice and Bob. In the asymptotic ($K \to \infty$) regime the last term in brackets vanishes, so we only need to lower bound $H_{\min}^{\epsilon}(\boldsymbol{X}_1 \cdots \boldsymbol{X}_K \mid \boldsymbol{E}_K)$ for Alice and Bob to have a lower

FIG. 3. Schematic of the most general coherent attack on K blocks of M_B symbols. The dotted circles enclose the modes present after kth block. Note that all the $\{\mathbf{W_k}\}$ have been present from the start, despite their being assigned to different k values in this figure.

bound on their SKE. The arguments that follow parallel the single-block case.

First, we use the chain rule for smooth min-entropy [53] repeatedly to obtain

$$H^{\epsilon}_{\min}(\boldsymbol{X}_1\cdots\boldsymbol{X}_K \mid \boldsymbol{E}_K) \geq H^{z}_{\min}(\boldsymbol{X}_K \mid \boldsymbol{E}_K) + \sum_{k=1}^{K-1} H^{z}_{\min}(\boldsymbol{X}_k \mid \boldsymbol{E}_K\boldsymbol{X}_{k+1}\cdots\boldsymbol{X}_K) - (K-1)f(z), \quad (12)$$

where $f(z) \sim \log(1/z)$ and $z = \epsilon/(3K-2)$. Because $\boldsymbol{E}_K\boldsymbol{X}_{k+1}\cdots\boldsymbol{X}_K$ can be obtained from $\boldsymbol{E}_k$ by a quantum operation, the data-processing inequality for smooth min-entropy [36] gives us

$$H^{z}_{\min}(\boldsymbol{X}_k \mid \boldsymbol{E}_K\boldsymbol{X}_{k+1}\cdots\boldsymbol{X}_K) \geq H^{z}_{\min}(\boldsymbol{X}_k \mid \boldsymbol{E}_k). \quad (13)$$

Next, after the kth block, we decrease Eve's smooth min-entropy by granting her access to everything other than $\boldsymbol{W}_k$ and $\boldsymbol{N}'_k$, i.e., Eve's system is enlarged to $\tilde{\boldsymbol{E}}_k \equiv \boldsymbol{E}_k\boldsymbol{W}_1\cdots\boldsymbol{W}_{k-1}\boldsymbol{W}_{k+1}\cdots\boldsymbol{W}_K\boldsymbol{N}'_1\cdots\boldsymbol{N}'_{k-1}$. Another use of the data-processing inequality then leads to

$$H^{z}_{\min}(\boldsymbol{X}_k \mid \boldsymbol{E}_k) \geq H^{z}_{\min}(\boldsymbol{X}_k \mid \tilde{\boldsymbol{E}}_k), \quad (14)$$

where the right-hand side corresponds to the case in which Eve has a pure state kth block's outset. Combining Eqs. (11)–(14), we get

$$\mathrm{SKE}(K, M_B) \geq \left[\sum_{k=1}^{K} H^{z}_{\min}(\boldsymbol{X}_k \mid \tilde{\boldsymbol{E}}_k) - (K-1)f(z) - \mathrm{leak}_{\mathrm{IR}} + \log(\epsilon^2_{\mathrm{PA}})\right]/KM_B. \quad (15)$$

Because $f(z) \sim \log(3K/\epsilon)$, we can let K and M_B increase while maintaining $K \gg M_B \gg \log(K) \gg 1$, and obtain, asymptotically,

$$\mathrm{SKE}(K, M_B) \geq \frac{1}{KM_B}\left[\sum_{k=1}^{K} H^{\epsilon/3K}_{\min}(\boldsymbol{X}_k \mid \tilde{\boldsymbol{E}}_k) - \mathrm{leak}_{\mathrm{IR}}\right]. \quad (16)$$

The preceding lower bound is achieved when Eve performs independent operations on each M_B-symbol block. If Alice and Bob's security testing leads to identical constraints on each block, then the asymptotic-regime lower bound is achieved by Eve's performing a block-wise coherent attack. In Eve's absence, QKD protocols operating with $M_B \gg 1$ give security-testing results that are nearly identical for all sufficiently-large blocks. When Eve's activities create substantial block-to-block variations in Alice and Bob's security-testing results, they abort the protocol.

However, in order to be fully rigorous, one still need to show that (16) is lower bounded by the bound in (6). However, the QAEP in ref. [52] does not apply directly, since there is no independent and identically distributed structure in (16). To close the last step, one would require generalization of QAEP, which is a future direction to pursue. Conditioned on the QAEP generalization, as was the case for the bound in (10), the bound in (16) and its implications apply to *all* TW-QKD protocols. Part of our analysis is similar to the idea of entropy accumulation [54], which has been successfully applied in device-independent QKD protocols [55, 56]. However, owing to the structure of TW-QKD, in which Eve can interactively alter the quantum states being sent between Alice and Bob, the framework of entropy accumulation does not apply directly to our problem.

C. Constraints and single-letterization

Here we assume a Gaussian TW-QKD protocol and return to (9) and (10), in which $\chi^{(M)}_E$ in (9) is bounded above by M_B times the multi-letter capacity formula from Ref. [40] across M_E modes. For simplicity, however, we will use the multi-letter capacity formula from Ref. [40] across $M = M_BM_E$ modes, which still establishes an upper bound on $\chi^{(M)}_E$. Going forward, we will use $\boldsymbol{S} \equiv S_1S_2\cdots S_M$, $\boldsymbol{B} \equiv B_1B_2\cdots B_M$, and $\boldsymbol{W} \equiv W_1W_2\cdots W_M$ to denote the modes involved. For Gaussian protocols, U_X is covariant with Ψ, thus Eve's information gain obeys the following multi-letter bound [37, 40],

$$\chi^{(M)}_E \leq \max_{\rho_{\boldsymbol{SW}}} F(\rho_{\boldsymbol{SW}}), \quad (17)$$

$$F(\rho_{\boldsymbol{SW}}) \equiv S(\rho_{\boldsymbol{B}}) - E_{(\Psi^{\otimes M})^c\otimes\mathcal{I}}(\rho_{\boldsymbol{SW}}). \quad (18)$$

In this bound: $S(\cdot)$ is the von Neumann entropy; ϕ^c denotes the complementary channel to the ϕ channel; $\mathcal{I}$ is the identity channel on $\boldsymbol{W}$; and $E_\phi(\cdot)$, the entropy gain of the completely-positive trace-preserving map ϕ applied to a system in state ρ, is defined to be $E_\phi(\rho) \equiv S[\phi(\rho)] - S(\rho)$. The maximization in (17) is over attacks that are constrained by the intrusion parameters that Alice and Bob derive from their security testing on the state $\rho_{\boldsymbol{SW}}$. We shall assume, in proceeding, that Bob independently encodes each mode ($M_E = 1$), so that $\rho_{B_m} = \int \mathrm{d}x\, p_X(x)\Psi(U_x\rho_{S_m}U_x^\dagger)$; when Bob uses $M_E > 1$ encoding, (17) is still an upper bound on $\chi^{(M)}_E$.

To facilitate evaluating (17), and thus the asymptotic-regime SKE from (6), the constraints that Alice and Bob derive from their security testing should satisfy two requirements.

(R1) The constraints lead to a single-letter upper bounds on Eve's information gain.

(R2) The constraints can be measured precisely in the asymptotic regime from Alice and Bob's performing an LOCC procedure.

Requirement (R1) ensures that evaluating the upper bound on Eve's information gain from the constraints is tractable, and requirement (R2) ensures that the constraints can be obtained with arbitrarily high precision from security testing over a sufficiently long QKD session.

Because $\rho_{\boldsymbol{SW}}$ is infinite dimensional, we use Gaussian extremality [57, 58]—which states that when the covariance matrix of the input state is fixed, continuous sub-additive (super-additive) function, which is invariant under local passive symplectic transforms, has its maximum (minimum) achieved by Gaussian states—to satisfy requirement (R1) and restrict the maximization in (17) to Gaussian states. Toward this end, Ref. [40] established the following two sub-additivity inequalities (Theorems 2 and 3 in Ref. [40]'s supplemental material),

$$F(\rho_{\boldsymbol{SW}}) \leq \sum_{m=1}^{M} F(\rho_{S_m W_m}), \tag{19}$$

$$F(\rho_{\boldsymbol{SW}}) \leq \sum_{m=1}^{M} F(\rho_{S_m \boldsymbol{W}}). \tag{20}$$

Here $F(\rho_{S_m W_m}) \equiv S(\rho_{B_m}) - E_{\Psi^c \otimes \mathcal{I}}(\rho_{S_m W_m})$ and $F(\rho_{S_m \boldsymbol{W}}) \equiv S(\rho_{B_m}) - E_{\Psi^c \otimes \mathcal{I}}(\rho_{S_m \boldsymbol{W}})$ are generalizations of Eq. (18). Because E_ϕ is convex [59], we have that $F(\rho_{\boldsymbol{SW}})$ is concave in quantum states. The subadditivity inequalities (19) and (20) then ensure that the maximum in (17) is achieved by Gaussian inputs, $\rho_{\boldsymbol{SW}}$ [40], that satisfy covariance-matrix constraints. Thus we will only consider constraints from security testing that restrict covariance matrices.

In Sec. III C 1, we revisit the covariance-matrix constraints considered in Ref. [40], and give its explicit form for Gaussian protocols. Although these constraints meet requirement (R1), they fail to satisfy requirement (R2), making them unsuitable for our goal of establishing a TW-QKD security framework. In Sec. III C 2, we introduce constraints—in the form of sums of pair-wise terms—and show that they meet requirements (R1) *and* (R2). Similarly, in Sec. III C 3, we generalize to sum constraints that are invariant under signal-mode permutations, and show that they too obey requirements (R1) and (R2). Under a collective attack, the precision with which the intrusion parameters from Secs. III C 2 and III C 3 can be estimated improves as the QKD session's duration increases, becoming perfect in the asymptotic limit. Moreover, standard CV-QKD covariance-estimation techniques can be applied for that purpose. It is an important and open problem, however, to find means for reliable estimation of these intrusion parameters when Eve performs a coherent attack. A procedure that would suffice in that regard is one that affords a robust measurement of $\overline{\boldsymbol{\Lambda}} \equiv \sum_{m=1}^{M} \boldsymbol{\Lambda}_{S_m W_m}/M$, where $\boldsymbol{\Lambda}_{S_m W_m}$ is the Wigner covariance matrix of $(S_m W_m)$.

There are two reasons why the single-letter bounds on Eve's coherent-attack information gain that result from using (19) or (20) in (17) may not be tight: (1) they assume that Eve collects all the light that Bob sends to Alice; and (2) they assume single-mode encoding. The first reason does not apply to long-distance QKD, because security analysis presumes Eve collects all the light lost in propagation from Bob to Alice, and that loss is 90% for a 50-km-long low-loss (0.2 dB/km) fiber and 99% for a 100-km-long fiber. Even for short-haul links the first reason does not apply to FL-QKD, because that protocol employs a high-gain optical amplifier in Bob's terminal. In contrast, FL-QKD employs multi-mode encoding with $M_E \gg 1$ [14–17], whereas the protocol from Ref. [21] uses single-mode encoding, so the latter is immune to the second reason although it is prone to the first.

1. *Separate pair-wise constraints*

Reference [40] imposed pair-wise constraints on the reduced density operators, $\{\rho_{S_m W_m} : 1 \leq n \leq M\}$, to reduce (17) to a single-letter formula via (19). To be specific, suppose that, when Eve mounts her attack, Alice and Bob's security-testing measurements allows them to determine the average photon numbers of all the $\{S_m\}$ modes,

$$\langle \hat{a}^\dagger_{S_m} \hat{a}_{S_m} \rangle = \kappa_S^{(m)} N_S, \text{ for } 1 \leq m \leq M, \tag{21}$$

and the total cross-correlation strengths for all $(S_m W_m)$ pairs,

$$|\langle \hat{a}_{S_m} \hat{a}_{W_m} \rangle|^2 + |\langle \hat{a}^\dagger_{S_m} \hat{a}_{W_m} \rangle|^2 = \kappa_f^{(m)} C_S^2, \text{ for } 1 \leq m \leq M. \tag{22}$$

The intrusion parameters $\{\kappa_S^{(m)}\}$ quantify the average photon numbers of Bob's $\{S_m\}$ modes relative to N_S, the average photon number of the $\{Y_m\}$ modes that Alice transmitted, while the intrusion parameters $\{\kappa_f^{(m)}\}$ quantify the total cross-correlation strengths of the $\{(S_m W_m)\}$ pairs relative to those of the $\{(Y_m W_m)\}$. In order for these parameters to be physically valid, we require that $\kappa_S^{(m)} \geq 0$ and $0 \leq \kappa_f^{(m)} \leq \min[\kappa_S^{(m)}, (1 + 2\kappa_S^{(m)} N_S)/(1 + 2N_S)]$, as shown in Appendix A.

Using (19), the information-gain bound in (17) reduces to a single-letter form [40]

$$\chi_E^{(M)} \leq \sum_{m=1}^{M} \chi_E\left(\kappa_S^{(m)}, \kappa_f^{(m)}\right), \tag{23}$$

where

$$\chi_E\left(\kappa_S^{(m)}, \kappa_f^{(m)}\right) \equiv \max_{\rho_{S_m W_m}} F(\rho_{S_m W_m}), \tag{24}$$

with the maximization being constrained by the intrusion parameters from Eqs. (21) and (22). The following theorem guarantees that Eq. (24) is easily evaluated.

Theorem 1 *For Gaussian TW-QKD protocols, with intrusion parameters given by Eqs. (21) and (22), the maximization in Eq. (24) results in*

$$\chi_E\left(\kappa_S^{(m)}, \kappa_f^{(m)}\right) = g(N_{B_m}) - E^\star_{\Psi^c \otimes \mathcal{I}}\left(\kappa_S^{(m)}, \kappa_f^{(m)}\right), \tag{25}$$

where $g(N_T) = (N_T + 1)\log_2(n_T + 1) - N_T \log_2(N_T)$ *is the von Neumann entropy of a thermal state with average photon number* N_T, $N_{B_m} = \langle \hat{a}^\dagger_{B_m} \hat{a}_{B_m} \rangle$ *from Eq. (3) for the* m*th mode, and* $E^\star_{\Psi^c \otimes \mathcal{I}}(\kappa_S, \kappa_f)$ *is a minimized entropy*

gain that can be evaluated as a three-parameter minimization of a closed-form analytic function.

When the intrusion parameters satisfy $\kappa_f^{(m)} \simeq \kappa_S^{(m)} \leq 1$*, the maximum is achieved by the beam-splitter light injection attack that was shown in Ref. [14] to realize Eve's optimum frequency-domain collective attack.*

The proof of Theorem 1 is similar to the frequency-domain collective attack proof from Ref. [14]; see Appendix A for the details. We emphasize that strong numerical evidence (see Appendix A) suggests that the beam-splitter light injection attack is the optimum attack when $\kappa_f^{(m)} \leq (1+\kappa_S N_S)/(1+N_S)$ for both the quantum-limited amplifier channel, $\mathcal{A}^0_{G_B}$, and its complementary channel, $\tilde{\mathcal{A}}^0_{G_B}$, and when $\kappa_S \leq 1$ for the pure-loss channel, $\mathcal{L}^0_{\eta_B}$.

Unfortunately, when Eve mounts a coherent attack each $\rho_{S_m W_m}$ may be different, which implies that Alice and Bob only get a single instance of that state from which it is impossible to get reliable estimates of $\kappa_S^{(m)}$ and $\kappa_f^{(m)}$. Thus the separate pair-wise constraints fail to satisfy requirement (R2).

2. Pair-wise sum constraint

As a first approach to remedying the separate pair-wise constraint's robustness deficiency, let us consider the pair-wise sum constraints,

$$\sum_{m=1}^{M} \langle \hat{a}^\dagger_{S_m} \hat{a}_{S_m} \rangle = M \overline{\kappa}_S N_S, \tag{26}$$

and

$$\sum_{m=1}^{M} \left[|\langle \hat{a}_{S_m} \hat{a}_{W_m} \rangle|^2 + |\langle \hat{a}^\dagger_{S_m} \hat{a}_{W_m} \rangle|^2 \right] = M \overline{\kappa}_f C_S^2, \tag{27}$$

which are so named because they are the sums of quantities involving only a single mode pair.

In turns out, as we now show, that the pair-wise sum constraints' intrusion parameters $\overline{\kappa}_S$ and $\overline{\kappa}_f$ allow the information-gain bound in (17) to be reduced to the single-letter formula

$$\chi_E^{(M)} \leq M \chi_E(\overline{\kappa}_S, \overline{\kappa}_f), \tag{28}$$

where $\chi_E(\overline{\kappa}_S, \overline{\kappa}_f)$ is obtained from Eq. (24) with $\kappa_S^{(m)} = \overline{\kappa}_S$ and $\kappa_f^{(m)} = \overline{\kappa}_f$. To demonstrate that this is so, let us first suppose $\chi_E\left(\kappa_S^{(m)}, \kappa_f^{(m)}\right)$ is a concave function, in which case we have that $\chi_E^{(M)} \leq \sum_{n=1}^{M} \chi_E\left(\kappa_S^{(n)}, \kappa_f^{(n)}\right) \leq M \chi_E(\overline{\kappa}_S, \overline{\kappa}_f)$. The second inequality becomes an equality when the mode pairs are independent and identically distributed. Moreover, given the average Wigner covariance matrix, $\overline{\mathbf{\Lambda}}$, we can obtain $\overline{\kappa}_S$ because $\sum_{m=1}^{M} \langle \hat{a}^\dagger_{S_m} \hat{a}_{S_m} \rangle / M = \overline{\kappa}_S N_S$ is one of $\overline{\mathbf{\Lambda}}$'s diagonal elements. We can also get a lower bound on $\overline{\kappa}_f$ from $\overline{\mathbf{\Lambda}}$, because $\overline{\mathbf{\Lambda}}$'s off-diagonal elements obey $|\sum_{m=1}^{M} \langle \hat{a}_{S_m} \hat{a}_{W_m} \rangle|^2 / M + |\sum_{m=1}^{M} \langle \hat{a}^\dagger_{S_m} \hat{a}_{W_m} \rangle|^2 / M \leq \overline{\kappa}_f C_S^2$. Then, because $\chi_E(\overline{\kappa}_S, \overline{\kappa}_f)$ increases with decreasing $\overline{\kappa}_f$ for fixed κ_S, we can use the intrusion parameters derived from $\overline{\mathbf{\Lambda}}$ in (28) to bound Eve's information gain.

To complete our demonstration that the pair-wise sum constraints provide an upper bound on Eve's information gain, we must verify that $\chi_E\left(\kappa_S^{(m)}, \kappa_f^{(m)}\right)$ from Eq. (25) is concave. The von Neumann entropy is concave, so all that needs to be shown is that $E^\star_{\Psi^c \otimes \mathcal{I}}\left(\kappa_S^{(m)}, \kappa_f^{(m)}\right)$ is convex. That term is the constrained minimum of an entropy gain whose lengthy closed-form expression makes is difficult to prove the desired convexity analytically. Our numerical work in Appendix A, however, indicates that Eq. (25) is indeed a concave function of $(\kappa_S^{(m)}, \kappa_f^{(m)})$ for $\mathcal{A}^0_{G_B}$, $\mathcal{L}^0_{\eta_B}$, and $\tilde{\mathcal{A}}^0_{G_B}$ (see Fig. 8). In practice, Alice and Bob's protocol will operate in the vicinity of some nominal set of intrusion parameters, so our numerical evidence should suffice for justifying the use of pair-wise sum constraints.

3. Permutation-invariant sum constraints

The pair-wise sum constraints' cross-correlation intrusion parameter, $\overline{\kappa}_f$ from Eq. (27), may be difficult to measure when, as in FL-QKD, Bob uses multi-mode encoding with $M_E \gg 1$. In this section, therefore, we will replace Eq. (27)'s cross-correlation constraint with the permutation-invariant constraint,

$$\sum_{m,n=1}^{M} \left[|\langle \hat{a}_{S_m} \hat{a}_{W_n} \rangle|^2 + |\langle \hat{a}^\dagger_{S_m} \hat{a}_{W_n} \rangle|^2 \right] = \overline{K}_f M C_S^2, \tag{29}$$

which constrains the total cross correlation between the $\{\hat{a}_{S_m}\}$ modes and all permutations of the $\{\hat{a}_{W_m}\}$ modes. Its measurement may be easier than that for the pair-wise sum constraint when $M_E \neq 1$. Because $\overline{K}_f \geq \overline{\kappa}_f$, a lower bound for $\overline{K}_f$ can also be obtained from the average covariance matrix $\overline{\mathbf{\Lambda}}$.

We now show that with $\overline{\kappa}_S$ and $\overline{K}_f$ from Eqs. (26) and (29) we get the information-gain upper bound

$$\chi_E^{(M)} \leq M \chi_E(\overline{\kappa}_S, \overline{K}_f). \tag{30}$$

To do so, we reduce the permutation-invariant sum constraints to the separate mode-pair constraints, Eqs. (21) and (22), as follows. We start by using (20) in (17) so that the maximization to be done is of $\sum_{m=1}^{M} F(\rho_{S_m \boldsymbol{W}})$. Next, we introduce an intermediate intrusion parameter,

$K_f^{(m)}$, defined by

$$\sum_{n=1}^{M}\left[|\langle\hat{a}_{S_m}\hat{a}_{W_n}\rangle|^2+|\langle\hat{a}^\dagger_{S_m}\hat{a}_{W_n}\rangle|^2\right]=K_f^{(m)}C_S^2, \quad (31)$$

so that Eq. (29) can be rewritten as $\sum_{m=1}^{M}K_f^{(m)}/M=\overline{K}_f$. An upper bound on the maximum of $\sum_{m=1}^{M}F(\rho_{S_m\boldsymbol{W}})$ can thus be obtained in two steps. First, for fixed $\kappa_S^{(m)},K_f^{(m)}$, obtain the maximum of $F(\rho_{S_m\boldsymbol{W}})$ over $\rho_{S_m\boldsymbol{W}}$. Then maximize over the set $\{\kappa_S^{(m)},K_f^{(m)}:1\le m\le M\}$. The first maximization is accomplished by the following theorem.

Theorem 2 *For a Gaussian TW-QKD protocol with references modes $\boldsymbol{W}$ and a signal mode S_m, we have that*

$$\chi'_E\left(\kappa_S^{(m)},K_f^{(m)}\right)\equiv\max_{\rho_{S_mW_1W_2}}F(\rho_{S_m\boldsymbol{W}}) \quad (32)$$

$$=\max_{\rho_{S_mW_1W_2}}[S(\rho_B)-E_{\Psi^c\otimes\mathcal{I}}(\rho_{S_mW_1W_2})]. \quad (33)$$

under the Eq. (21) constraint and

$$|\langle\hat{a}_{S_m}\hat{a}_{W_1}\rangle|^2+|\langle\hat{a}^\dagger_{S_m}\hat{a}_{W_1}\rangle|^2+|\langle\hat{a}_{S_m}\hat{a}_{W_2}\rangle|^2=K_f^{(m)}C_S^2, \quad (34)$$

where the maximization in Eq. (33) can be accomplished by a four-parameter maximization of a closed-form analytic function.

The proof's basic idea is to manipulate the $\boldsymbol{W}$ modes with properly chosen beam splitters; see Appendix B for the details. Unfortunately, the four-parameter maximization is analytically cumbersome, because of the lengthy nature of the closed-form expression involved. Consequently we again resort to numerics. As shown in Appendix B, we find that for the $\mathcal{A}^0_{G_B}$ and $\tilde{\mathcal{A}}^0_{G_B}$ channels with various G_B values, as well as for the $\mathcal{L}^0_{\eta_B}$ channel with various η_B values, the maximum is achieved, for various N_S values, when $|\langle\hat{a}^\dagger_{S_m}\hat{a}_{W_1}\rangle|^2=0$. At this point, suitable beam splitting of the $\boldsymbol{W}$ modes can make $\langle\hat{a}_{S_m}\hat{a}_{W_2}\rangle=0$. This collapses the Eq. (34) constraint to the single-mode pair constraint in Eq. (22), giving us $\chi'_E\left(\kappa_S^{(m)},K_f^{(m)}\right)=\chi_E\left(\kappa_S^{(m)},K_f^{(m)}\right)$. Combined with concavity arguments, we obtain the information-gain bound in (30).

IV. SECRET-KEY EFFICIENCIES

In this section, we evaluate the asymptotic SKEs, given by Eq. (6) under Eve's coherent attack, for two Gaussian TW-QKD protocols: the TMSV protocol from Refs. [21, 26, 28, 29], and FL-QKD [14–17]. These protocols' SKRs can be obtained, if desired, by multiplying their SKEs by Bob's encoding rate, e.g., $R=10\,\text{Gbaud}$ for state-of-the art equipment. We assume that asymptotic-regime operation permits the intrusion parameters $\overline{\kappa}_S,\overline{\kappa}_f$ or $\overline{\kappa}_S,\overline{K}_f$ to be measured perfectly, and using those parameters we can bound Eve's information gain per mode using $\chi_E(\overline{\kappa}_S,\overline{\kappa}_f)$ or $\chi_E(\overline{\kappa}_S,\overline{K}_f)$ in Eq. (25). With that result in hand we can get a lower bound on Alice and Bob's SKE once we have evaluated their Shannon information in bits/symbol. For that evaluation we need to specify Bob's encoding operation and Alice's measurement on the light each receives in the protocol under consideration. In what follows we will do so assuming that the Alice-to-Bob and Bob-to-Alice channels, in the absence of Eve, are optical-fiber links with 0.2 dB/km loss, so that $\kappa_S=10^{-0.02L}$, where L is the one-way distance in km between Alice and Bob. We shall neglect the additional losses associated with Alice and Bob's security testing.

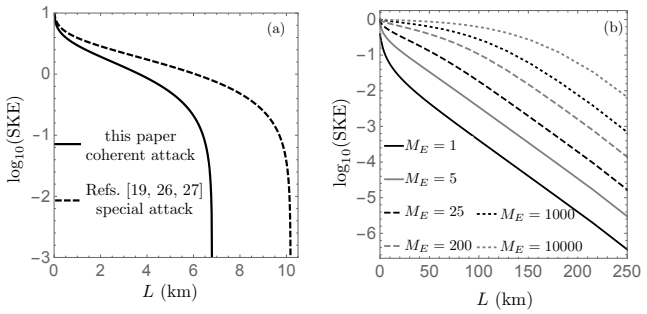

FIG. 4. Secret-key efficiencies in bits/symbol versus one-way path length (channel transmissivity $\kappa_S=10^{-0.02L}$) for attacks that give $\overline{\kappa}_S=\kappa_S$ and $\overline{\kappa}_f=\kappa_S$ and post-processing that gives perfect reconciliation efficiency. The solid curves are coherent-attack SKE lower bounds obtained from this paper's framework. (a) Results for the TMSV protocol with $N_S\gg1$ and $E_X\gg1$; the dashed curve is the SKE lower bound from Refs. [21, 28, 29]. (b) Results for the FL-QKD protocol with $G_B=10^6$, N_S chosen at each L to maximize the SKE, and various M_E values.

A. TMSV protocol with random displacement

In the TMSV protocol with random displacement [21, 28, 29], Alice has access to the full TMSV state and Bob performs single-mode encoding using zero-mean, circulo-complex, Gaussian-distributed displacements that add average photon number E_X to each mode he receives. Bob does not employ an additional operation after his encoding, thus Ψ is the noiseless identity channel that is equivalent to $\mathcal{A}^0_1$, and hence $N_B=\kappa_SN_S+E_X$ from Eq. (3) in the absence of Eve, or when her attack does not alter Bob's average received photon number. Alice uses a dual-homodyne receiver to measure both quadratures of the light she receives. Given the intrusion parameters $\overline{\kappa}_S$ and $\overline{\kappa}_f$ from Eqs. (26) and (27), our framework provides asymptotic security for this protocol against coherent attacks.

To illustrate the SKEs predicted by our framework for the TMSV protocol, we consider an attack—like Eve's

passive attack in which she only interacts with the light lost in propagation between Alice and Bob and between Bob and Alice—that preserves Alice and Bob's covariance matrix, so that $\overline{\kappa}_S = \kappa_S$ and $\overline{\kappa}_f = \kappa_S$. Under this attack, Alice and Bob's Shannon information is [28] $I_{AB} = \log_2(\kappa_S E_X + \kappa_S^2 N_S + 1)$, and their resulting SKE is

$$\text{SKE} = \max[I_{AB} - \chi_E(\kappa_S, \kappa_S), 0], \tag{35}$$

where we have assumed perfect reconciliation efficiency, $\beta = 1$.

Figure 4(a) plots our coherent-attack SKE and the special-attack SKE from Refs. [21, 28, 29] versus the one-way path length, L, where we have taken $N_S \gg 1$ and $E_X \gg 1$, which makes this results independent of the exact values of those system parameters. This figure shows our SKE prediction to be much lower than the previous result. This gap is primarily due to our giving Eve access to all the light on the Bob-to-Alice channel which, for the short distances over which the TMSV protocol operates, is overly conservative, viz., $\kappa_S = 0.63$ at $L = 10\,\text{km}$. Indeed, for Eve's passive attack the SKE from Refs. [21, 28, 29] *is* the TMSV protocol's true performance. But our framework provides an SKE lower bound for an arbitrary coherent attack—which can result in $\overline{\kappa}_S \neq \kappa_S$ and $\overline{\kappa}_f \neq \kappa_S$—whereas the SKE result from Refs. [21, 28, 29] does not.

We expect our SKE lower bound to be much tighter for more robust protocols' long-distance operation, wherein $\kappa_S \ll 1$. Moreover, we might tighten our SKE bound for short-distance protocols by adding security testing on the Bob-to-Alice channel. For example, Bob might merge signal light from his own TMSV source with his B mode in his transmission to Alice while retaining that source's idler light for them to use in an LOCC procedure that will provide intrusion parameters quantifying Eve's intrusion on the Bob-to-Alice channel.

B. FL-QKD protocol

FL-QKD [14, 16, 17] is a two-way continuous-variable QKD protocol. Alice transmits unmodulated light to Bob. Bob binary-phase-shift encodes ($\theta_X = 0$ or $\pi\,\text{rad}$, $d_X = 0$) that light with random bits [60], and sends the encoded light back to Alice, who homodyne detects what she receives. FL-QKD introduces two major innovations: (1) Alice transmits broadband amplified spontaneous emission (ASE) light to Bob at low brightness (< 1 photon/mode) while retaining a high-brightness ($\gg 1$ photon/mode) version for use as her homodyne receiver's local oscillator. (2) Bob sends his encoded version of the light he received from Alice through a high-gain optical amplifier ($\Psi = \mathcal{A}^0_{G_B}$ with $G_B \gg 1$) before transmission back to Alice.

The preceding innovations completely defeat passive eavesdropping and enable FL-QKD to achieve Gbit/s SKRs against such an attack for the following reasons: (1) Alice's low-brightness transmission, after Bob's encoding operation, gets buried in the ASE noise of his high-gain amplifier. This noise makes it impossible to retrieve Bob's bit string without a high-brightness replica of the light Alice sent to Bob. Alice has such a reference, but the no-cloning theorem precludes Eve's generating one from Alice's low-brightness transmission. (2) Bob's encoding rate ($R \sim 10\,\text{Gbit/s}$) is much lower than the bandwidth ($W_B \sim 2\,\text{THz}$) of Alice's ASE transmission. The resulting high value of the bit-time $\times$ optical-bandwidth product ($W_B/R \sim 200$) enables Alice to send many photons per bit time to Bob, thus mitigating the Alice-to-Bob channel's loss in the same manner as in classical optical communication. (3) Bob's high-gain amplifier can completely overcome the Bob-to-Alice channel's loss. Consequently, FL-QKD is a two-way protocol whose effective propagation loss is that of one-way transmission.

Were *passive* eavesdropping the only threat faced by FL-QKD, its protocol security would be completely assured. Like other two-way protocols, however, FL-QKD is vulnerable to an *active* eavesdropping attack, in which Eve shines her own light into Bob's terminal—while saving her own reference beam—and then determines his bit string by using her reference to detect his encoding of her illumination from light she culls from the Bob-to-Alice channel. FL-QKD has been shown—both theoretically [14] and experimentally [16, 17] to defeat active eavesdropping by channel monitoring that uses a very low brightness photon-pair source at Alice's terminal, together with photon-counting measurements at both Alice and Bob's terminals, to bound the amount light Eve has injected into Bob. In fact, this monitoring, whose photon-pair source is a spontaneous parametric downconverter that produces multi-mode TMSV states, provides security against the optimum frequency-domain collective attack [14]. A great virtue of the present paper is that its framework can be applied to ensure FL-QKD's security against a coherent attack, as we now show.

Because $\boldsymbol{Y}$, Alice's transmission to Bob, merges her low-brightness ASE light with the signal beam from her SPDC source, Alice only has access to *part* of $\boldsymbol{W}$, the purification of that transmission. That part, $\boldsymbol{W}'$, is her SPDC source's idler beam that she retains for use in security testing. Nevertheless, that retained light suffices for our asymptotic-regime security framework, because $\langle \hat{a}_{S_m} \hat{a}_{W'_n} \rangle = \sqrt{\tau}\,\langle \hat{a}_{S_m} \hat{a}_{W_n} \rangle$ and $\langle \hat{a}^\dagger_{S_m} \hat{a}_{W'_n} \rangle = \sqrt{\tau}\,\langle \hat{a}^\dagger_{S_m} \hat{a}_{W_n} \rangle$ for all m, n, where τ is the fraction of Alice's transmission to Bob that is due to her SPDC source. Thus, with Alice and Bob determining their Shannon information from error-probability measurements, and assuming that they can obtain the intrusion parameters $\overline{\kappa}_S$ and $\overline{K}_f$, they have what they need to set a lower bound on the asymptotic-regime, coherent-attack SKE.

Our final task will be to illustrate the behavior of that bound when Eve's attack does not impact Alice and Bob's covariance matrix, so that $\overline{\kappa}_S = \kappa_S$ and $\overline{K}_f = \kappa_S$, and their reconciliation efficiency is perfect, $\beta = 1$ [61].

In this case they have an assured SKE that satisfies

$$\mathrm{SKE} = \max[I_{AB} - M_E\,\chi_E(\kappa_S, \kappa_S), 0]. \tag{36}$$

This SKE is plotted versus one-way path length in Fig. 4(b) for various M_E values with I_{AB} obtained from Alice and Bob's theoretical error probability [14], $G_B = 10^6$, and source brightness, N_S, chosen at each L to maximize SKE. For $M_E = 200$ and $R = 10\,\mathrm{Gbit/s}$, Fig. 4(b) predicts an SKR $= R\,$SKE in excess of $2\,\mathrm{Gbit/s}$ at $L = 50\,\mathrm{km}$, as found for those parameter values in our previous frequency-domain collective attack security analysis [14] with the equivalent of $\overline{\kappa}_S = \kappa_S$, $\overline{K}_f = 0.99\,\kappa_S$, and $\beta = 0.94$.

Figure 4(b) also underscores the value of multi-mode encoding in achieving high SKEs, and hence high bits/s SKRs for a given symbol rate R. All QKD protocols have bits/mode SKRs bounded above by the PLOB bound [18], $-\log_2(1-\kappa_S)$ bits/mode. Figure 4(b)'s single-mode encoding ($M_E = 1$) curve is well *below* that bound, but its $M_E \gg 1$ curves report bits/symbol rates that are well *above* $-\log_2(1-\kappa_S)$. This is why, for the same symbol rate R, FL-QKD can realize much higher bits/s SKRs than the predominant decoy-state BB84 protocol, because the latter employs single-mode encoding and its state-of-the-art implementation [12] has bits/mode performance on par with Fig. 4(b)'s $M_E = 1$ curve at 50 km one-way path length.

V. SUMMARY AND DISCUSSION

In this paper we have taken significant steps toward an asymptotic-regime, coherent-attack security proof for TW-QKD protocols. First, we showed that the noisy entanglement-assisted channel capacity formula [40] provides an upper bound on Eve's information gain from her most general coherent attack. Then, we exhibited covariance-matrix constraints that can provide efficiently calculable bounds on her information gain for Gaussian TW-QKD protocols, and showed that the resulting upper bound can be achieved by a collective attack. Finally, we applied our results to two such protocols, the TMSV protocol [21, 26, 28, 29] and FL-QKD [14–17]. The latter example is especially important, because FL-QKD offers the potential for Gbit/s SKRs over metropolitan-area distances without the need for any new technology but its current security analysis only assures protection against a frequency-domain collective attack [14]. As a result, developing LOCC security tests that will permit Alice and Bob to obtain the intrusion parameters employed in our framework is open problem of great significance. These parameters can, in principle, be obtained from standard homodyne measurements when Eve's attack is collective, rather than coherent, and Alice and Bob's QKD protocol uses single-mode encoding, but a measurement approach that works for coherent attacks on multi-mode encoding is needed. One possibility may be to use the reliable state tomography technique [62]. Note that the pairwise-sum constraint in Eq. (27) is *not* invariant to the basis chosen by Alice and Bob for their modes [63]. But Alice and Bob only need to measure this constraint in a particular basis, to bound Eve's information gain, as long as the mode transformations within Alice and Bob's equipment are described by the channels from Sec. II. The permutation-invariant sum constraint in Eq. (29), on the other hand, *is* invariant to the choice of basis, because it can be written in terms correlations of the continuous-time field operators, $\hat{E}_S(t)$ and $\hat{E}_W(t)$, for Bob's received signal and Alice's purification [63]. Even if one or both of the preceding constraints can be measured, the general composite-security, finite-key analysis for Eve's coherent attack will still need to be worked out for FL-QKD and other Gaussian TW-QKD protocols.

Finally, we must emphasize that our security-proof framework's goal is to establish the *protocol* security of TW-QKD. It does not address such protocols' *implementation* security, i.e., side-channel attacks that exploit device characteristics—including deviations from their normal operating regimes—to compromise key exchange. That said, QKD still offers implementation security that is independent of future technological advances: any attack must be executed with the technology that is available at the time of the key exchange.

ACKNOWLEDGMENTS

QZ, ZZ, and JHS acknowledge support from Air Force Office of Scientific Research Grant No. FA9550-14-1-0052. JHS also acknowledges support from Office of Naval Research Contract No. N00014-16-C-2069, and QZ also acknowledges support from the Claude E. Shannon Research Assistantship. NL acknowledges support by NSERC under the Discovery Program. The Institute for Quantum Computing is supported by the Government of Canada and the Province of Ontario. QZ thanks the Perimeter Institute for its hospitality, Rotem Arnon-Friedman for discussions of entropy accumulation, and Felix Leditzky for discussions.

Appendix A: Proof of Theorem 1

Because Theorem 1 deals with a single mode-pair, we shall omit mode-index superscripts and subscripts and employ the notation from Fig. 1 throughout what follows. Thus our objective is to show that $F(\rho_{SW}) \equiv S(\rho_B) - E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})$, when maximized over states ρ_{SW} satisfying

$$\langle \hat{a}_S^\dagger \hat{a}_S \rangle = \kappa_S N_S, \tag{A1}$$

$$|\,\langle \hat{a}_S \hat{a}_W \rangle\,|^2 + |\,\langle \hat{a}_S^\dagger \hat{a}_W \rangle\,|^2 = \kappa_f C_S^2, \tag{A2}$$

obeys

$$\chi_E(\kappa_S, \kappa_f) = g(N_B) - E^\star_{\Psi^c\otimes\mathcal{I}}(\kappa_S, \kappa_f). \tag{A3}$$

Here, $g(N_B)$ is the von Neumann entropy of a thermal state with average photon number N_B where N_B is given by Eq.(3), and $E^{\star}_{\Psi^c\otimes\mathcal{I}}(\kappa_S,\kappa_f)$ is the entropy gain minimized over the preceding constraints.

Before proceeding with the details, let us outline the structure of the proof. Equations (A1) and (A2) are functions of ρ_{SW}'s covariance matrix $\mathbf{\Lambda}_{SW}$. The subadditivity of $F(\rho_{SW})$ therefore implies that the constrained maximum is achieved by a Gaussian-state ρ_{SW} [40]. Thus we need only consider an eavesdropper's using a Gaussian unitary, namely a $(K+1)$-mode Bogoliubov transformation [41] parameterized by a set of variables. Owing to Eq. (3), $S(\rho_B)$ is bounded above by $g(N_B)$. To complete the proof we need a non-trivial lower bound on $E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW}) = S(\rho_{N'W}) - S(\rho_{SW})$, where N' is the environment mode after Bob's Gaussian channel Ψ. Moreover, to obtain that bound we only need the covariance matrices $\mathbf{\Lambda}_{SW}$ and $\mathbf{\Lambda}_{N'W}$ of ρ_{SW} and $\rho_{N'W}$, which can be found from Alice's $\mathbf{\Lambda}_{YW}$ and the parameters of Eve's Bogoliubov transformation. Then $E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})$ is obtained by a symplectic diagonalization that turns out to depend on only three parameters of the Bogoliubov transformation, given the constraints Eqs. (A1) and (A2). Minimizing over these three parameters yields $E^{\star}_{\Psi^c\otimes\mathcal{I}}(\kappa_S,\kappa_f)$. However, $E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})$'s closed-form expression is rather complicated, which prevents analytical minimization, hence we will rely on numerical minimization. That said, we will use series expansion in the vicinity of $\kappa_f = \kappa_S$ to show that the beam-splitter light injection attack [14] is always a local minimum in that region, wherein Alice and Bob's security testing has severely limited Eve's intrusion.

Proof. Let Eve's Gaussian unitary—her $K+1$-mode Bogoliubov transformation [41]—be,

$$\hat{a}_S = u_0\hat{a}_Y + v_0^*\hat{a}_Y^\dagger + \sum_{k=1}^{K}(u_k\hat{e}_V^{(k)} + v_k^*\hat{e}_V^{(k)\dagger}) + \alpha. \quad \text{(A4)}$$

where $\hat{a}_Y$ is the photon annihilation operator of Alice's Y mode, and $\{\,\hat{e}^{(k)} : 1 \le k \le K\,\}$ are the photon annihilation operators of Eve's ancilla modes, all of which are in their vacuum states. We require Eq. (A4) to yield a proper free-field commutator bracket for $\hat{a}_S$, thus the complex-valued coefficients $\{\,u_k, v_k : 0 \le k \le K\,\}$ must satisfy

$$|u_0|^2 + \mathbf{u}^\dagger\mathbf{u} - |v_0|^2 - \mathbf{v}^\dagger\mathbf{v} = 1, \quad \text{(A5)}$$

where $\mathbf{u}^\dagger = \begin{bmatrix} u_1^* & u_2^* & \cdots & u_K^* \end{bmatrix}$, with † denoting conjugate transpose, and a similar definition for $\mathbf{v}^\dagger$. Equations (A1) and (A2) impose their own restrictions on $\{u_k, v_k, \alpha\}$:

$$|\alpha|^2 + |v_0|^2 + \mathbf{v}^\dagger\mathbf{v} = (\kappa_S - \kappa_f)N_S. \quad \text{(A6)}$$

$$|u_0|^2 + |v_0|^2 = \kappa_f, \quad \text{(A7)}$$

We will maximize $S(\rho_B)$ and minimize $E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})$ separately, and show that they can be achieved simultaneously.

1. Maximizing $S(\rho_B)$

Here we show that Eve's Gaussian unitary with $\alpha = 0$ achieves the constrained maximization of $S(\rho_B)$. Because ρ_B is a displaced thermal state, we know that

$$\max_{\rho_{SW}} S(\rho_B) = g(N_B - |\alpha|^2), \quad \text{(A8)}$$

where N_B is given by Eq. (3) and the $\{u_k, v_k, \alpha\}$ satisfy Eqs. (A5)–(A7), which implies that $\alpha = 0$ maximizes $S(\rho_B)$ under the given constraints. Furthermore, because the entropy-gain term is independent of the displacement α, we have that $\chi_E(\kappa_S,\kappa_f)$ is achieved by $\alpha = 0$.

2. Minimizing $E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})$

Here we perform the constrained minimization,

$$\min_{\rho_{SW}} E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW}) \equiv \min_{\rho_{SW}} S(\rho_{N'W}) - S(\rho_{SW}), \quad \text{(A9)}$$

where $\rho_{N'W} = \Psi^c\otimes\mathcal{I}(\rho_{SW})$ is the joint state of the environment and the purification after Bob's channel Ψ. Because $\rho_{N'W}$ and ρ_{SW} are Gaussian, their entropies are given, in terms of their covariance matrices' symplectic eigenvalues—$\{\nu_\pm\}$ for $\mathbf{\Lambda}_{N'W}$ and $\{\mu_\pm\}$ for $\mathbf{\Lambda}_{SW}$)—which leads to

$$\begin{aligned} E_{\Psi^c\otimes\mathcal{I}}(\rho_{N'W}) = {} & g[(4\nu_+ - 1)/2] + g[(4\nu_- - 1)/2] \\ & - g[(4\mu_+ - 1)/2] - g[(4\mu_- - 1)/2]. \end{aligned} \quad \text{(A10)}$$

where the symplectic eigenvalues must satisfy Eqs. (A5)–(A7) with $\alpha = 0$.

Maximizing Eq. (A10) over the $\{u_k, v_k\}$ is more readily accomplished by rewriting Eqs. (A5)–(A7) in terms of $\{\gamma, \delta, \theta_v, \theta_{uv}\}$ chosen such that

$$u_0 = \sqrt{\kappa_f}\,\sin(\gamma), \quad \text{(A11a)}$$

$$v_0 = \sqrt{\kappa_f}\,\cos(\gamma)e^{i\theta_v}, \quad \text{(A11b)}$$

$$\mathbf{u}^\dagger\mathbf{u} = (\kappa_S - \kappa_f)N_S + 1 - \kappa_f + \kappa_f\cos^2(\gamma), \quad \text{(A11c)}$$

$$\mathbf{v}^\dagger\mathbf{v} = (\kappa_S - \kappa_f)N_S - \kappa_f\cos^2(\gamma), \quad \text{(A11d)}$$

$$\mathbf{v}^\dagger\mathbf{u} = \sqrt{(\mathbf{v}^\dagger\mathbf{v})(\mathbf{u}^\dagger\mathbf{u})}\,\cos(\delta)e^{i\theta_{uv}}. \quad \text{(A11e)}$$

In these expressions: $\gamma \in [0, \pi/2]$ satisfies

$$1 - \frac{1}{\kappa_f} - \left(\frac{\kappa_S}{\kappa_f} - 1\right)N_S \le \cos^2(\gamma) \le \left(\frac{\kappa_S}{\kappa_f} - 1\right)N_S; \quad \text{(A12)}$$

$\delta \in [0, \pi/2]$; and u_0 has been taken to be non-negative, without loss of generality, because global phase is irrelevant.

The foregoing reformulation makes it easy to show that *all* states ρ_{SW} must have κ_S and κ_f, defined by Eqs. (21) and (22), that satisfy

$$0 \le \kappa_f \le \min[\kappa_S, (1 + 2\kappa_S N_S)/(1 + 2N_S)]. \quad \text{(A13)}$$

Specifically: $\kappa_f \geq 0$ follows from its definition in Eq. (22); $\kappa_f \leq \kappa_S$ follows from $(\kappa_S - \kappa_f)N_S = |v_0|^2 + \mathbf{v}^\dagger\mathbf{v} \geq 0$; $\kappa_f \leq (1+2\kappa_S N_S)/(1+2N_S)$ follows from $2(\kappa_S-\kappa_f)N_S + 1 - \kappa_f = \mathbf{u}^\dagger\mathbf{u} + \mathbf{v}^\dagger\mathbf{v} \geq 0$; and the generality of the result is because the κ_f limits apply to the covariance matrix of an arbitrary, not just a Gaussian, ρ_{SW}.

a. *Covariance matrix of $\hat{a}_S$ and $\hat{a}_W$*

Equations (1) and (A4) enable us to show that the covariance of $\hat{a}_S$ and $\hat{a}_W$ is given by

$$\mathbf{\Lambda}_{SW} = \frac{1}{4}\begin{bmatrix} \mathbf{A}_S & \mathbf{C}_{SW} \\ \mathbf{C}_{SW} & \mathbf{A}_W \end{bmatrix}, \tag{A14}$$

where:

$$\mathbf{A}_S = 2\begin{bmatrix} A_S + \mathrm{Re}(w) & \mathrm{Im}(w) \\ \mathrm{Im}(w) & A_S - \mathrm{Re}(w) \end{bmatrix}, \tag{A15}$$

with $A_S = 1/2 + \kappa_S N_S$ and $w = \mathbf{v}^\dagger\mathbf{u} + (2N_S+1)v_0^* u_0$;

$$\mathbf{C}_{SW} = 2C_S \begin{bmatrix} u_0 + \mathrm{Re}(v_0) & \mathrm{Im}(v_0) \\ -\mathrm{Im}(v_0) & -u_0 + \mathrm{Re}(v_0) \end{bmatrix}, \tag{A16}$$

with $C_S = \sqrt{N_S(N_S+1)}$; and $\mathbf{A}_W = (2N_S+1)\mathbf{I}_2$.

b. *Covariance matrix of $\hat{a}'_N$ and $\hat{a}_W$*

Because Bob's encoding, U_X, is covariant with his channel, Ψ, we can omit U_X in calculating $\mathbf{\Lambda}_{N'W}$ for Bob's three channels, i.e., his quantum-limited amplifier channel ($\Psi = \mathcal{A}^0_{G_B}$), his pure-loss channel ($\Psi = \mathcal{L}^0_{\eta_B}$), and his contravariant quantum-limited amplifier channel ($\Psi = \tilde{\mathcal{A}}^0_{G_B}$).

1. Quantum-limited amplifier channel, with $\hat{a}'_N = \sqrt{G_B - 1}\,\hat{a}_S^\dagger + \sqrt{G_B}\,\hat{a}_N$ and $G_B \geq 1$. Here we have that

$$\mathbf{\Lambda}_{N'W} = \frac{1}{4}\begin{bmatrix} \mathbf{A}_{N'} & \mathbf{C}_{N'W} \\ \mathbf{C}_{N'W} & \mathbf{A}_W \end{bmatrix}, \tag{A17}$$

where:

$$\mathbf{A}_{N'} = 2\begin{bmatrix} A' + \mathrm{Re}(x) & -\mathrm{Im}(x) \\ -\mathrm{Im}(x) & A' - \mathrm{Re}(x) \end{bmatrix}, \tag{A18}$$

with $A' = 1/2 + G_B N_B + (G_B - 1)(\kappa_S N_S + 1)$ and $x = (G_B - 1)w$; and

$$\mathbf{C}_{N'W} = 2\sqrt{G_B - 1}\,C_S \times \begin{bmatrix} u_0 + \mathrm{Re}(v_0) & \mathrm{Im}(v_0) \\ \mathrm{Im}(v_0) & u_0 - \mathrm{Re}(v_0) \end{bmatrix}. \tag{A19}$$

2. Pure-loss channel with $\hat{a}'_N = \sqrt{1-\eta_B}\,\hat{a}_S - \sqrt{\eta_B}\,\hat{a}_N$ and $0 \leq \eta_B \leq 1$. Here we find that

$$\mathbf{\Lambda}_{N'W} = \frac{1}{4}\begin{bmatrix} \mathbf{A}'_N & \mathbf{C}_{N'W} \\ \mathbf{C}_{N'W} & \mathbf{A}_W \end{bmatrix}, \tag{A20}$$

where:

$$\mathbf{A}_{N'} = 2\begin{bmatrix} A' + \mathrm{Re}(x) & \mathrm{Im}(x) \\ \mathrm{Im}(x) & A' - \mathrm{Re}(x) \end{bmatrix}, \tag{A21}$$

with $A' = 1/2 + (1-\eta_B)N_S + \eta_B N_B$ and $x = (1-\eta_B)w$; and

$$\mathbf{C}_{N'W} = \sqrt{1-\eta_B}\mathbf{C}_{SW}. \tag{A22}$$

3. Contravariant quantum-limited amplifier channel with $\hat{a}'_N = \sqrt{G_B}\,\hat{a}_S + \sqrt{G_B - 1}\,\hat{a}_N^\dagger$ and $G_B \geq 1$. Now we get

$$\mathbf{\Lambda}_{N'W} = \frac{1}{4}\begin{bmatrix} \mathbf{A}_{N'} & \mathbf{C}_{N'W} \\ \mathbf{C}_{N'W} & \mathbf{A}_W \end{bmatrix}, \tag{A23}$$

where:

$$\mathbf{A}_{N'} = 2\begin{bmatrix} A' + \mathrm{Re}(x) & \mathrm{Im}(x) \\ \mathrm{Im}(x) & A' - \mathrm{Re}(x) \end{bmatrix}, \tag{A24}$$

with $A' = 1/2 + G_B\kappa_S N_S + (G_B - 1)(N_B + 1)$ and $x = G_B w$; and

$$\mathbf{C}_{N'W} = \sqrt{G_B}\,\mathbf{C}_{SW}. \tag{A25}$$

c. *Minimization over $\gamma, \delta, \theta_v, \theta_{uv}$*

With $\mathbf{\Lambda}_{SW}$ and $\mathbf{\Lambda}_{N'W}$ in hand, it is straightforward to obtain the symplectic eigenvalues $\nu_\pm$ and $\mu_\pm$, from which we get $E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})$ using Eq. (A10). The only parameters to be optimized over in minimizing $E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})$ are then $\gamma, \delta, \theta_v, \theta_{uv}$, because the κ_S and κ_f constraints and are implicit in Eqs. (A11). At this point it is convenient to make two further parameter changes. First, we introduce ζ such that $\cos(\gamma) = \sqrt{(\kappa_S - \kappa_f)N_S/\kappa_f}\,\cos(\zeta)$ with $\cos^2(\zeta) \leq \kappa_f/(\kappa_S - \kappa_f)N_S$, and second, we define $\xi = \theta_v + \theta_{uv}$. Then, because the $\{\nu_\pm, \mu_\pm\}$ only depend on γ, δ, and $\theta_v + \theta_{uv}$, we have reduced our task to minimizing a closed-form $E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})$ expression over the choice of three parameters: $\zeta \in [0, \pi/2], \delta \in [0, \pi/2]$, and $\xi \in [-\pi, \pi]$.

For $\mathcal{A}^0_{G_B}$, $\mathcal{L}^0_{\eta_B}$, and $\tilde{\mathcal{A}}^0_{G_B}$ we find that the only solution to $\partial_\zeta E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW}) = \partial_\delta E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW}) = \partial_\xi E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW}) = 0$ is $\zeta = \delta = \pi/2$ (corresponding to $\gamma = \delta = \pi/2$), at which point $\xi = \theta_v + \theta_{uv}$ can be arbitrary. For $\kappa_f \leq (1 + \kappa_S N_S)/(1 + N_S)$, one can verify numerically that $\gamma = \delta = \pi/2$ is indeed the global

FIG. 5. Numerically-obtained entropy-gain minimization results for the quantum-limited amplifier channel with $N_S = 0.1$ and $G_B = 1.5$. (a) Minimum entropy gain, $E^{\star}_{\Psi^c\otimes\mathcal{I}}(\kappa_S, \kappa_f)$. (b) Optimum δ value. (c) Optimum γ value. In (b) and (c) the green line, $\kappa_f = (1 + 2\kappa_S N_S)/(1 + 2N_S)$, and the gray line, $\kappa_f = \kappa_S$, mark the (A13) upper limit on possible κ_f values, and the red line, $\kappa_f = (1 + \kappa_S N_S)/(1 + N_S)$, is the κ_f value below which the local minimum at $\gamma = \delta = \pi/2$ is also the global minimum.

FIG. 6. Numerically-obtained entropy-gain minimization results for the pure-loss channel with $N_S = 0.1$ and $\eta_B = 0.2$. (a) Minimum entropy gain, $E^{\star}_{\Psi^c\otimes\mathcal{I}}(\kappa_S, \kappa_f)$. (b) Optimum δ value. (c) Optimum γ value. In (b) and (c) the green line, $\kappa_f = (1 + 2\kappa_S N_S)/(1 + 2N_S)$, and the gray line, $\kappa_f = \kappa_S$, mark the (A13) upper limit on possible κ_f values, and the red line, $\kappa_f = (1 + \kappa_S N_S)/(1 + N_S)$, is the κ_f value below which the local minimum at $\gamma = \delta = \pi/2$ is also the global minimum for sufficiently small κ_S.

minimum of $E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})$ for the $\mathcal{A}^0_{G_B}$ and $\tilde{\mathcal{A}}^0_{G_B}$ channels. The situation is more complicated for the $\mathcal{L}^0_{\eta_B}$ channel, because for this channel there is a parameter region in which the global minimum is not achieved at the stationary point (local minimum). However, the convexity of $E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})$ with respect to κ_S and κ_f—see Fig. 8, below—combined with Alice and Bob's choosing $\kappa_S \leq 1$ for QKD, leads to the pure-loss channel's minimum $E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})$ being at its stationary point.

Figures 5–7 present numerically-obtained $E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})$ minimization results for the $\mathcal{A}^0_{G_B}$ channel (with $N_S = 0.1$ and $G_B = 1.5$), the $\mathcal{L}^0_{\eta_B}$ channel (with $N_S = 0.1$ and $\eta_B = 0.2$), and $\tilde{\mathcal{A}}^0_{G_B}$ channel (with $N_S = 0.1$ and $G_B = 1.5$), respectively. Plotted versus κ_S and κ_f in each figure are: (a) $E^{\star}_{\Psi^c\otimes\mathcal{I}}(\kappa_S, \kappa_f) = \min_{\rho_{SW}} E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})$, (b) the optimum δ value, and (c) the optimum γ value. The green line, $\kappa_f = (1 + 2\kappa_S N_S)/(1 + 2N_S)$, and the gray line, $\kappa_f = \kappa_S$, in (b) and (c) mark the (A13) upper limit on possible κ_f values. The red line, $\kappa_f = (1 + \kappa_S N_S)/(1 + N_S)$, in (b) and (c) is the κ_f value below which the local minimum at $\gamma = \delta = \pi/2$ is also the global minimum for the amplifier channels, and for the pure-loss channel when κ_S is sufficiently small (a region that includes $\kappa_S \leq 1$, as noted earlier).

Although Figs. 5–7 only provide information about one set of N_S, G_B and η_B values, the behaviors shown in these figures are generic. Indeed, we have verified that this is for $G_B = 10, 100$, and, by asymptotic expansions, for $G_B \gg 1$ and $N_S \ll 1$. Furthermore, the asymptotic results allow us to show that the beam-splitter active injection attack achieves $E^{\star}_{\Psi^c\otimes\mathcal{I}}(\kappa_S, \kappa_f)$ when $G_B \gg 1$ and $N_S \ll 1$.

FIG. 7. Numerically-obtained entropy-gain minimization results for the complementary quantum-limited amplifier channel with $N_S = 0.1$ and $G_B = 1.5$. (a) Minimum entropy gain, $E^{\star}_{\Psi^c\otimes\mathcal{I}}(\kappa_S, \kappa_f)$. (b) Optimum δ value. (c) Optimum γ value. In (b) and (c) the green line, $\kappa_f = (1 + 2\kappa_S N_S)/(1 + 2N_S)$, and the gray line, $\kappa_f = \kappa_S$, mark the (A13) upper limit on possible κ_f values, and the red line, $\kappa_f = (1 + \kappa_S N_S)/(1 + N_S)$, is the κ_f value below which the local minimum at $\gamma = \delta = \pi/2$ is also the global minimum.

d. *Asymptotic results*

The closed-form expression for $E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})$ as a function of ζ, δ and ξ is complicated, preventing us from minimizing it analytically. That is not the case, however, when $\kappa_f \simeq \kappa_S$. Physically, this corresponds to Alice and Bob's security testing confining Eve's attack to the low-intrusion regime, e.g., when Eve limits herself to a passive attack in which she only interacts with light that is lost in propagation between Alice and Bob and between Bob and Alice. For this low-intrusion regime let us write κ_f as

$$\kappa_f = (1 - f_E)\kappa_S, \tag{A26}$$

where $0 \leq f_E \ll 1$ is a function of the attack parameters ζ, δ and ξ, and then evaluate $E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})$ to first order in f_E, viz.,

$$\begin{aligned} E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW}) = {} & E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})|_{f_E=0} \\ & + (\partial_{f_E} E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})|_{f_E=0}) f_E + O(f_E^2). \end{aligned} \tag{A27}$$

It turns out that the zeroth-order term is independent of ζ, δ, and ξ. Thus, Eve's optimum ζ, δ and ξ values when $0 \leq f_E \ll 1$ are given by

$$\arg\min_{\zeta,\delta,\xi} \partial_{f_E} E_{\Psi^c\otimes\mathcal{I}}(\rho_{SW})|_{f_E=0}, \tag{A28}$$

and using those values in Eq. (A27) will then yield $E^{\star}_{\Psi^c\otimes\mathcal{I}}(\kappa_S, \kappa_f)$ to first order in f_E.

Note that from (A13) and (A26), we have that $\kappa_S \leq 1/[1 - (1 + 2N_S)f_E]$, whence

$$\mu_-|_{f_E=0} = 1, \tag{A29}$$
$$\mu_+|_{f_E=0} = 1 + 2(1 - \kappa_S)N_S > 1. \tag{A30}$$

So, to complete our asymptotic analysis, we need only find the symplectic eigenvalues, $\nu_\pm|_{f_E=0}$, for Bob's three possible channels.

1. For pure-loss channel, $\mathcal{L}^0_{\eta_B}$, we find that

$$\nu_-|_{f_E=0} = 1, \tag{A31}$$
$$\nu_+|_{f_E=0} = 1 + 2[1 - \kappa_S(1 - \eta_B)]N_S > 1. \tag{A32}$$

Applying $\lim_{x\to 0} \partial_x g(x) = \infty$ to Eq. (A10), we see that it suffices to consider

$$\min_{\zeta,\delta,\xi} \partial_{f_E}(\nu_- - \mu_-)|_{f_E=0}, \tag{A33}$$

to obtain $E^{\star}_{\Psi^c\otimes\mathcal{I}}(\kappa_S, \kappa_f)$, The minimization in (A33) can be done analytically, giving the result $\zeta = \delta = \pi/2$.

2. For $G_B > 1$, both quantum-limited amplifier, $\mathcal{A}^0_{G_B}$, and its complementary channel, $\tilde{\mathcal{A}}^0_{G_B}$, have $\nu_+|_{f_E=0} > \nu_-|_{f_E=0} > 1$. Thus to obtain $E^{\star}_{\Psi^c\otimes\mathcal{I}}(\kappa_S, \kappa_f)$, it suffices to consider

$$\min_{\zeta,\delta,\xi} \partial_{f_E}(-\mu_-)|_{f_E=0}. \tag{A34}$$

The minimization in (A34) can be done analytically, giving the result $\zeta = \delta = \pi/2$.

e. *Optimum attack*

At $\zeta = \delta = \pi/2$, we have

$$u_0 = \sqrt{\kappa_f}, \tag{A35a}$$
$$v_0 = 0, \tag{A35b}$$
$$\mathbf{u}^\dagger\mathbf{u} = (\kappa_S - \kappa_f)N_S + 1 - \kappa_f, \tag{A35c}$$
$$\mathbf{v}^\dagger\mathbf{v} = (\kappa_S - \kappa_f)N_S, \tag{A35d}$$
$$\mathbf{v}^\dagger\mathbf{u} = 0, \tag{A35e}$$

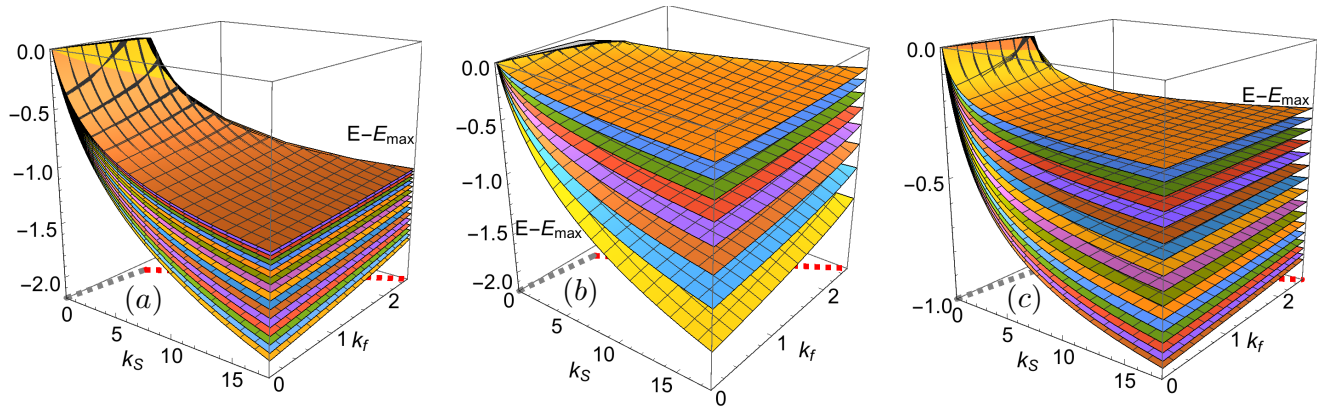

FIG. 8. Plots of $E - E_{\max}$ versus κ_S and κ_f for $N_S = 0.1$, with $E \equiv E^{\star}_{\Psi^{c}\otimes\mathcal{I}}(\kappa_S, \kappa_f)$ and $E_{\max} \equiv \max_{\kappa_S,\kappa_f} E^{\star}_{\Psi^{c}\otimes\mathcal{I}}(\kappa_S, \kappa_f)$. (a) Quantum-limited amplifier channel with, from bottom to top, $\log_{10}(G_B - 1)$ increasing from -1 to 0.5 in 0.1 increments. (b) Pure-loss channel with, from top to bottom, η_B increasing from 0.2 to 1 in 0.1 increments. (c) Contravariant quantum-limited amplifier channel with, from bottom to top, $\log_{10}(G_B - 1)$ increasing from -1 to 0.5 in 0.1 increments. In (a)–(c), the gray line, $\kappa_f = \kappa_S$, marks part of the (A13) upper limit on possible κ_f values, and the red line, $\kappa_f = (1 + \kappa_S N_S)/(1 + N_S)$, is the κ_f value below which the entropy-gain's local minimum at $\gamma = \delta = \pi/2$ is also its global minimum.

which are the parameter values of the beam-splitter injection attack considered in the Ref. [14]. With the optimum parameters given by Eqs. (A35), we can evaluate $E^{\star}_{\Psi^{c}\otimes\mathcal{I}}(\kappa_S, \kappa_f)$ via Eq. (A10). Combined with $\max_{\rho_{SW}} = S(\rho_B)$, we obtain $\chi_E(\kappa_S, \kappa_f)$ in Eq. (25).

In particular, the covariance matrix, $\mathbf{\Lambda}^{\star}_{SW}$, of the optimum input state, $\rho^{\star}_{SW}$, is

$$\mathbf{\Lambda}^{\star}_{SW} = \frac{1}{4}\begin{bmatrix} (1 + 2\kappa_S N_S)\mathbf{I}_2 & \sqrt{k_f}\,\mathbf{C}_{YW} \\ \sqrt{k_f}\mathbf{C}_{YW} & \mathbf{A}_W \end{bmatrix}, \tag{A36}$$

with symplectic eigenvalues $\mu^{\star}_{\pm}$. The optimum output state, $\rho^{\star}_{N'W}$ and its covariance matrix, $\mathbf{\Lambda}^{\star}_{N'W}$ depend on which channel Bob employs.

1. For the $\mathcal{A}^{0}_{G_B}$ channel, we get

$$\mathbf{\Lambda}^{\star}_{N'W} = \frac{1}{4}\begin{bmatrix} \mathbf{A}^{\star}_{N'} & \sqrt{k_f(G_B - 1)}\,\mathbf{C}_{YW} \\ \sqrt{k_f(G_B - 1)}\,\mathbf{C}_{YW} & \end{bmatrix}, \tag{A37}$$

with $\mathbf{A}^{\star}_{N'} = [1 + 2(G_B - 1)(1 + \kappa_S N_S)]\mathbf{I}_2$.

2. For the $\mathcal{L}^{0}_{\eta_B}$ channel, we get

$$\mathbf{\Lambda}^{\star}_{N'W} = \frac{1}{4}\begin{bmatrix} [1 + 2(1 - \eta_B)\kappa_S N_S]\mathbf{I}_2 & \sqrt{k_f(1 - \eta_B)}\,\mathbf{C}_{YW} \\ \sqrt{k_f(1 - \eta_B)}\,\mathbf{C}_{YW} & \mathbf{A}_W \end{bmatrix}. \tag{A38}$$

3. For the $\tilde{\mathcal{A}}^{0}_{G_B}$ channel, we get

$$\mathbf{\Lambda}^{\star}_{N'W} = \frac{1}{4}\begin{bmatrix} -1 + 2G_B[1 + 2(1 + \kappa_S N_S)]\mathbf{I}_2 & \sqrt{G_B k_f}\,\mathbf{C}_{YW} \\ \sqrt{G_B k_f}\,\mathbf{C}_{YW} & \mathbf{A}_W \end{bmatrix}. \tag{A39}$$

With $\nu^{\star}_{\pm}$ denoting the symplectic eigenvalues of $\mathbf{\Lambda}^{\star}_{N'W}$, we have that ,

$$\chi_E(\kappa_S, \kappa_f) = g(N_B) - E^{\star}_{\Psi^{c}\otimes\mathcal{I}}(\kappa_S, \kappa_f), \tag{A40}$$

with

$$E^{\star}_{\Psi^{c}\otimes\mathcal{I}}(\kappa_S, \kappa_f) = g[(4\nu^{\star}_{+} - 1)/2] + g[(4\nu^{\star}_{-} - 1)/2] - g[(4\mu^{\star}_{+} - 1)/2] - g[(4\mu^{\star}_{-} - 1)/2]. \tag{A41}$$

■

We complete this section by presenting our numerical verification, shown in Fig. 8, that $E^{\star}_{\Psi^{c}\otimes\mathcal{I}}(\kappa_S, \kappa_f)$ is convex, where, for better visualization, we have plotted $E - E_{\max}$ with $E \equiv E^{\star}_{\Psi^{c}\otimes\mathcal{I}}(\kappa_S, \kappa_f)$ and $E_{\max} \equiv \max_{\kappa_S,\kappa_f} E^{\star}_{\Psi^{c}\otimes\mathcal{I}}(\kappa_S, \kappa_f)$. Although these plots assume $N_S = 0.1$, we have verified that similar behaviors prevail at other N_S values of interest.

Appendix B: Proof of Theorem 2

Our proof uses the fact that performing arbitrary local unitaries on the $\boldsymbol{W}$ modes preserves $F(\rho_{S_m\boldsymbol{W}})$. In particular, we have the following lemma; see Appendix C for its proof.

Lemma 3 *For the Eq. (31) constraint, i.e.,*

$$\sum_{n=1}^{M}\left[|\langle \hat{a}_{S_m}\hat{a}_{W_n}\rangle|^2 + |\langle \hat{a}^{\dagger}_{S_m}\hat{a}_{W_n}\rangle|^2\right] = K_f^{(m)}C_S^2, \tag{B1}$$

we can apply beam-splitter unitaries to the $\boldsymbol{W}$ modes that result in output modes $\tilde{\boldsymbol{W}}$ modes that reduce Eq. (B1) to

$$|\langle \hat{a}_{S_m}\hat{a}_{\tilde{W}_1}\rangle|^2 + |\langle \hat{a}^{\dagger}_{S_m}\hat{a}_{\tilde{W}_1}\rangle|^2 + |\langle \hat{a}_{S_m}\hat{a}_{\tilde{W}_2}\rangle|^2 = K_f^{(m)}C_S^2. \tag{B2}$$

In what follows we shall omit the tildes on the preceding output modes. Bear in mind that the beam-splitter unitaries that we are using for this proof are a *conceptual* tool, i.e., they do *not* need to be implemented in the TW-QKD system.

With Lemma 3 in hand, we will maximize $F(\rho_{S_m \boldsymbol{W}})$ over the reduced density operator ρ_{S,W_1,W_2} subject to the constraints from Eq. (21),

$$\langle \hat{a}^\dagger_{S_m} \hat{a}_{S_m} \rangle = \kappa_S^{(m)} N_S, , \tag{B3}$$

and (B2), to obtain

$$\chi'_E\left(\kappa_S^{(m)}, K_f^{(m)}\right) = \max_{\rho_{S_m W_1 W_2}} [S(\rho_B) - E_{\Psi^c \otimes \mathcal{I}}(\rho_{S_m W_1 W_2})]. \tag{B4}$$

It can be shown that the $\boldsymbol{W}$ modes which emerge from Lemma 3's beam-splitter unitaries are still in independent, identically-distributed thermal states with average photon number N_S. Also, Ref. [40]'s subadditivity result implies we need only consider $\rho_{S_m W_1 W_2}$ that are Gaussian. Hence our goal for completing Theorem 2's proof is maximizing Eq. (B4) for Gaussian $\rho_{S_m W_1 W_2}$ that obey Eqs. (B2) and (B3). In the rest of the proof, which is similar to what we did in Appendix A, we will omit the m subscripts and superscripts and use S, W_1, W_2 to denote the three modes under consideration.

To begin, we note that the $S(\rho_B)$ maximization from Appendix A 1 applies in the present circumstances, i.e., $\max_{\rho_{S W_1 W_2}} S(\rho_B) = g(N_B)$, and this maximum is achieved by having $\langle \hat{a}_S \rangle = 0$. The optimum Gaussian state $\rho_{S W_1 W_2}$ is therefore zero-mean with $\langle \hat{a}^\dagger_S \hat{a}_S \rangle = \kappa_S N_S$, $\langle \hat{a}^\dagger_{W_1} \hat{a}_{W_1} \rangle = \langle \hat{a}^\dagger_{W_2} \hat{a}_{W_2} \rangle = N_S$, and $\langle \hat{a}^\dagger_{W_1} \hat{a}_{W_2} \rangle = \langle \hat{a}_{W_1} \hat{a}_{W_2} \rangle = 0$, so four additional complex-valued parameters, $\langle \hat{a}^2_S \rangle$, $\langle \hat{a}_S \hat{a}_{W_1} \rangle$, $\langle \hat{a}^\dagger_S \hat{a}_{W_1} \rangle$, $\langle \hat{a}_S \hat{a}_{W_2} \rangle$—equivalently eight real parameters—complete its characterization.

Now, by appropriate phase shifts of the S, W_1 and W_2 modes—which will not affect the entropy-gain term—we can assume that

$$\langle \hat{a}^2_S \rangle = c_1 \geq 0, \text{ where } c_1 \leq \kappa_S N_S, \tag{B5}$$

$$\langle \hat{a}_S \hat{a}_{W_1} \rangle = a_1 \geq 0, \tag{B6}$$

$$\langle \hat{a}^\dagger_S \hat{a}_{W_1} \rangle = b_1 e^{i\theta}, \text{ where } b_1 \geq 0, \theta \in [0, 2\pi), \tag{B7}$$

$$\langle \hat{a}_S \hat{a}_{W_2} \rangle = a_2 \geq 0. \tag{B8}$$

Consequently, the entropy-gain minimization,

$$\min_{\rho_{S W_1 W_2}} E_{\Psi^c \otimes \mathcal{I}}(\rho_{S W_1 W_2}) = \min_{\rho_{S W_1 W_2}} [S(\rho_{N' W_1 W_2}) - S(\rho_{S W_1 W_2})], \tag{B9}$$

will only involve five parameters, $\{c_1, a_1, b_1, \theta, a_2\}$, of which only four are independent, because Eq. (B2) implies that

$$a_1^2 + b_1^2 + a_2^2 = K_f C_S^2. \tag{B10}$$

Furthermore, with $\{\nu_k : 1 \leq k \leq 3\}$ and $\{\mu_k : 1 \leq k \leq 3\}$ being the symplectic eigenvalues of the covariance matrices $\boldsymbol{\Lambda}_{S W_1 W_2}$ and $\boldsymbol{\Lambda}_{N' W_1 W_2}$, we have that

$$E_{\Psi^c \otimes \mathcal{I}}(\rho_{S W_1 W_2}) = \sum_{k=1}^{3} \{g[(4\nu_k - 1)/2] - g[(4\mu_k - 1)/2]\}. \tag{B11}$$

The covariance matrices that we need are given as follows. For $\boldsymbol{\Lambda}_{S W_1 W_2}$ we have that

$$\boldsymbol{\Lambda}_{S W_1 W_2} = \frac{1}{4} \begin{bmatrix} \mathbf{A}_S & \mathbf{C}_{S W_1} & \mathbf{C}_{S W_2} \\ \mathbf{C}_{S W_1} & \mathbf{A}_W & \mathbf{0} \\ \mathbf{C}_{S W_2} & \mathbf{0} & \mathbf{A}_W \end{bmatrix}, \tag{B12}$$

where

$$\mathbf{A}_S = \begin{bmatrix} 1 + 2(\kappa_S N_S + c_1) & 0 \\ 0 & 1 + 2(\kappa_S N_S - c_1) \end{bmatrix}, \tag{B13}$$

$$\mathbf{C}_{S W_1} = 2 \begin{bmatrix} a_1 + b_1 \cos\theta & b_1 \sin\theta \\ b_1 \sin\theta & -a_1 + b_1 \cos\theta \end{bmatrix}, \tag{B14}$$

$\mathbf{C}_{S W_2} = 2 a_2 \, \mathrm{Diag}[1, -1]$, and $\mathbf{A}_W = (2N_S + 1)\mathbf{I}_2$. For $\boldsymbol{\Lambda}_{N' W_1 W_2}$, however, we need expressions for each of Bob's three channels.

1. For the $\mathcal{A}^0_{G_B}$ channel, we get

$$\boldsymbol{\Lambda}_{N' W_1 W_2} = \frac{1}{4} \begin{bmatrix} \mathbf{A}_{N'} & \mathbf{C}_{N' W_1} & \mathbf{C}_{N' W_2} \\ \mathbf{C}_{N' W_1} & \mathbf{A}_W & \mathbf{0} \\ \mathbf{C}_{N' W_2} & \mathbf{0} & \mathbf{A}_W \end{bmatrix}, \tag{B15}$$

where

$$\mathbf{A}_{N'} = \begin{bmatrix} 1 + 2x_{N'+} & 0 \\ 0 & 1 + 2x_{N'-} \end{bmatrix}, \tag{B16}$$

with $x_{N'\pm} = (G_B - 1)(1 + \kappa_S N_S \pm c_1)$,

$$\mathbf{C}_{N' W_1} = 2\sqrt{G_B - 1} \begin{bmatrix} a_1 + b_1 \cos\theta & b_1 \sin\theta \\ -b_1 \sin\theta & a_1 - b_1 \cos\theta \end{bmatrix}, \tag{B17}$$

and $\mathbf{C}_{N' W_2} = 2\sqrt{G_B - 1}\, a_2 \, \mathrm{Diag}[1, 1]$.

2. For the $\mathcal{L}^0_{\eta_B}$ channel, we get

$$\boldsymbol{\Lambda}_{N' W_1 W_2} = \frac{1}{4} \begin{bmatrix} \mathbf{A}_{N'} & \mathbf{C}_{N' W_1} & \mathbf{C}_{N' W_2} \\ \mathbf{C}_{N' W_1} & \mathbf{A}_W & \mathbf{0} \\ \mathbf{C}_{N' W_2} & \mathbf{0} & \mathbf{A}_W \end{bmatrix}, \tag{B18}$$

where

$$\mathbf{A}_{N'} = \begin{bmatrix} 1 + 2x_{N'+} & 0 \\ 0 & 1 + 2x_{N'-} \end{bmatrix}, \tag{B19}$$

with $x_{N\pm} = (1 - \eta_B)(\kappa_S N_S \pm c_1)$, $\mathbf{C}_{N' W_1} = \sqrt{1 - \eta_B}\, \mathbf{C}_{S W_1}$, and $\mathbf{C}_{N' W_2} = \sqrt{1 - \eta_B}\, \mathbf{C}_{S W_2}$

3. For the $\tilde{\mathcal{A}}^{0}_{G_B}$ channel, we get

$$\mathbf{\Lambda}_{N'W_1W_2} = \frac{1}{4}\begin{bmatrix} \mathbf{A}_{N'} & \mathbf{C}_{N'W_1} & \mathbf{C}_{N'W_2} \\ \mathbf{C}_{N'W_1} & \mathbf{A}_{W} & \mathbf{0} \\ \mathbf{C}_{N'W_2} & \mathbf{0} & \mathbf{A}_{W} \end{bmatrix}, \tag{B20}$$

where

$$\mathbf{A}_{N'} = \begin{bmatrix} -1+2x_{N'+} & 0 \\ 0 & -1+2x_{N'-} \end{bmatrix}, \tag{B21}$$

with $x_{N'\pm} = G_B(1+\kappa_S N_S \pm c_1)$, $\mathbf{C}_{N'W_1} = \sqrt{G_B}\,\mathbf{C}_{SW_1}$, and $\mathbf{C}_{N'W_2} = \sqrt{G_B}\,\mathbf{C}_{SW_2}$

At this point it is possible—for all three of Bob's channels—obtain closed-form expressions for the entropy gain that are functions of $\{c_1, a_1, b_1, \theta, a_2\}$. In principle, these expressions can be minimized, subject to Eq. (B10), but in practice they are too complicated for that to be done analytically. Numerical minimization can be done, however, for which transforming to

$$c_1 = \kappa_S N_S \cos^2(\tau_r), \tag{B22}$$

$$a_1 = \sqrt{K_f}\, C_S \cos(\tau_1), \tag{B23}$$

$$b_1 = \sqrt{K_f}\, C_S \sin(t_1)\cos(\tau_2), \tag{B24}$$

$$a_2 = \sqrt{K_f}\, C_S \sin(t_1)\sin(\tau_2), \tag{B25}$$

with $\tau_r \in [0,\pi/2]$, $\tau_1 \in [0,\pi/2]$, and $\tau_2 \in [0,\pi]$, automatically ensures that Eq. (B10) is satisfied, and reduces the entropy gain's numerical minimization to a four-dimensional optimization.

The preceding analysis completes the proof of Theorem 2 modulo our proving Lemma 3, which we accomplish in Appendix C.

Appendix C: Proof of Lemma 3

Proof. Our objective is to show that a collection of beam-splitter unitaries involving the $\boldsymbol{W}$ modes can reduce Eq. (B1) to Eq. (B2). We begin by showing how to eliminate the undesired phase-insensitive cross correlations, i.e., the $\langle \hat{a}^{\dagger}_{S_m}\hat{a}_{W_n}\rangle\}$ for $2 \le n \le M$. First, we apply phase shifts to the $\boldsymbol{W}$ modes so that all $\langle \hat{a}^{\dagger}_{S_m}\hat{a}_{W_n}\rangle\} \ge 0$ for $1 \le n \le M$, with $\langle \hat{a}^{\dagger}_{S_m}\hat{a}_{W_1}\rangle > 0$ [64]. Next, starting with $n = 2$ and continuing until $n = M$, we use beam splitters to effect the following transformations,

$$\begin{aligned} \hat{a}^{(n)}_{W_1} &= \sqrt{1-\eta_n}\,\hat{a}^{(n-1)}_{W_1} + \sqrt{\eta_n}\,\hat{a}_{W_n}, \\ \hat{a}'_{W_n} &= \sqrt{\eta_n}\,\hat{a}^{(n-1)}_{W_1} - \sqrt{1-\eta_n}\,\hat{a}_{W_n}, \end{aligned} \tag{C1}$$

with

$$\eta_n \equiv \frac{\langle \hat{a}^{\dagger}_{S_m}\hat{a}_{W_n}\rangle^2}{\langle \hat{a}^{\dagger}_{S_m}\hat{a}^{(n-1)}_{W_1}\rangle^2 + \langle \hat{a}^{\dagger}_{S_m}\hat{a}_{W_n}\rangle^2}, \tag{C2}$$

where $\hat{a}^{(1)}_{W_1} \equiv \hat{a}_{W_1}$ is the W_1 mode's initial photon-annihilation operator, and $\hat{a}'_{W_n}$, for $2 \le n \le M$, is the W_n mode's photon annihilation operator *after* its beam-splitter transformation. For $2 \le n \le M$, it is easily verified that this process results in

$$\begin{aligned} \langle \hat{a}^{\dagger}_{S_m}\hat{a}^{(n)}_{W_1}\rangle &= \sqrt{\langle \hat{a}^{\dagger}_{S_m}\hat{a}^{(n-1)}_{W_1}\rangle^2 + \langle \hat{a}^{\dagger}_{S_m}\hat{a}_{W_n}\rangle^2}, \\ \langle \hat{a}^{\dagger}_{S_m}\hat{a}'_{W_n}\rangle &= 0. \end{aligned} \tag{C3}$$

Collapsing this iteration into a single formula gives us our desired result,

$$\begin{aligned} \langle \hat{a}^{\dagger}_{S_m}\hat{a}^{(M)}_{W_1}\rangle &= \sqrt{\sum_{n=1}^{M}\langle \hat{a}^{\dagger}_{S_m}\hat{a}_{W_n}\rangle^2}, \\ \langle \hat{a}^{\dagger}_{S_m}\hat{a}'_{W_n}\rangle &= 0, \quad \text{for } 2 \le n \le M. \end{aligned} \tag{C4}$$

It is also straightforward to obtain expressions for $\langle \hat{a}_{S_m}\hat{a}^{(M)}_{W_1}\rangle$ and $\{\langle \hat{a}_{S_m}\hat{a}'_{W_n}\rangle : 2 \le n \le M\}$, all of which, in general, will be nonzero. To suppress the unwanted phase-sensitive cross correlations, we parallel what we just did for the phase-insensitive case.

First, we apply phase shifts to $\{\hat{a}'_{W_n} : 2 \le n \le M\}$ so that all $\langle \hat{a}_{S_m}\hat{a}'_{W_n}\rangle \ge 0$ for $2 \le n \le M$, with $\langle \hat{a}_{S_m}\hat{a}'_{W_2}\rangle > 0$ [63]. Next, starting with $n = 3$ and continuing until $n = M$, we use beam splitters to effect the following transformations,

$$\begin{aligned} \hat{a}'^{(n)}_{W_2} &= \sqrt{1-\eta'_n}\,\hat{a}'^{(n-1)}_{W_2} + \sqrt{\eta_n}\,\hat{a}'_{W_n}, \\ \hat{a}''_{W_n} &= \sqrt{\eta'_n}\,\hat{a}'^{(n-1)}_{W_2} - \sqrt{1-\eta'_n}\,\hat{a}'_{W_n}, \end{aligned} \tag{C5}$$

with

$$\eta'_n \equiv \frac{\langle \hat{a}_{S_m}\hat{a}'_{W_n}\rangle^2}{\langle \hat{a}_{S_m}\hat{a}'^{(n-1)}_{W_2}\rangle^2 + \langle \hat{a}_{S_m}\hat{a}'_{W_n}\rangle^2}, \tag{C6}$$

where $\hat{a}'^{(2)}_{W_2} \equiv \hat{a}'_{W_2}$ is the W'_2 mode's initial photon-annihilation operator, and $\hat{a}''_{W_n}$, for $3 \le n \le M$, is the W'_n mode's photon annihilation operator *after* its beam-splitter transformation. For $3 \le n \le M$, it is easily verified that this process results in

$$\begin{aligned} \langle \hat{a}_{S_m}\hat{a}'^{(n)}_{W_2}\rangle &= \sqrt{\langle \hat{a}_{S_m}\hat{a}'^{(n-1)}_{W_2}\rangle^2 + \langle \hat{a}_{S_m}\hat{a}'_{W_n}\rangle^2}, \\ \langle \hat{a}_{S_m}\hat{a}''_{W_n}\rangle &= 0. \end{aligned} \tag{C7}$$

Finally, because the beam-splitter transformations pre-

serve total correlations, we have that

$$\sum_{n=1}^{M} |\langle \hat{a}_{S_m} \hat{a}_{W_n} \rangle|^2$$

$$= |\langle \hat{a}_{S_m} \hat{a}^{(M)}_{W_1} \rangle|^2 + \sum_{n=2}^{M} |\langle \hat{a}_{S_m} \hat{a}'_{W_n} \rangle|^2 \tag{C8}$$

$$= |\langle \hat{a}_{S_m} \hat{a}^{(M)}_{W_1} \rangle|^2 + |\langle \hat{a}_{S_m} \hat{a}'^{(M)}_{W_2} \rangle|^2 + \sum_{n=3}^{M} |\langle \hat{a}_{S_m} \hat{a}''_{W_n} \rangle|^2$$

$$= |\langle \hat{a}_{S_m} \hat{a}^{(M)}_{W_1} \rangle|^2 + |\langle \hat{a}_{S_m} \hat{a}'^{(M)}_{W_2} \rangle|^2, \tag{C9}$$

where we used Eq. (C7) in Eq. (C9). Combining Eq. (C4) and Eq. (C9), we complete the proof. ■

[1] https://www.top500.org/statistics/perfdevel/.

[2] D. Castelvecchi, *Quantum Computers Ready To Leap Out Of The Lab In 2017*, Nature **541**, 9 (2017).

[3] I. L. Chuang, L. M. Vandersypen, X. Zhou, D. W. Leung, and S. Lloyd, *Experimental Realization Of A Quantum Algorithm*, Nature **393**, 143 (1998).

[4] L. M. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, *Experimental Realization Of Shor's Quantum Factoring Algorithm Using Nuclear Magnetic Resonance*, Nature **414**, 883 (2001).

[5] R. L. Rivest, A. Shamir, and L. Adleman, *A Method For Obtaining Digital Signatures And Public-Key Cryptosystems*, Commun. ACM **21**, 120 (1978).

[6] N. Koblitz, *Elliptic Curve Cryptosystems*, Math. of Comput. **48**, 203 (1987).

[7] V. S. Miller, in *Conference on the theory and application of cryptographic techniques* (Springer, 1985) pp. 417–426.

[8] D. J. Bernstein, in D. J. Bernstein, J. Buchmann, and E. Dahman, eds., *Post-Quantum Cryptography* (Springer, Berlin, 2009) pp. 1–14.

[9] P. Shor, *Polynomial-Time Algorithms For Prime Factorization And Discrete Logarithms On A Quantum Computer*, SIAM J. Comput. **26**, 1484 (1997).

[10] C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution And Coin Tossing*, Theor. Comput. Sci. **560**, 7 (2014).

[11] Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, X. Jiang, L. Zhang, J. Wang, L.-X. You, J.-Y. Guan, *et al.*, *Measurement-Device-Independent Quantum Key Distribution Over 200 km*, Phys. Rev. Lett. **113**, 190501 (2014).

[12] M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, *Efficient Decoy-state Quantum Key Distribution With Quantified Security*, Opt. Express **21**, 24550 (2013).

[13] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, *Continuous-variable Quantum Key Distribution With 1 Mbps Secure Key Rate*, Opt. Express **23**, 17511 (2015).

[14] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, *Floodlight Quantum Key Distribution: A Practical Route To Gigabit-per-second Secret-key Rates*, Phys. Rev. A **94**, 012322 (2016).

[15] Q. Zhuang, Z. Zhang, and J. H. Shapiro, *High-Order Encoding Schemes for Floodlight Quantum Key Distribution*, Phys. Rev. A **98**, 012323 (2018).

[16] Z. Zhang, Q. Zhuang, F. N. C. Wong, and J. H. Shapiro, *Floodlight Quantum Key Distribution: Demonstrating A Framework For High-rate Secure Communication*, Phys. Rev. A **95**, 012332 (2017).

[17] Z. Zhang, C. Chen, Q. Zhuang, F. N. C. Wong, and J. H. Shapiro, *Experimental Quantum Key Distribution At 1.3 Gbit/s Secret-Key Rate Over A 10-dB-Loss Channel*, Quantum Sci. Tech. **3**, 025007 (2018).

[18] S. Pirandola, R. Laurenza, L. Banchi and C. Ottaviani, *Fundamental Limits Of Repeaterless Quantum Communications*, Nat. Commun. **8**, 15043 (2017).

[19] The PLOB bound, states that secret bits per mode cannot exceed $-\log_2(1-\eta)$ for a channel with transmissivity η. It was preceded by the TGW bound [20], which stated that secret bits per mode is bounded above by $\log_2[(1+\eta)/(1-\eta)]$ for a channel with transmissivity η. Unlike the TGW bound, however, the PLOB bound is achievable [18].

[20] M. Takeoka, S. Guha, and M. M. Wilde, *Fundamental Rate-loss Tradeoff For Optical Quantum Key Distribution*, Nat. Commun. **5**, 5235 (2014).

[21] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, *Continuous-variable Quantum Cryptography Using Two-way Quantum Communication*, Nat. Phys. **4**, 726 (2008).

[22] K. Boström and T. Felbinger, *Deterministic Secure Direct Communication Using Entanglement*, Phys. Rev.

Lett. **89**, 187902 (2002).
[23] N. J. Beaudry, M. Lucamarini, S. Mancini, and R. Renner, *Security Of Two-way Quantum Key Distribution*, Phys. Rev. A **88**, 062302 (2013).
[24] Y.-G. Han, Z.-Q. Yin, H.-W. Li, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, *Security Of Modified Ping-Pong Protocol In Noisy And Lossy Channel*, Sci. Rep. **4**, 4936 (2014).
[25] Y.-C. Zhang, Z. Li, C. Weedbrook, S. Yu, W. Gu, M. Sun, X. Peng, and H. Guo, *Improvement Of Two-way Continuous-variable Quantum Key Distribution Using Optical Amplifiers*, J. Phys. B: At., Mol. Opt. Phys. **47**, 035501 (2014).
[26] C. Weedbrook, C. Ottaviani, and S. Pirandola, *Two-way Quantum Cryptography At Different Wavelengths*, Phys. Rev. A **89**, 012309 (2014).
[27] C. I. Henao and R. M. Serra, *Practical Security Analysis Of Two-way Quantum-key-distribution Protocols Based On Nonorthogonal States*, Phys. Rev. A **92**, 052317 (2015).
[28] C. Ottaviani, S. Mancini, and S. Pirandola, *Two-way Gaussian Quantum Cryptography Against Coherent Attacks In Direct Reconciliation*, Phys. Rev. A **92**, 062323 (2015).
[29] C. Ottaviani and S. Pirandola, *General Immunity And Superadditivity Of Two-way Gaussian Quantum Cryptography*, Sci. Rep. **6**, 22225 (2016).
[30] H.-K. Lo and H. F. Chau, *Unconditional Security Of Quantum Key Distribution Over Arbitrarily Long Distances*, Science **283**, 2050 (1999).
[31] P. W. Shor and J. Preskill, *Simple Proof Of Security Of The BB84 Quantum Key Distribution Protocol*, Phys. Rev. Lett. **85**, 441 (2000).
[32] R. Renner, *Symmetry Of Large Physical Systems Implies Independence Of Subsystems*, Nat. Phys. **3**, 645 (2007).
[33] R. Renner and J. I. Cirac, *de Finetti Representation Theorem For Infinite-Dimensional Quantum Systems And Applications To Quantum Cryptography*, Phys. Rev. Lett. **102**, 110504 (2009).
[34] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, *Security Of Continuous-Variable Quantum Key Distribution Against General Attacks*, Phys. Rev. Lett. **110**, 030502 (2013).
[35] M. Sun, X. Peng, Y. Shen, and H. Guo, *Security Of A New Two-way Continuous-variable Quantum Key Distribution Protocol*, Int. J. Quantum Inf. **10**, 1250059 (2012).
[36] R. Renner, *Security Of Quantum Key Distribution*, Int. J. Quantum Inf. **6**, 1 (2008).
[37] I. Devetak and A. Winter, *Distillation Of Secret Key And Entanglement From Quantum States*, Proc. Royal Soc. A **461**, 207 (2005).
[38] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The Security Of Practical Quantum Key Distribution*, Rev. Mod. Phys. **81**, 1301 (2009).
[39] M. A. Nielsen, *Conditions For A Class Of Entanglement Transformations*, Phys. Rev. Lett. **83**, 436 (1999).
[40] Q. Zhuang, Y. Zhu, and P. W. Shor, *Additive Classical Capacity Of Quantum Channels Assisted By Noisy Entanglement*, Phys. Rev. Lett. **118**, 200503 (2017).
[41] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Gaussian Quantum Information*, Rev. Mod. Phys. **84**, 621 (2012).
[42] For simplicity, this figure presumes single-mode symbol encoding, but multi-mode symbol encoding, as employed FL-QKD, will be included in the information-gain bounds to be develped below.
[43] In FL-QKD, Alice mixes amplified spontaneous emission (ASE) into the her Y mode, hence her only being able to access part of Y's purification W; see Sec. IV B for more information.
[44] P. Coles, E. M. Metodiev, and N. Lütkenhaus *Numerical Approach For Unstructured Quantum Key Distribution*, Nat. Commun. **7**, 11712 (2016).
[45] F. Caruso, V. Giovannetti, and A. S. Holevo *One-mode Bosonic Gaussian Channels: A Full Weak-degradability Classification*, New J. Phys. **8**, 310 (2006).
[46] R. García-Patrón, C. Navarrete-Benlloch, S. Lloyd, J. H. Shapiro, and N. J. Cerf, *Majorization Theory Approach To The Gaussian Channel Minimum Entropy Conjecture*, Phys. Rev. Lett. **108**, 110505 (2012).
[47] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2010).
[48] A. Leverrier, and P. Grangier, *Unconditional Security Proof Of Long-Distance Continuous-Variable Quantum Key Distribution With Discrete Modulation*, Phys. Rev. Lett. **102**, 180504 (2009).
[49] Bob's number of modes per encoded symbol is $M_E = T_B W_A$, where T_B-s is the time duration of Bob's symbol and W_A-Hz is the bandwidth of Alice's transmitted light. Side-channel attacks are not considered in the current framework, i.e., we assume that the M_E modes are all that enters Bob's lab in each symbol duration;As a first step to ward off Eve's attacking the QKD protocol, by illuminating Bob's terminal with out-of-band light that would be encoded by Bob and returned to her, we consider Bob employing an optical filter—not shown in Fig. 2—to limit the light entering his encoder to the spectral region of Alice's transmitted light.
[50] We will assume that cT_B, where c is light speed, is a distance that can be wholly confined within Bob's laboratory, making it impossible for Eve to employ intra-symbol feedback in her most general block-coherent attack.
[51] O. Fawzi and R. Renner, *Quantum Conditional Mutual Information And Approximate Markov Chains*, Commun. Math. Phys., **340**, 575 (2015).
[52] M. Tomamichel, R. Colbeck, and R. Renner, *A Fully Quantum Asymptotic Equipartition Property*, IEEE Trans. Inf. Theory **55**, 5840 (2009).
[53] A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner, *Chain Rules For Smooth Min- And Max-Entropies*, IEEE Trans. Inf. Theory **59**, 2603–2612 (2013).
[54] F. Dupuis, O. Fawzi, and R. Renner, *Entropy Accumulation*, arXiv:1607.01796 [quant-ph].
[55] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, *Practical Device-independent Quantum Cryptography Via Entropy Accumulation*, Nat. Commun. **9**, 459 (2018).
[56] R. Arnon-Friedman, R. Renner, and T. Vidick, *Simple And Tight Device-independent Security Proofs*, arXiv:1607:01797 [quant-ph].
[57] M. M. Wolf G. Giedke and J.I. Cirac, *Extremality Of*

Gaussian Quantum States, Phys. Rev. Lett. **96**, 080502 (2006).

[58] R. García-Patrón and N.J. Cerf, *Unconditional Optimality Of Gaussian Attacks Against Continuous-variable Quantum Key Distribution*, Phys. Rev. Lett. **97**, 190503 (2006).

[59] A. S. Holevo, *Entropy Gain And The Choi-Jamiolkowski Correspondence For Infinite-dimensional Quantum Evolutions*, Theor. Math. Phys. **166**, 123 (2011).

[60] Subsequent work has shown that FL-QKD's SKR can be increased by replacing its binary-phase-shift encoding with a high-order encoding scheme [15].

[61] It is noteworthy that binary encoding, as used in FL-QKD, has more efficient reconciliation schemes than those currently available for continuous-variable encoding, as used in the TMSV protocol.

[62] M. Christandl and R. Renner, *Reliable Quantum State Tomography*, Phys. Rev. Lett. **109**, 120403 (2012).

[63] Let $\hat{E}_S(t)$ and $\hat{E}_W(t)$ be the continuous-time, positive-frequency field operators—with $\sqrt{\text{photons/s}}$ units—of Bob's signal and Alice's purification. Also, let $\{\hat{a}_{S_m} : 1 \leq m \leq M\}$ and $\{\hat{a}_{W_m} : 1 \leq m \leq M\}$ be the excited (non-vacuum state) modal annihilation operators in the Fourier-series expansions of these field operators for the $0 \leq t \leq T_B$ block of M_B symbols. Then, Parseval's theorem for the two-dimensional Fourier series gives us $\sum_{m,n=1}^{M} |\langle \hat{a}_{S_m} \hat{a}_{W_n} \rangle|^2 = \int_0^{T_B} dt \int_0^{T_B} du \, |\langle \hat{E}_S(t) \hat{E}_W(u) \rangle|^2$, and $\sum_{m,n=1}^{M} |\langle \hat{a}^\dagger_{S_m} \hat{a}_{W_n} \rangle|^2 = \int_0^{T_B} dt \int_0^{T_B} du \, |\langle \hat{E}^\dagger_S(t) \hat{E}_W(u) \rangle|^2$, which proves the basis-invariance of the pairwise-permutation constraints. For the pairwise-sum constraints to be basis invariant we require that $\langle \hat{E}_S(t) \hat{E}_W(u) \rangle$ only depend on $t + u$, *and* $\langle \hat{E}^\dagger_S(t) \hat{E}_W(u) \rangle$ only depend on $t - u$, i.e., conditions that do *not* hold in general.

[64] There is no loss of generality in assuming that $\langle \hat{a}^\dagger_{S_m} \hat{a}_{W_1} \rangle \neq 0$. If all the $\langle \hat{a}^\dagger_{S_m} \hat{a}_{W_n} \rangle$ vanish then, no beam-splitter transformations are needed to suppress the unwanted phase-insensitive cross correlations, and, if at least one of them is nonzero, we can take that $\boldsymbol{W}$ mode and call it the $n = 1$ mode. The same will be true, below, when we null out the unwanted phase-sensitive cross correlations, i.e., there will either be a $2 \leq n \leq M$ value for which $\langle \hat{a}_{S_m} \hat{a}'_{W_n} \rangle$ is nonzero—in which case we relabel that mode as the $n = 2$ mode—or there are no phase-sensitive cross correlations that must be suppressed.