Overcoming Fundamental Bounds on Quantum Conference Key Agreement

Giacomo Carrara⊙, Gláucia Murta⊙, and Federico Grasselli⊙[*]

Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstraße 1, Düsseldorf D-40225, Germany

Twin-field quantum key distribution (TFQKD) enables two distant parties to establish a shared secret key, by interfering weak coherent pulses (WCPs) in an intermediate measuring station. This allows TFQKD to reach greater distances than traditional QKD schemes and makes it the only scheme capable of beating the repeaterless bound on the bipartite private capacity. Here, we generalize TFQKD to the multipartite scenario. Specifically, we propose a practical conference key agreement protocol that only uses WCPs and linear optics and prove its security with a multiparty decoy-state method. Our protocol allows an arbitrary number of parties to establish a secret conference key by single-photon interference, enabling it to overcome recent bounds on the rate at which conference keys can be established in quantum networks without a repeater.

I. INTRODUCTION

Quantum key distribution (QKD) allows two parties to take advantage of quantum mechanical properties to share a common secret key with information-theoretic security. In the past decades, QKD developed at an increasingly high pace and today represents one of the most mature applications of quantum information science, both in terms of theoretical development and experimental implementation [1,2]. More recently, in view of building quantum communication networks, a lot of effort has been put into generalizing QKD to the multipartite scenario with conference key agreement (CKA) [3–9], which has already seen the first experimental implementations [10,11]. CKA exploits the correlations offered by multipartite entanglement to deliver the same conference key to a set of parties and it has recently been extended to guarantee anonymity of the communicating parties in a larger network [12–14].

However, CKA protocols are faced with the difficulty of establishing multipartite entanglement over large distances, limiting their applicability in real-world scenarios. In particular, most of the protocols proposed so far exploit Greenberger-Horne-Zeilinger (GHZ) correlations, which are known to be difficult to distribute at large distances [3–8].

In the bipartite case, a variant of QKD, named twin-field QKD (TFQKD) [15–19], enables two parties to share keys at much longer distances than most other QKD protocols. The founding idea of TFQKD [17–19] consists in a measurement-device independent (MDI) scheme where a single photon sent by either of the parties interferes in an intermediate untrusted relay, thus halving the communication distance. This enables TFQKD to beat the well-known repeaterless Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound on the secret key capacity [20] (see also Refs. [21,22] for other preliminary bounds), as demonstrated by several experiments [23–33].

In an effort to extend the range of CKA, Ref. [34] introduces a CKA protocol based on single-photon interference that is inspired by the TFQKD setup. This protocol, however, is highly unpractical as it requires each party to entangle solid-state qubits with the optical signals sent to the relay. Moreover, each party must store their qubit until the relay announces the interference outcome and then measure the qubit accordingly.

Alternatively, more practical generalizations of TFQKD were devised in Refs. [8,35–37], where the parties are only required to send weak coherent pulses or interfere the pulses with linear optics. However, the protocols in Refs. [35–37] are not MDI and, what is more, are limited to tripartite configurations and cannot be scaled to an arbitrary number of parties.

In this work, we introduce an MDI CKA protocol that does not present such drawbacks. Our protocol can be realized using only weak coherent pulses interfered with linear optics at an untrusted relay and allows an arbitrary number of parties to establish a conference key. In particular, our protocol postselects correlations belonging to *W*-class states [38] through single-photon interference, independently of the number of parties. This enables our CKA protocol to operate at much higher losses than previous CKA schemes, which require either the simultaneous

_____
[*]federico.grasselli@hhu.de

distribution of photonic multipartite entangled states [3–5,10,11] or the postselection of GHZ-type correlations [6–8].

We prove the security of our protocol against collective attacks in the asymptotic regime by developing a multiparty decoy-state analysis [39–41], through which we derive analytical upper bounds on multipartite yields. We simulate the performance of our protocol with a realistic channel model that accounts for photon loss, dark counts in the detectors as well as phase and polarization misalignment.

Furthermore, we benchmark the protocol's conference key rate with recent upper bounds that apply to arbitrary quantum networks, namely the single-message multicast bound derived in Ref. [42], adopting a similar approach used to benchmark bipartite TFQKD setups. In particular, we consider network architectures where the relay is removed and compute their single-message multicast bounds. Our simulations show that our CKA protocol can overcome such bounds for certain noise regimes and number of parties, thus paving the way for long-distance CKA in quantum networks.

The paper is structured as follows. In Sec. II we describe our CKA protocol and in Sec. III we prove its security. In Sec. IV we detail our multipartite decoy-state method. We simulate the protocol's performance in Sec. V and conclude in Sec. VI. Appendix A describes the optical setup in the untrusted relay. In Appendix B we draw the connection between our protocol and the correlations of W states. The analytical upper bounds on multipartite yields are derived in Appendix C. Appendix D contains details on the channel model and related calculations, while Appendix E provides details on the numerical simulations.

II. PROTOCOL

In this section we present our CKA protocol based on single-photon interference, which is schematically represented in Fig. 1. We limit the description to the asymptotic regime, where the effects due to finite detection statistics are negligible.

In the following, the symbol $\vec{v}$ stands for the binary representation of the integer v, with components $v_i \in \{0, 1\}$, and $|\vec{v}|$ is the Hamming weight of the vector $\vec{v}$.

The CKA protocol is run by N parties, which we denote $A_0, A_1, \ldots, A_{N-1}$.

Protocol 1 (CKA protocol)

1. Quantum state distribution and measurement: repeat the following steps a sufficiently large number of times.

1.1. Each party A_i prepares an optical mode a_i in a state that depends on whether the round is labeled as a PE round or KG round (the type of round could be predetermined, e.g., by a short preshared key held by every party [4,5]). In a PE round, they prepare a phase-randomized coherent
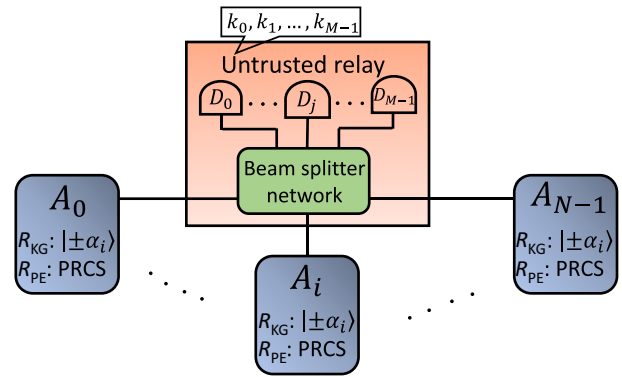

FIG. 1. Schematic representation of our CKA protocol. In a key generation (KG) round, each party sends one of two coherent states $|\pm\alpha_i\rangle$ at random. In a parameter estimation round (PE), they send a phase-randomized coherent state (PRCS). In an honest implementation of the protocol, the relay combines the signals from each party with a beam-splitter network with M inputs and a threshold detector at each of the M outputs (see Fig. 2 for the case $M = 4$ and Appendix A for general M). The relay announces the detection pattern $\vec{k} = (k_0, k_1, \ldots, k_{M-1})$.

state (PRCS):

$$\rho_{a_i}(\beta_i) = e^{-\beta_i} \sum_{n=0}^{\infty} \frac{\beta_i^n}{n!} |n\rangle\langle n|, \tag{1}$$

where the intensity β_i of the coherent state is chosen at random from a finite set $\mathcal{S}_i$ and where $|n\rangle$ is a Fock state. They record the intensity β_i. In a KG round, each party A_i prepares the coherent state $|x_i\alpha_i\rangle_{a_i}$ for a fixed $\alpha_i \in \mathbb{R}$, where $x_i = \pm 1$ is randomly chosen. They record the outcome x_i.

1.2. Every party sends their optical pulse to an untrusted relay through an insecure channel.

1.3. The untrusted relay performs an arbitrary operation on the N optical signals and announces the pattern $\vec{k} \in \{0, 1\}^M$, with $M \geq N$. [In an honest implementation of the protocol, $k_j = 1$ ($k_j = 0$) corresponds to a click (no click) in threshold detector D_j.] The round gets discarded if $|\vec{k}| \neq 1$ and we label Ω_j the event where $k_j = 1$ and $k_{\neq j} = 0$.

2. Parameter estimation: the parties partition their outcomes and intensities in M sets, where each set corresponds to the event Ω_j (for $j = 0, \ldots, M - 1$). For each partition, the parties reveal a fraction of their outcomes in order to estimate the probabilities $\Pr(\Omega_j | x_0, x_i, R_{KG})$ that event Ω_j occurs in a KG round, given that parties A_0 and A_i prepared coherent states $|x_0\alpha_0\rangle$ and $|x_i\alpha_i\rangle$, respectively. With the estimated probabilities, the parties calculate the quantum bit error rate (QBER) with respect to reference party A_0, for every party pair and every partition ($Q^j_{X_0,X_i}$). Similarly, for each partition the parties reveal the intensities β_i used in the PE rounds and estimate the so-called *gains*, $G^j_{\beta_0,\ldots,\beta_{N-1}} := \Pr(\Omega_j | \beta_0, \ldots, \beta_{N-1})$, i.e.,

the probability of the event Ω_j in a PE round, given that the parties prepared PRCSs in Eq. (1) with intensities $\beta_0, \ldots, \beta_{N-1}$, respectively. Using the gains, the parties compute an upper bound $(\overline{Q}_Z^j)$ on the phase error rate (Q_Z^j) of the protocol.

3. *Classical postprocessing:* the parties extract a secret conference key from the remaining (undisclosed) KG outcomes. To do so, for each partition labeled by Ω_j, party A_i flips their outcomes x_i when $(-1)^{\vec{j} \cdot \vec{i}} = -1$. The parties then perform error correction and privacy amplification. The asymptotic conference key rate of the protocol is

$$r = \sum_{j=0}^{M-1} \Pr(\Omega_j | R_{\mathrm{KG}}) \left[1 - h(\overline{Q}_Z^j) - \max_{i \geq 1} h(Q_{X_0 X_i}^j) \right], \quad (2)$$

where $h(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ is the binary entropy and where $\Pr(\Omega_j | R_{\mathrm{KG}}) = (1/4) \sum_{x_0, x_i = \pm 1} \Pr(\Omega_j | x_0, x_i, R_{\mathrm{KG}})$ is the probability of event Ω_j in a KG round.

We prove the security of the CKA protocol in Sec. III. We remark that the security holds for any implementation of the quantum channels and of the relay, as far as the relay announces a pattern in every round.

In an honest implementation of the protocol, the optical signals are sent through potentially noisy and lossy channels to the relay, where they interfere in a balanced beam-splitter (BBS) network of M inputs and M outputs, with $M \geq N$ and M being a power of 2. The BBS network for $M = 4$ is depicted in Fig. 2, while the structure for generic M is reported in Appendix A. We note that the total number of beam splitters required by the BBS network scales favourably with the number N of parties, as $\mathcal{O}(N \log_2 N)$. The network transforms the input modes $(\hat{a}_i^\dagger)$ in a balanced combination of the output modes $(\hat{d}_j^\dagger)$, i.e.,

$$\hat{a}_i^\dagger \rightarrow \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} (-1)^{\vec{j} \cdot \vec{i}} \hat{d}_j^\dagger. \quad (3)$$

We point out that a setup designed with M inputs can be used by any number of parties $N \leq M$, by simply pairing the modes of the N parties with $M - N$ additional modes in the vacuum state. However, it is worth noting that adding unused ports in the BBS network introduces unwanted noise and may reduce the performance of the protocol. Then, the relay measures each output mode d_j with a threshold detector D_j, for $j = 0, \ldots, M - 1$, and announces the detection pattern $\vec{k} \in \{0,1\}^M$, where $k_j = 1$ if detector D_j clicked and $k_j = 0$ otherwise. The round is retained only when exactly one detector clicks (event Ω_j for some j).

In the following, we provide the formulas to compute the QBER $(Q_{X_0 X_i}^j)$ and the upper bound on the phase error
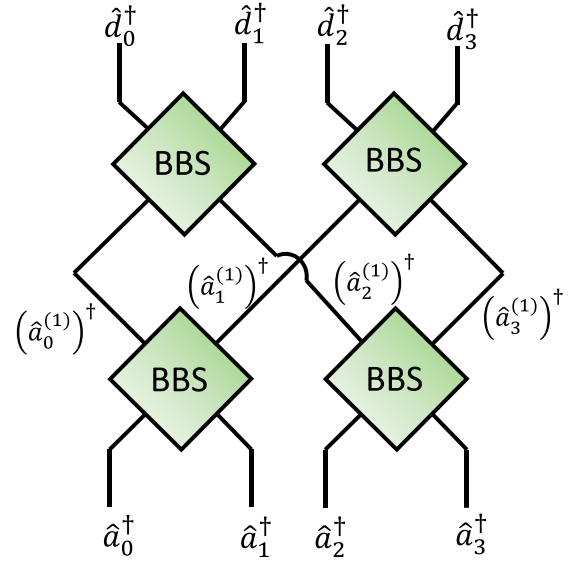

FIG. 2. BBS network for $M = 4$ inputs, which can be used by $N = 2$, $N = 3$, and $N = 4$ parties. We indicate the input modes with $\hat{a}_i^\dagger$ and the output modes with $\hat{d}_i^\dagger$, for $i = 0, 1, 2, 3$. The network for a general number of inputs ($M = 2^s$) is described in Appendix A.

rate $(\overline{Q}_Z^j)$. The QBER is defined for every pair of parties (A_0, A_i) and for every partition labeled by Ω_j, as follows:

$$Q_{X_0, X_i}^j = \Pr(X_0 \neq (-1)^{\vec{j} \cdot \vec{i}} X_i | \Omega_j, R_{\mathrm{KG}}), \quad (4)$$

where X_i is the binary random variable with outcomes $x_i = \pm 1$. The QBER is computed through Bayes' theorem:

$$Q_{X_0, X_i}^j = \sum_{x_0 \neq (-1)^{\vec{j} \cdot \vec{i}} x_i} \frac{\Pr(\Omega_j | x_0, x_i, R_{\mathrm{KG}})}{4 \Pr(\Omega_j | R_{\mathrm{KG}})}. \quad (5)$$

The computation of the upper bound on the phase error rate is more involved. Indeed, it requires the derivation of upper bounds on quantities called *yields* and defined as

$$Y_{n_0, \ldots, n_{N-1}}^j := \Pr(\Omega_j | n_0, \ldots, n_{N-1}), \quad (6)$$

i.e., the probability of the event Ω_j given the hypothetical scenario where the parties send Fock states with photon numbers $n_0, \ldots, n_{N-1}$. In Eq. (34), we provide analytical upper bounds $(\overline{Y}_{n_0, \ldots, n_{N-1}}^j)$ on the yields as a function of the estimated gains $G_{\beta_0, \ldots, \beta_{N-1}}^j$. Then, one can compute the

upper bound on the phase error rate as follows:

$$\overline{Q}_Z^j = \frac{1}{\Pr(\Omega_j | R_{\mathrm{KG}})} \sum_{v \in \mathcal{V}} \left(\sum_{n_0 + \cdots + n_{N-1} \leq \overline{n}} \times \prod_{i=0}^{N-1} c_{i,n_i}^{(v_i)} \sqrt{\overline{Y}_{n_0,\ldots,n_{N-1}}^j} + \Delta_{v,\overline{n}} \right)^2, \qquad (7)$$

where $\overline{n}$ is a positive even number, while the set $\mathcal{V}$, the coefficients $c_{i,n_i}^{(v_i)}$ and the quantity $\Delta_{v,\overline{n}}$ are defined as follows:

$$\mathcal{V} = \left\{ v \in \{0, 2^N - 1\} : |\vec{v}| \mod 2 = 0 \right\}, \qquad (8)$$

$$c_{i,n}^{(l)} = \begin{cases} e^{-\alpha_i^2/2} \frac{\alpha_i^n}{\sqrt{n!}} & \text{if } n + l \text{ is even} \\ 0 & \text{if } n + l \text{ is odd} \end{cases} \qquad (9)$$

$$\Delta_{v,\overline{n}} = \sum_{n_0 + \cdots + n_{N-1} \geq \overline{n}+2} \prod_{i=0}^{N-1} c_{i,n_i}^{(v_i)}. \qquad (10)$$

The full derivation of the upper bound (7) on the phase error rate is provided Sec. III.

We remark that the protocol presented here uses the correlations of postselected W-like states to obtain a secret conference key. In Appendix B we clarify the connection between the correlations generated in the CKA protocol and the W state. Moreover, we note that, for two parties ($N = 2$), our protocol reduces to the TFQKD protocol introduced in Ref. [17] (see Appendix A).

III. SECURITY PROOF

Here we prove the security of the CKA protocol presented in Sec. II under the assumption of collective attacks.

Theorem 1.—The CKA protocol (Protocol II), under collective attacks by the eavesdropper and in the asymptotic limit, generates a conference key with rate r, given by Eq. (2).

Proof.—In the asymptotic limit and under collective attacks, the achievable conference key rate r of a CKA protocol with one-way reconciliation is lower bounded by the following [9]:

$$r \geq H(X_0|E) - \max_{i \geq 1} H(X_0|X_i), \qquad (11)$$

where $H(X_0|E)$ ($H(X_0|X_i)$) is the von Neumann (Shannon) entropy of the KG outcome of reference party A_0, conditioned on the eavesdropper's total side information (party A_i's KG outcome), and it is evaluated on the state shared by the parties in a KG round. Note that the probability of a KG round is set to one in Eq. (11), since, asymptotically, the fraction of PE rounds becomes negligible.

In the case of our protocol, we postselect the KG rounds where event Ω_j occurred and discard all the other rounds. And for each event Ω_j, we independently extract a conference key. Hence, the asymptotic conference key rate of the whole protocol is bounded by

$$r \geq \sum_{j=0}^{M-1} \Pr(\Omega_j | R_{\mathrm{KG}}) \left[H(X_0|E)_{\Omega_j} - \max_{i \geq 1} H(X_0|X_i)_{\Omega_j} \right], \qquad (12)$$

where the entropies are computed on the state shared by the parties in a KG round, conditioned on event Ω_j.

Recall that, in an honest implementation, Ω_j corresponds to the event where only detector D_j clicks. Although our proof holds regardless of the physical details associated to the event Ω_j, in the following we often refer to Ω_j in terms of detector clicks for concreteness.

The second term in Eq. (12) is the conditional Shannon entropy between the KG outcomes of parties A_0 and A_i, when only detector D_j clicked. Thus, it can be readily bounded through Fano's inequality with the corresponding QBER in Eq. (4) as follows:

$$H(X_0|X_i)_{\Omega_j} \leq h(Q_{X_0, X_i}^j). \qquad (13)$$

In order to lower bound the first conditional entropy in Eq. (12), we employ the entropic uncertainty relation [43]. To apply the uncertainty relation, we need to view the outcome X_0 corresponding to the coherent state prepared by party A_0 as the result of a fictitious measurement. To this aim, we consider an equivalent formulation of the protocol where each party, in a KG round, first prepares the following entangled state between their optical mode a_i and a virtual qubit Q_i:

$$|\psi_i\rangle_{Q_i a_i} = \frac{1}{\sqrt{2}} \left(|+\rangle_{Q_i} |\alpha_i\rangle_{a_i} + |-\rangle_{Q_i} |-\alpha_i\rangle_{a_i} \right), \qquad (14)$$

where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$, and then measures their qubit in the X basis. Note that, from the eavesdropper's point of view, the fictitious protocol is completely equivalent to the actual protocol, even in the case that the parties delay their X-basis measurement until after the relay's announcement. This allows us to consider the state of the N qubits and optical modes, conditioned on detector D_j clicking in a KG round, prior to the X-basis measurements. The state reads

$$|\chi_j\rangle_{Q_0 Q_1 \ldots Q_{N-1} E} := \frac{\hat{K}_j \left(\bigotimes_{i=0}^{N-1} |\psi_i\rangle_{Q_i a_i} \right)}{\sqrt{\Pr(\Omega_j | R_{\mathrm{KG}})}}, \qquad (15)$$

where $\hat{K}_j$ is the Kraus operator [44] that models the action of the untrusted relay, i.e., the eavesdropper, when

it announces the event Ω_j. The operator $\hat{K}_j$ acts between the Fock space of optical modes $a_0 \ldots a_{N-1}$ and a generic Hilbert space $\mathcal{H}_E$, i.e., $\hat{K}_j : \mathcal{H}_{a_0} \otimes \cdots \otimes \mathcal{H}_{a_{N-1}} \to \mathcal{H}_E$.

We remark that, due to the assumption of collective attacks, the operator $\hat{K}_j$ remains the same in every KG and PE round. Nevertheless, due to the partial distinguishability of the states prepared in KG and PE rounds, $\hat{K}_j$ could model the attempt to guess the type of round followed by an operation, which is specific to KG and PE rounds. This implies that, in general, $\Pr(\Omega_j|R_{\text{KG}}) \neq \Pr(\Omega_j|R_{\text{PE}})$.

With the pure state in Eq. (15), we can apply the entropic uncertainty relation by considering the hypothetical scenario where party A_0 performs either an X-basis or a Z-basis measurement on their qubit. We thus obtain the following lower bound on the first entropy in Eq. (12):

$$H(X_0|E)_{\Omega_j} \geq 1 - H(Z_0|Q_1 \ldots Q_{N-1})_{\Omega_j}, \qquad (16)$$

where both conditional entropies are computed on the state (15). We then derive an upper bound on the entropy on the right-hand side of Eq. (16) by using the fact that quantum maps on the conditioning systems can only increase the entropy [45]:

$$H(Z_0|Q_1 \cdots Q_{N-1})_{\Omega_j} \leq H(Z_0|\prod_{i=1}^{N-1} Z_i)_{\Omega_j}$$
$$\leq h(Q_Z^j). \qquad (17)$$

In the second line, we use Fano's inequality and the definition of phase error rate:

$$Q_Z^j = \Pr(\prod_{i=0}^{N-1} Z_i = 1|\Omega_j, R_{\text{KG}}), \qquad (18)$$

which expresses the probability that, in the hypothetical scenario where each party measures in the Z basis their virtual qubit, the product of the outcomes is one. By employing Eqs. (13) and (17) in Eq. (12), we obtain the following expression for the asymptotic conference key rate of our CKA protocol:

$$r \geq \sum_{j=0}^{M-1} \Pr(\Omega_j|R_{\text{KG}}) \left[1 - h(Q_Z^j) - \max_{i \geq 1} h(Q_{X_0 X_i}^j) \right]. \quad (19)$$

To complete the security proof, we still need to bound the phase error rate (Q_Z^j) with the statistics collected by the parties in the PE rounds. The derivation of the bound is inspired by the security proof in Ref. [17] for a bipartite TFQKD protocol.

By definition (18), the phase error rate is the probability that an even number of parties obtains -1 as the outcome of their Z-basis measurement, in the hypothetical scenario in which all parties measured their virtual qubit in the Z

basis in a KG round and detector D_j clicks. Through the N-qubit state (15), which describes the state of the virtual qubits in a KG round conditioned on the click of detector D_j, we are able to express the phase error rate as follows:

$$Q_Z^j = \sum_{v \in \mathcal{V}} \left\| \langle \vec{v}|_{Q_0 \ldots Q_{N-1}} |\chi_j\rangle \right\|^2, \qquad (20)$$

where the set $\mathcal{V}$ is defined in Eq. (8), i.e., the set of binary strings with parity zero. In order to bound the expression in Eq. (20), we observe that, for $l = 0, 1$, we have $_{Q_i}\langle l|\psi_i\rangle_{Q_i a_i} = |C_i^{(l)}\rangle_{a_i}$, where $|C_i^{(l)}\rangle_{a_i}$ are unnormalized "cat states":

$$|C_i^{(l)}\rangle_{a_i} = \frac{|\alpha_i\rangle + (-1)^l |-\alpha_i\rangle}{2} = \sum_{n=0}^{\infty} c_{i,n}^{(l)} |n\rangle_{a_i}, \qquad (21)$$

with $c_{i,n}^{(l)}$ defined in Eq. (9). By employing the states in Eq. (21), we can derive an upper bound on each term in the sum of Eq. (20) as follows:

$$\Pr(\Omega_j|R_{\text{KG}}) \left\| \langle \vec{v}|_{Q_0 \ldots Q_{N-1}} |\chi_j\rangle \right\|^2$$
$$= \left\| \hat{K}_j \bigotimes_{i=0}^{N-1} |C_i^{(v_i)}\rangle_{a_i} \right\|^2$$
$$= \left\| \sum_{n_0, \ldots, n_{N-1}=0}^{\infty} \hat{K}_j \bigotimes_{i=0}^{N-1} c_{i,n_i}^{(v_i)} |n_i\rangle \right\|^2$$
$$\leq \left(\sum_{n_0, \ldots, n_{N-1}=0}^{\infty} \left\| \hat{K}_j \bigotimes_{i=0}^{N-1} c_{i,n_i}^{(v_i)} |n_i\rangle \right\| \right)^2$$
$$= \left(\sum_{n_0, \ldots, n_{N-1}=0}^{\infty} \prod_{i=0}^{N-1} c_{i,n_i}^{(v_i)} \sqrt{Y_{n_0, \ldots, n_{N-1}}^j} \right)^2, \qquad (22)$$

where we use the fact that $\hat{K}_j$ acts only on the optical systems in the first equality and the triangle inequality in the third line. Moreover, we identified

$$\left\| \hat{K}_j |n_0\rangle_{a_0} \ldots |n_{N-1}\rangle_{a_{N-1}} \right\|^2 = \Pr\left(\Omega_j|n_0, \ldots, n_{N-1} \right)$$
$$=: Y_{n_0, \ldots, n_{N-1}}^j, \qquad (23)$$

as the yields. We derive an upper bound on the phase error rate by employing the inequality (22) in Eq. (20). We

obtain

$$Q_Z^j \leq \overline{Q}_Z^j = \frac{1}{\Pr(\Omega_j | R_{KG})} \sum_{v \in \mathcal{V}} \left(\sum_{n_0,\ldots,n_{N-1}=0}^{\infty} \times \prod_{i=0}^{N-1} c_{i,n_i}^{(v_i)} \sqrt{Y_{n_0,\ldots,n_{N-1}}^j} \right)^2, \qquad (24)$$

where the set $\mathcal{V}$ is given in Eq. (8) and the coefficients $c_{i,n_i}^{(v_i)}$ are given in Eq. (9).

The bound in Eq. (24) is not yet sufficient to obtain a computable lower bound on the key rate (19) of our CKA protocol, i.e., an expression that can be evaluated from the observed statistics. Indeed, the yields in Eq. (24) are not directly observed and must be estimated through a multipartite decoy-state method.

From the detection statistics of PE rounds, the parties can estimate the gains. By recalling that, under the assumption of collective attacks, the Kraus operator $\hat{K}_j$ corresponding to the event Ω_j is the same in every round, we can express the gains as follows:

$$G_{\beta_0,\ldots,\beta_{N-1}}^j = \sum_{n_0,\ldots,n_{N-1}=0}^{\infty} \text{Tr}\left[\hat{K}_j \bigotimes_{i=0}^{N-1} e^{-\beta_i} \frac{\beta_i^{n_i}}{n_i!} |n_i\rangle \langle n_i| \hat{K}_j^\dagger \right]$$

$$= \sum_{n_0,\ldots,n_{N-1}=0}^{\infty} \prod_{i=0}^{N-1} P_{\beta_i}(n_i) \text{Tr}\left[\hat{K}_j \bigotimes_{i=0}^{N-1} |n_i\rangle \langle n_i| \hat{K}_j^\dagger \right]$$

$$= \sum_{n_0,\ldots,n_{N-1}=0}^{\infty} \prod_{i=0}^{N-1} P_{\beta_i}(n_i) Y_{n_0,\ldots,n_{N-1}}^j, \qquad (25)$$

where we use Eq. (23) in the last equality and defined the Poisson distribution $P_\lambda(n) = e^{-\lambda}\lambda^n/n!$. The last expression links the observed gains to the yields and forms the basis of our multipartite decoy-state method, which we detail in Sec. IV. Our method allows us to obtain analytical upper bounds $\overline{Y}_{n_0,\ldots,n_{N-1}}^j$ on any yield.

Although our method is general and works for any choice of photon numbers $n_0, \ldots, n_{N-1}$, in practice it is not necessary to bound every yield appearing in Eq. (24) with a nontrivial upper bound. This is because the product of the coefficients defined in Eq. (9) satisfies

$$\prod_{i=0}^{N-1} c_{i,n_i}^{(v_i)} \neq 0 \iff n_{\text{tot}} := \sum_{i=0}^{N-1} n_i \text{ is even.} \qquad (26)$$

Therefore, the only yields contributing to the phase error rate upper bound in Eq. (24) are those with $n_{\text{tot}} = 0, 2, 4, \ldots$ and so on. Moreover, the product of the coefficients rapidly decreases with n_{tot}, implying that it is

sufficient to nontrivially bound only the yields corresponding to the first few values of n_{tot}, while the rest of the yields can be bounded by one.

With the yields' bounds, we can further bound the quantity in Eq. (24) and obtain the following upper bound on the phase error rate:

$$Q_Z^j \leq \overline{Q}_Z^j = \frac{1}{\Pr(\Omega_j | R_{KG})} \sum_{v \in \mathcal{V}} \left(\sum_{n_0+\cdots+n_{N-1} \leq \overline{n}} \times \prod_{i=0}^{N-1} c_{i,n_i}^{(v_i)} \sqrt{\overline{Y}_{n_0,\ldots,n_{N-1}}^j} + \Delta_{v,\overline{n}} \right)^2, \qquad (27)$$

where $\overline{Y}_{n_0,\ldots,n_{N-1}}^j$ are the nontrivial bounds derived in Sec. IV and $\Delta_{v,\overline{n}}$ is the residual term obtained by bounding by one all the remaining yields. We have

$$\Delta_{v,\overline{n}} = \sum_{n_0+\cdots+n_{N-1} \geq \overline{n}+2} \prod_{i=0}^{N-1} c_{i,n_i}^{(v_i)}, \qquad (28)$$

where $\overline{n}$ is an even number.

By employing Eq. (27) in Eq. (19), we recover the computable lower bound on the conference key rate in Eq. (2). This concludes the security proof. ∎

As a final remark, we stress that the assumption on collective attacks, i.e., the operator $\hat{K}_j$ being constant in every round, is instrumental in our proof. Extending the security proof to coherent attacks would mean that $\hat{K}_j$ could not only guess the type of the current round, but also depend on the sequence of previous guesses, thus not remaining constant throughout the protocol run. The security of our protocol under coherent attacks could be proved by adapting the technique in Ref. [46]. Indeed, in Ref. [46] the authors perform a full finite-key analysis against coherent attacks for the TFQKD protocol in Ref. [17], which is recovered by our protocol when $N = 2$. We conjecture that the asymptotic key rate of our protocol would not be affected by coherent attacks, as suggested by taking the asymptotic limit of the finite key rate in Ref. [46] and realizing that it coincides with our asymptotic key rate, Eq. (2), when $N = 2$.

IV. MULTIPARTITE DECOY-STATE METHOD

In this section we present a technique that generalizes the decoy-state method to the multipartite scenario and provides an analytical upper bound on any yield $Y_{n_0,\ldots,n_{N-1}}^j$, when an arbitrary number of parties N use the same set of two decoy intensities: $\mathcal{S} = \{\beta_0, \beta_1\}$.

The starting point of the multipartite decoy-state method is the equation that relates the observed gains with the

yields, Eq. (25), which we report here for clarity:

$$G^j_{\vec{f}} = \sum_{n_0,\dots,n_{N-1}=0}^{\infty} Y^j_{n_0,\dots,n_{N-1}} \prod_{i=0}^{N-1} \frac{e^{-\beta_{f_i}} \beta_{f_i}^{n_i}}{n_i!}, \quad (29)$$

where we introduce the binary vector $\vec{f}$ that fixes the choice of intensity to β_{f_i} for party A_i.

Of note, the yields are independent of $\vec{f}$, i.e., of the selected intensities. Thus, Eq. (29) can be interpreted as a system of 2^N linear equations, each one labeled by $\vec{f}$, where the yields are the unknowns. By performing appropriate linear combinations of the system of equations, one can derive equalities where only a subset of yields survive, thus reducing the number of unknowns. However, the number of unknowns is infinite, implying that such a technique cannot generate the exact solution for each yield. Nevertheless, from the linear combinations presenting a reduced number of yields, one can still obtain nontrivial upper bounds.

For concreteness, consider the following toy example of an equality linking a function B of the observed statistics to a (possibly infinite) subset of yields, Y and Y_i,

$$B = cY + \sum_i c_i Y_i, \quad (30)$$

where c and c_i are real coefficients. Suppose that our goal is to derive an upper bound on the yield Y. To do so, we first split the sum of the other yields in two sums, one in which the coefficients c_i have the same sign as c and another where they have opposite sign. By labeling $s_i := \text{sign}(c_i)$ (s) the sign of coefficient c_i (c), we have

$$B = cY + \sum_{i:s_i=s} c_i Y_i + \sum_{i:s_i \neq s} c_i Y_i. \quad (31)$$

Now, by multiplying both sides by s and isolating Y, we get

$$Y|c| = sB - \sum_{i:s_i=s} |c_i| Y_i + \sum_{i:s_i \neq s} |c_i| Y_i. \quad (32)$$

Then, it is straightforward to obtain an upper bound on Y by minimizing the yields Y_i whose coefficients have the same sign as the coefficient of Y ($s_i = s$) and by maximizing the other yields ($s_i \neq s$). In the case we do not have nontrivial bounds on the yields Y_i, we simply set the former to zero and the latter to one. In many cases, the described procedure can lead to a nontrivial bound on Y:

$$Y \leq \min\left\{ B/c + \sum_{i:s_i \neq s} |c_i/c|, 1 \right\}, \quad (33)$$

where the minimum is taken to ensure that the bound is never greater than 1.

In Appendix C, we apply this method on the system in Eq. (29) and obtain a nontrivial upper bound on the generic yield $Y^j_{n_0,\dots,n_{N-1}}$, given by

$$\overline{Y}^j_{n_0,\dots,n_{N-1}} = \min\{U^j_{n_0,\dots,n_{N-1}}, 1\},$$

$$U^j_{n_0,\dots,n_{N-1}} = \prod_{\substack{i \text{ s.t.} \\ n_i \neq 0}} \frac{n_i!}{\beta_0^{n_i} - \beta_1^{n_i}} \left[\frac{B^j_{\vec{h}}(-1)^{N-m}}{(\beta_0 - \beta_1)^{N-m}} \right.$$

$$+ \left(e^{\beta_0} - e^{\beta_1} \right)^m \sum_{k=0}^{\lfloor (N-m-1)/2 \rfloor} \binom{N-m}{2k+1}$$

$$\left. \times \left(\frac{\beta_1 e^{\beta_0} - \beta_0 e^{\beta_1} + \beta_0 - \beta_1}{\beta_0 - \beta_1} \right)^{2k+1} \right], \quad (34)$$

where $\vec{h}$ is the binary vector with components:

$$h_i = \begin{cases} 1 & \text{if } n_i \geq 1 \\ 0 & \text{if } n_i = 0, \end{cases} \quad (35)$$

while $m = |\vec{h}|$, $\lfloor x \rfloor$ is the floor function, and $B^j_{\vec{h}}$ is given by

$$B^j_{\vec{h}} = \sum_{f=0}^{2^N-1} (-1)^{|\vec{f}|} \beta_0^{(\vec{1}-\vec{h})\cdot\vec{f}} \beta_1^{(\vec{1}-\vec{h})\cdot(\vec{1}-\vec{f})} \frac{G^j_{\vec{f}}}{\prod_{i=0}^{N-1} e^{-\beta_{f_i}}}. \quad (36)$$

As a final remark, our analytical technique can be generalized to scenarios with different and more intensities for each party. Besides, we point out that the calculation of the yields' bounds required by the phase error rate bound in Eq. (7) can also be done numerically by using linear programming techniques [16].

V. SIMULATIONS

In order to assess the performance of our protocol, we simulate its key rate (2) under a channel model that includes different sources of noise. First, we model the losses between each party and the detectors at the relay with the same pure-loss channel with transmittance η. We also account for a polarization and phase misalignment of 2% between the reference party A_0 and each other party. Moreover, we account for dark counts in the detectors by computing the key rates considering different dark-count probabilities, namely, 10^{-8}, 10^{-9}, and 10^{-10}. In Appendix D we describe the channel model in detail and provide the calculations of the protocol's statistics under such model.

In our symmetric channel model each party experiences the same loss. Thus, the optimal signal intensities are independent of the party, implying that we can set $\alpha_i = \alpha$ and $S_i = S$ for every i, without losing in performance. Under these conditions, we analytically verify (see Appendix D)

that the detection statistics, i.e., $\Pr(\Omega_j | x_0, x_i, R_{KG})$ and $\Pr(\Omega_j | \beta_0, \ldots, \beta_{N-1})$, are independent of which detector clicks (j) and of the party (i).

This readily implies that the QBER in Eq. (5) is independent of the party and of the detector and we can indicate it as $Q^j_{X_0 X_i} = Q_X$. Similarly, the analytical upper bounds on the yields presented in Sec. IV are independent of j since the gains are independent of j. We employ our yields bounds, Eq. (34), in the calculation of the bound $\overline{Q}_Z$ on the phase error rate (7), where we choose $\bar{n} = 4$ as the cutoff number above which every yield is trivially bounded by one. The choice is motivated by the fact that, for $\bar{n} = 4$, the residual term $\Delta_{v,\bar{n}}$ in Eq. (10) becomes negligible.

By considering the discussed symmetries, the asymptotic conference key rate of our simulations simplifies to

$$r \geq M \Pr(\Omega | R_{KG}) \left[1 - h(\overline{Q}_Z) - h(Q_X) \right], \quad (37)$$

where $\Pr(\Omega | R_{KG})$ is the probability that a fixed detector clicks in a KG round and $M \geq N$ is the number of detectors in the relay.

In order to benchmark the performance of our protocol, we follow the approach used for TFQKD schemes. Typically, the key rate of a TFQKD protocol is benchmarked against the repeaterless bound [20], i.e., the bound on the private capacity between Alice and Bob when the relay between the two parties is removed. If the TFQKD rate surpasses the repeaterless bound, this indicates that adding an untrusted relay enables higher secret key rates and proves the usefulness of the TFQKD protocol. Similarly, in our multipartite setting we compare the conference key rate of our protocol with the ultimate conference key rate that could be achieved in the quantum network without the relay. This is the single-message multicast bound of the quantum network [42] and it depends on the network architecture. In our scenario, there are at least two network configurations (star network and fully connected network) that can arise when removing the relay, which we depict in Fig. 3.

In the star network (left configuration in Fig. 3), there is a pure-loss bosonic channel with transmittance η^2 between
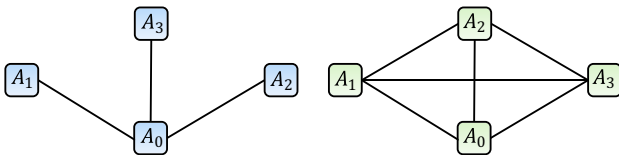

FIG. 3. Two possible network configurations that arise when the relay is removed, for $N = 4$ parties. In the left configuration, there is a bipartite link between A_0 and each other party (star network). In the right configuration, each party is connected with each other (fully connected network). The transmittance of the channel connecting any two parties is η^2.

party A_0 and each other party A_i (for $i = 1, \ldots, N - 1$). In this case, the single-message multicast bound is independent of the number of parties N and coincides with the bipartite repeaterless bound [20] used to benchmark TFQKD protocols:

$$r \leq -\log_2 (1 - \eta^2) =: R_1. \quad (38)$$

In the right configuration of Fig. 3, the resulting network is fully connected, such that each party is linked to each other with the same pure-loss bosonic channel with transmittance η^2. In this case, the single-message multicast bound reads [42]

$$r \leq -(N - 1) \log_2 (1 - \eta^2) =: R_2(N). \quad (39)$$

In this network configuration the single-message multicast bound increases with the number of parties, N. This could be explained by the quadratic scaling of the number of bipartite links with N, compared to the linear scaling of the star network. It is worthwhile to emphasize that, in order to obtain the network configurations of Fig. 3 when removing the relay, additional pure-loss channels need to be added on top of the existing channels used by our protocol. For instance, the star network can be seen as the result of a combination of six channels with transmittance η: three channels connect A_0 to the point where the relay was located and are subsequently linked to the three channels connecting to parties A_1, A_2, and A_3. While our CKA protocol requires only four such channels (from the relay to each of the parties) when $N = 4$. This contrasts with the benchmarking of bipartite TFQKD against the repeaterless bound, where the relay is removed and the two original channels are linked together without the need to add further channels. Therefore, when comparing the multicast bounds (38) and (39) with the CKA rate of our protocol, one should consider that the multicast bounds can only be attained if additional channels are used.

In Fig. 4, we plot the key rate (37) of our protocol for $N = 3$, $N = 4$, and $N = 5$ parties (for every N, we fix the number of inputs M in the BBS network to the smallest power of two such that $M \geq N$), together with the multicast bounds, Eqs. (38) and (39). In Fig. 4(a), we compute the phase error rate bound in Eq. (7) with our analytical upper bounds on the yields (34) obtained with two decoy intensities fixed to $\beta_0 = 0.5$ and $\beta_1 = 0$, respectively. In Fig. 4(b), instead, we assume that the relevant yields in the phase error rate bound (7) are known and use their exact analytical expression (D74) (see Appendix D for the calculation). This corresponds to the limit where the parties have an infinite number of decoy intensities and can estimate the yields exactly. In both plots, we optimize the key rate at each level of loss over the signal amplitude α. Further details on the numerical simulations and on the optimal values for α are reported in Appendix E.
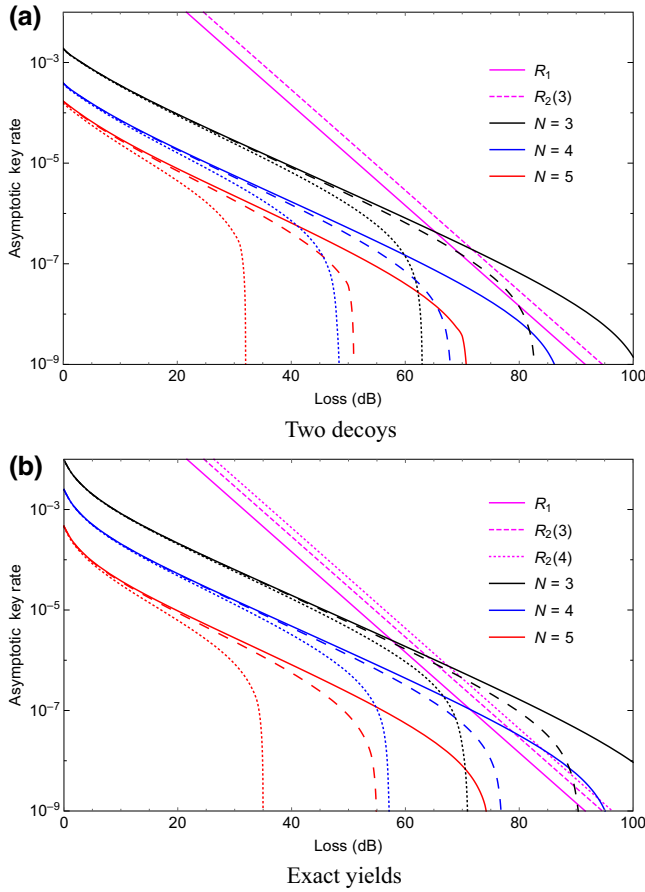
FIG. 4. Asymptotic conference key rate of our protocol [Eq. (37)] as a function of the loss (in dB) between any two parties, when (a) each party uses two decoy intensities; (b) the parties can perfectly estimate the yields. We plot the key rate for different dark-count probabilities: $p_d = 10^{-10}$ (solid lines), $p_d = 10^{-9}$ (dashed lines), and $p_d = 10^{-8}$ (dotted lines) and a different number of parties N, while we fix the polarization and phase misalignment to 2%. We report the single-message multicast bound R_1 [Eq. (38), solid magenta line] for the star network and the bounds $R_2(3)$ and $R_2(4)$ [Eq. (39), dashed and dotted magenta line] for the fully connected network. (a) For sufficiently high loss, our protocol with two decoys can overcome the multicast bounds for both configurations when $N = 3$. (b) A tighter estimation of the yields (e.g., by adding decoy intensities) would allow our protocol to overcome both multicast bounds for $N = 3$ and $N = 4$.

From Fig. 4(a) we observe that our protocol, already with two decoy intensities per party, is capable of overcoming both the single-message multicast bounds R_1 and R_2, for three parties and in the high-loss regime. This is explained by the fact that our protocol relies on single-photon interference events, regardless of the number of parties, hence its key rate scales with the transmittance between one party and the relay: $r \sim \eta$. Conversely, the multicast bounds in Eqs. (38) and (39) for a quantum network without a relay cannot scale better than $r \sim \eta^2$.

However, as the number of parties increases, the key rate of our protocol drops due to the unavoidable QBER inherited from W-state correlations and cannot beat the multicast bounds. This can be mitigated by increasing the number of decoy intensities per party, as suggested by Fig. 4(b) that represents the best-case scenario of infinite decoys. Indeed, we observe a significant improvement of the key rate, especially in the high-loss regime, allowing it to overcome the multicast bounds R_1 and R_2 for three and four parties. The advantage provided by our protocol could extend beyond four parties when compared to more realistic multicast bounds that account for additional noise on top of pure loss (for example, the noise model used in the simulations), as well as tighter multicast bounds (the multicast bounds used in our comparison are not proven to be tight and might be quite loose [42]).

The improvement of the key rate in the high-loss regime occurs because adding decoy intensities to the multipartite decoy-state method allows for tighter yields' bounds when evaluating the phase error rate through (7). As a consequence, the optimal value of the signal intensity (α^2) can increase without severely affecting the phase error rate bound, as shown in Appendix E. In turn, higher signal intensities increase the probability that exactly one detector clicks (up to the limit where multiple-photon contributions become dominant), thus increasing the key rate. The gain in the key rate is particularly visible in the high-loss regime, where the effect of dark counts on the detector clicks is comparable to the arrival of a signal.

In parallel, the key rate computed with the exact yields [Fig. 4(b)] is higher than the one computed with two decoys [Fig. 4(a)] even in the low-loss regime. This is due to the fact that the latter is not optimized over the decoy intensities. In particular, the value of $\beta_0 = 0.5$ is chosen such that it is close-to-optimal only for high losses, thus explaining the suboptimal behavior of the key rate with two decoys at low losses.

VI. CONCLUSION

We design a practical, measurement-device-independent, conference key agreement protocol that delivers a shared conference key to an arbitrary number of parties. In the protocol, each party only has to transmit coherent pulses to an untrusted relay, which interferes the pulses in a network of balanced beam splitters and performs threshold measurements. Our protocol harnesses single-photon interference at the relay in order to establish a common key. This can be understood by realizing that the correlations postselected by our protocol correspond to the correlations of a W state, which can indeed generate conference keys [9].

We prove the security of our protocol against collective attacks and derive an analytical expression for the asymptotic key rate, by combining the entropic uncertainty

relation [43] with an developed multipartite decoy-state analysis. We emphasize that our protocol and its security proof are general and can account for scenarios with arbitrary asymmetric losses. Moreover, we provide extended numerical simulations with a realistic channel model that accounts for phase and polarization misalignment, photon loss, and dark counts in the detectors. We show that our protocol is capable, in certain regimes, of overcoming the ultimate conference key rates achievable in a quantum network without a relay, by comparing it to single-message multicast bounds [42].

A notable byproduct of our work is the derivation of analytical upper bounds on the yields of any combination of Fock states sent by the parties, which may find application in other multipartite protocols where yields need to be estimated. Our analytical bounds on the yields are the first bounds derived for an arbitrary number of parties.

At the same time, our protocol represents the first example of a CKA protocol that can beat single-message multicast bounds in quantum networks [42]. This heralds a key step for long-distance CKA, similarly to how the introduction of TFQKD [15] allowed QKD to reach much longer distances by beating the repeaterless bound [20]. Indeed, our results show that adding an untrusted relay, with a relatively simple optical setup, in a quantum network, can increase the rate at which the network users establish conference keys over long distances. In particular, the scaling improvement in the key rate (the key rate scales with η instead of η^2) matches the one that could be achieved by future quantum repeaters.

In addition, our protocol is readily implementable with current technology as it does not add further experimental requirements compared to state-of-the-art experiments on TFQKD protocols [23–33]. As a matter of fact, for two parties our CKA scheme reduces to the bipartite TFQKD protocol in Ref. [17], which has already been implemented in several experiments [23,25,28,31]. In such experiments, phase-tracking and phase-locking techniques are required in order to ensure that the parties' signals remain in phase. This, however, might become more challenging when more parties are involved. A solution could be found by multiplexing in time and/or frequency as shown in Refs. [47,48]. We remark that the implementation of our CKA protocol would represent the first instance of a multipartite conference key agreement, which does not rely on GHZ-type states.

The work presented in this paper can be further developed along different lines of research. From a security perspective, a complete finite-key analysis along the lines of the proof given in Ref. [46] for bipartite TFQKD is required, in order to prove the protocol secure in the presence of statistical fluctuations and coherent attacks.

Moreover, our decoy-state analysis assumes a highly symmetrical configuration where every party uses the same set of decoy intensities, which is optimal in the scenario of symmetric channel losses analyzed in this work. However, real-life scenarios would likely display asymmetric channel losses, which require a more general decoy analysis with independent decoy intensities for each party, as shown for the bipartite case in Ref. [49]. On a similar note, our decoy analysis employs only two decoy settings per party, which is not sufficient to achieve close-to-optimal key rates (i.e., key rates obtained with infinite decoy settings), as shown by Fig. 4. Hence, it is likely that using more than two decoy settings to derive numerical or analytical bounds on the yields appearing in the phase error rate could improve the resulting key rate.

Finally, the efficiency of the protocol at lower losses could be improved by retaining those rounds where more than one detector clicks and using them to extract extra conference key bits. The security proof presented in this work could be naturally extended to make use of such rounds.

To conclude, we believe that our work constitutes a significant step towards increasing the practicality of multipartite cryptographic protocols and their applicability in high-loss regimes.

Note added.—Recently, another CKA scheme has been posted on preprint servers [50], with our same goal of extending the communication distance of CKA. However, we believe that the protocol in Ref. [50] is much more technologically demanding than ours. For the legitimate users, the protocol in Ref. [50] requires the parallel generation of multiple one-photon pulses from each party, compared to only a phase randomized weak coherent pulse in our protocol. For the measuring station, the protocol in Ref. [50] requires a quantum nondemolition measurement that heralds the arrival of a photon, followed by a GHZ-state analyzer acting on the heralded signals, while in our protocol we require only an interferometric measurement as depicted in Fig. 2.

CODE AVAILABILITY

The code used to run the simulations can be made available upon request to the authors.

APPENDIX A: THE BALANCED BEAM-SPLITTER NETWORK

In this Appendix, we provide a complete description of the BBS network that describes the honest implementation of the untrusted relay. The network is composed of s layers, labeled by $r = 0, \ldots, s - 1$, and each layer receives as input $M = 2^s$ optical modes $\hat{a}_i^{(r)}$, for $0 \leq i \leq M - 1$. Note that for $r = 0$ the modes correspond to the modes arriving at the relay from the parties.

In a generic layer r, the optical mode $\hat{a}_i^{(r)}$ is mixed with the mode $\hat{a}_{i+2^r}^{(r)}$ in a BBS, for all modes $\hat{a}_i \in F_r$. The set F_r for layer r contains the modes:

$$F_r := \bigcup_{k=0}^{2^{s-r-1}-1} \{\hat{a}_{k2^{r+1}}, \hat{a}_{k2^{r+1}+1}, \ldots, \hat{a}_{k2^{r+1}+2^r-1}\}. \quad (A1)$$

For example, F_0 contains the even modes and F_1 contains modes $0, 1, 3, 4$, and so on. This pattern repeats until the last layer, that contains the first half of the modes. Each layer contains $M/2$ beam splitters. Hence, the total number of beam splitters in the BBS network, in terms of the number of inputs M, is

$$n_{\mathrm{BS}} = \frac{M}{2} \log_2 M. \quad (A2)$$

We note that the BBS network, due to its structure, must be prepared for a number of inputs M equal to a power of 2 but can be used by any number of parties $N \leq M$. We also remark that, for $s = 1$, the BBS network reduces to a single beam splitter and coincides with the setup used in the TFQKD protocol of Ref. [17].

We are interested in the evolution of the creation operators in layer r through a BBS, which is given by

$$(\hat{a}_i^{(r)})^\dagger \rightarrow \frac{1}{\sqrt{2}}[(\hat{a}_i^{(r+1)})^\dagger + (\hat{a}_{i+2^r}^{(r+1)})^\dagger] \quad \forall i \in F_r$$

$$(\hat{a}_j^{(r)})^\dagger \rightarrow \frac{1}{\sqrt{2}}[(\hat{a}_{j-2^r}^{(r+1)})^\dagger - (\hat{a}_j^{(r+1)})^\dagger] \quad \forall j \in \overline{F}_r, \quad (A3)$$

where $\overline{F}_r$ indicates the complement of F_r.

By going through all layers until $r = s - 1$, we are able to transform each input mode in a balanced combination of all the output modes, whose coefficients are at most a minus sign. The global mode transformation, which includes the transformation of each layer, is given in the following theorem.

Theorem 2.—Given $M = 2^s$ input modes in the BBS network described above where, in each layer r, the modes

transform according to Eq. (A3). Then, the global evolution of the modes over all the s layers is given by

$$\hat{a}_i^\dagger \rightarrow \frac{1}{(\sqrt{2})^s} \sum_{k=0}^{2^s-1} f_{k,i}^{(s)} (\hat{a}_k^{(s)})^\dagger \quad \forall i = 0, \ldots, 2^s - 1, \quad (A4)$$

where the function $f_{k,i}^{(s)}$ is given by

$$f_{k,i}^{(s)} = \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l \rfloor \lfloor i/2^l \rfloor}, \quad (A5)$$

and $\lfloor \cdot \rfloor$ is the floor function. Moreover, $f_{k,i}^{(s)}$ can be recast as follows:

$$f_{k,i}^{(s)} = (-1)^{\vec{k} \cdot \vec{i}}, \quad (A6)$$

where $\vec{k}$ and $\vec{i}$ are the binary vectors of length s representing the integers k and i in binary representation.

Proof.—The theorem is proved by induction on s. Hence, the first step of the proof is to prove the result for $s = 1$, i.e., just two inputs. We thus have two optical modes $\hat{a}_0^\dagger$ and $\hat{a}_1^\dagger$ mixed in a BBS. The transformation of the modes is given in Eq. (A3), for $r = 0$, i.e.,

$$\hat{a}_0^\dagger \rightarrow \frac{1}{\sqrt{2}}[(\hat{a}_0^{(1)})^\dagger + (\hat{a}_1^{(1)})^\dagger]$$

$$\hat{a}_1^\dagger \rightarrow \frac{1}{\sqrt{2}}[(\hat{a}_0^{(1)})^\dagger - (\hat{a}_1^{(1)})^\dagger]. \quad (A7)$$

The formula provided in the theorem's statement, Eq. (A4), for $s = 1$ reads

$$\hat{a}_i \rightarrow \frac{1}{\sqrt{2}} \sum_{k=0}^{1} (-1)^{ki} (\hat{a}_k^{(1)})^\dagger, \quad (A8)$$

which is equivalent to the transformation of the modes of Eq. (A7). The theorem is thus proved for $s = 1$.

Now, in the inductive step we assume that the theorem's statement in Eq. (A4) is correct for generic s and show that it induces the same transformation for $s + 1$, i.e., that the theorem holds for $s + 1$.

We start by adding to the modes labeled by i another set of 2^s modes, labeled by $j = 2^s, \ldots, 2^{s+1} - 1$, that undergoes the same kind of transformations, i.e.,

$$\hat{a}_j^\dagger \rightarrow \frac{1}{(\sqrt{2})^s} \sum_{k=2^s}^{2^{s+1}-1} f_{k,j}^{(s)} (\hat{a}_k^{(s)})^\dagger \quad \forall j = 2^s, \ldots, 2^{s+1} - 1. \quad (A9)$$

We now follow the prescription in Eq. (A3) and combine the modes in the $s + 1$ layer of the BBS network. This means that we combine the mode $(\hat{a}_i^{(s)})^\dagger$ with the corresponding mode $(\hat{a}_{i+2^s}^{(s)})^\dagger$, and obtain

$$(\hat{a}_i^{(s)})^\dagger \to \frac{1}{\sqrt{2}}[(\hat{a}_i^{(s+1)})^\dagger + (\hat{a}_{i+2^s}^{(s+1)})^\dagger] \quad \forall i = 0, \ldots, 2^s - 1$$

$$(\hat{a}_j^{(s)})^\dagger \to \frac{1}{\sqrt{2}}[(\hat{a}_{j-2^s}^{(r+1)})^\dagger - (\hat{a}_j^{(s+1)})^\dagger] \quad \forall j = 2^s, \ldots, 2^{s+1} - 1.$$

$$(A10)$$

We use the assumption in the inductive step. That is, we use Eqs. (A4) and (A9) to describe the transformations of the modes in the first s layers. We separately address the transformations on the first 2^s modes $\hat{a}_i^\dagger$, described by Eq. (A4), and the transformations on the other 2^s modes $\hat{a}_j^\dagger$, described by Eq. (A9).

    1.   For the modes $\hat{a}_i^\dagger$ with $i = 0, \ldots, 2^s - 1$, we employ the first equation in Eq. (A10) together with Eq. (A4). We obtain the following transformation of the modes after $s + 1$ layers:

$$\hat{a}_i^\dagger \to \frac{1}{(\sqrt{2})^s} \sum_{k=0}^{2^s-1} f_{k,i}^{(s)} \frac{1}{\sqrt{2}}[(\hat{a}_k^{(s+1)})^\dagger + (\hat{a}_{k+2^s}^{(s+1)})^\dagger]$$

$$= \frac{1}{(\sqrt{2})^{s+1}} \left(\sum_{k=0}^{2^s-1} f_{k,i}^{(s)} (\hat{a}_k^{(s+1)})^\dagger + \sum_{k=0}^{2^s-1} f_{k,i}^{(s)} (\hat{a}_{k+2^s}^{(s+1)})^\dagger \right)$$

$$(A11)$$

Now let us consider the coefficient $f_{k,i}^{(s+1)}$. By definition (A5), we have

$$f_{k,i}^{(s+1)} = \prod_{l=0}^{s} (-1)^{\lfloor k/2^l \rfloor \lfloor i/2^l \rfloor}$$

$$= (-1)^{\lfloor k/2^s \rfloor \lfloor i/2^s \rfloor} \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l \rfloor \lfloor i/2^l \rfloor}$$

$$= (-1)^{\lfloor k/2^s \rfloor \lfloor i/2^s \rfloor} f_{k,i}^{(s)}. \quad (A12)$$

However, since $i = 0, \ldots, 2^s - 1$ we have that $\lfloor i/2^s \rfloor = 0 \; \forall i$, which in turn implies

$$f_{k,i}^{(s+1)} = f_{k,i}^{(s)} \quad \forall i = 0, \ldots, 2^s - 1, \forall k. \quad (A13)$$

We use this result in Eq. (A11) combined with a rescaling of the second sum with $k \to k - 2^s$ to write

$$\hat{a}_i^\dagger \to \frac{1}{(\sqrt{2})^{s+1}} \left(\sum_{k=0}^{2^s-1} f_{k,i}^{(s+1)} (\hat{a}_k^{(s+1)})^\dagger \right.$$

$$\left. + \sum_{k=2^s}^{2^{s+1}-1} f_{k-2^s,i}^{(s)} (\hat{a}_k^{(s+1)})^\dagger \right), \quad (A14)$$

where

$$f_{k-2^s,i}^{(s)} = \prod_{l=0}^{s-1} (-1)^{\lfloor (k-2^s)/2^l \rfloor \lfloor i/2^l \rfloor} = \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l - 2^{s-l} \rfloor \lfloor i/2^l \rfloor}.$$

$$(A15)$$

Since $k \geq 2^s$ we have that $k/2^l \geq 2^{s-l}$. Moreover, $s > l$ for every l, which means that 2^{s-l} is a positive, even integer. We thus can write

$$f_{k-2^s,i}^{(s)} = \prod_{l=0}^{s-1} (-1)^{\left(\lfloor k/2^l \rfloor - 2^{s-l} \right) \lfloor i/2^l \rfloor}$$

$$= \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l \rfloor \lfloor i/2^l \rfloor} (-1)^{-2^{s-l} \lfloor i/2^l \rfloor}$$

$$= \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l \rfloor \lfloor i/2^l \rfloor} = f_{k,i}^{(s)} = f_{k,i}^{(s+1)}, \quad (A16)$$

where $(-1)^{-2^{s-l} \lfloor i/2^l \rfloor} = 1 \; \forall i$ because 2^{s-l} is even for all l and where we use Eq. (A13) in the last equality. With the last expression, we can simplify (A14) as follows:

$$\hat{a}_i^\dagger \to \frac{1}{(\sqrt{2})^{s+1}} \left(\sum_{k=0}^{2^s-1} f_{k,i}^{(s+1)} (\hat{a}_k^{(s+1)})^\dagger \right.$$

$$\left. + \sum_{k=2^s}^{2^{s+1}-1} f_{k,i}^{(s+1)} (\hat{a}_k^{(s+1)})^\dagger \right)$$

$$= \frac{1}{(\sqrt{2})^{s+1}} \sum_{k=0}^{2^{s+1}-1} f_{k,i}^{(s+1)} (\hat{a}_k^{(s+1)})^\dagger, \quad (A17)$$

which concludes the proof for $i = 0, \ldots, 2^s - 1$.

    2.   For the modes $\hat{a}_j^\dagger$, with $j = 2^s, \ldots, 2^{s+1} - 1$, we combine the second equation in Eq. (A10) with the assumption (A9) and obtain

$$\hat{a}_j^\dagger \to \frac{1}{(\sqrt{2})^{s+1}} \left(\sum_{k=2^s}^{2^{s+1}-1} f_{k,j}^{(s)} (\hat{a}_{k-2^s}^{(s+1)})^\dagger - \sum_{k=2^s}^{2^{s+1}-1} f_{k,j}^{(s)} (\hat{a}_k^{(s+1)})^\dagger \right).$$

$$(A18)$$

Once again, we can rescale the first sum with $k \to k + 2^s$ in the last expression and obtain

$$\hat{a}_j^\dagger \to \frac{1}{(\sqrt{2})^{s+1}} \left(\sum_{k=0}^{2^s-1} f_{k+2^s,j}^{(s)} (\hat{a}_k^{(s+1)})^\dagger - \sum_{k=2^s}^{2^{s+1}-1} f_{k,j}^{(s)} (\hat{a}_k^{(s+1)})^\dagger \right).$$

(A19)

Since 2^{s-l} is a positive, even integer, we can simplify the coefficient in the first sum as follows:

$$f_{k+2^s,j}^{(s)} = \prod_{l=0}^{s-1} (-1)^{\left(\lfloor k/2^l \rfloor + 2^{s-l} \right) \lfloor j/2^l \rfloor}$$

$$= \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l \rfloor \lfloor j/2^l \rfloor} (-1)^{2^{s-l} \lfloor j/2^l \rfloor}$$

$$= \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l \rfloor \lfloor j/2^l \rfloor} = f_{k,j}^{(s)}.$$

(A20)

Moreover, since $k = 0, \ldots, 2^s - 1$, one has that $\lfloor k/2^s \rfloor = 0$ and hence that

$$f_{k,j}^{(s+1)} = \prod_{l=0}^{s} (-1)^{\lfloor k/2^l \rfloor \lfloor j/2^l \rfloor}$$

$$= (-1)^{\lfloor k/2^s \rfloor \lfloor j/2^s \rfloor} \prod_{l=0}^{s-1} (-1)^{\lfloor k/2^l \rfloor \lfloor j/2^l \rfloor}$$

$$= (-1)^{\lfloor k/2^s \rfloor \lfloor i/2^s \rfloor} f_{k,i}^{(s)} = f_{k,i}^{(s)},$$

(A21)

which means that we can replace the coefficient $f_{k+2^s,j}^{(s)}$ in the first sum of Eq. (A19) with $f_{k,j}^{(s+1)}$. Regarding the second sum in Eq. (A19), we can write the coefficient as

$$(-1) f_{k,j}^{(s)} = (-1)^{g(k,j)} f_{k,j}^{(s)},$$

(A22)

where $g(k,j)$ is a function that is odd for $j, k = 2^s, \ldots, 2^{s+1} - 1$. For instance, we can choose the function to be the following:

$$g(k,j) = \lfloor k/2^s \rfloor \lfloor j/2^s \rfloor.$$

(A23)

Then, the coefficient of the second sum in Eq. (A19) becomes

$$(-1) f_{k,j}^{(s)} = (-1)^{\lfloor k/2^s \rfloor \lfloor j/2^s \rfloor} f_{k,j}^{(s)} \equiv f_{k,j}^{(s+1)}.$$

(A24)

With the above expressions, we can recast Eq. (A19) as follows and conclude the proof for $j = 2^s, \ldots, 2^{s+1} - 1$:

$$\hat{a}_j^\dagger \to \frac{1}{(\sqrt{2})^{s+1}} \left(\sum_{k=0}^{2^s-1} f_{k,j}^{(s+1)} (\hat{a}_k^{(s+1)})^\dagger \right.$$

$$\left. + \sum_{k=2^s}^{2^{s+1}-1} f_{k,j}^{(s+1)} (\hat{a}_k^{(s+1)})^\dagger \right)$$

$$= \frac{1}{(\sqrt{2})^{s+1}} \sum_{k=0}^{2^{s+1}-1} f_{k,j}^{(s+1)} (\hat{a}_k^{(s+1)})^\dagger.$$

(A25)

The combination of the two results in Eqs. (A17) and (A25) imply that the global transformation of the modes, for $M = 2^{s+1}$ inputs, is given by Eq. (A4) where s is replaced by $s + 1$. This proves the theorem for $s + 1$ and concludes the proof. ∎

APPENDIX B: *W*-STATE CORRELATIONS

In this Appendix we present the logical steps that brought us to design the protocol presented in Sec. II and show the connection between the correlations generated by our protocol and the correlations of the *W* state [38].

We start by describing an Ideal protocol, i.e., a protocol that is less practical than the one presented in the main text but has the merit of elucidating the core ideas that lead to the CKA protocol of Sec. II. The protocol is run by N parties, which we call $A_0, \ldots, A_{N-1}$, and consists of the following steps.

Protocol 2 (Ideal protocol)

---

1. Quantum part: repeat what follows for a sufficient amount of iterations.

1.1. Every party holds an optical mode a_i and a qubit Q_i and prepares the following entangled state:

$$|\phi_i\rangle = \sqrt{q_i}|0\rangle_{Q_i}|0\rangle_{a_i} + \sqrt{1 - q_i}|1\rangle_{Q_i}|1\rangle_{a_i}, \quad \text{(B1)}$$

where $|0\rangle_{Q_i}$ and $|1\rangle_{Q_i}$ are two orthogonal states of the qubit, $|0\rangle_{a_i}$ and $|1\rangle_{a_i}$ are the vacuum and one-photon state of the optical mode, respectively, and $0 < q_i < 1$.

1.2. Every party sends their optical pulse through a noisy and lossy channel to an untrusted relay.

1.3. In the untrusted relay, the optical signals interfere in a BBS network of $M = 2^s$ inputs and M outputs, for some natural number s with $M \geq N$. The BBS network is described in Appendix A. The network transforms the input modes in a balanced combination of the output modes, i.e.,

$$\hat{a}_i^\dagger \to \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} (-1)^{\vec{j} \cdot \vec{i}} \hat{a}_j^\dagger, \quad \text{(B2)}$$

where $\hat{a}_i^\dagger$ and $\hat{d}_j^\dagger$ are the creation operators of the input and output modes, respectively, and $\vec{j}$ and $\vec{i}$ the binary representations of the integers j and i and $\vec{j} \cdot \vec{i}$ is their scalar product.

1.4. The untrusted relay measures each output mode d_j with a threshold detector D_j, for $j = 0, \ldots, M-1$. The relay announces the detection pattern $\vec{k} \in \{0,1\}^M$ for each detector, where $k_j = 1$ if detector D_j clicked and $k_j = 0$ otherwise. The round gets discarded unless only one detector clicked, i.e., if $|\vec{k}| = 1$, where $|\vec{x}|$ is the Hamming weight of vector $\vec{x}$.

1.5. Each party A_i measures their qubit Q_i. If the round is labeled as a PE round, each party measures in the Z basis and obtains an outcome $Z_i = \pm 1$. If the round is a KG round, each party measures in the X basis and obtains outcome $X_i = \pm 1$.

2. Parameter estimation: the parties partition their outcomes in M sets, where each set corresponds to the event Ω_j where only detector D_j clicks. For each partition, the parties reveal a fraction of their X-basis outcomes in order to compute the QBER, with respect to reference party A_0. The QBER is defined as

$$Q_{X_0,X_i}^j = \Pr(X_0 \neq (-1)^{\vec{j}\cdot\vec{i}} X_i | \Omega_j, R_{KG}). \quad (B3)$$

Similarly, for each partition of outcomes the parties reveal their Z-basis outcomes and evaluate the phase error rate, defined as follows:

$$Q_Z^j = \Pr(\prod_{i=0}^{N-1} Z_i = 1 | \Omega_j, R_{KG}). \quad (B4)$$

3. Classical postprocessing: the parties extract a secret conference key from the remaining undisclosed X-basis outcomes. To do so, for each partition labeled by Ω_j, party A_i flips their X-basis outcomes when $(-1)^{\vec{j}\cdot\vec{i}} = -1$. The parties then perform error correction and privacy amplification.

We remark that the probabilities defining the QBER (B3) and the phase error rate (B4) are conditioned on the event that only detector D_j clicked and the round was chosen to be a KG round. While the QBER can be directly computed from the outcomes collected in KG rounds, the phase error rate refers to the hypothetical scenario where the parties measured in the Z basis in a KG round. However, since the only difference between KG and PE rounds is the local qubit measurement, the choice of the type of round can be delayed until the qubit measurement is performed. Hence, the phase error rate, as defined in Eq. (B4), effectively coincides with the analogous quantity observed from the PE data: $Q_Z^j \equiv \Pr(\prod_{i=0}^{N-1} Z_i = 1 | \Omega_j, R_{PE})$. As we discuss below, this fact does not hold in our CKA protocol (Sec. II), where the

phase error rate (18) is indirectly bounded with the PE statistics thanks to a multiparty decoy-state method.

The Ideal protocol is designed to exploit the correlations of a particular class of multipartite, W-type states, which are postselected due to single-photon interference. As a matter of fact, a noisy version of such states is recovered as the conditional state of the qubit systems postselected on the event that only detector D_j clicks. In order to see this more clearly, one can derive such a state under the Ideal conditions of no losses in the channels and $q_i = q \to 1$ for every i—indeed, the optimal values of q are close to one [34], hence we approximate the state to first order in $(1-q)$. Under these simplifications, the state of the qubits $Q_0 \ldots Q_{N-1}$ shared by the N parties, once postselected on the click of detector D_j, reads

$$|W_j\rangle_{Q_0,\ldots Q_{N-1}} := \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{\vec{j}\cdot\vec{i}} |\vec{b}_i\rangle_{Q_0,\ldots Q_{N-1}}, \quad (B5)$$

where the vector $\vec{b}_i$ is defined as the N-bit vector of all zeroes except for the ith element that is one.

The state in Eq. (B5) is a W-type state, where each term in the sum presents a real phase determined by the detector that clicked. The state is postselected from the events where only one photon is effectively sent by any of the parties with equal probability. Indeed, under the above approximations, the probability that the W-type state in Eq. (B5) is postselected is $q^{N-1}(1-q)N/M$.

In this regard, the Ideal protocol resembles the CKA protocol of Ref. [34] as it exploits the multipartite correlations of a W state to establish a shared conference key. As a matter of fact, we note that in the classical postprocessing the parties flip their X-basis outcomes according to $(-1)^{\vec{j}\cdot\vec{i}}$, where $\vec{i}$ depends on the party and $\vec{j}$ on the detector that clicked. This can be equivalently seen as party A_i applying a Z gate on their qubit before the X-basis measurement, if $\vec{j} \cdot \vec{i}$ is odd. In other words, party A_i applies the gate $Z^{\vec{j}\cdot\vec{i}}$ (note that $Z^2 = \mathbb{1}$). Since such a gate does not change the Z-basis outcomes in the PE rounds, we can assume, without loss of generality, that party A_i applies the gate $Z^{\vec{j}\cdot\vec{i}}$ before measuring their qubit in any basis. If we now apply the gates in the postselected state of the qubits (B5), we obtain

$$\begin{aligned} |W_j\rangle_{Q_0,\ldots Q_{N-1}} &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{\vec{j}\cdot\vec{i}} \bigotimes_{k=0}^{N-1} Z^{\vec{j}\cdot\vec{k}} |\vec{b}_i\rangle_{Q_0,\ldots Q_{N-1}} \\ &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} (-1)^{\vec{j}\cdot\vec{i}} (-1)^{\vec{j}\cdot\vec{i}} |\vec{b}_i\rangle_{Q_0,\ldots Q_{N-1}} \\ &= \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |\vec{b}_i\rangle_{Q_0,\ldots Q_{N-1}}, \quad (B6) \end{aligned}$$

where we use the fact that the operator $Z^{\vec{j}\cdot\vec{k}}$ has no effect on the ket $|\vec{b}_i\rangle$ except for $k = i$, i.e., when it acts on the ith qubit that is in state $|1\rangle$. From Eq. (B6) we see that the postselected state, after the local operations that simulate the classical postprocessing of the outcomes, coincides with the W state, as claimed. The Ideal protocol presents a crucial difference from the protocol in Ref. [34], which is made explicit in the following remark:

Remark.—In Ref. [34] the parties needed to tailor their KG measurements depending on which detector clicks, in order to neutralize the effects of complex phases in their postselected W-type state. In the Ideal protocol, thanks to the bespoke BBS network, the postselected state (B5) only presents real phases, which are corrected as discussed above by simply flipping the KG outcomes and without changing the measurement basis.

This implies that, in the Ideal protocol, the parties' measurements are independent of the relay's announcements, hence they commute with the action of the relay. This enables us to reformulate the Ideal protocol in prepare-and-measure (PM) form. In the resulting PM protocol, the parties first measure their qubits and record the outcome. Then they send the optical mode, whose state is conditioned on the outcome, to the relay. Hence, the PM protocol coincides with the Ideal protocol except for Step 1.1.

Protocol 3 (Prepare-and-measure protocol)

1.   Quantum part: repeat what follows for a sufficient amount of iterations.

1.1. Each party A_i prepares an optical mode a_i in a state that depends on whether the round is labeled as a PE or KG round.

(a) In a PE round, they prepare the vacuum state $|0\rangle_{a_i}$ with probability q_i, corresponding to the outcome $Z_i = +1$, and the one-photon state $|1\rangle_{a_i}$ with probability $1 - q_i$, corresponding to the outcome $Z_i = -1$.

(b) In a KG round, they prepare with equal probability either the state $|+\rangle_{a_i} = \sqrt{q_i}|0\rangle_{a_i} + \sqrt{1 - q_i}|1\rangle_{a_i}$, corresponding to the outcome $X_i = +1$, or the state $|-\rangle_{a_i} = \sqrt{q_i}|0\rangle_{a_i} - \sqrt{1 - q_i}|1\rangle_{a_i}$, corresponding to the outcome $X_i = -1$.

1.2. same as in Ideal prot.

1.3. same as in Ideal prot.

1.4. same as in Ideal prot.

2.   same as in Ideal prot.

3.   same as in Ideal prot.

Note that, while the PM protocol is more practical than the Ideal protocol (e.g., it does not require qubit-photon entanglement), it is equivalent to the latter from the point of view of security, since an adversary could not distinguish which of the two protocols is run. Despite the increased practicality, the PM protocol still requires the preparation of single-photon states and their superposition with the vacuum. This prompts us to reduce even further the complexity of the protocol's implementation and obtain a practical, prepare-and-measure, CKA protocol.

In order to derive a practical CKA protocol, we observe that the states prepared in the KG rounds of the PM protocol ($|\pm\rangle_{a_i}$) can be approximated by coherent states of suitable amplitude ($|\pm\alpha_i\rangle$, for $\alpha_i \in \mathbb{R}$), where the information about the X-basis outcome is encoded in the amplitude's sign. At the same time, the statistics collected in PE rounds and used to compute the phase error rate (B4) are linked to the so-called yields, i.e., the probability that a detector clicks given that each party sent a fixed number of photons. This suggests us to prepare phase-randomized coherent states in PE rounds and use their detection statistics to apply the decoy-state method and compute the yields, with which we bound the phase error rate. This heuristic reasoning leads us to the practical CKA protocol presented in Sec. II, where, we recall, each party A_i prepares a coherent state $|x_i\alpha_i\rangle_{a_i}$ with $x_i = \pm1$ in KG rounds and phase-randomized coherent states in PE rounds.

We emphasize that, in the protocol of Sec. II, the choice of the type of round (KG or PE) cannot be delayed until after the action of the untrusted relay, contrary to the Ideal protocol. Indeed, the average state prepared by A_i in KG rounds, $(1/2)(|\alpha_i\rangle\langle\alpha_i| + |-\alpha_i\rangle\langle-\alpha_i|)$, differs from the average state prepared in PE rounds, $(1/|\mathcal{S}_i|)\sum_k \rho_{a_i}(\beta_k)$, due to the coherences of the former in the Fock basis. This means that an adversary controlling the relay could partially distinguish the type of round being executed and act accordingly. Another way to see this is that there is no equivalent entanglement-based version of the CKA protocol. That is, party A_i cannot find two suitable POVMs (one for KG rounds and one for PE rounds) such that the state of their optical mode, conditioned on measuring with one of the two POVMs a fictitious system entangled with the optical mode, corresponds to the state that A_i should prepare in that round [51].

One of the implications of the above fact is that the phase error rate (B4) affecting the KG rounds cannot be directly observed from the statistics of the PE rounds, as instead happens in the Ideal protocol. Nevertheless, in the security proof provided in Sec. III, we show how to use the PE statistics to derive an upper bound on the phase error rate (B4). Specifically, we develop a multipartite decoy-state method that allows us to bound certain yields through the PE statistics. The yields, in turn, are needed to analytically upper bound the phase error rate with Eq. (7).

This concludes our connection between the Ideal protocol, which manifestly makes use of W-state correlations and whose phase error rate can be directly observed in PE rounds, and the CKA protocol discussed in the main text, whose phase error rate is bounded by PE statistics combined with the decoy-state method.

APPENDIX C: ANALYTICAL UPPER BOUND ON THE YIELDS

In this Appendix, we report the full derivation of the analytical bounds on the yields as a function of the observed gains, Eq. (34). The bounds are derived with a multipartite decoy-state method in which each party is provided with the same set of two decoy intensities: $\mathcal{S} = \{\beta_0, \beta_1\}$.

We recall that the gains are probabilities that can be directly estimated from the observed data and are defined as $G_{\vec{f}}^j := \Pr\left(\Omega_j | \beta_{f_0}, \ldots, \beta_{f_{N-1}}\right)$, where $\vec{f}$ is an N-dimensional binary vector that covers all the possible choices of intensities by the parties. From Eq. (25) in Sec. III, we show that the gains are related to the yields by the following equality:

$$
\begin{aligned}
G_{\vec{f}}^j &= \sum_{n_0,\ldots,n_{N-1}=0}^{\infty} Y_{n_0,\ldots,n_{N-1}}^j \prod_{i=0}^{N-1} P_{\beta_{f_i}}(n_i) \\
&= \sum_{n_0,\ldots,n_{N-1}=0}^{\infty} Y_{n_0,\ldots,n_{N-1}}^j \prod_{i=0}^{N-1} \frac{e^{-\beta_{f_i}} \beta_{f_i}^{n_i}}{n_i!} \\
&= \prod_{i=0}^{N-1} e^{-\beta_{f_i}} \sum_{n_0,\ldots,n_{N-1}=0}^{\infty} \frac{Y_{n_0,\ldots,n_{N-1}}^j}{n_0! \cdots n_{N-1}!} \prod_{i=0}^{N-1} \beta_{f_i}^{n_i}.
\end{aligned}
\tag{C1}
$$

We remark that, in principle, the gains can depend on the detector D_j that clicks and so can the yields. However, for simplicity of notation, in this section we drop the superscript j from the gains and yields. Moreover, in our simulations, due to the symmetric losses affecting each party, the gains and hence the yields are independent of which detector clicks (see Appendix D). Hence their dependency on j vanishes.

The last equality in Eq. (C1) brings us to define a rescaled gain, $\tilde{G}$, as follows:

$$
\tilde{G}_{\vec{f}} := \frac{G_{\vec{f}}}{\prod_{i=0}^{N-1} e^{-\beta_{f_i}}} = \sum_{n_0,\ldots,n_{N-1}=0}^{\infty} \frac{Y_{n_0,\ldots,n_{N-1}}}{n_0! \cdots n_{N-1}!} \prod_{i=0}^{N-1} \beta_{f_i}^{n_i}.
\tag{C2}
$$

We now define, from a fixed binary vector $\vec{h}$ of dimension N and Hamming weight $|\vec{h}| = m$, the following quantity:

$$
B_{\vec{h}} := \sum_{n_0,\ldots,n_{N-1}=0}^{\infty} \frac{Y_{n_0,\ldots,n_{N-1}}}{n_0! \cdots n_{N-1}!} \prod_{i=0}^{N-1} \left(\beta_1^{1-h_i} \beta_0^{n_i} - \beta_0^{1-h_i} \beta_1^{n_i}\right),
\tag{C3}
$$

which can be recast as a combination of rescaled gains $\tilde{G}_{\vec{f}}$. To see this, we expand the product over i in the last expression as a sum of 2^N products, each labeled by a binary

vector $\vec{f}$, where each term in the sum is the product of either $\beta_1^{1-h_i} \beta_0^{n_i}$ or $-\beta_0^{1-h_i} \beta_1^{n_i}$ for every $i = 0, \ldots, N-1$. In particular, $f_i = 0$ ($f_i = 1$) indicates that the former (latter) quantity is picked. With this in mind, we can write

$$
\begin{aligned}
&\prod_{i=0}^{N-1} \left(\beta_1^{1-h_i} \beta_0^{n_i} - \beta_0^{1-h_i} \beta_1^{n_i}\right) \\
&= \sum_{f=0}^{2^N-1} \prod_{i=0}^{N-1} \beta_{f_i}^{n_i} (-1)^{f_i} \beta_0^{(1-h_i)f_i} \beta_1^{(1-h_i)(1-f_i)} \\
&= \sum_{f=0}^{2^N-1} (-1)^{|\vec{f}|} \beta_0^{(\vec{1}-\vec{h})\cdot\vec{f}} \beta_1^{(\vec{1}-\vec{h})\cdot(\vec{1}-\vec{f})} \prod_{i=0}^{N-1} \beta_{f_i}^{n_i}.
\end{aligned}
\tag{C4}
$$

By replacing the last expression in Eq. (C3), we can employ Eq. (C2) to directly relate $B_{\vec{h}}$ and $\tilde{G}_{\vec{f}}$. We obtain

$$
B_{\vec{h}} = \sum_{f=0}^{2^N-1} (-1)^{|\vec{f}|} \beta_0^{(\vec{1}-\vec{h})\cdot\vec{f}} \beta_1^{(\vec{1}-\vec{h})\cdot(\vec{1}-\vec{f})} \tilde{G}_{\vec{f}}.
\tag{C5}
$$

This expression is fundamental as is constitutes the link between the quantity $B_{\vec{h}}$, which in the following is used to bound the yields, and the observed gains.

By recasting Eq. (C3) as follows:

$$
\begin{aligned}
B_{\vec{h}} = \sum_{n_0,\ldots,n_{N-1}=0}^{\infty} \frac{Y_{n_0,\ldots,n_{N-1}}}{n_0! \cdots n_{N-1}!} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} (\beta_0^{n_i} - \beta_1^{n_i}) \\
\times \prod_{\substack{i \text{ s.t.} \\ h_i=0}} (\beta_1 \beta_0^{n_i} - \beta_0 \beta_1^{n_i}),
\end{aligned}
\tag{C6}
$$

we notice that, whenever $h_i = 1$, the coefficient of the yields $Y_{n_0,\ldots,0,\ldots,n_{N-1}}$ (i.e., with with $n_i = 0$) is null, implying that they do not contribute to the value of $B_{\vec{h}}$. Similarly, when $h_i = 0$, all yields of the form $Y_{n_0,\ldots,1,\ldots,n_{N-1}}$ are removed. With this observation, we can now obtain a nontrivial upper bound on any yield $Y_{n_0,\ldots,n_{N-1}}$ in terms of a certain combination of $B_{\vec{h}}$.

To do so, we recast Eq. (C6) as follows, where in the first term we sum only over the indexes n_i that correspond to $h_i = 1$ and set all the other photon indexes to zero, while in the second term we account for all the other possibilities:

$$B_{\vec{h}} = (-1)^{N-m}(\beta_0 - \beta_1)^{N-m} \sum_{(n_0,\ldots,n_{N-1})\in\mathcal{N}(\vec{h})} \frac{Y_{n_0,\ldots,n_{N-1}}}{n_0!\cdots n_{N-1}!} \prod_{\substack{i \text{ s.t.}\\ h_i=1}} (\beta_0^{n_i} - \beta_1^{n_i})$$

$$+ \sum_{(n_0,\ldots,n_{N-1})\in\tilde{\mathcal{N}}(\vec{h})} \frac{Y_{n_0,\ldots,n_{N-1}}}{n_0!\cdots n_{N-1}!} \prod_{\substack{i \text{ s.t.}\\ h_i=1}} (\beta_0^{n_i} - \beta_1^{n_i}) \prod_{\substack{i \text{ s.t.}\\ h_i=0}} (\beta_1\beta_0^{n_i} - \beta_0\beta_1^{n_i}), \tag{C7}$$

where the sets of indexes $\mathcal{N}(\vec{h})$ and $\tilde{\mathcal{N}}(\vec{h})$ are defined as

$$\mathcal{N}(\vec{h}) := \{(n_0,\ldots,n_{N-1}) : n_i = h_i r_i, r_i \geq 1\}, \tag{C8}$$

$$\tilde{\mathcal{N}}(\vec{h}) := \{(n_0,\ldots,n_{N-1}) : n_i \geq 1 \text{ (if } h_i = 1); \; n_i \geq 2 \text{ or } n_i = 0 \text{ (if } h_i = 0)\} \setminus \mathcal{N}(\vec{h}), \tag{C9}$$

where k_i are integers. Note that the sum over n_i in the second term skips the case $n_i = 1$ for $h_i = 0$ since this contribution is null in Eq. (C6) (see observation above).

We observe that the yields in the first sum in Eq. (C7) contain exactly m nonzero photon numbers, which allowed us to factor out the quantities $(\beta_1\beta_0^{n_i} - \beta_0\beta_1^{n_i})$. Now, we split the second sum in Eq. (C7) in a sum of $N - m$ terms, where each term contains only yields with $m + k$ nonzero photon numbers, for $k = 1,\ldots,N - m$. In this way, we can factor out the quantities $(\beta_1\beta_0^{n_i} - \beta_0\beta_1^{n_i})$ even in the second sum. This becomes relevant later, when we want to evaluate the sign in front of each yield. In order to sum over the various combinations of yields with $m + k$ photon numbers, we introduce the binary vectors $\vec{h}^{(k)}$, which can be seen as "expansions" of the vector $\vec{h}$ obtained by flipping k of its zeros to ones. Thus, we have that $|\vec{h}^{(k)}| = m + k$ and that $h_i^{(k)} = 1$ whenever $h_i = 1$, which can be formally stated as the condition: $\vec{h}^{(k)} \wedge \vec{h} = \vec{h}$, where $\wedge$ is the bitwise AND operation. Analogously to $\vec{h}$, when $h_i^{(k)} = 0$ we fix the corresponding photon number n_i to zero. Then, in analogy with $\mathcal{N}(\vec{h})$, we define a set of indexes $\mathcal{N}(\vec{h}, \vec{h}^{(k)})$ for each expansion $\vec{h}^{(k)}$ that represents the combinations of photon numbers that are allowed by the chosen vector $\vec{h}^{(k)}$:

$$\mathcal{N}(\vec{h}, \vec{h}^{(k)}) := \left\{(n_0,\ldots,n_{N-1}) : n_i = h_i^{(k)} r_i, r_i \geq 1 + h_i^{(k)} - h_i\right\}, \tag{C10}$$

where we account for the fact that each additional bit equal to one in $\vec{h}^{(k)}$, which is a zero in $\vec{h}$, corresponds to an index n_i that starts from two instead of one. According to this, we obtain

$$B_{\vec{h}} = (-1)^{N-m}(\beta_0 - \beta_1)^{N-m} \sum_{(n_0,\ldots,n_{N-1})\in\mathcal{N}(\vec{h})} \frac{Y_{n_0,\ldots,n_{N-1}}}{n_0!\cdots n_{N-1}!} \prod_{\substack{i \text{ s.t.}\\ h_i=1}} (\beta_0^{n_i} - \beta_1^{n_i})$$

$$+ \sum_{k=1}^{N-m} (-1)^{N-m-k}(\beta_0 - \beta_1)^{N-m-k}(\beta_0\beta_1)^k \sum_{(n_0,\ldots,n_{N-1})\in\mathcal{N}_k(\vec{h})} \frac{Y_{n_0,\ldots,n_{N-1}}}{n_0!\cdots n_{N-1}!} \prod_{\substack{i \text{ s.t.}\\ h_i=1}} (\beta_0^{n_i} - \beta_1^{n_i}) \prod_{\substack{i \text{ s.t.}\\ h_i^{(k)}-h_i=1}} (\beta_0^{n_i-1} - \beta_1^{n_i-1}), \tag{C11}$$

where we define the following set that accounts for all possible choices of $\vec{h}^{(k)}$, for a given k:

$$\mathcal{N}_k(\vec{h}) := \bigcup_{\substack{\vec{h}^{(k)}\in\{0,1\}^N:\\ |\vec{h}^{(k)}|=m+k\\ \vec{h}^{(k)}\wedge\vec{h}=\vec{h}}} \mathcal{N}(\vec{h}, \vec{h}^{(k)}), \tag{C12}$$

where the operation $\wedge$ represents the entry-wise product. Now, we wish to isolate a specific yield $Y_{u_0,\ldots,u_{N-1}}$ from the first sum in Eq. (C11) in order to derive an upper bound on it. Note that we can choose any combination of photon numbers

$(u_0, \ldots, u_{N-1})$ such that $u_i = h_i k_i$, for $k_i \geq 1$. Since the choice of the vector $\vec{h}$ is arbitrary, the photon numbers are also arbitrary. By isolating the yield $Y_{u_0,\ldots,u_{N-1}}$ in Eq. (C11), we obtain

$$
B_{\vec{h}} = (-1)^{N-m}(\beta_0 - \beta_1)^{N-m} Y_{u_0,\ldots,u_{N-1}} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} \frac{(\beta_0^{u_i} - \beta_1^{u_i})}{u_i!}
$$

$$
+ (-1)^{N-m}(\beta_0 - \beta_1)^{N-m} \sum_{(n_0,\ldots,n_{N-1}) \in \mathcal{N}(\vec{h}) \setminus \{(u_0,\ldots,u_{N-1})\}} \frac{Y_{n_0,\ldots,n_{N-1}}}{n_0! \cdots n_{N-1}!} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} (\beta_0^{n_i} - \beta_1^{n_i})
$$

$$
+ \sum_{k=1}^{N-m} (-1)^{N-m-k}(\beta_0 - \beta_1)^{N-m-k}(\beta_0\beta_1)^k \sum_{(n_0,\ldots,n_{N-1}) \in \mathcal{N}_k(\vec{h})} \frac{Y_{n_0,\ldots,n_{N-1}}}{n_0! \cdots n_{N-1}!} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} (\beta_0^{n_i} - \beta_1^{n_i}) \prod_{\substack{i \text{ s.t.} \\ h_i^{(k)}-h_i=1}} (\beta_0^{n_i-1} - \beta_1^{n_i-1}).
$$

$$\tag{C13}$$

We now derive an upper bound on $Y_{u_0,\ldots,u_{N-1}}$. To this aim, we observe that the yield $Y_{u_0,\ldots,u_{N-1}}$ and each of the yields in the second term in Eq. (C13) are multiplied by coefficients of the same sign. Indeed, they are multiplied by the same number of terms of the form $(\beta_0^s - \beta_1^s)$. More quantitatively, the sign of the coefficient $C_{u_0,\ldots,u_{N-1}}$ of $Y_{u_0,\ldots,u_{N-1}}$ and of the coefficients of the yields in the second term is

$$
\text{sign}(C_{u_0,\ldots,u_{N-1}}) = (-1)^{N-m} \left[\text{sign}(\beta_0 - \beta_1)\right]^N. \tag{C14}
$$

By similar arguments, the yields in the third term in Eq. (C13) are multiplied by coefficients $C_{n_0,\ldots,n_{N-1}}$ with the following sign:

$$
\text{sign}(C_{n_0,\ldots,n_{N-1}}) = (-1)^{N-m-k} \left[\text{sign}(\beta_0 - \beta_1)\right]^N. \tag{C15}
$$

In order to extract an upper bound on $Y_{u_0,\ldots,u_{N-1}}$, we need to minimize all the yields carrying the same sign as $Y_{u_0,\ldots,u_{N-1}}$ and maximize all the yields with opposite sign in Eq. (C13). In our case, this means setting to zero all the yields in the first sum and all the yields in the second sum that correspond to even values of k. The other yields are set to one. By applying this reasoning to Eq. (C13), we obtain the following expression satisfied by an upper bound $U_{u_0,\ldots,u_{N-1}}$ on $Y_{u_0,\ldots,u_{N-1}}$:

$$
B_{\vec{h}} = (-1)^{N-m}(\beta_0 - \beta_1)^{N-m} U_{u_0,\ldots,u_{N-1}} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} \frac{(\beta_0^{u_i} - \beta_1^{u_i})}{u_i!} + \sum_{\substack{k=1 \\ k \text{ odd}}}^{N-m} (-1)^{N-m-k}(\beta_0 - \beta_1)^{N-m-k}(\beta_0\beta_1)^k
$$

$$
\times \sum_{(n_0,\ldots,n_{N-1}) \in \mathcal{N}_k(\vec{h})} \frac{1}{n_0! \cdots n_{N-1}!} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} (\beta_0^{n_i} - \beta_1^{n_i}) \prod_{\substack{i \text{ s.t.} \\ h_i^{(k)}-h_i=1}} (\beta_0^{n_i-1} - \beta_1^{n_i-1}). \tag{C16}
$$

In order to simplify the above expression, we first focus on the term with the sum over k, which we denote $B_{\vec{h}}^{(2)}$ and recast as follows:

$$
B_{\vec{h}}^{(2)} = \sum_{\substack{k=1 \\ k \text{ odd}}}^{N-m} (-1)^{N-m-k}(\beta_0 - \beta_1)^{N-m-k}(\beta_0\beta_1)^k \sum_{(n_0,\ldots,n_{N-1}) \in \mathcal{N}_k(\vec{h})} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} \frac{\beta_0^{n_i} - \beta_1^{n_i}}{n_i!} \prod_{\substack{i \text{ s.t.} \\ h_i^{(k)}-h_i=1}} \frac{\beta_0^{n_i-1} - \beta_1^{n_i-1}}{n_i!}
$$

$$
= \sum_{\substack{k=1 \\ k \text{ odd}}}^{N-m} (-1)^{N-m-k}(\beta_0 - \beta_1)^{N-m-k}(\beta_0\beta_1)^k
$$

$$
\times \sum_{\substack{\vec{h}^{(k)} \in \{0,1\}^N : \\ |\vec{h}^{(k)}|=m+k \\ \vec{h}^{(k)} \wedge \vec{h} = \vec{h}}} \sum_{(n_0,\ldots,n_{N-1}) \in \mathcal{N}(\vec{h},\vec{h}^{(k)})} \prod_{\substack{i \text{ s.t.} \\ h_i=1}} \frac{\beta_0^{n_i} - \beta_1^{n_i}}{n_i!} \prod_{\substack{i \text{ s.t.} \\ h_i^{(k)}-h_i=1}} \frac{\beta_0^{n_i-1} - \beta_1^{n_i-1}}{n_i!}, \tag{C17}
$$

where in the second equality we split the second sum over all the different subsets $\mathcal{N}(\vec{h}, \vec{h}^{(k)})$ in $\mathcal{N}_k(\vec{h})$ using Eq. (C12). We can now swap the innermost sum in the last expression with the products and obtain

$$B_{\vec{h}}^{(2)} = \sum_{\substack{k=1 \\ k\,\text{odd}}}^{N-m}(-1)^{N-m-k}(\beta_0 - \beta_1)^{N-m-k}(\beta_0\beta_1)^k \sum_{\substack{\vec{h}^{(k)}\in\{0,1\}^N: \\ |\vec{h}^{(k)}|=m+k \\ \vec{h}^{(k)}\wedge\vec{h}=\vec{h}}} \prod_{\substack{i\,\text{s.t.} \\ h_i=1}}\left(\sum_{n_i=1}^{\infty}\frac{\beta_0^{n_i}-\beta_1^{n_i}}{n_i!}\right)\prod_{\substack{i\,\text{s.t.} \\ h_i^{(k)}-h_i=1}}\left(\sum_{n_i=2}^{\infty}\frac{\beta_0^{n_i-1}-\beta_1^{n_i-1}}{n_i!}\right). \quad \text{(C18)}$$

It can now be easily seen, using the Taylor series of the exponential function, that the following identities hold:

$$\sum_{n=1}^{\infty}\frac{\beta_0^n-\beta_1^n}{n!} = e^{\beta_0}-e^{\beta_1}, \quad \text{(C19)}$$

$$\sum_{n=2}^{\infty}\frac{\beta_0^{n-1}-\beta_1^{n-1}}{n!} = \frac{1}{\beta_0\beta_1}\left(\beta_1 e^{\beta_0}-\beta_0 e^{\beta_1}+\beta_0-\beta_1\right). \quad \text{(C20)}$$

By using the above identities in Eq. (C18), we obtain

$$B_{\vec{h}}^{(2)} = \sum_{\substack{k=1 \\ k\,\text{odd}}}^{N-m}(-1)^{N-m-k}(\beta_0 - \beta_1)^{N-m-k}\sum_{\substack{\vec{h}^{(k)}\in\{0,1\}^N: \\ |\vec{h}^{(k)}|=m+k \\ \vec{h}^{(k)}\wedge\vec{h}=\vec{h}}}(e^{\beta_0}-e^{\beta_1})^m\left(\beta_1 e^{\beta_0}-\beta_0 e^{\beta_1}+\beta_0-\beta_1\right)^k,, \quad \text{(C21)}$$

where we observe that the argument of the sum over $\vec{h}^{(k)}$ is independent of $\vec{h}^{(k)}$. Therefore, the sum reduces to counting all the possible choices of $\vec{h}^{(k)}$ for a given k. This number is given by the possible combinations of k bits in $\vec{h}^{(k)}$ that are set to one, chosen among the $N-m$ elements that correspond to zeroes in $\vec{h}$. Hence, we have $\binom{N-m}{k}$ choices and we obtain

$$B_{\vec{h}}^{(2)} = \sum_{\substack{k=1 \\ k\,\text{odd}}}^{N-m}(-1)^{N-m-k}(\beta_0 - \beta_1)^{N-m-k}\binom{N-m}{k}(e^{\beta_0}-e^{\beta_1})^m\left(\beta_1 e^{\beta_0}-\beta_0 e^{\beta_1}+\beta_0-\beta_1\right)^k$$

$$= \sum_{k=0}^{\lfloor(N-m-1)/2\rfloor}(-1)^{N-m-2k-1}(\beta_0 - \beta_1)^{N-m-2k-1}\binom{N-m}{2k+1}\left(e^{\beta_0}-e^{\beta_1}\right)^m\left(\beta_1 e^{\beta_0}-\beta_0 e^{\beta_1}+\beta_0-\beta_1\right)^{2k+1}, \quad \text{(C22)}$$

where $\lfloor x\rfloor$ is the floor function. Finally, by employing (C22) in Eq. (C16), we obtain the following equality satisfied by the upper bound on the selected yield

$$B_{\vec{h}} = (-1)^{N-m}(\beta_0 - \beta_1)^{N-m}U_{u_0,\dots,u_{N-1}}\prod_{\substack{i\,\text{s.t.} \\ h_i=1}}\frac{(\beta_0^{u_i}-\beta_1^{u_i})}{u_i!}+\sum_{k=0}^{\lfloor(N-m-1)/2\rfloor}(-1)^{N-m-2k-1}(\beta_0 - \beta_1)^{N-m-2k-1}$$

$$\times\binom{N-m}{2k+1}\left(e^{\beta_0}-e^{\beta_1}\right)^m\left(\beta_1 e^{\beta_0}-\beta_0 e^{\beta_1}+\beta_0-\beta_1\right)^{2k+1}. \quad \text{(C23)}$$

By isolating the yield's upper bound and relabeling $u_i \to n_i$, we obtain the final expression of the yield bound: $\overline{Y}_{n_0,\dots,n_{N-1}} = \min\{U_{n_0,\dots,n_{N-1}}, 1\}$, where

$$U_{n_0,\dots,n_{N-1}} = \prod_{\substack{i\,\text{s.t.} \\ n_i\neq0}}\frac{n_i!}{\beta_0^{n_i}-\beta_1^{n_i}}\left[\frac{B_{\vec{h}}\,(-1)^{N-m}}{(\beta_0-\beta_1)^{N-m}}+\left(e^{\beta_0}-e^{\beta_1}\right)^m\sum_{k=0}^{\lfloor(N-m-1)/2\rfloor}\binom{N-m}{2k+1}\left(\frac{\beta_1 e^{\beta_0}-\beta_0 e^{\beta_1}+\beta_0-\beta_1}{\beta_0-\beta_1}\right)^{2k+1}\right],$$

$$\quad \text{(C24)}$$

where $B_{\vec{h}}$ is given in Eq. (C5) (and in principle can depend on the detector D_j through the gains) and $m = |\vec{h}|$, while $\vec{h}$ is the binary vector with components h_i defined by

$$h_i = \begin{cases} 1 & \text{if } n_i \geq 1 \\ 0 & \text{if } n_i = 0. \end{cases} \tag{C25}$$

APPENDIX D: CHANNEL MODEL

In this Appendix we describe our channel model and compute the detection statistics of the protocol. The channel model includes the following sources of noise.

1. Pure-photon loss: the optical mode of party goes through the same lossy channel. The lossy channel is modeled with a beam splitter with transmittance η, where the additional input port of the beam splitter is fed with the vacuum.

2. Polarization misalignment: the optical mode of each party undergoes a polarization misalignment modeled by a unitary operation that maps the creation operator of each mode according to

$$\hat{a}_i^\dagger \to \cos\theta_i \hat{a}_{i,P}^\dagger - \sin\theta_i \hat{a}_{i,P_\perp}^\dagger, \tag{D1}$$

where $\hat{a}_{i,P}^\dagger$ is the creation operator on the original polarization and $\hat{a}_{i,P_\perp}^\dagger$ is the creation operator on the orthogonal polarization.

3. Phase shift: the optical mode of each party undergoes a phase shift ϕ_i, modelled by multiplying the mode operator $\hat{a}_i^\dagger$ by a phase ϕ_i.

4. Dark counts in the detectors: each detector is affected by dark counts, with a probability p_d that is equal for all detectors and independent on the state sent.

In Sec. V we argue that since the channel of each party is equally lossy, the optimal choice for the signal intensities is the same for each party. Hence, here we assume that the amplitudes of each party in KG and PE rounds coincide: $\alpha_i = \alpha$ and $S_i = S$, for every i. Moreover, we choose the same polarization misalignment between the reference party A_0 and each other party. This means that we choose a misalignment of θ_0 for A_0 and θ_1 for the other parties. Similarly for the phase shift, we set $\phi_0 = 0$ and $\phi_i = \phi$ for $i \neq 0$.

1. Computation of $\Pr(\Omega_j | x_0, x_1, \ldots, x_{N-1}, R_{KG})$

We start by computing the detection probability $\Pr(\Omega_j | x_0, x_1, \ldots, x_{N-1}, R_{KG})$, which is the probability that only detector D_j clicks, given that party A_i prepared, in a KG round, the coherent state $|x_i\alpha\rangle$, with $x_i = \pm 1$. This detection probability is needed to compute the QBER, Eq. (4), through Eq. (5).

The state prepared by the N parties in a KG round, before any noise or loss is applied, reads

$$|\psi_{\text{in}}\rangle = \bigotimes_{i=0}^{N-1} |x_i\alpha\rangle. \tag{D2}$$

We now apply the sources of noise discussed above.

1. The resulting state after the lossy channel is the following:

$$|\psi_{\text{in}}'\rangle = \bigotimes_{i=0}^{N-1} |x_i\sqrt{\eta}\alpha\rangle. \tag{D3}$$

2. After applying the polarization misalignment, we obtain

$$|\psi_{\text{in}}''\rangle = \bigotimes_{i=0}^{N-1} |x_i\cos\theta_i\sqrt{\eta}\alpha\rangle_P |-x_i\sin\theta_i\sqrt{\eta}\alpha\rangle_{P_\perp}. \tag{D4}$$

3. After the phase shift ϕ_i is applied on each mode, we get

$$|\psi_{\text{in}}'''\rangle = \bigotimes_{i=0}^{N-1} \left|x_i \cos\theta_i e^{i\phi_i}\sqrt{\eta}\alpha\right\rangle_P \left|-x_i \sin\theta_i e^{i\phi_i}\sqrt{\eta}\alpha\right\rangle_{P_\perp}. \tag{D5}$$

The state in Eq. (D5) is the global state of the N parties' modes, after the noisy and lossy channel and before entering the BBS network. We now evolve the modes through the M-input and M-output BBS network, according to the transformation in Eq. (3). We define the coefficients of the inverse transformation of the modes as $f_{i,j} := (-1)^{-\bar{i}\cdot\bar{j}}$. Here, we make the nonrestrictive assumption that the N modes sent by the parties correspond to the first N inputs of the BBS network. A different choice would not alter the protocol's performance. The output state after the BBS network reads

$$|\psi_{\text{out}}\rangle = \bigotimes_{j=0}^{M-1} \left|\sqrt{\frac{\eta}{M}}\alpha \sum_{i=0}^{N-1} x_i f_{i,j}\cos\theta_i e^{i\phi_i}\right\rangle_P \left|-\sqrt{\frac{\eta}{M}}\alpha \sum_{i=0}^{N-1} x_i f_{i,j}\sin\theta_i e^{i\phi_i}\right\rangle_{P_\perp}. \tag{D6}$$

At this point, the relay performs a threshold measurement on each mode that returns a click in the corresponding detector if one or more photons are detected. We are interested in the probability that only detector D_j clicks, i.e., $\Pr(\Omega_j|x_0,x_1,\ldots,x_{N-1},R_{\text{KG}})$. By including the effect of dark counts, we can express such probability as follows:

$$\Pr(\Omega_j|x_0,x_1,\ldots,x_{N-1},R_{\text{KG}}) = p_d(1-p_d)^{M-1}\text{Tr}\left[\rho_{\text{out}}\bigotimes_{k=0}^{M-1}|0\rangle\langle0|_k\right] + (1-p_d)^{M-1}\text{Tr}\left[\rho_{\text{out}}(\mathbb{1}_j - |0\rangle\langle0|_j)\bigotimes_{k\neq j}|0\rangle\langle0|_k\right]$$

$$= (1-p_d)^{M-1}\text{Tr}\left[\rho_{\text{out}}\mathbb{1}_j\bigotimes_{k\neq j}|0\rangle\langle0|_k\right] - (1-p_d)^{M}\text{Tr}\left[\rho_{\text{out}}\bigotimes_{k=0}^{M-1}|0\rangle\langle0|_k\right], \tag{D7}$$

where $|0\rangle\langle0|_k$ is the projector on the vacuum of the output mode k for polarizations P and $P_\perp$, as the detectors do not distinguish polarization, and $\rho_{\text{out}} = |\psi_{\text{out}}\rangle\langle\psi_{\text{out}}|$. We calculate both terms appearing in Eq. (D7). For the second term, we have

$$\text{Tr}\left[\rho_{\text{out}}\bigotimes_{k=0}^{M-1}|0\rangle\langle0|_k\right] = \prod_{k=0}^{M-1}\exp\left[-\left|\sqrt{\frac{\eta}{M}}\alpha\sum_{i=0}^{N-1}x_i f_{i,k}\cos\theta_i e^{i\phi_i}\right|^2 - \left|\sqrt{\frac{\eta}{M}}\alpha\sum_{i=0}^{N-1}x_i f_{i,k}\sin\theta_i e^{i\phi_i}\right|^2\right]$$

$$= \exp\left[-\frac{\eta}{M}\alpha^2\sum_{k=0}^{M-1}\left(\left|\sum_{i=0}^{N-1}x_i f_{i,k}\cos\theta_i e^{i\phi_i}\right|^2 + \left|\sum_{i=0}^{N-1}x_i f_{i,k}\sin\theta_i e^{i\phi_i}\right|^2\right)\right]. \tag{D8}$$

We now focus on the sum over k in the last expression and use the fact that we fix the angles θ_i and ϕ_i as discussed above. The sum over k simplifies to

$$\sum_{k=0}^{M-1}\left(\left|\sum_{i=0}^{N-1}x_i f_{i,k}\cos\theta_i e^{i\phi_i}\right|^2 + \left|\sum_{i=0}^{N-1}x_i f_{i,k}\sin\theta_i e^{i\phi_i}\right|^2\right)$$

$$= \sum_{k=0}^{M-1}\left(\left|x_0\cos\theta_0 + \cos\theta_1 e^{i\phi}\sum_{i=1}^{N-1}x_i f_{i,k}\right|^2 + \left|x_0\sin\theta_0 + \sin\theta_1 e^{i\phi}\sum_{i=1}^{N-1}x_i f_{i,k}\right|^2\right)$$

$$
= \sum_{k=0}^{M-1} \left(x_0^2 \cos^2 \theta_0 + \cos^2 \theta_1 \left| \sum_{i=1}^{N-1} x_i f_{i,k} \right|^2 + x_0^2 \sin^2 \theta_0 + \sin^2 \theta_1 \left| \sum_{i=1}^{N-1} x_i f_{i,k} \right|^2 \right.
$$

$$
\left. + 2x_0 \cos \theta_0 \cos \theta_1 \cos \phi \sum_{i=1}^{N-1} x_i f_{i,k} + 2x_0 \sin \theta_0 \sin \theta_1 \cos \phi \sum_{i=1}^{N-1} x_i f_{i,k} \right)
$$

$$
= \sum_{k=0}^{M-1} \left(1 + \left| \sum_{i=1}^{N-1} x_i f_{i,k} \right|^2 + 2x_0 \cos \theta \cos \phi \sum_{i=1}^{N-1} x_i f_{i,k} \right), \tag{D9}
$$

where we use that $x_i = \pm 1$, $\cos \theta_i{}^2 + \sin \theta_i{}^2 = 1$ and $\cos \theta_0 \cos \theta_1 + \sin \theta_0 \sin \theta_1 = \cos(\theta_0 - \theta_1)$ and where we define $\theta := \theta_0 - \theta_1$. Consider the following lemma for the function $f_{i,k}$, which coincides with $f_{k,i}$ in Eq. (A6).

Lemma 1.—For $f_{k,i}$ as defined by (A6), it holds

$$
\sum_{i=0}^{M-1} f_{k,i} = M \, \delta_{k,0}. \tag{D10}
$$

Proof.—To show the result of the lemma we first recall that the function $f_{k,i}$ is given by

$$
f_{k,i} = (-1)^{\vec{k} \cdot \vec{i}}, \tag{D11}
$$

where $\vec{k}$ and $\vec{i}$ are the binary vectors of length s that represent the numbers k and i in binary representation. Then, the sum over i of $f_{k,i}$ can be recast as

$$
\sum_{i=0}^{M-1} f_{k,i} = \sum_{\vec{i} \in \{0,1\}^s} (-1)^{\vec{k} \cdot \vec{i}} = \sum_{c=0}^{|\vec{k}|} (-1)^c \binom{|\vec{k}|}{c} 2^{s-|\vec{k}|}, \tag{D12}
$$

where in the second equality we perform the sum over all the possible values c of $\vec{k} \cdot \vec{i}$ and count how many distinct vectors $\vec{i}$ lead to the same scalar product $c = \vec{k} \cdot \vec{i}$. This number is given by the ways in which we can select c bits equal to one in $\vec{k}$ (the binomial coefficient), which fixes the corresponding c bits in $\vec{i}$ to be one and also fixes other $|\vec{k}| - c$ bits in $\vec{i}$ to be zero since they correspond to the ones in $\vec{k}$ that have not been selected. At this point, the vector $\vec{i}$ is almost all fixed, except for the bits that correspond to the $s - |\vec{k}|$ zero bits in $\vec{k}$. Since such bits in $\vec{i}$ can be arbitrary as they would not contribute to the scalar product, the total number of possibilities is given by $2^{s-|\vec{k}|}$.

Now, we can simplify the expression in Eq. (D12) as follows:

$$
\sum_{i=0}^{M-1} f_{k,i} = \sum_{c=0}^{|\vec{k}|} (-1)^c \binom{|\vec{k}|}{c} 2^{s-|\vec{k}|} = 2^{s-|\vec{k}|} \sum_{c=0}^{|\vec{k}|} \binom{|\vec{k}|}{c} (-1)^c (1)^{|\vec{k}|-c} = 2^{s-|\vec{k}|} (1-1)^{|\vec{k}|} = M \delta_{k,0}, \tag{D13}
$$

where we use the binomial formula in the third line and that $M = 2^s$ together with the definition of Kronecker δ in the last line. This concludes the proof. ∎

By applying Lemma 3 in Eq. (D9), we can simplify the term with the cosines as follows:

$$\sum_{k=0}^{M-1}\left(\left|\sum_{i=0}^{N-1}x_if_{i,k}\cos\theta_ie^{i\phi_i}\right|^2+\left|\sum_{i=0}^{N-1}x_if_{i,k}\sin\theta_ie^{i\phi_i}\right|^2\right)=\sum_{k=0}^{M-1}\left(1+\left|\sum_{i=1}^{N-1}x_if_{i,k}\right|^2+2x_0\cos\theta\cos\phi\sum_{i=1}^{N-1}x_if_{i,k}\right)$$

$$=\sum_{k=0}^{M-1}\left(1+\left|\sum_{i=1}^{N-1}x_if_{i,k}\right|^2\right)+2x_0\cos\theta\cos\phi\sum_{i=1}^{N-1}x_iM\delta_{i,0}$$

$$=\sum_{k=0}^{M-1}\left(1+\left|\sum_{i=1}^{N-1}x_if_{i,k}\right|^2\right)=M+\sum_{k=0}^{M-1}\left|\sum_{i=1}^{N-1}x_if_{i,k}\right|^2, \qquad (D14)$$

where the sum with the Kronecker δ $\delta_{i,0}$ is identically zero since the index i starts from one.

We now expand the square in the last expression and obtain

$$\sum_{k=0}^{M-1}\left(\left|\sum_{i=0}^{N-1}x_if_{i,k}\cos\theta_ie^{i\phi_i}\right|^2+\left|\sum_{i=0}^{N-1}x_if_{i,k}\sin\theta_ie^{i\phi_i}\right|^2\right)=M+\sum_{k=0}^{M-1}\left|\sum_{i=1}^{N-1}x_if_{i,k}\right|^2$$

$$=M+\sum_{k=0}^{M-1}\sum_{i,i'=1}^{N-1}x_ix_{i'}f_{i,k}f_{i',k}=M+\sum_{i,i'=1}^{N-1}x_ix_{i'}\sum_{\vec{k}\in\{0,1\}^s}(-1)^{(\vec{i}+\vec{i}')\cdot\vec{k}},$$

$$(D15)$$

where we remark that the result of Lemma 3 cannot be directly applied to the innermost sum since $(\vec{i}+\vec{i}')$ is not a binary vector. However, we can use the lemma to compute such a sum. In order to do so, we observe that the vector $(\vec{i}+\vec{i}')$ deviates from a binary vector only in the elements r where $i_r=i'_r=1$, and we have $\vec{i}\cdot\vec{i}'$ many such elements. These elements do not contribute to the value of $(-1)^{(\vec{i}+\vec{i}')\cdot\vec{k}}$ regardless of the value of k_r. Hence, we can define shorter vectors $\vec{m}\in\{0,1\}^{s-\vec{i}\cdot\vec{i}'}$ and $\vec{l}\in\{0,1\}^{s-\vec{i}\cdot\vec{i}'}$ that correspond to the remaining $s-\vec{i}\cdot\vec{i}'$ elements of $\vec{i}+\vec{i}'$ and $\vec{k}$, respectively, where $i_r+i'_r\neq2$. By definition, we have that $(-1)^{(\vec{i}+\vec{i}')\cdot\vec{k}}=(-1)^{\vec{m}\cdot\vec{l}}$. Now, in order to replace the sum over $\vec{k}$ with a sum over $\vec{l}$, we must account for the fact that, for every fixed value of $\vec{l}$ and hence of $(-1)^{\vec{m}\cdot\vec{l}}$, there are $2^{\vec{i}\cdot\vec{i}'}$ vectors $\vec{k}$ such that $(-1)^{(\vec{i}+\vec{i}')\cdot\vec{k}}=(-1)^{\vec{m}\cdot\vec{l}}$. Therefore, we can recast the innermost sum in Eq. (D15) as follows:

$$\sum_{\vec{k}\in\{0,1\}^s}(-1)^{(\vec{i}+\vec{i}')\cdot\vec{k}}=2^{\vec{i}\cdot\vec{i}'}\sum_{\vec{l}\in\{0,1\}^{s-\vec{i}\cdot\vec{i}'}}(-1)^{\vec{m}\cdot\vec{l}}=2^{\vec{i}\cdot\vec{i}'}2^{s-\vec{i}\cdot\vec{i}'}\delta_{\vec{m},\vec{0}}=M\delta_{\vec{m},\vec{0}}=M\delta_{\vec{i},\vec{i}'}, \qquad (D16)$$

where in the second equality we used Lemma 3 since now $\vec{m}$ is a binary vector and in the fourth equality we use the fact that the δ $\delta_{\vec{m},\vec{0}}$ effectively implies that $\vec{i}=\vec{i}'$ over the whole set of s elements since $\vec{m}$ is given by the elements of $\vec{i}+\vec{i}'$ corresponding to the positions where the two vectors are not both equal to one.

Thus, by using Eq. (D16) in Eq. (D15), we obtain

$$\sum_{k=0}^{M-1}\left(\left|\sum_{i=0}^{N-1}x_if_{i,k}\cos\theta_ie^{i\phi_i}\right|^2+\left|\sum_{i=0}^{N-1}x_if_{i,k}\sin\theta_ie^{i\phi_i}\right|^2\right)=M+M\sum_{i,i'=1}^{N-1}x_ix_{i'}\delta_{\vec{i},\vec{i}'}$$

$$=M\left(1+\sum_{i=1}^{N-1}x_i^2\right)=MN, \qquad (D17)$$

where we use the fact that $x_i=\pm1$. Finally, by employing Eq. (D17) in Eq. (D8), we obtain

$$\mathrm{Tr}\left[\rho_{\mathrm{out}}\bigotimes_{k=0}^{M-1}|0\rangle\langle0|_k\right]=e^{-N\eta\alpha^2}, \qquad (D18)$$

which concludes the calculation of the second trace in Eq. (D7).

We now move on to calculate the first trace in Eq. (D7). In a similar manner to Eq. (D8), we can write

$$\text{Tr}\left[\rho_{\text{out}}\mathbb{1}_j\bigotimes_{k\neq j}|0\rangle\langle0|_k\right] = \prod_{k\neq j}\exp\left[-\left|\sqrt{\frac{\eta}{M}}\alpha\sum_{i=0}^{N-1}x_if_{i,k}\cos\theta_ie^{i\phi_i}\right|^2 - \left|\sqrt{\frac{\eta}{M}}\alpha\sum_{i=0}^{N-1}x_if_{i,k}\sin\theta_ie^{i\phi_i}\right|^2\right]$$

$$= \exp\left[-\frac{\eta}{M}\alpha^2\sum_{k\neq j}\left(\left|\sum_{i=0}^{N-1}x_if_{i,k}\cos\theta_ie^{i\phi_i}\right|^2 + \left|\sum_{i=0}^{N-1}x_if_{i,k}\sin\theta_ie^{i\phi_i}\right|^2\right)\right]$$

$$= \exp\left[-\frac{\eta}{M}\alpha^2\sum_{k\neq j}C_k\right] = \exp\left[-\frac{\eta}{M}\alpha^2\left(\sum_{k=0}^{M-1}C_k - C_j\right)\right] = e^{-N\eta\alpha^2}e^{(\eta/M)\alpha^2C_j}, \qquad (D19)$$

where in the third line we define

$$C_k := \left|\sum_{i=0}^{N-1}x_if_{i,k}\cos\theta_ie^{i\phi_i}\right|^2 + \left|\sum_{i=0}^{N-1}x_if_{i,k}\sin\theta_ie^{i\phi_i}\right|^2, \qquad (D20)$$

and we use Eq. (D18) in the last line. With analogous calculations to those leading to Eq. (D9), one can simplify C_j as follows:

$$C_j = 1 + \left|\sum_{i=1}^{N-1}x_if_{i,j}\right|^2 + 2x_0\cos\theta\cos\phi\sum_{i=1}^{N-1}x_if_{i,j}. \qquad (D21)$$

We now recall that in the postprocessing of the protocol, party A_i flips their X-basis outcome, x_i, if $f_{i,j} = (-1)^{\vec{i}\cdot\vec{j}} = -1$. For this, we identify the sum $\sum_{i=1}^{N-1}x_if_{i,j}$ in the last expression as the sum of the postprocessed X-basis outcomes of the parties (excluding A_0) and can label it as follows:

$$\sum_{i=1}^{N-1}x_if_{i,j} =: S^j_{x_1,\ldots,x_{N-1}}. \qquad (D22)$$

This allows us to recast C_j as follows:

$$C_j = 1 + (S^j_{x_1,\ldots,x_{N-1}})^2 + 2S^j_{x_1,\ldots,x_{N-1}}x_0\cos\theta\cos\phi. \qquad (D23)$$

By using the last expression in Eq. (D19), we obtain the final form of the first trace in Eq. (D7):

$$\text{Tr}\left[\rho_{\text{out}}\mathbb{1}_j\bigotimes_{k\neq j}|0\rangle\langle0|_k\right] = e^{-N\eta\alpha^2}e^{(\eta/M)\alpha^2\left(1+(S^j_{x_1,\ldots,x_{N-1}})^2+2S^j_{x_1,\ldots,x_{N-1}}x_0\cos\theta\cos\phi\right)}$$

$$= e^{-(MN-1)\eta\alpha^2/M}e^{\eta\alpha^2\left((S^j_{x_1,\ldots,x_{N-1}})^2+2S^j_{x_1,\ldots,x_{N-1}}x_0\cos\theta\cos\phi\right)/M}. \qquad (D24)$$

Finally, by combining Eqs. (D18) and (D24) in Eq. (D7), we obtain the following expression for the probability that only detector D_j clicks, conditioned on the parties preparing coherent states $|x_0\alpha\rangle,\ldots,|x_{N-1}\alpha\rangle$ in a KG round:

$$\Pr(\Omega_j|x_0,x_1,\ldots,x_{N-1},R_{\text{KG}})$$

$$= (1-p_d)^{M-1}e^{-(MN-1)\eta\alpha^2/M}e^{\eta\alpha^2\left((S^j_{x_1,\ldots,x_{N-1}})^2+2S^j_{x_1,\ldots,x_{N-1}}x_0\cos\theta\cos\phi\right)/M}$$

$$- (1-p_d)^Me^{-N\eta\alpha^2}, \qquad (D25)$$

where $S^j_{x_1,\ldots,x_{N-1}}$ is given in Eq. (D22) and $\theta = \theta_0 - \theta_1$.

2. Computation of $\Pr(\Omega_j | R_{\mathrm{KG}})$

We now calculate the probability that detector D_j clicks in a KG round, i.e.,

$$\Pr(\Omega_j | R_{\mathrm{KG}}) = \frac{1}{2^N} \sum_{(x_0,\ldots,x_{N-1}) \in \{1,-1\}^N} \Pr(\Omega_j | x_0, x_1, \ldots, x_{N-1}, R_{\mathrm{KG}})$$

$$= -(1-p_d)^M e^{-N\eta\alpha^2} + \frac{(1-p_d)^{M-1}}{2^N} e^{-(MN-1)\eta\alpha^2/M}$$

$$\times \sum_{(x_0,\ldots,x_{N-1}) \in \{1,-1\}^N} e^{\eta\alpha^2 \left((S^j_{x_1,\ldots,x_{N-1}})^2 + 2 S^j_{x_1,\ldots,x_{N-1}} x_0 \cos\theta \cos\phi\right)/M}. \tag{D26}$$

We denote the leftover sum in the last expression as Σ for brevity. Then, we can simplify it as follows:

$$\Sigma = \sum_{(x_1,\ldots,x_{N-1}) \in \{1,-1\}^{N-1}} \left(e^{\eta\alpha^2 \left((S^j_{x_1,\ldots,x_{N-1}})^2 + 2 S^j_{x_1,\ldots,x_{N-1}} \cos\theta \cos\phi\right)/M} + e^{\eta\alpha^2 \left((S^j_{x_1,\ldots,x_{N-1}})^2 - 2 S^j_{x_1,\ldots,x_{N-1}} \cos\theta \cos\phi\right)/M} \right)$$

$$= \sum_{(x_1,\ldots,x_{N-1}) \in \{1,-1\}^{N-1}} e^{\eta\alpha^2 (S^j_{x_1,\ldots,x_{N-1}})^2/M} \left(e^{\eta\alpha^2 2 S^j_{x_1,\ldots,x_{N-1}} \cos\theta \cos\phi/M} + e^{-\eta\alpha^2 2 S^j_{x_1,\ldots,x_{N-1}} \cos\theta \cos\phi/M} \right)$$

$$= 2 \sum_{(x_1,\ldots,x_{N-1}) \in \{1,-1\}^{N-1}} e^{\eta\alpha^2 (S^j_{x_1,\ldots,x_{N-1}})^2/M} \cosh\left(2\frac{\eta\alpha^2}{M} S^j_{x_1,\ldots,x_{N-1}} \cos\theta \cos\phi \right). \tag{D27}$$

At this point, we define a vector $\vec{y} \in \{1,-1\}^{N-1}$ such that $y_i = x_i f_{i,j}$. Then, we can rewrite $S^j_{x_1,\ldots,x_{N-1}} = \sum_i y_i$. Of note, since we sum over all possible vectors $(x_1,\ldots,x_{N-1})$, we reach all possible values for $\vec{y}$. This implies that we can recast the sum over $(x_1,\ldots,x_{N-1})$ as a sum over all possible vectors $\vec{y}$. This has the consequence that the probability of detector D_j clicking is independent of j. With these considerations, we rewrite the last expression as follows:

$$\Sigma = 2 \sum_{\vec{y} \in \{1,-1\}^{N-1}} e^{\eta\alpha^2 (\sum_i y_i)^2/M} \cosh\left(2\frac{\eta\alpha^2}{M} (\sum_i y_i) \cos\theta \cos\phi \right). \tag{D28}$$

Now let us call k the number of ones in the vector $\vec{y}$. We have that $\sum_i y_i = k - (N-1-k) = 2k+1-N$. Since there are $\binom{N-1}{k}$ different vectors $\vec{y}$ that have a fixed number k of ones, we can recast the last expression as follows:

$$\Sigma = 2 \sum_{k=0}^{N-1} \binom{N-1}{k} e^{\eta\alpha^2 (2k+1-N)^2/M} \cosh\left(2\frac{\eta\alpha^2}{M} (2k+1-N) \cos\theta \cos\phi \right). \tag{D29}$$

By inserting the last expression in Eq. (D26), we obtain the final expression for the probability that detector D_j clicks in a KG round:

$$\Pr(\Omega_j | R_{\mathrm{KG}}) = -(1-p_d)^M e^{-N\eta\alpha^2} + \frac{(1-p_d)^{M-1}}{2^{N-1}} e^{-(MN-1)\eta\alpha^2/M}$$

$$\times \sum_{k=0}^{N-1} \binom{N-1}{k} e^{\eta\alpha^2 (2k+1-N)^2/M} \cosh\left(2\frac{\eta\alpha^2}{M} (2k+1-N) \cos\theta \cos\phi \right), \tag{D30}$$

where $\theta = \theta_0 - \theta_1$. As discussed above, the probability that a specific detector clicks is independent of j, as expected given our symmetric channel model.

3. Computation of $Q^j_{X_0, X_i}$

The QBER is computed through Eq. (5), which we report here for clarity:

$$Q^j_{X_0, X_i} = \sum_{x_0 \neq x_i f_{i,j}} \frac{\Pr\left(\Omega_j | x_0, x_i, R_{KG}\right)}{4 \Pr(\Omega_j | R_{KG})}, \tag{D31}$$

where the only quantity that still needs to be computed is $\Pr\left(\Omega_j | x_0, x_i, R_{KG}\right)$. By definition, we have

$$\Pr(\Omega_j | x_0, x_i, R_{KG}) = \frac{1}{2^{N-2}} \sum_{(x_1, \dots, \hat{x}_i, \dots, x_{N-1}) \in \{1, -1\}^{N-2}} \Pr(\Omega_j | x_0, x_1, \dots, x_{N-1}, R_{KG})$$

$$= -(1 - p_d)^M e^{-N\eta\alpha^2} + \frac{(1 - p_d)^{M-1}}{2^{N-2}} e^{-(MN-1)\eta\alpha^2/M}$$

$$\times \sum_{(x_1, \dots, \hat{x}_i, \dots, x_{N-1}) \in \{1, -1\}^{N-2}} e^{\eta\alpha^2 \left((S^j_{x_1, \dots, x_{N-1}})^2 + 2S^j_{x_1, \dots, x_{N-1}} x_0 \cos\theta \cos\phi\right)/M}, \tag{D32}$$

where $(x_1, \dots, \hat{x}_i, \dots, x_{N-1})$ are $(N-2)$-dimensional vectors where the ith element is removed. Then, we can define a vector $\vec{y} \in \{1, -1\}^{N-1}$ with $y_l = x_l f_{l,j}$ for $l \neq i$ and $y_i = 0$, such that $S^j_{x_1, \dots, x_{N-1}} = \sum_l y_l + x_i f_{i,j}$. Since the sum in the last expression runs over all vectors $(x_1, \dots, \hat{x}_i, \dots, x_{N-1})$, we can reach all possible choices of $\vec{y}$, meaning that we can recast the sum as a sum over all possible choices of $\vec{y}$. With these considerations, we recast Eq. (D32) as follows:

$$\Pr(\Omega_j | x_0, x_i, R_{KG}) = -(1 - p_d)^M e^{-N\eta\alpha^2} + \frac{(1 - p_d)^{M-1}}{2^{N-2}} e^{-(MN-1)\eta\alpha^2/M}$$

$$\times \sum_{\substack{\vec{y} \in \{1, -1\}^{N-1}: \\ y_i = 0}} e^{\eta\alpha^2 \left((\sum_l y_l + x_i f_{i,j})^2 + 2(\sum_l y_l + x_i f_{i,j}) x_0 \cos\theta \cos\phi\right)/M}. \tag{D33}$$

We label the sum as Σ' and focus on it

$$\Sigma' = \sum_{\substack{\vec{y} \in \{1, -1\}^{N-1}: \\ y_i = 0}} e^{\eta\alpha^2 \left((\sum_l y_l)^2 + 1 + 2x_i f_{i,j} \sum_l y_l + 2x_i f_{i,j} x_0 \cos\theta \cos\phi + 2x_0 \cos\theta \cos\phi \sum_l y_l\right)/M}$$

$$= e^{\eta\alpha^2 (1 + 2x_0 x_i f_{i,j} \cos\theta \cos\phi)/M} \sum_{\substack{\vec{y} \in \{1, -1\}^{N-1}: \\ y_i = 0}} e^{\eta\alpha^2 \left((\sum_l y_l)^2 + 2\sum_l y_l (x_i f_{i,j} + x_0 \cos\theta \cos\phi)\right)/M}. \tag{D34}$$

By replicating the argument in the calculation of $\Pr(\Omega_j | R_{KG})$, we can replace the sum over $\vec{y}$ with a sum over k, which is the number of ones in $\vec{y}$:

$$\Sigma' = e^{\eta\alpha^2 (1 + 2x_0 x_i f_{i,j} \cos\theta \cos\phi)/M} \sum_{k=0}^{N-2} \binom{N-2}{k} e^{\eta\alpha^2 (2k+2-N)^2/M} e^{2\eta\alpha^2 (2k+2-N)(x_i f_{i,j} + x_0 \cos\theta \cos\phi)/M}. \tag{D35}$$

By inserting this in Eq. (D33), we obtain the final expression for the probability that detector D_j clicks, given that party A_0 (A_i) prepared coherent state $|x_0 \alpha\rangle$ ($|x_i \alpha\rangle$):

$$\Pr(\Omega_j | x_0, x_i, R_{KG}) = -(1 - p_d)^M e^{-N\eta\alpha^2} + \frac{(1 - p_d)^{M-1}}{2^{N-2}} e^{-(MN-2-2x_0 x_i f_{i,j} \cos\theta \cos\phi)\eta\alpha^2/M}$$

$$\times \sum_{k=0}^{N-2} \binom{N-2}{k} e^{\eta\alpha^2 (2k+2-N)^2/M} e^{2\eta\alpha^2 (2k+2-N)(x_i f_{i,j} + x_0 \cos\theta \cos\phi)/M}. \tag{D36}$$

With Eq. (D36) we can finally compute the QBER as follows:

$$
\begin{aligned}
Q^j_{X_0, X_i} &= \sum_{x_0 \neq x_i f_{i,j}} \frac{\Pr\left(\Omega_j \,|\, x_0, x_i, R_{\mathrm{KG}}\right)}{4 \Pr(\Omega_j \,|\, R_{\mathrm{KG}})} = \frac{-(1 - p_d)^M e^{-N\eta\alpha^2}}{2 \Pr(\Omega_j \,|\, R_{\mathrm{KG}})} + \frac{(1 - p_d)^{M-1}}{2^N \Pr(\Omega_j \,|\, R_{\mathrm{KG}})} e^{-(MN - 2 + 2\cos\theta\cos\phi)\eta\alpha^2/M} \\
&\qquad\qquad \times \sum_{k=0}^{N-2} \binom{N-2}{k} e^{\eta\alpha^2 (2k+2-N)^2/M} \\
&\qquad\qquad \times \left(e^{2\eta\alpha^2 (2k+2-N)(1-\cos\theta\cos\phi)/M} + e^{-2\eta\alpha^2(2k+2-N)(1-\cos\theta\cos\phi)/M} \right) \\
&= \frac{-(1 - p_d)^M e^{-N\eta\alpha^2}}{2 \Pr(\Omega_j \,|\, R_{\mathrm{KG}})} + \frac{(1 - p_d)^{M-1}}{2^{N-1} \Pr(\Omega_j \,|\, R_{\mathrm{KG}})} e^{-(MN - 2 + 2\cos\theta\cos\phi)\eta\alpha^2/M} \\
&\qquad\qquad \times \sum_{k=0}^{N-2} \binom{N-2}{k} e^{\eta\alpha^2 (2k+2-N)^2/M} \cosh\left(2\frac{\eta\alpha^2}{M}(2k+2-N)(1-\cos\theta\cos\phi) \right),
\end{aligned}
\tag{D37}
$$

which is also independent of j ($\Pr(\Omega_j \,|\, R_{\mathrm{KG}})$ is independent of j, see Eq. (D30)), as well as i, due to the symmetry of the considered noise model.

4. Computation of $\Pr(\Omega_j \,|\, \beta_0, \beta_1, \ldots, \beta_{N-1})$

We now calculate the gains, i.e., the probability that only detector D_j clicks in a PE round where the parties prepared phase-randomized coherent states with intensities $\beta_0, \beta_1, \ldots, \beta_{N-1}$. We recall that the state (1) sent by party A_i can be equivalently described as follows:

$$
\rho_{a_i}(\beta_i) = \frac{1}{2\pi} \int_0^{2\pi} d\varphi_i |\sqrt{\beta_i} e^{i\varphi_i}\rangle \langle \sqrt{\beta_i} e^{i\varphi_i}|,
\tag{D38}
$$

where $\beta_i \in \mathcal{S}_i$. Thus, the state sent by all parties reads

$$
\rho_{\mathrm{in}} = \bigotimes_{i=0}^{N-1} \rho_{a_i}(\beta_i) = \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \cdots d\varphi_{N-1} \bigotimes_{i=0}^{N-1} |\sqrt{\beta_i} e^{i\varphi_i}\rangle \langle \sqrt{\beta_i} e^{i\varphi_i}|.
\tag{D39}
$$

We now apply our channel model comprising a pure-loss channel and a polarization misalignment (we neglect the phase shift as the states are already phase randomized). After going through the lossy and noisy channel, ρ_{in} evolves to

$$
\begin{aligned}
\rho'_{\mathrm{in}} = \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \ldots d\varphi_{N-1} \bigotimes_{i=0}^{N-1} &| \cos\theta_i \sqrt{\eta\beta_i} e^{i\varphi_i}\rangle \langle \cos\theta_i \sqrt{\eta\beta_i} e^{i\varphi_i}|_P \\
&\otimes |-\sin\theta_i \sqrt{\eta\beta_i} e^{i\varphi_i}\rangle \langle -\sin\theta_i \sqrt{\eta\beta_i} e^{i\varphi_i}|_{P_\perp}.
\end{aligned}
\tag{D40}
$$

The final step consists in evolving ρ'_{in} through the BBS network. We obtain the following state:

$$
\begin{aligned}
\rho_{\mathrm{out}} = \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \ldots d\varphi_{N-1} \bigotimes_{k=0}^{M-1} &\left| \sqrt{\frac{\eta}{M}} \sum_{i=0}^{N-1} f_{i,k} \cos\theta_i \sqrt{\beta_i} e^{i\varphi_i} \right\rangle \left\langle \sqrt{\frac{\eta}{M}} \sum_{i=0}^{N-1} f_{i,k} \cos\theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|_P \\
&\otimes \left| -\sqrt{\frac{\eta}{M}} \sum_{i=0}^{N-1} f_{i,k} \sin\theta_i \sqrt{\beta_i} e^{i\varphi_i} \right\rangle \left\langle -\sqrt{\frac{\eta}{M}} \sum_{i=0}^{N-1} f_{i,k} \sin\theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|_{P_\perp},
\end{aligned}
\tag{D41}
$$

which we remark is not anymore a product state of phase-randomized coherent states. Now, similarly to the calculation of $\Pr(\Omega_j | x_0, \ldots, x_{N-1}, R_{\mathrm{KG}})$, we can express each gain as follows:

$$\Pr(\Omega_j | \beta_0, \beta_1, \ldots, \beta_{N-1}) = (1 - p_d)^{M-1} \mathrm{Tr}\left[\rho_{\mathrm{out}} \mathbb{1}_j \bigotimes_{k \neq j} |0\rangle\langle 0|_k \right] - (1 - p_d)^M \mathrm{Tr}\left[\rho_{\mathrm{out}} \bigotimes_{k=0}^{M-1} |0\rangle\langle 0|_k \right], \qquad \text{(D42)}$$

where $|0\rangle\langle 0|_k$ is the projector on the vacuum of the output mode k for polarizations P and $P_\perp$, since the detectors do not distinguish polarization. We now evaluate the two terms in Eq. (D42). Let us begin with the second, i.e.,

$$\mathrm{Tr}\left[\rho_{\mathrm{out}} \bigotimes_{k=0}^{M-1} |0\rangle\langle 0|_k \right] = \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \ldots d\varphi_{N-1}$$

$$\times \prod_{k=0}^{M-1} \left| \langle 0 | \sqrt{\frac{\eta}{M}} \sum_{i=0}^{N-1} f_{i,k} \cos\theta_i \sqrt{\beta_i} e^{i\varphi_i} \rangle \right|^2 \left| \langle 0 | - \sqrt{\frac{\eta}{M}} \sum_{i=0}^{N-1} f_{i,k} \sin\theta_i \sqrt{\beta_i} e^{i\varphi_i} \rangle \right|^2$$

$$= \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \ldots d\varphi_{N-1}$$

$$\times \prod_{k=0}^{M-1} \exp\left[-\left| \sqrt{\frac{\eta}{M}} \sum_{i=0}^{N-1} f_{i,k} \cos\theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 - \left| \sqrt{\frac{\eta}{M}} \sum_{i=0}^{N-1} f_{i,k} \sin\theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 \right]$$

$$= \int_0^{2\pi} \frac{d\varphi_0 \ldots d\varphi_{N-1}}{(2\pi)^N} \exp\left[-\frac{\eta}{M} \sum_{k=0}^{M-1} \left(\left| \sum_{i=0}^{N-1} f_{i,k} \cos\theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 + \left| \sum_{i=0}^{N-1} f_{i,k} \sin\theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 \right) \right]$$

$$\equiv \int_0^{2\pi} \frac{d\varphi_0 \ldots d\varphi_{N-1}}{(2\pi)^N} e^{-\frac{\eta}{M} \sum_{k=0}^{M-1} C_k}. \qquad \text{(D43)}$$

Let us now focus on the sum of the terms labeled C_k. By expanding the squares in C_k we obtain

$$\sum_{k=0}^{M-1} C_k = \sum_{k=0}^{M-1} \left(\sum_{i=0}^{N-1} \left| f_{i,k} \cos\theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 + \sum_{\substack{i,i'=0 \\ i \neq i'}}^{N-1} f_{i,k} f_{i',k} \cos\theta_i \cos\theta_{i'} \sqrt{\beta_i \beta_{i'}} e^{i(\varphi_i - \varphi_{i'})} \right.$$

$$+ \sum_{i=0}^{N-1} \left| f_{i,k} \sin\theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 + \sum_{\substack{i,i'=0 \\ i \neq i'}}^{N-1} f_{i,k} f_{i',k} \sin\theta_i \sin\theta_{i'} \sqrt{\beta_i \beta_{i'}} e^{i(\varphi_i - \varphi_{i'})} \right)$$

$$= \sum_{k=0}^{M-1} \left(\sum_{i=0}^{N-1} \cos^2\theta_i \beta_i + 2 \sum_{\substack{i,i'=0 \\ i < i'}}^{N-1} f_{i,k} f_{i',k} \cos\theta_i \cos\theta_{i'} \sqrt{\beta_i \beta_{i'}} \cos(\varphi_i - \varphi_{i'}) \right.$$

$$+ \sum_{i=0}^{N-1} \sin^2\theta_i \beta_i + 2 \sum_{\substack{i,i'=0 \\ i < i'}}^{N-1} f_{i,k} f_{i',k} \sin\theta_i \sin\theta_{i'} \sqrt{\beta_i \beta_{i'}} \cos(\varphi_i - \varphi_{i'}) \right). \qquad \text{(D44)}$$

Now, we use the result in Eq. (D16) (derived from Lemma 3) to argue that

$$\sum_{k=0}^{M-1} f_{i,k} f_{i',k} = \sum_{k=0}^{M-1} (-1)^{(\vec{i}+\vec{i'})\cdot\vec{k}}$$
$$= M\delta_{\vec{i},\vec{i'}}. \tag{D45}$$

By applying this result in Eq. (D44), and by noting that $\vec{i}$ and $\vec{i'}$ must differ in the sums that involve them, we are left with

$$\sum_{k=0}^{M-1} C_k = \sum_{k=0}^{M-1} \left(\sum_{i=0}^{N-1} \beta_i \cos\theta_i{}^2 + \sum_{i=0}^{N-1} \beta_i \sin\theta_i{}^2 \right) = M \sum_{i=0}^{N-1} \beta_i. \tag{D46}$$

By using this result in Eq. (D43), we can directly integrate over the phases and obtain the following expression for the second term in Eq. (D42):

$$\text{Tr}\left[\rho_{\text{out}} \bigotimes_{k=0}^{M-1} |0\rangle\langle 0|_k \right] = e^{-\eta \sum_i \beta_i}. \tag{D47}$$

Regarding the first term in Eq. (D42), we can express it as follows:

$$\text{Tr}\left[\rho_{\text{out}} \mathbb{1}_j \bigotimes_{k\neq j} |0\rangle\langle 0|_k \right] = \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \ldots d\varphi_{N-1} e^{-(\eta/M)\sum_{k=0, k\neq j}^{M-1} C_k}$$
$$= \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \ldots d\varphi_{N-1} e^{-(\eta/M)\left(\sum_{k=0}^{M-1} C_k - C_j\right)}$$
$$= e^{-\eta \sum_i \beta_i} \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \ldots d\varphi_{N-1} e^{\eta C_j/M}. \tag{D48}$$

Now we calculate the coefficient C_j by expanding its squares:

$$C_j = \left| \sum_{i=0}^{N-1} f_{i,j} \cos\theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2 + \left| \sum_{i=0}^{N-1} f_{i,j} \sin\theta_i \sqrt{\beta_i} e^{i\varphi_i} \right|^2$$
$$= \sum_{i=0}^{N-1} \beta_i + 2 \sum_{\substack{i,i'=0 \\ i<i'}}^{N-1} f_{i,j} f_{i',j} (\cos\theta_i \cos\theta_{i'} + \sin\theta_i \sin\theta_{i'}) \sqrt{\beta_i \beta_{i'}} \cos(\varphi_i - \varphi_{i'})$$
$$= \sum_{i=0}^{N-1} \beta_i + 2 \sum_{\substack{i,i'=0 \\ i<i'}}^{N-1} f_{i,j} f_{i',j} \cos(\theta_i - \theta_{i'}) \sqrt{\beta_i \beta_{i'}} \cos(\varphi_i - \varphi_{i'}). \tag{D49}$$

Now we use the fact that $\theta_i = \theta_1$ for every $i \geq 1$. By splitting the second sum into two terms, where the first has $i = 0$ fixed and in the second $i \geq 1$, we obtain

$$C_j = \sum_{i=0}^{N-1} \beta_i + 2\cos\theta \sum_{i=1}^{N-1} f_{i,j} \sqrt{\beta_0 \beta_i} \cos(\varphi_0 - \varphi_i) + 2 \sum_{\substack{i,i'=1 \\ i<i'}}^{N-1} f_{i,j} f_{i',j} \sqrt{\beta_i \beta_{i'}} \cos(\varphi_i - \varphi_{i'}), \tag{D50}$$

where $\theta = \theta_0 - \theta_1$. By using this expression in Eq. (D48), we obtain the following expression for the first term in Eq. (D42):

$$\text{Tr}\left[\rho_{\text{out}} \mathbb{1}_j \bigotimes_{k\neq j} |0\rangle\langle 0|_k \right] = e^{-\eta(1-1/M)\sum_i \beta_i} I_j(\beta_0, \ldots, \beta_{N-1}), \tag{D51}$$

where we define the integral:

$$I_j(\beta_0, \ldots, \beta_{N-1}) := \frac{1}{(2\pi)^N} \int_0^{2\pi} d\varphi_0 \ldots d\varphi_{N-1}$$

$$\times \exp\left[\frac{2\eta}{M}\left(\cos\theta \sum_{i=1}^{N-1} f_{i,j}\sqrt{\beta_0\beta_i}\cos(\varphi_0 - \varphi_i) + \sum_{\substack{i,i'=1\\i<i'}}^{N-1} f_{i,j}f_{i',j}\sqrt{\beta_i\beta_{i'}}\cos(\varphi_i - \varphi_{i'})\right)\right]. \quad \text{(D52)}$$

By employing Eqs. (D51) and (D47) in Eq. (D42), we obtain the following compact expression for the gains:

$$\Pr(\Omega_j|\beta_0, \beta_1, \ldots, \beta_{N-1})$$
$$= (1 - p_d)^{M-1} e^{-\eta(1-1/M)\sum_i \beta_i} I_j(\beta_0, \ldots, \beta_{N-1}) - (1 - p_d)^M e^{-\eta\sum_i \beta_i}, \quad \text{(D53)}$$

where $I_j(\beta_0, \ldots, \beta_{N-1})$ is given in Eq. (D52).

Of note, due to our symmetric channel model, the gains are independent of which detector D_j clicks. To show this, we argue that the integral in Eq. (D52) is actually independent of j. To this aim, we label the function to be integrated in Eq. (D52) as follows:

$$F_j(\varphi_0, \ldots, \varphi_{N-1}) := \exp\left[\frac{2\eta}{M}\left(\cos\theta \sum_{i=1}^{N-1}(-1)^{\vec{i}\cdot\vec{j}}\sqrt{\beta_0\beta_i}\cos(\varphi_0 - \varphi_i) + \sum_{\substack{i,i'=1\\i<i'}}^{N-1}(-1)^{(\vec{i}+\vec{i'})\cdot\vec{j}}\sqrt{\beta_i\beta_{i'}}\cos(\varphi_i - \varphi_{i'})\right)\right] \quad \text{(D54)}$$

and observe that this function is periodic in each variable φ_i, with period 2π. The only dependency of F_j on j comes from the ± 1 signs inside the sums. We can reabsorb such signs by defining alternative integration variables $\Phi_i := \varphi_i - \pi \cdot (\vec{i} \cdot \vec{j})$, which allow us to simplify the summands as follows:

$$(-1)^{\vec{i}\cdot\vec{j}}\cos(\varphi_0 - \varphi_i) = \cos(\Phi_0 - \Phi_i), \quad \text{(D55)}$$

$$(-1)^{(\vec{i}+\vec{i'})\cdot\vec{j}}\cos(\varphi_i - \varphi_{i'}) = (-1)^{\vec{i'}\cdot\vec{j}-\vec{i}\cdot\vec{j}}\cos(\varphi_i - \varphi_{i'}) = \cos(\Phi_i - \Phi_{i'}). \quad \text{(D56)}$$

Then, by performing the change of variable $\Phi_i := \varphi_i - \pi \cdot (\vec{i} \cdot \vec{j})$ in the integral and by using the fact that the function F_j is periodic in each variable, we obtain

$$I_j(\beta_0, \ldots, \beta_{N-1}) = \frac{1}{(2\pi)^N} \int_{-\pi(\vec{i}\cdot\vec{j})}^{2\pi-\pi(\vec{i}\cdot\vec{j})} d\Phi_0 d\Phi_1 \ldots d\Phi_{N-1} F_0(\Phi_0, \Phi_1, \ldots, \Phi_{N-1})$$

$$= \frac{1}{(2\pi)^N} \int_0^{2\pi} d\Phi_0 d\Phi_1 \ldots d\Phi_{N-1} F_0(\Phi_0, \Phi_1, \ldots, \Phi_{N-1}) = I_0(\beta_0, \ldots, \beta_{N-1}), \quad \text{(D57)}$$

which confirms that I_j is independent of j. The final formula for the gains is thus

$$\Pr(\Omega_j|\beta_0, \beta_1, \ldots, \beta_{N-1}) = (1 - p_d)^{M-1} e^{-\eta(1-1/M)\sum_i \beta_i} I(\beta_0, \ldots, \beta_{N-1}) - (1 - p_d)^M e^{-\eta\sum_i \beta_i}, \quad \text{(D58)}$$

where the integral

$$I(\beta_0, \ldots, \beta_{N-1}) = \int_0^{2\pi} \frac{d\varphi_0 \ldots d\varphi_{N-1}}{(2\pi)^N} \exp\left[\frac{2\eta}{M}\left(\cos\theta \sum_{i=1}^{N-1}\sqrt{\beta_0\beta_i}\cos(\varphi_0 - \varphi_i) + \sum_{\substack{i,i'=1\\i<i'}}^{N-1}\sqrt{\beta_i\beta_{i'}}\cos(\varphi_i - \varphi_{i'})\right)\right], \quad \text{(D59)}$$

is evaluated numerically in our simulations. Note that we freely relabeled the variables in the integral back to φ_i.

5. Computation of $\mathbf{Pr}(\Omega_j | n_0, \ldots, n_{N-1})$

Here we calculate the analytical expression of any yield $Y^j_{n_0,\ldots,n_{N-1}}$, defined in Eq. (6) as the probability that detector D_j clicks given the hypothetical scenario in which party A_i sent exactly n_i photons.

We remark that in an experiment the parties cannot, in general, learn the exact value of each yield with the decoy-state analysis, but can derive upper bounds as shown in Appendix C. In the limit of an infinite number of decoy intensities, the yields' upper bounds would tend to the exact values computed here.

To evaluate $Y^j_{n_0,\ldots,n_{N-1}}$, we consider the scenario in which the parties send the state $\bigotimes_{i=0}^{N-1} |n_i\rangle$, where $|n_i\rangle$ is a Fock state of n_i photons. The state can be written as

$$|\xi(n_0,\ldots,n_{N-1})\rangle = \left(\prod_{i=0}^{N-1} \frac{(\hat{a}_i^\dagger)^{n_i}}{\sqrt{n_i!}}\right) |0\rangle, \tag{D60}$$

where $\hat{a}_i^\dagger$ is the creation operator of the optical mode of party A_i and $|0\rangle$ represents the vacuum state on all modes. We now introduce, step by step, the effect of all sources of noise and then apply the BBS network.

The lossy channel transforms each party's mode according to

$$\hat{a}_i^\dagger \to \sqrt{\eta}\hat{a}_i^\dagger + \sqrt{1-\eta}\hat{l}_i^\dagger, \tag{D61}$$

where $\hat{l}_i^\dagger$ is the creation operator of the loss mode of party A_i. The input state $|\xi\rangle$ is transformed as follows:

$$\begin{aligned}
|\xi'(n_0,\ldots,n_{N-1})\rangle &= \left(\prod_{i=0}^{N-1} \frac{(\sqrt{\eta}\hat{a}_i^\dagger + \sqrt{1-\eta}\hat{l}_i^\dagger)^{n_i}}{\sqrt{n_i!}}\right) |0\rangle \\
&= \left[\prod_{i=0}^{N-1} \left(\sum_{k_i=0}^{n_i} \binom{n_i}{k_i} \frac{\eta^{k_i/2}(1-\eta)^{(n_i-k_i)/2}}{\sqrt{n_i!}} (\hat{a}_i^\dagger)^{k_i}(\hat{l}_i^\dagger)^{n_i-k_i}\right)\right] |0\rangle \\
&= \sum_{k_0=0}^{n_0} \cdots \sum_{k_{N-1}=0}^{n_{N-1}} \binom{n_0}{k_0} \cdots \binom{n_{N-1}}{k_{N-1}} \frac{\eta^{\sum_i k_i/2}(1-\eta)^{\sum_i(n_i-k_i)/2}}{\sqrt{n_0!\cdots n_{N-1}!}} \sqrt{(n_0-k_0)!\cdots(n_{N-1}-k_{N-1})!} \\
&\quad \times \left[\prod_{i=0}^{N-1}(\hat{a}_i^\dagger)^{k_i}\right] |0\rangle_{a_0,\ldots,a_{N-1}} \otimes |n_0-k_0\rangle_{l_0} \otimes \cdots \otimes |n_{N-1}-k_{N-1}\rangle_{l_{N-1}},
\end{aligned} \tag{D62}$$

where we just use the binomial expansion in the second line and where a_i and l_i are used to indicate the optical mode and the loss mode of party A_i, respectively.

We now note that the loss modes are not observed by the parties and thus need to be traced out. The density matrix $\rho' = |\xi'\rangle\langle\xi'|$ will thus have two sets of indices $(k_0,\ldots,k_{N-1})$ and $(k_0',\ldots,k_{N-1}')$. However, it is immediate to see from Eq. (D62) that tracing out the loss modes will impose the conditions $k_i = k_i'$ $\forall i$. Thus we are left with the state

$$\begin{aligned}
\rho' &= \sum_{k_0=0}^{n_0} \cdots \sum_{k_{N-1}=0}^{n_{N-1}} \binom{n_0}{k_0}^2 \cdots \binom{n_{N-1}}{k_{N-1}}^2 \eta^{\sum_i k_i}(1-\eta)^{\sum_i(n_i-k_i)} \frac{(n_0-k_0)!\cdots(n_{N-1}-k_{N-1})!}{n_0!\cdots n_{N-1}!} \\
&\quad \times \left[\prod_{i=0}^{N-1}(\hat{a}_i^\dagger)^{k_i}\right] |0\rangle\langle 0|_{a_0,\ldots,a_{N-1}} \left[\prod_{i=0}^{N-1}(\hat{a}_i)^{k_i}\right] \\
&= \sum_{k_0=0}^{n_0} \cdots \sum_{k_{N-1}=0}^{n_{N-1}} \binom{n_0}{k_0} \cdots \binom{n_{N-1}}{k_{N-1}} \frac{\eta^{\sum_i k_i}(1-\eta)^{\sum_i(n_i-k_i)}}{k_0!\cdots k_{N-1}!} \left[\prod_{i=0}^{N-1}(\hat{a}_i^\dagger)^{k_i}\right] |0\rangle\langle 0|_{a_0,\ldots,a_{N-1}} \left[\prod_{i=0}^{N-1}(\hat{a}_i)^{k_i}\right],
\end{aligned} \tag{D63}$$

where we use the fact that $(n_i-k_i)!/n_i! = 1/\binom{n_i}{k_i}k_i!$ and where, from now on, for simplicity of notation we neglect the explicit dependence of the state on $n_0,\ldots,n_{N-1}$.

We now introduce the polarization misalignment, while we skip the phase misalignment since its effect cancels out on tensor products of Fock states. The polarization misalignment acts on the creation operators of each mode as follows:

$$\hat{a}_i^\dagger \rightarrow \cos\theta_i \hat{a}_{i,P}^\dagger - \sin\theta_i \hat{a}_{i,P_\perp}^\dagger, \tag{D64}$$

where we recall that in our channel model we set $\theta_i = \theta_1$ for $i \geq 1$, i.e., we introduce only a misalignment between the reference party A_0 and the other parties. For simplicity of notation we omit the label P and consider the polarization P to be the input polarization and label the orthogonal polarization with $\perp$. By applying the above transformation to the creation operators in Eq. (D63) and by using again the binomial expansion we obtain

$$\prod_{i=0}^{N-1}\left(\cos\theta_i\hat{a}_i^\dagger - \sin\theta_i\hat{a}_{i,\perp}^\dagger\right)^{k_i} = \prod_{i=0}^{N-1}\left(\sum_{l_i=0}^{k_i}(-1)^{k_i-l_i}\binom{k_i}{l_i}(\cos\theta_i)^{l_i}(\sin\theta_i)^{k_i-l_i}(\hat{a}_i^\dagger)^{l_i}(\hat{a}_{i,\perp}^\dagger)^{k_i-l_i}\right)$$

$$= \sum_{l_0=0}^{k_0}\cdots\sum_{l_{N-1}=0}^{k_{N-1}}(-1)^{\sum_i(k_i-l_i)}\binom{k_0}{l_0}\cdots\binom{k_{N-1}}{l_{N-1}}(\cos\theta_0)^{l_0}$$

$$\times (\sin\theta_0)^{k_0-l_0}(\cos\theta_1)^{\sum_{i=1}^{N-1}l_i}(\sin\theta_1)^{\sum_{i=1}^{N-1}(k_i-l_i)}\left[\prod_{i=0}^{N-1}(\hat{a}_i^\dagger)^{l_i}(\hat{a}_{i,\perp}^\dagger)^{k_i-l_i}\right]. \tag{D65}$$

By using this expression in Eq. (D63), we obtain

$$\rho'' = \sum_{k_0=0}^{n_0}\cdots\sum_{k_{N-1}=0}^{n_{N-1}}\sum_{l_0=0}^{k_0}\cdots\sum_{l_{N-1}=0}^{k_{N-1}}\sum_{l_0'=0}^{k_0}\cdots\sum_{l_{N-1}'=0}^{k_{N-1}}\binom{n_0}{k_0}\cdots\binom{n_{N-1}}{k_{N-1}}\binom{k_0}{l_0}\cdots\binom{k_{N-1}}{l_{N-1}}\binom{k_0}{l_0'}\cdots\binom{k_{N-1}}{l_{N-1}'}$$

$$\times (-1)^{\sum_i(2k_i-l_i-l_i')}\frac{\eta^{\sum_i k_i}(1-\eta)^{\sum_i(n_i-k_i)}}{k_0!\cdots k_{N-1}!}\times(\cos\theta_0)^{l_0+l_0'}(\sin\theta_0)^{2k_0-l_0-l_0'}(\cos\theta_1)^{\sum_{i=1}^{N-1}(l_i+l_i')}(\sin\theta_1)^{\sum_{i=1}^{N-1}(2k_i-l_i-l_i')}$$

$$\times\left[\prod_{i=0}^{N-1}(\hat{a}_i^\dagger)^{l_i}(\hat{a}_{i,\perp}^\dagger)^{k_i-l_i}\right]|0\rangle\langle0|_{a_0,\dots,a_{N-1},a_{0,\perp},\dots,a_{N-1,\perp}}\left[\prod_{i=0}^{N-1}(\hat{a}_i)^{l_i'}(\hat{a}_{i,\perp})^{k_i-l_i'}\right]. \tag{D66}$$

We now let the state evolve through the optical setup of the BBS network. The resulting transformation of the incoming creation operators is given in Eq. (3), as proved in Appendix A. This brings us to the following state of the output modes in the BBS network:

$$\rho_{\text{out}} = \sum_{k_0=0}^{n_0}\cdots\sum_{k_{N-1}=0}^{n_{N-1}}\sum_{l_0=0}^{k_0}\cdots\sum_{l_{N-1}=0}^{k_{N-1}}\sum_{l_0'=0}^{k_0}\cdots\sum_{l_{N-1}'=0}^{k_{N-1}}\binom{n_0}{k_0}\cdots\binom{n_{N-1}}{k_{N-1}}\binom{k_0}{l_0}\cdots\binom{k_{N-1}}{l_{N-1}}\binom{k_0}{l_0'}\cdots\binom{k_{N-1}}{l_{N-1}'}$$

$$\times (-1)^{\sum_i(2k_i-l_i-l_i')}\frac{\eta^{\sum_i k_i}(1-\eta)^{\sum_i(n_i-k_i)}}{k_0!\cdots k_{N-1}!}(\cos\theta_0)^{l_0+l_0'}(\sin\theta_0)^{2k_0-l_0-l_0'}(\cos\theta_1)^{\sum_{i=1}^{N-1}(l_i+l_i')}(\sin\theta_1)^{\sum_{i=1}^{N-1}(2k_i-l_i-l_i')}$$

$$\times\left[\prod_{i=0}^{N-1}\left(\frac{1}{\sqrt{M}}\sum_{s=0}^{M-1}(-1)^{\vec{s}\cdot\vec{i}}\hat{d}_s^\dagger\right)^{l_i}\left(\frac{1}{\sqrt{M}}\sum_{s'=0}^{M-1}(-1)^{\vec{s}'\cdot\vec{i}}\hat{d}_{s',\perp}^\dagger\right)^{k_i-l_i}\right]|0\rangle\langle0|_{d_0,\dots,d_{N-1},d_{0,\perp},\dots,d_{N-1,\perp}}$$

$$\times\left[\prod_{i=0}^{N-1}\left(\frac{1}{\sqrt{M}}\sum_{q=0}^{M-1}(-1)^{\vec{q}\cdot\vec{i}}\hat{d}_q\right)^{l_i'}\left(\frac{1}{\sqrt{M}}\sum_{q'=0}^{M-1}(-1)^{\vec{q}'\cdot\vec{i}}\hat{d}_{q',\perp}\right)^{k_i-l_i'}\right]. \tag{D67}$$

From the definition of yields, $Y_{n_0,\dots,n_{N-1}}^j = \Pr(\Omega_j|n_0,\dots,n_{N-1})$, we can express them as follows by including dark counts (each detector has a probability p_d of a dark count):

$$Y_{n_0,\dots,n_{N-1}}^j = (1-p_d)^{M-1}\text{Tr}\left[\rho_{\text{out}}\mathbb{1}_j\bigotimes_{r\neq j}^{M-1}|0\rangle\langle0|_r\right] - (1-p_d)^M\text{Tr}\left[\rho_{\text{out}}\bigotimes_{r=0}^{M-1}|0\rangle\langle0|_r\right], \tag{D68}$$

where the identity operator and the projector on the vacuum are defined on both modes of polarization, since the detectors cannot distinguish them. We note that calculating the second trace in Eq. (D68) is trivial: projecting all modes onto the vacuum forces all indexes to be equal to zero, thus yielding the result:

$$\text{Tr}\left[\rho_{\text{out}} \bigotimes_{r=0}^{M-1} |0\rangle\langle 0|_r \right] = (1-\eta)^{\sum_i n_i}. \tag{D69}$$

In order to calculate the first trace in Eq. (D68), we would need to expand the sums over the detectors' creation modes using multinomial expansions. However, since we need to project onto the vacuum state in all modes except modes d_j and $d_{j,\perp}$, this operation will force all the terms in the multinomial expansion to vanish, except for the terms containing $\hat{d}_j$ or $\hat{d}_{j,\perp}$. Therefore, the reduced state of ρ_{out} after projecting onto the vacuum all modes except the jth mode, $\rho_{\text{out}}^{(j)} := \langle 0_1, \ldots, 0_{j-1}, 0_{j+1}, \ldots, 0_{M-1} | \rho_{\text{out}} | 0_1, \ldots, 0_{j-1}, 0_{j+1}, \ldots, 0_{M-1} \rangle$, reads

$$\begin{aligned}
\rho_{\text{out}}^{(j)} = &\sum_{k_0=0}^{n_0} \cdots \sum_{k_{N-1}=0}^{n_{N-1}} \sum_{l_0=0}^{k_0} \cdots \sum_{l_{N-1}=0}^{k_{N-1}} \sum_{l'_0=0}^{k_0} \cdots \sum_{l'_{N-1}=0}^{k_{N-1}} \binom{n_0}{k_0} \cdots \binom{n_{N-1}}{k_{N-1}} \binom{k_0}{l_0} \cdots \binom{k_{N-1}}{l_{N-1}} \binom{k_0}{l'_0} \cdots \binom{k_{N-1}}{l'_{N-1}} \\
&\times (-1)^{\sum_i(2k_i-l_i-l'_i)} \frac{\eta^{\sum_i k_i}(1-\eta)^{\sum_i(n_i-k_i)}}{k_0!\cdots k_{N-1}!}(\cos\theta_0)^{l_0+l'_0}(\sin\theta_0)^{2k_0-l_0-l'_0}(\cos\theta_1)^{\sum_{i=1}^{N-1}(l_i+l'_i)}(\sin\theta_1)^{\sum_{i=1}^{N-1}(2k_i-l_i-l'_i)} \\
&\times \left[\prod_{i=0}^{N-1}\left(\frac{(-1)^{\vec{j}\cdot\vec{i}}}{\sqrt{M}}\right)^{k_i}\left(\hat{d}_j^\dagger\right)^{l_i}\left(\hat{d}_{j,\perp}^\dagger\right)^{k_i-l_i} \right] |0\rangle\langle 0|_{d_j,d_{j,\perp}} \left[\prod_{i=0}^{N-1}\left(\frac{(-1)^{\vec{j}\cdot\vec{i}}}{\sqrt{M}}\right)^{k_i}\left(\hat{d}_j\right)^{l'_i}\left(\hat{d}_{j,\perp}\right)^{k_i-l'_i} \right] \\
= &\sum_{k_0=0}^{n_0} \cdots \sum_{k_{N-1}=0}^{n_{N-1}} \sum_{l_0=0}^{k_0} \cdots \sum_{l_{N-1}=0}^{k_{N-1}} \sum_{l'_0=0}^{k_0} \cdots \sum_{l'_{N-1}=0}^{k_{N-1}} \binom{n_0}{k_0} \cdots \binom{n_{N-1}}{k_{N-1}} \binom{k_0}{l_0} \cdots \binom{k_{N-1}}{l_{N-1}} \binom{k_0}{l'_0} \cdots \binom{k_{N-1}}{l'_{N-1}} \\
&\times (-1)^{\sum_i(2k_i-l_i-l'_i)} \frac{\eta^{\sum_i k_i}(1-\eta)^{\sum_i(n_i-k_i)}}{M^{\sum_i k_i}k_0!\cdots k_{N-1}!}(\cos\theta_0)^{l_0+l'_0}(\sin\theta_0)^{2k_0-l_0-l'_0}(\cos\theta_1)^{\sum_{i=1}^{N-1}(l_i+l'_i)}(\sin\theta_1)^{\sum_{i=1}^{N-1}(2k_i-l_i-l'_i)} \\
&\times \left[\left(\hat{d}_j^\dagger\right)^{\sum_i l_i}\left(\hat{d}_{j,\perp}^\dagger\right)^{\sum_i(k_i-l_i)} \right] |0\rangle\langle 0|_{d_j,d_{j,\perp}} \left[\left(\hat{d}_j\right)^{\sum_i l'_i}\left(\hat{d}_{j,\perp}\right)^{\sum_i(k_i-l'_i)} \right],
\end{aligned} \tag{D70}$$

where we use the fact that $\left((-1)^{\vec{j}\cdot\vec{i}}\right)^{2\sum_i k_i} = 1$. We observe that, as expected, the yields do not depend on j, i.e., on the detector that clicked, due to our symmetric channel model.

We can now compute the first trace in Eq. (D68) by simply taking the trace of $\rho_{\text{out}}^{(j)}$. We note that this forces the identity $\sum_i l_i = \sum_i l'_i$ on the indexes, allowing us to obtain the following expression:

$$\text{Tr}\left[\rho_{\text{out}} \mathbb{1}_j \bigotimes_{r\neq j} |0\rangle\langle 0|_r \right] = \text{Tr}[\rho_{\text{out}}^{(j)}] = Q(n_0,\ldots,n_{N-1}), \tag{D71}$$

where we define

$$\begin{aligned}
Q(n_0,\ldots,n_{N-1}) = &\sum_{k_0=0}^{n_0} \cdots \sum_{k_{N-1}=0}^{n_{N-1}} \sum_{(l_0,\ldots,l_{N-1},l'_0,\ldots,l'_{N-1})\in\mathcal{L}(k_0,\ldots,k_{N-1})} \\
&\times \binom{n_0}{k_0} \cdots \binom{n_{N-1}}{k_{N-1}} \binom{k_0}{l_0} \cdots \binom{k_{N-1}}{l_{N-1}} \binom{k_0}{l'_0} \cdots \binom{k_{N-1}}{l'_{N-1}} \\
&\times \frac{\eta^{\sum_i k_i}(1-\eta)^{\sum_i(n_i-k_i)}}{M^{\sum_i k_i}k_0!\cdots k_{N-1}!}(\cos\theta_0)^{l_0+l'_0}(\sin\theta_0)^{2k_0-l_0-l'_0} \\
&\times (\cos\theta_1)^{\sum_{i=1}^{N-1}(l_i+l'_i)}(\sin\theta_1)^{\sum_{i=1}^{N-1}(2k_i-l_i-l'_i)}\left(\sum_i l_i\right)!\left(\sum_i(k_i-l_i)\right)!,
\end{aligned} \tag{D72}$$

where the summation set is defined as

$$\mathcal{L}(k_0, \ldots, k_{N-1}) := \left\{ (l_0, \ldots, l_{N-1}, l'_0, \ldots, l'_{N-1}) : 0 \le l_i \le k_i, \ 0 \le l'_i \le k_i, \ \sum_{i=0}^{N-1} l_i = \sum_{i=0}^{N-1} l'_i \right\}. \tag{D73}$$
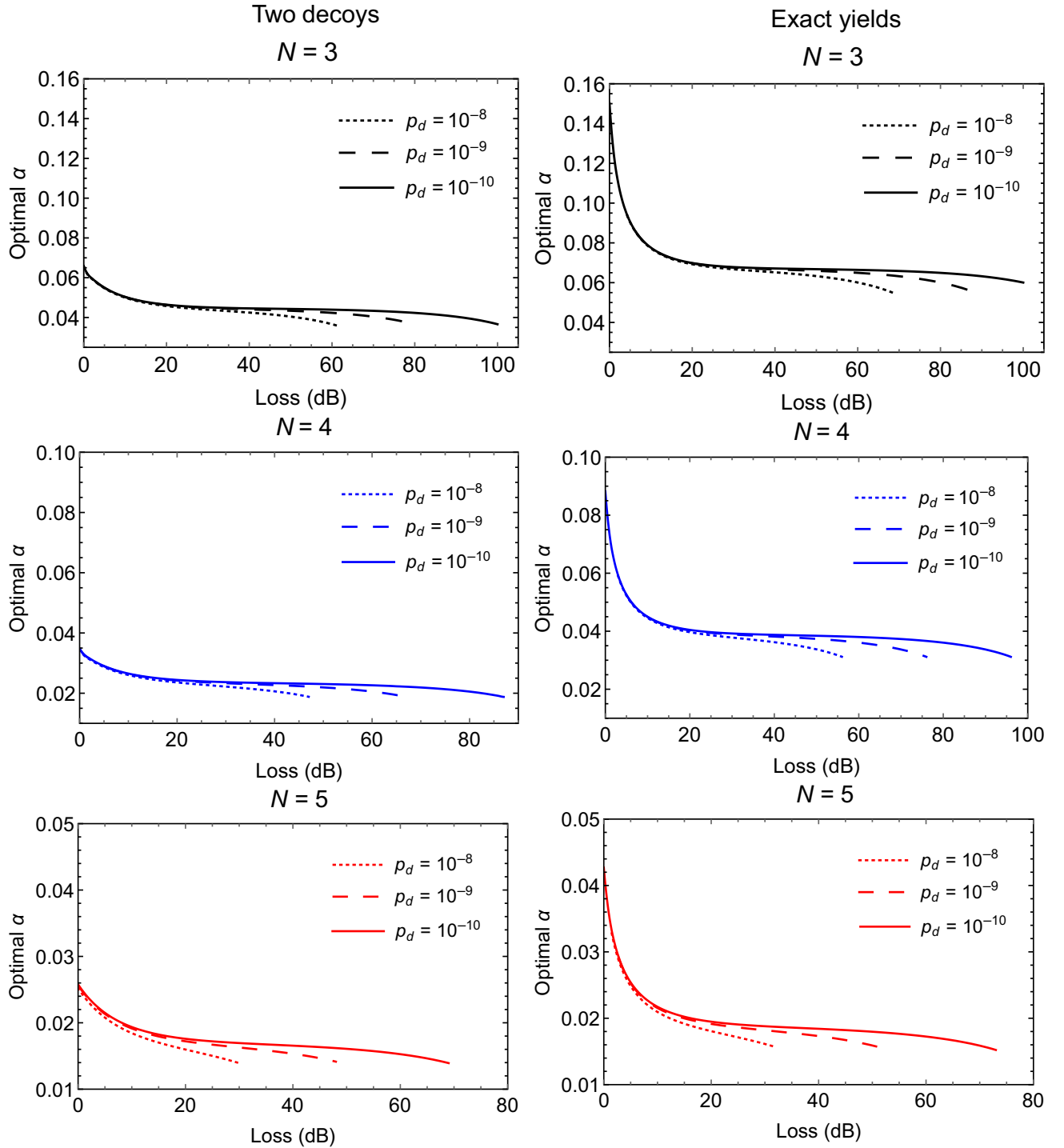

FIG. 5. The optimal value of the signal amplitude (α) that maximizes the key rate plotted in Fig. 4, for different values of the dark-count probability (p_d) and number of parties (N). On the left, the key rate is computed by using the analytical bounds on the yields (34) in the phase error rate bound (7), while the plots on the right use the exact expressions of the yields for our channel model (D74). We observe that a tighter bound on the yields allows for a higher value of α and leads to a higher key rate (see Fig. 4).

By using Eqs. (D69) and (D71) in Eq. (D68), we obtain the final expression for the yields in our channel model:

$$Y^j_{n_0,\dots,n_{N-1}} = (1 - p_d)^{M-1} Q(n_0,\dots,n_{N-1})$$
$$- (1 - p_d)^M (1 - \eta)^{\sum_i n_i}, \qquad \text{(D74)}$$

where $Q(n_0,\dots,n_{N-1})$ is defined in Eq. (D72) and we emphasize once again that the yields are independent of j.

APPENDIX E: NUMERICAL SIMULATIONS

In this Appendix we provide more details about the numerical simulations presented in Sec. V of the paper.

In our simulations, we set a polarization and a phase misalignment between the reference party A_0 and each other party of 2%. This means that the parameters θ_i and ϕ_i, introduced in Appendix D to describe the polarization rotation and the phase mismatch of party A_i, are set to $\phi_0 = 0$, $\phi_{i\geq 1} = \phi$, $\theta_{i\geq 1} = \theta_1$, and $\phi = \theta_0 - \theta_1 = \arcsin\sqrt{0.02}$. We compute the protocol's key rate for three values of p_d, i.e., the probability of a dark count in a given detector, namely, $p_d = 10^{-8}, 10^{-9}$, and 10^{-10}.

As for the decoy-state analysis, we consider two decoy intensities for each party, β_0 and β_1, and use the analytical bounds derived in Sec. IV to compute the upper bound (7) on the phase error rate. The decoy intensity β_0 is fixed to $\beta_0 = 0.5$, which we verify is a close-to-optimal value for all loss parameters, while $\beta_1 = 0$ is optimal. In Sec. V we also plot the key rate in the case in which the exact value of the yields is known, which corresponds to the limit where the parties have an infinite number of decoy intensities. The exact values of the yields are computed for our channel model in Appendix D and are reported in Eq. (D74). We then replaced the exact yields $Y_0,\dots,Y_{N-1}$ in the phase error rate bound (7), in place of the yields' bounds $\bar{Y}_0,\dots,\bar{Y}_{N-1}$.

The key rates in Fig. 4 are optimized over the signal amplitude α for all values of loss and is computed for $N = 3, 4$, and 5 parties. In Fig. 5 we provide the optimal values of α for every loss, both when we use the yields bounds obtained with two decoys and when we use the exact expressions of the yields from the channel model. By comparing the optimal values of α in the two cases, we deduce that tighter bounds on the yields would allow for a higher optimal value of α. This is explained by the fact that having tighter bounds on the yields in the phase error rate bound (7) allows the yields' coefficients in that expression to grow, i.e., α to grow, without increasing the phase error rate bound. In turn, greater values of α can increase the key rate due to a higher chance of having a detector click [see Fig. 4(b)]. Therefore, we deduce that increasing the number of decoy intensities used by each party would lead to better yields' bounds and hence to a significantly improved key rate.

In order to reduce the number of yields that are nontrivially bounded in Eq. (7), we remark that the polarization and phase angles θ_i and ϕ_i are the same for all parties except for reference party A_0. Moreover, the signal and decoy intensities are the same for all parties as well as the losses. Therefore, the channel model is symmetric under the permutation of parties $A_1, A_2, \dots, A_{N-1}$. This implies, in particular, that the yields in Eq. (7) satisfy

$$Y_{n_0,n_1,\dots,n_{N-1}} = Y_{n_0,\sigma(n_1,\dots,n_{N-1})}, \qquad \text{(E1)}$$

where $\sigma(n_1,\dots,n_{N-1})$ represents a permutation of the indexes $n_1,\dots,n_{N-1}$. The permutational symmetry of the yields in our channel model implies that, in computing the phase error rate bound (7) for a cutoff $\bar{n} = 4$ (above which every yield is bounded by one), we need only to bound the following yields for $N = 3$: $Y_{0,0,0}, Y_{2,0,0}, Y_{0,2,0}, Y_{4,0,0}, Y_{0,4,0} Y_{1,1,0}, Y_{0,1,1}, Y_{2,2,0}, Y_{0,2,2}, Y_{1,3,0}, Y_{0,1,3}, Y_{1,1,2}$.

Similarly, for $N = 4$ we bound only the yields: $Y_{0,0,0,0}, Y_{2,0,0,0}, Y_{0,2,0,0}, Y_{4,0,0,0}, Y_{0,4,0,0}, Y_{1,1,0,0}, Y_{0,1,1,0}, Y_{2,2,0,0}, Y_{0,2,2,0}, Y_{1,3,0,0}, Y_{0,1,3,0}, Y_{1,1,2,0}, Y_{0,1,1,2}, Y_{1,1,1,1}$.

And for $N = 5$ we bound only the yields: $Y_{0,0,0,0,0}, Y_{2,0,0,0,0}, Y_{2,0,0,0,0}, Y_{4,0,0,0,0}, Y_{0,4,0,0,0} Y_{1,1,0,0,0}, Y_{0,1,1,0,0}, Y_{2,2,0,0,0}, Y_{0,2,2,0,0}, Y_{1,3,0,0,0}, Y_{0,1,3,0,0}, Y_{1,1,2,0,0}, Y_{0,1,1,2,0}, Y_{1,1,1,1,0}, Y_{0,1,1,1,1}$.

[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, Adv. Opt. Photonics **12**, 1012 (2020).

[2] 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).

[3] K. Chen and H. Lo, Multi-partite quantum cryptographic protocols with noisy GHZ states, Quantum Inf. Comput. **7**, 689 (2007).

[4] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, Multi-partite entanglement can speed up quantum key distribution in networks, New J. Phys. **19**, 093012 (2017).

[5] F. Grasselli, H. Kampermann, and D. Bruß, Finite-key effects in multipartite quantum key distribution protocols, New J. Phys. **20**, 113014 (2018).

[6] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, Modular network for high-rate quantum conferencing, Commun. Phys. **2**, 118 (2019).

[7] Z. Zhang, R. Shi, and Y. Guo, Multipartite continuous variable quantum conferencing network with entanglement in the middle, Appl. Sci. **8**, 1312 (2018).

[8] S. Zhao, P. Zeng, W.-F. Cao, X.-Y. Xu, Y.-Z. Zhen, X. Ma, L. Li, N.-L. Liu, and K. Chen, Phase-Matching Quantum Cryptographic Conferencing, Phys. Rev. Appl. **14**, 024010 (2020).

[9] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, Quantum conference key agreement: A review, Adv. Quantum Technol. **3**, 2000025 (2020).

[10] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, Experimental quantum conference key agreement, Sci. Adv. **7**, eabe0395 (2021).

[11] A. Pickston, J. Ho, A. Ulibarrena, F. Grasselli, M. Proietti, C. L. Morrison, P. Barrow, F. Graffitti, and A. Fedrizzi, Experimental network advantage for quantum conference key agreement, ArXiv:2207.01643 (2022).

[12] F. Hahn, J. de Jong, and A. Pappa, Anonymous Quantum Conference Key Agreement, PRX Quantum **1**, 020325 (2020).

[13] F. Grasselli, G. Murta, J. de Jong, F. Hahn, H. Kampermann, and A. Pappa, Secure Anonymous Conferencing in Quantum Networks, PRX Quantum **3**, 040306 (2022).

[14] L. Rückle, J. Budde, J. de Jong, F. Hahn, A. Pappa, and S. Barz, Experimental anonymous conference key agreement using linear cluster states, ArXiv:quant-ph/2207.09487 (2022).

[15] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature **557**, 400 (2018).

[16] X. Ma, P. Zeng, and H. Zhou, Phase-Matching Quantum Key Distribution, Phys. Rev. X **8**, 031043 (2018).

[17] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, npj Quantum Inf. **5**, 64 (2019).

[18] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 062323 (2018).

[19] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Twin-Field Quantum Key Distribution Without Phase Postselection, Phys. Rev. Appl. **11**, 034053 (2019).

[20] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[21] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. **5**, 5235 (2014).

[22] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Direct and Reverse Secret-Key Capacities of a Quantum Channel, Phys. Rev. Lett. **102**, 050503 (2009).

[23] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, Nat. Photonics **13**, 334 (2019).

[24] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental Twin-Field Quantum Key Distribution Through Sending or Not Sending, Phys. Rev. Lett. **123**, 100505 (2019).

[25] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System, Phys. Rev. X **9**, 021046 (2019).

[26] X.-T. Fang, *et al.*, Implementation of quantum key distribution surpassing the linear rate-transmittance bound, Nat. Photonics **14**, 422 (2020).

[27] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, M.-J. Li, H. Chen, H. Li, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km, Phys. Rev. Lett. **124**, 070501 (2020).

[28] M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, M.-J. Li, Z. Yuan, and A. J. Shields, 600-km repeater-like quantum communications with dual-band stabilization, Nat. Photonics **15**, 530 (2021).

[29] H. Liu, *et al.*, Field Test of Twin-Field Quantum Key Distribution Through Sending-or-Not-Sending over 428 km, Phys. Rev. Lett. **126**, 250502 (2021).

[30] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas, Nat. Photonics **15**, 570 (2021).

[31] C. Clivati, A. Meda, S. Donadello, S. Virzì, M. Genovese, F. Levi, A. Mura, M. Pittaluga, Z. Yuan, A. J. Shields, M. Lucamarini, I. P. Degiovanni, and D. Calonico, Coherent phase transfer for real-world twin-field quantum key distribution, Nat. Commun. **13**, 157 (2022).

[32] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution over 830-km fibre, Nat. Photonics **16**, 154 (2022).

[33] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, D.-F. Zhao, W.-J. Zhang, F.-X. Chen, H. Li, L.-X. You, Z. Wang, Y. Chen, X.-B. Wang, Q. Zhang, and J.-W. Pan, Quantum Key Distribution over 658 km Fiber with Distributed Vibration Sensing, Phys. Rev. Lett. **128**, 180502 (2022).

[34] F. Grasselli, H. Kampermann, and D. Bruß, Conference key agreement with single-photon interference, New J. Phys. **21**, 123002 (2019).

[35] X.-Y. Cao, Y.-S. Lu, Z. Li, J. Gu, H.-L. Yin, and Z.-B. Chen, High key rate quantum conference key agreement with unconditional security, IEEE Access **9**, 128870 (2021).

[36] X.-Y. Cao, J. Gu, Y.-S. Lu, H.-L. Yin, and Z.-B. Chen, Coherent one-way quantum conference key agreement based on twin field, New J. Phys. **23**, 043002 (2021).

[37] J.-L. Bai, Y.-M. Xie, Z. Li, H.-L. Yin, and Z.-B. Chen, Post-matching quantum conference key agreement, Opt. Express **30**, 28865 (2022).

[38] W. Dür, G. Vidal, and J. I. Cirac, Three qubits can be entangled in two inequivalent ways, Phys. Rev. A **62**, 062314 (2000).

[39] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).

[40] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[41] X.-B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).

[42] S. Pirandola, General upper bound for conferencing keys in arbitrary quantum networks, IET Quantum Commun. **1**, 22 (2020).

[43] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, The uncertainty principle in the presence of quantum memory, Nat. Phys. **6**, 659 (2010).

[44] Note that we can assume, without loss of generality, that there is only one Kraus operator for each announcement Ω_j. Indeed, if there were more, the eavesdropper would be able to distinguish which operator acted on the optical modes with an ancillary classical flag. The flag would be part of the side information E, allowing the expansion of the entropy $H(X_0|E)_{\Omega_j}$ over each value of the flag, which coincides with the scenario of having only one Kraus operator.

[45] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, Cambridge, 2010).

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

[47] Y.-M. Xie, Y.-S. Lu, C.-X. Weng, X.-Y. Cao, Z.-Y. Jia, Y. Bao, Y. Wang, Y. Fu, H.-L. Yin, and Z.-B. Chen, Breaking the Rate-Loss Bound of Quantum Key Distribution with Asynchronous Two-Photon Interference, PRX Quantum **3**, 020315 (2022).

[48] P. Zeng, H. Zhou, W. Wu, and X. Ma, Mode-pairing quantum key distribution, Nat. Commun. **13**, 3903 (2022).

[49] F. Grasselli, Á. Navarrete, and M. Curty, Asymmetric twin-field quantum key distribution, New J. Phys. **21**, 113032 (2019).

[50] C.-L. Li, Y. Fu, W.-B. Liu, Y.-M. Xie, B.-H. Li, M.-G. Zhou, H.-L. Yin, and Z.-B. Chen, Breaking universal limitations on quantum conference key agreement without quantum memory, ArXiv:2212.05226 (2022).

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