Quantum weak coin flipping with a single photon

Mathieu Bozzio,[1,2] Ulysse Chabaud,[1] Iordanis Kerenidis,[3] and Eleni Diamanti[1]
[1]*Sorbonne Université, CNRS, LIP6, 4 Place Jussieu, F-75005 Paris, France*
[2]*Institut Polytechnique de Paris, Télécom Paris, LTCI, 19 Place Marguerite Perey, 91129 Palaiseau, France*
[3]*Université de Paris, CNRS, IRIF, 8 Place Aurélie Nemours, 75013 Paris, France*

(Received 20 February 2020; accepted 30 July 2020; published 19 August 2020)

Weak coin flipping is among the fundamental cryptographic primitives which ensure the security of modern communication networks. It allows two mistrustful parties to remotely agree on a random bit when they favor opposite outcomes. Unlike other two-party computations, one can achieve information-theoretic security using quantum mechanics only: both parties are prevented from biasing the flip with probability higher than $1/2+\epsilon$, where ϵ is arbitrarily low. Classically, the dishonest party can always cheat with probability 1 unless computational assumptions are used. Despite its importance, no physical implementation has been proposed for quantum weak coin flipping. Here, we present a practical protocol that requires a single photon and linear optics only. We show that it is fair and balanced even when threshold single-photon detectors are used, and reaches a bias as low as $\epsilon = 1/\sqrt{2} - 1/2 \approx 0.207$. We further show that the protocol may display a quantum advantage over a few-hundred meters with state-of-the-art technology.

DOI: 10.1103/PhysRevA.102.022414

I. INTRODUCTION

Modern communication networks are continuously expanding, as the number of users and available online resources increases. On a daily basis, users must inevitably trust local network nodes and transmission channels in order to perform sensitive tasks such as private data transmission, online banking, electronic voting, delegated computing, and many more. A complex network can be secured by relying on a collection of simpler cryptographic *primitives*, or building blocks, which are combined to guarantee overall security. Strong coin flipping (SCF) is one of such primitives, in which two parties remotely agree on a random bit such that none of the parties can bias the outcome with probability higher than $1/2+\epsilon$, where ϵ is the protocol bias. SCF is fundamental in multiparty computation [1], online gaming, and more general randomized consensus protocols involving leader election [2].

Weak coin flipping (WCF) is a version of coin flipping in which both parties have a preferred, opposite outcome: it effectively designates a winner and a loser. In the classical world, information-theoretically secure SCF and WCF are impossible: they require computational assumptions or trusting a third party [3–6]. Using quantum properties, on the other hand, enables information-theoretically secure SCF and WCF: the lowest possible bias for quantum SCF is $\epsilon = 1/\sqrt{2} - 1/2$ [7], while quantum WCF may achieve a bias arbitrarily close to zero [8,9]. Remarkably, quantum WCF is also involved in the construction of optimal quantum SCF and quantum bit commitment schemes [10,11]. Although the works from [8,9] proved the existence of quantum WCF protocols achieving arbitrarily low biases, no explicit protocol was provided. In 2002, two explicit protocols with small biases were proposed: the work from [12] achieved $\epsilon \approx 0.239$, while [13] achieved $\epsilon = 1/\sqrt{2} - 1/2 \approx 0.207$, which is, incidentally, the SCF lower bound. Later, it was shown that the scheme from [13], in fact, belonged to a larger family of WCF protocols with $\epsilon = 1/6 \approx 0.167$ [14,15]. Very recently, a new explicit family of protocols achieved $\epsilon \approx 1/10$ [16], followed by arbitrarily low biases [17].

While quantum SCF protocols have been experimentally demonstrated [18–20], no implementation has been proposed for quantum WCF. This may be explained by two reasons. First, it is difficult to find an encoding and implementation which is robust to losses: a dishonest party may always declare an abort when they are not satisfied with the flip's outcome. Second, none of the previously mentioned protocols translate trivially into a simple experiment: they involve performing single-shot generalized measurements [13] or generating beyond-qubit states [12].

In this work, we introduce a family of quantum WCF protocols, inspired by [13], which achieve biases as low as $\epsilon = 1/\sqrt{2} - 1/2 \approx 0.207$. These protocols involve simple projective measurements instead of generalized ones, require a single photon and linear optics only, and need, at most, three rounds of communication between the parties. The information is encoded by mixing the single photon with vacuum on an unbalanced beam splitter, which generates entanglement between the photon number modes [21]: both parties may then agree on a random bit, while the entanglement is simultaneously verified. We also use a version of our schemes to construct a quantum SCF protocol with bias ≈ 0.31. We further derive a practical security proof for both number-resolving and threshold single-photon detectors, considering the extension to infinite Hilbert spaces. Since the presence of losses may enable classical protocols to reach lower cheating

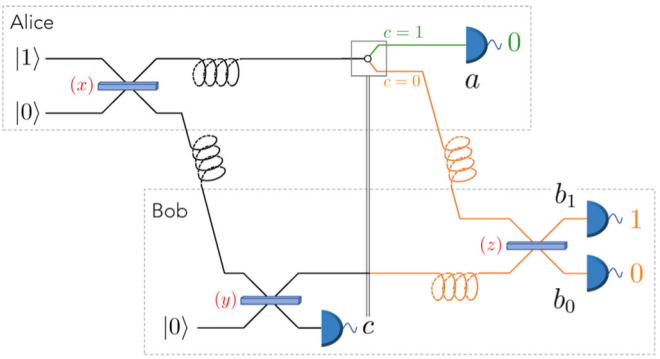

FIG. 1. Representation of the honest protocol. The dashed boxes indicate Alice and Bob's laboratories, respectively. The beam-splitter reflectivities are indicated in red brackets. $|0\rangle$ and $|1\rangle$ are the vacuum and single-photon Fock states, respectively. Curly lines represent the fiber used for quantum communication from Alice to Bob, or delay lines within Alice's or Bob's laboratory, when waiting for the other party's communication. Bob broadcasts the classical outcome c, which controls an optical switch on Alice's side. The protocol when Bob declares $c = 0/1$ is represented in orange or green. The final outcomes $(a, b_1, b_0) = (0, 1, 0)$ are the expected outcomes when both parties are honest.

probabilities than quantum protocols, we finally show that our fair and balanced quantum protocol bears no classical equivalent over a few-hundred meters of lossy optical fiber and nonunit detection efficiency.

II. PROTOCOL AND CORRECTNESS

In the honest protocol, Alice and Bob wish to toss a fair coin, with *a priori* knowledge that they each favor opposite outcomes. Figure 1 represents the implementation of the honest protocol, which follows five distinct steps. Defining $x \in [0, \frac{1}{2}]$ as a free protocol parameter, these read as follows:

(i) Alice mixes a single photon with the vacuum on a beam splitter of reflectivity x.

(ii) Alice keeps the first spatial mode and directs the second spatial mode to Bob.

(iii) Bob mixes the state he receives with the vacuum on a beam splitter of reflectivity $y = 1 - \frac{1}{2(1-x)}$.

(iv) Bob measures the second register of his state with a single-photon detector and broadcasts the outcome $c \in \{0, 1\}$.

(v) The last step is a verification step, which splits into two cases. If $c = 0$, Alice sends her state to Bob, who mixes it with his state on a beam splitter of reflectivity $z = 2x$. He then measures the two output modes with single-photon detectors. He declares Alice the winner if the outcome $(b_1, b_0) = (1, 0)$ is obtained. If $c = 1$: Bob discards his state, and Alice measures her state with a single-photon detector. She declares Bob the winner if the outcome is $a = 0$.

We show that the protocol is fair, i.e., that the probability of winning for each party is $\frac{1}{2}$ when they are both honest.

Single photons are quantized excitations of the electromagnetic field, which are described by the action of the creation operator onto the vacuum. Beam splitters act linearly on creation operators and leave the vacuum invariant. Hence, the evolution of the quantum state over the three modes up to Bob's measurement reads

$$\begin{aligned} |100\rangle &\underset{(x),12}{\rightarrow} \sqrt{x}\,|100\rangle + \sqrt{1-x}\,|010\rangle \\ &\underset{(y),23}{\rightarrow} \sqrt{x}\,|100\rangle + \sqrt{(1-x)y}\,|010\rangle \\ &\quad + \sqrt{(1-x)(1-y)}\,|001\rangle\,, \end{aligned} \tag{1}$$

where the notation (t), kl indicates the reflectivity of the beam splitter and the corresponding spatial modes. Hence, the probability that Bob obtains outcome $c = 1$ when measuring the third register is $P(1) = (1 - x)(1 - y)$, while the probability of outcome $c = 0$ is $P(0) = 1 - P(1)$. Having set $y = 1 - \frac{1}{2(1-x)}$ ensures $P(0) = P(1) = \frac{1}{2}$. When $c = 1$, the state on modes 1 and 2 is projected onto $|00\rangle$, while $c = 0$ projects the state onto $\sqrt{2x}\,|10\rangle + \sqrt{1-2x}\,|01\rangle$. In the first case, the measurement performed by Alice outputs $a = 0$ with probability 1. In the second case, the measurement performed by Bob after the beam splitter with reflectivity z outputs $(b_1, b_0) = (1, 0)$ with probability 1. Hence, the probability that Alice [Bob] wins is directly given by $P_h^{(A)} = P(0)$ $[P_h^{(B)} = P(1)]$. This shows that the protocol is fair since $P(0) = P(1) = \frac{1}{2}$.

III. SECURITY

We now derive the security of the protocol. Namely, we obtain the probabilities of winning when Bob is dishonest and Alice is honest, and vice versa.

A. Dishonest Bob, Honest Alice

Dishonest Bob should always declare the outcome $c = 1$ in order to maximize his winning probability. The outcome of the coin flip is then confirmed if Alice obtains the outcome $a = 0$ upon verification. Bob thus needs to maximize the probability of the outcome $a = 0$, applying a general quantum operation to his half of the state. However, the probability that the detector clicks is independent of Bob's action. It is given by x, so that Bob's winning probability is upper bounded by $(1 - x)$. This upper bound is reached if Bob discards his half of the state and broadcasts $c = 1$. Then, Bob's optimal cheating probability is $P_d^{(B)} = 1 - x$.

B. Dishonest Alice, Honest Bob

Alice wins when Bob declares $c = 0$ and the outcome of his quantum measurement is $(b_1, b_0) = (1, 0)$. The most general strategy of Dishonest Alice is to send a (mixed) state σ, while Bob performs the rest of the protocol honestly. We find that the security is easily derived if Bob is allowed photon number-resolving detectors (see Appendix B for details of all the proofs). Remarkably, the protocol is still secure even when Bob only uses threshold detectors, which is essential to the practicality of the protocol. Moreover, Alice's optimal cheating probability remains the same in both cases: $P_d^{(A)} = 1 - (1 - y)(1 - z)$, which equals $\frac{1}{2(1-x)}$ for $y = 1 - \frac{1}{2(1-x)}$ and $z = 2x$. In particular, for all values of x, we retrieve the property shared by the protocols of [13]: $P_d^{(A)} P_d^{(B)} = \frac{1}{2}$. The underlying idea in the security analysis for threshold and number-resolving detectors is that Alice must generate

the state which maximizes the overlap with Bob's projectors $|100\rangle\langle 100|$ and $\sum_{n=1}^{\infty}|n00\rangle\langle n00|$, respectively.

Setting $x = 1 - 1/\sqrt{2}$, we obtain a version of the protocol which is balanced, i.e., both players have the same cheating probability $1/\sqrt{2}$. The protocol bias is then $\epsilon = 1/\sqrt{2} - 1/2 \approx 0.207$.

Moreover, following [10], we show in Appendix C that a suitable choice of parameters x, y, z yielding an unbalanced quantum WCF protocol allows one to construct a quantum SCF protocol with bias ≈0.31.

IV. FAULT TOLERANCE

A. Noise

We now investigate how imperfect state generation, nonideal beam splitters, and single-photon detector dark counts affect the correctness and security of the protocol. While we fixed the parameter values to $y = 1 - \frac{1}{2(1-x)}$ and $z = 2x$ in the ideal setting, we now allow the three parameters x, y, z to vary freely.

The vacuum and single-photon encoding is very robust to noise, in comparison to polarization or phase encoding for instance: the only property that must be preserved through propagation is the photon number. Alice may simply produce a heralded single photon via spontaneous parametric down-conversion (SPDC) [22], which generates a photon pair: one may be used for the flip, while the other may herald the presence of the first one. Given the photon-pair emission probability p, accidentally emitting two pairs at the same time using SPDC occurs with probability p^2. Since p may be arbitrarily tuned by changing the pump power, p^2—and therefore the probability of two photons being accidentally generated by Alice at once—may then be decreased to negligible values.

Note that in the case where Alice's single-photon source is probabilistic but heralded (as in SPDC), she may always inform Bob of a successful state generation prior to his announcement of c without compromising security. In what follows, we may therefore assume that both parties have agreed on the presence of an initial state, and hence know when the protocol occurs.

Noise will therefore stem from the nonideal reflectivities of the beam splitters, and the nonzero detector dark-count probability p_{dc}. For each party, these may affect the protocol correctness in two ways: an undesired bias of the flip and an added abort probability during the verification process.

Deviations on the beam-splitter reflectivities x, y, and z will first change the honest winning probabilities: these may be recalculated by replacing the ideal reflectivity $r \in \{x, y\}$ with an imperfect r'. Regarding honest aborts, a beam splitter with reflectivity z' instead of z may be applied on the resulting state when $c = 0$. Noisy detectors may cause an unwanted abort corresponding to a click because of dark counts. However, with superconducting nanowire single-photon detectors, this probability is typically very low, of the order of $p_{dc} < 10^{-8}$ [23].

We can therefore conclude that any source of noise may be incorporated in the security analysis by simply replacing parameters x, y, and z with x', y', and z'. Furthermore, this source of error will most likely be negligible with current technology. We therefore solely focus on the more consequential effects of losses.

B. Losses

Losses can be due to nonunit channel and delay line transmissions, as well as nonunit detection efficiency. We label η_t the transmission efficiency of the quantum channel from Alice to Bob. We also define as $\eta_f^{(i)}$ the transmission of party i's fiber delay, while $\eta_d^{(i)}$ denotes the detection efficiency of party i's single-photon detectors. Here, we assume the efficiencies of Bob's detectors to be the same, and that each party introduces a fiber delay whenever they are waiting for the other party's communication. The delay time, therefore, depends on the distance between the two parties.

In the presence of losses, the protocol may also abort when both parties are honest, when the photon is lost. We derive, in Appendix D, the expressions for the two honest winning probabilities $P_h^{(A)}$ and $P_h^{(B)}$, and hence the probability P_{ab} of abort, in the presence of losses:

$$\begin{aligned} P_h^{(A)} &= \eta_t \eta_d^{(B)} \left(\sqrt{xz\eta_f^{(A)}} + \sqrt{(1-x)y(1-z)\eta_f^{(B)}}\right)^2, \\ P_h^{(B)} &= \eta_t \eta_d^{(B)} (1-x)(1-y), \\ P_{ab} &= 1 - P_h^{(A)} - P_h^{(B)}. \end{aligned} \tag{2}$$

Note that the overall correctness does not depend on Alice's detection efficiency $\eta_d^{(A)}$ since the declaration of outcome c depends solely on Bob's detector, and the verification step on Alice's side involves detecting the vacuum.

V. SECURITY IN THE PRESENCE OF LOSSES

Dishonest Bob's best strategy is to perform the same attack as in the lossless case because he has no control over Alice's half of the subsystem. His winning probability is then $P_d^{(B)} = 1 - x\eta_f^{(A)}\eta_d^{(A)}$. However, in a more general game-theoretic scenario, Bob's best strategy will, in fact, depend on the rewards and sanctions associated with honest aborts and "getting caught cheating" aborts. In other words, Bob has to minimize his risk-to-reward ratio. Maximizing his winning probability makes him run the risk of getting caught cheating with probability $x\eta_f^{(A)}\eta_d^{(A)}$.

Dishonest Alice must still generate the state which maximizes the $(b_1, b_0, c) = (1, 0, 0)$ outcome on Bob's detectors after his honest transformations have been applied. However, the expression for Bob's corresponding projector now changes, as there is a finite probability $(1 - \eta_d^{(B)})^n$ that the n-photon component is projected onto the vacuum. The 0 outcome on one spatial mode is therefore triggered by the projection $\Pi_0 = \sum_{n=0}^{\infty}(1 - \eta_d^{(B)})^n |n\rangle\langle n|$. The total projector responsible for the $(b_1, b_0, c) = (1, 0, 0)$ outcome then reads $\Pi_{100} = (\mathbb{1} - \Pi_0) \otimes \Pi_0 \otimes \Pi_0$. We show in Appendix E that Dishonest Alice's maximum winning probability $P_d^{(A)}$ satisfies

$$\begin{aligned} &\max_{l>0} \left\{ \left[1 - \left(1 - y\eta_f^{(B)}\right)(1-z)\eta_d^{(B)}\right]^l - \left(1 - \eta_d^{(B)}\right)^l \right\} \\ &\quad \leqslant 1 - (1-y)(1-z). \end{aligned} \tag{3}$$

The value of the upper bound on the right-hand side is Alice's cheating probability in the lossless case. This shows

that Alice cannot take advantage of Bob's imperfect detectors or his lossy delay line in order to increase her cheating probability. We now provide a sketch of the proof: since passive linear optical elements act linearly on creation operators, equal losses on different modes may be commuted through the interferometer of the protocol. This allows one to upper bound Alice's maximum winning probability by her winning probability in an equivalent picture in which the losses happen just after her state preparation, then followed by a lossless protocol. In that case, it is as if Dishonest Alice was trying to cheat in the lossless protocol, while being restricted to lossy state preparation instead of ideal state preparation.

VI. PRACTICAL PROTOCOL PERFORMANCE

We now analyze the performance of our protocol in a practical setting, by enforcing three conditions on the free parameters: the protocol must be fair, balanced, and perform strictly better than any classical protocol. The latter condition is not required in an ideal implementation since quantum WCF always provides a security advantage over classical WCF. Allowing for abort cases, however, may enable some classical protocols to perform better than quantum ones. This is because increasing the abort probability effectively decreases Alice and Bob's cheating probabilities. We say that the protocol allows for quantum advantage when it provides a strictly lower cheating probability than any classical protocol with the same abort probability. This is obtained using the bounds from [24], which yield the best classical cheating probability $P_d^C = 1 - \sqrt{P_{ab}}$ for our protocol (see Appendix F). The three conditions may then be translated into the following system of equations, where we define $P_d^Q = P_d^{(A)} = P_d^{(B)}$:

$$\begin{aligned} &(i) \quad P_h^{(A)} = P_h^{(B)} \quad \text{fairness} \\ &(ii) \quad P_d^{(A)} = P_d^{(B)} \quad \text{balance} \\ &(iii) \quad P_d^Q < P_d^C \quad \text{quantum advantage.} \end{aligned} \tag{4}$$

Figure 2 shows a choice of parameters for which system (4) is satisfied, up to a distance of d km.

VII. DISCUSSION

By noticing a nontrivial connection between the early protocol from [13] and linear optical transformations, we answer the question of the implementability of quantum weak coin flipping, and show that it is achievable with current technology over a few-hundred meters. Both parties require a set of beam splitters and single-photon threshold detectors. State generation on Alice's side can be performed with any heralded probabilistic single-photon source. Only Alice requires an optical switch, which is commercially available. Although short-term quantum storage is needed, a spool of optical fiber with twice the length of the quantum channel suffices, and provides the required storage and retrieval efficiency.

As the distance increases, the issue of interferometric stability should also be considered. Prior to the protocol, Alice and Bob may use similar techniques to twin-field quantum key distribution implementations to lock the interference [25,26], as it is in their interest to collaborate on this task to avoid the protocol from aborting.

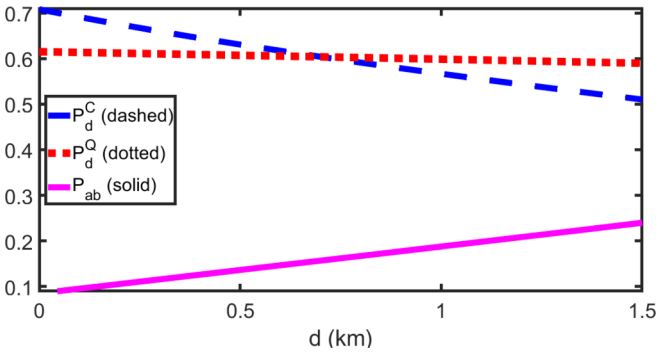

FIG. 2. Practical quantum advantage for a fair and balanced protocol. Numerical values for the lowest classical and quantum cheating probabilities, P_d^C and P_d^Q, are plotted as a function of distance d in dashed blue and dotted red lines, respectively. Honest abort probability P_{ab} (responsible for P_d^Q being lower than our ideal quantum cheating probability $1/\sqrt{2}$) is plotted as a solid magenta line. Our quantum protocol performs strictly better than any classical protocol when $P_d^Q < P_d^C$. We set $\eta_f = \eta_s \eta_t^2$, where η_s is the fiber delay transmission corresponding to 500 ns of optical switching time, and $\eta_t^2 = (10^{-\frac{0.2}{10}d})^2$ is the fiber delay transmission associated with traveling distance d twice (once for quantum, once for classical) in single-mode fibers with attenuation 0.2 dB/km. We have $\eta_d = 0.95$ and $z = 0.57$. For performance with lower $\eta_d = 0.90$, please see Appendix G.

On the fundamental level, our results also raise the question of a potentially deeper connection between the large family of protocols from [8,14,15]—which achieves biases as low as 1/6—and linear optics. Recalling that the protocol from [13], and hence our protocol, is conjectured to be optimal for this family, its extension to many rounds should be necessary in order to lower the bias. The optimality of the one-round protocol is crucial, as a recent result shows that the WCF bias decreases very inefficiently with the number of rounds [27].

ACKNOWLEDGMENTS

We thank Atul Singh Arora and Simon Neves for useful discussions on quantum weak coin flipping and on experimental requirements for heralded single-photon sources, respectively. We acknowledge the support of the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 820445 (QIA) and the ANR through the ANR-17-CE39-0005 (quBIC) project.

APPENDICES

In the following appendices, we give detailed proofs of the results presented in the main text. Appendix A contains the preliminary technical results. In Appendix B, we provide the security analysis for Dishonest Alice. In Appendix C, we show how an unbalanced version of our WCF protocol may yield a SCF protocol. In Appendix D, we derive the completeness of the protocol in the lossy case, and, in Appendix E, we extend the security analysis to the case of a lossy protocol. In Appendix F, we solve the system in Eq. (4) of the main text and derive the constraints that the parameters of the protocol must satisfy in order to obtain a fair and balanced protocol

which still outperforms all classical WCF protocols in the lossy case. Finally, in Appendix G, we display the practical performance of our fair and balanced protocol for various detection efficiencies.

APPENDIX A: PRELIMINARY RESULTS

Single photons are obtained by the action of the creation operator onto the vacuum. Beam splitters act linearly on creation operators, and leave the vacuum invariant. More precisely, a beam splitter of reflectivity t acting on modes k, l maps the creation operators $\hat{a}_k^\dagger, \hat{a}_l^\dagger$ onto $\hat{b}_k^\dagger, \hat{b}_l^\dagger$, where

$$\begin{pmatrix} \hat{b}_k^\dagger \\ \hat{b}_l^\dagger \end{pmatrix} = H_{kl}^{(t)} \begin{pmatrix} \hat{a}_k^\dagger \\ \hat{a}_l^\dagger \end{pmatrix}, \tag{A1}$$

and where

$$H_{kl}^{(r)} = \begin{pmatrix} \sqrt{r} & \sqrt{1-r} \\ \sqrt{1-r} & -\sqrt{r} \end{pmatrix}. \tag{A2}$$

In the following, we make use of a simple reduction which allows one to simplify calculations in the proofs:

Lemma 1. Let $U = (H^{(z)} \otimes \mathbb{1})(\mathbb{1} \otimes H^{(y)})$, with $z > 0$. For all density matrices τ,

$$\begin{aligned} &\mathrm{Tr}[(\tau \otimes |0\rangle\langle 0|)U^\dagger(\mathbb{1} \otimes |00\rangle\langle 00|)U] \\ &\quad = \mathrm{Tr}[(\tau \otimes |0\rangle\langle 0|)V^\dagger(|0\rangle\langle 0| \otimes \mathbb{1} \otimes |0\rangle\langle 0|)V], \end{aligned} \tag{A3}$$

where $V = (\mathbb{1} \otimes H^{(b)})(H^{(a)} \otimes \mathbb{1})[\mathbb{1} \otimes R(\pi) \otimes \mathbb{1}]$, with $a = \frac{y(1-z)}{1-(1-y)(1-z)}$ and $b = 1-(1-y)(1-z)$, and $R(\pi)$ a phase shift of π acting on mode 2.

Proof. The action of U on the creation operators is given by

$$\begin{aligned} U &= \begin{pmatrix} \sqrt{z} & \sqrt{1-z} & 0 \\ \sqrt{1-z} & -\sqrt{z} & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{y} & \sqrt{1-y} \\ 0 & \sqrt{1-y} & -\sqrt{y} \end{pmatrix} \\ &= \begin{pmatrix} \sqrt{z} & \sqrt{y(1-z)} & \sqrt{(1-y)(1-z)} \\ \sqrt{1-z} & -\sqrt{yz} & -\sqrt{(1-y)z} \\ 0 & \sqrt{1-y} & -\sqrt{y} \end{pmatrix}. \end{aligned} \tag{A4}$$

Linear interferometers map product coherent states onto product coherent states, and, for all $\alpha \in \mathbb{C}$, we have that $U^\dagger |\alpha 00\rangle = |\beta_1\beta_2\beta_3\rangle$, where

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix} = \begin{pmatrix} \alpha\sqrt{z} \\ \alpha\sqrt{y(1-z)} \\ \alpha\sqrt{(1-y)(1-z)} \end{pmatrix}. \tag{A5}$$

We have $V = (\mathbb{1} \otimes H^{(b)})(H^{(a)} \otimes \mathbb{1})[\mathbb{1} \otimes R(\pi) \otimes \mathbb{1}]$, with $a, b \in [0, 1]$, and $R(\pi)$ a phase shift of π acting on mode 2. The action of V on the creation operators is given by

$$\begin{aligned} V &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{b} & \sqrt{1-b} \\ 0 & \sqrt{1-b} & -\sqrt{b} \end{pmatrix} \begin{pmatrix} \sqrt{a} & \sqrt{1-a} & 0 \\ \sqrt{1-a} & -\sqrt{a} & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &\quad \times \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} \sqrt{a} & -\sqrt{1-a} & 0 \\ \sqrt{b(1-a)} & \sqrt{ab} & \sqrt{1-b} \\ \sqrt{(1-a)(1-b)} & \sqrt{a(1-b)} & -\sqrt{b} \end{pmatrix}. \end{aligned} \tag{A6}$$

For all $\alpha \in \mathbb{C}$, $V^\dagger |0\alpha 0\rangle = |\gamma_1\gamma_2\gamma_3\rangle$, where

$$\begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \gamma_3 \end{pmatrix} = \begin{pmatrix} \alpha\sqrt{b(1-a)} \\ \alpha\sqrt{ab} \\ \alpha\sqrt{1-b} \end{pmatrix}. \tag{A7}$$

Since $a = \frac{y(1-z)}{1-(1-y)(1-z)}$ and $b = 1-(1-y)(1-z)$, we have $b(1-a) = z$, $ab = y(1-z)$, and $1-b = (1-y)(1-z)$, so $(\beta_1, \beta_2, \beta_3) = (\gamma_1, \gamma_2, \gamma_3)$. Then,

$$\begin{aligned} &\mathrm{Tr}[(\tau \otimes |0\rangle\langle 0|)U^\dagger(\mathbb{1} \otimes |00\rangle\langle 00|)U] \\ &\quad = \frac{1}{\pi}\int_{\mathbb{C}} d^2\alpha \mathrm{Tr}[(\tau \otimes |0\rangle\langle 0|)U^\dagger |\alpha 00\rangle\langle \alpha 00| U] \\ &\quad = \frac{1}{\pi}\int_{\mathbb{C}} d^2\alpha \mathrm{Tr}[(\tau \otimes |0\rangle\langle 0|)V^\dagger |0\alpha 0\rangle\langle 0\alpha 0| V] \\ &\quad = \mathrm{Tr}[(\tau \otimes |0\rangle\langle 0|)V^\dagger(|0\rangle\langle 0| \otimes \mathbb{1} \otimes |0\rangle\langle 0|)V], \end{aligned} \tag{A8}$$

where we used the completeness relation of coherent states $\mathbb{1} = \frac{1}{\pi}\int_{\mathbb{C}} |\alpha\rangle\langle\alpha| d^2\alpha$. ■

We also recall a useful simple property, which we will use extensively in the following:

Lemma 2. Equal losses on various modes can be commuted through passive linear optical elements acting on these modes.

This result was proven, e.g., in [28], and we give here a quick proof for completeness.

Proof. One way to prove this statement is to use the fact that any interferometer may be decomposed as beam splitters and phase shifters [29]. Then, losses trivially commute with phase shifters and are easily shown to commute with beam splitters. Indeed, consider a beam splitter of reflectivity t acting on modes 1 and 2. Its action on the creation operators of the modes is given by

$$\hat{a}_1^\dagger, \hat{a}_2^\dagger \to \sqrt{t}\hat{a}_1^\dagger + \sqrt{1-t}\hat{a}_2^\dagger, \sqrt{1-t}\hat{a}_1^\dagger - \sqrt{t}\hat{a}_2^\dagger, \tag{A9}$$

while equal losses η on both modes act as

$$\hat{a}_1^\dagger, \hat{a}_2^\dagger \to \sqrt{\eta}\hat{a}_1^\dagger, \sqrt{\eta}\hat{a}_2^\dagger. \tag{A10}$$

Hence, the action of the beam splitter followed by losses is given by

$$\hat{a}_1^\dagger, \hat{a}_2^\dagger \to \sqrt{\eta}(\sqrt{t}\hat{a}_1^\dagger + \sqrt{1-t}\hat{a}_2^\dagger), \sqrt{\eta}(\sqrt{1-t}\hat{a}_1^\dagger - \sqrt{t}\hat{a}_2^\dagger), \tag{A11}$$

while losses followed by the beam splitter act as

$$\begin{aligned} \hat{a}_1^\dagger, \hat{a}_2^\dagger \to \sqrt{t}(\sqrt{\eta}\hat{a}_1^\dagger) + \sqrt{1-t}(\sqrt{\eta}\hat{a}_2^\dagger), \\ \sqrt{1-t}(\sqrt{\eta}\hat{a}_1^\dagger) - \sqrt{t}(\sqrt{\eta}\hat{a}_2^\dagger), \end{aligned} \tag{A12}$$

which is equal to the previous evolution. ■

In what follows, we let the parameters x, y, z vary freely and derive the relation these parameters need to satisfy to enforce a honest protocol without abort cases. As presented in the main text, when both parties are honest (Fig. 1), the evolution of the quantum state over the three modes up to

Bob's first measurement reads

$$\begin{aligned}|100\rangle &\underset{(x),12}{\rightarrow} \sqrt{x}\,|100\rangle + \sqrt{1-x}\,|010\rangle \\ &\underset{(y),23}{\rightarrow} \sqrt{x}\,|100\rangle + \sqrt{(1-x)y}\,|010\rangle \\ &\quad + \sqrt{(1-x)(1-y)}\,|001\rangle\,, \end{aligned} \tag{A13}$$

where the notation (t), kl indicates the reflectivity of the beam splitter and the corresponding spatial modes. Hence, the probability that Bob obtains outcome $c = 1$ when measuring the third register is $P(1) = (1-x)(1-y)$, while the probability of outcome $c = 0$ is $P(0) = 1 - P(1)$.

If Bob registers the outcome $c = 1$, then the postmeasurement state on Alice's side is $|0\rangle$, which will always pass the verification step.

If Bob registers the outcome $c = 0$, then the postmeasurement state reads

$$\sqrt{\frac{x}{1-(1-x)(1-y)}}\,|10\rangle + \sqrt{\frac{(1-x)y}{1-(1-x)(1-y)}}\,|01\rangle\,. \tag{A14}$$

The value of the parameter z should be fixed to

$$z = \frac{x}{1-(1-x)(1-y)}, \tag{A15}$$

so that this state passes the verification step and the protocol does not abort in the honest case. We assume this relation holds in the following. In that case, the winning probabilities of Alice and Bob in the honest case are given by

$$\begin{aligned} P_h^{(A)} &= 1-(1-x)(1-y), \\ P_h^{(B)} &= (1-x)(1-y). \end{aligned} \tag{A16}$$

The protocol is fair when $(1-x)(1-y) = \frac{1}{2}$. In that case, $y = 1 - \frac{1}{2(1-x)}$ and $z = 2x$.

Let us also recall from the main text that in the general case, the winning probability of Dishonest Bob is given by

$$P_d^{(B)} = 1 - x. \tag{A17}$$

APPENDIX B: SECURITY ANALYSIS FOR DISHONEST ALICE WITHOUT LOSSES

1. Bob has number-resolving detectors

When using number-resolving single-photon detectors, any projection onto the $n > 1$ photon subspace leads to Alice getting caught cheating. Alice must therefore maximize the overlap with the projective measurement $|100\rangle\langle 100|$ only (Fig. 3).

Let σ be the state sent by Alice. Let $U = (H^{(z)} \otimes \mathbb{1})(\mathbb{1} \otimes H^{(y)})$, with $z = \frac{x}{1-(1-x)(1-y)}$. Alice needs to maximize the probability of the overall outcome $(b_1, b_0, c) = (1, 0, 0)$, which is given by

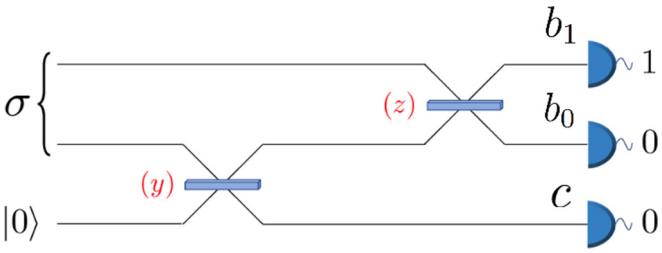

FIG. 3. Dishonest Alice. Alice aims to maximize the outcome $(b_1, b_0, c) = (1, 0, 0)$: an outcome 0 on the third mode means that Bob declared Alice the winner, while an outcome (1,0) for modes 1 and 2 means that Alice passed Bob's verification. The reflectivities of the beam splitter are given by $y = 1 - \frac{1}{2(1-x)}$ and $z = 2x$.

$$P_d^{(A)} = \mathrm{Tr}[U(\sigma \otimes |0\rangle\langle 0|)U^\dagger\,|100\rangle\langle 100|], \tag{B1}$$

since Bob uses number-resolving detectors. By convexity of the probabilities, we may assume without loss of generality that Alice sends a pure state $\sigma = |\psi\rangle\langle\psi|$, which allows us to write

$$\begin{aligned} P_d^{(A)} &= \mathrm{Tr}[U(|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0|)U^\dagger\,|100\rangle\langle 100|] \\ &= \mathrm{Tr}[(|\psi\rangle\langle\psi| \otimes |0\rangle\langle 0|)U^\dagger\,|100\rangle\langle 100|\,U] \\ &= \mathrm{Tr}[\langle\psi| \otimes \langle 0|\,U^\dagger\,|100\rangle\langle 100|\,U\,|\psi\rangle \otimes |0\rangle]. \end{aligned} \tag{B2}$$

We have

$$\begin{aligned} U^\dagger\,|100\rangle &= (\mathbb{1} \otimes H^{(y)})(H^{(z)} \otimes \mathbb{1})\,|100\rangle \\ &= (\mathbb{1} \otimes H^{(y)})(\sqrt{z}\,|100\rangle + \sqrt{1-z}\,|010\rangle) \\ &= \sqrt{z}\,|100\rangle + \sqrt{y(1-z)}\,|010\rangle \\ &\quad + \sqrt{(1-y)(1-z)}\,|001\rangle\,, \end{aligned} \tag{B3}$$

and therefore

$$\begin{aligned} U^\dagger|100\rangle\langle 100|U &= z|100\rangle\langle 100| + y(1-z)|010\rangle\langle 010| \\ &\quad + (1-y)(1-z)|001\rangle\langle 001| \\ &\quad + \sqrt{yz(1-z)}(|100\rangle\langle 010| + |010\rangle\langle 100|) \\ &\quad + \sqrt{z(1-y)(1-z)}(|100\rangle\langle 001| + |001\rangle \\ &\quad \times \langle 100|) + (1-z)\sqrt{y(1-y)}(|010\rangle\langle 001| \\ &\quad + |001\rangle\langle 010|). \end{aligned} \tag{B4}$$

Substituting back into Eq. (B2) then reduces to

$$\begin{aligned} P_d^{(A)} &= \langle\psi|[z|10\rangle\langle 10| + y(1-z)|01\rangle\langle 01| + \sqrt{yz(1-z)}(|10\rangle\langle 01| + |01\rangle\langle 10|)]|\psi\rangle \\ &:= \langle\psi|(\sqrt{z}|10\rangle + \sqrt{y(1-z)}|01\rangle)(\sqrt{z}\langle 10| + \sqrt{y(1-z)}\langle 01|)|\psi\rangle \\ &= |\langle\psi|(\sqrt{z}|10\rangle + \sqrt{y(1-z)}|01\rangle)|^2. \end{aligned} \tag{B5}$$

Using the Cauchy-Schwarz inequality then allows one to upper bound $P_d^{(A)}$ as

$$P_d^{(A)} \leqslant \|\psi\|^2 \|(\sqrt{z}|10\rangle + \sqrt{y(1-z)}|01\rangle)\|^2 \leqslant [1-(1-y)(1-z)]\|\psi\|^2, \tag{B6}$$

which is maximized for $\|\psi\| = 1$. Hence, we finally get

$$P_d^{(A)} \leqslant 1-(1-y)(1-z). \tag{B7}$$

In order to find Alice's optimal cheating strategy (i.e., the optimal pure state $|\phi\rangle$ that she must send to achieve this bound), we remark that the unnormalized state $\sqrt{z}|10\rangle + \sqrt{y(1-z)}|01\rangle$ maximizes the expression in Eq. (B6). Normalizing this state then provides Alice's optimal strategy, which is to prepare the state

$$|\phi\rangle := \sqrt{\frac{z}{1-(1-y)(1-z)}}|10\rangle + \sqrt{\frac{y(1-z)}{1-(1-y)(1-z)}}|01\rangle. \tag{B8}$$

Hence,

$$P_d^{(A)} = 1-(1-y)(1-z). \tag{B9}$$

In the case of a fair protocol, $y = 1-\frac{1}{2(1-x)}$ and $z = 2x$, so

$$P_d^{(A)} = \frac{1}{2(1-x)}, \tag{B10}$$

and Alice's optimal strategy is to prepare the state

$$|\phi_x\rangle := 2\sqrt{x(1-x)}|10\rangle + (1-2x)|01\rangle. \tag{B11}$$

2. Bob has threshold detectors

Unlike the previous case, incorrect outcomes with higher photon number could still pass the test: for $n \geqslant 1$, the threshold detectors cannot discriminate between a $|100\rangle$ and $|n00\rangle$ projection. We show in the following that this does not help a Dishonest Alice, and that the strategy described previously for the case of number-resolving detectors is still optimal in the case of threshold detectors.

With the same notations as in the previous proof, Alice needs to maximize the probability of the overall outcome $(b_1, b_0, c) = (1, 0, 0)$, and hence the overlap with the projector $\sum_{n=1}^{\infty}|n00\rangle\langle n00| = (\mathbb{1}-|0\rangle\langle 0|)\otimes|00\rangle\langle 00|$. This allows us to write

$$P_d^{(A)} = \mathrm{Tr}\{U(|\psi\rangle\langle\psi|\otimes|0\rangle\langle 0|)U^\dagger[(\mathbb{1}-|0\rangle\langle 0|)\otimes|00\rangle\langle 00|]\}, \tag{B12}$$

since Bob uses threshold detectors, where $U = (H^{(z)}\otimes\mathbb{1})(\mathbb{1}\otimes H^{(y)})$, with $z = \frac{x}{1-(1-x)(1-y)}$.

Linear optical evolution conserves the photon number. Hence, if Alice sends the vacuum state, the detectors will never click. Removing the two-mode vacuum component of the state prepared by Alice and renormalizing therefore always increases her winning probability. Since we are looking for the maximum winning probability, we can assume, without loss of generality, that $\langle\psi|00\rangle = 0$, i.e.,

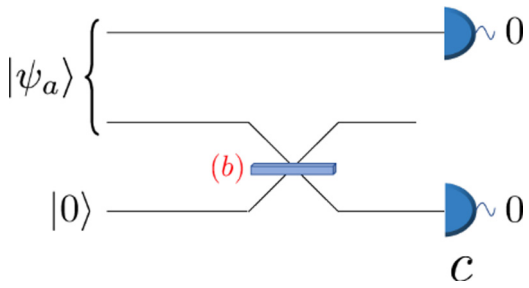

FIG. 4. Equivalent picture for Dishonest Alice. In the original dishonest setup of Fig. 3, Alice aims to maximize the outcome $(b_1, b_0, c) = (1, 0, 0)$. This is equivalent to Alice maximizing outcome 0 on spatial modes 1 and 3, independently of what is detected on mode 2. The outcomes indicated correspond to Alice winning. The reflectivity is $b = 1-(1-y)(1-z)$.

$$\mathrm{Tr}[U(|\psi\rangle\langle\psi|\otimes|0\rangle\langle 0|)U^\dagger|000\rangle\langle 000|] = |\langle\psi|00\rangle|^2. \tag{B13}$$

So maximizing the winning probability in Eq. (B12) is equivalent to maximizing

$$\tilde{P}_d^{(A)} = \mathrm{Tr}[U(|\psi\rangle\langle\psi|\otimes|0\rangle\langle 0|)U^\dagger(\mathbb{1}\otimes|00\rangle\langle 00|)], \tag{B14}$$

given the constraint $\langle\psi|00\rangle = 0$. We have

$$\tilde{P}_d^{(A)} = \mathrm{Tr}[U(|\psi\rangle\langle\psi|\otimes|0\rangle\langle 0|)U^\dagger(\mathbb{1}\otimes|00\rangle\langle 00|)] = \mathrm{Tr}[(|\psi\rangle\langle\psi|\otimes|0\rangle\langle 0|)U^\dagger(\mathbb{1}\otimes|00\rangle\langle 00|)U]. \tag{B15}$$

With Lemma 1 and Eq. (B15), we may thus write

$$\tilde{P}_d^{(A)} = \mathrm{Tr}[(|\psi\rangle\langle\psi|\otimes|0\rangle\langle 0|)V^\dagger(|0\rangle\langle 0|\otimes\mathbb{1}\otimes|0\rangle\langle 0|)V], \tag{B16}$$

where $V = (\mathbb{1}\otimes H^{(b)})(H^{(a)}\otimes\mathbb{1})[\mathbb{1}\otimes R(\pi)\otimes\mathbb{1}]$, with $a = \frac{y(1-z)}{1-(1-y)(1-z)}$ and $b = 1-(1-y)(1-z)$. Let us now define

$$|\psi_a\rangle := H^{(a)}[\mathbb{1}\otimes R(\pi)]|\psi\rangle. \tag{B17}$$

The constraints $\langle\psi|00\rangle = 0$ and $\langle\psi_a|00\rangle = 0$ are equivalent because the above transformation leaves the total number of photons invariant. With Eq. (B16), we obtain

$$\tilde{P}_d^{(A)} = \mathrm{Tr}[(|\psi_a\rangle\langle\psi_a|\otimes|0\rangle\langle 0|)(\mathbb{1}\otimes H^{(b)}) \times (|0\rangle\langle 0|\otimes\mathbb{1}\otimes|0\rangle\langle 0|)(\mathbb{1}\otimes H^{(b)})], \tag{B18}$$

with the constraint $\langle\psi_a|00\rangle = 0$.

Maximizing this expression thus corresponds to maximizing the probability of the outcome (0,0) when measuring modes 1 and 3 of the state obtain by mixing the second half of $|\psi_a\rangle$ with the vacuum on a beam splitter of reflectivity $b = 1-(1-y)(1-z)$ (Fig. 4).

We now show that an optimal strategy for Alice is to ensure that $|\psi_a\rangle = |01\rangle$. Let us write

$$|\psi_a\rangle = \sum_{p+q>0}\psi_{pq}|pq\rangle, \tag{B19}$$

where we take into account the constraint $\langle\psi_x|00\rangle = 0$. Then, with Eq. (B18), we obtain

$$\begin{aligned}\tilde{P}_d^{(A)} &= \sum_{p+q>0,p'+q'>0} \psi_{pq}\psi^*_{p'q'}\mathrm{Tr}\{|pq0\rangle\langle p'q'0|[|0\rangle\langle 0|\otimes H^{(b)}(\mathbb{1}\otimes|0\rangle\langle 0|)H^{(b)}]\}\\ &= \sum_{q>0,q'>0} \psi_{0q}\psi^*_{0q'}\mathrm{Tr}[|q0\rangle\langle q'0|H^{(b)}(\mathbb{1}\otimes|0\rangle\langle 0|)H^{(b)}]\\ &= \sum_{n\geqslant 0,q>0,q'>0} \psi_{0q}\psi^*_{0q'}\mathrm{Tr}[|q0\rangle\langle q'0|H^{(b)}|n0\rangle\langle n0|H^{(b)}]\\ &= \sum_{n>0}|\psi_{0n}|^2|\langle n0|H^{(b)}|n0\rangle|^2\\ &= \sum_{n>0}|\psi_{0n}|^2 b^n,\end{aligned} \tag{B20}$$

where we used, in the fourth line, the fact that $H^{(b)}$ does not change the number of photons. Since $b \in [0, 1]$, this shows that

$$\begin{aligned}\tilde{P}_d^{(A)} &\leqslant b\sum_{n>0}|\psi_{0n}|^2\\ &= b,\end{aligned} \tag{B21}$$

since $|\psi_a\rangle$ is normalized, and this bound is reached for $|\psi_{01}|^2 = 1$, i.e., $|\psi_a\rangle = |01\rangle$. With Eq. (B17), this implies that an optimal strategy for Alice is to prepare the state

$$\begin{aligned}|\psi\rangle &= (\mathbb{1}\otimes R(\pi))H^{(a)}|01\rangle\\ &= \sqrt{1-a}|10\rangle + \sqrt{a}|01\rangle\\ &= \sqrt{\frac{z}{1-(1-y)(1-z)}}|10\rangle\\ &\quad + \sqrt{\frac{y(1-z)}{1-(1-y)(1-z)}}|01\rangle\\ &= |\phi\rangle,\end{aligned} \tag{B22}$$

where $|\phi\rangle$ is the state that Dishonest Alice needs to send to maximize her winning probability when Bob uses number-resolving detectors [Eq. (B8)]. Her winning probability is then

$$P_d^{(A)} = 1-(1-y)(1-z). \tag{B23}$$

We therefore recover the same result as for number-resolving detectors. Once again, if the protocol is fair, then $y = 1 - \frac{1}{2(1-x)}$ and $z = 2x$, so

$$P_d^{(A)} = \frac{1}{2(1-x)}, \tag{B24}$$

and an optimal strategy for Alice is to prepare the state

$$|\phi_x\rangle := 2\sqrt{x(1-x)}|10\rangle + (1-2x)|01\rangle. \tag{B25}$$

APPENDIX C: QUANTUM SCF PROTOCOL

An unbalanced quantum WCF protocol can be turned into a quantum SCF protocol using an additional classical protocol, as described in [10]. In particular, let us consider a WCF protocol such that

$$\begin{aligned}P_h^{(A)} &= p, \quad P_h^{(B)} = 1-p,\\ P_d^{(A)} &= p+\epsilon, \quad P_d^{(B)} = 1-p+\epsilon,\end{aligned} \tag{C1}$$

for $p \in [0, 1]$ and $\epsilon > 0$. Then, the corresponding SCF protocol has bias [10]

$$\max\left[\frac{1}{2}-\frac{1}{2}(p-\epsilon), \frac{1}{2-(p+\epsilon)}-\frac{1}{2}\right]. \tag{C2}$$

For our WCF protocol, we have Eqs. (A16), (A17), and (B23):

$$\begin{aligned}P_h^{(A)} &= 1-(1-x)(1-y),\\ P_h^{(B)} &= (1-x)(1-y),\\ P_d^{(A)} &= 1-(1-y)(1-z),\\ P_d^{(B)} &= 1-x,\end{aligned} \tag{C3}$$

with the constraint $z = \frac{x}{1-(1-x)(1-y)}$ [so that the protocol does not abort in the honest case, Eq. (A15)]. Enforcing the conditions in Eq. (C1) and optimizing over the corresponding SCF bias implies

$$\begin{aligned}x &= \frac{y^2}{(1-y)(1-2y)},\\ z &= \frac{y}{(1-y)^2},\\ 1-\frac{x}{2} &= \frac{1}{2-y-z+yz},\end{aligned} \tag{C4}$$

which in turn give the values

$$x \approx 0.38, \quad y \approx 0.31, \quad z \approx 0.66, \tag{C5}$$

by enforcing $x, y, z \in [0, 1]$, and a bias of ≈ 0.31, which is a lower bias than the best implemented SCF protocol so far [20].

APPENDIX D: CORRECTNESS, WITH LOSSES

We give a representation of the honest protocol with losses in Fig. 5. The efficiency of Alice's and Bob's detectors are

denoted $\eta_d^{(A)}$ and $\eta_d^{(B)}$, respectively. The efficiency of the quantum channel from Alice to Bob is denoted η_t, and $\eta_f^{(A)}$ and $\eta_f^{(B)}$ are the efficiencies of Alice's and Bob's fiber delay lines, respectively.

The honest winning probability for Bob is directly given by his chance of detecting the photon (the photon gets to his detector and does not get lost):

$$P_h^{(B)} = \eta_t \eta_d^{(B)} (1-x)(1-y). \tag{D1}$$

On the other hand, Alice wins if the photon, starting from her first input mode, is detected by Bob in the last step.

The evolution of the creation operator of the first mode during the lossy honest protocol is given by

$$\begin{aligned}
\hat{a}_1^\dagger &\to \sqrt{x}\hat{a}_1^\dagger + \sqrt{1-x}\hat{a}_2^\dagger \\
&\to \sqrt{x\eta_f^{(A)}}\hat{a}_1^\dagger + \sqrt{(1-x)\eta_t}\hat{a}_2^\dagger \\
&\to \sqrt{x\eta_f^{(A)}}\hat{a}_1^\dagger + \sqrt{(1-x)\eta_t y}\hat{a}_2^\dagger + \sqrt{(1-x)(1-y)\eta_t}\hat{a}_3^\dagger \\
&\to \sqrt{x\eta_f^{(A)}}\hat{a}_1^\dagger + \sqrt{(1-x)\eta_t y}\hat{a}_2^\dagger + \sqrt{(1-x)(1-y)\eta_t \eta_d^{(B)}}\hat{a}_3^\dagger \\
&\to \sqrt{x\eta_f^{(A)}\eta_t}\hat{a}_1^\dagger + \sqrt{(1-x)\eta_t y \eta_f^{(B)}}\hat{a}_2^\dagger + \sqrt{(1-x)(1-y)\eta_t \eta_d^{(B)}}\hat{a}_3^\dagger \\
&\to \left(\sqrt{x\eta_f^{(A)}\eta_t z} + \sqrt{(1-x)\eta_t y \eta_f^{(B)}(1-z)}\right)\hat{a}_1^\dagger + \left(\sqrt{x\eta_f^{(A)}\eta_t(1-z)} - \sqrt{(1-x)\eta_t y \eta_f^{(B)} z}\right)\hat{a}_2^\dagger + \sqrt{(1-x)(1-y)\eta_t \eta_d^{(B)}}\hat{a}_3^\dagger \\
&\to \left(\sqrt{x\eta_f^{(A)}\eta_t z \eta_d^{(B)}} + \sqrt{(1-x)\eta_t y \eta_f^{(B)}(1-z)\eta_d^{(B)}}\right)\hat{a}_1^\dagger + \left(\sqrt{x\eta_f^{(A)}\eta_t(1-z)\eta_d^{(B)}} - \sqrt{(1-x)\eta_t y \eta_f^{(B)} z \eta_d^{(B)}}\right)\hat{a}_2^\dagger \\
&\quad + \sqrt{(1-x)(1-y)\eta_t \eta_d^{(B)}}\hat{a}_3^\dagger.
\end{aligned} \tag{D2}$$

In particular, the photon reaches Bob's uppermost detector with probability

$$\begin{aligned}
P_h^{(A)} &= \left(\sqrt{x\eta_f^{(A)}\eta_t z \eta_d^{(B)}} + \sqrt{(1-x)\eta_t y \eta_f^{(B)}(1-z)\eta_d^{(B)}}\right)^2 \\
&= \eta_t \eta_d^{(B)} \left(\sqrt{xz\eta_f^{(A)}} + \sqrt{(1-x)y(1-z)\eta_f^{(B)}}\right)^2.
\end{aligned} \tag{D3}$$

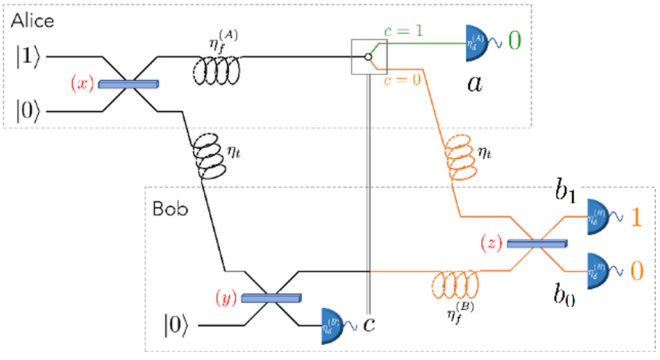

FIG. 5. Representation of the honest protocol with losses. The dashed boxes indicate Alice and Bob's laboratories, respectively. The reflectivity of the beam splitters is indicated in red brackets. The efficiencies of the detectors are indicated in white. Curly lines represent the fiber used for quantum communication from Alice to Bob, or delay lines within Alice's or Bob's laboratory. $|0\rangle$ and $|1\rangle$ are the vacuum and single-photon Fock states, respectively. Bob broadcasts the classical outcome c, which controls an optical switch on Alice's side. The protocol when Bob declares $c = 0/1$ is represented in orange or green. The final outcomes are the expected outcomes when both parties are honest.

Finally, the protocol aborts for all other detection events:

$$P_{ab} = 1 - P_h^{(A)} - P_h^{(B)}. \tag{D4}$$

APPENDIX E: SECURITY ANALYSIS FOR DISHONEST ALICE, WITH LOSSES

The losses η correspond to a probability $1-\eta$ of losing a photon. These can be modeled as a mixing with the vacuum on a beam splitter of reflectivity η. Dishonest Bob wins with probability

$$P_d^{(B)} = 1 - x\eta_f^{(A)}\eta_d^{(A)}, \tag{E1}$$

by performing the same attack as in the lossless case since he has no control over Alice's laboratory. In what follows, we provide the security analysis for Dishonest Alice.

1. Lossy delay line

We show in this section that Alice's maximum winning probability when Bob is using a delay line of efficiency η_f is always lower than when Bob's delay line is perfect, i.e., $\eta_f = 1$, independently of the efficiency η_d of his detectors. The lossy delay line of efficiency η_f may be modeled as a mixing with the vacuum on a beam splitter of transmission η_f.

Alice prepares a state σ, which goes through the interferometer depicted in Fig. 6, and wins if the measurement outcome obtained by Bob is $(b_1, b_0, c) = (1, 0, 0)$. In particular, note that the outcome 0 must be obtained for the third mode. Hence, Alice's winning probability is always lower than if the

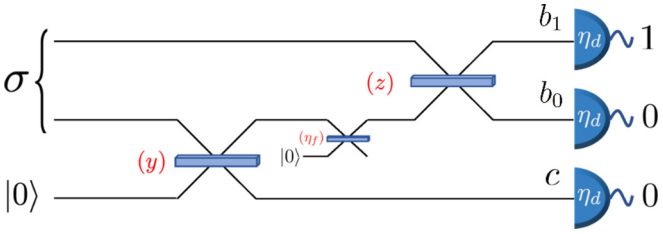

FIG. 6. Alice aims to maximize the outcome $(b_1, b_0, c) = (1, 0, 0)$ by sending the state σ. The lossy delay line is represented by a mixing with the vacuum on a beam splitter of transmission amplitude η_f. The quantum efficiency of the detectors is indicated in white.

third mode was mixed with the vacuum on a beam splitter of transmission amplitude η_f just before the detection (Fig. 7) since this increases the probability of the outcome 0 for this mode. Let us assume that this is the case. Then, by Lemma 2, the losses η_f on output modes 2 and 3 may be commuted back through the beam splitter of reflectivity y, acting on modes 2 and 3.

Since the input state on mode 3 is the vacuum, the losses on this mode may then be removed (Fig. 8). In that case, the probability of winning is clearly lower than when the delay line is perfect (Fig. 9) because Alice is now restricted to lossy state preparation instead of ideal state preparation.

This reduction shows that Alice's maximum winning probability when Bob is using a lossy delay line is always lower than when Bob's delay line is perfect, independently of the efficiency η_d of his detectors.

Moreover, Alice's maximum cheating probability and optimal cheating strategy may be inferred from the case where Bob has a perfect delay line, as we show in what follows. By convexity of the probabilities, Alice's best strategy is to send a pure state, $|\psi\rangle = \sum_{k,l\geqslant 0} \psi_{kl}|kl\rangle$. Let us denote by W the interferometer depicted in Fig. 6, including the detection losses. Let us consider the evolution of Alice's state and the vacuum on the third input mode through the interferometer W. The creation operator for the first mode evolves as

$$\begin{aligned}\hat{a}_1^\dagger &\to \sqrt{z}\hat{a}_1^\dagger + \sqrt{1-z}\hat{a}_2^\dagger \\ &\to \sqrt{z\eta_d}\hat{a}_1^\dagger + \sqrt{(1-z)\eta_d}\hat{a}_2^\dagger \\ &= W\hat{a}_1^\dagger W^\dagger, \end{aligned} \tag{E2}$$

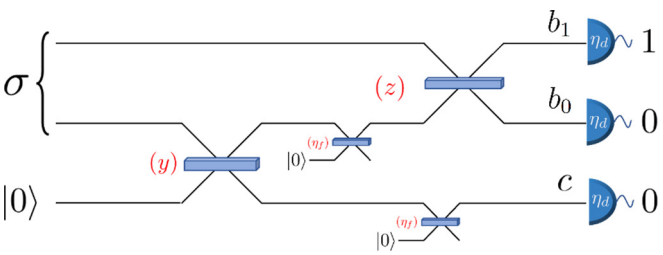

FIG. 7. Adding losses on the third mode increases Alice's winning probability.

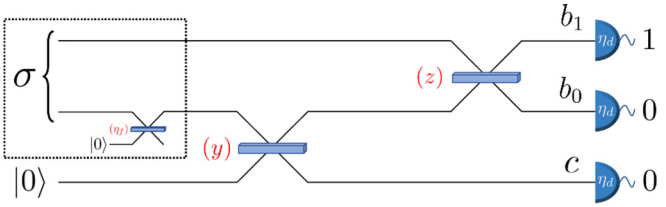

FIG. 8. The losses η_f are commuted back to Alice's state preparation. The losses on input mode 3 can be omitted since the input state is the vacuum.

while the creation operator for the second mode evolves as

$$\begin{aligned}\hat{a}_2^\dagger &\to \sqrt{y}\hat{a}_2^\dagger + \sqrt{1-y}\hat{a}_3^\dagger \\ &\to \sqrt{y\eta_f}\hat{a}_2^\dagger + \sqrt{1-y}\hat{a}_3^\dagger \\ &\to \sqrt{y(1-z)\eta_f}\hat{a}_1^\dagger - \sqrt{yz\eta_f}\hat{a}_2^\dagger + \sqrt{1-y}\hat{a}_3^\dagger \\ &\to \sqrt{y(1-z)\eta_f\eta_d}\hat{a}_1^\dagger - \sqrt{yz\eta_f\eta_d}\hat{a}_2^\dagger + \sqrt{(1-y)\eta_d}\hat{a}_3^\dagger \\ &= W\hat{a}_2^\dagger W^\dagger. \end{aligned} \tag{E3}$$

Hence, the output state (before the ideal threshold detection) is given by

$$\begin{aligned} W|\psi 0\rangle &= W\sum_{k,l\geqslant 0}\psi_{kl}|kl0\rangle \\ &= W\left[\sum_{k,l\geqslant 0}\frac{\psi_{kl}}{\sqrt{k!l!}}(\hat{a}_1^\dagger)^k(\hat{a}_2^\dagger)^l\right]|000\rangle \\ &= \left[\sum_{k,l\geqslant 0}\frac{\psi_{kl}}{\sqrt{k!l!}}(W\hat{a}_1^\dagger W^\dagger)^k(W\hat{a}_2^\dagger W^\dagger)^l\right]|000\rangle \\ &= \sum_{k,l\geqslant 0}\frac{\psi_{kl}}{\sqrt{k!l!}}\left[\sqrt{z\eta_d}\hat{a}_1^\dagger + \sqrt{(1-z)\eta_d}\hat{a}_2^\dagger\right]^k \\ &\quad\times\left[\sqrt{y(1-z)\eta_f\eta_d}\hat{a}_1^\dagger - \sqrt{yz\eta_f\eta_d}\hat{a}_2^\dagger\right. \\ &\quad\left.+\sqrt{(1-y)\eta_d}\hat{a}_3^\dagger\right]^l|000\rangle. \end{aligned} \tag{E4}$$

Now Alice's maximum cheating probability is given by

$$P_d^{(A)} = \mathrm{Tr}[W|\psi 0\rangle\langle\psi 0|W^\dagger(\mathbb{1} - |0\rangle\langle 0|)|00\rangle\langle 00|]. \tag{E5}$$

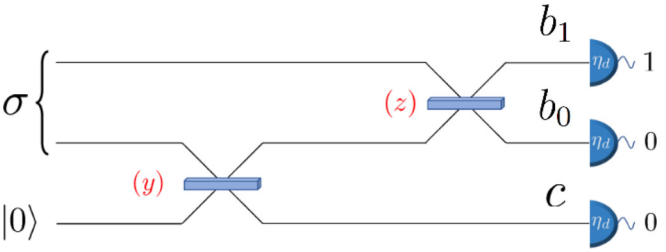

FIG. 9. Alice aims to maximize the outcome $(b_1, b_0, c) = (1, 0, 0)$ by sending the state σ. The delay line efficiency η_f is equal to 1.

Hence, the state after a successful projection $(\mathbb{1} - |0\rangle\langle 0|)|00\rangle\langle 00|$, which has norm $P_d^{(A)}$, reads

$$\left\{\sum_{k+l>0}\frac{\psi_{kl}}{\sqrt{k!l!}}(z\eta_d)^{k/2}[y(1-z)\eta_f\eta_d]^{l/2}(\hat{a}_1^\dagger)^{k+l}\right\}|000\rangle. \quad \text{(E6)}$$

When Bob has a perfect delay line ($\eta_f = 1$), this state reads

$$\left\{\sum_{k+l>0}\frac{\psi_{kl}}{\sqrt{k!l!}}(z\eta_d)^{k/2}[y(1-z)\eta_d]^{l/2}(\hat{a}_1^\dagger)^{k+l}\right\}|000\rangle, \quad \text{(E7)}$$

and its norm is the winning probability of Alice in that case. Hence,

$$P_d^{(A)}[\eta_f, \eta_d, y, z] = P_d^{(A)}[1, \eta_d, y\eta_f, z], \quad \text{(E8)}$$

i.e., we can obtain Alice's cheating probability by solving the case with perfect delay line, and replacing the parameter y by $y\eta_f$. In the following, we thus derive Alice's optimal strategy in that case.

2. Perfect delay line

Let σ be the state sent by Alice, and η_d the detector efficiency. She needs to maximize the probability of the overall outcome $(b_1, b_0, c) = (1, 0, 0)$ at the output of the interferometer depicted in Fig. 10, and hence the overlap with the projector:

$$\Pi_{(1,0,0)}^{\eta_d} = \left[\mathbb{1} - \sum_m (1-\eta_d)^m |m\rangle\langle m|\right] \otimes \left[\sum_{n,p}(1-\eta_d)^{n+p}|n\rangle\langle n| \otimes |p\rangle\langle p|\right]. \quad \text{(E9)}$$

By convexity of the probabilities, we may assume without loss of generality that Alice sends a pure state $\sigma = |\psi\rangle\langle\psi|$. Moreover, the imperfect threshold detectors of quantum efficiency η_d can be modeled by mixing the state to be measured with the vacuum on a beam splitter of transmission amplitude η_d, followed by an ideal threshold detection [30]. In that case, this corresponds to losses η_d on modes 1, 2, and 3, followed by ideal threshold detections. By Lemma 2, commuting the losses back through the interferometer leads to the equivalent picture depicted in Fig. 11, where the losses on input mode 3 have been omitted since the input state is the vacuum.

In that case, Alice's probability of winning is clearly lower than when the threshold detectors are perfect (Fig. 3) because she is restricted to lossy state preparation instead of ideal state preparation. Let $|\tilde{\psi}\rangle$ be the lossy state obtained by applying losses η_d on both modes of Alice's prepared state $|\psi\rangle$. Alice's winning probability may then be written as

$$\begin{aligned} P_d^{(A)} &= \mathrm{Tr}[U(|\tilde{\psi}\rangle\langle\tilde{\psi}| \otimes |0\rangle\langle 0|)U^\dagger(\mathbb{1} - |0\rangle\langle 0|) \otimes |00\rangle\langle 00|] \\ &= \mathrm{Tr}[U(|\tilde{\psi}\rangle\langle\tilde{\psi}| \otimes |0\rangle\langle 0|)U^\dagger(\mathbb{1} \otimes |00\rangle\langle 00|)] - \mathrm{Tr}[U(|\tilde{\psi}\rangle\langle\tilde{\psi}| \otimes |0\rangle\langle 0|)U^\dagger|000\rangle\langle 000|], \end{aligned} \quad \text{(E10)}$$

where $U = (H^{(z)} \otimes \mathbb{1})(\mathbb{1} \otimes H^{(y)})$ is the unitary corresponding to the general interferometer of the lossless protocol. By Lemma 1, we have

$$\mathrm{Tr}[(\tau \otimes |0\rangle\langle 0|)U^\dagger(\mathbb{1} \otimes |00\rangle\langle 00|)U] = \mathrm{Tr}[(\tau \otimes |0\rangle\langle 0|)V^\dagger(|0\rangle\langle 0| \otimes \mathbb{1} \otimes |0\rangle\langle 0|)V], \quad \text{(E11)}$$

for any density matrix τ, where $V = (\mathbb{1} \otimes H^{(b)})(H^{(a)} \otimes \mathbb{1})[\mathbb{1} \otimes R(\pi) \otimes \mathbb{1}]$, with $a = \frac{y(1-z)}{y+z-yz}$ and $b = y + z - yz$, and $R(\pi)$ a phase shift of π acting on mode 2. Hence,

$$P_d^{(A)} = \mathrm{Tr}[V(|\tilde{\psi}\rangle\langle\tilde{\psi}| \otimes |0\rangle\langle 0|)V^\dagger(|0\rangle\langle 0| \otimes \mathbb{1} \otimes |0\rangle\langle 0|)] - \mathrm{Tr}[|\tilde{\psi}\rangle\langle\tilde{\psi}||00\rangle\langle 00|], \quad \text{(E12)}$$

where we used $U^\dagger|000\rangle = |000\rangle$ for the second term. Setting $|\tilde{\psi}_x\rangle = (H^{(a)} \otimes \mathbb{1})[\mathbb{1} \otimes R(\pi)]|\tilde{\psi}\rangle$ yields

$$P_d^{(A)} = \underbrace{\mathrm{Tr}[(|\tilde{\psi}_x\rangle\langle\tilde{\psi}_x| \otimes |0\rangle\langle 0|)(\mathbb{1} \otimes H^{(b)})(|0\rangle\langle 0| \otimes \mathbb{1} \otimes |0\rangle\langle 0|)(\mathbb{1} \otimes H^{(b)})]}_{\equiv P_1} - \underbrace{\mathrm{Tr}[|\tilde{\psi}_x\rangle\langle\tilde{\psi}_x||00\rangle\langle 00|]}_{\equiv P_2}, \quad \text{(E13)}$$

where we used $|00\rangle = [\mathbb{1} \otimes R(\pi)]H^{(a)}|00\rangle$ for the second term P_2.

Let us consider the first term P_1. Since $|\tilde{\psi}\rangle$ is the state obtained by applying losses η_d on both modes of the state $|\psi\rangle$, we obtain the equivalent picture in Fig. 12, where we have added losses η_d also on mode 3 since the input state is the vacuum.

Let $|\psi_x\rangle = H^{(a)}[\mathbb{1} \otimes R(\pi)]|\psi\rangle$. With Lemma 2, commuting the losses η_d to the output of the interferometer in Fig. 12, and combining the losses on mode 2 and 3, yields

$$P_1 = \mathrm{Tr}\left[|\psi_x\rangle\langle\psi_x|\Pi_{(0)}^{\eta_d} \otimes \Pi_{(0)}^{\eta_d(1-b)}\right], \quad \text{(E14)}$$

where $\Pi_{(0)}^{\eta}$ is the positive operator-valued measure (POVM) element corresponding to no click for a threshold detector of quantum efficiency η (recall that this is the same as an ideal detector preceded by a mixing with the vacuum on a beam splitter of transmission amplitude η). The same reasoning for the second term P_2 gives

$$P_2 = \mathrm{Tr}\left[|\psi_x\rangle\langle\psi_x|\Pi_{(0)}^{\eta_d} \otimes \Pi_{(0)}^{\eta_d}\right], \quad \text{(E15)}$$

and we finally obtain, with Eq. (E13),

$$P_d^{(A)} = \mathrm{Tr}\left[|\psi_x\rangle\langle\psi_x|\Pi_{(0)}^{\eta_d} \otimes \left(\Pi_{(0)}^{\eta_d(1-b)} - \Pi_{(0)}^{\eta_d}\right)\right]. \quad \text{(E16)}$$

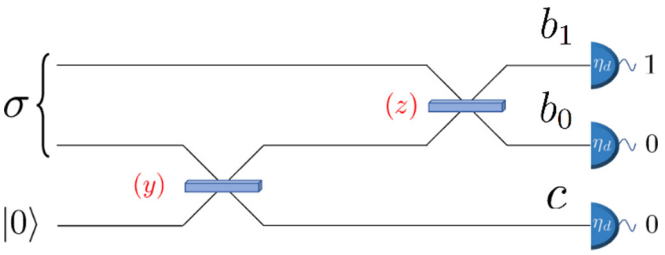

FIG. 10. Alice aims to maximize the outcome $(b_1, b_0, c) = (1, 0, 0)$ by sending the state σ. The quantum efficiency of the detectors is indicated in white.

Let us write $|\psi_x\rangle = \sum_{k,l\geqslant 0}^{+\infty} \psi_{kl}|kl\rangle$. With the expression of the POVM in Eq. (E9), the last equation reads

$$\begin{aligned} P_d^{(A)} &= \sum_{k,l\geqslant 0} |\psi_{kl}|^2 (1-\eta_d)^k \{[1-\eta_d(1-b)]^l - (1-\eta_d)^l\} \\ &\leqslant \max_{k,l\geqslant 0} (1-\eta_d)^k \{[1-\eta_d(1-b)]^l - (1-\eta_d)^l\} \\ &\quad \times \sum_{k,l\geqslant 0} |\psi_{kl}|^2 \\ &= \max_{k,l\geqslant 0} (1-\eta_d)^k \{[1-\eta_d(1-b)]^l - (1-\eta_d)^l\} \\ &= \max_{l\geqslant 1} \{[1-\eta_d(1-b)]^l - (1-\eta_d)^l\} \\ &= \max_{l\geqslant 1} \{[1-\eta_d(1-y)(1-z)]^l - (1-\eta_d)^l\}, \end{aligned} \tag{E17}$$

where we used $b = y + z - yz$. Let $l_0 \in \mathbb{N}^*$ such that $\max_{l\geqslant 1} \{[1-\eta_d(1-b)]^l - (1-\eta_d)^l\} = [1-\eta_d(1-b)]^{l_0} - (1-\eta_d)^{l_0}$. This last expression is an upper bound for $P_d^{(A)}$, which is attained for $\psi_{kl} = \delta_{k,0}\delta_{l,l_0}$, i.e., $|\psi_x\rangle = |0l_0\rangle$. Thus, the best strategy for Alice is to send the state

$$\begin{aligned} |\psi\rangle &= [\mathbb{1} \otimes R(\pi)] H^{(a)} |\psi_x\rangle \\ &= [\mathbb{1} \otimes R(\pi)] H^{(a)} |0l_0\rangle, \end{aligned} \tag{E18}$$

where $a = \frac{y(1-z)}{y+z-yz}$, and her winning probability is then

$$P_d^{(A)} = [1-\eta_d(1-y)(1-z)]^{l_0} - (1-\eta_d)^{l_0}, \tag{E19}$$

when Bob has a perfect delay line. Recalling Eq. (E8), the best strategy for Alice when Bob has a lossy delay line of

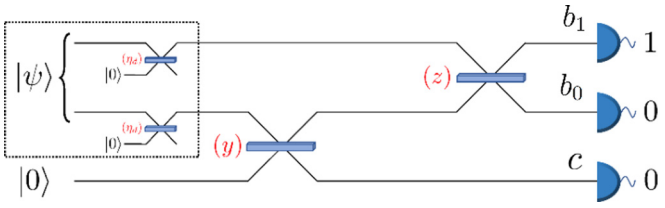

FIG. 11. The quantum efficiency is modeled as losses η_d on modes 1, 2, and 3, which are then commuted through the interferometer, back to Alice's state preparation. The losses on input mode 3 can be omitted since the input state is the vacuum.

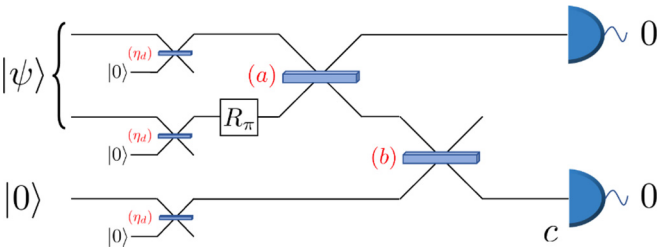

FIG. 12. An equivalent picture for the first term P_1 of Eq. (E13). The term P_1 is the probability of the simultaneous outcomes 0 for modes 1 and 3.

efficiency η_f is to send the state

$$\begin{aligned} |\psi\rangle &= [\mathbb{1} \otimes R(\pi)] H^{(a)} |\psi_x\rangle \\ &= [\mathbb{1} \otimes R(\pi)] H^{(a)} |0l_1\rangle, \end{aligned} \tag{E20}$$

where $a = \frac{y(1-z)\eta_f}{y\eta_f + z - yz\eta_f}$, and $l_1 \in \mathbb{N}^*$ maximizes $[1-\eta_d(1-y\eta_f)(1-z)]^l - (1-\eta_d)^l$. Her winning probability is then

$$\begin{aligned} P_d^{(A)} &= \max_{l>0} \{[1-(1-y\eta_f)(1-z)\eta_d]^l - (1-\eta_d)^l\} \\ &= [1-\eta_d(1-y\eta_f)(1-z)]^{l_1} - (1-\eta_d)^{l_1} \\ &= \eta_d [1-(1-y\eta_f)(1-z)] \sum_{j=0}^{l_1-1} (1-\eta_d)^j \\ &\quad \times [1-\eta_d(1-y\eta_f)(1-z)]^{l_1-j-1} \\ &\leqslant \eta_d [1-(1-y\eta_f)(1-z)] \sum_{j=0}^{l_1-1} (1-\eta_d)^j \\ &= \eta_d [1-(1-y\eta_f)(1-z)] \frac{1-(1-\eta_d)^{l_1}}{1-(1-\eta_d)} \\ &= [1-(1-y\eta_f)(1-z)][1-(1-\eta_d)^{l_1}] \\ &\leqslant 1-(1-y\eta_f)(1-z) \\ &\leqslant 1-(1-y)(1-z), \end{aligned} \tag{E21}$$

and this last expression is the winning probability when there are no losses.

Let us derive the value of l_1. For this, we define

$$\begin{aligned} r &= 1-\eta_d(1-y\eta_f)(1-z), \\ s &= 1-\eta_d. \end{aligned} \tag{E22}$$

We then consider a $\lambda_1 \in \mathbb{R}^{*+}$ which maximizes $(r^\lambda - s^\lambda)$ for $\lambda \in \mathbb{R}^{*+}$. We have

$$\frac{d}{d\lambda_1}(r^{\lambda_1} - s^{\lambda_1}) = 0 \Leftrightarrow \lambda_1 = \frac{\ln\ln s - \ln\ln r}{\ln r - \ln s}, \tag{E23}$$

for strictly nonzero r and s, and where ln denotes the complex logarithm function. This allows one to deduce

$$l_1 = \begin{cases} \text{floor}(\lambda_1) & \text{if} \quad r^{\text{floor}(\lambda_1)} - s^{\text{floor}(\lambda_1)} \geqslant r^{\text{ceil}(\lambda_1)} - s^{\text{ceil}(\lambda_1)} \\ \text{ceil}(\lambda_1) & \text{if} \quad r^{\text{ceil}(\lambda_1)} - s^{\text{ceil}(\lambda_1)} \geqslant r^{\text{floor}(\lambda_1)} - s^{\text{floor}(\lambda_1)}. \end{cases} \tag{E24}$$

APPENDIX F: SOLVING THE SYSTEM FROM EQ. (4)

1. Condition (i)

The first condition enforces a fair protocol, i.e., $P_h^{(A)} = P_h^{(B)}$. With Eqs. (D1) and (D3), we aim to solve for y as a function of x and z:

$$\begin{aligned} (i) &\Leftrightarrow \eta_t \eta_d^{(B)} \Big(\sqrt{xz\eta_f^{(A)}} + \sqrt{(1-x)y(1-z)\eta_f^{(B)}}\Big)^2 = \eta_t \eta_d^{(B)} (1-x)(1-y), \\ (i) &\Leftrightarrow (1-x)\big[(1-z)\eta_f^{(B)} + 1\big]y + 2\sqrt{x(1-x)z(1-z)\eta_f^{(A)}\eta_f^{(B)}}\sqrt{y} + xz\eta_f^{(A)} - (1-x) = 0. \end{aligned} \tag{F1}$$

We make the substitution $Y = \sqrt{y}$ in order to transform Eq. (F1) into a second-order polynomial equation. We then take only the positive solution (since y must be positive), which reads

$$Y = \frac{\sqrt{xz(1-z)\eta_f^{(A)}\eta_f^{(B)} - \big[(1-z)\eta_f^{(B)} + 1\big]\big[xz\eta_f^{(A)} - (1-x)\big]} - \sqrt{xz(1-z)\eta_f^{(A)}\eta_f^{(B)}}}{\sqrt{1-x}\big[(1-z)\eta_f^{(B)} + 1\big]}. \tag{F2}$$

We may finally write

$$(i) \Leftrightarrow \quad y = f\big(x, z, \eta_f^{(i)}, \eta_d, \eta_t\big), \tag{F3}$$

where

$$f\big(x, z, \eta_f^{(i)}, \eta_d, \eta_t\big) = \frac{\Big(\sqrt{(1-x)\big[(1-z)\eta_f^{(B)} + 1\big] - xz\eta_f^{(A)}} - \sqrt{xz(1-z)\eta_f^{(A)}\eta_f^{(B)}}\Big)^2}{(1-x)\big[(1-z)\eta_f^{(B)} + 1\big]^2}.$$

Note that y should be a real number, and hence we require that the expression under the first square root of $f(x, z, \eta_f^{(i)}, \eta_d, \eta_t)$ is positive, i.e.,

$$z \leqslant \frac{(1-x)\big(1+\eta_f^{(B)}\big)}{x\eta_f^{(A)} + (1-x)\eta_f^{(B)}}. \tag{F4}$$

Furthermore, note that for $\eta_f^{(A)} = \eta_f^{(B)} = \eta_f$, y should be an increasing function of η_f, and therefore a decreasing function of d when $\eta_f = 10^{-\frac{0.2}{10}2d}$. Mathematically speaking, this is to prevent $y'(d) \to \infty$ and $y(d) > 1$. Physically speaking, this condition ensures that as the probability of transmitting the photon (and of preserving it for verification) gets smaller, Bob should encourage a detection on the third mode, which evens out the honest probabilities of winning.

2. Condition (ii)

The second condition enforces a balanced protocol, i.e., $P_d^{(A)} = P_d^{(B)}$. With Eqs. (E1) and (E21), this translates into the following expression for x:

$$(ii) \Leftrightarrow x = g\big(y, z, \eta_f^{(i)}, \eta_d^{(i)}\big), \tag{F5}$$

where

$$g\big(y, z, \eta_f^{(i)}, \eta_d^{(i)}\big) = \frac{1}{\eta_f^{(A)}\eta_d^{(A)}}\left(1 - \max_{l \geqslant 1}\left\{\big[1 - \eta_d^{(B)}\big(1 - y\eta_f^{(B)}\big)(1-z)\big]^l - \big(1-\eta_d^{(B)}\big)^l\right\}\right). \tag{F6}$$

3. Condition (iii)

We recall the general coin flipping formalism from [24], in which any classical or quantum coin flipping protocol may be expressed as

$$\text{CF}(p_{00}, p_{11}, p_{*0}, p_{*1}, p_{0*}, p_{1*}), \tag{F7}$$

where p_{ii} is the probability that two honest players output value $i \in \{0, 1\}$, p_{*i} is the probability that Dishonest Alice forces Honest Bob to declare outcome i, and p_{i*} is the probability that Dishonest Bob forces Honest Alice to declare outcome i. In this formalism, a perfect SCF protocol can then be expressed as $\text{CF}(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$, while a perfect WCF may be expressed as $\text{CF}(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, 1, 1, \frac{1}{2})$. We may now express our quantum WCF protocol in the lossless setting as

$$\text{CF}\left(\frac{1}{2}, \frac{1}{2}, \left[\frac{1}{2(1-x)}\right], 1, 1, [1-x]\right). \tag{F8}$$

In the lossy setting, note that the probabilities that Alice and Bob each choose to lose (i.e., p_{*1} and p_{0*}, respectively) both remain 1. When Dishonest Bob chooses to lose, he may always declare outcome 0 regardless of what he detects, which

yields $p_{0*} = 1$. When Dishonest Alice chooses to lose, she may send a state $|n\rangle$ to Bob, and so

$$\begin{aligned} p_{*1} &= \mathrm{Tr}[H^{(y)}|n0\rangle\langle n0|H^{(y)} I \otimes (I - \Pi_0)] \\ &= 1 - \mathrm{Tr}\big[H^{(y)}|n0\rangle\langle n0|H^{(y)}(I \otimes \Pi_0)\big], \end{aligned} \tag{F9}$$

where $\Pi_0 = \sum_{l \geqslant 0}(1-\eta)^l |l\rangle\langle l|$.

Now,

$$\begin{aligned} H^{(y)}|n0\rangle &= H^{(y)} \frac{(\hat{a}_1^\dagger)^n}{\sqrt{n!}}|00\rangle = \frac{1}{\sqrt{n!}}(\sqrt{y}\hat{a}_1^\dagger + \sqrt{1-y}\hat{a}_2^\dagger)^n|00\rangle \\ &= \frac{1}{\sqrt{n!}} \sum_{k=0}^{n} \binom{n}{k} y^{\frac{k}{2}} (1-y)^{\frac{n-k}{2}} \hat{a}_1^{\dagger k} \hat{a}_2^{\dagger (n-k)}|00\rangle = \sum_{k=0}^{n} \sqrt{\binom{n}{k} y^k (1-y)^{n-k}}|k\ (n-k)\rangle. \end{aligned} \tag{F10}$$

We thus obtain, by linearity of the trace,

$$p_{*1} = 1 - \sum_{l,l' \geqslant 0} (1-\eta)^l \sum_{k,k'=0}^{n} \sqrt{\binom{n}{k} y^k (1-y)^{n-k}} \sqrt{\binom{n}{k'} y^{k'} (1-y)^{n-k'}} \mathrm{Tr}[|k\ (n-k)\rangle\langle k'\ (n-k')||l'l\rangle\langle l'l|] \tag{F11}$$

$$\begin{aligned} &= 1 - \sum_{k=0}^{n} (1-\eta)^{n-k} \binom{n}{k} y^k (1-y)^{n-k} \\ &= 1 - [y + (1-\eta)(1-y)]^n, \end{aligned} \tag{F12}$$

which goes to 1 when n goes to infinity, for $y < 1$. Hence, in the lossy setting, the protocol becomes

$$\mathrm{CF}\big(P_h^{(A)}, P_h^{(B)}, P_d^{(A)}, 1, 1, P_d^{(B)}\big), \tag{F13}$$

where $P_d^{(A)} = \max_{l>0}[1 - (1 - y\eta_f^{(A)})(1-z)\eta_d^{(B)}]^l - (1-\eta_d^{(B)})^l$ and $P_d^{(B)} = 1 - x\eta_f^{(A)}\eta_d^{(A)}$.

Using Theorem 1 from [24], there exists a classical protocol that implements an information-theoretically secure coin flip with our parameters if and only if the following conditions hold:

$$\begin{aligned} P_h^{(A)} &\leqslant P_d^{(A)}, \\ P_h^{(B)} &\leqslant P_d^{(B)}, \\ P_{ab} = 1 - P_h^{(A)} - P_h^{(B)} &\geqslant \big(1 - P_d^{(A)}\big)\big(1 - P_d^{(B)}\big). \end{aligned} \tag{F14}$$

Our quantum protocol therefore presents an advantage over classical protocols if at least one of these conditions *cannot* be satisfied. Since we are interested in fair and balanced protocols, setting $P_h = P_h^{(A)} = P_h^{(B)}$ and $P_d = P_d^{(A)} = P_d^{(B)}$ allows one to rewrite (F14) as

$$\begin{aligned} &P_h \leqslant P_d, \\ P_{ab} = 1 - 2P_h \geqslant (1 - P_d)^2 &\Leftrightarrow P_h \leqslant \tfrac{1}{2}[1 - (1 - P_d)^2]. \end{aligned} \tag{F15}$$

Let us finally remark that for all x, we have $\frac{1}{2}[1-(1-x)^2] = x - \frac{x^2}{2} \leqslant x$, so the first inequality above is implied by the second. The system is thus equivalent to the second inequality,

$$P_{ab} = 1 - 2P_h \geqslant (1 - P_d)^2, \tag{F16}$$

provided that $P_h^{(A)} = P_h^{(B)} = P_h$ and $P_d^{(A)} = P_d^{(B)} = P_d$.

In order to get a clearer insight into the meaning of quantum advantage, we express this condition in terms of cheating probability: our protocol displays quantum advantage if and only if the lowest classical cheating probability,

$$P_d^C = 1 - \sqrt{1 - 2P_h} = 1 - \sqrt{P_{ab}}, \tag{F17}$$

exceeds our quantum cheating probability P_d^Q.

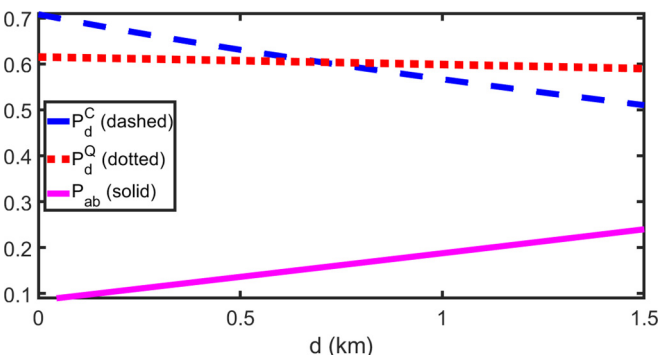

FIG. 13. Parameters $\eta_d = 0.95$ and $z = 0.57$. Note that honest abort probability P_{ab} is plotted as a solid magenta line.

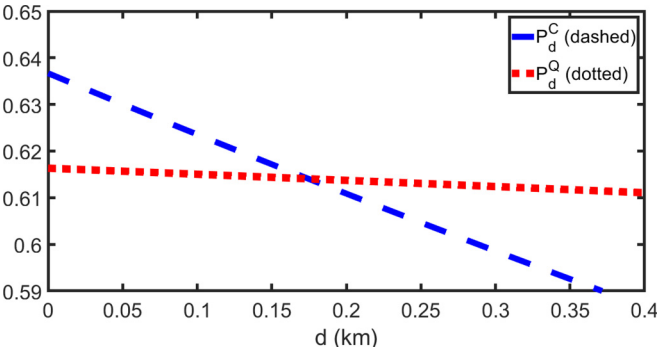

FIG. 14. Parameters $\eta_d = 0.90$ and $z = 0.63$. Note that honest abort probability has been omitted in order to zoom in, but it lies around 0.15 for these distances.

APPENDIX G: PRACTICAL QUANTUM ADVANTAGE FOR VARIOUS DETECTION EFFICIENCIES

In Figs. 13 and 14, we plot the numerical solutions to the system from Eq. (4) in order to display the quantum advantage as a function of distance for various detection efficiencies. Numerical values for the lowest classical and quantum cheating probabilities, P_d^C and P_d^Q, are plotted as a function of distance d in blue and red, respectively. Our quantum protocol performs strictly better than any classical protocol when $P_d^Q < P_d^C$. We set $\eta_f = \eta_s \eta_t^2$, where η_s is the fiber delay transmission corresponding to 500 ns of optical switching time, and $\eta_t^2 = (10^{-\frac{0.2}{10}d})^2$ is the fiber delay transmission associated with traveling distance d twice (once for quantum, once for classical) in single-mode fibers with attenuation 0.2 dB/km.

[1] O. Goldreich, S. Micali, and A. Wigderson, How to play ANY mental game, in *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing (STOC '87)* (Association for Computing Machinery, New York, 1987), pp. 218–229.

[2] D. Alistarh, J. Aspnes, V. King, and J. Saia, Distrib. Comput. **31**, 489 (2018).

[3] M. Blum, SIGACT News **15**, 23 (1983).

[4] R. Cleve, Limits on the security of coin flips when half the processors are faulty, in *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing (STOC '86)* (Association for Computing Machinery, New York, 1986), pp. 364–369.

[5] A. Ambainis, J. Comput. Syst. Sci. **68**, 398 (2004).

[6] G. Berlin, G. Brassard, F. Bussieres, and N. Godbout, Phys. Rev. A **80**, 062321 (2009).

[7] A. Kitaev, Talk at the 6th Workshop on Quantum Information Processing (QIP 2003), MSRI, Berkeley, CA (unpublished).

[8] C. Mochon, arXiv:0711.4114.

[9] D. Aharonov, A. Chailloux, M. Ganz, I. Kerenidis, and L. Magnin, SIAM J. Comput. **45**, 633 (2016).

[10] A. Chailloux and I. Kerenidis, Optimal quantum strong coin flipping, in *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science (FOCS '09), 2009* (IEEE, Piscataway, NJ, 2009), pp. 527–533.

[11] A. Chailloux and I. Kerenidis, Optimal bounds for quantum bit commitment, in *Proceedings of the IEEE 52nd Annual Symposium on Foundations of Computer Science, 2011* (IEEE, Piscataway, NJ, 2011), pp. 354–362.

[12] I. Kerenidis and A. Nayak, Inf. Proc. Lett. **89**, 131 (2004).

[13] R. W. Spekkens and T. Rudolph, Phys. Rev. Lett. **89**, 227901 (2002).

[14] C. Mochon, Quantum weak coin-flipping with bias of 0.192, in *45th Annual IEEE Symposium on Foundations of Computer Science, Rome, Italy, 2004* (IEEE, Piscataway, NJ, 2004), pp. 2–11.

[15] C. Mochon, Phys. Rev. A **72**, 022341 (2005).

[16] A. S. Arora, J. Roland, and S. Weis, Quantum weak coin flipping, in *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing (STOC 2019)* (Association for Computing Machinery, New York, 2019), pp. 205–216.

[17] A. S. Arora, J. Roland, and C. Vlachou, arXiv:1911.13283.

[18] G. Molina-Terriza, A. Vaziri, R. Ursin, and A. Zeilinger, Phys. Rev. Lett. **94**, 040501 (2005).

[19] G. Berlín, G. Brassard, F. Bussières, N. Godbout, J. A. Slater, and W. Tittel, Nat. Commun. **2**, 561 (2011).

[20] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti, Nat. Commun. **5**, 3717 (2014).

[21] O. Morin, J.-D. Bancal, M. Ho, P. Sekatski, V. D'Auria, N. Gisin, J. Laurat, and N. Sangouard, Phys. Rev. Lett. **110**, 130401 (2013).

[22] C. Couteau, Contemp. Phys. **59**, 291 (2018).

[23] R. H. Hadfield, Nat. Photonics **3**, 696 (2009).

[24] E. Hänggi and J. Wullschleger, Tight bounds for classical and quantum coin flipping, in *Theory of Cryptography*, Lecture Notes in Computer Science, Vol. 6597, edited by Y. Ishai (Springer, Berlin, Heidelberg, 2011).

[25] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Nat. Photon. **13**, 334 (2019).

[26] 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, Phys. Rev. Lett. **124**, 070501 (2020)

[27] C. A. Miller, The impossibility of efficient quantum weak coin flipping, in *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing (STOC 2020)* (Association for Computing Machinery, New York, 2020), pp. 916–929.

[28] D. W. Berry and A. I. Lvovsky, Phys. Rev. Lett. **105**, 203601 (2010).

[29] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).

[30] A. Ferraro, S. Olivares, and M. G. Paris, arXiv:quant-ph/0503237.