PHYSICAL REVIEW A **94**, 032315 (2016)

Loss-tolerant quantum secure positioning with weak laser sources

Charles Ci Wen Lim,[1,*] Feihu Xu,[2] George Siopsis,[3] Eric Chitambar,[4] Philip G. Evans,[1] and Bing Qi[1,3]
[1]*Quantum Information Science Group, Computational Sciences and Engineering Division, Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831-6418, USA*
[2]*Research Laboratory of Electronics, Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, Massachusetts 02139, USA*
[3]*Department of Physics and Astronomy, The University of Tennessee, Knoxville, Tennessee 37996-1200, USA*
[4]*Department of Physics and Astronomy, Southern Illinois University, Carbondale, Illinois 62901, USA*
(Received 21 July 2016; published 14 September 2016)

Quantum position verification (QPV) is the art of verifying the geographical location of an untrusted party. Recently, it has been shown that the widely studied Bennett & Brassard 1984 (BB84) QPV protocol is insecure after the 3 dB loss point assuming local operations and classical communication (LOCC) adversaries. Here, we propose a time-reversed entanglement swapping QPV protocol (based on measurement-device-independent quantum cryptography) that is highly robust against quantum channel loss. First, assuming ideal qubit sources, we show that the protocol is secure against LOCC adversaries for any quantum channel loss, thereby overcoming the 3 dB loss limit. Then, we analyze the security of the protocol in a more practical setting involving weak laser sources and linear optics. In this setting, we find that the security only degrades by an additive constant and the protocol is able to verify positions up to 47 dB channel loss.

DOI: 10.1103/PhysRevA.94.032315

I. INTRODUCTION

How can one verify that an untrusted party (someone with no credentials) is indeed at a particular geographical location? In cryptography, this problem is closely related to the task of *position verification*, where a prover P has to convince a set of remote verifiers $V_1, V_2, \ldots,$ that he or she is at a certain geographic position pos^* [1]. At the end of the task, the verifiers either agree or disagree with the prover: agreement means the prover gains a geographical credential, while disagreement means the prover remains with zero credentials. Beyond position verification, such geographical credentials can also be used to build other cryptographic tasks like authentication and key distribution.

In the classical setting, it has been shown that position verification is insecure against unbounded adversaries [1]. This impasse is mainly due to the fact that colluding adversaries can retrieve, store, and share classical challenges with each other. One solution is to adopt the so-called *bounded-retrieval model* and limit the amount of information that an adversary can retrieve from the public channel [1]. However, this model is difficult to justify in practice. Drawing insights from the bounded-retrieval model, researchers proposed quantum position verification (QPV) as a means to achieve information-theoretic security [2–7]. The basic idea is to replace classical challenges with quantum challenges (quantum states) and utilize the *quantum no-cloning principle* to bound the amount of retrievable information. Unfortunately, this intuition is not enough to guarantee unconditional security in the quantum setting, because colluding adversaries can make use of pre-shared entanglement to perform nonlocal computation with one round of classical communication [3,4,6,8–11]. In light of these impossibility results, the most obvious solution is to consider adversaries with no preshared entanglement, a scenario that is known as the NPE model [6]. Assuming perfect channel transmittance, the Bennett & Brassard 1984 (BB84) QPV protocol has been proven secure against the NPE model [6], and more generally against adversaries with linearly bounded entanglement [11–13].

In the case of high quantum channel loss, it turns out that the situation is much more constrained. In particular, it has been shown that BB84 QPV is highly vulnerable against loss-dependent attacks and is insecure after the 3 dB loss point [14]. This weakness is in part due to the design of the verification challenge. To see this, recall that in BB84 QPV, one verifier V_1 sends a qubit prepared in one of the four BB84 states to the prover P, while the other verifier V_2 sends the basis information. Then, the prover is asked to extract the encoded bit from the qubit by using the received basis information. Now, if the quantum channel loss is sufficiently high, then the adversaries can break the protocol with the following local operations and classical communication (LOCC) attack: First, the adversary nearest to V_1 (called E_1) measures V_1's qubit in a randomly chosen basis and sends the measurement result and the basis choice to the other adversary E_2, who is located next to V_2. Likewise, E_2 duplicates the basis information of V_2 and sends a copy to E_1. Finally, the adversaries report E_1's measurement outcome to their respective verifiers if the basis choices of E_1 and V_2 are the same. Otherwise, they claim no detection. Evidently, this attack works whenever the quantum channel loss is greater than $1/2$, thus implying a 3 dB loss limit. More crucially, this means that BB84 QPV is not useful in practice because most free-space quantum communication systems have more than 3 dB loss [15].

One way to overcome the above limitation is to go beyond the BB84 encoding scheme and encode the qubits in more than two bases. More concretely, if the number of possible encoding bases is N, then the above LOCC attack can only succeed with probability $1/N$. Following this intuition, it has

*limc@ornl.gov

been shown that multibasis QPV using weak laser sources is secure against specific LOCC attacks up to 13 dB loss and a 0.01 quantum bit error rate [14]. Another solution is to use quantum memories and separate the quantum transmission phase from the (classical) basis distribution phase [5]. That is, the quantum challenge (a collection of quantum states) is first delivered to the prover and stored in a quantum memory. Then, the verifiers only send the classical challenge after the prover confirms that the quantum challenge has been received. Thus assuming perfect classical communication, the protocol is essentially secure against loss-dependent attacks. However, such a protocol may require long-lived quantum memories.

Here, we present a QPV protocol that is secure against LOCC adversaries for any quantum channel loss. The protocol is based on the concept of measurement-device-independent quantum key distribution (MDI-QKD) [16,17], which uses time-reversed entanglement swapping to check for quantum correlations [18]. The basic idea is that if the prover is indeed at the claimed position, then he or she should be able to perform a *local* entangling measurement on the verifiers' BB84 qubits and create quantum correlations between them (as in entanglement swapping). However, if the prover is dishonest and is not at the claimed position, then by definition he or she can only collude with other dishonest provers to perform LOCC measurements on the qubits. In this case, no quantum correlations can be created between the verifiers. Therefore, by comparing the measured error rate against some tolerated error rate, the verifiers can check if the prover is at the claimed position. Furthermore, like MDI-QKD, our QPV protocol does not require quantum memories and can be implemented with weak laser sources, linear optics, and standard single-photon detectors.

For practical reasons, we consider the sequential multiround setting where the verifiers only send out their BB84 qubits after receiving the measurement outcome from the previous round. In this setting, the standard relativistic constraints [see Fig. 1] only apply to each individual round. One of the main advantages of sequential multiround is that the adversaries are limited to independent attacks (also known as *collective attacks* in quantum cryptography), which greatly simplifies the security analysis. However, sequential multiround setting includes the possibility that the adversaries could use the first round to distribute entanglement for later rounds and break the protocol. To rule out such a possibility, the most consistent solution, arguably, is to assume LOCC adversaries, which by definition precludes the distribution of entanglement at any point in the protocol. Alternatively, we can also keep the NPE model and further assume the adversaries lose their entanglement at the start of every round. In this work, we consider security against LOCC adversaries and leave the security of NPE model for future work. Here, it is implicit that security against LOCC adversaries means security against LOCC attacks that are compatible with the underlying relativistic constraints (i.e., those with one round of classical communication).

The paper is organized as follows: For pedagogical reasons, in Sec. II we first present the details of our QPV protocol with ideal BB84 qubit states (called Protocol I). Then, in Sec. III we analyze the security of our qubit protocol against LOCC adversaries. In Sec. IV, we extend Protocol I to weak laser sources using the decoy-state method [19] (called Protocol II) and derive its security bound. Finally, in Sec. VI, we conclude with a discussion on possible future work.

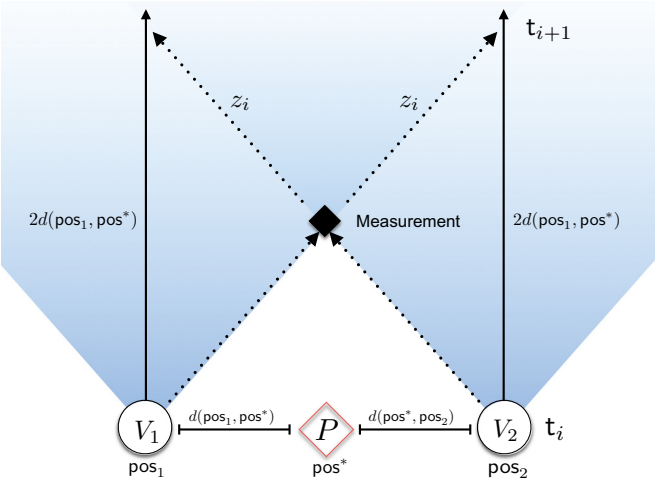

FIG. 1. Relativistic constraints. We assume that all quantum and classical signals travel at the speed of light and that the speed of light is normalized to unity. In this case, the time required to send a message from one position to another position is equal to the Euclidean distance between them. More specifically, the Euclidean distance between pos_1 and pos^* is defined as $d(\mathsf{pos}_1,\mathsf{pos}^*)$ where $d(\cdot,\cdot)$ is the distance measure in $\mathbb{R}$. The protocol is based on a N-fold sequential repetition setting, where the verifiers only send out their qubit states at intervals of $\mathsf{t}_{i+1} - \mathsf{t}_i = 2d(\mathsf{pos}_1,\mathsf{pos}^*) = 2d(\mathsf{pos}^*,\mathsf{pos}_2)$. Note that, for simplicity, we assume the prover is located at the center.

II. QUBIT PROTOCOL

For simplicity, we consider the one-dimensional scenario where everyone is positioned on a straight line. In this scenario, the verifiers are assumed to have access to a private classical channel [20] and each verifier is equipped with a local source of randomness and a trusted BB84 qubit preparation device. More specifically, each qubit preparation device accepts two bits k_1, k_2 as an input and generates ω_{k_1,k_2} by using

$$\omega_{0,0} := \frac{\mathbb{I}+\mathbb{X}}{2}, \quad \omega_{0,1} := \frac{\mathbb{I}-\mathbb{X}}{2},$$
$$\omega_{1,0} := \frac{\mathbb{I}+\mathbb{Y}}{2}, \quad \omega_{1,1} := \frac{\mathbb{I}-\mathbb{Y}}{2},$$

where $\mathbb{X}$ and $\mathbb{Y}$ (together with $\mathbb{Z}$) are the standard Pauli matrices. Our QPV protocol is framed in an m-fold sequential repetition picture and is characterized by two threshold parameters, i.e., the tolerated number of detection events, n_{th}, and the tolerated error rate, $\delta_{\text{th}} < 1/4$. The protocol concludes by outputting either $\{\mathtt{Y},\mathtt{N}\}$, where $\mathtt{Y}$ means agreement and $\mathtt{N}$ means disagreement. Below, we describe our protocol in more detail.

PROTOCOL I. QPV with BB84 qubits.

Protocol with ideal BB84 qubits

1. Preparation. The preparation phase is carried out $i = 1,2,\ldots,m$ times, one after the other. In each ith run, the verifiers first use the private classical channel to generate a random basis choice b_i. Then, they each generate a random bit (which we denote by x_i and y_i, respectively) and use it to prepare a qubit and send it to the prover. The transmission is synchronized in such a way that the qubits reach pos^* at time $\mathsf{t}_i + \tau$, where $\tau = d(\mathsf{pos}_1, \mathsf{pos}^*) = d(\mathsf{pos}^*, \mathsf{pos}_2)$, i.e., see Fig. 1.

2. Measurement. The prover makes an entangling measurement on $\omega_{b_i,x_i} \otimes \omega'_{b_i,y_i}$ and obtains one of the three possible outcomes: $z_i \in \{0,1,\varnothing\}$. The outcome is then reported to the verifiers.

3. Quota check. The verifiers accept the measurement outcome z_i only if it arrives in time. If one of the outcomes does not arrive in time or the verifiers receive different outcomes, they abort the protocol and output N. If the protocol does not abort at the end of the measurement phase, the verifiers perform a *quota check*: they calculate $s_{1,1} = |\mathcal{Z}|$, where $\mathcal{Z} = \{i : z_i \neq \varnothing\}$, and check if $s_{1,1} \geqslant n_{\text{th}}$. If the check is positive, they select a random subset $\mathcal{Z}'$ of size n_{th} from $\mathcal{Z}$. Otherwise, they abort and output N.

4. Verification. Conditioned on passing the quota check, the verifiers compute the error rate and check if

$$\hat{\delta}_{\text{test}} = \frac{r_{1,1}}{s_{1,1}} \leqslant \delta_{\text{th}},$$

where $r_{1,1} = |\mathcal{E}|$ and $\mathcal{E} = \{i : z_i \neq x_i \oplus y_i | z_i \in \mathcal{Z}'\}$. If the check is positive, they agree with the prover and output Y, otherwise they output N.

Let us first present an optical implementation based on single-photon sources and linear optics which shows that the above protocol is cryptographically complete (see Sec. III for a brief discussion and Ref. [1] for a more formal definition). Starting from the preparation phase, the verifiers each use their randomly generated bit values (k_1,k_2) to prepare one of the four possible polarized single-photon states, $\{[|H\rangle + (i)^{k_1}(-1)^{k_2}|V\rangle]/\sqrt{2}\}$, and send it to the prover. Assuming linear optics, the prover can implement a Bell-state measurement (BSM) with $1/2$ efficiency, i.e., one that is capable of discriminating between two Bell states [21,22] (see Fig. 2). In this case, the expected error rate and detection rate are 0 and $1/2$, respectively. That is, whenever the verifiers send the same polarized state (i.e., $x_i = y_i$), they get Ψ^+ (i.e., $z = 0$) with probability $1/2$, Ψ^- (i.e., $z = 1$) with zero probability, and an inconclusive outcome with probability $1/2$. For different polarized states (i.e., $x_i \neq y_i$), they get Ψ^+ with zero probability, Ψ^- with probability $1/2$, and an inconclusive outcome with probability $1/2$. Therefore, the verifiers will always agree with the honest prover if $n_{\text{th}} \leqslant m/2$ is chosen. In this case, the protocol is perfectly complete in the asymptotic limit.

III. SECURITY OF QUBIT PROTOCOL

From a prepare and measure perspective, the basic idea of our protocol is to have the prover guess the XOR of the verifiers' bit values. That is, in each round of the protocol the prover is given a random joint state $\omega_{b,x} \otimes \omega'_{b,y}$ and is supposed to guess the underlying $x \oplus y$. The main security principle of Protocol I is that the best measurement (i.e., one that gives the highest guessing probability) is necessarily an entangling measurement, which according to our security model is only possible at the claimed position pos^*. As we will soon see below, LOCC adversaries (due to their limited measurement possibilities) can only guess $x \oplus y$ with at most probability $3/4$.

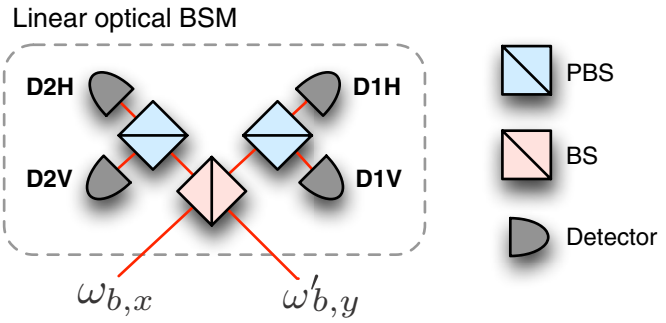

FIG. 2. BSM based on linear optics. A successful Bell-state measurement corresponds to the following detection patterns: a coincident detection in D_{1H} and D_{2V}, or in D_{1V} and D_{2H}, indicates a projection into the Bell state $|\Psi^-\rangle$, while a click in D_{1H} and D_{1V}, or in D_{2H} and D_{2V}, reveals a projection into the Bell state $|\Psi^+\rangle$

To start with, the most general strategy is to maximize the guessing probability over all two-qubit positive-operator valued measure (POVM) operators $\{\Pi_z\}_{z=0,1,\varnothing}$ constrained to an average quantum channel loss parameter (denoted by η). Mathematically, the maximum guessing probability is given by

$$P^{\max}_{\text{guess}}(\eta) := \max_{\{\Pi_z\}_z} \frac{1}{2} \frac{\text{Tr}[\rho_0\Pi_0 + \rho_1\Pi_1]}{\eta}, \tag{1}$$

where

$$\rho_0 := \frac{1}{4} \sum_{\substack{b,x,y \\ \text{s.t.} x \oplus y = 0}} \omega_{b,x} \otimes \omega'_{b,y},$$

$$\rho_1 := \frac{1}{4} \sum_{\substack{b,x,y \\ \text{s.t.} x \oplus y = 1}} \omega_{b,x} \otimes \omega'_{b,y},$$

and $\text{Tr}[\rho_i\Pi_\varnothing] = 1 - \eta$ for $i = 0,1$. Note that for $\eta = 1$, Eq. (1) is given by the Helstrom's bound [23], i.e., $P^{\max}_{\text{guess}}(1) = 1/2 + \|\rho_0 - \rho_1\|_1/4 = 3/4$.

In the case of dishonest LOCC prover(s), the maximum guessing probability is

$$P^{\max}_{\text{guess}}(\eta|\text{LOCC}) := \max_{\{\Pi^{\text{LOCC}}_z\}_z} \frac{1}{2} \frac{\text{Tr}[\rho_0\Pi_0 + \rho_1\Pi_1]}{\eta}, \tag{2}$$

where the maximization is now taken over all two-qubit LOCC measurements. This maximization problem is however difficult to solve because the mathematical characterization of LOCC measurements is highly complex (even for two-qubit measurements with one round of communication). To overcome this problem, we use a circuitous approach based

on positive partial transpose (PPT) measurements which have two advantages over LOCC measurements. First, the set of LOCC measurements is a proper subset of PPT measurements, which means the guessing probability taken over all PPT measurements is necessarily an upper bound on Eq. (2), i.e., $P^{\max}_{\text{guess}}(\eta|\text{PTT}) \geqslant P^{\max}_{\text{guess}}(\eta|\text{LOCC})$. Second, we may reformulate the maximization of $P^{\max}_{\text{guess}}(\eta|\text{PTT})$ as a semidefinite program (SDP) [24], where the optimization is taken over all two-qubit positive operators satisfying the PPT condition (which in turn is represented by a set of linear and positive semidefinite conditions) [25,26]. More concretely, we may express the maximization of $\eta P^{\max}_{\text{guess}}(\eta|\text{PTT})$ (for a fixed η) as

$$\begin{aligned} \texttt{maximize}: \ & \tfrac{1}{2}\text{Tr}[\rho_0\Pi_0 + \rho_1\Pi_1], \\ \texttt{subject to}: \ & \Pi_0 + \Pi_1 + \Pi_\varnothing = \mathbb{1}, \\ & \text{Tr}[\rho_i\Pi_\varnothing] = 1-\eta, \quad i = 0,1 \\ & \Pi_k^{T_\text{B}} \succeq 0, \quad k = 0,1,\varnothing, \end{aligned}$$

where T_B means the partial transpose with respect to the measurement on the second qubit. The optimal solution to the above SDP (primal program) is $3/4\eta$ (see Appendix A 2), which implies the guessing probability for LOCC adversaries is upper bounded by

$$P^{\max}_{\text{guess}}(\eta|\text{LOCC}) \leqslant \tfrac{3}{4}. \tag{3}$$

Interestingly, we see that $P^{\max}_{\text{guess}}(\eta|\text{LOCC})$ is bounded by a constant term that is independent of the detection efficiency η. In fact, it can be shown that this bound is tight, i.e., there exists a LOCC measurement that reaches the PPT bound for any η. To show this, suppose that there are two adversaries, E_1 and E_2, who are positioned next to V_1 and V_2, respectively. Furthermore, suppose that they share a source of shared randomness, λ, which takes values from $\{0,1\}$ with probabilities $\Pr[\lambda = 0] = 1-\eta$ and $\Pr[\lambda = 1] = \eta$, respectively. Now, in each round of the protocol, if $\lambda = 1$, the adversaries measure their respective qubits in the diagonal basis $\mathbb{X}$ and exchange the measurement outcomes. Then, they compute the XOR of their outcomes and send it to the verifiers. If $\lambda = 0$, they jointly report no detection. By using this measurement strategy, it can be easily verified that the guessing probability is $3/4$ for any detection efficiency. Alternatively, the upper bound can also be reached by using the $\mathbb{Y}$ basis, or by using a statistical mixture of $\mathbb{X}$ and $\mathbb{Y}$ bases with the aid of additional shared randomness.

From the above, it is clear that no coalition of LOCC adversaries can correctly predict $x \oplus y$ even if η is arbitrarily small. Coupled with the earlier example that an honest prover (who is at the claimed position and using linear optics) is able to correctly predict $x \oplus y$ for $\eta \leqslant 1/2$, it follows that a conclusive verification of the prover's geographical position is equivalent to checking if the expected error rate is smaller than the minimum LOCC error rate, $\delta_{\text{LOCC}} := 1 - P^{\max}_{\text{guess}}(\eta|\text{LOCC}) = 1/4$.

Before we present the security of Protocol I, let us first briefly explain and define what it means for the protocol to be secure. The security of a generic QPV protocol is generally analyzed by using two conditions; namely, the completeness condition and the soundness condition [1]. The completeness condition, roughly speaking, is a measure of how often the protocol will agree with an honest prover. Note that in the preceding section, we have already shown (by using an ideal optical model) that Protocol I is perfectly complete in the asymptotic limit for $n_{\text{th}} \leqslant m/2$. The soundness condition, which we will be analyzing in more detail below, is a conservative measure of how often the protocol will agree with a coalition of adversaries. More precisely, the soundness condition (adapted to our security model) is defined as

Definition. (Soundness) The protocol is said to be ε-sound if for any coalition of LOCC adversaries $E_1, E_2, E_3, \ldots,$ at positions $\mathsf{pos}'_1, \mathsf{pos}'_2, \mathsf{pos}'_3, \ldots \neq \mathsf{pos}^*$ and using resources only at these positions, the verifiers agree with probability at most ε.

The goal of the security analysis is to compute an upper bound on the soundness error, ε, in terms of the protocol parameters, i.e., the tolerated number of detection events, n_{th}, and the tolerated error rate, δ_{th}.

Result 1. (Security with qubits) Given n_{th} and δ_{th}, the protocol is $\varepsilon_{\text{qubit}}$-sound against LOCC adversaries with

$$\varepsilon_{\text{qubit}} \leqslant e^{-2n_{\text{th}}(1/4-\delta_{\text{th}})^2}. \tag{4}$$

Proof sketch. The soundness of the protocol is obtained by asking what is the maximum probability that the verifiers agree with the adversaries. In what follows, for brevity reasons, we will denote the event that the protocol passes the quota check by Ω_{qc} and omit the conditioning on LOCC attacks (since this is clear in the context). First, we note that the soundness error is upper bounded by the probability that the verifiers agree with adversaries conditioned on Ω_{qc}, i.e.,

$$\begin{aligned} \varepsilon_{\text{qubit}} &= \Pr[\Omega_{\text{qc}}]\Pr[\texttt{Y}|\Omega_{\text{qc}}] + \Pr\left[\Omega^{\text{c}}_{\text{qc}}\right]\Pr\left[\texttt{Y}\middle|\Omega^{\text{c}}_{\text{qc}}\right] \\ &\leqslant \Pr[\texttt{Y}|\Omega_{\text{qc}}], \end{aligned}$$

where we used $\Pr[\Omega_{\text{qc}}] \leqslant 1$ and $\Pr[\texttt{Y}|\Omega^{\text{c}}_{\text{qc}}] = 0$ to get the inequality. Next, we note that the protocol outputs Y only if the measured error rate $\hat{\delta}_{\text{test}}$ is less than or equal to the tolerated error rate δ_{th}. This gives

$$\varepsilon_{\text{qubit}} \leqslant \Pr[\texttt{Y}|\Omega_{\text{qc}}] = \Pr[\hat{\delta}_{\text{test}} \leqslant \delta_{\text{th}}|\Omega_{\text{qc}}].$$

The above probability term can be modeled by a Bernoulli experiment with n_{th} trials. More precisely, for each element in $\mathcal{Z}'$, let $\hat{W}_i$ be an indicator random variable taking values in $\{0,1\}$, where 0 means no error and 1 means otherwise. Let $\hat{\delta}_{\text{test}} = \sum_{i=1}^{n_{\text{th}}} \hat{W}_i/n_{\text{th}}$, then the probability of $\text{E}[\hat{\delta}_{\text{test}}] - \hat{\delta}_{\text{test}} \geqslant \beta$ for some $\beta > 0$ is bounded by the Hoeffding's inequality [27]:

$$\Pr[\text{E}[\hat{\delta}_{\text{test}}] - \hat{\delta}_{\text{test}} \geqslant \beta] \leqslant e^{-2n_{\text{th}}\beta^2}.$$

Finally, by setting $\text{E}[\hat{\delta}_{\text{test}}] = \delta_{\text{LOCC}}$, and $\beta = 1/4 - \delta_{\text{th}}$, we have

$$\varepsilon_{\text{qubit}} \leqslant \Pr[\delta_{\text{th}} \geqslant \hat{\delta}_{\text{test}}|\Omega_{\text{qc}}] \leqslant e^{-2n_{\text{th}}(1/4-\delta_{\text{th}})^2}.$$

■

From the above, we see that the soundness error is exponentially small in $n_{\text{th}}(1/4 - \delta_{\text{th}})$. This means that Protocol I can be made highly reliable by choosing a large n_{th} and a stringent error threshold (i.e., a small δ_{th}). More importantly, the soundness error is independent of the detection rate, which means that Protocol I is secure against arbitrary quantum channel loss.

IV. DECOY-STATE METHOD

In Protocol I we have assumed that the verifiers are able to reliably prepare ideal qubit states. However in practice, this assumption is unrealistic as it requires true single-photon sources. A more practical option is to use weak laser sources, which are good approximations of probabilistic single-photon sources. More concretely, the output of a laser with intensity $\mu = |\alpha|^2$ is described by a coherent state, $|\alpha\rangle = e^{-\mu/2}\sum_{n=0}\alpha^n/\sqrt{n!}|n\rangle$, where $\{|n\rangle\}_n$ is the photon number (Fock) basis. Assuming that the laser is phase randomized, the photon number of each output state follows a Poisson distribution with its mean given by the laser's intensity [28]. In this case, the output state is described by

$$\rho_{\text{laser}} = \frac{1}{2\pi}\int_0^{2\pi} d\theta\,|\alpha|e^{i\theta}\rangle\langle|\alpha|e^{i\theta}| = \sum_{n=0}^{\infty}\frac{\mu^n}{n!}e^{-\mu}|n\rangle\langle n|,$$

where θ is the phase of the state and $|n\rangle\langle n|$ is the density matrix of the n-photon state. This means that in each round, the laser source emits a vacuum state with probability $e^{-\mu}$, a single-photon state with probability $\mu e^{-\mu}$, and a multiphoton state with probability $1-(1+\mu)e^{-\mu}$. Thus, we may think of weak laser sources as probabilistic single-photon sources if the laser intensity is sufficiently small.

However, in the case of QPV, the nonvanishing multiphoton probability is a major security issue, especially when the quantum channel loss is high. In particular, colluding adversaries can post select laser pulses with three photons or more and perform unambiguous state discrimination to determine the verifier's basis and bit information with success probability $\geqslant 1/2$ [29]. If the quantum channel loss is high enough, then it is not hard to see that QPV is reduced to the classical version (with classical challenges) when all $n < 3$ laser pulses are blocked and returned as empty detections. Importantly, this implies that the security of QPV with weak laser sources is not independent of the quantum channel loss.

In the following, we will show that QPV with weak laser sources is still highly robust against quantum channel loss, tolerating up to 47 dB loss assuming realistic parameters. The central idea is to use the decoy-state method [19] to estimate the number of single-photon detections, i.e., the number of instances in which both verifiers send single-photon states and a successful BSM outcome is announced (denoted by $s_{1,1}$), and the number of errors in these single-photon detections (denoted by $r_{1,1}$) [30,31]. Then, by using these estimates, the verifiers can verify the position of the prover by checking if the estimated single-photon error rate is smaller than the tolerated error rate (as in Protocol I).

We consider a decoy-state method with three intensities, $\mathcal{I} := \{\mu_1,\mu_2,\mu_3\}$, where $\mu_1 > \mu_2+\mu_3$ and $\mu_2 > \mu_3 \geqslant 0$. The relevant estimates are (1) a lower bound on $s_{1,1}$ and (2) an upper bound on $r_{1,1}$, which we denote by random variables $\hat{s}^{\text{lb}}_{1,1}$ and $\hat{r}^{\text{ub}}_{1,1}$, respectively. Accordingly, this means that there are two possible statistical errors, one due to the estimation of $s_{1,1}$ and the other due to the estimation of $r_{1,1}$. The reliability of these estimates is parametrized by a nonnegative security parameter, ν. Below we present the protocol in more detail.

PROTOCOL II. QPV with decoy-state method.

Protocol with decoy-state method

1. Preparation. The prepare and measurement phase is carried out $i = 1,2,\ldots,m$ times, one after the other. Like in the qubit protocol, the verifiers agree on a random basis choice b_i using the private classical channel, and they each independently generate a random bit. For the decoy-state method, they each select an intensity value from $\mathcal{I} := \{\mu_1,\mu_2,\mu_3\}$ with probabilities p_{μ_1}, p_{μ_2}, and p_{μ_3}, respectively. We write g_i and h_i to denote their respective intensity choices for each ith round. Finally, the verifiers each prepare a weak laser pulse based on their generated values and send the encoded laser pulse to the prover.

2. Measurement. The prover makes an entangling measurement on the laser pulses and report the outcome, $z_i \in \{0,1,\varnothing\}$, back to the verifiers.

3. Quota check. Similar to the qubit protocol, the verifiers only accept the measurement outcomes if they are consistent with the timing constraints. If one of the outcomes does not meet the timing constraint or the verifiers receive different outcomes, the protocol aborts and the verifiers output N. If the protocol does not abort at the end of the measurement phase, the verifiers perform a quota check. Setting $n^{u,v}_{\text{obs}} = |\mathcal{Z}^{u,v}|$ for $u,v = \mu_1,\mu_2,\mu_3$ and $n_{\text{obs}} = \sum_{u,v} n^{u,v}_{\text{obs}}$, the verifiers compute a lower bound on $s_{1,1}$ (see Appendix B 2) by using

$$\hat{s}^{\text{lb}}_{1,1} = \left\lfloor \frac{(\mu_1^2-\mu_3^2)(\mu_1-\mu_3)\gamma_2 - (\mu_2^2-\mu_3^2)(\mu_2-\mu_3)\gamma_1}{(\mu_1-\mu_3)^2(\mu_2-\mu_3)^2(\mu_1-\mu_2)} \right\rfloor, \quad (5)$$

where

$$\begin{aligned}\gamma_1 &:= \chi^{\mu_1,\mu_1} + \chi^{\mu_3,\mu_3} - \chi^{\mu_1,\mu_3} - \chi^{\mu_3,\mu_1} \\ &\quad + \nu^{\frac{1}{2}} n_{\text{obs}}^{\frac{1}{2}}(\xi^{\mu_1,\mu_1} + \xi^{\mu_3,\mu_3} + 2\xi^{\mu_1,\mu_3}), \\ \gamma_2 &:= \chi^{\mu_2,\mu_2} + \chi^{\mu_3,\mu_3} - \chi^{\mu_2,\mu_3} - \chi^{\mu_3,\mu_2} \\ &\quad - \nu^{\frac{1}{2}} n_{\text{obs}}^{\frac{1}{2}}(\xi^{\mu_2,\mu_2} + \xi^{\mu_3,\mu_3} + 2\xi^{\mu_2,\mu_3}),\end{aligned}$$

with $\xi^{u,v} := \exp(u+v)p_u^{-1}p_v^{-1}$ and $\chi^{u,v} := \xi^{u,v}n^{u,v}_{\text{obs}}$ for all $u,v \in \mathcal{I}$. The verifiers proceed to the verification step if

$$s^{\text{lb}}_{1,1} \geqslant n_{\text{th}},$$

otherwise they abort the protocol and output N.

4. Verification. The verifiers first calculate the number of errors (denoted by $m^{u,v}_{\text{obs}}$) in each $\mathcal{Z}^{u,v}$ and the total number of errors, $m_{\text{obs}} = \sum_{u,v} m^{u,v}_{\text{obs}}$. Then, they compute an upper bound on $r_{1,1}$ by using

$$\hat{r}^{\text{ub}}_{1,1} = \min\left\{\left\lceil \frac{\gamma_3}{(\mu_2-\mu_3)^2}\right\rceil, \left\lceil \frac{\hat{s}^{\text{lb}}_{1,1}}{2}\right\rceil\right\}, \quad (6)$$

where

$$\begin{aligned}\gamma_3 &:= \zeta^{\mu_2,\mu_2} + \zeta^{\mu_3,\mu_3} - \zeta^{\mu_2,\mu_3} - \zeta^{\mu_3,\mu_2} \\ &\quad + \nu^{\frac{1}{2}} m_{\text{obs}}^{\frac{1}{2}}(\xi^{\mu_2,\mu_2} + \xi^{\mu_3,\mu_3} + 2\xi^{\mu_2,\mu_3}).\end{aligned}$$

with $\zeta^{u,v} := \xi^{u,v}m^{u,v}_{\text{obs}}$. Finally, the verifiers agree with the prover and output Y if

$$\hat{\delta}^{\text{decoy}}_{\text{test}} = \frac{\hat{r}^{\text{ub}}_{1,1}}{\hat{s}^{\text{lb}}_{1,1}} \leqslant \delta_{\text{th}},$$

Otherwise, they output N.

V. SECURITY ANALYSIS AND SIMULATION

A crucial step in the security analysis of Protocol I is that the verifiers are able to directly observe $s_{1,1}$ and $r_{1,1}$ and check if the protocol has sufficient statistics, i.e., $s_{1,1} \geqslant n_{\text{th}}$, and if the verification is correct, i.e., $r_{1,1}/s_{1,1} \leqslant \delta_{\text{th}}$. However, in the case of weak laser sources, the direct observation of $s_{1,1}$ and $r_{1,1}$ is not possible as the verifiers do not know which of the successful BSM detections are due to single-photon emissions. To overcome this issue, Protocol II uses the decoy-state method as a means to construct random one-sided intervals for $s_{1,1}$ and $r_{1,1}$. In particular, the intervals $\hat{s}^{\text{lb}}_{1,1}$ and $\hat{r}^{\text{ub}}_{1,1}$, as specified in Eqs. (5) and (6), are constructed to capture $s_{1,1}$ and $r_{1,1}$ with very high probability in each run of the protocol.

The key point here is that, although the decoy-state method can be made very reliable (i.e., by choosing a large ν), there is still a nonvanishing probability that the intervals will fail to capture $s_{1,1}$ and $r_{1,1}$ in the right direction. That is, there could be instances of the protocol in which the computed intervals are wrong and yet the verifiers agree with the adversaries. In terms of the security analysis, this means that there is a strictly nonzero probability that the verifiers will agree with the adversaries, thereby implying an additional source of soundness errors. Here, it is important to emphasize that this source of soundness error (which is due to the uncertainties in the decoy-state method) is fundamentally different from the soundness error captured by Eq. (4), which is induced by the uncertainty in the error rate distribution. Below, we show that the soundness error of Protocol II is the same as Protocol I except for an additive error term that is due to the statistical errors of the decoy-state method used.

Result 2. (Security with weak laser sources) Given $\{\mu_1,\mu_2,\mu_3\}$, $\{p_u \times p_v\}_{u,v}$, n_{th}, δ_{th}, and ν, the protocol is $\varepsilon_{\text{decoy}}$-sound with

$$\varepsilon_{\text{decoy}} < \varepsilon_{\text{qubit}} + 2\epsilon_1 + \epsilon_2, \tag{7}$$

where $\epsilon_1 := 1-(1-e^{-2\nu})^7$ and $\epsilon_2 := 1-(1-e^{-2\nu})^4$.

Proof sketch. Here, we start from a general scenario and assume that the adversaries use $s_{1,1} > n_{\text{th}}$ with probability κ and $s_{1,1} \leqslant n_{\text{th}}$ with probability $1-\kappa$. Note that this choice of partitioning is not restrictive (since κ is not fixed) and is merely used to facilitate the security analysis. Let the event $s_{1,1} > n_{\text{th}}$ be denoted by Θ, then the soundness error can be written as

$$\varepsilon_{\text{decoy}} = 1-\kappa \Pr[\mathtt{N}|\Theta] - (1-\kappa)\Pr[\mathtt{N}|\Theta^{\text{c}}].$$

By conditioning on Ω_{qc}, we further get

$$\begin{aligned}\varepsilon_{\text{decoy}} = {}& \kappa \Pr[\Omega_{\text{qc}}|\Theta](1-\Pr[\mathtt{N}|\Theta,\Omega_{\text{qc}}]) \\ & + (1-\kappa)\Pr[\Omega_{\text{qc}}|\Theta^{\text{c}}](1-\Pr[\mathtt{N}|\Theta^{\text{c}},\Omega_{\text{qc}}]).\end{aligned}$$

The above can be simplified by setting $\Pr[\mathtt{N}|\Theta^{\text{c}},\Omega_{\text{qc}}]=0$ and κ, $\Pr[\Omega_{\text{qc}}|\Theta] \leqslant 1$ to get a bound that is independent of κ (which is unknown),

$$\varepsilon_{\text{decoy}} < 1-\Pr[\mathtt{N}|\Theta,\Omega_{\text{qc}}] + \Pr[\Omega_{\text{qc}}|\Theta^{\text{c}}]. \tag{8}$$

Now, let us focus on the event Θ, where there are two parts to it. The first part consists in bounding the probability that $\hat{r}_{1,1}/s_{1,1} > \delta_{\text{th}}$. This is given by Eq. (4) with n_{th} replaced by $s_{1,1}$: $\Pr[\hat{r}_{1,1}/s_{1,1} > \delta_{\text{th}}] > 1-\varepsilon'_{\text{qubit}}$, where we used $\varepsilon'_{\text{qubit}}$ to remind that $s_{1,1}$ has been used instead of n_{th}. Then from $\varepsilon'_{\text{qubit}} < \varepsilon_{\text{qubit}}$, we have

$$\Pr[\hat{r}_{1,1}/s_{1,1} > \delta_{\text{th}}] > 1-\varepsilon_{\text{qubit}}, \tag{9}$$

which is now expressed in terms of the protocol parameters. The second part consists of bounding the reliability of the decoy-state method. Recall that the goal is to provide a lower bound on $s_{1,1}$ and an upper bound on $\hat{r}_{1,1}=r_{1,1}$ (i.e., for a given realization of $\hat{r}_{1,1}$). These bounds are given by $\hat{s}^{\text{lb}}_{1,1}$ and $\hat{r}^{\text{ub}}_{1,1}$, which are one-sided interval estimates. Suppose for the moment the reliability of these estimates are known, i.e., $\Pr[s_{1,1} > \hat{s}^{\text{lb}}_{1,1}] > 1-\epsilon_1$ and $\Pr[r_{1,1} < \hat{r}^{\text{ub}}_{1,1}|\hat{r}_{1,1}=r_{1,1}] > 1-\epsilon_2$. Then, by taking the ratio distribution, we can construct a one-sided interval for the single-photon error rate,

$$\Pr\left[r_{1,1}/s_{1,1} < \hat{r}^{\text{ub}}_{1,1}/\hat{s}^{\text{lb}}_{1,1}\middle|\hat{r}_{1,1}=r_{1,1}\right] > (1-\epsilon_1)(1-\epsilon_2). \tag{10}$$

Operationally, this means that, given $s_{1,1}$ and $r_{1,1}$, the decoy-state method *will* output a single-photon error rate estimate, $\hat{r}^{\text{ub}}_{1,1}/\hat{s}^{\text{lb}}_{1,1}$, that is larger than the true single-photon error rate $r_{1,1}/s_{1,1}$ with probability greater than $(1-\epsilon_1)(1-\epsilon_2)$. Notice that the probability statement is about the computed interval and not about the true single-photon error rate.

Now it remains to put everything together. First, we have that the probability of rejection conditioned on Θ is given by

$$\Pr[\mathtt{N}|\Theta,\Omega_{\text{qc}}] = \Pr\left[\delta_{\text{th}} < \hat{r}^{\text{ub}}_{1,1}/\hat{s}^{\text{lb}}_{1,1}\middle|\Theta,\Omega_{\text{qc}}\right],$$

which is essentially Eq. (10) conditioned on the event $\hat{r}_{1,1} > \lceil \delta_{\text{th}} s_{1,1} \rceil$. More precisely, we have $\Pr[\mathtt{N}|\Theta,\Omega_{\text{qc}}] = \Pr[\hat{r}_{1,1} > \lceil \delta_{\text{th}} s_{1,1} \rceil|\Theta]\Pr[r_{1,1}/s_{1,1} < \hat{r}^{\text{ub}}_{1,1}/\hat{s}^{\text{lb}}_{1,1}|\hat{r}_{1,1}=r_{1,1}]$, which together with Eq. (9) implies

$$\Pr[\mathtt{N}|\Theta,\Omega_{\text{qc}}] > (1-\epsilon_1)(1-\epsilon_2)(1-\varepsilon_{\text{qubit}}).$$

Plugging this in Eq. (8), we thus get

$$\begin{aligned}\varepsilon_{\text{decoy}} &< 1-(1-\epsilon_1)(1-\epsilon_2)+\varepsilon_{\text{qubit}}+\Pr[\Omega_{\text{qc}}|\Theta^{\text{c}}] \\ &< 1-(1-\epsilon_1)(1-\epsilon_2)+\varepsilon_{\text{qubit}}+\epsilon_1 \\ &< 2\epsilon_1+\epsilon_2+\varepsilon_{\text{qubit}},\end{aligned}$$

where in the second inequality we used $\Pr[\Omega_{\text{qc}}|\Theta^{\text{c}}] \leqslant \epsilon_1$.

Finally, in Appendix B 2 we show that the statistical errors ϵ_1 and ϵ_2 can be parametrized using a fixed security constant, ν, giving

$$\epsilon_1 = 1-(1-e^{-2\nu})^7, \quad \epsilon_2 = 1-(1-e^{-2\nu})^4,$$

which concludes our proof sketch. ■

A way to evaluate the feasibility of our protocol is to look for the loss point (in dB) at which the error rate, $\hat{r}^{\text{ub}}_{1,1}/\hat{s}^{\text{lb}}_{1,1}$, is greater than 1/4. To this end, we consider a symmetric photonic

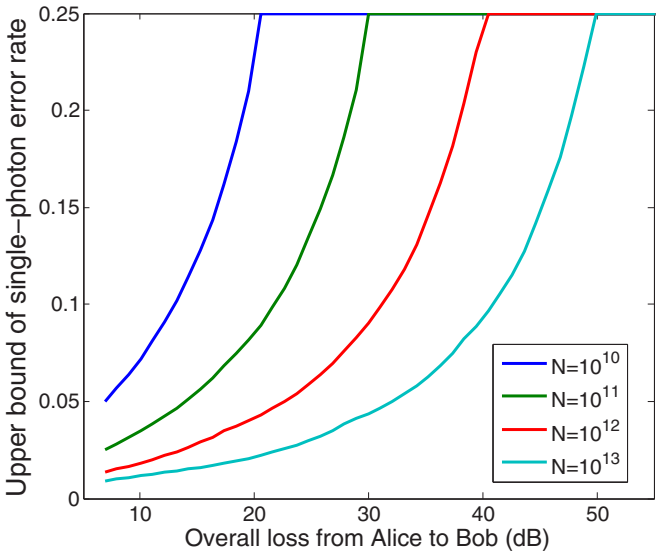

FIG. 3. The upper bound of the estimated single-photon error rate versus overall loss between Alice and Bob. The simulation assumes a baseline QBER of 0.1%. The the detectors are assumed to have an efficiency of 64% and a dark count rate of 2.5×10^{-6}. The starting cutoff point is about 6.8 dB, which is the total loss in the BSM. The numerical results are obtained using $N = 10^x$ with $x = 10,11,12,13$ (from left to right).

implementation where the prover is positioned at the center between the verifiers, i.e., see Fig. 1. The implementation is based on polarized photons, linear optical elements and threshold detectors. Following standard channel error models for photonic quantum communication (e.g., see Ref. [30]), we assume two sources of error; namely, polarization misalignment errors and background noise. In this case, the quantum bit error rate (QBER) is made up of two components: a baseline error rate (polarization misalignment errors) and a loss-dependent error rate (due to detector dark counts). Evidently in our consideration, the limit on the amount of tolerable loss is largely determined by the detector dark count rate. For the simulation, we borrow experimental parameters from a recent MDI-QKD experiment [32]: the baseline error rate is fixed to 0.1% and the detectors (with 64% efficiency) are assumed to have a dark count rate of 2.5×10^{-6}. Also, the security parameter of the decoy-state method is fixed to $\nu = 10$, giving an overall error probability of $\sim 10^{-8}$. In Fig. 3, we plot $\hat{r}^{\mathrm{ub}}_{1,1}/\hat{s}^{\mathrm{lb}}_{1,1}$ for $N = 10^x$ with $x = 10,11,12,13$ against the overall quantum channel loss (dB). From the simulation, we see that our protocol is able to tolerate up to about 47 dB loss with weak laser sources.

VI. CONCLUSION AND OUTLOOK

In the above, we have presented a time-reversed entanglement swapping QPV protocol that is highly robust against detection losses. By using a proof technique from Refs. [25,26], we first showed that Protocol I (assuming ideal BB84 qubits) is secure against arbitrary local operations and classical communication (LOCC) attacks for any quantum channel loss. In particular, the soundness error of the protocol is shown to be independent of the overall detection loss and is exponentially small in the number of rounds with conclusive measurement outcomes. This is in contrast to the widely studied BB84 QPV protocol, which is insecure when the quantum channel loss is $\geqslant 1/2$ assuming LOCC attacks [14]. In Sec. IV, we extended Protocol I to weak laser sources using a practical decoy-state method with three intensities (denoted by Protocol II). We found that the soundness error of Protocol II only degrades by an additive error term that is dependent on the reliability of the underlying decoy-state method. In addition, we performed numerical simulations by using realistic experimental conditions and found that secure position verification is possible up to about 47 dB loss.

Evidently, our proposed protocol is not the complete solution to practical QPV. In particular, what we have addressed here is only the overall detection loss, assuming the verifiers are able to accurately prepare their quantum states. To this end, it would be useful to investigate the impact of state-preparation errors, especially considering the fact that such errors are known to severely degrade the security performance of quantum key distribution [33]. One possible solution is to adopt the notion of *loss-tolerant quantum cryptography* [34] and employ mismatched basis statistics to guarantee the loss-tolerant property of our protocol in the presence of state-preparation errors. Another interesting line of research would be to look at the semi-device-independent security of our protocol assuming that the dimension of the verifier's quantum challenges (states) is fixed. Several results have been obtained in this direction for measurement-device-independent QKD [35,36], to which suggest that similar conclusions could hold for our QPV protocol.

ACKNOWLEDGMENTS

This work was performed at Oak Ridge National Laboratory (ORNL), operated by UT-Battelle for the U.S. Department of Energy under Contract No. DE-AC05-00OR22725. The authors acknowledge support from ORNL laboratory directed research and development program (LDRD), the U.S. Department of Energy Cybersecurity for Energy Delivery Systems (CEDS) program program under contract M614000329, and the U.S. Office of Naval Research (ONR).

This manuscript has been authored by UT-Battelle, LLC under Contract No. DE-AC05-00OR22725 with the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes. The Department of Energy will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (http://energy.gov/downloads/doe-public-access-plan).

APPENDIX A: DETAILS OF SEMIDEFINITE PROGRAM

1. Semidefinite program: preliminaries

In order for us to provide a more precise description of our semidefinite programs, we would need to introduce a few mathematical notations; some of which may be different from those used in the main text. We let V_1 and V_2 complex Hilbert spaces be denoted by $\mathcal{A}$ and $\mathcal{B}$, respectively. The set of linear operators, Hermitian operators, and positive semidefinite operators acting on the composite Hilbert space are written as $\mathrm{L}(\mathcal{A}\otimes\mathcal{B})$, $\mathrm{Herm}(\mathcal{A}\otimes\mathcal{B})$, and $\mathrm{Pos}(\mathcal{A}\otimes\mathcal{B})$, respectively. Furthermore, we write $Q\succeq 0$ to indicate that Q is positive semidefinite. The set of density operators corresponding to the verifiers' quantum systems is defined as $\mathrm{D}(\mathcal{A}\otimes\mathcal{B}):=\{\rho\in\mathrm{Pos}(\mathcal{A}\otimes\mathcal{B}):\mathrm{Tr}[\rho]=1\}$. Additionally, we would require the partial transpose operation, $T_{\mathcal{B}}=\mathbb{I}_{\mathrm{L}(\mathcal{A})}\otimes T$, which performs the transpose operation T on V_2's Hilbert space. Accordingly, the set of positive partial transpose (PPT) operators is defined as $\mathrm{PPT}(\mathcal{A}:\mathcal{B}):=\{Q:T_{\mathcal{B}}(Q)\succeq 0, Q\in\mathrm{Pos}(\mathcal{A}\otimes\mathcal{B})\}$. Also, we denote a diagonal matrix by $Q=\mathrm{diag}[\lambda_1,\lambda_2,\lambda_3,\lambda_4]$.

2. Optimal guessing probabilities

As mentioned in the main text, the bound for PPT measurements can be analytically solved by using convex optimization techniques; namely, semidefinite programming [24]. More specifically, the idea is to find feasible analytical solutions for the primal and dual programs which provide lower and upper bounds on the optimal value (i.e., the weak duality principle). If the solutions lead to values that coincide, then we say that the optimal solution for the semidefinite program is found. That is, by the strong duality principle, the duality gap is zero. In the following, we will show that the considered semidefinite programs have zero duality gaps.

Result 3 (Optimal guessing probability for PPT measurements). The maximum probability of discriminating ρ_0 and ρ_1 using measurements $\{\Pi_0,\Pi_1,\Pi_\varnothing\}\in\mathrm{PPT}(\mathcal{A}\otimes\mathcal{B})$ for any conclusive rate $\eta\in(0,1]$ is

$$P^{\max}_{\mathrm{guess}}(\eta|\mathrm{PPT})=\tfrac{3}{4}. \tag{A1}$$

Proof sketch. The primal program for PPT measurements is given as

Primal program (PPT)

$$\begin{aligned}
\texttt{maximize}:\ & \tfrac{1}{2}\mathrm{Tr}[\rho_0\Pi_0+\rho_1\Pi_1],\\
\texttt{subject to}:\ & \Pi_0+\Pi_1+\Pi_\varnothing=\mathbb{1}_{\mathcal{A}\otimes\mathcal{B}},\\
& \mathrm{Tr}[\rho_i\Pi_\varnothing]=1-\eta,\quad i=0,1,\\
& \Pi_k\in\mathrm{PPT}(\mathcal{A}:\mathcal{B}),\quad k=0,1,\varnothing,
\end{aligned}$$

and the corresponding dual program is

Dual program (PPT)

$$\begin{aligned}
\texttt{minimize}:\ & \mathrm{Tr}[Y]-(1-\eta)\gamma,\\
\texttt{subject to}:\ & 2[Y-T_{\mathcal{B}}(Q_i)]-\rho_i\succeq 0,\quad i=0,1,\\
& 4[Y-T_{\mathcal{B}}(Q_2)]-\gamma\mathbb{1}_{\mathrm{L}(\mathcal{A}\otimes\mathcal{B})}\succeq 0,\\
& Y\in\mathrm{Herm}(\mathcal{A}\otimes\mathcal{B}),\\
& Q_i\in\mathrm{Pos}(\mathcal{A}\otimes\mathcal{B}),\quad i=0,1,2,\\
& \gamma\in\mathbb{R}.
\end{aligned}$$

To prove Eq. (A1), we need to construct feasible solutions for the primal and dual programs and show that their optimization values are identical. For the primal program, a feasible solution is

$$\tilde{\Pi}_0=\frac{1}{2}\begin{bmatrix}\eta&0&0&0\\0&\eta&\eta&0\\0&\eta&\eta&0\\0&0&0&\eta\end{bmatrix},\quad \tilde{\Pi}_0=\frac{1}{2}\begin{bmatrix}\eta&0&0&0\\0&\eta&-\eta&0\\0&-\eta&\eta&0\\0&0&0&\eta\end{bmatrix},$$

$$\tilde{\Pi}_\varnothing=\mathrm{diag}[1-\eta,1-\eta,1-\eta,1-\eta].$$

Using this solution, we get $\eta P^{\max}_{\mathrm{guess}}(\eta|\mathrm{PPT})\geqslant 3\eta/4$. For the dual program, a feasible solution is

$$\tilde{Y}=\frac{3}{16}\mathbb{1}_{\mathrm{L}(\mathcal{A}\otimes\mathcal{B})},\quad \tilde{\gamma}=\frac{3}{4},$$

$$Q_0=\frac{1}{16}\begin{bmatrix}1&0&0&-1\\0&0&0&0\\0&0&0&0\\-1&0&0&1\end{bmatrix},\quad Q_1=\frac{1}{16}\begin{bmatrix}1&0&0&1\\0&0&0&0\\0&0&0&0\\1&0&0&1\end{bmatrix},$$

$$Q_2=0_{\mathrm{L}(\mathcal{A}\otimes\mathcal{B})},$$

which gives $\eta P^{\max}_{\mathrm{guess}}(\eta|\mathrm{PPT})\leqslant 3\eta/4$. Putting everything together, the obtained optimal values give Eq. (A1). ■

APPENDIX B: DETAILS OF DECOY-STATE METHOD

Here, we provide the details for the bounds from the decoy-state analysis presented in the main text. The analysis is mainly based on Ref. [31].

1. Decoy-state method: preliminaries

Our decoy-state method consists of both verifiers randomly setting the intensities of their respective laser pulses to one of the three intensity levels, $\mathcal{I}=\{\mu_1,\mu_2,\mu_3\}$ where $\mu_1>\mu_2+\mu_3$ and $\mu_2>\mu_3\geqslant 0$. To analyze the finite-size effects of the decoy-state method, we consider an equivalent protocol, where V_1 (V_2) has the ability to send k-photon (l-photon) states, and they only decide on the choice of the average photon-number after the prover announces a successful measurement. In what follows, we will first introduce basic notations for the decoy-state analysis and then provide the relevant bounds for $s_{1,1}$ and $r_{1,1}$.

Let $s_{k,l}$ be the number of successful measurements announced by the prover given that V_1 has sent k-photon states and V_2 has sent m-photon states. In this case, it is not hard to see that $\sum_{k,l=0}^{\infty}s_{k,l}=\sum_{u,v}n^{u,v}=n$ is the total number of detections, where $n_{u,v}$ is the number of detections assigned to intensity settings u and v. Furthermore, we expect the size of $n_{u,v}$ to be

$$\tilde{n}^{u,v}=\sum_{k,l=0}^{\infty}p_{u,v|k,l}s_{k,l}, \tag{B1}$$

where $p_{u,v|k,l}$ is the conditional probability of choosing the intensity settings u and v given that V_1 sent a k-photon state and V_2 sent a l-photon state. More formally, the difference between the expected value ($\tilde{n}^{u,v}$) and the observed value ($n^{u,v}$) can be quantified by using the Hoeffding's inequality [27]:

$$|\tilde{n}^{u,v}-n^{u,v}|<\Delta(n,\epsilon_1), \tag{B2}$$

where $\Delta(n,\epsilon_1) := \sqrt{n/2\ln(1/\epsilon_1)}$. The same statistical inequality can also be made for the expected number of errors and the observed number of errors for any pair of intensity settings. Let $r_{k,l}$ be the number of errors associated with $s_{k,l}$, $m = \sum_{k,l=0}^{\infty} r_{k,l}$ be the total number of errors, and

$$\tilde{m}^{u,v} = \sum_{k,l=0}^{\infty} p_{u,v|k,l} r_{k,l}, \tag{B3}$$

be the expected number of errors assigned to intensity settings u and v. Then, the difference between $\tilde{m}^{u,v}$ and $m^{u,v}$ is given by

$$|\tilde{m}^{u,v} - m^{u,v}| < \Delta(m,\epsilon_2), \tag{B4}$$

which holds with probability at least $1 - 2\epsilon_2$.

A central ingredient in Eqs. (B1) and (B3) is the probability of choosing intensities u,v given k,l photons (i.e., $p_{u,v|k,l}$), which is not directly accessible in Protocol II. To estimate this quantity, we note that with Bayes' rule, for all u and v, we have

$$p_{u,v|k,l} = \frac{p_{u,v}}{\tau_{k,l}} p_{k,l|u,v} = \frac{p_{u,v}}{\tau_{k,l}} \frac{e^{-(u+v)} u^k v^l}{k!l!}, \tag{B5}$$

where $p_{u,v}$ denotes the probability that V_1 chooses intensity u and V_2 chooses intensity v, and

$$\tau_{k,l} := \sum_{u,v} p_{u,v} e^{-(u+v)} \frac{u^k v^l}{k!l!} \tag{B6}$$

is the probability that V_1 prepares a k-photon state and V_2 prepares a l-photon state.

2. Estimation of $s_{1,1}$ and $r_{1,1}$

Next, we discuss how to calculate $s_{1,1}$. This is done by exploiting the structure of Eq. (B1) and following the approach proposed by Refs. [30,31]. The estimation method is mainly based on Gaussian elimination. For brevity, let $\xi^{u,v} := \exp(u+v) p_u^{-1} p_v^{-1}$ for all $u,v \in \mathcal{I}$, then we have $s_{1,1} \geqslant s_{1,1}^{\mathrm{lb}}$ where

$$s_{1,1}^{\mathrm{lb}} = \left\lfloor \frac{(\mu_1^2 - \mu_3^2)(\mu_1 - \mu_3)\gamma_2' - (\mu_2^2 - \mu_3^2)(\mu_2 - \mu_3)\gamma_1'}{(\mu_1 - \mu_3)^2(\mu_2 - \mu_3)^2(\mu_1 - \mu_2)} \right\rfloor, \tag{B7}$$

and

$$\gamma_1' := \xi^{\mu_1,\mu_1}\tilde{n}^{\mu_1,\mu_1} + \xi^{\mu_3,\mu_3}\tilde{n}^{\mu_3,\mu_3} - \xi^{\mu_1,\mu_3}\tilde{n}^{\mu_1,\mu_3} - \xi^{\mu_3,\mu_1}\tilde{n}^{\mu_3,\mu_1}, \tag{B8}$$

$$\gamma_2' := \xi^{\mu_2,\mu_2}\tilde{n}^{\mu_2,\mu_2} + \xi^{\mu_3,\mu_3}\tilde{n}^{\mu_3,\mu_3} - \xi^{\mu_2,\mu_3}\tilde{n}^{\mu_2,\mu_3} - \xi^{\mu_3,\mu_2}\tilde{n}^{\mu_3,\mu_2}. \tag{B9}$$

An upper bound on the number of errors associated with the single-photon detection events is given in Refs. [30,31]:

$$r_{1,1}^{\mathrm{ub}} = \min\left\{ \left\lceil \frac{\gamma_3'}{(\mu_2 - \mu_3)^2} \right\rceil, \left\lceil \frac{s_{1,1}^{\mathrm{lb}}}{2} \right\rceil \right\}, \tag{B10}$$

where

$$\gamma_3' := \xi^{\mu_2,\mu_2}\tilde{m}^{\mu_2,\mu_2} + \xi^{\mu_3,\mu_3}\tilde{m}^{\mu_3,\mu_3} - \xi^{\mu_2,\mu_3}\tilde{m}^{\mu_2,\mu_3} - \xi^{\mu_3,\mu_2}\tilde{m}^{\mu_3,\mu_2}. \tag{B11}$$

At this point, Eqs. (B7) and (B10) are given in terms of $\tilde{n}^{u,v}$ and $\tilde{m}^{u,v}$, which are expected values. To rewrite the equations in terms of the observed values, we use Eqs. (B2) and (B4) to get

$$n^{u,v} - \sqrt{\nu n} < \tilde{n}^{u,v} < n^{u,v} + \sqrt{\nu n}, \tag{B12}$$

$$m^{u,v} - \sqrt{\nu m} < \tilde{m}^{u,v} < m^{u,v} + \sqrt{\nu m}, \tag{B13}$$

for all $u,v \in \mathcal{I}$. Thus for a given security parameter $\nu > 0$, the error probability for these inequalities is $\exp(-2\nu)$. In other words, each of the above inequalities holds with probability at least $1 - \exp(-2\nu)$. Note that Eqs. (B7) and (B10) use seven estimators and four estimators, respectively.

Finally, by applying Eqs. (B12) and (B13) to Eqs. (B7) and (B10), we arrive at the main equations for Protocol II, Eqs. (5) and (6).

[1] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, Lect. Notes Comput. Sci. **5677**, 391 (2009).

[2] A. Kent, R. Beausoleil, W. Munro, and T. Spiller, US patent US20067075438 (2006).

[3] A. Kent, W. J. Munro, and T. P. Spiller, Phys. Rev. A **84**, 012326 (2011).

[4] A. Kent, Phys. Rev. A **84**, 022335 (2011).

[5] R. A. Malaney, Phys. Rev. A **81**, 042319 (2010); R. Malaney, in *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE* (IEEE, New York, 2011).

[6] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, SIAM J. Comput. **43**, 150 (2014).

[7] K. Chakraborty and A. Leverrier, Phys. Rev. A **92**, 052304 (2015).

[8] L. Vaidman, Phys. Rev. Lett. **90**, 010402 (2003).

[9] S. R. Clark, A. J. Connor, D. Jaksch, and S. Popescu, New J. Phys. **12**, 083034 (2010).

[10] H. K. Lau and H. K. Lo, Phys. Rev. A **83**, 012322 (2011).

[11] S. Beigi and R. König, New J. Phys. **13**, 093036 (2011).

[12] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, New J. Phys. **15**, 103002 (2013).

[13] J. Ribeiro and F. Grosshans, arXiv:1504.07171.

[14] B. Qi and G. Siopsis, Phys. Rev. A **91**, 042337 (2015).

[15] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. Leeb, and A. Zeilinger, IEEE J. Sel. Top. Quantum Electron. **9**, 1541 (2003).

[16] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[17] H. K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[18] A preliminary proposal was made in B. Qi, H.-K. Lo, C. C.-W. Lim, G. Siopsis, E. A. Chitambar, R. Pooser, P. G. Evans, and W. Grice, in *Proceedings of the 2015 IEEE International Conference on Space Optical Systems and Applications (ICSOS), New Orleans, LA* (IEEE, New York, 2015), pp. 1–6.

[19] W. Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); H. K. Lo, X. Ma, and K. Chen, *ibid.* **94**, 230504 (2005); X. B. Wang, *ibid.* **94**, 230503 (2005).

[20] In fact, it suffices to assume that the verifiers share an authenticated classical channel: they can perform sifting (as in QKD) to postselect measurement outcomes with matching bases.

[21] L. Vaidman and N. Yoran, Phys. Rev. A **59**, 116 (1999).

[22] N. Lütkenhaus, J. Calsamiglia, and K. A. Suominen, Phys. Rev. A **59**, 3295 (1999).

[23] C. Helstrom, J. Stat. Phys. **1**, 231 (1969).

[24] L. Vandenberghe and S. Boyd, SIAM Rev. **38**, 49 (1996).

[25] A. Cosentino, Phys. Rev. A **87**, 012321 (2013).

[26] C. C. W. Lim, Phys. Rev. A **93**, 020101(R) (2016).

[27] W. Hoeffding, J. Am. Stat. Assoc. **58**, 13 (1963).

[28] Y. Zhao, B. Qi, and H. K. Lo, Appl. Phys. Lett. **90**, 044106 (2007).

[29] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

[30] F. Xu, M. Curty, B. Qi, and H. K. Lo, New J. Phys. **15**, 113007 (2013); F. Xu, H. Xu, and H. K. Lo, Phys. Rev. A **89**, 052333 (2014).

[31] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H. K. Lo, Nat. Commun. **5**, 3732 (2014).

[32] Y. L. Tang *et al.*, Phys. Rev. X **6**, 011024 (2016).

[33] D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comput. **5**, 325 (2004).

[34] K. Tamaki, M. Curty, G. Kato, H. K. Lo, and K. Azuma, Phys. Rev. A **90**, 052314 (2014).

[35] Z. Q. Yin, Chi-Hang Fred Fung, X. Ma, C. M. Zhang, H. W. Li, W. Chen, S. Wang, G. C. Guo, and Z. F. Han, Phys. Rev. A **88**, 062322 (2013).

[36] Z. Q. Yin, Chi-Hang Fred Fung, X. Ma, C. M. Zhang, H. W. Li, W. Chen, S. Wang, G. C. Guo, and Z. F. Han, Phys. Rev. A **90**, 052319 (2014).