Single-Qubit Loss-Tolerant Quantum Position Verification Protocol Secure against Entangled Attackers

Llorenç Escolà-Farràs and Florian Speelman
QuSoft, CWI Amsterdam, Science Park 123, 1098 XG Amsterdam, The Netherlands
and Multiscale Networked Systems (MNS), Informatics Institute,
University of Amsterdam, Science Park 904, 1098 XH Amsterdam, The Netherlands

(Received 14 March 2023; accepted 17 August 2023; published 6 October 2023)

We give a tight characterization of the relation between loss tolerance and error rate of the most popular protocol for quantum position verification, which is based on BB84 states. Combining it with classical information, we show, using semidefinite programming, for the first time a fault-tolerant protocol that is secure against attackers who preshare a linear amount of entanglement (in the classical information), arbitrarily slow quantum information and that tolerates a certain amount of photon loss. We also extend this analysis to the case of more than two bases, showing even stronger loss tolerance for that case. Finally, we show that our techniques can be applied to improve the analysis of one-sided device-independent quantum key distribution protocols.

DOI: 10.1103/PhysRevLett.131.140802

Introduction.—Securely finding out a party's location (position verification) or writing messages that can only be read at a certain location are potentially impactful tasks part of the field of *position-based cryptography*. These tasks are unachievable using only classical information, because a general attack exists even when using computational assumptions [1]. Because of the no-cloning theorem [2] the general classical attack does not apply if quantum information is used instead [3,4], however, a general quantum attack exists which requires exponential entanglement [5,6]. This means that hope for protocols secure against reasonable amounts of entanglement is alive, and indeed there has been much analysis on attacks on specific protocols [3,7–15], and security analysis under extra assumptions, such as the random oracle model [16–18].

One of the simplest and best-studied quantum position verification (QPV) protocols [3,7], which constitutes the basis of this work, is based on BB84 states. This protocol is secure against unentangled adversaries [5], even when multiple rounds are performed in parallel [19]. The protocol, explained in detail below, consists of one verifier (V_0) sending a BB84 state to the prover and the other verifier (V_1) sending classical information describing in which basis the prover has to measure either the computational basis or the Hadamard basis. The prover then has to broadcast the measurement outcome to both verifiers, with all communication happening at the speed of light. An extended version of this protocol, $\mathrm{QPV}^{f}_{\mathrm{BB84}}$, combines $2n$ classical bits from both verifiers to determine the basis in which to measure the qubit, and this version can be proven to require an amount of entanglement that grows with the classical information, making it an appealing candidate to aim toward implementation [20].

Applying QPV experimentally encounters implementation problems, of which two are large enough that they fundamentally force us to redesign our protocols. Whereas the transmission of classical information without loss at the speed of light is technologically feasible, e.g., via radio waves, the quantum counterpart faces obstacles. First, most QPV protocols require quantum information to be transmitted at the speed of light in vacuum, but for practical applications this is often unattainable, e.g., the speed of light in optical fibers is significantly lower than in vacuum. Second, a sizable fraction of photons is lost in transmission in practice. For this loss problem, we can distinguish two recent approaches. The first is to create protocols which are secure against any amount of loss, which we can call fully loss-tolerant protocols [21]. These protocols could be excellent realistic candidates for an implementation of QPV, but in the longer term they have two shortcomings: they are not secure against much entanglement, and they require fast transmission of quantum information [22,23].

In the current work, we therefore advance another approach, by bounding the combination of loss rate and error rate that an attacker can achieve, and thereby constructing what we may call partially loss-tolerant protocols; in particular, we are able to extend the security of the $\mathrm{QPV}_{\mathrm{BB84}}$ and $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ protocols to the lossy case. For attackers that do not preshare entanglement, but that are allowed to perform local operations and a single simultaneous round of quantum communication (LOBQC) [14], we give a tight characterization of the relation between the allowed error and loss for $\mathrm{QPV}_{\mathrm{BB84}}$. Importantly, we are able to also show that these results can be adapted to show entanglement lower bounds for the lossy version of

$\mathrm{QPV}^{f}_{\mathrm{BB84}}$, and we therefore obtain a QPV protocol that is secure against partial loss and against attackers who preshare roughly $n/2$ entangled qubits. Nevertheless, the above protocols have a loss tolerance of at most ∼3 dB. To bypass this, we show that if the verifiers encode the qubit in $m \geq 3$ bases in the Bloch sphere, the protocol becomes more loss tolerant, showing a trend of security for a transmission rate above $1/m$ for unentangled attackers, which extends to entangled attackers (with slightly worse loss tolerance).

In particular, we show that, for $m = 5$, the protocol is loss tolerant even if the attackers preshare a linear amount of entanglement in the classical information n and 70% of the photons are lost. In practice, if telecom wavelength (∼1550 nm) single-photon sources are used, and the photons are sent through optical fibers with a loss of 0.15 dB/km [24], that translates to a feasible distance of around 35 km (slightly reduced by the detector efficiency). This means that for example, if each verifier sends 1 kB of classical information, the protocol is secure against attackers who preshare a state of at most 4×10^3 entangled qubits. In the present work, we solve the semidefinite programming (SDPs) for the complete range of error for $m = 3, 5$, thereby obtaining an exhaustive characterization for these cases. In order to implement secure QPV for longer distances than 35 km, it is possible to solve the presented SDP (see Supplemental Material [25]) for larger m, according to the requirements of the experimental setup.

Finally, we describe how our techniques can also be applied to improve the analysis of one-sided device-independent quantum key distribution (QKD) protocols. We achieve our results by finding semidefinite programming bounds for lossy versions of monogamy-of-entanglement (MoE) games, using techniques that could be of interest in finding bounds for other quantum-cryptographic primitives in the presence of realistic transmission errors.

Preliminaries.—Throughout this work, we will use the following notation: for $n \in \mathbb{N}$, f is a Boolean function $f\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Basis 0 and 1 denote computational and Hadamard basis, respectively. The Hadamard transformation is denoted by H. When clear from the context, tensor products and identity matrices will be omitted and also quantum states in the expected value between brackets, e.g., $\langle\psi|\mathbb{I} \otimes A|\psi\rangle = \langle A\rangle$, where A is an observable and $|\psi\rangle$ a quantum state. $\mathcal{D}(\cdot,\cdot)$ denotes the trace distance. $\mathbb{E}$ denotes the expected value, and $\mathbf{1}_*(\mathbf{a}) = 1$ if $* = a$ and 0 otherwise is the indicator function. For a random variable X, taking values on a finite set $\mathfrak{X} = \{\mathsf{x}_1, \ldots, \mathsf{x}_d\}$, a probability distribution p is specified by $p_{\mathsf{x}_i} = \Pr[X = \mathsf{x}_i], \mathsf{x}_i \in \mathfrak{X}$, and p can be represented by a probability vector $\mathbf{p} = (p_{\mathsf{x}_1}, \ldots, p_{\mathsf{x}_d})$. The set of all probability distributions $\mathbf{p}$ over $\mathfrak{X}$ is $\Delta_{d-1} = \{\mathbf{p} \in \mathbb{R}^d | \sum_{\mathsf{x}_i \in \mathfrak{X}} p_{\mathsf{x}_i} = 1, p_i \geq 0\}$, which is known as the probability simplex, and it is a $(d-1)$-dimensional manifold.

The $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$ *protocol and its general attack.*—A generic one-dimensional (the main ideas generalize to higher dimensions) QPV protocol is described in the following way: two verifiers V_0 and V_1, placed on the left and right of P, send quantum and classical messages to P at the speed of light, and she has to pass a challenge and reply correctly to them at the speed of light as well. The verifiers are assumed to have perfectly synchronized clocks and if any of them receives a wrong answer or the timing does not correspond with the time it would have taken for light to travel back from the honest prover, the verifiers abort the protocol. Moreover, the time consumed by the prover to perform the challenge is assumed to be negligible.

We introduce a variation of $\mathrm{QPV}_{\mathrm{BB84}}$ where we consider that the quantum information sent through the quantum channel between V_0 and P can be lost. Let η be the transmission rate of this channel. We also consider that an honest party is assumed to have error rate p_{err}, and thus will also respond with a wrong answer sometimes. This error can arise, for example, either from measurement errors or from noise in the quantum channel where the qubit is sent through. We define one round of the lossy-function-BB84 QPV protocol, denoted by $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$, as follows:

Definition 1.—One round of $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$ consists of the following: (1) V_0 and V_1 secretly agree on two random bit strings $x, y \in \{0,1\}^n$, and V_0 prepares the EPR pair $|\Phi^+\rangle$. (2) V_0 sends one qubit Q of $|\Phi^+\rangle$ and x to P, and V_1 sends y to P, coordinating their times so that Q, x and y arrive at P at the same time. The classical information is required to travel at the speed of light, however, the quantum information can be sent arbitrarily slow. (3) Immediately, P measures Q in the basis $f(x,y)$ and broadcasts her outcome to V_0 and V_1. If the photon is lost, she sends $\perp$. (4) Verifier V_0 performs the measurement $\{V_0^{f(x,y)}, V_1^{f(x,y)}\}$, where $V_i^{f(x,y)} = H^{f(x,y)}|i\rangle\langle i|H^{f(x,y)}$, $i \in \{0,1\}$ to their half of the Einstein-Podolsky-Rosen (EPR) pair. Let a and b denote answers that V_0 and V_1 receive, respectively. If both a and b arrive on time and $a = b$, the verifiers record "C", "$\perp$", and "W", if the responses are correct (i.e., matching V_0's measurement outcome), $\perp$ or wrong, respectively. If either a or b do not arrive on time or $a \neq b$, the verifiers output '↯' (abort).

The protocol $\mathrm{QPV}^{\eta,f}_{\mathrm{BB84}}$ consists of sequentially executing r rounds.

The above description corresponds to the purified version of the originally stated $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ (for $\eta = 1$), which is equivalent to it. In every round, an honest party will reproduce outcomes such that the verifiers will record "C", "$\perp$", "W", and "↯" with probability $p_{\mathrm{C}} = \eta(1 - p_{\mathrm{err}})$, $p_\perp = 1 - \eta$, $p_{\mathrm{W}} = \eta p_{\mathrm{err}}$, and $p_{↯} = 0$, respectively. This defines a probability vector $\mathbf{p} = (p_{\mathrm{C}}, p_\perp, p_{\mathrm{W}}, p_{↯})$. For $\eta = 1$, $p_{\mathrm{err}} = 0$, $y \in \{0,1\}$ and $f(x,y) = y$, one recovers $\mathrm{QPV}_{\mathrm{BB84}}$ [3].

The most general attack to a one-dimensional QPV protocol is to place an adversary between V_0 and the prover, Alice, and another adversary between the prover and V_1,

Bob. Let q be the number of qubits that Alice and Bob each have as part of some preshared state at the beginning of the protocol. A general attack of the ith round of $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$ consists of the following: (1) Alice intercepts the qubit Q and applies an arbitrary quantum operation to it and to her qubits, possibly entangling them. She keeps part of the resulting state, q qubits at most, and sends the rest to Bob. Since the qubit Q can be sent arbitrarily slow by V_0 (the verifiers only time the classical information), this happens before Alice and Bob can intercept x and y. At this stage, Alice, Bob, and V_0 share a quantum state $|\psi^i\rangle$ of $2q+2$ qubits. (2) Alice intercepts x and Bob intercepts y, and they apply a unitary $U_A^{i,x}$ and $U_B^{i,y}$ on their local registers, respectively. Alice sends a part of her local state and x to Bob, and Bob sends a part of his local state and y to Alice. Denote by $\rho^{i,xy}$ their joint state. (3) Each party performs a POVM $\{A_a^{i,xy}\}$ and $\{B_b^{i,xy}\}$, $a,b\in\{0,1,\perp\}$, on their registers and they send their outcomes a and b to V_0 and V_1, respectively.

The tuple $\{\rho^{i,xy},A_a^{i,xy},B_b^{i,xy}\}_{x,y,a,b}=:S^i$, where $\rho^{i,xy}$ is described by $|\psi^i\rangle$ and $U_A^{i,x}$ and $U_B^{i,y}$, will be called a "(q-qubit) strategy." In every round of the protocol, the attackers will pick a strategy S^i that can depend on the previous rounds. A strategy S^i will induce a probability vector $\mathbf{q}^i=(q_{\mathrm{C}}^i,q_{\perp}^i,q_{\mathrm{W}}^i,q_{\lightning}^i)$, where the subscripts have the same interpretation as above and the probabilities are given by

$$
\begin{aligned}
q_{\mathrm{C}}^i &= \sum_{a\in\{0,1\},x,y}\mathrm{Tr}[\rho^{i,xy}V_a^{f(x,y)}A_a^{i,xy}B_a^{i,xy}]/2^{2n},\\
q_{\perp}^i &= \sum_{x,y}\mathrm{Tr}[\rho^{i,xy}A_{\perp}^{i,xy}B_{\perp}^{i,xy}]/2^{2n},\\
q_{\mathrm{W}}^i &= \sum_{a\in\{0,1\},x,y}\mathrm{Tr}[\rho^{i,xy}V_a^{f(x,y)}A_{1-a}^{i,xy}B_{1-a}^{i,xy}]/2^{2n},\\
q_{\lightning}^i &= \sum_{a\neq b\in\{0,1,\perp\},x,y}\mathrm{Tr}[\rho^{i,xy}A_a^{i,xy}B_b^{i,xy}]/2^{2n}.
\end{aligned}
$$

An attack is *successful* if the verifiers cannot distinguish if their data came from the distribution $\mathbf{p}\ldots\mathbf{p}$ (r times) or from $\mathbf{q}^1\ldots\mathbf{q}^r$.

Exact loss-tolerance and sequential repetition of $\mathrm{QPV}_{\mathrm{BB84}}^{\eta}$.—Whereas $\mathrm{QPV}_{\mathrm{BB84}}$ can be perfectly broken by attackers who preshare one EPR pair, in [33] it was proven its security against unentangled attackers. Later on, introducing MoE games [19], see below, it was shown that the optimal probability that the attackers are correct is $q_{\mathrm{C}}=\cos^2(\pi/8)$, achieved by the strategy $S_{\mathrm{TKFW}}=\{|\phi\rangle\langle\phi|,A_a^y=\delta_{a0},B_a^y=\delta_{a0}\}$ (the subscript refers to the author's names) where $|\phi\rangle=\cos(\pi/8)|0\rangle+\sin(\pi/8)|1\rangle$, leading to $\mathbf{q}_{\mathrm{TKFW}}=[\cos^2(\pi/8),0,\sin^2(\pi/8),0]$. The general attack to $\mathrm{QPV}_{\mathrm{BB84}}$ for unentangled attackers is described as above with $q=0$. Notice that, since they share no entanglement, any quantum operation that Bob could perform as a function of y in step 2 can be included in Alice's operation (see, e.g., [5,19]). Moreover, the fact that $q=0$ does not restrict the dimension of the state ρ in step 3, since Alice can have arbitrary local ancillary systems.

Consider the *lossy*-$\mathrm{QPV}_{\mathrm{BB84}}$ protocol, recovered for $f(x,y)=y\in\{0,1\}$ in $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$. On the one hand, S_{TKFW} is an optimal attack for $\eta=1$, if $q=0$. On the other hand, let Alice make a random guess $\tilde{y}$ for y, measure the qubit Q in the $\tilde{y}$ basis and broadcast the outcome and $\tilde{y}$ to Bob. After one round of simultaneous communication with Bob, they both know if the guess was correct. If so, they send the outcome to the verifiers, otherwise, they claim no photon arrived. Alice's basis guess will be correct half of the time and therefore, if $\eta\leq\frac{1}{2}$, the attackers will be correct whenever they answer. We denote this strategy by S_{guess}, which leads to $\mathbf{q}_{\mathrm{guess}}=(\frac{1}{2},\frac{1}{2},0,0)$.

Our security approach will be based on what we introduce as a *lossy* MoE game with parameter $\eta\in[0,1]$ (the range of $\eta\leq\frac{1}{2}$ will become relevant when extending the protocol), which is a generalization of a MoE game.

Definition 2.—A *lossy* MoE game with parameter $\eta\in[0,1]$ consists of a finite dimensional Hilbert space $\mathcal{H}_V$, corresponding to party V, and a list of measurements $\{V_v^y\}_{v\in\mathcal{V}}$ on $\mathcal{H}_V$, indexed by $y\in\mathcal{Y}$, where $\mathcal{V}$ and $\mathcal{Y}$ are finite sets. Two collaborative parties, Alice and Bob, with associated Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, prepare an arbitrary quantum state ρ_{VAB} and send ρ_V to V, holding on ρ_A and ρ_B, respectively. V chooses $y\in\mathcal{Y}$ uniformly at random and measures ρ_V using $\{V_v^y\}$ to obtain the measurement outcome v. Then she announces y to Alice and Bob. The collaborative parties make a guess of v and they win the game if and only if both either guess v correctly or their strategy or they both respond $\perp$ with probability $1-\eta$. That is, for any strategy $\{\rho_{VAB},A_v^y,B_v^y\}_{v\in\mathcal{V}\cup\{\perp\},y\in\mathcal{Y}}$, where ρ_{VAB} is a density operator on $\mathcal{H}_V\otimes\mathcal{H}_A\otimes\mathcal{H}_B$ and for all $y\in\mathcal{Y}$, $\{A_v^y\}_{v\in\mathcal{V}\cup\{\perp\}}$ and $\{B_v^y\}_{v\in\mathcal{V}\cup\{\perp\}}$ are POVMs on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, and $(1/|\mathcal{Y}|)\sum_{y\in\mathcal{Y}}\mathrm{Tr}[\rho_{VAB}\mathbb{I}\otimes A_{\perp}^y\otimes B_{\perp}^y]=1-\eta$.

In [19] it is shown that any strategy can be purified in the sense that, enlarging the corresponding Hilbert spaces if necessary, $\rho_{VAB}=|\phi\rangle\langle\phi|$ is a pure state for $|\phi\rangle\in\mathcal{H}_V\otimes\mathcal{H}_A\otimes\mathcal{H}_B$ and $\{A_v^y\}$, $\{B_v^y\}$ are projective measurements, which, from now on, we will assume to be the case. In a similar way as in [19], having a strategy to break $\mathrm{QPV}_{\mathrm{BB84}}^{\eta}$ implies having a strategy for the lossy MoE game where V corresponds to the verifiers with associated Hilbert space $\mathcal{H}_V=\mathbb{C}^2$, with $\mathcal{Y}=\{0,1\}$ and $\mathcal{V}=\{0,1\}$, who perform the collection of measurements $\{V_0^y,V_1^y\}_{y\in\{0,1\}}$. We will bound the probability that the attackers are correct by numerically maximizing their probability of *answer* (not responding $\perp$) in the above lossy MoE game. We want to find the maximum of $q_{\mathrm{C}}+q_{\mathrm{W}}$ given that $q_{\lightning}=0$ (otherwise

the verifiers abort) and a probability of error p_{err}. The advantage of this approach is that $q_{\text{C}} + q_{\text{W}} = \frac{1}{2}\sum_{y,a\in\{0,1\}}\langle A_a^y B_a^y\rangle$ no longer depends on V_i^y but only on the state and the measurements that the verifiers use. The amount $q_{\text{C}} + q_{\text{W}}$ has the interpretation of the probability that the attackers *answer* a round without being caught.

Let $\mathcal{Q}$ be the set of probabilities attained by quantum mechanics. Navascués, Pironio, and Acín (NPA) [34] introduced a recursive way to construct a hierarchy of subsets $\mathcal{Q}_\ell \supset \mathcal{Q}_{\ell+1} \supset \mathcal{Q}$ for all $\ell \in \mathbb{N}$ with the property that each of them can be tested using SDP and are such that $\cap_{\ell\in\mathbb{N}}\, \mathcal{Q}_\ell = \mathcal{Q}$, where ℓ corresponds to the so-called level of the NPA hierarchy, see Supplemental Material [25], Sec. A. Combining the NPA hierarchy with extra linear equations involving V_i^y, we present a semidefinite program (SDP) that upper bounds the value of $q_{\text{C}} + q_{\text{W}}$, which is actually tight. With this bound, since $q_{\text{C}} + q_{\text{W}} + q_\perp = 1$, we also find the corresponding $q_\perp^*$, where $*$ denotes optimal, providing the optimal η that the attackers can reproduce, i.e., $q_\perp^* = 1 - \eta$. Moreover, $q_{\text{W}|\not\perp} = p_{\text{err}}$, where $|\not\perp$ denotes conditioned on answering (since the attackers want to mimic what an honest prover would do), and therefore, $q_{\text{C}|\eta}^* = (1 - p_{\text{err}})/(1 - q_\perp^*)$, which denotes the optimal probability of being correct if they answer (given that they have to answer with probability η). In an analogy to [19], this quantity corresponds to the *winning* probability of the lossy-MoE game, recovering their definition for $\eta = 1$.

The elements $\langle A_a^y B_b^{y'}\rangle$, $\forall\ a,\ b \in \{0,1,\perp\}$, $\forall\ y, y' \in \{0,1\}$, will appear in the maximization problem solvable via SDP, and are bounded by linear constraints given by $\mathcal{Q}_\ell$. In addition to these constraints, we impose several additional linear constraints derived from $\text{QPV}_{\text{BB84}}^{\eta}$, i.e., $q_{\not z} = 0$, which imply

$$\langle A_a^y B_b^y\rangle = 0 \quad \forall\ a \neq b \in \{0,1,\perp\}, \quad \forall\ y \in \{0,1\}, \tag{1}$$

and the prover subject to a measurement error p_{err}, see Proposition 1.

Proposition 1.—Let $a, b \in \{0,1\}$ and $\tilde{y} \in \{y, y'\}$, where $y, y' \in \{0,1\}$. Then,

$$\sum_{ab}(2 - \|V_a^y + V_b^{y'}\|)\langle A_a^y B_b^{y'}\rangle \leq p_{\text{err}}\sum_{a,\tilde{y}}\langle A_a^{\tilde{y}} B_a^{\tilde{y}}\rangle. \tag{2}$$

For every level ℓ of the NPA hierarchy, the following SDP provides an upper bound of $q_{\text{C}} + q_{\text{W}}$:

$$\max \frac{1}{2}\sum_{y,a\in\{0,1\}}\langle A_a^y B_a^y\rangle;$$

such that the linear constraints of level ℓ of the NPA hierarchy and Eqs. (1) and (2). (3)

The numerical results for the level "$1 + AB$", see code [35], provide a nontrivial upper bound to $q_{\text{C}}^* + q_{\text{W}}^*$, and, due to the above reasoning, this translates to an upper bound to $q_{\text{C}|\eta}^*$, which we denote by $w(\eta)$, i.e., $q_{\text{C}|\eta}^* \leq w(\eta)$, see Fig. 1 for a numerical representation of $w(\eta)$. Moreover, the results are tight, since the upper bound is reached by the strategy consisting of playing the convex combination of S_{TFKW}, with probability $(2\eta - 1)$, and S_{guess}, with probability 2η. In Fig. 2 there are represented the numerical solutions in the form of $\mathbf{q} = (q_{\text{C}}, q_\perp, q_{\text{W}} + q_{\not z}) \in \Delta_2$, which coincide with the straight line given by the two points $\mathbf{q}_{\text{TKFW}}$ and $\mathbf{q}_{\text{guess}}$, which corresponds to the convex combinations of the two above strategies. This is wrapped up in the following result.

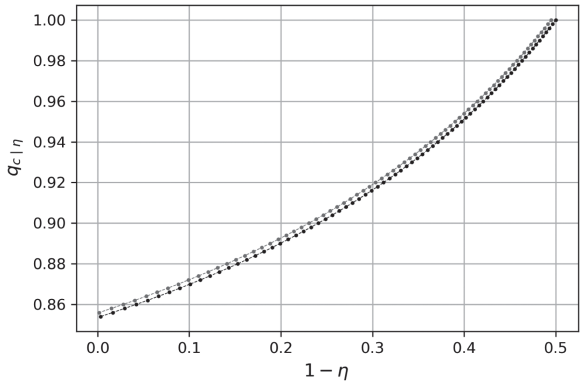

FIG. 1. Numerical representation of the functions $w(\eta)$ (black dots) and $\tilde{w}^{\xi}(\eta)$ (gray dots) obtained by SDPs.

Result 1.—Given that the (nonentangled) attackers answer with probability η and never respond inconsistent answers, the optimal probability that they are correct in a round of $\text{QPV}_{\text{BB84}}^{\eta}$ for $\eta \in [\frac{1}{2}, 1]$ is

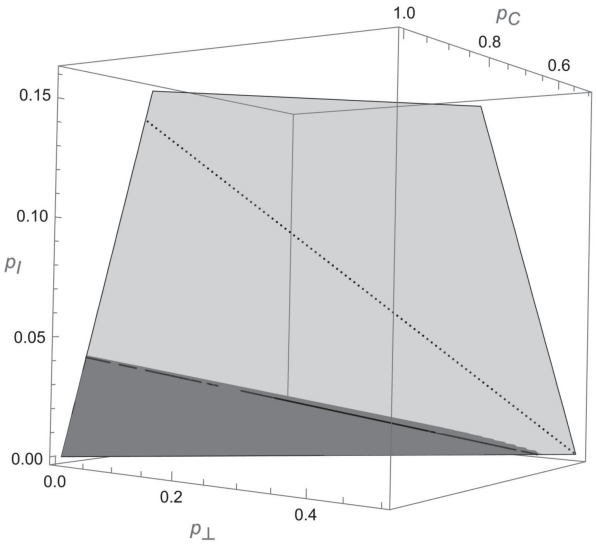

FIG. 2. Probability simplex Δ_2 for probabilities taking values on $\mathfrak{X} = \{\text{C}, \perp, \text{I}\}$. Black dots correspond to numerical solutions of (3) for $\ell = 2$. The dark region is the set of probabilities that Theorem 2 excludes and the black straight line is the intersection between Δ_2 and the plane $\gamma_{\text{C}} p_{\text{C}} - \gamma_\perp p \gamma_\perp - \gamma_{\text{I}} p_{\text{I}} = 0$.

$$q_{\mathrm{C}}^{*}=\cos^2\left(\frac{\pi}{8}\right)\eta+\sin^2\left(\frac{\pi}{8}\right)(1-\eta). \tag{4}$$

After r sequential rounds, the verifiers have to decide to either accept or reject the prover's location. Consider the following relaxation where the verifiers categorize wrong and abort answers identically, i.e., they count them as incorrect (I) answers. Denote by $\mathbf{a}_i \in \{\mathrm{C}, \perp, \mathrm{I}\}$ whether the answer they recorded in round i was correct, no photon, or incorrect. Consider the following payoff function $T_i(\mathbf{a}_i) = \sin^2(\pi/8)\mathbf{1}_{\mathrm{C}}(\mathbf{a}_i) - \sin^2(\pi/8)\mathbf{1}_{\perp}(\mathbf{a}_i) - \cos^2(\pi/8)\mathbf{1}_{\mathrm{I}}(\mathbf{a}_i)$, for every round i of the protocol. Let $\Gamma_r = \sum_{i=1}^{r} T_i(\mathbf{a}_i)$ be the total "score" after r rounds. For an honest prover (HP), for every i, $\mathbb{E}[T_i^{\mathrm{HP}}] = \sin^2(\pi/8)\eta(1-p_{\mathrm{err}}) - \sin^2(\pi/8)(1-\eta) - \cos^2(\pi/8)\eta p_{\mathrm{err}} =: \alpha(\eta, p_{\mathrm{err}})$, and therefore $\mathbb{E}[\Gamma_r^{\mathrm{HP}}] = r\alpha$ for simplicity we will assume the dependence on η and p_{err} implicit. Similarly, let Γ_r^{att} denote the total score that the attackers (att) get.

Theorem 1.—Let η and p_{err} be such that $\alpha > 0$. Then, any sequential strategy that attackers who do not preshare entanglement but are allowed to do LOBQC to break $\mathrm{QPV}_{\mathrm{BB84}}^{\eta}$ fulfills that $\mathbb{E}[\Gamma_r^{\mathrm{att}}] \leq 0$. Moreover, the probability that the attackers obtain a total score $r\alpha$, which is the expected value for an honest prover, is exponentially small: $\Pr[\Gamma_r^{\mathrm{att}} \geq r\alpha] \leq e^{-r\alpha^2/2}$.

Theorem 1 shows that there is a way to distinguish $\mathbf{p}\ldots\mathbf{p}$ from $\mathbf{q}^1\ldots\mathbf{q}^r$ with exponentially high probability, i.e., that after r rounds the attackers will be *caught*. The points (η, p_{err}) such that $\alpha > 0$ correspond to the points below $w(\eta)$ in Fig. 1 and also below the black dots in Fig. 2.

Security of $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$ *against entangled attackers.*—For our security approach, consider the relaxation where the attackers are allowed to respond different answers with probability ξ and have a response rate in the interval $[(1-\eta)-\xi, (1-\eta)+\xi]$. Fix $\xi = 0.005$ and replace the linear constraints (3) and (2) in the SDP (3) by $\langle A_a^y B_b^y\rangle \leq \xi \;\forall\; a \neq b \in \{0,1,\perp\},\;\forall\; y \in \{0,1\}$, and $\sum_{ab}(2 - \|V_a^y + V_b^{y'}\|)\langle A_a^y B_b^{y'}\rangle \leq p_{\mathrm{err}}\sum_a(4\xi + \langle A_a^y B_a^y\rangle + \langle A_a^{y'} B_a^{y'}\rangle)$. Adding ξ to the solution of this semidefinite programming, see [35], we find a nontrivial bound $\tilde{w}^{\xi}(\eta)$ on the optimal probability of being correct with the above relaxation. See Fig. 1 for a numerical representation of $\tilde{w}^{\xi}(\eta)$.

Definition 3.—We say that a state $|\phi\rangle$ is (Δ, η) good on input j, for $\Delta > 0$ if there exists positive operator-valued measure (POVMs) $\{A_a^{xy}\}$ and $\{B_b^{xy}\}$, $a, b \in \{0, 1, \perp\}$ such that its corresponding probability of being correct given that $f(x, y) = j$ is greater than or equal to $\tilde{w}^{\xi}(\eta) + \Delta$.

Lemma 1.—Let $|\phi_0\rangle$ and $|\phi_1\rangle$ be (Δ, η) good on inputs 0 and 1, respectively. Then, $\mathcal{D}(|\phi_0\rangle, |\phi_1\rangle) \geq \eta\Delta$.

Notice that Lemma 1 implies that the attackers cannot use a state that is simultaneously (Δ, η) good for both inputs 0 and 1. This implies that Alice and Bob in some sense have to decide what strategy they follow before they communicate. Consequently, if the dimension of the state they share is small enough, a classical description of the first part of their strategy yields a *compression* of f. Lemma 1 allows us to redo a similar proof as in [20] using a counting argument with ε-nets that leads to the following theorem:

Theorem 2.—Let $\Delta = 0.013$. If the number of qubits that the attackers preshare at the beginning of $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$ for $\eta \in [0.53, 1]$ is such that $q \leq n/2 - 5$, then, a uniformly random function f fulfills the following with probability at least $1 - 2^{-2^n}$:

$$q_{\mathrm{C}|\eta}^{*} < \frac{1}{4}(1 - (\tilde{w}^{\xi}(\eta) + \Delta)). \tag{5}$$

See Fig. 2 for the set of probabilities in Δ_2 excluded by Theorem 2. Analogously to $\mathrm{QPV}_{\mathrm{BB84}}^{\eta}$, security for sequential repetition follows from the payoff function for entangled (ent) attackers $T_i^{\mathrm{ent}}(\mathbf{a}_i) = \gamma_{\mathrm{C}}\mathbf{1}_{\mathrm{C}}(\mathbf{a}_i) - \gamma_{\perp}\mathbf{1}_{\perp}(\mathbf{a}_i) - \gamma_{\mathrm{I}}\mathbf{1}_{\mathrm{I}}(\mathbf{a}_i)$, where $(\gamma_{\mathrm{C}}, \gamma_{\perp}, \gamma_{\mathrm{C}}) = (1/\sqrt{488625947})(943, 1107, 22057)$. Theorem 1 is recovered for entangled attackers with $q \leq n/2 - 5$ for $\alpha^{\mathrm{ent}} := \gamma_{\mathrm{C}}\eta(1-p_{\mathrm{err}}) - \gamma_{\perp}(1-\eta) - \gamma_{\mathrm{I}}\eta p_{\mathrm{err}}$. The values for which $\alpha^{\mathrm{ent}} > 0$ correspond to the points below the straight line in Fig. 2.

Extension to m bases.—We study an extension of $\mathrm{QPV}_{\mathrm{BB84}}^{\eta,f}$ where the verifiers encode the qubit in m different bases over the Bloch sphere, similarly to [36], Chap. 5, and [37]. Doing an analogous analysis as in the previous sections, we show that this translates to more loss-tolerant QPV, see Supplemental Material [25], Secs. D and E. For the numerical cases we work out ($m = 3,\ 5$),we show security for $\eta > (1/m)$ without entanglement and for $\eta \geq 0.36,\ 0.3$, respectively, against entangled attackers.

Application to QKD.—In [19] security of one-sided device-independent quantum key distribution (DIQKD) BB84 [38] was proven using a monogamy-of-entanglement game. We apply the above techniques to prove security of DIQKD, finding a range of transmission rates and errors such that the protocol is secure when one qubit is sent between the two parties distributing the key, see Supplemental Material, Sec. F [25]. However, the interesting case is the asymptotic behavior for arbitrary number of qubits, which we leave as an open question.

We thank the Dutch Ministry of Economic Affairs and Climate Policy (EZK), supporting this work as part of the Quantum Delta NL programme, and Jaume de Dios Pont for fruitful discussions about the probability simplex.

[1] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, in *Advances in Cryptology–CRYPTO 2009, 29th Annual International Cryptology Conference*, Lecture Notes in Computer Science Vol. 5677 (Springer, New York, 2009), pp. 391–407.

[2] W. K. Wootters and W. Zurek, Nature (London) **299**, 802 (1982).
[3] A. Kent, W. J. Munro, and T. P. Spiller, Phys. Rev. A **84**, 012326 (2011).
[4] R. A. Malaney, Phys. Rev. A **81**, 042319 (2010).
[5] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, SIAM J. Comput. **43**, 150 (2014).
[6] S. Beigi and R. König, New J. Phys. **13**, 093036 (2011).
[7] T. S. Adrian Kent, William Munro, and R. Beausoleil Tagging systems. US patent nr 2006/0022832, (2006).
[8] H.-K. Lau and H.-K. Lo, Phys. Rev. A **83**, 012322 (2011).
[9] J. Ribeiro and F. Grosshans, arXiv:1504.07171.
[10] K. Chakraborty and A. Leverrier, Phys. Rev. A **92**, 052304 (2015).
[11] F. Speelman, in *Proceedings of the 11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016)* (Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, Berlin, 2016).
[12] K. Dolev, arXiv:1909.05403.
[13] K. Dolev and S. Cree, arXiv:2203.10106.
[14] A. Gonzales and E. Chitambar, IEEE Trans. Inf. Theory **66**, 2951 (2019).
[15] S. Cree and A. May, Quantum **7**, 1079 (2023).
[16] D. Unruh, in *Advances in Cryptology–CRYPTO 2014*, edited by J. A. Garay and R. Gennaro (Springer Berlin Heidelberg, Berlin, Heidelberg, 2014), pp. 1–18.
[17] J. Liu, Q. Liu, and L. Qian, in *Proceedings of the 13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, Leibniz International Proceedings in Informatics (LIPIcs) Vol. 215, edited by M. Braverman (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Dagstuhl, Germany, 2022), pp. 100:1–100:11.
[18] F. Gao, B. Liu, and Q. Wen, Sci. China Phys. Mech. Astron. **59**, 1 (2016).
[19] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, New J. Phys. **15**, 103002 (2013).
[20] A. Bluhm, M. Christandl, and F. Speelman, Nat. Phys. 1 (2022).
[21] C. C. W. Lim, F. Xu, G. Siopsis, E. Chitambar, P. G. Evans, and B. Qi, Phys. Rev. A **94**, 032315 (2016).
[22] R. Allerstorfer, H. Buhrman, F. Speelman, and P. Verduyn Lunel, arXiv:2106.12911.
[23] R. Allerstorfer, H. Buhrman, F. Speelman, and P. Verduyn Lunel, arXiv:2208.04341.
[24] X. Cao, M. Zopf, and F. Ding, J. Semicond. **40**, 071901 (2019).
[25] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.131.140802 for comprehensive details, extensive results, and complete proofs, which includes Refs. [26–32].
[26] K. Azuma, Tohoku Math. J. **19**, 357 (1967).
[27] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[28] M. Ledoux and M. Talagrand, *Probability in Banach Spaces: Isoperimetry and Processes*, A Series of Modern Surveys in Mathematics Series Vol. 23 (Springer, Berlin, 1991).
[29] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library Vol. 16 (North-Holland, Amsterdam, 1977).
[30] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition* (Cambridge University Press, Cambridge, England, 2011).
[31] D. Niemietz, P. Farrera, S. Langenfeld, and G. Rempe, Nature (London) **591**, 570 (2021).
[32] E. W. Weisstein, Sphere point picking, Wolfram MathWorld, https://mathworld.wolfram.com/SpherePointPicking.html.
[33] H. Buhrman, S. Fehr, C. Schaffner, and F. Speelman, in *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science–ITCS '13* (ACM Press, Berkeley, 2013).
[34] M. Navascués, S. Pironio, and A. Acín, New J. Phys. **10**, 073013 (2008).
[35] L. Escolà-Farràs and F. Speelman, https://github.com/llorensescola/QPV_NPA_hierarchy.
[36] F. Speelman, Position-based quantum cryptography and catalytic computation, Ph.D. thesis, University of Amsterdam, 2016.
[37] B. Qi and G. Siopsis, Phys. Rev. A **91**, 042337 (2015).
[38] C. H. Bennett and G. Brassard, *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Process (Bangalore)* (IEEE, Piscataway, NJ, 1984).