



UvA-DARE (Digital Academic Repository)

Continuous-variable quantum position verification secure against entangled attackers

Escolà-Farràs, L.; Ray, A.A.; Allerstorfer, R.; Škorić, B.; Speelman, F.

DOI

[10.1103/physreva.110.062605](https://doi.org/10.1103/physreva.110.062605)

Publication date

2024

Document Version

Final published version

Published in

Physical Review A

License

Article 25fa Dutch Copyright Act (<https://www.openaccess.nl/en/policies/open-access-in-dutch-copyright-law-taverne-amendment>)

[Link to publication](#)

Citation for published version (APA):

Escolà-Farràs, L., Ray, A. A., Allerstorfer, R., Škorić, B., & Speelman, F. (2024). Continuous-variable quantum position verification secure against entangled attackers. *Physical Review A*, 110(6), Article 062605. <https://doi.org/10.1103/physreva.110.062605>

General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, P.O. Box 19185, 1000 GD Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (<https://dare.uva.nl>)

Continuous-variable quantum position verification secure against entangled attackersLlorenç Escolà-Farràs ^{1,2} Arpan Akash Ray ³ Rene Allerstorfer ¹ Boris Škorić ³ and Florian Speelman ^{1,2}¹*QuSoft and CWI Amsterdam, Amsterdam 1098 XG, The Netherlands*²*QuSoft and Informatics Institute, University of Amsterdam, Amsterdam 1098 XH, The Netherlands*³*TU Eindhoven, Eindhoven 5612 AZ, The Netherlands*

(Received 24 April 2024; revised 17 October 2024; accepted 19 November 2024; published 11 December 2024)

A continuous-variable (CV) quantum position verification (QPV) protocol was recently studied and proven to be secure if and only if attackers do not preshare any entanglement. In the discrete-variable (DV) analog of that protocol, it had been shown that modifying how the classical challenge is sent from the verifiers to the prover leads to a lower bound on the amount of entanglement needed by the attackers. In this work we show that similar conclusions can be drawn for CV QPV. We design a CV QPV protocol in which the quantum part of the challenge is a coherent state and the classical part consists of n -bit strings coming from both verifiers. We show that the protocol is secure against attackers who have fewer than cn preshared entangled qubits, where c is a constant. The security proof is given for a certain range of attenuation and excess noise and holds even if the quantum information travels arbitrarily slowly.

DOI: [10.1103/PhysRevA.110.062605](https://doi.org/10.1103/PhysRevA.110.062605)**I. INTRODUCTION**

Position-based cryptography uses the geographic location of a party as the only cryptographic credential to authenticate it, without further assumptions. For instance, to authenticate a website or online media, one could verify that the server is located where it should be or that the media were recorded where it was claimed to have been (instead of being created by AI or untrusted parties, for example). Part of position-based cryptography is the task of position verification, where an untrusted prover P aims to convince verifiers that the prover is present at a certain position P . This primitive was first introduced in [1], and it has been shown that no classical position-verification protocol can exist, due to a universal attack based on cloning input information. Quantum position verification (QPV) was thus introduced, wherein this attack would fail as quantum information cannot be cloned [2]. Quantum position verification has been studied by several authors [3–6]. Proposed QPV protocols rely on both relativistic constraints in a d -dimensional Minkowski space-time $M^{(d,1)}$ and the laws of quantum mechanics. Mostly, the case $d = 1$ is found in the literature, i.e., verifying the position of P along a single axis (by two verifiers V_0 and V_1 who are located on the left and right of P , respectively), since it makes the analysis easier and the main ideas generalize to higher dimensions. Despite the promise it offered, a universal quantum attack against QPV has since been found [7,8]. However, this attack consumes an amount of entanglement exponential in the input size and is therefore not practically feasible. Thus, we may still find secure QPV protocols in the bounded-entanglement model.

The analysis of the entanglement resources needed turns out to be a deep question in its own right [9–17]. Many protocols have since been proposed [18–23] and different security models have been studied [24–27]. Recent work has focused on the practicality of implementing position-verification

protocols. Aspects such as channel loss and error tolerance of certain QPV protocols have begun to be taken into consideration [23,27,28]. Finally, most previous QPV protocols have been based on finite-dimensional quantum systems, with the exception of those in [22,29].

Continuous-variable quantum systems are relevant for quantum communication and quantum-limited detection and imaging techniques, as they provide a quantum description of the propagating electromagnetic field. Much research has been conducted on continuous-variable (CV) quantum key distribution (QKD). Initially proposed using discrete [30–32] and Gaussian [33] representations of squeezed states, a range of techniques was subsequently introduced for Gaussian-encoded CV QKD using coherent states [34–37].

The primary advantage of CV QKD over its discrete-variable (DV) analog is practicality (see, e.g., [38]). Fundamentally, CV systems are much simpler to handle and leverage several decades of experience in coherent optical communication technology. Unlike DV systems, no true single-photon preparation or detection is necessary, which is still expensive and technically challenging (especially if photon-number resolution is desired). In contrast, homodyne and heterodyne measurements are much easier and cheaper to implement. Much existing infrastructure is geared towards handling light at low-loss telecom wavelengths (1310 and 1550 nm), whereas an ideal single-photon source in these wavelength bands still has to be discovered, and frequency up-conversion is challenging and introduces new losses and errors.

In [22] the CV analog of the QPV_{BB84} protocol [39] based on BB84 states [40] was defined and analyzed. In this article we extend the CV QPV literature by considering the CV version of the practically interesting QPV_{BB84}^f [12,28] protocol. Crucially, in QPV_{BB84}^f the classical input information is split up (into, say, x and y) and each verifier sends out either x or y .}}

The prover then applies the appropriate measurement based on the value $f(x, y)$ for the chosen protocol function f . The advantage of this is that the quantum resources required for a successful attack become larger and scale linearly in the size n of the classical input strings x and y . Thus, increasing the classical input size makes the quantum attack harder, a very favorable property of $\text{QPV}_{\text{BB84}}^f$. We are theoretically, and also potentially practically, motivated to investigate whether this property holds the same way in the CV case as well. Employing previous results from [12,22], the main takeaway of this work is that, indeed, the CV protocol shares the desired characteristics regarding entanglement attacks of the discrete-variable version. More concretely, we show that, for a random function f , the protocol remains secure against attackers who preshare CV entangled states with a cutoff at the photon number linear in n . Moreover, the protocol remains secure even if the quantum information is sent arbitrarily slowly. We also present an analysis of the protocol for nonzero levels of attenuation and excess noise in the CV channel. We provide the proofs of our results in the Appendixes.

II. PRELIMINARIES

Let $X \in \mathcal{X}$ be a continuous random variable with probability density function $f(x)$. The differential Shannon entropy $h(X)$ is defined as $h(X) = -\int_{\mathcal{X}} f(x) \log_2 f(x) dx$. Let $\tilde{h}(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ if $x \leq \frac{1}{2}$ and $\tilde{h}(x) = 1$ if $x > \frac{1}{2}$.

As introduced in [41], let ρ_{AB} be a bipartite state on systems A and B , which correspond to a system to be measured and a system held by an observer. Let X be a continuous random variable, $\alpha = 2^{-n}$ for some $n \in \mathbb{N}$, and consider the intervals $\mathcal{I}_{k;\alpha} := (k\alpha, (k+1)\alpha)$ for $k \in \mathbb{Z}$. Here $\rho_B^{k;\alpha}$ denotes the subnormalized density matrix in B when x is measured in $\mathcal{I}_{k;\alpha}$, ρ_B^x denotes the conditional reduced density matrix in B so that $\int_{\mathcal{I}_{k;\alpha}} \rho_B^x dx = \rho_B^{k;\alpha}$, and Q_α denotes the random variable that indicates which interval x belongs to. The quantum conditional von Neumann entropy is defined as $H(Q_\alpha|B)_\rho := -\sum_{k \in \mathbb{Z}} D(\rho_B^{k;\alpha} || \rho_B)$. The differential quantum conditional von Neumann entropy is defined as

$$h(X|B)_\rho := -\int_{\mathbb{R}} D(\rho_B^x || \rho_B) dx. \quad (1)$$

For our setting, we consider the Hamiltonian of the harmonic oscillator with $H = \hbar\omega\hat{N}$, with the unusual energy convention that the ground state has energy 0 instead of $\frac{1}{2}\hbar\omega$. Throughout the paper, we take units such that $\hbar\omega = 1$ (note that we will consider a fixed wavelength for an input state below).

When sent through a channel, a continuous-variable state gets attenuated and acquires excess noise. We will denote by $t \in [0, 1]$ the attenuation parameter and by $u \geq 0$ the excess noise power of the quantum channel connecting V_0 and P .

III. THE $\text{QPV}_{\text{coh}}^f$ PROTOCOL

In the QPV scheme of [22], a coherent state is sent by one verifier and a classical challenge by the other verifier, specifying in which direction the prover has to perform a

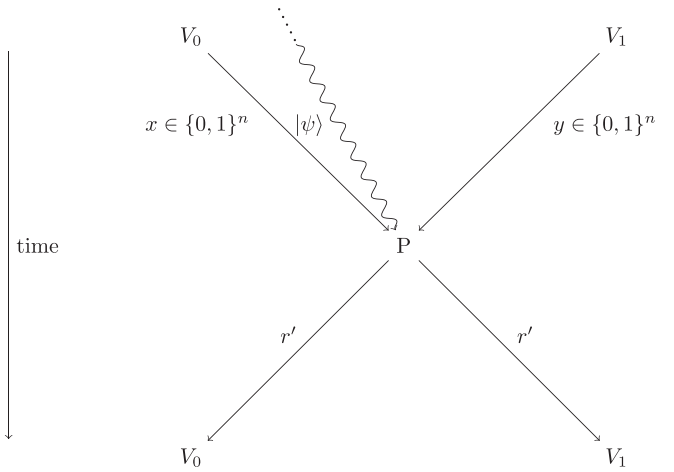


FIG. 1. Schematic representation of one round of the $\text{QPV}_{\text{coh}}^f$ protocol. The coherent state $|\psi\rangle$ originates from V_0 in the past.

homodyne measurement. We introduce a variant of [22] based on the ideas in [9,12,24]: The classical part of the challenge now comes from both verifiers.

The $\text{QPV}_{\text{coh}}^f$ protocol works as follows (see Fig. 1 for a schematic representation).

Definition 1. Let $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ be a $2n$ -bit Boolean function. A round of the $\text{QPV}_{\text{coh}}^f$ protocol consists of the following steps.

(a) The verifiers V_0 and V_1 randomly choose bit strings $x, y \in \{0, 1\}^n$, respectively. They compute $f(x, y)$ and set $\theta = \frac{\pi}{2} f(x, y)$. They draw two random variables (r, r^\perp) from the Gaussian distribution \mathcal{N}_{0,σ^2} for $\sigma \gg 1$. The verifier V_0 prepares a coherent state $|\psi\rangle$ with quadratures $(x_0, p_0) = (r \cos \theta + r^\perp \sin \theta, r \sin \theta - r^\perp \cos \theta)$.

(b) The verifier V_0 sends $|\psi\rangle$ and x to P , and V_1 sends y to P such that all information arrives at P simultaneously. The classical information is required to travel at the speed of light, whereas the quantum information can be arbitrarily slow.

(c) Immediately, P computes $\theta = \frac{\pi}{2} f(x, y)$ and performs a homodyne measurement on $|\psi\rangle$ in the direction θ , resulting in a value $r' \in \mathbb{R}$. The prover broadcasts r' to both verifiers at the speed of light.

After N rounds, the verifiers have received a sample of responses which we denote by $(r'_i)_{i=1}^N$. The verifiers check whether all responses arrived at the correct time and whether the reported values $(r'_i)_{i=1}^N$ satisfy

$$\frac{1}{N} \sum_{i=1}^N \frac{(r'_i - r_i \sqrt{t})^2}{\frac{1}{2} + u} < \gamma, \quad \gamma := 1 + \frac{2\sqrt{\ln \frac{1}{\varepsilon_h}}}{\sqrt{N}} + \frac{2 \ln \frac{1}{\varepsilon_h}}{N},$$

where ε_h is an upper bound on the honest prover's failure probability.

The excess noise can be modeled as $u = u_0 \sigma^2$ due to the prevalence of phase noise [42], with, for instance, a reasonable parameter value $u_0 = 0.01$. The protocol becomes insecure for $u > 0.25$, and thus the constant u_0 places a practical upper limit on the modulation variance.

In [22] it was shown that the prover's uncertainty about r is given by $h(R|P)_\psi = \frac{1}{2} \log_2 \frac{\pi e(1+2u)}{t}$.

In the purified version of $\text{QPV}_{\text{coh}}^f$, the verifier V_0 prepares the two-mode squeezed state $|\Psi\rangle_{VP}$ given by $|\Psi\rangle = \sqrt{1-\lambda^2} \sum_{m=0}^{\infty} \lambda^m |mm\rangle$ in Fock space, where $\lambda = \tanh \sinh^{-1} \sigma$. Note that $\lambda < 1$. The verifier V_0 performs a heterodyne measurement with quadratures rotated by an angle θ on their register. The measurement outcomes are $r/\sqrt{2}\lambda$ and $-r^\perp/\sqrt{2}\lambda$, resulting in displacement (r, r^\perp) in the state sent to the prover P . Then P performs a homodyne measurement under angle θ to recover r , as in the original protocol. The V_0 's heterodyne measurement can be described as a double-homodyne measurement. First V_0 mixes its own mode with the vacuum using a beam splitter, resulting in a two-mode state. On one of these modes, V_0 then performs a homodyne measurement in the θ direction and on the other mode in the $\theta + \frac{\pi}{2}$ direction. Let $U = R/\lambda\sqrt{2}$ be the displacement in the θ direction as measured by V_0 . Then

$$h(U|P)_\Psi = \frac{1}{2} \log_2 \left(\frac{\pi e(1+2u)}{2t\lambda^2} \right) + O\left(\frac{1}{\sigma}\right) \rightarrow h(U|P)_\Psi$$

in the regime $\sigma \gg 1$ (or $\lambda \rightarrow 1$), where $h(U|P)_\Psi = \frac{1}{2} \log_2 \frac{\pi e(1+2u)}{t}$.

IV. SECURITY AGAINST BOUNDED ENTANGLEMENT

We will show that with high probability, attackers who possess CV entangled states with a cutoff at photon number linear in n will not be able to attack the protocol. To do so, we consider an ‘‘imaginary world’’ where the $\text{QPV}_{\text{coh}}^f$ protocol, instead of using the state $|\Psi\rangle$, is executed with a cutoff at photon number 2^{m_0} using the state $|\Psi_{m_0}\rangle$, given by

$$|\Psi_{m_0}\rangle = \sqrt{\frac{1-\lambda^2}{1-(\lambda^2)^{2^{m_0}}}} \sum_{m=0}^{2^{m_0}-1} \lambda^m |mm\rangle. \quad (2)$$

The state $|\Psi_{m_0}\rangle$ is an approximation of the state $|\Psi\rangle$ and can be made arbitrary close to it by increasing m_0 . Note that $\mathcal{P}(|\Psi\rangle, |\Psi_{m_0}\rangle) = \lambda^{2^{m_0}}$, i.e., $|\Psi_{m_0}\rangle$ is double exponentially close (in m_0) to $|\Psi\rangle$. By replacing $|\Psi\rangle$ by $|\Psi_{m_0}\rangle$, the probability that the verifiers accept the action of an honest party will change with probability at most $O(\lambda^{2^{m_0}})$. The cutoff reduces the dimension of the Hilbert space from infinite to 2^{m_0} , which is the dimension of an m_0 -qubit state space. The energy E of the V subsystem is given by

$$E = \langle \Psi_{m_0} | H_V | \Psi_{m_0} \rangle = \frac{\lambda^2 + (2^{m_0} - 1)\lambda^{2^{m_0}+2} - 2^{m_0}\lambda^{2^{m_0}+1}}{(\lambda^2 - 1)(\lambda^{2^{m_0}+1} - 1)}, \quad (3)$$

which tends to σ^2 (the energy of the challenge state chosen by the verifiers) as m_0 tends to infinity.

The most general attack to $\text{QPV}_{\text{coh}_{m_0}}^f$ for adversaries with a cutoff at the photon number, with the Hilbert space isomorphic to a multiqubit Hilbert space, consists of an adversary Alice between V_0 and P , and an adversary Bob between V_1 and P . They proceed as follows.

(i) The attackers prepare a joint CV state with a cutoff at the photon number of q qubits each.

(ii) Alice intercepts the quantum information sent from V_0 . At this stage V_0 , they share a state $|\chi\rangle_{VPAA_cBB_c}$ of dimension

2^{2q+2m_0} . Here V is the register kept by V_0 , and P is the challenge register that V_0 sends. Alice controls registers P , A , and A_c and Bob registers B and B_c . Moreover, Alice and Bob intercept x and y and perform arbitrary quantum channels depending on the intercepted classical information $U_{PAA_c}^x$ and $V_{BB_c}^y$, respectively, ending up with the state $|\phi\rangle_{VPAA_cBB_c}$.

(iii) Alice and Bob send a copy of x and y to the other attacker, respectively. Alice keeps registers P and A and sends register A_c to Bob and Bob keeps register B and sends B_c to Alice.

(iv) Upon receiving the information sent by the other party, Alice and Bob locally apply arbitrary positive-operator-valued measures (POVMs) $\{A_{PAB_c}^{xy}\}$ and $\{B_{A_cB}^{xy}\}$ to obtain classical answers, which will be sent to their closest verifier, respectively.

Due to the Stinespring dilation, we can consider the quantum channels to be unitaries. Notice that we consider strategies starting with the state $|\chi\rangle_{VPAA_cBB_c}$ instead of $|\Psi_{m_0}\rangle_{VP} \otimes |\chi\rangle_{AA_cBB_c}$. This will give more power to the attackers, but it will include the fact that the quantum information sent from V_0 can travel arbitrarily slow, and the attackers are allowed to modify $|\Psi_{m_0}\rangle_{VP} \otimes |\chi\rangle_{AA_cBB_c}$ to end up with any arbitrary state $|\chi\rangle_{VPAA_cBB_c}$.

The tuple $\{|\chi\rangle_{VPAA_cBB_c}, U_{PAA_c}^x, V_{BB_c}^y, A_{PAB_c}^{xy}, B_{A_cB}^{xy}\}_{xy}$ is a q -qubit strategy for $\text{QPV}_{\text{coh}}^f$. Moreover, we say that a q -qubit strategy for $\text{QPV}_{\text{coh}}^f$ is (ε, l) -perfect if for l pairs of strings (x, y) , for $\theta \in \{0, \frac{\pi}{2}\}$,

$$h(U_\theta|PAB_c)_\phi \leq h(U|P)_\Psi + \varepsilon; \quad h(U_\theta|A_cB)_\phi \leq h(U|P)_\Psi + \varepsilon. \quad (4)$$

Notice that there is no θ dependence on the right-hand side of the inequality since $h(U|P)_\Psi$ does not depend on θ . The parameter ε (discussed in the analysis below) will quantify the difference between the uncertainty of the honest prover and attackers. It will have to be picked depending on the number of rounds that the protocol is run sequentially. We define

$$\mathcal{S}_\theta^\varepsilon := \{|\phi\rangle_{VPAA_cBB_c} \in \mathbb{C}^{2^{2q+2m_0}} \mid \exists \text{ POVMs } A_{PAB_c}^{xy}, B_{A_cB}^{xy} \text{ s.t. (4) holds}\}. \quad (5)$$

Intuitively, $\mathcal{S}_\theta^\varepsilon$ is the set of so-called good states to attack the protocol for either $\theta = 0$ or $\theta = \pi/2$. We will see that a good state for the $\theta = 0$ case cannot be too close (in trace distance) to a good state for the $\theta = \pi/2$ case, and this will restrict the attackers.

Proposition 1. Let $\varepsilon > 0$, $|\phi_0\rangle_{VPAA_cBB_c} \in \mathcal{S}_0^\varepsilon$, and $|\phi_{\pi/2}\rangle_{VPAA_cBB_c} \in \mathcal{S}_{\pi/2}^\varepsilon$, with bounded energies $\text{Tr}(\rho^0 H)$, $\text{Tr}(\rho^1 H) \leq E$, where ρ^0 and ρ^1 are the respective density matrices of $|\phi_0\rangle$ and $|\phi_{\pi/2}\rangle$. The corresponding Hamiltonian is the harmonic oscillator on system V and identity on the other systems. Let $\frac{1}{2} \geq \alpha \geq 0$ and $\tilde{\varepsilon} > 0$ be such that

$$\varepsilon < \frac{1}{2} \log_2 \frac{4t}{e(1+2u)} - \left(\frac{1+\alpha}{2(1-\alpha)} + \alpha \right) \times \left[2\tilde{\varepsilon} \left(\log_2(E+1) + \log_2 \frac{e}{\alpha(1-\tilde{\varepsilon})} \right) + 6\tilde{h} \left(\frac{1+\alpha}{1-\alpha} \tilde{\varepsilon} \right) \right], \quad (6)$$

where $\tilde{h}(x) = -x \log_2 x - (1-x) \log_2(1-x)$ if $x \leq \frac{1}{2}$ and $\tilde{h}(x) = 1$ if $x > \frac{1}{2}$. Then

$$\frac{1}{2} \|\phi_0\rangle - |\phi_{\pi/2}\rangle\|_1 > \tilde{\varepsilon}. \quad (7)$$

Now we are in position to state our main result, Theorem 1, which states that at least one of the attackers has strictly more uncertainty about the correct response than the honest prover. This statement is conditioned on the energy of the harmonic oscillator, the attenuation parameter, and the excess noise fulfilling certain relations, and on a bounded amount of preshared entanglement held by the attackers.

Theorem 1. Let $E, t, u > 0$ and $\varepsilon \in [0, 1]$ be such that $\tilde{\varepsilon} > 0$ exists and $\frac{1}{2} \geq \alpha \geq 0$ such that

$$\begin{aligned} \varepsilon < \frac{1}{2} \log_2 \frac{4t}{e(1+2u)} - \left(\frac{1+\alpha}{2(1-\alpha)} + \alpha \right) \\ \times \left[2\tilde{\varepsilon} \left(\log_2(E+1) + \log_2 \frac{e}{\alpha(1-\tilde{\varepsilon})} \right) \right. \\ \left. + 6\tilde{h} \left(\frac{1+\alpha}{1-\alpha} \tilde{\varepsilon} \right) \right] \end{aligned} \quad (8)$$

holds. Let $n = \Theta(m_0)$. Let the number of qubits that Alice and Bob each controls at the beginning of the protocol be $q = O(n - m_0)$. Then, with probability $1 - O(\lambda^{2m_0})$, the following holds. A random function f fulfills the following with probability at least $1 - O(2^{-2n})$: For every state $|\phi\rangle$ the attackers use to answer to the verifiers, for $\theta \in \{0, \frac{\pi}{2}\}$, the uncertainties for Alice (A) and Bob (B) when attacking the protocol $\text{QPV}_{\text{coh}}^f$ are such that

$$\max\{h(U_\theta|A)_\phi, h(U_\theta|B)_\phi\} \geq h(U|P)_\psi + \frac{\varepsilon}{4}. \quad (9)$$

From (8) we see that the ε will need to be picked taking a value at most $\frac{1}{2} \log_2 \frac{4t}{e(1+2u)}$. In order to have non-negative $\tilde{\varepsilon}$, we need $4t > e(1+2u)$ (see Fig. 2). The maximum value of ε will be upper bounded by $\varepsilon < \frac{1}{2} \log_2 \frac{4t}{e(1+2u)} \leq \frac{1}{2} \log_2 \frac{4}{e} \simeq 0.278652$ since the maximum value is reached by $t = 1$ and $u = 0$.

Let $(r_i^{\text{att}})_{i=1}^N$ be the sample of the attackers after N independent and identically distributed rounds, picking N such that $N(\frac{1}{1/2+u} e^{\varepsilon/2} - \gamma)^2 = \Omega(\frac{1}{\varepsilon_h})$. The probability that the verifiers accept is

$$\mathbb{P} \left(\frac{1}{N} \sum_{i=1}^N \frac{(\sqrt{t}r_i - r_i^{\text{att}})^2}{1/2+u} \leq \gamma \right) \leq O(\varepsilon_h). \quad (10)$$

In order to have explicit expressions in Theorem 1 instead of $n = \Theta(m_0)$ and $q = O(n - m_0)$, we have to fix the value of $\tilde{\varepsilon}$. To obtain better bounds, we are interested in picking $\tilde{\varepsilon}$ as large as possible. Given the parameters E, t, u , and ε , known by the verifiers, we will be interested in picking values of α such that (8) holds for $\tilde{\varepsilon}$ as large as possible. This needs to be done numerically, since (8) leads to a transcendental equation (see below for this analysis).

V. CONCRETE BOUNDS FOR PERFECT CHANNELS

Consider a perfect channel connecting V_0 and P , given by $t = 1$ and $u = 0$. We set $\varepsilon = 0.1$ and assume the protocol

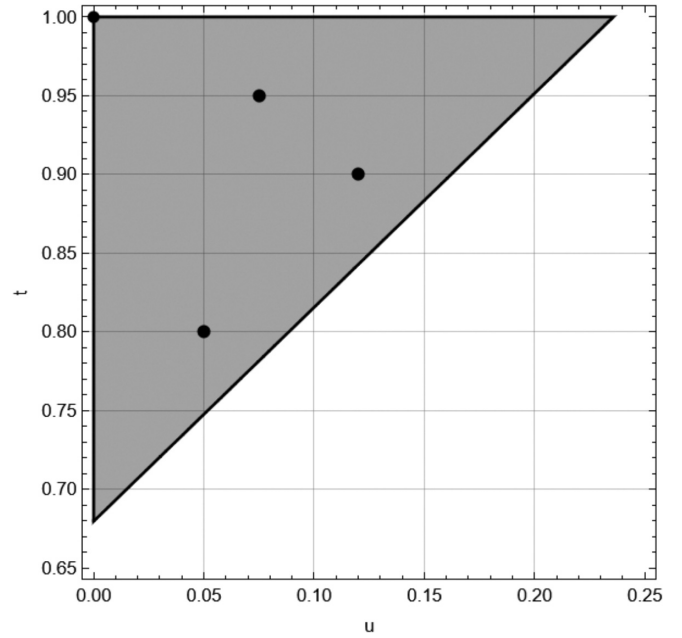


FIG. 2. Necessary condition for u and t so that (8) is fulfilled (gray region). The blue dots are specific (u, t) for which we do numerical analysis.

is played enough rounds to statistically distinguish the honest party with an uncertainty $h(U|P)_\psi \rightarrow \frac{1}{2} \log_2 \frac{\pi e}{2} \simeq 1.0471$ from the uncertainty of at least one of the attackers being at least $\frac{1}{2} \log_2 \frac{\pi e}{2} + \frac{\varepsilon}{4} \simeq 1.0721$. We set an energy bound $E = 10^3$ in units such that $\hbar\omega = 1$. Then the largest $\tilde{\varepsilon}$ that fulfills (8) is $\tilde{\varepsilon} \simeq 0.0037$ for $\alpha \simeq 0.036$ [see Fig. 3 for a representation of the inequality (8)]. With these parameters we have that Theorem 1 can be restated with $n > 2(m_0 + 5)$ and $q \leq \frac{n}{2} - m_0 - 5$.

Notice that the energy term in (8) scales as $\tilde{\varepsilon} \log_2(E+1)$, which scales logarithmically with E and has a small factor $\tilde{\varepsilon}$ in front. Therefore, the inequality remains quite stable with

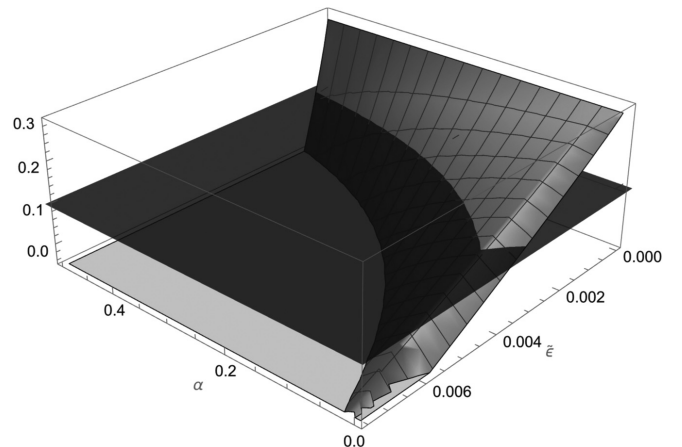


FIG. 3. Representation of the left- (transparent black) and right- (gray surface) hand sides of the inequality (8) for $\varepsilon = 0.1$, $E = 10^3$, $t = 1$, and $u = 0$. The region where the gray surface is above the black plane gives $(\alpha, \tilde{\varepsilon})$ such that the inequality (8) holds.

TABLE I. Maximum value of $\tilde{\varepsilon}$ fulfilling (8), given ε , t , and u , with its corresponding value of α that attains it.

| ε | t | u | α | $\tilde{\varepsilon}$ |
|---------------|------|-------|----------|-----------------------|
| 0.03 | 0.8 | 0.05 | 0.013 | 0.00031 |
| 0.03 | 0.9 | 0.12 | 0.013 | 0.00029 |
| 0.07 | 0.95 | 0.075 | 0.025 | 0.00131 |

respect to E . For instance, if one picks $E = 10, 10^2, 10^4$, the values of the maximum $\tilde{\varepsilon}$ remain almost unchanged.

VI. CONCRETE BOUNDS FOR IMPERFECT CHANNELS

We do the analysis for an imperfect channel for some (u, t) , picking the parameters plotted in Fig. 2. For the values of ε , t , and u in Table I, we find the maximum $\tilde{\varepsilon}$ for $E = 10^3$ and we have the same linear bounds as in the case of a perfect channel.

VII. CONCLUSION

We have shown that quantum position verification can be securely applied against bounded entangled attackers by using coherent states and classical information, which are efficient and economic to prepare in a laboratory. We show that the protocol that we describe remains secure for certain attenuation and excess noise, even if the coherent state travels arbitrarily slow (still far from the speed of light in vacuum with current technology).

In the discrete-variable case Ref. [23] has recently found a way around the problem of transmission loss. It is an interesting open question whether the idea in [23] also could work for CV QPV to make the practical appeal of studying these protocols higher.

$$|h(A|B)_\rho - h(A|B)_\sigma| \leq \left(\frac{1+\alpha}{1-\alpha} + 2\alpha \right) \left[2\tilde{\varepsilon} \left(\log_2(E+1) + \log_2 \frac{e}{\alpha(1-\tilde{\varepsilon})} \right) + 6\tilde{h} \left(\frac{1+\alpha}{1-\alpha} \tilde{\varepsilon} \right) \right], \quad (\text{A3})$$

where

$$\tilde{h}(x) := \begin{cases} -x \log_2 x - (1-x) \log_2 (1-x) & \text{if } x \leq \frac{1}{2} \\ 1 & \text{if } x \geq \frac{1}{2}. \end{cases} \quad (\text{A4})$$

Furthermore, we will make use of the following estimation inequality.

Theorem A1 (from [45]). Let X be a random variable and $\hat{X}(Y)$ an estimator of X given side information Y . Then

$$\mathbb{E}\{[X - \hat{X}(Y)]^2\} \geq \frac{1}{2\pi e} e^{2h_{\text{nats}}(X|Y)}, \quad (\text{A5})$$

where $h_{\text{nats}}(X|Y)$ is the conditional entropy in natural units. Moreover, if X is Gaussian and $\hat{X}(Y)$ is its mean, then equality holds.

APPENDIX A: BACKGROUND

The trace distance between two quantum states ρ and σ is given by $\frac{1}{2}\|\rho - \sigma\|_1$. We write $\frac{1}{2}\|\psi_1\rangle - |\psi_2\rangle\|_1$ for pure states $|\psi_1\rangle$ and $|\psi_2\rangle$. The fidelity between two quantum states ρ and σ is defined as $F(\rho, \sigma) := \text{Tr}(\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}})$ and their purified distance as $\mathcal{P}(\rho, \sigma) := \sqrt{1 - F(\rho, \sigma)^2}$.

The basis of our security proofs is the quantum-mechanical uncertainty principle. We use the following form for the differential entropy in a tripartite setting of a guessing game, as is often useful in the context of quantum cryptography.

Lemma A1 (from [41]). Let ρ_{ABC} be a tripartite density matrix on systems A , B , and C . Let Q and P denote the random variables of position and momentum, respectively, resulting from a homodyne measurement on the A system and let the following hold: $h(Q|B)_\rho, h(P|C)_\rho > -\infty$ and $H(Q_\alpha|B)_\rho, H(P_\alpha|C)_\rho < \infty$ for any $\alpha > 0$. Then

$$h(Q|B)_\rho + h(P|C)_\rho \geq \log_2(2\pi). \quad (\text{A1})$$

We will make use of a type of Alicki-Fannes [43] inequality for continuity of the conditional entropy for continuous variables in terms of the energy as shown in [44]. Consider the Hamiltonian on a system A being the harmonic oscillator with

$$H = \hbar\omega\hat{N}, \quad (\text{A2})$$

with the unusual energy convention that the ground state has energy 0 instead of $\frac{1}{2}\hbar\omega$. Throughout the paper, we consider units such that $\hbar\omega = 1$ (note that we will consider below a fixed wavelength for an input state).

Lemma A2 (Lemma 18 in [44]). Let $\alpha \in [0, \frac{1}{2}]$. Consider a Hamiltonian $H = H_A \otimes \mathbb{I}_B$, with system A composed of one harmonic oscillator and arbitrary system B . Let there be states ρ and σ on the bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$ with $\text{Tr}(\rho H), \text{Tr}(\sigma H) \leq E$. If $\frac{1}{2}\|\rho - \sigma\|_1 \leq \tilde{\varepsilon}$, then

APPENDIX B: PROOF OF PROPOSITION 1

We will use the following notation. For $\theta \in \{0, \frac{\pi}{2}\}$ we will denote by $\bar{\theta}$ the remaining value, i.e., if $\theta = 0$, then $\bar{\theta} = \frac{\pi}{2}$ and if $\theta = \frac{\pi}{2}$, then $\bar{\theta} = 0$. Let ρ^θ and $\rho^{\bar{\theta}}$ be the density matrices of $|\phi_\theta\rangle_{VPAcBBc}$ and $|\phi_{\bar{\theta}}\rangle_{VPAcBBc}$, respectively. By hypothesis,

$$h(U_\theta|PAB_c)_{\rho^\theta} \leq h(U|P)_\psi + \varepsilon, \quad (\text{B1})$$

$$h(U_{\bar{\theta}}|PAB_c)_{\rho^{\bar{\theta}}} \leq h(U|P)_\psi + \varepsilon.$$

By Lemma A1,

$$h(U_\theta|PAB_c)_{\rho^\theta} + h(U_{\bar{\theta}}|A_cB)_{\rho^{\bar{\theta}}} \geq \log_2 2\pi. \quad (\text{B2})$$

Then

$$\begin{aligned} h(U_{\bar{\theta}}|A_cB)_{\rho^{\bar{\theta}}} &\geq \log_2 2\pi - h(U_\theta|PAB_c)_{\rho^\theta} \\ &\geq \log_2 2\pi - h(U|P)_\psi - \varepsilon, \end{aligned} \quad (\text{B3})$$

where in the last inequality we used (B1). Therefore,

$$h(U_{\bar{\theta}}|A_c B)_{\rho^\theta} - h(U_{\bar{\theta}}|PAB_c)_{\rho^{\bar{\theta}}} \geq \log_2 2\pi - 2h(U|P)_\psi - 2\varepsilon. \quad (\text{B4})$$

In the regime $\sigma \gg 1$, $h(U|P)_\psi \rightarrow \frac{1}{2} \log_2 \frac{\pi e(1+2u)}{2t}$ and thus

$$h(U_{\bar{\theta}}|A_c B)_{\rho^\theta} - h(U_{\bar{\theta}}|PAB_c)_{\rho^{\bar{\theta}}} \geq \log_2 \frac{4t}{e(1+2u)} - 2\varepsilon > 0, \quad (\text{B5})$$

where the last inequality comes from the fact that, by hypothesis, $\frac{1}{2} \log_2 \frac{4t}{e(1+2u)} > \varepsilon$. This leads to

$$|h(U_{\bar{\theta}}|A_c B)_{\rho^\theta} - h(U_{\bar{\theta}}|PAB_c)_{\rho^{\bar{\theta}}}| \geq \log_2 \frac{4t}{e(1+2u)} - 2\varepsilon. \quad (\text{B6})$$

By hypothesis, $\log_2 \frac{4t}{e(1+2u)} - 2\varepsilon > (\frac{1+\alpha}{1-\alpha} + 2\alpha)\{2\tilde{\varepsilon}[\log_2(E + 1) + \log_2 \frac{e}{\alpha(1-\tilde{\varepsilon})}] + 6\tilde{h}(\frac{1+\alpha}{1-\alpha}\tilde{\varepsilon})\}$. Thus, by the contrapositive of Lemma A2,

$$\frac{1}{2} \|\rho^\theta - \rho^{\bar{\theta}}\|_1 > \tilde{\varepsilon}. \quad (\text{B7})$$

APPENDIX C: PROOF OF THEOREM 1

In order to prove Theorem 1, we need the following definition, lemmas, and proposition.

Definition C1 (from [12]). Let $q, k, n \in \mathbb{N}$ and $\varepsilon > 0$. Then $g: \{0, 1\}^{3k} \rightarrow \{0, 1\}$ is an $(\varepsilon, 1)$ -classical rounding of size k if for all $f: \{0, 1\}^{2n} \rightarrow \{0, 1\}$, for all states $|\chi\rangle$ on $2q + 2m_0$ qubits, for all $l \in \{1, \dots, 2^{2n}\}$, and for all (ε, l) -perfect q -qubit strategies for $\text{QPV}_{\text{coh}}^f$, there are functions $f_A: \{0, 1\}^n \rightarrow \{0, 1\}^k$, $f_B: \{0, 1\}^n \rightarrow \{0, 1\}^k$, and $\gamma \in \{0, 1\}^k$ such that $g(f_A(x), f_B(y), \gamma) = f(x, y)$ on at least l pairs (x, y) .

Lemma C1 (from [46]). Let $\|\cdot\|$ be any norm on \mathbb{R}^{n_0} for $n_0 \in \mathbb{N}$. There is a δ net S of the unit sphere of $(\mathbb{R}^{n_0}, \|\cdot\|)$ of cardinality at most $(1 + 2/\delta)^{n_0}$.

Lemma C2 (from [12]). Let $|x\rangle, |y\rangle \in \mathbb{C}^d$, for $d \in \mathbb{N}$, be two unit vectors. Then $\mathcal{P}(|x\rangle, |y\rangle) \leq \| |x\rangle - |y\rangle \|_2$.

Proposition C1. Let ε and $\tilde{\varepsilon}$ be such that if $|\varphi_\theta\rangle \in \mathcal{S}_\theta^\varepsilon$ and $|\varphi_{\bar{\theta}}\rangle \in \mathcal{S}_{\bar{\theta}}^\varepsilon$ implies $\mathcal{P}(|\varphi_\theta\rangle, |\varphi_{\bar{\theta}}\rangle) > \tilde{\varepsilon}$, then there is an (ε, q) -classical rounding of size $k = 2^{2q+2m_0} \log_2(1 + \frac{4}{\sqrt[3]{4(2+\tilde{\varepsilon})-2}})$.

Proof. We follow the same techniques as in the proof of Lemma 3.12 in [12]. Let $\delta < \sqrt[3]{\frac{2+\tilde{\varepsilon}}{2}} - 1$ and consider δ nets $\mathcal{N}_S, \mathcal{N}_A$, and \mathcal{N}_B , where the first is for the set of pure states on $2q + 2m_0$ qubits in the Euclidean norm and the other nets are for the set of unitaries in dimension 2^q in the operator norm. They are such that $|\mathcal{N}_S|, |\mathcal{N}_A|, |\mathcal{N}_B| \leq 2^k$, with k to be set later. Let $|\varphi\rangle \in \mathcal{N}_S$, $U_A \in \mathcal{N}_A$, and $U_B \in \mathcal{N}_B$ be the elements with indices $x' \in \{0, 1\}^k$, $y' \in \{0, 1\}^k$, and $\gamma \in \{0, 1\}^k$, respectively. We define g as $g(x, y, \gamma) = 0$ if $U \otimes V|\varphi\rangle$ is closer to $\mathcal{S}_\theta^\varepsilon$ than to $\mathcal{S}_{\bar{\theta}}^\varepsilon$ in purified distance and $g(x, y, \gamma) = 1$ if $U \otimes V|\varphi\rangle$ is closer to $\mathcal{S}_{\bar{\theta}}^\varepsilon$ than to $\mathcal{S}_\theta^\varepsilon$ in purified distance. If neither is the case, we make the arbitrary choice $g(x, y, \gamma) = 1$. By the assumption on ε , $\mathcal{S}_\theta^\varepsilon \cap \mathcal{S}_{\bar{\theta}}^\varepsilon = \emptyset$, and thus g is well defined.

We are going to show that g is an (ε, q) -classical rounding. Consider an arbitrary $f: \{0, 1\}^{2n} \rightarrow \{0, 1\}$ and an arbitrary state $|\chi\rangle$ on $2q + 2m_0$ qubits. Let $|\chi\rangle$ and $\{U_A^x, U_B^y\}_{xy}$ be from

a q -qubit strategy for $\text{QPV}_{\text{coh}_{m_0}}^f$ and choose γ , $f_A(x)$, and $f_B(y)$ to be the closest elements to $|\chi\rangle$, U_A^x , and U_B^y , respectively, in their corresponding δ nets in the Euclidean and the operator norm, respectively (if not unique, make an arbitrary choice), and let $|\varphi\rangle$, U_A , and U_B be their corresponding elements. Assume $U_A^x \otimes U_B^y |\chi\rangle \in \mathcal{S}_\theta^\varepsilon$. Then

$$\begin{aligned} & \mathcal{P}(U_A^x \otimes U_B^y |\chi\rangle, U_A \otimes U_B |\varphi\rangle) \\ & \leq \|U_A^x \otimes U_B^y |\chi\rangle - U_A \otimes U_B |\varphi\rangle\|_2 \\ & \leq \|(U_A + U_A^x - U_A) \otimes (U_B + U_B^y - U_B)(|\varphi\rangle + |\chi\rangle) - U_A \otimes U_B |\varphi\rangle\|_2 \\ & \leq 3\delta + 3\delta^2 + \delta^3 < \frac{\tilde{\varepsilon}}{2}, \end{aligned} \quad (\text{C1})$$

where in the first inequality we have used Lemma C2 and in the second we have used the triangle inequality and the inequality $\|X \otimes Y\|_2 \leq \|X\|_\infty \|Y\|_\infty \| |x\rangle \|_2$, together with $\|U_A^x - U_A\|_\infty, \|U_B^y - U_B\|_\infty, \| |\chi\rangle - |\varphi\rangle \| \leq \delta$. Thus, $U_A \otimes U_B |\varphi\rangle$ is closer to $\mathcal{S}_\theta^\varepsilon$ than to $\mathcal{S}_{\bar{\theta}}^\varepsilon$.

Consider an (ε, l) -perfect strategy for $\text{QPV}_{\text{coh}_{m_0}}^f$ and let (x, y) be such that $h(U_\theta | PAB_c)_\varphi, h(U_\theta | A_c B)_\psi \leq h(U | P)_\psi + \varepsilon$ for $f(x, y) = 0$. In particular, we have that $U_A^x \otimes U_B^y |\chi\rangle \in \mathcal{S}_i^\varepsilon$, and because of (C1), $f(x, y) = g(f_A(x), f_B(y), \gamma)$. Since there are at least l pairs (x, y) fulfilling it, $f(x, y) = g(f_A(x), f_B(y), \gamma)$ holds on at least l pairs (x, y) and therefore g is an (ε, q) -classical rounding. The size of k follows from Lemma C1. ■

Lemma C3. Let $\varepsilon \in [0, 1]$ and $E, t, u > 0$ be such that there exist $\tilde{\varepsilon} > 0$ and α such that (6) holds. Let $k, q \in \mathbb{N}$ and $n = \Omega(m_0)$. Moreover, fix an (ε, q) -classical rounding g of size k with $k = 2^{2q+2m_0} \log_2(1 + \frac{4}{\sqrt[3]{4(2+\tilde{\varepsilon})-2}})$. Let $q = O(n - m_0)$. Then, with probability $1 - O(\lambda^{2^{m_0}})$, the following holds.

A uniformly random $f: \{0, 1\}^{2n} \rightarrow \{0, 1\}$ fulfills the following with probability at least $1 - O(2^{-2^n})$: For any $f_A: \{0, 1\}^n \rightarrow \{0, 1\}^k$ and $f_B: \{0, 1\}^n \rightarrow \{0, 1\}^k$, with $\gamma \in \{0, 1\}^k$, the equality $g(f_A(x), f_B(y), \gamma) = f(x, y)$ holds on less than $\frac{3}{4}$ of all pairs (x, y) .

Proof. We want to estimate the probability that for a randomly chosen f , we can find f_A and f_B such that the corresponding function g fulfills $\mathbb{P}_{x,y}[f(x, y) = g(f_A(x), f_B(y), \gamma)] \geq \frac{3}{4}$. In a similar manner as in [12], we have that

$$\begin{aligned} & \mathbb{P}[f: \exists f_A, f_B, \gamma \text{ s.t. } \mathbb{P}_{x,y}[f(x, y) = g(f_A(x), f_B(y), \gamma)]] \\ & \leq 2^{(2^{n+1}+1)k} 2^{2^{2n}h(1/4)} 2^{-2^{2n}}, \end{aligned} \quad (\text{C2})$$

where h denotes the binary entropy function. If $q = O(n - m_0)$ and $k = 2^{2q+2m_0} \log_2(1 + \frac{4}{\sqrt[3]{4(2+\tilde{\varepsilon})-2}})$, the above expression is strictly upper bounded by $O(2^{-2^n})$. ■

Now we are in position to prove Theorem 3. By Lemma C3, with probability at least $1 - O(2^{-2^n})$, the function f is such that there are no $(\varepsilon, \frac{3}{4}2^{2n})$ -perfect q -qubit strategies for $\text{QPV}_{\text{coh}}^f$. That means that for every strategy, on a fraction at least $\frac{1}{4}$ of (x, y) , either $h(U_\theta | PAB_c)_\varphi \geq h(U | P)_\psi + \frac{\varepsilon}{4}$ or $h(U_\theta | A_c B)_\psi \geq h(U | P)_\psi + \frac{\varepsilon}{4}$.

**APPENDIX D: BOUNDING ATTACK SUCCESS
PROBABILITY AFTER REPEATED INDEPENDENT
AND IDENTICALLY DISTRIBUTED ROUNDS**

For the following, recall that $\sigma \gg 1$, or equivalently $\lambda \rightarrow 1$. To estimate the number of (independent) rounds N we have to run for the attack success probability to become vanishingly small, we cannot assume a specific attack distribution and we have to assume the attackers have access to an ideal channel. By Eq. (8) we know that

$$\begin{aligned} h(U_\theta|E)_\phi &:= \max\{h(U_\theta|PAB_c)_\phi, h(U_\theta|A_cB)_\phi\} \\ &\geq h(U|P)_\psi + \frac{\varepsilon}{4} = \frac{1}{2} \log_2 \left(\pi e \frac{1/2+u}{t} \right) + \frac{\varepsilon}{4}. \end{aligned} \quad (\text{D1})$$

Now substituting again $R = \sqrt{2}\lambda U$ yields

$$h(R|E)_\phi \geq h(R|P)_\psi + \frac{\varepsilon}{4} \quad (\text{D2})$$

$$= \frac{1}{2} \log_2 \left(2\pi e \frac{1/2+u}{t} \right) + \frac{\varepsilon}{4} \quad (\text{D3})$$

$$\geq \frac{1}{2} \log_2(\pi e) + \frac{\varepsilon}{4}, \quad (\text{D4})$$

where the lower bound is smallest for the ideal channel with $t = 1$ and $u = 0$, which we assume attackers can use. Via the continuous variable version of Fano's inequality, Theorem 12, we can straightforwardly convert this into a lower bound for

the estimation error of the attackers. We obtain

$$\mathbb{E}[(R - r')^2] \geq \frac{1}{2\pi e} e^{2h_{\text{max}}(R|E)_\phi} = \frac{1}{2} e^{\varepsilon/2}. \quad (\text{D5})$$

Thus $\mathbb{E}(\sqrt{t}R - r')^2 \geq \frac{1}{2} e^{\varepsilon/2}$ for any transmission t . The probability that the attackers' score falls below the threshold γ is at most the probability that the score differs from $\mathbb{E}(\sqrt{t}R - r')^2/(1/2+u)$ by more than the difference $\Delta \stackrel{\text{def}}{=} \frac{1/2}{1/2+u} e^{\varepsilon/2} - \gamma$. We can then use the Chebyshev inequality for the random variable of the score to get

$$\begin{aligned} \mathbb{P} \left(\left| \frac{1}{N} \sum_{i=1}^N \frac{(\sqrt{t}R_i - r'_i)^2}{1/2+u} - \frac{\mathbb{E}(\sqrt{t}R - r')^2}{1/2+u} \right| \geq \Delta \right) \\ \leq \frac{\tilde{\sigma}^2}{N\Delta^2} = O\left(\frac{1}{N\Delta^2}\right), \end{aligned} \quad (\text{D6})$$

where $\tilde{\sigma}^2 = \mathbb{V}\left(\frac{(\sqrt{t}R - r')^2}{1/2+u}\right)$ is the variance. We set the tolerance for the success probability to ε_h for simplicity. If we then set $N\Delta^2 = \Omega\left(\frac{1}{\varepsilon_h}\right)$, we get

$$\mathbb{P} \left(\frac{1}{N} \sum_{i=1}^N \frac{(\sqrt{t}R_i - r'_i)^2}{1/2+u} \leq \gamma \right) \leq O(\varepsilon_h). \quad (\text{D7})$$

The required number of rounds N can be obtained by first setting the tolerated ε_h and then solving $N\Delta^2 = \Omega\left(\frac{1}{\varepsilon_h}\right)$ for N . This means we accept the honest prover with probability $1 - \varepsilon_h$, while accepting attackers with probability ε_h , after N independent and identically distributed rounds.

-
- [1] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, in *Advances in Cryptology—CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, 2009*, edited by S. Halevi, Lecture Notes in Computer Science Vol. 5677 (Springer, Berlin, 2009), pp. 391–407.
- [2] W. K. Wootters and W. Zurek, *Nature (London)* **299**, 802 (1982).
- [3] A. Kent, W. Munro, T. Spiller, and R. Beausoleil, Tagging systems, U.S. Patent No. US20060022832A1 (2 February 2006).
- [4] R. A. Malaney, *Phys. Rev. A* **81**, 042319 (2010).
- [5] R. A. Malaney, *IEEE Global Telecommunications Conference GLOBECOM, Miami, 2010* (IEEE, Piscataway, 2010).
- [6] H.-K. Lau and H.-K. Lo, *Phys. Rev. A* **83**, 012322 (2011).
- [7] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, *SIAM J. Comput.* **43**, 150 (2014).
- [8] S. Beigi and R. König, *New J. Phys.* **13**, 093036 (2011).
- [9] H. Buhrman, S. Fehr, C. Schaffner, and F. Speelman, in *Proceedings of the Fourth Conference on Innovations in Theoretical Computer Science, Berkeley, 2013* (ACM, New York, 2013), pp. 145–158.
- [10] F. Speelman, *11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016)*, Leibniz International Proceedings in Informatics (LIPIcs) (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Saarbrücken, 2016), Vol. 61, pp. 1–24.
- [11] K. Dolev and S. Cree, [arXiv:2203.10106](https://arxiv.org/abs/2203.10106).
- [12] A. Bluhm, M. Christandl, and F. Speelman, *Nat. Phys.* **18**, 623 (2022).
- [13] J. Cree and A. May, *Quantum* **7**, 1079 (2023).
- [14] R. Allerstorfer, H. Buhrman, A. May, F. Speelman, and P. V. Lunel, Relating non-local quantum computation to information theoretic cryptography, *Quantum* **8**, 1387 (2024).
- [15] H. Apel, T. Cubitt, P. Hayden, T. Kohler, and D. Pérez-García, Security of position-based quantum cryptography limits Hamiltonian simulation via holography, *J. High Energy Phys.* **08** (2024) 152.
- [16] V. Asadi, E. Culf, and A. May, [arXiv:2402.18647](https://arxiv.org/abs/2402.18647).
- [17] V. Asadi, R. Cleve, E. Culf, and A. May, [arXiv:2402.18648](https://arxiv.org/abs/2402.18648).
- [18] K. Chakraborty and A. Leverrier, *Phys. Rev. A* **92**, 052304 (2015).
- [19] R. Allerstorfer, H. Buhrman, F. Speelman, and P. V. Lunel, [arXiv:2106.12911](https://arxiv.org/abs/2106.12911).
- [20] A. Gonzales and E. Chitambar, *IEEE Trans. Inf. Theory* **66**, 2951 (2019).
- [21] J. Liu, Q. Liu, and L. Qian, in *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, Leibniz International Proceedings in Informatics (LIPIcs), edited by M. Braverman (Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Saarbrücken, 2022), Vol. 215, pp. 1–11.
- [22] R. Allerstorfer, L. Escolà-Farràs, A. A. Ray, B. Škorić, F. Speelman, and P. V. Lunel, [arXiv:2308.04166](https://arxiv.org/abs/2308.04166).

- [23] R. Allerstorfer, A. Bluhm, H. Buhrman, M. Christandl, L. Escolà-Farràs, F. Speelman, and P. V. Lunel, [arXiv:2312.12614](#).
- [24] D. Unruh, in *Advances in Cryptology—CRYPTO 2014*, edited by J. A. Garay and R. Gennaro, Lecture Notes in Computer Science Vol. 8617 (Springer, Berlin, 2014), pp. 1–18.
- [25] F. Gao, B. Liu, and Q. Wen, *Sci. China Phys. Mech. Astron.* **59**, 110311 (2016).
- [26] K. Dolev, [arXiv:1909.05403](#).
- [27] R. Allerstorfer, H. Buhrman, F. Speelman, and P. V. Lunel, [arXiv:2208.04341](#).
- [28] L. Escolà-Farràs and F. Speelman, *Phys. Rev. Lett.* **131**, 140802 (2023).
- [29] B. Qi and G. Siopsis, *Phys. Rev. A* **91**, 042337 (2015).
- [30] T. C. Ralph, *Phys. Rev. A* **61**, 010303(R) (1999).
- [31] M. Hillery, *Phys. Rev. A* **61**, 022309 (2000).
- [32] M. D. Reid, *Phys. Rev. A* **62**, 062308 (2000).
- [33] N. J. Cerf, M. Lévy, and G. Van Assche, *Phys. Rev. A* **63**, 052311 (2001).
- [34] F. Grosshans and P. Grangier, *Phys. Rev. Lett.* **88**, 057902 (2002).
- [35] F. Grosshans, G. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, *Nature (London)* **421**, 238 (2003).
- [36] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, *Quantum Inf. Comput.* **3**, 535 (2003).
- [37] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, *Phys. Rev. Lett.* **93**, 170504 (2004).
- [38] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Rev. Mod. Phys.* **84**, 621 (2012).
- [39] A. Kent, W. J. Munro, and T. P. Spiller, *Phys. Rev. A* **84**, 012326 (2011).
- [40] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore*, 1984 (IEEE, Piscataway, 1984), pp. 175–179.
- [41] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, *J. Math. Phys.* **55**, 122205 (2014).
- [42] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, *Adv. Quantum Technol.* **1**, 1870011 (2018).
- [43] R. Alicki and M. Fannes, *J. Phys. A: Math. Gen.* **37**, L55 (2004).
- [44] A. Winter, *Commun. Math. Phys.* **347**, 291 (2016).
- [45] T. M. Cover, *Elements of Information Theory* (Wiley, New York, 1999).
- [46] M. Ledoux and M. Talagrand, *Probability in Banach Spaces: Isoperimetry and Processes*, Classics in Mathematics Vol. 23 (Springer, Berlin, 1991).