Continuous-variable Quantum Position Verification secure against entangled attackers

Continuous-variable Quantum Position Verification secure against entangled attackers

Rene Allerstorfer[1], Llorenç Escolà-Farràs[2], Arpan Akash Ray[3], Boris Škorić[3], and Florian Speelman[2]

[1] *QuSoft & CWI Amsterdam, The Netherlands*
[2] *QuSoft & Informatics Institute, University of Amsterdam, The Netherlands*
[3] *TU Eindhoven, The Netherlands*

April 23, 2024

Abstract

Motivated by the fact that coherent states may offer practical advantages it was recently shown that a continuous-variable (CV) quantum position verification (QPV) protocol using coherent states could be securely implemented if and only if attackers do not pre-share any entanglement. In the discrete-variable (DV) analogue of that protocol it was shown that modifying how the classical input information is sent from the verifiers to the prover leads to a favourable scaling in the resource requirements for a quantum attack. In this work, we show that similar conclusions can be drawn for CV-QPV. By adding extra classical information of size n to a CV-QPV protocol, we show that the protocol, which uses a coherent state and classical information, remains secure, even if the quantum information travels arbitrarily slow, against attackers who pre-share CV (entangled) states with a linear (in n) cutoff at the photon number. We show that the protocol remains secure for certain attenuation and excess noise.

Contents

1 Introduction

Position-based cryptography utilises 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 was recorded *where* it claims to have been (instead of being created by a powerful AI or untrusted parties, for example). Part of position-based cryptography is the task of position verification, where an untrusted prover aims to convince verifiers that he is present at a certain position P.

This primitive was first introduced by Chandran, Goyal, Moriarty, and Ostrovsky [CGMO09], and it has been shown that no classical position-verification protocol can exist, due to a universal attack based on cloning input information. This attack fails in the quantum setting because of the no-cloning theorem [WZ82]. Quantum position verification (QPV) has been studied[1] since the early 2000s by several authors [KMSB06, Mal10a, Mal10b, LL11]. Proposed QPV protocols rely on both relativistic constraints (in a d-dimensional Minkowski space-time $M^{(d,1)}$) and the laws of quantum mechanics. In the literature, usually the case $d = 1$ studied for simplicity, i.e. verifying the position of P in a line (by two verifiers V_0 and V_1 who are placed on the left and right of P, respectively), since it makes the analysis easier and the main ideas generalize to higher dimensions. Despite the failure of the classical universal attack, a universal quantum attack has been found [BCF+14, BK11]. 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 [BFSS13, Spe16, DC22, BCS22, CM23, ABM+23, ACH+24, ACM24, ACCM24]. Many protocols have since been proposed [CL15, ABSL22b, GC19, LLQ22, AEFR+23, ABB+23] and different security models have been studied [Unr14, GLW16, Dol22, ABSL22a]. Recent work has focused on the practicality of implementing position-verification protocols. Aspects such as channel loss and error tolerance of certain QPV protocols must be taken into account [ABSL22a, EFS23, ABB+23].

Most previous QPV protocols have been based on finite-dimensional quantum systems, with the exception of [QS15, AEFR+23].

Continuous-variable quantum systems are relevant for quantum communication and quantum-limited detection and imaging techniques because they provide a quantum description of the propagating electromagnetic field. Of particular relevance are the eigenstates of the annihilation operator, also known as coherent states, and their quadrature squeezed counterparts known as squeezed coherent states. Much research regarding continuous-variable quantum key distribution (QKD) has been conducted. Firstly proposed with discrete [Ral99, Hil00, Rei00] and Gaussian [CLA01] encoding of squeezed states, soon a variety of protocols were published on Gaussian-modulated CV-QKD with coherent states [GG02, GAW+03, GCW+03, WLB+04]. In this paper, we employ many techniques that are common in CV-QKD. Theoretical reviews with practical considerations of CV-QKD can be found in [GPS07, Lev09].

CV systems are much simpler to handle in practice and leverage several decades of experience in coherent optical communication technology. One particular advantage is that no true single-photon preparation or detection is necessary. Clean creation and detection of single photons is still expensive and technically challenging, especially if photon number resolution is desired. In contrast, homodyne and heterodyne measurements are easy to implement and much existing infrastructure is geared towards handling light at low-loss telecom wavelengths (1310nm, 1550nm), 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 [AEFR+23], the CV analogue of the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol, first introduced and studied in [KMS11, BCF+14, LL11], was defined and analysed. In this article, we extend the CV-QPV literature by considering the CV version of the practically interesting protocol $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ [BCS22, EFS23], where the classical input information is split up (into, say, x, y) and each verifier sends out one part of it. 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 required quantum resources for a successful attack become larger and scale linearly in the size n of the *classical* input strings x, y. Thus, increasing the classical input size makes the quantum attack harder – a very favourable property of $\mathrm{QPV}^{f}_{\mathrm{BB84}}$. It is theoretically, and also potentially practically, interesting whether this property holds the same way in the CV case, which is why we study it.

Employing previous results from [BCS22] and [AEFR+23], the main take-away of this work is that, indeed, the CV protocol shares the desired characteristics regarding entanglement attacks of the discrete variable version. However, it was shown in [QS15] that a simple generic attack exists as long as the transmission is $t \leq 1/2$ for this type of CV-QPV protocol.

[1] under the name of 'quantum tagging'

More concretely, we show that, for a random function f, the protocol remains secure against attackers who pre-share a quantum resource state with dimension linear in n. Moreover, the protocol remains secure even if the quantum information is sent arbitrarily slowly. We also consider attenuation and excess noise in the CV channel in our analysis. The underlying technique is to lower bound the attackers' entropy about the quadrature value R that the protocol asks for. To do so, we employ the continuity of the conditional entropy for continuous variables in terms of the energy as shown in [Win16]. This then implies that the sample the attackers respond with will necessarily have a higher variance than the honest sample, which allows the verifiers to distinguish between an honest and a dishonest sample.

2 Preliminaries

Let $\mathcal{H}$, $\mathcal{H}'$ be finite-dimensional Hilbert spaces, we denote by $\mathcal{B}(\mathcal{H}, \mathcal{H}')$ the set of bounded operators from $\mathcal{H}$ to $\mathcal{H}'$ and $\mathcal{B}(\mathcal{H}) = \mathcal{B}(\mathcal{H}, \mathcal{H})$. Denote by $\mathcal{S}(\mathcal{H})$ the set of quantum states on $\mathcal{H}$, i.e. $\mathcal{S}(\mathcal{H}) = \{\rho \in \mathcal{B}(\mathcal{H}) \mid \rho \geq 0, \mathrm{Tr}[\rho] = 1)\}$. A pure state will be denoted by a ket $|\psi\rangle \in \mathcal{H}$. The trace distance between two quantum states ρ and σ is given by

$$\frac{1}{2}\|\rho - \sigma\|_1. \tag{1}$$

We will write $\frac{1}{2}\||\psi_1\rangle - |\psi_2\rangle\|_1$ for pure states $|\psi_1\rangle, |\psi_2\rangle$. The fidelity bewteen two quantum states ρ and σ is defined as

$$F(\rho, \sigma) := \mathrm{Tr}\left[\sqrt{\sqrt{\sigma}\rho\sqrt{\sigma}}\right], \tag{2}$$

in particular, for pure states $|\psi_1\rangle, |\psi_2\rangle$, $F(|\psi_1\rangle, |\psi_2\rangle) = |\langle\psi_1|\psi_2\rangle|$. The purified distance for quantum states ρ and σ is defined as

$$\mathcal{P}(\rho, \sigma) := \sqrt{1 - F(\rho, \sigma)^2}. \tag{3}$$

Definition 2.1. *Let X be a continuous random variable with probability density function $f(x)$, and let $\mathcal{X}$ be its support set. The* differential Shannon entropy *$h(X)$ is defined as*

$$h(X) = -\int_{\mathcal{X}} f(x) \log f(x)\, \mathrm{d}x, \tag{4}$$

where, if not otherwise mentioned, we use log in base 2.

Lemma 2.2. *Let $\beta > 0$ and $X \in \mathbb{R}$. It holds that $h(\beta X) = h(X) + \log \beta$.*

As introduced in [FBT+14], 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 sub-normalized 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. These notions are used in the continuous version of the conditional entropy.

Definition 2.3. *The* quantum conditional von Neumann entropy *is defined as*

$$H(Q_\alpha|B)_\rho := -\sum_{k\in\mathbb{Z}} D(\rho_B^{k;\alpha}||\rho_B). \tag{5}$$

Definition 2.4. *The* differential quantum conditional von Neumann entropy *is defined as*

$$h(X|B)_\rho := -\int_{\mathbb{R}} D(\rho_B^x||\rho_B)\, \mathrm{d}x. \tag{6}$$

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 2.5. *[FBT+14] 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*

$$h(Q|B)_\rho + h(P|C)_\rho \geq \log(2\pi). \tag{7}$$

We will make use of a type of Alicki-Fannes [AF04] inequality for continuity of the conditional entropy for continuous variables in terms of the energy as shown in [Win16]. Consider the Hamiltonian on a system A being the harmonic oscillator with

$$H = \hbar\omega\hat{N}, \tag{8}$$

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

Lemma 2.6. *(Lemma 18, [Win16]) 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 $\mathrm{Tr}[\rho H], \mathrm{Tr}[\sigma H] \leq E$. If $\frac{1}{2}\|\rho - \sigma\|_1 \leq \tilde{\varepsilon}$, then*

$$|h(A|B)_\rho - h(A|B)_\sigma| \leq \left(\frac{1+\alpha}{1-\alpha} + 2\alpha\right)\left[2\tilde{\varepsilon}\left(\log(E+1) + \log\frac{e}{\alpha(1-\tilde{\varepsilon})}\right) + 6\tilde{h}\left(\frac{1+\alpha}{1-\alpha}\tilde{\varepsilon}\right)\right], \tag{9}$$

where

$$\tilde{h}(x) := \begin{cases} -x\log x - (1-x)\log(1-x) & \text{if } x \leq \frac{1}{2} \\ 1 & \text{if } x \geq \frac{1}{2}. \end{cases} \tag{10}$$

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

Theorem 2.7. *[Cov99] Let X be a random variable and $\hat{X}(Y)$ an estimator of X given side information Y, then*

$$\mathbb{E}\left[\left(X - \hat{X}(Y)\right)^2\right] \geq \frac{1}{2\pi e} e^{2h_{\mathrm{nats}}(X|Y)}, \tag{11}$$

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

3 The $\mathrm{QPV}^f_{\mathrm{coh}}$ protocol

Based on the ideas in [BFSS13, Unr14, BCS22], we introduce a variation of the quantum position verification protocol studied in [AEFR+23]. Instead of only a single verifier sending classical information, both verifiers send classical information that, combined, determine the action of the prover. 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. Then, the protocol is described as follows:

Definition 3.1. *Let $n \in \mathbb{N}$ and consider a $2n$-bit boolean function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. A round of the $\mathrm{QPV}^f_{\mathrm{coh}}$ protocol is described as follows.*

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

2. *The verifier V_0 sends $|\psi\rangle$ and x to P, and the verifier 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.*

3. *Immediately, P computes $f(x,y)$ and performs a homodyne measurement on $|\psi\rangle$ in the direction $\theta = 0$ if $f(x,y) = 0$ or $\theta = \frac{\pi}{2}$ if $f(x,y) = 1$, 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 as $(r'_i)_{i=1}^N$. The verifiers check whether all prover responses arrived at the correct time, and whether the reported values $(r'_i)_{i=1}^N$ satisfy

$$\frac{1}{N}\sum_{i=1}^{N}\frac{\left(r'_i - r_i\sqrt{t}\right)^2}{\frac{1}{2}+u} < \gamma, \qquad \text{with} \qquad \gamma \overset{\text{def}}{=} 1 + \frac{2}{\sqrt{N}}\sqrt{\ln\frac{1}{\varepsilon_{\text{hon}}}} + \frac{2}{N}\ln\frac{1}{\varepsilon_{\text{hon}}}. \tag{12}$$

Here ε_{hon} is an upper bound on the honest prover's failure probability (as a parameter of the protocol). See Fig. 1 for a schematic representation of the $\text{QPV}_{\text{coh}}^{f}$ protocol.

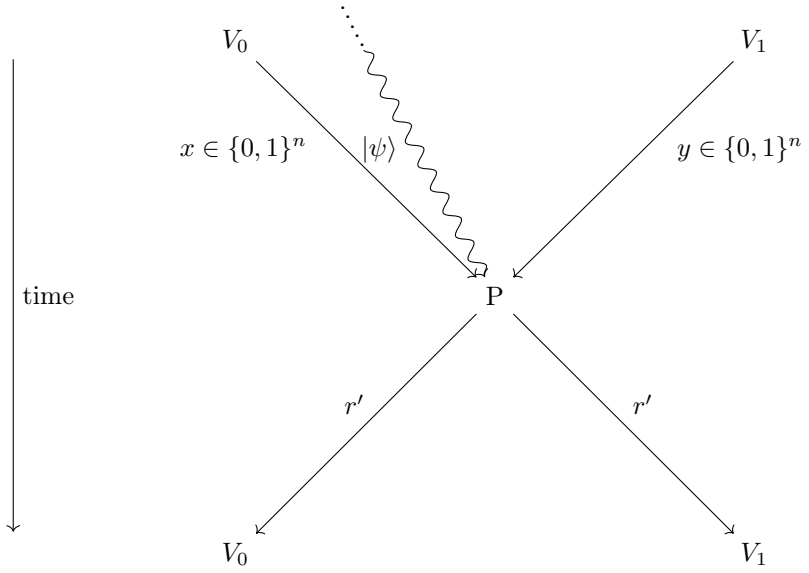

Figure 1: One round of the $\text{QPV}_{\text{coh}}^{f}$ protocol. The coherent state $|\psi\rangle$ originates from V_0 in the past.

The excess noise can be modeled as $u = u_0\sigma^2$, with, for instance, a reasonable $u_0 = 0.01$, due to the prevalence of phase noise [LPF+18]. The protocol becomes insecure for $u > 0.25$, and thus the constant u_0 places a practical upper limit on the modulation variance σ.

The protocol in [AEFR+23] is as in Definition 3.1 but instead of sending x and y, V_1 directly sends θ. For the honest party, the only difference is that he has to compute $f(x,y)$ to determine θ. 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 $\bar{\theta} = 0$.

The honest prover's uncertainty about the displacements r, drawn by the random variable denoted by R in each round, conditioned on his measurement outcomes r', drawn from the random variable denoted by R' in each round, is the same as in the protocol where θ is sent directly from V_1, since the only change for P is to compute $f(x,y)$ to determine θ. This uncertainty was calculated in [AEFR+23] to be

$$h(R|R')_\psi = \frac{1}{2}\log 2\pi e\Sigma^2, \tag{13}$$

where

$$\Sigma^2 = \left(\frac{1}{\sigma^2} + \frac{t}{1/2+u}\right)^{-1}. \tag{14}$$

It is well known that the preparation of a coherent state with Gaussian distributed displacements $x_0, p_0 \sim \mathcal{N}_{0,\sigma^2}$ is equivalent to preparing a two-mode squeezed state with squeezing parameter

$\sinh^{-1}\sigma$ and then performing a heterodyne $(\hat{x},\hat{p})$ measurement on one mode, with measurement outcome $\frac{(x_0,-p_0)}{\sqrt{2}\tanh\sinh^{-1}\sigma}$. For notational brevity, we set $\lambda = \tanh\sinh^{-1}\sigma$.

In the purified version of $\mathrm{QPV}^f_{\mathrm{coh}}$, the verifier V_0 prepares the two-mode squeezed state $|\Psi\rangle_{V_0P}$ with the above mentioned λ-dependent squeezing, which is given by

$$|\Psi\rangle = \sqrt{1-\lambda^2}\sum_{m=0}^{\infty}\lambda^m|mm\rangle, \tag{15}$$

in the Fock space. Notice 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. P then performs a homodyne measurement under angle θ to recover r, as in the original protocol.

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 beamsplitter, resulting in a two-mode state. On one of these modes, V_0 then performs a homodyne measurement in the θ-direction, on the other mode in the $\theta+\frac{\pi}{2}$ direction.

In [AEFR+23] it is shown that the honest prover's uncertainty about R evaluates to

$$h(R|P)_{\Psi} = \frac{1}{2}\log\frac{\pi e(1+2u)}{t} + O\left(\frac{1}{\sigma}\right). \tag{16}$$

Let $U = R/(\lambda\sqrt{2})$ be the displacement in the θ direction as measured by V_0.

Then

$$\begin{aligned} h(U|P)_{\Psi} &= h\left(\frac{R}{\sqrt{2}\lambda}\middle|P\right)_{\Psi} = h(R|P)_{\Psi} - \log(\sqrt{2}\lambda) \\ &= \frac{1}{2}\log\frac{\pi e(1+2u)}{t} + O\left(\frac{1}{\sigma}\right) - \log(\sqrt{2}\lambda). \end{aligned} \tag{17}$$

In the regime $\sigma \gg 1$ (i.e. $\lambda \to 1$),

$$h(U|P)_{\Psi} \to h(U|P)_{\psi} = \frac{1}{2}\log\frac{\pi e(1+2u)}{2t}. \tag{18}$$

Unless stated otherwise, we will work in the regime $\sigma \gg 1$. Recall that σ is in control of the verifiers.

4 Security against bounded entanglement

In this section, we prove security of the $\mathrm{QPV}^f_{\mathrm{coh}}$ protocol, showing 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 $\mathrm{QPV}^f_{\mathrm{coh}}$ 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

$$|\Psi_{m_0}\rangle = \sqrt{\frac{1-\lambda^2}{1-(\lambda^2)^{2^{m_0}}}}\sum_{m=0}^{2^{m_0}-1}\lambda^m|mm\rangle. \tag{19}$$

We will denote this variation of the protocol by $\mathrm{QPV}^f_{\mathrm{coh}_{m_0}}$. 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

$$\mathcal{P}(|\Psi\rangle, |\Psi_{m_0}\rangle) = \lambda^{2^{m_0}}, \tag{20}$$

i.e. $|\Psi_{m_0}\rangle$ is double exponentially close (in m_0) to $|\Psi\rangle$ (recall that $\lambda < 1$). If one replaces the state $|\Psi\rangle$ 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 of the V_0 subsystem is given by

$$\langle\Psi_{m_0}|H_{V_0}|\Psi_{m_0}\rangle_{V_0P} = \frac{\lambda^2 + (2^{m_0}-1)\lambda^{2^{m_0+1}+2} - 2^{m_0}\lambda^{2^{m_0+1}}}{(\lambda^2-1)\left(\lambda^{2^{m_0+1}}-1\right)} = \frac{2^{m_0}\left(\frac{\sigma^2}{\sigma^2+1}\right)^{2^{m_0}}}{\left(\frac{\sigma^2}{\sigma^2+1}\right)^{2^{m_0}}-1} + \sigma^2, \tag{21}$$

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

The most general attack to $\mathrm{QPV}^f_{\mathrm{coh}_{m_0}}$ for adversaries with a photon-number cutoff such that their Hilbert space is isomorphic to a multi-qubit 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:

1. *Preparing:* The attackers prepare a joint (possibly entangled) CV state with a cutoff at the photon number of q qubits each.
2. *Intercepting:* Alice intercepts the quantum information sent from V_0. At this stage, V_0, Alice and Bob 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 the registers P, A and A_c, and Bob possesses the registers B and B_c. Moreover, Alice and Bob intercept x and y and perform arbitrary quantum channels depending on the intercepted classical information: $U^x_{PAA_c}$ and $V^y_{BB_c}$, respectively, ending up with the state $|\phi\rangle_{VPAA_cBB_c}$.
3. *Communicating:* 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.
4. *Measuring:* Upon receiving the information sent by the other party, Alice and Bob locally apply arbitrary POVMs $\{A^{xy}_{PAB_c}\}$ and $\{B^{xy}_{A_cB}\}$ 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.

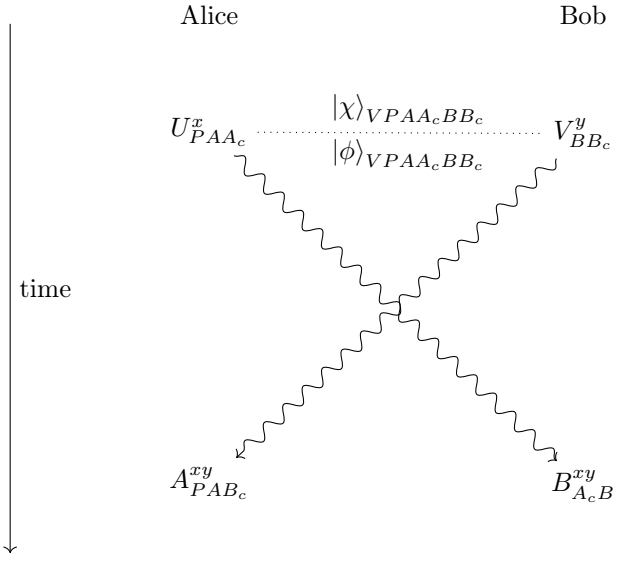

Figure 2: Schematic depiction of a generic attack on $\mathrm{QPV}^f_{\mathrm{coh}_{m_0}}$.

Definition 4.1. *The tuple* $\{|\chi\rangle_{VPAA_cBB_c}, U^x_{PAA_c}, V^y_{BB_c}, A^{xy}_{PAB_c}, B^{xy}_{A_cB}\}_{xy}$ *is a* q-qubit strategy for $\mathrm{QPV}^f_{\mathrm{coh}_{m_0}}$. *Moreover, we say that a* q*-qubit strategy for* $\mathrm{QPV}^f_{\mathrm{coh}_{m_0}}$ *is* (ε, l)*-perfect if for* l *pairs of strings* (x, y)*, for* $\theta \in \{0, \frac{\pi}{2}\}$*,*

$$h(U_\theta|PAB_c)_\phi \leq h(U|P)_\psi + \varepsilon \quad \textit{and} \quad h(U_\theta|A_cB)_\phi \leq h(U|P)_\psi + \varepsilon. \tag{22}$$

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, see 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. Next, we define '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. This restricts the attackers.

Remark 4.2. *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 $|\chi\rangle_{VPAA_cBB_c}$.*

Definition 4.3. *Let $\varepsilon \geq 0$, and let q be the number of qubits that Alice and Bob each hold at the* preparing *stage of a multi-qubit attack on $\mathrm{QPV}^f_{\mathrm{coh}_{m_0}}$. We define $\mathcal{S}^\varepsilon_\theta$ as*

$$\mathcal{S}^\varepsilon_\theta := \{|\phi\rangle_{VPAA_cBB_c} \in \mathbb{C}^{2q+2m_0} \mid \exists \text{ POVMs } \{A^{xy}_{PAB_c}\}, \{B^{xy}_{A_cB}\} \text{ s.t. (22) holds}\}. \tag{23}$$

Proposition 4.4. *Let $\varepsilon > 0$, and $|\phi_0\rangle_{VPAA_cBB_c} \in \mathcal{S}^\varepsilon_0$, and $\left|\phi_{\frac{\pi}{2}}\right\rangle_{VPAA_cBB_c} \in \mathcal{S}^\varepsilon_{\frac{\pi}{2}}$, with bounded energies $\mathrm{Tr}\left[\rho^0 H\right], \mathrm{Tr}\left[\rho^1 H\right] \leq E$, where ρ^0 and ρ^1 are the respective density matrices of $|\phi_0\rangle$ and $\left|\phi_{\frac{\pi}{2}}\right\rangle$. 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*

$$\varepsilon < \frac{1}{2}\log\frac{4t}{e(1+2u)} - \left(\frac{1+\alpha}{2(1-\alpha)} + \alpha\right)\left[2\tilde{\varepsilon}\left(\log(E+1) + \log\frac{e}{\alpha(1-\tilde{\varepsilon})}\right) + 6\tilde{h}\left(\frac{1+\alpha}{1-\alpha}\tilde{\varepsilon}\right)\right]. \tag{24}$$

Then,

$$\frac{1}{2}\||\phi_0\rangle - \left|\phi_{\frac{\pi}{2}}\right\rangle\|_1 > \tilde{\varepsilon}. \tag{25}$$

Notice that the energy bound E is the energy given by the Hamiltonian corresponding to one harmonic oscillator in the V system (21), which approaches σ^2 from below. Moreover, from (24), we see that the ε will need to be picked taking a value at most $\frac{1}{2}\log\frac{4t}{e(1+2u)}$. In order to have non-negative $\tilde{\varepsilon}$, we need

$$4t > e(1+2u), \tag{26}$$

see Fig. 3. The maximum value of ε will be upper bounded by

$$\varepsilon < \frac{1}{2}\log\frac{4t}{e(1+2u)} \leq \frac{1}{2}\log\frac{4}{e} \simeq 0.278652, \tag{27}$$

since the maximum value is reached by $t = 1$ and $u = 0$.

Proof. Let ρ^θ and $\rho^{\bar{\theta}}$ be the density matrices of $|\phi_\theta\rangle_{VPAA_cBB_c}$ and $|\phi_{\bar{\theta}}\rangle_{VPAA_cBB_c}$, respectively. By hypothesis,

$$h(U_\theta|PAB_c)_{\rho^\theta} \leq h(U|P)_\psi + \varepsilon, \text{ and } h(U_{\bar{\theta}}|PAB_c)_{\rho^{\bar{\theta}}} \leq h(U|P)_\psi + \varepsilon. \tag{28}$$

By Lemma 2.5,

$$h(U_\theta|PAB_c)_{\rho^\theta} + h(U_{\bar{\theta}}|A_cB)_{\rho^\theta} \geq \log 2\pi. \tag{29}$$

Then,

$$h(U_{\bar{\theta}}|A_cB)_{\rho^\theta} \geq \log 2\pi - h(U_\theta|PAB_c)_{\rho^\theta} \geq \log 2\pi - h(U|P)_\psi - \varepsilon, \tag{30}$$

where in the last inequality we used (28). Therefore,

$$h(U_{\bar{\theta}}|A_cB)_{\rho^\theta} - h(U_{\bar{\theta}}|PAB_c)_{\rho^{\bar{\theta}}} \geq \log 2\pi - 2h(U|P)_\psi - 2\varepsilon. \tag{31}$$

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

$$h(U_{\bar{\theta}}|A_cB)_{\rho^\theta} - h(U_{\bar{\theta}}|PAB_c)_{\rho^{\bar{\theta}}} \geq \log\frac{4t}{e(1+2u)} - 2\varepsilon > 0, \tag{32}$$

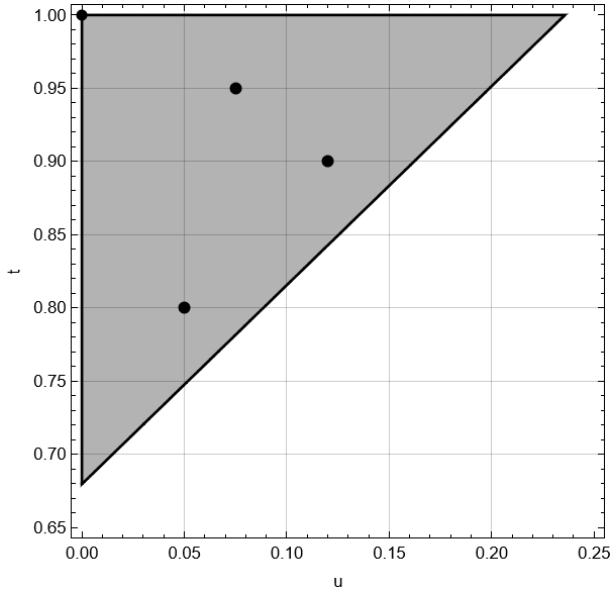

Figure 3: Necessary condition for u and t so that (24) is fulfilled (gray region). The blue dots are specific (u,t) for which we do numerical analysis in Section 5.

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

$$|h(U_{\bar{\theta}}|A_cB)_{\rho^\theta} - h(U_{\bar{\theta}}|PAB_c)_{\rho^{\bar{\theta}}}| \geq \log\frac{4t}{e(1+2u)} - 2\varepsilon, \tag{33}$$

By hypothesis, $\log\frac{4t}{e(1+2u)} - 2\varepsilon > \left(\frac{1+\alpha}{1-\alpha}+2\alpha\right)\left[2\tilde{\varepsilon}\left(\log(E+1)+\log\frac{e}{\alpha(1-\tilde{\varepsilon})}\right)+6\tilde{h}\left(\frac{1+\alpha}{1-\alpha}\tilde{\varepsilon}\right)\right]$. Thus, by the contrapositive of Lemma 2.6,

$$\frac{1}{2}\|\rho^\theta - \rho^{\bar{\theta}}\|_1 > \tilde{\varepsilon}. \tag{34}$$

□

Definition 4.5. *[BCS22] Let $q,k,n\in\mathbb{N}$, $\varepsilon>0$. Then, $g:\{0,1\}^{3k}\to\{0,1\}$ is an $(\varepsilon,1)$-classical rounding of size k if for all $f:\{0,1\}^{2n}\to\{0,1\}$, for all states $|\psi\rangle$ on $2q+2m_0$ qubits, for all $l\in\{1,...,2^{2n}\}$ and for all (ε,l)-perfect q-qubit strategies for $\mathrm{QPV}^f_{\mathrm{coh}_{m_0}}$, there are functions $f_A:\{0,1\}^n\to\{0,1\}^k$, $f_B:\{0,1\}^n\to\{0,1\}^k$ 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 4.6. *[LT91] Let $|||*|||$ 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 $(\mathbb{R}^{n_0},|||*|||)$ of cardinality at most $(1+2/\delta)^{n_0}$.*

Lemma 4.7. *[BCS22] 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 4.8. *Let ε, $\tilde{\varepsilon}$ be such that if $|\varphi_\theta\rangle\in\mathcal{S}^{\tilde{\varepsilon}}_\theta$ and $|\varphi_{\bar{\theta}}\rangle\in\mathcal{S}^{\tilde{\varepsilon}}_{\bar{\theta}}$ implies $\mathcal{P}(|\varphi_\theta\rangle,|\varphi_{\bar{\theta}}\rangle)>\tilde{\varepsilon}$, then there is an (ε,q)-classical rounding of size $k=2^{2q+2m_0}\log\left(1+\frac{4}{\sqrt[3]{4(2+\tilde{\varepsilon})}-2}\right)$.*

Proof. We follow the same techniques as in the proof of Lemma 3.12 in [BCS22]. 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 Euclidean norm and the other nets are for the set of unitaries in dimension 2^q in 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 $\mathcal{S}^{\tilde{\varepsilon}}_\theta$ than to $\mathcal{S}^{\tilde{\varepsilon}}_{\bar{\theta}}$ in purified distance and $g(x,y,\gamma)=1$

if $U \otimes V|\varphi\rangle$ is closer to $\mathcal{S}_{\tilde{\theta}}^{\varepsilon}$ 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, $\mathcal{S}_{\theta}^{\varepsilon} \cap \mathcal{S}_{\tilde{\theta}}^{\varepsilon} = \emptyset$, and thus g is well-defined.

We are going to show that g is an (ε, q)-classical rounding. Consider an arbitrary $f : \{0,1\}^{2n} \to \{0,1\}$ and an arbitrary state $|\chi\rangle$ on $2q + 2m_0$ qubits. Let $|\chi\rangle$, $\{U_A^x, U_B^y\}_{xy}$ be from a q-qubit strategy for $\mathrm{QPV}_{\mathrm{coh}_{m_0}}^{f}$, 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 operator norm, respectively, (if not unique, make an arbitrary choice) and let $|\varphi\rangle, U_A, U_B$ be their corresponding elements. Assume $U_A^x \otimes U_B^y|\chi\rangle \in \mathcal{S}_{\theta}^{\varepsilon}$. Then,

$$\begin{aligned}
\mathcal{P}(U_A^x \otimes U_B^y|\chi\rangle, U_A \otimes U_B|\varphi\rangle) &\leq \|U_A^x \otimes U_B^y|\chi\rangle - U_A \otimes U_B|\varphi\rangle\|_2 \\
&\leq \|(U_A + U_A^x - U_A) \otimes (U_B + U_B^y - U_B)(|\varphi\rangle + |\chi\rangle - |\varphi\rangle) - U_A \otimes U_B|\varphi\rangle\|_2 \\
&\leq 3\delta + 3\delta^2 + \delta^3 < \frac{\tilde{\varepsilon}}{2},
\end{aligned} \tag{35}$$

where in the first inequality, we have used Lemma 4.7, in the second, we have used the triangle inequality and the inequality $\|X \otimes Y|x\rangle\|_2 \leq \|X\|_\infty \|Y\|_\infty \||x\rangle\|_2$, 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 $\mathcal{S}_{\tilde{\theta}}^{\varepsilon}$.
Consider an (ε, l)-perfect strategy for $\mathrm{QPV}_{\mathrm{coh}_{m_0}}^{f}$ and let (x,y) be such that $h(U_\theta|PAB_c)_\varphi, h(U_\theta|A_cB)_\varphi \leq h(U|P)_\psi + \varepsilon$ 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 (35), $f(x,y) = g(f_A(x), f_B(y), \gamma)$. 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 4.6. □

Lemma 4.9. *Let $\varepsilon \in [0,1]$, $E, t, u > 0$ be such that there exist $\tilde{\varepsilon} > 0$ and α such that (24) holds. Let k, $q \in \mathbb{N}$, $n = \Omega(m_0)$. Moreover, fix an (ε, q)-classical rounding g of size k with $k = 2^{2q+2m_0} \log\left(1 + \frac{4}{\sqrt[3]{4(2+\tilde{\varepsilon})}-2}\right)$. Let $q = O(n - m_0)$. Then, with probability $1 - O(\lambda^{2^{m_0}})$*

the following holds:

A uniformly random $f : \{0,1\}^{2n} \to \{0,1\}$ fulfills the following with probability at least $1 - O(2^{-2^n})$:

For any $f_A : \{0,1\}^n \to \{0,1\}^k$, $f_B : \{0,1\}^n \to \{0,1\}^k$, $\gamma \in \{0,1\}^k$, the equality $g(f_A(x), f_B(y), \gamma) = f(x,y)$ holds on less than $3/4$ 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 fulfils $\mathbb{P}_{x,y}[f(x,y) = g(f_A(x), f_B(y), \gamma)] \geq 3/4$. In a similar manner as in [BCS22], we have that

$$\mathbb{P}[f : \exists f_A, f_B, \gamma \text{ s.t. } \mathbb{P}_{x,y}[f(x,y) = g(f_A(x), f_B(y), \gamma)]] \leq 2^{(2^{n+1}+1)k} 2^{2^{2n} h(1/4)} 2^{-2^{2n}}, \tag{36}$$

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

In order to have explicit expressions 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 parameters E, t, u and ε, known by the verifiers, we will be interested in picking values of α such that (24) holds for $\tilde{\varepsilon}$ as large as possible. This needs to be done numerically, since (24) leads to a transcendental equation, see Section 5 for this analysis. This applies as well for the below theorem, which in short states that if the number of qubits the attackers pre-share at the beginning of the protocol, with high probability at least one of them will have a finite gap to the uncertainty of the honest prover regarding the value of the random variable U. That is, at least one attacker will have strictly larger uncertainty than the prover.

Theorem 4.10. *Let $\varepsilon \in [0,1]$, $E, t, u > 0$ (under the control of the verifiers) be such that there exists $\tilde{\varepsilon} > 0$ and α such that (24) holds. Let $n = \Theta(m_0)$. Let the number of qubits that Alice and Bob each control at the beginning of the protocol be*

$$q = O(n - m_0). \tag{37}$$

Then, with probability $1 - O(\lambda^{2^{m_0}})$ *the following holds. A random function* f *fulfills the following with probability at least* $1 - O(2^{-2^n})$ *: the uncertainties for Alice and Bob when attacking the protocol* $\mathrm{QPV}^f_{\mathrm{coh}}$ *are such that*

$$\max\{h(U_\theta|PAB_c)_\phi, h(U_\theta|A_cB)_\phi\} \geq h(U|P)_\psi + \frac{\varepsilon}{4}, \tag{38}$$

for every state $|\phi\rangle \in \mathbb{C}^{2q+2m_0}$*, for* $\theta \in \{0, \frac{\pi}{2}\}$*.*

Proof. By Lemma 4.9, 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 $\mathrm{QPV}^f_{\mathrm{coh}_{m_0}}$. That means that for every strategy, on a fraction at least $\frac{1}{4}$ of (x, y), either $h(U_\theta|PAB_c)_\phi \geq h(U|P)_\psi + \frac{\varepsilon}{4}$ or $h(U_\theta|A_cB)_\phi\} \geq h(U|P)_\psi + \frac{\varepsilon}{4}$. □

4.1 Bounding attack success probability after repeated i.i.d. rounds

For the following, remember that $\sigma \gg 1$, equivalently $\lambda \to 1$. 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. (38) we know that

$$h(U_\theta|E)_\phi \coloneqq \max\{h(U_\theta|PAB_c)_\phi, h(U_\theta|A_cB)_\phi\} \geq h(U|P)_\psi + \frac{\varepsilon}{4} \tag{39}$$

$$= \frac{1}{2}\log\left(\pi e \frac{1/2+u}{t}\right) + \frac{\varepsilon}{4}. \tag{40}$$

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

$$h(R|E)_\phi \geq h(R|P)_\psi + \frac{\varepsilon}{4} \tag{41}$$

$$= \frac{1}{2}\log\left(2\pi e \frac{1/2+u}{t}\right) + \frac{\varepsilon}{4} \tag{42}$$

$$\geq \frac{1}{2}\log(\pi e) + \frac{\varepsilon}{4}, \tag{43}$$

where the last equation follows from eq. (18) and 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 2.7, we can straightforwardly convert this into a lower bound for the estimation error of the attackers. We obtain

$$\mathbb{E}\Big[(R - r')^2\Big] \geq \frac{1}{2\pi e} e^{2h_{\mathrm{nats}}(R|E)_\phi} = \frac{1}{2}e^{\varepsilon/2}. \tag{44}$$

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 $\Delta \coloneqq \frac{1/2}{1/2+u}e^{\varepsilon/2} - \gamma$. Let $(r_i'^{\mathrm{att}})_{i=1}^N$ be the sample of the attackers after N i.i.d. rounds. Then we can then use the Chebyshev inequality for the random variable of the score to get

$$\mathbb{P}\left[\left|\frac{1}{N}\sum_{i=1}^{N}\frac{(\sqrt{t}r_i - r_i'^{\mathrm{att}})^2}{1/2+u} - \frac{\mathbb{E}(\sqrt{t}R - r')^2}{1/2+u}\right| \geq \Delta\right] \leq \frac{\tilde{\sigma}^2}{N\Delta^2} = O\left(\frac{1}{N\Delta^2}\right), \tag{45}$$

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 attack success probability to $\varepsilon_{\mathrm{att}} = \varepsilon_{\mathrm{hon}}$ for simplicity. If we then set $N\Delta^2 = \Omega\left(\frac{1}{\varepsilon_{\mathrm{hon}}}\right)$, we get

$$\mathbb{P}\left[\frac{1}{N}\sum_{i=1}^{N}\frac{(\sqrt{t}R_i - r_i')^2}{1/2+u} \leq \gamma\right] \leq O(\varepsilon_{\mathrm{hon}}). \tag{46}$$

The required number of rounds N can be obtained by first setting the tolerated $\varepsilon_{\mathrm{hon}}$ and then solving $N\Delta^2 = \Omega\left(\frac{1}{\varepsilon_{\mathrm{hon}}}\right)$ for N. This means we accept the honest prover with probability at least $1 - \varepsilon_{\mathrm{hon}}$, while accepting attackers with probability at most $\varepsilon_{\mathrm{hon}}$ after N i.i.d. rounds.

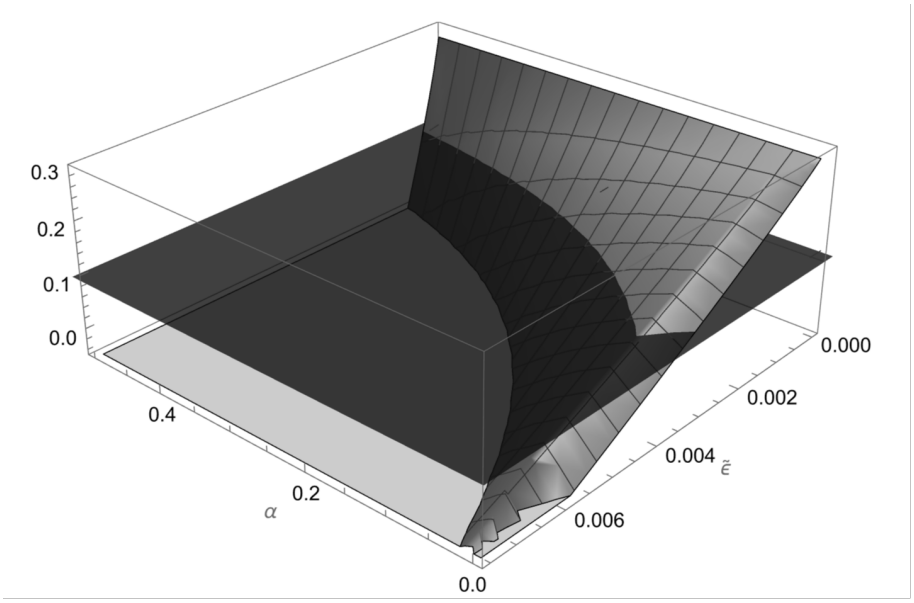

Figure 4: Representation of the left (transparent black) and right (gray surface) hand sides of the inequality (24) for $\varepsilon = 0.1, E = 10^3, t = 1$ and $u = 0$. The region where the gray surface is above the black plain gives the $(\alpha, \tilde{\varepsilon})$ such that the inequality (24) holds.

5 Concrete linear bounds for given experimental parameters

In the above section, we proved that, if V_0 prepares a two-mode squeezed state with squeezing parameter ζ and $\lambda = \tanh \zeta$, with probability $1 - O(\lambda^{2^{m_0}})$ attackers who pre-share $q = O(n - m_0)$ qubits will not be able to mimic arbitrarily close an honest prover. For that, we need that ε, E, t and u are such that exists $\tilde{\varepsilon} > 0$ and α for which (24) holds. In order to have parameters fulfilling (24) for $\varepsilon > 0$ we need that the attenuation parameter t and the excess noise power u of the quantum channel connecting V_0 and P fulfill the relation (26). In the section we analyze perfect and imperfect channels.

5.1 Perfect channel

We start by considering a perfect channel connecting V_0 and P, given by $t = 1$ and $u = 0$. We fix $\varepsilon = 0.1$ and assume the protocol is played enough rounds to statistically distinguish the honest party with an uncertainty

$$h(U|P)_\psi \to \frac{1}{2} \log \frac{\pi e}{2} \simeq 1.0471, \tag{47}$$

from the uncertainty of at least one of the attackers being lower bounded by

$$\frac{1}{2} \log \frac{\pi e}{2} + \frac{\varepsilon}{4} \simeq 1.0721. \tag{48}$$

Fix an energy bound $E = 10^3$ in units such that $\hbar\omega = 1$. Then, the largest $\tilde{\varepsilon}$ that fulfills (24) is

$$\tilde{\varepsilon} \simeq 0.0037, \tag{49}$$

for $\alpha \simeq 0.036$, see Fig. 4 for a representation of the inequality (24) where the value of ε is fixed and represented as the black plane and the gray surface represents the right-hand side of the inequality.

Notice that the energy term in (24) scales as $\tilde{\varepsilon} \log(E + 1)$, i.e. logarithmically in E with a small factor $\tilde{\varepsilon}$ in front. Therefore, the inequality remains very stable with respect to E. For instance, if one picks $E = 10, 10^2, 10^4$, the values of the maximum $\tilde{\varepsilon}$ remain almost unchanged.

For the values of $\varepsilon = 0.1$ and $\tilde{\varepsilon} = 0.004$, the size of the (ε, q)-classical rounding in Proposition 4.8 is $k = 12 \cdot 2^{2q+2m_0}$. Then, (36) in the proof of Proposition 4.8 is strictly upper bounded by 2^{-2^n}

if $q \leq \frac{n}{2} - m_0 - 5$, for $n > 2(m_0 + 5)$. Then, for the above energies, Theorem 4.10 can be restated as follows.

Corollary 5.1. *Let $\varepsilon = 0.1$, $t = 1, u = 0$. Let $n > 2(m_0 + 5)$. Let the number of qubits that each Alice and Bob control at the beginning of the protocol be*

$$q \leq \frac{n}{2} - m_0 - 5. \tag{50}$$

Then, with probability $1 - O(\lambda^{2^{m_0}})$ the following holds. A random function f fulfills the following with probability at least $1 - 2^{-2^n}$: the uncertainties for Alice and Bob when attacking the protocol $\mathrm{QPV}^f_{\mathrm{coh}}$ are such that

$$\max\{h(U_\theta|PAB_c)_\phi, h(U_\theta|A_cB)_\phi\} \geq h(U|P)_\psi + \frac{\varepsilon}{4}, \tag{51}$$

for every state $|\phi\rangle \in \mathbb{C}^{2q+2m_0}$, for $\theta \in \{0, \frac{\pi}{2}\}$.

5.2 Imperfect channel

We do the analysis for an imperfect channel for some (u, t) such that condition (26) is fulfilled. We pick the parameters plotted in Fig. 3. For the values of ε, t and u in Table 1, we find the maximum $\tilde{\varepsilon}$ for $E = 10^3$, and we have the same linear bounds as in Corollary 5.1.

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

Table 1: Maximum value of $\tilde{\varepsilon}$ fulfilling (24) given ε, t and u with its corresponding value of α that attains it.

6 Open problems

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

Acknowledgments

We thank Philip Verduyn Lunel for valuable discussions. RA was supported by the Dutch Research Council (NWO/OCW), as part of the Quantum Software Consortium programme (project number 024.003.037). FS and LEF are supported by the Dutch Ministry of Economic Affairs and Climate Policy (EZK), as part of the Quantum Delta NL programme. BŠ and AAR acknowledge the support from Groeifonds Quantum Delta NL KAT2.

References

[ABB+23] Rene Allerstorfer, Andreas Bluhm, Harry Buhrman, Matthias Christandl, Llorenç Escolà-Farràs, Florian Speelman, and Philip Verduyn Lunel. Making existing quantum position verification protocols secure against arbitrary transmission loss, 2023. arXiv:2312.12614.

[ABM+23] Rene Allerstorfer, Harry Buhrman, Alex May, Florian Speelman, and Philip Verduyn Lunel. Relating non-local quantum computation to information theoretic cryptography, 2023. arXiv:2306.16462.

[ABSL22a] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. On the role of quantum communication and loss in attacks on quantum position verification, 2022. arXiv:2208.04341.

[ABSL22b] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. Towards practical and error-robust quantum position verification, 2022. arXiv:2106.12911.

[ACCM24] Vahid Asadi, Richard Cleve, Eric Culf, and Alex May. Linear gate bounds against natural functions for position-verification, 2024. arXiv:2402.18648.

[ACH+24] Harriet Apel, Toby Cubitt, Patrick Hayden, Tamara Kohler, and David Pérez-García. Security of position-based quantum cryptography limits hamiltonian simulation via holography, 2024. arXiv:2401.09058.

[ACM24] Vahid Asadi, Eric Culf, and Alex May. Rank lower bounds on non-local quantum computation, 2024. arXiv:2402.18647.

[AEFR+23] Rene Allerstorfer, Llorenç Escolà-Farràs, Arpan Akash Ray, Boris Škorić, Florian Speelman, and Philip Verduyn Lunel. Security of a continuous-variable based quantum position verification protocol, 2023. arXiv:2308.04166.

[AF04] R Alicki and M Fannes. Continuity of quantum conditional information. *Journal of Physics A: Mathematical and General*, 37(5):L55–L57, 2004. doi:http://doi.org/10.1088/0305-4470/37/5/L01.

[BCF+14] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. *SIAM Journal on Computing*, 43(1):150–178, 2014. doi:http://doi.org/10.1137/130913687.

[BCS22] Andreas Bluhm, Matthias Christandl, and Florian Speelman. A single-qubit position verification protocol that is secure against multi-qubit attacks. *Nature Physics*, 2022. doi:http://doi.org/10.1038/s41567-022-01577-0.

[BFSS13] Harry Buhrman, Serge Fehr, Christian Schaffner, and Florian Speelman. The garden-hose model. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, ITCS '13. ACM, 2013. doi:http://doi.org/10.1145/2422436.2422455.

[BK11] Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011. doi:http://doi.org/10.1088/1367-2630/13/9/093036.

[CGMO09] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography. In *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference*, volume 5677 of *Lecture Notes in Computer Science*. Springer, 2009. doi:http://doi.org/10.1137/100805005.

[CL15] Kaushik Chakraborty and Anthony Leverrier. Practical position-based quantum cryptography. *Physical Review A*, 92(5), 2015. doi:http://doi.org/10.1103/PhysRevA.92.052304.

[CLA01] Nicolas J. Cerf, Mel Lévy, and Gilles Van Assche. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A*, 63:052311, 2001. doi:http://doi.org/10.1103/PhysRevA.63.052311.

[CM23] Joy Cree and Alex May. Code-routing: a new attack on position verification. *Quantum*, 7, 2023. doi:10.22331/q-2023-08-09-1079.

[Cov99] Thomas M. Cover. *Elements of information theory*. John Wiley & Sons, 1999. doi:http://doi.org/10.1002/047174882X.

[DC22] Kfir Dolev and Sam Cree. Non-local computation of quantum circuits with small light cones, 2022. arXiv:2203.10106.

[Dol22] Kfir Dolev. Constraining the doability of relativistic quantum tasks, 2022. arXiv:1909.05403.

[EFS23] Llorenç Escolà-Farràs and Florian Speelman. Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers. *Phys. Rev. Lett.*, 131:140802, 2023. doi:http://doi.org/10.1103/PhysRevLett.131.140802.

[FBT+14] Fabian Furrer, Mario Berta, Marco Tomamichel, Volkher B. Scholz, and Matthias Christandl. Position-momentum uncertainty relations in the presence of quantum memory. *Journal of Mathematical Physics*, 55(12), 2014. doi:http://doi.org/10.1063/1.4903989.

[GAW+03] Frédéric Grosshans, Gilles Assche, Jerome Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier. Quantum key distribution using Gaussian-modulated coherent states. *Nature*, 421:238–41, 02 2003. doi:http://doi.org/10.1038/nature01289.

[GC19] Alvin Gonzales and Eric Chitambar. Bounds on instantaneous nonlocal quantum computation. *IEEE Transactions on Information Theory*, 66(5):2951–2963, 2019. doi:http://doi.org/10.1109/TIT.2019.2950190.

[GCW+03] Frédéric Grosshans, Nicolas J. Cerf, Jérôme Wenger, Rosa Tualle-Brouri, and Philippe Grangier. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quantum Info. Comput.*, 3(7), 2003. doi:http://doi.org/10.26421/QIC3.s-6.

[GG02] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, 2002. doi:http://doi.org/10.1103/PhysRevLett.88.057902.

[GLW16] Fei Gao, Bin Liu, and QiaoYan Wen. Quantum position verification in bounded-attack-frequency model. *SCIENCE CHINA Physics, Mechanics & Astronomy*, 59(11), 2016. doi:http://doi.org/10.1007/s11433-016-0234-0.

[GPS07] Raul Garcia-Patron Sanchez. *Quantum information with optical continuous variables: from Bell tests to key distribution.* PhD thesis, Université libre de Bruxelles, 2007.

[Hil00] Mark Hillery. Quantum cryptography with squeezed states. *Phys. Rev. A*, 61:022309, 2000. doi:http://doi.org/10.1103/PhysRevA.61.022309.

[KMS11] Adrian Kent, William J. Munro, and Timothy P. Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Physical Review A*, 84(1), 2011. doi:http://doi.org/10.1103/PhysRevA.84.012326.

[KMSB06] Adrian Kent, William Munro, Timothy Spiller, and Raymond Beausoleil. Tagging systems. US patent nr. 2006/0022832, 2006.

[Lev09] Anthony Leverrier. *Theoretical study of continuous-variable quantum key distribution.* Phd thesis, Télécom ParisTech, 2009.

[LL11] Hoi-Kwan Lau and Hoi-Kwong Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Physical Review A*, 83(1), 2011. doi:http://doi.org/10.1103/PhysRevA.83.012322.

[LLQ22] Jiahui Liu, Qipeng Liu, and Luowen Qian. Beating Classical Impossibility of Position Verification. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, volume 215 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 100:1–100:11, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. doi:10.4230/LIPIcs.ITCS.2022.100.

[LPF+18] Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes Hübel. Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations (adv. quantum technol. 1/2018). *Advanced Quantum Technologies*, 1(1):1870011, 2018. URL: https://onlinelibrary.wiley.com/doi/abs/10.1002/qute.201870011, arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/qute.201870011, doi:10.1002/qute.201870011.

[LT91] Michel Ledoux and Michel Talagrand. *Probability in Banach Spaces: Isoperimetry and Processes, volume 23 of A Series of Modern Surveys in Mathematics Series*. Springer, 1991. doi:10.1007/978-3-642-20212-4.

[Mal10a] Robert A. Malaney. Location-dependent communications using quantum entanglement. *Physical Review A*, 81(4), 2010. doi:http://doi.org/10.1103/PhysRevA.81.042319.

[Mal10b] Robert A. Malaney. Quantum location verification in noisy channels. In *IEEE Global Telecommunications Conference GLOBECOM*, 2010. doi:http://doi.org/10.1109/GLOCOM.2010.5684009.

[QS15] Bing Qi and George Siopsis. Loss-tolerant position-based quantum cryptography. *Physical Review A*, 91(4):042337, 2015. doi:http://doi.org/10.1103/PhysRevA.91.042337.

[Ral99] Timothy C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61:010303, 1999. doi:http://doi.org/10.1103/PhysRevA.61.010303.

[Rei00] Margaret D. Reid. Quantum cryptography with a predetermined key using continuous-variable Einstein-Podolsky-Rosen correlations. *Phys. Rev. A*, 62:062308, 2000. doi:http://doi.org/10.1103/PhysRevA.62.062308.

[Spe16] Florian Speelman. Instantaneous Non-Local Computation of Low T-Depth Quantum Circuits. In *11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016)*, volume 61 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 9:1–9:24. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2016. doi:10.4230/LIPIcs.TQC.2016.9.

[Unr14] Dominique Unruh. Quantum position verification in the random oracle model. In *Advances in Cryptology – CRYPTO 2014*. Springer Berlin Heidelberg, 2014. doi:http://doi.org/10.1007/978-3-662-44381-1_1.

[Win16] Andreas Winter. Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints. *Communications in Mathematical Physics*, 347(1), 2016. doi:http://doi.org/10.1007/s00220-016-2609-8.

[WLB+04] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. Quantum cryptography without switching. *Phys. Rev. Lett.*, 93:170504, 2004. doi:http://doi.org/10.1103/PhysRevLett.93.170504.

[WZ82] William K. Wootters and Wojciech Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982. doi:http://doi.org/10.1038/299802a0.