Security of a Continuous-Variable based Quantum Position Verification Protocol

Security of a Continuous-Variable based Quantum Position Verification Protocol

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

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

August 9, 2023

Abstract

In this work we study quantum position verification with continuous-variable quantum states. In contrast to existing discrete protocols, we present and analyze a protocol that utilizes coherent states and its properties. Compared to discrete-variable photonic states, coherent states offer practical advantages since they can be efficiently prepared and manipulated with current technology. We prove security of the protocol against any unentangled attackers via entropic uncertainty relations, showing that the adversary has more uncertainty than the honest prover about the correct response as long as the noise in the quantum channel is below a certain threshold. Additionally, we show that attackers who pre-share one continuous-variable EPR pair can break the protocol.

1 Introduction

Position-based cryptography allows for protocols in which the geographical location of a party is used as a cryptographic credential. Consider, for example, the establishment of trust between you and someone at a claimed location. Or sending a confidential message that can only be decrypted at a specific location. 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], but despite the failure of the classical universal attack, a universal quantum attack has since 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, CM22, BCS22, ABM+23]. Many protocols have since been proposed [CL15, ABSV21, GC19, LLQ22] and different security models have been studied [Unr14, GLW16, Dol19, ABSV22]. 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 [ABSV22, EFS22].

Almost all previously studied QPV protocols have in common that they contain only finite-dimensional quantum systems. The study of QPV using continuous-variable (CV) quantum information, i.e., using infinite-dimensional quantum states, was first mentioned in [QS15], in which a

[1] under the name of 'quantum tagging'

general attack was shown in the transmission regime $t \leq 1/2$, but the security of the protocol was not further analyzed.

The best known example of CV quantum information is the quantized harmonic oscillator [BvL05, CLP07, ALS10], which is usually described by continuous variables such as position and momentum. Continuous-variable quantum systems are particularly 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, the so-called coherent states, and their quadrature squeezed counterparts known as squeezed coherent states. The maiden appearance of CV quantum states in a quantum communication protocol was the CV variant of quantum key distribution (QKD). 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 borrowed from the wealth of research available on CV-QKD. Theoretical reviews with practical considerations of CV-QKD can be found in [GPS07, Lev09].

We extend the ideas of finite-dimensional QPV protocols, and more formally analyze a QPV protocol very similar to the one mentioned in [QS15]. We provide a general proof of security against attackers who do not have access to entanglement, taking into account attenuation and excess noise in the quantum channel. By way of illustration, we also analyze a number of specific attacks. We show that the attackers can break the scheme if they pre-share one pair of strongly entangled modes.

In the finite-dimensional case, usually the job of the prover is to complete a task *correctly*, and attackers are detected by a suspiciously high error rate. This property of QPV protocols changes in the continuous setting, where even the honest prover's answers are drawn from a probability distribution. Therefore, the verifiers' job is to distinguish an honest sample from an adversarial one.

Although the generalization of QPV to CV is interesting in itself, the motivation here is practical. 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 a lot of 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. Furthermore, loss causes a decrease in the signal-to-noise ratio in homodyne measurements rather than giving a "no detection" event. This may open new avenues for protection against the usual lossy attack in discrete variable QPV protocols, in which attackers make use of the "no detection" rounds.

2 Preliminaries

In this section, we introduce the continuous-variable formalism that one encounters in CV-QKD, and some information-theoretic results. The goal of this section is threefold. First, we present the different types of CV states used in the paper. We then discuss displacement measurements that can be performed on these states and how a noisy channel is modeled. Finally, we close the section with some useful results from classical and quantum information theory.

2.1 Gaussian states

The Wigner function fully describes an N-mode bosonic quantum state ρ and can be obtained from ρ by the Wigner formula [Wig32]

$$W(\mathbf{x}, \mathbf{p}) = \frac{1}{\pi^N} \int_{\mathbb{R}^N} e^{2i\mathbf{p}\cdot\mathbf{y}} \langle \mathbf{x} - \mathbf{y} | \rho | \mathbf{x} + \mathbf{y} \rangle \, \mathrm{d}\mathbf{y}. \tag{1}$$

This is sometimes also called the Wigner transformation of the density matrix. The inverse transformation is archived via the Weyl transform. Gaussian states are defined by the property that

their Wigner function is a Gaussian function in phase space. The Wigner function of Gaussian states reads

$$W_{\mathrm{G}}(\mathbf{r}) = \frac{1}{\pi^N \sqrt{\det \Gamma}} \exp\{-(\mathbf{r}-\mathbf{d})^T \Gamma^{-1} (\mathbf{r}-\mathbf{d})\}, \tag{2}$$

where $\mathbf{r} = (x_1, p_1, \ldots, x_N, p_N)$ are the quadrature variables. The vector $\mathbf{d}$ is the displacement vector,

$$d_i = \mathbb{E}\hat{r}_i = \mathrm{Tr}[\rho \hat{r}_i]. \tag{3}$$

And Γ is the covariance matrix,

$$\Gamma_{ij} = \mathrm{Tr}\big[\rho\big((\hat{r}_i - d_i)(\hat{r}_j - d_j) + (\hat{r}_j - d_j)(\hat{r}_i - d_i)\big)\big]. \tag{4}$$

2.2 Displacement measurements of CV states

Here we describe homodyne and heterodyne measurements, the two types of possible displacement measurements. For the physics of the measurement process, refer to Chapter 1 of [GPS07].

Homodyne

Consider a Wigner function $W(\mathbf{x}, \mathbf{p})$. A homodyne measurement of the quadrature x_i, yields the following marginal probability distribution

$$f_{X_i}(x_i) = \int_{\mathbb{R}^{2N-1}} W(\mathbf{x}, \mathbf{p})\, \mathrm{d}\mathbf{p}\, \mathrm{d}x_1 \ldots \mathrm{d}x_{i-1}\, \mathrm{d}x_{i+1} \ldots \mathrm{d}x_N. \tag{5}$$

One can choose any axis x_θ along which to perform a homodyne measurement, given a mode. In this case, we rotate our reference frame corresponding to the mode to be measured by an angle θ. We can then perform an integral similar to the one above to obtain $f_{X_\theta}(x_\theta)$.

Heterodyne

A heterodyne measurement is essentially a double homodyne measurement. The selected mode from $W(\mathbf{x}, \mathbf{p})$ is mixed with vacuum on a balanced beamsplitter. A homodyne measurement is then performed on the two output modes, each in conjugate directions. The result obtained is captured by the theorem which follows.

Theorem 2.1. *The heterodyne measurement of a one-mode Gaussian state with displacement (x_0, p_0), produces two Gaussian distributions, centered around $x_0/\sqrt{2}$ and $-p_0/\sqrt{2}$ respectively.*

Proof. A balanced beamsplitter is represented by the following symplectic matrix

$$S = \begin{pmatrix} \sqrt{\frac{1}{2}}\mathbb{1}_2 & \sqrt{\frac{1}{2}}\mathbb{1}_2 \\ -\sqrt{\frac{1}{2}}\mathbb{1}_2 & \sqrt{\frac{1}{2}}\mathbb{1}_2 \end{pmatrix}. \tag{6}$$

As the input state is Gaussian, and mixing preserves Gaussian states, the output states are also Gaussian. The new displacements under this transformation are the given by

$$(x_0, p_0, 0, 0) S^T = (x_0/\sqrt{2}, p_0/\sqrt{2}, -x_0/\sqrt{2}, -p_0/\sqrt{2}). \tag{7}$$

□

Noisy CV channel

Whereas a discrete qubit state passing through a noisy channel suffers from qubit loss, bit errors, and phase errors, a continuous-variable state gets attenuated and acquires excess noise. Consider a coherent state with displacement (x_0, p_0). Let $t \in [0, 1]$ be the attenuation parameter, and let

$u \geq 0$ denote the excess noise power.[2] The effect of the channel is that the displacement becomes $(x_0, p_0)\sqrt{t}$, and the covariance matrix goes from $\mathbb{1}_2$ to $\mathbb{1}_2(1+2u)$. The outcome of a homodyne measurement now has the variance $\frac{1}{2}+u$ instead of just the $\frac{1}{2}$ from shot noise. In terms of signal and noise, the signal has changed by a factor t and the noise has increased by a factor $1+2u$. Overall, the signal-to-noise ratio has changed by a factor $\frac{t}{1+2u}$.

2.3 Continuous-variable EPR state and teleportation

Consider two modes labeled A and B. The Wigner function of the two-mode squeezed vacuum state (TMSV) with squeezing parameter $\zeta \geq 0$ is given by

$$\begin{aligned} W_{\text{TMSV}}(x_a, p_a, x_b, p_b) &= \frac{1}{\pi^2} \exp\{-e^{-2\zeta}[(x_a+x_b)^2 + (p_a-p_b)^2] - e^{2\zeta}[(x_a-x_b)^2 + (p_a+p_b)^2]\} \\ &= \frac{1}{\pi^2} \exp\left\{ -\begin{pmatrix} x_a & p_a & x_b & p_b \end{pmatrix} \Gamma(\zeta)^{-1} \begin{pmatrix} x_a \\ p_a \\ x_b \\ p_b \end{pmatrix} \right\}, \end{aligned} \tag{8}$$

with covariance matrix

$$\Gamma(\zeta) = \begin{pmatrix} \cosh(2\zeta)\mathbb{1}_2 & \sinh(2\zeta)Z \\ \sinh(2\zeta)Z & \cosh(2\zeta)\mathbb{1}_2 \end{pmatrix}, \qquad \text{where} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{9}$$

Throughout this paper $\mathbb{1}_n$ denotes the n-dimensional identity matrix. In the limit of the squeezing parameter $\zeta \to \infty$ we have $W_{\text{TMSV}}(x_a, p_a, x_b, p_b) \to C\delta(x_a - x_b)\delta(p_a + p_b)$, for a constant C, which corresponds to the continuous-variable maximally entangled EPR state.

Consider a heterodyne measurement performed on the A mode. The state of the A mode, viewed in isolation, is a thermal state with covariance matrix $K_A = \mathbb{1}_2 \cosh 2\zeta$. Using a 50/50 beamsplitter this state gets mixed with the vacuum, resulting in a two-mode $A'A''$ state with covariance matrix

$$K_{A'A''} = \frac{1}{2}\begin{pmatrix} \mathbb{1}_2 + K_A & \mathbb{1}_2 - K_A \\ \mathbb{1}_2 - K_A & \mathbb{1}_2 + K_A \end{pmatrix} = \begin{pmatrix} \mathbb{1}_2 \cosh^2\zeta & -\mathbb{1}_2 \sinh^2\zeta \\ -\mathbb{1}_2 \sinh^2\zeta & \mathbb{1}_2 \cosh^2\zeta \end{pmatrix}. \tag{10}$$

In mode A' the x-quadrature is measured, and in mode A'' the p-quadrature. The Wigner function for $x_{a'}$ and $p_{a''}$ is obtained by integrating out $p_{a'}$ and $x_{a''}$ from the Wigner function $A'A''$, resulting in a product of two Gaussian distributions, $\mathcal{N}_{0,\frac{1}{2}\cosh^2\zeta}(x_{a'})\mathcal{N}_{0,\frac{1}{2}\cosh^2\zeta}(p_{a''})$.

If the heterodyne measurement has resulted in $(x_{a'}, p_{a''})$, then the post-measurement state of the B subsystem is a Gaussian state with displacement $(x_B, p_B) = (x_{a'}, -p_{a''})\sqrt{2}\tanh\zeta$ and covariance $\mathbb{1}_2$, i.e. a coherent state (see chapter 2 of [Lev09]). Note that the components x_B and p_B are Gaussian-distributed with variance $\frac{1}{2}\cosh^2\zeta \cdot (\sqrt{2}\tanh\zeta)^2 = \sinh^2\zeta$. In Section 3.2 we tune $\sinh\zeta = \sigma$ so that x_B, p_B have Gaussian statistics with variance σ^2.

Teleportation

The teleportation of an unknown continuous-variable quantum state using a CV EPR pair was proposed by Vaidman [Vai94] and is described as follows:

1. Alice and Bob share a CV-EPR pair described by the Wigner function (8). Alice possesses the single-mode quantum state $|\psi\rangle$ to be teleported.

2. With a balanced beamsplitter, Alice mixes $|\psi\rangle$ with her mode of the CV-EPR pair and then does a measurement of the x-quadrature in one mode and the p-quadrature in the other mode (i.e. she performs a heterodyne measurement). We denote the outcome of the measurement as (d_x, d_p). The result is that Bob's half of the EPR pair is transformed to a displaced version of $|\psi\rangle$, with displacement $(\sqrt{2}d_x, -\sqrt{2}d_p)$. Alice sends the classical (d_x, d_p) to Bob.

[2] In the CVQKD literature the excess noise power is often written as $\frac{1}{2}t\xi$, where the proportionality with t comes from the fact that the adversary mixes in his own quantum state using the same beamsplitter that also taps off part of the sender's state. In our case we have no such adversarial action.

3. Bob applies a displacement $(-\sqrt{2}d_x, \sqrt{2}d_p)$ to his state to obtain $|\psi\rangle$.

2.4 Information theory

We now define some basic notions of information theory that will be used in the paper. First, we present some definitions and properties regarding CV entropies.

Definition 2.2. *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*

$$h(X) = -\int_{\mathcal{X}} f(x) \log f(x)\, \mathrm{d}x, \tag{11}$$

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

Lemma 2.3. *Let $\alpha > 0$ and $X \in \mathbb{R}$. It holds that $h(\alpha X) = h(X) + \log \alpha$.*

Definition 2.4. *The von Neumann entropy of a state ρ is defined as $S(\rho) = -\operatorname{Tr}[\rho \log \rho]$.*

The von Neumann entropy of Gaussian states is provided by the following lemma, which will be needed to calculate entropies of the honest prover.

Lemma 2.5. *[HSH99] Let ρ be an N-mode CV Gaussian state with $2N \times 2N$ covariance matrix Γ. Let $\nu_1, \ldots, \nu_N$ be the symplectic eigenvalues of Γ. Let the function g be given by*

$$g(x) = (x+1)\log(x+1) - x \log x. \tag{12}$$

The von Neumann entropy of ρ is given by

$$S(\rho) = \sum_{i=1}^{N} g\left(\frac{\nu_i - 1}{2}\right). \tag{13}$$

Lemma 2.6. *[Lev09] The symplectic eigenvalue of a single-mode covariance matrix Γ is given by $\sqrt{\det \Gamma}$.*

In Section 3.3.3 we consider $\sigma \gg 1$ and are interested in the behavior of g in that regime. The following lemma is not too hard to see from (12).

Lemma 2.7. *The large-argument behavior of the function g, defined in (12), is given by $g(x) \sim \log(ex) + \mathcal{O}(1/x)$.*

Another useful quantity to compare two quantum states is the relative entropy.

Definition 2.8. *Let ρ and σ be two density matrices. Their* Umegaki's quantum relative entropy *$D(\cdot||\cdot)$ is defined as*

$$D(\rho||\sigma) = \operatorname{Tr}[\rho \log \rho - \rho \log \sigma]. \tag{14}$$

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 2.9. *The* quantum conditional von Neumann entropy *is defined as*

$$H(Q_\alpha|B)_\rho := -\sum_{k\in\mathbb{Z}} D(\rho_B^{k;\alpha}||\rho_B). \tag{15}$$

Definition 2.10. *We define the* differential quantum conditional von Neumann entropy *is defined as*

$$h(X|B)_\rho := -\int_{\mathbb{R}} D(\rho_B^x||\rho_B)\,\mathrm{d}x. \tag{16}$$

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 2.11. *[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*

$$h(Q|B)_\rho + h(P|C)_\rho \geq \log(2\pi). \tag{17}$$

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

Theorem 2.12. *[Cov99] Let X be a random variable and $\hat{X}(Y)$ an estimator of X given side information Y, then*

$$\mathbb{E}\left[\left(X - \hat{X}(Y)\right)^2\right] \geq \frac{1}{2\pi e} e^{2h_{\mathrm{nats}}(X|Y)}, \tag{18}$$

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 the equality holds.

3 The Protocol

3.1 Prepare-and-measure

Consider two spatially separated verifiers V_1 and V_2, and a prover P somewhere in between them. Let $\mathcal{A}$ be a publicly known set of angles in $[0, 2\pi)$ such that $\alpha \in \mathcal{A} \implies \alpha + \pi/2 \in \mathcal{A}$. Let σ be a publicly known parameter, $\sigma \gg 1$. A single round of the protocol consists of the following steps (for a diagrammatic picture see Fig. 1):

1. The verifiers draw random $\theta \in \mathcal{A}$ and two random variables $(r, r^\perp)$ from the Gaussian distribution $\mathcal{N}_{0,\sigma^2}$. Verifier V_1 prepares a coherent state $|\psi\rangle$ with quadratures $(x_0, p_0) = (r\cos\theta + r^\perp \sin\theta,\ r\sin\theta - r^\perp\cos\theta)$. Then V_1 sends $|\psi\rangle$ to the prover, and V_2 sends θ to the prover.

2. The prover receives θ and $|\psi\rangle$ and performs a homodyne measurement on $|\psi\rangle$ in the θ direction, resulting in a value $r' \in \mathbb{R}$. The prover sends r' to both verifiers.

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

$$\frac{1}{n}\sum_{i=1}^{n} \frac{\left(r'_i - r_i\sqrt{t}\right)^2}{\frac{1}{2} + u} < \gamma \qquad \text{with } \gamma \stackrel{\text{def}}{=} 1 + \frac{2}{\sqrt{n}}\sqrt{\ln\frac{1}{\varepsilon_{\mathrm{hon}}}} + \frac{2}{n}\ln\frac{1}{\varepsilon_{\mathrm{hon}}}. \tag{19}$$

Here $\varepsilon_{\mathrm{hon}}$ is an upper bound on the honest prover's failure probability, see Section 3.3. $\varepsilon_{\mathrm{hon}}$ is a protocol parameter and can be set to a desired value. The verifiers *reject* if not all these checks are satisfied. We refer to the sum in (19) as the *score*.

3.2 Entanglement based version of the protocol

In security proofs for qubit-based schemes, it is customary to re-formulate a protocol into an EPR based form. The act of one party (V) preparing and sending a qubit state in a particular basis $\mathcal{B}$ is equivalent to V preparing a maximally entangled two-qubit state (EPR pair) and then measuring

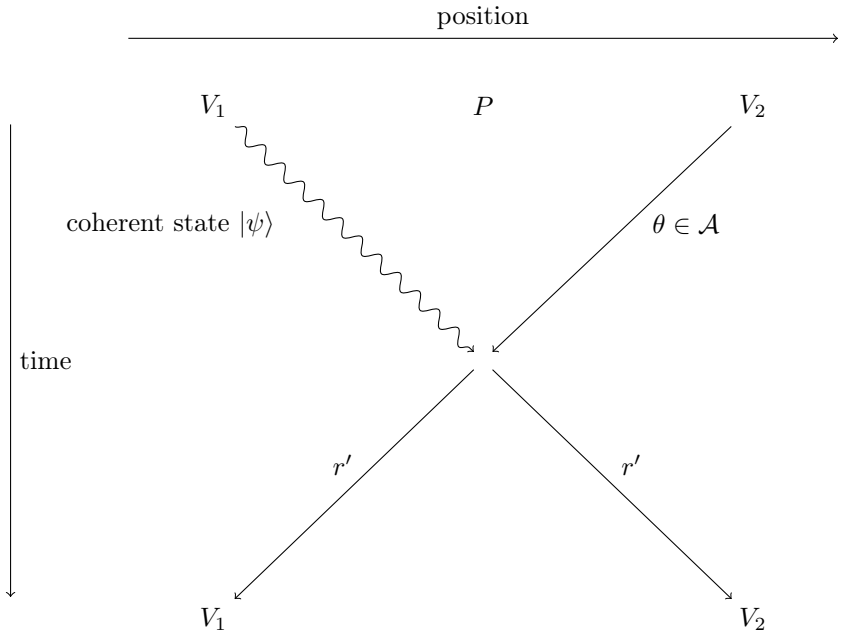

Figure 1: Schematic representation of the protocol described in Section 3.1. Undulated lines represent quantum information, whereas straight lines represent classical information.

one of the qubits in the $\mathcal{B}$ basis while the other qubit is sent. The act of measuring can be postponed. This has the advantage that in the security analysis the basis choice can be delayed, and it is then possible to base security on the properties of entangled states.

We will do an analogous reformulation for CV states. In fact, we work with exactly the same states as Gaussian-modulated CV-QKD [LPF+18]. We tune the squeezing parameter ζ such that $\sinh\zeta = \sigma$, as explained in Section 2.3. Preparing 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 ζ and then performing a heterodyne $(\hat{x}, \hat{p})$ measurement on one mode, with measurement outcome $\frac{(x_0,-p_0)}{\sqrt{2}\tanh\zeta}$.

In our particular case, the verifier V_1 prepares the two-mode squeezed state ρ_{VP} and performs the heterodyne measurement with quadratures that are rotated by the angle θ on the V subsystem. The measurement outcomes are $r/(\sqrt{2}\tanh\zeta)$ and $-r^\perp/(\sqrt{2}\tanh\zeta)$, resulting in displacement $(r, r^\perp)$ in the state sent to the prover (i.e. subsystem P). The prover then performs a homodyne measurement under angle θ to recover r, similar to the prepare and measure scheme.

In the security analysis in Section 5 we will explicitly write V_1's heterodyne measurement as a double-homodyne measurement. First V_1 mixes its own mode with the vacuum using a beamsplitter, resulting in a two-mode state. On one of these modes V_1 then performs a homodyne measurement in the θ-direction, on the other mode in the $\theta + \frac{\pi}{2}$ direction.

3.3 Honest prover

3.3.1 Success probability

We show that the honest prover has a failure probability smaller than ε_{hon}.

Lemma 3.1. *(Eq.(4.3) in [LM00]) Let X be a χ^2_n distributed random variable. It holds that*

$$\mathbb{P}[X - n \geq 2\sqrt{na} + 2a] \leq e^{-a}. \tag{20}$$

In round i, the honest prover performs a homodyne measurement under an angle θ_i, on a coherent state that has displacement r_i in the θ_i direction (and displacement $r_i^\perp$ in the $\theta_i + \frac{\pi}{2}$ direction). The measurement outcome R'_i is Gaussian-distributed with mean r_i and variance $\frac{1}{2}$ (shot noise).

The random variable $Z = \sum_{i=1}^{n} (R'_i - r_i\sqrt{t})^2/(\frac{1}{2}+u)$ is chi-square distributed with parameter n, i.e. $Z \sim \chi^2_n$. The probability that the honest prover fails to pass verification is given by

$$\mathbb{P}[Z \geq n\gamma] = \mathbb{P}\left[Z \geq n + 2\sqrt{n \ln \frac{1}{\varepsilon_{\text{hon}}}} + 2\ln\frac{1}{\varepsilon_{\text{hon}}}\right]. \tag{21}$$

By Lemma 3.1 this is upper bounded by ε_{hon}.

3.3.2 A posteriori distribution and entropy of R conditioned on measurement

We determine how much uncertainty the honest prover has about the displacements r_i, given the measurement outcomes r'_i. For notational brevity we omit the round index i. We write the probability density for R as f_R. Since r' is the result of a measurement under angle θ, conditioning on θ is implicit and will be omitted from the notation.

The prover's posterior distribution of R, given r', is

$$f_{R|R'}(r|r') = \frac{f_{RR'}(r,r')}{f_{R'}(r')} = \frac{f_R(r) f_{R'|R}(r'|r)}{f_{R'}(r')}. \tag{22}$$

Using $f_R = \mathcal{N}_{0,\sigma^2}$, $f_{R'|R}(r'|r) = \mathcal{N}_{r\sqrt{t},\frac{1}{2}+u}(r')$ and $f_{R'} = \mathcal{N}_{0,t\sigma^2+\frac{1}{2}+u}$ we get, after some algebra,

$$f_{R|R'}(r|r') = \mathcal{N}_{M,\Sigma^2}(r) \qquad \text{with } \Sigma^2 \stackrel{\text{def}}{=} \left(\frac{1}{\sigma^2} + \frac{t}{1/2+u}\right)^{-1}, \quad M \stackrel{\text{def}}{=} \frac{r'}{\sqrt{t}} \cdot \frac{1}{1+\frac{1/2+u}{t\sigma^2}}. \tag{23}$$

For $t\sigma^2 \gg 1$ this tends to a normal distribution centered on $r'/\sqrt{t}$, with variance $(\frac{1}{2}+u)/t$. From the Gaussian probability density function (23) we directly obtain the differential entropy of R given R',

$$h(R|R') = \frac{1}{2}\log 2\pi e \Sigma^2. \tag{24}$$

3.3.3 Entropy of R conditioned on the prover's quantum state

Let ρ_{VP} be the entangled state that is prepared by V_1 as described in Section 3.2. Here P denotes the prover's quantum system. The heterodyne measurement on the V system yields $(r, r^\perp)$. The measurement maps ρ_{VP} to $\rho_{RR^\perp P}$. We write the post-measurement state as

$$\rho_{RR^\perp P} = \int_{\mathbb{R}^2} f_{RR^\perp}(r,r^\perp) |r\rangle\langle r|_R \otimes |r^\perp\rangle\langle r^\perp|_{R^\perp} \otimes \rho_P^{rr^\perp} \, \mathrm{d}r\mathrm{d}r^\perp. \tag{25}$$

The (differential) entropy of R, conditioned on the prover's quantum state, can be expanded as

$$h(R|P) = h(R) + S(P|R) - S(P). \tag{26}$$

From the definition of conditional entropy, $S(P|R) = \mathbb{E}_r S(\mathbb{E}_{r^\perp} \rho_P^{rr^\perp})$ and $S(P) = S(\mathbb{E}_{r,r^\perp} \rho_P^{rr^\perp})$. As discussed in Section 3.2, $\rho_P^{rr^\perp}$ would be a coherent state in an ideal case. However, in a noisy channel, the state becomes a Gaussian with covariance matrix $(1+2u)\mathbb{1}_2$ and displacement $(x_0\sqrt{t}, p_0\sqrt{t})$. The expectations are Gaussian integrals and hence are exactly solvable. Solving these integrals, we end up with the corresponding Gaussian Wigner functions and symplectic eigenvalues

$$\text{for } \mathbb{E}_{r^\perp}\rho_P^{rr^\perp}: \quad W_r(x,p) \sim \exp\left(-\frac{p^2}{2\sigma^2 t + 2u + 1} - \frac{\left(x - r\sqrt{t}\right)^2}{2u+1}\right), \quad \nu = \sqrt{2t\sigma^2 + 2u + 1}, \tag{27}$$

$$\text{for } \mathbb{E}_{r,r^\perp}\rho_P^{rr^\perp}: \quad W(x,p) \sim \exp -\frac{p^2 + x^2}{2\sigma^2 t + 2u + 1}, \quad \nu = 2t\sigma^2 + 2u + 1. \tag{28}$$

We use the g function (cf. lemma 2.5) to calculate the corresponding entropy

$$S(P|R) = g\left(\frac{1}{2}\sqrt{2t\sigma^2 + 2u + 1} - \frac{1}{2}\right), \tag{29}$$

$$S(P) = g(t\sigma^2 + u). \tag{30}$$

Finally, by definition R is Gaussian and $h(R) = \frac{1}{2}\log 2\pi e\sigma^2$. All together this yields

$$h(R|P) = \frac{1}{2}\log 2\pi e\sigma^2 + g\left(\frac{1}{2}\sqrt{2t\sigma^2+2u+1}-\frac{1}{2}\right) - g(t\sigma^2+u) \overset{\text{Lemma 2.7}}{=} \frac{1}{2}\log\frac{\pi et}{1+2u} + O\left(\frac{1}{\sigma}\right). \tag{31}$$

For large σ this is essentially the same as $h(R|R')$ in (24).

4 Security against specific attacks

Before showing security against a general attack, we highlight security against some specific attacks that one might naturally think of. We look into three specific attacks where the adversaries do not have access to entanglement: performing a heterodyne measurement, state splitting and performing a homodyne measurement under a guessed angle. These examples provide some insight into the security but do not constitute a general security proof. A rigorous security proof for the case of adversaries who do not pre-share entanglement is given in Section 5.

The most general attack of a 1-dimensional QPV protocol consists of placing two attackers Alice A and Bob B between V_1 and P, and V_2 and P, respectively. For attackers that do not pre-share entanglement,[3] an attack proceeds as follows. Alice intercepts the quantum state sent to the prover P. Alice applies a local operation to her quantum system and sends some classical and/or quantum information to the second attacker Bob. The most general action Bob can take is to intercept the message θ and broadcast it, since any quantum operation can be embedded in Alice's actions. After one round of simultaneous communication, Alice and Bob use their respective quantum and classical information to produce a classical output and respond to their closest verifier such that the answer arrives on time. For the following analysis, we describe the attacks per round of the protocol.

4.1 Heterodyne attack

In a *heterodyne attack*, Alice performs a heterodyne measurement on the coherent state she intercepts and sends the result (x', p') to Bob. At the end, A and B report the best guess for r that they can produce based on x', p', θ. Let us denote this as the estimator $\tilde{r}$. It holds that $\tilde{r} = \tilde{x}\cos\theta + \tilde{p}\sin\theta$, where $\tilde{x}$ is an estimator for x_0, and similarly $\tilde{p}$. The posterior distribution of x_0 given x' is

$$f_{X_0|X'}(x_0|x') = \frac{f_{X_0}(x_0)f_{X'|X_0}(x'|x_0)}{f_{X'}(x')} = \frac{\mathcal{N}_{0,\sigma^2}(x_0)\mathcal{N}_{\frac{x_0}{\sqrt{2}},\frac{1}{2}}(x')}{\mathcal{N}_{0,\frac{\sigma^2}{2}+\frac{1}{2}}(x')} = \mathcal{N}_{x'\sqrt{2}\frac{\sigma^2}{1+\sigma^2},\frac{\sigma^2}{1+\sigma^2}}(x_0). \tag{32}$$

Hence $\tilde{x} = x'\sqrt{2}\frac{\sigma^2}{1+\sigma^2}$ and $\tilde{p} = -p'\sqrt{2}\frac{\sigma^2}{1+\sigma^2}$. Given x_0, y_0, θ, the random variable $\tilde{R}$ is Gaussian with mean $\frac{\sigma^2}{1+\sigma^2}r$ and variance $\frac{1}{2}(\sqrt{2}\frac{\sigma^2}{1+\sigma^2}\cos\theta)^2 + \frac{1}{2}(\sqrt{2}\frac{\sigma^2}{1+\sigma^2}\sin\theta)^2 = (\frac{\sigma^2}{1+\sigma^2})^2$. This gives

$$\mathbb{E}(\tilde{R}-r)^2 = \left(\frac{\sigma^2}{1+\sigma^2}\right)^2 + r^2\left(\frac{1}{1+\sigma^2}\right)^2 \approx 1 \qquad \text{for } \sigma \gg 1, \tag{33}$$

which is easily distinguishable from the honest prover's value $\frac{1}{2}$.[4] From (32) we obtain the variance of R from the attackers' point of view as $\frac{\sigma^2}{1+\sigma^2}(\cos\theta)^2 + \frac{\sigma^2}{1+\sigma^2}(\sin\theta)^2 = \frac{\sigma^2}{1+\sigma^2}$. The attackers' ignorance about R is thus quantified as

$$h(R|X'P'\Theta) = \frac{1}{2}\log\left(2\pi e\frac{\sigma^2}{1+\sigma^2}\right), \tag{34}$$

with conditioning on Θ being made explicit.

[3] We restrict our analysis to the case where the attackers do not pre-share entanglement, since we show in Section 6 that there exists a perfect attack if they pre-share an EPR pair.

[4] Note that the unbiased estimator $x'\sqrt{2}\cos\theta - p'\sqrt{2}\sin\theta$ would yield $\mathbb{E}(\tilde{R}-r)^2 = 1$, which is larger than (33).

4.2 Splitting attack

In a *splitting attack*, Alice intercepts the coherent quantum state sent by V_1, and as in the case of the previous attack, she used a beamsplitter to mix it with a state of her own. She now sends one of the outputs from the beamsplitter to Bob. This allows both attackers to perform a homodyne measurement under the correct angle θ. Unlike the heterodyne attack, this also allows the attackers the freedom to choose the transmittance parameter T and the quantum state that Alice uses. However, the attackers must be cautious to report a set of numbers that have identical means and variances. To see why, let us assume that Alice reports numbers with mean m_a and Bob's results have the mean m_b. Let the respective variances be $v_a = v_b$. The verifiers can immediately identify an attack if the results have a dissimilar average. To avoid this, Alice (or Bob) must multiply their results with a finite number c such that $m_b = cm_a$ (or $m_a = cm_b$). However, it would lead to the verifiers possessing a final distribution with indeed the same mean, but different variances. The precision of the protocol can be altered to detect said variance. A similar argument can be constructed when the variances are unequal. Thus, a successful attack must follow $m_a = m_b$ and $v_a = v_b$. Now, we propose the following theorem.

Theorem 4.1. *Consider a 2-mode Gaussian Wigner function $W_{\mathbf{d},\gamma}(x_1, p_1, x_2, p_2)$ which under a beamsplitter transformation of transmittance T transforms into $W'_{\mathbf{d}',\gamma'}(x'_1, p'_1, x'_2, p'_2)$. If $|\mathbb{E}[r'_1]| = |\mathbb{E}[r'_2]|$ and $\mathrm{var}(r'_1) = \mathrm{var}(r'_2)$, then $\mathbf{d}_2 = 0$ and $T = 1/2$, for $r \in \{x, p\}$. Here, $\mathbf{d} = (\mathbf{d}_1, \mathbf{d}_2)$ and $\mathbf{d}' = (\mathbf{d}'_1, \mathbf{d}'_2)$.*

Proof. We have the following relationship between the covariance matrices of the input and output states

$$\gamma' = S\gamma S^T. \tag{35}$$

Where S is the symplectic matrix corresponding to a beamsplitter with transmittance T given by

$$S = \begin{pmatrix} \sqrt{T}\mathbb{1}_2 & \sqrt{1-T}\mathbb{1}_2 \\ -\sqrt{1-T}\mathbb{1}_2 & \sqrt{T}\mathbb{1}_2 \end{pmatrix}. \tag{36}$$

The input matrix γ is the direct sum of the constituent matrices,

$$\gamma = \gamma_1 \oplus \gamma_2. \tag{37}$$

Assuming some displacements $\mathbf{d}'$, we calculate the exponent in $W_{\mathbf{d}',\gamma'}$,

$$(\mathbf{r}_1 - \mathbf{d}'_1, \mathbf{r}_2 - \mathbf{d}'_2)\gamma'^{-1}(\mathbf{r}_1 - \mathbf{d}'_1, \mathbf{r}_2 - \mathbf{d}'_2)^T. \tag{38}$$

Substituting, after some matrix multiplications

$$(\mathbf{r}_1 - \mathbf{d}'_1, \mathbf{r}_2 - \mathbf{d}'_2)\gamma'^{-1}(\mathbf{r}_1 - \mathbf{d}'_1, \mathbf{r}_2 - \mathbf{d}'_2)^T \tag{39}$$

$$= (\mathbf{r}_1 - \mathbf{d}'_1, \mathbf{r}_2 - \mathbf{d}'_2)\frac{1}{D}\begin{pmatrix} (T\gamma_2 + (1-T)\gamma_1)\mathbb{1}_2 & \sqrt{T(1-T)}(\gamma_2 - \gamma_1)\mathbb{1}_2 \\ \sqrt{T(1-T)}(\gamma_2 - \gamma_1)\mathbb{1}_2 & (T\gamma_1 + (1-T)\gamma_2)\mathbb{1}_2 \end{pmatrix}\begin{pmatrix} \mathbf{r}_1 - \mathbf{d}'_1 \\ \mathbf{r}_2 - \mathbf{d}'_2 \end{pmatrix} \tag{40}$$

$$= \frac{1}{D}\big((T\gamma_2 + (1-T)\gamma_1)(\mathbf{r}_1 - \mathbf{d}'_1)^2 + (T\gamma_1 + (1-T)\gamma_2)(\mathbf{r}_2 - \mathbf{d}'_2)^2\big), \tag{41}$$

where D is the determinant of γ'. We are given that $\mathrm{var}(r'_1) = \mathrm{var}(r'_2)$. From the construction of the Wigner function, it is clear that the coefficients in (41) must be identical for this to be true, so

$$T\gamma_2 + (1-T)\gamma_1 = T\gamma_1 + (1-T)\gamma_2 \Rightarrow T = 1/2. \tag{42}$$

The displacement transforms as

$$(\mathbf{d}'_1, \mathbf{d}'_2) = (\mathbf{d}_1, \mathbf{d}_2)S^T = (\sqrt{T}\mathbf{d}_1 + \sqrt{1-T}\mathbf{d}_2, -\sqrt{1-T}\mathbf{d}_1 + \sqrt{T}\mathbf{d}_2). \tag{43}$$

As $|\mathbb{E}[r'_1]| = |\mathbb{E}[r'_2]|$ (or $|\mathbf{d}'_1| = |\mathbf{d}'_2|$),

$$|\sqrt{T}\mathbf{d}_1 + \sqrt{1-T}\mathbf{d}_2| = |-\sqrt{1-T}\mathbf{d}_1 + \sqrt{T}\mathbf{d}_2|. \tag{44}$$

The only meaningful case from this equation yields

$$\mathbf{d}_2 = \frac{\sqrt{T} - \sqrt{1-T}}{\sqrt{T} + \sqrt{1-T}} \mathbf{d}_1. \tag{45}$$

When $T = 1/2$, this leads to $\mathbf{d}_2 = \mathbf{0}$. □

The above theorem fixes the displacement and the transmittance parameter. However, as we see, there is no restriction on the attackers for choosing the covariance matrix for their quantum state. Since the strongest attack must have the smallest spread, the natural choice is indeed the minimum uncertainty state, that is, a state with unit covariance.

Hence, the strongest attack is carried out by mixing a vacuum state with the target using a balanced beamsplitter.

After mixing, A and B have a coherent state with displacement $\frac{(x_0,p_0)}{\sqrt{2}}$ and $-\frac{(x_0,p_0)}{\sqrt{2}}$ respectively. Taking into account that B compensates for the minus sign, a homodyne measurement under the correct angle θ yields an outcome u with distribution $f_{U|R}(u|r) = \mathcal{N}_{\frac{r}{\sqrt{2}},\frac{1}{2}}(u)$ for both attackers. Their a posteriori distribution for R is

$$f_{R|U}(r|u) = \frac{f_R(r) f_{U|R}(u|r)}{f_U(u)} = \frac{\mathcal{N}_{0,\sigma^2}(r)\mathcal{N}_{\frac{r}{\sqrt{2}},\frac{1}{2}}(u)}{\mathcal{N}_{0,\frac{\sigma^2}{2}+\frac{1}{2}}(u)}, \tag{46}$$

which is the same as for the heterodyne attack. The rest of the analysis is identical to that case.

4.3 Attackers perform a homodyne measurement under a guessed angle

In this attack, Alice picks a random angle φ and does a homodyne measurement under this angle. She forwards the result m to Bob. The distribution of m is given by $f_{M|X_0P_0\Phi}(m|x_0p_0\varphi) = \mathcal{N}_{x_0\cos\varphi + p_0\sin\varphi,\frac{1}{2}}(m) = \mathcal{N}_{r\cos(\varphi-\theta)+r^\perp\sin(\varphi-\theta),\frac{1}{2}}(m)$. The attackers' posterior distribution for R is

$$\begin{aligned}
f_{R|M\Phi\Theta}(r|m\varphi\theta) &= \frac{f_\Theta(\theta) f_\Phi(\varphi) f_R(r) f_{M|R\Theta\Phi}(m|r\theta\varphi)}{f_\Theta(\theta) f_\Phi(\varphi) f_{M|\Theta\Phi}(m|\theta\varphi)} && (47)\\
&\propto f_R(r) f_{M|R\Theta\Phi}(m|r\theta\varphi) && (48)\\
&= f_R(r)\mathbb{E}_{r^\perp} f_{M|RR^\perp\Theta\Phi}(m|rr^\perp\theta\varphi) && (49)\\
&= f_R(r)\mathbb{E}_{r^\perp}\mathcal{N}_{r\cos(\varphi-\theta)+r^\perp\sin(\varphi-\theta),\frac{1}{2}}(m) && (50)\\
&= \mathcal{N}_{0,\sigma^2}(r)\mathcal{N}_{r\cos(\varphi-\theta),\frac{1}{2}+\sigma^2\sin^2(\varphi-\theta)}(m). && (51)
\end{aligned}$$

After some algebra this can be rewritten as

$$f_{R|M\Phi\Theta}(r|m\varphi\theta) = \mathcal{N}_{\mu,S^2}(r) \quad \text{with } \mu = m\cos(\varphi-\theta)\frac{\sigma^2}{\frac{1}{2}+\sigma^2}, \quad S^2 = \sigma^2\frac{\frac{1}{2}+\sigma^2\sin^2(\varphi-\theta)}{\frac{1}{2}+\sigma^2}. \tag{52}$$

The attackers send μ to the verifiers. For the expected score we get

$$\begin{aligned}
\mathbb{E}(R-\mu)^2 &= \mathbb{E}R^2 + \mathbb{E}\mu^2 - 2\mathbb{E}\mu R && (53)\\
&= \sigma^2 + \left(\frac{\sigma^2}{\frac{1}{2}+\sigma^2}\right)^2 \mathbb{E}m^2\cos^2(\varphi-\theta) - 2\frac{\sigma^2}{\frac{1}{2}+\sigma^2}\mathbb{E}mr\cos(\varphi-\theta). && (54)
\end{aligned}$$

We introduce the notation $\delta = \varphi - \theta$. We use the distribution of m conditioned on $rr^\perp\varphi\theta$ to write

$$\begin{aligned}
\mathbb{E}\cos^2\delta\, m^2 &= \mathbb{E}\cos^2\delta\left[\frac{1}{2} + (r\cos\delta + r^\perp\sin\delta)^2\right] && (55)\\
&= \frac{1}{2}\mathbb{E}\cos^2\delta + (\mathbb{E}r^2)\mathbb{E}\cos^4\delta + (\mathbb{E}[r^\perp]^2)\mathbb{E}\cos^2\delta\sin^2\delta && (56)\\
&= \frac{1}{2}\mathbb{E}\cos^2\delta + \sigma^2\mathbb{E}\cos^2\delta && (57)\\
&= \frac{1}{2}\left(\frac{1}{2} + \sigma^2\right). && (58)
\end{aligned}$$

Here we have used that $\mathbb{E}\cos^2\delta = \frac{1}{2}$ because of the uniform φ. Furthermore we have

$$\mathbb{E}mr\cos\delta = \mathbb{E}(r^2\cos^2\delta + rr^\perp\sin\delta\cos\delta) = \sigma^2/2 + 0. \tag{59}$$

Substitution of (58,59) into (54) yields

$$\mathbb{E}(R-\mu)^2 = \frac{\sigma^2}{2}\cdot\frac{\sigma^2+1}{\sigma^2+\frac{1}{2}}. \tag{60}$$

This is much larger than the honest prover's value $1/2+u$ for sufficiently large σ.

5 Security against general attacks by unentangled adversaries

In this section, we show that we not only have security against the above described attacks, but that the result generalizes to all attackers that do not pre-share entanglement by lower bounding their uncertainty higher than the prover's. This is captured by the following theorem.

Theorem 5.1. *For at least one attacker E participating in a general attack, the differential entropy of R given side information held by E follows the inequality*

$$h(R|E) \geq \frac{1}{2}\log\frac{4\pi}{1+\sigma^{-2}}, \tag{61}$$

where σ is the same as defined in Section 3.2. Furthermore, this attacker's response r' satisfies the inequality

$$\mathbb{E}(R-r')^2 \geq \frac{2}{e}\cdot\frac{1}{1+\sigma^{-2}}. \tag{62}$$

Proof. In the entanglement-based protocol, the verifiers perform a heterodyne measurement. This is achieved by mixing one half of the TMS state with vacuum (denoted by O) and then performing a homodyne measurement per mode, in orthogonal directions θ and $\theta+\frac{\pi}{2}$, so

$$\rho_{VP} \overset{\text{Mixing}}{\underset{\text{with } O}{\longrightarrow}} \rho_{\bar{V}\bar{O}P}, \tag{63}$$

where the bar represents the modes after mixing. Here P is the subsystem sent to the prover and $\bar{V}$ is the subsystem on which the θ measurement will be applied.

The attackers (Alice and Bob) perform a quantum operation on the mode P and any ancilla mode. We call the subsystem that Alice holds as A, and the one sent to Bob as B. The resulting state is $\rho_{\bar{V}\bar{O}AB}$. We are interested in the tripartite state $\rho_{\bar{V}AB}$. We write the result of a homodyne measurement on $\bar{V}$ under angle θ as $U_\theta \in \mathbb{R}$, and we write $\bar{\theta} = \theta + \frac{\pi}{2}$. Lemma 2.11 gives

$$\forall\theta\in\mathcal{A} \qquad h(U_\theta|A) + h(U_{\bar{\theta}}|B) \geq \log 2\pi. \tag{64}$$

Averaging over θ, and using the fact that averaging over $\bar{\theta}$ is the same as averaging over θ, gives

$$\mathbb{E}_{\theta\in\mathcal{A}}h(U_\theta|A) + \mathbb{E}_{\theta\in\mathcal{A}}h(U_{\bar{\theta}}|B) \geq \log 2\pi \tag{65}$$

$$\implies \mathbb{E}_{\theta\in\mathcal{A}}h(U_\theta|A) + \mathbb{E}_{\theta\in\mathcal{A}}h(U_\theta|B) \geq \log 2\pi. \tag{66}$$

The last expression can be written as

$$h(U|A\Theta) + h(U|B\Theta) \geq \log 2\pi, \tag{67}$$

where the angle Θ is now represented as a random variable. It follows that

$$\max\Big\{h(U|A\Theta),\ h(U|B\Theta)\Big\} \geq \frac{1}{2}\log 2\pi. \tag{68}$$

Finally, we note that $R = U\sqrt{2}\tanh\zeta$ (with $\sinh\zeta = \sigma$) and use Lemma 2.3 to conclude

$$h(R|E) \geq \frac{1}{2}\log 2\pi + \frac{1}{2}\log\frac{2}{1+\sigma^{-2}} = \frac{1}{2}\log\frac{4\pi}{1+\sigma^{-2}}, \tag{69}$$

Here, we have set $\max\Big\{h(R|A\Theta),\ h(R|B\Theta)\Big\} = h(R|E)$. The result for $\mathbb{E}(R-r')^2$ follows directly from the Fano inequality (Theorem 2.12). □

5.1 Comparison between attacker and honest prover

We will now work in the $\sigma \gg 1$ limit. The protocol works only if the attackers have more ignorance about the value R than the honest prover. Note that we assume that the attackers are powerful and have access to an ideal channel ($t = 1, u = 0$). For $\sigma \to \infty$, the difference between their entropies (61), (24) satisfies

$$h(R|E) - h(R|R') \geq \frac{1}{2} \log\left(\frac{4}{e} \cdot \frac{t}{1+2u}\right). \tag{70}$$

The argument of the logarithm needs to be larger than 1. This is the case when

$$t > \frac{e}{4} \approx 0.680 \quad \wedge \quad u \leq \frac{t \cdot 4/e - 1}{2}. \tag{71}$$

Note that Fano's inequality applied to the honest prover's entropy (24) would yield the expression $\mathbb{E}(\sqrt{t}R - r')^2 \approx \Sigma^2$ (as $\sqrt{t}R|R'$ is Gaussian with mean r' in large σ limit), with Σ^2 as defined in (23), evaluating to $\Sigma^2 \approx (1/2 + u)/t$. On the other hand, the expected error of the attacker is lower bound by $2/e \approx 0.74$, which is strictly greater than $(1/2+u)/t$ for certain parameter ranges, as depicted in Figure 2. This proves security of the protocol against a general attack in these parameter ranges.

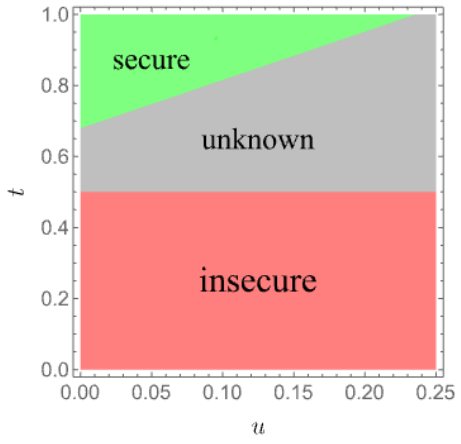

Figure 2: Security of the proposed CV-QPV protocol. For $t \leq 1/2$ it is insecure (red), as shown in [QS15]. For values in the green region, we prove security. Currently, no conclusions can be drawn about the grey region.

As long as equation (70) is positive, i.e.

$$\frac{t}{1+2u} > \frac{e}{4}, \tag{72}$$

there's a finite gap between the attacker and the honest entropy about R. Then an attack fails if the score is greater than γ (cf. Section 3.1). 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. We know that

$$\mathbb{E}(R - r')^2 \geq \frac{2}{e}, \tag{73}$$

thus $\mathbb{E}(\sqrt{t}R - r')^2 \geq 2/e$ 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 $\Delta \stackrel{\text{def}}{=} (2/e)/(1/2+u) - \gamma$[5]. Thus we can use the Chebyshev inequality

[5] In the regime where $\Delta > 0$, which is the case for $u \lesssim 2/e - 1/2 \approx 0.24$ for sufficiently large n where $\gamma \approx 1$. This value can also be observed in Figure 2 at $t = 1$.

for the random variable of the score to get

$$\mathbb{P}\left[\left|\frac{1}{n}\sum_{i=1}^{n}\frac{(\sqrt{t}R_i - r'_i)^2}{1/2+u} - \frac{\mathbb{E}(\sqrt{t}R - r')^2}{1/2+u}\right| \geq \Delta\right] \leq \frac{\tilde{\sigma}^2}{n\Delta^2} = O\left(\frac{1}{n\Delta^2}\right), \tag{74}$$

where $\tilde{\sigma}^2 = \mathbb{V}\left[\frac{(\sqrt{t}R-r')^2}{1/2+u}\right]$. If we set $n\Delta^2 = \Omega\left(\frac{1}{\varepsilon_{\text{att}}}\right)$ then we get

$$\mathbb{P}\left[\frac{1}{n}\sum_{i=1}^{n}\frac{(\sqrt{t}R_i - r'_i)^2}{1/2+u} \leq \gamma\right] \leq O(\varepsilon_{\text{att}}). \tag{75}$$

6 Perfect attack with a single EPR pair

It turns out that our protocol can be attacked if Alice and Bob pre-share one CV EPR pair (see Section 2 for formal descriptions of CV entanglement and teleportation). The entanglement attack proceeds as follows:

1. Alice and Bob pre-share an ideal EPR pair.
2. Alice teleports $|\psi\rangle$ to Bob. She forwards the measured displacement (d_x, d_p) to Bob.
3. Bob intercepts θ and immediately performs a homodyne measurement under angle θ on his own half of the EPR pair, obtaining outcome $\mu \in \mathbb{R}$. He forwards θ, μ to Alice.
4. Alice receives θ, μ. She computes $r' = \mu - d_x \cos\theta - d_p \sin\theta$ and sends r' to V_1.
5. Bob receives d_x, d_p. He computes $r' = \mu - d_x \cos\theta - d_p \sin\theta$ and sends r' to V_2.

The state $|\psi\rangle$ is a coherent state with displacement (x_0, p_0). The effect of the teleportation is that Bob's half of the EPR pair becomes a coherent state with displacement $(x_0 + d_x, p_0 + d_p)$. Bob's homodyne measurement commutes with the teleport-induced displacement: the undoing of the displacement can be done *after* Bob's measurement. The noise in r' with respect to r is just shot noise, exactly as for the honest prover. Other noises originating from loss or excess noise can just be simulated by the attacker.

Hence, in the case of an ideal pre-shared EPR pair, the responses from the attackers are statistically indistinguishable from honest prover responses.

7 Discussion

The security analysis of CV-QPV differs from the discrete variable case, as the honest prover now responds with a sample from a probability distribution. Thus, to prove security (in the setting without pre-shared entanglement), we needed to show that an attack necessarily produces a different distribution than the honest one and that the verifiers can distinguish these distributions. We have shown that this can be done using an entropic uncertainty relation for the differential entropy together with a continuum version of the Fano inequality. We included attenuation and excess noise in the honest channel and showed security for a small range of parameters. We further showed that the considered CV-QPV protocol is broken if one CV-EPR pair is pre-shared between the attackers.

Since continuous-variable systems have some practical advantages over discrete ones (see Section 1) we hope that this work may spur interest into the further study of QPV in the context of continuous variables and we hope our techniques can be useful there.

An immediate next step could be to extend this protocol to the case where the classical information θ is computed via a function $f(x, y)$ taking inputs x, y from both verifiers, similar to the discrete variable $\text{QPV}^{f}_{\text{BB84}}$ protocol [BCS22, EFS22], and to study CV entanglement attacks on that.

More generally, one may ask how far results on QPV for discrete variable protocols generalize or naturally carry over to the CV setting. For example, can the recent formulation of CV port-based teleportation [PBP23] be used to immediately re-formalize the general attack on discrete variable QPV [BK11] in the CV setting? Do the known attacks, which scale with properties of circuit decompositions of the provers' unitary [Spe16, DC22], naturally generalize, for example to CV equivalents of T-count or T-depth?

Acknowledgments

We thank Kfir Dolev for interesting initial discussions on the topic of CV-QPV. RA was supported by the Dutch Research Council (NWO/OCW), as part of the Quantum Software Consortium programme (project number 024.003.037). PVL was supported by the Dutch Research Council (NWO/OCW), as part of the NWO Gravitation Programme Networks (project number 024.002.003). 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

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

[ABSV21] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. Towards practical and error-robust quantum position verification. *arXiv preprint arXiv:2106.12911*, 2021.

[ABSV22] Rene Allerstorfer, Harry Buhrman, Florian Speelman, and Philip Verduyn Lunel. On the role of quantum communication and loss in attacks on quantum position verification. *arXiv preprint arXiv:2208.04341*, 2022.

[ALS10] Ulrik L. Andersen, Gerd Leuchs, and Christine Silberhorn. Continuous-variable quantum information processing. *Laser & Photonics Reviews*, 4(3):337–354, 2010.

[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, jan 2014.

[BCS22] Andreas Bluhm, Matthias Christandl, and Florian Speelman. A single-qubit position verification protocol that is secure against multi-qubit attacks. *Nature Physics*, pages 1–4, 2022.

[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 Press, 2013.

[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, sep 2011.

[BvL05] Samuel L. Braunstein and Peter van Loock. Quantum information with continuous variables. *Rev. Mod. Phys.*, 77:513–577, Jun 2005.

[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*, pages 391–407. Springer, 2009.

[CL15] Kaushik Chakraborty and Anthony Leverrier. Practical position-based quantum cryptography. *Physical Review A*, 92(5), nov 2015.

[CLA01] Nicolas J. Cerf, Mel Lévy, and Gilles Van Assche. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A*, 63:052311, Apr 2001.

[CLP07] Nicolas J. Cerf, Gerd Leuchs, and Eugene S Polzik. *Quantum information with continuous variables of atoms and light*. World Scientific, 2007.

[CM22] Sam Cree and Alex May. Code-routing: A new attack on position-verification. *arXiv preprint arXiv:2202.07812*, 2022.

[Cov99] Thomas M. Cover. *Elements of information theory*. John Wiley & Sons, 1999.

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

[Dol19] Kfir Dolev. Constraining the doability of relativistic quantum tasks. *arXiv preprint arXiv:1909.05403*, 2019.

[EFS22] Llorenç Escolà-Farràs and Florian Speelman. Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers, 2022.

[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.

[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.

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

[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):535–552, oct 2003.

[GG02] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, Jan 2002.

[GLW16] Fei Gao, Bin Liu, and QiaoYan Wen. Quantum position verification in bounded-attack-frequency model. *SCIENCE CHINA Physics, Mechanics & Astronomy*, 59(11):1–11, 2016.

[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, Jan 2000.

[HSH99] Alexander S. Holevo, Masaki Sohma, and Osamu Hirota. Capacity of quantum Gaussian channels. *Phys. Rev. A*, 59:1820–1828, Mar 1999.

[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*. Theses, Télécom ParisTech, November 2009.

[LL11] Hoi-Kwan Lau and Hoi-Kwong Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Physical Review A*, 83(1), jan 2011.

[LLQ22] Jiahui Liu, Qipeng Liu, and Luowen Qian. Beating classical impossibility of position verification. In *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.

[LM00] Beatrice Laurent and Pascal Massart. Adaptive estimation of a quadratic functional by model selection. *Annals of statistics*, pages 1302–1338, 2000.

[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. *Advanced Quantum Technologies*, 1(1):1800011, 2018.

[Mal10a] Robert A. Malaney. Location-dependent communications using quantum entanglement. *Physical Review A*, 81(4), apr 2010.

[Mal10b] Robert A. Malaney. Quantum location verification in noisy channels. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*. IEEE, dec 2010.

[PBP23] Jason L. Pereira, Leonardo Banchi, and Stefano Pirandola. Continuous variable port-based teleportation. *arXiv preprint arXiv:2302.08522*, 2023.

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

[Ral99] Timothy C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61:010303, Dec 1999.

[Rei00] Margaret D. Reid. Quantum cryptography with a predetermined key using continuous-variable Einstein-Podolsky-Rosen correlations. *Phys. Rev. A*, 62:062308, Nov 2000.

[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)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2016.

[Unr14] Dominique Unruh. Quantum position verification in the random oracle model. In *Advances in Cryptology – CRYPTO 2014*, pages 1–18, Berlin, Heidelberg, 2014. Springer Berlin Heidelberg.

[Vai94] Lev Vaidman. Teleportation of quantum states. *Physical Review A*, 49(2):1473, 1994.

[Wig32] Eugene Wigner. On the quantum correction for thermodynamic equilibrium. *Physical review*, 40(5):749, 1932.

[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, Oct 2004.

[WZ82] William K. Wootters and Wojciech Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.