Perfect cheating is impossible for single-qubit position verification

Carl A. Miller[1,2] and Yusuf Alnawakhtha[2]

[1]National Institute of Standards and Technology, Gaithersburg, MD, USA
[2]Joint Center for Quantum Information and Computer Science (QuICS), University of Maryland, College Park, MD, USA

(Dated: July 1, 2024)

In quantum position verification, a prover certifies her location by performing a quantum computation and returning the results (at the speed of light) to a set of trusted verifiers. One of the very first protocols for quantum position verification was proposed in (Kent, Munro, Spiller 2011): the prover receives a qubit Q from one direction, receives an orthogonal basis $\{v, v^\perp\}$ from the opposite direction, then measures Q in $\{v, v^\perp\}$ and broadcasts the result. A number of variants of this protocol have been proposed and analyzed, but the question of whether the original protocol itself is secure has never been fully resolved. In this work we show that there is no perfect finite-dimensional cheating strategy for the original KMS measurement protocol. Our approach makes use of tools from real algebraic geometry.

Digital communication often requires one party to authenticate another at a distance. While secret keys and biometrics are credentials commonly used for authentication, one can imagine situations in which a party's position in space is also a natural credential for partaking in a protocol. Consider, for example, communication with a diplomat residing at an embassy: one might want to confirm that the messages one receives have been issued from the geographical location of the embassy as an added layer of security. Alternatively, in a healthcare setting, one might want to ensure that one's medical records cannot be accessed outside of a healthcare provider's building. Unfortunately, it has been shown that verifying a party's position is impossible classically [1] due to a general attack where multiple adversaries collude to simulate the actions of a single party in the honest position. This attack, however, requires the adversaries to have the ability to make copies of the messages they receive from the verifiers. This observation led to proposals for Quantum Position Verification (QPV) [2] which utilizes "no-cloning" to bar such attacks.

Among the protocols proposed in the early papers on QPV [3–6], one of the simplest — and arguably the least demanding in terms of quantum resources — is a protocol from [3] which we will refer to as the **single-qubit measurement protocol**. Suppose that a prover $\mathbf{P}$ is located in between two verifiers $\mathbf{V}_1$ and $\mathbf{V}_2$. The verifiers secretly agree on a random one-dimensional projector P on $\mathbb{C}^2$. The first verifier $\mathbf{V}_1$ transmits P to $\mathbf{P}$, while the second verifier $\mathbf{V}_2$ prepares a qubit by encoding b into the eigenbasis for P and simultaneously transmits the qubit to $\mathbf{P}$. The prover $\mathbf{P}$ receives both messages, recovers the bit b by applying the measurement $\{P, \mathbb{I} - P\}$, and transmits the result back to both $\mathbf{V}_1$ and $\mathbf{V}_2$. All transmissions are assumed to happen at the speed of light. Our goal is to prove that $\mathbf{P}$'s responses in this protocol could not be faked by any parties who are not at $\mathbf{P}$'s purported location, even if multiple adversaries were to cooperate from different points in space.

Curiously, despite more than a decade of activity on the theory of QPV, the full security of this initial scheme has remained an open question. Lau and Lo [7] showed that if the possible choices for P are restricted to $\{|0\rangle\langle 0|, |+\rangle\langle +|\}$ (the "BB84" case) then two adversaries can easily cheat by sharing a single EPR pair. They then considered the more general case in which P can be arbitrary, and they showed that, in contrast, cheating strategies based on shared entangled qubits or qutrits (i.e., cheating strategies of dimension up to 3) cannot exist. Chakraborty and Leverrier [8] showed that if P is restricted to a particular finite subset — namely, the kth level of the Clifford hierarchy — then a perfect finite-dimensional cheating strategy exists, although it requries an amount of entanglement that grows with k. More recently, Olivo et al. [9] found new cheating strategies for other basis sets of the form $\{P_0, P_\theta\}$, where P_θ denotes the projector onto $(\cos\theta)|0\rangle + (\sin\theta)|1\rangle$.

General QPV cheating results, such as those based on port-based teleportation [5], show that adversaries can *approximately* cheat, up to an arbitrarily small error term, by pre-sharing an amount of entanglement that increases as the error term shrinks. But, these results likewise leave a central question unanswered: does there exist a general perfect cheating strategy for the single-qubit measurement protocol? In the current work, we answer this question in the negative: there is no such strategy. In particular, we prove that any cheating strategy that is based on a finite-dimensional entangled system can only succeed perfectly for a finite number of possible basis choices (see Theorem 7). Our proof uses a tool from real algebraic geometry (the Milnor-Thom theorem). We have thus illuminated one of the central difficulties in constructing QPV cheating strategies.

While Theorem 7 shows in principle that the single-qubit measurement protocol is resistant to attacks, the theorem is not error-tolerant, and so a natural next step would be to explore security results that are more practically significant. Bluhm et al. [10] have shown that the security of single-qubit protocols can be enhanced by encoding the basis choice into two bit strings, x and y, and then having $\mathbf{V}_1$ transmit x to $\mathbf{P}$ and $\mathbf{V}_2$ transmit y to $\mathbf{P}$ along with the prepared qubit. While [10] only used the two BB84 bases, the follow-up work of Escolà-Farràs and Speelman [11] found better performance by using a larger set of basis measurements. Integrating our results with those from other papers on single-qubit QPV, and possibly using more tools from algebraic geometry, could lead to further results.

DEFINITIONS AND NOTATION

A **quantum register** is a complex Hilbert space $\mathcal{H}$ together with a fixed isomorphism $\mathcal{H} \cong \mathbb{C}^n$ with $n \geq 1$. The image of the standard basis for $\mathbb{C}^n$ under this isomorphism is referred to as the standard basis for $\mathcal{H}$. The expression $\mathbb{I}_{\mathcal{H}}$ denotes the identity map on $\mathcal{H}$. If $\mathcal{H}, \mathcal{J}$ are quantum registers, then we may write $\mathcal{HJ}$ for the tensor product $\mathcal{H} \otimes \mathcal{J}$. If $c = \sum_{ij} c_{ij} e_i \otimes f_j \in \mathcal{H} \otimes \mathcal{J}$, where e_i and f_j denote standard basis vectors, then $\mathrm{Mat}(c)$ denotes the vector c in matrix form:

$$\mathrm{Mat}(c) \; = \; [c_{ij}]_{ij} \tag{1}$$

Note that $\mathrm{Mat}(c)$ determines a linear map from $\mathcal{J}$ to $\mathcal{H}$. The expression $L(\mathcal{H})$ denotes the set of all linear maps from $\mathcal{H}$ to itself.

An **analog register** is a subset $D \subseteq \mathbb{R}^n$ of a finite-dimensional real vector space. We refer to the elements of D as the **states** of the analog register.

A **qubit** is a quantum system of dimension 2. Let $\mathbb{S}$ denote the set of all one-dimensional orthogonal projectors on $\mathbb{C}^2$ (the Bloch sphere). Every element of $\mathbb{S}$ can be uniquely expressed in terms of Pauli operators as

$$\left(\mathbb{I} + aX + bY + cZ\right)/2, \tag{2}$$

where $\mathbb{I}$ denotes the 2×2 identity matrix, $(a, b, c) \in \mathbb{R}^3$ is a unit vector, and

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; Y = \begin{bmatrix} 0 & i \\ -i & 0 \end{bmatrix}, \; Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{3}$$

A **pure state** of a quantum register $\mathcal{A}$ is a unit vector in $\mathcal{A}$. A **density operator** on $\mathcal{A}$ is positive semidefinite linear operator of trace 1. Quantum registers are denoted by calligraphic letters (e.g., $\mathcal{A}, \mathcal{B}$). Linear operators and vectors are denoted by Greek or plain Roman letters. If $A \colon \mathcal{V} \to \mathcal{W}$ is a linear map between Hilbert spaces, then A^* denotes its adjoint (i.e., its conjugate transpose). The letters X, Y, Z denote the Pauli operators on $\mathbb{C}^2$.

Two density matrices ρ, χ on a quantum register $\mathcal{A}$ are **perfectly distinguishable** if the support of ρ is orthogonal to the support of χ. Two density matrices α, β on a bipartite quantum register $\mathcal{A} \otimes \mathcal{B}$ are **perfectly distinguishable on** $\mathcal{B}$ if the support of $\mathrm{Tr}_{\mathcal{A}} \alpha$ in $\mathcal{B}$ is orthogonal to that of $\mathrm{Tr}_{\mathcal{A}} \beta$.

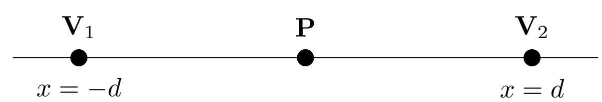
A **quantum channel** Σ from a quantum register $\mathcal{V}$ to a quantum register $\mathcal{W}$ is a completely positive trace-preserving map from $L(\mathcal{V})$ to $L(\mathcal{W})$. Such a channel is an **isometric** channel if it is of the form $\Sigma(M) = UMU^*$ where $U \colon \mathcal{V} \to \mathcal{Z}$ is an isometry.

A subset $V \subseteq \mathbb{R}^m$ is **open** if for any $v \in V$, there exists a ball of radius $\epsilon > 0$ centered on v which is also contained in V. A subset of $\mathbb{R}^m$ is **closed** if its complement is open. A closed subset $W \subseteq \mathbb{R}^m$ is **connected** if it cannot be expressed as the disjoint union of two nonempty closed sets. A **connected component** of a closed set $Z \subseteq \mathbb{R}^m$ is a nonempty subset of Z which is closed and connected. Two subsets $U \subseteq \mathbb{R}^n$ and $V \subseteq \mathbb{R}^m$ are **di eomorphic** if there exists a bijective map $F \colon U \to V$ such that F and F^{-1} are infinitely differentiable.

THE SINGLE-QUBIT MEASUREMENT PROTOCOL

The single-qubit measurement protocol is conducted as follows. The protocol is a one-dimensional position verification protocol, and so we assume that all parties involved are located on a single line with a disinguished point (the origin). The line is parametrized by a real value $x \in \mathbb{R}$, so that $x = \ell$ refers to the point r meters to the right of the origin (or $-\ell$ meters to the left of the origin, if ℓ is negative). Time is measured in seconds. (We will generally omit units.)

In the honest case, two verifiers $\mathbf{V}_1$ and $\mathbf{V}_2$ are located at $x = -d$ and $x = d$, respectively, where d is a positive real parameter. An honest prover $\mathbf{P}$ is located at $x = 0$.



The protocol proceeds as follows. Let c denote the speed of light.

1. The verifiers choose an element $P \in \mathbb{S}$ and a bit $z \in \{0, 1\}$.

2. At time $t = 0$, the verifier $\mathbf{V}_1$ transmits P to the right (in an analog register). The verifier $\mathbf{V}_2$ prepares a qubit $\mathcal{Q}$ in state P if $z = 0$, and in state $\mathbb{I} - P$ if $z = 1$, and transmits $\mathcal{Q}$ to the left.

3. At time $t = d/c$, the prover $\mathbf{P}$ applies the measurement $\{P, \mathbb{I} - P\}$ to the qubit $\mathcal{Q}$, and broadcasts the result.

4. At time $t = 2d/c$, the verifiers $\mathbf{V}_1$ and $\mathbf{V}_2$ receive bit messages (from $\mathbf{P}$) which we denote by z_1 and z_2 respectively. The verifiers check whether the bits z, z_1, z_2 all agree; if they do, the verifiers ACCEPT. Otherwise, the verifiers ABORT.

HIDDEN MEASUREMENT CHANNELS

Definition 1 *Let $\mathcal{Q}$ be a qubit register, and let P be an element of the Bloch sphere $\mathbb{S}$. A quantum channel*

$$\Phi \colon L(\mathcal{Q}) \to L(\mathcal{V}_1 \otimes \mathcal{V}_2),$$

*(where $\mathcal{V}_1, \mathcal{V}_2$ are quantum registers) is a **hidden measurement channel** for P if the states*

$$\Phi(P) \quad and \quad \Phi(\mathbb{I} - P)$$

are perfectly distinguishable on $\mathcal{V}_1$ and perfectly distinguishable on $\mathcal{V}_2$.

If a bit b is encoded into the basis defined by $\{P, \mathbb{I} - P\}$ and given as input to the channel Φ described above, then b can be recovered from either the system $\mathcal{V}_1$ or the system $\mathcal{V}_2$. However, it may not be obvious (from a mathematical description of Φ) *how* to recover b from $\mathcal{V}_1$ or $\mathcal{V}_2$. This is the reason for calling such a channel a "hidden" measurement channel.

The following theorem considers channels like those in Definition 1, but with an additional input register.

Theorem 2 *Let*

$$\colon L(\mathcal{W} \otimes \mathcal{Q}) \to L(\mathcal{V}_1 \otimes \mathcal{V}_2)$$

be a quantum channel, where $\mathcal{W}, \mathcal{V}_1, \mathcal{V}_2$ are quantum registers and $\mathcal{Q}$ is a qubit register. Let Λ be the set of all pairs (P, w) where $P \in \mathbb{S}$ and w is a unit vector in $\mathcal{W}$, such that the quantum channel from $\mathcal{Q}$ to $\mathcal{V}_1 \otimes \mathcal{V}_2$ defined by

$$\rho \mapsto \quad (ww^* \otimes \rho)$$

is a hidden measurement channel for P. Let $n = \dim(\mathcal{W})$. Then, at most $4 \cdot 7^{2n+2}$ distinct values of $P \in \mathbb{S}$ occur in the pairs contained in Λ.

Proof. It suffices to prove the theorem under the assumption that is an isometric channel $(\cdot) = U(\cdot)U^*$ defined by a linear map

$$U \colon \mathcal{W} \otimes \mathcal{Q} \to \mathcal{V}_1 \otimes \mathcal{V}_2, \tag{4}$$

satisfying $U^*U = \mathbb{I}$, and so we make that assumption for the remainder of the proof [12]. For any $w \in \mathcal{W}$, let

$$\begin{aligned} R_w &= \operatorname{Mat}(U(w \otimes e_1)) &(5)\\ S_w &= \operatorname{Mat}(U(w \otimes e_2)), &(6) \end{aligned}$$

where e_1, e_2 are the standard basis vectors for $\mathcal{Q}$. Note that $\langle R_w, S_{w'} \rangle = 0$ for any $w, w' \in \mathcal{W}$. If

$$P = \begin{bmatrix} p & q \\ \overline{q} & r \end{bmatrix} \in \mathbb{S}, \tag{7}$$

then the marginal state of $(ww^* \otimes P)$ on $\mathcal{V}_1$ is given by

$$pR_wR_w^* + qR_wS_w^* + \overline{q}S_wR_w^* + rS_wS_w^* \tag{8}$$

and the marginal state of $(ww^* \otimes P)$ on $\mathcal{V}_2$ is given by

$$pR_w^*R_w + qR_w^*S_w + \overline{q}S_w^*R_w + rS_w^*S_w \tag{9}$$

If P is the orthogonal projector onto the vector $(x, y) \in \mathbb{C}^2$, then the channel $(ww^* \otimes (\cdot))$ is a hidden measurement channel for $\{P, \mathbb{I} - P\}$ if and only if the following two equations hold:

$$\begin{aligned} (xR_w + yS_w)(-\overline{y}R_w + \overline{x}S_w)^* &= 0, &(10)\\ (xR_w + yS_w)^*(-\overline{y}R_w + \overline{x}S_w) &= 0. &(11) \end{aligned}$$

An alternative criteria for the hidden measurement channel condition — one which is expressed directly in terms of the entries of P — is the following. The channel $(ww^* \otimes (\cdot))$ is a hidden measurement channel for $\{P, \mathbb{I} - P\}$ if and only if the following two equations hold:

$$\begin{bmatrix} p\mathbb{I} & q\mathbb{I} \\ \overline{q}\mathbb{I} & r\mathbb{I} \end{bmatrix} \begin{bmatrix} R_wR_w^* & R_wS_w^* \\ S_wR_w^* & S_wS_w^* \end{bmatrix} \begin{bmatrix} (1-p)\mathbb{I} & -q\mathbb{I} \\ -\overline{q}\mathbb{I} & (1-r)\mathbb{I} \end{bmatrix} = 0,$$

$$\begin{bmatrix} p\mathbb{I} & q\mathbb{I} \\ \overline{q}\mathbb{I} & r\mathbb{I} \end{bmatrix} \begin{bmatrix} R_w^*R_w & R_w^*S_w \\ S_w^*R_w & S_w^*S_w \end{bmatrix} \begin{bmatrix} (1-p)\mathbb{I} & -q\mathbb{I} \\ -\overline{q}\mathbb{I} & (1-r)\mathbb{I} \end{bmatrix} = 0.$$

(This becomes apparent, e.g., by performing a change of basis on $\mathcal{Q}$ to make P the projector onto the standard basis vector $(1, 0)$.)

The following lemma will be central to the proof of Theorem 2.

Lemma 3 *Let (P, v) and (L, w) be elements of Λ. Then,*

$$\|v - w\| \geq \quad \left(\sqrt{\|P - L\|_1}\right).$$

Proof of Lemma 3. Without loss of generality, we assume that P is the projector onto the vector $(1, 0) \in \mathcal{Q}$ and L is the projector onto the vector $(\cos\theta, \sin\theta) \in \mathcal{Q}$ for some $\theta \in [0, \pi/2]$. Let

$$\begin{aligned} V &= R_v\\ V' &= S_v\\ W &= (\cos\theta)R_w + (\sin\theta)S_w\\ W' &= -(\sin\theta)R_w + (\cos\theta)S_w. \end{aligned}$$

The assumptions made so far imply the following conditions:

$$\|V\|_2 = \|V'\|_2 = \|W\|_2 = \|W'\|_2 = 1$$
$$V(V')^* = 0, \ V^*(V') = 0$$
$$W(W')^* = 0, \ W^*(W') = 0$$
$$\langle V, W \rangle = (\cos\theta) \langle v, w \rangle$$
$$\langle V, W' \rangle = -(\sin\theta) \langle v, w \rangle$$
$$\langle V', W \rangle = (\sin\theta) \langle v, w \rangle$$
$$\langle V', W' \rangle = (\cos\theta) \langle v, w \rangle$$

Let $B\colon \mathcal{W} \to \mathcal{W}$ denote orthogonal projection onto the support of VV^* (which is orthogonal to the support of $V'(V')^*$), and let $B^\perp = \mathbb{I} - B$. We have the following, in which we apply the equalities $B^\perp V = 0$, $W(W')^* = 0$, $(V')^* B = 0$, and then the Cauchy-Schwartz inequality:

$$\begin{aligned}
\mathrm{Re}\,\langle V, W'\rangle &= \mathrm{Re}\,\mathrm{Tr}[V(W')^*] \\
&= \mathrm{Re}\,\mathrm{Tr}[BV(W')^*B + B^\perp V(W')^* B^\perp] \\
&= \mathrm{Re}\,\mathrm{Tr}[BV(W')^*B] \\
&= \mathrm{Re}\,\mathrm{Tr}[B(V-W)(W')^*B] \\
&= \mathrm{Re}\,\mathrm{Tr}[B(V-W)(W'-V')^*B] \\
&\leq \|B(V-W)\|\,\|(W'-V')^*B\| \\
&\leq \|V-W\|\,\|W'-V'\| \\
&= \sqrt{(2-2\mathrm{Re}\,\langle V,W\rangle)(2-2\mathrm{Re}\,\langle V',W'\rangle)}
\end{aligned}$$

Therefore,

$$(\sin\theta)\mathrm{Re}\,\langle v,w\rangle \;\leq\; 2 - 2(\cos\theta)\mathrm{Re}\,\langle v,w\rangle \tag{12}$$

which implies

$$\mathrm{Re}\,\langle v,w\rangle \;\leq\; \frac{2}{\sin\theta + 2\cos\theta} \tag{13}$$

and

$$\begin{aligned}
\|v-w\| &= \sqrt{2-2\mathrm{Re}\,\langle v,w\rangle} &(14)\\
&\geq \sqrt{2 - \frac{4}{\sin\theta + 2\cos\theta}} &(15)\\
&\geq (\sqrt{\theta}) &(16)\\
&\geq (\sqrt{\|P-L\|_1}), &(17)
\end{aligned}$$

as desired. □

Lemma 4 *Let $\pi\colon [0,1] \to \Lambda$ be an infinitely di erentiable path in Λ, expressed as $\pi(t) = (\pi_1(t), \pi_2(t)) \in \mathbb{S} \times \mathcal{W}$. Then, $\pi_1(0) = \pi_1(1)$.*

Proof. Let $C = \max_{0 \leq t \leq 1} \|\pi_2'(t)\|$. Then, $\|\pi_2(t) - \pi_2(s)\|$ is always less than or equal to $C|t-s|$ for all $t, s \in [0,1]$. By Lemma 3,

$$\|\pi_1(t) - \pi_1(s)\| \;\leq\; O(C^2(t-s)^2) \tag{18}$$

for any $t, s \in [0,1]$. For any positive integer N, applying inequality (18) inductively with t drawn from the set $\{j/N \mid j \in \{0,1,\ldots,N\}\}$ yields the inequality

$$\|\pi_1(0) - \pi_1(1)\| \;\leq\; O(C^2/N). \tag{19}$$

Since this inequality holds for any N, we must have $\pi_1(0) = \pi_1(1)$. □

Now we prove Theorem 2. We begin by describing the set Λ in terms of a system of polynomial equations. Recall that X, Y, Z denote the Pauli operators on $\mathbb{C}^2$. For any unit vector $c = (c_1, c_2, c_3) \in \mathbb{R}^3$, let

$$P_c \;=\; (\mathbb{I} + c_1 X + c_2 Y + c_3 Z)/2. \tag{20}$$

Based on the equations immediately above Lemma 3, the set Λ can be precisely described as the set of all pairs (P_c, w) with $c \in \mathbb{R}^3$ and $w \in \mathcal{W}$, such that

$$\begin{aligned}
&\|c\|^2 = \|w\|^2 = 1, &(21)\\
&(P_c \otimes \mathbb{I}_{\mathcal{V}_1}) \begin{bmatrix} R_w R_w^* & R_w S_w^* \\ S_w R_w^* & S_w S_w^* \end{bmatrix} ((\mathbb{I}_{\mathcal{Q}} - P_c) \otimes \mathbb{I}_{\mathcal{V}_1}) \;=\; 0 \\
&(P_c \otimes \mathbb{I}_{\mathcal{V}_2}) \begin{bmatrix} R_w^* R_w & R_w^* S_w \\ S_w^* R_w & S_w^* S_w \end{bmatrix} ((\mathbb{I}_{\mathcal{Q}} - P_c) \otimes \mathbb{I}_{\mathcal{V}_2}) \;=\; 0.
\end{aligned}$$

Since Λ is a real algebraic set, it can be expressed as the disjoint union of a finite number of sets $S_i \subseteq \mathbb{R}^3 \times \mathbb{C}^n$ each of which is diffeomorphic to a hypercube $(0,1)^{d_i}$ with $d_i \geq 0$ (see Theorem 5.38 in [13]). Lemma 4 clearly implies that on each set S_i, the $\mathbb{S}$-component is constant. Therefore there are only a finite number of $\mathbb{S}$-components occurring in Λ. We can decompose Λ into a disjoint union of a finite number of closed subsets of the form

$$\Lambda_P \;=\; \{(P,w) \in \Lambda \mid w \in \mathcal{W}\}. \tag{22}$$

Lastly, we observe from the three equations in (21) that Λ is defined by a fourth-degree real polynomial system on $2n+3$ variables, and therefore the Milnor-Thom theorem (Theorem 2 in [14]) implies that the set Λ has at most $4 \cdot 7^{2n+2}$ connected components. Therefore, Λ_P is nonempty for at most $4 \cdot 7^{2n+2}$ values of P.

This completes the proof. □

MAIN RESULT

We mathematically characterize cheating strategies for the single-qubit measurement protocol. As is standard in QPV, we assume a cheating model in which there are exactly two adversaries, one located to the left of $x = 0$ and the other to the right of $x = 0$. We label the adversaries as **A** (Alice), located at $x = -h$, and **B** (Bob), located at $x = h$, where h is a positive real number less than d. (Cheating strategies that involve more than 2 adversaries on the line segment between $\mathbf{V}_1$ and $\mathbf{V}_2$ can be simulated strategies in this form.)

Definition 5 *A* ***cheating strategy*** *for a subset $T \subseteq \mathbb{S}$ consists of the following data.*

1. *Quantum registers $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$.*
2. *A pure quantum state $\psi \in \mathcal{A} \otimes \mathcal{B}$.*
3. *For every $P \in T$, an isometry*

$$U_P\colon \mathcal{A} \to \mathcal{A} \otimes \mathcal{C}. \tag{23}$$

4. *An isometry*

$$V\colon \mathcal{B} \otimes \mathcal{Q} \to \mathcal{B} \otimes \mathcal{D}. \tag{24}$$

The systems $\mathcal{A}$ and $\mathcal{B}$ represent Alice and Bob's local memories, respectively. It is assumed that before the protocol begins, Alice and Bob prepare $\mathcal{A}$ and $\mathcal{B}$ in the state ψ, and the verifier $\mathbf{V}_2$ chooses a random bit z and encodes it into $\mathcal{Q}$ in the basis $\{P, \mathbb{I}-P\}$. At time $(d-h)/c$, Alice receives P, applies the isometry U_P, and sends the system $\mathcal{C}$ to Bob. She also re-broadcasts P. Then, also at time $(d-h)/c$, Bob receives $\mathcal{Q}$, applies the isometry V to $\mathcal{B}$ and $\mathcal{Q}$ together, and sends the system $\mathcal{D}$ to Alice.

At time $(d+h)/c$, Alice is in possession of the systems $\mathcal{A}$ and $\mathcal{D}$, and Bob is in possession of $\mathcal{B}$ and $\mathcal{C}$. We make the following definition.

Definition 6 *A cheating strategy for a subset $T \subseteq \mathbb{S}$ (as in Definition 5) is **perfect** if for every $P \in T$, the states*

$$U_P V(\psi \otimes P) \text{ and } U_P V(\psi \otimes (\mathbb{I} - P)) \tag{25}$$

are perfectly distinguishable on $\mathcal{AD}$ and perfectly distinguishable on $\mathcal{BC}$.

In other words, the cheating strategy is perfect if at time $(d+h)/c$ there are local measurements that Alice and Bob can perform that will allow them to both perfectly guess the bit f.

Theorem 7 *Suppose that $(\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}, \psi, \{U_P\}, V)$ is a perfect cheating strategy for a subset $T \subseteq \mathbb{S}$. Let*

$$m \;=\; \dim \mathcal{A} \cdot \dim \mathcal{B} \cdot \dim \mathcal{C}. \tag{26}$$

Then, $|T| \leq 4 \cdot 7^{2m+2}$.

Proof. For each $P \in T$, let $\psi_P \in \mathcal{A} \otimes \mathcal{B} \otimes \mathcal{C}$ be the state defined by $\psi_P = U_P \psi$. Then, the states in expression (25) can alternatively be expressed as

$$V(\psi_P \otimes P) \text{ and } V(\psi_P \otimes (\mathbb{I} - P)). \tag{27}$$

Since the cheating strategy is perfect, $V(\psi_P \otimes (\cdot))$ is a hidden measurement channel (with respect to the partition $(\mathcal{AD} \mid \mathcal{BC})$) for all $P \in T$. By Theorem 2, this is possible only if $|T| \leq 4 \cdot 7^{2m+2}$. $\square$

ACKNOWLEDGEMENTS

The authors thank Yi-Kai Liu, Dustin Moody, and Harry Tamvakis for their help with this paper. The opinions expressed in this paper are solely those of the authors, and do not reflect any official opinions or endorsements by NIST.

[1] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, Position based cryptography, in *Annual International Cryptology Conference* (Springer, 2009) pp. 391–407.

[2] A. Kent, W. Munro, T. Spiller, and R. Beausoleil, Tagging systems (2006), U.S. Patent No. 2006/0022832 A1.

[3] A. Kent, W. J. Munro, and T. P. Spiller, Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints, Physical Review A **84**, 012326 (2011).

[4] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Scha ner, Position-based quantum cryptography: Impossibility and constructions, SIAM Journal on Computing **43**, 150 (2014).

[5] S. Beigi and R. König, Simplified instantaneous non-local quantum computation with applications to position-based cryptography, New Journal of Physics **13**, 093036 (2011).

[6] R. A. Malaney, Location-dependent communications using quantum entanglement, Physical Review A **81**, 042319 (2010).

[7] H.-K. Lau and H.-K. Lo, Insecurity of position-based quantum-cryptography protocols against entanglement attacks, Physical review a **83**, 012322 (2011).

[8] K. Chakraborty and A. Leverrier, Practical position-based quantum cryptography, Phys. Rev. A **92**, 052304 (2015).

[9] A. Olivo, U. Chabaud, A. Chailloux, and F. Grosshans, Breaking simple quantum position verification protocols with little entanglement, arXiv preprint arXiv:2007.15808 (2020).

[10] A. Bluhm, M. Christandl, and F. Speelman, A single-qubit position verification protocol that is secure against multi-qubit attacks, Nature Physics **18**, 623 (2022).

[11] L. Escolà-Farràs and F. Speelman, Single-qubit loss-tolerant quantum position verification protocol secure against entangled attackers, Physical Review Letters **131**, 140802 (2023).

[12] The Stinespring dilation theorem (see section 2.2 in [15]) implies that any channel from $\mathcal{WQ}$ to $\mathcal{V}_1\mathcal{V}_2$ can be expanded to an isometric channel $'$ from $\mathcal{WQ}$ to $\mathcal{V}_1\mathcal{V}_2\mathcal{V}_3$ for some additional quantum register $\mathcal{V}_3$. If is a hidden measurement channel for a projector P then $'$ is obviously also a hidden measurement channel for P for the partition $(\mathcal{V}_1 \mid \mathcal{V}_2\mathcal{V}_3)$. The generalization follows.

[13] S. Basu, R. Pollack, and M.-F. Roy, *Algorithms in Real Algebraic Geometry*, 2nd ed., Algorithms and Computation in Mathematics, Vol. 10 (Springer, 2006).

[14] J. Milnor, On the Betti numbers of real varieties, Proceedings of the American Mathematical Society **15**, 275 (1964).

[15] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, 2018).