Position-Based Quantum Cryptography: Impossibility and Constructions

Harry Buhrman* Nishanth Chandran† Serge Fehr‡ Ran Gelles†
Vipul Goyal§ Rafail Ostrovsky¶ Christian Schaffner‖

September 13, 2010

Abstract

In this work, we study position-based cryptography in the quantum setting. The aim is to use the geographical position of a party as its only credential. On the negative side, we show that if adversaries are allowed to share an arbitrarily large entangled quantum state, no secure position-verification is possible at all. That is, we show a generic attack that breaks any position-verification scheme of a very general form. On the positive side, we show that if adversaries do not share any entangled quantum state but can compute arbitrary quantum operations, secure position-verification is achievable. Jointly, these results suggest the interesting question whether secure position-verification is possible in case of a bounded amount of entanglement. Our positive result can be interpreted as resolving this question in the simplest case, where the bound is set to zero.

In models where secure positioning is achievable, it has a number of interesting applications. For example, it enables secure communication over an insecure channel without having any pre-shared key, with the guarantee that only a party at a specific location can learn the content of the conversation. More generally, we show that in settings where secure position-verification is achievable, other position-based cryptographic schemes are possible as well, such as secure position-based authentication and position-based key agreement.

*Centrum Wiskunde & Informatica (CWI) and University of Amsterdam, The Netherlands. Email: Harry.Buhrman@cwi.nl. This work is supported by a NWO VICI grant and the EU 7th framework grant QCS.

†Department of Computer Science, UCLA, Los Angeles, CA, USA. Email: {nishanth, gelles}@cs.ucla.edu. This work is supported in part by NSF grants 0716835, 0716389, 0830803, and 0916574.

‡Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands. Email: Serge.Fehr@cwi.nl.

§Microsoft Research, Bangalore, India. Email: vipul@microsoft.com.

¶Department of Computer Science and Mathematics, UCLA, Los Angeles, CA, USA. Email: rafail@cs.ucla.edu. This work is supported in part by IBM Faculty Award, Xerox Innovation Group Award, the Okawa Foundation Award, Intel, Teradata, BSF grant 2008411, NSF grants 0716835, 0716389, 0830803, 0916574 and U.C. MICRO grant.

‖Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands. Email: Christian.Schaffner@cwi.nl

1 Introduction

1.1 Background

At CRYPTO 2009, Chandran, Goyal, Moriarty, and Ostrovsky [CGMO09] introduced the notion of *position-based cryptography*. The goal of position-based cryptography is to use the geographical position of a party as its only "credential". For example, one would like to send a message to a party at a geographical position *pos* with the guarantee that the party can decrypt the message only if he or she is physically present at *pos*.

A central task in position-based cryptography is the problem of *position-verification*. We have a *prover* P at position *pos*, wishing to convince a set of *verifiers* $V_0, \ldots, V_k$ (at different points in geographical space) that he (i.e. the prover) is indeed at that position *pos*. The prover can run an interactive protocol with the verifiers in order to do this. The main technique for such a protocol is known as distance bounding [BC94]. In this technique, a verifier sends a random nonce to P and measures the time taken for P to reply back with this value. Assuming that communication is bounded by the speed of light, this technique gives an upper bound on the distance of P from the verifier.

The problem of secure positioning has been studied before in the field of wireless security, and there have been several proposals for this task ([BC94, SSW03, VN04, Bus04, CH05, SP05, ZLFW06, CCS06]). However, [CGMO09] shows that there exists no protocol for secure positioning that offers security in the presence of *multiple colluding* adversaries. In other words, the set of verifiers cannot distinguish between the case when they are interacting with an honest prover at *pos* and the case when they are interacting with multiple colluding dishonest provers, none of whom are at position *pos*. Their impossibility result holds even if we make computational hardness assumptions, and it also rules out most other interesting position-based cryptographic tasks.

In light of the strong impossibility result, [CGMO09] considers a model in which verifiers can broadcast large bursts of information and there is a bound on the amount of information that the set of adversaries can retrieve (this model is known as the Bounded Retrieval Model (BRM) and has been used widely in cryptography). In this model, [CGMO09] constructs information-theoretically secure protocols for the task of position-verification as well as position-based key exchange (wherein the verifiers, in addition to verifying the position claim of a prover, also exchange a secret key with the prover). While these protocols give us a way to realize position-based cryptography, the BRM has its drawbacks. Firstly, it requires the verifiers to be able to broadcast large bursts of information and this might be difficult to do; secondly, and perhaps more importantly, the bound on the amount of information that an adversary retrieves might be hard to impose. This leaves us with the following question—is there any other assumption or setting in which position-based cryptography is realizable?

1.2 Our Approach And Our Results

In this work, we study position-based cryptography in the *quantum* setting. To start with, let us briefly explain why moving to the quantum setting might be useful. The impossibility result of [CGMO09] relies heavily on the fact that an adversary can locally store all information he receives *and* at the same time share this information with other colluding adversaries, located elsewhere. Recall that the positive result of [CGMO09] in the BRM circumvents the impossibility result by assuming that an adversary *cannot* store all information he receives. By going to the quantum setting, one may be able to circumvent the impossibility result thanks to the following observation. If some information is encoded into a quantum state, then the above attack fails due to the no-cloning principle: the adversary can either store the quantum state or send it to a colluding adversary (or do something in-between, like store part of it), but not both.

However, this intuition turns out to be not completely accurate. Once the adversaries pre-share entangled states, they can make use of quantum teleportation [BBC$^+$93]. Although teleportation on its own does not appear to immediate conflict with the above intuition, we show that, based on techniques by Vaidman [Vai03], adversaries holding a large amount of entangled quantum states can successfully attack any position-based quantum scheme. We analyze our generic attack against an arbitrary 1-round position-verification scheme (as given in Fig. 1), but the attack works similarly against multi-round schemes.

Interestingly, pre-sharing entangled quantum systems is vital for attacking the position-verification scheme, because we show that otherwise, there exist schemes that are secure in the information-theoretic sense. If the adersary is not allowed any pre-shared entanglement, we show how to construct secure protocols for several position-based cryptographic tasks: position-verification, authentication, and key exchange.

This leads to an interesting open question regarding the amount of pre-shared entanglement required to break the positioning scheme: the case of a large amount of pre-shared states yields a complete break of any scheme while having no pre-shared states leads to information-theoretically secure schemes. The threshold of pre-shared quantum systems that keeps the system secure is yet unknown.

1.3 Related Work

Chandran et al. [CGMO09] show that even under cryptographic hardness assumptions, position-verification using *classical* protocols is impossible against colluding malicious provers.

To the best of our knowledge, quantum schemes for position-based cryptography have first been considered by Kent in 2002 under the name of "quantum tagging". Together with Munro, Spiller and Beausoleil, a patent for an (insecure) scheme was filed for HP Labs in 2004 and granted in 2006 [KMSB06]. Their results have not appeared in the academic literature until 2010 [KMS10]. In that paper, they describe several basic schemes and describe how to break them using teleportation-based attacks. They propose other variations (Schemes IV–VI in [KMS10]) not suspect to their teleportation attack and conjecture their security. Our general attack presented here shows that these schemes are insecure as well.

Concurrent and independent of our work reported here and the work on quantum tagging described above, the approach of using quantum techniques for secure position-verification was proposed by Malaney [Mal10a, Mal10b]. However, the proposed scheme is merely claimed secure, and no rigorous security analysis is provided. As pointed out in [KMS10], Malaney's schemes can also be broken by a teleportation-based attack.

To complete the historic picture, we note that a previous version of the present paper has been made public in May 2010 by a subset of the authors [CFG+10]. After the appearance of [KMS10] we have realized that our schemes are merely secure against adversaries without pre-shared entnaglement.

In a recent note [Ken10], Kent considers a different model for position-based cryptography where the prover is assumed to share with the verifiers a classical key unknown to the adversary. In this case, quantum key distribution can be used to expand that key ad infinitum. This classical key stream is then used as authentication resource.

In [GLM02], Giovannetti et al. show how to measure the distance between two parties by quantum cryptographic means so that only trusted people have access to the result. This is a different kind of problem than what we consider here, and the techniques used there are not applicable in our setting.

1.4 Our Attack and our Schemes in More Detail

Position-Verification - A Simple Approach. Let us briefly discuss here the 1-dimensional case in which we have two verifiers V_0 and V_1, and a prover P at position *pos* that lies on the straight line between V_0 and V_1. Now, to verify P's position, V_0 sends a BB84 qubit $H^\theta|x\rangle$ to P, and V_1 sends the corresponding basis θ to P. The sending of these messages is timed in such a way that $H^\theta|x\rangle$ and θ arrive at position *pos* at the same time. P then has to measure the qubit in the given basis to obtain x, and immediately send x to V_0 and V_1, who verify the correctness of x and if it has arrived "in time".

The intuition for this scheme is the following. Consider a dishonest prover $\hat{P}_0$ between V_0 and P, and a dishonest prover $\hat{P}_1$ between V_1 and P. (It is not too hard to see that additional dishonest provers do not help.) When $\hat{P}_0$ receives the BB84 qubit, she does not know yet the corresponding basis θ. Thus, if she measures it immediately when she receives it, then she is likely to measure it in the wrong basis and $\hat{P}_0$ and $\hat{P}_1$ will not be able to provide the correct x. However, if she waits until he knows the basis θ, then $\hat{P}_0$ and $\hat{P}_1$ will be too late in sending x to V_1 in time. Similarly, if she forwards the BB84 qubit to $\hat{P}_1$, who receives θ before $\hat{P}_0$ does, then $\hat{P}_0$ and $\hat{P}_1$ will be too late in sending x to V_0. It seems that in order to break the

scheme $\hat{P}_0$ needs to store the qubit until she receives the basis θ and at the same time send a copy of it to $\hat{P}_1$. But this is impossible by no-cloning.

The Attack. The above intuition turns out to be wrong. Using pre-shared entanglement, $\hat{P}_0$ and $\hat{P}_1$ can perform quantum teleportation which enables them (in some sense) to act coherently on the complete state immediately upon reception. Together with the observation by Kent *et al.* [KMS10] that the Pauli-corrections resulting from the teleportation commute with the actions of the honest prover in the above protocol proves the intuition wrong.

Based on ideas by Vaidman [Vai03], we give a general attack which breaks *any* (1-round) position-verification scheme. In the attack, $\hat{P}_0$ and $\hat{P}_1$ teleport states back and forth many times in a clever way, *without* awaiting the classical measurement outcomes from the other party's teleportations.

Position-Verification in the No Pre-shared Entanglement (No-PE) Model. On the other hand, the above intuition is correct in the No-PE model, where the adversaries are not allowed to have pre-shared entangled quantum states. However, rigorously proving the security of the scheme in the No-PE model is non-trivial. Our proof is based on the *strong complementary information tradeoff* (CIT) due to Renes and Boileau [RB09] (see also [BCC$^+$10]), and it guarantees that for any strategy, the success probability of $\hat{P}_0$ and $\hat{P}_1$ is bounded by approximately 0.89. By repeating the above simple scheme sequentially, we obtain a secure multi-round positioning scheme with exponentially small soundness error. The scheme can easily be extended to arbitrary dimension d. The idea is to involve additional verifiers $V_2, \ldots, V_d$ and have the basis θ secret-shared among $V_1, V_2, \ldots, V_d$.

Position-based authentication and key-exchange in the No-PE Model. Our position-based authentication scheme is based on our position-verification scheme. The idea is to start with a "weak" authentication scheme for a 1-bit message m: the verifiers and P execute the secure position-verification scheme; if P wishes to authenticate $m = 1$, then P correctly finishes the scheme by sending x back, but if P wishes to authenticate $m = 0$, then P sends back an "erasure" $\perp$ instead of the correct reply x with some probability q (which needs to be carefully chosen). This authentication scheme is weak in the sense that turning 1 into 0 is easy for the adversary, but turning a 0 into a 1 fails with constant probability.

The idea is now to use a suitable *balanced* encoding of the actual message to be authenticated, so that for any two messages, the adversary needs to turn many 0's into 1's. Unfortunately, an arbitrary balanced encoding is not good enough. The reason for this is that we do not assume the verifiers and the honest P to be synchronized. This allows the adversary to make use of honest P who is authenticating one index of the encoded message, in order to authenticate another index of the modified encoded message towards the verifiers.

Nevertheless, we show that the above approach does work for carefully chosen codes. We show that, for instance, the bit-wise encoding which maps 0 into 00...0 11...1 and 1 into 11...1 00...0 is such a code.

Our solution borrows some ideas from [RW03, KR09, CKOR10] on authentication based on weak secrets. However, since in our setting we cannot do liveness tests (to check that the verifier is alive in the protocol), the techniques from [RW03, KR09, CKOR10] do not help us directly.

Given a position-based authentication scheme, one can immediately obtain a position-based key exchange scheme simply by (essentially) executing an arbitrary quantum-key-distribution scheme (e.g. [BB84]), which assumes an authenticated classical communication channel, and authenticate the classical communication by means of the position-based authentication scheme.

1.5 Organization of the paper

In Section 2, we begin by introducing notation, and presenting the relevant background from quantum information theory. In Section 3, we describe the problem of position-verification and define our standard quantum model, as well as the No-PE model in more detail. In Section 4, we show that there does not exist any protocol for position-verification (and hence, any protocol for position-based cryptographic tasks) in the

standard quantum model. We present our position-verification protocol in the No-PE model in Section 5. Section 6 is devoted to our position-based authentication protocol and showing how to combine the above tools to obtain position-based key exchange.

2 Preliminaries

2.1 Notation and Terminology

We assume the reader to be familiar with the basic concepts of quantum information theory and refer to [NC00] for an excellent introduction; we merely fix some notation here.

Qubits. A *qubit* is a quantum system A with state space $\mathcal{H}_A = \mathbb{C}^2$. The *computational basis* $\{|0\rangle, |1\rangle\}$ (for a qubit) is given by $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$, and the *Hadamard basis* by $H\{|0\rangle, |1\rangle\} = \{H|0\rangle, H|1\rangle\}$, where H denotes the 2-dimensional *Hadamard matrix*, which maps $|0\rangle$ to $(|0\rangle + |1\rangle)/\sqrt{2}$ and $|1\rangle$ to $(|0\rangle - |1\rangle)/\sqrt{2}$. The state space of an n-qubit system $A = A_1 \cdots A_n$ is given by $\mathcal{H}_A = (\mathbb{C}^2)^{\otimes n} = \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$.

Since we mainly use the above two bases, we can simplify terminology and notation by identifying the computational basis $\{|0\rangle, |1\rangle\}$ with the bit 0 and the Hadamard basis $H\{|0\rangle, |1\rangle\}$ with the bit 1. Hence, when we say that an n-qubit state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ is measured in basis $\theta \in \{0,1\}^n$, we mean that the state is measured qubit-wise where basis $H^{\theta_i}\{|0\rangle, |1\rangle\}$ is used for the i-th qubit. As a result of the measurement, the string $x \in \{0,1\}^n$ is observed with probability $|\langle\psi|H^\theta|x\rangle|^2$, where $H^\theta = H^{\theta_1} \otimes \cdots \otimes H^{\theta_n}$ and $|x\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle$.

An important example 2-qubit state is the *EPR pair* $|\Phi_{AB}\rangle = (|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2} \in \mathcal{H}_A \otimes \mathcal{H}_B = \mathbb{C}^2 \otimes \mathbb{C}^2$, which has the following properties: if qubit A is measured in the computational basis, then a uniformly random bit $x \in \{0,1\}$ is observed and qubit B collapses to $|x\rangle$. Similarly, if qubit A is measured in the Hadamard basis, then a uniformly random bit $x \in \{0,1\}$ is observed and qubit B collapses to $H|x\rangle$.

Density Matrices and Trace Distance. For any complex Hilbert space $\mathcal{H}$, we write $\mathcal{D}(\mathcal{H})$ for the set of all *density matrices* acting on $\mathcal{H}$. We measure closeness of two density matrices ρ and σ in $\mathcal{D}(\mathcal{H})$ by their *trace distance*: $\delta(\rho,\sigma) := \frac{1}{2}\mathrm{tr}|\rho - \sigma|$. One can show that for any physical processing of two quantum states described by ρ and σ, respectively, the two states behave in an indistinguishable way except with probability at most $\delta(\rho,\sigma)$. Thus, informally, if $\delta(\rho,\sigma)$ is very small, then without making a significant error, the two quantum states can be considered equal.

Classical and Hybrid Systems (and States). Subsystem X of a bipartite quantum system XE is called *classical*, if the state of XE is given by a density matrix of the form $\rho_{XE} = \sum_{x\in\mathcal{X}} P_X(x)|x\rangle\langle x| \otimes \rho_E^x$, where $\mathcal{X}$ is a finite set of cardinality $|\mathcal{X}| = \dim(\mathcal{H}_X)$, $P_X : \mathcal{X} \to [0,1]$ is a probability distribution, $\{|x\rangle\}_{x\in\mathcal{X}}$ is some fixed orthonormal basis of $\mathcal{H}_X$, and ρ_E^x is a density matrix on $\mathcal{H}_E$ for every $x \in \mathcal{X}$. Such a state, called *hybrid* state (also known as *cq*-state, for *c*lassical and *q*uantum), can equivalently be understood as consisting of a *random variable* X with distribution P_X and range $\mathcal{X}$, and a system E that is in state ρ_E^x exactly when X takes on the value x. This formalism naturally extends to two (or more) classical systems X, Y etc. as well as to two (or more) quantum systems.

Teleportation. The goal of teleportation is to transport a quantum state from one location to another by only communicating classical information. Teleportation requires pre-shared entanglement among the two locations. Specifically, to teleport a qubit Q in an arbitrary (and typically unknown) state $|\psi\rangle$ from Alice to Bob, Alice performs a Bell-measurement on Q and her half of an EPR-pair, yielding a classical measurement outcome $k \in \{0,1,2,3\}$. This classical information is communicated to Bob, indicating which of the four Pauli-corrections $\{\mathbb{I}, X, Z, XZ\}$ he has to apply on the other half of the corresponding EPR pair, which is held by Bob, to recover the state $|\psi\rangle$.

2.2 Some Quantum Information Theory

The *von Neumann entropy* of a quantum state $\rho \in \mathcal{D}(\mathcal{H})$ is given by $\mathrm{H}(\rho) := -\mathrm{tr}(\rho \log(\rho))$, where here and throughout the article, log denotes the binary logarithm. $\mathrm{H}(\rho)$ is non-negative and at most $\log(\dim(\mathcal{H}))$. For a bi-partite quantum state $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, the *conditional* von Neumann entropy of A given B is defined as $\mathrm{H}(\rho_{AB}|B) := \mathrm{H}(\rho_{AB}) - \mathrm{H}(\rho_B)$. In cases where the state ρ_{AB} is clear from the context, we may write $\mathrm{H}(A|B)$ instead of $\mathrm{H}(\rho_{AB}|B)$. If X and Y are both classical, then $\mathrm{H}(X|Y)$ coincides with the classical conditional Shannon entropy. Furthermore, in case of conditioning (partly) on a classical state, the following holds.

Lemma 1. *For any tri-partite state ρ_{ABY} with classical Y: $\mathrm{H}(A|BY) = \sum_y P_Y(y)\, \mathrm{H}(\rho^y_{AB}|B)$.*

Lemma 1 along with the concavity of H and Jensen's inequality implies that for classical Y: $\mathrm{H}(A) \geq \mathrm{H}(A|Y) \geq 0$. The proof of Lemma 1 is given in Appendix A.

The following theorem, known as Holevo bound [Hol73] (see also [NC00]), plays an important role in many applications of quantum information theory. Informally, it says that measuring only reduces your information. Formally, and tailored to the notation used here, it ensures the following.

Theorem 1 (Holevo bound)**.** *Let $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ be an arbitrary bi-partite state, and let ρ_{AY} be obtained by measuring B in some basis to observe (classical) Y. Then $\mathrm{H}(A|Y) \geq \mathrm{H}(A|B)$.*

For classical X and Y, the Fano inequality [Fan61] (see also [CT91]) allows to bound the probability of correctly guessing X when having access to Y. In the statement below and throughout the article, $\mathrm{h} : [0,1] \to [0,1]$ denotes the *binary entropy function* defined as $\mathrm{h}(p) = -p\log(p) - (1-p)\log(1-p)$ for $0 < p < 1$ and as $\mathrm{h}(p) = 0$ for $p = 0$ or 1, and $\mathrm{h}^{-1} : [0,1] \to [0, \frac{1}{2}]$ denotes its inverse on the branch $0 \leq p \leq \frac{1}{2}$.

Theorem 2 (Fano inequality)**.** *Let X and Y be random variables with ranges $\mathcal{X}$ and $\mathcal{Y}$, respectively, and let $\hat{X}$ be a guess for X computed solely from Y. Then $q := P[\hat{X} \neq X]$ satisfies*

$$\mathrm{h}(q) + q\log(|\mathcal{X}| - 1) \geq \mathrm{H}(X|Y)\ .$$

In particular, for binary X: $q \geq \mathrm{h}^{-1}(\mathrm{H}(X|Y))$.

2.3 Strong Complementary Information Tradeoff

The following entropic uncertainty principle, called *strong complementary information tradeoff* (CIT) in [RB09] and generalized in [BCC+10], is at the heart of our security proofs. It relates the uncertainty of the measurement outcome of a system A with the uncertainty of the measurement outcome when the complementary basis is used instead, and it guarantees that there can coexist at most one system E that has full information on *both* possible outcomes. Note that by the *complementary* basis $\bar{\theta}$ of a basis $\theta = (\theta_1, \ldots, \theta_n) \in \{0,1\}^n$, we mean the n-bit string $\bar{\theta} = (\bar{\theta}_1, \ldots, \bar{\theta}_n) \in \{0,1\}^n$ with $\bar{\theta}_i \neq \theta_i$ for all i.

Theorem 3 (CIT)**.** *Let $|\psi_{AEF}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_E \otimes \mathcal{H}_F$ be an arbitrary tri-partite state, where $\mathcal{H}_A = (\mathbb{C}^2)^{\otimes n}$. Let the hybrid state ρ_{XEF} be obtained by measuring A in basis $\theta \in \{0,1\}^n$, and let the hybrid state σ_{XEF} be obtained by measuring A (of the original state $|\psi_{AEF}\rangle$) in the complementary basis $\bar{\theta}$. Then*

$$\mathrm{H}(\rho_{XE}|E) + \mathrm{H}(\sigma_{XF}|F) \geq n\ . \tag{1}$$

CIT in particular implies the following:

Corollary 1. *Let $|\psi_{AEF}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_E \otimes \mathcal{H}_F$ be an arbitrary tri-partite state, where $\mathcal{H}_A = (\mathbb{C}^2)^{\otimes n}$. Let Θ be uniformly distributed in $\{0,1\}^n$ and let X be the result of measuring A in basis Θ. Then*

$$\mathrm{H}(X|\Theta E) + \mathrm{H}(X|\Theta F) \geq n\ . \tag{2}$$

Proof. By Lemma 1, we can write

$$\begin{aligned} \mathrm{H}(X|\Theta E) + \mathrm{H}(X|\Theta F) &= \frac{1}{2^n}\sum_\theta \mathrm{H}(\rho^\theta_{XE}|E) + \frac{1}{2^n}\sum_\theta \mathrm{H}(\rho^\theta_{XF}|F) \\ &= \frac{1}{2^n}\sum_\theta \left(\mathrm{H}(\rho^\theta_{XE}|E) + \mathrm{H}(\rho^{\bar\theta}_{XF}|F)\right). \end{aligned} \tag{3}$$

Note that ρ^θ_{XE} is obtained by measuring A of $|\psi_{AEF}\rangle$ in basis θ (and ignoring F), and $\rho^{\bar\theta}_{XF}$ is obtained by measuring A of $|\psi_{AEF}\rangle$ in the complementary basis $\bar\theta$ (and ignoring E). Hence, Theorem 3 applies and we can conclude that $\mathrm{H}(\rho^\theta_{XE}|E) + \mathrm{H}(\rho^{\bar\theta}_{XF}|F) \geq n$ and thus $\mathrm{H}(X|\Theta E) + \mathrm{H}(X|\Theta F) \geq n$. □

3 Setup and Position-Verification

3.1 The Model

We informally describe the model we use for the upcoming sections, which is a quantum version of the Vanilla (standard) model introduced in [CGMO09] (see there for a full description). We also describe our *restricted model* used for our security proof, that we call the no pre-shared entanglement (No-PE) model. We consider entities $V_0, \ldots, V_k$ called *verifiers* and an entity P, the (honest) *prover*. Additionally, we consider a coalition $\hat{P}$ of *dishonest provers* (or *adversaries*) $\hat{P}_0, \ldots, \hat{P}_\ell$. All entities can perform arbitrary quantum (and classical) operations and can communicate quantum (and classical) messages among them. For our positive results, we consider a restricted model, in which the amount of entanglement pre-shared between the dishonest provers is bounded. We define the *No-PE model* to be such that the coalition of provers $\hat{P}$ do not pre-share *any* entangled states. That is, a dishonest prover can send quantum communication only after it receives the verifiers message.

For simplicity, we assume that quantum operations and communication is noise-free; however, our results generalize to the more realistic noisy case, assuming that the noise is low enough. We require that the verifiers have a private and authentic channel among themselves, which allows them to coordinate their actions by communicating before, during or after protocol execution. We stress however, that this does not hold for the communication between the verifiers and P: $\hat{P}$ has full control over the destination of messages communicated between the verifiers and P (both ways). This in particular means that the verifiers do not know per-se if they are communicating with the honest or a dishonest prover (or a coalition of dishonest provers).

The above model is now extended by incorporating the notion of *time* and *space*. Each entity is assigned an arbitrary but fixed position *pos* in the d-dimensional space $\mathbb{R}^d$, and we assume that messages to be communicated travel at fixed velocity v (e.g. with the speed of light) , and hence the time needed for a message to travel from one entity to another equals the Euclidean distance between the two (assuming that v is normalized to 1). This holds for honest and dishonest entities. We assume on the other hand that local computations take no time.

Finally, we assume that the verifiers have precise and synchronized clocks, so that they can coordinate exact times for sending off messages and can measure the exact time of a message arrival. We do not require P's clock to be precise or in sync with the verifiers. However, we do assume that P cannot be reset.

This model allows to perform reasonings of the following kind. Consider a verifier V_0 that is at position pos_0 and who sends a challenge ch_0 to the (supposedly honest) prover claiming to be at position *pos*. If V_0 receives a reply within time $2d(pos_0, pos)$, where $d(\cdot,\cdot)$ is the Euclidean distance measure in $\mathbb{R}^d$ and thus also measures the time a message takes from one point to the other, then V_0 can conclude that he is communicating with a prover that is within distance $d(pos_0, pos)$.

Throughout the article, we require that the honest prover P is *enclosed* by the verifiers $V_0, \ldots, V_k$ in that the prover's position $pos \in \mathbb{R}^d$ lies within the tetrahedron, i.e., convex hull, $\mathrm{Hull}(pos_0, \ldots, pos_k) \subset \mathbb{R}^d$ formed by the respective positions of the verifiers. Note that in this work we consider only *stand-alone security*, i.e., there exists only a single execution with a single honest prover, and we do not guarantee concurrent security.

3.2 Secure Position-Verification

A position-verification scheme should allow a prover P at position $pos \in \mathbb{R}^d$ (in d-dimensional space) to convince a set of $k+1$ verifiers $V_0, \ldots, V_k$, which are located at respective positions $pos_0, \ldots, pos_k \in \mathbb{R}^d$, that he is indeed at position pos. We assume that P is enclosed by $V_0, \ldots, V_k$. We require that the verifiers jointly accept if an honest prover P is at position pos, and we require that the verifiers reject with "high" probability in case of a dishonest prover that is not at position pos. The latter should hold even if the dishonest prover consist of a *coalition* of collaborating dishonest provers $\hat{P}_0, \ldots, \hat{P}_\ell$ at arbitrary positions $apos_0, \ldots, apos_\ell \in \mathbb{R}^d$ with $apos_i \neq pos$ for all i. We refer to [CGMO09] for the general formal definition of the completeness and security of a position-verification scheme. In this article, we focus on position-verification schemes of the following form:

Definition 1. *A* **1-round position-verification scheme** PV *consists of a challenge generator* Chlg*, which outputs a list of challenges* $(ch_0, \ldots, ch_k)$ *and auxiliary information* x*, a response algorithm* Resp*, which on input a list of challenges outputs a list of responses* $(x'_0, \ldots, x'_k)$*, and a verification algorithm* Ver *with* $\mathsf{Ver}(x'_1, \ldots, x'_k, x) \in \{0, 1\}$*.* PV *is said to have* **perfect completeness** *if* $\mathsf{Ver}(x'_1, \ldots, x'_k, x) = 1$ *with probability 1 for* $(ch_0, \ldots, ch_k)$ *and* x *generated by* Chlg *and* $(x'_0, \ldots, x'_k)$ *by* Resp *on input* $(ch_0, \ldots, ch_k)$*.*

The algorithms Chlg, Resp and Ver are used as described in Fig. 1 to verify the claimed position of a prover P. We clarify that in order to have all the challenges arrive at P's (claimed) location pos *at the same time*, the verifiers agree on a time T and each V_i sends off his challenge ch_i at time $T - d(pos_i, pos)$. As a result, all ch_i's arrive at P's position pos at time T. In step 3, V_i receives x'_i *in time* if x'_i arrives at V_i's position pos_i at time $T + d(pos_i, pos)$. Throughout the article, we use this simplified terminology. Furthermore, we are sometimes a bit sloppy in distinguishing a party, like P, from its location pos.

Common input to the verifiers: their respective positions $pos_0, \ldots, pos_k$, and P's (claimed) position pos.

0. V_0 generates $(ch_0, \ldots, ch_k)$ and x using Chlg, and sends ch_i to V_i for $i = 1, \ldots, k$.
1. Every V_i sends ch_i to P in such a way that all ch_i's arrive at the same time at P's position pos.
2. P computes $(x'_0, \ldots, x'_k) := \mathsf{Resp}(ch_0, \ldots, ch_k)$ as soon as all the ch_i's arrive, and he sends x'_i to V_i for every i.
3. The V_i's jointly accept if and only if all V_i's receive x'_i in time and $\mathsf{Ver}(x'_1, \ldots, x'_k, x) = 1$.

Figure 1: Generic 1-round position-verification scheme.

We stress that we allow Chlg, Resp and Ver to be *quantum* algorithms and ch_i, x and x'_i to be quantum information. In our constructions, only ch_0 will actually be quantum; thus, we will only require quantum communication from V_0 to P, all other communication is classical. Also, in our constructions, $x'_1 = \ldots = x'_k$, and $\mathsf{Ver}(x'_1, \ldots, x'_k, x) = 1$ exactly if $x'_i = x$ for all i.

Definition 2. *A 1-round position-verification scheme* $\mathsf{PV} = (\mathsf{Chlg}, \mathsf{Resp}, \mathsf{Ver})$ *is called* ε**-sound** *if for any position* $pos \in \mathrm{Hull}(pos_0, \ldots, pos_k)$*, and any coalition of dishonest provers* $\hat{P}_0, \ldots, \hat{P}_\ell$ *at arbitrary positions* $apos_0, \ldots, apos_\ell$*, all* $\neq pos$*, when executing the scheme from Fig. 1 the verifiers accept with probability at most* ε*. We then write* PV^ε *for such a protocol.*

In order to be more realistic, we must take into consideration physical limitations of the equipment used, such as measurement errors, computation durations, etc. Those allow a dishonest prover which resides arbitrarily close to P to appear as if she resides at pos. Thus, we assume that all the adversaries are at least Δ-distanced from pos, where Δ is determined by those imperfections. For sake of simplicity, this Δ is implicit in the continuation of the paper.

A position-verification scheme can also be understood as a (position-based) *identification* scheme, where the identification is not done by means of a cryptographic key or a password, but by means of the geographical location.

4 Impossibility of Position-Verification with Unlimited Adversary

4.1 Setting and Notation

For simplicity, we consider the one-dimensional case, with two verifiers V_0 and V_1, but the attack can be generalized to higher dimensions and more verifiers.

We consider an arbitrary 1-round position-verification scheme as specified in Fig. 1. We let A_i be the quantum system used to communicate the challenge ch_i from V_i to P. For simplicity, we assume that the output system to communicate the replay x'_i back to V_i is of the same size and also denote it by A_i. We let B be the quantum system that stores the auxiliary information x. Specifically, Chlg produces a quantum state $\rho_{A_0A_1B}$, and the systems A_0 and A_1 are sent to P by V_0 and V_1, respectively. Resp instructs P to apply some unitary transformation U to A_0 and A_1, resulting in state $\sigma_{A_0A_1B} = (U \otimes \mathbb{I})\rho_{A_0A_1B}(U^\dagger \otimes \mathbb{I})$. Then, P has to send A_0 and A_1 immediately back to V_0 and V_1, respectively. For simplicity, let us further assume that both systems A_0 and A_1 consist of n qubits.

We would like to point out that assuming Resp to be a unitary transformation and restricting both input- and output-systems to be of equal size is without loss of generality; a general quantum operation can be taken care of simply by adding some ancilla to, say, A_0.

We show below that any pair of dishonest provers, $\hat{P}_0$ and $\hat{P}_1$, with $pos_0 < apos_0 < pos < apos_1 < pos_1$, can transform $\rho_{A_0A_1B}$ into $\sigma_{A_0A_1B}$ and provide V_0 and V_1 in time with the systems A_0 and A_1. Our attack is based on a scheme for "instantaneous measurement of non-local variables" by Vaidman [Vai03]. Similarly to the teleportation attacks presented by Kent, Munro and Spiller [KMS10], it uses the entanglement between the dishonest provers to teleport states back and forth.

4.2 Attack

Our attack makes use of teleportation, as described in Section 2.1. However, it is used in a somewhat unusual and suprising way: the receiver of a teleported quantum state acts on the received state, e.g. by applying a unitary transformation and/or teleporting it back, *before* receiving the measurement outcome k and thus *without* applying the Pauli-correction. All the teleportation steps in our attack and the subsequent actions on the received state should be understood in this sense.

The steps of the attack are the following (see Fig. 2). For ease of notation, we do not write the B system holding the verifier's auxiliary information.

1. When ρ_{A_0} reaches $\hat{P}_0$, she uses her first n EPR-halves to teleport the state to $\hat{P}_1$. Let us denote the measurement outcome by $k \in \{0,1,2,3\}^n$. In this and all following teleportation steps, all classical measurement outcomes are sent immediately to $\hat{P}_1$ (and vice versa).

2. Let us denote by $\rho^1_{A_0A_1}$ the state consisting of the first n EPR-halves held by $\hat{P}_1$ joined with the state ρ_{A_1} she received from V_1. $\hat{P}_1$ acts as if no error occurred in the teleportation step and applies the unitary transform U on $\rho^1_{A_0A_1}$ to obtain the state $\sigma^1_{A_0A_1} = U\rho^1_{A_0A_1}U^\dagger$. She then teleports all $2n$ qubits of $\sigma^1_{A_0A_1}$ back to $\hat{P}_0$ using the next $2n$ EPR-halves shared with $\hat{P}_0$. Let us denote the classical outcome of the teleportation measurement by $\ell \in \{0,1,2,3\}^{2n}$. As above, she immediately forwards these classical measurement outcomes to $\hat{P}_0$.

3. Let us denote by $\hat{\sigma}^1_{A_0A_1}$ the (uncorrected) state $\hat{P}_0$ receives when $\hat{P}_1$ teleports $\sigma^1_{A_0A_1}$ to her. If the outcome of the initial teleportation was the string $k = 0\ldots0$ consisting of n zeros (indicating that no correction needs to be applied), we have that $\rho^1_{A_0A_1} = \rho_{A_0A_1}$ and thus $\sigma^1_{A_0A_1} = \sigma_{A_0A_1}$. In this case, $\hat{P}_0$ sends the second system $\hat{\sigma}^1_{A_1}$ of the received (uncorrected) state to $\hat{P}_1$. When ℓ arrives at $\hat{P}_0$, she

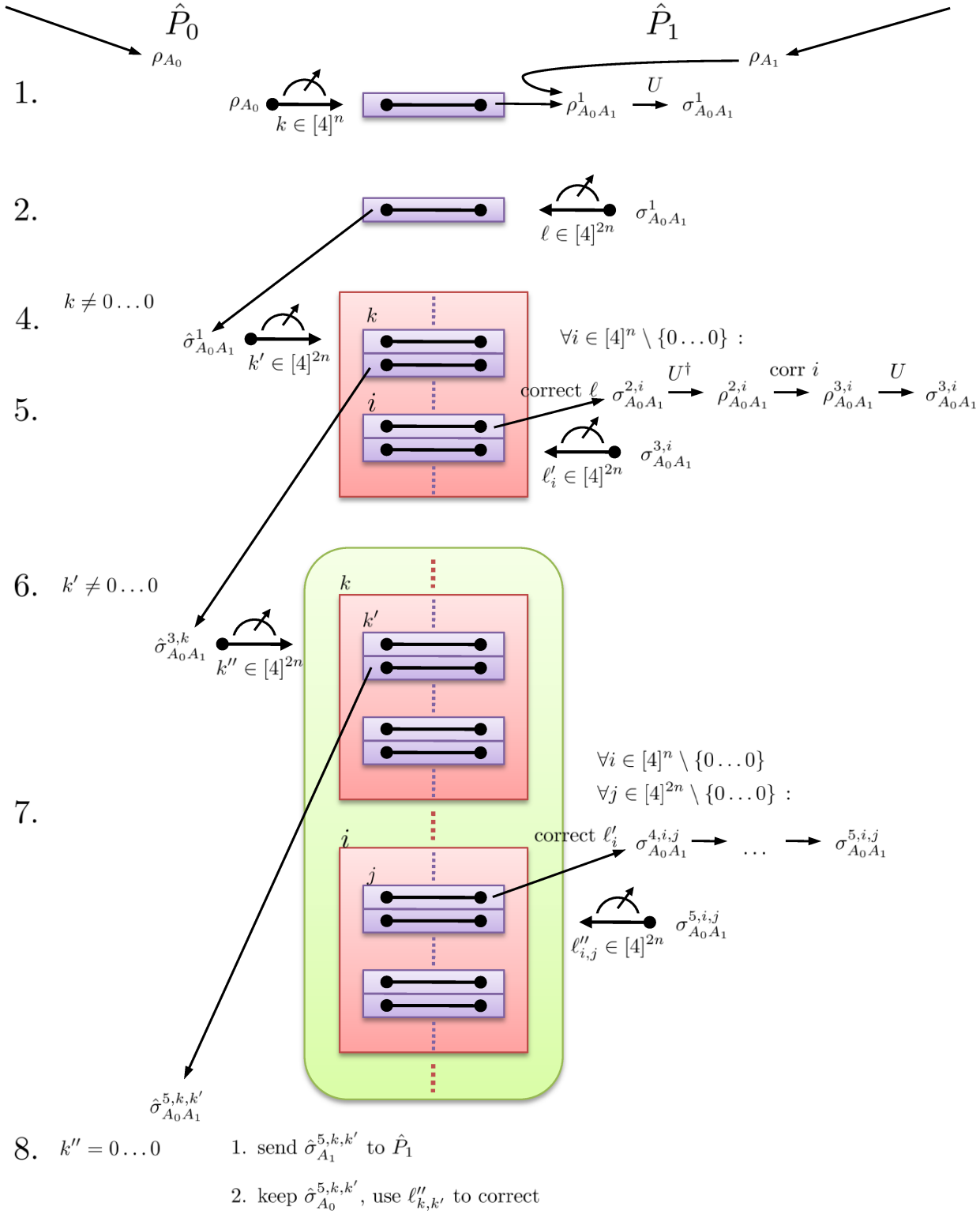

Figure 2: Schematic of the attack steps (described in the main text) with two levels of recursion. $\hat{P}_0$'s measurement outcomes in the first two teleportation steps are different from the all-zero string, $k, k' \neq 0 \dots 0$, only the third step succeeds in $k'' = 0 \dots 0$. Dot-arrows with measurement signs are used to denote the teleportation of a state using the EPR pair on the same level, resulting in a classical outcome $k \in [4]$ where $[4]$ is the abbreviation for the set $\{0, 1, 2, 3\}$.

holds enough information to correct her n EPR-halves $\hat{\sigma}^1_{A_0}$ to the state $\sigma^1_{A_0} = \sigma_{A_0}$ which she sends to V_0. Similarly, when $\hat{P}_1$ receives (together with $k = 0\ldots0$) the uncorrected system $\hat{\sigma}^1_{A_1}$ from $\hat{P}_0$, she uses ℓ to correct it to $\sigma^1_{A_1} = \sigma_{A_1}$ and sends it to V_1. It is clear that the attack succeeds in this case. However, what happens if $k \neq 0\ldots0$?

4. In that case, $\hat{P}_0$ uses her next $2n(4^n-1)$ EPR-halves to teleport $\hat{\sigma}^1_{A_0A_1}$ back to $\hat{P}_1$. At the same time, $\hat{P}_0$ "informs" $\hat{P}_1$ by the use of the channel what error k occurred in the first teleportation step. Concretely, let us divide the next $4n(4^n-1)$ shared EPR-pairs into 4^n-1 clusters of $4n$ EPR-pairs each. Every cluster is labelled with one of the 4^n-1 non-zero measurement outcomes for $k \in \{0,1,2,3\}^n \setminus \{0\ldots0\}$. $\hat{P}_0$ uses the first $2n$ qubits of the cluster with label k to teleport $\hat{\sigma}^1_{A_0A_1}$ back to $\hat{P}_1$. This yields classical outcome $k' \in \{0,1,2,3\}^{2n}$. The other clusters with labels $i \neq k$ are not used by $\hat{P}_0$.

5. For every cluster-label i, $\hat{P}_1$ treats the first $2n$ qubits of cluster i as follows: Pretending that $k' = 0\ldots0$, i.e., no error occurred in the last teleportation step from $\hat{P}_0$ to $\hat{P}_1$, she first corrects the Pauli-errors that occurred in the previous teleportation of $\sigma^1_{A_0A_1}$ from $\hat{P}_1$ to $\hat{P}_0$ according to her outcome ℓ, resulting in state $\sigma^{2,i}_{A_0A_1}$. She undoes the unitary operation yielding

$$\rho^{2,i}_{A_0A_1} = U^\dagger \sigma^{2,i}_{A_0A_1} U\,.$$

$\hat{P}_1$ applies the Pauli-correction corresponding to error i to $\rho^{2,i}_{A_0}$ and joins it with $\rho^{2,i}_{A_1}$ to get the state $\rho^{3,i}_{A_0A_1}$. Note that if k' indeed happens to be $0\ldots0$ and for $i = k$, the resulting state $\rho^{3,i}_{A_0A_1}$ equals the original state $\rho_{A_0A_1}$. She re-applies the unitary transformation to obtain

$$\sigma^{3,i}_{A_0A_1} = U \rho^{3,i}_{A_0A_1} U^\dagger\,.$$

The $2n$ qubits of state $\sigma^{3,i}_{A_0A_1}$ are then teleported back to $\hat{P}_0$ using the second $2n$ qubits in cluster i resulting in classical outcomes $\ell'_i \in \{0,1,2,3\}^{2n}$.

6. If the outcome of the teleportation of $\hat{\sigma}^1_{A_0A_1}$ was $k' = 0\ldots0$, $\hat{P}_0$ sends the second system A_1 of the received state $\hat{\sigma}^{3,k}_{A_0A_1}$ to $\hat{P}_1$. In this case, $\hat{P}_1$ indeed corrected the Pauli-error k from the first teleportation and we have that $\sigma^{3,k}_{A_0A_1} = \sigma_{A_0A_1}$. When ℓ'_k arrives at $\hat{P}_0$, she holds enough information to correct her n EPR-halves $\hat{\sigma}^{3,k}_{A_0}$ of cluster k to the state $\sigma^{3,k}_{A_0} = \sigma_{A_0}$ which she sends to V_0. Similarly, when $\hat{P}_1$ receives k and $k' = 0\ldots0$, $\hat{P}_1$ corrects $\hat{\sigma}^{3,k}_{A_1}$ to $\sigma^{3,k}_{A_1} = \sigma_{A_1}$ using ℓ'_k and sends it to V_1 to successfully complete the attack. If $k' \neq 0\ldots0$, the players enter the next layer of recursion:[1]

Let us divide the following $4n(4^n-1)(4^{2n}-1)$ shared EPR-pairs in 4^n-1 clusters of $4n(4^n-1)$ EPR-pairs each (the red blocks in Step 6 of Fig. 2). Each cluster is further divided into sub-clusters of $4n$ EPR-pairs each. Every cluster is labelled with one of the 4^n-1 non-zero measurement outcomes for k. Sub-clusters of cluster i are labelled with one of the $4^{2n}-1$ non-zero measurement outcomes for k'_i. $\hat{P}_0$ uses the first $2n$ qubits of subcluster labelled k' of cluster labelled k to teleport $\hat{\sigma}^{3,k}_{A_0A_1}$ back to $\hat{P}_1$. This yields classical outcome $k'' \in \{0,1,2,3\}^{2n}$. The other (sub-)clusters are not used by $\hat{P}_0$.

7. For every subcluster-label j of every cluster-label i, $\hat{P}_1$ treats the first $2n$ qubits of subcluster j of cluster i as follows: Assuming that $k'' = 0\ldots0$, i.e., no error occurred in the last teleportation step from $\hat{P}_0$ to $\hat{P}_1$, $\hat{P}_1$ knows that errors $k = i$ and $k' = j$ have occurred in the previous teleportation steps. Together with the knowledge of her own outcomes ℓ and ℓ_i, she undoes her previous actions, performs the right corrections according to i and j and applies the unitary resulting in the state $\sigma^{4,i,j}_{A_0A_1}$. These $2n$ qubits are then teleported back to $\hat{P}_0$ using the second $2n$ qubits in subcluster j of cluster i yielding classical outcomes $\ell''_{i,j} \in \{0,1,2,3\}^{2n}$.

[1] We note that only $\hat{P}_0$ actually learns "when" the attack has succeeded. In a concrete instantiation, the dishonest provers agree beforehand on a fixed number of recursion layers. As the non-signalling principle prevents $\hat{P}_1$ from instantaneously learning $\hat{P}_0$'s measurement outcomes, she simply continues the attack for all pre-agreed levels of recursions. Only when $\hat{P}_0$'s classical communication reaches $\hat{P}_1$, she learns at which level the attack has succeeded.

8. If the outcome of the teleportation of $\hat{\sigma}^{3,k}_{A_0A_1}$ was $k'' = 0\ldots0$, $\hat{P}_0$ sends the second system A_1 of the received state $\hat{\sigma}^{4,k,k'}_{A_0A_1}$ to $\hat{P}_1$. In this case, $\hat{P}_1$ indeed corrected the Pauli-errors k and k' from the first and second teleportations and we have that $\sigma^{4,k,k'}_{A_0A_1} = \sigma_{A_0A_1}$. When $\ell''_{k,k'}$ arrives at $\hat{P}_0$, she holds enough information to correct her n EPR-halves $\hat{\sigma}^{4,k,k'}_{A_0}$ of subcluster k' of cluster k to the state $\sigma^{4,k,k'}_{A_0} = \sigma_{A_0}$ which she sends to V_0. Similarly, when $\hat{P}_1$ receives k, k' and $k'' = 0\ldots0$, $\hat{P}_1$ corrects $\hat{\sigma}^{4,k,k'}_{A_1}$ to $\sigma^{4,k,k'}_{A_1} = \sigma_{A_1}$ using $\ell''_{k,k'}$ and sends it to V_1 to successfully complete the attack. Otherwise, the next layer of recursion is entered, etc.

4.3 Analysis

The attack succeeds if $\hat{P}_0$'s measurement outcome equals the all-zero string at some layer of the recursion. The chance that the first teleportation outcome k is the all-zero string is $\frac{1}{4^n}$. For the following layers of recursion, the probability of success is the same, namely $\frac{1}{4^{2n}}$. Therefore, the probability that the attack fails in each of r layers of recursion is at most $(1 - \frac{1}{4^n})(1 - \frac{1}{4^{2n}})^{r-1}$. Thus, with an unbounded amount of entanglement between the dishonest provers, this attack can be performed with a success probability arbitrarily close to 1.

The amount of EPR pairs used by the dishonest provers increases exponentially with the number of recursion layers. It is an interesting open question whether such a large amount of entanglement is necessary to perform this general attack.

5 Secure Position-Verification in the No-PE model

We show the possibility of secure position-verification in the No-PE model. We consider the following basic 1-round position-verification scheme in the No-PE model, given in Fig. 3. It is based on the BB84 encoding. In all our protocols all parties abort if they receive any message which is inconsistent with the protocol, for instance (classical) message with a wrong length, or different number of received qubits than expected, etc.

0. V_0 chooses two random bits $x, \theta \in \{0,1\}$ and sends them privately to V_1.
1. V_0 prepares the qubit $H^\theta|x\rangle$ and sends it to P, and V_1 sends the bit θ to P, so that $H^\theta|x\rangle$ and θ arrive at the same time at P.
2. When $H^\theta|x\rangle$ and θ arrive, P measures $H^\theta|x\rangle$ in basis θ to observe $x' \in \{0,1\}$, and sends x' to V_0 and V_1.
3. V_0 and V_1 accept if on both sides x' arrives in time and $x' = x$.

Figure 3: Position-verification scheme $\mathsf{PV}^{\varepsilon}_{\mathrm{BB84}}$ based on the BB84 encoding.

Theorem 4. *In the No-PE model, the 1-round position-verification scheme $\mathsf{PV}^{\varepsilon}_{\mathrm{BB84}}$ from Fig. 3 is ε-sound with $\varepsilon = 1 - \mathrm{h}^{-1}(\frac{1}{2})$.*

A numerical calculation shows that $\mathrm{h}^{-1}(\frac{1}{2}) \geq 0.11$ and thus $\varepsilon \leq 0.89$. A particular attack for a dishonest prover $\hat{P}$, sitting in-between V_0 and P, is to measure the qubit $H^\theta|x\rangle$ in the *Breidbart* basis, resulting in an acceptance probability of $\cos(\pi/8)^2 \approx 0.85$. This shows that our analysis is pretty tight.

Proof. In order to analyze the position-verification scheme it is convenient to consider an equivalent *purified* version, given in Fig. 4. The only difference between the original and the purified scheme is the point in time when V_0 measures A (indeed, preparing $|\Phi_{AB}\rangle$ and measuring A in basis θ is just one possible way to prepare $H^\theta|x\rangle$) and the point in time when V_1 learns x. This, however, has no influence on the view of the

0. V_0 and V_1 privately agree on a random bit $\theta \in \{0,1\}$.
1. V_0 prepares an EPR pair $|\Phi_{AB}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, keeps qubit A and sends qubit B to P, and V_1 sends the bit θ to P, so that B and θ arrive at the same time at P.
2. When B and θ arrive, P measures B in basis θ to observe $x' \in \{0,1\}$, and sends x' to V_0 and V_1.
3. Only now, when x' arrives, V_0 measures qubit A in basis θ to observe x, and privately sends x to V_1. V_0 and V_1 accept if on both sides x' arrives in time and $x' = x$.

Figure 4: EPR version of $\mathsf{PV}^{\varepsilon}_{\mathrm{BB84}}$.

(dishonest or honest) prover, nor on the joint distribution of θ, x and x', and thus neither on the probability that V_0 and V_1 accept. It therefore suffices to analyze the purified version.

We first consider security against two dishonest provers $\hat{P}_0$ and $\hat{P}_1$, where $\hat{P}_0$ is between V_0 and P and $\hat{P}_1$ is between V_1 and P. In the end we will argue that a similar argument holds for multiple dishonest provers on either side.

Since V_0 and V_1 do not accept if x' does not arrive in time and dishonest provers do not use pre-shared entanglement in the No-PE-model, any potentially successful strategy of $\hat{P}_0$ and $\hat{P}_1$ must look as follows. As soon as $\hat{P}_1$ receives the bit θ from V_1, she forwards (a copy of) it to $\hat{P}_0$. Also, as soon as $\hat{P}_0$ receives the qubit A, she applies an arbitrary quantum operation to the received qubit A (and maybe some ancillary system she possesses) that maps it into a bipartite state E_0E_1 (with arbitrary state space $\mathcal{H}_{E_0} \otimes \mathcal{H}_{E_1}$), and $\hat{P}_0$ keeps E_0 and sends E_1 to $\hat{P}_1$. Then, as soon as $\hat{P}_0$ receives θ, she applies some measurement (which may depend on θ) to E_0 to obtain $\hat{x}_0$, and as soon as $\hat{P}_1$ receives E_1, she applies some measurement (which may depend on θ) to E_1 to obtain $\hat{x}_1$, and both send $\hat{x}_0$ and $\hat{x}_1$ immediately to V_0 and V_1, respectively. We will now argue that the probability that $\hat{x}_0 = x$ *and* $\hat{x}_1 = x$ is upper bounded by ε as claimed.

Let $|\psi_{A\,E_0E_1}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_{E_0} \otimes \mathcal{H}_{E_1}$ be the state of the tri-partite system $A\,E_0E_1$ after $\hat{P}_0$ has applied the quantum operation to the qubit B. Note that in the No-PE model, the quantum operation and thus $|\psi_{A\,E_0E_1}\rangle$ does not depend on θ.[2] Recall that x is obtained by measuring A in either the computational (if $\theta = 0$) or the Hadamard (if $\theta = 1$) basis. Writing x, θ, etc. as random variables X, Θ, etc., it follows from CIT (specifically Corollary 1) that $\mathrm{H}(X|\Theta E_0) + \mathrm{H}(X|\Theta E_1) \geq 1$. Let Y_0 and Y_1 denote the classical information obtained by $\hat{P}_0$ and $\hat{P}_1$ as a result of measuring E_0 and E_1, respectively, with bases that may depend on Θ. By the Holevo bound (Theorem 1), it follows from the above that

$$\mathrm{H}(X|\Theta Y_0) + \mathrm{H}(X|\Theta Y_1) \geq 1 \ ,$$

therefore $\mathrm{H}(X|\Theta Y_i) \geq \frac{1}{2}$ for at least one $i \in \{0,1\}$. By Fano's inequality (Theorem 2), we can conclude that the corresponding error probability $q_i = P[\hat{X}_i \neq X]$ satisfies $\mathrm{h}(q_i) \geq \frac{1}{2}$. It thus follows that the failure probability

$$q = P[\hat{X}_0 \neq X \vee \hat{X}_1 \neq X] \geq \max\{q_0, q_1\} \geq \mathrm{h}^{-1}(\frac{1}{2}) \ ,$$

and the probability of V_0 and V_1 accepting, $P[\hat{X}_0 = X \wedge \hat{X}_1 = X] = 1 - q$, is indeed upper bounded by ε as claimed.

It remains to argue that more than two dishonest provers in the No-PE model cannot do any better. The reasoning is the same as above. Namely, in order to respond in time, the dishonest provers that are closer to V_0 than P must map the qubit A—possibly jointly—into a bipartite state E_0E_1 *without knowing* θ, and jointly keep E_0 and send E_1 to the dishonest provers that are "on the other side" of P (i.e., closer to V_1). Then, the reply for V_0 needs to be computed from E_0 and θ (possibly jointly by the dishonest provers that are closer to V_0), and the response for V_1 from E_1 and θ. Thus, it can be argued as above that the success probability is bounded by ε as claimed.

□

[2] We point out that once the adversaries pre-share entangled states, more general attacks (such as the one described in Section 4) are possible and this reasoning no longer holds.

5.1 Reducing the Soundness Error

In order to obtain a position-verification scheme with a negligible soundness error, we can simply repeat the 1-round scheme $\mathsf{PV}^{\varepsilon}_{\text{BB84}}$ from Fig. 3. Repeating the scheme n times *in sequence*, where the verifiers launch the next execution only after the previous one is finished, reduces the soundness error to ε^n. This follows immediately from the security of the 1-round scheme.

Corollary 2. *In the No-PE model, the n-fold sequential repetition of $\mathsf{PV}^{\varepsilon}_{\text{BB84}}$ from Fig. 3 is ε^n-sound with $\varepsilon = 1 - \mathrm{h}^{-1}(\frac{1}{2})$.*

In terms of round complexity, a more efficient way of repeating $\mathsf{PV}^{\varepsilon}_{\text{BB84}}$ is by repeating it *in parallel*: V_0 sends n BB84 qubits $H^{\theta_1}|x_1\rangle, \ldots, H^{\theta_n}|x_n\rangle$ and V_1 sends the corresponding bases $\theta_1, \ldots, \theta_n$ to P so that they all arrive at the same time at P's position, and P needs to reply with the correct list $x_1, \ldots, x_n$ in time. This is obviously more efficient in terms of round complexity and appears to be the preferred solution. However, we do not have a proof for the security of the parallel repetition of $\mathsf{PV}^{\varepsilon}_{\text{BB84}}$.

5.2 Position-Verification in Higher Dimensions

The scheme $\mathsf{PV}^{\varepsilon}_{\text{BB84}}$ can easily be extended into higher dimensions. The scheme for d dimensions is a generalization of the scheme $\mathsf{PV}^{\varepsilon}_{\text{BB84}}$ in Fig. 3, where now the challenges of the verifiers V_1, V_2, ..., V_d form a *sum sharing* of the basis θ, i.e., are random $\theta_1, \theta_2, \ldots, \theta_d \in \{0,1\}$ such that their modulo-2 sum equals θ. As specified in Fig. 1, the state $H^{\theta}|x\rangle$ and the shares θ_i are sent by the verifiers to P such that they arrive at P's (claimed) position at the same time. P can then reconstruct θ and measure $H^{\theta}|x\rangle$ in the correct basis to obtain $x' = x$, which he sends to all the verifiers who check if x' arrives in time and equals x.

We can argue security by a reduction to the scheme in 1 dimension. For the sake of concreteness, we consider here 3 dimensions. For 3 dimensions, we need at set of (at least) 4 non-coplanar verifiers $V_0, \ldots, V_3$, and the prover P needs to be located inside the tetrahedron defined by the positions of the 4 verifiers. We consider a coalition of dishonest provers $\hat{P}_0, \ldots, \hat{P}_\ell$ at arbitrary positions but different to P. We may assume that $\hat{P}_0$ is closest to V_0. It is easy to see that there exists a verifier V_j such that $d(\hat{P}_0, V_j) > d(P, V_j)$. Furthermore, we may assume that V_j is not V_0 and thus we assume for concreteness that it is V_1. We now strengthen the dishonest provers by giving them θ_2 and θ_3 for free from the beginning. Since, when θ_2 and θ_3 are given, θ can be computed from θ_1 and vice versa, we may assume that V_1 actually sends θ as challenge rather than θ_1. But now, θ_2 and θ_3 are now just two random bits, independent of θ and x, and are thus of no help to the dishonest provers and we can safely ignore them.

As $\hat{P}_0$ is further away from V_1 than P is, $\hat{P}_0$ cannot afford to store $H^{\theta}|x\rangle$ until he has learned θ. Indeed, otherwise V_1 will not get a reply in time. Therefore, before she learns θ, $\hat{P}_0$ needs to apply a quantum transformation to $H^{\theta}|x\rangle$ with a bi-partite output and keep one part of the output, E_0, and send the other part, E_1 in direction of V_1. Note that this quantum transformation is independent of θ, as long as $\hat{P}_0$ does not share an entangled state with the other dishonest provers (who might know θ by now). Then, $\hat{x}_0$ and $\hat{x}_1$, the replies that are sent to V_0 and V_1, respectively, need then to be computed from θ and E_0 alone and from θ and E_1 alone. It now follows from the analysis of the scheme in 1 dimension that the probability that both $\hat{x}_0$ and $\hat{x}_1$ coincide with x is at most $\varepsilon = 1 - \mathrm{h}^{-1}(\frac{1}{2})$.

Corollary 3. *The above generalization of $\mathsf{PV}^{\varepsilon}_{\text{BB84}}$ to d dimensions is ε-sound in the No-PE model with $\varepsilon = 1 - \mathrm{h}^{-1}(\frac{1}{2})$.*

6 Position-Based Authentication and Key-Exchange

In this section we consider a new primitive: position-based authentication. In contrast to position-verification, where the goal of the verifiers is to make sure that entity P is at the claimed location *pos*, here the verifiers want to make sure that a given message m originates from an entity P that is at the claimed location *pos*. We stress that it is not sufficient to first execute a position-verification scheme with P to ensure that P is at position *pos* and then have P send or confirm m, because a coalition of dishonest provers may do a

man-in-the-middle attack and stay passive during the execution of the positioning scheme but then modify the communicated message m.

Formally, in a position-based authentication scheme the prover takes as input a message m and the verifiers $V_0, \ldots, V_k$ take as input a message m' and the claimed position *pos* of P, and we require the following security properties.

- ε_c-*Completeness:* If $m = m'$, P is honest and at the claimed position *pos*, and if there is no (coalition of) dishonest prover(s), then the verifiers jointly accept except with probability ε_c.
- ε_s-*Soundness:* For any $pos \in \text{Hull}(pos_0, \ldots, pos_k)$ and for any coalition of dishonest provers $\hat{P}_0, \ldots, \hat{P}_\ell$ at locations all different to *pos*, if $m \neq m'$ then the verifiers jointly reject except with probability ε_s.

We build a position-based authentication scheme based on our position-verification scheme. The idea is to incorporate the message to be authenticated into the replies of the position-verification scheme. Our construction is very generic and may also be useful for turning other kinds of identification schemes (not necessarily position-based schemes) into corresponding authentication schemes. Our aim is merely to show the existence of such a scheme; we do not strive for optimization. We begin by proposing a weak position-based authentication scheme for a 1-bit message m.

6.1 Weak 1-bit authentication scheme

Let PV^ε be a 1-round position-verification scheme between $k+1$ verifiers $V_0, \ldots, V_k$ and a prover P. For simplicity, we assume that, like for the scheme $\mathsf{PV}^\varepsilon_{\text{BB84}}$ from Section 5, x and $x'_0, \ldots, x'_k$ are classical, and Ver accepts if $x'_i = x$ for all i, and thus we understand the output of $\mathsf{Resp}(ch_0, \ldots, ch_k)$ as a single element x' (supposed to be x). We require PV^ε to have perfect completeness and soundness $\varepsilon < 1$. We let $\perp$ be some special symbol. We consider the weak authentication scheme given in Fig. 5 for a 1-bit message $m \in \{0,1\}$. We assume that m has already been communicated to the verifiers and thus there is agreement among the verifiers on the message to be authenticated. The weak authentication scheme works by executing the 1-round position-verification scheme PV^ε, but letting P replace his response x' by $\perp$ with probability q, to be specified later.

0. V_0 generates $(ch_0, \ldots, ch_k)$ and x using Chlg and sends ch_i and x to V_i for $i = 1, \ldots, k$.
1. Every verifier V_i sends ch_i to P in such a way that all ch_is arrive at the same time at P.
2. When the ch_is arrive, P computes the authentication tag t as follows and sends it back to all the verifiers. If $m = 1$ then $t := \mathsf{Resp}(ch_0, \ldots, ch_k)$, and if $m = 0$ then $t := \perp$ with probability q and $t := \mathsf{Resp}(ch_0, \ldots, ch_k)$ otherwise.
3. If different verifiers have received different values for t, or it didn't arrive in time, the verifiers abort. Otherwise, they jointly accept if $t = x$ or both $m = 0$ and $t = \perp$.

Figure 5: A generic position-based weak authentication scheme $\mathsf{wAUTH}^\varepsilon$ for a 1-bit message m.

We now analyze the success probability of an adversary authenticating a bit $m' \in \{0,1\}$. We consider the case where there is no honest prover present (we call this an *impersonation attack*), and the case where an honest prover is active and authenticates the bit $m \neq m'$ (we call this a *substitution attack*).

The following properties are easy to verify and follow from the security property of PV^ε.

Lemma 2. *Let $\hat{P}$ be a coalition of dishonest provers not at the claimed position and trying to authenticate message $m' = 1$. In case of an impersonation attack, the verifiers accept with probability at most ε, and in case of a substitution attack (with $m = 0$), the verifiers accept with probability at most $\delta = (1-q) + q\varepsilon = 1 - q(1-\varepsilon) < 1$.*

On the other hand, $\hat{P}$ can obviously authenticate $m' = 0$ by means of a substitution attack with success probability 1; however, informally, $\hat{P}$ has bounded success probability in authenticating message $m' = 0$ by means of an impersonation attack unless he uses the tag $\perp$. (This fact is used latter to obtain a strong authentication scheme.)

Let us try to extend the above in order to get a strong authentication scheme. Based on the observation that by performing a substitution attack on $\mathsf{wAUTH}^{\varepsilon}$, it is easy to substitute the message bit $m = 1$ by $m' = 0$ but non-trivial to substitute $m = 0$ by $m' = 1$, a first approach to obtain an authentication scheme with good security might be to apply $\mathsf{wAUTH}^{\varepsilon}$ bitwise to a *balanced encoding* of the message. Such an encoding should ensure that for any distinct messages m and m', there are many positions in which the encoding of m' is 1 but the encoding of m is 0. Unfortunately, this is not good enough. The reason is that P and the verifiers are not necessarily synchronized. For instance, assume we encode $m = 0$ into $c = 010101...01$ and $m' = 1$ into $c' = 101010...10$, and authentication works by doing $\mathsf{wAUTH}^{\varepsilon}$ bit-wise on all the bits of the encoded message. If $\hat{P}$ wants to substitute $m = 0$ by $m' = 1$ then he can simply do the following. He tries to authenticate the first bit 1 of c' towards the verifiers by means of an impersonation attack. If he succeeds, which he can with constant probability, then he simply authenticates the remaining bits 01010...10 of c' by using P, who is happy to authenticate all of the bits of $c = 010101...01$. Because of this issue of $\hat{P}$ bringing P and the verifiers out of sync, we need to be more careful about the exact encoding we use.

6.2 Secure Position-Based Authentication Scheme

We specify a special class of codes, which is strong enough for our purpose.

Definition 3. *Let $c \in \{0,1\}^N$. A vector $e \in \{-1,0,1\}^{2N}$ is called an* **embedding** *of c if by removing all the -1 entries in e we obtain c. Furthermore, for two strings $c, c' \in \{0,1\}^N$ we say that c'* **λ-dominates** *c if for all embeddings e and e' of c and c' (at least) one of the following holds: (a) the number of positions $i \in \{1,\ldots,2N\}$ for which $e'_i = 1$ and $e_i < 1$ is at least λ, or (b) there exist a consecutive sequence of indices I such that the set $J = \{i \in I : e'_i > -1\}$ has size $|J| \geq 4\lambda$ and it contains at least λ indices $i \in J$ with $e_i = -1$.*

For instance, let $c = 00...0\,11...1$ and $c' = 11...1\,00...0$, where the blocks of 0's and 1's are of length $N/2$. It is not hard to see that the two codewords $N/4$-dominate each other. However, $\tilde{c}' = 0101...01$ does not dominate $\tilde{c} = 1010...10$, since $\tilde{c}'$ can be embedded into $\ddagger 0101...01\ddagger\ddagger...\ddagger$ and $\tilde{c}$ into $1010...10\ddagger\ddagger...\ddagger$, where here and later we use $\ddagger$ to represent -1.

Definition 4. *A code C is* **λ-dominating***, if any two codewords in C λ-dominate each other.*

We note that the requirement for λ-dominating codes can be relaxed in various ways to allow a greater range of codes.

Let $\mathsf{wAUTH}^{\varepsilon}$ be the above weak authentication scheme satisfying Lemma 2. In order to authenticate a message $m \in \{0,1\}^{\mu}$ in a strong way (with λ a security parameter), an encoding c of m using a λ-dominating code C is bit-wise authenticated by means of $\mathsf{wAUTH}^{\varepsilon}$, and the verifiers perform statistics over the number of $\perp$s received. The resulting authentication scheme is given in Fig. 6; as for the weak scheme, we assume that the message m has already been communicated.

Theorem 5. *The generic position-based authentication scheme* AUTH *(Fig. 6) is $Ne^{-2q\lambda}$-complete.*

Proof. An honest prover which follows the above scheme can fail only if for some round r, $n_{\perp} > 8q\lambda$. Using Chernoff bound [Che52], the probability of having $n_{\perp} > 8q\lambda$ at a specific round r, is upper bounded by $e^{-2q\lambda}$. Using the union bound for every possible round j, we bound the failure probability with $Ne^{-2q\lambda}$. □

Before we analyze the security of the authentication scheme, let us discuss the possible attacks on it. Here we treat $\hat{P}$ as a single identity, however $\hat{P}$ represents a collaboration of adversaries. Similarly, we refer the $k+1$ verifiers as a single entity, V. We point out that we do not assume that honest P and V

0. P and the verifiers encode m into a codeword $c = (c_1, \ldots, c_N) \in C$, for a λ-dominating code C.
1. For $j = 1, \ldots, N$, the following is repeated in sequence.
   1.1 P authenticates c_j by means of $\mathsf{wAUTH}^\varepsilon$. Let t_i be the corresponding tag received.
   1.2 If $j > 4\lambda$ then the verifiers compute $n_\perp(j) = |\{i \in \{j - 4\lambda, \ldots, j\} : c_i = 0 \wedge t_i = \perp\}|$.
2. If any of the $\mathsf{wAUTH}^\varepsilon$ executions fails, or if $n_\perp(j) > 8q\lambda$ for some round $j > 4\lambda$ then the verifiers jointly reject. Otherwise, m is accepted.

Figure 6: A generic position-based authentication scheme AUTH.

have synchronized clocks. Therefore, we allow $\hat{P}$ to arbitrarily schedule and interleave the N executions of $\mathsf{wAUTH}^\varepsilon$ that V performs with the N executions that P performs. The only restriction on the scheduling is that P and V perform their executions of $\mathsf{wAUTH}^\varepsilon$ in the specified order.

This means that at any point in time during the attack when P has executed $\mathsf{wAUTH}^\varepsilon$ for the bits $c_1, \ldots, c_{j-1}$ and V has executed $\mathsf{wAUTH}^\varepsilon$ for the bits $c'_1, \ldots, c'_{j'-1}$ and both are momentarily inactive (at the beginning of the attack: $j = j' = 1$), $\hat{P}$ can perform one of the following three actions. (1) Activate V to run $\mathsf{wAUTH}^\varepsilon$ on $c'_{j'}$ but not activate P; this corresponds to an impersonation attack. (2) Activate V to run $\mathsf{wAUTH}^\varepsilon$ on $c'_{j'}$ and activate P to run $\mathsf{wAUTH}^\varepsilon$ on c_j; this corresponds to a substitution attack if $c_j \neq c'_{j'}$. (3) Activate P to run $\mathsf{wAUTH}^\varepsilon$ on c_j but not activate V; this corresponds to "fast-forwarding" P. We note that $\hat{P}$'s choice on which action to perform may be adaptive and depend on what he has seen so far. However, since V and P execute $\mathsf{wAUTH}^\varepsilon$ for each position within c independently, information gathered from previous executions of $\mathsf{wAUTH}^\varepsilon$ does not improve $\hat{P}$'s success probability to break the next execution.

It is now easy to see that any attack with its (adaptive) choices of (1), (2) or (3) leads to embeddings e and e' of c and c', respectively. Indeed, start with empty strings $e = e' = \emptyset$ and update them as follows. For each of $\hat{P}$'s rounds, update e by $e‡$ and e' by $e'c'_{j'}$ if $\hat{P}$ chooses (1), update e by ec_j and e' by $e'c'_{j'}$ if he chooses (2), and update e by ec_j and e' by $e'‡$ if he chooses (3). In the end, complete e and e' by padding them with sufficiently many ‡s to have them of length $2N$. It is clear that the obtained e and e' are indeed valid embeddings of c and c', respectively.

Theorem 6. *For any $\varepsilon > 0$ and $0 < q < (1 - \varepsilon)/8$, the generic position-based authentication scheme AUTH (Fig. 6) is $2^{-\Omega(\lambda)}$-sound in the No-PE model.*

Proof. Let m and $m' \neq m$ be the messages input by P and the verifiers, respectively, and let c and c' be their encodings. Furthermore, let e and e' be their embeddings, determined (as explained above) by $\hat{P}$'s attack. By the condition on the λ-dominating code C we know that one of the two properties (a) or (b) of Definition 3 holds. If (a) holds, then the number of positions $i \in \{1, \ldots, 2N\}$ for which $e'_i = 1$ and $e_i \in \{-1, 0\}$ is λ. In this case, by construction of the embeddings, in his attack $\hat{P}$ needs to authenticate (using $\mathsf{wAUTH}^\varepsilon$) the bit 1 at least λ times (by means of an impersonation or a substitution attack). By Lemma 2, the success probability of $\hat{P}$ is thus at most δ^λ, which is $2^{-\Omega(\lambda)}$. In the case where property (b) holds, there exists a consecutive sequence of indices I such that the set $J = \{i \in I : e'_i > -1\}$ has size $|J| \geq 4\lambda$ and contains at least λ indices $i \in J$ with $e_i = -1$. For any such index $i \in J$ with $e_i = -1$, $\hat{P}$ needs to authenticate (using $\mathsf{wAUTH}^\varepsilon$) the bit e'_i by means of an impersonation attack, while he may use $\perp$ for (at most) a $8q$-fraction of those i's.

However, by the ε-soundness of PV^ε, if we require $\varepsilon < 1 - 8q$, then the probability of $\hat{P}$ succeeding in this is exponentially small in λ. □

A possible choice for a dominating code for μ-bit messages is the *balanced repetition code* $C^\mu_{\ell\text{-BR}}$, obtained by applying the code $C_{\ell\text{-BR}} = \{00..011..1, 11..100..0\} \subset \{0,1\}^{2\ell}$ bit-wise.

Lemma 3. *For any ℓ and μ, the balanced repetition code $C^\mu_{\ell\text{-BR}}$ is $\ell/4$-dominating.*

Proof. Let $c, c' \in \{0,1\}^{2\ell\mu}$ be two distinct code words from $C^{\mu}_{\ell\text{-BR}}$, and let e and e' be their respective embeddings. Note that c is made up of blocks of 0's and 1's of length ℓ. Correspondingly, e is made up of blocks of 0's and 1's of length ℓ, with ‡'s inserted at various positions. Let $I_1, \ldots, I_{2\mu}$ be the index sets that describe these 0 and 1-blocks of e. In other words, they satisfy: $I_j < I_{j+1}$ element-wise, $|I_j| = \ell$, and $\{e_i : i \in I_j\}$ equals $\{0\}$ or $\{1\}$. Furthermore, the sequence of e_i's with $i \in I_1 \cup \ldots \cup I_{2\mu}$ equals c, and as such, for any odd j, one of I_j and I_{j+1} is a 0-block and one a 1-block. Let $\phi : \{1, \ldots, \mu\} \to \{1, \ldots, 2\mu\}$ be the function such that $I_{\phi(k)}$ is the k-th 1-block in $I_1, \ldots, I_{2\mu}$. The corresponding we can do with c' and e', resulting in blocks $I'_1, \ldots, I'_{2\mu}$ and function ϕ'. For any j, we define $cl(I'_j)$ to be the smallest "interval" in $\{1, \ldots, 4\mu\ell\}$ that contains I'_j.

For 1-blocks I_j and $I'_{j'}$, we say that I_j *overlaps* with $I'_{j'}$ if $|I_j \cap cl(I'_{j'})| \geq 3\ell/4$. We make the following case distinction.

Case 1: $I_{\phi(k')}$ does not overlap with $I'_{\phi'(k')}$ for some k'. If all the indices in $I_{\phi(k')} \setminus cl(I'_{\phi'(k')})$ are larger than those in $cl(I'_{\phi'(k')})$, then $e'_i = 1$ for all $i \in I'_{\phi'(1)} \cup \ldots \cup I'_{\phi'(k')}$ but $e_i < 1$ for at least $\ell/4$ of these i's. A similar argument can be used when all these indices are smaller than those in $cl(I'_{\phi'(k')})$. If neither of the above holds, then $e'_i = 1$ for all $i \in I'_{\phi'(k')}$ but $e_i < 1$ for at least $\ell/4$ of these i's. Hence, property (a) of Definition 3 is satisfied (with parameter $\ell/4$).

Case 2: $I_{\phi(k)}$ overlaps with $I'_{\phi'(k)}$ for every k. Since c and c' are distinct, and by the structure of the code, there must exist two subsequent 1-blocks $I_{\phi(k)}$ and $I_{\phi(k+1)}$ such that the number of 0-blocks between $I_{\phi(k)}$ and $I_{\phi(k+1)}$ is strictly smaller than the number of 0-blocks between the corresponding 1-blocks $I'_{\phi'(k)}$ and $I'_{\phi'(k+1)}$. If there is no 0-block between $I_{\phi(k)}$ and $I_{\phi(k+1)}$ and (at least) one 0-block between $I'_{\phi'(k)}$ and $I'_{\phi'(k+1)}$ then by the assumption on the overlap, at least half of the indices i in the 0-block $I'_{\phi'(k)+1}$ satisfy $e_i = ‡$. If there is one 0-block between $I_{\phi(k)}$ and $I_{\phi(k+1)}$ and two 0-blocks between $I'_{\phi'(k)}$ and $I'_{\phi'(k+1)}$ then at least a quarter of the indices $i \in I'_{\phi'(k)+1} \cup I'_{\phi'(k)+2}$ satisfy $e_i = ‡$. In both (sub)cases, property (b) of Definition 3 is satisfied (with $\lambda = \ell/4$). □

Plugging in the concrete secure positioning scheme from Section 5.2, we obtain a secure realization of position-based authentication scheme in $\mathbb{R}^d$, in the No-PE model.

6.3 Position-Based Key Exchange

The goal of a position-based key exchange scheme is to have the verifiers agree with honest prover P at location *pos* on a key $K \in \{0,1\}^L$, in such a way that no dishonest prover has any (non-negligible amount of) information on K beyond its bit-length L, as long as he is not located at *pos*.[3] Formally, we require the following security properties.

- ε_c-*Completeness:* If P is honest and at the claimed position *pos*, and if there is no (coalition of) dishonest prover(s), then P and $V_0, \ldots, V_k$ output the same key K of positive length, except with probability ε_c.

- ε_s-*Security:* For any position $pos \in \text{Hull}(pos_0, \ldots, pos_k)$ and for any coalition $\hat{P}$ of dishonest provers at locations all different to *pos*, the hybrid state ρ_{KE}, consisting of the key K output by the verifiers and the collective quantum system of $\hat{P}$ at the end of the scheme, satisfies $\delta(\rho_{KE}, \rho_{\tilde{K}E}) \leq \varepsilon_s$, where $\tilde{K}$ is chosen independently and at random of the same bit-length as K.

Note that the security properties only ensure that the *verifiers* can be convinced that $\hat{P}$ has no information on the key they obtain; no such security is guaranteed for P. Indeed, $\hat{P}$ can always honestly execute the scheme with P, acting as verifiers. Also note that the security properties do not provide any guarantee to the verifiers that P has obtained the *same* key in case of an active attack by $\hat{P}$, but this can always be achieved e.g. with the help of a position-based authentication scheme by having P send an authenticated hash of his key.

[3] The length L of the key may depend on the course of the scheme. In particular, an adversary may enforce it to be 0.

A position-based key exchange scheme can easily be obtained by taking any quantum key-distribution (QKD) scheme that requires authenticated communication, and do the authentication by means of a position-based authentication scheme, like the scheme from the previous section. One subtlety to take care of is that QKD schemes usually require *two-way* authentication, whereas position-based authentication only provides authentication from the prover to the verifiers. However, this can easily be resolved as follows. Whenever the QKD scheme instructs V_0 (acting as Alice in the QKD scheme) to send a message m in an authenticated way to P (acting as Bob), V_0 sends m without authentication to P, but then in the next step P authenticates the message m' he has received (supposedly $m' = m$) toward the verifiers, who abort and output an empty key K in case the authentication fails.

Using standard BB84 QKD, we obtain a concrete position-based key exchange scheme. The security of that scheme follows from the security of the BB84 protocol [LC99, BBB$^+$00, SP00, May01, BOHL$^+$05, Ren05] and of the position-based authentication scheme.

7 Conclusion and Open Questions

Continuing a very recent line of research [Mal10a, Mal10b, CFG$^+$10, KMS10, Ken10], we have given a general proof that information-theoretic position-verification quantum schemes are impossible, thereby answering an open question about the security of schemes proposed in [KMS10] to the negative. On the positive side, we have provided schemes secure under the assumption that dishonest provers do not use pre-shared entanglement. Our results naturally lead to the question: How much entanglement is needed in order to break position-verification protocols? Can we show security in the bounded-quantum-storage model [DFSS05] where adversaries are limited to store, say, a linear fraction of the communicated qubits?

Acknowledgments

We thank Charles Bennett, Frédéric Dupuis and Louis Salvail for interesting discussions. HB would like to thank Sandu Popescu for explaining Vaidman's scheme to him.

References

[BB84] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175, 1984.

[BBB$^+$00] Eli Biham, Michel Boyer, P. Oscar Boykin, Tal Mor, and Vwani P. Roychowdhury. A proof of the security of quantum key distribution. In *STOC'00*, pages 715–724, New York, 2000. ACM Press.

[BBC$^+$93] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70(13):1895–1899, Mar 1993.

[BC94] Stefan Brands and David Chaum. Distance-bounding protocols. In *EUROCRYPT'93*, pages 344–359. Springer, 1994.

[BCC$^+$10] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M. Renes, and Renato Renner. The uncertainty principle in the presence of quantum memory. *Nature Physics*, 2010.

[BOHL$^+$05] M. Ben-Or, M. Horodecki, D.W. Leung, D. Mayers, and J. Oppenheim. The universal composable security of quantum key distribution. In *TCC'05*, pages 386–406. Springer, 2005.

[Bus04] Laurent Bussard. *Trust Establishment Protocols for Communicating Devices*. PhD thesis, Eurecom-ENST, 2004.

[CCS06] Srdjan Capkun, Mario Cagalj, and Mani Srivastava. Secure localization with hidden and mobile base stations. In *IEEE INFOCOM*, 2006.

[CFG+10] Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, and Rafail Ostrovsky. Position-based quantum cryptography. arXiv/quant-ph:1005.1750, May 2010.

[CGMO09] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky. Position Based Cryptography. In *CRYPTO'09*, page 407. Springer, 2009. Full version: `http://eprint.iacr.org/2009/364`.

[CH05] Srdjan Capkun and Jean-Pierre Hubaux. Secure positioning of wireless devices with application to sensor networks. In *IEEE INFOCOM*, pages 1917–1928, 2005.

[Che52] H. Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *The Annals of Mathematical Statistics*, pages 493–507, 1952.

[CKOR10] Nishanth Chandran, Bhavana Kanukurthi, Rafail Ostrovsky, and Leonid Reyzin. Privacy amplification with asymptotically optimal entropy loss. In *STOC'10*, pages 785–794, New York, 2010. ACM Press.

[CT91] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley, 1991.

[DFSS05] Ivan Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded quantum-storage model. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 449–458. IEEE, 2005.

[Fan61] Robert Fano. *Transmission of information; a statistical theory of communications*. M.I.T. Press, 1961.

[GLM02] Vittorio Giovannetti, Seth Lloyd, and Lorenzo Maccone. Quantum cryptographic ranging. *Journal of Optics B*, 4(4):042319, Aug 2002.

[Hol73] A. S. Holevo. Information-theoretical aspects of quantum measurement. *Problemy Peredači Informacii*, 9(2):31–42, 1973.

[Ken10] Adrian Kent. Quantum tagging with cryptographically secure tags. arXiv/quant-ph:1008.5380, Aug 2010.

[KMS10] Adrian Kent, Bill Munro, and Tim Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signalling constraints. arXiv/quant-ph:1008.2147, Aug 2010.

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

[KR09] Bhavana Kanukurthi and Leonid Reyzin. Key agreement from close secrets over unsecured channels. In *EUROCRYPT'09*, pages 206–223. Springer, 2009.

[LC99] Hoi-Kwong Lo and H. F. Chau. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science*, 283(5410):2050–2056, 1999.

[Mal10a] Robert A. Malaney. Location-dependent communications using quantum entanglement. *Phys. Rev. A*, 81(4):042319, Apr 2010.

[Mal10b] Robert A. Malaney. Quantum location verification in noisy channels, Apr 2010. arXiv/quant-ph:1004.2689.

[May01] Dominic Mayers. Unconditional security in quantum cryptography. *J. ACM*, 48(3):351–406, 2001.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge university press, 2000.

[RB09] JM Renes and JC Boileau. Conjectured strong complementary information tradeoff. *Phys. Rev. Let.*, 103(2):020402, 2009.

[Ren05] Renato Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zürich (Switzerland), September 2005. `http://arxiv.org/abs/quant-ph/0512258`.

[RW03] Renato Renner and Stefan Wolf. Unconditional authenticity and privacy from an arbitrarily weak secret. In *CRYPTO'03*, pages 78–95. Springer, 2003.

[SP00] Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Let.*, 85(2):441–444, Jul 2000.

[SP05] Dave Singelee and Bart Preneel. Location verification using secure distance bounding protocols. In *IEEE MASS'10*, 2005.

[SSW03] Naveen Sastry, Umesh Shankar, and David Wagner. Secure verification of location claims. In *WiSe'03*, pages 1–10, 2003.

[Vai03] Lev Vaidman. Instantaneous measurement of nonlocal variables. *Phys. Rev. Lett.*, 90(1):010402, Jan 2003.

[VN04] Adnan Vora and Mikhail Nesterenko. Secure location verification using radio broadcast. In *OPODIS'04*, pages 369–383, 2004.

[ZLFW06] Yanchao Zhang, Wei Liu, Yuguang Fang, and Dapeng Wu. Secure localization and authentication in ultra-wideband sensor networks. *IEEE Journal on Selected Areas in Communications*, 24:829–835, 2006.

A Proof of Lemma 1

In this section we prove the following lemma (Lemma 1): *For any tri-partite state ρ_{ABY} with classical Y,*

$$\mathrm{H}(A|BY) = \sum_y P_Y(y)\,\mathrm{H}(\rho^y_{AB}|B).$$

We first consider the case of an "empty" B. Y being classical means that ρ_{AY} is of the form $\rho_{AY} = \sum_y P_Y(y)\rho^y_A \otimes |y\rangle\langle y|$. Let us write $\lambda^y_1, \ldots, \lambda^y_n$ for the eigenvalues of ρ^y_A. Note that the eigenvalues of ρ_{AY} are then given by $P_Y(y)\lambda^y_i$ with $y \in \mathcal{Y}$ and $i \in \{1, \ldots, n\}$. It follows that

$$\begin{aligned}\mathrm{H}(\rho_{AY}|Y) &= \mathrm{H}(\rho_{AY}) - \mathrm{H}(\rho_Y) = -\mathrm{tr}\big(\rho_{AY}\log(\rho_{AY})\big) + \mathrm{tr}\big(\rho_Y\log(\rho_Y)\big)\\ &= -\Big(\sum_{y,i} P_Y(y)\lambda^y_i \log\big(P_Y(y)\lambda^y_i\big) - \sum_y P_Y(y)\log\big(P_Y(y)\big)\Big)\\ &= -\sum_y P_Y(y)\sum_i \lambda^y_i\log(\lambda^y_i) = \sum_y P_Y(y)\,\mathrm{H}(\rho^y_A)\,.\end{aligned}$$

In general, we can no conclude that

$$\begin{aligned}\mathrm{H}(\rho_{ABY}|BY) &= \mathrm{H}(\rho_{ABY}) - \mathrm{H}(\rho_{BY}) = \sum_y P_Y(y)\,\mathrm{H}(\rho^y_{AB}) - \sum_y P_Y(y)\,\mathrm{H}(\rho^y_B)\\ &= \sum_y P_Y(y)\big(\mathrm{H}(\rho^y_{AB}) - \mathrm{H}(\rho^y_B)\big) = \sum_y P_Y(y)\,\mathrm{H}(\rho^y_{AB}|B)\,,\end{aligned}$$

which proves the claim.