UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

Position-based quantum cryptography: impossibility and constructions

Buhrman, H.; Chandran, N.; Fehr, S.; Gelles, R.; Goyal, V.; Ostrovsky, R.; Schaffner, C.

DOI
10.1007/978-3-642-22792-9_24

Publication date
2011

Document Version
Final published version

Published in
Advances in Cryptology – CRYPTO 2011

Link to publication

Citation for published version (APA):
Buhrman, H., Chandran, N., Fehr, S., Gelles, R., Goyal, V., Ostrovsky, R., & Schaffner, C. (2011). Position-based quantum cryptography: impossibility and constructions. In P. Rogaway (Ed.), *Advances in Cryptology – CRYPTO 2011: 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011: proceedings* (pp. 429-446). (Lecture Notes in Computer Science; Vol. 6841). Springer. https://doi.org/10.1007/978-3-642-22792-9_24

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

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

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

Download date:25 Jan 2022

Position-Based Quantum Cryptography: Impossibility and Constructions

Harry Buhrman[1,2,⋆], Nishanth Chandran[3,⋆⋆], Serge Fehr[1], Ran Gelles[3,⋆⋆], Vipul Goyal[4], Rafail Ostrovsky[3,⋆⋆⋆], and Christian Schaffner[2,1,†]

[1] Centrum Wiskunde & Informatica (CWI), The Netherlands
[2] University of Amsterdam, The Netherlands
[3] University of California (UCLA), CA, USA
[4] Microsoft Research, Bangalore, India

Abstract. The aim of position-based cryptography is to use the geographical position of a party as its only credential. In this work, we study position-based cryptography in the quantum setting.

We show that if collaborating adversaries are allowed to pre-share an arbitrarily large entangled quantum state, then position-verification, and as a consequence position-based cryptography in general, is *impossible* (also) in the quantum setting.

To this end, we prove that with the help of sufficient pre-shared entanglement, any non-local quantum computation, i.e., any computation that involves quantum inputs from two parties at different locations, can be performed *instantaneously* and *without any communication*, up to local corrections that need to be applied to the outputs. The latter can be understood in that the parties obtain their respective outputs "encrypted", where each corresponding encryption key is known by the opposite party. This result generalizes to any number of parties, and it implies that any non-local quantum computation can be performed using a *single* round of mutual communication (in which the parties exchange the encryption keys), and that any position-verification scheme can be broken, assuming sufficient pre-shared entanglement among the adversaries.

On the positive side, we show that for adversaries that are restricted to not share any entangled quantum states, 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.

⋆ Supported by a NWO VICI grant and the EU 7th framework grant QCS.
⋆⋆ Supported in part by NSF grants 0716835, 0716389, 0830803, and 0916574.
⋆⋆⋆ Supported in part by IBM Faculty Award, Xerox Innovation Group Award, the Okawa Foundation Award, Intel, Teradata, DARPA, BSF grant 2008411, NSF grants 0716835, 0716389, 0830803, 0916574 and U.C. MICRO grant.
† Supported by a NWO VENI grant.

P. Rogaway (Ed.): CRYPTO 2011, LNCS 6841, pp. 429–446, 2011.
© International Association for Cryptologic Research 2011

1 Introduction

1.1 Background

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*. The general concept of position-based cryptography was introduced by Chandran, Goyal, Moriarty and Ostrovsky [1]; certain specific related tasks have been considered before under different names (see below and Sect. 1.3).

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 P is indeed at that position *pos*. The prover can run an interactive protocol with the verifiers in order to convince them. The main technique for such a protocol is known as distance bounding [2]. 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 the speed of 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 ([2,3,4,5,6,7,8,9]). However, [1] 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 which is at position *pos*. Their impossibility result holds even if one makes computational hardness assumptions, and it also rules out most other interesting position-based cryptographic tasks.

In light of the strong impossibility result, [1] considers a setting that assumes restrictions on the parties' storage capabilities, called the Bounded-Retrieval Model (BRM) in the full version of [1], and constructs secure protocols for position-verification and for 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 underlying setting is relatively hard to justify in practice.

This leaves us with the 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 [1] 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 [1] in the BRM circumvents the impossibility result by assuming

that an adversary *cannot* store all information he receives. By considering 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 [10]. Although teleportation on its own does not appear to immediate conflict with the above intuition, we show that, based on techniques by Vaidman [11], adversaries holding a large amount of entangled quantum states can perform *instantaneous nonlocal quantum computation*, which in particular implies that they can compute any unitary operation on a state shared between them, using only local operations and *one* round of classical mutual communication. Based on this technique, we show how a coalition of adversaries can attack and break any position-verification scheme.

Interestingly, sharing entangled quantum systems is vital for attacking the position-verification scheme. We show that there exist schemes that are secure in the information-theoretic sense, if the adversary is not allowed to pre-share or maintain entanglement. Furthermore, 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

To the best of our knowledge, quantum schemes for position-verification 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 [12]. Their results have not appeared in the academic literature until 2010 [13]. 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 [13]) not suspect to their teleportation attack and leave their security as an open question. 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 [14,15]. However, the proposed scheme is merely claimed secure, and no rigorous security analysis is provided. As pointed out in [13], Malaney's schemes can also be broken by a teleportation-based attack. Chandran et al. have proposed and proved a secure

quantum scheme for position-verification [16]. However, their proof implicitly assumed that the adversaries have no pre-shared entanglement; as shown in [13], their scheme also becomes insecure without this assumption.

In a subsequent paper [17], Lau and Lo use similar ideas as in [13] to show the insecurity of position-verification schemes that are of a certain (yet rather restricted) form, which include the schemes from [14,15] and [16]. Furthermore, they propose a position-verification scheme that resists their attack, and they conjecture it secure. While these protocols might be secure if the adversaries do not pre-share entanglement, our attack shows that all of them are insecure in general.

In a recent note [18], Kent considers a different model for position-based cryptography where the prover's position is *not* his only credential, but he is assumed to additionally 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.

The idea of performing "instantaneous measurements of nonlocal variables" has been put forward by Vaidman [11] and was further investigated by Clark et al. [19]. The concept of instantaneous nonlocal quantum computation presented here is an extension of Vaidman's task. After the appearance and circulation of our work, Beigi and König [20] used the technique of port-based teleportation by Ishizaka and Hiroshima [21,22] to reduce the amount of entanglement required to perform instantaneous nonlocal quantum computation (from our double exponential) to exponential.

In [23], 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 basis θ to obtain x, and immediately send x to both 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 she 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 excluded by the no-cloning principle.

The Attack and Instantaneous Nonlocal Quantum Computation. 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. Combining this with the observation by Kent et al. [13] that the Pauli-corrections resulting from the teleportation commute with the actions of the honest prover in the above protocol shows that colluding adversaries can perfectly break the protocol.

Much more generally, we will show how to break *any* position-verification scheme, possibly consisting of multiple (and interleaved) rounds. To this end, we will show how to perform *instantaneous nonlocal quantum computation*. In particular, we prove that any unitary operation U acting on a composite system shared between players can be computed using only a single round of mutual classical communication. Based on ideas by Vaidman [11], the players teleport quantum 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-PE Model. On the other hand, the above intuition is correct in the *no pre-shared entanglement* (No-PE) model, where the adversaries are not allowed to have pre-shared entangled quantum states prior the execution the protocol, or, more generally, prior the execution of each round of the protocol in case of multi-round schemes. Even though this model may be somewhat unrealistic and artificial, analyzing protocols in this setting serves as stepping stone to obtaining protocols which tolerate adversaries who pre-share and maintain some *limited* amount of entanglement. But also, rigorously proving security in the restrictive (for the adversary) No-PE model is already non-trivial and requires heavy machinery. Our proof uses the *strong complementary information trade-off* (CIT) due to Renes and Boileau [24], 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 get a secure multi-round positioning scheme with exponentially small soundness error. We note that when performing sequential repetitions in the No-PE model, the adversaries must enter each round with no entanglement; thus, they are not allowed to generate entanglement in one round, store it, and use it in the next round(s).

Position-based authentication and key-exchange in the No-PE Model. Based on (sequential repetitions of) our position-verification scheme in the No-PE model, we can also construct schemes for position-based authentication and for position-based key-exchange, and prove their security in the No-PE model. Due to space limitation, these schemes and their analyses only appear in the full version of this paper [25].

2 Preliminaries

2.1 Notation and Terminology

We assume familiarity with the basic concepts of quantum information theory and refer to [26] for an excellent introduction; we merely fix some notation here.

Qubits. A *qubit* is a quantum system A with a 2-dimensional 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 the 2^n-dimensional space $\mathcal{H}_A = (\mathbb{C}^2)^{\otimes n} = \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$.

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 of a 2-qubit state is the *EPR pair*, which is given by $|\Phi_{AB}\rangle = (|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2} \in \mathcal{H}_A \otimes \mathcal{H}_B = \mathbb{C}^2 \otimes \mathbb{C}^2$ and 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 $H|x\rangle$.

Teleportation. The goal of teleportation is to transfer a quantum state from one location to another by only communicating classical information. Teleportation requires pre-shared entanglement among the two locations. To teleport a qubit Q in an arbitrary 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 $k \in \{0,1,2,3\}$. Instantaneously, the other half of the corresponding EPR pair, which is held by Bob, turns into the state $\sigma_k^\dagger|\psi\rangle$, where $\sigma_0, \sigma_1, \sigma_2, \sigma_3$ denote the four Pauli-corrections $\{\mathbb{I}, X, Z, XZ\}$, respectively, and $\sigma^\dagger$ denotes the complex conjugate of the transpose of σ. The classical information k is then communicated to Bob who can recover the state $|\psi\rangle$ by performing σ_k on his EPR half. Note that the operator σ_k is Hermitian, thus $\sigma_k^\dagger = \sigma_k$.

3 Setup and the Task of Position Verification

3.1 The Security Model

We informally describe the model we use for the upcoming sections, which is a quantum version of the Vanilla (standard) model introduced in [1] (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, which prohibits entanglement between the dishonest verifiers. Specifically, the *No-PE model* is such that the dishonest provers enter every new round of communication, initiated by the verifiers, with no pre-shared entanglement. That is, in every round, a dishonest prover can send an entangled quantum state only *after* it receives the verifier's message, and the dishonest provers cannot maintain such an entangled state in order to use it in the next round. As mentioned in the introduction, considering this simple (but possibly unrealistic) model may help us in obtaining protocols that are secure against adversaries with *limited* entanglement.

For simplicity, we assume that quantum operations and communication are 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 authenticated 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 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 reason as follows. Consider a verifier V_0 at position pos_0, 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 $d(pos_0, pos)$.

We stress that in our model, the honest prover P has no advantage over the dishonest provers beyond being at its position *pos*. In particular, P does not share any secret information with the verifiers, nor can he per-se authenticate his messages by any other means.

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, $\text{Hull}(pos_0, \ldots, pos_k) \subset \mathbb{R}^d$ 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 $V_0, \ldots, V_k$, who 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 [1] for the general formal definition of the completeness and security of a position-verification scheme. In this article, we mainly focus on position-verification schemes of the following form:

Definition 1. *A 1-round* ***position-verification*** *scheme* $\mathsf{PV} = (\mathsf{Chlg}, \mathsf{Resp}, \mathsf{Ver})$ *consists of the following three parts. 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* $\mathsf{Ver}(x'_0, \ldots, x'_k, x) \in \{0, 1\}$.

PV *is said to have* **perfect completeness** *if* $\mathsf{Ver}(x'_0, \ldots, x'_k, x) = 1$ *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.

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, $x'_0 = \ldots = x'_k$, and $\mathsf{Ver}(x'_0, \ldots, x'_k, x) = 1$ 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* $pos \in \text{Hull}(pos_0, \ldots, pos_k)$*, and any coalition*

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

0. V_0 generates a list of challenges $(ch_0, \ldots, ch_k)$ and auxiliary information 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 $\mathsf{Ver}(x'_0, \ldots, x'_k, x) = 1$.

Fig. 1. Generic 1-round position-verification scheme

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.

4 Instantaneous Nonlocal Quantum Computation

In order to analyze the (in)security of position-verification schemes, we first address a more general task, which is interesting in its own right: *instantaneous nonlocal quantum computation*[1]. Consider the following problem, involving two parties Alice and Bob. Alice holds A and Bob holds B of a tripartite system ABE that is in some unknown state $|\psi\rangle$. The goal is to apply a known unitary transformation U to AB, but *without* using any communication, just by local operations. In general, such a task is clearly impossible, as it violates the non-signalling principle. The goal of instantaneous nonlocal quantum computation is to achieve almost the above but without violating non-signalling. Specifically, the goal is for Alice and Bob to compute, without communication, a state $|\varphi'\rangle$ that coincides with $|\varphi\rangle = (U \otimes \mathbb{I})|\psi\rangle$ up to *local* and *qubit-wise* operations on A and B, where $\mathbb{I}$ denotes the identity on E. Furthermore, these local and qubit-wise operations are determined by *classical* information that Alice and Bob obtain as part of their actions. In particular, if Alice and Bob share their classical information, which can be done with *one* round of simultaneous mutual communication,

[1] This is an extension of the task of "instantaneous measurement of nonlocal variables" introduced by Vaidman [11].

then they can transform $|\varphi'\rangle$ into $|\varphi\rangle = U|\psi\rangle$ by local qubit-wise operations. Following ideas by Vaidman [11], we show below that instantaneous nonlocal quantum computation, as described above, is possible if Alice and Bob share sufficiently many EPR pairs.

In the following, let $\mathcal{H}_A$, $\mathcal{H}_B$ and $\mathcal{H}_E$ be Hilbert spaces where the former two consist of n_A and n_B qubits respectively, i.e., $\mathcal{H}_A = (\mathbb{C}^2)^{\otimes n_A}$ and $\mathcal{H}_B = (\mathbb{C}^2)^{\otimes n_B}$. Furthermore, let U be a unitary matrix acting on $\mathcal{H}_A \otimes \mathcal{H}_B$. Alice holds system A and Bob holds system B of an arbitrary and unknown state $|\psi\rangle \in \mathcal{H}_{ABE} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$. Additionally, Alice and Bob share an arbitrary but finite number of EPR pairs.

Theorem 1. *For every unitary U and for every $\varepsilon > 0$, given sufficiently many shared EPR pairs, there exist local operations $\mathcal{A}$ and $\mathcal{B}$, acting on Alice's and Bob's respective sides, with the following property. For any initial state $|\psi\rangle \in \mathcal{H}_{ABE}$, the joint execution $\mathcal{A} \otimes \mathcal{B}$ transforms $|\psi\rangle$ into $|\varphi'\rangle$ and provides classical outputs k to Alice and ℓ to Bob, such that the following holds except with probability ε. The state $|\varphi'\rangle$ coincides with $|\varphi\rangle = (U \otimes \mathbb{I})|\psi\rangle$ up to local qubit-wise operations on A and B that are determined by k and ℓ.*

We stress that $\mathcal{A}$ acts on A as well as on Alice's shares of the EPR pairs, and the corresponding holds for $\mathcal{B}$. Furthermore, being equal up to local qubit-wise operations on A and B means that $|\varphi\rangle = (V^A_{k,\ell} \otimes V^B_{k,\ell} \otimes \mathbb{I})|\varphi'\rangle$, where $\{V^A_{k,\ell}\}_{k,\ell}$ and $\{V^B_{k,\ell}\}_{k,\ell}$ are fixed families of unitaries which act qubit-wise on $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. In our construction, the $V^A_{k,\ell}$ and $V^B_{k,\ell}$'s will actually be tensor products of one-qubit Pauli operators.

As an immediate consequence of Theorem 1, we get the following.

Corollary 1. *For every unitary U and for every $\varepsilon > 0$, given sufficiently many shared EPR pairs, there exists a nonlocal operation $\mathcal{AB}$ for Alice and Bob which consists of local operations and* one *round of mutual communication, such that for any initial state $|\psi\rangle \in \mathcal{H}_{ABE}$ of the tripartite system ABE, the joint execution of $\mathcal{AB}$ transforms $|\psi\rangle$ into $|\varphi\rangle = (U \otimes \mathbb{I})|\psi\rangle$, except with probability ε.*

For technical reasons, we will actually prove the following extension of Theorem 1, which is easily seen equivalent. The difference to Theorem 1 is that Alice and Bob are additionally given classical inputs: x to Alice and y to Bob, and the unitary U that is to be applied to the quantum input depends on x and y. In the statement below, x ranges over some arbitrary but fixed finite set $\mathcal{X}$, and y ranges over some arbitrary but fixed finite set $\mathcal{Y}$.

Theorem 2. *For every family $\{U_{x,y}\}$ of unitaries and for every $\varepsilon > 0$, given sufficiently many shared EPR pairs, there exist families $\{\mathcal{A}_x\}$ and $\{\mathcal{B}_y\}$ of local operations, acting on Alice's and Bob's respective sides, with the following property. For any initial state $|\psi\rangle \in \mathcal{H}_{ABE}$ and for every $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, the joint execution $\mathcal{A}_x \otimes \mathcal{B}_y$ transforms the state $|\psi\rangle$ into $|\varphi'\rangle$ and provides classical outputs k to Alice and ℓ to Bob, such that the following holds except with probability ε. The state $|\varphi'\rangle$ coincides with $|\varphi\rangle = (U_{x,y} \otimes \mathbb{I})|\psi\rangle$ up to local qubit-wise operations on A and B that are determined by k and ℓ.*

The solution works by teleporting states back and forth in a clever way [11], but *without* communicating the classical outcomes of the Bell measurements, so that only local operations are performed. Thus, in the formal proof below, whenever we say that a state is teleported, this should be understood in this sense, i.e., the sender makes a Bell measurement resulting in some classical information, and the receiver takes his shares of the EPR pairs as the received state, but does/can not (yet) correct it.

Proof. To simplify notation, we assume that the joint state of A and B is pure, and thus we may ignore system E. However, all our arguments also hold in case the state of A and B is entangled with E.

Next, we observe that it is sufficient to prove Theorem 2 for the case where B is "empty", i.e., $\dim \mathcal{H}_B = 1$ and thus $n_B = 0$. Indeed, if this is not the case, then Alice and Bob can do the following. Bob first teleports B to Alice. Now, Alice holds $A' = AB$ with $n_{A'} = n_A + n_B$, and Bob's system has collapsed and thus Bob holds no quantum state anymore, only classical information. Then, they do the nonlocal computation, and in the end Alice teleports B back to Bob. The modification to the state of B introduced by teleporting it to Alice can be taken care of by modifying the set of unitaries $\{U_{x,y}\}$ accordingly (and making it dependent on Bob's measurement outcome, thereby extending the set $\mathcal{Y}$). Also, the modification to the state of B introduced by teleporting it back to Bob does not harm the requirement of the joint state being equal to $|\varphi\rangle = U_{x,y}|\psi\rangle$ up to local qubit-wise operations.

Hence, from now on, we may assume that B is "empty", and we write n for n_A. Next, we describe the core of how the local operations $\mathcal{A}_x$ and $\mathcal{B}_y$ work. To simplify notation, we assume that $\mathcal{X} = \{1, \ldots, m\}$. Recall that Alice and Bob share (many) EPR pairs. We may assume that the EPR pairs are grouped into groups of size n; each such group we call a *teleportation channel*. Furthermore, we may assume that m of these teleportation channels are labeled by the numbers 1 up to m, and that another m of these teleportation channels are labeled by the numbers $m + 1$ up to $2m$.

1. Alice teleports $|\psi\rangle$ to Bob, using the teleportation channel that is labeled by her input x. Let us denote her measurement outcome by $k_\circ \in \{0, 1, 2, 3\}^n$.
2. For every $i \in \{1, \ldots, m\}$, Bob does the following. He applies the unitary $U_{i,y}$ to the n qubits that make up his share of the EPR pairs given by the teleportation channel labeled by i. Then, he teleports the resulting state to Alice using the teleportation channel labeled by $m + i$. We denote the corresponding measurement outcome by $\ell_{\circ,i}$.
3. Alice specifies the n qubits that make up her share of the EPR pairs given by the teleportation channel labeled by $m + x$ to be the state $|\varphi'\rangle$.

Let us analyze the above. With probability $1/4^n$, namely if $k_\circ = 0 \cdots 0$, teleporting $|\psi\rangle$ to Bob leaves the state unchanged. In this case, it is easy to see that the resulting state $|\varphi'\rangle$ satisfies the required property of being identical to $|\varphi\rangle = U_{x,y}|\psi\rangle$ up to local qubit-wise operations determined by $\ell_{\circ,x}$, and thus

determined by x and $\ell_\circ = (\ell_{\circ,1}, \ldots, \ell_{\circ,m})$. This proves the claim for the case where $\varepsilon \geq 1 - 1/4^n$.

We now show how to reduce ε. The crucial observation is that if in the above procedure $k_\circ \neq 0 \cdots 0$, and thus $|\varphi'\rangle$ is not necessarily identical to $|\varphi\rangle$ up to local qubit-wise operations, then

$$|\varphi'\rangle = V_{\ell_{\circ,x}} U_{x,y} V_{k_\circ} |\psi\rangle = V_{\ell_{\circ,x}} U_{x,y} V_{k_\circ} U_{x,y}^\dagger |\varphi\rangle \,,$$

where $V_{\ell_{\circ,x}}$ and $V_{k_\circ}$ are tensor products of Pauli matrices. Thus, setting $|\psi'\rangle := |\varphi'\rangle$, $x' := (x, k_\circ)$ and $y' := (y, \ell_\circ)$, and $U'_{x',y'} := U_{x,y} V_{k_\circ} U_{x,y}^\dagger V_{\ell_{\circ,x}}$, the state $|\varphi\rangle$ can be written as $|\varphi\rangle = U'_{x',y'} |\psi'\rangle$. This means, we are back to the original problem of applying a unitary, $U'_{x',y'}$, to a state, $|\psi'\rangle$, held by Alice, where the unitary depends on classical information x' and y', known by Alice and Bob, respectively. Thus, we can re-apply the above procedure to the new problem instance. Note that in the new problem instance, the classical inputs x' and y' come from larger sets than the original inputs x and y, but the new quantum input, $|\psi'\rangle$, has the same qubit size, n. Therefore, re-applying the procedure will succeed with the same probability $1/4^n$.

As there is a constant probability of success in each round, re-applying the above procedure sufficiently many times to the resulting new problem instances guarantees that except with arbitrary small probability, the state $|\varphi'\rangle$ will be of the required form at some point (when Alice gets $k_\circ = 0 \cdots 0$). Say, this is the case at the end of the j-th iteration. Then, Alice stops with her part of the procedure at this point, keeps the state $|\varphi'\rangle$, and specifies k to consist of j and of her classical input into the j-th iteration (which consists of x and of the $k_\circ$'s from the prior $j-1$ iterations). Since Bob does not learn whether an iteration is successful or not, he has to keep on re-iterating up to some bound, and in the end he specifies ℓ to consist of the $\ell_\circ$'s collected over all the iterations. The state $|\varphi'\rangle$ then equals $|\varphi\rangle = U_{x,y}|\psi\rangle$ up to local qubit-wise operations that are determined by k and ℓ. □

Doing the maths shows that the number of EPR pairs needed by Alice and Bob in the scheme described in the proof is double exponential in $n_A + n_B$, the qubit size of the joint quantum system.

In recent subsequent work [20], Beigi and König have used a different kind of quantum teleportation by Ishizaka and Hiroshima [21,22] to reduce the amount of entanglement needed to to perform instantaneous nonlocal quantum computation to exponential in the qubit size of the joint quantum system. It remains an interesting open question whether such an exponentially large amount of entanglement is necessary.

5 Impossibility of Unconditional Position Verification

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 position-verification scheme in our model (as specified in Sect. 3.1). We recall that in this model, the verifiers must base their

decision solely on *what* the prover replies and *how long* it takes him to reply, and the honest prover has no advantage over a coalition of dishonest provers beyond being at the claimed position[2]. Such a position-verification scheme may be of the form as specified in Fig. 1, but may also be made up of several, possibly interleaved, rounds of interaction between the prover and the verifiers.

For the honest prover P, such a general scheme consists of steps that look as follows. P holds a local quantum register R, which is set to some default value at the beginning of the scheme. In each step, P obtains a system A from V_0 and a system B from V_1, and V_0 and V_1 jointly keep some system E. Let $|\psi\rangle$ be the state of the four-partite system $ABRE$; it is determined by the scheme and by the step within the scheme we are focussing on. P then has to apply a fixed[3] known unitary transformation U to ABR, and send the (transformed) systems A and B back to V_0 and V_1 (and keep R). Note that after the transformation, the state of $ABRE$ is given by $|\varphi\rangle = (U \otimes \mathbb{I})|\psi\rangle$, where $\mathbb{I}$ is the identity acting on $\mathcal{H}_E$. For technical reasons, as in Sect. 4, it will be convenient to distinguish between classical and quantum inputs, and therefore, we let the unitary U depend on classical information x and y, where x has been sent by V_0 along with A, and y has been sent by V_1 along with B.

We now show that a coalition of two dishonest provers $\hat{P}_0$ and $\hat{P}_1$, where $\hat{P}_0$ is located in between V_0 and P and $\hat{P}_1$ is located in between V_1 and P, can perfectly simulate the actions of the honest prover P, and therefore it is impossible for the verifiers to distinguish between an honest prover at position *pos* and a coalition of dishonest provers at positions different from *pos*. The simulation of the dishonest provers perfectly imitates the *computation* as well as the *timing* of an honest P. Since in our model this information is what the verifiers have to base their decision on, the general impossibility of position-verification in our model follows.

Consider a step in the scheme as described above, but now from the point of view of $\hat{P}_0$ and $\hat{P}_1$. Since $\hat{P}_0$ is closer to V_0, he will first receive A and x; similarly, $\hat{P}_1$ will first receive B and y. We specify that $\hat{P}_1$ takes care of and maintains the local register R. If the step we consider here is the *first* step in the scheme, then the state of $ABRE$ equals $|\psi\rangle$, as in the case of an honest P. In order to have an invariant that holds for all the steps, we actually relax this statement and merely observe that the state of $ABRE$, say $|\psi'\rangle$, equals $|\psi\rangle$ up to local and qubit-wise operations on the subsystem R, determined by classical information $x_\circ$ and $y_\circ$, where $\hat{P}_0$ holds $x_\circ$ and $\hat{P}_1$ holds $y_\circ$. This invariant clearly holds for the first step in the scheme, when R is in some default state, and we will show that it also holds for the other steps.

By Theorem 2, it follows that without communication, just by instantaneous local operations, $\hat{P}_0$ and $\hat{P}_1$ can transform the state $|\psi'\rangle$ into a state $|\varphi'\rangle$ that coincides with $|\varphi\rangle = (U_{x,y} \otimes \mathbb{I})|\psi\rangle$ up to local and qubit-wise transformations on

[2] In particular, the prover does not share any secret information with the verifiers, differentiating our setting from models as described for example in [18].

[3] U is fixed for a fixed scheme and for a fixed step within the scheme, but of course may vary for different schemes and for different steps within a scheme.

A, B and R, determined by classical information k (known to $\hat{P}_0$) and ℓ (known to $\hat{P}_1$). Note that the initial state is not $|\psi\rangle$, but rather a state of the form $|\psi'\rangle = (V_{x_\circ,y_\circ} \otimes \mathbb{I})|\psi\rangle$, where $x_\circ$ is known to $\hat{P}_0$ and $y_\circ$ to $\hat{P}_1$. Thus, Theorem 2 is actually applied to the unitary $U'_{x',y'} = U_{x,y}V^\dagger_{x_\circ,y_\circ}$, where $x' = (x_\circ, x)$ and $y' = (y_\circ, y)$. Given $|\varphi'\rangle$ and k and ℓ, $\hat{P}_0$ and $\hat{P}_1$ can now exchange k and ℓ using *one* mutual round of communication and transform $|\varphi'\rangle$ into $|\varphi''\rangle$ that coincides with $|\varphi\rangle$ up to qubit-wise operations only on R, and send A to V_0 and B to V_1. It follows that the state of ABE and the time it took $\hat{P}_0$ and $\hat{P}_1$ for the computation and communication is identical to that of an honest P, i.e., $\hat{P}_0$ and $\hat{P}_1$ have perfectly simulated this step of the scheme.

Finally, we see that the invariant is satisfied, when moving on to the next step in the scheme, where $\hat{P}_0$ and $\hat{P}_1$ receive new A and B (along with new classical x and y) from V_0 and V_1, respectively. Even if this new round interleaves with the previous round in that the new A and B etc. arrive *before* $\hat{P}_0$ and $\hat{P}_1$ have finished exchanging (the old) k and ℓ, it still holds that the state of $ABRE$ is as in the case of honest P up to qubit-wise operations on the subsystem R. This implies that the above procedure works for all the steps and thus that $\hat{P}_0$ and $\hat{P}_1$ can indeed perfectly simulate honest P's actions throughout the whole scheme.

6 Secure Position-Verification in the No-PE Model

In this section 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. 2. It is based on the BB84 encoding.

We implicitly specify that parties abort if they receive any message that is inconsistent with the protocol, for instance (classical) messages with a wrong length, or different number of received qubits than expected, etc.

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

The function $\mathrm{h} : [0,1] \to [0,1]$ 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 $0 \le p \le \frac{1}{2}$. A numerical calculation shows that $\mathrm{h}^{-1}(\frac{1}{2}) \ge 0.11$ and thus $\varepsilon \le 0.89$. A particular attack for a dishonest prover $\hat{P}$, sitting in-between V_0 and P, is to measure

0. V_0 chooses two random bits $x, \theta \in \{0,1\}$ and privately sends them 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 $x' = x$.

Fig. 2. Position-verification scheme $\mathsf{PV}^{\varepsilon}_{\mathrm{BB84}}$ based on the BB84 encoding

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. The proof uses several concepts of quantum information theory which are explained in more detail in the full version of this paper [25]. A key idea in this proof is the use of the *complementary information trade-off* (CIT) [24] (see also [27] for a generalization). In a form useful for us, CIT states that for any tri-partite state $|\psi_{AEF}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_E \otimes \mathcal{H}_F$ with $\mathcal{H}_A = (\mathbb{C}^2)^{\otimes n}$, the following holds. If Θ is uniformly distributed in $\{0,1\}^n$ and X is the result of measuring A in basis Θ, then $\mathrm{H}(X|\Theta E) + \mathrm{H}(X|\Theta F) \geq n$, where H is the (conditional) von Neumann entropy.

In order to analyze the position-verification scheme it is convenient to consider an equivalent *purified* version, given in Fig. 3. The only difference between the original and the purified scheme is the preparation of the bit $H^\theta|x\rangle$. In the purified version, it is done by preparing $|\Phi_{AB}\rangle = (|0\rangle|0\rangle + |1\rangle|1\rangle)/\sqrt{2}$ and measuring A in basis θ. This changes the point in time when V_0 measures A, and the point in time when V_1 learns x. This, however, has no influence on the view of the (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.

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 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 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 $x' = x$.

Fig. 3. EPR version of $\mathsf{PV}^{\varepsilon}_{\mathrm{BB84}}$

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. It is important to realize that the state $|\psi_{A\,E_0E_1}\rangle$ is independent of θ. This is because $\hat{P}_0$ has to apply the quantum operation to B *before* learning θ.[4] 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 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 well-known Holevo bound, 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, 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. See full details in [25].

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. □

The soundness error can be further reduced by sequentially repeating the scheme, assuming that the adversaries do not share entanglement at the beginning of each round. Also, 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 $V_1, V_2, \ldots, V_d$.

7 Other Position-based Cryptographic Tasks

In the full version of this paper [25], we show the following additional results. Using a generic position-verification scheme, we construct a position-based *authentication* scheme, which ensures that a communicated message m originates from an entity P that is at some specific location. In combination with an off-the-shelf quantum-key-distribution (QKD) scheme, this results in a position-based

[4] We stress that this independency breaks down if $\hat{P}_0$ and $\hat{P}_1$ may start off with an entangled state, because then $\hat{P}_1$ can act on his part of the entangled state in a θ-dependent way, which makes the overall state dependent of θ.

key-distribution scheme, which enables the verifiers to exchange a cryptographic key K with the prover, with the guarantee that only the honest prover at location *pos* obtains K, but any adversary (or coalition of adversaries) not at location *pos* learns no information on K. Using our position-verification scheme in the No-PE model as underlying scheme, we obtain secure position-based *authentication* and position-based *key-distribution* schemes in the No-PE model.

8 Conclusion and Open Questions

We have proven a general impossibility result for position-based quantum cryptography, thereby showing the insecurity of several recently proposed schemes [13,14,15,16,17]. Our no-go result has already sparked subsequent work [20] about the *amount* of entanglement needed to break general position-verification schemes.

On the positive side, we have shown the existence of secure position-based quantum cryptographic schemes under the (strong) assumption that adversaries do not share any entanglement (prior to each round). An interesting open question is the existence of secure schemes under more relaxed and realistic assumptions, like in the bounded-quantum-storage model [28], where adversaries are limited in the number of qubits they can store reliably?

Acknowledgements. We thank Charles Bennett, Frédéric Dupuis and Louis Salvail for interesting discussions. HB would like to thank Sandu Popescu for explaining Vaidman's scheme and pointing [19] out to him.

References

1. Chandran, N., Goyal, V., Moriarty, R., Ostrovsky, R.: Position based cryptography. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 391–407. Springer, Heidelberg (2009)
2. Brands, S., Chaum, D.: Distance-bounding protocols. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 344–359. Springer, Heidelberg (1994)
3. Sastry, N., Shankar, U., Wagner, D.: Secure verification of location claims. In: WiSe 2003, pp. 1–10 (2003)
4. Vora, A., Nesterenko, M.: Secure location verification using radio broadcast. In: Higashino, T. (ed.) OPODIS 2004. LNCS, vol. 3544, pp. 369–383. Springer, Heidelberg (2005)
5. Bussard, L.: Trust Establishment Protocols for Communicating Devices. PhD thesis, Eurecom-ENST (2004)
6. Capkun, S., Hubaux, J.P.: Secure positioning of wireless devices with application to sensor networks. In: IEEE INFOCOM, 1917–1928 (2005)
7. Singelee, D., Preneel, B.: Location verification using secure distance bounding protocols. In: IEEE MASS'10 (2005)
8. Zhang, Y., Liu, W., Fang, Y., Wu, D.: Secure localization and authentication in ultra-wideband sensor networks. IEEE Journal on Selected Areas in Communications 24, 829–835 (2006)

9. Capkun, S., Cagalj, M., Srivastava, M.: Secure localization with hidden and mobile base stations. In: IEEE INFOCOM (2006)
10. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. Phys. Rev. Lett. 70(13), 1895–1899 (1993)
11. Vaidman, L.: Instantaneous measurement of nonlocal variables. Phys. Rev. Lett. 90(1), 010402 (2003)
12. Kent, A., Munro, W., Spiller, T., Beausoleil, R.: Tagging systems, US patent nr 2006/0022832 (2006)
13. Kent, A., Munro, B., Spiller, T.: Quantum tagging: Authenticating location via quantum information and relativistic signalling constraints, arXiv/quant-ph:1008.2147 (2010)
14. Malaney, R.A.: Location-dependent communications using quantum entanglement. Phys. Rev. A 81(4), 042319 (2010)
15. Malaney, R.A.: Quantum location verification in noisy channels, arXiv/quant-ph:1004.2689 (2010)
16. Chandran, N., Fehr, S., Gelles, R., Goyal, V., Ostrovsky, R.: Position-based quantum cryptography, arXiv/quant-ph:1005.1750 (2010)
17. Lau, H.K., Lo, H.K.: Insecurity of position-based quantum-cryptography protocols against entanglement attacks. Phys. Rev. A 83(1), 012322 (2011)
18. Kent, A.: Quantum tagging with cryptographically secure tags, arXiv/quant-ph:1008.5380 (2010)
19. Clark, S.R., Connor, A.J., Jaksch, D., Popescu, S.: Entanglement consumption of instantaneous nonlocal quantum measurements. New Journal of Physics 12(8), 083034 (2010)
20. Beigi, S., Koenig, R.: Simplified instantaneous non-local quantum computation with applications to position-based cryptography, arXiv/quant-ph:1101.1065 (2011)
21. Ishizaka, S., Hiroshima, T.: Asymptotic teleportation scheme as a universal programmable quantum processor. Phys. Rev. Lett. 101(24), 240501 (2008)
22. Ishizaka, S., Hiroshima, T.: Quantum teleportation scheme by selecting one of multiple output ports. Phys. Rev. A 79(4), 042306 (2009)
23. Giovannetti, V., Lloyd, S., Maccone, L.: Quantum cryptographic ranging. Journal of Optics B 4(4), 042319 (2002)
24. Renes, J., Boileau, J.: Conjectured strong complementary information tradeoff. Phys. Rev. Let. 103(2), 020402 (2009)
25. Buhrman, H., Chandran, N., Fehr, S., Gelles, R., Goyal, V., Ostrovsky, R., Schaffner, C.: Position-Based Quantum Cryptography: Impossibility and Constructions. Full version of this paper (2010), `http://arxiv.org/abs/1009.2490`
26. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
27. Berta, M., Christandl, M., Colbeck, R., Renes, J.M., Renner, R.: The uncertainty principle in the presence of quantum memory. Nature Physics (2010)
28. Damgård, I., Fehr, S., Salvail, L., Schaffner, C.: Cryptography in the bounded quantum-storage model. In: 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS), pp. 449–458. IEEE, Los Alamitos (2005)