Position-Based Quantum Cryptography

Nishanth Chandran* Serge Fehr† Ran Gelles* Vipul Goyal‡ Rafail Ostrovsky§

Abstract

In this work, we initiate the study of position-based cryptography in the quantum setting. The aim of position-based cryptography is to use the geographical position of a party as its only credential. This has interesting applications, e.g., it enables two military bases to talk to each other over insecure (i.e. neither private nor authenticated) channels and without having any pre-shared key, with the guarantee that only parties within the bases learn the content of the conversation.

Position-based cryptography in the classical setting has recently been rigorously studied by Chandran, Goyal, Moriarty and Ostrovsky [CGMO09]. They showed that position-based cryptography is *impossible* when there are multiple colluding adversaries at various positions in geographical space, and without assuming any restriction on these adversaries. This impossibility result holds even if the adversaries are assumed to have limited computation power. On the positive side, they proved security of certain position-based cryptographic schemes in the so-called Bounded Retrieval Model (BRM). The BRM is a very strong assumption. Very informally, their model assumes that a huge amount of information can be sent in an instantaneous "burst" of data and that adversaries can not retrieve nor store all the data from such a burst. Their work left open the interesting question whether it is possible to develop position-based secure protocols solely based on the laws of physics and without any adversarial restrictions.

This is exactly the question that we resolve in this paper. That is, we investigate the possibility of doing position-based cryptography in the *quantum* setting. We present schemes for several important position-based cryptographic tasks: positioning, authentication, and key exchange, and we prove them unconditionally secure, i.e., without assuming any restriction on the adversaries (beyond the laws of quantum mechanics). Our position-based key exchange scheme for instance solves the above motivating example of privately communicating between military bases, without using secure channels or a pre-shared key. At the core of our security proofs lies the *strong complementary information tradeoff* recently introduced by Renes and Boileau [RB09], which can also be understood as an entropic uncertainty relation with quantum side information [BCC+09]. An attractive feature of all our schemes is that they only involve "simple" quantum operations, namely to prepare, communicate and measure-upon-arrival individual qubits; no quantum computations are needed.

We stress that the above position-based tasks are impossible in the classical setting without limiting the adversary (e.g. his information retrieval bound). Therefore, our work shows that position-based quantum cryptography is one of the rare examples besides QKD for which there is such a strong separation between classical and quantum cryptography, i.e., where quantum cryptography offers unconditional security whereas by classical cryptographic means security is impossible if the adversary is not restricted.

Besides the schemes for which we give rigorous security proofs, we also present a couple of significantly more efficient schemes for which we can merely conjecture security; proving them secure (or insecure) remains an interesting challenge. Our results open a fascinating new direction for position-based security in cryptography where security of protocols is solely based on the laws of physics and proofs of security do not require any pre-existing infrastructure.

*Department of Computer Science, UCLA, Email:{nishanth,gelles}@cs.ucla.edu

†Cryptology and Information Security Group, CWI, Amsterdam, Email: Serge.Fehr@cwi.nl

‡Microsoft Research, India, Email: vipul@microsoft.com

§Department of Computer Science and Mathematics, UCLA, Email: rafail@cs.ucla.edu

1 Introduction

1.1 Background

Recently, 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*. As noted in [CGMO09], such a protocol could have important applications: if we trust physical perimeter security and so can guarantee that any person entering a secure facility has been authorized to do so, then one can send messages to a party present inside the facility or allow such parties to access confidential data without having to share any secret or credential information with them.

A central task in position-based cryptography is the problem of secure *positioning.* 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 takes place at 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] show that there exists no protocol for secure positioning that offers security in the presence of *multiple colluding* adversaries $\hat{P}_1, \ldots, \hat{P}_\ell$. 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] considered 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] constructed information-theoretically secure protocols for the task of secure positioning 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 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 initiate the study of 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! Thus, going to the quantum setting may indeed be a promising approach.

We show in this paper, for the first time, that this is really the case. We put forward quantum cryptographic schemes for several position-based tasks: secure positioning, authentication, and key exchange, and we prove these scheme unconditionally secure against an arbitrary coalition of adversaries. As already mentioned, a secure positioning scheme can be used to convince the verifiers $V_0, \ldots, V_k$ of the geographic position *pos* of P. A position-based authentication scheme on the other hand convinces the verifiers that a message m originates from P at position *pos*. Finally, a position-based key exchange scheme ensures that the verifiers share a secret key with P at position *pos*, and anyone that is not at position *pos* does not have any information regarding the key. If this is possible, and the key is sufficiently long, then perfectly secure communication with a device only located in a certain position is possible. In this paper, we resolve all these questions in the affirmative, in arbitrary dimension, and without any computational nor physical assumptions, and only using quantum laws of physics.

We stress that we prove security of our schemes for the above tasks without any restriction on the power of the adversaries; they may have unbounded classical and quantum memory, and they may have unbounded computing power; the only assumption is that the laws of quantum mechanics hold. Therefore, our results show that position-based quantum cryptography is one of the rare examples besides QKD for which there is a strong separation between classical cryptography and quantum cryptography, in that the latter offers unconditional security whereas the former does not offer any security if the adversary is unrestricted.

An additional attractive feature of all our solutions is that our schemes merely require one of the verifiers, V_0, to prepare individual qubits and send them to P, and P needs to measure them immediately upon arrival. No quantum computation is needed, and all other communication may be classical.

1.3 Our Schemes in More Detail

Secure positioning. Our secure positioning scheme is extremely simple. 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, so 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 why this is secure 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.[1] When $\hat{P}_0$ receives the BB84 qubit, he does not know yet the corresponding basis θ. Thus, if he measures it immediately when he receives it, then he 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 he waits until he knows the basis θ, then it is not too hard to see that $\hat{P}_0$ and $\hat{P}_1$ will be too late in sending x to V_1 in time. And, similarly, if he 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 he 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!

Proving the above intuition correct is non-trivial. Our proof is based on the *strong complementary information tradeoff* (CIT) due to Renes and Boileau [RB09] (see also [BCC$^+$09]), 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. On the other hand, parallel repetition of the above scheme would result in a more efficient 1-round scheme. However, the security of the parallel repetition does not necessarily follow from the security of the underlying scheme, and our techniques do not seem strong enough to prove security of the parallel repetition. We leave the security of the parallel repetition as an interesting open problem.

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 $V_1, V_2, \ldots, V_d$. Details are given later.

Position based authentication. Our position-based authentication scheme is based on our secure positioning scheme, combined with a technique used by Renner and Wolf in [RW03]. The idea is to start with a "weak" authentication scheme for a 1-bit message m, which works as follows. The verifiers and P execute the secure positioning 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

[1] It is not too hard to see that additional dishonest provers do not help.

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 for instance the specific encoding which maps 0 into 00...0 11...1 and 1 into 11...1 00...0, where all blocks of 0's and 1's are of length $N/2$, is good enough. First, we consider a 1-bit message m. The security of the resulting authentication scheme follows from proving that in order to succeed in changing a 0 to a 1 (or vice-versa), an adversary must succeed $\Omega(N)$ times in the secure positioning protocol "on his own" (i.e., without the help of the prover P) and hence has success probability $2^{-\Omega(N)}$. To authenticate longer messages, we let P sequentially authenticate the message bitwise. Proving that this is secure is non-trivial, again because of the out-of-sync issue, which potentially allows the adversary to intertwine different executions of the authentication scheme between the verifiers and the prover (unless we insert long delays between the executions). Nevertheless, with carefully chosen parameters and a sophisticated analysis, we can show security of the authentication scheme, when executed bit-by-bit, for arbitrary long messages.

Position based key exchange. 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.

We also suggest a direct and significantly more efficient construction of a position-based key exchange scheme. Unfortunately, our proof techniques do not seem to be strong enough to prove security of that scheme, and thus we can merely conjecture its security. Proving its security (or showing that it is not secure) hence remains an interesting open problem.

1.4 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 our quantum model in more detail. We present our protocol for secure positioning in Section 4. Section 5 is devoted to our position-based authentication protocol and finally, in Section 6, we show how to combine the above tools to obtain position-based key exchange.

2 Preliminaries

2.1 Notation and Terminology

Quantum Systems and States. 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 terminology and notation here. A *quantum system* is associated with a complex Hilbert space, $\mathcal{H} = \mathbb{C}^d$, its *state space*. The *state* of the system is given, in the case of a *pure* state, by a norm-1 state vector $|\psi\rangle \in \mathcal{H}$, respectively, in the case of a *mixed* state, by a trace-1 positive-semi-definite matrix $\rho : \mathcal{H} \to \mathcal{H}$, called *density matrix*. We write $\mathcal{D}(\mathcal{H})$ for the set of all density matrices acting on $\mathcal{H}$. We typically give quantum systems abstract names, A, B etc., and we write $\mathcal{H}_A$ for the state space of system A, and ρ_A (respectively $|\varphi_A\rangle$ in case of a pure state) for the state of A. The state space of a *bi-partite* (or *tri-* or *multi-partite*) quantum system AB, which consists of two (or three or more) subsystems, is given by the tensor product $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. If the state of AB is given by ρ_{AB} then the state of subsystem A on its own is given by the *partial trace* $\rho_A = \mathrm{tr}_B(\rho_{AB})$, and correspondingly for B. In order to simplify language, we are often a bit sloppy in distinguishing between a quantum system, its state, and the state vector or density matrix describing the state.

Measuring a system A in basis $\{|i\rangle\}_{i\in I}$, where $\{|i\rangle\}_{i\in I}$ is an orthonormal basis of $\mathcal{H}_A$, means applying the measurement described by the projectors $\{|i\rangle\langle i|\}_{i\in I}$. This has the effect that outcome $i \in I$ is observed with probability $p_i = \mathrm{tr}(|i\rangle\langle i|\rho_A)$ (respectively $p_i = |\langle i|\varphi_A\rangle|^2$ in case of a pure state). If A is a subsystem of a bipartite system AB, then it means applying the measurement described by the projectors $\{|i\rangle\langle i| \otimes \mathbb{I}_B\}_{i\in I}$, where $\mathbb{I}_B$ is the identity operator on $\mathcal{H}_B$.

We measure closeness of two states 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 ρ respectively σ, 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 quantum state ρ can be considered to be equal to σ.

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 $|0\rangle = \binom{0}{1}$, 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 is measures 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.

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 $|x\rangle$, and, 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 $H|x\rangle$.

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.

2.2 Some Quantum Information Theory

The *von Neumann entropy* of a quantum state $\rho \in \mathcal{D}(\mathcal{H})$ is given by $\mathrm{H}(\rho) := -\mathrm{tr}\big(\rho\log(\rho)\big)$, 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:* $\mathrm{H}(A|BY) = \sum_y P_Y(y)\,\mathrm{H}(\rho_{AB}^y|B)$.

Lemma 1 in particular implies that for classical Y: $\mathrm{H}(A) \geq \mathrm{H}(A|Y) \geq 0$.[2] The proof of Lemma 1 is given in Appendix A.

[2] For the first inequality, one additionally needs the concavity of H in combination with Jensen's inequality.

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: $q \geq \mathrm{h}^{-1}\big(\mathrm{H}(X|Y)\big)$.

Note that by incorporating the Holevo bound, the Fano inequality can be generalized to hybrid states in order to bound the probability of correctly guessing X by measuring and processing a quantum system E.[3]

2.3 Strong Complementary Information Tradeoff

The following entropic uncertainty principle, called *strong complementary information tradeoff* (CIT) in [RB09] and generalized in [BCC+09], 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*

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

CIT as expressed above 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*

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

PROOF. By Lemma 1, we can write

$$\mathrm{H}(X|\Theta E) + \mathrm{H}(X|\Theta F) = \frac{1}{2^n}\sum_{\theta}\mathrm{H}(\rho^{\theta}_{XE}|E) + \frac{1}{2^n}\sum_{\theta}\mathrm{H}(\rho^{\theta}_{XF}|F) = \frac{1}{2^n}\sum_{\theta}\big(\mathrm{H}(\rho^{\theta}_{XE}|E) + \mathrm{H}(\rho^{\bar{\theta}}_{XF}|F)\big) \,.$$

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] We would like to point out that the resulting bound is not what is commonly known as the *quantum Fano inequality.*

3 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 consider entities $V_0, \dots, V_k$ called *verifiers* and an entity P, the (honest) *prover*. Additionally, we consider a coalition $\hat{P}$ of *dishonest provers* (or *adversaries*) $\hat{P}_0, \dots, \hat{P}_\ell$. All entities can perform arbitrary quantum (and classical) operations and can communicate quantum (and classical) messages among them.[4] 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, which so far could be described by quantum interactive Turing machines, 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 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 the speed of light 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 at which a message is received. We do not require P's clock to be precise or in sync with the verifiers. However, we do assume that P's clock only runs forward (i.e. P cannot be reset). This is the place to mention that we consider only *stand-alone security*, i.e., there exists only a single execution of a single honest prover, and we do not guarantee concurrent security.

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 will always (sometimes implicitly) require that the honest prover P is *enclosed* by the verifiers $V_0, \dots, V_k$ in that the prover's position $pos \in \mathbb{R}^d$ lies within the tetrahedron, i.e., convex hull, $\mathrm{Hull}(pos_0, \dots, pos_k) \subset \mathbb{R}^d$ formed by the respective positions $pos_0, \dots, pos_k$ of $V_0, \dots, V_k$.

4 Secure Positioning

A secure positioning 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 $V_0, \dots, V_k$, which are located at respective positions $pos_0, \dots, pos_k \in \mathbb{R}^d$, that he is indeed at position *pos*. We assume that P is enclosed by $V_0, \dots, V_k$, i.e., $pos \in \mathrm{Hull}(pos_0, \dots, pos_k)$. We require that the verifiers jointly accept if 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 $\hat{P}_0, \dots, \hat{P}_\ell$ at arbitrary positions $apos_0, \dots, apos_\ell \in \mathbb{R}^d$ with $apos_i \neq pos$ for all i. We refer to [CGMO09] for the general formal definition of the completeness and security of a secure positioning scheme. In this article, we focus on secure positioning schemes that are of the form as specified in the following definition.

Definition 1 *A* **1-round secure positioning scheme** SP *consists of a challenge generator* Chlg*, which outputs a list of challenges* $(ch_0, \dots, ch_k)$ *and some auxiliary information* x*, and a response algorithm* Resp*, which on input a list of challenges outputs a response* x'*.* SP *is said to have* **perfect completeness** *if* $\mathsf{Resp}(ch_0, \dots, ch_k) = x$ *with probability 1 for* $(ch_0, \dots, ch_k)$ *and* x *generated by* Chlg*.*

[4] In order to obtain "practical" schemes, we will minimize the quantum operations of the honest entities and the quantum communication among them.

The algorithms Chlg and Resp are used as described in Figure 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 $T - d(pos_i, pos)$.[5] As a result, all ch_i's arrive at P's position pos at time T. In step 3, V_i receives x' *in time* if x' 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 positions $pos_0, \dots, pos_k$, and the (claimed) position pos of P.

0. V_0 generates $(ch_0, \dots, ch_k)$ and x using Chlg, and sends ch_i and x to V_i for $i = 1, \dots, k$.
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. When all the ch_i's arrive, P computes $x' := \mathsf{Resp}(ch_0, \dots, ch_k)$ and sends x' to all V_i's.
3. The V_i's jointly accept if and only if all V_i's receive the same x' in time and $x' = x$.

Figure 1: Generic 1-round positioning scheme.

We stress that we allow Chlg and Resp to be *quantum* algorithms and the challenges ch_i to be quantum states, but for simplicity we require x and x' to be classical. In our constructions, only ch_0 will actually be quantum, and ch_1 up to ch_k will be classical; thus, we will only require quantum communication from V_0 to P, all other communication may be classical. Furthermore, in our constructions, the only thing quantum about the algorithms Chlg and Resp will be that Chlg involves the preparation of a quantum state (namely the challenge ch_0) and Resp involves a measurement. Thus, no involved and currently infeasible quantum computations are required.

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

Obviously, for the problem we address here, we only need to consider *either* an honest prover P *or* a coalition of dishonest provers $\hat{P}$. In the subsequent sections, where we study position-based authentication and key exchange, we will also need to consider a coalition of dishonest provers that attack an honest execution of the scheme between P and the verifiers.

A secure positioning 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.

4.1 The Basic Scheme in 1 Dimension

We propose the following basic 1-round secure positioning scheme, given in Figure 2. 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.

[5] Recall, $d(pos_i, pos)$ is the Euclidean distance between pos_i and pos and coincides with the time needed for ch_i to travel from pos_i to pos (given that the speed of light is normalized to 1).

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 2: A secure positioning scheme $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$ based on the BB84 encoding.

Theorem 4 *The 1-round secure positioning scheme* $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$ *from Figure 2 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 about 0.85. This shows that our analysis is rather tight.[6]

Proof. In order to analyze the positioning scheme it is convenient to consider an equivalent *purified* version, given in Figure 3. 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 (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 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 3: EPR version of $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$.

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, 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, it forwards (a copy of) it to $\hat{P}_0$. Also, as soon as $\hat{P}_0$ receives the qubit A, it applies an arbitrary quantum operation to the received qubit A 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 P_1 receives θ, it 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, it 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 the quantum operation and thus $|\psi_{A\,E_0E_1}\rangle$ does not depend on θ. Recall that x is obtained by measuring A in either the computational (if $\theta = 0$) or the Hadamard (if

[6] We suspect that our analysis is not fully tight and that 0.85 is the real soundness error.

$\theta = 1$) 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

$$\mathrm{h}(q_i) \geq \tfrac{1}{2}$$

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 cannot do any better. This can be reasoned similarly to 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 $E_0 E_1$ *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. □

4.2 Reducing the Soundness Error

In order to obtain a secure positioning scheme with a negligible soundness error, we can simply repeat the 1-round scheme $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$ from Figure 2. 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 *The n-fold sequential repetition of $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$ from Figure 2 is ε^n-sound with $\varepsilon = 1 - \mathrm{h}^{-1}(\frac{1}{2})$.*

A more efficient way of repeating $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$ 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. Unfortunately, we do not have a proof for the security of the parallel repetition of $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$. We state its security as a conjecture and leave it as an open problem to resolve it.

Conjecture 1 *The n-fold parallel repetition of $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$ from Figure 2 is δ^n-sound for some $\delta < 1$.*

We actually suspect δ to be $\cos(\pi/8)^2 \approx 0.85$, which is obtained by measuring all qubits in the Breidbart basis.

We would like to point out that, similar to the proof of Theorem 4, the CIT (Corollary 1) allows to conclude that at least one of $\hat{P}_0$ and $\hat{P}_1$ has Shannon entropy $n/2$ in the n-bit string X to be guessed. However, this is not sufficient to conclude that the guessing probability is negligible.

4.3 Secure Positioning in Higher Dimensions

The scheme $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$ can easily be extended into higher dimensions. 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.

The scheme for 3 dimensions is a generalization of the scheme $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$ in Figure 2, where now the challenges of the verifiers V_1, V_2 and V_3 form a *sum sharing* of the basis θ, i.e., are random $\theta_1, \theta_2, \theta_3 \in \{0,1\}$

such that their modulo-2 sum equals θ. As specified in Figure 1, the state $H^\theta|x\rangle$ and the shares $\theta_1, \theta_2, \theta_3$ 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. 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 he 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. 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 $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$ to d dimensions is ε-sound with $\varepsilon = 1 - \mathrm{h}^{-1}(\frac{1}{2})$.*

5 Position-Based Authentication

In this section we consider a new primitive: position-based authentication. In contrast to secure positioning, 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 secure positioning 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 $m = m'$, if 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 position $pos \in \mathrm{Hull}(pos_0, \ldots, pos_k)$ 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 secure positioning scheme. The idea is to incorporate the message to be authenticated into the replies of the positioning 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. We begin by proposing a weak but simple position-based authentication scheme for 1-bit message m.

5.1 Weak 1-bit authentication scheme

Let $\mathsf{SP}^{\varepsilon}$ be a secure 1-round secure positioning scheme between $k+1$ verifiers $V_0, \ldots, V_k$ and a prover P. We require $\mathsf{SP}^{\varepsilon}$ to have perfect completeness and soundness $\varepsilon < 1$. $\mathsf{SP}^{\varepsilon}$ may for instance be the scheme $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$ from Section 4. We let $\perp$ be some special symbol. We consider the weak authentication scheme given in Figure 4 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 secure positioning scheme $\mathsf{SP}^{\varepsilon}$, but letting P replace his response x' by an "erasure" (i.e. by $\perp$) with probability q, where we choose $0 < q < (1-\varepsilon)/4$.

0. V_0 generates $(ch_0, \dots, ch_k)$ and x using Chlg and sends ch_i and x to V_i for $i = 1, \dots, k$.
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_i's arrive, P computes the authentication tag t as follows and sends it back to all the verifiers. If $m = 1$ then $t := \mathsf{Resp}(ch_0, \dots, ch_k)$, and if $m = 0$ then $t := \perp$ with probability q and $t := \mathsf{Resp}(ch_0, \dots, ch_k)$ 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 4: 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 $\mathsf{SP}^{\varepsilon}$.

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 $\delta = 1 - q(1-\varepsilon) < 1$.*

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 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 then 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 careful about the exact choice of the encoding of the message.

5.2 Secure Position-Based Authentication Scheme

To prevent the adversary from using the honest provers replay, we must encode m using a code with certain properties. For this purpose we introduce the notion of *dominating codes.*

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'* **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* $\Omega(N)$*, or (b) the number of positions for which* $e'_i = 0$ and $e_i = -1$ *is* $\Omega(N)$ *and is larger than the number of positions for which* $e'_i = 0$ *but* $e_i \in \{0, 1\}$.

For instance, $c = 00...0\,11...1$ and $c' = 11...1\,00...0$, where the blocks of 0's and 1's are of length $N/2$, dominate each other, which is not too hard to see. However, $\tilde{c}' = 0101...01$ does not dominate $\tilde{c} = 1010...10$, since $\tilde{c}'$ can be embedded into ‡0101...01‡‡...‡ and $\tilde{c}$ into 1010...10‡‡...‡, where ‡ represents -1.

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

Corollary 4 *Let* C *be a dominating code (with* $|C| \geq 2$*) and let* $c \in C$*. Define* n_0, n_1 *to be the number of* 0*s and the number of* 1*s in* c*, then for every* $c \in C$*,* $n_0 = \Omega(N)$*,* $n_1 = \Omega(N)$*.*

Let $\mathsf{wAUTH}^\varepsilon$ be the above weak authentication scheme satisfying Lemma 2. In order to authenticate a 1-bit message $m \in \{0,1\}$ in a strong way, an encoding c of m using a dominating code C is bit-wise authenticated by means of $\mathsf{wAUTH}^\varepsilon$, and the verifies perform statistics over the number of $\perp$s received. A possible choice for C is the *balanced repetition code* $C_{\text{BR}} = \{00...0\,11...1, 11...1\,00...0\} \subset \{0,1\}^N$. The resulting authentication scheme is given in Figure 5; as for the weak scheme, we assume that the message m has already been communicated.

0. P and the verifiers encode m into a codeword $c = (c_1, \ldots, c_N) \in C$, for a dominating code C.
1. For $j = 1, \ldots, N$, the following is repeated in sequence.
   2.1 P authenticates c_j by means of $\mathsf{wAUTH}^\varepsilon$. Let t_i be the corresponding tag received.
   2.2 The verifiers keep track of the number of rounds in which P replied with $\perp$, i.e., they compute $n_0 = |\{j : c_j = 0\}|$ and $n_\perp = |\{j : c_j = 0 \wedge t_j = \perp\}|$.
2. If any of the $\mathsf{wAUTH}^\varepsilon$ executions fails, or if $n_\perp > 2qn_0$ then the verifiers jointly reject. Otherwise, m is accepted.

Figure 5: A generic position-based authentication scheme AUTH.

Theorem 5 *The above generic position-based authentication scheme is* $2^{-\Omega(N)}$*-complete.*

Proof. An honest prover which follows the above scheme can fail only if $n_\perp > 2qn_0$. Using Chernoff bound [Che52], the probability of having $n_\perp > 2qn_0$ is upper bounded by $e^{-qn_0/2}$. Since for every $c \in C$, $n_0 = \Omega(N)$ (Corollary 4), the theorem follows. □

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 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 as well as 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 active 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 every of $\hat{P}$'s rounds where he chooses between (1), (2) or (3), update e by $e\ddagger$ 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 $e'\ddagger$ if he chooses (3). In the end, complete e and e' by padding them with sufficiently many $\ddagger$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, with $\ddagger$ representing positions with value -1.

Theorem 6 *For any $\varepsilon > 0$, the position-based authentication scheme from Figure 5 is $2^{-\Omega(N)}$-sound.*

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 dominating code C we know that one of the following two properties (a) or (b) holds. (a) The number of positions $i \in \{1, \ldots, 2N\}$ for which $e'_i = 1$ and $e_i \in \{-1, 0\}$ is $\Omega(N)$. In this case, by construction of the embeddings, in his attack $\hat{P}$ needs to authenticate (using $\mathsf{wAUTH}^\varepsilon$) the bit 1 a linear number of times (by means of an impersonation or a substitution attack). By Lemma 2, the success probability of $\hat{P}$ is thus at most $\delta^{\Omega(N)}$, which is $2^{-\Omega(N)}$. (b) Defining the index subsets $\mathit{Bad} := \{i : e'_i = 0 \wedge e_i = -1\}$ and $\mathit{Good} := \{i : e'_i = 0 \wedge e_i \in \{0, 1\}\}$, it holds that $|\mathit{Bad}| = \Omega(N)$ and $|\mathit{Bad}| \geq |\mathit{Good}|$. In this case, we can argue as follows. For any i with $e'_i = 0$, $\hat{P}$ needs to authenticate (using $\mathsf{wAUTH}^\varepsilon$) the bit 0 by means of an impersonation attack, but he may only use $\perp$ as tag for a $2q$-fraction of those i's. This means that he may use $\perp$ as tag for at most a $4q$-fraction of the i's in Bad, and for all the remaining $i \in \mathit{Bad}$ he must provide the correct reply to the underlying secure positioning scheme. However, by the ε-soundness of SP^ε, where $\varepsilon < 1 - 4q$, the probability of $\hat{P}$ succeeding in this is exponentially small (in N, determined by the choice of code). □

Plugging in the concrete secure positioning scheme from Section 4.3, we obtain a secure realization of position-based authentication scheme in $\mathbb{R}^d$. The scheme is described in Appendix C.1 (Figure 7).

5.3 Authenticating Arbitrarily-Long Messages

Although the scheme AUTH from above is designed for 1-bit messages, it can be used to authenticate messages m of arbitrary length. We assume that the verifiers expect a message of a fixed length n, and that the executions of $\mathsf{wAUTH}^\varepsilon$ are performed in the specified order. Extending the authentication scheme to arbitrary lengths can be done in the following ways:

One can try to find dominating codes for larger message spaces [if such codes exist]; then the scheme AUTH and its analysis can stay unchanged. Another method would be to encode the message m bit-by-bit using a dominating code (for each bit). The encoding of m might not result in a dominating code and thus AUTH might not be secure for this case, if the adversary is allowed to interleave authentication executions of adjacent m's bits. In Appendix B (see Theorem 7) we show that the security of the sequential application of AUTH can also be shown by a careful choice of the probability q, namely, $q < (1 + \varepsilon)/16n$, and a careful choice of the code C, namely the balanced repetition code C_{BR}, and a more involved analysis.

We point out that the above approach results in rather inefficient position-based authentication schemes that require a large number of communication rounds. For large messages, the efficiency can be somewhat improved by using generic techniques, like first authenticating the message m by means of a standard authentication code with a (short) key randomly chosen by P, and then simultaneously announcing and authenticating the key by means of the position-based authentication scheme. Finding significantly more efficient solutions, and in particular finding 1-round position-based authentication schemes, is left as an interesting open problem.

6 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*.[7] 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.

6.1 A Generic Construction

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 the standard[8] BB84 scheme as our QKD, we obtain the position-based key exchange scheme described in Appendix C.2. The security of this scheme follows from the security of the BB84 protocol [LC99, BBB$^+$00, SP00, May01, BOHL$^+$05] and of the position-based authentication scheme.

Due to the inefficiency of the underlying authentication scheme, the above construction is very inefficient, in particular in the number of communication rounds. Thus, the above should be considered as a proof that position-based quantum key exchange with unconditional security is possible in principle. We leave the search for efficient position-based key exchange schemes for future research, possibly inspired by the approach from the next section.

6.2 A Direct Construction with Conjectured Security

We propose a simple and relatively efficient position-based key exchange scheme. Unfortunately we do not have a security proof, and we leave it as an open problem to find an attack or prove its security. For simplicity, we describe it for the 1-dimensional setting, with two verifiers; a scheme for higher dimensions can be obtained by the same approach as in Section 4.3.

The scheme is parameterized by positive integers N and L, and it makes use of a universal hash function $g : \mathcal{R} \times \{0,1\}^N \to \{0,1\}^L$. The purpose of the universal hash function is to perform *privacy amplification*.

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

[8] More accurately, we use a variant of BB84 in which the entire classical authenticated communication is performed from P to V. However, the standard BB84 scheme (with two-directional authenticated channel) can still be used using the method described above.

The scheme is given in Figure 6 below. $2^{-\Omega(N)}$-Completeness is trivially satisfied; below, we state the security of the scheme as a conjecture.

0. V_0 and V_1 privately agree on two random strings $x = (x_1, \ldots, x_N)$ and $\theta = (\theta_1, \ldots, \theta_N)$ in $\{0,1\}^N$.
1. For $i = 1, \ldots, N$, the following is repeated (in sequence or in parallel).
   - 1.1 V_0 prepares the qubit $H^{\theta_i}|x_i\rangle$ and sends it to P, and V_1 sends the bit θ_i to P, so that $H^{\theta_i}|x_i\rangle$ and θ_i arrive at the same time at P.
   - 1.2 When $H^{\theta_i}|x_i\rangle$ and θ_i arrive, P measures $H^{\theta_i}|x_i\rangle$ in basis θ_i to observe $x'_i \in \{0,1\}$. Furthermore, P sets $x''_i := x'_i$ with probability $\frac{1}{2}$ and $x''_i := \perp$ otherwise.
   - 1.3 V_0 and V_1 check on both sides if x''_i arrives in time and if $x''_i \in \{x_i, \perp\}$.
2. If any check in step 1.3 fails, or if V_0 and V_1 have received different values for $x'' = (x''_1, \ldots, x''_N) \in \{0,1,\perp\}$, or if the number of $\perp$s within x'' is $\geq \frac{3}{4}N$, then V_0 and V_1 abort.
   Otherwise, V_0 chooses a random seed $r \in \mathcal{R}$ and sends it to P, and V_0 and P compute K and K' respectively as $K = g(r,x)$ and $K' = g(r,x')$.

Figure 6: A simple and efficient key exchange scheme.

Conjecture 2 *For a suitable choice of $L = O(N)$, the scheme from Figure 6 is $2^{-\Omega(N)}$-secure.*

7 Conclusion

We have initiated an exciting new line of research: position-based quantum cryptography. We have shown the existence of quantum cryptographic schemes for position-based tasks that can be rigorously proven secure without assuming any limitation on the adversaries' resources – security is based solely on the laws of quantum mechanics. In combination with the impossibility result of [CGMO09], this shows a strong separation between classical and quantum cryptography, similarly to the case of QKD. On the other hand, our schemes with conjectured security show that position-based quantum cryptography still offers room for further interesting research.

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 *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (STOC)*, pages 715–724, New York, 2000. ACM Press.

[BBB$^+$02] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor. Security of Quantum Key Distribution against All Collective Attacks1. *Algorithmica*, 34:372–388, 2002.

[BC94] Stefan Brands and David Chaum. Distance-bounding protocols. In *EUROCRYPT '93: Advances in cryptology*, pages 344–359. Springer-Verlag New York, Inc., 1994.

[BCC$^+$09] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M. Renes, and Renato Renner. An entropic uncertainty relation with quantum side information. `http://arxiv.org/abs/0909.0950`, 2009.

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

[CGMO09] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky. Position Based Cryptography. In *Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology*, 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.

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

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

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

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

[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. *Physical review letters*, 103(2):020402, 2009.

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

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

[SP05] Dave Singelee and Bart Preneel. Location verification using secure distance bounding protocols. In *IEEE Conference on Mobile Adhoc and Sensor Systems Conference*, 2005.

[SSW03] Naveen Sastry, Umesh Shankar, and David Wagner. Secure verification of location claims. In *WiSe '03: Proceedings of the 2003 ACM workshop on Wireless security*, pages 1–10, 2003.

[VN04] Adnan Vora and Mikhail Nesterenko. Secure location verification using radio broadcast. In *OPODIS '04: 8th International Conference on Principles of Distributed Systems*, 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.

Appendix

A Some Technical Lemmas

A.1 Proof of Lemma 1

In this section we proof the following lemma: *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

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

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.

B Authenticating Bit-Wise Encoded Messages is Secure

We now prove that the authentication scheme of Figure 5 can be used to authenticate a message of arbitrary length n. This is obtained by setting $q \leq (1-\varepsilon)/16n$, and encoding the message $m = m_1 m_2 \cdots m_n$ bit-wise by means of the *balanced repetition code* $C_{\mathrm{BR}} \subset \{0,1\}^N$ which maps 0 into $C_{\mathrm{BR}}(0) = 000...0\,111...1$ and 1 into $C_{\mathrm{BR}}(1) = 111...1\,000...0$, where the 0- and the 1-blocks are of length $N/2$.[9] For simplicity we assume that N is even.

Lemma 3 *Assume that an adversary tries to authenticate $c' \in \{0,1\}^N$ by performing* impersonation attack *at least γN times, for some constant γ (i.e., using only $(1-\gamma)N$ callings to P). Let $n_0 = |\{j : c'_j = 0\}|$, then for $\frac{1}{8n}n_0 < \gamma \leq 1$, and $q < (1-\varepsilon)/16n$ the probability of success is bounded by*

$$e^{-(\gamma - \frac{1}{8n}n_0)^2(1-\varepsilon)\frac{N}{2\gamma}} = 2^{-\Omega(N)}\ .$$

Proof. We will assume that the adversary succeeds to authenticate the remaining $(1-\gamma)N$ rounds with probability 1. In this case, the adversary is allowed to answer $\perp$ at most $2qn_0N < \frac{2}{16n}(1-\varepsilon)n_0N$ times. However, in expectation, $(1-\varepsilon)\gamma N$ of the times the response will be $\perp$ (or an error). Letting $\gamma > \frac{1}{8n}n_0$ and using Chernoff inequality, the lemma follows. □

Note that the above is true regardless to the message that the honest prover is authenticating, i.e., it holds both for $m' = m$ and $m' \neq m$.

[9] We are a bit sloppy here and do not distinguish between the set of codewords and the encoding function.

Lemma 4 *Assume $m \in \{0,1\}^n$ is encoded bitwise to $c = \tilde{c}_1\tilde{c}_2\cdots\tilde{c}_n$, with $\tilde{c}_i \in \{0,1\}^N$, by means of the balance repetition code C_{BR}. Then in order to authenticate a position i in which $m'_i \neq m_i$, the adversary must call P at least $N/8$ times with positions that are not in $\tilde{c}_i$, i.e., at least $N/8$ bits of $\tilde{c}_j$, $j \neq i$, otherwise his success probability is bounded by $2^{-\Omega(N)}$.*

Proof. Look at an index i such that $m'_i \neq m_i$. Assume for contradiction that P is called more than $7N/8$ times from indices of $\tilde{c}_i$ corresponding to the block i.

Let us look on the case where $m_i = 0, m'_i = 1$; thus $\tilde{c}_i = 000...0\,111...1, \tilde{c}'_i = 111...1\,000...0$. Since the adversary has a higher success probability in authenticating 0 over 1 (by means of $\mathsf{wAUTH}^{\varepsilon}$), we can assume that the best scenario for the adversary is to have $N/8$ ones from a previous block, say $\tilde{c}_{i-1}$. This is equivalent to the case where the adversary authenticates

$$c' = \underbrace{111\ldots1}_{N/2}\,\underbrace{000\ldots0}_{N/2},\ \text{using}\ c = \underbrace{11..1}_{N/8}\,\underbrace{000\ldots0}_{N/2}\,\underbrace{111\ldots1}_{N/2}.$$

The notion of dominating can be extended in a trivial way to codewords of unequal lengths, and using this extended notion, it is easy to verify that c' dominates c. As a corollary of Theorem 6, any authentication of (a message with encoding) c' which is performed using an honest prover replies for the encoding c would fail with high probability as long c' dominates c. We can conclude that the adversary can not authenticate c' except with a negligible probability, by using less than $N/8$ calls of P with positions in $\tilde{c}_j, j \neq i$.

The other case ($m_i = 1, m'_i = 0$, thus $\tilde{c}_i = 111...1\,000...0, \tilde{c}'_i = 000...0\,111...1$) is similar. □

We can conclude that using this encoding, any adversary that tries to authenticate $m' \neq m$ must use P's responses for some block $\tilde{c}_j$ in order to authenticate $\tilde{c}'_i$, if $m'_i \neq m_i$. Now, when trying to authenticate the block $\tilde{c}'_j$, the adversary would face a problem, since many of P's responses for that block are used for authenticating $\tilde{c}'_i$. The following theorem shows that there exist at least one block $\tilde{c}'_{i'}$ that the adversary would fail to authenticate with high probability, and thus the scheme is secure.

Theorem 7 *If the balanced repetition code $C_{\mathrm{BR}} \subset \{0,1\}^N$ is used as code C, and if q is chosen $0 < q \leq (1-\varepsilon)/16n$ in the underlying scheme $\mathsf{wAUTH}^{\varepsilon}$, then the bit-wise execution of the authentication scheme from Figure 5 is $2^{-\Omega(N/n)}$-sound for n-bit messages.*

Thus, in order to get an exponentially small soundness error, N has to be chosen quadratic in n.

Proof. Since $m' \neq m$ there exists position i which they differ, $m'_i \neq m_i$. By lemma 4, in order to authenticate the block $\tilde{c}'_i$ the adversary must use P with at least $N/8$ positions in $\tilde{c}_j$, $j \neq i$. It follows that at least $N/16$ are taken from one of the adjacent[10] blocks $\tilde{c}_j$, $j = i \pm 1$. Without loss of generality we assume that $j = i + 1$; the proof for $j = i - 1$ is similar.

Let us look on the case where the adversary authenticates $\tilde{c}'_j$. The adversary can not use P replies of $\tilde{c}_i$, but it can use ξ replies from the consecutive block $j + 1$. If $\xi \leq N/16 - N/16n$ than by Lemma 3, the success probability for authenticating j is negligible. Otherwise, $\xi > N/16 - N/16n$, which must be taken from $\tilde{c}_{j+1}$. The same reasoning holds for the $(j+1)$-th block: $N/16 - N/16n$ of $\tilde{c}_{j+1}$ positions were used for block j; then either the adversary uses less than $N/16 - 2 \cdot (N/16n)$ positions from $\tilde{c}_{j+2}$ and fails by Lemma 3 or otherwise, we can focus on the authentication of the $(j+2)$-th block instead. This continues until we reach the last block $\tilde{c}_n$ which has no consecutive block to use, yet the previous round called P for at least $N/16 - (n-1)(N/16n) = N/16n$ times with positions from $\tilde{c}_n$, and by Lemma 3 the authentication of n-th block would fail. We conclude that at least one of the blocks along the way will fail (with high probability). □

[10] Otherwise, i.e., if the positions are taken from block other than the immediate adjacent blocks, the adversary clearly fails on at least one block, due to Lemma 3.

C Concrete realization of quantum position-based primitives

In this section we describe a position-based message authentication scheme, and a position-based key exchange protocol, both based on the secure positioning scheme $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$ described in Figure 2

C.1 Position-Based Authentication scheme based on $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$

The following is a realization of a $2^{-\Omega(N)}$-complete and $2^{-\Omega(N)}$-sound position-based authentication scheme, based on the general authentication scheme (Figure 5) with $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$ as the underlying secure-positioning primitive. The scheme can be used either for 1-bit message m or an arbitrary length message, using the methods described in section 5.3.

0. $V_0, \ldots, V_k$ privately agree on two random strings $x = (x_1, \ldots, x_k)$ and $\theta = (\theta_1, \ldots, \theta_n)$ in $\{0,1\}^k$,
1. The verifiers and P encode the message m into a codeword $c \in C$, for a dominating code $C \subseteq \{0,1\}^N$.
2. For $i = 1, \ldots, N$, the following is repeated in sequence.

   2.1 V_0 prepares the qubit $H^{\theta_i}|x_i\rangle$ and sends it to P. $V_1, \ldots, V_k$ send a k-out-of-k sharing of the bit θ_i to P, so that $H^{\theta_i}|x_i\rangle$ and (all the shares of) θ_i arrive at the same time at P.

   2.2 When $H^{\theta_i}|x_i\rangle$ and θ_i arrive, P measures $H^{\theta_i}|x_i\rangle$ in basis $H^{\theta_i}\{|0\rangle, |1\rangle\}$ to observe $x'_i \in \{0,1\}$.

   2.3 If $c_i = 1$, P sends x'_i to $V_1, \ldots, V_k$. Otherwise, P sends back x'_i with probability $1 - q$ or $\perp$ with probability q.

   2.4 Let t_i be the corresponding tag received. $V_0, \ldots, V_k$ check that t_i arrives in time and that all sides received the same tag t_i. If $t_i \neq x_i$ *and* $(c_i = 0, t_i \neq \perp)$, the verifiers abort.

   2.5 The verifiers keep track of the number of rounds in which P replied with $\perp$, i.e., they compute $n_0 = |\{j : c_j = 0\}|$ and $n_\perp = |\{j : c_j = 0 \wedge x''_j = \perp\}|$.
3. If any check in step 2.5 fails, or if different verifiers have received different values for c, or if $\eta_\perp > 2qn_0$ then $V_1, \ldots, V_k$ abort. Otherwise, $V_1, \ldots, V_k$ accept the message m.

Figure 7: A position-based authentication scheme based on BB84 encoding.

C.2 Position-based Key Exchange Protocol Based on BB84 and $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$

The following is a realization of a position-based quantum key exchange protocol. The scheme uses BB84 as the underlying QKD system, and realizes position-based authentication using $\mathsf{SP}^{\varepsilon}_{\text{BB84}}$ described in Figure 2.

0. $V_0, \ldots, V_k$ privately and randomly choose strings $x = (x_1, \ldots, x_{(4+\delta)n})$ and $\theta = (\theta_1, \ldots, \theta_{(4+\delta)n})$ in $\{0,1\}^{(4+\delta)n}$.
1. For $i = 1, \ldots, (4+\delta)n$, the following is repeated in sequence[11].
   1.1 V_0 prepares the qubit $H^{\theta_i}|x_i\rangle$ and sends it to P.
   1.2 When $H^{\theta_i}|x_i\rangle$ arrives, P randomly chooses a basis $\theta'_i \in \{0,1\}$ and measures $H^{\theta_i}|x_i\rangle$ in basis $H^{\theta'_i}\{|0\rangle, |1\rangle\}$ to observe $x'_i \in \{0,1\}$.
2. P signals the verifiers that all the qubits were received using the SP-authentication scheme.
3. After all the qubits were received by P, V_0 sends the string θ used to encode the qubits.
4. Set X_{sift} to be the string composed of those positions i such that $\theta_i = \theta'_i$. With high probability (with respect to δ), $|X_{\text{sift}}| \geq 2n$, otherwise, abort the protocol. ¿From this point and on, we assume $|X_{\text{sift}}| = 2n$. P randomly chooses n positions $I \subset \{1, \ldots, 2n\}$ in X_{sift}. Set X_{err} to be the substring defined by positions I, and X_{inf} to be the substring defined by the other n positions, $\{1, \ldots, 2n\} \setminus I$.
5. Using the SP-authentication scheme (Figure 5), P sends the following information in authenticated way: θ, θ', I, X_{err}, Error correction (EC) information for X_{inf} and Privacy Amplification (PA) information for generating a key K from X_{inf}[12].
6. If any of the messages fails being authenticated, abort the protocol. Otherwise, $V_0, \ldots, V_k$ verify that θ received in step 5 equals the one sent to P in step 3, and compare X_{err} to the appropriate positions of x. If the error rate is higher than some predefined parameter ρ_e, abort the protocol.
7. Otherwise, $V_0, \ldots, V_k$ compute X_{inf} using x and the EC information, and compute K using the PA information and X_{inf}.

Figure 8: A position-based QKD scheme.

[11] This step can be replaced by a single step in which all the qubits are sent to P in a single transmission.

[12] Both EC and PA can be done with uni-directional communication from P to the verifiers, using pre-defined matrices P_{EC} and P_{PA}; see for instance [BBB$^+$02].