Position-Based Quantum Cryptography: Impossibility and Constructions

Full version available at `http://arxiv.org/abs/1009.2490`

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

Abstract

In this work, we study position-based cryptography in the quantum setting. The aim is to use the geographical position of a party as its only credential. On the negative side, we show that if adversaries are allowed to share an arbitrarily large entangled quantum state, no secure position-verification is possible at all. To this end, we prove the following very general result. Assume that Alice and Bob share a (possibly) unknown quantum state $|\psi\rangle_{AB}$ and some classical information x, y respectively. Their goal is to calculate and share a new state $|\Psi\rangle_{\tilde{A}\tilde{B}} = U_{x,y}|\psi\rangle_{AB}$, where $\{U_{i,j}\}$ is a set of fixed unitary operations. Clearly, since both the quantum state and the classical state that determines the unitary are distributed among the players, they need to communicate. The question that we ask here is how many rounds of communication are needed, where by a round we define both Alice and Bob sending both classical and quantum messages to each other without waiting for messages of other parties. It is easy to achieve such a task using two rounds of classical communication. Surprisingly, in case Alice and Bob share enough entanglement to start with, we show that the same task can be done using a single round of classical communication in which Alice and Bob send simultaneously to each other the classical data involved. In the paper, we generalize this theorem to multiple players. As an immediate consequence of this theorem, we show a generic attack that breaks any position-verification scheme. On the positive side, we show that if adversaries do not share any entangled quantum state but can compute arbitrary quantum operations, secure position-verification is achievable. Jointly, these results suggest the interesting question whether secure position-verification is possible in case of a bounded amount of entanglement. Our positive result can be interpreted as resolving this question in the simplest case, where the bound is set to zero. In models where secure positioning is achievable, it has a number of interesting applications. For example, it enables secure communication over an insecure channel without having any pre-shared key, with the guarantee that only a party at a specific location can learn the content of the conversation. More generally, we show that in settings where secure position-verification is achievable, other position-based cryptographic schemes are possible as well, such as secure position-based authentication and position-based key agreement.

1 Background

The goal of position-based cryptography, as introduced by Chandran, Goyal, Moriarty and Ostrovsky [CGMO09] in the classical setting, is to do cryptography without digital cryptographic keys, but where instead the geographical position of a party acts as its (only) "credential". For example, one would like to send a message to a party at a geographical position *pos* with the guarantee that the party can decrypt the message only if he or she is physically present at *pos*. A central task in position-based cryptography is the problem of *position-verification*. We have a *prover* P at position *pos*, wishing to convince a set of *verifiers* $V_0, \ldots, V_k$ (at different points in geographical space) that he (i.e. the prover) is indeed at that position *pos*. The prover can run an interactive protocol with the verifiers in order to do this. The main technique for such a protocol is known as distance bounding [BC94]. In this technique, a verifier sends a random nonce to P and measures the time taken for P to reply back with this value. Assuming that communication is bounded by the speed of light, this

*Centrum Wiskunde & Informatica (CWI) and University of Amsterdam, The Netherlands. Email: Harry.Buhrman@cwi.nl.
†Department of Computer Science, UCLA, Los Angeles, CA, USA. Email: {nishanth, gelles}@cs.ucla.edu.
‡Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands. Email: {Serge.Fehr,Christian.Schaffner}@cwi.nl.
§Microsoft Research, Bangalore, India. Email: vipul@microsoft.com.
¶Department of Computer Science and Mathematics, UCLA, Los Angeles, CA, USA. Email: rafail@cs.ucla.edu.

technique gives an upper bound on the distance of P from the verifier. The problem of position-verification has been studied before in the field of wireless security, and there have been several proposals for this task. However, [CGMO09] shows that there exists no protocol for position-verification that offers security in the presence of *multiple colluding* adversaries. In other words, the set of verifiers cannot distinguish between the case when they are interacting with an honest prover at *pos* and the case when they are interacting with multiple colluding dishonest provers, none of whom are at position *pos*. Their impossibility result holds even if we make computational hardness assumptions, and it also rules out most other interesting position-based cryptographic tasks. On the positive side, they give a scheme which is secure under the (questionable) assumption that the adversaries cannot store a large amount of classical information. This leaves us with the following question—is there any other assumption or setting in which position-based cryptography is realizable?

2 Our Approach and Our Results

In this work, we study position-based cryptography in the *quantum* setting. This seems to be a promising approach; by going to the quantum setting, one may be able to circumvent the impossibility result due to the no-cloning principle. If some information is encoded into a quantum state, then the above attack fails because the adversary can either store the quantum state or send it to a colluding adversary (or do something in-between, like store part of it), but not both. However, this intuition turns out to be not completely accurate. Once the adversaries pre-share entangled states, they can make use of quantum teleportation [BBC$^+$93]. Although teleportation on its own does not appear to immediate conflict with the above intuition, we show that, based on techniques by Vaidman [Vai03], adversaries holding a large amount of entangled quantum states can successfully attack any position-based quantum scheme. We analyze our generic attack against an arbitrary 1-round position-verification scheme, but the attack works similarly against multi-round schemes. More generally, we prove a general result that any distributed quantum computation can be achieved in a single round of communication if the players start out with enough EPR pairs. Interestingly, pre-sharing entangled quantum systems is vital for attacking the position-verification scheme, because we show that otherwise, there exist schemes that are secure in the information-theoretic sense. If the adversary is not allowed any pre-shared entanglement, we show how to construct secure protocols for several position-based cryptographic tasks: position-verification, authentication, and key exchange. This leads to an interesting open question regarding the amount of pre-shared entanglement required to break the positioning scheme: the case of a large amount of pre-shared states yields a complete break of any scheme while having no pre-shared states leads to information-theoretically secure schemes. The threshold of pre-shared quantum systems that keeps the system secure is yet unknown.

3 Our Attack and our Schemes in More Detail

Position-Verification - A Simple Approach. Let us briefly discuss here the 1-dimensional case in which we have two verifiers V_0 and V_1, and a prover P at position *pos* that lies on the straight line between V_0 and V_1. Now, to verify P's position, V_0 sends a BB84 qubit $H^\theta|x\rangle$ to P, and V_1 sends the corresponding basis θ to P. The sending of these messages is timed in such a way that $H^\theta|x\rangle$ and θ arrive at position *pos* at the same time. P then has to measure the qubit in the given basis to obtain x, and immediately send x to V_0 and V_1, who verify the correctness of x and if it has arrived "in time". The intuition for this scheme is the following. Consider a dishonest prover $\hat{P}_0$ between V_0 and P, and a dishonest prover $\hat{P}_1$ between V_1 and P. (It is not too hard to see that additional dishonest provers do not help.) When $\hat{P}_0$ receives the BB84 qubit, she does not know yet the corresponding basis θ. Thus, if she measures it immediately when she receives it, then she is likely to measure it in the wrong basis and $\hat{P}_0$ and $\hat{P}_1$ will not be able to provide the correct x. However, if she waits until he knows the basis θ, then $\hat{P}_0$ and $\hat{P}_1$ will be too late in sending x to V_1 in time. Similarly, if she forwards the BB84 qubit to $\hat{P}_1$, who receives θ before $\hat{P}_0$ does, then $\hat{P}_0$ and $\hat{P}_1$ will be too late in sending x to V_0. It seems that in order to break the scheme $\hat{P}_0$ needs to store the qubit until she receives the basis θ and at the same time send a copy of it to $\hat{P}_1$. But this is impossible by no-cloning.

The Attack. The above intuition turns out to be wrong. Using pre-shared entanglement, $\hat{P}_0$ and $\hat{P}_1$ can perform quantum teleportation which enables them (in some sense) to act coherently on the complete state immediately upon reception. Although simply teleportating the BB84 qubit from $\hat{P}_0$ to $\hat{P}_1$ does not break

the scheme, because standard teleportation also requires $\hat{P}_0$ to send some classical information to $\hat{P}_1$, we show that based on ideas by Vaidman [Vai03], there exists a general attack which breaks *any* (1-round) position-verification scheme. In the attack, $\hat{P}_0$ and $\hat{P}_1$ teleport states back and forth many times in a clever way, *without* awaiting the classical measurement outcomes from the other party's teleportations.

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

Position-based authentication and key-exchange in the No-PE Model. Based on our position-verification scheme in the No-PE model, we show the existence of a position-based authentication scheme in the No-PE model. The goal of such an authentication scheme is be able to verify that a received message m was sent by a party at some specific position *pos*, and m was not tampered with during the transmission.

Given a position-based authentication scheme, one can immediately obtain a position-based key exchange scheme in the No-PE model 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.

4 Related Work

Recently, several papers on position-based quantum cryptography have been published on arXiv: [Mal10a, Mal10b, KMS10, Ken10, LL10]. Both papers [KMS10] and [LL10] show the insecurity of *certain* position-verification schemes (like the BB84-based scheme sketched in Section 3). None of the paper gives a *general* impossibility result. The papers [Mal10a, Mal10b, LL10] give constructions of position-verification schemes which they claim/conjecture secure, and [LL10] gives a security proof of the proposed scheme in a restricted setting. [KMS10] also proposes several constructions of position-verification schemes that are not subject to their attack, but no strong claims about their security is made. None of these papers addresses more enhanced position-based schemes, like authentication or key agreement. In [Ken10], Kent considers a different model for position-based cryptography where the prover is assumed to share with the verifiers a classical key unknown to the adversary. In this case, using this classical key stream as authentication resource, quantum key distribution can be used to expand that key ad infinitum. To clarify the historic picture, we note that a previous version of the present paper has been made public in May 2010 by a subset of the authors [CFG$^+$10]. After the appearance of [KMS10] we have realized that our schemes are merely secure against adversaries without pre-shared entanglement. In subsequent work, involving the full set of authors, we then developed the general impossibility result.

5 Impact on Quantum Information Theory

Position-based quantum cryptography is an exciting new area of quantum cryptography with implementable protocols that go beyond the well-known distribution of keys. Our general impossibility proof sets the borders of what is possible in this model. Our schemes give an idea of the kind of applications one can hope for—given realistic restrictions on the amount of entanglement the adversaries can handle. Rigorously proving security in the general case is a challenging open problem. We expect many interesting connections to entropic uncertainty relations, the limited-quantum-storage model, non-local games, parallel repetition and other areas in quantum information theory to arise from our work.

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.

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

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

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

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

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

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

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

[LL10] Hoi-Kwan Lau and Hoi-Kwong Lo. Insecurity of position-based quantum cryptography protocols against entanglement attacks. arXiv/quant-ph:1009.2256, Sep 2010.

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

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

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

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