The Garden-Hose Game
and Application to Position-Based Quantum Cryptography
(QIP 2012 Abstract)

Harry Buhrman*§, Serge Fehr*, Christian Schaffner$^{\S *}$, and Florian Speelman*§
**Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands*
§*University of Amsterdam (UvA), The Netherlands*

"No man ever steps in the same river twice, for it's not the same river and he's not the same man."
— Heraclitus of Ephesus

Background: Position-based (Quantum) 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*. The general concept of position-based cryptography was introduced by Chandran, Goyal, Moriarty and Ostrovsky [1].

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* $V_0, \dots, V_k$ (at different points in geographical space) that P is indeed at that position *pos*. The prover can run an interactive protocol with the verifiers in order to convince them. The main technique for such a protocol is known as distance bounding [2]. In this technique, a verifier sends a random nonce to P and measures the time taken for P to reply back with this value. Assuming that the speed of communication is bounded by the speed of light, this technique gives an upper bound on the distance of P from the verifier.

The problem of secure position-verification has been studied before in the field of wireless security, and there have been several proposals for this task ([2–9]). However, [1] shows that there exists no protocol for secure 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 which is at position *pos*.

The impossibility result of [1] relies heavily on the fact that an adversary can locally store all information he receives *and* at the same time share this information with other colluding adversaries, located elsewhere. Due to the no-cloning theorem, such a strategy will not work in the quantum setting, which opens the door to secure protocols that use quantum information. The quantum model was first studied by Kent et al. under the name of "quantum tagging" [10, 11]. Several schemes were developed [11–15] and proven later to be insecure. Finally in [16] it was shown that in general no unconditionally secure quantum position-verification scheme is possible. Any scheme can be broken using a double exponential amount of EPR pairs in the size of the messages of the protocol. Later, Beigi and König improved in [17] the double exponential dependence to single exponential making use of port-based teleportation [18, 19].

Due to the exponential overhead in EPR pairs, the general no-go theorem does not rule out the existence of quantum schemes that are secure for all practical purposes. Such schemes should have the property that the protocol, when followed honestly, is feasible, but cheating the protocol requires unrealistic amounts of resources, for example EPR pairs or time.

Analyzing the Beigi-König Scheme

To this end, Beigi and König [17] proposed a position-verification scheme using mutually unbiased bases. They showed that if the colluding parties are not allowed to send quantum, but only classical information to each other, then a linear amount of entanglement is necessary to break the scheme. They left open whether more entanglement was needed. As a first contribution, we close this gap and show that a linear number of EPR pairs is also *sufficient* to break the scheme.

An Interesting Class of Schemes

Furthermore, we consider a class of schemes that only involve a single qubit, and $2n$ classical bits. Such schemes were first considered by Kent et al. [11]. We focus on the one-dimensional set-up. The schemes easily generalize to three-dimensional space. The prover wants to convince the two verifiers, V_0 and V_1, that he is at position *pos* on the line in between them. V_0 sends a qubit $|\phi\rangle$ prepared in a random basis to P. In addition, V_0 sends a string $x \in \{0,1\}^n$ and V_1 a $y \in \{0,1\}^n$ to P. All messages are timed such that they arrive at the same time at P's claimed position. After receiving $|\phi\rangle, x$ and y, P computes a predetermined Boolean function $f(x,y)$.[1] He sends $|\phi\rangle$ to V_0 if $f(x,y) = 0$ and to V_1 otherwise. V_0 and V_1 check that they receive the correct qubit in time corresponding to *pos* and measure the received qubit in the basis corresponding to which it was prepared. In order to cheat the scheme, we imagine two provers P_0 and P_1 on either side of the claimed position *pos*, who try to simulate the correct behavior of an honest P at *pos*.

The attack described in [11] and the general no-go theorems from [16, 17] imply that there is a strategy for P_0 and P_1 such that they can accomplish the following. P_0 receives $|\phi\rangle, x$ and P_1 receives y. They are allowed to simultaneously send a single message to each other such that upon receiving that message they both know $f(x,y)$ and if $f(x,y) = 0$ then P_0 still has $|\phi\rangle$, otherwise P_1 has it in his possession. This teleportation-based cheating strategy however requires an exponential amount of EPR pairs (in n). We show in this paper that the number of EPR pairs required for such a protocol can be upper-bounded by a complexity measure that is related to the non-uniform space complexity of computing f. This complexity can sometimes be much smaller. For example, it follows that if $f(x,y)$ can be computed in logspace, then there is a cheating strategy that only requires a polynomial amount of entanglement. Our proof is inspired by *permutation branching programs* introduced by Barrington [20] and a general technique to make log-space computations reversible [21].

The motivation for considering this particular protocol for position-verification is the hope that for "complicated enough" functions $f(x,y)$, the amount of entanglement needed to successfully break the security of the protocol grows (at least) linearly in the bit length n of the classical strings x, y. If this intuition is true, it is a very interesting property of the protocol that we obtain a favorable relation between quantum and classical difficulty of operations in the following sense: if we increase the length of the classical inputs x, y, we require more *classical* computing power of the honest prover, whereas more *quantum* resources (in form of entangled states) are required by the adversary to break the protocol. Thus, the more classical resources the honest users use to faithfully execute the scheme, the more quantum resources the adversary needs in order to break it. To the best of our knowledge, such a trade-off has never been observed for a quantum-cryptographic protocol.

We give some first indications that the above may indeed be true. We show that if f is injective in x (meaning that $\forall x \neq x' \; \exists y : f(x,y) \neq f(x',y)$) or in y (defined accordingly), then for any attack that succeeds with certainty, the two dishonest provers require a joint quantum working space consisting of at least a logarithmic amount of qubits in n. Also, we show that if the entangled starting state for the dishonest provers is *fixed*, e.g. a list of EPR pairs, then there exists a function f for which the starting state must consist of at least linearly many qubits in n to allow for a perfect attack. Restricting to perfect attacks makes the claims rather weak from a cryptographic point of view; we hope that this can be improved in future work.

The Garden-Hose Complexity

In order to isolate the properties of attacks on these one-qubit schemes, we define a new model of communication complexity which we call the *garden-hose model.* Alice and Bob as usual have to compute a Boolean function $f(x,y)$. In order to do so they possess a number of water pipes that lay between them. Moreover, they each have additional pieces of hose that they can use to connect up the ends of the water pipes that are at their side. For example, Alice may choose to connect pipe 17 with 19 and pipe 28 with 687 etc. Bob connects up the ends of the pipes on his side. For each input they can use a different connection scheme. In order to compute the function, Alice in addition has a source of water

[1] We assume for simplicity that computation does not take any time.

that she connects to one of the the pipes on her side. She now opens the water tap. It is easy to see that the water will flow out on one side only. If this is Alice's then they proclaim the function value to be 0 otherwise the function value is 1. We define the garden-hose complexity of f to be the minimum number of pipes needed to compute f.

The garden-hose model links the number of EPR pairs sufficient to attack a quantum position-verification scheme to traditional complexity theory: the number of EPR pairs needed for a successful attack is upper bounded by the garden-hose complexity of f. Unfortunately, so far it is unclear whether the garden-hose complexity by any means gives a lower bound on the number of EPR pairs needed. If it does, then this gives a nice handle on proving security of such schemes based on complexity-theoretical assumptions. In order to have a practical scheme, we will need a function f in the complexity class P that has "large" garden-hose complexity. The existence of a function in P with super-polynomial garden-hose complexity will separate the complexity class P from LOGSPACE, which is a long standing open problem.

Beyond its connection to position-based quantum cryptography, we feel that the garden-hose complexity is interesting in its own right, and trying to understand its connections to other complexity measures appears like a challenging goal. In this paper we give some first answers, but many questions regarding the garden-hose complexity require further research.

Summary

In summary, the main results of this paper are the following:

- We show that a quantum position-verification protocol by Beigi and König [17] can be attacked with a linear amount of EPR pairs, establishing that their lower bound is optimal up to a constant factor.
- We study an interesting class of position-verification schemes that may have the following property: the more classical resources the honest users use to faithfully execute the scheme, the more quantum resources the adversary needs in order to break it. We give some first results towards proving this desirable property.
- We introduce a new model of communication complexity, called the garden-hose model. The model is an abstraction of certain types of attacks against the above class of position-verification schemes. As such, tools from classical communication complexity can be used to obtain upper bounds on the number of EPR pairs needed to break a given scheme.
- We prove almost-linear lower bounds in the garden-hose model for concrete functions like inner product, majority, and equality. We show that random functions have exponential garden-hose complexity.
- We establish that all functions computable in log space have polynomial garden-hose complexity. As a corollary, we obtain the following interesting connection between proving the security of quantum protocols and classical complexity theory: If there is an f in P such that there is no attack on our scheme using a polynomial number of EPR pairs, then P $\neq$ LOGSPACE.
- Our approach may lead to practical secure quantum position-verification schemes whose security is based on classical complexity-theoretical assumptions such as P is different from LOGSPACE.

[1] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, in *CRYPTO 2009* (Springer, 2009), pp. 391–407.
[2] S. Brands and D. Chaum, in *EUROCRYPT'93* (Springer, 1994), pp. 344–359, ISBN 3-540-57600-2.
[3] N. Sastry, U. Shankar, and D. Wagner, in *WiSe'03* (2003), pp. 1–10, ISBN 1-58113-769-9.
[4] A. Vora and M. Nesterenko, in *OPODIS'04* (2004), pp. 369–383.
[5] L. Bussard, Ph.D. thesis, Eurecom-ENST (2004).
[6] S. Capkun and J.-P. Hubaux, in *IEEE INFOCOM* (2005), pp. 1917–1928.
[7] D. Singelee and B. Preneel, in *IEEE MASS'10* (2005).
[8] Y. Zhang, W. Liu, Y. Fang, and D. Wu, IEEE Journal on Selected Areas in Communications **24**, 829 (2006).

[9] S. Capkun, M. Cagalj, and M. Srivastava, in *IEEE INFOCOM* (2006).

[10] A. Kent, W. Munro, T. Spiller, and R. Beausoleil, *Tagging systems* (2006), uS patent nr 2006/0022832.

[11] A. Kent, W. J. Munro, and T. P. Spiller, Phys. Rev. A **84**, 012326 (2011).

[12] R. A. Malaney, Phys. Rev. A **81**, 042319 (2010).

[13] N. Chandran, S. Fehr, R. Gelles, V. Goyal, and R. Ostrovsky (2010), arXiv:1005.1750v2.

[14] R. A. Malaney, *Quantum location verification in noisy channels* (2010), arXiv:1004.4689v1.

[15] H.-K. Lau and H.-K. Lo, Phys. Rev. A **83**, 012322 (2011).

[16] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, in *Advances in Cryptology CRYPTO 2011*, edited by P. Rogaway (Springer Berlin / Heidelberg, 2011), vol. 6841 of *Lecture Notes in Computer Science*, pp. 429–446, ISBN 978-3-642-22791-2.

[17] S. Beigi and R. König, arXiv:1101.1065v1 (2011), 1101.1065, URL `http://arxiv.org/abs/1101.1065`.

[18] S. Ishizaka and T. Hiroshima, Phys. Rev. Lett. **101**, 240501 (2008).

[19] S. Ishizaka and T. Hiroshima, Phys. Rev. A **79**, 042306 (2009).

[20] D. A. Barrington, Journal of Computer and System Sciences **164**, 150 (1989).

[21] K.-J. Lange, P. McKenzie, and A. Tapp, in *Proceedings of Computational Complexity. Twelfth Annual IEEE Conference* (IEEE Comput. Soc, 1997), pp. 45–50.