Device-independence for two-party cryptography and position verification

Jérémy Ribeiro,[1] Le Phuc Thinh,[1, 2] Jędrzej Kaniewski,[1, 3] Jonas Helsen,[1] and Stephanie Wehner[1]

[1] *QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands*
[2] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[3] *Department of Mathematical Sciences, University of Copenhagen,*
Universitetsparken 5, 2100 Copenhagen, Denmark

(Dated: April 29, 2016)

Quantum communication has demonstrated its usefulness for quantum cryptography far beyond quantum key distribution (QKD). One domain is two-party cryptography (2PC), whose goal is to allow two parties Alice and Bob to solve joint tasks, while protecting the honest party against the actions of a malicious one. Well-known examples of such tasks are oblivious transfer [1], bit commitment, secure identification and private information retrieval.

Another interesting application is position-based cryptography (PBC) whose goal is to use the geographical location of an entity as its (only) credential. At the heart of these is the task of position-verification (PV) where a person wants to convince the (honest) verifiers that she is located at a particular location. Quantum protocols for PV have been proposed that make use of quantum communication to enhance the security [2, 3]. We will refer to such protocols as quantum position-verification (QPV).

Unfortunately, it is impossible to achieve security for such tasks without making assumptions on the powers of the adversary, even using quantum communication [4–6]. This is in stark contrast to quantum key distribution where security against an all-powerful adversary (obeying the law of physics) is attainable. The reason can be traced back to a key difference between the two cryptographic tasks: while Alice and Bob can cooperate to check on the actions of an eavesdropper in QKD, in 2PC they do not trust each other and need to fend for themselves.

Nevertheless, due to the practical importance of 2PC one is willing to make assumptions in order to achieve security. Classically, one often relies on computational hardness assumptions such as the difficulty of factoring large numbers. However, as technology progresses the validity of such assumptions diminishes: it has been proven that factoring can be efficiently done on a quantum computer. An adversary can even retroactively break the security of a past execution of a cryptographic protocol. However, it has been realized that security can also be achieved from certain physical assumptions. The appeal of using physical instead of computational assumptions is that the assumptions only need to hold during the course of the protocol. That is, if the assumption is invalidated at a later point in time, security cannot be broken retroactively. Therefore, we are interested in the security of 2PC under physical constraints on the adversary's power.

If we allow quantum communication, one possible physical assumption is the bounded quantum-storage model [7, 8], and more generally the noisy-storage model [9, 10]. Here, the adversary is allowed to have an unlimited amount of classical storage, but his ability to store quantum information is limited. This is a relevant assumption since storing quantum information is hard. Significantly, however, security can always be achieved by sending more qubits than the storage device can handle. Specifically, If we assume that the adversary can store at most r qubits, then security can be achieved by sending n qubits, where $r \leq n - O(\log n)$ [9], which is essentially optimal since no protocol can be secure if $r \geq n$ [11, 12]. The corresponding quantum protocols require only very simple quantum states and measurements - and no quantum storage - to be executed by the honest parties, and their feasibility has been demonstrated experimentally [13, 14]. It is known that the noisy-storage model allows protocols for tasks such as oblivious transfer, bit commitment, as well as position-based cryptography [2, 6, 15, 16].

In all these security proofs, however, we assumed perfect knowledge of the quantum devices used in the protocol. That is, we know precisely what measurements the devices make, or what quantum states they prepare. Here, we present a general method to prove security for 2PC and PV, even if we only have limited knowledge of the quantum devices. Chiefly, we assume that the quantum devices function as black boxes, into which we can only give a classical input, and record a classical output. The classical input indicates the choice of a measurement that we would wish to perform, although we are not guaranteed that the device actually performs this measurement. The classical output can be understood as the outcome of that measurement. The classical processing itself is assumed to be verified and trusted. This idea of imagining black box devices is known as device-independent (DI) quantum cryptography [17–20]. There is a large body of work in DI quantum key distribution (see e.g. [21–23]), but in contrast there is hardly any work in DI 2PC. A protocol has been proposed by Silman [24] for bit commitment which does not make physical assumptions, and hence only achieved a very weak primitive. First steps towards DI PV have also been made in [25], and for one-sided DI in [15].

	arXiv:1601.06752	**arXiv:soon**
Bound on P_{guess}	$d\left(\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1+\zeta}{2}}\right)^n$	$\sqrt{d}\left(\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1+\zeta}{2}}\right)^n - o(\cdot)$
Adversary memory	reduction to classical adversary	deals with the memory directly
Jordan's lemma	not used	reduction of dimensionality thanks to Jordan's lemma
Absolute effective anti-commutator	used	used

Table I: Comparison of the proof techniques in the two papers joined for this submission. Our new work relates the security directly to the entanglement cost of the adversary's storage channel, however, we borrow concepts on how to test our quantum devices from our earlier work. Security is possible whenever $P_{\text{guess}} < 2^{-\gamma n}$ for some $\gamma > 0$, which depends on the dimension d of the adversary's storage device as well as the parameter ζ estimated during the Bell test (see below). Our new analysis allows security even for a storage device that is twice as large.

I. RESULTS

Here, we present a general method for proving the DI cryptography for two-party cryptography and position-verification. Specifically, we give the first device independent security proof of two-party cryptography and position verification in the noisy-storage model. We accomplish this by introducing an appropriate model for DI in these settings, and subsequently studying a general "guessing game" that can be related to both tasks. To obtain DI security, we perform a Bell test on a subset of the devices. It is an appealing feature of our analysis that security can be attained for any violaton of a Bell's inequality. Our proof method relates the security of the protocols to the entanglement cost of the adversary's quantum storage device, which means we can achieve security against an adversary with a much larger storage device than methods based on reducing to a classical adversary. While the adversary can be fully general during the course of the protocol, we assume in this first work that the devices he prepared earlier are memoryless.

Achieving DI security for 2PC and PV presents us new challenges which require a different approach than what is known from QKD.

1. In QKD Alice and Bob are always honest, while Eve is always trying to break the protocol. In DI QKD it is therefore natural to give the power to prepare the devices to Eve. Analogously, we will assume here that all the devices used in the protocol are always prepared by the dishonest party.

2. In the following section we will see that the protocol we start with uses quantum communication between Alice and Bob. This means that the adversary who prepared the devices will receive *quantum communication* coming back from the devices. This is in sharp contrast to DI QKD, in which Eve prepares the devices – with which she is possibly entangled – and then Alice and Bob simply push buttons on the devices to perform measurements. That is, there is no quantum communication going back to Eve. This feature introduces a significant difference between the security analysis of DI QKD and the DI two-party cryptography protocol considered here and requires us to develop novel proof techniques.

To analyze 2PC protocols, we focus on the simpler primitive of Weak String Erasure (WSE) [10], which can in turn be used to implement bit commitment using classical communication. WSE is a two-party protocol (we call the two protagonists Alice and Bob) whose goal is that at the end of its execution Alice holds a random bit string $x \in \{0,1\}^n$ and Bob holds a random substring of x called $x_{\mathcal{I}}$, where $\mathcal{I}$ is the set of indexes corresponding to the bit form x that are in $x_{\mathcal{I}}$. WSE is secure for a honest Bob if Alice cannot get the set $\mathcal{I}$, and for a honest Alice if it is hard for Bob to guess the entire string x. The security for the honest Bob is trivial, but for a honest Alice we prove that,

- **WSE** is secure against an adversary (Bob) who holds a noisy storage device and who is allowed to create the honest party's devices (but these devices have to be memoryless).

To obtain secure PV, we use the fact that the security of WSE can be used to analyze the security of Quantum Position Verification. In QPV there are three protagonists in the honest case: two are called verifiers (V_1 and V_2) and one is called the prover (P). The prover claims to be at some geographical position, and the QPV protocol permits to prove whether or not he is at his claimed location (For simplicity we restrict to one physical dimension). The prover receive two messages from the verifiers, as to perform some operation and reply within a certain time. As a signal cannot travel faster than light the time constraint, constrains the prover's position.

Then a dishonest prover alone cannot cheat on this protocol (he cannot reply on time to both verifiers). But

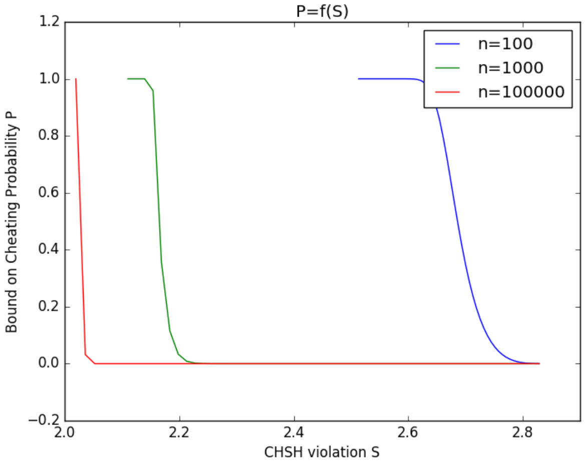

Figure 1: Security is possible for any violation of the CHSH inequality, but depending on the violation we need to send a larger number of qubits n.

if we assume the existence of two cheaters who together impersonate a single prover there exists a general attack on the protocol [6]. This attack however requires an exponential amount of entanglement with respect to the amount of quantum information they receive from verifiers. Moreover we can assume without loss of generality that there are at most two provers.

As the security on QPV can be reduced to the security of WSE, we prove that

- **QPV** is secure against adversaries who share a "noisy" entangled state and who cannot use quantum communication but are allowed to create the honest party's devices (these devices have to be memoryless).

II. METHODS

In order to prove DI security for Weak String Erasure and for Quantum Position Verification, we analyse a related guessing game. This guessing game is a two-party game whose players are Alice and Bob. Bob is allowed to create the two devices Alice will use (Fig. 2). Alice can only input classical information in her devices. However Alice can use these two devices to perform a Bell test (CHSH game). This Bell test certifies the quality of the devices. After having tested her devices, Alice uses the main device to prepare a bipartite (arbitrary) state and measures a half of it by inputting $\theta \in \{0,1\}^n$ in her main device, gets an outcome $x \in \{0,1\}^n$, and sends the other part of the quantum system to Bob. Later she sends him the input she used to perform her measurements. When Bob has received all information he has to guess Alice's measurement outcome x. If Bob is all powerful then he can guess x: he just has to store the quantum system until he receives the bases θ and then he can measure his system in those bases. That's why we analyse the case where Bob is limited to storing a finite amount of quantum information: we bound the dimension of his quantum memory by d (or in the noisy storage model, we bound the entanglement cost of his memory by d).

In order to find a bound on Bob's winning probability, we needed to assume that all devices used by Alice are memoryless (memoryless hypothesis), so they behave in the same way each time Alice uses them. This implies that Alice's measurement operators are a tensor product of binary measurement operators, the state she prepares has also a tensor product form. This memoryless hypothesis also permits Alice to perform the Bell test before the actual guessing game, and from this test, to estimate an upper bound $\zeta := \frac{S}{4}\sqrt{8-S^2}$ on a quantity we call the effective absolute anti-commutator of Alice's measurement noted ϵ_+, where S is the left hand side of the Bell's inequality (CHSH): $S \leq 2$.

- **Main technical result:** Assuming Alice's devices have memoryless behavior, and Bob has a noisy storage device, there is a DI upper-bound on the success probability of Bob in the guessing game, which decays exponentially in n, the length of Alice's measurement outcomes $x \in \{0,1\}^n$. This bound holds for any Bell violation, *i.e.* $\forall S \in]2, 2\sqrt{2}]$ (see Fig. 1).

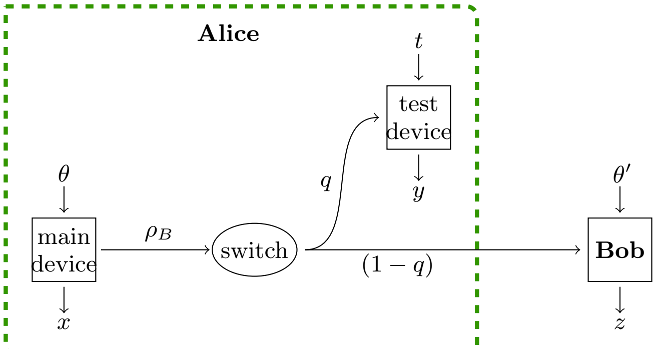

Figure 2: The main device prepares a bipartite state ρ_{AB}, ρ_A is measured by the main device according to $\theta \in \{0,1\}^n$ randomly chosen and get $x \in \{0,1\}^n$. The other part ρ_B of the state is sent to a switch that Alice controls. This switch splits the state ρ_B in two parts: one is sent to the testing device (with probability q), to test the devices, and the other is sent to Bob to play the guessing game. Bob wins if $z = x$.

[1] M. O. Rabin., Technical Report TR-81 .

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

[3] R. A. Malaney, Phys. Rev. A **81**, 042319 (2010), arXiv:1003.0949 [quant-ph].

[4] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).

[5] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).

[6] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, SIAM Journal on Computing **43**, 150 (2014), http://dx.doi.org/10.1137/130913687.

[7] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner, "Advances in cryptology - crypto 2007: 27th annual international cryptology conference, santa barbara, ca, usa, august 19-23, 2007. proceedings," (Springer Berlin Heidelberg, Berlin, Heidelberg, 2007) Chap. Secure Identification and QKD in the Bounded-Quantum-Storage Model, pp. 342–359.

[8] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner, BRICS Report Series **12** (2005), 10.7146/brics.v12i20.21886.

[9] F. Dupuis, O. Fawzi, and S. Wehner, IEEE Transactions on Information Theory **61**, 1093 (2015).

[10] R. Konig, S. Wehner, and J. Wullschleger, IEEE Transactions on Information Theory **58**, 1962 (2012).

[11] D. Mayers, Phys. Rev. Lett , 3414 (1997).

[12] H. kwong Lo and H. F. C. L, in *Ideal Quantum Coin Tossing Are Impossible, Los Alamos Preprint Archive, http://xxx.lanl.gov/abs/quant-ph/9711065*.

[13] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs, Nature Communications **5**, 3418 (2014), arXiv:1308.5098 [quant-ph].

[14] N. H. Y. Ng, S. K. Joshi, C. Chen Ming, C. Kurtsiefer, and S. Wehner, Nature Communications **3**, 1326 (2012), arXiv:1205.3331 [quant-ph].

[15] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner, New Journal of Physics **15**, 103002 (2013), arXiv:1210.4359 [quant-ph].

[16] J. Ribeiro and F. Grosshans, arXiv:1504.07171 (2015).

[17] D. Mayers and A. Yao, Quantum Info. Comput. **4**, 273 (2004).

[18] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, Phys. Rev. Lett. **98**, 230501 (2007).

[19] J. Barrett, R. Colbeck, and A. Kent, Phys. Rev. A **86**, 062326 (2012).

[20] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[21] U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).

[22] J. Barrett, R. Colbeck, and A. Kent, Phys. Rev. A **86**, 062326 (2012), arXiv:1209.0435 [quant-ph].

[23] B. W. Reichardt, F. Unger, and U. Vazirani, ArXiv e-prints (2012), arXiv:1209.0448 [quant-ph].

[24] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar, Phys. Rev. Lett. **106**, 220501 (2011).

[25] A. Kent, Phys. Rev. A **84**, 022335 (2011).