Device-independent two-party cryptography

Jędrzej Kaniewski,[1,2] Thomas Vidick,[3] and Stephanie Wehner[1,2]

[1] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[2] *QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, the Netherlands*
[3] *Department of Computing and Mathematical Sciences,*
California Institute of Technology, Pasadena, CA, USA

(Dated: June 28, 2015)

Device-independent information processing has received a lot of attention recently, mainly in the context of randomness expansion [CK10, VV12, CVY13, BPPP14, MS14] and quantum key distribution (QKD) [BHK05, AGM06, ABG+07, BCK13, VV14]. In these two cases the power of device-independent protocols and the limitations they come with are reasonably well understood. Another important branch of cryptography considers the scenario in which two potentially mistrustful parties want to interact to perform a certain task while revealing as little private information as possible. This is known under the name of two-party (or mistrustful) cryptography and it includes many realistic tasks like coin tossing [Blu81] or private information retrieval [CGKS98].

Quantum information theory does not allow to perform such tasks securely against an all-powerful adversary. One solution is to relax the security requirements (i.e. allow each party a fixed, non-vanishing cheating probability) and device-independent protocols in this setting for bit commitment and coin tossing have been proposed [SCA+11]. Alternatively, one might construct protocols which give (essentially) perfect security against technologically limited adversaries, e.g. whose quantum storage is bounded [DFSS05, DFR+07] or more generally noisy [WST08]. Oblivious transfer was shown to be a basic building block for two-party cryptography, out of which other primitives of interest can be constructed [Kil88]. We consider another universal primitive called *weak string erasure* [KWW12]. In weak string erasure Alice and Bob interact to produce a random string of bits such that if they both follow the protocol Alice knows the entire string, while Bob only knows a subset of the bits. Security for Alice means that Bob should not be able to guess the entire string, while security for Bob means that Alice should not know which bits are known to him.

Protocols implementing weak string erasure using trusted devices in the noisy storage model were proposed in Ref. [WST08]. Given the similarity of this task to randomness generation and recent results on device-independent quantum key distribution, a natural question arises of whether two-party cryptography can be made device-independent or, on a more technical level, whether techniques developed for QKD can be adapted to the two-party world. Note that the two-party scenario is conceptually slightly more complicated than the QKD scenario in the following sense. In QKD there are two honest parties who always follow the protocol and there is a third party which chooses the best cheating strategy available. In the two-party setting there are only two parties (as the name suggests) but we need to consider separately the case in which (a) they are both honest (then, the protocol should terminate and produce the desired output) and (b) one of the parties attempts to cheat (then, the protocol should protect the privacy of the honest party).

In this submission we propose a protocol implementing device-independent weak string erasure and prove its security in the bounded storage model under two extra assumptions:

- We assume that the devices are memoryless, i.e. they behave in the same way every time they are used.
- We assume that the dishonest party (Bob) performs a collective attack, i.e. attacks each round independently.

At the beginning Bob prepares two quantum devices sharing a large number of EPR pairs, which he passes to Alice. Each device has two buttons corresponding to the perfect CHSH [CHSH69] measurements. She tests the devices by playing the CHSH game multiple times and if the observed violation is high enough she uses one of them to produce randomness by performing a fixed number of measurements where the basis is chosen uniformly at random for every round. The other device is passed to Bob who guesses at random which measurement Alice is going to perform and performs the corresponding measurement on his system. Once Alice announces the basis information, he knows that in certain rounds (where he has guessed her basis choice correctly) they share perfect correlations (this is the set he is allowed to learn) but the rest of the string he will be fully ignorant about. This shows that the protocol is correct. Security for honest Bob is quite straightforward: since Alice receives nothing during the protocol she has no knowledge about which bits of her string Bob successfully learnt. Security for honest Alice is more difficult to prove but the intuition is as follows. Perfect cheating would be possible if Bob could store the entire quantum system until Alice announces the basis information. However, since we work in the bounded storage model, he is unable do so and he is forced to make some partial measurement before he learns the basis information. Since the measurements performed by Alice are incompatible (they can be used to observe a certain CHSH violation) their results cannot be predicted without quantum memory. This results in some amount of uncertainty which is exactly the security requirement for honest Alice. More specifically, we show that the amount of uncertainty grows linearly in the number of rounds played by Alice and we also find a lower bound on the amount of uncertainty *per round* as a function of the observed CHSH violation. Last but not least, we provide first steps towards a proof of security against more general attacks of Bob and, finally, devices with memory.

[ABG$^+$07] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-Independent Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.*, 98(23): 230501, 2007.
DOI: 10.1103/PhysRevLett.98.230501.

[AGM06] A. Acín, N. Gisin, and L. Masanes. From Bell's Theorem to Secure Quantum Key Distribution. *Phys. Rev. Lett.*, 97(12): 120405, 2006.
DOI: 10.1103/PhysRevLett.97.120405.

[BCK13] J. Barrett, R. Colbeck, and A. Kent. Memory attacks on device-independent quantum cryptography. *Phys. Rev. Lett.*, 110(1): 010503, 2013.
DOI: 10.1103/PhysRevLett.110.010503.

[BHK05] J. Barrett, L. Hardy, and A. Kent. No signaling and quantum key distribution. *Phys. Rev. Lett.*, 95(1): 010503, 2005.
DOI: 10.1103/PhysRevLett.95.010503.

[Blu81] M. Blum. Coin Flipping by Telephone. *Proc. 1st CRYPTO*, 1981.

[BPPP14] J. Bouda, M. Pawłowski, M. Pivoluska, and M. Plesch. Device-independent randomness extraction for arbitrarily weak min-entropy source. *Phys. Rev. A*, 032313, 2014.
DOI: 10.1103/PhysRevA.90.032313.

[CGKS98] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan. Private information retrieval. *Journal of the ACM*, 45(6): 965–982, 1998.
DOI: 10.1145/293347.293350.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15): 880–884, 1969.
DOI: 10.1103/PhysRevLett.23.880.

[CK10] R. Colbeck and A. Kent. Private Randomness Expansion With Untrusted Devices. *J. Phys. A*, 095305: 11, 2010.
DOI: 10.1088/1751-8113/44/9/095305.

[CVY13] M. Coudron, T. Vidick, and H. Yuen. Robust randomness amplifiers: Upper and lower bounds. 2013.
arXiv: 1305.6626.

[DFR$^+$07] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner. A Tight High-Order Entropic Quantum Uncertainty Relation with Applications. *Proc. 27th CRYPTO*, pages 360–378, 2007.

[DFSS05] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography In the Bounded Quantum-Storage Model. *Proc. 46th IEEE FOCS*, pages 449 – 458, 2005.
DOI: 10.1109/SFCS.2005.30.

[Kil88] J. Kilian. Founding Cryptography on Oblivious Transfer. *Proc. 20th ACM STOC*, pages 20–31, 1988.
DOI: 10.1145/62212.62215.

[KWW12] R. König, S. Wehner, and J. Wullschleger. Unconditional Security From Noisy Quantum Storage. *IEEE Trans. Inf. Theory*, 58(3): 1962–1984, 2012.
DOI: 10.1109/TIT.2011.2177772.

[MS14] C. A. Miller and Y. Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. *Proc. 46th ACM STOC*, pages 417–426, 2014.
DOI: 10.1145/2591796.2591843.

[SCA$^+$11] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar. Fully Distrustful Quantum Bit Commitment and Coin Flipping. *Phys. Rev. Lett.*, 106(22): 220501, 2011.
DOI: 10.1103/PhysRevLett.106.220501.

[VV12] U. Vazirani and T. Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. *Proc. 44th ACM STOC*, pages 61–76, 2012.
DOI: 10.1145/2213977.2213984.

[VV14] U. Vazirani and T. Vidick. Fully Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.*, 113(14): 140501, 2014.
DOI: 10.1103/PhysRevLett.113.140501.

[WST08] S. Wehner, C. Schaffner, and B. Terhal. Cryptography from Noisy Storage. *Phys. Rev. Lett.*, 100(22): 220502, 2008.
DOI: 10.1103/PhysRevLett.100.220502.