Unconditionally secure device-independent quantum key distribution with only two devices[*]

Jonathan Barrett, Roger Colbeck, and Adrian Kent

(Dated: 3rd October 2012)

Device-independent quantum key distribution is the task of using uncharacterized quantum devices to establish a shared key between two users. If a protocol is secure regardless of the device behaviour, it can be used to generate a shared key even if the supplier of the devices is malicious. To date, all device-independent quantum key distribution protocols that are known to be secure require separate isolated devices for each entangled pair, which is a significant practical limitation. We introduce a protocol that requires Alice and Bob to have only one device each. Although inefficient, our protocol is unconditionally secure against an adversarial supplier limited only by locally enforced signalling constraints.

Key distribution is the task of establishing shared secret strings between two parties, and is sufficient for secure communication. Classical key distribution protocols base their security on assumptions about an eavesdropper's computational or technological power. On the other hand, quantum key distribution protocols (e.g. [2, 3]) promise security against an arbitrarily powerful eavesdropper, and do so in the presence of realistic noise levels. However, in order for the security proofs to apply, the devices must operate according to certain specifications. Deviations from these can introduce security flaws, which can be difficult to identify (see e.g. [4] for practical illustrations of such attacks).

The difficulty associated with verifying the operation of quantum devices has led to much interest in device-independent quantum cryptography protocols. Ideally, such protocols guarantee security by tests on the outputs of the devices: no specification of their internal functionality is required. In a sense, the protocol verifies the devices' security *on-the-fly*.

Device-independent cryptography was first introduced by Mayers and Yao [5] (albeit under a different name) and the first quantum key distribution protocol to be proven device-independently secure was the Barrett-Hardy-Kent (BHK) protocol [6]. The BHK security proof applies not only against an arbitrarily powerful quantum eavesdropper (who also supplies the devices) but even against an eavesdropper and device-supplier who has discovered and makes use of any post-quantum physical theory, provided that, within the theory, the honest parties can enforce local signalling

[*] An online technical version of this work is available at [1]

constraints. The applicability of the BHK protocol and proof to device-independent quantum cryptography was explicitly pointed out by later authors, who went on to develop some more efficient device-independent protocols with security proofs against restricted eavesdroppers [7–9] as well as other protocols shown to be unconditionally secure [10–14].

From a theoretical perspective, the BHK protocol provided an existence theorem for a task that had not been known to be possible. Practically, however, it has drawbacks. One is that, as formulated, it generates only a single bit of secure key. Although it can be modified using an idea from [15] to produce an arbitrarily long key, even with this modification, the protocol is inefficient and unable to tolerate reasonable levels of noise.

A serious practical problem with all the protocols with proven unconditional device-independent security [6, 10, 13, 14] is that they require that each (purportedly) entangled pair used in the protocol is isolated from the others. The protocols thus require a separate and isolated pair of devices for each entangled pair to ensure full device-independent security. This evidently makes such protocols costly to implement in practice.

We introduce here a protocol that evades this limitation, requiring only a single device for each user. Our protocol is a refinement of the BHK protocol, necessary in order to allow security when used with only two devices. As we have discussed elsewhere [16], the composability of device independent protocols is problematic if devices are reused in subsequent implementations. Here we show that if devices are not reused, then our protocol is secure according to a universally composable security definition, even against an adversary who supplies the devices and is restricted only by signalling constraints. As described, our protocol generates a single secure key bit. We also indicate how it can be modified using the idea in [15], to produce a key of arbitrary length. In addition, since it is composable, further key bits can be generated by running the protocol several times (although in this case, fresh devices are required for each run).

We see the value of our protocol as an existence theorem showing that device-independent quantum key distribution *is* in principle possible with only two devices. Whether this task can be achieved more efficiently and with reasonable noise tolerance remains (as far as we are aware) an open question.

We also show that some apparently natural extensions of existing efficient and noise-tolerant protocols to two devices are insecure against eavesdroppers restricted only by signalling constraints, and in some cases also against quantum eavesdroppers. This is significant within a recent line of work on the impossibility of privacy amplification against non-signalling eavesdroppers [17, 18], since privacy amplification is a key tool used to make the protocols more efficient.

In [17], the two-device case was considered for protocols based on CHSH correlations. There it was shown that privacy amplification via hashing is not possible against an adversary limited only by the impossibility of signalling between the parties. However, in [17], signalling was permitted within the devices (so that outputs could depend on later inputs). (Although, as currently described, this is unphysical, it is natural to consider this for protocols in which each party makes all their inputs at the start, and then receives all of their outputs together.) For protocols in which each party waits for an output before giving their next input, the most natural signalling constraints are ones that allow later outputs to depend on all previous inputs, but do not allow outputs to depend on future inputs (we call these *time-ordered non-signalling conditions*). A situation that is close to this case (but with subtle and potentially important differences) has been recently studied in [18]. There protocols based on CHSH correlations were again considered, and it was shown that privacy amplification via hashing is not possible for adversaries limited by "almost" time-ordered non-signalling conditions.

We show that privacy amplification is not possible against adversaries limited by time-ordered non-signalling conditions if one bit of information passes from the devices to the adversary. Roughly, one could think of this as the non-signalling conditions are violated by one bit. Although any literal violation is physically unreasonable, if Alice and Bob want to test their devices in some way (as is usually the case), then they need to communicate some of the device outputs, and this provides a channel enabling this single bit to get to Eve and compromise security.

Remark: In some concurrent work an alternative technique for proving security of device-independent QKD with two devices has been suggested [19].

[1] Barrett, J., Colbeck, R. & Kent, A. Unconditionally secure device-independent quantum key distribution with only two devices. e-print `arXiv:1209.0435` (2012).

[2] Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, 175–179. IEEE (New York, 1984).

[3] Ekert, A. K. Quantum cryptography based on Bell's theorem. *Physical Review Letters* **67**, 661–663 (1991).

[4] Gerhardt, I. *et al.* Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Communications* **2**, 349 (2011).

[5] Mayers, D. & Yao, A. Quantum cryptography with imperfect apparatus. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS-98)*, 503–509 (IEEE Computer Society,

Los Alamitos, CA, USA, 1998).

[6] Barrett, J., Hardy, L. & Kent, A. No signalling and quantum key distribution. *Physical Review Letters* **95**, 010503 (2005).

[7] Acin, A., Gisin, N. & Masanes, L. From Bell's theorem to secure quantum key distribution. *Physical Review Letters* **97**, 120405 (2006).

[8] Scarani, V. *et al.* Secrecy extraction from no-signaling correlations. *Physical Review A* **74**, 042339 (2006).

[9] Acin, A. *et al.* Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters* **98**, 230501 (2007).

[10] Masanes, L. *et al.* Unconditional security of key distribution from causality constraints. e-print `quant-ph/0606049v4` (2009).

[11] Masanes, L. Universally composable privacy amplification from causality constraints. *Physical Review Letters* **102**, 140501 (2009).

[12] Hänggi, E., Renner, R. & Wolf, S. Quantum cryptography based solely on Bell's theorem. In Gilbert, H. (ed.) *Proceedings of the 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt'10)*, 216–234 (Springer, 2010). Also available `arXiv:0911.4171`.

[13] Hänggi, E. & Renner, R. Device-independent quantum key distribution with commuting measurements. e-print `arXiv:1009.1833` (2010).

[14] Masanes, L., Pironio, S. & Acín, A. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature Communications* **2**, 238 (2011).

[15] Barrett, J., Kent, A. & Pironio, S. Maximally non-local and monogamous quantum correlations. *Physical Review Letters* **97**, 170409 (2006).

[16] Barrett, J., Colbeck, R. & Kent, A. Prisoners of their own device: Trojan attacks on device-independent quantum cryptography. e-print `arXiv:1201.4407` (2012).

[17] Hänggi, E., Renner, R. & Wolf, S. The impossibility of non-signalling privacy amplification. e-print `arXiv:0906.4760` (2009).

[18] Friedman, R. A., Hänggi, E. & Ta-Shma, A. Towards the impossibility of non-signalling privacy amplification from time-like ordering constraints. e-print `arXiv:1205.3736` (2012).

[19] Reichardt, B. W., Unger, F. & Vazirani, U. Classical command of quantum systems via rigidity of CHSH games. e-print `arXiv:1209.0449` (2012).