Memory attacks on device-independent quantum cryptography*

Jonathan Barrett,[1,†] Roger Colbeck,[2,3,‡] and Adrian Kent[4,3,§]

[1] *Department of Mathematics, Royal Holloway, University of London, Egham Hill, Egham, TW20 0EX, U.K.*
[2] *Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland*
[3] *Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada.*
[4] *Centre for Quantum Information and Foundations, DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WA, U.K.*

(Dated: 20th May 2012)

Device-independent quantum cryptographic schemes aim to guarantee security to users based only on the output statistics of any components used, and without the need to verify their internal functionality. Since this would protect users against untrustworthy or incompetent manufacturers, sabotage or device degradation, this idea has excited much interest, and many device-independent schemes have been proposed. Here we identify a critical weakness of device-independent quantum cryptographic protocols that rely on public communication between secure laboratories. Untrusted devices may record their inputs and outputs and reveal information about them via publicly discussed outputs during later runs. Reusing devices thus compromises the security of a protocol and risks leaking secret data. Possible defences include securely destroying or isolating used devices. However, these are costly and often impractical. We briefly consider other possible defences available in scenarios where device reuse is restricted.

Quantum cryptography aims to exploit the properties of quantum systems to ensure the security of various tasks. The best known example is quantum key distribution (QKD), which can enable two parties to share a secret random string and thus exchange messages secure against eavesdropping, and we mostly focus on this task for concreteness. While all classical key distribution protocols rely for their security on assumed limitations on an eavesdropper's computational power, the advantage of quantum key distribution protocols (e.g. [2, 3]) is that they are provably secure against an arbitrarily powerful eavesdropper, even in the presence of realistic levels of losses and errors [4]. However, the security proofs require that quantum devices function according to particular specifications. Any deviation – which might arise from a malicious or incompetent manufacturer, or through sabotage or degradation – can introduce exploitable security flaws (see e.g. [5] for practical illustrations).

The possibility of quantum devices with deliberately concealed flaws, introduced by an untrustworthy manufacturer or saboteur, is particularly concerning, since (i) it is easy to design quantum devices that appear to be following a secure protocol but are actually completely insecure, and (ii) there is no general technique for identifying all possible security loopholes in standard quantum cryptography devices. This has led to much interest in device-independent quantum protocols, which aim to guarantee security *on the fly* by testing the device outputs [6–16]: no specification of their internal functionality is required.

Known provably secure schemes for device-independent quantum key distribution are inefficient, as they require either independent isolated devices for each entangled pair to ensure device-independent security [7, 11–13], or a large number of entangled pairs to generate a single bit [7, 17]. Finding an efficient secure device-independent quantum key distribution scheme using two (or few) devices has remained an open theoretical challenge. Nonetheless, in the absence of tight theoretical bounds on the scope for device-independent quantum cryptography, progress to date has encouraged optimism (e.g. [18]) about the prospects for device-independent QKD as a practical technology, as well as for device-independent quantum randomness expansion [14–16] and other applications of device-independent quantum cryptography (e.g. [19]).

However, one key question has been generally neglected in work to date on device-independent quantum cryptography, namely what happens if and when devices are reused. Specifically, are device-reusing protocols *composable* – i.e. do individually secure protocols of this type remain secure when combined? It is clear that reuse of untrusted devices cannot be *universally composable*, i.e. such devices cannot be securely reused for completely general purposes. However, for device-independent quantum cryptography to have significant practical value, one would hope that devices can at least be reused for the same purpose. For example one would like to be able to implement a QKD protocol many times, with a guarantee that all the generated keys can be securely used in an arbitrary environment so long as the devices are kept secure. We focus on this type of composability here.

We describe a new type of attack that highlights pitfalls in producing protocols that are composable (in the above sense) with device-independent security for reusable devices, and show that for all known protocols such composability fails in the strong sense that purportedly secret data become completely insecure. In short,

*A more detailed version of this work can be found at [1].

†Electronic address: jon.barrett@rhul.ac.uk
‡Electronic address: colbeck@phys.ethz.ch
§Electronic address: a.p.a.kent@damtp.cam.ac.uk

the problem is that a malicious adversary can program devices to store data in one protocol and leak it in subsequent protocols, in ways that are hard or impossible to counter if the devices are indeed reused. The leaks do not exploit new side channels (which proficient users are assumed to block), but instead occur through the device choosing its outputs as part of a later protocol.

To illustrate this, consider a device-independent scheme that allows two users (Alice and Bob) to generate and share a purportedly secure cryptographic key. A malicious manufacturer (Eve) can design devices so that they record and store all their inputs and outputs. A well designed device-independent protocol can prevent the devices from leaking information about the generated key *during that protocol*. However, data about these inputs and outputs, and hence about the secure key, can be leaked *whenever the devices are later used*. The devices can make their outputs in later runs depend on the inputs and outputs of earlier runs, and the protocol then requires Alice and Bob to publicly exchange at least some information about these later outputs, so communicating data about the original key to Eve. Moreover, in many existing protocols, such leaks can be surreptitiously hidden in the noise. This allows the devices to operate indefinitely like hidden spies, apparently complying with security tests, but actually eventually leaking all the purportedly secure data.

We stress that our results do not imply that quantum key distribution *per se* is insecure or impractical. In particular, our attacks do not apply to standard QKD protocols in which the devices' properties are fully trusted, nor if the devices are trusted to be memoryless (but otherwise untrusted), nor necessarily to protocols relying on some other type of partially trusted devices. Our target is the possibility of (full) device-independent quantum cryptographic security, applicable to users who purchase devices from a potentially sophisticated and adversarial supplier and rely on no assumption about the devices' internal workings. We show that, without further restriction on device reuse, device-independent composable security is not attainable by any of the methods proposed thus far.

We also discuss some possible partial defences and counter-measures against our attacks. A theoretically simple one is to dispose of – i.e. securely destroy or isolate – untrusted devices after a single use. While this would restore universal composability, it is clearly costly and would severely limit the practicality of device-independent quantum cryptography. Another interesting possibility is to try to design protocols for device-independent QKD guaranteed secure for some fixed large number of device reuses, or to study protocols for device-independent tasks that are secure in some weaker sense. These and other defences could be valuable in some scenarios, and many interesting questions remain open. Nonetheless, in our view, the attacks we have described merit a serious reappraisal of the practical possibilities of quantum cryptography using completely untrusted devices.

Acknowledgements

We thank Anthony Leverrier and Gonzalo de la Torre for [20], Lluís Masanes, Serge Massar and Stefano Pironio for helpful comments. AK was partially supported by a Leverhulme Research Fellowship, a grant from the John Templeton Foundation, and the EU Quantum Computer Science project (contract 255961). This work was supported by the CHIST-ERA DIQIP project. Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation.

[1] Barrett, J., Colbeck, R. & Kent, A. Prisoners of their own device: Trojan attacks on device-independent quantum cryptography. e-print `arXiv:1201.4407` (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] Renner, R. *Security of Quantum Key Distribution*. Ph.D. thesis, Swiss Federal Institute of Technology, Zurich (2005). Also available as `quant-ph/0512258`.

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

[6] 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).

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

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

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

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

[11] Masanes, L., Renner, R., Christandl, M., Winter, A. & Barrett, J. Unconditional security of key distribution from causality constraints. e-print `quant-ph/0606049v4` (2009).

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

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

[14] Colbeck, R. *Quantum and Relativistic Protocols For Secure Multi-Party Computation*. Ph.D. thesis, University of Cambridge (2007). Also available as `arXiv:0911.3814`.

[15] Pironio, S. *et al.* Random numbers certified by Bell's theorem. *Nature* **464**, 1021–1024 (2010).

[16] Colbeck, R. & Kent, A. Private randomness expansion with untrusted devices. *Journal of Physics A* **44**, 095305 (2011).

[17] Barrett, J., Colbeck, R. & Kent, A. in preparation (2012).

[18] Ekert, A. Less reality, more security. *Physics World* (2009).

[19] Silman, J. *et al.* Fully distrustful quantum bit commitment and coin flipping. *Physical Review Letters* **106**, 220501 (2011).

[20] de la Torre, G. & Leverrier, A. (2012). Personal communication.