Simple and tight device-independent security proofs*

(Abstract submitted to QCrypt 2016)

Rotem Arnon-Friedman[1], Renato Renner[1], and Thomas Vidick[2]

[1]*Institute for Theoretical Physics, ETH-Zürich, CH-8093, Zürich, Switzerland*
[2]*Department of Computing and Mathematical Sciences, California Institute of Technology, Pasadena, CA, USA*

Abstract

Device-independent (DI) cryptography aims at achieving security that holds irrespective of the quality, or trustworthiness, of the physical devices used in the implementation of the protocol. Such a surprisingly high level of security is made possible due to the phenomena of quantum non-locality. The lack of any a priori characterisation of the device used in a DI protocol makes proving security a challenging task. Indeed, proofs for, e.g., DI quantum key distribution (DIQKD) were only achieved recently and result in far from optimal key rates while being quite complex.

In this work we show that a newly developed tool, the "entropy accumulation theorem" of Dupuis et al. [1], can be effectively applied to give fully general proofs of DI security that yield essentially tight parameters for a broad range of DI tasks. At a high level our technique amounts to establishing a reduction to the scenario in which the untrusted device operates in an identical and independent way in each round of the protocol. This makes the proof much simpler and allows us to achieve significantly better quantitative results for the case of general quantum adversaries.

As concrete applications we give simple and modular security proofs for DIQKD and randomness expansion protocols based on the CHSH inequality. For both tasks we establish essentially optimal key rates and noise tolerance that are much higher than what was known before. Our results considerably decrease the gap between theory and experiments, thereby marking an important step towards practical DI protocols and their implementations.

Motivation – proving device-independent security

Device-independent (DI) cryptographic protocols aim at achieving an unprecedented level of security: guarantees that hold (almost) irrespective of the quality, or trustworthiness, of the complex physical devices used to implement the protocol. Security in such protocols is based on the statistics observed by the honest parties when running the protocol, which allow them to decide whether the possibly faulty or even malicious devices used pose any security risk.

As an example, consider the task of DI quantum key distribution (DIQKD). There, the honest parties, called Alice and Bob, share a two-component device (one held by Alice; the other by Bob). The manufacturer of the device claims that it will produce (with high probability) identical and secret keys, unknown even to her, as the result of alleged measurements made by the device on the quantum state it contains. In the DI setting Alice and Bob (and perhaps even the manufacturer herself) cannot open the device and assess whether it works as claimed; they must therefore treat the device as a black box with which they can only interact according to the protocol. The protocol should thus be "strong enough" such that its security can be proven based on those interactions alone.

It is already well known that DI protocols are made possible due to quantum non-locality and Bell inequalities [2–4] (see also [5, 6] for excellent reviews). In general, a Bell inequality [7] can be thought of as a game played by the honest parties using the device they share. The game has a special "feature" – there exists a quantum non-local strategy (i.e., measuring some entangled state) which achieves a winning probability ω_q greater than all classical strategies. Hence, if the honest parties observe that using their device they win the game with probability ω_q then they conclude that it must be non-local. According to quantum physics the winning probability in a game is directly related to the amount of secret randomness produced during the game [8, 9], which can be used to prove security of the relevant protocol.

*Full version is attached.

Indeed, in the past decade (and even earlier) many DI cryptographic protocols, based on this idea, have been considered. A limited list includes QKD [4, 10, 11], randomness expansion [8, 12–15] and amplification [16, 17], verified quantum computation [18, 19], bit commitment [20] and weak string erasure [21].

Proving security in the DI setting, where very little is known a priori about the underlying quantum systems, is often challenging. One assumption commonly used [10, 22–30] to simplify this task is that the device held by the honest parties makes the same measurements on identical (and independent) quantum states in every round of the protocol $i \in [n]$. This implies that the device is initialised in some (unknown) state of the form $\rho^{\otimes n}$, i.e., an independent and identically distributed (i.i.d.) state, and that the measurements have a similar structure. In that case, the total entropy (or "secret randomness") derived during the protocol by the honest parties can be easily related to the sum of the entropies generated in each round separately.[1] A bound on the entropy accumulated in a single round can usually be derived from the expected winning probability in the game played in that round (i.e., the Bell violation), which in turn can be easily estimated during the protocol in the i.i.d. case using standard Chernoff-type bounds.

Unfortunately, even though quite convenient (and, in many cases, seemingly necessary) for the analysis, the i.i.d. assumption is a very strong one in the DI scenario. In particular, under such an assumption the device cannot use any internal memory (i.e., its actions in one round cannot depend on the previous rounds) or even display time-dependent behavior (due to inevitable imperfections for example). Furthermore, once it is assumed that the honest parties' state has a tensor product structure, its purification to the adversary can be assumed to have the same structure without loss of generality. Thus, the i.i.d. assumption also heavily restricts the side information available to the adversary.

When considering device-*dependent* protocols, such as the BB84 protocol [32], de Finetti theorems [33, 34] can usually be used to reduce the task of proving security in the most general case to that of proving security with an i.i.d. assumption as described above. Unfortunately, the same theorems cannot be used in the DI case (one reason, for example, is that they depend on the dimension of the underlying states), and while other de Finetti-type theorems [35, 36] were developed for the case in which the states and measurements are unknown it is still not clear how to use them in DIQKD. Hence, in the DI setting, one cannot simply reduce a general security proof to one proven under the i.i.d. assumption.

Without this assumption, however, not much is a priori known about the structure of the untrusted device and hence neither about its output. Therefore, security proofs that proved security directly for the most general case had to use far more complicated techniques and statistical analysis compared to the i.i.d. case.[2] For DIQKD, for example, security in the non-i.i.d setting was first established in [11]; see also [37], which gives a secure protocol but with vanishing rate and no noise tolerance. A more recent proof of security is given in [15]. The security proofs of those works are quite complex and achieve relatively low key rates and noise tolerance (if any).

Our contribution – the results and their importance

In this work we demonstrate that a newly developed tool, the "entropy accumulation theorem" (EAT) [1], can be effectively applied to give proofs of security with essentially tight parameters for a broad range of DI protocols. Our main contribution is a general framework, consisting of a flexible protocol and analysis, for applying the EAT to establish quantitative results on DI security.

Our technique amounts to establishing a reduction to the i.i.d. setting, in a way that is virtually lossless in terms of parameters. As a consequence we are able to extend the tight results known for e.g. DIQKD under the i.i.d. assumption to the most general setting. Our technique is simpler and allows for more modular protocols than previous ad-hoc approaches. As more and more DI protocols are being proposed it is highly important to have a simple, yet strong, proof technique to prove security.

The significance of our quantitative results is twofold. First, they establish the a priori surprising result

[1] Formally the bound can be calculated using the quantum asymptotic equipartition [31] for example.

[2] This led to clearly sub-optimal proofs both in terms of modularity and of the parameters achieved (e.g., key rates or amount of tolerable noise).

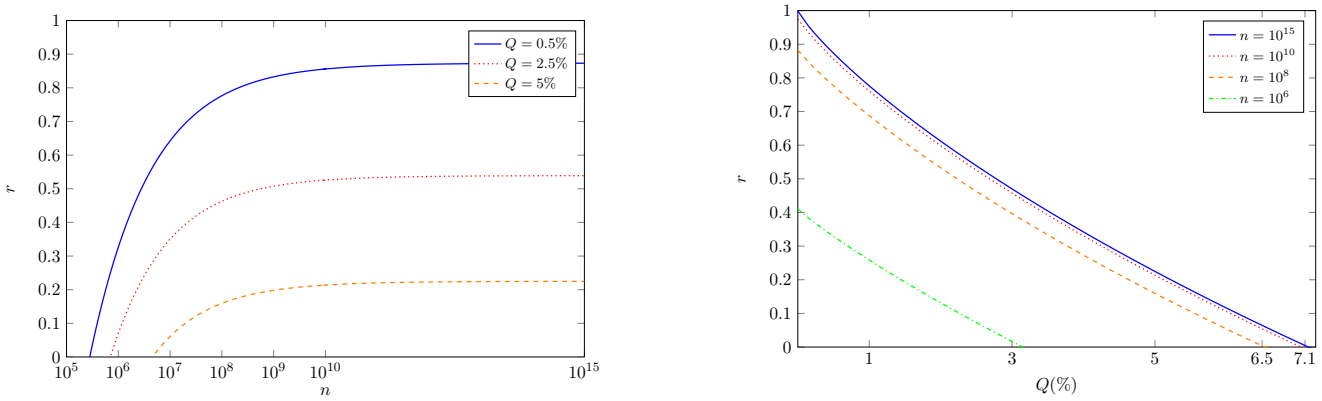

Figure 1: Key rates of our DIQKD protocol as a function of the number of rounds n (left) and the error rate Q (right). For the technical details see Section 5.5 in the main text.

that general quantum adversaries do not force weaker rates, i.e., it is possible to achieve rate vs. noise tradeoffs which are as good as those achieved in much more restricted settings (such as under the i.i.d. assumption). Second, our rates considerably decrease the gap between theory and experiments, thereby marking an important step towards practical DI protocols and their implementation.

We provide two concrete applications. To begin with, we consider a DIQKD protocol based on the CHSH inequality [38] and prove its security. The achieved key rate and noise tolerance are significantly higher than in previous works (see figure). For large enough n, the key rate as a function of the noise tolerance essentially coincides with the optimal result of [10], derived for the restricted i.i.d. and asymptotic case (i.e., when the device is used $n \to \infty$ times). In particular, as in [10], we show that the protocol can tolerate up to the optimal error rate of 7.1% while still producing a positive key rate. (For comparison[3], in [11] the maximal noise tolerance was 1.6%). Moreover, the achieved key rates are comparable to those achieved in device-*dependent* QKD protocols [39, 40] already from $n = 10^6$.

As a second application we consider a randomness expansion protocol based on the CHSH inequality. Here as well, we obtain an expansion rate which essentially matches the optimal rate achieved in [8] against *classical* adversaries only, while our result holds against *quantum* adversaries. This is much better than the rates obtained in previous works [13, 15, 41].

Main ideas of the proof. The main tool used in the proof is the EAT [1]. The EAT can be understood as some kind of a chain rule for the conditional smooth min-entropy, which quantifies how entropy "accumulates" across many random variables generated through a certain iterative quantum processes as long as it fulfils a number of technical conditions (see Section 2.6 in the main text for the details).

Our technical contribution consists in showing how the EAT can be used to provide a complete analysis of security in the DI setting, with the additional benefit of yielding essentially optimal parameters. Towards this we take the following three main steps. First, we propose modular hypothetical protocol that can be considered as a "skeleton" for many DI tasks. This protocol is fine-tuned such that the entropy generated throughout it can be analysed using the EAT, by ensuring that the appropriate conditions are met, and such that it can be used as a building block in the analysis of more complex protocols while preserving strong quantitative results. Next, we combine the results of [10], derived for the i.i.d. case, together with our protocol to get a good lower-bound on the generated entropy rate when using the CHSH inequality. Finally, we show how the hypothetical protocol can be related to actual more complex protocols of interest, such as DIQKD protocols. This relation is used to prove security of a DIQKD protocol we propose, with essentially optimal key rate and noise tolerance.

[3]The noise models of the two works are a bit different; the value of 1.6% is the relevant one after equating the models.

References

[1] Frederic Dupuis, Omar Fawzi, and Renato Renner. Entropy accumulation. To appear soon on the arXiv, 2016.

[2] Artur K Ekert. Quantum cryptography based on Bell's theorem. *Physical review letters*, 67(6):661, 1991.

[3] Dominic Mayers and Angela Yao. Quantum cryptography with imperfect apparatus. In *Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on*, pages 503–509. IEEE, 1998.

[4] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Physical Review Letters*, 95(1):010503, 2005.

[5] Valerio Scarani. The device-independent outlook on quantum physics (lecture notes on the power of bell's theorem). *arXiv preprint arXiv:1303.3081*, 2013.

[6] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86(2):419, 2014.

[7] John S Bell et al. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1(3):195–200, 1964.

[8] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzimitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, et al. Random numbers certified by Bell's theorem. *Nature*, 464(7291):1021–1024, 2010.

[9] Antonio Acín, Serge Massar, and Stefano Pironio. Randomness versus nonlocality and entanglement. *Physical review letters*, 108(10):100402, 2012.

[10] Stefano Pironio, Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009.

[11] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Physical review letters*, 113(14):140501, 2014.

[12] Roger Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, Trinity College, University of Cambridge, November 2006.

[13] Umesh Vazirani and Thomas Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 61–76. ACM, 2012.

[14] Matthew Coudron and Henry Yuen. Infinite randomness expansion and amplification with a constant number of devices. *arXiv preprint arXiv:1310.6755*, 2013.

[15] Carl A Miller and Yaoyun Shi. Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 417–426. ACM, 2014.

[16] Roger Colbeck and Renato Renner. Free randomness can be amplified. *Nature Physics*, 8(6):450–453, 2012.

[17] Kai-Min Chung, Yaoyun Shi, and Xiaodi Wu. Physical randomness extractors: Generating random numbers with minimal assumptions. *arXiv preprint arXiv:1402.4797*, 2014.

[18] Alexandru Gheorghiu, Elham Kashefi, and Petros Wallden. Robustness and device independence of verifiable blind quantum computing. *New Journal of Physics*, 17(8):083040, 2015.

[19] Michal Hajdušek, Carlos A Pérez-Delgado, and Joseph F Fitzsimons. Device-independent verifiable blind quantum computation. *arXiv preprint arXiv:1502.02563*, 2015.

[20] Nati Aharon, Serge Massar, Stefano Pironio, and Jonathan Silman. Device-independent bit commitment based on the chsh inequality. *arXiv preprint arXiv:1511.06283*, 2015.

[21] Jędrzej Kaniewski and Stephanie Wehner. Device-independent two-party cryptography secure against sequential attacks. *arXiv preprint arXiv:1601.06752*, 2016.

[22] Antonio Acin, Nicolas Gisin, and Lluis Masanes. From bell's theorem to secure quantum key distribution. *Physical review letters*, 97(12):120405, 2006.

[23] Antonio Acín, Serge Massar, and Stefano Pironio. Efficient quantum key distribution secure against no-signalling eavesdroppers. *New Journal of Physics*, 8(8):126, 2006.

[24] Valerio Scarani, Nicolas Gisin, Nicolas Brunner, Lluis Masanes, Sergi Pino, and Antonio Acín. Secrecy extraction from no-signaling correlations. *Physical Review A*, 74(4):042339, 2006.

[25] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[26] Lluis Masanes. Universally composable privacy amplification from causality constraints. *Physical review letters*, 102(14):140501, 2009.

[27] Esther Hänggi, Renato Renner, and Stefan Wolf. Efficient device-independent quantum key distribution. In *Advances in Cryptology–EUROCRYPT 2010*, pages 216–234. Springer, 2010.

[28] Esther Hänggi and Renato Renner. Device-independent quantum key distribution with commuting measurements. *arXiv preprint arXiv:1009.1833*, 2010.

[29] Lluís Masanes, Stefano Pironio, and Antonio Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature communications*, 2:238, 2011.

[30] Lluis Masanes, Renato Renner, Matthias Christandl, Andreas Winter, and John Barrett. Full security of quantum key distribution from no-signaling constraints. *Information Theory, IEEE Transactions on*, 60(8):4973–4986, 2014.

[31] Marco Tomamichel, Roger Colbeck, and Renato Renner. A fully quantum asymptotic equipartition property. *Information Theory, IEEE Transactions on*, 55(12):5840–5847, 2009.

[32] Charles H Bennett and Gilles Brassard. Proceedings of the ieee international conference on computers, systems, and signal processing, bangalore, india, 1984. 1984.

[33] Renato Renner. Symmetry of large physical systems implies independence of subsystems. *Nature Physics*, 3(9):645–649, 2007.

[34] Matthias Christandl, Robert König, and Renato Renner. Postselection technique for quantum channels with applications to quantum cryptography. *Physical Review Letters*, 102(2):020504, 2009.

[35] Matthias Christandl and Ben Toner. Finite de Finetti theorem for conditional probability distributions describing physical theories. *Journal of Mathematical Physics*, 50:042104, 2009.

[36] Rotem Arnon-Friedman and Renato Renner. de Finetti reductions for correlations. *Journal of Mathematical Physics*, 56(5):052203, 2015.

[37] Ben W Reichardt, Falk Unger, and Umesh Vazirani. Classical command of quantum systems. *Nature*, 496(7446):456–460, 2013.

[38] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical review letters*, 23(15):880, 1969.

[39] Valerio Scarani and Renato Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Physical review letters*, 100(20):200501, 2008.

[40] Valerio Scarani and Renato Renner. Security bounds for quantum cryptography with finite resources. In *Theory of Quantum Computation, Communication, and Cryptography*, pages 83–95. Springer, 2008.

[41] Carl A Miller and Yaoyun Shi. Universal security for randomness expansion from the spot-checking protocol. *arXiv preprint arXiv:1411.6608*, 2014.