# Challenges for a DIQKD implementation

Gláucia Murta, Suzanne van Dam, Jérémy Ribeiro, Ronald Hanson, and Stephanie Wehner
*QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands*

Quantum key distribution (QKD) is the paradigmatic example of quantum cryptography. The possibility of exploring quantum properties of systems permits to achieve unconditional security in the distribution of a classical key, which is impossible if one is bounded by classical resources. Several analysis of quantum key distribution have been done along the years [1–3], and the security of the simplest QKD protocol, the BB84 [4], is now well stablished. Moreover, reasonable key rates can be achieved with current technology [5, 6].

Nevertheless, the BB84 protocol can be immediately broken if the adversary can prepare a system of higher dimension without the awareness of Alice and Bob [7]. But quantum systems allow us to do more! And we can perform a QKD protocol in a device-independent (DI) way. *Device-independence* models quantum systems and measurement apparatuses as black boxes, where the only feature used for the analysis is the statistics of inputs and outputs of the experiment. In the device-independent scenario no more assumptions are necessary on the dimension of the underlying system or on the behaviour of the measurement devices, and the security is based solely on the fact that the statistics of the experiment violate a Bell inequality [8].

A lot of effort has been taken to establish security of QKD in the device-independent scenario [7, 9–18]. An asymptotic analysis which tolerates a reasonable amount of noise was established in [7]. However, the analysis of Ref. [7] uses the i.i.d. (independent and identically distributed) assumption, *i.e.* the assumption that in each round of the protocol the state shared by Alice and Bob is the same and moreover their devices behave in the same way. Only very recently an appropriate technique was developed to allow for the analysis of DIQKD in the most adversarial scenario [19, 20], where an eavesdropper could attack the systems in an arbitrary way and, moreover, the devices of Alice and Bob could behave arbitrarily, which includes having memory of the previous rounds.

Even under the i.i.d. assumption, low detection efficiencies open a loophole for a secure implementation of DIQKD. Techniques of heralded entanglement allow to overcome this problem [21]. However, the rate of generation of entangled events with current technology still represents a challenge for a fully DIQKD implementation.

With the aim to prove security for reasonable key rates in a device-independent scenario:

- We discuss the hypotheses present in the device-independent model, both in the most adversarial scenario and with the i.i.d. assumption.

- Using techniques of Refs. [19, 20], we plot the optimal key rates achievable for the finite regime in the most adversarial scenario, aiming at implementations with Nitrogen-Vacancy systems [22].

- We compare with the key rates achievable under the i.i.d. assumption, using the available tools for security proof: the non-asymptotic version of the asymptotic equipartition property and the extensivity of the collision entropy. And we discuss the possibility of implementation with current technology.

- We discuss possibilities for obtaining better rates (improvements on the security analysis and the use of different Bell inequalities).

[1] Peter W. Shor and John Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.

[2] Hoi-Kwong Lo. Proof of unconditional security of six-state quatum key distribution scheme. *Quantum Info. Comput.*, 1(2):81–94, August 2001.

[3] Renato Renner. *Security of quantum key distribution.* Diss., Naturwissenschaften, ETH Zürich, Nr. 16242, 2006, 2005.

[4] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560, Part 1:7 – 11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[5] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nat Commun*, 3:634.

[6] M. Tomamichel and A. Leverrier. A largely self-contained and complete security proof for quantum key distribution. *e-prints, arXiv: 1506.08458*, June 2015.

[7] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, 2009.

[8] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics 1*, pages 195–200, 1964.

[9] Antonio Acín, Nicolas Gisin, and Lluis Masanes. From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.*, 97:120405, Sep 2006.

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

[11] Valerio Scarani, Nicolas Gisin, Nicolas Brunner, Lluis Masanes, Sergi Pino, and Antonio Acín. Secrecy extraction from no-signaling correlations. *Phys. Rev. A*, 74:042339, Oct 2006.

[12] Marco Tomamichel and Esther Hänggi. The link between entropic uncertainty and nonlocality. *Journal of Physics A: Mathematical and Theoretical*, 46(5):055301, 2013.

[13] Charles Ci Wen Lim, Christopher Portmann, Marco Tomamichel, Renato Renner, and Nicolas Gisin. Device-independent quantum key distribution with local Bell test. *Phys. Rev. X*, 3:031006, Jul 2013.

[14] L. Masanes, R. Renner, M. Christandl, A. Winter, and J. Barrett. Full security of quantum key distribution from no-signaling constraints. *IEEE Transactions on Information Theory*, 60(8):4973–4986, Aug 2014.

[15] Lluis Masanes, Stefano Pironio, and Antonio Acin. Secure device-independent quantum key distribution with causally independent measurement devices. *Nat Commun*, 2:238, 03 2011.

[16] Jonathan Barrett, Roger Colbeck, and Adrian Kent. Unconditionally secure device-independent quantum key distribution with only two devices. *Phys. Rev. A*, 86:062326, Dec 2012.

[17] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of chsh games. *e-prints, arXiv:1209.0448*, 2012.

[18] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Phys. Rev. Lett.*, 113:140501, Sep 2014.

[19] F. Dupuis, O. Fawzi, and R. Renner. Entropy accumulation. *e-prints, arXiv: 1607.01796*, July 2016.

[20] R. Arnon-Friedman, R. Renner, and T. Vidick. Simple and tight device-independent security proofs. *e-prints, arXiv:1607.01797*, July 2016.

[21] Christoph Simon and William T. M. Irvine. Robust long-distance entanglement and a loophole-free bell test with ions and photons. *Phys. Rev. Lett.*, 91:110405, Sep 2003.

[22] W. B. Gao, A. Imamoglu, H. Bernien, and R. Hanson. Coherent manipulation, measurement and entanglement of individual solid-state spins using optical fields. *Nat Photon*, 9:363 – 373.