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 established. 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).


