Device-Independent Quantum Key Distribution

A. Acín (1,2), N. Brunner (3), N. Gisin (3), S. Massar (4), S. Pironio (1), V. Scarani (5)
1: ICFO-Institut de Ciencies Fotoniques, 08860 Castelldefels (Barcelona), Spain, Antonio.Acin@icfo.es
2: ICREA-Institucio Catalana per la Recerca i Estudis Avançats, 08010 Barcelona, Spain
3: GAP-Otique, Université de Genève, CH-1211 Genève 4, Switzerland
4: Laboratoire d'Information Quantique, Université Libre de Bruxelles, B-1050 Brussels, Belgium
5: Centre for Quantum Technologies and Department of Physics, National University of Singapore, Singapore

Abstract

Quantum Key Distribution is usually based on three main assumptions: (i) the validity of Quantum Mechanics, (ii) the assumption of no-information leakage from the honest parties' labs and (iii) the fact that the honest parties have a sufficiently good knowledge of their devices. All the three assumptions are necessary for the security of standard protocols, such as BB84. We show how to remove the third assumption and construct QKD protocols whose security can then be proven without making any assumptions on the devices. These protocols, that are named Device Independent, offer a stronger form of security since they require the minimal assumptions. The key ingredient in our construction is the non-local correlations achievable by measuring quantum states.

Introduction

The security of Quantum Key Distribution schemes, as any other cryptographic protocol, does not come from scratch and is based on several assumptions. First of all, any eavesdropper, however powerful, should obey the quantum laws. Second, it is assumed that there is no information leakage from the honest parties' labs[1]. Finally, a third essential requirement in the security analysis of Quantum Key Distribution is that Alice and Bob have a sufficiently good control of the quantum devices used for the correlation distribution. This assumption is often critical: the security of the BB84 protocol [1], for instance, is entirely compromised if Alice and Bob, instead of sharing qubits as usually assumed, share four-dimensional systems [2,3].

At first sight, control of the apparatuses seems to be an inescapable requirement. Remarkably, this is not the case: we present a device-independent security proof against collective attacks for the QKD protocol described in Ref. [4]. Our proof is device-independent in the sense that it needs no assumptions about the way the QKD devices work or on what quantum system they operate.

Motivation

The motivation for studying Device-Independent QKD schemes is twofold. First of all, they give the strongest form of security achievable by quantum means, since the security proof relies on the minimal assumptions, namely the validity of Quantum Mechanics and the fact that there is no information leakage from the honest parties' labs. Second, although their experimental implementation has to face important challenges, it represents a new type of schemes whose practical realization is more robust against technological imperfections. Provided the desired correlations are observed, our security analysis applies in a simple way to situations where the apparatuses are noisy, where uncontrolled side channels are present, or more generally where the QKD devices are entirely untrusted and acquired from a malicious party, possibly from the eavesdropper itself.

Main achievements

The physical basis for our device-independent security proof is the fact that measurements on entangled particles can provide Alice and Bob with non-local correlations, that is, correlations that cannot be reproduced by shared randomness (local variables), as detected by the violation of Bell-type inequalities. Considered in the perspective of QKD, the fact that Alice and Bob's symbols are correlated in a non-local way, whatever be the underlying physical details of the apparatuses that produced those symbols, implies that Eve cannot have full information about them, otherwise her own symbol would be a local variable able to reproduce the correlations.

This intuition has been around for some time [5,6,7]. Quantitative progress has been possible however only recently, thanks to the pioneering work of Barrett,

Hardy and Kent [8] and to further extensions [2,4,9]. For conceptual interest and mathematical simplicity, all these works studied security against a supra-quantum Eve, who could perform any operation compatible with the no-signalling principle.

In this contribution, we focus on the more realistic situation in which Eve is constrained by quantum physics and present the first example of Device-Independent QKD. More precisely, we prove that the quantum realization of the CHSH protocol described in Ref. [4] offers universally-composable security against collective attacks.

[1] It is unclear whether this can be even considered an assumption, but we mention it here for the sake of clarity.

Our main result is a tight bound on the Holevo information between one of the authorized parties and the eavesdropper, as a function of the amount of violation of a Bell-type inequality. The obtained rates are comparable with those derived for BB84 in the standard scenario where assumptions on the devices are allowed. In particular, our protocol has a positive secret key rate for errors below 7.1 %.

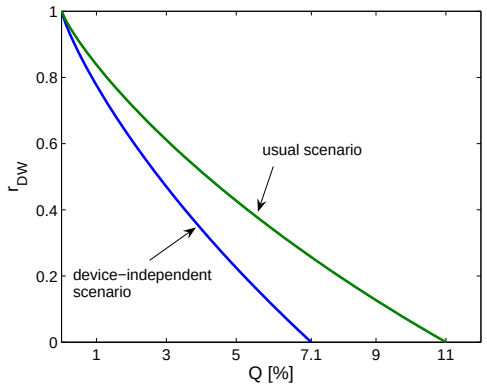

Figure 1: Comparison of the extractable secret-key rates against collective attacks in the usual scenario and in the device-independent scenario.

Conclusions

Device-Independent protocols arguably represent the "purest" form of QKD protocols since their security is based on the minimal assumptions. Our results are just the first step in the study of this new type of protocols. Many open questions indeed remain open. From a theoretical point of view, it would be interesting to extend our analysis to other protocols. Clearly, the main theoretical open question is whether the security of the protocols still holds under completely general attack. As mentioned, at present, the security proof only works for collective attacks. In a collective attack, Eve applies the same attack on each particle of Alice and Bob, but no other limitations are imposed to her. In particular she can keep her systems in a quantum memory and perform a (coherent) measurement on them at any time. Collective attacks are very meaningful in standard QKD because a bound on the key rate for these attacks becomes automatically a bound for the most general attacks if a de Finetti theorem can be applied [10]. Whether such a reduction is possible in the device-independent scenario is an interesting question per se.

From a more applied point of view, the implementation of these protocols faces important challenges. In particular, it requires a loophole-free violation of a Bell inequality (unless other assumptions are made). The detection loophole thus becomes an interesting issue in applied physics

References

1. C. H. Bennett and G. Brassard, Proceedings IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India (IEEE, New York, 1984), 175.
2. A. Acín et al, Phys. Rev. Lett. 97 (2006), 120405.
3. F. Magniez et al, quant-ph/0512111.
4. A. Acín et al, New J. Phys. 8 (2006), 126.
5. A. K. Ekert, Phys. Rev. Lett. 67 (1991), 661.
6. C. H. Bennett et al, Phys. Rev. Lett. 68 (1992), 557.
7. D. Mayers et al, Quant. Inf. Comp. 4 (2004), 273.
8. J. Barrett et al, Phys. Rev. Lett. 95 (2005), 010503.
9. L. Masanes et al, quant-ph/0606049.
10. R. Renner, Security of Quantum Key Distribution, PhD thesis, quant-ph/0512258.