Secret key rates for the Continuous-Variable Quantum Key Distribution platform

E. Karpov, Raúl García-Patron, Nicolas Cerf
Centre for Quantum Information and Communication, Université Libre de Bruxelles
ekarpov@ulb.ac.be

Abstract

We report on the results of the evaluation of the secret key rate for a realistic scheme of quantum key distribution with continuous variables taking into account the efficiency of optical detectors. Based on the results on the optimality of Gaussian attacks we obtain secure bounds for individual and collective attacks for non-perfect efficiency of reconciliation algorithms. We show that in case of reverse reconciliation scheme the electronic noise due to imperfect detectors on the receiver's side can increase, in principle, the tolerance to noise of the overall scheme.

Introduction

Quantum Key Distribution (QKD) provides two remote parties, Alice and Bob with a common random sequence of bits (secret key), unknown to any third party. All QKD schemes use a quantum channel for the transmission of optical signals in quantum regime and a public but authenticated classical channel for reconciliation of the results of measurements of transmitted quantum states. Continuous-variable QKD (CVQKD) uses the encoding of information into the quadratures of the electromagnetic field and homodyne (heterodyne) measurements, which require only on-shelf telecom components and not the more sophisticated single-photon technology as with discrete-variable QKD. However, CVQKD needs elaborate classical error correction algorithms in order to extract secret bits from correlated results of quantum measurements. Depending on the type of classical information exchange used by these reconciliation algorithms one distinguishes two-way or one-way reconciliation schemes and direct (from Alice to Bob) or reverse one-way reconciliation [1].

We present a framework for the security analysis of CVQKD protocols using Gaussian quantum states. Using our approach we compare the security bounds for Gaussian CVQKD protocols for two general classes of attacks. This method is applied to the CVQKD scheme implemented at the Institut d'Optique Palaiseau [2], which uses reverse reconciliation algorithms. We analyze the effect the electronic detection noise on the secret key rates.

Motivation

The main advantage of Quantum Key Distribution is a possibility to prove unconditional security of the key distribution protocols by upper bounding the information that the adversary, Eve, can acquire in the worst case. Unconditional security implies quite "generous" assumptions for the ability of Eve, who is allowed to have an unlimited computational power and full control over the channel. The actions of Eve are limited only by the laws of quantum mechanics and Eve has no access to the laboratories of Alice and Bob. For the purpose of analysis one specifies different classes of possible Eve's attacks:

Individual attack. Eve attacks individually each pulse sent by Alice, and stores her ancilla in a quantum memory. After listening to the information exchange between Alice and Bob via the classical channel (but before error correction) Eve performs an appropriate measurement on her ancilla. The maximum information accessible to Eve is bounded by the classical Shannon mutual information I_{BE} (in case of reverse reconciliation).

Collective attack. Eve attacks individually each pulse sent by Alice and applies the optimal collective measurement on the ensemble of stored ancillae only after having listened to the communication between Alice and Bob during the key distillation procedure. The maximum information accessible to Eve is limited by the Holevo bound χ_{BE}.

Coherent attack. This is the most powerful attack. Eve attacks collectively all pulses sent by Alice and applies an optimal joint measurement over all the ancillae after having monitored all key distillation messages.

The theoretical bound for the key rate ("raw" key rate) is defined for reverse reconciliation CVQKD as $\Delta I^{Shannon} = I_{AB} - I_{BE}$ for individual attacks and $\Delta I^{Holevo} = I_{AB} - \chi_{BE}$ for collective attacks. The security against the coherent attack is conjectured to be provable in the same way as for discrete variables. In that case, under the assumption of the symmetry of the privacy amplification and of the channel probe protocols, the coherent attack was proven not to be more powerful than the collective one.

The security analysis of CVQKD is significantly simplified if one uses Gaussian quantum input states because these states are completely determined by the average values and second moments of the quaratures. We prove that individual and collective Gaussian attacks on CVQKD protocol using the Gaussian input states is optimal [3, 4]. Thus, without loss of generality of the results for Gaussian inputs, we can limit our analysis to Gaussian transformations, which makes the problem analytically tractable.

Method

Our method uses the EPR-based scheme, which is equivalent to the prepare-and-measure CVQKD-scheme implemented in the realistic set-up. The reason of introducing the new scheme is that it provides a unified description of all protocols based on the Gaussian modulation of Gaussian states and homodyne or heterodyne detection, so that one can describe all these protocols by only changing some parameters of the scheme.

The main idea is to present Alice's quantum state preparation as the measurement of one part (A) of a two-mode squeezed state when sending another part (B0) to Bob through the quantum channel, see Fig. 1. The two-mode squeezed state is completely determined by its covariance matrix γAB0 which contains only one parameter, the variance V. By measuring A and multiplying her measurement results by the factor $\alpha=[(V-1)(V+1)]^{1/2}$) Alice estimates and thus effectively prepares state B_0.

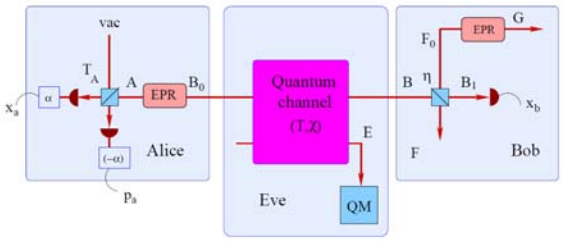

Figure 1: Entanglement-based scheme of CVQCD. The transmittances T_A and η characterize Alice's preparation and Bob's measurement, while the transmittance T and the noise χ are controlled by Eve. The QM box denotes Eve's quantum memory.

Alice's beam splitter transmission coefficient determines different CVQKD protocols. Indeed, $T_A=1$ corresponds to homodyne detection which, effectively prepares squeezed states used by the protocol presented in Ref. [5]. Transmittance $T_A=1/2$ corresponds to heterodyne detection which effectively prepares coherent states used by the protocol presented in Ref. [1, 6].

Main achievements

We have developed a method of calculating the key rates that are available to Alice and Bob applying CVQKD protocols using Gaussian signals. With the help of the developed method we have

- evaluated secret key rates for the experimentally implemented CVQKD as function of the physical parameters of the channel and of the QKD set-up;
- compared the security of four CVQKD protocols;
- analyzed the effect of the electronic detection noise and shown that for ideal conditions (high modulation and perfect reconciliation efficiency $\beta=1$) electronic detection noise always increases the tolerance of the protocol to the detection;
- found an improvement of the tolerance of realistic CVQKD protocols to the channel noise, see Fig. 2.

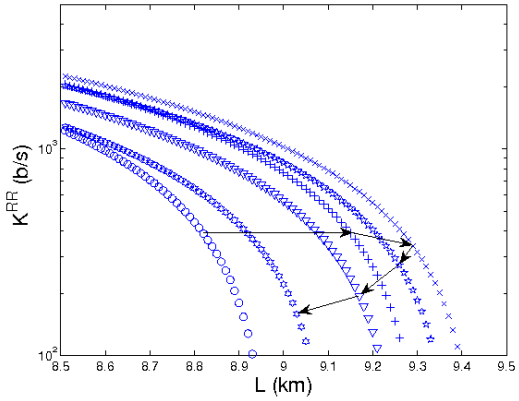

Figure 2: Increasing maximal distance of CVQKD due to detection noise for realistic reconciliation efficiency $\beta=0.87$. The arrow indicates the change of detection noise from $\chi_D=0$ to $\chi_D=0.44$.

Conclusions

The security of Gaussian CVQKD protocols is proven against individual and coherent attacks. The unconditional security requiring analysis of coherent attacks is conjectured to be provable by analogy with proof for the discrete variable QKD.

Reference

1. F. Grosshans et al Nature, 421 (2003) 238.
2. J. Lodewyck et al Phys. Rev. A, 76 (2007) 042305.
3. F. Grosshans et al Phys. Rev. Lett., 92 (2004) 047905.
4. R. García-Patron et al Phys. Rev. Lett., 97 (2006) 190503.
5. N. J. Cerf et al Phys. Rev. A, 63 (2001) 052311.
6. F. Grosshans et al Phys. Rev. Lett., 88 (2002) 057902.