

# Unconditional security of continuous-variable quantum key distribution

Anthony Leverrier (1), Evgueni Karpov (2), Philippe Grangier (3), and Nicolas J. Cerf (4)

1: Institut Telecom / Telecom ParisTech, CNRS LTCI, 46, rue Barrault, 75634 Paris Cedex 13, France, anthony.leverrier@enst.fr

2: Quantum Information and Communication, Ecole Polytechnique, CP 165/59, Université Libre de Bruxelles, 50 av. F. D. Roosevelt, B-1050 Brussels, Belgium, ekarpov@ulb.ac.be

3: Laboratoire Charles Fabry, Institut d'Optique, CNRS, Université Paris-Sud, Campus Polytechnique, RD 128, 91127 Palaiseau Cedex, France, philippe.grangier@institutoptique.fr

4: Quantum Information and Communication, Ecole Polytechnique, CP 165/59, Université Libre de Bruxelles, 50 av. F. D. Roosevelt, B-1050 Brussels, Belgium, ncerf@ulb.ac.be

## Abstract

The unconditional security of continuous-variable quantum key distribution is established for all schemes based on the estimation of the channel loss and excess noise [1]. It is proved that, in the limit of large keys, Gaussian attacks are asymptotically optimal among the most general (coherent) attacks, where the transmission is tapped using arbitrary ancillas and stored in a quantum memory as a whole. Then, it is shown that the previously derived bounds on the achievable secret key rates against collective attacks remain asymptotically valid for arbitrary coherent attacks.

## Introduction

Quantum key distribution (QKD) is probably to date the most successful application of quantum information sciences. This technique, based on the transmission of quantum signals between two authorized parties (Alice and Bob), enables them to generate a random bit string, called secret key, which is provably unknown to an eavesdropper (Eve) with arbitrary computational and technological power. The secret key rate  $K$  is essentially given by the difference between Eve and Bob's uncertainties about the data sent by Alice. Denoting Alice, Bob, and Eve's classical variables (after measurement) by  $a$ ,  $b$ , and  $e$ , one has

$$K = H(a|e) - H(a|b), \quad (1)$$

where the exact definition of the conditional entropy  $H$  depends on the type of attacks considered: individual, collective or coherent. The second term of the r.h.s. of Eq. (1) is simply measured while running the protocol since it is accessible to the legitimate parties, so only the first term needs to be estimated, or, more precisely, bounded below. For individual attacks,  $H(a|e)$  denotes the Shannon conditional entropy, and can be calculated explicitly for a Gaussian attack. For collective attacks, it must be replaced by  $S(a|E)$ , which denotes the von Neumann conditional entropy and can again be computed exactly for a Gaussian attack. Physically, this means that Eve accesses the Holevo information about Alice's variable  $a$  by making an appropriate measurement on her quantum system  $E$  (instead of accessing the Shannon information between  $a$  and her measurement  $e$ ). For individual and collective attacks, Gaussian attacks have been proved to be optimal as they minimize  $H(a|e)$  and

$S(a|E)$  for a given channel transmission and excess noise, which largely simplifies the security analysis.

To address *unconditional security*, one must consider the most general class of attacks, namely coherent attacks, and the first term of the r.h.s. of Eq. (1) must be replaced by the *quantum smooth min-entropy*  $S_{\min}(a|E)$ , as introduced in [2]. The min-entropy (or Rényi entropy of parameter  $\infty$ ) is particularly relevant for the security study of cryptographic protocols as it quantifies the guessing probability, i.e., the probability that Eve correctly guesses the value of the classical variable  $a$  [3]. Replacing Shannon or von Neumann entropies by min-entropies encapsulates the idea that the entire transmission, made of  $n$  symbols, is tapped as a whole. The min-entropy can be viewed as a one-shot quantity, while Shannon or von Neumann entropies are computed on a single-symbol basis and get a meaning only by assuming that there are many identical transmissions.

## Motivation

QKD protocols can be classified in discrete-variable protocols, based on photon counting (e.g., BB84), and continuous-variable protocols, based on homodyne detection [4]. We are concerned with this latter class of protocols in the following, in particular those based on the Gaussian modulation of Gaussian (coherent or squeezed) states. For discrete-variable protocols, the unconditional security can be proved by using a quantum de Finetti theorem stating that symmetric states are "close to" product states [5]. An  $n$ -partite state is said to be symmetric if it is invariant under any permutation of its subsystems. If the protocol is symmetric, one concludes that the smooth min-entropy of the symmetric state shared by Alice and Bob is asymptotically equal to ( $n$  times) the von Neumann entropy, as used for calculating the secret

key rates against collective attacks. This proves that coherent attacks are not more powerful than collective attacks. Unfortunately, this approach cannot be applied as such to the security of continuous-variable protocols against coherent attacks as it would require extending a de Finetti theorem to infinite dimensional Hilbert spaces. Such an extension, however, has just been shown to hold provided that experimentally verifiable conditions are fulfilled [6].

### **Main achievements**

We show that there exists another way to address the security of continuous-variable QKD, which circumvents the need for a de Finetti theorem in infinite dimension. The idea is to exploit the extremality of Gaussian states with respect to the (non smooth) min-entropy. The extremality of Gaussian states has led to powerful results in the past, as it was used, e.g., to prove the optimality of Gaussian attacks among collective attacks. The point of using Gaussian states here is that even if symmetric Gaussian states are not known to be exponentially close to product states, their min-entropy is equal to the min-entropy of a well-defined product state. Then, using the link between the smooth min-entropy and the von Neumann entropy, one shows that the secret key rate against coherent attacks can be asymptotically bounded below by a secret key rate against Gaussian collective attacks. This establishes the proof of the unconditional

security of continuous-variable QKD against the most general attacks.

### **Conclusions**

We have proved that the most general attacks against continuous-variable quantum key distribution protocols cannot beat Gaussian collective attacks, up to some finite-size corrections which vanish in the limit of a large key size. Our proof holds for all protocols based on probing the quantum channel via the second-order moments of Alice and Bob's continuous data.

### **Acknowledgements**

We acknowledge support from the European Union under project SECOQC (IST-2002-506813), from the French Agence Nationale de la Recherche Under projects PROSPIQ (No. ANR-06-NANO-041-05) and SEQUIRE (No. ANR-07-SESU-011-01), and from the Brussels-Capital Region under projects CRYPTASC and Prospective Research for Brussels.

### **References**

1. A. Leverrier, et al., arXiv: 0809.2252
2. R. Renner, Ph. D. thesis, ETH Zurich (2005)
3. R. Koenig, et al., arXiv: 0807.1338 (2008)
4. N. J. Cerf and P. Grangier, JOSA B 24, 324(2007)
5. R. Renner, Nature Physics 3, 645 (2007)
6. R. Renner and J. I. Cirac, arXiv 0809.2243 (2008)