QUANTUM KEY DISTRIBUTION USING PRACTICAL PHOTONIC SYSTEMS

Eleni Diamanti[1]

[1] *LTCI, CNRS - Télécom ParisTech, 23 avenue d'Italie, 75013 Paris, France*

eleni.diamanti@telecom-paristech.fr

RÉSUMÉ

In this work, we present the state-of-the-art in the field of quantum key distribution using continuous variables. In particular, we discuss long-distance practical photonic implementations of continuous-variable quantum key distribution (CVQKD) protocols and current issues related to potential security loopholes in such implementations. We conclude with perspectives in this field.

MOTS-CLEFS : *Quantum cryptography; Continuous variables; Photonic systems.*

1. INTRODUCTION

The ability to distribute secret keys with information-theoretic security is undoubtedly one of the most important achievements of the field of quantum information processing and communications [1]. The rapid progress in this field has enabled quantum key distribution (QKD) in real-world conditions and commercial devices are now available. Here we are interested in QKD protocols where the key information is encoded on quantum continuous variables, such as the values of quadrature components of coherent states of light. Such continuous-variable QKD (CVQKD) protocols present the major advantage that they only require standard telecommunication technology, and in particular, that they do not use photon counters.

2. LONG-DISTANCE EXPERIMENTS AND SIDE-CHANNEL ATTACKS

In the last few years, CVQKD protocols have been the subject of important advancements : security proofs against general eavesdropping attacks are available for protocols using Gaussian modulation [2], and field implementations over deployed telecommunication networks have been successfully demonstrated [3, 4]. However, important issues, namely the limited range of these implementations and the practical security of CVQKD systems, have only recently been addressed. Here, we present the state-of-the-art in long-distance fiber optic experiments for quantum key distribution with continuous variables and discuss the resistance of CVQKD systems to eavesdropping attacks exploiting auxiliary information channels that are typically not taken into account in security proofs.

We describe a practical implementation of CVQKD over 80 km of optical fibre based on an improved optical setup and newly designed error-correction algorithms required to extract the secret key from the correlated data shared between the two communicating parties, Alice and Bob [5]. Note that previous implementations had been limited to less than 25 km. The employed error-correction codes are suitable for CVQKD protocols using Gaussian modulation of coherent states and homodyne detection, and are available for a wide range of signal-to-noise ratios, which is a crucial element for long-distance operation conditions. Additionally, finite-size effects on the parameter estimation procedure of the QKD protocol were taken into account for the generation of the secret key [6], leading to the strongest level of security reported to date for such distances.

Furthermore, we are interested in current issues related to security loopholes in practical CVQKD systems due to the existence of side-channel attacks, linked, for instance, to the possible manipulation of the classical phase reference signal that is transmitted through the optical channel [7], or to the exploitation of back reflections from optical components to suitably chosen probe signals, which can reveal some part of the secret key [8]. Countermeasures to such attacks are typically easy to implement.

CONCLUSION

Perspectives for continuous-variable quantum key distribution systems range from achieving further improved performance of such systems to examining their ability for integration into existing telecommunication networks. In the long run, exploiting the standard components employed in CVQKD systems to develop silicon photonic chips for quantum key distribution may open the way to the widespread use of this technology for high-security applications within communication networks.

RÉFÉRENCES

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution", Rev. Mod. Phys. **81**, 1301 (2009).

[2] A. Leverrier, R. Garcia-Patron, R. Renner, and N. J. Cerf, "Security of continuous-variable quantum key distribution against general attacks", Phys. Rev. Lett. **110**, 030502 (2013).

[3] M. Peev et al, "The SECOQC quantum key distribution network in Vienna", New J. Phys. **11**, 075001 (2009).

[4] P. Jouguet et al, "Field Test of Classical Symmetric Encryption with Continuous Variable Quantum Key Distribution", Opt. Express **20**, 14030 (2012).

[5] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution", Nature Photon. **7**, 378 (2013).

[6] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, "Analysis of Imperfections in Practical Continuous-Variable Quantum Key Distribution", Phys. Rev. A **86**, 032309 (2012).

[7] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing Calibration Attacks on the Local Oscillator in Continuous-Variable Quantum Key Distribution", Phys. Rev. A **87**, 062313 (2013).

[8] I. Khan, N. Jain, B. Stiller, P. Jouguet, S. Kunz-Jacques, E. Diamanti, C. Marquardt, and G. Leuchs, "Trojan-horse attacks on practical continuous-variable quantum key distribution systems", QCrypt 2014.