



Development of a Global Network for Secure
Communication based on Quantum Cryptography
www.secoqc.net

SECOQC White Paper on Quantum Key Distribution and Cryptography

Abstract

The SECOQC White Paper on Quantum Key Distribution and Cryptography is the outcome on a thorough consultation and discussion among the participants of the European project SECOQC (www.secoqc.net). This paper is a review article that attempts to position Quantum Key Distribution (QKD) in terms of cryptographic applications. A detailed comparison of QKD with the solutions currently in use to solve the key distribution problem, based on classical cryptography, is provided. We also detail how the work on QKD networks lead within SECOQC will allow the deployment of long-distance secure communication infrastructures based on quantum cryptography. The purpose of the White Paper is finally to promote closer collaboration between classical and quantum cryptographers. We believe that very fruitful research, involving both communities, could emerge in the future years and try to sketch what may be the next challenges in this direction.

Editing Author: Romain Alléaume, romain.alleaume@enst.fr

Contributors:

Romain Alléaume¹, Jan Bouda², Cyril Branciard³, Thierry Debuisschert⁴, Mehrdad Dianati¹, Nicolas Gisin³, Mark Godfrey⁵, Philippe Grangier⁶, Thomas Länger⁷, Anthony Leverrier¹, Norbert Lütkenhaus⁸, Philippe Painchault⁹, Momtchil Peev⁶, Andreas Poppel¹⁰, Thomas Pornin¹¹, John Rarity⁵, Renato Renner¹², Grégoire Ribordy¹³, Michel Riguidel¹, Louis Salvail¹⁴, Andrew Shields¹⁵, Harald Weinfurter¹⁶, Anton Zeilinger¹⁰.

Affiliations:

- 1 Ecole Nationale Supérieure des Télécommunications, Paris, France.
- 2 Masaryk University, Brno, Czech Republic .
- 3 University of Geneva, Switzerland.
- 4 Thales Research and Technology, Orsay, France.
- 5 University of Bristol, United Kingdom.
- 6 CNRS, Institut d'Optique, Orsay, France.
- 7 Austrian Research Center, Vienna, Austria.
- 8 University of Erlangen, Germany & Institute for Quantum Computing, Waterloo, Canada.
- 9 Thales Communications, Colombes, France.
- 10 University of Vienna, Austria.
- 11 Cryptolog International, Paris, France.
- 12 University of Cambridge, United Kingdom.
- 13 Id Quantique SA, Geneva, Switzerland.
- 14 University of Aarhus, Denmark.
- 15 Toshiba Research Europe Ltd, Cambridge, United Kingdom.
- 16 Ludwig-Maximilians-University Munich, Germany

SECOQC Coordinator: Christian Monyk, christian.monyk@arcs.ac.at