Prof. Nicolas Gisin, Uni Genève

QCrypt

SECURE HIGH-SPEED COMMUNICATION BASED ON QUANTUM KEY DISTRIBUTION

Prof. Andreas P. Burg, EPFL

Prof. Norbert Felber, ETHZ

Prof. Etienne Messerli, HES-SO

Dr. Grégoire Ribordy, IDQ

What it's about…

Developing a system for sending cryptographic keys whose security is guaranteed by quantum physics and using this key to encrypt data with the highest rate ever of 100 Gb/s.

Context and project goals

Today's information society has an ever-growing need for secure data transmission. QCrypt offers at the same time an elegant solution for quantum-secure cryptographic key exchange and data encryption at a world record rate of 100 Gb/s.

How the project differentiates from similar competition in the field

The QCrypt is, to the team's knowledge, the only project developing both advanced Quantum Key Distribution (QKD) and high-speed encryption systems designed for working together. Moreover, either system is at the cutting edge in its own right: The QKD prototype offers record secure bit rates with real-time hardware based key distillation. In contrast to commercial encryption systems supporting a single link running up to 10 Gbit/s, the encryptors combine ten independent 10G user streams (in plain text) into a single 100 Gbit/s secured stream (encrypted text).

Quick summary of the project status and key results

In QKD the team has a complete, working prototype with unprecedented real time hardware key distillation, finite key security analyses and fully automated operation over a single fibre using wavelength division multiplexing. On the encryption side, error-free data encryption at 40 Gbit/s with 100% throughput was demonstrated.

Patents

Patent for the synchronisation of the two QKD devices in preparation.

Success stories

The complete system including QKD and encryptors was presented at the Nano-Tera.ch annual meeting in Kursaal Berne (see picture). It worked during the two days, under rather difficult conditions with respect to a standard telecom environment, without any interruption.

Main publications

Luca Henzen, VLSI Circuits for Cryptographic Authentication, Series in Microelectronics, Volume 214, Hartung-Gorre Printing House, Konstanz, Germany, 2011, ISSN 0936-5362, ISBN 978-3-86628-367-1

E. Messerli, O. Auberson, Révolution dans la cryptographie quantique, Newsletter Alliance N°3 Infocom, 28.10.2011 ; Accepted

E. Messerli, O. Auberson, Y. Graf, Quand la lumière sécurise davantage les réseaux, Swiss Engineering RTS N°10, 11.10.2011 ; Accepted

E. Messerli, O. Auberson, Révolution pour le très haut débit, Market.ch N°91, Sept 2011

M. Tomamichel, C. C. W. Lim, N. Gisin, R. Renner, Tight finite-key analysis for quantum cryptography, Nat Commun. 3, 634 (2012).

N. Walenta, T. Lunghi, O. Guinnard, R. Houlmann, H. Zbinden, and N. Gisin, Sine gating detector with simple filtering for low-noise infra-red single photon detection at room temperature, J. Appl. Phys. 112, 063106 (2012).

L. Henzen, J. Aumasson, W. Meier, R. Phan, VLSI Characterization of the Cryptographic Hash Function BLAKE, IEEE Transactions on Very Large Scale Integration (VLSI) Systems 19, 1746-1754 (2011).

T. Lunghi, C. Barreiro, O. Guinnard, R. Houlmann, X. Jiang, M. A. Itzler and H. Zbinden, Free Running Single Photon Detection based on a negative feedback InGaAs APD, J. of Mod. Opt., 59, 1481 (2012).

F.K. Gürkaynak, Suggestions for Hardware Evaluation of Cryptographic Algorithms, Proc. DIAC - Directions in Authenticated Ciphers, 153-157 (2012).

F.K. Gürkaynak, K. Gaj, B. Muheim, E. Homsirikamol, C. Keller, M. Rogawski, H. Kaeslin, J.P. Kaps, Lessons Learned from Designing a 65nm ASIC for Evaluating Third Round SHA-3 Candidates, Proc. The Third SHA-3 Candidate Conference, 208 -230 (2012).

M. Muehlberghuber, C. Keller, C. Pendl and N. Felber, 100 Gbit/s Authenticated Encryption Based on Quantum Key Distribution, Proc. IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC), Santa Cruz, USA (2012).

Nino Walenta, Andreas Burg, Dario Caselunghe, Jeremy Constantin, Nicolas Gisin, Olivier Guinnard, Raphael Houlmann, Pascal Junod, Boris Korzh, Natalia Kulesza, Matthieu Legré, Charles Ci Wen Lim, Tommaso Lunghi, Laurent Monat, Christopher Portmann, Mathilde Soucarros, Patrick Trinkler, Gregory Trolliet, Fabien Vannel, Hugo Zbinden, A fast and versatile QKD system with hardware key distillation and wavelength multiplexing, New J. Physics 16, 013047 (2014)

"M. Muehlberghuber, C. Keller, F. Gürkaynak and N. Felber, FPGA-Based High-Speed Authenticated Encryption System (to be published), IFIP Advances in Information and Communication Technologiy,

VLSI-Soc: From Algorithms to Circuits and System-on-Chop Design"

C. Keller, F. Gürkaynak, H. Kaeslin and N. Felber, True Random Number Generation and Unique Identifier Extraction using Dynamic Memoy-Based Physically Unclonable Functions (to be published), Proc. ISCAS International Symposium on Circuits and Systems, Melbourne, Aus (2014)