Continuous QKD and data encryption at up to 100 Gbit/s

Hugo Zbinden[1], Nino Walenta[1], Olivier Guinnard[1], Raphael Houlmann[1], Charles Lim Ci Wen[1], Boris Korzh[1], Tommaso Lunghi[1], Nicolas Gisin[1], , Andreas Burg[2], Jeremy Constantin[2], Matthieu Legré[3], Patrick Trinkler[3], Dario Caselunghe[3], Natalia Kulesza[3], Gregory Trolliet[4], Fabien Vannel[4], Pascal Junod[5], Olivier Auberson[5], Yoan Graf[5], Gilles Curchod[5], Gilles Habegger[5], Etienne Messerli[5], Christopher Portmann[1,6], Luca Henzen[7], Christoph Keller[7], Christian Pendl[7,8], Michael Mühlberghuber[7], Christoph Roth[7], Norbert Felber[7], Frank Gürkaynak[9], Daniel Schöni[9], Beat Muheim[9]

[1]Group of Applied Physics-Optique, University of Geneva, Chemin de Pinchat 22, 1211 Geneva, Switzerland
[2]Telecommunications Circuits Laboratory, École Polytechnique Fédérale de Lausanne, 1015 Lausanne, Switzerland
[3]idQuantique SA, Chemin de la Marbrerie 3, 1227, Geneva, Switzerland
[4]University of Applied Sciences Western Switzerland in Geneva (hepia), Rue de la Prairie 4, CH-1202 Geneva, Switzerland
[5]University of Applied Sciences Western Switzerland in Yverdon-les-Bains (HEIG-VD), Route de Cheseaux 1, CH-1401 Yverdon, Switzerland
[6]Institute for Theoretical Physics, ETH Zurich, Wolfgang-Pauli-Str. 27, 8093 Zurich, Switzerland
[7]Integrated Systems Laboratory, ETH Zurich, Gloriastrasse 35, 8092 Zurich, Switzerland
[8]Institute for Applied Information Processing and Communications, Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria
[9]Microelectronics Design Center, ETH Zurich, Gloriastrasse 35, 8092 Zurich, Switzerland

Introduction

Today's society relies heavily on confidential and authenticated communication. QKD, a solution for information theoretically secure key exchange, has been subject of a rapid development since the mid 1990's. Starting from the early proof of feasibility experiments, faster and faster (with bit rates of the order of Mbits [1, 2]) and long reaching systems (up to 250km [3]) have been developed. However, most of the early experiments focused on the physical layer: photon generation, manipulation, transmission and detection. And still today, rare are the systems which enclose all necessary components for secure and fast QKD. Indeed, those components are numerous and need multidisciplinary competences. Important and often forgotten parts include random number generation, real-time error correction and privacy amplification, secure authentication and finite key security analysis. Only implementing all these steps one can obtain secret keys ready to use for encryption. This is preferably done with One Time Pad encoding. However, this limits data rates to about 1 Mb/s over shorter distances, which is fine for a few niche applications, but nor compatible with today's high rate fiber links.

Here, we present the results of the project QCRYPT [4], a collaborate effort of eight research teams in Switzerland with the ambition to produce a complete and practical fiber based QKD and high speed encryption system. For the QKD part, we put the emphasis on continuous operation with a wavelength multiplexed service channel for synchronization and distillation, efficient hardware real-time distillation, finite key security analysis and frugal authentication. For the secure high-speed encryption of large data volumes, we developed a system able to multiplex up to ten 10 Gbit/s Ethernet inputs, pass the 100 Gbit/s data stream through authenticated encryption before transmitting it over an optical fiber to the decryptor. The cipher cores apply and frequently

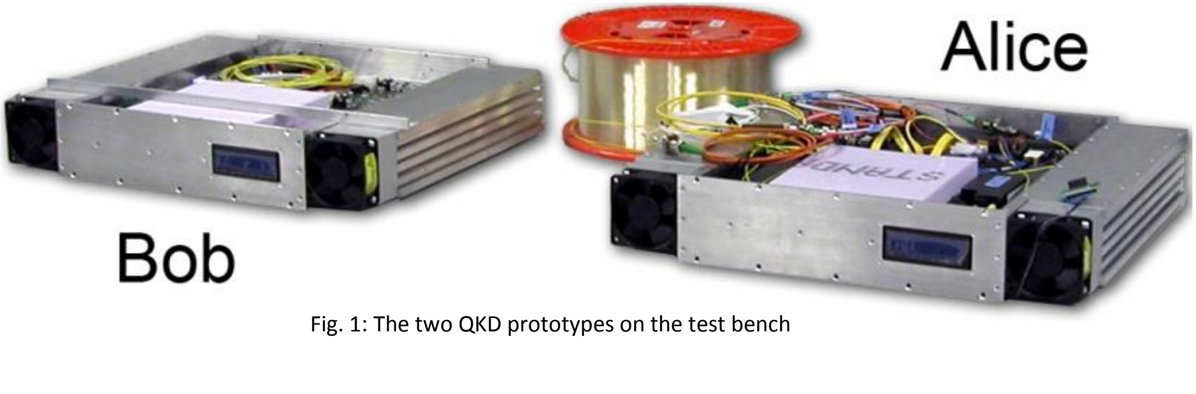

Fig. 1: The two QKD prototypes on the test bench

refresh the quantum keys delivered by the QKD system. We will demonstrate the whole system live at the conference on the booth of id Quantique.

QKD

The QKD systems of Alice and Bob are built around FPGAs (field programmable gate array, Xilinx Virtex 6) which manage the fast interfaces for the optical components for QKD, as well as all the sub-protocols which accompany QKD. Those protocols comprise synchronization, alignment, sifting, error correction and verification, privacy amplification, authentication, key management, encryption, administration and logging. Two communication links are established, a quantum channel for the COW protocol [5], and a bi-directional classical service channel. We employ dense wavelength-division multiplexing to transmit all these classical communication channels together with the quantum channel simultaneously over a single fiber.

We implemented a forward error correction code in the FPGA using a quasi-cyclic LDPC code as described in [6]. The presented implementation provides corrected rates up to 235 Mbit/s at 625 MHz clock frequency and its code rate can be adapted to different error rates. However, to guarantee the correctness of the final key, it is necessary to further reduce the probability that uncorrected errors remain after error correction. Therefore, we implemented a subsequent verification step, where Bob transmits an additional hash checksum for each error correction block to Alice. The checksums are generated using polynomial hashing, with a new random seed for each checksum. For each block, the hash, as well as the random choice of hash function is forwarded through the authenticated channel to Alice, where its correctness is verified. If a checksum mismatch occurs, the associated block is dropped.

We don't perform parameter estimation by random sampling, where Alice and Bob publicly compare the outcomes of a certain amount of randomly chosen detections with the expected outcomes, and calculate the error rate in each basis. Indeed, this method has the disadvantages that (i) it reduces immediately the final secret key rate as all revealed outcomes have to be discarded and (ii) in a finite key scenario it implies a high uncertainty of our estimate on the true error rate in the remaining, unrevealed detections. Instead, once we obtained a block of 10^6 bits error corrected and verified bits, Alice compares her corrected key with her original random bit sequence and counts the total of mismatches, which provides an exact number for the error rate. From this we calculate for each key block our estimate on the true bit error rate in the quantum channel.

Our FPGA implementation for privacy amplification uses Toeplitz hashing. Although this approach is not the most efficient in terms of communication bandwidth, it allows parallelized computation and efficient, scalable implementation in the FPGA hardware. Most importantly attributed to secret key rates in finite key scenarios, we have chosen a fix input length for privacy amplification of 10^6 bits. Our presented hardware implementation for privacy amplification has shown to treat up to 48 Mbit/s input rate and the compression ratio can be adjusted between 0 and 0.3.

For information-theoretic secure authentication of the classical communication we use polynomial hashing. This scheme is very efficient with respect to consumed secret bits as well as required operations. Still, we further decrease the secret bit consumption for authentication. Instead of new hash functions for each message we reuse always the same but keep it secret by encrypting every authentication tag with a one-time-pad. As a consequence, the amount of consumed secret bits is reduced to roughly a third. This authentication scheme was recently proven to be composably secure [7]. Finally, the prototype can distribute secret key up to 1 Mbit/s at short distances. The keys are then transferred from the key manager to a PC and to the fast encryptors.

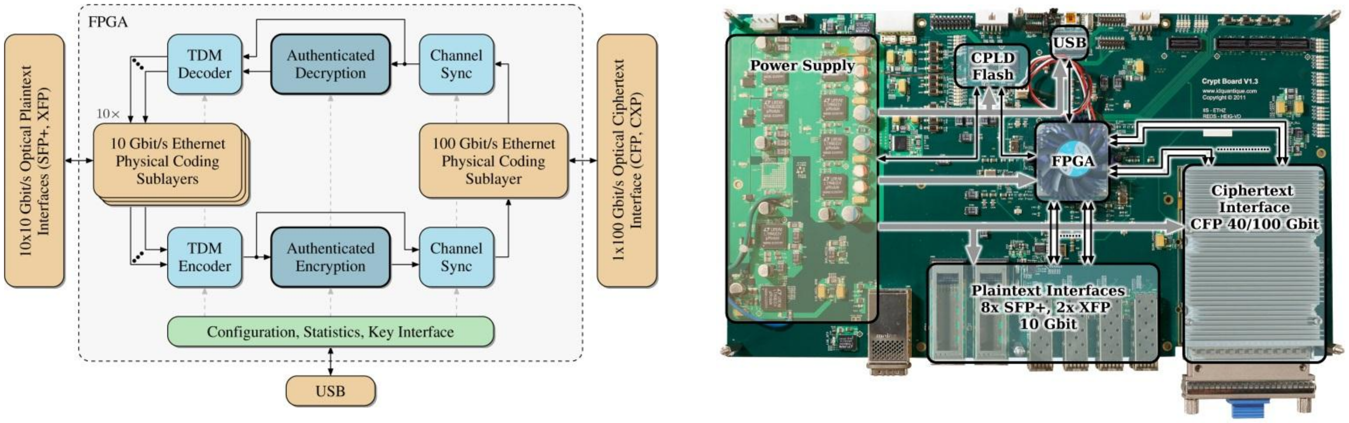
FPGA
TDM Decoder
Authenticated Decryption
Channel Sync
10×
10 Gbit/s Ethernet Physical Coding Sublayers
100 Gbit/s Ethernet Physical Coding Sublayer
TDM Encoder
Authenticated Encryption
Channel Sync
Configuration, Statistics, Key Interface
USB
10x10 Gbit/s Optical Plaintext Interfaces (SFP+, XFP)
1x100 Gbit/s Optical Ciphertext Interface (CFP, CXP)
Power Supply
CPLD Flash
USB
FPGA
Crypt Board V1.3
Ciphertext Interface CFP 40/100 Gbit
Plaintext Interfaces 8x SFP+, 2x XFP 10 Gbit

Fig. 2: High-level block diagram of the 100 Gbit/s encryption system. Right: 1st prototype PCB of the system.

100 Gbit/s Authenticated Encryption System

Fig. 2 (left) gives a high-level overview of the whole 100 Gbit/s data processing system. Plaintext data of the ten 10 Gbit/s Ethernet clients on the left side are converted to parallel in the physical coding sublayers and multiplexed into a single 100 Gbit/s data stream by the TDM encoder. This stream is encrypted and authenticated with the secure quantum key fed through the USB interface. The resulting ciphertext stream is then encapsulated into Ethernet frames and sent through the physical coding sublayer to the 100 Gbit/s optical interface. The receiving path of the system works similarly from right to left, decrypting and authenticating the received 100 Gbit/s data. The design ensures that all 10 Gbit/s Ethernet clients see a fully transparent link. The authenticated encryption core can be selected between OCB-Serpent, GCM-Serpent, OCB-AES or GCM-AES, providing alternative authenticated encryption scheme in case successful attacks should be developed against the existing primitives. The high refreshing rate of secret keys from the provably secure QKD makes the combined system to the fastest and most secure solution for huge data communication available today.

Missing suitable development boards, we have adopted a two-stage design process realizing two printed circuit boards (PCB). The first prototype is shown in Fig. 2 (right). The main functions are highlighted. The FPGA in the center performs all the data processing in the “FPGA”-marked area. It is one of the largest Stratix IV FPGAs in a 1932-pin ball grid array (BGA) package. The main challenge of the board design was the signal quality of the electrical 10 Gbit/s connections to all optical interfaces on a PCB with 24 conducting layers for the complex routing and high-current power distribution. We reached the goal of bit error rates below 10^{-15}.

References

[1] A. Tanaka *et al*., IEEE Journal of Quantum Electronics **48**, 542 (2012).
[2] A. R. Dixon, *et al*., Applied Physics Letters **96**, 161102 (2010).
[3] D. Stucki *et al*., New Journal of Physics **11**, 075003 (2009).
[4] www.nano-tera.ch/projects/404.php
[5] D. Stucki *et al*., Applied Physics Letters **87**, 194108 (2005).
[6] C. Roth *et al*., in Solid State Circuits Conference (A-SSCC), 2010 IEEE Asian (2010).
[7] C. Portmann, arXiv:1202.1229 [cs.IT] (2012).