Published in *Proceedings Volume 6583, Photon Counting Applications, Quantum Optics, and Quantum Cryptography*, Prague, Czech Republic, 16-19 april 2007, which should be cited to refer to this work.

DOI: 10.1117/12.722952

Coherent one-way quantum key distribution

Damien Stucki, Sylvain Fasel, Nicolas Gisin, Yann Thoma, Hugo Zbinden
Université de Genève / GAP-O
20 rue de l'École-de-médecine
CH-1211 Genève 4
Damien.Stucki@physics.unige.ch

Abstract

Quantum Key Distribution (QKD) consists in the exchange of a secrete key between two distant points [1]. Even if quantum key distribution systems exist and commercial systems are reaching the market [2], there are still improvements to be made: simplify the construction of the system; increase the secret key rate. To this end, we present a new protocol for QKD tailored to work with weak coherent pulses and at high bit rates [3]. The advantages of this system are that the setup is experimentally simple and it is tolerant to reduced interference visibility and to photon number splitting attacks, thus resulting in a high efficiency in terms of distilled secret bits per qubit.

After having successfully tested the feasibility of the system [3], we are currently developing a fully integrated and automated prototype within the SECOQC project [4].

We present the latest results using the prototype. We also discuss the issue of the photon detection, which still remains the bottleneck for QKD.

Introduction

The figure 1 presents the COW protocol. The information is encoded in time. Alice sends coherent pulses that are either empty or have a mean photon number μ<1, typically μ=0.5 (μ-pulse). Each logical bit of information is encoded by sequences of two pulses, μ-0 for a logical "0" or 0-μ for a logical "1". For security reason, Alice can also send decoy sequences μ-μ. To obtain the key, Bob measures the time-of-arrival of the photons on his data-line, detector D_B. To ensure the security Bob randomly measures the coherence between successive non-empty pulses, bit sequences "1-0" or decoy sequences, with the interferometer and detectors D_{M1} and D_{M2}. If wavelength of the laser and the phase in the interferometer are well aligned, we have all detections on D_{M1} and no detection on D_{M2}. A loss of coherence and therefore a reduction of the visibility reveals the presence of an eavesdropper, in which case the key is simply discarded, hence no information will be lost.

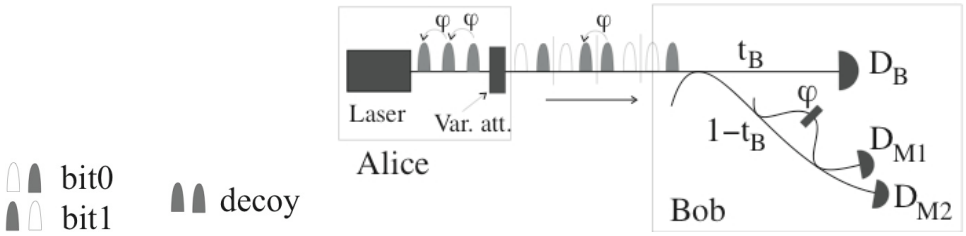

Figure 1: COW protocol

We still can underline that the system is very simple. Alice, the emitter, only needs to generate a sequence of coherent pulses. On Bob side, the data-line consists of only one detector, it can't be simpler, and the monitoring line is still there to ensure the security based on quantum physics.

The protocol is as follows:

- Alice generates a sequence of 0 and 1 logical bit (with probability (1-f)/2, for both case) and also of decoy sequence with probability f, and she sends the sequence of pulses to Bob
- Bob measures the time of detection on the detector D_B to generate the raw key and on the monitoring detector D_{M2} for the security
- Bob classically reveals the number of the bit when the data detector D_B clicks and the time of detections on the monitoring detector D_{M2}.
- From the time detection on the monitoring detectors, Alice check visibility at the output of the interferometer for decoy sequence and for bits sequences "1,0". If there is an eavesdropper, she will break the coherence between two successive μ-pulses and she can then be detected.
- If the security is guaranteed, Alice indicates to Bob which bits he has to removed from his raw key because they correspond to decoy sequences
- From the raw key, Alice and Bob generate the secret key with the classical processes of error correction and privacy amplification and obtain a shared secret key.

Experiment

The figure 2 presents a schematic of the implementation of COW QKD system for the SECOQC project. A large part of the system consists of electronics, computers and software.

Alice and Bob mainboards (www.ces.com) contain Virtex II Pro field programmable gate array (FPGA), Gigabit Ethernet link and SFP connectors. Ethernet link is used to connect the card to computer. Electrical and optical SFP modules allow the communication between the mainboards and the discrete electronics developed at GAP-O. Optical SFP modules are used for the synchronisation and the presifting between Alice and Bob (see below).

The programming of the FPGAs has been done by GAP-O and ARCsr Seibersdorf [5]. On Alice's side, the FPGA is used to generate the sequences of pulses. we use the RocketIO of the FPGA as serializer to output the data of Alice and as deserializer to input the data in Bob [6]. The pulse frequency is of 625MHz, thus the logical bit frequency is about 300MHz taking into account that we have about 10% of decoy sequences. We use a true-random generator (TRNG), used as frequent fresh seeds for a pseudo-random number generator in the FPGA. The sequence of electrical pulses goes through discrete electronics to translate the electronics level and amplify the signal to modulate the DFB laser at 1550nm with the lithium niobate intensity modulator. We still have a variable attenuator to adjust the mean number of photon μ to 0.5. Finally, we also have some digital-to-analog (DAC) converters and analog-to-digital converters (ADC) and laser diode controllers (TEC and LDC) to control the system.

On Bob's side, there is a 10/90 coupler at the input. Most of photons go directly on the detector D_B to generate the raw key with an InGaAs/InP avalanche photodiode (APD) detector. The rest of the photons goes in the interferometer and can be detected by the second APD detector D_{M2}.

Between Alice and Bob there are different channels. The sequence of coherent pulses coding the key is send on the quantum channel, a standard telecom fibre, but with no classical channel in order to avoid noise. In parallels, we send a synchronisation signal from Alice to Bob. The presifting channel is used to allow Alice to store only the data corresponding to a detection on Bob's side. This saves Alice from storing too large quantity of data. The classical procedures of error correction and privacy amplification are done on the classical channels (Alice to Bob and inversely). The last four channels can be in the same fibre.

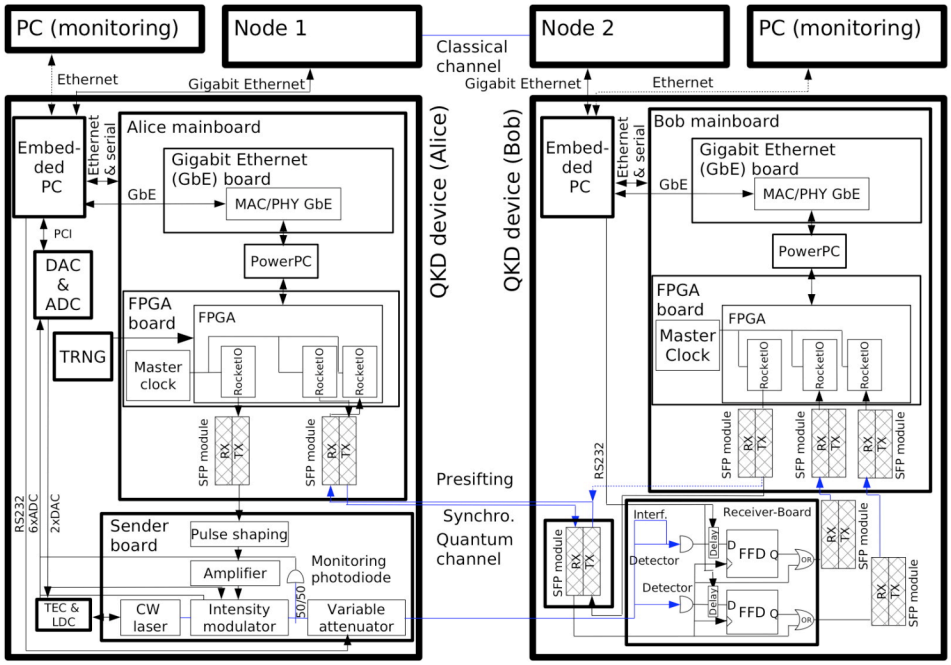

Figure 2: schematic of implementation of COW QKD protocol

Results

The measured mean secret key rate is larger than 2.2kHz, including authentication cost. If we take into account the alignment time, which is normally below 5%, we reach an average net key rate of about 2kHz key generation over 12 hours. We still have to improve the stability of the system to do measurement over days.

For the moment, the Quantum Bit Error Rate (QBER) is still too large, between 5 and 7%. To reduce this value, we are still working on the detectors and on the intensity modulator, see next two paragraphs.

We have tested a new detection system with InGaAs/InP photodiodes and with this new system we can reduce the noise probability by a factor 3 or 4. We obtain detection of 10% with a dark count probability of 10E-6 per ns or 30% and 2x10E-5. We are still working on the improvement of the duty cycle for the detection, since for the moment the detectors are active only 1% of the time. We hope to increase the detection duty cycle, and with InGaAs/InP detectors it should be possible to obtain 10kHz of net key. Note that for the moment, these improvements are not fully integrated in the system.

Due to the high modulation rate, we still do not achieve a satisfactory extinction of the intensity modulators. This introduces noise because empty pulses may contain still some light. This explains about 4% of the QBER the remaining part being due to the detector. We are still working on this problem.

Conclusion

Today's point-to-point quantum cryptography system developments involve more electronics and software than optics. Our system looks promising, though there is still a long way to assure the necessary reliability over weeks and months.

References

[1] N. Gisin et al., Rev. Mod. Phys., 74, 145-195 (2002)

[2] www.idquantique.com, www.magiq.com.

[3] D. Stucki et al., Appl. Phys. Lett. 87, 194108 (2005).

[4] www.secoqc.net

[5] www.arcs.ac.at

[6] A serializer takes n bits in parallels at input at a frequency f and send bit per bit at a frequency nxf. A deserializer takes data in serie of n data at frequency nxf and outputs n data in parallels at frequency f.