Prototype of a Quantum Cryptography System for the End User

R. PIZZI, D. ROSSETTI
Department of Information Technologies
Università degli Studi di Milano, Crema Campus
via Bramante 65, 26013 Crema CR
ITALY
rita.pizzi@unimi.it  http://www.dti.unimi.it/pizzi

Abstract: It is known that the quantum cryptography protocols are able to detect immediately any attempt to attack the key generation and the exchange process. The well-known BB84 protocol (C. Bennet e G. Brassard 1984) uses the quantum property which states that orthogonally polarized states can be completely discriminated, thus can be used to codify information. The developed system adopts a properly costumized BB84 protocol.

The hardware instrumentation includes two fast PCs with acquisition card, a 4-channels transmitter, 4 high-efficiency LED diodes, a receiver with 4 high-sensitivity avalanche photodiodes, and suitable optical devices. Transmitter and receiver have been realized by means of two custom electronic cards, that are driven by two separated PCs with suitable software devoted to the signal generation and decoding procedures. The system is a prototype that can be further improved in order to be used in end user money transactions and to allow each one to afford the quantum cryptography security level. The system can be further downsized to develop quantum cryptography circuits embeddable in mobile devices to ensure the maximum security in money transfer and controlled access.

Key-Words: Quantum, Cryptography, Photon, Polarization

1 Introduction

After the enthusiasm of the first research years, the technical problems connected to the real implementation of quantum gates eliminated the idea of quantum information as a big promise for an immediate future. However, research goes on with slow but continuous achievements [1][2][3][4].

But it is often not known that a real-world application of quantum information is mature ad produces commercial applications: it is quantum cryptography, that allows the secure data transmission without the need to make any assumption about the computing power of an attacker [5][6][7][8].

Quantum cryptography uses photons to transfer information, using the quantum principle that if anyone tries to spy on the photons' travel along its path, their encoded state will change, allowing to immediately detect this intrusion.

Nowadays Quantum Cryptography works on optical fiber only on limited distances, experimentally over 100 km [9][10]. Quantum repeaters should be introduced to improve distance and usability.

Researchers throughout the world are experimenting new techniques in order to transmit quantum keys through the air rather than over optical fiber lines. The idea is that information can be transmitted to satellites and from satellites to the earth again.

The quantum cryptography performances have already captured the interest of banks, companies and institutions, and many of them are testing this technology, that is commercially available: MagiQ Technologies New York [11], idQuantique Geneve [12] SmartQuantum York [13] already sell quantum cryptography systems, and QinetiQ, Toshiba e the NIST institution are deeply involved in this technology.

Nowadays the cost of a Quantum Cryptography system can be estimated around one hundred of thousands of dollars, but we expect that it will get cheaper and manage longer distances in the next few years. These expected progresses are targeted to multinational and financial companies. Nonetheless, the need of secure data transactions is universal and the existence of a security technology that cannot be jeopardized by the advances of the computing power, as in classical cryptography, becomes more and more interesting while the online transactions become more and more widespread in the daily life of any citizen. We know that crimes connected to ATM terminals, mail orders, online transactions, are growing day by day.

This is the reason why the transition from a complex and expensive quantum cryptography technology to low-cost systems suitable for end user applications should be explored with the maximum attention [14].
Our prototype is intended to move along this direction and shows the feasibility of a compact and affordable quantum cryptography, to be included in the user’s PDA or smart phone.

2 The System

2.1 The BB84 Protocol

The basic idea of quantum cryptography dates back to 1969 when a PhD student at Columbia University, Stephen Wiesner, proposed it to his friend Charles Bennett. Only many years later Bennet formulated together with Gilles Brassard a complete quantum cryptography protocol, the so-called BB84 algorithm [15][16][17].

It is known that the act of observation affects a quantum system and modifies it. Thus the main difference between classical and quantum bits is the fact that in the first case we have fixed and manageable objects, in the second one any external action inevitably corrupts the bits themselves. A theorem shows that any interference with the original target string involves a certain probability to corrupt the sequence of the results obtained by Alice (the transmitter) and Bob (the receiver) [18][19].

The inviolability of the quantum code does not depend on the ability of the eavesdropper, nor on the computing power that he has at its disposal, but stems from a law of nature.

Let’s imagine now that Alice and Bob decide to use photons to encode their communications (quantum channel). Alice and Bob can also communicate via a public channel (phone, Internet). Alice chooses photons polarized in four different directions: horizontal (A), vertical (B) to +45° (C) and -45° (D).

Alice chooses a random series of polarized photons and records them before sending them to Bob. Bob is endowed with analyzers that allow detection of the polarization of photons.

Bob carries out the reading, using an analyzer at random for each photon, and records the sequence of the used analyzers.

After analyzing a number of photons of suitable length, on the public channel Bob communicates his sequence to Alice, avoiding to include the obtained results. Alice checks the sequence and, on the public channel, Alice and Bob agree to delete the cases in which they performed measurements on different directions, without specifying the photon polarizations. They share now a correct sequence of photons.

For the above mentioned theorem, you can also determine if Eve (the eavesdropper) has tried to intercept the message. In fact Alice and Bob choose a small set of the consistent series of photons and verify through the public channel if there is a due correspondence between the initial input sent from Alice and the results obtained by Bob. If such correspondence is confirmed, Alice and Bob can derive the result that no one has tried to read the message.

In fact, the probability that on N measures no discordant result is present will be \( \left( \frac{3}{4} \right)^N \), i.e. the event you have N coincident results even in the presence of an eavesdropper is absolutely negligible. The errors of communication that still exist can be minimized with error correction and privacy amplification software [20] [21].

2.2. Transmission and Receiving process

The developed hardware consists of two custom circuit boards: transmitter and receiver.

The transmitter consists of an electronic circuit suitable to drive four high-performance LED diodes. Equally, it was necessary to develop a four-channel receiver equipped with high-sensitivity avalanche photodiodes. The two cards are driven by two separated computers equipped with appropriate software, written in C, to generate and decode the signals.
The transmission circuit is driven by software that generates two random logic signals, formed by two individual bits, applied to two pins of the parallel port, then sent to the circuit. Another synchronization bit is generated to ensure the same duration for the transmitted bits.

The transmission circuit through a multiplexer modifies the two bits into four random bits which drive the transistors which are responsible for lighting the high-precision Agilent HLMP-EL08-VY000 LEDs. Fig. 1 shows that the sequence of two bits from the PC, through the multiplexer, switches on the four LEDs in sequence.

The receiving circuit is the most complex one as it must re-establish the data sequence in a reliable way.

An acquisition card acquires and sends the bits to the second PC after amplification, suitable processing and level adjusting.

The PerkinElmer C30902EH avalanche photodiode, able to detect the single photon, is the component responsible for transforming the light received from the LEDs into electrical signals. Even though this component has an extremely high sensitivity, the current output is very weak and must be amplified.

The receiver’s front-end uses the IVC102 integrated circuit, with a high impedance input FET that allow to detect a current in the fA range, followed by a second amplification and a trigger circuit.

The integration time depends on the current input and on the internal capacitance and we can vary it from 30 µs to 1 minute. The output voltage of the IVC102 at the end of the integration period will be proportional to the current input.

The time diagrams shown in Fig. 2 give an idea of the dynamics and the performances of the component. The amplifier gain can be varied by changing the internal integration capacitance, by adding external capacitors.

Our case involves the construction of four individual channels on a single card, using four IVC102 integrated circuit with SMD technology. The chosen integration capacitance value is 100pF.

Standard lenses and polarizing filters complete the system.

The adopted optics can vary depending on the system applications, which can be developed both in free air or via optical fibers. In free air, as is the case of personal devices applications, the performances of the system should be improved as the BER increases dramatically due to presence of thermal and optical noise.
3 Conclusions and Future Developments

We described a compact and affordable prototype of a quantum cryptography system for the end user. The implementation of both hardware and software has been completed and we are facing the stage of calibration and testing. This stage is expected to be concluded within summer 2009, in order to use the system for educational purposes as early as the next academic year.

The commercial applicability of the system is linked to improved system performances, what will happen with the replacement of some components: primarily the photodiodes will be replaced with the DTC-cooled C30902SH that can be operated at -20 °C, reducing thermal noise and allowing constant performances over an extended temperature change. Secondly, the random number generator, currently developed with a software algorithm, will be replaced with the IdQuantique QRNG system, a portable and low-cost device.

In fact it is known that any algorithmic random number generator, although advanced, is in principle predictable.

Finally, robust error correction and privacy amplification algorithms will be implemented. Once tested and refined, this system can be proposed as an affordable and effective device for commercial exploitation of quantum cryptography for the end user.

References: