ISSN:2231-0711
www.ijcset.net

Affordable Quantum Cryptography System for Mobile Devices

Rita Pizzi[#1], Danilo Rossetti[#], Davide D'Arenzo[#]

[#]*Department of Information Technology*
Via Bramante 65 , 26026 Crema CR
Università degli Studi di Milano
[1]rita.pizzi@unimi.it

***Abstract*— The today's technology allows us to design simple quantum cryptography circuits embeddable in mobile devices to ensure the maximum security in money transfer and controlled access. It is known that the quantum cryptography protocols allow a virtually perfectly secure key generation and exchange process. This technology uses the quantum property which states that orthogonally polarized states can be completely discriminated, thus can be used to codify information.**

The system presented in this paper 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 highsensitivity photodiodes, and suitable optic devices.

Transmitter and receiver consist of two custom electronic cards with suitable software for random bit generation and decoding procedures The software also allows to reconstruct the shared secure key. The system has been realized with the purpose to be included in mobile devices and to allow each one to afford the quantum cryptography security level, both for ATM operations and e-commerce transactions.

***Keywords*— Quantum cryptography, BB84, secure key**

I. INTRODUCTION

It is known that research is under way for years to realize the quantum computer, but progresses are slow due to serious technological obstacles [1,2,3,4]. However, a practical application of methods of quantum information exists: it is quantum cryptography [5,6,7,8].

Quantum cryptography (QC) allows the secure transmission of data regardless of the computational power of potential intruders.

Currently QC allows transactions up to 100 mile through optical fiber. [9,10]. Few weeks ago Durban, South Africa, announced that the city has been completely wired with this methodology and it will soon be the turn of Tokyo and London. However, this technology must be improved, first and foremost it is urgent to solve the problem of quantum repeaters, which would give the possibility to increase the distances. Many researchers are working on the idea of not only transmit data over optical fiber but also in free air using satellites.

The high performance of the QC have captured the interest of banks, corporations and institutions. Several companies already provide commercial systems: MagiQ

Technologies New York, idQuantique Geneve, SmartQuantum York [11,12,13]. QinetiQ UK (defense), Toshiba Corporation, Tokyo, and U.S., and the NIST (National Institute of Standards and Technology, U.S. government agency) are acquiring the technology.

The cost of these systems currently stands at around $ 100,000, but it is expected that the price declines rapidly with increasing dissemination.

However, the need for secure transactions is not only a problem of big companies: even home users that access to ATMs and those using the Internet for online transactions require the utmost security.

This is why a QC system compact and low cost [14] might be of interest to a wide range of users. The system described below is a working miniaturized QC module ready to be included in a Smartphone.

II. METHODS

The birth of QC can be settled around 1969, when a graduate student proposed the first idea of a secure quantum information transmission to Charles Bennett. Bennet formalized the idea much later, in 1984, along with Gilles Brassard [15,16,17].

It is known that in quantum physics the act of observation affects the quantum system and thus its information content.

So if Alice (transmitter) sends quantum information to Bob (the receiver), any intruder E (Eva) will alter the sequence information, and whatever its computational power will not be able to recover the initial sequence.

The BB84 protocol is based on the polarization properties of photons. It is known that polarizing filters can block or allow the photon transmission according to their state of Polarization (Fig.1).

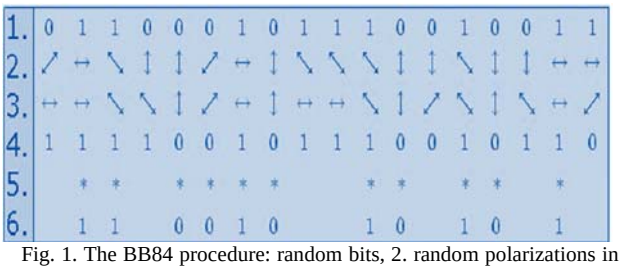

Fig. 1. The BB84 procedure: random bits, 2. random polarizations in transmission, 3. random polarizations in reception, 4. actually received bits , 5. coincident polarizations, 6. shared quantum secure key

Now imagine that A and B can communicate through a quantum channel (photons) and a public channel (e.g. Internet or the telephone).

A chooses a random series of polarized photons with four different polarizations: vertical, horizontal, 45 °, -45 °, the record and sends it to B. B in turn uses a random polarization analyzer to receive the photons.

On the public channel, B communicates to A the sequence of polarizations detected by his receiver.

A controls the sequence and on the public channel which communicates with B cancels all the bits where the sequence of polarizations reported by B does not coincide with that of A.

A and B now share an identical sequence of polarizations, a secret key that is perfectly safe.

.

If an intruder E tries to intercept sequence of photons, A and B would notice it immediately [18,19,20]. In fact there is a specific statistical error for this type of transmission: if the intruder intercepts the sequence of photons, thanks to the laws of quantum physics the statistics suddenly changes, revealing the presence of an intruder, and A and B can immediately stop the transmission.

Errors can then be further minimized through techniques of error correction and privacy amplification [21].

III. THE PROPOSED SYSTEM

Our system consists of two parts, the transmitter and receiver, that perform a customized BB84 procedure.

The transmitter is a custom electronic circuit that drives four high-performance LEDs, with polarizing filters. Their intensity is appropriately attenuated. Software generates random logic signals that light up in sequence the four LEDs (Fig. 2).

The receiver circuit must restore the sequence data starting from the received photons.

To this purpose, four high-performance photodiodes (PerkinElmer C30902EH avalanche photodiodes) convert the photons passed through four polarizing filters into electrical signals which are then converted into bits. This is made possible by a logic analyzer that shows the peak voltage from the photodiodes (Fig.3).

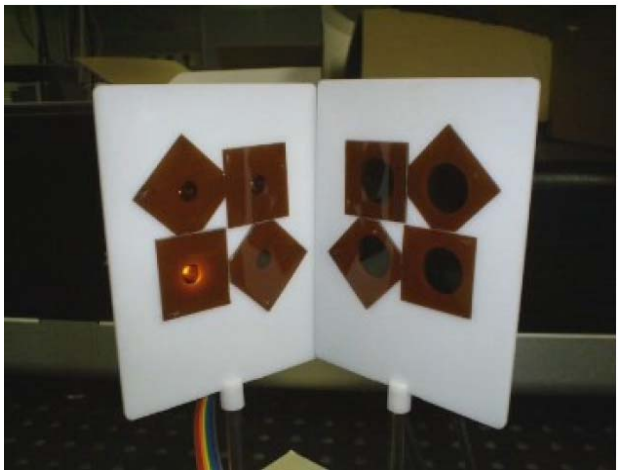

Fig. 2. The prototype on optical bench

A software written in C drives the entire process on two separated PCs.

In the first PC software, using the Blum Blum Shub algorithm for pseudo-random number generation, it generates and synchronizes the sequence of bits that through the parallel port will light up the LEDs. On the second PC the software reads and synchronizes the reconstructed signal by means of a logic status analyzer .

We also fully implemented the comparison procedure of the sequences generated by transmitter and receiver on the public channel, getting in clear the secure key at the end of the execution process.

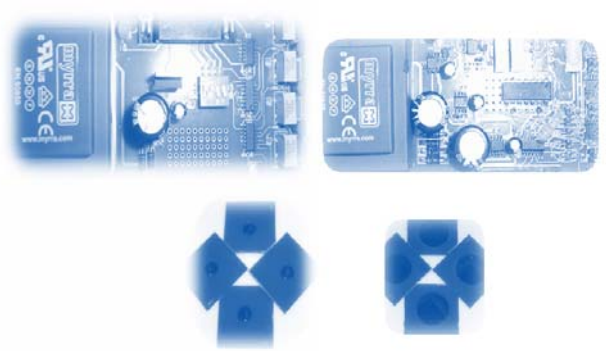

Fig. 3. The transmitter and receiver modules

IV. CONCLUSIONS AND FUTURE DEVELOPMENTS

The main difference between the expensive commercial QC systems and our proposal is the use of four polarized LEDs instead of a cumbersome and expensive laser technology that switches polarization at extremely high speed.

Currently the system is a compact prototype on optical bench, but we are working on its downsizing to make it available for use on optical fiber for Internet transactions, or applicable to ATM terminals.

By transferring the C-written firmware into a processor memory, the transmitting module will be extremely small and suitable to be applied to a smart phone.

The receiving module is already small enough to be included into an ATM terminal.

It can also be adopted by companies that are willing to improve the online transaction security of their e-commerce transactions. The end-user will plug his transmitting module into a small reader connected to the home PC, not bigger than a normal card reader.

Performances of the system are now improved through the use of high performance components, i.e. avalanche photodiodes that ensure the reliable detection of a single photon. We will also replace the pseudo-random number generator with the more secure hardware IdQuantique generator, a portable and low-cost solution.

The software algorithms are also going to be improved by applying robust methods of error correction and privacy amplification.

REFERENCES

[1] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM Journal on Computing* No. 26, 1997, pp. 1484-1509.

[2] M. Nielsen, and I. Chuang, *Quantum Computation and Quantum Information.*Cambridge University Press, 2000.

[3] D. Bouwmeester, A. Ekert, and A. Zeilinger, *The Physics of Quantum Information*, Springer-Verlag, 2000.

[4] J. Gruska, *Quantum Computing*, McGraw-Hill, 1999.

[5] A. Ekert, "Quantum cryptography based on Bell's Theorem", *Physical ReviewLetters*, Vol.67, N.6, 1991, pp. 661-663.

[6] C. Elliot, "Quantum Cryptography", *IEEE Security and Privacy Magazine*, Vol.2 No 4, 2004, pp. 57-61.

[7] V. Scarani, H. Bechmann-Pasquinucci , N. J. Cerf , M. Du˘sek , N. L¨utkenhaus, M. Peev, "The Security of Practical Quantum Key Distribution", *arXiv:0802.4155v2 [quant-ph] 19*, Sep 2008.

[8] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum cryptography", *Reviews of Modern Physics* No 74, 2002, pp. 145-195.

[9] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber", *Appl. Phys. Lett.* 84, 3762, 2004.

[10] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller and J. E. Nordholt," Long-distance quantum key distribution in optical fiber", *New J. Phys*. Vol. 8 No. 193, 2006.

[11] MagiQ Technologies. http://www.magiqtech.com/

[12] ID Quantique, http://www.idquantique.com/

[13] SmartQuantum, http://www.smartquantum.com

[14] J. L. Duligall, M. S. Godfrey, K. A. Harrison, W. J. Munro and J. G. Rarity, "Low Cost and Compact Quantum Key Distribution", *arXiv:quant-ph/0608213v2 3*, Oct 2006.

[15] G. Brassard, N. Lutkenhaus, T. Mor and B.C. Sanders," Limitations on practical quantum cryptography", *Phys. Rev. Lett. (USA)* Vol**.** 85 , pp.1330-3, 2000.

[16] G. Brassard, Modern Cryptology: A Tutorial, *in. Lecture Notes in Computer Science*, Vol. 325, Springer-Verlag, 1998.

[17] C.H. Bennett, and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", In *Proceedings of International Conference on Computers, Systems and Signal Processing*, New York, 1984.

18] D. Mayers," Unconditional security in quantum cryptography", *Journal of theACM*, Vol. 48, No. 3, 2001, pp. 351-406.

[19] W.K. Wootters and W.H Zurek, "A Single Quantum Cannot be Cloned", *Nature*, No. 299, 1982, pp. 802--803.

[20] M. Maurer and J. L. Massey, "Cascade ciphers: The importance of being first", *Journal of Cryptology*, Vol. 6, No. 1, 1993, pp. 55–61.

[21] Bennett, C. H., Brassard, G., & Robert, J. M., "Privacy amplification by public discussion", *SIAM Journal on Computing*, Vol.17, N. 2, 1998, pp. 210-229.