Quantum Cryptography: Approaching Communication Security from a Quantum Perspective

Alberto Porzio
CNR – SPIN and INFN – Napoli
Monte Sant'Angelo, via Cintia
80126 Napoli, Italy
e-mail address: alberto.porzio@spin.cnr.it

***Abstract*— Quantum cryptography aims at solving the everlasting problem of unconditional security in private communication. Every time we send personal information over a telecom channel a sophisticate algorithm protect our privacy making our data unintelligible to unauthorized receivers. These protocols resulted from the long history of cryptography. The security of modern cryptographic systems is guaranteed by complexity: the computational power that would be needed for gaining info on the code key largely exceed available one. Security of actual crypto systems is not "by principle" but "practical". On the contrary, quantum technology promises to make possible to realize provably secure protocols. Quantum cryptology exploits paradigmatic aspects of quantum mechanics, like superposition principle and uncertainty relations. In this contribution, after a brief historical introduction, we aim at giving a survey on the physical principles underlying the quantum approach to cryptography. Then, we analyze a possible continuous variable protocol.**

Keywords—Quantum cryptography; Continuous Variable

I. INTRODUCTION

Ever since its birth in the early 20th century, quantum mechanics started a scientific revolution. So that, every time we use electronics devices or transmit and receive information we unwittingly exploit our knowledge of the quantum nature. However, there is still plenty of room for exploiting quantum properties in information technologies. Since the early 80's of last century, scientists have recognized quantum aspects as a resource for realizing protocols forbidden by classical laws of physics. Moreover, we all know that the increase in performances in modern computers goes hand in hand with size reduction. So that, soon or later, a single transistor will be so small that it will be necessary to account for quantum effects to fully understand and deterministically predict its behaviour.

II. A BIT OF HISTORY

The first documented use of a trick for a secret communication dates back to the ancient Greeks. In his Histories, Herodotus tells of a messenger that had a message imprinted on the scalp under his hairs. Then, he went to an allied king camp with the only instruction of asking to be shaved thus proving that the quest for secret *unbreakable* communication roots at the very beginning of human history.

True cryptology is based on the presence of a *code*: a (complex) mathematical tool that allows to hide the message in such a way that only authorised parties (aware of the code) can decrypt it. So that, the two main goals for cryptographist are: a) to communicate in a way unintelligible to unauthorised third parties; b) to authenticate the communication channel.

Up to the development of radio and telegraph, crypto-messages conveyed on paper so that two parties had to physically share the code at a former time [1]. In such a paper-based world, interception was easy to detect. Later, the moving to immaterial communication has first meant the search for more complex coding then, the discard of specific crypto-machine replaced by specific computational algorithms.

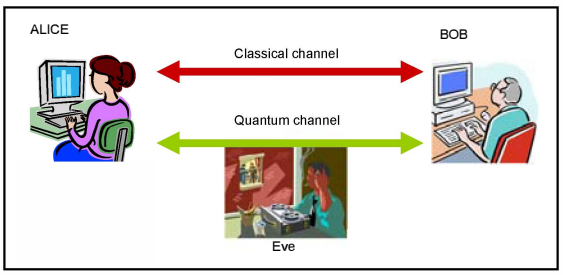

Fig. 1 The setting of a generic QC link: Alice and Bob connect by two channels a quantum one, into which Eve can tap without any restriction other than the laws of physics, and by an authenticated classical one, into which Eve can only passively listen.

Nowadays, communication run over *open* channels so that avoiding interceptions is impossible. Thus, it is

necessary to code the message in a way that would be impossible for an intruder to break the code.

The security of a cipher alphabet was, by that time, demanded to complex electro-mechanical machines able, at the sender station, to shuffle the original message into a pseudo-random sequence of symbols and to revert the process at the receiver. The idea behind mechanical crypto-machines was to make the decoding so complex that no man would have been able to solve it. The quest for complexity took cryptology into a completely novel scenario.

The increasing in complexity triggered extensive research in the field.

III. THE BIRTH OF QC

As often happens in science, while actual algorithms have satisfied the "commercial" quest for a "practically" secure system, scientists have continued the search for provably secure ones. Moreover, security of RSA, the most used crypto protocol nowadays, resides on the, not disproven, fact that no efficient factorization algorithm able to break it in reasonable times is known.

We now know that if quantum computers will be ever available, RSA could be broken by Shor's quantum algorithm [2] able to factorize large numbers in a very efficient manner exploiting entangled states. The quantum door was open!

Before giving a look inside, we need to get familiar with a generic setting for a QC protocol (see Fig. 1). **Alice** is the sender, **Bob**, the receiver and **Eve** represents the *eavesdropper*. A **quantum channel** is a channel open to the public and on which anyone can manipulate information, contrarily to a **classical channel** where only *listening* is allow for third parties. A QC link requires Alice and Bob to talk over a classical channel to authenticate their-selves and send classical information forth and back. Then, a quantum channel will convey quantum information between the two.

As mentioned, the open classical problem was essentially the *key distribution* process. In general, a QC protocol will provide Alice and Bob with nearly identical shared keys. Then the two parties have to compare their strings in order to estimate the communication error level. These errors can be caused by Eve interceptions, channel imperfections (as losses), and detectors' inefficiencies and/or dark counts. To make it more difficult, distinguish among these types of errors is physically impossible. Therefore, to theoretically evaluating the level of security of a specific protocol one has to assume all the errors due to eavesdropping. QC tries to answer to the following question: "Is really possible to generate and distribute, in a provably secure way, a sequence of truly random numbers to form a shared trusted key?"

QM provides the answer. It tells us that any quantum measurement destroys the information the quantum system is carrying [3]. Moreover, the *no-cloning* theorem [4] forbids *cloning* of the state of a *quantum* system. So that, if we will be able to prepare quantum systems able to carry the information in their quantum state then only one user can faithfully receive that information. The conceptual scheme is: a) Alice prepare a quantum system in well definite (and known to her) quantum states; b) faithfully transmit them to Bob site; c) Bob measure quantum states.

This *proof-of-principle* scheme that have triggered several proposal for QC protocols. The first one by Charles Bennett and Gilles Brassard, and is, nowadays, worldwide known as the BB84 protocol [5]. Thanks to the possibility of realizing coherent superposition of quantum states, it is possible to convey over a single channel two distinct information coded onto a single quantum system. At the same, thanks to the Heisenberg indeterminacy principle, only one information is accessible at the end of the transmission.

Later, it has been found that also systems, more complex than single quanta ones, can convey quantum information provided that: a) they can be prepared as coherent superposition; b) there is an easy access, on them, to a pair of quantum non-commuting observables obeying to the Heisenberg principle.

These ideas translate into the telecommunication language. Bright, laser-like, beams will play as complex systems.

A. *Continuous variable quantum cryptography*

Fifteen years later than BB84 in 1999, Ralph recognised that it would have been possible to encode quantum information onto bright beams [6] as phase and amplitude modulation of a pair of entangled carrier beams. In the *quantum* domain, the field quadratures, a pair of non-commuting observables, represent phase and amplitude of optical field. The name *continuous variable*

comes from the fact that these operators can assume a continuum of values.

The first CV proposals borrowed from DV protocols three key elements: a) the use of different measurements; b) the introduction of random elements both at the transmitter and at the receiver; c) the requirement for classical communication at the end of transmission in order to distil the key from a longer data set. The technologic challenge, in the CV context, is, on the contrary, rather different and simpler relying, more than in the DV case, on techniques and methods already integrated in standard telecom network as *e.g.* the use of modulation coding/decoding and homodyne and/or heterodyne detection. However, these first proposals were still conceived with binary alphabets [7].

The turning point for CV QC was the finding that more sophisticate modulation techniques would have strongly enhanced the system performances. In particular, the use of Gaussian modulation [8] makes it possible to use multi-digit alphabets strongly enhancing the in principle attainable bit rate. This intuition, paved the way to a rapid development of different systems of increasing performances mostly based on coherent states [9]. The use of coherent states, states laying at the classical-quantum boundary, allows to overcome decoherence limitations [10,11]. Shortly after, no-switching protocols [12], have further simplified the CV scheme demonstrating that, at the receiver station, simultaneous measurement of two non-commuting observables can be made with no random switching of the measurement apparatus, thus allowing to greatly simplifying the setup and enhancing the allowed bit rates.

It is important to note that these last two protocols are, today, the most promising approaches for realizing commercial system. In the following, we will shortly describe the above protocol that is the progenitor of all the CV ones. In particular, we will try to enlighten the characteristics of a general CV QC scheme.

The scheme of the protocol is very simple: a) Alice maps a random variable a onto a quantum system and sends it to Bob; b) Bob measures the signals extracting b (strongly) correlated to Alice's a; c) Alice and Bob by classical post-processing obtain the secret key from their own raw data (a and b).

The Gaussian modulated coherent state protocol, initially proposed by Grosshans and Grangier [9], consists of a quantum part followed by a properly designed classical post-processing. The former starts with the generation [13], at Alice site, of a set of coherent states $|X_A + iY_A\rangle$ where X_A and Y_A are randomly Gaussian distributed variables with "zero" mean value and a given variance (chosen by Alice). These states travel to Bob station and, upon arrival, he measures either X_B or Y_B for each of them by homodyne detection. At this point quantum communication ends. Alice and Bob share an ensemble of Gaussian distributed correlated data. We note that the vacuum noise entering the system through loss mechanisms and/or interception makes the values obtained by Bob different but correlated to the values encoded by Alice.

The classical post-processing comes straightaway. Bob tells, on a classical channel, which observable X_B or Y_B he has measured for each time slot so that Alice can discharge useless data. At this point they share two Gaussian distributed set of correlated variables. They need to transform continuous values into binary strings. This happens by the *sliced* reconciliation protocol [14]; also used to discharge data affected by transmission errors. Standard privacy amplification can be, at the end, applied for extracting the secret key.

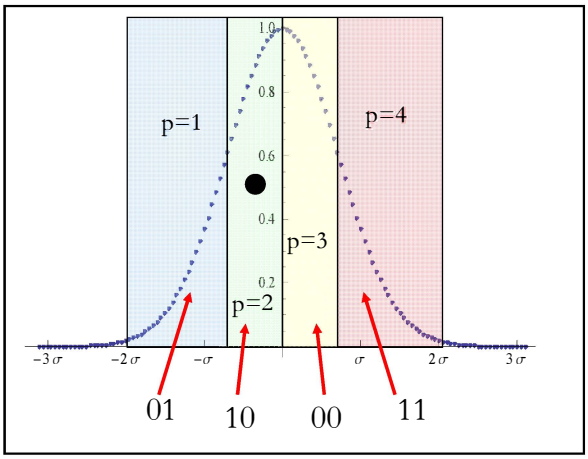

Fig. 2. Graphic representation of the sliced reconciliation protocol that allows distilling a multi-bit string of digitalized value from a Gaussian distributed random variable. The distribution is sliced into n (in Fig. $n=4$) regions each statistically containing the same number of data. Then, to each region a (multi-)bit value is assigned following an algorithm designed to increase data distinguishability [15].

In Fig. 2 a graphic representation of the sliced protocol is given. The Gaussian distribution of the data is sliced into n regions of equal statistical weight. Then,

to each region a string of *n/2* bit is assigned by an algorithm designed for increasing data distinguish-ability. Then each measurement get its value from the statistical region it falls in. Note that such a protocol convert into a digital binary string not the single datum but its position in the data distribution. In this way the only request for building a key is that Alice and Bob data are similarly distributed.

We conclude this section by noting that all, DV as well as CV, protocols require sophisticate mathematical tools for the so call reconciliation and privacy amplification steps. QC seats in between different fields of science involving mathematics, physics, and information and communication technologies.

IV. CONCLUSIONS

As a summary of this contribution we wish to conclude by comparing, shortly, DV and CV protocols.

Single photons, DV, protocols require specially designed systems where single photon detection, actually showing very low efficiency (10%) in the telecom window, plays a crucial role for reaching high bit-rates. Moreover, key rates are limited also by the problem of realising single deterministic sources of single photon states. At the same time, the protocols are quite simple and security has been unconditionally proven.

On the contrary, CV systems employ weak coherent light readily attainable in standard lasers. Homodyne detection guarantee efficiencies as high as more than 90% with commercial components. The rate is strongly enhanced by multi-bit transmission Gaussian protocols up to Mbit per second. The integration of CV systems in standard existing telecom infrastructure is rather immediate.

While decoherence, actually, limits intrinsically the distance a CV link can reach, in the DV case it "only" reduces the attainable key rate.

For the above reason a definitive answer to the crucial question whether CV is better or not than DV is not possible. We believe that, actually, the two approach will continue to be both pursued.

REFERENCES

[1] Brief histories of crypto techniques and machineries is at: http://en.wikipedia.org/wiki/History_of_cryptography ;

[2] P.W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring" in Proceedings of the 35th Annual Symposium on Foundations of Computer Science (ed. Goldwasser, S.) pp. 124–134 (IEEE Computer Society Press, 1994), see also SIAM J. Comput. 26:1484 (1997);

[3] Carl W. Helstrom, "Quantum Detection and Estimation Theory", (Academic Press Inc., New York, 1976, ISBN 0123400503); J. A. Wheeler and W. H. Zurek, "Quantum Theory and Measurement", (Princeton Univ. Press, Princeton, 1984, ISBN 0691083169);

[4] W. K. Wootters, e W. H. Zurek, "A single quantum cannot be cloned", Nature, vol. 299, pp. 802-803, Oct 1982;

[5] C.H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing", Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, December 1984, pp.175-179 (1984);

[6] T. C. Ralph, "Continuous variable quantum cryptography", Phys. Rev. A, vol. 61, n. 1, pp. (010303)1-4, Jan 1999;

[7] A. Porzio, V. D'Auria, P. Aniello, M.G.A. Paris, S. Solimeno, Quantum communication exploiting above threshold OPO intensity correlations and polarization encoding", Opt. and Laser in Engineering, vol. 45, n. 4, pp. 463-467, Apr. 2007;

[8] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States", Phys. Rev. Lett., vol. 88, n. 5, pp. (057902)1-4, Jan 2002;

[9] F. Grosshans, G. van Assche, J. Wenger, R. Tualle-Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states", Nature, vol. 421, n. 3, pp. 238-241, Jan. 2003;

[10] D. Buono, G. Nocerino, A. Porzio and S. Solimeno, "Experimental analysis of decoherence in continuous-variable bipartite systems", Phys. Rev. A, vol. 86, n. 4, pp. (042308)1-12, Oct. 2012;

[11] G Nocerino, D Buono, A Porzio and S Solimeno, "Survival of continuous variable entanglement over long distances", Phys. Scr., vol. T153, pp. (014049)1-6, Mar. 2013;

[12] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum Cryptography Without Switching", Phys. Rev. Lett., vol. 93, n. 17, pp. (170504)1-4, Oct. 2004;

[13] G Mauro D'Ariano, Martina De Laurentis, Matteo G A Paris, Alberto Porzio and Salvatore Solimeno, "Quantum tomography as a tool for the characterization of optical devices", J. Opt. B: Quantum Semiclass. Opt., vol. 4, n. 3, S127-S132, Jun. 2002;

[14] N.J. Cerf, S. Iblisdir, and G. Van Assche, "Cloning and cryptography with quantum continuous variables", Eur. Phys. J. D, vol. 18, n. 2, pp. 211-218, Feb. 2002;

[15] Gilles Van Assche, Jean Cardinal, and Nicolas J. Cerf, "Reconciliation of a Quantum-Distributed Gaussian Key", IEEE Trans. Inf. Th., vol. 50, n. 2, pp. 394-400, Fab. 2004.