A new idea of Xor Quantum survey code Based on Error Correcting Codes

Aris Skander

Electromagnetism and Telecommunication Laboratory, Department of Electronics
Faculty of Engineering. Constantine University, 25000 ALGERIA.
arisskander@yahoo.fr

Abstract

Quantum Error Correction will be necessary for preserving coherent states against noise and other unwanted interactions in quantum computation and communication. We have made a modest contribution for securing quantum information using error code correction approach by the BB84 protocol. The aim of the research presented in this paper is to investigate the Xor Linear code with Generator Matrix in the quantum error correction. These techniques were found to provide a successful method of quantum automated and a variety of the ciphers application, we would like to explain Quantum Cryptography by the example of a standard polarization-based setup (BB84 protocol). We estimate the practical limits of quantum cryptography. Then we will present a special setup of Generator Matrix with linear codes. We will discuss the performances of Xor linear code in current Quantum method applied in our laboratory and, as a conclusion; we are principally interested to examine the relationship of Xor linear codes and Generator Matrix which combines with cryptographic protection as secure as quantum information.

Keywords: *Xor linear codes, generator matrix, qubit, Quantum Key Exchange, error correction, quantum.*

1. INTRODUCTION

Communication at high speeds, long distances, and in unknown environments often requires combating noise that may affect or destroy data before it has reached its intended destination. When designing robust, practical communication systems, it is important to take such effects into account and engineer a system to be as immune to noise as possible. Classical communications often relies upon various error detection and correction schemes, from the simple parity check to a variety of more sophisticated correction algorithms, designed to ensure nearly error-free transmission of data. Classical error-correction systems often employ redundancy and checksums to accomplish error correction; however, error correction in quantum communication channels is complicated by the fact that a qubit's state is affected by measurement. Furthermore, one may only have a single copy of each qubit to work with in quantum algorithms: in quantum cryptography algorithms such as BB84, for instance, it does not make sense to re-transmit qubits prior to establishing a key. In this paper, we explore the problem of quantum communications and present some of the simple algorithms Xor linear codes with generation matrix that have been proposed to correct errors of various types in a channel of qubits.

2. Quantum cryptography

To understand how quantum cryptography works we can consider the "BB84" communication protocol, which was introduced in 1984 by Charles Bennett of IBM and Gilles Brassard from the University of Montreal. Alice and Bob are connected by a quantum channel and a classical public channel (see Fig.1). If single photons are used to carry information the quantum channel is usually optical fibre. The public channel, however, can be any communication link, such as phone line or internet. Let us stop now a little and say something about information. The

information in computer world is represented by series of 0's and 1's that assembled together in defined order present information. That information can be anything numbers, words, pictures, we only need to know how to interpret that binary information. Well, that 0 and 1 while travelling your phone lines is represented like some voltage. Usually in the world of digital electronics logical 0 and 1 are represented like 0V and 5V considering the ground (sometimes -5V and 5V, and 0V can represent some other state) [1].

Alice begins by sending a message to Bob using a photon gun to send a stream of photons randomly chosen in one of four polarizations that correspond to vertical, horizontal or diagonal in opposing directions (0,45,90 or 135 degrees). For each individual photon, Bob will randomly choose a filter and use a photon receiver to count and measure the polarization which is either rectilinear (0 or 90 degrees) or diagonal (45 or 135 degrees), and keep a log of the results based on which measurements were correct vis-à-vis the polarizations that Alice selected. While a portion of the stream of photons will disintegrate over the distance of the link, only a predetermined portion is required to build a key sequence for a onetime pad. Next, using an out of- band communication system, Bob will inform Alice to the type of measurement made and which measurements were of the correct type without mentioning the actual results. The photons that were incorrectly measured will be discarded, while the correctly measured photons are translated into bits based on their polarization. These photons are used to form the basis of a onetime pad for sending encrypted information. It is important to point out that neither Alice nor Bob are able to determine what the key will be in advance because the key is the product of both their random choices. Thus, quantum cryptography enables the distribution of a one-time key exchanged securely [2].

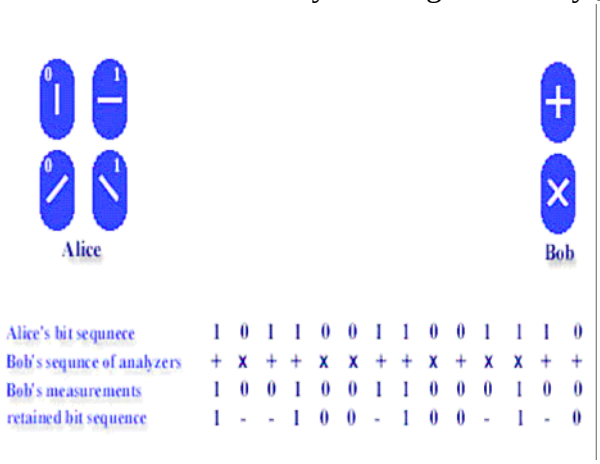

Figure. 1. BB84 algorithm application setup

3. Practical limits of Quantum Cryptography

In the preceding chapters we learned about the principles of Quantum Cryptography and a rather elegant and promising experimental implementation.

In this chapter we want to establish the practical limits of the Quantum cryptography: the data rate and the quantum bit error rate [3, 4].

3.1 The Data Rate

Let us consider a Quantum Cryptography setup with a laser pulse rate v. μ is the average number of photons at the output of Alice, η_d and η_t are the detector and transfer efficiency, respectively. Hence the raw data rate R, i.e. the number of exchanged bits per second before any error correction, is given by:

$$R = q\,\mu\,v\,\eta_t\,\eta_d \qquad (1)$$

q is a systematic factor depending on the chosen implementation. It cannot be bigger than 1⁄2 due to the fact that half of the time the randomly chosen bases of Alice and Bob are not compatible. The raw bit rate *R* will be further reduced when error correction and privacy amplification are applied, depending on the error rate and the used algorithm. The total transfer η_t efficiency between the outputs of Alice to the detector can be expressed as:

$$\eta_t = 10^{\frac{-(Lfl+Lb)}{10}} \tag{2}$$

where *L*f is the losses in the fibre in dB/km, *l* is the length of the link in km and *L*B are internal losses at Bob in dB.

The losses in optical fibres are typically around 2 dB=km at 800 nm, 0,35 dB=km in the 1300 nm telecom window, and 0,2 dB=km in the 1550 nm telecom window.

3.2 The Quantum Bit Error Rate

The error is generally expressed as the ratio of wrong bits to the total amount of detected bits. We call this quantity quantum bit error rate (QBER). It is equivalent to the ratio of the probability of getting a false detection to the total probability of detection per pulse:

$$\begin{aligned} QBER &= \frac{P_{opt}P_{phot} + P_{dark}}{P_{phot} + 2P_{dark}} \cong P_{opt} + \frac{P_{dark}}{P_{phot}} \\ &= QBER_{opt} + QBER_{\det} \end{aligned} \tag{3}$$

whit $P_{dark} = n_{dark}\Delta\tau$, and $P_{phot} = \mu n_t n_d$ we obtain:

$$QBER_{\det} = \frac{n_{dark}\Delta t}{\mu n_t n_d} \tag{4}$$

P_{dark}, P_{phot}, and P_{opt} are the probabilities to get a dark count, to detect a photon, and the probability that a photon went to an erroneous detector, respectively. n_{dark} is the dark count rate of the detector and $\Delta\tau$ is the detection time window. This formula applies for a setup with two detectors. Since a dark count will with a 50% chance not lead to an error, but just to an additional count, there is a factor two in the denominator, but not in the numerator. Note that the QBER is independent of the factor *q* of (3), since we do not consider errors when incompatible bases are used [5].

The QBER consists of two parts. The first part is what we call $QBER_{\text{opt}}$, that is the fraction of photons P_{opt} whose polarization or phase is erroneously determined, i.e. the fraction of photons who end up in the wrong detector. This is mainly due to depolarization and to poor polarization alignments or due to the limited visibility of the interferometers. P_{opt} Can be determined by measuring the polarization ratio, the extinction ratio or the classical fringe visibility *V*. In our interferometer setup presented in the preceding section we measured a P_{opt} of 0:15%. Generally P_{opt} below 1% can be easily achieved with any setup.

The second part, $QBER_{\text{det}}$, is due to the dark count rate of the photon counters and increases with decreasing transfer efficiency ηt . Hence $QBER_{\text{det}}$ is the determining factor for longer transmission distances. The detector dark count rate finally limits in combination with the losses in the fibres the transmission distance. Since fibre losses have already attained the physical limits, the detectors deserve a thorough discussion [6, 7].

4. Quantum error detection and correction

Quantum error-correcting codes are based on qubits and protect quantum states from error. An important challenge in quantum codes is that the quantum error can be continuous. Specifically, we can consider a quantum error as an arbitrary unitary linear operator lhat transfers a quantum state lo a corrupted state. For one-qubit systems, the quantum error operator is a 2 x 2 complex unitary matrix. In this paper we consider three types of quantum errors: The bit flip error represented by matrix *X ,* the phase flip error represented by matrix Z, and the combination of bit and phase flips *Y = -iZX.* Together with the identity matrix, *I,* X, *Y,* and *Z* are the well known Pauli matrices [8]:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Any unitary operator acting on one qubit can be expressed as a linear combination of the Pauli matrices. Therefore, a code capable of correcting these three types of errors are able to correct any errors generated as linear combinations of these matrices. A Pauli operator on *N* qubits can be expressed as a sequence of *N* operators, each one of them being a PauIi matrix and acting on a different qubit [9].

A stabilizer group *S* is a set of Pauli operators on *N* qubits, so that the set is closed under multiplication and any two operators in he set commute (which occurs when disregarding the position where one of them is equal to *I,* they differ in an even number of positions). Obviously, it is enough to check the commutation property on a set of generators. Given the set of stabilizer generators *{Si),* a quantum codeword is defined as a state $|\psi\rangle$ that is a +1 eigenstate of all the stabilizers (i.e., $Si|\psi\rangle = |\psi\rangle$ for all *i*). The set of error operators *{E}* is a set of Pauli operators taking a quantum state > to the corrupted state $E|\psi\rangle$. Since all of them are Pauli operators, a given error operator *E* either commutes or anticommutes with each stabilizer generator *Si.* Therefore, $E|\psi\rangle$ is an eigenstate of *Si* for all *i.* The syndrome is defined as the "commutation status" (either commute or non-commute) of $E|\psi\rangle$ with respect to all the stabilizers, and is completely determined by the commutation properties of *E* with the stabilizers and independent of the quantum state $|\psi\rangle$.

Given any Pauli operator on *N* qubits, we can write it uniquely as a product of an X-containing operator (i.e., using only matrices X and *I),* a Z-containing operator, and if phase factor (+1, -1, *i or - i).* Then, we can express the X-(Z) containing operator as a binary string of length *N,* with' 1' standing for X *(Z) and* '0' *for* I. For instance,

$$\begin{aligned} XIYZYI &= -(XIXIXI) \times (IIZZZI) \\ &= (101010/001110) \end{aligned} \tag{5}$$

In this way, we can represent each stabilizer as a binary vector, and write the set of generators of *S* as a binary matrix *A* = (H/G), where row *i* of *H* corresponds to the X-containing operator of stabilizer generator *i,* and row *i* of G is the binary representation of the Z-containing operator of stabilizer generator *i.* With this binary representation, the commutatively of stabilizers appears as orthogonal of the rows of G and *H* with respect to a twisted product. In matrix representation, the twisted product property can be expressed as:

$$G H^T + H G^T = 0. \tag{6}$$

A Pauli error operator *E* can be interpreted as a binary string (*e)* of length *2N.* By reversing the order of the X and Z strings in the error operator, the ordinary dot product (mod 2) of (*e)* with a row of the matrix *A* is 0 if *E* and the stabilizer represented by that row commute and 1 otherwise. Thus, the quantum syndrome for the error operator *E* is exactly the classical syndrome (*Ae)* where matrix *A = (H/G),* called quantum parity check *matrix,* acts as the standard parity check matrix and

(*e*) as binary error pattern. Therefore, we can conclude that from any binary matrix *(H/G)* of size M_Q x *2N* satisfying (1), it is possible to construct an equivalent quantum code that encodes $N - M_Q$ qubits in *N* qubits.

5. Problematic

In spite of the considerable progress in the quantum encryption (encoding) many questions remain asked and many problems cannot be solved using the present techniques (Noise due to quantum uncertainty).

Noise due to quantum uncertainty: In quantum mechanics, Heisenberg's uncertainty principle forbids two non-commuting observables to both take a definite value simultaneously. For instance, in a state of the electromagnetic field in which the energy is well-defined, the field amplitude cannot take a definite value. This is true, in particular, in the electromagnetic vacuum (i.e., in the total absence of light) where the measurable energy is strictly zero. Because of the uncertainty principle, however, the field amplitude cannot also take the value of zero but must fluctuate randomly.

These *vacuum fluctuations* have very important consequences for optical telecommunications, as they constitute a fundamental source of noise that contaminates an optical signal at every stage of its life, its generation noises. Since the subject of the quantum noise is limitations of optical communications systems. We review here very briefly a few well-known examples of the direct manifestations of vacuum fluctuations in the different functionalities of a telecommunications system.

6. Discussion

The noise in physical qubits is fundamentally asymmetric: in most devices, phase errors are much more probable than bit flips. We propose a quantum error correcting code which takes advantage of this asymmetry and shows good performance at a relatively small cost in redundancy, requiring less than a doubling of the number of physical qubits for error correction.

This precise point is the aim of our work; we will try knowing a new error correction code in quantum method cryptography thus coupling them with techniques borrowed from signal processing with purely quantum theories in order not to lose the information or to make sure to maintain the communication between Alice and Bob using BB84 protocol.

7. Xor Linear Codes with Generator Matrix

We focus on systematic Xor LCGM codes, which are linear codes with sparse generator matrix, [I P], with P = [p_m]. The information message to be transmitted, u = [$u_1, u_2, \ldots, u_L$] together with the coded (parity) bits, c = [$c_1, c_2, \ldots, c_M$] generated as c = P.u, are transmitted through the channel.

The corrupted sequence at the decoder is denoted as (u)' (c)'] where $c_m' = c_m + e_{1m}$ and $u_l' = u_l + e_{2l}$, with e_{1m} and e_{2l} being the error pattern {or noise) introduced by the channel. Notice that the code above is an L/(L+M) rate systematic code. We will use the notation (X, Y) LCGM code to indicate that the degrees of the systematic bit nodes and the parity nodes are X and Y, respectively.

7.1 Xor Linear Codes

In order to have a total secured emission, we must introduce coding part in the information message u = [$u_1, u_2, \ldots, u_L$] , before this setup secure transmission of polarization photons bases. The message: 1101001110010111…

Part 1: 11/01/00/11/10/01/01/11/… We cut the message by pairs of bits.

Part 2: We carry out the XOR sum for the bits existing in the pairs before to find an **origin Bit**: (0), (1), (0) …

Part 3: We call on a **parity bit**:

- If the number is even 0.

- If the number is odd 1.

A new message that is a set of 00 and 11 with a masking technique at the some time, then we risk the least error detection to Bob's message reception: (00), (11), (00)…

Part 4: There is a problem that intervenes in this part and that is how to know whether the XOR = 1, if the bits (01) or (10) and whether the XOR =0 the bits (00) or (11), thus additional bits are necessary, they are the **XOR Bits:**

XOR =0:
00 (0 for the bits 00, 0 for the XOR) 00
11 (1 for the bits11, 0 for the XOR) 10
XOR =1:
01(0 for 01, 1 for XOR) 01
10(1 for 10, 1 for XOR) 11

AB ⟶ XOR Bits
C ⟶ parity bit
D ⟶ origin Bit

When we call on all combinations that may appear while applying this method:

00 ⟶ 1000, 11 ⟶ 0000

01 ⟶ 0111, 10 ⟶ 1111

The first three bits have always the some which speeds up the errors detection.

8. Conclusion

Quantum key distribution process requires error correction code in order to secure the transmitted data in optical communication networks.

Our survey involves different sources of noise generated in optical communication systems and in order to protect the information we should use the BB84 protocol with cryptography control error reconciliation. A large scale protection in quantum information is the aim of our research work carried out within our laboratory.

We have made a modest contribution for securing quantum information using error code correction approach by the BB84 protocol. Several experiments have demonstrated the viability of the conduction of free space quantum cryptography at the surface of the Earth, we propose in this survey a new idea for coding error corrector in BB 84 with Xor Linear Codes with Generator Matrix in order not to lose, and to secure the information during the communications between the users. Our future aim is to elaborate an algorithm capable of detecting and correcting errors in quantum cryptography.

Acknowledgements

We would like to thank Prof. Malek Benslama for his support in Electromagnetism and Telecommunication Laboratory which he is heading, and we are grateful for his supervision of this work.

REFERENCE

[1] P. Shor, “Algorithms for Quantum Computation Discrete Logarithms and Factoring”. 35th Annual Symposium on Foundations of Computer Science, USA, Nov. 1994. IEEE Press.
[2] H. Zbinden, H. Bechmann-Pasquinucci, N. Gisin, G. Ribordy, “Quantum cryptography”, Appl. Phys, pp. 743–748 (1998), Springer-Verlag.
[3] P. Domokos, M. Raimond, A. Brune and S. Haroche, “Simple Cavity- QED Two-bit Universal Quantum Logic Gate: The Principle and Expected Performances”. Phys. Rev. Lett., 52:3554, 1995.
[4] M. Planat, “Complementary and quantum security”. IEEE, ISEC’05 19-21 June 2005 Jijel Algeria.
[5] A. M. Steane,’’ Error correcting codes in quantum theory’’, Physical Review Letters, pp. 77-793, 1996.
[6] C.H. Bennet and all: Quantum cryptography. Scientific American, pp 51-57, October 1992.
[7] D. Gottesman,’’Class of quantum error-correcting codes saturating the quantum Hamming bound’’. Phys. Rev. A, 54:1862, 1996.
[8] Shor P.W,’’Quantum error-correcting codes need not completely reveal the error syndrome,’’. ArXive e-print quant-ph/9604006, 1996.
[9] A. R. Calderbank and P. W. Shor, “Good quantum error-correcting codes exist,” Phys. Rev. A, vol. 54, no. 2, pp.1098-1105, August 1996.

Article received: 2008-05-17