



GLOBAL JOURNAL OF COMPUTER SCIENCE AND TECHNOLOGY  
Volume 11 Issue 12 Version 1.0 July 2011  
Type: Double Blind Peer Reviewed International Research Journal  
Publisher: Global Journals Inc. (USA)  
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

# Network Security Based on Quantum Cryptography & Multi-qubit Hadamard Matrices

By Sandip Dutta, Anand Kumar, N.C.Mahanti

*Birla Institute of Technology Mesra, Ranchi India*

**Abstracts** - An approach is described for generating a secret key using polarized photons in quantum systems. A message is encoded and decoded by using code generated through the properties of Hadamard matrices. The algorithm uses the features of certain existing algorithms and makes the transmission of data through an insecure channel less vulnerable to various attacks. The algorithm uses the concept of bases: rectilinear and diagonal for the sender and the receiver respectively [1]. This is a deterministic algorithm in which the two communicating parties use the same orthogonal bases to measure each qubit in the transmitted message. The algorithm uses the concept described by Lester-Hill [2] in the intermediate steps of the cryptographic process. The key that is transmitted over the network is made less vulnerable to the man-in-the-middle attack using the Diffie-Hellman concept of key exchange [3].

**Keywords** : Network security, Quantum cryptography, photon polarization, deterministic one step quantum key distribution, polarization filter, Hadamard matrices, qubit, man-in-the-middle attack, sequency value.

**GJCST Classification** : C.2.0



*Strictly as per the compliance and regulations of:*



# Network Security Based on Quantum Cryptography & Multi-qubit Hadamard Matrices

Sandip Dutta<sup>α</sup>, Anand Kumar<sup>Ω</sup>, N.C.Mahanti<sup>β</sup>

**Abstract** - An approach is described for generating a secret key using polarized photons in quantum systems. A message is encoded and decoded by using code generated through the properties of Hadamard matrices. The algorithm uses the features of certain existing algorithms and makes the transmission of data through an insecure channel less vulnerable to various attacks. The algorithm uses the concept of bases: rectilinear and diagonal for the sender and the receiver respectively [1]. This is a deterministic algorithm in which the two communicating parties use the same orthogonal bases to measure each qubit in the transmitted message. The algorithm uses the concept described by Lester-Hill [2] in the intermediate steps of the cryptographic process. The key that is transmitted over the network is made less vulnerable to the man-in-the-middle attack using the Diffie-Hellman concept of key exchange [3].

**Keywords** : Network security, Quantum cryptography, photon polarization, deterministic one step quantum key distribution, polarization filter, Hadamard matrices, qubit, man-in-the-middle attack, sequency value.

## I. INTRODUCTION

Quantum cryptography is an emerging technology in which two parties can secure network communication by applying the phenomena of quantum physics. The concept of quantum cryptography was first given by Charles Bennett and Gills Brassard in 1984 (the first known quantum distribution scheme). Quantum cryptography takes its sources from quantum mechanics and is based on fact that light comes in little packets called photons, which have a property of getting aligned along some particular axes and this phenomena is known as Polarization. Photons can be polarized by being passed through a polarizing filter. A polarizing filter is a device or procedure that accepts any photons as input but produces only those photons having a certain kind of polarization particular to the polarizing filter as output. If a beam of light (i.e. a stream of photons) is passed through a polarizing filter, all the photons emerging from it will be aligned in the direction of filter's axis (e.g. vertical or horizontal). If a beam is now passed through

a second polarizing filter, the intensity of light emerging from the second filter is proportional to the square of the cosine of the angle between the axes. This confirms to the Lambert's cosine law. If the two axes are perpendicular, no photons get through. Photons vibrate in all directions as they travel. Although photons can have any directional orientation ranging from 0° to 360°, for purposes of quantum cryptography, we can assume here that there are only four directional orientations. We can denote these four orientations with four symbols



The quantum cryptography allows a bit string to be agreed between two communications parties without having two parties to meet face to face, and yet that two parties can be sure with a high confidence that the agreed bit string is shared exclusively between them thereby deferring the chances of eavesdropping, if there be any.

The polarized photons are used in BB84 to allow two communicating parties, conventionally "Alice" and "Bob", to establish a secret common key sequence. For this Alice needs two sets of polarizing filters. Set one consists of vertical filters and horizontal filters. This choice is called a rectilinear basis. A basis is just a coordinate system. Second set of filters is the same, except rotated 45°. This choice is called the diagonal basis. Thus Alice has two bases, which she can rapidly insert into her beam at will. Alice does not have four separate filters but a crystal whose polarization can be switched electrically to any of the four allowed directions at great speeds. Bob has the same equipment as Alice.

To send a one-time pad of 1001110 with these bases, Alice's photon pattern is shown in the following figure [6]. Given the one time pad and the sequence of bases, the polarization to use for each bit is uniquely determined. Bits sent one photon at a time are called **qubits**.

*Author <sup>α</sup> : Dept. of Information Technology, Birla Institute of Technology, Mesra, Ranchi -835215, India.*

*Email : sandipdutta@bitmesra.ac.in*

*Author <sup>Ω</sup> : Dept. of Computer Science, Birla Institute of Technology, Mesra, Ranchi - 835215, India. Email : anand\_130@ymail.com*

*Author <sup>β</sup> : Dept. of Applied Mathematics, Birla Institute of Technology, Mesra, Ranchi - 835215, India. Email : ncmahanti@rediffmail.com (http://www.bitmesra.ac.in)*

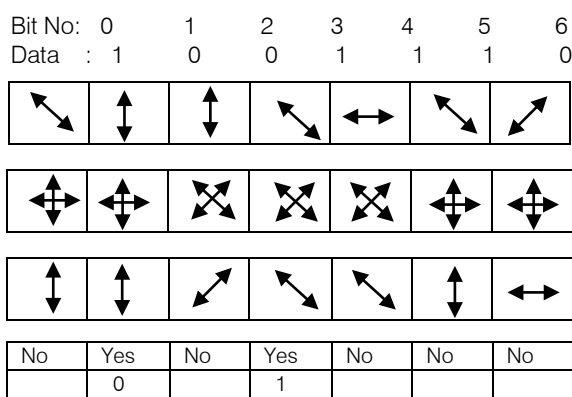


Fig. 1: Bit transmission by quantum cryptography  
(Source: Tanenbaum, A. S., "Computer Networks," p.733)

In the algorithm, if Bob picks the correct basis he gets the correct bit otherwise he gets a random bit.

Hadamard matrices [4] are a class of square matrices first described by James Sylvester in 1867. Hadamard matrices possess several curious and interesting properties [5] which are used in the proposed algorithm:

1. The matrices are symmetric which means the  $m^{\text{th}}$  row is equal to  $m^{\text{th}}$  column.
2. A normalized  $H_n$  has  $n(n-1)/2$  elements of -1 and  $n(n+1)/2$  elements of +1.
3. For normalized Hadamard matrices of order 2 or greater, every row (except the first) or column (except the first) has  $n/2$  elements of +1 and  $n/2$  elements of

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \begin{matrix} =0 \\ =1 \\ =2 \\ =3 \end{matrix}$$

Order = 4

$$\begin{matrix} g_0 = \\ g_1 = \\ g_2 = \\ g_3 = \\ g_4 = \\ g_5 = \\ g_6 = \\ g_7 = \end{matrix} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix} \begin{matrix} =0 \\ =1 \\ =2 \\ =3 \\ =4 \\ =5 \\ =6 \\ =7 \end{matrix}$$

Order = 8

Fig. 2: Hadamard matrices in increasing order of sequency value

## II. PREVIOUS WORK

The principle of cryptography using quanta is based on physics, not mathematics, and is an emerging technology. Not much has been done very significantly in this field and the works are not too efficient and the area is still open to a wide domain of experiments.

## III. PROPOSED ALGORITHM

In the algorithm that we propose, we perform sanitation on the existing features of certain algorithms to enhance the efficiency of our algorithm. We have assumed the communicating parties to be the conventional **Alice** and **Bob** and the intruder as **Trudy**.

-1.

4. Any two rows or any two columns are orthogonal.
5. Every pair of rows and every pair of columns differ in exactly  $n/2$  places.
6. A Hadamard matrix may be transformed into an equivalent Hadamard matrix either by interchanging any two rows or any two columns or by multiplying any row or any column by -1.

Another interesting property is the sequence number of each row, which indicates the number of transitions from +1 to -1 and from -1 to +1. A rows sequence number is called its sequency because it measures number of zero crossings in a given interval. Each row has its own unique sequency value in the range  $[0, N-1]$ .

Approach that we used to generate codes from Hadamard matrix is to generate Hadamard matrix of desired order, change all -1 entries to 0 and arrange the matrix in the increasing order of their sequency and then fetch desired number of rows from the matrix and XOR these rows to generate Hadamard codes as shown in figure below.



Now from the below shown Hadamard matrix of order 8 we can generate Hadamard codes as  $g_0 = [1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1 \ 1]$ ,  $g_1 = [1 \ 1 \ 1 \ 1 \ 0 \ 0 \ 0 \ 0]$ ,  $g_2 = [1 \ 1 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1]$ ,  $g_3 = [1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0]$  and so on,  $g_0 \oplus g_1 = [0 \ 0 \ 0 \ 0 \ 1 \ 1 \ 1 \ 1]$ ,  $g_0 \oplus g_1 \oplus g_2 = [1 \ 1 \ 0 \ 0 \ 1 \ 1 \ 0 \ 0]$ . In similar way we can generate Hadamard matrix of any desired order and generate any number of codes from it.

Here goes the description of the algorithm. The algorithm uses the term qubit. This represents a binary digit in the form of a photon transmitted at a time.

Alice computes word length from the plain text and performs modulus 2 operation if she wants to encrypt plaintext with  $2 \times 2$  matrix in accordance with the Lester-Hill algorithm, if the result is 0 she sends word length to Bob else she appends a dummy letter to make the length even, increments word length by 1 and then sends to Bob. Both Alice and Bob compute seven times the word length and generate the Hadamard matrix of desired order depending on the result for e.g. if the word length is 3 then  $3 \times 7 = 21$ . They thus generate Hadamard matrix of order 24 since 24 is the smallest number greater than 21.

Now, both Alice and Bob change all -1 entries of the matrix to 0 and arrange the entire matrix in the increasing order of its sequency value.

Having done with the Hadamard matrix, Alice and Bob use the authenticated Diffie-Hellman key exchange algorithm (Diffie-Hellman key exchange algorithm [7] using the concept of digital signature for authentication of the two communicating parties **and** eliminating the man-in-the-middle attack, thus the name Authenticated). Suppose they exchange a secret key as 160. Then, both parties perform operation  $g_1 \oplus g_6 \oplus g_0 \oplus g_{16} \oplus g_{10} \oplus g_{60} \oplus g_{160}$ , ignoring the generator values that does not exist in the generated matrix. The g's represent the corresponding row numbers to be selected for the key creation. After the above operation both parties have generated the same bit sequence of 1's and 0's. Alice then informs Bob by sending a plaintext message thereby indicating her choices like 1 as rectilinear and 0 as diagonal and so on

1  Rectilinear 0  Diagonal

and encodes the plaintext message using Hill cipher (say by a  $2 \times 2$  matrix). Each character of the plaintext is converted into a bit string by taking the 7-bit ASCII value representation. A new one time pad is generated again

by Alice and this depends entirely on her choice. This one time pad (or the key) is generated from the Hadamard matrix and this serves as the symmetric key for the cryptographic process. e.g.  $g_1 \oplus g_{18} \oplus g_{10} \oplus g_{15} \oplus g_{55}$

Finally, she performs XOR operation between the bits of the encoded message and those of the generated one time pad to produce the cipher text.

Now, in order to transmit the one-time pad to Bob, both parties set their basis according to previously generated bit sequence and the agreed pattern of the representation of the bits, the bits are transmitted securely to Bob. This process is called deterministic one step quantum-key distribution. The one time pad is used by Bob as well to decrypt the message that was encrypted and the phenomenon to be used is the same Hill cipher.

The key for the Hill cipher is again transmitted by Alice in a similar manner by converting key into binary bit string and again setting up similar basis on both ends and then the bits are transmitted across the insecure channel securely. At the receiver's end, Bob receives the key, computes the inverse of key and recovers the plaintext message in the original form. The following is the diagrammatic representation of the proposed algorithm:

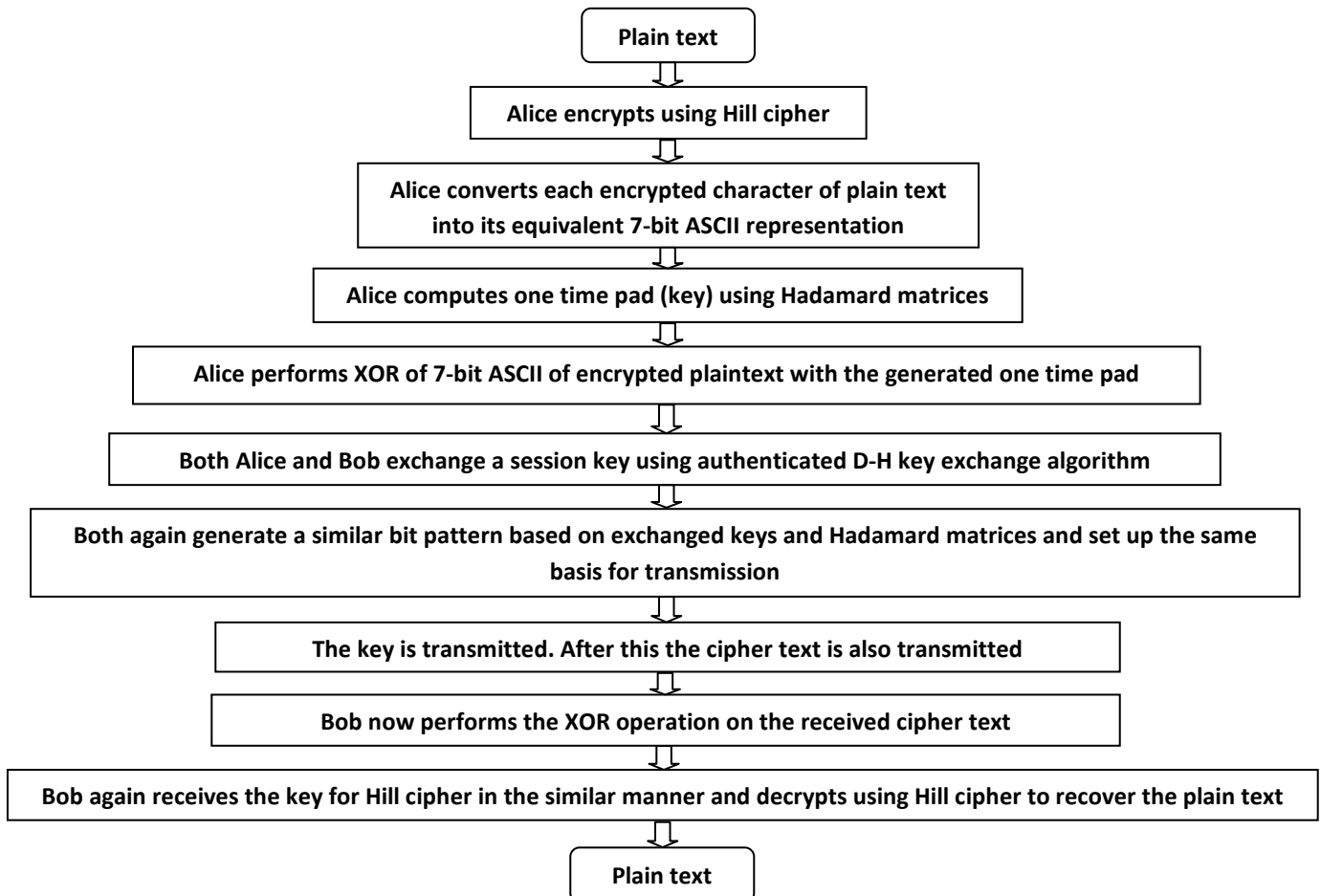


Fig. 3 : Flow Sequence of Proposed Algorithm

## IV. EVALUATION

The proposed scheme is a deterministic one step quantum key distribution. The argument in favour of this statement is that both Alice and Bob use the same basis for the data transmission by agreeing on a common basis before they start the message transmission. This is an enhancement to the feature of the Bennet and Brassard algorithm in which a lot of the qubits get distorted in the transmission process due to the difference in the selection of the basis.

Since we have used the authenticated version of the Diffie-Hellman key exchange algorithm, the man-in-the-middle attack possibility is eliminated.

The algorithm uses random sequence generation of binary bits. Since the occurrence of all the plaintexts that are possible is equally likely, the message that is transmitted possesses no information and thus the message to be transmitted can be said to be safe from all types of attacks irrespective of the computational capability present with the cryptanalyst.

## V. CONCLUSION

The ongoing enhancements in the internet technology continue to be ever increasing and the advent of modern computers to support more and more remote computation will lead to an ever increasing in the requirement of the network data transmission. This will tempt attackers to gain illegitimate access to information for various reasons. Thus the algorithm we propose here is going to serve the needs of the people in the times to come. With the passage of time, the algorithm will become more and more powerful with improvements by those who use it.

## REFERENCES RÉFÉRENCES REFERENCIAS

1. Bennet, C. H., Brassard, G., "Quantum Cryptography: public key distribution and coin tossing," in *Proc IEEE Intern'l conference on Computers, systems and signal processing*, Bangalore, India, December 10-12, 1984.
2. Stinson, D., "*Cryptography: Theory and Practice*," Boca Raton, FL, CRC press, 2002.
3. Diffie, W., and Hellman, M., "*New Directions in Cryptography*," Proceedings of the AFIPS National Computer Conference, June 1976.
4. [http://www.wikipedia.org/Hadamard\\_matrix](http://www.wikipedia.org/Hadamard_matrix)
5. Horadam, K.J., "*Hadamard Matrices and their applications*," Princeton University Press, 2007.
6. Tanenbaum, A. S., "*Computer Networks*, 4/e," Prentice Hall, 2003.
7. Stallings, W., "*Cryptography and Network Security*, 4/e," Pearson, Prentice Hall, 2006.