Indian Journal of Science and Technology, *Vol 10(3), DOI: 10.17485/ijst/2017/v10i3/110635, January 2017*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Quantum Cryptography: A Review

Seema S. Kute[1] and Chitra G. Desai[2]

[1]Department of CS and IT, Dr. B.A.M.U., Aurangabad–431004, Maharashtra, India; seemak0518@yahoo.in
[2]Department of Computer Science, NDA, Khadakwasla, Pune–411023, Maharashtra, India; chitragdesai@gmail.com

Abstract

Background/Objectives: The preferment from conventional computing to quantum computing has created new challenges in the field of cryptography. The cryptographic algorithms which ensured intractability in conventional computing surfaces serious challenge in quantum computing. **Methods/Statistical Analysis:** By applying the quantum mechanics quantum cryptography can be used to unrestrictedly for reliable data communications. **Findings:** The cryptography currently in use, known as conventional cryptography, depends absolutely on the hardness of the mathematical concepts. Elliptical curve cryptography today known as modern cryptography is used extensively for securing financial transactions. Advances in quantum computing, can easily break this security by reverse computing keys faster than the conventional computers. **Application/Improvements:** This paper is an attempt to review fundamentals of quantum cryptography to as to represent it in easiest possible way for a novice demonstrating quantum onetime pad.

Keywords: Conventional Cryptography, Density Matrix, Quantum Cryptography, Quantum One Time Pad

1. Introduction

Cryptography is the study of methods of sending messages in secretes form so that only the intended recipient is able to read the message after applying a specific key. The process of converting the message into some disguised form is called Encryption. The plain text is converted into cipher text by using some key called as Encryption key. At the receiver's end, the recovering of plaintext from cipher text is required. The process of converting the message into its original form is called Decryption. Keys play important role in cryptography. The classification of the cryptographic algorithms is basically on the type of key used. There are two types of keys-Symmetric (secrete key) and asymmetric (public key)[1,6,8,22,23].

In secret key cryptography, both the sender and receiver share a common key which is kept secret. The same key is used for encryption as well as decryption. Hence, it is also called as Symmetric Key Cryptography. In asymmetric key cryptography, two distinct keys are used.

The limitations of symmetric key cryptography, particularly, key distribution was the reason that the asymmetric cryptography started gaining the importance over the time period. Eventually, elliptical curve cryptography known as modern cryptography is being used extensively for securing financial transactions. Advances in quantum computing, can easily break this security by reverse computing keys faster than the conventional computers[2-5,7].

Assume that Alice and Bob are communicating through an insecure communication channel with best of the conventional cryptography algorithm for encryption and decryption which is almost intractable for any conventional computing system. Now, suppose, there is Eve who is an intruder is constantly listening to the communication channel through which Alice and Bob send and receive message and has powerful quantum computing resources. Suppose Alice and Bob are using factoring based algorithm then even can make use of quantum algorithm for factoring[14]. The other applications are quantum key distribution[17]. Quantum digital signatures are another application[15]. These and many more signify the need of quantum cryptography.

2. Literature Review

At the beginning of the twentieth century, 1917, the well-known One Time Pad (OTP) encryption was introduced by Verman[20]. To ensure security OTP demands a very

*Author for correspondence

long key, a key as long as the plain text. Practically it is very difficult to deal with long keys from implementation perspective. In 1940, the seminal paper of Shannon[15] changed the way to look at cryptography. He put forth a very fundamental idea of Information Theoretic Security i.e., the cipher text should not reveal the information about the plain text. Cryptography was thereafter viewed as more applied stream of mathematics and information theory. Since then several cryptographic algorithms were proposed. To make OTP practical the stream ciphers were introduced. The basic idea behind stream ciphers was to pseudorandom key instead of random key. Stream cipher cannot be termed as perfectly secure because the key size is small. As we know from OTP that for being perfectly secure the key length must be greater than or equal to the message being encrypted. Thus the security of the stream cipher lies with the pseudorandom generator which needs to hold the property of being unpredictable. Symmetric algorithms were being used mostly DES[19] made its own place in the history. However, the limitations of symmetric key gave birth to the concept of public key cryptography[9].

These algorithms were based on integer factorization or discrete logarithms or elliptical curves and also efforts were made to propose algorithms based on two hard problems. The well-known example of integer factorization based algorithm is RSA[10], proposed in 1978 based on the concept of public key cryptography proposed by Diffie and Hellman[9] in 1976. The strength of this algorithm motivated several researchers in the field of cryptography to propose new cryptographic algorithms with RSA as the basis. The example of discrete logarithm based cryptography is the one proposed by Elgamal in 1985[11].

To attain high level security obligation, the key size of the conventional public key cryptosystem has to be sufficiently large, which in lower speed and consumption of more bandwidth. To overcome this problem the solution that came up was the elliptical curve cryptosystem. Elliptical curve cryptosystem was discovered in 1985 by Victor Miller and Neil Koblitz[19].

Quantum cryptography was originated by Bennett ,Bassard and Wiesner[13]. Quantum coding was first introduced by Wiesner[15] in 1983. Then Bennet and et.al.[17] used quantum coding in conjunction with public key cryptographic techniques to yield several schemes for unforgeable subway tokens. Several others contributed to quantum cryptography and quantum key distribution. Though quantum computing is not that feasible, quantum cryptography is achievable over shorter distance. In the next section we discuss the concept of quantum encryption with the help of quantum one time pad.

3. Classical and Qubits

3.1 Classical Bits

The classical information is represented using classical bits i.e. 0 and 1. Classical cryptography works on classical bits. Quantum cryptography works on quantum bits also called as qubits. A qubit can be in a superposition between zero and one. Qubits are different from classical bits for e.g. they cannot be copied.

The reason that the quantum cryptography needs to be dealt separately from the classical cryptography is that the information represented in both is different.

Referring to the various sources of quantum cryptography as listed in references below, the next section is an attempt to put forth essential of qubit.

3.2 Qubits

Before we see qubit, a special way to write vectors known as "bra-ket" notation needs to be understood. Let v be the vector, then we write $|v> \in \mathbb{C}^2$ to denote a vector in a two dimensional vector space. For example, the "ket" of vector v is $|v> = \begin{pmatrix}1\\0\end{pmatrix}$.

The bra of this vector is triangle transpose, *T* denotes the transpose.

$$|v> = ((\ |0>)^*)^T = \begin{pmatrix}1^*\\0^*\end{pmatrix} \quad (1)$$

* denotes the entry wise conjugate, and Thus a "ket", denoted $|\cdot>$ is a d-dimensional column vector and the "bra" $<\cdot|$ is a d- dimensional row vector.

Let us write the classical bits as:

$$0 \rightarrow |0> = \begin{pmatrix}1\\0\end{pmatrix} \quad 1 \rightarrow |1> = \begin{pmatrix}0\\1\end{pmatrix}$$

3.2.1 *Definition of a Qubit*

A state of a qubit can be represented as a 2-dimentional ket vector $|\Psi> \epsilon C^2$, therefore

$$|\Psi> = \alpha|0> + \beta|1> \quad (2)$$

where α and $\beta \in \mathbb{C}$ and are the amplitudes. And,

$$|\alpha|^2 + |\beta|^2 = 1 \quad (3)$$

Inner product helps us to decide upon whether the qubit is a valid qubit.

$$< \Psi|1\Psi > = < \Psi|\Psi > \quad (4)$$

$$< \Psi|\Psi > = (\alpha^* \beta^*) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha^*\alpha + \beta^* \beta = |\alpha|^2 + |\beta|^2 = 1$$

So this is a qubit.

For example, Let us consider a qubit

$$|0> = \begin{pmatrix} 1 \\ 0 \end{pmatrix} |1> = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

We have, $|\Psi > = \alpha|0> + \beta|1> = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

Let, $\alpha = \frac{1}{\sqrt{2}}$ & $\beta = \frac{1}{\sqrt{2}}$

Hence, $|\Psi > = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \left(\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

To check whether it is a valid qubit, we have

$$< \Psi|\Psi > = \frac{1}{2} (1\ 1) \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{2}(1 \cdot 1 + 1 \cdot 1) = 1/2(2) = 1$$

Thus, it is a valid qubit. The quantum states of a qubits are given by:

$$|\Psi > \ \epsilon \ xC^d$$

$D = 2^n$, with $< \Psi|\Psi > = 1$

The state of one of many qubits is given by tensor product for example the state of two qubits (A & B) in terms of a vector Ψ_{AB} is,

$$|\Psi >_A = \alpha_A |0>_A + \beta_A |1>_A = \begin{pmatrix} \alpha_A \\ \beta_A \end{pmatrix} \quad (5)$$

$$|\Psi >_B = \alpha_B |0>_B + \beta_B |1>_B = \begin{pmatrix} \alpha_B \\ \beta_B \end{pmatrix} \quad (6)$$

The joint state,

$$|\Psi >_{AB} = |\Psi >_A \cdot |\Psi >_B = \begin{pmatrix} \alpha_A |\Psi >_B \\ \beta_A |\Psi >_B \end{pmatrix} = \begin{pmatrix} \alpha_A \alpha_B \\ \alpha_A \beta_B \\ \beta_A \alpha_B \\ \beta_B \beta_A \end{pmatrix}$$

For example, the tensor product of $A \otimes B$

$$|0> \otimes |0> = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0 \begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00>$$

Table 1 shows the 2 classical bits and how they are represented in 2 qubits[24].

Table 1. Representation of classical bits and Qubits[24].

2 Classical Bits	2 Qubits (Quantum Bits)
00	α 00
01	β 01
10	μ 10
11	€ 11

3.2.2 *Density Matrix*

Suppose n is the number of qubits then, we define qubit as a vector in a complex space of dimension 2^n. Practically we will deal with more than one qubit at a time and therefore it is not possible to work with qubits by representing them into vectors. It is required that the vectors be represented as matrix. To describe the quantum system in a mixed state we use density matrix[24]. The density matrix is denoted by ρ (rho). The matrix ρ, associated to the state Ψ can be computed by taking the ket of Ψ times the bra of Ψ, which is just the outer product.

$$\rho = \sum_j p_j |\Psi_j >< \Psi_j| \quad (7)$$

Consider, the mixed state $|0>$ with probability $\frac{1}{2}$ and $|1>$ with probability $\frac{1}{2}$.

Then, $|0><0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} (1\ 0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

and

$$|1><1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix} (0\ 1) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

Thus, in this case

$$\rho = \frac{1}{2}|0><0| + \frac{1}{2}|1><1| = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

$$= \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$$

4. Classical One Time Pad

In 1917, Gilbert Verman was invented the electrical One-Time Pad for telegraph encryption[23]. Let M,K ,C be the message, key and cipher space respectively. Where,

M = $m_1 m_2 \ldots\ldots m_i$ is a message of length i bits. K= $k_1 k_2 \ldots\ldots k_i$, is of the exact length i and it constructs a cipher text string C= $c_1 c_2 \ldots .c_{i...}$ Let us consider that we have single bit message m and key k. Therefore the encryption function is

$$e = m \oplus k \quad (8)$$

And the decryption function is:

$$m = e \oplus k \quad (9)$$

One time pad has perfect secrecy i.e., from the cipher text we will not be able to obtain any information about the encrypted plain text if we do not know the key. However to obtain perfect secrecy, the key length must greater than or equal to message length which is difficult for practical implementation. Also the key K must be used only once and never used again (Figure 1).

5. Quantum One Time Pad

Using quantum one time pad[16,18] we demonstrate here how the qubit is encrypted. The following example demonstrates quantum encryption scheme. Let Alice and Bob send a qubit $|\Psi>$ to Bob using the key $\mathbf{k}$.

Let Eve be an intruder who tries to listen the communication between Alice and Bob but cannot learn anything about $|\Psi>$

Before sending the message $|\Psi>$Alice performs some operation on $|\Psi>$ that depends on key $\mathbf{k}$. Eve who knows nothing about the key $\mathbf{k}$ sees some state ρ. When ρ reaches Bob he applies some decryption function. Using the decryption function Bob applies transformation using the key $\mathbf{k}$ to obtain the sate $|\Psi>$

Let us consider the classical bit m in terms of standard basis as a quantum state i.e.:

$$|e> = X^k|m> \quad (10)$$

Computing x or is the same as applying bit flip operation, if $\mathbf{k} = 1$ and doing nothing when $\mathbf{k} = 0$. Here $\mathbf{X}$ is the bit flip operation.

For decryption, Bob applies decryption function to obtain the message $|\mathbf{m}>$, therefore

$$|m> = X^k|e> \quad (11)$$

Further, the above vector is converted to vector into density matrix.

Sender	Receiver
M: 0 1 0 0 1 0 0 1	C: 1 1 0 1 0 0 0 0
K: 1 0 0 1 1 0 0 1	K: 1 0 0 1 1 0 0 1
C: 1 1 0 1 0 0 0 0	M: 0 1 0 0 1 0 0 1

Figure 1. Example of 8 bit OTP.

$$|e>\rightarrow |e><e| = X^k|m><m|X^k$$

As we know that Eve knows nothing about the key $\mathbf{k}$. So the probability that $\mathbf{k} = 0$ is $1/2$ and $\mathbf{k} = 1$ is $1/2$. Therefore:

$$\rho = \frac{1}{2}|m><m| + \frac{1}{2}|m><m|X$$

Considering the standard basis we get:

$$\rho = \frac{1}{2}|0><0| + \frac{1}{2}|1><1| = \frac{1}{2}\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} = \text{maximally mixed state}$$

The maximally mixed state which is independent of the message $\mathbf{m}$. Therefore Eve cannot gain anything about the message $\mathbf{m}$ from it.

6. Conclusion

Quantum computing has changed the way the conventional systems use to function using classical bits. Quantum systems use qubits which are very much different in nature as compared to the classical bits. All conventional cryptographic algorithms turn futile in front of quantum computing due to enormous speed at which these algorithms operate. The present paper briefs the journey of cryptography from classical one time pad to quantum cryptography. Then the difference between classical bits and qubits along with the representation is presented referring to the various sources in the references. Finally, the classical one time pad and quantum one time pad are demonstrated.

7. References

1. Sasirekha N, Hemalatha M, Quantum Cryptography using Quantum Key Distribution and its Applications, International Journal of Engineering and Advanced Technology (IJEAT). 2014 April; 33(4):2249–8958.
2. Rohit Kumar, Samudra Gupt Maurya, Ritika Chugh, Manoj PV. Current Refuge Trends using Classical and Quantum Cryptography, Internatinal Journal of Computer Science and Information Technologies. 2014; 5(3):2974–77.
3. Hiskett P, Hughes R, Lita E, Miller A, Nam S, Miller A, Nordholt J, Rosenberg D. Long-Distance Quantum Key Distribution in Optical Fibre., New Journal of Physics. 2006.
4. Martinez-Mateo, Jesus, David Elkouss, Vicente Martin. Key Reconciliation for High Performance Quantum Key Distribution, Scientific reports. 2013; 3.

5. Bennett CH. Quantum Cryptography using any Two Non Orthogonal States, Physical Review Letters.1992; 68(21):3121–24.
6. Bennett CH, Brassard G, Crepeau C, Maurer UM. Generalized Privacy Amplification, IEEE Transactions on Information Theory. 1995; 41(6):1915–23.
7. Choi KS, Chou CW, Deng H, Felinto D, Kimble HJ, Laurat J, Riedmatten H. Functional Quantum Nodes for Entanglement Distribution Over Scalable Quantum Networks, Science. 2007; 316(5829):1316–20.
8. Rishi Dutt Sharma. Quantum Cryptography: A New Approach to Information Security, International Journal of Power System Operation and Energy Management (IJPSOEM). 2011; 1(1).
9. Diffie Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory. 1976; 22:644–54.
10. Rivest RL, Shamir, Adleman L. A Method for Obtaining Digital Signatures and Public Key Cryptosystems, Commun. ACM. 1978; 21:120–26.
11. ElGamal T. A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms, IEEE Trans. Inform. Theory. 1985 Jul; IT–31(4).
12. Wiesner S. Conjugate Coding, Written Circa 1970 and Belatedly Published in Sigact News. 1983; 15(1).
13. Bennett CH, Brassard G, Breidbart S, Wiesner S. Quantum Cryptography, or Unforgeable Subway Tokens, Advances in Cryptology: Proceedings of Crypto 82, Santa Barbara, Plenum Press, (August 1982).
14. Shor PW. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, SIAM J. Comp. 1997; 26:1484. See also quant-ph/9508027.
15. Gottesman D. Chuang IL. Quantum Digital Signatures, quant-ph/0105032.
16. Fernando GSL. Brandão and Jonathan Oppenheim, Quantum One-Time Pad in the Presence of an Eavesdropper, Phys. Rev. Lett. Jan 2012.
17. Bennett CH, Brassard G. Quantum Cryptography: Public Key Distribution and Coin Tossing, In Proc. IEEE Int. Conf. on Comp.,Sys. and Signal Process., Bangalore;1984. p. 175–79.
18. Shukla R, Prakash HO. Sampurna Suraksha: Unconditionality Secure and Authenticated One Time Pad Cryptosystem, IEEE Conference: International Conference on Machine Intelligence and Research Advancement; 2013. p. 174–178.
19. Millar V. Use of Elliptic Curves in Cryptography, CRYPTO. 1985; p. 417–26.
20. Menezes A, van Oorschot PC, Vanstone S., Handbook of Applied Cryptography, Boca Raton, FL: CRC Press; 1996.
21. http://homepage.univie.ac.at/reinhold.bertlmann/pdfs/T2_Skript_Ch_9corr.pdf.
22. Henle F. BB84 Demo. http://www.cs.dartmouth.edu/~henle/Quantum/cgi-bin/Q2.cgi (2002).
23. https://physicsandcake.files.wordpress.com/2010/02/qc_for_beginners.pdf.
24. http://www.qudev.ethz.ch/content/QSIT15/QSIT15_V03_slides.pdf.