Quantum Cryptography

Papri Das
Assistant Professor,
School of IT,
AURO University, India

Security has grained down to every aspect of human life. From simple mobiles to sophisticated bank accounts all are secure. In today's world, when Terabytes of confidential data are exchanged over network, why to give data security an after-thought. Cryptography is a medium to provide data security on the network. From the 16th century this technique has been promoted in various ways. Traditional cryptography (symmetric and asymmetric) have reached a saturation point with the advent of quantum computers. Cracking a key using a quantum computer is not at all a difficult task. This scattered situation was normalized with the rise of 'Quantum Cryptography'. Quantum refers to the minimum amount of physical entity involved in an interaction. Quantum Cryptography is based on the elementary particle of light i.e. 'Photon' and has overcome major gap of traditional cryptography i.e. passive interception. Quantum Cryptography has already made its debut in the practical world successfully. This technique is not much commercialized and has several loopholes too. It is progressing at a very fast rate but has not yet reached its epitome of success. Ignoring all odds, if we consider the progress of the computer world in terms of fast processing, we can say that 'Quantum Cryptography is the future of cryptographic world'.

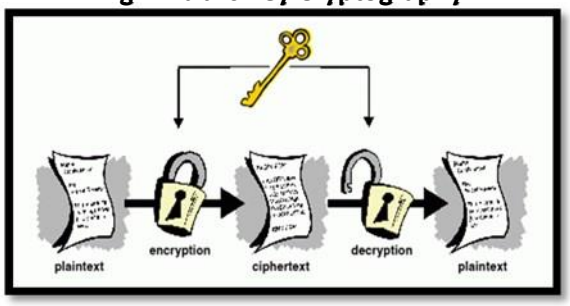
INTRODUCTION

Security has grained down to every aspect of human life. From simple mobiles to sophisticated bank accounts all are secure. In today's world, when Terabytes of confidential data are exchanged over network, why to give data security an after- thought. Taking the analogy of bank, we keep our money in the bank locker which provides us the assurance that there occurs no theft, no unwanted transactions and all our assets remains safe. If such strong security is provided to the money which we use, why should personal data security over the internet be compromised? While in banks we use lockers, pin number, passcodes, biometrics etc. for authentication and authorization, in the computer world we use cryptography for data security.

The word 'Cryptography' come from Greek word 'kryptos' which means 'hidden'. It is th e technique of converting message into unreadable form such that only the anticipated user can read the message by reconverting it in to original message. The original message is called 'Plain text' and the unreadable message is called 'Cipher text'. The process of encoding plain text into cipher text is called 'Encryption' and the process of decoding cipher text into plain text is called 'Decryption'. The parameter which regulates the functional output of the encryption or decryption process (algorithm) is called 'Key'. There are four main objectives of cryptography:
a) Confidentiality b) Integrity c) Non-Repudiation d) Authentication. Broadly there are two types of cryptographic methods i.e. Private key encryption and Public key encryption. These methods have been successfully adapted and commercially used all around the world for different purposes like email, ATM's, corporate data security, etc.

TRADITIONAL CRYPTOGRAPHY

Fig.1-Public Key Cryptography



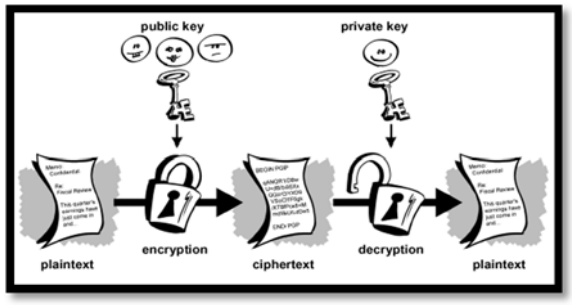


Fig.2-Public Key Cryptography

For years, traditional cryptography has served us by efficientlyfulfilling its objectives. It is been useful in authentication, digital signature, time stamping, electronic money, secure socket layer (SSL) protocol, etc. Traditional private/symmetric/single key cryptography is an algorithm which uses the same key for encryption as well as decryption and is shared by both the parties i.e. sender and receiver. Whereas public key cryptography shares two different keys i.e. private key and public key in which public key is allocate to allthe other parties

in communication whereas private key is kept secret by recipient from other parties in communication. Private and public key cryptography, both have their distinct and unique drawback. The problem with public key is based on the incredible size of the key and the algorithm used to encrypt the plain text. Its advantage is that in order to crack a 128-bit key, there can be 10^{38} possible solutions [source: Dartmouth College]. Even if billion of computers work together, it will take trillion years to crack the key [source: Dartmouth College]. But this isn't problematic now. In the coming years, the current computers will be replaced by 'Quantum Computers' (Quantum computers is a rarely used device which make use of atoms to crack mathematical calculation in a fraction of seconds for modern encryption algorithm. Ordinary computers uses bits or bytes which are strictly 0 or 1 whereas quantum computer uses qubits (quantum bits) which can be in several states concurrently.). These quantum computers work at the quantum level which means they could perform the calculation (cracking the key) in time much less than the current computers. This means public key cryptography will no more be secure and secret key cryptography will be preferred. Secret key cryptography has its own loophole. If two users decide to communicate using secret key cryptography, how will the users exchange key if they are on the other part of the world? The only possible solution is to meet and exchange key but if the key is leaked, again the meeting has to take place. In nutshell, traditional cryptography has reached its saturation point. Soon the transistor technology will be replaced by quantum technology and will give rise to a new era of 'Quantum Cryptography'.

QUANTUM CRYPTOGRAPHY

Quantum comes from the Latin word, meaning 'how much'. Quantum is the atomic particle of any physical entity, for instance, cell is quantum of human body. Quantum cryptography uses 'Light' as its medium with 'photon' being its atomic particle. Photons are small massless particles which exists in all possible positions at a time called the wave function. It means that a photon spins vertically, diagonally and horizontally at same time (Analogy: A person trying to move North, South, East and West at same time). Light in this state is called 'un-polarized light'. In order to give the photons a spin or direction, we use different bases or filters such as rectilinear, diagonal bases, etc. Light with directed photons (spin) is called polarized light. Once the photon is polarized, its spin can't be accurately measured again except with the same filter used to polarize it. Hence, if a photon with diagonal spin is measured with a vertical filter, it will affect the behavior of the photon. This origins the loss of information of the photons original polarization and so the information attached with the photon.

Quantum Cryptography, unlike traditional cryptography which banks on mathematics, rely on physics to develop cryptosystem which is difficult to crack by the eavesdropper. It is more secure as it uses photon to transfer the key between the parties. The photons are converted into key using binary codes. Each spin is associated with a binary number-0 or 1 (decided by the cryptographer). Quantum cryptography is still in its developing

phase and many protocols have been establish such as BB84, decoy state protocol, E91 protocol, COW protocol, KMB09 protocol, SARG04 and many more. The fi rst protocol introduced in 19 84 was the BB84 protocol by Charles Bennett and Gilles Brassard. The protocol works as follows:-

1. Alice generated a length (k) of random number (0 & 1), then directs it on quantum channel to be read by Bob.
2. If there is eavesd ropping from Eve, Eve will be the one who will have to read the quantum channel object first. Eve can alter the bits with two types of attacks: intercept/resend or beam splitting.
3. Then, Bob reads the restructured version from quantum channel object, supposing that Bob doesn't know about the tapping from Eve.
4. Bob then measures the bits he rea d from quantum channel object with his selected own bases. Then Bob broadcasts the bases he made to Alice through public channel, located at Alice's.
5. Sifting raw key begin, Alice read Bob's measurement at public channel object and confirm to Bob th e position Bob has measures in the right bases (m bits) by announcing it at public channel.
6. Next, Alice and Bob estimate er ror to detect eaves dropper. They both compute and equate their bit error rate (e). If they found that their error rate is higher than maximum bit error rate ($e > e_{max}$), they will suspend the communication and start again. (e_{max} has a predetermined value)
7. Now, both Alice and Bob will have a shared key, which is called "raw key". This key is not really shared since Alice and Bob's version are different. They exclude the m bits from the raw key.
8. Both Alice and Bob then performs error correction on their raw key to find erroneous bits in un- compared parts of keys and privacy amplification to minimize the number of bits that an eavesdropper knows in the final key. Finally the same string of bits become their shared secret key.

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Fig.3- Tabular representation of BB84 Protocol

NOTE: The objective of quantum cryptology is t o prevent attempts of eavesdropper. Quantum cryptography is th e first cryptology that defends against passive interception. As we cannot predict a p hoton spin without upsetting its b ehavior, Heisenberg's Uncertainty Principle surfaces when Eve make s her own s py measurements. Hence, if there is any eavesdropping, the spin of the photon will change giving high

error rate, which means that the process (key generation) should begin again.

Despite of strong security that quantum cryptography provides us, it has drawbacks. The major drawback is 'distance'; works for short distance. The original quantum system in 1989 worked over a distance of only 36 centimeters. With improvement of technology, quantum cryptography has s uccessfully worked over 93 miles (150 km), which is not enough to transmit data with modern telecommunication system. This problem arises because of the interference a photon faces. A photon's spin canbe affected if it bumps into other particles. Hence, when aphoton is receiv ed it m ay not be polarized the way it was originally polarized, which leads to loss of information. A group of Austrian researchers have solved this issue centered on the entanglement of photons. At the quantum level, photons depend on one anot her after going through particle reactions, and they get into entangled state. It d oesn't mean that two photons are physically attached. In entangled pairs, each photon has the reverse spin of the other. If spin of one is measured, the spin of t he other can b e inferred. The peculiarity of the entangled pairs is that they stay entangled, even when they'reparted at a distance. Resea rchers kept a photon from an entangled pair at both end of a fiber optic. When one photonwas inferred in one polarization, its entangled equivalent acquired opposite polarization, which meant that the polarization of other photon can be predicted. It transferred itsinformation to its en tangled companion. This solved the problem of di stance in quantum cryptography, because the actions of entangled photons could be predicted.

Conclusion

Quantum cryptography, even though it is sti ll developing, has been applied successfully with accurate results. Since 2007, Switzerland uses quantum cryptography to conduct secure online voting. In Geneva, the result of votes are encrypted over a dedicated optical cable using quantum cryptography. A company named Quintesse nceLabs working for NASA will ensure that the co mmunication with astron aut and satellites from Earth is secure. American power grids, most vulnerable target of cyber-attack, are encrypted using a small device called'QKard' to protect against cyber enemies using the concept of quantum cryptography. Though there are many practical application of quantum cryptography, it has not fully evolved to replace the traditional cryptography. The notion of quantum cryptography has become an epidemic. Scientist and researchers are coming up with different protocols to try and establish a strong base of quantum cryptography. It is progressing at a very fast rate but has not yet reached its epitome of success. Ignoring all odds, if we consider the progress of thecomputer world in terms of fast processing, we can say th at 'Quantum Cryptography is the future of cryptographic world'.

References:-

1. http://www.academia.edu/2124032/Security_Using_BB84_Quantum_Key_Distribution._Protocols
2. http://science.howstuffworks.com/science-vs- myth/everyday-myths/quantum-cryptology6.htm
3. http://en.wikipedia.org/wiki/Quantum_key_distributi on
4. D. C. a. G. Hogben, D. Catteddu and G. Hogben, "Cloud Computing Benefits, risks and recommendations for information security," filefile:///E:/30-10-2014%20backup/Downloads/Cloud%20Computing%20Security%20Risk%20Assessment.pdf, November 2009
5. D. Jamil and H. Zaki, "SECURITY ISSUES IN CLOUD COMPUTING AND COUNTERMEASURES," International Journal of Engineering Science and Technology vol 3 no 4, pp. pp 2672-2676,

2011.

6. T. G. Peter Mell, "http://csrc.nist.gov/publications/nistpubs/800-145/SP800- 145.pdf," September 2011. [Online].

7. c. Wang, k. Ren and Q. Wang, "Security Challenges for the Public Cloud," IEEE computer society Issue No.01 - January/February (2012 vol.16), pp. pp: 69-73, 2012

8. R. Cohen, "Sem antic cloud abstraction," http://www.elasticvapor.com/2009/02/semantic-cloud- abstraction.html, 2009.

9. V. Cerf, "Clou d Computing and the Internet," Google resarch blog, 2009.

10. D. Koo, J. Hur, H. Yoon, Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage, Computers & Electrical Engineering 39 (1) (2013) 34–46.

11. E. M. Moha med, S. El-Etriby, H. Abdul-kader, Randomness testing of modern encryption techniques in cloud environment, in: Informatics and Systems (INFOS), 2012 8th International