Charushila Kadu, Dipti Sonwane, Dheera Jadhwani / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 6, November- December 2012, pp.188-191

How to Avoid Passive Attacks on Data Using BB84 Protocol in Quantum Cryptography: A Review

Charushila Kadu, Dipti Sonwane, Dheera Jadhwani
Computer Science Department,
G.H.Raisoni Institute of Engineering and Management, Jalgaon

Abstract

This paper discuss about new type of cryptography known as quantum cryptography. We know that, cryptography is an art of converting data from one form to another one so that it would not be easily known by outside world. Many algorithms have been introduced for converting from plain text to cipher text. Though there are various secured algorithms are available for encryption, it is very difficult to avoid passive attacks on data. Passive attacks are very dangerous as both parties included in communication never know that their communication is getting attacked and hence this attack becomes dangerous. Popular example for passive attack is eavesdropping which is also now as dangerous because if anyone is eavesdropping your communication, how you will come to know about that? This paper discusses the concept of quantum cryptography as a solution to this attack.

Keywords— quantum cryptography, passive attacks, encryption key, eavesdropping, encryption algorithm

I. WHAT IS QUANTUM CRYPTOGRAPHY?

We all know that cryptography is a technique of converting data from one form into another for its safety. Several different algorithms are implemented for maintains safety of data in cryptography. Use of algorithm get differs from the type of cryptography we are using for the encryption. Mostly, there are two types of attacks on data in network. These are active and passive attacks. We know that comparative to active attacks; passive attacks are most dangerous one as parties taking part in communication don't aware about something happening wrong with their data. If we know about the attack (active attack) which is taking place on our data, we can take some actions against it, but if we don't know that data is being attacked then its security is naturally under high risk. Then, how to avoid passive attacks like release of message content, traffic analysis? Quantum cryptography is the best solution to overcome this problem. Quantum cryptography uses quantum mechanical effect to encryption or decryption. Quantum mechanical effect includes quantum communication and quantum computation. Quantum communication for key exchange and use of quantum computers are the best example of use quantum cryptography. Quantum cryptography gives guarantee to detect attacks like eavesdropping in key distribution as try of listening keys disturb complete quantum data.

What is the need of quantum cryptography?

Quantum cryptography can transmit a secret key over a long distance which is secure in principle and based on laws of physics. Several methods of key distribution are available but they all are based on unproven mathematical assumption. These all methods are always on risk of being attacked by the attacker. If you want long-term security, then its really a matter of fact. Quantum key distribution is known as a subset of quantum cryptography which is developed for transferring and distributing keys during symmetric encryption.

II. TYPES OF QUANTUM CRYPTOGRAPHY

A. Post-quantum cryptography

Post quantum cryptography refers public – key cryptosystems which cannot be brake by quantum computers. Basic need behind the evolution post quantum cryptography is that most of the popular public cryptographic systems are based on integer factorization problem and discrete logarithmic algorithm which are easily breakable by large quantum computers using Shor's algorithm.[1][2].Though, current available experimental quantum cryptography is very secure, most of the cryptographers are searching new algorithms for if quantum cryptography also have danger form attackers in future. In contrast to this, symmetric cryptography which is performed by symmetric ciphers and hash functions are still secured from quantum computers.[2][5] . Though Grover's algorithm can increase the attacks on symmetric cipher text, the danger can be avoided by increasing the size of key used for encryption.

B. Position based-quantum cryptography

Position based quantum cryptography is based on fixed geographical location. Suppose there are two parties are interested in communication and if they are using position-based quantum cryptography then one party can send message to another party only if the other one is at particular expected location otherwise data will not be delivered. How the verification task is performed

then? Basic task of position-verification is that, receiver has to convince verifier that he is located at particular location. This technique is successful when there are many restrictions on adversaries. First position-based quantum techniques were investigated by Kent in 2002 which is known as quantum tagging. A patent for position based-quantum cryptography known as US-patent [13] was granted in 2006, and scientific literature published results in 2010.[14] Several position-based quantum cryptography protocols have been suggested mostly using quantum entanglement.

III. QKD AND QUBITS

Quantum key distribution is most well known and developed application of quantum cryptography which is also known as QKD. QKD explain the process of using quantum cryptography for distributing key between two parties taking part in communication without disturbing third party. If these parties are communicating with each other and if third party try to eavesdrop the content, then complete bit pattern may get disturbs.

Security of quantum key distribution can be easily proved without imposing any type of restriction on eavesdropper which is not possible by using classical cryptography, which is known as "unconditional security". But there may be chances of man-in-middle-attacks if eve becomes able to impersonate Alice or Bob. Quantum cryptography is commercially available in the form of QKD only. Basic unit of quantum information is quantum bit known as qubit. Value of the quantum bit is taken as its polarization as value of classical bit can be taken as 0 or 1 only.

A. Quantum properties

As we know that digital systems use binary states like one/zero, on/Off or Yes/No, what is the state of quantum bit? Qubit is considered as single photon and its manipulation is shown in Fig 1.

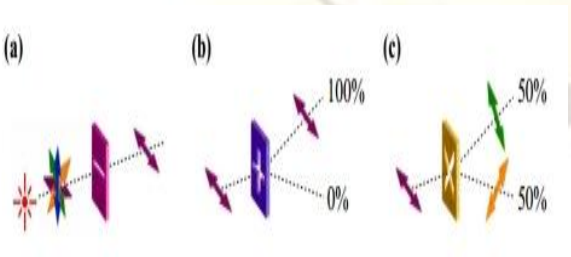

Fig. 1 qubit and single Photon

a): A photon is emitted from light source and passes through linear polarizer, here we consider horizontal polarizer. This process will create qubit with horizontal polarization.

b) When this horizontally-polarized qubit is passed through vertically polarizing beam splitter, it always gains its horizontal polarization.

c) What happen if the horizonatally-polarized photon passes through diagonally-oriented beam splitter:

- There are 50% chances of finding the photon at one of the exit.
- Photon will detect at one of the exit.
- The polarization of photon will changed into the corresponding diagonal polarization.

Expected output for the step c is photon will be blocked and not passed through and it will change polarization. Polarized photon will convey digital information, details of which are shown in Fig.2.

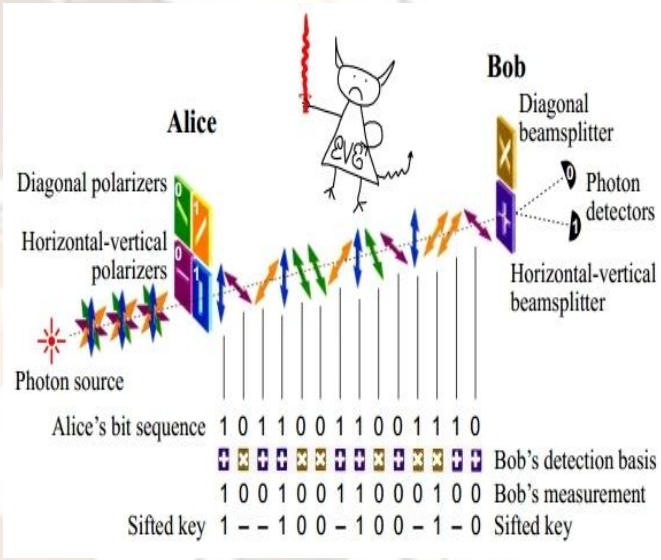

Fig. 2 polarized photons conveying digital information

B. BB84 Protocol

BB84 protocol is the first quantum cryptographic protocol discovered by Charles H. Bennet of IBM New York and Gilles Brassard of the University of Montreal in 1984.This protocol is based upon the technique of generation of secretes keys for encryption and decryption. This is implemented in different technologies which are as follows.

- Single Photon polarization
- Two Photon entanglements
- Single photon Self interference phase modulation

Here we will how BB84 protocol works for single photon polarization is discussed.

.

- Alice will create photon by single photon from light source.

- Then, photon will send through polarizer and naturally it gives one of the possible polarization out of four one. They are as Horizontal (Zero bit), Vertical (One bit), 45 degree left (Zero bit), 45 degree right (One bit).
- Then, photon starts travelling towards Bob's location.
- At receiver end, bob will be having two beam splitters a vertical/horizontal and diagonal and two photon detectors.
- Bob will randomly choose one of the two splitter and check photon detectors.
- Same process is repeated until the complete key will be transmitted to the Bob.
- Then, Bob will inform Alice about the beam splitter he have been used.
- Then Alice will compare the information with the different sequence of polarizes that are used by her to send the key.
- Alice will inform Bob where there is use the right beam splitter in the sequence of bit.
- Finally both Alice and Bob know key used in communication between them.

It is quite best method of exchanging key.

C. Working Principle of BB84 Protocol

First Alice will transmit a random sequence of qubits to Bob over a quantum channel. this sequence is generated by her by repeatedly encoding a randomly selected bit with two selected base from two different bases. It also results in random sequence of four selected quantum states. Base-value –combinations was recorded by Alice which is used during generation in future. The two bases are applied for encoding and decoding. But they should yield correct result when aligned and produced.

D. Key generation

Bob receives the qubits directly from Alice when not intercepted. As Alice only transmits qubit without any information, Bob has to derive the information from the qubits through randomly selecting sequence through its own base. If the bases selected by Bob match with the sequence at the time of encoding, then the result is considered as correct. Bob will record the sequence of his own bases and the different measurement of result made by him.

Then Bob and Alice will communicate with each other to compare their bases sequences. Only the value which is used for encoding and decoding key by them, while other bits are removed from the sequences. The remaining sequence is nothing but random private key which is also known as sifted key. As this raw key is not enough suitable for using encryption and decryption, it is used for generating another key which will be used to perform different quantum cryptographic task on data.

Different cryptographic tasks such as encryption, transmission and decryption of data is performed by various conventional tools over standard communication network so far secrete key protocols are implemented. By keeping encryption key secrete or documental secured, optimal data security is achieved. This is the way how data is encrypted with randomly generated key. This type of data encryption never containing unique patterns of itself which can be used for code breaking.

E. Eavesdropping Detection

When third party try to listen your data on quantum channel, all the sequences of qubit get disturbed. Suppose, Eve listens the qubits, then he will send bits to Bob with his listening. If all the bases used by the Eve are different then measurements will go wrong. Hence, eavesdropping can be easily detected in quantum cryptography. As we know that, avoiding passive attacks are very important to maintain the security of your data. Quantum cryptography definitely provides you a very proper way of keeping your data safe from eavesdropper.

REFERENCES

[1] "Cerberis Encryption Solution - Layer 2 Encryption with Quantum Key Distribution". id Quantique. http://www.idquantique.com/network-encryption/cerberis-layer2-encryption-and-qkd.html. Retrieved 1 march 2012

[2] "Products". MagiQ. http://www.magiqtech.com/MagiQ/Products.html. Retrieved 1 march 2012.

[3] Crépeau, Claude; Joe, Kilian (1988). "Achieving Oblivious Transfer Using Weakened Security Assumptions (Extended Abstract)". FOCS 1988. IEEE. pp. 42–52

[4] Joe, Kilian (1988). "Founding cryptography on oblivious transfer". STOC 1988. ACM. pp. 20–31. http://external.nj.nec.com/homepages/joe/collected-papers/Kil88b.ps.

[5] Gilles, Brassard; Crépeau, Claude; Richard, Jozsa; Langlois, Denis (1993). "A Quantum Bit Commitment Scheme Provably Unbreakable by both Parties". FOCS 1993. IEEE. pp. 362–371.

[6] Mayers, Dominic (1997). "Unconditionally Secure Quantum Bit Commitment is Impossible". *Physical Review Letters* (APS) **78** (17): 3414–3417. arXiv:quant-ph/9605044. Bibcode 1997PhRvL..78.3414M. doi:10.1103/PhysRevLett.78.3414. Preprint at arXiv:quant-ph/9605044v2

[7] Mayers, Dominic (1997). "Unconditionally Secure Quantum Bit Commitment is Impossible". *Physical Review Letters* (APS)

78 (17): 3414–3417. arXiv:quant-ph/9605044. Bibcode 1997PhRvL..78.3414M. doi:10.1103/PhysRevLett.78.3414. Preprint at arXiv:quant-ph/9605044v2

[8] Damgård, Ivan; Fehr, Serge; Salvail, Louis; Schaffner, Christian (2005). "Cryptography In the Bounded Quantum-Storage Model". FOCS 2005. IEEE. pp. 449–458. A full version is available at arXiv:quant-ph/0508222.

[9] Wehner, Stephanie; Schaffner, Christian; Terhal, Barbara M. (2008). "Cryptography from Noisy Storage". *Physical Review Letters* (APS) **100** (22): 220502. arXiv:0711.2895. Bibcode 2008PhRvL.100v0502W. doi:10.1103/PhysRevLett.100.220502. PMID 18643410. http://link.aps.org/abstract/PRL/v100/e220502. A full version is available at arXiv:0711.2895

[10] Koenig, Robert; Wehner, Stephanie; Wullschleger, Juerg. "Unconditional security from noisy quantum storage".A full version is available at arXiv: 0906.1030.

[11] Koenig, Robert; Wehner, Stephanie; Wullschleger, Juerg. "Unconditional security from noisy quantum storage".A full version is available at arXiv:0906.1030

[12] Cachin, Christian; Crépeau, Claude; Marcil, Julien (1998). "Oblivious Transfer with a Memory-Bounded Receiver". FOCS 1998. IEEE. pp. 493–502.

[13] Dziembowski, Stefan; Ueli, Maurer (2004). "On Generating the Initial Key in the Bounded-Storage Model". LNCS. **3027**. Eurocrypt 2004. Springer. pp. 126–137. Preprint available at [1].

[14] Chandran, Nishanth; Moriarty, Ryan; Goyal, Vipul; Ostrovsky, Rafail (2009). *Position-Based Cryptography*. A full version is available at IACR eprint:2009/364.

[15] Kent, Adrian; Munro, Bill; Spiller, Tim (2010). "Quantum Tagging with Cryptographically Secure Tags". A full version is available at arXiv:1008.2147