ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 1, January 2013

# Cryptography Using Quantum Key Distribution in Wireless Networks

Srinivasa Rao Katakam
*CMR Institute of Technology*
*Hyderabad,India*

M.S.R.Lakshmi Reddy
*CMR Institute of Technology*
*Hyderabad,India*

## Abstract

**Despite years of intensive research, the main deterrents of widely deploying secure communication between wireless nodes remains the cumbersome key setup process. In this paper, we address this problem and we introduce a novel security primitive that enables message authentication in wireless networks without the use of preestablished or precertified keys. Quantum cryptography utilizes the Quantum Physical Effects to offer completely secure communication even in the presence of an intruder who is assumed to possess infinite computational power and access to the communication channel. It overcomes the shortcomings of Classical Cryptography by not relying on the computational difficulty in breaking the key. This paper aims at discussing the features of the Quantum Cryptography, the BB84 protocol for Quantum Key Distribution, the milestones achieved so far and an provides an overview of model of wireless network using the BB84 protocol with a modified algorithm for Quantum Key Distribution**

***Key Words- BB84 Protocol, Quantum Cryptography, Quantum Key Distribution***

### 1. Introduction

With ever growing technology both cryptographers, who encrypt messages, and cryptanalysts, who break those codes, have equal opportunities and facilities. We have no surety that the most secured information of a defense organization is really secure even after using most secure classical encryption methods. Quantum Cryptography seems to be a promising solution providing absolute security in such communications. Its works by identifying the threats and combats them by using basic laws of Quantum Physics [1].

The rest of the paper is organized as follows: Section 2 provides an overview of Classical cryptography. Section 3 and 4 discuss the underlying fundamentals of Quantum Cryptography. BB84 protocol is discussed in details in section5.

### 2. An Overview of Classical Cryptography

Based upon the number of keys employed for encryption and decryption classical cryptography can be divided into three categories:

- Secret Key or Symmetric Key Cryptography: Both parties make use of the same key.
- Public Key or Asymmetric Key Cryptography: Two keys are used, one for encryption and another for decryption.
- Hash Functions: Mathematical transformation is used to irreversibly "encrypt" information

The Classical Cryptography relies heavily on the computational complexity of mathematical functions. Although this method can provide high levels of security, it is not fail-safe. Progress in mathematics could render even the most secure networks vulnerable to attacks. Also, it can't provide any indication of eavesdropping.

### 3. Quantum Cryptography- a Background

Heisenberg's Uncertainty Principle forms the basis of Quantum Cryptography or more specifically Quantum Key Distribution (QKD).

Contrary to the reliance of classical cryptography on mathematical functions, Quantum Cryptography depends on Quantum Physical Effects and ensures that any eavesdropping on a Quantum Key Exchange process and copying of the key does not go undetected due to the extremely fragile nature of Qubits (or photons) transferred for the same [5]. Also, a completely random sequence is used to generate the key, which is very difficult while employing classical schemes.

Quantum Cryptography has its origin in two very important features of Quantum Mechanics:

- Uncertainty Principle: It states that if one measures the value of one quantum observable for eg. the position of a particle then this measurement will induce an uncertainty in the values of other observable say, momentum in this case. Hence, this

implies that the state of a Quantum System is disturbed because of any measurement [4]. The security of Quantum Cryptography relies on this uncertainty.

- Entanglement Property: It says that the states of two or more objects are linked together or are "entangled" with each other in such a manner that no one object can be defined without complete account of its counterpart, irrespective of the spatial distances between them [2].

## 4. Quantum Cryptography- How it Works?

The QKD sends the key encrypted as Qubits or units of Quantum Information. In contrast to a bit which is designated either as a '0' or a '1', a Qubit can be a '0' or a '1' or a superposition of both. Physical implementation of Qubits is in the form of photons [3].

The key is sent at a single photon level on a photon-by-photon basis. The natural laws of Quantum mechanics make sure that the act of intercepting or just monitoring these photons to read them, changes their state permanently, thereby, erasing the original information carried by them. Hence, if an eavesdropper measures the photons the communicating parties are able to detect its presence. As a consequence, the eavesdropper can neither copy photon nor read the information encoded on the photons without altering it. The generation of keys is absolutely random, which renders the system complete security.

Alice and Bob, generate a key using first the single dedicated but an insecure Quantum Communication Channel and then the public data channel using Quantum Key Distribution method [9]. A Quantum Channel is a communication channel able to transmit Quantum Information (eg. photons) as well as Classical Information (eg. Text). After the keys have been generated the two parties communicate with each other using the insecure public classical data channel. The messages are encrypted using the key generated and an encryption algorithm as per requirements. For instance: AES or Triple DES can be used [6].

In the entire process we assume that the eavesdropper Eve has unlimited computing power and access to both these channels, though she cannot alter messages on the public channel. The BB84 protocol implementing the QKD is discussed later.

## 5. BB84 Protocol : Employing Quantum Cryptography

BB84 was named after its inventors Charles Bennett and Gilles Brassard and after the year 1984 in which it was published as an unconditionally secure system. It is also known as Polarized Photons protocol as it makes use of the pulses of polarized photons to transmit the information, with one photon per pulse.

The sender Alice and receiver Bob can use any pair of conjugate states (described below). They both have a link of Quantum Communication Channel in between them allowing the Quantum States (A Quantum State is any mathematical object that fully describes the system) to be transmitted. The transmission of photons can take place either in an optic fiber media or free space. BB84 makes use of two pairs of states, conjugate to each other and the two states within a pair are orthogonal to each other. Since these are Conjugate States hence the pair acts as Fourier Transform Duals. These pairs of orthogonal states are referred to as a basis [3].

Alice and Bob are both equipped with two polarizers each, one in the $0_o$ /$90^o$ (+) or rectilinear basis and one in the $45_o$ /$135^o$ (X) or diagonal basis.
We have assumed that Alice sends photons to Bob over the high speed quantum channel and they discuss the result over a public channel (Figure 1). An eavesdropper Eve with infinite computational power, tries to intercept this transmission as she has full access to both the channels.

In order to start the generation of key, Alice randomly chooses a bit (0 or 1), a base (rectilinear or diagonal) and it then polarizes a photon in one of the four directions according to the bit and the basis chosen by her.

**Table 1. Random encoding of bits**

| Basis | 0 | 1 |
|---|---|---|
| + | \| | - |
| X | / | \ |

Once the state has been decided Alice transmits a single photon in that state to Bob, using the quantum channel. As Bob is unaware of the basis or the direction Alice could have selected for the polarizer, he randomly selects a polarizer to measure the photon, with an equal probability. If Bob's choice matches the direction chosen by Alice then Bob will measure the correct polarization state or else Bob's measurement will be incorrect [7].

This process is then repeated, with Alice recording the state, basis and time of each photon sent and Bob recording the time, measurement basis used and measurement result

After the successfully transmission of one sequence of photons, both Alice and Bob begin their discussion on the public channel to decide the key. For each measurement, Bob tells Alice only the basis he used for measurement and Alice confirms the basis as correct or incorrect. If the basis is correct the result is kept else both Alice and Bob discard that bit. In the entire conversation only the basis are discussed and the results of each are never revealed. Hence, after the complete discussion all the false measurements are discarded, leaving two identical sequence of photons, one with Alice and other with Bob. Eventually this sequence is converted to bit string by deciding on which photon directions should be 0 and which should be 1.

**Table 2. Discussion on Public Channel about the basis**

| Alice sends with | + | X | + | + | X | + | X |
|---|---|---|---|---|---|---|---|
| Alice sends to Bob | \| | \ | - | \| | \ | - | \| |
| Bob measures with | + | X | X | X | X | + | X |
| Bob's result | \| | \ | / | \ | \ | - | / |
| Valid data | \| | \ | | | \ | - | |
| Translated to key | 1 | 0 | | | 0 | 1 | |

Now, suppose Eve tries to intercept the photons in transmission and forwards the replaced photons to Bob, prepared in the state Eve measured. Since Eve has no clue about the basis chosen by Alice, so, she also guesses the basis to be used at random [8]. If Eve's guess is correct she would measure the correct polarization state and would prepare similar correct state to be sent to Bob. But, if her guess is wrong, then the measured state will be random, which in turn will also destroy the state to be sent to Bob. So now even if Bob measures this state in the same basis as selected by Alice, then also he would get a random answer.

**Table 3. Discussion on Public Channel with Eve**

| Alice sends with | + | X | X | + | + | X |
|---|---|---|---|---|---|---|
| Alice sends to Bob | \| | \ | \ | - | \| | / |
| Evemeasures with | + | + | + | + | X | + |
| Eve sends to Bob | \| | - | - | - | \ | \| |
| Bob measures with | + | X | + | + | X | X |
| Bob's result | \| | / | \| | - | \ | \ |
| Shared secret key | 1 | 0 | | 0 | | 0 |
| Error in the key | N | Y | | N | | N |

### 6. Reconciliation

This is achieved by starting with an agreed random permutation of bits in the strings and then splitting the resulting string into blocks of size $p$. This constant $p$ is chosen such that one block would be unlikely to contain more than one error. Alice and Bob then compare the parity of each block. If they find a block of mismatched priority, they keep on dividing them continuously into smaller and smaller blocks, comparing parities each time, until the error is found. To make sure, that Eve gains nothing out of the process Alice and Bob discard the last bit of each block whose parity is discussed on the public channel.

### 7. Privacy Amplification

After a complete sequence of strings has been received, both Alice and Bob should have identical key strings 'S' (assuming no errors induced by the turbulent atmosphere). So far, Eve may have accumulated some information about the key by intercepting the transmission or by Photon Number Splitting attack. Though Alice and Bob discarded last bit of each parity set during the Reconciliation Phase still, Eve could deduce about the parity bits using the information that she possessed initially. In order to prevent Eve from gaining advantage from the information she already has, Alice and Bob generate a much smaller key string 'K' from 'S' such that Eve's expected knowledge about K is below a minimum threshold value.

Let K be 'p'-bits and S be 'm'-bits in length such that p<m. We assume that Eve knows at most 'n' parity (or physical) bits of S, therefore a Universal Hash Function

$$g: \{0,1\}^m \rightarrow \{0,1\}^p$$

can be used to compute K.

$$K = g(S).$$

As Eve is unaware of the function which was used to amplify the privacy so, she doesn't possess the key string K which would later be used to encrypt the actual data [10]. One might wonder that, how to decide that how much information has been leaked to Eve? To do so, it can be assumed that all the errors caused in the key string have been caused by eavesdropping. Following this assumption and hence adding several standard deviations to the results, Alice and Bob can have a safe upper bound on the number of bits leaked to Eve.

### 8. Disadvantages

Practically, the protocol suffers from the following disadvantages:

**8.1.** The Real photon detectors always have some noise, so even if there is no unauthorized party involved the bits measured by Alice and Bob may differ.

**8.2.** Secondly, in practice many implementations use laser pulses attenuated to a very low level to send the quantum states. These pulses carry very small but varying number of photons. If there is one photon per pulse then there won't be any problem, but in case the pulses carried more than one photon, then Eve can split off the extra photons and transmit a single photon to Bob. Eve can then measure her photons in the correct basis and obtain information on the key without being detected.

To eliminate the effects of these problems Alice and Bob should first reconcile their data through public discussion. This discussion should be so that it should not provide Eve with more information than she may already have, but at the same time must ensure that Alice and Bob end up with identical key strings. To make the existing information with Eve worthless we can later implement Privacy Amplification.

### 9. QKD in Wireless Systems

In case of the free space being used as the quantum channel there is a high background noise through a turbulent medium. Though a challenging problem but it can be overcome by carefully choosing experimental parameters and using various optical techniques developed for laser communication. Atmosphere offers a high transmission window for light with a wavelength of around 770 mu. Using rugged, low-power semiconductor lasers and their polarization properties controlled with off-the-shelf optical components one can easily produce photons at this wavelength. The atmosphere is non-birefringent at these wavelengths and hence will allow faithful transmission of the QKD Polarization states [4].

However, due to variations in refractive index atmosphere will introduce a jitter in photon arrival time. Since the jitters are between 0.01sec to 0.1 sec they can be compensated by transmitting a bright timing laser pulse at a different wavelength for short time of around 100 ns before each QKD photon.

A more serious concern is that the large background of photons from the sun (or even the moon) could swamp the single-photon QKD signal. However, a combination of sub-nanosecond timing, narrow wavelength filters, and a small solid angle for photon acceptance (spatial filtering) at the receiver can render this background tractable.

### 10. Proposed Wireless System Implementing the BB84 Protocol

Based on BB84 protocol we propose an easily realizable system to implement the same technology but in an even safer manner. We intend to identify the weak spots of Eve and utilize them to encase our system in the shell of absolute security. In our system, as specified earlier, Alice and Bob are the two communicating parties, but they have their machines or QCB (Quantum Cryptography Box)machines synchronized. This QCB performs the tasks of deciding the basis, polarizing the photons and recording the time as well the status of the photons sent on the transmitter side. Whereas, on the receiver side it does the job of detecting the photons, deciding the basis and recording the time and results accordingly.

Furthermore, at the transmitter end the QCB produces a ~1-ns optical "bright pulse" from a "timing pulse" laser operating at a wavelength of ~768 nm. After a ~100 ns delay we send the normal data pulse at ~773 nm from "data" diode laser through the polarizer after selecting a basis. At Bob's QCB receiver the light pulses are collected by a Cassegrain Telescope and directed into a polarization analysis and detection system [3]. An avalanche photodiode detector is triggered by the bright pulse which sets up an electronic timing "window" about 5-ns long in which the QKD optical data pulse is expected.

Again, these machines can continuously send or receive photons. Alice uses QCB fitted with the polarizer, to convert bits to photons. These photons travel to Bob via a wireless network.

On the other end, when Bob receives these photons he randomly selects a basis for the polarizer, passes these photons through the QCB fitted with a polarizer to decipher them. This process is done on a photon-by-photon basis until a sufficient amount of photons have been sent. The discussion regarding the correctness of the key is done on the classical channel in the same manner.

Now in order to provide an extra security feature, Bob and Alice use the decimal equivalent of the previously decided key to indicate the number of machine cycles for which the photons will be discarded [11]. As Eve's machine is not synchronized with the machines of the communicating parties, she would be unaware of the exact time interval for which the photons are being discarded and hence would not be able to decipher the subsequent keys correctly.

Difficulty in deciphering the key by randomly selecting a basis with an added security of delay in producing the next valid bit makes the system very hard to break into. So, even if Eve has some previous knowledge about the key it becomes very difficult for carry on with deriving the correct key as she doesn't know anything about the configuration of the QCB's Alice and Bob are using.

### 11. Practical Application: in Indian as well as Global Scenario

Recent misuse of wireless internet by terrorists have increased the need for security in the same. Our Secure Box can be used to secure Defense Organizations internal wireless communication. Though such a system will have one time investment but where the information is of such high importance an investment such as this can be made.

### 12. Practicality

Owing to the indefatigable efforts of researchers all over the world to make this technique more realizable, many milestones have been recorded so far which have confirmed that this technology is here to stay. The longest distance covered so far by Quantum Key Distribution using optic fibers has been 148.7 km by Los Alamos/NIST using the BB84 protocol, while the target for realizing QKD over 144 kms using entangled photons scheme and later with BB84 has also been achieved.

DARPA (Defense Advanced Research Projects Agency) has been using Quantum Cryptography network since 2004, which is being built by BBN Technologies, Harvard University, Boston University and QinetiQ.

Three companies namely: Quantique, MagiQ Technologies and SmartQuantum can be called the pioneers in producing Quantum Cryptography devices on a commercial scale.

### 13. Conclusion

QKD indeed possesses the potential to bring a revolution in the field of network security. The continued decrease in the implementation prices would make sure that its scope is not restricted to only military purposes but would also spread to other fields as well which desperately need total security in their operations like banking, stocks etc. The system we have proposed aims at increasing the complexity and uncertainty on the part of the eavesdropper. At the same time we have made sure that this system enforces the underlying principle behind Quantum Cryptography and doesn't add to the implementation costs and complexity for the authorized parties.

### 14. References

[1] Quantiki, what are qubits, http://www.quantiki.org/wiki/index.php/What_is_Quantum_Computation%3F#What_are_qubits.3F

[2] Costs of Quantum Cryptography reduced, http://www.networkworld.com/news/2008/060308-discovery-slashes-quantum-cryptography.html

[3] MagiQ Technologies, Inc. Application of Quantum Cryptography for Government and Military. Pages 10-11.

[4] Geir Ove Myhr. Practical Quantum Cryptography. Pages 1-2

[5] Charles h. Bennett, Gilles Bras Sard and Artur K. Kert. Scientiffic American July 1992. Quantum Cryptography. http://www.dhushara.com/book/quantcos/aq/qcrypt.htm

[6] C.A. Boyd and A. Mathuria, Protocols for Key Establishment and Authentication. Springer-Verlag New York, Inc., 2003.

[7] M. Cagalj, S.Capkun, and J.-P. Hubaux, "Key Agreement in Peer-to-Peer Wireless Network," Proc. IEEE, Special Issue on Security and Cryptography, vol. 94, no. 2, pp. 467-478, Feb. 2006.

[8] S. Laur, N. Asokan, and K. Nyberg, "Efficient Mutual Data Authentication Using Manually Authenticated Strings: Preliminary Version," Report 2005/424, Cryptology ePrint Archive, 2005.

[9] W. Mao, Modern Cryptography, Theory & Practice. Prentice Hall, 2004.

[10] M. Bellare and P. Rogaway, "Entity Authentication and Key Distribution," Proc. 13th Ann. Int'l Cryptology Conf., pp. 232-249, 1993.

[11] M. Bellare, R. Canetti, and H. Krawczyk, "A Modular Approach to the Design and Analysis of Authentication and Key Exchange Protocols," Proc. 30th Ann. Symp. Theory of Computing, 1998.

### 15. Acknowledgements

- Dr. Chandra Shekhar Rai (Reader), University School of Information Technology
GGSIPU, New Delhi

**Authors:**

**Mr. Srinivasa Rao Katakam**, working as Asst.Prof in Dept. of CSE in CMR Institute of Technology, Hyderabad, Andhra Pradesh, India. Has 7 years of teaching experience in Computer Science field.

**Mr. M.Sri Rama Lakshmi Reddy**, working as Asst.Prof in Dept. of CSE in CMR Institute of Technology, Hyderabad, Andhra Pradesh, India. Has 5 years of teaching experience in Computer Science field.