Quantum Cryptography – Current Methods and Technology

Emmanuel H. Gadzama, Olawale S. Adebayo & Joseph A. Ojeniyi
Department of Cyber Security
Federal University of Technology
Minna, Nigeria
E-mail: ehgadzama@gmail.com
Phone: +234-8126980414

ABSTRACT

Quantum cryptography is an emerging technology in which two parties can secure network Communications by applying the phenomena of quantum physics. The security of these transmissions is based on the inviolability of the laws of quantum mechanics. Quantum cryptography was born in the early seventies when Steven Wiesner wrote "conjugate coding". The quantum cryptography relies on two important elements of quantum mechanics - the Heisenberg uncertainty principle and the principle of photon polarization. The Heisenberg uncertainty principle states that, it is not possible to measure the quantum state of any system without distributing that system. The principle of photon polarization states that, an eavesdropper cannot copy unknown qubits i.e. unknown quantum states, due to no-cloning Theorem which was first presented by Wootters and Zurek in 1982. This paper concentrates on the theory of quantum cryptography, and how this technology contributes to the network security. The paper summarizes the current state of Quantum cryptography, and the real world application implementation of this technology and finally the future direction in which quantum cryptography trails.

Keywords: Cryptography, Security, Polarization, Quantum, Systems and Transmissions.

iSTEAMS Conference Proceedings Paper Citation Format
Emmanuel H. Gadzama, Olawale S. Adebayo & Joseph A. Ojeniyi (2018): Quantum Cryptography – Current Methods and Technology. Proceedings of the 14th iSTEAMS International Multidisciplinary Conference, AlHikmah University, Ilorin, Nigeria, Vol. 14, Pp 11-18

1. INTRODUCTION

The aim of cryptography is to transmit information in such a way that access to it is restricted entirely to the intended recipient, even if the transmission itself is received by others. This science is of increasing significance with the advent of broadcast and network communication, such as electronic transactions, the Internet, e-mail, and cell phones, here sensitive monetary, business, political, and personal communications are transmitted over public channels. Cryptography works by a sender scrambling or encrypting the original message or plaintext in a systematic way that obscures its meaning. The encrypted message or crypto-text is conveyed, and the receiver recovers the message by crumbling or decrypting the transmission. Current cryptographic techniques are usually identified as "traditional" or "modern." The traditional methods use operations of coding (use of alternative words or phrases), transposition (reordering of plaintext), and substitution (alteration of plaintext characters).

The traditional methods were designed to be simple, for hand encoding and decoding. By contrast, contemporary techniques use computers, and rely on extremely long keys, convoluted algorithms, and intractable problems to achieve assurances of security. There are two branches of contemporary cryptographic techniques: public key encryption and secret key encryption [1, 2]. In Public Key Cryptography, messages are substituted using an encryption method so complicated that even full disclosure of the scrambling operation provides no useful information for how it can be undone. Respective participant has a "public key" and a "private key"; the former is used by others to encrypt messages, and the latter is used by the participant to decrypt them. The key practical problem with secret key encryption is exchanging a secret key. In principle any two users who desired to communicate could first meet to agree on a key in advance, but in practice this could be inconvenient.

Further methods for establishing a key such as the use of secure courier or private knowledge could be impractical for routine communication between many users. Any talk of how the key is to be chosen that takes place on a public communication channel could in principle be accepted and used by an eavesdropper. Going by the quantum theory [3], light waves are opagated as discrete particles known as photons. A photon can said to be a mass-less particle, the quantum of the electromagnetic field, carrying energy, momentum, and angular momentum. Entangled pairs are said to be pairs of photons generated by certain particle reactions. Each pair comprises two photons of different but related polarization. Entanglement can affect the randomness of measurements. For instance, we measure a beam of photons E1 with a polarization filter, one-half of the incident photons will pass the filter, irrespective of its orientation. Whether a specific photon will pass the filter is random.

But, if we measure a beam of photons E2 consisting of entangled companions of the E1 beam with a filter oriented at 90 degrees to the first filter, then if an E1 photon passes its filter, its E2 companion will similarly pass its filter. Also, if an E1 photon does not pass its filter then its E2 companion will not. The basis of quantum cryptography lies in the Heisenberg uncertainty principle, which states that certain pairs of physical properties are related in such a way that measuring one property prevents the observer from concurrently knowing the value of the other. In specific, when measuring the polarization of a photon, the choice of what direction to measure affects all subsequent measurements. Quantum cryptography, or quantum key distribution (QKD) [4], uses quantum mechanics to ensure secure communication. It also enables two parties to produce a shared random bit string known only to them, which can be used as a key to encrypt and decrypt messages. A vital and unique property of quantum cryptography is the ability of the two communicating users to detect the presence of any third party trying to gain knowledge of the key.

Quantum cryptography is merely used to produce and distribute a key, not to transmit any message data. Quantum cryptography is dissimilar from traditional cryptographic systems in that it relies more on physics, rather than mathematics, as a key aspect of its security model. Quantum cryptography uses our present knowledge of physics to develop a cryptosystem that is not able to be crushed - that is, one that is wholly secure against being compromised without awareness of the sender or the receiver of the messages. The prodigy of quantum cryptography is that it explains the problem of key distribution. For example a user can propose a key by sending a series of photons with random polarizations. This order can then be used to generate a sequence of numbers. This procedure is known as quantum key distribution. If the key is interrupted by an eavesdropper, this can be detected and it is of no significance, since it is only a set of random bits and can be discarded.

The sender can then convey or transmit another key. When a key has been securely received, it can be used to encrypt a message that can be transmitted by conventional means: telephone, e-mail, or regular postal mail. In the previous few years, an outstanding surge of interest from international scientific and business communities has propelled QC into mainstream computer science and physics. Additionally, new developments are making QC increasingly practical. The first QC experiment operated over a distance of 32cm in 1989, and today, it is performed over distances of hundreds of kilometers using optical fibers.

1.1. Quantum Cryptography Technologies

Experimental implementations of quantum cryptography have been in existence since 1990, and today quantum cryptography has performed over distances of 30-40 kilometers using optical fibers. Basically, two technologies make quantum key distribution possible: the equipment for creating single photons and equipment for detecting them. The ideal source for this, is a so-called photon gun that fires a single photon on demand. As hitherto, nobody has succeeded in building a practical photon gun, but several research efforts are under way. A lot of researchers are working on a light emitting p-n junction that produces well-spaced single photons on demand.

Some are also working with a diamond-like material in which one carbon atom in the structure has been replaced with nitrogen. That substitution creates a situation similar to a hole in a type semiconductor, which emits single photons when excited by a laser. Several groups are also working on ways of making single ions emit single photons. Suffice to state that none of these technologies, however, is mature enough to be used in current quantum cryptography experiments. In view of this, physicists have to rely on other techniques that are by no means perfect from a security viewpoint. The most common is the practice of reducing the intensity of a pulsed laser beam to such a level that, on average, each pulse contains only a single photon.

2. REVIEW OF RELATED WORKS

Quantum key distribution primarily depends on three algorithms; BB84, B92, and EPR. These protocols exchange qubits over quantum channel and then apply probabilistic measures to adjust the key bits sequence. The BB84 uses rectilinear and diagonal bases to pass data from sender to receiver. The used bases are shown in equation (1). Likewise, B92 employs non-orthogonal bases to send qubits to the receiving side. In the same vein, EPR uses one of the interesting quantum properties which is entanglement to transfer data between parties. Two entangled states are indicated in equation (2).

$$\{|\rightarrow\rangle|\uparrow\rangle\} = \left\{\frac{1}{\sqrt{2}}[1,0]^T, \frac{1}{\sqrt{2}}[1,1]^T\right\} \qquad (1)$$

$$\frac{|00> + |11>}{\sqrt{2}} \qquad (2)$$

It is worthy to note that the first concept of quantum key exchange was introduced by Bennett and Brassard in 1984 [4]. The implementation results in IBM laboratory of the first quantum cryptography experiment were remarkable and indicated that quantum cryptography is promising for secret key exchange [5]. The uncertainty principle was applied in this experiment in place of mathematical modeling. Also, in [5], new principles were introduced for secret key exchange against two types of intruders who intercept and resend data. Figure 2 illustrates the main clue in reconciliation between sender and receiver.

In [6], new security algorithm to distribute a key over the quantum channel was presented by the authors. In this algorithm, it is presumed that two quantum channels between the sender and the receiver while using diagonal bases {↗, ↖} and rectilinear bases {,}. The sender sends the equal data using two channels. The receiver measures the first channel's data by using diagonal basis as well as using rectilinear basis for the second channel. By measuring the two channels, the receiver cancels any measured bit that has a probability less than 1. It also keeps the remaining certain bits with a probability of 1. By this strategy, the parties agree on the quantum bases sequence that are used to transmit the data.

Two protocols were introduced by using three party quantum key distributions [6]. The proposed work achieved session agreement by using only unitary operation. In other words, QKD is trusted from all parties, where the sender uses some classical concepts such as checksum, and then adds the checksum result to the original message. The main advantage of this algorithm is that it allows authorized users to use qubits as a session key.

A proposal introduced in [7], supports security over direct communications in addition to improving authentication. The trusted server manages the communication amongst authenticated users. To enhance security, the communication is shared into two stages. The first stage is called authentication and attackers check. It uses hash function and unitary matrix property to improve data authentication where each user has a unique ID over the network. In the second stage, direct communication ensues by dividing the data into blocks and using entangled bits.

A new proposal that merges between the merits of classical cryptography and quantum cryptography using Quantum Key Distribution Protocol (QKDP) was presented in [8]. The Quantum key distribution primarily depends on three algorithms; BB84, B92, and EPR. These protocols exchange qubits over quantum channel and thereafter apply probabilistic measures to adjust the key bits sequence. The BB84 algorithm uses rectilinear and diagonal bases to pass data from sender to receiver. The used bases are shown in equation (1). Likewise, B92 algorithm employs non-orthogonal bases to send qubits to the receiving side. In the same vein, EPR algorithm uses one of the interesting quantum properties which is entanglement to transfer data between parties. Two entangled states are indicated in equation (2).

In [8], the authors presented QKDP consisting of two phases; the first step is connection setup where the sender and the receiver agree about the bases that can be used during the connection. The next step is key distribution where the trusted center (TC) notifies users on communication process. From the onset, TC generates a random number and a session key by employing hashing function thereafter sends them to the authenticated users. When the users receive the qubits, it would then be measured by using the established bases from the first phase and verify the result to check if it is the key they agreed on or not. Subsequently, the sender starts sending data.

A secure algorithm was introduced to improve the data confidentiality and user authentication by using multi-party applications [9]. A Multicast Network Security model divides the process into three segments. The first phase is user authentication where only legitimate users can receive messages. In the second segment, Quantum key distribution generates secure keys to encrypt and decrypt messages. In the final phase, the data can be encrypted by using generated keys from the second phase and then send to legitimate users.

In [10], a Quantum Key Distribution (QKD) protocol with a two-way quantum channel was introduced. The algorithm works by sending data more than once among the users and they will compute the Quantum Bit Error Rate (QBER). This algorithm consists of 10 steps and the steps are repeated for 20 rounds. After the rounds, a shifted key process is applied to agree on the bases that will be used amongst the users.

Sarath *et. al.* in [11], proposed a scheme for digital authentication using hash function. The scheme utilizes quantum characteristics and principles to perform one way hash function. The scheme was proposed by the authors as an improvement to the BB84 protocol which supports authentication by considering programming polarizer. In this scheme, Dual quantum channels were required. The protocol had a combination of quantum and classical processes that provided high degree of security.

BB84 Encoding Scheme:
The security of the BB84 protocol originates from encoding the quantum information in non-orthogonal states, where BB84 uses two pairs of states with each pair conjugate to the other as well as the two within a pair being orthogonal to each other. The typical polarization state pairs being used are rectilinear Basis of vertical (0) and horizontal (90), the diagonal basis of 45 and 135 or the circular basis of left and right-handed. All of these three bases are conjugate to each other, so any two can be used together.

B92 Encoding Scheme:
In 1992, Charles Bennett developed the B92 encoding scheme. This quantum encoding protocol was similar to BB84, but used only two of the four BB84 state (0 and 45) to represent 0 and 1. By using B92, sender would encode the bits in two non-orthogonal BB84 states in a way that no one can determine a bit with certainty, because no measurement can differentiate between two non-orthogonal quantum states.

Ekert Encoding Scheme:
In 1991, Arthur Ekert developed the Ekert Scheme. The scheme uses entangled pairs of photons. The photon pairs can be created by sender, receiver or a third party. The pairs are created by splitting a single photon into two, using a laser. After the split, one of the photons is sent by the sender or on behalf of the sender to the receiver whereas the other photon is kept.

3. PROPOSED ALGORITHM

Cryptography is a method to combine the relative ease and convenience of key exchange in public key cryptography with the ultimate security of a onetime pad. In this paper, we proposed a three-party key distribution protocol. Alice and Bob want to have a secured communication with each other and would require a secret key to secure their communicating channel from a trusted third party. In protocols like BB84 and B92, the sender and the receiver are not able to know the secret key until the last step when they finish the comparison of their bases. Thus, when a third party is introduced, BB84 and B92 cannot be applied since there is no mechanism to precisely distribute the same key to multiple parties. In this proposed protocol, we are considering how to include three or more parties in the key distribution process. Our specific objective is to improve key distribution system by applying some classical concepts and quantum techniques. By applying public key concepts, we can improve user authentication and data integrity process. The proposed algorithm attains a high percentage of the correct bases.

Besides, we don't need the physical channel to check the Qubits sequence where the quantum bases are shared by using asymmetric key distribution center.

The proposed algorithm consists of two phases:
1. User Authentication & Quantum Bases distribution
2. Data Transfer over the Quantum channel

For Alice and Bob to obtain a session key, the following steps take place amongst the three parties:

User Authentication and Quantum Bases Distribution

1. Alice sends request to have a connection with Bob
Alice → QKD: EPR-Alice(IDAlice || IDBob)
QKD will register the connection request status in log file and check the ID of Alice for user Authentication. Moreover, QKD checks Bob's ID status (Busy, Free). If Bob is free, QKD moves to step 2.

2. QKD sends to Bob a connection request having Alice's request

QKD → Bob: EPU-Bob(IDAlice || IDBob)

3. When Bob sends reply by accepting the connection with Alice, Bob will send to QKD a confirmation message

Bob → QKD: EPR-Bob(IDAlice || IDBob)
QKD decrypts the message and adds connection's status between Alice and Bob and both of them are authenticated to send and receive data.

4. QKD then starts distributing quantum bases (+, X) in some sequence to encode the message to Alice and Bob in an encrypted message using their public keys.

4. 1 QKD → Alice: $E_{PU\text{-}Alice}(ID_{Alice} || ID_{Bob} || QB)$.
4. 2 QKD → Bob: $E_{PU\text{-}Bob}(ID_{Alice} || ID_{Bob} || QB)$

Data Transfer over Quantum Channel

5. After Alice and Bob have received the quantum bases from QKD, Alice sends an encrypted message using the quantum bases to Bob
Alice→Bob: EPR-Alice(EQB(M)||EPU-Bob(IDAlice))

6. Bob and Alice then send a random part of the message to QKD by using Private Key of sender (Alice, Bob).
Bob →QKD: $E_{PR\text{-}Bob}(E_{QB}(M)||E_{PU\text{-}QKD}(ID_{Bob}))$
Alice →QKD: $E_{PR\text{-}Alice}(E_{QB}(M)||E_{PU\text{-}QKD}(ID_{Alice}))$

QKD will be able to decrypt the messages and compare between them. If there are any mismatching bits, then QKD concludes that there is an intruder.

7. QKD thereafter sends notification messages to Alice and Bob to inform them there is an intruder or not.

QKD → Bob: $E_{PU\text{-}Bob}$ (E_{QB}(Notify))
QKD→Alice: $E_{PU\text{-}Alice}(E_{QB}$(Notify))

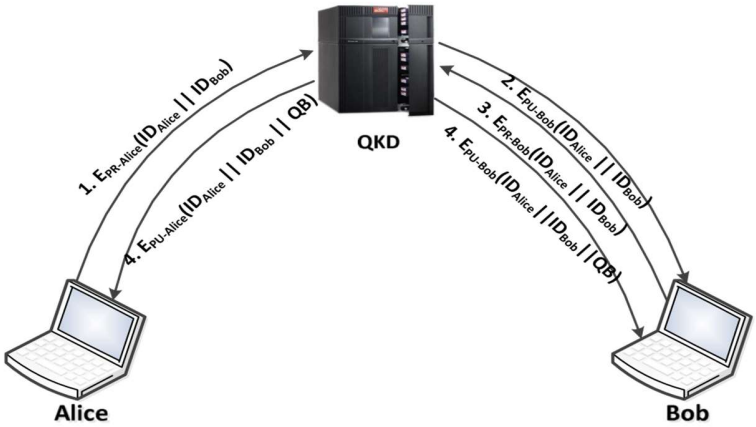

Figure 1. User Authentication and Quantum Bases Distribution

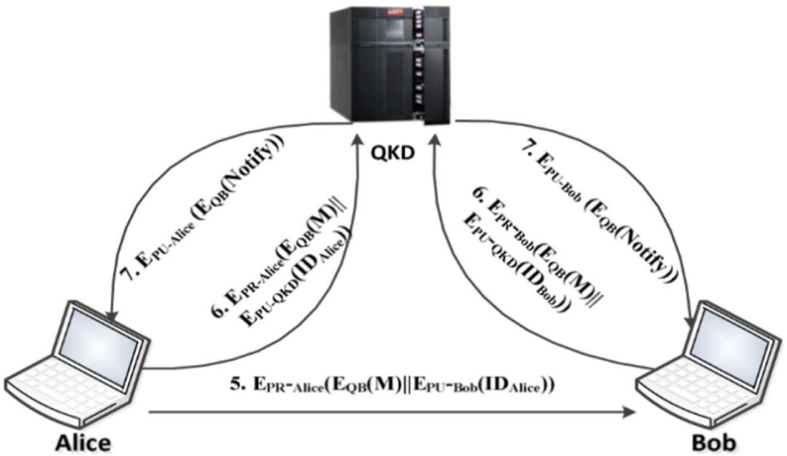

Figure 2. Data Transfer over Quantum Channel

4. ANALYSIS OF ALGORITHM

Quantum cryptography promises to transform secure communication by providing security based on the fundamental laws of physics, instead of the current state of mathematical algorithms or computing technology. The devices used for implementing such methods exist and the performance of demonstration systems is being continuously improved.

Figures 1 and 2 above show the steps involved in the algorithm. If the Notified message is acceptable, the connection will be alive until QKD sends any error notification or Alice stops sending. In our proposed protocol, we improve security over the quantum channel. Respective message is authenticated by the sender using its private key. Moreover, data authentication enhancement is achieved when parties send random pieces to QKD center and notify them. By applying this protocol we eliminate the guessing theory applied in early protocols such as BB84, B92, and EPR. We have improved the capacity to identify if there is an intruder or not.

The proposed algorithm comprise of two general phases and seven steps. In this section, the proposed algorithm is analyzed and compared with other algorithms. Table 1 below shows a comparison with respect to used bases, classical channel as well as user authentication. Table 2, shows a comparison as regards to number of used phases and the use of cryptography.

In the BB84, B92 and EPR protocols, there is a probability of mismatching bases. Considering this possibility, the length of bases will be relatively smaller to the original length. For instance, if there is an attacker, the percent will be 50%, which means that half of key will be discarded. In the proposed protocol, we can transfer the message by using the whole key length. By using public key encryption algorithm, it is possible to send the quantum bases sequence from QKD to Alice and Bob. Furthermore, we have enhanced user's authentication where the above three algorithms did not provide. In the like manner, earlier protocols used classical channel to compare between the sender and the receiver bases. In our proposed algorithm, the sender and the receiver both send random parts from the message to QKD to check if there is an intruder or not.

Table 1. Compression between QKD, BB82, B92 and EPR

Algorithm	No. of phase	Classical cryptography
[9]	Two phases	Hashing function
[10]	Three phases	XOR classical Gate
[11]	One Phase	Hashing function
Proposed Algorithm	Two phases	RSA

Table 2. Comparison between QDKP and other protocols

Algorithm	Bases	Classical Channel	User Authentication
BB82	+, X	Yes	No
B92	Non-orthogonal	Yes	No
EPR	Entanglement Bit	Yes	No
Proposed Algorithm	+, X	No	Yes

5. CONCLUSION

Quantum key distribution protocols BB84, B92 and EPR communicate by using a classical channel to compare the bases. This approach facilitates eliminating the erroneous qubits. In this paper we introduced a novel security quantum algorithm that employs public key encryption algorithm to generate keys to improve security over quantum communication channel. Moreover, the introduced algorithm enhances user's authentication and data privacy.

REFERENCES

[1] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of two quantum key- distribution Protocols," Phys. Rev. A vol. 73, 2006.
[2] C. Elliott, D. Pearson, and G. Troxel, "Quantum cryptography in practice," Karlsruhe, Germany: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications 2003.
[3] E.A. Poe, The Gold Bug, in Tales of Mystery and Imagination, Wordsworth Editions Ltd., Ware, pp. 1-46 (1993).
[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984.
[5] N. Benletaief, H. Rezig, and A. Bouallegue, "Reconciliation for practical quantum key distribution with BB84 protocol," in Mediterranean Microwave Symposium (MMS), 2011 11th, 2011, pp. 219-222.
[6] D. Jin, P. Verma, and S. Kartalopoulos, "Key Distribution Using Dual Quantum Channels," in *Information Assurance and Security, 2008. ISIAS'08. Fourth International Conference on*, 2008, pp. 327-332.
[7] X.-y. Yang, Z. Ma, X. Lu, and H.-x. Li, "Quantum secure direct communication based on partially entangled states," in *Information Assurance and Security, 2009. IAS'09. Fifth International Conference on*, 2009, pp. 11-14.
[8] S. Ranganathan, N. Ramasamy, S.K.K. Arumugam, B. Dhanasekaran, P. Ramalingam, V. Radhakrishnan, and R. Karpuppiah, "A Three Party Authentication for Key Distributed Protocol Using Classical and Quantum Cryptography," *International Journal of Computer Science Issues(IJCSI),* vol. 7, 2010.
[9] S. Ali, O. Mahmoud, and A. A. Hasan, "Multicast network security using quantum key distribution (QKD)," in *Computer and Communication Engineering (ICCCE), 2012 International Conference on*, 2012, pp. 941-947.
[10] F. Zamani and P. K. Verma, "A QKD protocol with a two-way quantum channel," in *Advanced Networks and Telecommunication Systems (ANTS), 2011 IEEE 5th International Conference on*, 2011, pp. 1-6.
[11] R. Sarath, A. S. Nargunam, and R. Sumithra, "Dual channel authentication in cryptography using quantum stratagem," in *Computing, Electronics and Electrical Technologies (ICCEET), 2012 International Conference on*, 2012, pp. 1044-1048.