# AN APPROACH FOR IoT SECURITY USING QUANTUM KEY DISTRIBUTION

A. Beatrice Dorothy, S. Britto Ramesh Kumar

**Abstract**— Quantum cryptography is a way to deal with cryptography dependent on the laws of quantum mechanics. Cryptography depends on key sharing which plays a vital role. For providing a provable security during key distribution, quantum cryptography is used. There are many secure protocols and algorithms were proposed already in quantum cryptography. The Quantum Key Distribution faces several security issues, one among them, is Eavesdropper during the communication. It is an important issue which leads to thrashing of security by Man-in-the-middle (MITM) attack. In this paper, to detect eavesdropping and to enhance security during encryption, a Modified RSA method for encryption is proposed. The BB84 protocol for private key generation and distribution through quantum channel is used. Therefore, the proposed technique provides secure quantum key generation and distribution by which it prevents Eavesdropping security threat.

**Index Terms**— Quantum Channel, BB84 protocol, RSA, Modified RSA, Quantum Key Distribution.

## 1 INTRODUCTION

CRYPTOGRAPHY is the technique of secret libretto with the intention of keeping the data secret. Cryptographic security depends on mathematical hard problems. Factoring large numbers is an issue persists in all the cryptographic techniques. Even though it is hard to factor the numbers, still the eavesdropper can read, modify and fabricate the data passed through the communication channel. For that, cryptography provides security services like non-repudiation, authentication, confidentiality and integrity. But still breaking such security system is easy for the eavesdropper. To overcome this issue, Quantum cryptography is evolved.

Quantum Cryptography (QC) was proposed by Stephen Wiesner at British Columbia University and he introduced the perception of quantum conjugate coding [1]. The QC evolved to solve the issues in the existing cryptographic techniques. As public key algorithms are secure than the symmetric key algorithms. But quantum cryptography has proven more proficiently secure than the public key algorithms. Thus to overcome the issues in public key algorithms and to provide provable security during key distribution QC was proposed. This quantum cryptography ensures unbreakable encryption. This is because, in QC, the generated key is kept back secret and separate from data. Basically in QC, key distribution is a separate phase and encryption is a separate phase. First the key is generated and distributed from sender to receiver. In [2], Quantum Key Distribution (QKD), a secret key is shared among two distinct parties. QKD is only for key distribution. The generated key can be used through some preferred encryption algorithm towards encrypt or decrypt the message which is passed through the communication channel. The inimitable feature of QKD is that it is simple to identify the adversary's presence. With the existing protocols, the difference among the keys can be weigh up easily which is caused by the eavesdropper.

In order to detect the eavesdropper and to distribute the key, we employ BB84 protocol for the key distribution. The protocol is provably secure. The property of quantum mechanism, enable us that information gain is only feasible by disturbing the signal and a classical channel. For encryption, Modified RSA (MRSA) algorithm is proposed. The key retrieved by BB84 protocol in the Quantum key distribution is taken as the private key d, for MRSA encryption algorithm. With the aid of shared secret key, the public key e is generated. This provides additional security. Usually, by knowing public key e, private key d is generated. Performing key distribution and taking that distributed key as private key d, the possibility of finding the key and plaintext P will be reduced. For encryption, the ASCII values of the characters can be taken and encrypted using proposed Modified RSA.

The rest of the paper is organized as follows. The works related to the detection of eavesdropping during QKD is shown in section 2. Section 3 describes the proposed methodology for QKD and detection of eavesdropping. The usage of shared secret key (SSK) in public key algorithm MRSA for performing encryption/decryption with an example is discussed in section 4. In section 5, the experimental results are shown. Section 6 ends with conclusion.

## 2 LITERATURE REVIEW

Mohamed Elboukhari et al. [3], presented a novel extension of the TLS protocol based on QKD. They introduced a scheme for integrating Quantum Cryptography in the protocol. The approach improved the security of the process of authentication and data encryption. Also, they described an example to illustrate the feasibility of our scheme's implementation.

In [4], David Gaharia and Joel Wibron have investigated the possibility of eavesdropping upon a quantum key distribution

- *A. Beatrice Dorothy is currently pursuing Ph.D in Computer Science in St. Joseph's College, Tiruchirappalli, India. E-mail: adorothybrice@gmail.com*
- *Dr. S. Britto Ramesh Kumar is Assistant Professor in Dept. of Computer Science in St. Joseph's College, Tiruchirappalli, India. E-mail: brittork@gmail.com*

using the BB84 protocol by the intercept-resend method. The Bell inequality and the error rate were calculated to determine if an eavesdropper was present. Neha Chhabra [5] has generated random secret key and detected and eavesdropping. Quantum cryptography was developed which promised more secure communication.

In [6], Abhishek Agnihotri has concentrated on the research directions in which quantum cryptography speeded up. And also, they outlined the implementation of real world application. Vivek Singh and Bhawna Chauhan [7], have surveyed some of the quantum key distribution algorithms. All the algorithms were secure to eavesdropping and provided the secure way of key distribution. But the algorithms stoped after eavesdropping detection. In [8], Ammar Odeh et al. have introduced a new method for quantum key distribution between three or more parties where around was a trusted center endow with the clients the required information to cautiously communicate among each other.

Rajni Goel et al. [9], have summarized the current state of quantum cryptography and it provided potential extensions of its feasibility as a mechanism for securing existing communication systems. In [10], N.Sasirekha and M.Hemalatha analysed few application areas of quantum cryptography and its limitations. It is concluded that to transmit sensitive information between two or more points, some stronger technique was needed. Aparna Singh [11], has focused on quantum cryptography and that technology used for secure key distribution in both centralized and decentralized network, all along with limitations.

In [12], Luis Adrian Lizama-Pérez et al. have proposed the negative acknowledgment state by the quantum key distribution protocol which is capable of detecting the eavesdropping activity of the Intercept Resend with Faked Sates (IRFS) attack without requiring additional optical components different from the BB84 protocol. Hitesh Singh et al.[13], have concerned on protocols that share a secret key was explained and comparative study of all protocols was shown. QKD Protocols were based on principles from quantum physics and information theory.

In [14], D N Kartheek et al. have presented quantum key distribution protocols (QKDP) to secure the large networks, which leads in new directions in classical and quantum cryptography. The proposed QKDPs easily resisted replay and passive attacks and also efficiently achieved key verification and user authentication. Charles H.Bennett and GillesBrassard [15], have presented a protocol for coin-tossing by exchange of quantum messages, which was secure against traditional kinds of hoaxing, even with unlimited computing power by an opponent.

## 3 MRSA: A Proposed Methodology

Enhancing the security for any quantum cryptosystems is based on the proposed MRSA. The proposed method provides additional layer of security because the SSK is taken from QKD and used as e in public key algorithm RSA. In this proposed method two separate phases are there. One is key distribution and another is encryption/decryption. The proposed method uses ASCII encoding for encoding the text. The SSK from QKD is considered as e and for the whole text messages that e is used as d. The novelty is that in QKD; basically two basis (b) were used in photon polarization (pp). But in this proposed work four basis are used as this will increase the probability of finding the key. So for the eavesdropper it is difficult to find the key. Even if the key is eavesdropped the users can detect the discrepancy in the key as the sender knows the state in which he/she polarized the photon. The proposed algorithm describes the QKD and encryption/decryption in QC.

The steps involved in Proposed MRSA Algorithm

1. For Sender
   a. Formation of modified photon polarization structure.
   b. The photons polarization basis is formed according to the structure.
   c. Sender's random bit g is generated.
   d. Sender's random sending basis is generated using RND function.
   e. Sender sends the polarized photons.
2. For Receiver
   a. Random measuring basis is performed by the receiver using RND function.
   b. Photon polarization is measured by the receiver based on the previous step.
   c. Then the sender and receiver discuss the shared and received key.
   d. Finally the shared secret key is generated.
3. If the retrieved key>k bits, then the sender discards the operation and will resend the message through another quantum channel. (k is the overall bits).
4. Encryption
   a. s is taken as private key.
   b. Choose two primes p and q.
   c. Compute n=pq
   d. Then compute e and d as e is taken from s.
   e. For performing encryption of each bit in the plaintext, ASCII value of the text will be taken.
   f. Perform encryption using C=Me mod n.
   g. Perform decryption using M=Cd mod n.
5. Repeat the steps 1 and 2 until k<s.

**Algorithm 1: QKD (b, rb, pp, RAND, SSK)**

Begin{main}
1. b (+,×,/,\)←{0,1}
   a. assign {→} to 0 ←{ + }
   b. assign {↗} to 0 ←{ + }
   c. assign { ↑ } to 0 ←{ × }
   d. assign {↖} to 0 ←{ × }
   e. assign {←} to 0 ←{ / }
   f. assign {↙} to 0 ←{ / }
   g. assign { ↓ } to 0 ←{ \ }
   h. assign {↘} to 0 ←{ \ }
2. read rb
3. generate RAND number
4. assign RAND ← rb
5. pp ← rb

6. do same for receiver
7. generate SSK

End{main}

---

### 3.1 BB84 Protocol for QKD

Key distribution plays a vital role in quantum communication. In data security, key distribution is the major part. For that in cryptography, generally key distribution is done using public and symmetric key algorithms. But quantum key distribution protocols broken those algorithms security. Those algorithms were eavesdropped easily. To overcome this issue cryptography used quantum protocols for key distribution. The quantum protocol proved the level of security against other cryptographic algorithms. This paper attempts to distribute key using BB84 protocol. According to BB84 protocol, the sender generates a random bit (rb). Then for that random bit, sender generates a random number using RAND function and polarizes the photons. This is shared with the receiver and the receiver measures the random bit using the RAND function and polarizes the photon accordingly. Thus the secret shared key is generated. Then the secret shared key compares the bit strings. If the eavesdropper retrieved any information of the polarized photon then it causes error in receiver's measurement. If more than e bits differ, both sender and the receiver break off the key and will transmit through some other channel.

The retransmission of another channel is a default process in quantum cryptography. That is like other methods there is no need for selection and saving the channels. The retransmission channel is decided by the users if they feel the transmitted data is travelling through an unsecured channel.

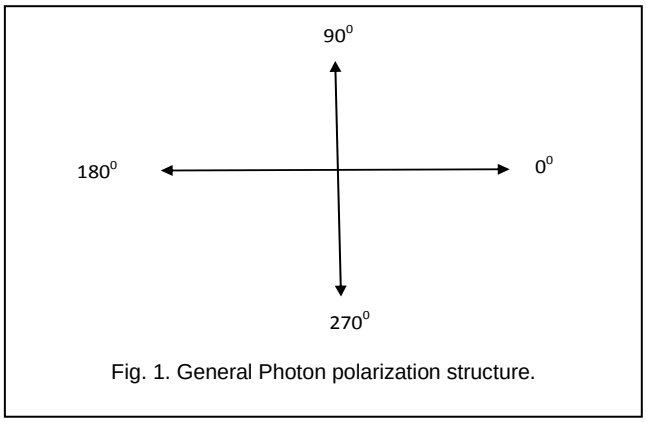


Fig. 1. General Photon polarization structure.

After the key generation as well as successful detection and distribution of keys, the SSK is taken as the private key for RSA algorithm. Further, the generated key is used for encryption and decryption in proposed MRSA. The general structure of photon polarization is shown in Fig.1.

The general photon polarization uses four axes which can be easily predictable. That is the eavesdropper can easily predict the photon polarization and can retrieve the key easily when it is distributed in a quantum channel. Then the eavesdropping can be detected easily which leads the sender to share the message through an alternate quantum channel. But in the modified photon polarization, the number of axes is eight and it increases the probability of finding the key easily. Then after successful polarization and distribution of key without eavesdropping, the proposed MRSA is used for encryption and decryption of message. The modified photon polarization structure is shown in Fig. 2.

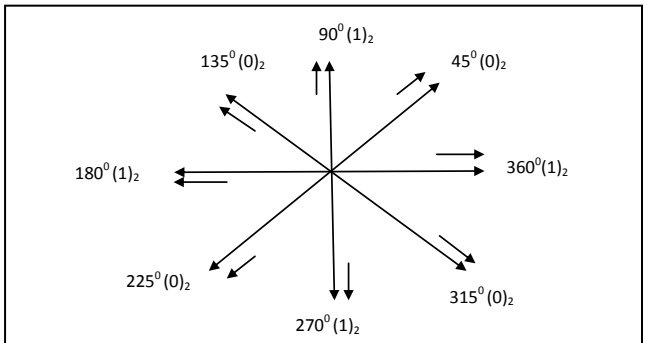


Fig. 2. Modified photon polarization structure.

According to BB84 protocol, the modified photon polarization is shown in Table. 1. The primary step in BB84 protocol is quantum transmission. The sender creates a random bit (0 or 1) and then randomly selects from it, one of the two bases (rectilinear or diagonal) which is transmitted in the channel. Then, a photon polarization state is prepared which depends on the bit value and basis, as shown in the Table. 1.

Before polarization a random number is generated for each bit and based on that random number the bits are polarized and the sender then transmits a single photon in the state precise to the receiver, using the quantum channel. By polarizing the bits with eight states, the possibility of finding the original bit is difficult for the eavesdropper. This procedure is repeated for the random bit state, with sender documenting the state, basis and time of each photon sent.

As the receiver does not know the premise the photons were encoded in, everything receiver can do is to choose a premise indiscriminately to quantify in, either rectilinear or

TABLE 1
PHOTON POLARIZATION BASIS FORMATION

| Basis | 0 | 1 |
|---|---|---|
| + | → | ↗ |
| × | ↑ | ↖ |
| / | ← | ↙ |
| \ | ↓ | ↘ |

diagonal. Receiver does this for every photon receiver gets, the recording time, estimation premise utilized and estimation result. After the receiver has estimated each and every one of the photons, receiver speaks with the sender over general society traditional channel. Sender communicates the basis of

every photon which was sent in, and the receiver measured the basis of every photon assess in. They both dispose photon inference (bits) where receiver utilized an alternate premise, which is half by and large, leaving a large portion of the bits as a mutual key.

### 3.2 Key distribution using BB84 protocol in quantum channel- An Example

In this paper, BB84 protocol is taken RAND function is used and photon polarization structure is modified slightly and changed the basis is formulated. Photon polarization generates a shared secret key finally which is then used as private key in proposed MRSA. The key is distributed through the quantum channel and eavesdropping is noted which is shown in Table.2. If the probability of eavesdropping is not more, then the key distribution is not discarded.

Hence the probability of the eavesdropped key is 40%. So the eavesdropper lost the chance of eavesdropping. The key is transmitted to the receiver. The sender and receiver uses RAND function to form and measure the basis. The random key generated by sender is {155, 12, 254, 144, 92, 208, 332, 21, 158, 223, 126}, the receiver measured the basis using {125, 20, 260, 294, 313, 171, 262, 14, 147, 269, 100}. Thus the SSK retrieved from the table.2 is 01011. The corresponding decimal of 1011 is 11. This 11 is taken as private key and used in MRSA. Thus for every QKD a SSK will be generated and different SSK's can be used for each time of encryption.

TABLE 2
QKD AND GENERATION OF SSK

| **Sender's rb** | **1** | **0** | **1** | **0** | **1** | **1** | **0** | **1** | **1** | **1** | **1** |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Sender's random sending basis** | × | + | / | × | + | / | \ | + | × | / | + |
| **PP Sender sends** | ↖ | → | ↙ | ↖ | ↗ | ← | ↘ | → | ↖ | ↙ | → |
| **Eve's random measuring basis** | × | + | / | / | + | / | \ | \ | × | × | \ |
| **Polarization Eve measures and sends** | ↖ | → | ← | ↙ | ↗ | ← | ↓ | ↘ | ↖ | ↑ | ↓ |
| **Receiver's random measuring basis** | × | + | / | \ | \ | × | / | + | × | / | × |
| **PP Receiver measures** | ↑ | → | ↙ | ↓ | ↓ | ↗ | ↙ | → | ↖ | ↙ | ↑ |
| **SSK** | | **0** | **1** | | | | | **0** | **1** | **1** | |
| **Errors in key** | | ✔ | ✘ | | | | | ✘ | ✔ | ✘ | |

*{rb- random bit, PP- photon polarization, SSK- Shared Secret Key}*

## 4 ENCRYPTION AND DECRYPTION IN QC

In quantum cryptography key distribution protocols are proposed and used. But for encryption quantum cryptography uses public and symmetric key algorithms. The security of public key algorithms was already broken by quantum algorithms so to overcome that and to enhance the security, a modified RSA (MRSA) method is proposed in this paper in which the private key is generated from the distributed SSK and the encryption/decryption is performed. For text encryption, the plaintext message is taken and its ASCII value is found for each character. Then the ASCII value of each character is taken as the public key and the encryption is performed. This provides additional layer of security.

### 4.1 RSA (Rivest–Shamir–Adleman)

RSA is a well known public key algorithm which is utilized for encryption and decryption. It is extensively used for secure data transmission. The encryption key is public and the decryption key is kept secret. The RSA algorithm basically has three phases, key generation, encryption and decryption. Usually private key is generated from public key. But in this proposed MRSA, public key is derived from private key. Generating public key from private key is very difficult and hence it makes the possibility of finding the keys hard and enhances the security. The RSA algorithm generates the keys in the following way: Choose two different prime numbers pq. Compute n=pq. Find $\phi(n) = (p-1)(q-1)$. Choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$. Determine d as $d \equiv e^{-1} \pmod{\phi(n)}$. In this proposed MRSA, d is taken from SSK of BB84 protocol. Then encryption is done using $C=M^e \bmod n$ and decryption is performed using $M=C^d \bmod n$.

### 4.2 Modified RSA- An Example

In order to understand the relevance of the work, the SSK is taken from BB84 protocol. In this example, the SSK generated is 11. So d=11. Hence e, p and q must selected in a way that $d=e^{-1} \pmod{\phi(n)}$. In this scenario, private key {d,n} is known first. From d the other parameters are generated. Let p=11, q=13. Then n is computed as (11×13=143) pq. $\phi(n)=120$. The private key of the user is (11, 143) from SSK. The public key of the user is (11, 143) which is obtained from d. As the key generation is performed, the encryption is performed by taking the ASCII value of the plaintext.

The message to be encrypted is M="CRYPTOGRAPHY". The ASCII value of each character is computed first. That is the ASCII value of "CRYPTOGRAPHY is{67,82,89,80,84,79,71,82,65,80,72,89}. M is encrypted as $C=M^e \bmod n$. That is, C= 6711 mod 143= 111. The decryption is $M=C^{SSK} \bmod n$, that is M= 11111mod 143= 67. Thus the message is decrypted using SSK. Similar process is followed for other plaintext characters. Table. 3 show the encryption and decryption with proposed MRSA.

## 5 Results and Discussion

The proposed methodology is implemented in VC++ with version 6.0. The encryption, decryption time and security are calculated and it is compared with existing RSA and proposed MRSA. Table.4 shows the experimental results of existing RSA.

Table.5 shows the encryption, decryption and security of proposed MRSA method.

TABLE 3

ENCRYPTION AND DECRYPTION IN MRSA

| Sl. No. | Plaintext (PT) | ASCII (PT) | Encryption C= $M^e$ mod n | MDecryption M= $C^{SSK}$ mod n | PT |
|---|---|---|---|---|---|
| 1 | C | 67 | 111 | 67 | C |
| 2 | R | 82 | 49 | 82 | R |
| 3 | Y | 89 | 45 | 89 | Y |
| 4 | P | 80 | 124 | 80 | P |
| 5 | T | 84 | 128 | 84 | T |
| 6 | O | 79 | 79 | 79 | O |
| 7 | G | 71 | 115 | 71 | G |
| 8 | R | 82 | 49 | 82 | R |
| 9 | A | 65 | 65 | 65 | A |
| 10 | P | 80 | 124 | 80 | P |
| 11 | H | 72 | 28 | 72 | H |
| 12 | Y | 89 | 45 | 89 | Y |

Fig. 3 shows the Comparison graph for Encryption, Decryption time for existing RSA and proposed MRSA and Fig. 4 show the comparison result of security.

TABLE 4

ENCRYPTION AND DECRYPTION OF EXISTING RSA

| File Size (MB) | Encryption | Decryption | Security in (%) |
|---|---|---|---|
| 1 | 2099 | 3010 | 86 |
| 2 | 5371 | 5455 | 84 |
| 3 | 8864 | 8899 | 88 |
| 4 | 10985 | 11003 | 90 |
| 5 | 13927 | 13984 | 85 |

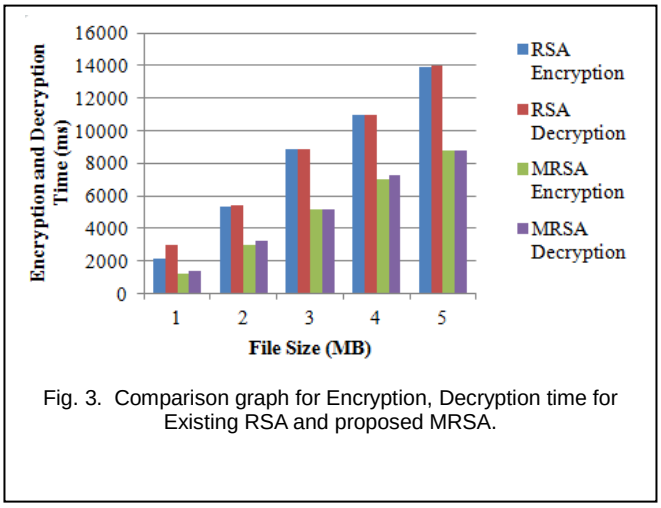


Fig. 3. Comparison graph for Encryption, Decryption time for Existing RSA and proposed MRSA.

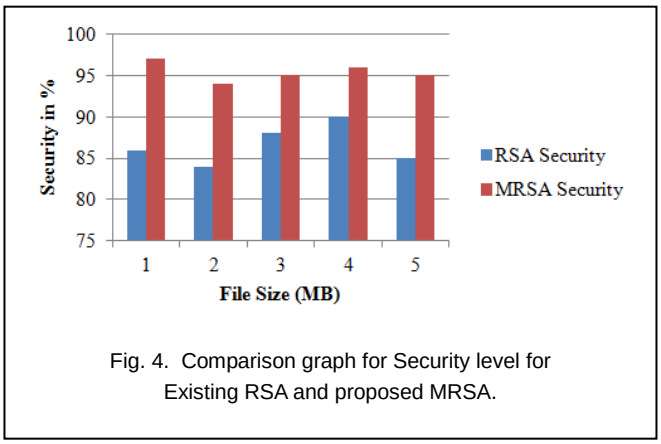


Fig. 4. Comparison graph for Security level for Existing RSA and proposed MRSA.

TABLE 5

ENCRYPTION AND DECRYPTION OF PROPOSED MRSA

| File Size (MB) | Encryption | Decryption | Security in (%) |
|---|---|---|---|
| 1 | 1248 | 1366 | 97 |
| 2 | 3002 | 3198 | 94 |
| 3 | 5136 | 5190 | 95 |
| 4 | 6983 | 7234 | 96 |
| 5 | 8778 | 8812 | 95 |

## 6 Conclusion

An alternate encryption method is proposed in QC. BB84 protocol was used for QKD. A modified structure for photon polarization is defined. The key is generated and distributed with the modified structure for photon polarization. The distributed key is taken as the private key which is generated, was then used for encryption and decryption. The proposed MRSA is compared with existing RSA. The proposed MRSA enhanced the security and encryption and decryption time. Further, the generation of SSK can be done for each character of plaintext message so that the possibility of retrieving the key will be difficult and the same can be incorporated in Internet of Things (IoT).

## REFERENCES


[1] https://en.wikipedia.org/wiki/Quantum_cryptography.

[2] https://en.wikipedia.org/wiki/Quantum_key_distribution.

[3] Mohamed Elboukhari, Mostafa Azizi and Abdelmalek Azizi, "Improving TLS Security by Quantum Cryptography", International Journal of Network Security & Its Applications (IJNSA), Vol.2, 2010.

[4] David Gaharia and Joel Wibron, "Detection of Eavesdropping in Quantum Key Distribution using Bell's Theorem and Error Rate Calculations", Research Academy for Young Scientists, 2011.

[5] Neha Chhabra, "Secret Key Generation and Eavesdropping detection using Quantum Cryptography", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 3, 2012.

[6] Abhishek Agnihotri, "The Next Level of Information Security-Impact of Quantum Cryptography", International Journal of Engineering Science Advance Research, Vol. 2, 2016.

[7] Vivek Singh and Bhawna Chauhan, "Survey on Various Quantum Key Distribution Algorithms", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 6, 2015.

[8] Ammar Odeh, Khaled Elleithy, Muneer Alshowkan, Eman Abdelfattah, "Quantum Key Distribution by Using Public Key Algorithm (RSA)", IEEE, 2013.

[9] Rajni Goel, Moses Garuba, Anteneh Girma, "Research Directions in Quantum Cryptography", International Conference on Information Technology (ITNG'07), 2007.

[10] N.Sasirekha, M.Hemalatha, "Quantum Cryptography using Quantum Key Distribution and its Applications", International Journal of Engineering and Advanced Technology (IJEAT), Vol. 3, 2014.

[11] Aparna Singh, "Centralized Key Distribution using Quantum Cryptography", International Journal of Computer Science and Mobile Computing (IJCSMC), Vol. 6, 2017.

[12] Luis Adrian Lizama-Pérez, José Mauricio López and Eduardo De Carlos López, "Quantum Key Distribution in the Presence of the Intercept-Resend with Faked States Attack", Entropy, Vol. 19, 2017.

[13] Hitesh Singh, D.L. Gupta, A.K Singh, "Quantum Key Distribution Protocols-A Review", IOSR Journal of Computer Engineering (IOSR-JCE), Vol. 16, 2014.

[14] D N Kartheek, M Abhilash Kumar, M R Pavan Kumar, "Security using Quantum Key Distribution Protocols (QKDPs)", International Journal of Scientific & Engineering Research(IJSER), Vol. 3, 2012.

[15] Charles H. Bennett, Gilles Brassard, "Quantum cryptography-Public key distribution and coin tossing", Theoretical Computer Science, Vol. 7, 2014.

[16] Beatrice A. Dorothy and Britto S. Ramesh Kumar, "DORBRI: An Architecture for the DoD Security Breaches Through Quantum IoT", Lecture Notes on Data Engineering and Communications Technologies (Springer), Vol.15, 2018.