Quantum Cryptography over Asymmetric Channel: Review

Rajni Bala, Research Scholar, Physics, Janaradan Rai Nagar Vidyapeeth, Udaipur (Rajasthan).
Dr. R.N Sharma, Professor, Physics, Janaradan Rai Nagar Vidyapeeth, Udaipur (Rajasthan).

INTRODUCTION

One of the most cutting-edge approaches to quantum cryptography is known as Measurement Device-Independent Quantum Cryptography (MDI-QKD), and its primary objective is to enhance the safety of communication via the use of asymmetric channels. Conventional methods for the distribution of quantum keys (QKD) are dependent on the secure transfer of quantum states between two entities, who are often referred to as Alice and Bob. These protocols, on the other hand, often depend on the precision of the measurement equipment that are used by both parties, which may be susceptible to hacking and other vulnerability issues in terms of security.

To provide security even in circumstances in which the measurement devices have been hacked or cannot be trusted, MDI-QKD is designed to accomplish this purpose. Because the dependability of these devices is essential to the safety of the quantum communication system as a whole, this is of utmost significance in scenarios that take place in the real world. A dependable solution that is not dependent on the specifics of the measurement equipment that is being used is provided by MDI-QKD. This is accomplished via the utilisation of a device-independent perspective.

It is the intention of the protocol to perform well over asymmetric channels, which means that the quantum states that are sent between parties may come into contact with different surroundings or conditions. This is a significant departure from symmetric channel scenarios, which are characterised by the assumption that the quantum communication channels used by all parties involved in the communication are similar.

The objective of MDI-QKD is to fortify the defences against potential attacks on measurement devices, which are considered to be vulnerable regions in traditional QKD implementations. MDI-QKD reinforces the resistance of quantum communication systems against various eavesdropping methods and other types of assaults, hence reducing the need that the measurement devices be trusted. This results in an overall improvement in the security of quantum communication systems.

The purpose of this introduction is to provide you with an understanding of the challenges that are associated with the use of conventional quantum key distribution. Additionally, we highlight the need of a technique that is both more secure and independent of the device being used. In the following parts, a comprehensive essay or study on this topic would go into great detail on the mathematical formulations, actual implementations, and probable applications of MDI-QKD over asymmetric channels. This would be done in great detail.

MEASUREMENT-DEVICE-INDEPENDENT QKD

For the sake of gaining a deeper understanding of how mdiQKD works, let us begin by describing a QKD protocol that is based on the Einstein-Podolsky-Rosen (EPR) algorithm Everybody, even Bob and Alice, makes an EPR.

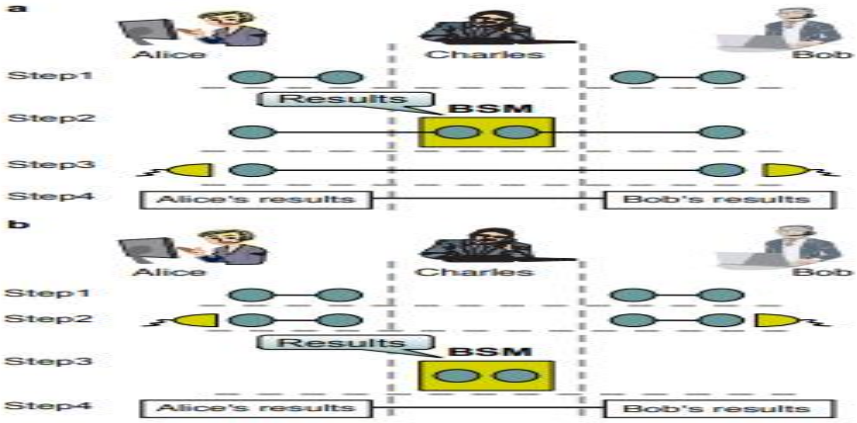

Figure The Einstein-Podolsky-Rosen (EPR) theory forms the foundation for a QKD approach

Figure (colours available online) A) The Einstein-Podolsky-Rosen (EPR) theory forms the foundation for a QKD approach. First, Bob and Alice work together to create an EPR pair, and then they split it in half and transmit it to Charles, who is an untrustworthy third party. Following the receipt of the signals, Charles is required to do a Bell state measurement (BSM) in order to carry out an entanglement swapping operation. This must be done prior to the dissemination of the results of his measurement. The next step is for Alice and Bob to select the X or Z bases that they will use to measure their particles in a random fashion.

QUANTUM CRYPTOGRAPHY

Benioff is credited with being the first person to identify the relationship between quantum physics and software development. His research, on the other hand, does not illustrate whether or not quantum mechanics offers greater processing power; rather, it demonstrates that quantum physics have a computing capability that is equivalent to that of a traditional computer. Following this, Feynman made a surprising forecast that predicted quantum mechanics might be more computationally competent than Turing machines. In addition, Feynman claimed that it would be more effective to duplicate quantum physics by employing computers that are based on quantum mechanical processes rather than by employing a regular computer to do this task.

In particular, Deutsch raises the question of whether or not the use of quantum computers may aid the resolution of classical problems in a more expedient manner than the utilization of conventional computers. For the purpose of doing research on this topic, he proposed the concept of quantum circuits and quantum transistor machines. After then, a comprehensive examination was carried out to determine whether or not the implementation of quantum mechanics into computers may potentially improve the efficiency of processing. Subsequent research has been carried out on notions that are comparable, and it has been shown that certain problems that need exponential time to solve in classical computers may be solved in polynomial time when calculating using quantum mechanics in computers. Recently, in, Shor successfully showed discrete logarithm and prime factorization polynomial time algorithms on a quantum computer, much to the pleasure of the cryptographers. Bits, also known as qubits, are utilised by a quantum computer in a manner that is analogous to how a conventional computer utilises bits (0 and 1). The quantum bits that make up a quantum state are what define it. In order to provide a description of the state of a quantum computer, basis vectors of a Hilbert space are necessary.

A qubit is a quantum state that is defined by the equation |Ψi = u|0i + v|1i, where u and v are vectors that belong to C and are basis vectors of the Hilbert space. This mathematical expression ensures that the sum of kuk 2 and kvk 2 equals 1. For the purposes of mathematics, a qubit is a value that is assigned to the vector space C 2, and the space C 2 n is the quantum state space that is associated with n qubits. The exponential dimensionality of quantum computing gives increased processing capability. This is due to the fact that quantum computation takes place in C 2 n. The components that make up a quantum computer are a limited number of ordered qubits.

The input for a classical issue that has to be addressed by a quantum computer can be a binary string of known length δ. This string can be utilised as the input for the problem. After then, the data is encoded to the initial quantum state of the computer, which is represented as a vector in the C 2 n space. In the space C 2 n, the state of a quantum computer is a unit vector after a calculation has been performed on it. Because quantum measurement is a probabilistic process, it is not necessary for quantum computing to always deliver an exact result. This is because quantum computing is a probabilistic process. With that being said, the right response is discovered at least two thirds of the time. The reader may choose to continue reading by going to. Among the many asymmetric key cryptography protocols that are used, the IFP, DLP, and ECDLP are three of the most significant and computationally unsolvable problems. These problems are used to develop a variety of protocols. Quantum computers are capable of doing computations at an exceedingly rapid pace and present a significant challenge to these problems.

DISTRIBUTION USING ENHANCED BB84 QUANTUM CRYPTOGRAPHY PROTOCOL AND KEY GENERATION

Within the scope of this chapter, the use of the enhanced BB84 quantum cryptography protocol for the generation and dissemination of secret keys is discussed. This particular chapter is divided into three sections. A presentation on quantum cryptography was given in the first section. The proposed work architecture, the generation of qubits, check bits, quantum keys, bitwise operations with quantum keys, and the public communication are all topics that are covered in the second section of the paper. The experimental results are analysed, and the chapter is ultimately summed in the third portion of the chapter for consideration.

Security problems are very important with regard to wireless body sensor networks (WBSN). The vulnerability of wireless body sensor networks to security breaches is higher than that of wired networks. A number of security challenges are associated with the WBSN, including the distribution of secret keys, authentication, confidentiality, and integrity. Both the dissemination of secret keys and the generation of new ones are essential security tasks in the WBSN. More sensitive data comes from sensors located on the body. If the data are changed from their original format while being watched remotely by a healthcare professional, it will have an effect on the treatments that are being administered. The patients' health would be greatly influenced as a result of this factor. The technique that has been provided for the production and distribution of keys may minimise the amount of power that is utilised for key distribution while still keeping the simplicity of the computations involved. While simultaneously prolonging the lifetime of a network, it maintains the security of the WBSN.

When medical data is sent via a wireless network, there is a possibility that it might be subject to attacks on sensitive health data. By using the cryptographic approach, it is possible to steer clear of situations like this one. It is necessary to make use of cryptographic methods and secret keys in order to encrypt and decode the patient's medical information. When this method is used, the parties involved in the communication process are provided with an indirect component of the secret key. When using quantum methods for communication, the participants in the conversation exchange the secret key with one another. It would be good to prevent both passive and active attacks on the access key to the hidden location.

Quantum Cryptography

When applied to the data, quantum cryptography applies quantum mechanics in order to give an extremely high level of protection for the information. Individuals who are not directly involved in the transmission of the information will be unable to comprehend the encryption format that is applied by quantum cryptography. For the purpose of keeping listeners from listening in on discussions, states of quantum photon polarisation are very helpful.

Classical cryptography operations make use of a variety of numerical methodologies, including permutations, mathematical calculations, and other numerical methods. Breaking down and figuring out these approaches is not difficult at all. During interactions, sensitive information about the human body, including as the rate of the heart, the temperature, and the impulses in the brain, are transformed and sent across a wireless link to medical experts and members of the immediate family. For this reason, additional security measures are necessary in order to provide cryptographic methods that cannot be successfully broken. There is the possibility of using the quantum cryptography protocol BB84 in order to provide a strong security solution for a wireless body sensor network. A representation of the quantum cryptography process may be seen in Figure The method of quantum cryptography is comprised of three different activities. In such case,

- Quantum mechanics-based encryption is the first option.
- A method for decrypting quantum information is referred to as .
- Quantum key generation is the third topic.
- Encryption by the use of quantum law

The use of quantum encryption ensures that both the confidentiality and integrity of information are maintained. Encryption refers to the process of altering the shape of the information under consideration. A cypher text format is used to transmit the information to the individuals who are permitted to communicate with the recipient. These individuals are the only ones who have the power to reverse the change and retrieve the data in its original form.

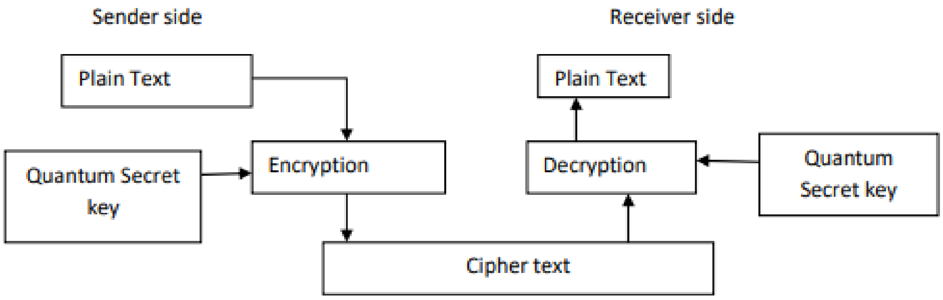

Figure Quantum cryptographic process

B. Quantum decryption

The process of decrypting medical data from human body sensors entails converting the data from a cypher text format into a plaintext one that can be understood by the user.

C. Quantum secret key

Qubits are arranged in a certain configuration to form the quantum secret key. It has the potential to make a contribution to the mathematical process of encrypting sensed data and to decode medical data obtained from sensors located on the human body. Distributing and retaining that key is of the utmost importance. In the event that the secret key is misplaced at any time throughout the life cycle of the information, the specified level of information security is not guaranteed. A sufficient amount of encryption is used in order to guarantee the confidentiality and authenticity of the medical data. The secret key is an important part of cryptography and is an essential component. This structure is based on the concept of two-photon polarisation,

(i) Rectilinear basis (+).

(ii) Diagonal basis (×).

According to Sandeep et al. (2018), the rectilinear basis may be divided into two kinds of polarisation: vertical polarisation (angle - 90 degrees) and horizontal polarisation (angle - 0 degrees). On the diagonal basis, there are two different polarisation states: 45 degrees and 135 degrees. Table presents the polarisation scheme that is used by the BB84 protocol.

Table BB84 protocol polarization scheme

Un-directional polaroid mode	Polaroid mode	Directional polaroid mode	Binary value
✛	⦶	↕	1
✛	⦶	↔	0
✕	⊘	⤢	1
✕	⦸	⤡	0

By using a quantum communication channel, it is possible for key information and encrypted information to be sent between parties that are conversing with one another. The implementation of this channel is made possible with the support of networks that are coupled with optical fibres. Quantum channels provide very robust protection for the confidentiality of information. Within the channel itself is a security system.

Figure Quantum communication channel

When listening in on a discussion via the classical channel, it is impossible to determine who is listening in on the conversation. The communication that takes place over the quantum channel that only sends in one way is shown in Figure As a consequence of this, there is now a possibility that the security around sensitive data may be breached. With a quantum channel, on the other hand, the transmission of secret key data from the transmitter to the receiver is accomplished via the use of light waves. Because the quantum communication channel is able to instantaneously recognise the presence of a third party among the parties that are authorised to connect, the eavesdropper is unable to listen in on the discussion that is taking place.

Key Generation for the EMRSACS System

For the objectives of key generation, encryption, and decryption, Kapoor (2018) has chosen four prime numbers as the variables of investigation. In this context, the transmission of sensitive information is reliant not only on these prime numbers but also on the procedures of factorization and multiplication.

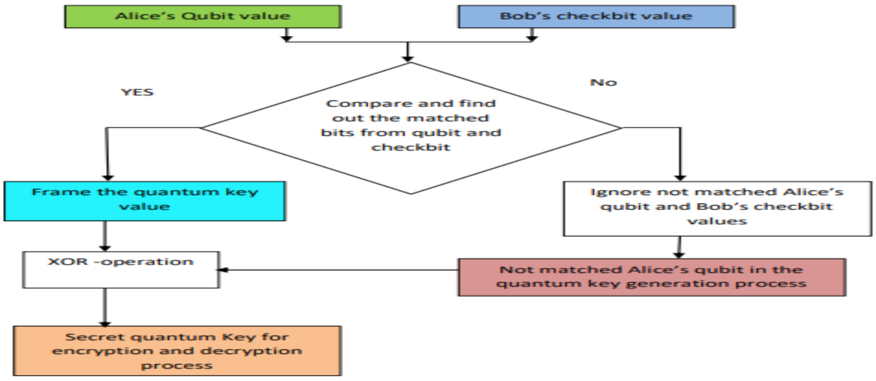
Alice's Qubit value
Bob's checkbit value
YES
No
Compare and find out the matched bits from qubit and checkbit
Frame the quantum key value
Ignore not matched Alice's qubit and Bob's checkbit values
XOR -operation
Not matched Alice's qubit in the quantum key generation process
Secret quantum Key for encryption and decryption process

Figure Quantum key generation process

$n = p * q * r * s$ ……………………(4.17)

$Pi(n) = (p-1) * (q-1) * (r-1) * (s-1)$ ……………………….(4.18)

$d * e \bmod Pi(n) = 1$ ……………………………..(4.19)

Multiplying four prime numbers "n" may be accomplished with the help of equation. A factorization of prime numbers and the multiplication of such numbers by Pi (n) may be accomplished with the help of equation. Following that, a value for the public key is chosen. For the purpose of determining the private key that is required for the decryption process, Equation is ultimately used. Figure illustrates the process of generating a secret quantum key value using the various techniques. What are the actions?

Step 1: It is possible for Alice, the sender, to choose the random binary value and the quantum basis by herself.

Step 2: The comparison of a binary value to a quantum basis is what results in the generation of the qubit value.

Step 3: The receiver, Bob, has the ability to choose their own random binary value and quantum basis using this option.

Step 4: After comparing the binary value of the receiver with the quantum basis, the check bit value is produced as a result of this comparison.

Step 5: Having compared the qubit and check bits, the matched bits are now framed in their respective positions.

Step 6: The mismatched bits of the sender are used in conjunction with the matched bits in order to carry out the bitwise operation. The process that is being used to frame the secret quantum key for secure communication is described here.

Security from EMRSACS

The original message, the public key, and the quantum key are the three values that are put into the encryption. For the purpose of converting plaintext into ciphertext, this process makes use of Equation .The technique has included the operation of modulus, which has been used.

$$C= (M^{e} \bmod (n))^{QK} \bmod n$$

……………………(4.20)

The Decryption of EMRSACS

The value of the quantum key, the private key, and the ciphertext are the three things that are required for the decoding process. Within the context of this technique, Equation is used to convert cypher text into plaintext. The technique has included the operation of modulus, which has been used.

$$M=(C^{d} \bmod (n))^{QK} \bmod n$$

…………………………………(4.21)

Encryption, decryption, and the generation of keys are all operations that are necessary for maintaining security. When it comes to communicating sensitive medical data about the human body, the solution that has been presented is suitable. It is possible that it will create data confidentially in a period of time.

FOUNDATIONS BASED ON EXPERIMENTAL RESEARCH

The proposed system necessitates the use of 64, 96, 150,208,298 bit key size values in order to facilitate the generation of keys, encryption, and decryption tasks. In order to determine whether or not the proposed method is successful, the following metrics are utilised: the amount of time required for key creation, encryption and decryption, memory requirements, overall execution time, and energy consumption. The security of the proposed system is evaluated in relation to attacks that consist of mathematical, temporal, and brute force computations.

Time of generation in relation to key size

The EMRSACS places a significant emphasis on the production of access keys. When a strong key is used, the security of the whole system becomes completely impregnable. The approach that has been presented involves not only the utilisation of four prime integers for the purpose of key generation, but also the encryption and decryption of undiscovered quantum keys. In order to complete the mathematical operations that include the four prime numbers, more time is necessary. This approach is considered to be fairly secure in WBSN.

Table presents a comparison of the timeframes required to generate keys for the system that was recommended, EMRSACS, and other encryption algorithms. To indicate the sizes of keys, bits are used. The time it takes to generate the key is expressed in milliseconds.

Table Key size Vs. Key generation time

Key size(bits)	**RSA Key generation time (ms)**	**Proposed-EMRSACS Key generation time (ms)**
64	157	216
96	184	257
150	263	413
208	381	542
298	476	691

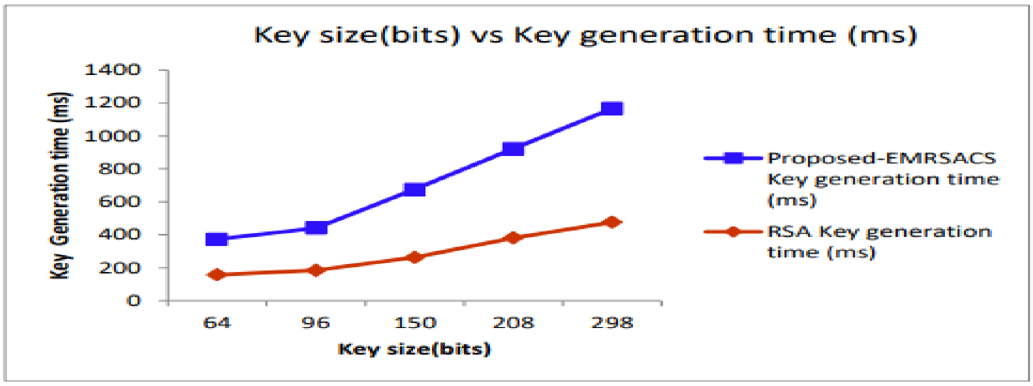

Figure Key size Vs. Key generation time

On display in Figure are the timeframes required to generate the RSA and EMRSACS keys. The level of security is also increased if the size of the key and the computational complexity are both too large. In comparison to RSA, the method that has been described would need a longer amount of time to produce keys.

Throughout the process, three different keys are created. The first of them is a public key, from which the user may choose a value according to their preferences. This is the second key, which is the private key. In order to calculate this key, the equation is used. Following this, the bitwise operator and the quantum mechanism are utilised in order to create the confidentiality of the quantum key. The process of key generation is essential to both the encryption and decryption procedures. For the purpose of facilitating the secure transmission of physiologically sensed information about the human body in applications that are associated with healthcare, the system that has been presented offers strong keys. The recommended method requires a longer amount of time to produce keys in compared to the RSA algorithm.

SUMMARY

This chapter addresses the issue of maintaining the confidentiality of data that is sent via a wireless connection. The proposed method improves wireless sensor networks (WBSNs) by encrypting and decrypting data with the use of a quantum key value that is concealed. As a result of the fact that the multiplication of two prime numbers is predictable, the RSA key creation technique is not very strong. The keys are generated by the use of this process, which makes use of four prime numbers. This method also results in the development of resilient keys, which is another benefit of the strategy that has been offered. An additional component that has the potential to jeopardise the security of data transmission is the RSA public key. It is possible to reduce the impact of this disadvantage by including the secret quantum key into the cryptography procedure as one of the parameters. It is not possible to launch attacks using brute force, mathematical methods, or temporal methods in the EMRSACS. Despite the fact that a brute force attack might be used to test possible private keys, the cryptography of the proposed approach is dependent on the quantum key that is kept secret. Attackers have the ability to deal with mathematical attacks. In the classic RSA approach, there are just two prime numbers that are employed, and it is not difficult to break their multiplication and factorization. There are four prime numbers included in the technique that has been offered. Immediately, the factorization of four prime numbers is too difficult to be considered feasible. The approach that is presented provides a higher level of confidentiality for the transmission of data. It is dependent on the length of time it takes to finish the decryption process that timing attacks are carried out. Four prime numbers and a quantum key that is kept a secret are used in the strategy that has been presented. The process of establishing quantum keys and factorising four prime numbers adds an additional layer of complexity to the data transmission security method in this particular scenario. During the time that the communication is valid, attackers are unable to anticipate it or break it apart. In comparison to RSA, the operations of generating keys, encrypting data, and decrypting data while using EMRSACS need more time. At the moment, the transmission of physiological data that is sensed by the human body takes a longer amount of time, and the security of communication is relatively robust. When compared to the RSA protocols that are currently in use, the method that has been recommended offers consistently good performance in terms of the amount of time required for key generation, encryption, and decryption. To defend against attacks based on time, mathematics, and brute force, it is possible to guarantee a high level of confidentiality about the data that is sensed from the body. When compared to RSA, the approach that has been presented provides a higher level of confidentiality for the generation of keys, encryption, and decryption.

CONCLUSION

There are three security requirements that are included in the research study that is being presented for secure communication in WBSN. The procedure begins with the generation and dissemination of secret keys, which are accomplished via the use of the Enhanced BB84 Quantum Cryptography protocol on the part of the participants. While the secret key is being sent, it may prevent an attacker from predicting the value of the secret key. EBB84QCP and a bitwise operator are responsible for the enhancement of the method for the distribution and production of secret keys. As the next stage in the process of meeting the security requirement, the Message Authentication Code, also known as Modified Enhanced Lattice Based Cryptography (MELBC), is used to establish authentication. Lattice-based double encryption techniques with a concealed quantum key and plaintext splitting methods are used in order to give high-level authentication. The last need for security is secrecy, which may be achieved via the use of the Enhanced Modified RSA cryptosystem technology. The use of four prime numbers, rather than two, is the method that is being used here. The use of a secret quantum key is employed for the goal of enhancing the RSA encryption and decryption processes. A tough approach is provided for both assuming the secret key value and breaking the encrypted material, which is one of the ways in which this feature differentiates itself from others. In order to guarantee that the WBSN is protected by a high level of security, each of the three security criteria is implemented using contemporary approaches.

BIBLIOGRAPHY

[1] Abdulameer K Hussain 2015, ‘A modified RSA algorithm for security enhancement and redundant messages elimination using K-nearest neighbor algorithm’, International Journal of Innovative Science, Engineering & Technology, vol. 2, no. 1, pp. 159-163.

[2] Achi, Harrisson, Thiziers, Haba, Cisse, Theodore, Jeremie, T, Zoueu & Babri Michel 2019, ‘Enhanced, modified and secured RSA cryptosystem based on n prime numbers and offline storage for medical data transmission via mobile phone’, International Journal of Advanced Computer Science and Applications, vol. 10, no. 10, pp. 353-360.

[3] Al-Batool, Al-Ghamdi, Ameenah, Al-Sulami, Asia Othman & Aljahdali 2020, ‘On the security and confidentiality of quantum key distribution’, Security and Privacy, vol. 3, no. 5, pp. 1-4.

[4] Biswapati, Jana, Soamdeep, Singha, Sharmistha & Jana 2013, ‘Key distribution in wireless sensor networks using quantum cryptography’, International Journal of Mobile & Adhoc Network, vol. 14, no. 4, pp. 250-256.

[5] Chaudhary, R, Aujla, GS, Kumar, N & Zeadally, S 2019, ‘Lattice-based public key cryptosystem for internet of things environment: Challenges and solutions’, IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4897-4909.

[6] Chinmoy, Ghosh, Amit Parag & Shrayasi Datta 2017, ‘Different vulnerabilities and challenges of quantum key distribution protocol: A Review’, International Journal of Advanced Research in Computer Science, vol. 8, no. 8, pp. 307-311.

[7] Hui, Li, Yuhan, Zhao & Yingpei, Sun 2015,’ Wireless sensor network based on high-dimensional quantum communication’, International Journal of Innovative Computing, Information and Control, vol. 11, no. 6, pp. 2119-2133.

[8] Jarrar, Ahmed, Ashish Kumar, Garg, Man, Singh, Sham, Bansal & Mohammad Amir 2014, ‘Quantum cryptography implementation in wireless networks’, International Journal of Science and Research, vol. 3, no. 4, pp. 129-133.

[9] Miralem, Mehic, Peppino, Fazio, Miroslav, Voznak, Erik & Chromy 2016, ‘Toward designing a quantum key distribution network simulation model’, Information and Communication Technologies and Services, vol. 14, no. 4, pp. 413-420.

[10] Muhamed Turkanovi & Marko Holbl 2014, ‘The(in)adequacy of applicative use of quantum cryptography in wireless sensor networks’, Quantum Information Processing, vol. 13, no. 10, pp. 2255-2275.

[11] National Institute of Information and Communications Technology (NICT) and ZenmuTech 2020, Quantum cryptography to encrypt, transmit and backup electronic medical records, Available from: . [20 November 2020]

[12] Sai Suguna, Y, Kavya Reddy, B, Keerthi Durga, V & Roshini, A 2018, ‘Secure quantum key distribution encryption method for efficient data communication in wireless body area sensor net-works’, International Journal of Engineering & Technology, vol. 7, no. 2.32, pp. 331-335.

[13] Saptarshi Sahoo, Pratik Roy, Amit Kumar Mandal & Indranil Basu 2021,’ Quantum Cryptography– A Theoretical Overview’, Journal of Quantum Computing, vol. 3, no. 4, pp. 151-160.

[14] Selena Larson, St. Jude‘s implantable cardiac devices attack 2017, Attacks information. Available from: .[9 January 2017].

[15] Shaheen Saad Al-Kaabi & Samir Brahim Belhaouari 2019, ‘Methods toward enhancing RSA algorithm: A survey’, International Journal of Network Security & Its Applications, vol. 11, no. 3, pp. 53-70.

[16] Shally Nagpal 2016,’ A Study on Quantum Cryptography and Key Generation Methods’, International Journal of Scientific & Engineering Research, vol. 7, no. 12, pp. 402-406.