ROOTINDEXING
JOURNAL ABSTRACTING AND INDEXING SERVICE
INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
January-June 2023, Submitted in February 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

Basics of Cryptography through Definitions: An Overview

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.

Basics of cryptography

This section, we give some basic definitions and concepts which are used in cryptography and necessary for the understanding of thesis

Definition 1.2.1 (Plaintext). A plaintext is an original understandable message.

Definition 1.2.2 (Ciphertext). It is a transformed message obtained by plaintext using some algorithm and which is sent over open communication channel or through some other medium.

Definition 1.2.3 (Key). A key is a bit string which contains some vital information and is used to convert plaintext into ciphertext and vice-versa.

Definition 1.2.4 (Encryption). It is an algorithm used to convert a plaintext into ciphertext

Definition 1.2.5 (Decryption). It is an algorithm used to transform ciphertext back into plaintext. The decryption and the encryption function are the inverse of each other.

Definition 1.2.6 (Cryptosystem). A cryptosystem is an algorithm which consists of a fivetuple set (P, C, K, E, D) with the following specifications: P - finite set of possible plaintext; C finite set of possible ciphertext; K - finite set of possible keys; E - set of encryption functions; D - set of decryption functions.

As discussed earlier cryptography is categorised in two parts: symmetric key cryptography and asymmetric key cryptography. In symmetric key cryptography, the algorithms use same key for the purpose of encryption and decryption. That is if there is an encryption function, $f_{(k)} : \mathcal{P} \to \mathcal{C}$ then the corresponding decryption function, $f_{(k)}^{-1} : \mathcal{C} \to \mathcal{P}$ will use the same key for the purpose of decryption such that $f_{(k)}^{-1}(f_{(k)}(m)) = m$ for every m ∈ P. The algorithms in symmetric key cryptography are categorised in two parts; the stream algorithms or stream ciphers which operate on a single plaintext bit (or a byte sometimes) at one time and the block algorithms or block ciphers which operate on group of bits (called block) at one time. In asymmetric key cryptography, algorithms use two keys, one is used for the purpose of encryption and the other is use for the purpose of decryption. That is if there is an encryption function $f_{e(k)} : \mathcal{P} \to \mathcal{C}$ then the corresponding decryption function will be $f_{d(k)}^{-1} : \mathcal{C} \to \mathcal{P}$ such that $f_{d(k)}^{-1}(f_{e(k)}(m)) =$ for every m ∈ P. The key used for the purpose of encryption is available publicly and the key used for the purpose of decryption is kept secret.

The asymmetric algorithms because the work done in the thesis is dedicated to the designing of asymmetric key cryptographic protocols. For more details on symmetric algorithms and some other worth mentioning work reader may refer to.

Definition 1.2.7 (The big-O function). Suppose f, g : N → R +. Then, f(n) = O(g(n)) if there exist a constant K such that, f(n) ≤ K.g(n) ∀ n. Some examples related to this notation are as follows:

Example Let $f(n) = 2n^2 + 3n - 3$ and $g(n) = n^2$ then $f = O(g)$ as $f(n) \leq 3n^2$.

1. log n = O(n) for 1 > > 0. In other words the log function is smaller then any power function for large n.
2. e −n = O(n 2).
3. f(n)(= a0 + a1n + . . . ain i) = O(n i).

Definition 1.2.9 (Polynomial time algorithm). An algorithm is said to be polynomial time algorithm if the number of basic bit operations to execute an algorithm are O(k d), where k is the size of input in bits and d ∈ R +.

Definition 1.2.10 (Exponential time algorithm). An algorithm is said to be exponential time algorithm if the number of basic bit operations to execute an algorithm are O(c f(k)), where c > 1 is a constant and f is a polynomial function of the size of input k ∈ N.

Definition 1.2.11 (Subexponential time algorithm). An algorithm is said to be subexponential time algorithm if the number of basic bit operations to execute an algorithm are

$$L_q(\alpha, c) = O(e^{(c+o(1))(ln\ q)^{\alpha}(lnln\ q)^{1-\alpha}}),$$

where α ∈ R, 0 < α < 1, c is a positive constant and q is input to the algorithm and not the size of the input.

Security notions and random oracle model

In an effort to close the knowledge gap that exists between theory and practice in the field of cryptography, the Random Oracle Model (ROM) was first established. In the situation presented here, an adversary and an honest individual are both able to gain access to an oracle. It is necessary to make use of a random hash function in order to instantiate the random oracle because there are no real-world implementations of the random oracle. The public is given access to the hash function that acts as a random oracle. This is done with the intention of preventing the adversary from independently computing the outcome. Numerous asymmetric key cryptography approaches, including zero knowledge proofs, encryption schemes, signcryption schemes, and signature systems, all have their security proofs given by the ROM. Also included in this category are signature systems. The following procedures are required in order to make use of the ROM:

1. In a table that is maintained by the oracle, queries can be made in the format of (x, y), and either an adversary or an honest party can make them. This function takes a binary string as its input and returns another binary string as its output.
2. Whenever a query is executed, the Oracle examines it in relation to previous instances of the query that have been stored in the table. If the query has been executed in the past, it will produce the same result. In the event that this is not the case, a string chosen at random is returned as the response to the query.
3. Any and all inquiries, whether they come from an ally or an adversary, are kept strictly discreet. A another way of putting it is that an adversary is unable to access inquiries that have been carried out by an honest party, and vice versa.

It is only possible for a party to execute polynomial time queries to ROM while they are in the process of conducting a series of inquiries.

Definition 1.2.12 (Random Oracle Model (ROM)). A random oracle is a map defined as;

$$R : \{0,1\}^* \rightarrow \{0,1\}^{\infty}.$$

In order to determine the map, each bit of R(x) is selected in a manner that is both uniform and distinct for each x. As elucidated in, the symbol ∞ is employed solely for the purpose of eliminating uncertainty regarding the suitable length of an output; it does not exhibit an output that is infinitely lengthy. One of the advantages of using ROM to show the security of an asymmetric key cryptography protocol is that it allows for the following benefits:

1. If it can be proved that a protocol is secure in ROM, then that protocol is said to be sound.
2. Discovering a method of assault on the system that has been demonstrated to be secure in ROM is a challenging task.

A number of security principles are discussed in order to determine the level of security that any protocol that makes use of ROM possesses. Specifically, this article discusses two different security concepts: the first is to encryption methods, while the second is about signature schemes.

Protection of the encryption scheme against the Chosen Ciphertext Attack (CCA) from the encryption scheme As was discussed before, there are four distinct types of assaults that may be employed against a system of encryption. There are four types of attacks: the known plaintext assault, the selected plaintext attack, the chosen ciphertext attack, and the isolated ciphertext attack. The ciphertext alone attack is the least severe of these four assaults, while the chosen ciphertext attack is the most severe of the four and the most severe overall. When conducting a chosen ciphertext attack, an adversary who has access to an oracle has the ability to ask questions about any ciphertext, other than the ciphertext that is being targeted, in order to identify the plaintext that corresponds to the ciphertext. An adversary will make an effort to extract the plaintext of a specific ciphertext by making use of the information that is gathered from these searches. The selected ciphertext assault is further subdivided into two categories: adaptively chosen ciphertext assaults and indifferently chosen ciphertext attacks, which are sometimes known as lunchtime or midnight attacks. Both of these types of attacks are included in the selected ciphertext assault. An indifferently chosen ciphertext attack is a less dangerous form of ciphertext attack when they are compared to an adaptively selected ciphertext attack. During an indifferently picked ciphertext attack, the ciphertexts that are searched in a random oracle may be connected to one another; nevertheless, none of these ciphertexts may be related to the ciphertext that is being targeted. By using an adaptively produced ciphertext, each and every ciphertext that is queried in a random oracle is related to the ciphertext that was supposed to be used. As demonstrated in the subsequent experiment, an encryption technique is deemed secure against the adaptive Chosen Ciphertext Attack (CCA) if the advantage of all attackers with Probabilistic Polynomial Time (PPT)∗ is modest. There are two phases in the adversary APPT: the guess stage and the find stage. Here are the stages.

PROPOSED WORK

It is vital to generate secret keys and distribute them across communication partners in order to ensure the security of communications in wireless body sensor networks. The WBSN is responsible for handling sensitive health information. Even though remote treatment is based on WBSN data, even minute changes to the data that is perceived by the human body may have a significant effect, such as the possibility of death. Using misleading information, a physician is given instructions to treat a patient in an inappropriate manner. A large amount of focus is placed on WBSN security. There is a connection between the mathematical basis and that of classical cryptography. It is not difficult for the adversaries to figure out the calculations that were utilised to produce the secret key. Quantum cryptography, on the other hand, is reliant on quantum physics in order to generate secret keys. It is not possible for attackers to get the value of the secret key in this scenario. An improved version of the Enhanced BB84 quantum cryptography protocol technique is offered as a solution to the problems that traditional cryptography has with regard to the manufacturing and distribution of secret keys. In order to

create a solid foundation for the production of secret keys in the WBSN, it is comprised of the respective steps listed below.

- Recommendations should be made for the development and distribution of secret keys for wireless body sensor networks that are based on the Enhanced BB84 quantum cryptography protocol (EBB84QCP).
- There is a generation of qubits on the sender side.
- This includes the generation of check bits on the receiver side.
- This includes the generation of quantum keys.
- The quantum secret key is constructed by the use of a bitwise operation, which relies on the unmatched bits of the sender as well as the matched bits of the parties involved in the communication.
- Discuss the possibility of disseminating the mechanism behind the generation of quantum secret keys via public communication channels.
- Analyse the performance of the EBB84QCP in respect to the key mismatch ratio and the amount of time it takes to generate keys.

Architecture of the Proposed Work

A comprehensive process for the proposed system is shown in Figure A bitwise operator and a quantum process are used in wireless body sensor networks in order to produce and disseminate the secret key. In order to ensure the secure distribution of keys inside the WBSN, the EBB84QCP approach that has been suggested includes the following components.

1. The sender, Alice, begins by selecting a random number and then moves on to converting it into binary form.
2. It is possible for Alice to choose a quantum basis in a random fashion.
3. By comparing the binary forms of her random bit and the quantum basis, Alice is able to generate the qubit values necessary for the simulation.
4. Bob picks a number at random and converts it into binary form using his computer. In the subsequent step, a quantum basis is used in order to compare the binary form of the random number. He is the one who generates the values of the check bit.
5. Alice examines the difference between the check bit value of Bob and her own qubit value.
6. Following the comparison, Alice was able to figure out the matching bit from the qubit and the check bit.
7. In order to construct the secret key and match the bits on both sides that were not matched, Alice used the XOR process.

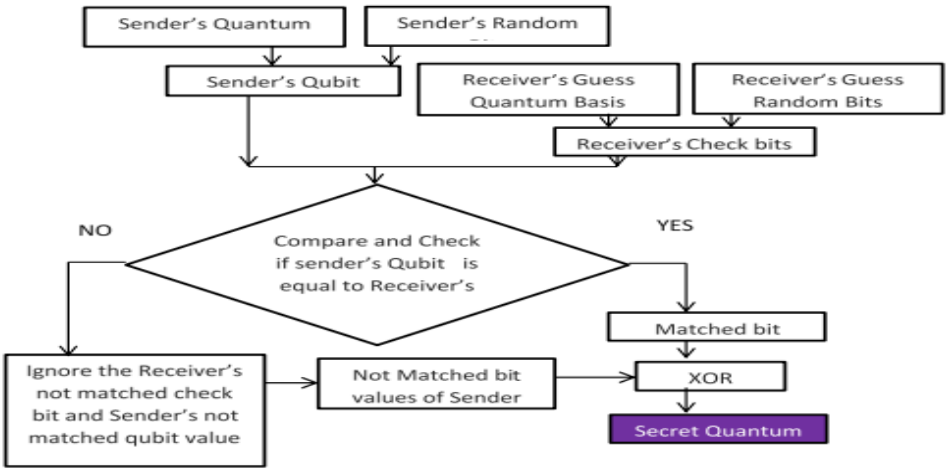

Figure Architecture of the proposed work

Following the XOR operation, Alice was ultimately responsible for determining the value of the secret key for communication. The value of the secret key is the fundamental component that underpins both encryption and decryption. For the purpose of conveying that significant

value, it is not meant to be communicated directly with the persons involved in the communication transaction. In order to prevent the attackers from determining the value of the secret key, the bitwise operator and quantum process that surrounds it prevent them from doing so.

The approach that has been proposed is comprised of the following components,

1. The production of qubits for use
2. Investigate the invention of the bit
3. The creation of quantum computer keys
4. Using a quantum key in a bitwise manner
5. Conversation made via the medium of public communication

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.

The Enhanced BB84 Quantum Cryptography Protocol (EBB84QCP) is designed to solve the issue of the creation and distribution of secret keys, which is a significant challenge in the WBSN. A total of six outstanding works are included in it. In the beginning, the sender is the one who generates the qubit. The check bits are produced by the receiver as a consequence of this. Further comparisons between the qubit and the check bit have been made by the sender in order to construct the secret key. In the subsequent step, the XOR operation is carried out by using the mismatched bit of the sender in conjunction with the quantum key. Following that, the sender and the receiver engage in a conversation on the particulars of the XOR operation and the manner in which the secret key is formed. In conclusion, the individuals who are participating in the communication engage in a roundabout exchange of their secret quantum key in order to carry out further cryptographic operations. In the event that they are present during the transmission, attackers are unable to anticipate the value of the key. In the WBSN, the strategy that has been offered involves the creation of bitwise operators and quantum methods for the distribution and production of strong keys.

To handle WBSN authentication, the MAC-MELBC approach is used as the recommended mechanism. It has successfully finished five actions that are necessary to ensure that authentication is successful. Patients and their sensors are the ones that first have to provide their information during the registration step. Validation of these registration details is accomplished with the aid of MAC. After that, the MELBC double encryption method is used in order to encrypt the information that pertains to phases 1 and 2. The MELBC implements a plaintext splitting in order to reduce the amount of computing resources required. As a last point of interest, the MELBC encryption and decryption process incorporates the exclusive

quantum key. It was possible for the MELBC-MAC approach to provide strong authentication with little processing by using a hybrid cryptosystem, which was the technique that was recommended.

The ultimate goal is to maintain confidentiality, which is done using the Enhanced-Modified RSA cryptosystem, also known as EMRSACS. The proposed method provides a high level of security since it makes use of two extra parameters, along with four prime numbers and their respective factorizations, as well as a secret quantum key. The processes of encryption and decryption used by EMRSACS need a lengthier amount of time to finish. There is a high level of confidentiality involved in this complex WBSN function.

Because of this, the aforementioned suggested methods provide a high level of security and privacy in WBSN. These methods make use of a variety of cryptographic techniques, such as the Enhanced BB84 Quantum Cryptography Protocol (EBB84QCP), Message Authentication Code Modified and Enhanced Lattice-Based cryptography (MAC-MELBC), and the Enhanced-Modified RSA cryptosystem (EMRSACS).

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] 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.

[5] Jiang, Q, Khan, MK, Lu, X, Ma, J & He, D 2016, 'A privacy preserving three-factor authentication protocol for E-Health clouds', The Journal of Supercomputing, vol. 72, no. 10, pp. 3826-3849.

[6] Kapoor, V 2013, 'Data encryption and decryption using modified RSA cryptography based on multiple public keys and 'n' prime number', International Journal of Scientific Research in Network Security and Communication, vol. 1, no. 1, pp. 35-38.

[7] 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.

[8] Nivetha, A, Preethy, Mary, S, Santosh & Kumar, J 2015, 'Modified RSA encryption algorithm using four keys', International Journal of Engineering Research & Technology, vol. 3, no. 7, pp. 1-5.

[9] Oey, CHW & Moh, S 2013, 'A survey on temperature-aware routing protocols in wireless body sensor networks', Sensors, vol. 13, no. 8, pp. 9860-9877.

[10] Pejman, Niksaz, Mashhad & Branch 2015, 'Wireless body area networks: Attacks and countermeasures', International Journal of Scientific & Engineering Research, vol. 6, no. 9, pp. 556-568