Enhanced Security in Secret Key Generation Through the Comprehensive BB84 Quantum Cryptography Protocol.

N. HariKrishna[1] Dr. R. Siva Rama Prasad[2],

Ph.D.
1. Research Scholar, Department of CSE, Acharya Nagarjuna University
2. Professor in the Dept of CSE, Acharya Nagarjuna University

Abstract:

Secret key distribution, authentication, confidentiality, and integrity are all security concerns within the WBSN. Generation and distribution of secret keys are fundamental security functions within the WBSN. Data from body sensors is more sensitive. Treatments will be affected if those data are altered from their initial version during remote health service monitoring. It will have a widespread impact on the health of patients. The computational simplicity and reduction in power consumption for key distribution are hallmarks of the proposed method for key generation and distribution. It preserves the security of the WBSN while extending the life of the network. A potential threat to health-related sensitive data exists while medical information is being transmitted over a wireless link. Using the cryptography process, it is possible to circumvent such a circumstance. Utilizing cryptographic algorithms and confidential keys, the patient's health information can be encrypted and decrypted. The secret key is shared indirectly with the corresponding communicating parties via the proposed method. In order for the communicating parties to share the secret key, quantum mechanisms are utilized. It aids in preventing both active and passive as saults against the secret key.

Keywords: Wireless Body Sensor Networks (WBSN), Cryptography, Quantum Cryptography.

I. Introduction:

In order to ensure that information is extremely secure, quantum cryptography employs quantum mechanics. The encryption format of information encrypted with quantum cryptography will be incomprehensible to any party external to the session. In order to prevent eavesdropping during communication, quantum photon polarization states are utilized. Phenomena, mathematical computations, and various Numerical methods comprise the foundation of traditional cryptography. It is simple to break and resolve these techniques. When communicating with physicians and close relatives, brain signals, pulse rate, and temperature, among other physiologically sensitive data, are converted via a wireless link. In order to provide unbreakable cryptographic methods, therefore, more robust security mechanisms are required. By employing the quantum cryptography protocol BB84, a wireless body sensor network can fortify its security system. The importance of security concerns in wireless body sensor networks (WBSN) cannot be overstated. Wireless body sensor networks are more sensitized to security breaches than their wired counterparts. Concerning security in the WBSN are the distribution of secret keys, authentication, integrity, and confidentiality. Production and dissemination of secret keys are fundamental security functions within the WBSN. Sensitive body sensor data is present. The remedies will be impacted if the aforementioned data are altered from their initial state during remote health surveillance. A widespread impact on the health of patients will result. The method for key generation and distribution that has been proposed is computationally straightforward and reduces the amount of energy required for key distribution. It increases the longevity of a network while preserving the WBSN's security. A vulnerability to health-related sensitive data may arise during the wireless transmission of medical information. Cryptography can be utilised to circumvent such a circumstance.

Secret keys and cryptographic algorithms are required to encrypt and decrypt the patient's health information. The procedure under consideration imparts the secret key to the respective communicating entities in an indirect manner. The confidential key is exchanged between the parties involved in the communication via quantum mechanisms. Preventing both active and passive assaults on the secret key is advantageous. Quantum cryptography was introduced in Section 1. Existing quantum cryptography algorithm was discussed in section 2. The proposed work architecture, qub it generation, check bit generation, quantum key generation, bitwise operation with quantum key, and public communication discussion are detailed in Section 3.The experimental results are discussed in Section 4, which also serves as a summary of the Chapter.

II. Literature Review:

A method for enhancing key management in wireless sensor networks by utilising quantum cryptography was proposed by Vijey Thayananthan et al. (2011)[2], Shally Nagpal (2016)[1], and Saptarshi Sahoo et al. (2021)[3]. Using this technique, sensor nodes can communicate securely. By avoiding intensive computations for critical generation processes, these methods offer many benefits. The wireless sensor network's bandwidth is increased as a result of quantum cryptography. Enhancing the security of wireless sensor networks can be facilitated by this. The authors investigated key generation and encoding techniques in quantum cryptography. Information regarding the process of generating quantum keys that are absolutely secure was also provided by the authors, who also elaborated on the process's complexity.

Quantum key distribution protocol SARG04 was implemented in wireless networks by Jarrar Ahmed et al. (2014)[4]. Between communicating parties, the authors employed four-way contact communication. Here Transferring the information requires the following: sifting the raw key, error estimation, error correction, and privacy amplification. Communication overhead constitutes a drawback of this approach.

A quantum testing protocol for wireless sensor networks was put forth by HuiLiet al. (2015) [5] in the realm of high dimensions. High-dimensional quantum entanglement exchanging communication protocol (HQCP) technology is compatible with it. This method has the benefit of rapidly identifying any unauthorised access or disruption to communication caused by a third party. Increasing throughput and bolstering the system's security in the absence of intruders are both benefits of this scheme. As security and confidentiality measures, the authors may opt to insert them. For securing data in wireless body sensor networks, Tallat Jabeen et al. (2020)[6] introduced a genetic-based algorithm. In WBSN, numerous security measures are implemented, including elliptic curve cryptography (ECC), advanced encryption standards (AES), and digital signatures. Utilising a public key, ECC employs cryptography. Algebraic processes are implemented utilising the structure of elliptic curves. Notwithstanding this, the proposed scheme efficiently safeguards data. Using the patient's information, this method generated a lightweight encryption algorithm based on genetics. Anamino acid table, mutation, crossover, and string mapping are all components of the proposed encryption operation. The cipher text was generated. A combination of the genetic algorithm and the Message Queuing Telemetry Transfer (MQTT) protocol to secure data in the WBSN with reduced energy consumption. The TCP/IP protocol is utilised by the Message Queuing Telemetry Transfer (MQTT). Communication between sensors is accomplished via MQTT. In IoT applications, it is presently used to transfer data. Data transfer can typically occur in a telemetry format. The communication bandwidth for this protocol is restricted. A key generation algorithm that requires a minimal number of computations and stages is an advantage of this scheme. Unanalyzation of the numerous WBSN assaults is a deficiency of this scheme.

A new technology for retrieving private information (PIR) from the database was proposed by Wen Yu Kon et al. (2020)[12]. The PIR protocol is used to monitor databases. It facilitates the user's access to the specified database entry. The information provided by the user is concealed from the data centre. Long-shared secret keys and randomness among the communicating parties comprised the quantum cryptography. Any external eavesdropper is detectable by the proposed method. This approach possesses the merit of QKD. By implementing a star topology within a network, the keys to PIR are supplied. By means of a tangible connection, the hub links consumers with data centres. Within this structure, no assaults occur. Computational burden constitutes a deficiency in the task. To prevent security vulnerabilities in wireless sensor networks (WSNs), Shadi Nashwan (2021)introduced a novel approach. For big data environments involving wireless sensor networks, the proposed scheme provides an anonymous access authentication method. Providing a collection of security services for the big data environment, this scheme's merit is that it efficiently implements perfect forward secrecy. Additional security assaults against this scheme had not been analysed by the author[8].

III. Proposed Method:

The generation of secret keys and their subsequent distribution among communication parties are critical components in ensuring secure communications within wireless body sensor networks. WBSN handles confidential health information. Massive consequences, such as mortality, can result from minor adjustments to human body sensed data, whereas remote treatment relies on WBSN data. Misleading information influences the physician's course of treatment. Security is a critical component of the WBSN. Traditional cryptography is founded upon a mathematical foundation. An adversarycanreadilyanticipatethecalculationsth atcomprisethegenerationofthe Confidential key. Despite this, the generation of secret keys via quantum cryptography is contingent upon quantum mechanics. An adversary is incapable of deducing the value of the secret key in this location. To tackle the challenges associated with classical cryptography, secret key generation, and distribution, we propose the Enhanced BB84 quantum cryptography protocol scheme. This scheme comprises the subsequent stages, all of which contribute to the establishment of a robust foundation for secret key generation within the WBSN.

- Suggest a method for the generation and dissemination of secret keys for wireless body sensor networks that utilises the Enhanced BB84 quantum cryptography protocol (EBB84QCP).
- Generation of qubitson the sender side
- Generation of check bits on the receiver side
- Generation of a quantum key Framing the quantum secret key via bitwise operation with matched bits of communicating parties and unmatched bits on the sender side
- Discuss the quantum secret key generation process in the public communication channel.
- Evaluate the performance of EBB84QCP with respect to the ratio of key mismatches to key generation time.
-

Architecture of the Proposed Work

The process flow of the system under consideration is illustrated in Figure 1. In order to generate and distribute the secret key within wireless body sensor networks, a quantum mechanism and bitwise operator are implemented. The subsequent procedures comprise the proposed EBB84QCP method for secure key distribution in the WBSN:

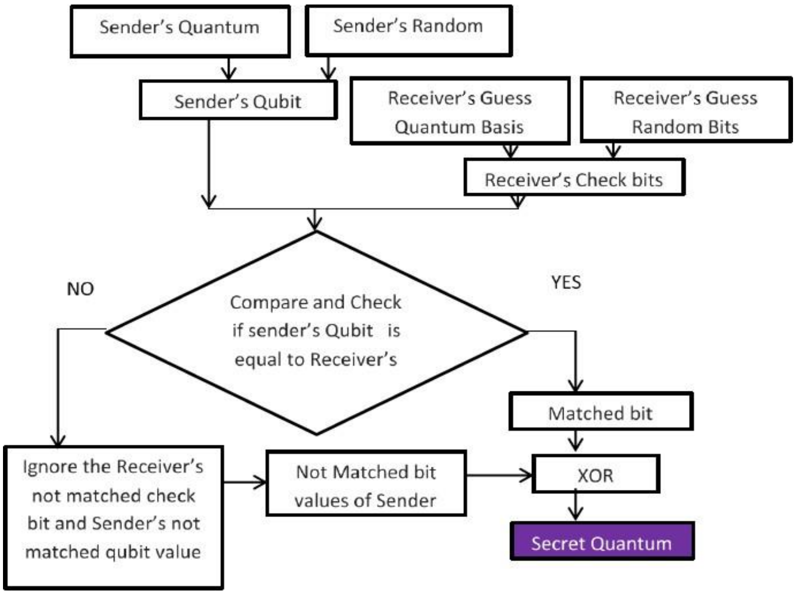

Sender's Quantum
Sender's Random
Sender's Qubit
Receiver's Guess Quantum Basis
Receiver's Guess Random Bits
Receiver's Check bits
NO
YES
Compare and Check if sender's Qubit is equal to Receiver's
Matched bit
Ignore the Receiver's not matched check bit and Sender's not matched qubit value
Not Matched bit values of Sender
XOR
Secret Quantum

Figure1: Architecture of the proposed work

1. The random number is selected by the submitter (Alice) and subsequently converted to binary format.
2. An arbitrary quantum basis can be chosen by Alice.
3. By comparing the binary and quantum basis forms of her random bits, Alice is able to derive the qubit values.
4. Bob proceeds to convert a number chosen at random into binary format. The binary representation of random numbers is subsequently compared to a quantum basis. He produces the values of the check bits.
5. Alice performs the comparison using the value of her qub it and Bob's check bits.
6. Alice identified the matched bit by comparing the qub it and the check bit.
7. Alice utilised XOR to combine the matched bits of both inputs, while utilising the unmatched bit on her side to construct the secret key.

Ultimately, Alice framed the confidential key value for communication following the XOR operation. The confidential key value serves as the foundation for both decryption and encryption. Without a direct method, that essential value is intended to be communicated to the parties involved in the exchange. Opponents are unable to forecast the value of the secret key due to the fact that it is encapsulated in a quantum mechanism and bitwise operator.

The proposed methodology comprises the subsequent modules:

1. Qubit production
2. Verify byte production
3. Generation of Quantum Keys
4. Operation in bits using a quantum key
5. Discourse in the channel of public communication

Qub it Production

The quantum mechanism is responsible for generating qub it values from the quantum basis and a random number (Chinmoy et al. 2017)[9]. The generation of qub it values occurs as follows:

Generation algorithm for qub its Quantum Basis and Random Number as Input The resultant qub it

Step1:The sender(Alice)chooses the quantum basis and the random number Step 2: Alice converts the random number to binary representation

Step 3:Alice executed the comparison operation using a quantum basis and the binary value of a random number.

The qub it value is other wise specified if the

binary value is 0 and the quantum basis value is rectilinear.
Else

The qub it value is otherwise specified if the binary value is 1, and the quantum basis value is rectilinear.
Else

Thequbitvalueisotherwisespecifiedifthebinaryvalueiszeroandthequantum basis value is diagonal.
Else

The qub it value is1ifthebinaryvalue is1, and the quantum basis value is diagonal. Step 4: Finally, the Qub it value was framed by the sender (Alice).
The generation of secret keys in traditional cryptography may involve a mathematical computation is shown in Figure 2. It can quickly penetrate both active and passive adversaries. The generation of confidential keys via quantum cryptography offers absolute security. The secret key value was beyond the comprehension and prediction of eavesdroppers operating on the wireless link.

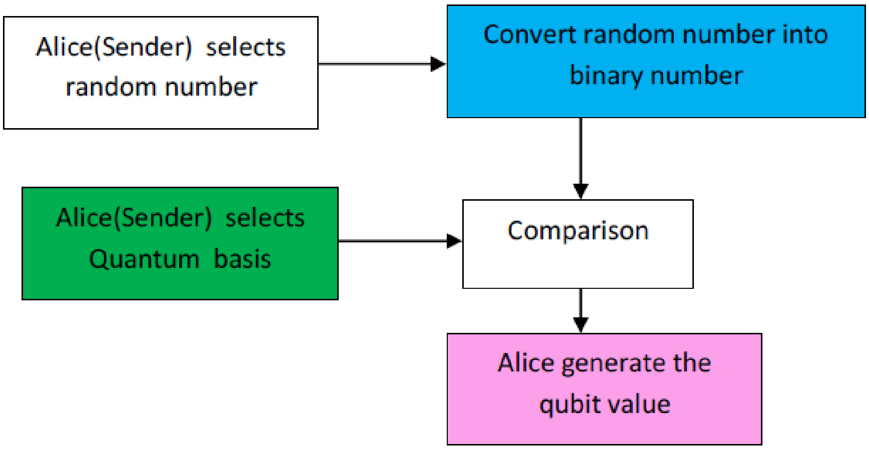

Alice(Sender) selects random number
Convert random number into binary number
Alice(Sender) selects Quantum basis
Comparison
Alice generate the qubit value

Figure 2: Qu bit generation

Bit Generation Verification

Bob, the Receiver, has the ability to select a stream of random integers and a random mixture of rectilinear and diagonal quantum basis.
Random number as input for the quantum basis Bit as an output
Step1:quantum basis and the random number are chosen by the receiver (Bob). Step 2:Bob performs a binary conversion of the random number.
Step 3:Bob conducting a comparison operation between the quantum basis and the binary value of a random number.
Otherwise, the check bit value is 1ifthequantumbasisvalueisrectilinearandthe binary value is 0.
Otherwise, thecheckbitvalueis1ifthequantumbasisvalueisrectilinear.

The alternative value for the check bit is whether the quantum basis value is diagonal and the binary value is 0.
The check bit value is1, given that the quantum basis value is diagonal. Step 4: the recipient transmits his check bit values to the sender.

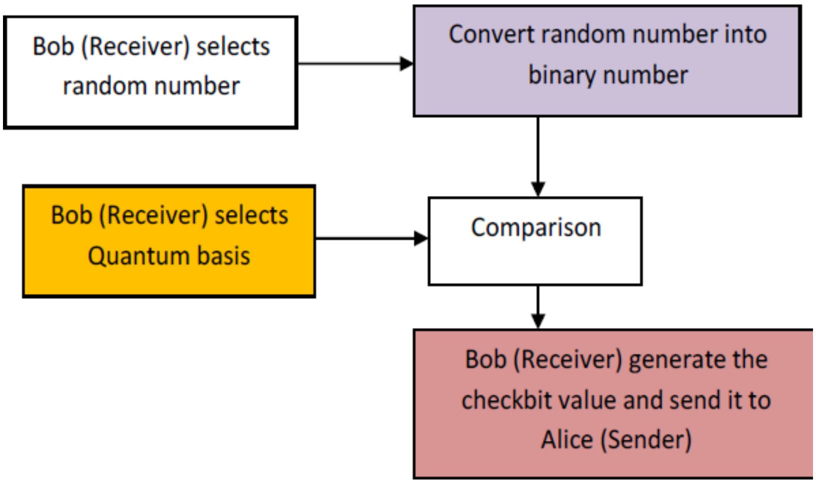

Bob (Receiver) selects random number
Convert random number into binary number
Bob (Receiver) selects Quantum basis
Comparison
Bob (Receiver) generate the checkbit value and send it to Alice (Sender)

Figure3: Check bit generation

The generation of the check bit is illustrated in Figure 3. The Receiver transmits the value of the check bit to the Sender in order to generate the quantum key value.

Quantum Generation of Keys

Alice and Bob, who are the parties communicating, possess a confidential quantum key. By utilising the enhanced BB84 quantum cryptography protocol, any potential interception of information during communication is effectively thwarted. Alice conducts a comparison between the qubit values and the check bit values after receiving the check bit from Bob. Upon comparison, Alice is able to select the quantum key-value in which both she and Bob employed the identical binary form and basis for the random number.

Bitwise Function Utilizing a Quantum Key

Alice (Sender) is presently cognizant of the quantum key value and Alice's unmatched bits from the qubit. The quantum key with the value "0011" and Alice's unmatched bits from qubit "1110" are utilized in a bitwise XOR operation (Naveen Kumar et al. 2011)[11]. Alice ultimately encodes the confidential quantum key value "1101" in preparation for subsequent encryption and decryption operations (Sandeep et al., 2018)[10].

XORProcessUsing a Quantum Key

Step1:AliceQubit (binary representation of a random number and quantum basis) Step 2 : Bob Quantum basis, binary representation of a random number; check bit

Step3:Alice examines the bit value and compare squ bit values. Step 4: If Bob's check bit and Alice's qubit matched
Otherwise, frames the quantum key value Disregard binary values
AliceexecutesabitwiseXORoperationinvolvingt hequantumkeyvalueandher unmatched bit as part of the quantum key generation procedure in step 5.
Frame the confidential quantum key for encryption and decryption in the sixth step. For the XOR operation, the quantum key-value and Alice's unmatched bits from the qubitare now taken into account. Using the XOR operation, the quantum key valueand Alice's unmatched bit are combined to generate the secret key value.

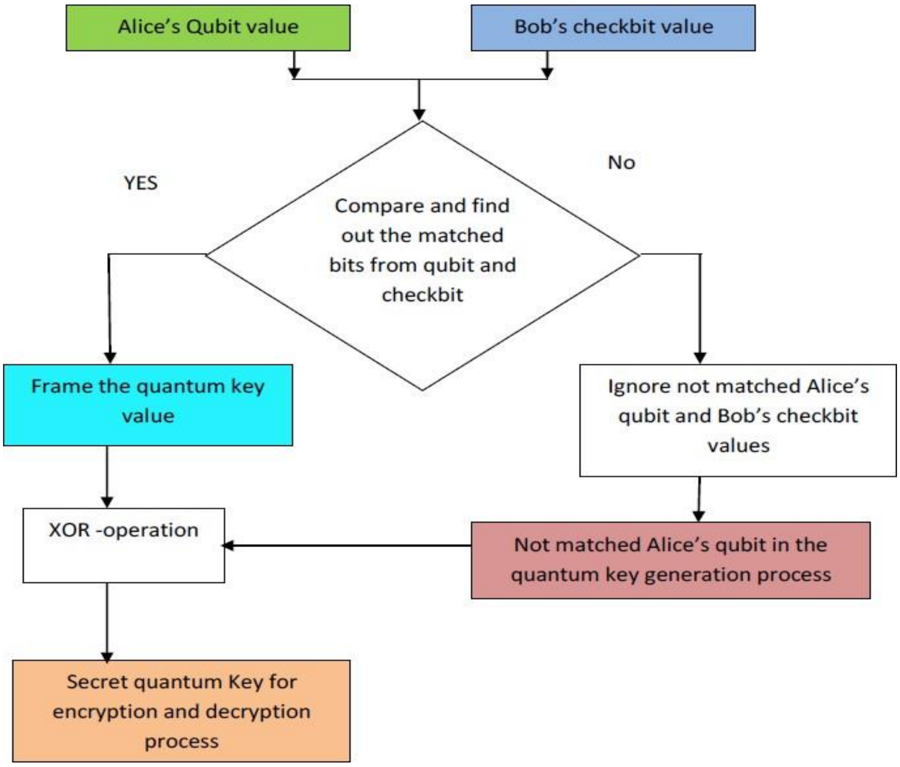

Alice's Qubit value
Bob's checkbit value
YES
No
Compare and find out the matched bits from qubit and checkbit
Frame the quantum key value
Ignore not matched Alice's qubit and Bob's checkbit values
XOR -operation
Not matched Alice's qubit in the quantum key generation process
Secret quantum Key for encryption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

Figure4: Bit wise operation frames the secret key value

As illustrated in Figure 4 , the proposed method operates bitwise. The quantum basis and corresponding binary value of the qubits of the sender and receiver wereexamined in this context. Equalquantumbasis and binary value were utilised by both the sender and receiver. For framing the quantum key value, these binary values are utilised.

Public Communication Channel Discussion

By utilising the two-way communication channel, Alice and Bob engaged in a discussionregardingtheprocessofgeneratingthe secretkeyvalue.Wireless connections facilitate the sharing ofqubit and check bitsamong the interlocutors.The sequential progression of events entails the discourse in the public channel.

1. Bobisprovided withAlice'squbit values. Utilising quantumcryptography, the data is encoded. Due to the quantum mechanism-based process and randomnature of each stage in the key generation procedure, adversaries may be unable to eavesdrop, deduce, or forecast the key value even if they are in close proximity to the communication channel.

2. Throughthecommunicationchannel,Bobtr ansmitsitscheckbitvaluesto Alice.

3. Boband Alice engaged ina conversationregarding the permissible bit for quantum key framing.

4. Subsequently, Alice requests that Bob select a specific stream of qubit values and incorporate the chosen quantumkey value into the XOR operation. At the conclusion of the cryptographic procedure, the sender and receiver exchange the confidential quantum key.

5. No confidential quantum key value is disclosed explicitly by the communicating parties in this discourse. By generating and distributing confidential keys over the wireless channel, the proposed system generates robust security.

IV. EXPERIMENTALRESULTS

The proposed methodology is executed utilising the Network Simulator-2 (NS2) and JAVA programming. The process of generating quantum keys is executed in Java. NS2 is utilised in the development of the comparative analysis against the security attack process. The quantum basis and binary values generated at random are taken into account when determining the sender's qubit.

Investigating the efficacy of the proposed method in comparison to an existing quantumcryptographymethod intermsofkeygenerationtimeRivest Cypher 5 (RC5) andRivest Cypher6(RC6)aresymmetrickeycryptographymethodsandtheScarani- Acin-Ribordy-Gisin 04 (SARG01) protocol. A series of five experiments were conducted utilising quantumbasis sizes of48, 128, 626, 910, and 1000 bits. The time required to generatekeys increasesprogressively inrelationtothequantumbasissize. Quantum basis versus time of key generation

SARG04 is among the quantum distribution protocols currently in existence. In lieuof two states, the secret key is generated using a quantum basis consisting of four states.TheSARG04methodisutilisedwhentheoriginatordesirestotransmitthe recipient the private key. n bits are chosen by the sender for the strings a and b. Following this, a qubit is encoded using quantum mechanics and constituted bythese two threads. Similarly, the receiver generates the value of the check bit using a quantum basis and transmits it to the sender. A comparison was performed between the values of the qubit and the check bit. The value of the secret key is encoded in matched bits and transmitted to both the sender and receiver.

The enhanced BB84 quantum cryptography protocol generates secrets at a faster rate than SARG04 secret key generation, as shown in Figure 5and Table 1.SARG04 is among the quantum distribution protocols currently in existence. It generates the secret key on a quantum basis consisting of four states as opposed to two. The study determined that the generation time of the proposed system's quantum secret key is shorter than that of the SARG04 key, using data from five experiments in which the quantum basis values were 48, 128, 626, 910, and 1000 bits.The key is generated by the proposed protocolutilising a quantum mechanism and bitwise operator. Asmaller number of rigorous number stages are utilised in the generation of the secret keys.The proposed scheme generates a secret key in a shorter amount of time than SARG04.

Table1: Quantum basis (bits) Vs. Key generation time (ms)

S.No	**Quantum basis size(bits)**	**SARG04–Secretkey Generation time SARG04 (ms)**	**Proposed protocol (EBB84QCP) Secretkey (ms)**
1	48	56	35
2	128	250	84
3	626	410	257
4	910	687	357
5	1000	920	780
6	2048	1107	994

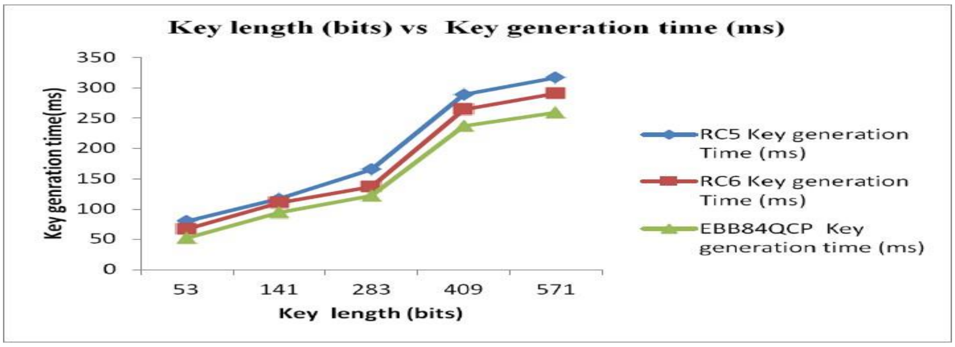


Figure5: Key length Vs. Key generation time

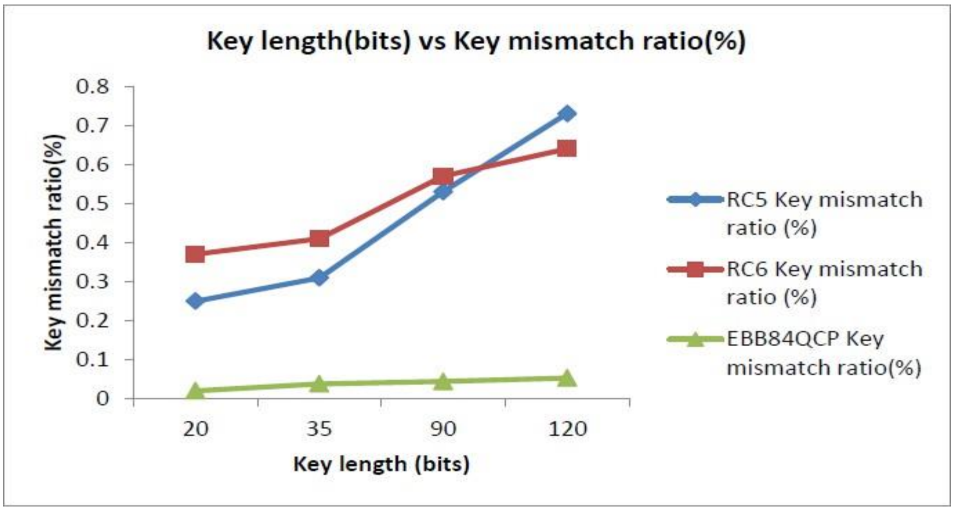
Key mismatch ratio.

The key mismatch ratio is calculated by dividing the quantity of erroneous bits (mismatch bits) present in the secret keys by the total number of bits used in the encryption and decryption procedure. Table 2 and Figure 6 illustrate the keymismatch ratio between the proposed system and RSA.Priority is given to bitwise operators and quantum mechanics in the proposed scheme. Its predictability by the assailants was impossible. In comparison to RC5 and RC6, the proposed method exhibits an exceptionally low mismatch key ratio.

Table2 Key length Vs. Key generation time

Key length bits RC5	Key generation Time(ms) RC6	Key generation Time (ms)	EBB84QCP Key generation time (ms)
53	80	67	52
141	117	110	94
283	165	137	122
409	289	264	237
571	317	291	259

Figure 6: Key length (bits) Vs. Key mismatch ratio (%)



A Comparative Examination of Security Vulnerabilities

Implantable cardiac devices, such as pacemakers, were developed by St. Jude in2016 (Source: Selena Larson 2017). It is capable of remote monitoring and control of the patient's cardiac function. Nonetheless, it grants the intruder device access. The Food and Drug Administration of the United States (FDA or USFDA) is a federal agency under the Department of Health. Human Services reports that by gaining access to a device's transmitter, hackers can exert control over it. Thus, if patients continue to use this device, it is possible for assailants to sustain and control the patients' cardiac activity. As a result, the assailants may potentially enter a critical situation regarding the health condition of the patient.

Utilising Network Simulator-2 (NS2), the efficacy of the proposed method is evaluated in the face of Man-in-the-Middle, Timing, and Replay attacks. The simulation parameters listed below are utilised. In aggregate, there are fifteen nodes. Approximately 0.0 to 0.5 percent of these nodes were malevolent. The number of nodes and this malevolent node are utilised as evaluation parameters.

Config of the sender: The source of the traffic is Constant Bit Rate (CBR),and the packet rate is five per second.

Receivers are configured as follows: An Agent Null with the default settings Upon activation, every node ceases at 0 seconds.

The dimensions of the area are 1600by1600.

There are perpetual adversaries in wireless connections. If an opportunity presents itself to obtain the secret key value, the assailants can readily obtain it and decipher the data. The secret key value is generated exclusively by the RC5 and RC6 cryptographic algorithms via the shift, XOR, shifting, and round functions. The resolution of these computer-oriented operations is a straightforward task for adversaries. However, the proposed algorithm has a solid foundation in cryptography, similar to quantum mechanics' bitwise operator. Attacks using secret keys will not occur. A type of surveillance attack is the man-in-the-middle attack (Chinmoy et al. 2017)[9]. The data transmission in the communication link is disrupted by the assailants (Al-Batool et al. 2020) [12]. Pwnirds may acquire logon credentials and personally identifiable information. They are capable of eavesdropping on the target and corrupting data. The EBB84QCP protocol prohibits man-in-the-middle attacks. Due to its reliance on a quantum mechanism for communication, this characteristic is incapable of predicting or intercepting transmitted information.

A timing assault examines the amount of time it takes for a network system to react to various inputs. If an adversary obtains knowledge of the key generation process's execution time, they can readily attempt various input combinations in an attempt to obtain the initial target information. The input and key generation procedure of the EBB84QCP are quantum polarization dependent. It is distinct from traditional key generation methods. One-way communication, qubit, check bit, and secret quantum key values are all incomprehensible to any third party involved in the exchange. Attackers are not designed to detect the proposed method's execution time.

Replay attackers have the capability to intercept the initial message and subsequently transmit it to the designated recipient, altering, adding, or removing the information. The information proposed by EBB84QCP is quantum cryptography data. Therefore, its meaning is incomprehensible to the assailants. Repetition attacks are not feasible using the proposed method.RC5, RC6, issues abound in the generation of confidential keys. The issues are the distribution of secret keys, user assumptions in the generation of secret keys, shift, swap, XOR operations, and the repeated use of the same round functions. Nevertheless, EBB84QCP is absent from these vulnerabilities in the generation of secret keys. The proposed technique is impervious to replay attacks, man-in-the-middle attacks, and timing attacks.

V. Conclusion:

The enhanced BB84 quantum cryptography protocol facilitates the generation and distributionofrobust secret keysamong the parties involved in medicalwirelessbody sensor networks. Five additionalcontributions are made to ensure the distributionand generation of keys remain secure. At the outset, qubits are produced at the endpoint. Additionally, a check bit is produced at the receiver end. The sender then framed the quantum key after performing the comparison operation between the sender's qubit and the receiver's check bit value. Alice subsequently constructs the secret quantum key byperforming an XOR bitwise operation with a quantumkeyand unmatched bits on her side. Subsequently, Alice (sender) imparts to Bob (receiver) all pertinentdetails pertaining to the formulation of the secret key through a wireless communication channel. Alice and Bob ultimately divulge the value of their confidential quantum key using the indirect approach. Even adversaries sharing communication connections are incapable of anticipating or comprehending the information. The sensitive data contained in wireless body sensors includes cerebral signals, heart rate, blood glucose level, and so forth. The secret key generated by the proposed scheme fortifies the cryptographic process governing the transmission of health informationregarding the human body. Comparing the proposed method to the SARG04, RC5, and RC6 methods. It provides superior protection against timing and man-in-the-middle attacks as well as key generation and distribution compared to SARG04, RC5, and RC6.

References:

[1] 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.

[2] Vijey Thayananthan & Ahmed Alzahrani 2011,' Analysis of Key Management and Quantum Cryptography in Wireless Sensors Networks', International Journal of Computer Application, Special Issue on Network Security and Cryptography, no. 2011, pp. 45-49.

[3] SaptarshiSahoo, PratikRoy, Amit Kumar Mandal &Indranil Basu2021,'Quantum Cryptography– A Theoretical Overview', Journal of Quantum Computing, vol. 3, no. 4, pp. 151-160.

[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] Hui, Li, Yuhan, Zhao & Yingpei, Sun 2015,' Wireless sensor network based on high-dimensional quantumcommunication',InternationalJournalofInnovativeComputing,InformationandControl,vol. 11, no. 6, pp. 2119-2133.

[6] G. Rama swamy, Dr.R.Satya Prasad, "Key Generation Using Genetic Algorthm For DNA Playfair Cryptosystem", Journal of Harbin Institute of Technology, ISSN: 0367-6234, Vol.54 Iss.9, 81-94, 2022.

[7] Tallat, Jabeen, Humaira, Ashraf, Asma, Khatoon, Shahab S, Band, Amir & Mosavi 2020, 'A lightweight genetic based algorithm for data security in wireless body area networks', IEEE Access, vol. 8, pp. 183460-183469.

[8] Zhou, Y&Wang, L2020,'Alattice-basedauthentication schemefor roamingserviceinubiquitous networks with anonymity', Security and Communication Networks, vol. 2020, pp. 1-19.

[9] Nashwan, S 2021, 'AAA-WSN: Anonymous access authentication scheme for wireless sensor networks in big data environment', Egyptian Informatics Journal, vol. 22, no. 7, pp. 15-26.

[10] 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.

[11] Sandeep, V & Niranjan, A 2018, 'Implementation of a modified BB84 algorithm for secure key exchange in a normal network', International Journal of Engineering Research & Technology, vol. 2, no. 14, pp. 48-50.

[12] G. Rama swamy, Dr.R.Satya Prasad, "Inspired Feistel DNA Based Cryptosystem Using D-Box And Image Based Key Generation ", Seybold Report, ISSN: 1533-9211, Vol.17 Iss.9, 1380-1396, 2022.

[13] 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

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

[15] Wen Yu, Kon, Charles Ci &Wen Lim 2020, 'Provably secure symmetric private information retrieval with quantum cryptography', Entropy, vol. 23, no. 1, pp. 1-27.