KSÜ Mühendislik Bilimleri Dergisi, 26(4), 2023
Araştırma Makalesi

KSU J Eng Sci, 26(4), 2023
Research Article

Kahramanmaras Sutcu Imam University
Journal of Engineering Sciences

Geliş Tarihi : 11.07.2023
Kabul Tarihi : 22.09.2023

Received Date : 11.07.2023
Accepted Date : 22.09.2023

QUANTUM KEY DISTRIBUTION IN SMART HOME SYSTEMS

AKILLI EV SİSTEMLERİNDE KUANTUM ANAHTAR DAĞITIMI

Nurcihan DERE[1] (ORCID: 0009-0009-6072-6990)
Eyup Emre ULKU[2] (ORCID: 0000-0002-1985-6461)

[1] Marmara University, Institute of Pure and Applied Sciences, Computer Engineering Department, İstanbul, Türkiye
[2] Marmara University, Faculty of Technology, Computer Engineering Department, İstanbul, Türkiye

*Sorumlu Yazar / Corresponding Author: Eyup Emre ULKU, emre.ulku@marmara.edu.tr

ABSTRACT

In recent years, with the increase in the widespread use of the internet, the usage areas and the number of users have increased rapidly. Technological advances and efforts to make life easier bring innovation and transformation in many sectors. One of these innovative approaches is the use of Internet of Things (IoT) in home systems. The concept of IoT refers to the ability of objects to communicate with each other over the internet. Smart home systems stand out as systems where different devices come together work in interaction and can be controlled remotely. While this communication and integration offers various advantages, it also brings security risks. Ensuring security in IoT systems basically includes objectives such as confidentiality, integrity, and authentication. In this study, how the key used in the encryption of data transmitted between the gateway and the cloud in smart home systems can be strengthened with the B92 Quantum Key Distribution protocol is implemented through a scenario. The effect of the Quantum Key Distribution protocol in providing privacy and its advantages against man-in-the-middle attacks are emphasized in this study.

Keywords: Quantum key distribution protocols, BB84, B92, internet of things, smart home systems

ÖZET

Son yıllarda, internetin yaygın kullanımının artmasıyla birlikte kullanım alanları ve kullanıcı sayısı hızla artış göstermektedir. Teknolojik ilerlemeler ve yaşamı kolaylaştırma amacıyla yapılan çalışmalar, birçok sektörde yenilik ve dönüşümü beraberinde getirmektedir. Bu yenilikçi yaklaşımlardan biri de ev sistemlerinde Nesnelerin İnterneti (IoT) kullanımıdır. IoT kavramı, nesnelerin internet üzerinden birbirleriyle iletişim kurabilme yeteneğini ifade eder. Akıllı ev sistemleri, farklı cihazların bir araya gelerek etkileşim içinde çalıştığı ve uzaktan kontrol edilebildiği sistemler olarak öne çıkar. Bu iletişim ve entegrasyon çeşitli avantajlar sunarken, aynı zamanda güvenlik risklerini de beraberinde getirmektedir. IoT sistemlerinde güvenlik sağlanması temelde gizlilik, bütünlük ve kimlik doğrulama gibi hedefleri içerir. Bu çalışmada, akıllı ev sistemlerinde gateway ile bulut arasında iletilen verilerin şifrelenmesinde kullanılan anahtarın B92 Kuantum Anahtar Dağıtım protokolü ile nasıl güçlendirilebileceği bir senaryo üzerinden gerçekleştirilmektedir. Kuantum Anahtar Dağıtım protokolünün gizlilik sağlamadaki etkisi ve ortadaki adam saldırılarına karşı sunduğu avantajlar bu çalışmada vurgulanmaktadır.

Anahtar Kelimeler: Kuantum anahtar dağıtım protokolleri, BB84, B92, nesnelerin interneti, akıllı ev sistemleri

ToCite: DERE, N., & ULKU, E. E., (2023). QUANTUM KEY DISTRIBUTION IN SMART HOME SYSTEMS. *Kahramanmaraş Sütçü İmam Üniversitesi Mühendislik Bilimleri Dergisi*, 26(4), 932-942.

INTRODUCTION

Internet of Things (IoT) deployments face significant security challenges due to the limited energy and computing power of IoT devices. These security issues are more serious in the age of quantum communication where attackers may have quantum computing capabilities (Al-Mohammed, Al-Ali, Yaacoub, Abualsaud, and Khattab, 2021a). Attacks that can be carried out on Internet of Things (IoT) systems can be listed as attacks on data transmitted between IoT devices and servers, attacks on software used in the IoT device, attacks that can be carried out to access this data when IoT data is stored in a cloud. Developing end-to-end secure IoT solutions involves multiple levels that combine core IoT security architecture features in 4 different layers, as shown in Figure 1. These layers are device layer, communication layer, cloud layer and lifecycle management layer (Scully). Cryptography methods are used in the IoT communication layer, as in many of systems, to ensure secure data transfer.

Figure 1. IoT Security Principles

Cryptography is all of the methods used to transform the information contained in a readable data into a form that cannot be understood by undesirable parties. The purpose of applied cryptography involves using a secret key, public key, and hash functions to ensure data confidentiality, data integrity, authentication, and non-repudiation in a secure network communication environment (Stallings & Brown, 2015).

In cryptography, symmetric or asymmetric algorithms are used to encrypt data. In symmetric encryption, the same key is used to encrypt and decrypt data. Advanced Encryption Standard (AES), Rivest Cipher 4 (RC4), and Data Encryption Standard (DES) are examples of symmetric encryption algorithms. Two different keys, public and private, are used in asymmetric encryption. Diffie–Hellman (DH) and Rivest-Shamir-Adleman (RSA) are asymmetric encryption algorithms. In these methods, which are used to ensure data confidentiality, passwords can be decrypted in a short time by quantum computers. Therefore, more secure quantum methods have been developed. While the purpose of QKD and classical key distribution are consistent, the implementation methods are different. Classical key distribution is based on the mathematical theory of computational complexity, while quantum key distribution is based on the fundamental principle of quantum mechanics (Qiao & Chen, 2009).

In today's encryption algorithms, a wide variety of mathematical techniques are used to prevent third parties listening to the line from obtaining the contents of the encrypted message, while in quantum cryptography, data is protected by the laws of physics (Toyran, 2003). In the quantum cryptography technique, Quantum Key Distribution method is used in order to transmit the key used to encrypt the message and decrypt the encrypted message reliably between the receiver and the transmitter. Quantum Key Distribution is an efficient method for sharing secure keys among a pair of remote users (Gopinath & Shyry, 2022b).

In smart home systems, the cloud layer is the layer where data from IoT devices is stored and the data is analyzed to take appropriate actions. Sensitive data stored in this layer is encrypted to protect against attackers. Confidentiality, which is important for security in smart home systems, is provided by encryption methods during data storage. Security at the communication layer is another security goal that needs to be met. Different security architectures are applied in the connection between IoT devices and the cloud. The message is transmitted in encrypted form by encryption with the public key used. This key needs to be securely created between the device and the cloud. It must be protected against man-in-the-middle attacks that can be carried out to obtain the password.

Classical encryption methods will not be able to provide full security against an attacker with quantum computing capability. More advanced quantum encryption methods should be used against such attacks. In this study, it is explained that the encryption key between IoT devices in smart home systems, and the cloud is created by quantum key distribution. Its advantages against attacks are evaluated.

Within the scope of the study, studies on quantum key distribution and quantum key distribution protocols, studies to increase security in quantum key distribution, and security studies in IoT devices were examined.

In the study of H A Al-Mohammed et al., it is explained that when attackers have the ability to perform quantum transactions, IoT devices will be insufficient to prevent significant security attacks due to their limited energy and processing capabilities. It is concluded that in IoT, Neural Network (NN) based approach to detect an attacker at the stage of quantum key distribution can achieve 99% success in detecting attackers (Al-Mohammed, Al-Ali, Yaacoub, Abualsaud, et al., 2021b).

According to the study of J Wang et al., long-term quantum resistant security of the final key can be achieved by eliminating potentially leaked key information with post-transaction-based quantum cryptography for quantum key distribution data (Wang, Zhou, Yin, and Chen, 2022).

In the study of T A Pham and N T Dang, quantum switches are created using radio-over-fiber (RoF) systems over fiber and sent from a key distribution server to IoT gateways. This system is a useful approach to deploy quantum key in 5G based IoT (Internet of Things) networks with low quantum bit error rate and high secret key rate (Pham & Dang, 2022).

According to the study of S Kuppam, B92 is more robust to an eavesdropper, with the ability to take fewer qubits than BB84 to detect an eavesdropper, potentially reducing the number of accurate measurements the eavesdropper can make (Kuppam, 2016).

In the study of E Gümüş, in the BB84 protocol, the probability of a photon being considered valid is 50%, depending on the receiver and the sender not using the same type of filter, while in the B92 protocol, this rate drops to 33%. This means that the transmission with the B92 protocol should take longer than the BB84 protocol in order to generate keys of equal length when the two protocols are compared. While the B92 protocol has a disadvantage in this respect, it gains an advantage in terms of security by providing a higher eavesdropping detection rate in "man in the middle" type attacks. Accordingly, it is understood that 40% of the bits accepted as valid in the BB84 protocol are listened to, while this rate increases to 50% in the B92 protocol (Gümüş, 2011).

In the study of X Xie and G -L Chen, encryption of the key using the Unique Code System (UQS) is examined to prevent the key from being decrypted by malicious attacks in the Quantum Key Distribution (QKD) protocol. According to this study, the Unique Code System has greatly increased security in critical systems (Xie & Chen, 2022).

According to the study of X Meng, Existing IoT systems use a relatively easy method of data encryption to secure data transmission, often referred to as lightweight cryptography. This method is at risk of being broken by quantum computers. Therefore, the IoT architecture needs to be redesigned considering the security challenges posed by quantum computers (Meng, Yu, Chen, Zhao, and Zhang, 2020).

In the study of S Sasikumar et al., the security of the QKDP simulation model, which uses a quantum system in cloud security, is used. This simulation model used a non-Abelian group-based encryption-decryption model to increase data security. The resulting keys are distributed via the quantum channel. In this simulation, the QKD protocol, No Cloning, and Heisenberg Uncertainty principles are applied, which ensures security. Secure communication in key distribution is increased with this model (Sasikumar et al., 2022).

In the study of T M Fernández-Caramés, in IoT specifically, there are five main types of IoT communications that need to be secured. These are communication between IoT nodes, communication between an IoT node and an IoT gateway, and communication between IoT gateways or edge computing devices. Communication between an IoT gateway and the cloud is ranked as communication between an IoT node and the cloud (Fernández-Caramés, 2019).

The following sections of the article are formed as follows. Quantum cryptography and Quantum Key Distribution protocols are explained. In the materials and methods section, the smart home system and quantum key distribution protocol designed in this study are explained. It is explained with a flow chart. In the result and discussion section, quantum key distribution protocols and smart home systems are evaluated in areas such as security and speed. use protocols. In the conclusion part, the method is evaluated, and the article is concluded.

QUANTUM CRYPTOGRAPHY (QUANTUM KEY DISTRIBUTION)

In quantum cryptography, quantum mechanics principles are used to securely transmit the key used to encrypt messages between the sending party and the receiving party. Quantum Key Distribution requires the existence of two communication networks between the receiver and transmitter. The first network is a quantum channel connected to the transmission of quantum random bit signals between the receiver and transmitter, the second network is a conventional channel (Al-Mohammed, Al-Ali, Yaacoub, Qidwai, et al., 2021b). These channels are shown in Figure 2. In the quantum channel, a known secure key is created between the receiver and the transmitter. The key is generated as a random bit sequence and is disposable (one time pad).

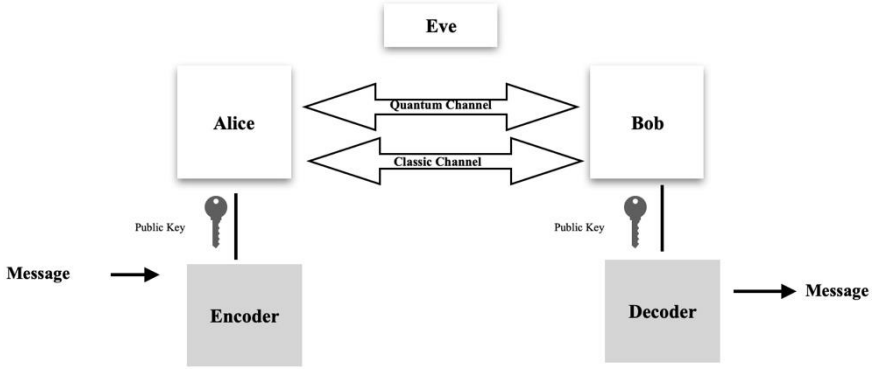


Figure 2. Quantum Key Distribution

Messages encrypted with this key are transmitted to the receiver over the classical channel. In quantum cryptography, a secure communication system can be established by using certain laws of quantum mechanics such as the Heisenberg uncertainty principle and photon polarization (Toyran, 2003). According to the Heisenberg uncertainty principle, in quantum physics, two properties (position and momentum) of an object cannot be measured at the same time (Hong, Foong, & Low, 2016), and the first measurement made for one of these properties sequentially makes the result of the second measurement uncertain.

Heisenberg's uncertainty principle is shown in Equation 1. This equation focuses on the momentum (p) and positions (x) of a quantum object. Δ represents the uncertainty and h is Planck's constant (Malik, 2021).

$$\Delta p \times \Delta x \geq h / 4\pi \quad (1)$$

In this communication, a third person trying to capture the key leaves traces on the network that will detect its presence. This is related to the Heisenberg uncertainty principle. According to the uncertainty principle introduced by Werner Heisenberg in 1927, both the position and momentum of a particle such as a photon or electron cannot be measured with perfect accuracy. More detailed experiments are required to obtain precise position information, and as these experiments are carried out, information about the momentum of the particle is gradually lost. These changes in the photon are detected in the quantum key distribution and the modified photons are cancelled. The key is created only with photons whose security is assured. Thus, quantum key distribution guarantees the confidentiality and security of the key (Gopinath & Shyry, 2022a).

Quantum Key Distribution is shown in Figure 2. In the system, the secure key is created via a quantum channel between the person who encrypts a message and sends it to the receiver (usually Alice) and the receiver (usually called Bob). The key consists of a randomly selected string of bits of sufficient length. After the secure key is created

in the quantum channel, Alice encrypts the messages using this key, and the messages are transmitted over the classical channel. Bob decrypts the encrypted message with the specified public key.

The third person (often called Eve) trying to eavesdrop on this communication tries to eavesdrop on the quantum line to get hold of the key. It measures transmitted bits while listening and causes errors. Alice and Bob can detect eavesdropping by checking the error bits. Also, even if Eve successfully eavesdropped while confirming Bob's received protons with Alice, this information would be of no use to Eve until she knew the correct polarization of each photon.

However, with today's technology, it is not possible to transmit error-free data (the "key" for quantum cryptography) over optical lines. For this reason, various key distribution protocols have been proposed for the accuracy and correction of the key transmitted over the line (Gümüş, 2011). Among these protocols, Bennett & Brassard 1984 (BB84) and Bennett 1992 (B92) protocols are mentioned in this section.

Bennett&Brassard 1984 (BB84)

The first key distribution protocol, BB84, was created by Charles Henry Bennett of IBM Research and Gilles Brassard of the University of Montreal (Zisu, 2019). For this reason, it is the most compared protocol with other protocols proposed after it in the literature (Gümüş, 2011). To create a disposable key in the BB84, the sender (Alice) and the receiver (Bob) have two crystal bases, linear (rectilinear) and diagonal, both of which make 45° angles to each other. Photon polarization states and bases are shown in Figure 3.

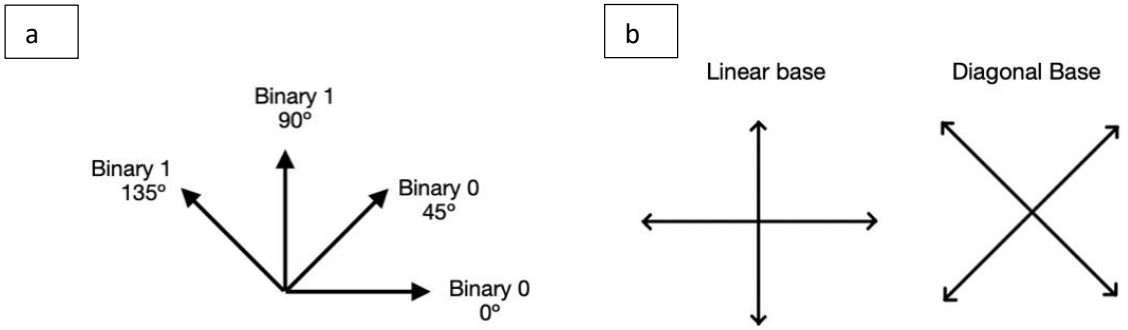


Figure 3.a. Photon Polarization States **b.** Photon Bases

In the BB84 protocol, Alice and Bob communicate over the quantum channel in the first step. Alice generates a random bit sequence to generate the encryption key. Alice transmits a qubit (quantum bit) prepared on a linear or diagonal basis to Bob via a fiber optic channel, using the bits in this sequence, respectively. Alice does not share the information on which basis the qubit was prepared with the receiver (Bob). Bob chooses one of the bases (linear or diagonal) and measures, recording the base he chose and the bit he got. If the base chosen is the same as the base Alice chose, the result will be congruent and Bob will guess the bit correctly. In the second step, Alice and Bob contact again over the classical channel. Bob shares the base type he uses for each qubit with Alice. Alice then tells which of the bases Bob has chosen are correct. Accordingly, the bits where the bases are selected differently are cancelled. As a result, the bit string remaining in Alice and Bob's hands will be the same. Table 1 shows the 8-bit communication process between Alice and Bob in the BB84 protocol.

Table 1. BB84 Communication Process (Yang, Jiao, Shi, and Liu, 2019)

Bits	**1.**	**2.**	**3.**	**4.**	**5.**	**6.**	**7.**	**8.**
Alice's Random Bits	0	1	1	0	1	0	0	1
Alice's Random Bases	+	+	x	+	x	x	x	+
Photons Alice Sends	↑	→	↘	↑	↘	↗	↗	→
Random Receiving Bases	+	x	x	x	+	x	+	+
Photons Bob Receives	↑	↗	↘	↗	→	↗	→	→
Public Discussion								
Key	0		1			0		1

Bennett 1992 (B92)

In 1992, Bennett proposed a protocol based on two nonorthogonal states for QKD. This protocol is called the B92 protocol. In the B92 quantum key distribution protocol, the Sender will encode the classical bits in two nonorthogonal states (Elboukhari, Azizi, & Azizi). Alice sends with 0º for bit 0 and 45º for bit 1. Figure 4 shows the polarization states in B92. Bob sent the sole that Alice had chosen. It applies it to the photon it is in, and if one of the states that Alice can choose (0º and 45º) comes as a result, it considers the bit invalid. It is considered valid if it achieves a degree perpendicular to the situations Alice chose. Figure 5 shows Bob's measurement and interpretation states.

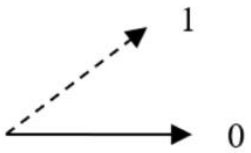
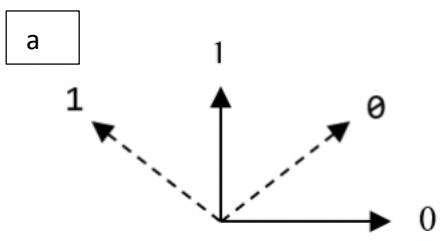


Figure 4. Sender's Nonorthogonal Polarization States (Anghel, Istrate, and Vlase, 2022)



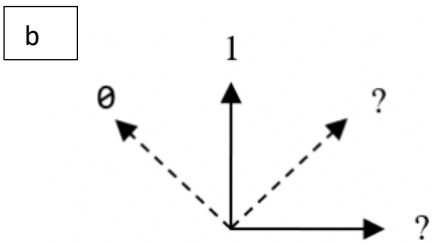


Figure 5.a. Receiver's Measurement **b.** Interpretation States (Anghel, Istrate, and Vlase, 2022)

The BB84 and B92 protocols are both based on the quantum uncertainty principle. Photons with four different polarization angles are used in the BB84 protocol. After the transmission of the photons is achieved, the base alignment with the classical channel takes place. In the B92 protocol, Alice sends photons with two different type of polarization angles. After all photons have been sent, there is no base check between Alice and Bob. Bob tells Alice which qubit will remain as the key shared between them (Yang, Jiao, Shi, and Liu, 2019).

MATERIAL AND METHODS

In the designed structure, devices in smart home systems transfer data to the cloud via a wide area network (WAN) and gateway. Figure 6 shows the related smart home system structure. Gateway in this structure acts as a gate for data transmission. Data to be transferred from smart devices to the cloud is encrypted with a key to ensure confidentiality. In this model, the secure key to be used for encryption is shared between the sender and the receiver using the quantum key distribution method.

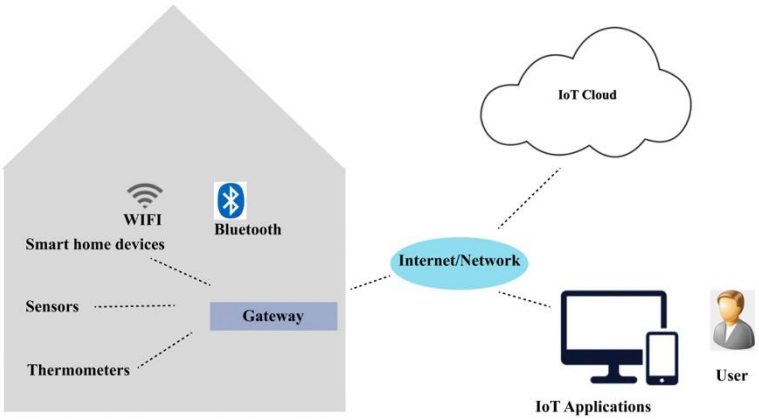


Figure 6. Smart Home System

Devices in smart home systems transmit data to the cloud through the wide area network (WAN) and gateway. The workflow of the proposed model is shown in Figure 7. The gateway in this structure functions as a gate for data transmission. Data transferred from smart devices to the gateway is encrypted with an encryption algorithm to ensure confidentiality while being transmitted from the gateway to the cloud. In this model, the secure key to be used for encryption is shared between the gateway and the cloud using the quantum key distribution method. With this shared key, data is encrypted and decrypted using conventional encryption methods. This structure was created to increase the security of smart home systems and to protect against possible security threats during data transmission.

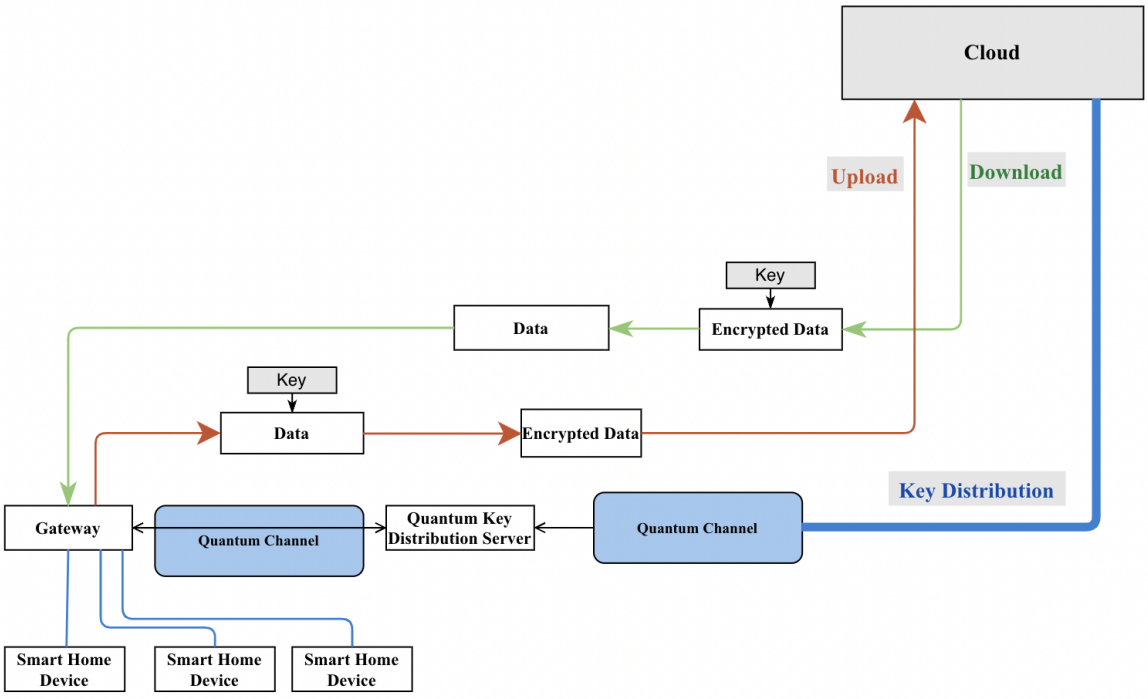


Figure 7. Workflow of the Proposed Model

The quantum key distribution scenario between the gateway and the cloud for the encryption key is as follows. To create a primary key, the communication is made with a quantum channel between the gateway and the cloud with the B92 protocol. In the first stage, the gateway randomly determines 16 bits, consisting of 0 and 1, to create a primary key. It sends these bits one by one to the gateway over the quantum channel. In this scenario, it is assumed that there is an eavesdropper listening on the communication line to obtain the primary key information. This dialog is shown in Table 2. In the table, the sending party, that is, the gateway, is named as Alice, and the receiving party as the cloud is named Bob. An eavesdropper trying to eavesdrop on the line and get the key is named Eve. Alice sends photons with linear polarization for 0º, photons with diagonal polarization for 45º. Eve captures and measures the photons, then sends the photons to Bob, maintaining the same polarization states. The presence of Eve can be detected if the measurement of Eve affects the polarization of the photons. Bob measures the transmitted photons and reports the measurement result to Alice. These bits are considered invalid if Bob gets 0º and 45º in the measurement result. It is considered valid when it finds 90º and -45º. Bob reports the measurement results back to Alice. Alice and Bob evaluate whether the communication is secure by looking at the measurement results they share among themselves. When the error and mismatch exceed the specified equal value, the entire key sequence can also be generated from scratch. (Wang et al., 2022). When the presence of an eavesdropper listening to the bit transmission is detected when the threshold value is not exceeded, that bit is canceled and the secure bits are kept. This communication is completed when 16 secure bits are obtained and the key is generated.

As seen in Table 2, the 3rd, 5th, 7th, 11th, 12th, 13th and 16th bits are considered valid in 16-bit transmission. The valid bitrate is 50%. The presence of eavesdropper (Eve) was detected in 3 out of 8 valid bits. Eavesdropper detection was also found to be 37.5% in this scenario.

RESULTS AND DISCUSSION

According to the model proposed in this article, 50% of the invalid bits are accepted for 16 bits in the B92 protocol. The presence of a potential eavesdropper trying to eavesdrop on the key distribution line was detected at 37.5% of the bits considered valid. Bits detected by the quantum key distribution protocol are considered invalid. This communication with the quantum channel continues until valid bits for the encryption key are obtained. In current applications, data transmission between the gateway and the cloud is done using classical encryption methods to ensure security in smart home systems. However, in the case of a quantum-capable attacker, these encryption methods will be easily decrypted. With the quantum key distribution methods in this study, key distribution will be performed more securely between the gateway and the cloud. With the quantum key distribution approach, smart home systems will be protected more securely against man-in-the-middle threats. In addition, once secure key sharing is achieved, it will be possible to securely encrypt and transmit data by combining keys with traditional encryption algorithms (asymmetric or symmetric). With this approach, it is aimed to create a stronger security layer by combining quantum cryptography with traditional cryptography.

When evaluated in terms of the quantum protocols to be used in key distribution, a public key can be generated faster than the B92 protocol due to the high number of valid bits in the BB84 protocol. The B92 protocol, on the other hand, is more successful in detecting an eavesdropper listening to the line. Therefore, it would be more appropriate to prefer the B92 protocol in smart home systems where security is more important and speed is relatively tolerable. On the other hand, in systems where speed is much more important and extra precautions are taken for security, the BB84 protocol can be evaluated.

Recent advances in the quantum field, like the research presented in this article, open up new possibilities for security methods in smart home systems. However, quantum technologies are still an emerging field and require complex infrastructure and hardware requirements for their use. Quantum technologies are an area that is not used on a large scale yet and has complex production and operating costs. Therefore, integrating quantum technologies into smart home systems can result in high costs. However, ongoing research and development shows that quantum technologies may find wider use in smart home systems in the future.

CONCLUSION

In this article, Quantum Key Distribution method scenario that can be used to increase the security at the communication layer in smart home systems is realized. Today, in the communication between the gateway and the cloud in smart home systems, the data is transmitted by being encrypted with classical encryption methods such as RSA, AES, DES. Among these methods, for example, in RSA, it is necessary to operate with large numbers to

increase security. However, in the age of quantum computers, these algorithms, however complex, can be solved by quantum computers in a short time. Therefore, there is a need to use quantum cryptography techniques to ensure security in IoT systems.

In this study, a quantum key distribution scenario is implemented using the B92 protocol, which uses the encryption key between the gateway and the cloud in smart home systems. In the scenario where 16 bits are transmitted, in case of an eavesdropper listening to the communication line, it was detected at a rate of 37.5% and the bits listened to according to the B92 protocol were deemed invalid. Even if the eavesdropper got a few bits by listening, they won't be able to get the whole key. Accordingly, the use of QKD compared to classical encryption methods will provide an advantage in detecting the attacker in man-in-the-middle attacks. However, practically using and integrating quantum technologies in smart home systems requires considering multiple technical, cost and security factors. Integrating quantum technologies into smart home systems requires further research and development. Studies should be carried out both for the development of quantum technologies itself and for adapting these technologies to smart home systems.

Table 2. 16 Bit Transmission With B92 Protocol

Bit Order	Alice's Bit	Alice's Photons	Eve's Selected Base	Eve's Photons Sent to Bob	Bob's Selected Base	Bob's Detected Photon	Compare Result	Bit Found by Bob	Does Eve Exist?
1	0	→	⊕	→	⊕	→	**Invalid**		
2	1	↗	⊗	↗	⊗	↗	**Invalid**		
3	1	↗	⊕	↑	⊕	↑	✓	1	**No**
4	0	→	⊗	↗	⊗	↗	**Invalid**		
5	1	↗	⊕	↑	⊗	↖	✓	0	**Yes**
6	0	→	⊗	↗	⊕	→	**Invalid**		
7	0	→	⊗	↖	⊕	↑	✓	1	**Yes**
8	1	↗	⊗	↗	⊕	↑	✓	1	**No**
9	0	→	⊕	→	⊕	→	**Invalid**		
10	1	↗	⊗	↗	⊗	↗	**Invalid**		
11	1	↗	⊕	↑	⊕	↑	✓	1	**No**
12	0	→	⊗	↖	⊗	↖	✓	0	**No**
13	0	→	⊗	↖	⊕	↑	✓	1	**Yes**
14	1	↗	⊕	↑	⊗	↗	**Invalid**		
15	1	↗	⊗	↗	⊕	→	**Invalid**		
16	0	→	⊕	→	⊗	↖	✓	0	**No**

REFERENCES

Al-Mohammed, H. A., Al-Ali, A., Yaacoub, E., Abualsaud, K., & Khattab, T. (2021a). Detecting Attackers during Quantum Key Distribution in IoT Networks using Neural Networks. Paper presented at the 2021 IEEE Globecom Workshops (GC Wkshps).

Al-Mohammed, H. A., Al-Ali, A., Yaacoub, E., Qidwai, U., Abualsaud, K., Rzewuski, S., & Flizikowski, A. (2021b). Machine learning techniques for detecting attackers during quantum key distribution in IoT networks with application to railway scenarios. IEEE Access, 9, 136994-137004.

Anghel, C., Istrate, A., & Vlase, M. (2022). A Comparison of Several Implementations of B92 Quantum Key Distribution Protocol. Paper presented at the 2022 26th International Conference on System Theory, Control and Computing (ICSTCC).

Elboukhari, M., Azizi, M., & Azizi, A. Achieving unconditional security by quantum cryptography. Intelligent Communication System, AL-Dahoud Ali, Walid A. Salameh, Linda Smail (Eds), 36-61.

Fernández-Caramés, T. M. (2019). From pre-quantum to post-quantum IoT security: A survey on quantum-resistant cryptosystems for the Internet of Things. IEEE Internet of Things Journal, 7(7), 6457-6480.

Gopinath, N., & Shyry, S. P. (2022a). Enhancing the cloud security using side channel attack free QKD with entangled fuzzy logic. Journal of Intelligent & Fuzzy Systems(Preprint), 1-11.

Gopinath, N., & Shyry, S. P. (2022b). Secured: quantum key distribution (SQKD) for solving side-channel attack to enhance security, based on shifting and binary conversion for securing data (SBSD) frameworks. Soft Computing, 1-8.

Gümüş, E. (2011). Kuantum kriptografi ve anahtar aağıtım protokolleri. Akademik Bilişim.

Hong, K. W., Foong, O.-M., & Low, T. J. (2016). Challenges in quantum key distribution: A review. Paper presented at the Proceedings of the 4th International Conference on Information and Network Security.

Kuppam, S. (2016). Modelling and Analysis of Quantum Key Distribution Protocols, BB84 and B92, in Communicating Quantum Processes (CQP) language and Analysing in PRISM. arXiv preprint arXiv:1612.03706.

Malik, P. (2021). A Light-based Interpretation of Schrodinger's Wave Equation and Heisenberg's Uncertainty Principle with Implications on Quantum Computation. Paper presented at the 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS).

Meng, X., Yu, X., Chen, W., Zhao, Y., & Zhang, J. (2020). Residual-adaptive key provisioning in quantum-key-distribution enhanced internet of things (q-iot). Paper presented at the 2020 International Wireless Communications and Mobile Computing (IWCMC).

Pham, T. A., & Dang, N. T. (2022). Quantum Key Distribution: A Security Solution for 5G-based IoT Networks. Paper presented at the 2022 International Conference on Advanced Technologies for Communications (ATC).

Qiao, H., & Chen, X.-y. (2009). Simulation of BB84 Quantum Key Distribution in depolarizing channel. Paper presented at the Proceedings of 14th Youth Conference on Communication.

Sasikumar, S., Sundar, K., Jayakumar, C., Obaidat, M. S., Stephan, T., & Hsiao, K.-F. (2022). Modeling and simulation of a novel secure quantum key distribution (SQKD) for ensuring data security in cloud environment. Simulation Modelling Practice and Theory, 121, 102651.

Scully, P. Understanding IoT Security – Part 1 of 3: IoT Security Architecture on the Device and Communication Layers. Retrieved from https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/ Accessed 20.06.23.

Stallings, W., & Brown, L. (2015). Computer security principles and practice (3 ed.). United States of America: Pearson, (Chapter 2).

Toyran, M. (2003). Kuantum Kriptografi. (Yüksek Lisans Yüksek Lisans). İstanbul Teknik Üniversitesi, İstanbul.

Wang, L.-J., Zhou, Y.-Y., Yin, J.-M., & Chen, Q. (2022). Authentication of quantum key distribution with post-quantum cryptography and replay attacks. arXiv preprint arXiv:2206.01164.

Xie, X., & Chen, G.-L. (2022). Feasibility Analysis of Quantum Key Distribution Technology in Unique Code Application. Paper presented at the 2022 7th International Conference on Intelligent Computing and Signal Processing (ICSP).

Yang, X., Jiao, J., Shi, Y., & Liu, Y. (2019). Modeling and Security Analysis Method of Quantum Key Distribution Protocol Based on Colored Petri Nets. Paper presented at the 2019 IEEE 19th International Conference on Communication Technology (ICCT).

Zisu, L. (2019). A Method to Improve the BB84 Protocol. Scientific Bulletin'Mircea cel Batran'Naval Academy, 22(1).