Quantum-Elliptic curve Cryptography for Multihop Communication in 5G Networks

A.S. Khan, J. Abdullah, N. Khan, AA Julahi, S Tarmizi

Network Security Research Group, Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak

ABSTRACT

The Internet of Things (IoT) depicts a giant network where every "thing" can be interconnected through the communication network. The communication can be initiated between people-people, people-things, and things-things. Meanwhile, the fifth generation (5G) mobile communicating systems are the mainspring to power the IoT concept in the upcoming future. However, the heterogeneous environment in 5G networks as well as the high dependency on radio spectrum have raised deep concerns about the security assurance against network attacks such as eavesdropping. In this paper, we propose an end-to-end security mechanism to ensure the multi-hop relay communications in 5G based IoT networks to stay secured. We design a scenario to explain the insecure multi-hop relay communications which involves Base Station (BS), Subscriber Station (SS) and Relay Station (RS). Next, we utilize Quantum Cryptography between BS to RS and RS to RS as well as adopting Elliptic Curve Cryptography between BS to SS or RS to SS to mitigate the network against typical replay attacks. By using the concept of integrating both cryptographic methods, the secret key that yield from Quantum Cryptography will be used in Elliptic Curve Cryptography to secure the transmission of information across IoT networks. Thereupon, extensive discussion has been carried out and it shows that the suggested mechanism has potential to ensure confidentiality, integrity, availability and non-repudiation in the proposed scenario. In the final part of this paper, we conclude our study by a comparison analysis between the two proposed cryptographic solutions. The comparison analysis illustrates the performance of each proposed strategy in terms of the achievable level of secrecy in IoT networks.

INDEX TERMS

Internet of Things (IoT), fifth generation (5G) network, cryptography, Quantum cryptography, Elliptic Curve cryptography.

1. Introduction

As the technology is continuously evolving, the definition for the Internet of Things (IoT) keeps expanding. Originally, IoT focuses on the connectivity as well as the sensory necessities for entities to be involved in ordinary IoT environments [1]. Along with the evolution of technology, the concept of IoT in current modern world provides more value to the demand for ubiquitous networks and secured information exchange among a variety of smart objects [2]. IoT illustrates that physical and virtual objects are accessible without time and place limitations. Among all existing and evolving communication technologies, the techniques for the fifth generation (5G) mobile communicating systems will be essential to accomplish the concept of IoT. However, the 5G system which is much better and faster than current 4G system will not be rolled out until year 2020 [3]. Although 5G system is yet to be launched, it is believed that 5G networks can achieve higher data rates, lower end-to-end latency, lower energy consumption, lower cost per information transfer, ubiquitous, uninterrupted and consistent connectivity [4]. Moreover, 5G system is much easier to manage as compared to previous generations and this indicates 5G system is more effective and efficient [5][6-12].

In the near future, the advancement in IoT and 5G technologies will bring a lot of significant changes to the public. IoT, the global infrastructure for the information society will enable a variety of objects to be recognizable and integrated into the communication networks. With such advanced objects being integrated into different industries, the quality of human's daily lives as well as the world's economy are believed will be boosted to a higher level. Soon, the communication services will be highly pervasive and distributed which in turn create a decentralized pool of resources interconnected through a dynamic network. Other than that, 5G technologies are also one of the hot issues being discussed due to its capability to create a seamless connection for massive things at a faster speed. 5G technology is able to power a huge number of connected devices that will reach out to different locations via a wireless communicating network. In short, it is a leading-edge technology which collects all networks into one platform in order to offer ubiquitous connectivity across the world.

Although the actualization of IoT is beneficial to numerous fields such as industry, education, healthcare, transportation and market, it brings up many issues related to security. When up to billions of smart devices are connected, it is difficult to assure the information being transmitted stays secured. Furthermore, 5G system is considered as heterogeneous network [13] and its properties of relying on radio propagation for broadcast

Manuscript received May 5, 2017
Manuscript revised May 20, 2017

purpose make it more vulnerable to eavesdropping attack. In order to prevent the messages in a private conversation being exposed to eavesdroppers, an end-to-end security mechanism will be applied to ensure the communications in 5G based IoT networks stay secured. In this paper, we will study two cryptographic strategies which are Elliptic Curve Cryptography and Quantum Cryptography. We will further look into their complex protocols and architectures in order to fully understand how both methods can guarantee secrecy of the communications in IoT networks.

In the first cryptographic method, Quantum Cryptography, it does not involve any data encryption nor decryption. It only transmits a common secret key between two parties through the polarization of lights [14]. For the latter cryptographic method, which is Elliptic Curve Cryptography, it uses Elliptic Curve Integrated Encryption Scheme (ECIES) for data encryption and decryption. Although both methods provide security to the multi-hop relay communications, they are still vulnerable to Man in the Middle (MITM) attack. In Quantum Cryptography, eavesdropper can disguise as a fake RS to receive private message from BS secretly. For Elliptic Curve Cryptography, eavesdropper can substitute his/her own keys for sender's and receiver's public keys during the initial exchange of key pairs. In order to counterattack MITM attack, we will integrate both methods to become an end-to-end security mechanism that can secure the multi-hop relay communications in 5G based IoT networks.

Apart from the discussion of cryptographic methods, we will as well take multiple relay networks into consideration to determine how the integration of both cryptographic methods can provide more secure transmission of information. A relay is employed in between the source and the destination to retransmit the private message. In this paper, we will consider two types of communications in terms of direct and indirect. For direct communication, BS will transmit directly to SS. Furthermore, indirect communication refers to at least two RSs being employed in between the BS and the SS. Then, we will identify how the integration of both cryptographic methods can achieve better secrecy in the multi-hop relay communications.

Subsequently, it will be Section II which describes the 5G system model and formulates the optimization problem. Whereas Section III and Section IV discuss about Quantum Cryptography and Elliptic Curve Cryptography respectively. For each technique, we will further discuss how they can overcome the network attacks and how they can ensure the confidentiality, integrity, availability and non-repudiation of information. Section V presents the comparison analysis between the two proposed cryptographic methods to evaluate secrecy performance of both methods in the relay transmission. Finally, this paper concludes in Section VI.

2. System model

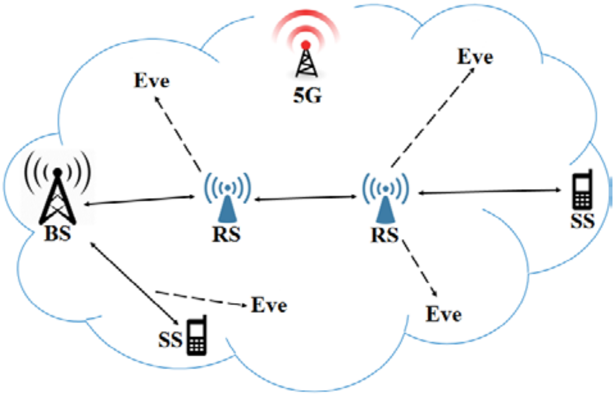

Fig 1 The scenario of insecure multi-hop relay communications 5G based IoT networks

The whole 5G network can share the wireless network to any or all stations. We have BS, RS and SS. As shown in Figure 1, we have two types of communications in the scenario which are direct and indirect. For indirect communication, RS will send an authentication request to BS, which includes the digital certificate of the RS. The connection will be counted as successful if the BS sends an authentication response to the RS with the digital certificate of BS and also the authentication key (AK). Once the AK is delivered to the RS, RS will check the AK with the BS to make sure it was not compromised. When the AK was confirmed received from BS, then the transmission of encrypted message begins. RS will apply the decode-and-forward protocol to decode, re-code and forward the message to next RS. Same step goes to the next RS. Then the second RS forward the message to SS. Direct communication refers to BS sends encrypted message directly to SS. Then, for all channels in the scenario included the RS itself are vulnerable. Based on Figure 1, when two devices communicate indirectly with each other, control links are supplied by the BS where both devices communicate via RS within the wireless network. Resource allocation, setting up of call, interference management, all are managed by the devices themselves in an allocable fashion. Thus, control of the BS is missing there. Despite being direct, the communication is fully managed by the BS since there is only a central controlling entity, i.e. the BS is present, interference management is possible [15]. This means that eavesdropper can attack on them. The foremost vital technical challenge is security. Parties who are sending and receiving the information should assure their data is not accessible to the relay, as well as the relay should be assured that the information that is handling is benign. We tend to distinguish between closed and opened access styles, wherever the user of a closed access device expressly permits the device to relay for a selected list of trustworthy sources.

From Figure 1, we can see that the multi-hop relays are limited to nodes which are at most two hops from the BS. Therefore, SS can connect to an RS which originally was connected to the BS, or they can connect directly to the BS. This will leave the connection vulnerable to Man-in-the-Middle attack. This is because it allows the eavesdroppers to make an independent connection with the SS or RS, and relays false messages or fetch private information from the connection. The reason why we propose Quantum and ECC cryptographic as a method to overcame the attacks is because Quantum cryptography allows the SS to sense the presence of an eavesdropper and ECC cryptography has relatively shorter key, yet still have the same level of security as RSA. Besides, decode-and-forward protocol is used to improve the performance of the system in the relay network. It works when the relay decodes and re-encodes the received signal and then forward it to the destination [16]. This process explains that the signal at the relay is having a hard time making decisions. This is mainly because the information sent by the previous relay does not include any additional information about the reliability of the source. The information might be sent from an unauthorized source or Rogue Relay Station (RRS). However, if encoded modulation protocol is used, the receiving RS will know that the information is from a "detect-and-forward" process from the previous station.

3. Quantum cryptography

Based on Figure 1, 5G wireless network between BS to RS and RS to RS are point to point. Pajic [17] mentioned that, to provide the best security in a cryptogram is not about the complexity of the algorithm in the encryption or decryption process. Rather, security is determined by the complexity of a key and how secure the channel for key transfer. In this scenario, private key cryptography is the best method to use. However, private key cryptography is vulnerable due to distribution of the private key in a widely wireless broadcasting channel which is also known as insecure channel. Unlike using LAN (Local Area Network) such as fiber optics, attackers can attack in any location in a 5G WLAN (Wireless Local Area Network). Therefore, Quantum Key Distribution (QKD) with BB84 protocol will be used to secure the channel from attacks. QKD uses two types of channel which are:

- Public channel
  - Communication between BS and RS for handshaking.
  - Transmission of encrypted message.
- Quantum channel.
  - Distribution of the shared key which in the form of polarized bit (Qubits).

Both channels can be implemented in a 5G wireless network [18].

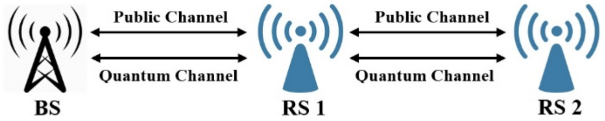

Fig. 2 Scenario between BS to RS and RS to RS

Based on the scenario in Figure 2, BS is installed with a QKD transmitter. Steps in performing QKD from BS to RS1 are as follow:

1) A string of random bits α = [0 1 1 0 1 0 0 1] (for easier to explain QKD, only 8 bits are used here. In an actual real life situation, α can be extended to 128 bits) is generated from the BS.

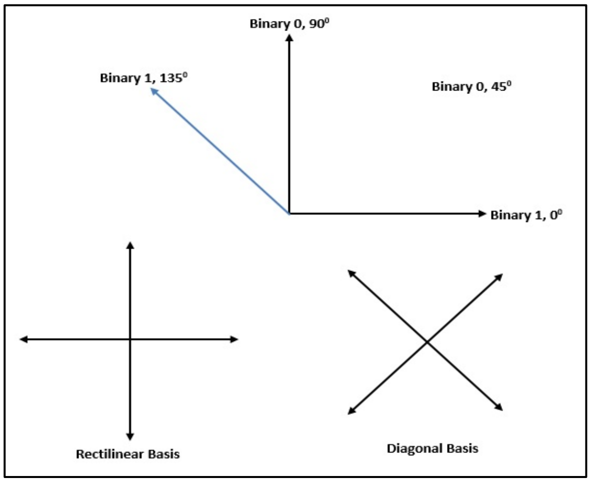

Fig. 3 Polarizing filters.

2) The QKD transmitter will polarize α into Quantum bits (qubits) by randomly choosing the bases for each bit either Rectilinear or Diagonal Basis. β = [+ + × + × × × +].
3) This will result in polarized key (qubits), *p* = [| - \ | \ / / -].
4) The qubits *p* will be transmitted through the quantum channel to RS.

RS1 is installed with both QKD Transmitter and Receiver. Steps for RS1 to measure the photons received from BS are as follow:

5) RS1 will first generate a random basis, β' to measure the incoming photons. This is represented by β' = [+ × × × + × + +].

6) *p* will pass through β’ and a set of new polarized qubits, *p’* will be obtained. When a Rectilinear polarized photon (| -) pass through a Rectilinear basis (+), it will retain its polarization. Else, if it passes through a Diagonal basis (×), it will transform to any Diagonal polarized photon (\ /) in an equal chance and vice versa. Since β’ is randomly chosen, the polarized photons of *p’* are estimated to be 50% same with *p*. Therefore *p’* = [| / \ / - / - -]. Thus, α’ = [0 0 1 0 1 0 1 1].
7) At this point, RS1 will send β’ to BS through the public channel for verification. BS will match β with β’ and the result *r* is obtained where *r* = [√ × √ × × √ × √]. (√ = matching, × = not matching).
8) *r* is then sent back to RS1 through the public channel and RS1 will distill α’ by using *r*, only the bits with the matching bases are retained, the bits with different bases will be discarded. A sifted key *s*, will be produced at this point where *s* = [0 _ 1 _ _ 0 _ 1].
9) Now, BS and RS1 will agree to use *s* = [0 1 0 1] as the shared secret key for Encryption and Decryption.
10) BS will use *s* to encrypt the plaintext into cypher text and send to RS1, then RS1 will use *s* to decrypt the cypher text into plaintext.

RS2 is also installed with both QKD Transmitter and Receiver. Steps for RS1 to relay messages to RS2 using QKD are as follow:

11) Since RS1 is equipped with QKD transmitter, steps (1) to (3) are repeated with a newly randomized α from the QKD transmitter.
12) The qubits *p* will be transmitted through the quantum channel to RS2.

Steps for RS2 to measure the photons received from RS1 will be the same as steps (5) to (10).

Each secret key will follow the One-Time Pad (OTP) rule. The secret key will only be used one time. Quantum Bit Error Rate (QBER) is defined as in the equation below:

$$QBER = \left(\frac{\text{Qpk}-\text{Qfk}}{\text{Qpk}}\right)*100$$

Where,
Qpk = number of qubits of the primary key
Qfk = number of qubits of the final key

QKD cannot travel indefinitely in a quantum channel. When photons travel in a free space, photons will interact with its environment, it may disperse, get absorbed or change its quantum state [19]. All these factors will contribute to the increase in QBER. For QKD to travel over a long distance, it has to be relayed. In our situation where we integrate QKD in a 5G network, QKD has the capabilities to be transmitted through air (free space) over 144km [20].

Unfortunately, QKD is still vulnerable to Man in the Middle (MITM) attacks where eavesdropper, Eve may use spoofing to disguise herself as a fake RS or also called as Rogue Relay Station (RRS). Where this RRS will imitate as either RS or SS. The RRS can disguise as a legit RS or SS and receive information from BS without both parties knowing. To encounter MITM attacks, some sort of authentication must be done. Few techniques can be used and one of them is “counter based” authentication method. This method provides QKD with better efficiency and security [21]. Since each RS1 needs to decrypt the cyphertext and encrypt it again to re-send to RS2. Eve can potentially hack the server in RS1 or RS2 to obtain the plaintext. Future improvements to overcome the issue of vulnerability in RS is to use “Quantum Repeaters” where each RS is equipped with this device to relay a quantum key without the need to measure it. This machine is still in an early development stage and is expected to be commercialized in the next 10 to 15 years [22].

In QKD, this technique can ensure the confidentiality of information by sharing a common secret key for cryptographic purposes later. The confidentiality of the transmitting data is then safeguarded by a chain with two links which are the quantum-distributed key and the encryption algorithm. Any eavesdropping activities are detectable due to the properties of quantum mechanics and once confirmed there’s an eavesdropper, both RS and BS will discard the key while there’s no confidential information has been transmitted yet.

QKD itself cannot ensure the integrity of the data since its only ensure the key that is going to be used for encryption is distributed securely and secretly between BS and RS or RS and RS. Therefore, to ensure integrity of information, encryption algorithm such as ECC as we proposed is used together with the secret key generated from QKD.

Next, QKD can ensure the availability of information due to the early detection of eavesdropper. Both BS and RS will distil the compromised secret key before using it to encrypt any data. Hence, the information is secure and still available in a way that the eavesdropper doesn’t has the chance to intercept the data transmission channel. Both of the stations will generate another secret key using QKD and make sure the key is safe to use before transmitting any information via the public channel.

Public key signature is used to authenticate the QKD session to ensure non-repudiation between both stations. Both of the stations will verify the digital certificates generated before any information exchange.

4. Elliptic curve cryptography

5G networks distribute communication networks to over a thousand of users simultaneously. In this case, we will be using the Elliptic Curve Cryptography (ECC) to secure the communication between the BS to the SS and from the RS to SS. ECC secures communication by encrypting the data. In this paper, we proposed a solution where Quantum Cryptography integrates with Elliptic Curve Cryptography to resolve the scenario in Figure 1. The difficulty to break the Elliptic Curve cryptography are based on the complexity of Elliptic Curve Discrete Logarithm Problem (ECDLP) [23]. The scheme to encrypt the data is Elliptic Curve Integrated Encryption Scheme (ECIES). ECIES uses the following functions:

- Key Agreement (KA): Function used for the generation of a shared secret by two parties
- Key Derivation Function (KDF): Mechanism that produces a set of keys from keying material and some optional parameters
- Encryption (ENC): Symmetric encryption algorithm.
- Message Authentication Code (MAC): Data used to authenticate messages.
- Hash (HASH): Digest function, used within the KDF and the MAC functions.

If BS wants to send a plaintext m to the SS. BS must follow this method:

1. BS (sender) creates ephemeral key pair (u, U) with public key U and private key u, plaintext P and domain parameter. In our proposed solution, we will use the output private key Q from Quantum Cryptography to temporarily replace the ephemeral private key in order to secure the transmission of information across 5G network.
2. Based on Figure 4 process (2), Key Agreement function (KA) will be used to create a shared secret value $(Q \times U)$ where Q is the QKD's private key and V is the SS's public key.
3. According to Figure 4 process (3), the shared value will be the input data for Key Derivation Function (KDF). The concatenation of the symmetric encryption key k_{ENC} and the MAC key k_{MAC} are the outputs of the process KDF. If the KDF outputs are "invalid", then the encryption process stopped.
4. The element of symmetric encryption key k_{ENC} will be used to produce encrypted message C by using the Symmetric Encryption Algorithm, ENC as shown in Figure 4 process (4).

$$\text{Message } C = k_{ENC}(P)$$

5. The selected MAC function will be used to produce a tag t by taking the encrypted message C, k_{MAC} and another optional parameter as shown in Figure 4 process (5).

$$t = k_{MAC}(C)$$

6. Lastly, BS will then send the cryptogram $CRY = (U, C, t)$ consisting public key U, tag t and encrypted message C to the SS.

To decrypt the message from BS, SS needs to:

1. Based on Figure 5 process (1), receiver will retrieve the cryptogram $CRY = (U, C, t)$ from sender to deal with those elements separately.
2. SS will use its private key v and the retrieved ephemeral public key U to produce the shared secret value $(v \times U)$ as shown in Figure 5 process (2).
3. By using the shared secret value and the same optional parameters that BS uses as input, SS has to produce the same encryption and MAC key by mean of the KDF procedure.
4. In Figure 5 process (4), SS will compare the tag and if the tag that received and value that has computed is different, SS has to reject the cryptogram due to failure in MAC verification procedure.

$$t^{'} = k_{MAC}(C)$$

5. In order to access the plaintext P that the BS intended to send to the SS, the SS must be deciphering the encrypted message using ENC and symmetric decryption scheme k_{DEC} if and only if the generated tag is correct.

$$P = k_{DEC}(C)$$

Let's say that eavesdropper sees the message and wanted to decrypt it. Without knowing the SS's private key to generate encryption as BS and using MAC and KDF functions, message cannot be decrypted if the value does not match. We can say that the plaintext is secured from the eavesdroppers.

The cases that commonly occurs is the message has been tampered, the sender denies sending the message and the receiver falsifies the message [24]. To secure the message from the cases above, ECIES uses a series of functions such as KDF, HASH and MAC functions [16].

Confidentiality is a protection of valuable, confidential and sensitive data or information from unauthorized party. It is also known as secrecy and privacy. ECC ensures confidentiality by encrypting the message so that only the target receiver can read the information. As explained in ECIES scheme above, it is impossible for the eavesdropper to decrypt the message if the private key is not known to provide the same optional parameter with BS. The security attacks that ECC can tackle in this case are spoofing and sniffing. Spoofing is when an attacker impersonates the users to steal data. Since only the legitimate user knows the private key and need to authenticate the value, it is difficult for the eavesdropper to access the data. Sniffing is a malware that monitor, read and capture data exchange. Since the message is encrypted in ECC, there is no way the data can be read.

Integrity of information is protecting the data from being altered by unauthorized parties. Since the message is encrypted and have a function to authenticate and protect the data, unauthorized party cannot read and alter the message [18]. A HASH function in ECC ensures the stability of the data from changing as it may produce a completely different output value. The most common use of hashing is data fingerprinting. The output identifier used to identify the file integrity. For example, the message that BS sends to SS is modified, the resulting hash of the file will be totally different. SS will identify the received file are not genuine and can request the file from BS again. The hashing algorithm tackles the potential attack on integrity in a 5G network such man-in-the-middle (MItM).

Availability is the assurance of resources that can be accessed by legitimate users. Elliptic Curve Cryptography encrypt the message and only the sender or receiver can decrypt the data. The protocol in the network with implementation of ECC can detect the attack that can disrupt the access to the resources. For example, Denial of Service (DoS) attack can be prevented by detecting the incoming heavy request and filtering the source address.

Non-repudiation is a guarantee that prevents both sender and receiver from denying the message that has been sent. The sender cannot repudiate the arrived message because it is signed [25]. The ECC uses the digital signature to provide security and non-repudiation of data. For example, BS wants to exchange encrypted message with SS. BS already has a certificate for its public key from common trusted certificate authority (CA). After encrypting the data, BS signs the whole message using its public key. Upon receiving the BS message, SS checks the certificate of BS's public key for validity and uses BS's public key to verify BS's signature. This certificate and public key verification to ensure non-repudiation of data between BS and SS. The sender cannot repudiate the arrived message because it is signed [25].

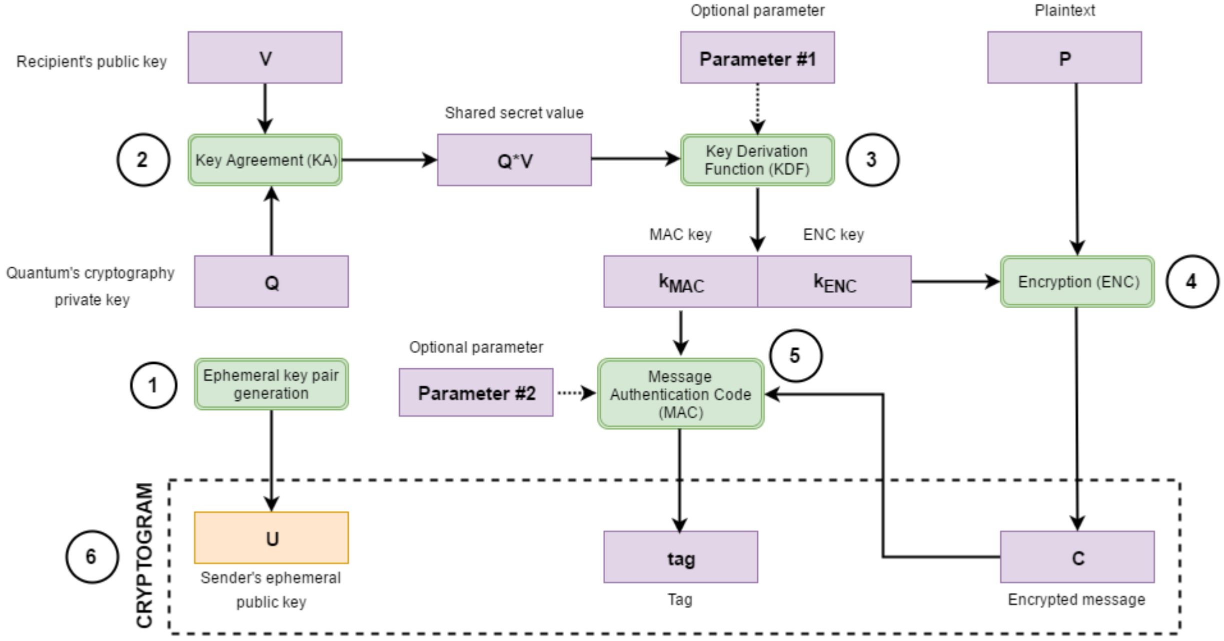

Fig. 4 Integration of Quantum Cryptography and Elliptic Curve Cryptography for encryption using Elliptic Curve Integrated Encryption Scheme.

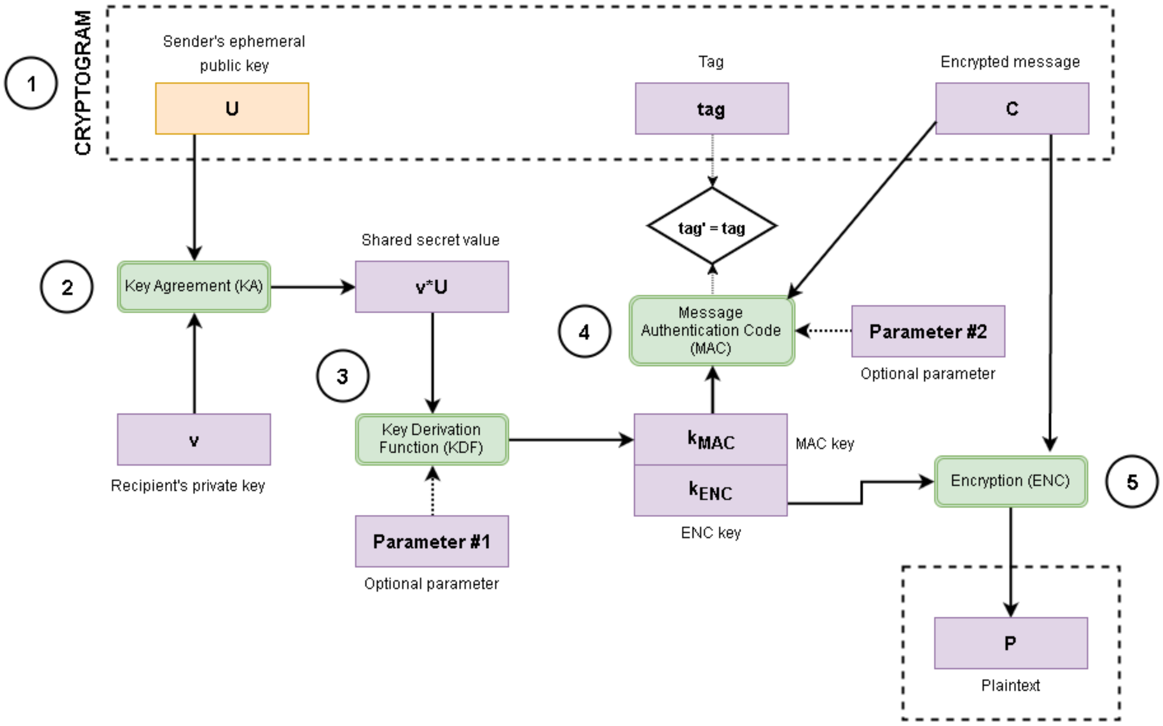

Fig. 5 Integration of Quantum Cryptography and Elliptic Curve Cryptography for decryption using Elliptic Curve Integrated Encryption Scheme.

5. Comparison analysis

Table 1: Comparison analysis between Elliptic Curve Cryptography and Quantum Cryptography

Cryptography **Aspects**	**Quantum**	**ECC**
Basis of knowledge	Quantum Key Distribution (QKD)	Elliptic Curve Theory
Channel	Both Classical Channel and Quantum Channel	Classical Channel
Encryption	✗	✓
Key generation	✓	✓
Key names	Secret Key only	Public Key and Secret Key
Key generation method	Quantum States	Elliptic Curve Equation
Key encryption method	Polarization of light	RSA algorithms
Name of bit	Bits with polarization (Qubits)	Normal bits numbers
Decryption	✗	✓
Complexity	Complex	Not complex
Easy to implement	✗	✓
Ease of use	✗	✓
Security Level	Highly secure	Good level of security
Encryption speed	-	Average

6. Conclusion

To secure 5G based IoT communications, an end-to-end security mechanism has been applied to secure the secret information being sent and received while achieving confidentiality, integrity, availability and non-repudiation at the same time. Quantum Cryptography has been utilized to secure the private key across the channel between BS to RS and RS to RS. The integration of Quantum Cryptography with Elliptic Curve Cryptography can resolve the problems faced in the scenario. The private key produced from QKD will be integrated into ECC to secure the transmission of secret message across the channel between RS to SS or BS to SS. Moreover, Elliptic Curve Integrated Encryption Scheme (ECIES) has been utilized for data encryption and decryption in ECC to secure the transmission of confidential message. In the end, extensive discussion has been done and we concluded that our suggested security mechanism has potential to achieve confidentiality, integrity, availability and non-repudiation across the 5G based IoT networks.

Acknowledgements

This work was supported by the Research and Innovation Management Centre, Universiti Malaysia Sarawak under Grant No. F08 (S150)/1131/2014/(15).

References

[1] Buyya, R. and Dastjerdi, A. V. (2016). Internet of Things: Principles and paradigms. [Online]. Available: https://books.google.com.my/books?id=_k11CwAAQBAJ&printsec=frontcover&dq=internet+of+things&hl=en&sa=X&redir_esc=y#v=onepage&q&f=false

[2] Khan, R., Khan, S. U., Zaheer, R., and Khan, S. (2012). Future Internet: The Internet of Things architecture, possible applications and key challenges. Presented at Proc. 10th Int. Conf. FIT, Islamabad, Pakistan, 2014. pp. 257-260.

[3] Prasad, R. (2014). 5G: 2020 and beyond. River Publishers.

[4] Hossain, E., Rasti, M., Tabassum, H., and Abdelnasser, A. (June 27, 2014). Evolution toward 5G multi-tier cellular wireless networks: An interference management perspective. IEEE Wireless Communications, 21(3), pp. 118-127.

[5] Rong, B., Qiu, X., Kadoch, M., Sun, S., and Li, W. (2016). 5G heterogeneous networks: Self-organizing and optimization. Springer International Publishing.

[6] Khan, A. S. (2014). "Secure and efficient distributed relay-based rekeying algorithm for group communication in mobile multihop relay network." International Journal of Communication Networks and Information Security 6(3): 189-199.

[7] Khan, A. S., N. Fisal, Z. A. Bakar, N. Salawu, W. Maqbool, R. Ullah and H. Safdar (2014). "Secure authentication and key management protocols for mobile multihop WiMAX networks." Indian Journal of Science and Technology 7(3): 282-295.

[8] Khan, A. S., N. Fisal, N. N. M. I. Ma'arof, F. E. I. Khalifa and M. Abbas (2011). "Security issues and modified version of PKM protocol in non-transparent multihop relay in IEEE 802.16j networks." International Review on Computers and Software 6(1): 104-109.

[9] Khan, A. S., N. Fisal, S. K. S. Yusof, S. H. S. Ariffin, M. Esa, N. N. Maarof and M. Abbas (2010). An improved authentication key management scheme for Multihop relay in IEEE 802.16m networks. 2010 In the Proceedings of IEEE Asia-Pacific Conference on Applied Electromagnetics, (APACE 2010), Port Dickson, Malaysia, 2010.

[10] Khan, A. S., H. Lenando and J. Abdullah (2014). "Lightweight message authentication protocol for mobile multihop relay networks." International Review on Computers and Software 9(10): 1720-1730.

[11] Khan, A. S., H. Lenando, J. Abdullah and N. Fisal (2015). "Secure authentication and key management protocols for mobile multihop WiMAX networks." Jurnal Teknologi 73(1): 75-81.

[12] Khan, A.S., Abdullah, J., Lenando, H., Nazim, J.M. Green resource allocation for multiple ofdma based networks: A survey (2016) Journal of Electronic Science and Technology, 14 (2), pp. 170-182.

[13] Peng, M., Li, Y., Zhao, Z., and Wang, C. (March 24, 2015). System architecture and key technologies for 5G heterogeneous cloud radio access networks. IEEE Network, 29(2), pp. 6-14.

[14] Bennet, C. H. and Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of the International Conference on Computers, Systems and Signal Processing. (pp. 175-179). Bangalore, India.

[15] Tehrani, Mohsen Nader, Mustafa Uysal, and Halim Yanikomeroglu. "Device-to-device communication in 5G cellular networks: challenges, solutions, and future directions." Communications Magazine, IEEE 52.5 (2014): 86-92. Retrieved from http://www.comsoc.org/ctn/device-device-communication-5g-cellular-networks-challenges-solutions-and-future-directions.

[16] D. Brennan, Linear diversity combining techniques," Proceedings of the IRE,vol. 47, no. 6, pp. 1075-1102, June 1959.

[17] P. Pajic, “Quantum Cryptograph,” thesis, 2013.

[18] P. Bhatia and R. Sumbaly, "FRAMEWORK FOR WIRELESS NETWORK SECURITY USING QUANTUM CRYPTOGRAPHY," pp. 1-1, 2014.

[19] J. Wiles, "QUANTUM BIT ERROR RATES IN QUANTUM KEY DISTRIBUTION USING ENTANGLED PHOTONS," 2005.

[20] T. Schmitt-Manderbach, H. Weier, M. Furst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger and H. Weinfurter, "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144km," in Munich, 2007, 2007 European Conference on Lasers and Electro-Optics and the International Quantum Electronics Conference.

[21] F. Sufyan, "Defeating Man-in-the-Middle Attack in Quantum Key Distribution," [Online]. Available: www.wcl.ee.upatras.gr.

[22] "Quantum Repeaters for Long Distance Fibre-Based Quantum Communication," QuRep, 2010. [Online]. Available: http://www.quantumrepeaters.eu/quantumrepeaters.eu/index.php/qcomm/quantum-repeaters/. [Accessed 30 11 2016]

[23] Hankerson, D., Menezes, A. & Vanstone, S. (2004). Guide to elliptic curve cryptography. NY, Springer.

[24] Naveena, A., & Reddy, K. R. (2016). A Review: Elliptical Curve Cryptography in Wireless Ad-hoc Networks.

[25] Zhong, H., Zhao, R., Cui, J., Jiang, X., & Gao, J. (2016). An Improved ECDSA Scheme for Wireless Sensor Network. International Journal of Future Generation Communication and Networking, 9(2), 73-82.