MJFAS
Malaysian Journal of Fundamental and Applied Sciences

Fakhruldeen *et al.* | Malaysian Journal of Fundamental and Applied Sciences, Vol. 19 (2023) 337-344

RESEARCH ARTICLE

# Post-quantum Techniques in Wireless Network Security: An Overview

**Hassan Falah Fakhruldeen[a,b*], Rana Abbas Al-Kaabi[a,c], Feryal Ibrahim Jabbar[d], Ibrahim H. Al-Kharsan[e], Sarah Jawad Shoja[f]**

[a]Computer Techniques Engineering Department, Faculty of Information Technology, Imam Ja'afar Al-Sadiq University, Baghdad, Iraq; [b]Department of Electrical Engineering, Faculty of Engineering, University of Kufa, Kufa, Najaf, Iraq; [c]College of Information Technology, University of Babylon, Hilla, Iraq; [d]Air conditioning and Refrigeratin Engineering Department, Al-Mustaqbal University College, Babylon, Iraq; [e]Computer Technical Engineering Department, College of Technical Engineering, The Islamic University, Najaf, Iraq; [f]College of Health & Medical Technology, Al-Ayen University, Nasiriyah, Iraq

Abstract. Post quantum is a general name to all the techniques which are safe against the quantum computer attack. The wireless network is one of the most important means of communication. Wireless network security is a top priority. Wireless networks use conventional cryptography, which has various flaws, whereas quantum cryptography claims to be completely secure. It wasn't long after quantum computers became operational that people began to think about new ways to secure electronic communications. After considering all of the weaknesses in conventional cryptosystems, individuals began to look for new ways to secure electronic communications. Traditional cryptography has many problems, but quantum cryptography addresses nearly all of them.

**Keywords:** BB84, E91, post-quantum, quantum computing, QKD.

## Introduction

With the help of cryptography, sensitive information can be transmitted securely, even while malicious actors are present. The difficulty of a one-way mathematical function has long been used in traditional cryptography. In terms of safety, you get what you pay for. It's a weak defense mechanism [1]. Neither the sender nor the recipient of a message can detect the presence of an adversary using standard cryptographic methods. RSA is the most popular classical cryptographic algorithm, and it relies on the difficulty of factoring a number generated by multiplying two huge prime integers. Since the advent of quantum computers, all classical cryptosystems have been cracked, prompting researchers to consider alternatives to classical cryptography to ensure the safety of future electronic communication. As flaws in classic cryptosystems became more apparent, people started looking for alternatives [2]. Some of quantum computing's benefits in the real world include the following: A qubit's quantum mechanical properties make it useful for a wide range of applications when combined with the right quantum data [3]. The cloning property of the qubit is worthless if the message conveyed through it is secret and a duplicate is wanted [4]. Quantum physics states that measuring a qubit degrades its state or its superposition. This will help you maintain the privacy of your conversations. Classical information systems employ bits to denote digital signals. Each classical bit can take either a 0 or 1 value, and there are 2n bit vectors for a vector of length n [5]. Post-quantum encryption (or quantum-resistant cryptography) provides a solution to the problem of developing safe cryptographic systems compatible with current protocols and networks [6]. Integer factorization, discrete logarithm, and elliptic curve discrete logarithm are three common mathematical difficulties used in today's most famous algorithms. When Shor's approach is combined with a sufficiently robust quantum computer, all of these issues become trivial to solve [7]. Despite the fact that quantum computers lack the necessary processing capacity to crack any practical cryptographic algorithms [8], for the off chance that this circumstance ever changes, multiple cryptographers are busy creating new algorithms. In quantum encoding, quantum states (or qubits) are used to store information in place of the bits used in regular digital transmission. As a standard quantum state representation, the photon is widely

***For correspondence:**
hassan.falah@sadiq.edu.iq

**Received:** 2 Nov. 2022
**Accepted:** 11 April 2023

used. Quantum keys are kept secure thanks to the peculiarities of quantum states. Based on what they do to distribute keys, quantum cryptography techniques can be broken down into two broad categories [9-12].

## Post Quantum Cryptography

When discussing cryptography in the post-quantum era, it is assumed that the hacker has access to a quantum computer. Researchers work under this premise while designing and assessing new cryptosystems. Once a quantum computer is created, public-key cryptography and digital signatures will be rendered useless [13, 14]. This section delves into the state of the art and future prospects for secure cryptosystems in the post-quantum era. Nowadays, cryptography is indispensable in all kinds of technological contexts. Most currency in use nowadays is electronic. The use of a pin code on a smartphone provides a measure of privacy; this is made possible through encryption [15]. Post-quantum cryptography, also termed quantum-resistant cryptography, aims to build secure cryptographic systems compatible with contemporary communication protocols and networks. [16]. It's possible that large-scale, functional quantum computers could soon be within reach. Developing quantum-safe algorithms is a laborious process. Picking a function that is hard to compute in one direction but easy in another is the first step. The user should be able to quickly and easily calculate these functions, but hackers will find them somewhat difficult [17]. Researchers also need to assess the efficacy of the offered algorithms. A theoretically sound algorithm may nonetheless not be user-friendly. In the case of algorithms with key sizes greater than one megabyte, for instance, the required bandwidth may be too great to make their use practicable [18]. Furthermore, there is the problem of cryptanalysis to consider. It is important for algorithms to be secure against timing and side-channel attacks. The necessity for speed in post-quantum cryptography arises from the fact that developing an appropriate algorithm is a time-consuming procedure [19]. As of 2015, the NSA has been using quantum-safe algorithms. Additionally, NIST has begun research towards standardizing cryptographic approaches for the era after quantum computing. There is no way to determine when a quantum computer strong enough to crack current cryptography will be available to the public. Data developed today may need to be encrypted with techniques that are immune to the effects of quantum computing if it is to be kept safe. Before quantum computers become widely available, the shift to cryptography that is immune to the effects of quantum computing must be completed. These adjustments are presently in the process of being made [20, 21].

## Post Quantum Cryptosystems

In contrast to encryption methods that are based on quantum physics, post-quantum cryptosystems are predicated on a series of mathematical problems that are simple for the receiver to answer but challenging for the hacker.

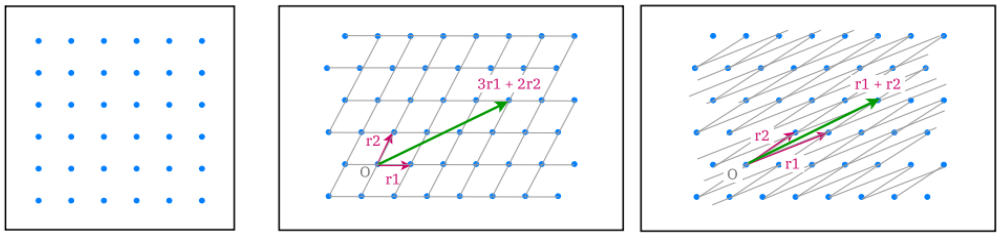
## Lattice-based Cryptography

Lattice-based in the subject of information security, cryptography is a subfield that can be utilized to make up for the deficiencies of the RSA algorithm. This method of encryption is founded on the fact that solving problems involving lattices is challenging for both classical and quantum computers. You might imagine a lattice as a grid of vectors or points in a two-dimensional space that goes on forever, as shown in Figure 1 a. traditionally, computers only have so much memory, yet we need an infinite number of items to accurately represent a lattice. This is why there needs to be a standardized means of representing lattices in computer cryptography. When discussing the methods used in cryptography to describe lattices in order to address memory-related issues on modern computers, the term "Basis of lattice" is commonly used to denote this prevalent approach. The "Basis of lattice" refers to the set of tiny vectors used to recreate the lattice's grid of points [22].
There can be various lattice bases, of which two specific varieties are utilized in lattice-based cryptography.

(1) On a short basis

(2) On a long basis

A lattice with a basis constructed entirely of short vectors is said to have a short basis (Figure 1 b). But if the lattice's basis is composed entirely of long vectors, we say that it has a long basis (Figure 1 c). One approach to see them is as the respective private and public keys for lattice-based encryption.




(a) 2-Dimensional Lattices (b) An example of a short basis (c) An example of a long basis

**Figure 1.** Lattice based cryptosystem [23]

## Multivariate Cryptography

It is a supplementary approach of cryptography that is predicated on multivariate equations (sometimes written as multivariate equations). In multivariate public key cryptosystems, nonlinear multivariate polynomials are utilized as the key generating function [24].

## Hash-based Cryptography

The term "hash-based cryptography" is used to describe any type of cryptographic primitive that relies on the security provided by hash functions. Considerations of its possible uses in post-quantum cryptography are intriguing. Current uses for hash-based encryption include zero-knowledge and computational integrity proofs like the zk-STARK proof system, digital signature systems like the Merkle signature method, and range proofs over issued credentials via the HashWires protocol. One-time signature schemes and Merkle tree structures meet in hash-based signature schemes. One-time signature schemes allow for the consolidation of numerous keys into a single, more robust structure because each key may only be used to sign a single message. The appropriate tool for the job is a Merkle tree. One "a-ha" moment was when I realized that the information was organized like a tree [25].

## Code-based Cryptography

Code-based cryptography is one of the most promising post-quantum cryptographic approaches. Numerous successful implementations of the most important cryptographic primitives (encryption, signature, zero-knowledge, hashing, etc.) can be constructed using this method. Additionally, this group's security is well understood. The following describes the core concept of encryption. Assume the sender (Alice) mistakesnly uses the recipient's (Bob) public key in the message (Figure 2). The problem is introduced in a way that only Bob can notice and fix because he has the private key. The bounded distance decoding problem is NP-Complete, making it inefficient for the hacker to fix the mistake [26-28].

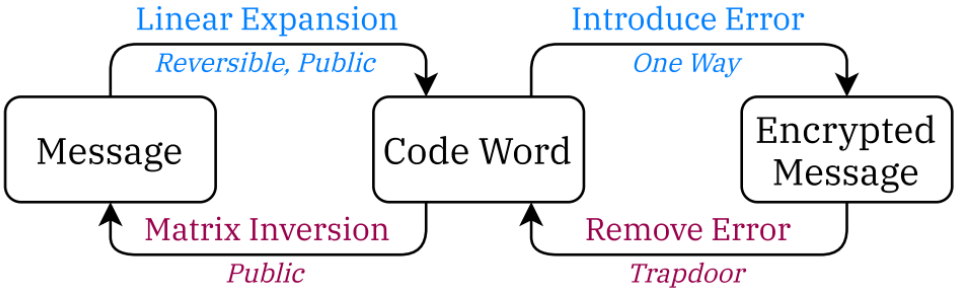



**Figure 2.** Code based cryptosystem [29]

## Isogeny-based Cryptography

If and when big quantum computers become viable, all currently frequently used public key cryptography methods will fail. Even the most enthusiastic proponents of quantum computing believe such machines are years, if not decades, away. However, developing, testing, and deploying new encryption methods can take years, if not decades, therefore researchers are

working now to have quantum-resistant encryption systems in place by the time they are required. Isogeny-based encryption is one type of quantum-resistant encryption technology. This class is notable for at least two methods: it employs the smallest keys and the most complex math [30].
To retain present levels of security, most post-quantum encryption techniques require substantially longer keys, two or three orders of magnitude longer. Isogeny-based encryption has the shortest keys of any proposed post-quantum encryption technology, with keys that are around the same size as those currently in use. Isogeny-based cryptography has a complex mathematical foundation [31].

## Quantum Cryptography Implementation in Wireless Network

To use quantum cryptography to safeguard key distribution in wireless networks is the major goal. We came to the conclusion that the IEEE 802.11 family of standards (also known as Wi-Fi) is the best option for quantum key distribution (QKD) due to the fact that the standard area is so limited. This suggests that Wi-Fi may be less susceptible to the kinds of environmental shifts that hinder the performance of quantum missions in Wi-Fi networks. This new method of communication makes use of both the standard Wi-Fi network and the more exotic quantum network [32]. Quantum cryptography solves all the problems with the classical method. A secure cryptosystem based entirely on quantum mechanical forces has been created for the first time [33]. The ability to identify a potential key thief is fundamental to quantum cryptography. Because monitoring them would destroy their quantum state, it is impossible to make a copy of a quantum bit. Let's pretend eavesdropper Eve is after a secret chat. The quantum cryptosystem is safe according to the No-Cloning theorem. Eve can only learn what she needs to know by inducing a perturbation in one of the photon's non-orthogonal states [34]. Protocols like as BB84, B92, E91, and SARG04 are already available for use in the implementation of quantum cryptography. BB84 is the default protocol used by the majority of internet users. In BB84, Alice and Bob are able to talk to one another over both private quantum channels (optical fibers) and open internet channels (internet etc.). There are two steps involved in distributing quantum keys [35].

## Via Quantum Channel (one way correspondence)

Alice chooses a random sequence of bits and encodes them using either a linear or diagonal base. First, let's do this. After encoding each bit with the appropriate polarization, Alice uses the quantum channel to send a photon to Bob for each bit. In Step 2, Bob gathers the polarized rays by picking bases at random [36,37]. By means of a freely accessible forum (including two-way interaction): Alice communicates with Bob about the polarization state she employed when sending a bit, but the bit's value remains secret. Bob uses this evaluation to figure out if the polarization state lists Alice provided him are similar to the lists he generated on his own [38].

## Via Public Channel (two-way communication)

Through the use of the shared medium, Alice informs Bob of the polarization state she has chosen for each bit she sends. Yet she keeps the actual bit value from him [39]. Then, Bob checks Alice's polarization state list against the one he compiled from a statistical sampling of the population. The raw key can be created by combining the two lists, but it is not safe because Eve can eavesdrop on selected data while in transit. Getting the right key entails four primary steps: coarse key sifting, error assessment, error remedy, and privacy intensification [40, 40].

## Threats to Current State Cryptography Systems

Cryptography ensures the confidentiality of data. In the post-industrial era of personal computers, its application has been widespread. SSL/TLS encryption is employed by every website we visit. Similarly, encryption protects the privacy of our emails and other electronic conversations [42]. Modern cryptosystems use the premise that some math problems are easier to solve in one direction. They are described using the term "computationally secure." This does not imply that cracking these systems is impossible, but it does imply that it takes a great deal of time a great deal of time that practically grows exponentially with input length. If a quicker algorithm is devised, these systems will fail. However, some cryptosystems are secure from an information-theoretic standpoint. Even if we gave these systems a limitless amount of computer power, they would still be impregnable. Consider the disposable pad (OTP). As the key and the data to be encrypted must have the same length, OTP is rarely used in reality [50]. One of the most prevalent types of cryptosystems is symmetric encryption, while asymmetric encryption is the other [43].

1. When both parties in a conversation use the same encryption method, the method is said to be symmetric. The message can be encrypted and decrypted with the same key. Up until 1976, it was

the gold standard for secure communications. In Figure 3a, we see Alice and Bob. In this exchange, Alice acts as the transmitter. So that only Bob can decipher the message. To hide the contents of her communication, Alice enters a key. This key is shared by Bob and Alice. Bob deciphers the message that was sent to him. By utilizing Alice's key, Bob can read her encrypted message [44].

2. Asymmetric encryption is a method of data security where two mathematically connected cryptographic keys are used to encrypt data in secret. They are referred to as public-private key pairs. After information is encrypted using a public key, it may be decrypted by only the corresponding private key. There is a mathematical connection between the keys, but you can't figure out which one would unlock the other. Those on the receiving end must produce both the public and private keys. Many distinct asymmetric encryption methods [45] are capable of generating such keys. To facilitate communication between themselves, Bob shares his public key with Alice, as depicted in Figure 3b. Therefore, Alice can encrypt the vital file she has to send to Bob using Bob's public key. Alice can send Bob the file through email, fax, or any other method she chooses now. With access to the matching private key, only Bob can read the encrypted file. Given that she only has access to the public key, Alice is unable to read the encrypted file [46]. This addresses a significant weakness of Symmetric cryptography, namely that it is possible for an adversary to decode a file if they acquire both the document and the public key. How effectively the other party safeguards his private key will decide how effective and secure this system is. Almost all critical data transmission use cases now make use of asymmetric encryption. All HTTPS websites, the most popular messaging services, email protocols, and so on all use asymmetric encryption [47, 48].

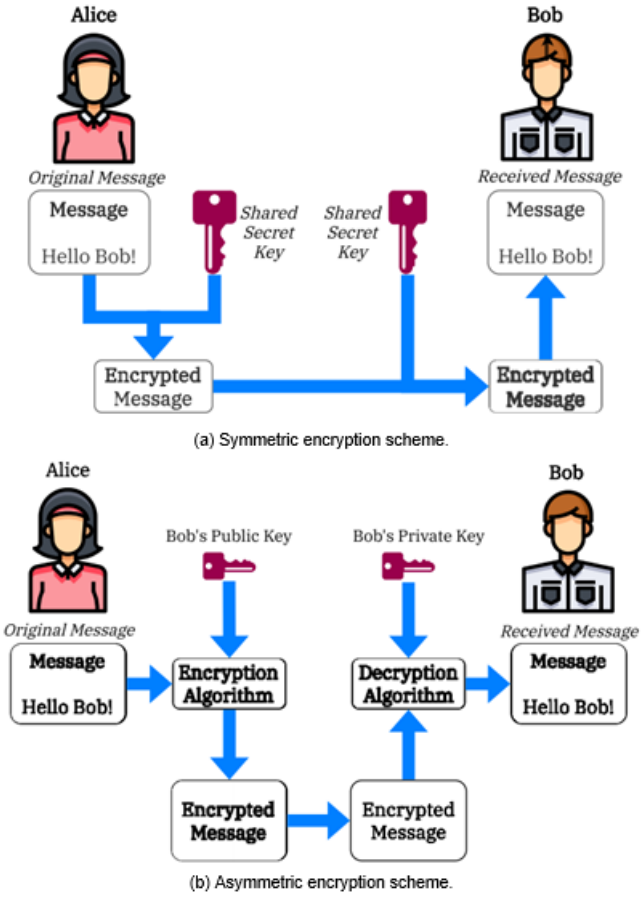



**Figure 3.** A flow diagram illustrating the encryption and decryption of data in symmetric and asymmetric encryption schemes [49].

## Challenges in Post-quantum Cryptography

In an ideal world, key-sharing and digital signature algorithms, which rely on public-key cryptography, will have "drop-in replacements" available that do not require the use of quantum computers. According to NIST, several of the proposed post-quantum cryptography standards are flawed to the point where they cannot be used independently. Excessive key or signature sizes, as well as sender-recipient asymmetry, fall into this category [50]. Implementations and standards

based on these techniques may need to provide support for, and answers to, issues like Public key validation, Public key reuse, unexpected decryption failure, and Selection of new auxiliary functions. Because of these obstacles and limits, it is unknown whether or not post-quantum algorithms will be able to integrate with current protocols. New and revised protocols will be required to detail the appropriate use of algorithms in various contexts, the partitioning of messages to address size issues, etc. Once the final algorithms have been selected, these new protocols must be established so that standardized implementations may be developed [51].

## Future Steps Towards the Post Quantum Techniques

The steps that need to be taken in order to successfully make the transition to post-quantum encryption. These include the following:
1. Once post-quantum algorithms have been selected, guidelines will be developed to describe how they should be implemented after they have been chosen.
2. Determining different uses for cryptography Cryptographic processes underpin a wide variety of components that make up today's technology. Because it is sometimes challenging for organizations to determine the locations within their environments where cryptography may expose them to a vulnerability, the development of tools and methods for identifying instances of cryptographic usage has become necessary.
3. The creation of mechanisms for the updating of algorithms. There are several situations in which traditional methods simply cannot be substituted for post-quantum cryptography algorithms. In order for these unique algorithms to function properly, it will be necessary to develop new protocols.

## Conclusion

Quantum computing is an exciting area of study that merges IT, Math, and Physics. It can handle tasks that even the most advanced modern supercomputers have trouble with. Quantum computers may not be able to completely replace traditional computers, but their ability to solve difficult problems may allow researchers to delve into hitherto uncharted areas of knowledge. One of the most promising future uses for quantum computers is in the realm of quantum simulation. New medicines and materials may be developed as a result of its capability to shed light on complex molecular and chemical interactions. The optimization of logistical processes, the assessment of financial risk, and the development of machine learning are just a few examples of how quantum computers could have a major impact on our daily lives. One way in which emerging technologies can have unintended consequences is by posing a threat to the existing cryptosystem. The risks to modern cryptography are discussed in this book, and they may have a significant impact on the current cryptosystem. Research and discussion center on the potential danger that quantum computers pose to the current cryptosystem. This research explores some of the many post-quantum cryptosystems now in development to address this issue. New, more efficient algorithms are being developed, and this may make it possible to avoid a slowdown in data transmission while still being resistant to quantum computing. Quantum key distribution (QKD) and other cryptosystems use quantum mechanics to counteract the threats posed by quantum computers. Thanks to the latest enhancements, we may have confidence that our communications will remain secure in the future.

## Conflicts of Interest

The author(s) declare(s) that there is no conflict of interest regarding the publication of this paper.

## Acknowledgment

This work is part of a research project, supported by the Ministry of Higher Education, Malaysia, and the University of Technology Malaysia. Also supported by Imam Ja'afar Al-Sadiq University, Baghdad, Iraq.

## References

[1] Vaudenay, S. (2006). *A classical introduction to cryptography: Applications for communications security*. Springer Science & Business Media.
[2] Scarani, V., Acin, A., Ribordy, G., & Gisin, N. (2004). Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, *92*(5), 057901.

[3] Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing* (pp. 212-219).

[4] Ahmed, J., Garg, A. K., Singh, M., Bansal, S., & Amir, M. (2014). Quantum cryptography implementation in wireless networks. *International Journal of Science and Research*, 129-133.

[5] Sadkhan, S. B., & Abbas, R. (2021, September). The role of quantum and post-quantum techniques in wireless network security-status, challenges and future trends. *2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA)* (pp. 296-302). IEEE.

[6] Chen, L., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., ... & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (Vol. 12). Gaithersburg, MD, USA: US Department of Commerce, National Institute of Standards and Technology.

[7] Khalique, A., Singh, K., & Sood, S. (2010). Implementation of elliptic curve digital signature algorithm. *International Journal of Computer Applications*, *2*(2), 21-27.

[8] Alsunbuli, B. N., Fakhruldeen, H. F., Ismail, W., & Mahyuddin, N. M. (2022). Hybrid beamforming with relay and dual-base stations blockage mitigation in millimetre-wave 5G communication applied in (VIOT). *Computers and Electrical Engineering*, *100*, 107953.

[9] Galbraith, S. D., & Gaudry, P. (2016). Recent progress on the elliptic curve discrete logarithm problem. *Designs, Codes and Cryptography*, *78*, 51-72.

[10] Hathot, S. F., Abbas, S. I., AlOgaili, H. A. T., & Salim, A. A. (2022). Influence of deposition time on absorption and electrical characteristics of ZnS thin films. *Optik*, *260*, 169056.

[11] Aldhuhaibat, M. J., Amana, M. S., Aboud, H., & Salim, A. A. (2022). Radiation attenuation capacity improvement of various oxides via high density polyethylene composite reinforcement. *Ceramics International*, *48*(17), 25011-25019.

[12] Salim, A. A., Ghoshal, S. K., & Bakhtiar, H. (2022). Prominent absorption and luminescence characteristics of novel silver-cinnamon core-shell nanoparticles prepared in ethanol using PLAL method. *Radiation Physics and Chemistry*, *190*, 109794.

[13] Sciarrino, F. (2013, March). Complete experimental toolbox for alignment-free quantum communication. *APS March Meeting Abstracts*, *2013*, C11-005.

[14] Jalil, R., Sabbar, A., Fakhruldeen, H. F., & Jabbar, F. I. (2022). Design and implementation of PC to PC data transmission using wireless visible light communication system. *Indonesian Journal of Electrical Engineering and Computer Science*, *26*(3), 1423-1428.

[15] Bennett, C. H., DiVincenzo, D. P., Smolin, J. A., & Wootters, W. K. (1996). Mixed-state entanglement and quantum error correction. *Physical Review A*, *54*(5), 3824.

[16] Ryan, P., Schneider, S. A., Goldsmith, M., Lowe, G., & Roscoe, B. (2001). *The modelling and analysis of security protocols: the CSP approach*. Addison-Wesley Professional.

[17] Fakhruldeen, T. S. M. H. F., & Mansour, T. S. A. (2018). All-optical NOT gate based on nanoring silver-air plasmonic waveguide. *Int. J. Eng. Technol.*, *7*, 2818-2821.

[18] Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., ... & Voznak, M. (2020). Quantum key distribution: a networking perspective. *ACM Computing Surveys (CSUR)*, *53*(5), 1-41.

[19] Waheed, S. R., Rahim, M. S. M., Suaib, N. M., & Salim, A. A. (2023). CNN deep learning-based image to vector depiction. *Multimedia Tools and Applications*, 1-20.

[20] Fakhruldeen, H. F., Al-Asady, H. A. J., Mahinroosta, T., Sohrabi, F., & Hamidi, S. M. (2021). Novel add-drop filter based on serial and parallel photonic crystal ring resonators (PCRR). *Journal of Optical Communications*.

[21] Bhatia, P., & Sumbaly, R. (2014). Framework for wireless network security using quantum cryptography. *arXiv preprint arXiv:1412.2495*.

[22] Arbaugh, W. A., Shankar, N., Wan, Y. J., & Zhang, K. (2002). Your 80211 wireless network has no clothes. *IEEE Wireless Communications*, *9*(6), 44-51.

[23] Ghori, M. R., Wan, T. C., & Sodhy, G. C. (2020). Bluetooth low energy mesh networks: Survey of communication and security protocols. *Sensors*, *20*(12), 3590.

[24] Fakhruldeen, H. F., & Mansour, T. S. (2020). Design of plasmonic NOT logic gate based on insulator–metal–insulator (IMI) waveguides. *Advanced Electromagnetics*, *9*(1), 91-94.

[25] Elliott, C., Pearson, D., & Troxel, G. (2003, August). Quantum cryptography in practice. *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications* (pp. 227-238).

[26] Waheed, S. R., Suaib, N. M., Rahim, M. S. M., Adnan, M. M., & Salim, A. A. (2021, April). Deep Learning Algorithms-based Object Detection and Localization Revisited. *Journal of Physics: Conference Series*, *1892*(1), 012001. IOP Publishing.

[27] Salim, A. A., Ghoshal, S. K., Shamsudin, M. S., Rosli, M. I., Aziz, M. S., Harun, S. W., ... & Bakhtiar, H. (2021). Absorption, fluorescence and sensing quality of Rose Bengal dye-encapsulated cinnamon nanoparticles. *Sensors and Actuators A: Physical*, *332*, 113055.

[28] Salim, A. A., Ghoshal, S. K., & Bakhtiar, H. (2021). Growth mechanism and optical characteristics of Nd: YAG laser ablated amorphous cinnamon nanoparticles produced in ethanol: Influence of accumulative pulse irradiation time variation. *Photonics and Nanostructures-Fundamentals and Applications*, *43*, 100889.

[29] Liu, Z., Choo, K. K. R., & Grossschadl, J. (2018). Securing edge devices in the post-quantum internet of things using lattice-based cryptography. *IEEE Communications Magazine*, *56*(2), 158-162.

[30] Salim, A. A., Ghoshal, S. K., Suan, L. P., Bidin, N., Hamzah, K., Duralim, M., & Bakhtiar, H. (2018). Liquid media regulated growth of cinnamon nanoparticles: Absorption and emission traits. *Malaysian Journal of Fundamental and Applied Sciences*, *14*(3-1), 447-449.

[31] Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. *arXiv preprint arXiv:1804.00200*.

[32] Buchmann, N. (2019). Strengthening trust in the identity life cycle: Enhancing electronic machine readable travel documents due to advances in security protocols and infrastructure (Doctoral dissertation).

[33] Somavilla, I. (2022). Essay Review: Dinda L. Gorlée," Wittgenstein's Secret Diaries: Semiotic Writing in Cryptography". *Nordic Wittgenstein Review*, 131-140.

[34] Dong, X., Dong, B., & Wang, X. (2020). Quantum attacks on some Feistel block ciphers. *Designs, Codes and Cryptography*, *88*(6), 1179-1203.
[35] Polnik, M., Mazzarella, L., Di Carlo, M., Oi, D. K., Riccardi, A., & Arulselvan, A. (2020). Scheduling of space to ground quantum key distribution. *EPJ Quantum Technology*, *7*(1), 3.
[36] Sharma, N., & Ketti Ramachandran, R. (2021). The emerging trends of quantum computing towards data security and key management. *Archives of Computational Methods in Engineering*, 1-14.
[37] Salim, A. A., Ghoshal, S. K., Bakhtiar, H., Krishnan, G., & Sapingi, H. H. J. (2020, April). Pulse laser ablated growth of Au-Ag nanocolloids: Basic insight on physiochemical attributes. *Journal of Physics: Conference Series*, *1484*(1), 012011. IOP Publishing.
[38] Tsai, C. W., Yang, C. W., Lin, J., Chang, Y. C., & Chang, R. S. (2021). Quantum key distribution networks: Challenges and future research issues in security. *Applied Sciences*, *11*(9), 3767.
[39] Sidhu, J. S., Joshi, S. K., Gündoğan, M., Brougham, T., Lowndes, D., Mazzarella, L., ... & Oi, D. K. (2021). Advances in space quantum communications. *IET Quantum Communication*, *2*(4), 182-217.
[40] Sadkhan, S. B., & Abbas, R. (2021, September). The role of quantum and post-quantum techniques in wireless network security-status, challenges and future trends. *2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA)* (pp. 296-302). IEEE.
[41] Hou, T. J., Gao, J., Hobbs, T. J., Xie, K., Dulat, S., Guzzi, M., ... & Yuan, C. P. (2021). New CTEQ global analysis of quantum chromodynamics with high-precision data from the LHC. *Physical Review D*, *103*(1), 014013.
[42] Sidhu, J. S., Joshi, S. K., Gündoğan, M., Brougham, T., Lowndes, D., Mazzarella, L., ... & Oi, D. K. (2021). Advances in space quantum communications. *IET Quantum Communication*, *2*(4), 182-217.
[43] George, I., Lin, J., & Lütkenhaus, N. (2021). Numerical calculations of the finite key rate for general quantum key distribution protocols. *Physical Review Research*, *3*(1), 013274.
[44] Ni, P., Lv, S., Zhu, X., Cao, Q., & Zhang, W. (2021). A light-weight on-line action detection with hand trajectories for industrial surveillance. *Digital Communications and Networks*, *7*(1), 157-166.
[45] Sadkhan, S. B., & Abbas, R. (2021, September). the role of quantum and post-quantum techniques in wireless network security-status, challenges and future trends. *2021 4th International Iraqi Conference on Engineering Technology and Their Applications (IICETA)* (pp. 296-302). IEEE.
[46] Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., ... & Wallden, P. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics*, *12*(4), 1012-1236.
[47] Bennett, C. H., & Brassard, G. (2020). Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*.
[48] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, *81*(3), 1301.
[49] Zou, Z. K., Zhou, L., Zhong, W., & Sheng, Y. B. (2020). Measurement-device–independent quantum secure direct communication of multiple degrees of freedom of a single photon. *Europhysics Letters*, *131*(4), 40005.
[50] Waheed, S. R., Adnan, M. M., Suaib, N. M., & Rahim, M. S. M. (2020, April). Fuzzy logic controller for classroom air conditioner. In *Journal of Physics: Conference Series*, *1484*(1), 012018. IOP Publishing.
[51] Jennewein, T., Simon, C., Weihs, G., Weinfurter, H., & Zeilinger, A. (2000). Quantum cryptography with entangled photons. *Physical review letters*, *84*(20), 4729.