Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 218 (2023) 2191–2200

Procedia
Computer Science

www.elsevier.com/locate/procedia

International Conference on Machine Learning and Data Engineering

A Survey on Quantum Computing for Internet of Things Security

Diksha Chawla[1] ,Pawan Singh Mehra[2]

[1]Delhi Technological University, Rohini, Delhi -110042, India

[2]Delhi Technological University, Rohini, Delhi -110042, India

Abstract

Quantum computing, based on quantum mechanical principle, can potentially provide significant advantages over classical computing. This advantage of quantum computing provides solutions to many previously unsolvable problems in secure communication and finance. IoT is an emerging technology that deals with a large amount of data. The data communicated in IoT need to be secured. The existing security architecture of IoT is based on cryptographic algorithms such as RSA and ECC. Quantum computing had a significant impact on the security of these algorithms. Therefore, our work analyses the security concerns of IoT smart applications and quantum-based solutions. This article provides a survey of quantum computing fundamentals and the impact of quantum computing on IoT security. Thus, this paper aims to provide a wide view of quantum-enabled IoT communication. The main challenges in implementing quantum-enabled communication are also analyzed in our work.

Keywords: Quantum Computing, Quantum Key Distribution (QKD), Internet of Things (IoT), Quantum Entanglement

1. Introduction

The usage of IoT is expanding in many applications such as intelligent environments, cities, smart grids etc. The number of devices connected in IoT communication provides decision-making ability to users. This vast spectrum of IoT-enabled applications [1], as represented in Figure 1, transfers a massive amount of data, which imposes security and privacy challenges. Without authentication and privacy, IoT applications will not be able to reach high demand. It may also create serious security threats to their potential users. IoT has challenges such as privacy, confidentiality and authentication. The existing scenario of IoT applications is based on RSA and ECC-based schemes [1]. However, with the emergence of quantum computers, such encryption primitives will no longer be secure. Quantum computer solves these classically unsolvable problems based on classical cryptographic primitives. Therefore, the security of this IoT communication network is ensured by Quantum computing. Quantum computing is based on the principle of uncertainty[2] and the no-cloning theorem[3]. The main aim of studying quantum computing is to design protocols and algorithms[4] to resolve IoT security issues, which are Quantum resistant. Classical computing manipulates individual bits, whereas quantum computer uses qubits. These qubits, with their associated probability, represent the quantum state. These qubits are based on Quantum mechanics principals such as superposition and entanglement. Superposition allows qubits to be in different possible combinations of values simultaneously. Entanglement creates a strong dependent relation between quantum particles. However, with the advancement of

1877-0509 © 2023 The Authors. Published by Elsevier B.V.

10.1016/j.procs.2023.01.195

quantum computing, the existing encryption methods are at a significant threat. Quantum key distribution(QKD) [5] is a highly active research area in quantum computing. It enables communicating parties to establish secret keys to communicate securely. Quantum Computing provides many benefits to the futuristic world, such as creating life-saving medicines, advancing artificial intelligence, and creating intelligent infrastructure. The recent advancements in quantum computing impose threats to cyber security algorithms. In the literature, many advantages of quantum computing for securing IoT communication based on the BB84 protocol have already been proposed. Many branches of quantum computing for secure IoT communication, such as QKD[6], Quantum entanglement[7], and Quantum Bit Commitment (QBC) protocols[8], have already been explored.

However, as per the authors' knowledge an in detail, Quantum Computing (QC) analysis for securing the IoT communication model considering different attacks on each layer is still unavailable. The main advantage of quantum computing is utilizing quantum superposition, quantum entanglement, Quantum Signature [9] and QKD to deliver secure data and use smart applications for effective decision-making. Therefore, in our work, we analyzed attacks on IoT layered architecture. We also reviewed the benefits of integrating the Quantum-based layer into the existing IoT layer architecture and its future perspective.

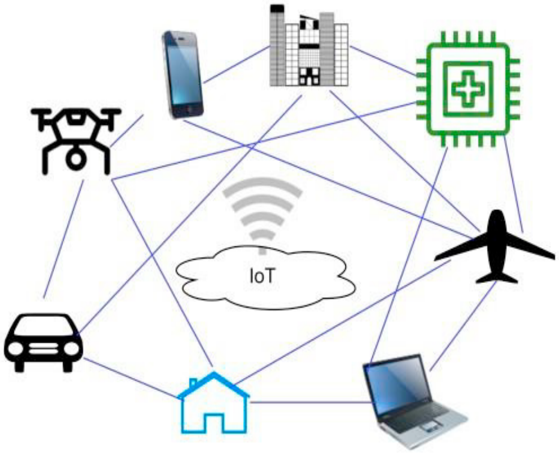
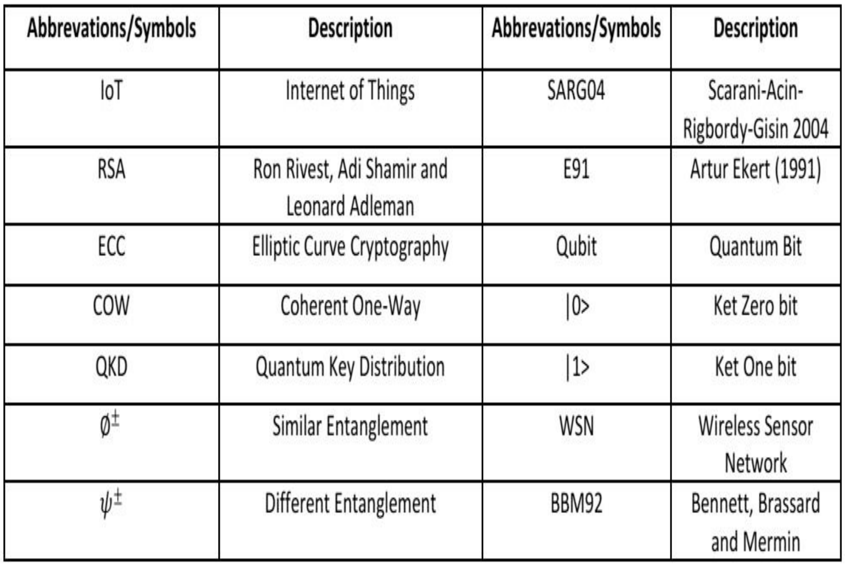


Fig. 1: Futuristic IoT architecture

Our work is organized into sections. Section 2 discusses previous work done on quantum-based communication. Next, in Section 3, IoT security issues and requirements of IoT security are elaborated. The Quantum fundamentals are discussed in Section 4. Quantum key distribution (QKD) is analyzed in section 5. Quantum-based authentication is analyzed in Section 6. In section 7, we discuss quantum-enabled IoT communication. In section 8, we discuss the challenges of IoT communication. Finally, in section 9, we concluded our work. Some of the frequently used abbreviations and symbols are represented in Table 1.

Table 1: List of abbreviations and symbols



Abbrevations/Symbols	Description	Abbrevations/Symbols	Description
IoT	Internet of Things	SARG04	Scarani-Acin-Rigbordy-Gisin 2004
RSA	Ron Rivest, Adi Shamir and Leonard Adleman	E91	Artur Ekert (1991)
ECC	Elliptic Curve Cryptography	Qubit	Quantum Bit
COW	Coherent One-Way	|0>	Ket Zero bit
QKD	Quantum Key Distribution	|1>	Ket One bit
$\emptyset^{\pm}$	Similar Entanglement	WSN	Wireless Sensor Network
$\psi^{\pm}$	Different Entanglement	BBM92	Bennett, Brassard and Mermin

1.1. Contributions

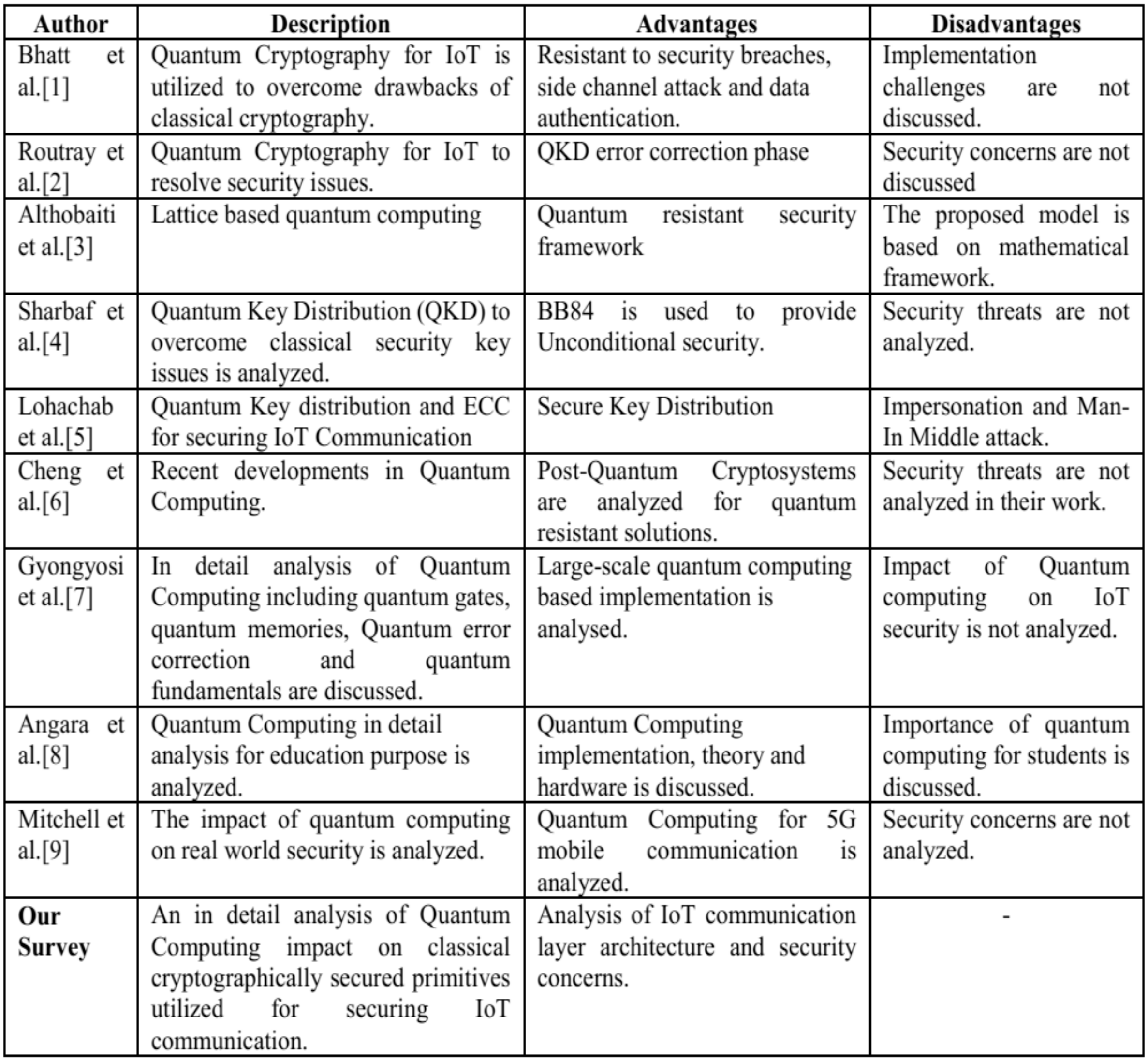
The main contributions of our work are as follows:

1. After understanding the IoT security concerns, a survey on quantum computing for Internet of Things (IoT) smart applications security is analyzed.
2. The main quantum-computing fundamentals and their importance for the security framework are discussed.
3. Thorough analyses of Quantum key security for secure IoT communication are discussed.
4. The main types of Quantum authentication methods and quantum-enabled IoT communication is analyzed.
5. The main challenges for quantum computing-based IoT cryptosystem are provided.

2. Literature survey

In IoT devices, as more devices are connected, enabling security to establish trust among users will become a challenge. Therefore, Hafizul et al.[10]proposed authentication protocol for IoT-enabled Wireless Sensor Networks (WSN). Their work overcomes security threats such as user and sensor node impersonation. IoT devices such as smartphones and wearable are full of sensors and embedded software. All these devices communicated through the internet. Farash et al.[11] proposed authentication protocol where users get data if they pass the authentication and key agreement scheme. Cryptography is used by Mitchell et al.[12] in their work discussed the impact of quantum computers on existing cryptographic primitives. According to Gill et al.[3]quantum advantage can be utilized in different domains such as medicine, cybersecurity, IoT, weather, and national laboratories to solve complex issues such as autonomous cars. Ralegankar et al.[13]work analyse as more data generated and transferred using UAV communication are vulnerable to different attacks such as data modification attacks and snooping attacks. To secure such communication, they proposed the BB84 protocol. Hassija et al.[4] analyses quantum applications for future communication. They also discussed various quantum algorithms such as cryptography, unstructured search, Quantum annealing, and amplitude estimation. Dorothy et al.[14] in their work proposed modified RSA protocol. They utilized BB84 protocols for a secure IoT framework. Rahman et al.[13] introduced quantum layer for adding security in classical IoT layer architecture. In their work, Gupta et al.[14] analyzed QKD and utilized COW protocol[15] to secure IoT communication. Cheng et al.[16]. Their work discusses the impact of quantum-based encryption over classical encryption methods and the requirement of quantum-resistant encryption methods. Yen et al.[17]in their work discuss the role of entanglement in mutual authentication. In their work, EL-Latif et al. [18]addressed the data protection and information sharing issues in network communications. They proposed the Quantum One-Way Hash Function (QOWHF) to resolve current and future communication frameworks. Most of the work on Quantum computing for securing IoT-enabled communication has been done in literature by many existing authors, as represented in Table: 2

Table 2: Existing work done by authors on quantum-enabled IoT security



Author	**Description**	**Advantages**	**Disadvantages**
Bhatt et al.[1]	Quantum Cryptography for IoT is utilized to overcome drawbacks of classical cryptography.	Resistant to security breaches, side channel attack and data authentication.	Implementation challenges are not discussed.
Routray et al.[2]	Quantum Cryptography for IoT to resolve security issues.	QKD error correction phase	Security concerns are not discussed
Althobaiti et al.[3]	Lattice based quantum computing	Quantum resistant security framework	The proposed model is based on mathematical framework.
Sharbaf et al.[4]	Quantum Key Distribution (QKD) to overcome classical security key issues is analyzed.	BB84 is used to provide Unconditional security.	Security threats are not analyzed.
Lohachab et al.[5]	Quantum Key distribution and ECC for securing IoT Communication	Secure Key Distribution	Impersonation and Man-In Middle attack.
Cheng et al.[6]	Recent developments in Quantum Computing.	Post-Quantum Cryptosystems are analyzed for quantum resistant solutions.	Security threats are not analyzed in their work.
Gyongyosi et al.[7]	In detail analysis of Quantum Computing including quantum gates, quantum memories, Quantum error correction and quantum fundamentals are discussed.	Large-scale quantum computing based implementation is analysed.	Impact of Quantum computing on IoT security is not analyzed.
Angara et al.[8]	Quantum Computing in detail analysis for education purpose is analyzed.	Quantum Computing implementation, theory and hardware is discussed.	Importance of quantum computing for students is discussed.
Mitchell et al.[9]	The impact of quantum computing on real world security is analyzed.	Quantum Computing for 5G mobile communication is analyzed.	Security concerns are not analyzed.
Our Survey	An in detail analysis of Quantum Computing impact on classical cryptographically secured primitives utilized for securing IoT communication.	Analysis of IoT communication layer architecture and security concerns.	-

3. IoT Security Issues

Innovative applications such as intelligent cities, smart agriculture, and innovative health care enabled the advancement of IoT-enabled communication. The IoT devices that support these applications transmit vast amounts of data in many different environments. The advancement in IoT applications increases cyber-attacks. It also poses threats to user privacy and confidentiality. The main security challenges concerning the IoT environment are authentication, integrity, authorization and trust management. Major security concerns encountered in IoT layered architecture[18], as represented in Figure 2. This section review threats to IoT layer architecture and the benefits of introducing the Quantum layer for IoT security.

3.1. Sensing Layer

Various sensing technologies enable IoT applications such as WSN, RFID, and GPS in this layer. All these technologies deal with IoT sensors and actuators. Sensors are used for perceiving data from surroundings, such as ultrasonic, camera, and temperature detection. Many attacks on this sensing layer are possible such as sensor node capturing, false data code injection, eavesdropping, and sleep deprivation attacks.

3.2. Network Layer

Computational units must process the data received from the lower (sensor) layer. The function of the network layer is to send the information acquired from the sensor layer to processing units. The processed data is required to enable IoT applications. However, due to open internet connectivity, network layers face serious security threats such as access control attacks, Denial of service attacks, attacks during data transient, etc.

3.3. Quantum Layer

The Quantum layer provides security to IoT applications. It includes secure key distribution. Due to quantum mechanics laws, the privacy and security of keys are guaranteed at this layer. However, this layer enabled quantum-based cryptography, which will suffer from security threats such as individual, collective and coherent attacks.

3.4. Application Layer

The application layer is accountable for providing services to the user for decision-making. The critical IoT applications are smart cities, intelligent environments, and competent health care and intelligent grids. IoT heterogeneous applications have severe issues of privacy, confidentiality and authentication of data. Eavesdropping attacks, access control, service interruption attack and malicious code attack are the major issues at the application layer.

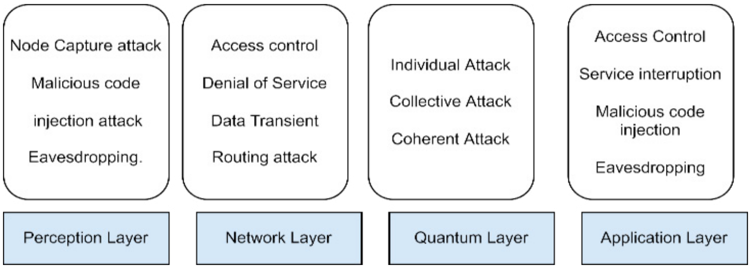


Fig. 2: Security threats on IoT layer architecture.

4. Quantum Fundamentals

The basic building block of Quantum computing is shown in figure 3, consisting of Quantum physical building blocks, Quantum Logic gates and a Quantum programming environment.

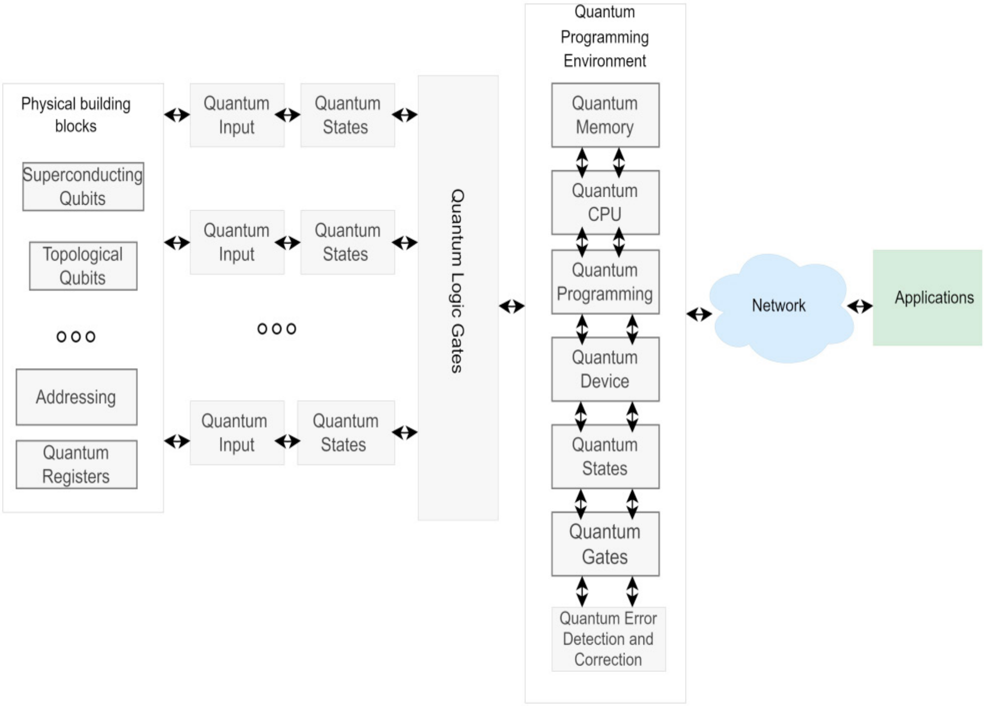


Fig.3: Architecture of Quantum Computing

4.1. From Classical bits to Quantum Bits

In classical computing, we use bits to process information; however, we use Quantum bits known as qubits in quantum computing. These qubits behave according to the laws of quantum mechanics. The quantum particles in spin up and downstate are written as$|0>$ *and* $|1>$. The group of n qubits store up to 2^n valid values with individual probability measuring each value.

4.2. Quantum Superposition

The qubits are in the linear combination of both $|0>$ *and* $|1>$, known as quantum superposition. A system can be in superposition[19] of all possible states simultaneously without being confined to one particular state. However, measurement collapses the superposition. It makes qubits to be measured in one of the qubit values$|0>$ *or* $|1>$.

5. Quantum Key Distribution

Quantum computers bring a huge risk to classical secret key structures. The initial target of quantum computers is asymmetric key structures. Therefore, quantum-based keys need to be utilized for a secure IoT communication framework. The foundation of the quantum key depends on quantum mechanics [16]. The method is based on sharing a secure key between communicating entities. The BB84[14], BBM92[20], SARG04[6] and E91[20] are secure quantum key distribution protocols. The QKD aims to securely distribute and transmit keys using quantum and classical channels. The concept of key distribution is based on sharing random bits using a random basis, which is sent to the receiver. The laws of quantum mechanics reduce the amount of information extracted from the quantum system.

6. Quantum Authentication

The identity authentication for verifying the integrity and confidentiality of messages ensures the security of the message. Mutual authentication between two entities ensures non-repudiation, integrity, and verification of messages. Quantum-based identity authentication can be achieved by using Quantum Signature and Entanglement.

6.1. Quantum Entanglement

The counterintuitive feature of quantum communication is quantum entanglement. When two particles are entangled, their states have to be defined concerning each other. The entangled states are also referred to as Bell states [19]. Four mutually orthonormal entangled states are expressed as in equations (1) and (2)[21]:

$$\emptyset^{\pm} = \frac{1}{\sqrt{2}}(|00> \pm |11>) \tag{1}$$

$$\psi^{\pm} = \frac{1}{\sqrt{2}}(|01> \pm |10>) \tag{2}$$

6.2. Quantum Signature

Quantum signatures are used to verify the authenticated user. Different kinds of Quantum signature protocols exist, such as Arbitrated quantum signature (AQS), Quantum blind signature (QBS) and quantum group signature[22]. A Quantum signature based on the Quantum walk has also been proposed. Quantum signatures are useful for applications such as Quantum Cheque[23], which ensure Non-repudiation and user impersonation attack.

7. Quantum-enabled Internet of Things (IoT)

IoT framework is an interconnection of heterogeneous devices interconnected with diverse technologies such as Wifi, Bluetooth, Zigbee, Bluetooth, and 6LOWPAN. These are IoT enabling technologies. These technologies enable data transfer in IoT applications such as smart cities, innovative medical infrastructure and intelligent farming. These applications require data privacy and confidentiality; therefore, IoT integration with quantum computing plays a significant role. The IoT communication infrastructure is secured by classical cryptography, such as Public and Private-key structures[24]are soon under attack by quantum computers. Quantum base shor's[25] and Grover's [26] algorithm already pose a threat theoretically to Public-key based infrastructure.

Security of sensitive information in IoT communication is required since the devices involved in IoT communication are resource-constrained and secure, lightweight cryptography is essential. In addition to that, the need to handle classical and quantum attacks opens the door toward quantum-resistant cryptography[27]. In future, IoT communication Quantum computing will become essential for secure communication. Figure: 4 show the comparison of existing quantum-based schemes analyzed by researchers.

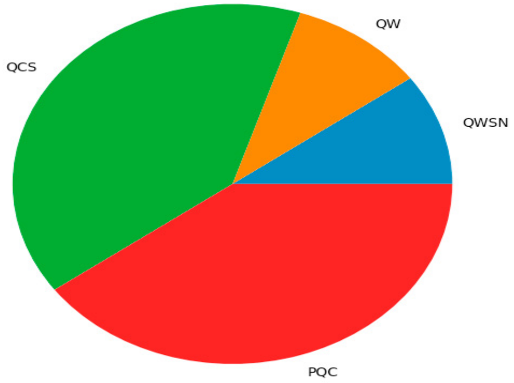


Fig. 4: Comparative analysis of existing quantum-based schemes [Quantum Computing Schemes (QCS), Quantum Walk (QW), Post Quantum Cryptography (PQC), Quantum wireless sensor Networks (QWSN)]

8. Challenges of Quantum based IoT

8.1. Quantum key distribution

It provides a secure way of communicating keys. However, suppose the presence of an eavesdropper was detected on the quantum channel. In that case, the entire process is discarded, and communication will not start again until no eavesdropping is found on the channel.

8.2. Short Distance Communication

The communication of mass users of IoT communication using the quantum channel is challenging due to the short-distance communication of QKD.

8.3. Quantum Reversible Computing

The quantum-based reversible computing[28] also poses a significant threat in the presence of eve.

8.4. Security Attack

The individual attack on quantum-based communication is also possible. In this, the attacker creates a new quantum channel by intercepting a quantum signal transmitted between Alice and Bob.

9. Conclusion

IoT is the interconnection of many heterogeneous devices as all devices are interconnected and provide many benefits to users to facilitate decision-making. Such technology, which contains our daily critical information in health care, intelligent cities and even military applications, must be secure. There are many classical cryptographic primitives, which provide secure communication based on complex mathematical structures. The security based on classical cryptographic structures is no longer secure due to quantum computing attacks. Therefore, IoT-enabled communication requires quantum-based security to resist futuristic quantum attacks. In our survey, we analyzed quantum-based cryptographically secured structures for IoT communication. This article provides a thorough survey of security attacks on IoT-based applications, quantum-resistant solutions for securing IoT communication, the quantum authentication methods, QKD and challenges in implementing quantum-enabled IoT communication. As a result of such a contribution, this article provides useful guidelines for future IoT researchers to consider more quantum-resistant solutions.

References

[1] M.A. Ferrag, L.A. Maglaras, H. Janicke, J. Jiang, L. Shu, Authentication Protocols for Internet of Things: A Comprehensive Survey, Secur. Commun. Networks. 2017 (2017). https://doi.org/10.1155/2017/6562953.

[2] A. Lohachab, Using Quantum Key Distribution and ECC for Secure Inter-Device Authentication and Communication in IoT Infrastructure, SSRN Electron. J. (2018). https://doi.org/10.2139/ssrn.3166511.

[3] S.S. Gill, A. Kumar, H. Singh, M. Singh, K. Kaur, M. Usman, R. Buyya, Quantum computing: A taxonomy, systematic review and future directions, Softw. - Pract. Exp. 52 (2022) 66–114. https://doi.org/10.1002/spe.3039.

[4] V. Hassija, V. Chamola, A. Goyal, S.S. Kanhere, N. Guizani, Forthcoming applications of quantum computing : peeking into the future, 1 (2020) 35–41. https://doi.org/10.1049/iet-qtc.2020.0026.

[5] S. Krithika, T. Kesavmurthy, Securing IOT network through quantum key distribution, Int. J. Innov. Technol. Explor. Eng. 8 (2019) 693–696. https://doi.org/10.35940/ijitee.F1141.0486S419.

[6] J. Ahmed, A.K. Garg, M. Singh, S. Bansal, M. Amir, Quantum Cryptography Implementation in Wireless Networks, 3 (2014) 129–133.

[7] S.T. Cheng, C.Y. Wang, M.H. Tao, Quantum communication for wireless wide-area networks, IEEE J. Sel. Areas Commun. 23 (2005) 1424–1432. https://doi.org/10.1109/JSAC.2005.851157.

[8] A. Broadbent, C. Schaffner, Quantum cryptography beyond quantum key distribution, Springer US, 2016. https://doi.org/10.1007/s10623-015-0157-4.

[9] S.R. Moulick, P.K. Panigrahi, Quantum cheques, Quantum Inf. Process. 15 (2016) 2475–2486. https://doi.org/10.1007/s11128-016-1273-4.

[10] SK. Hafizul, I. Prosanta, Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks, (2017).

[11] M.S. Farash, M. Turkanović, S. Kumari, M. Hölbl, An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment, Ad Hoc Networks. 36 (2016) 152–176. https://doi.org/10.1016/j.adhoc.2015.05.014.

[12] C.J. Mitchell, The impact of quantum computing on real-world security: A 5G case study, Comput. Secur. 93 (2020) 1–11. https://doi.org/10.1016/j.cose.2020.101825.

[13] V.K. Ralegankar, J. Bagul, B. Thakkar, R. Gupta, S. Tanwar, G. Sharma, I.E. Davidson, Quantum Cryptography-as-a-Service for Secure UAV Communication: Applications, Challenges, and Case Study, IEEE Access. (2021) 1–1. https://doi.org/10.1109/access.2021.3138753.

[14] A.B. Dorothy, S.B.R. Kumar, An approach for IoT security using quantum key distribution, Int. J. Sci. Technol. Res. 8 (2019) 1569–1574.

[15] S. Gupta, C. Dutta, Internet of Things Security Analysis of Networks using Quantum Key Distribution, Indian J. Sci. Technol. 9 (2016). https://doi.org/10.17485/ijst/2016/v9i48/105551.

[16] C. Cheng, R. Lu, A. Petzoldt, T. Takagi, Securing the Internet of Things in a Quantum World, IEEE Commun. Mag. 55 (2017) 116–120. https://doi.org/10.1109/MCOM.2017.1600522CM.

[17] C.A. Yen, S.J. Horng, H.S. Goan, T.W. Kao, Y.H. Chou, Quantum direct communication with mutual authentication, Quantum Inf. Comput. 9 (2009) 376–394. https://doi.org/10.26421/QIC9.5-6-2.

[18] M.S. Rahman, M. Hossam-E-Haider, Quantum IoT: A quantum approach in IoT security maintenance, 1st Int. Conf. Robot. Electr. Signal Process. Tech. ICREST 2019. (2019) 269–272. https://doi.org/10.1109/ICREST.2019.8644342.

[19] D.J. Egger, C. Gambella, J. Marecek, S. McFaddin, M. Mevissen, R. Raymond, A. Simonetto, S. Woerner, E. Yndurain, Quantum Computing for Finance: State-of-the-Art and Future Prospects, IEEE Trans. Quantum Eng. 1 (2021) 1–24. https://doi.org/10.1109/tqe.2020.3030314.

[20] N. Papanikolaou, An introduction to quantum cryptography, XRDS Crossroads, ACM Mag. Students. 11 (2005) 3–3. https://doi.org/10.1145/1144396.1144399.

[21] M.S. Kang, C.H. Hong, J. Heo, J.I. Lim, H.J. Yang, Controlled mutual quantum entity authentication using entanglement swapping, Chinese Phys. B. 24 (2015). https://doi.org/10.1088/1674-1056/24/9/090306.

[22] L. Jian, L. Na, Z. Yu, W. Shuang, D. Wei, C. Wei, M. Wenping, A survey on quantum cryptography, Chinese J. Electron. 27 (2018) 223–228. https://doi.org/10.1049/cje.2018.01.017.

[23] BK. Behera, A. Banerjee, P.K. Panigrahi, Experimental realization of quantum cheque using a five-qubit quantum computer, Quantum Inf. Process. 16 (2017) 1–12. https://doi.org/10.1007/s11128-017-1762-0.

[24] V. Teja, P. Banerjee, N.N. Sharma, R.K. Mittal, Quantum cryptography: State-of-art, challenges and future perspectives, 2007 7th IEEE Int. Conf. Nanotechnol. - IEEE-NANO 2007, Proc. (2007) 1296–1301. https://doi.org/10.1109/NANO.2007.4601420.

[25] A.I. Nurhadi, N.R. Syambas, Quantum Key Distribution (QKD) Protocols: A Survey, Proceeding 2018 4th Int. Conf. Wirel. Telemat. ICWT 2018. (2018) 1–5. https://doi.org/10.1109/ICWT.2018.8527822.

[26] R. Niederhagen, S. Css, P. Michael, W. Fraunhofer, D. Fraunhofer, S. Information, T. Sit, Practical Post-Quantum Cryptography White Paper Practical Post-Quantum Cryptography, (n.d.).

[27] SK. Routray, M.K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, S. Sarkar, Quantum cryptography for IoT: APerspective, IEEE Int. Conf. IoT Its Appl. ICIOT 2017. (2017). https://doi.org/10.1109/ICIOTA.2017.8073638.

[28] AG Aruna, KH Vani, C. Sathya, RS Meena, A Study on Reversible Logic Gates of Quantum Computing, 7 (2016) 427–432.