Turkish Journal of Computer and Mathematics Education *Vol.12 No.2 (2021), 450- 455*

Research Article

A Contemporary Study on Quantum-Computing Security Mechanisms in 5G Networks

Rydhm Beri[a], Rajwant kaur[b] and Kawaljit Kaur[c]

A Assistant Professor, University Institute of Computing, Chandigarh University
B Assistant Professor, University Institute of Computing, Chandigarh University
C Assistant Professor, University Institute of Computing, Chandigarh University

Article History: Received: 11 January 2021; Accepted: 27 February 2021; Published online: 5 April 2021

Abstract: 5G communication technology works with the integration of several technologies viz. Cloud Computing, network partitioning and software based networks. This integration allows the communication between thousands of device across the world which have enormous issues related to data protection, data authenticity, and data confidentiality. So, there is an immense need of secure protocols to face or resolve security related issues related to design and operation of 5G network. Moreover, some structured cryptography protocols required to develop and accomplish data security in 5G communication. The study focussing on the comprehensive consequences of quantum computing on security implementations of 5G mobile communications. The study discussing about the cryptographic algorithm used in 5G, and what are the various consequences of involvement of quantum computing.

Keywords: Cryptography, 5G Technology, Post Quantum, Quantum Computer

1. Introduction

Quantum computing is the contemporary research area which is applied in many fields to enhance security. Quantum computing highly influence the field of cryptography. It is still unknown that whether the enormous scope, general purpose quantum computer ever built as a complete system or not. Dyakonov[1], in his study discussed the basic difference between traditional computers and quantum computers and discussed that sustained endeavour is going on to develop quantum computers. Moreover, when these computers obtained that will include lots of security mechanism of modern cryptographic systems. It is always advisable, while designing an extensive cryptographic system there is a need to investigate the quantum computing which is to be included in the system. The main focus of the study is to discuss the part of endangered with the availability of quantum computer, and the various consequences occur when system security is broken. The study also focussing on the methodology to replace cryptography implemented in every part of the system. This might include the timeline necessary for specification update, or the time necessary for production alternative existing implementation. In application area the cumulative time for all these is considered. For instance the debit or credit cards having life duration of three-five years, and replacement of all these existing technologies with modern technology need a period of 10 years or more. Moreover, there is time required to replace infrastructure in which these modern cards can be used.

Mobile communication is the major area implementing cryptography techniques since the development of GSM system. GSM mainly considered as a 2G mobile communication technology. Mobile communication changes transmission capability and speed every year with the passage of time and generation. 5G is the modern way of mobile communication which is using across the world. As 5G is being used by different numerous people, it is required to implement security mechanisms to it so that safe transmission of data can offer to the client. Many reviews and investments are applied onto this technology and many more would apply.

Conventional Cryptography

Gilbert S Vernam in 1917, designed a machine known as one-time pad, for virtually producing non-repeating character sequence. Conventionally, the unique key was created similar to that of the message length for securing message. The key was discarded after every communication. Claude Shannon developed information theoretic secrecy basis in which the length of cryptographic key utilized for message encoding is having same length cryptographic key. Brnnet & Brassard[1] in 1984, proposed quantum cryptography first time which was dependent on No-Cloning theorem which implies that the security based on laws of physics .

Old style cryptography utilizes a few scientific methods to confine busybodies from knowing the substance of encoded messages. The most mainstream among them that are received globally have been portrayed underneath. In the present study we depict transmitter as ‘Alice’, the receiver of the message is depicted as ‘Bob’ and eavesdropper is depicted as ‘Eve’.

1.1.1 DES(Data Encryption Standard)

It was developed by IBM for data encryption. It was based on Lucifer and is the popular encryption standard used to encrypt data. DES[4], is the public key cryptographic technique in which the security of the data depends upon the secrecy of the key which consists of random string of large bits. The output bits of the algorithm does not

appear similar to that of input bits. Once the message is encrypted with the key, it will send to the receiver onto the public channel which might be vulnerable to eavesdropping attack. It is advisable to share the secret key information only over the very secure communication channel. The generated key firstly sent over the channel followed by the message. The major drawback of DES is it does not guarantee the complete security of the message.

1.1.2 Public Key Encryption

The previous encryption method involve in generation of separate key for every user which is a difficult task as number of keys increases with the increase in number of users. This is so because k users require k×(k-1)/2 number of keys and need to track the specific key of the specific user to whom he wants to communicate. Public key encryption method resolve this issue of generation multiple keys. Public key encryption also termed as asymmetric way to encrypt message as in this case user have to maintain only two keys i.e. a private key or a public key to encrypt or decrypt the message. The private key used by the sender of the message to encrypt it. The sender is free to announce public key as it partially involves in the process of encryption and decryption [48]. The receiver decrypt the message by combination of public and private key. Sender sends the message after encrypting with the public key and receiver decrypts the message with private key. This process also restricts sender to decrypt his own message. These methodologies are proved to be some mathematical operations are simpler to solve at one end not the other. As an example if someone wants to multiply two large prime numbers it proves easy as compared to finding the factors of the obtained results if sufficient resources are not available. First PKC i.e. RSA obtained the security mechanism from the fact that factorizing large numbers is very difficult to obtain. The major drawback of the conventional cryptographic techniques is the unavailability of the technique to detect eavesdropping.

1.1.3 One Time Pad Cryptosystem

This technique was evolved by Gilbert Vernam in 1917 and offers simple and effective solution to security. It is considered as the good cipher technique which ensures the accurate secrecy of the message. This cryptographic technique is based on sporadic keys set which can be written on paper sheets integrated to a pad. At receiving end receiver needs the pad similar to the sender end available for encryption and decryption purpose. The security mechanism implemented by OTP is inappropriate. The participants of the communication have to share the encoded message alongwith the secret key of same length. The key used to encrypt or decrypt the message can be utilized only once. This can be possible with the proper synchronized communication between sender and the receiver.

1.1.4 Quantum Cryptography:

The communication channel which implements quantum computing needs a pair of polarizing filter at both ends of the communication. For instance, the photographs at sender end can send by specific polarization so that it can be compared at the receiving end. Polarization filters can be implemented in rectilinear (vertical or horizontal orientation) or diagonal (45 and 135 degree orientation) of photons. Calcite crystal or two photomultiplier detectors capable to detect these two directions. In the event that the photon is on a level plane captivated it will be coordinated to upper channel and to vertical finder in the event that it is vertically energized. In the event that comparative contraption is turned at 45 it will record inclining bearings. Accordingly the turned contraption is futile for rectilinear bearing and vertical device for askew heading .henceforth we cannot quantify both at the same time consequently confirming Heisenberg vulnerability principle.BB84 Protocol was created by Charles H, Bennett of the IBM Thomas J. Watson Research Center and Gilles Brassard of the University of Montreal, quantum cryptography depends on the way that estimating a quantum framework, for example, a photon irreversibly changes its state and clears out data about the angles before estimation [1].

2. Quantum Computing effect on cryptography

2.1 Cryptanalysis

Yanofsky & Mannucci[2], suggest there will be a consequential impact on cryptography with the development of general-purpose highly-scalable quantum computer. Specifically, quantum algorithms are designed that affect both symmetric and asymmetric key cryptography algorithms. Shor [3], proposed an algorithm which affect asymmetric algorithm which is widely used even till now to maintain security. Alternatively Grover [4], proposed an algorithm which create lesser impact on security implementation of symmetric algorithm. Following are some points discussing the consequences of these algorithms on quantum computer which implemented them.

As per the contemporary key length, the problem of large calculations or computation of discrete logarithms is found to be insecure in the case of asymmetric cryptography techniques. Accordingly, the asymmetric techniques conceivably partitioned with the help of huge general-purpose quantum systems. Besides this, the increment in length of the key leads to secure current utilized techniques and will prove as good instead of using the algorithm infeasible to implement in many cases.

The key length of symmetric cryptography algorithms is apparently diminished. In case of quantum computer n-bits in a key of symmetric algorithm offers 2n/2 calculations where as in case of tradition computer systems the order was 2k. Moreover, in the case of quantum computing the calculations might be complex. Additionally, quantum attacks behave differently as compared with the traditional computer's attack like brute force. As per the traditional practices, it is unpredictable to find the quantum attacks complexity. As in the case of quantum computer 128-bit key provide same security level as that of 64-bit key which is quite low.

2.2 Security Consequences

It is intriguing to predict the future effect insecurity of cryptographic algorithms as in current use are rendered uncertain sooner or later. The algorithms that verifies the data integration and is valid for long-term, no consequential problems possible to identify until some new more secure algorithm developed till that time period. It is unsecure to store encrypted text(cyphertext) as when the some intruder crack encryption algorithm, the text can easily be decrypted to the original text(plaintext). Quantum computers has the capability to break the encryption algorithms, as its use made the existing encryption algorithms vulnerable. For instance if some data is encrypted using a key establishment technique and then the data travelled via unsecure communication channel, puts the data and key into risk by the availability of quantum computer.

2.3 Replacement Algorithms

As per the increase demand of security now a days, several organizations working together to design cryptographic standards which are better than previous. The security improvement in cryptographic field is possible only with the increase in key bits. Currently in symmetric key encryption 256-bit key is allowed used to encrypt data and is considered as powerful key. Although in case of asymmetric key encryption most of the algorithms are considered as insecure. Numerous organizations including ETSI, NIST, ISO/IEC working on the development of asymmetric key cryptography to secure data in the post-quantum era. Currently NIST organization built the effective Post-Quantum cryptography standard to secure data with asymmetric key cryptography [23].

In 2017, November, NIST commenced a procedure to engage, estimate and regulate different quantum-resistant asymmetric-key cryptography. In this procedure the primary stage requested public suggestions on minimum applicable requirements, submission specification, and estimation criteria for candidate algorithms. NIST revert back to these suggestions with the summary of the changes made to the algorithm standard. NIST received huge proposals for new algorithms, which it adopted according to the series of rounds as per the public suggestions and cryptanalysis.

3. Introduction to 5G Security

As compared with the growth of 4G networks, it was expected that 5G network will offer high QoS(Quality of Serives)[24]. It is visualized that 5G communication technology will offer high network bandwidth with reliable and fault tolerance capabilities to the users. IoT(Internet of Things) comes with the integration of 5G technology [25-35], with the connection capability of anything, anyplace, anytime, any communication technology or any services.

The use of Internet of Things (IoT) is growing rapidly and offers several solutions to every field. Some reports discussed that approximate to year 2020 there will be 75 billion IoT devices utilize among the humans across the world [11]. This gigantic growth needs some standard protocols and device architecture for service provisioning to IoT based devices. IoT device usually operates on battery and has limited computational capabilities with lesser storage capability. So, these devices are mainly responsible to capture real-time data and the processing as well as storage of the data is done possibly at some cloud server or fog server. As the data processing and storage is done on servers instead of IoT devices there is a need to implement security mechanisms onto the data so as to maintain security and relatability of obtained data. Some of the techniques to implement security on IoT devices includes, asymmetric cryptography (public key cryptography), symmetric cryptography (private key cryptography), and hash functions. Among these, public key cryptography is widely used in Internet based communication as it offers huge security mechanisms to email clients [12], websites [13], E-signature documents[14], E-Transactions[15], medical data[16], Enterprise Communication[17] and so on. Some of the algorithms of public key cryptography like ECC[19][20], RSA[18], DH[21] gain more popularity and even are the part of Internet standard such as Transport Layer Security(TLS).

IoT networks includes the capability to interconnect with sensors, service providers, applications with the help of its integration with 5G networks. Mainly the 5G networks allows the integration of several networking technologies like, SDN, NFV, network slicing, cloud computing and so forth. These sort of integration leads to the development of security and privacy concerns to the 5G network. So, there is an intensive need to design secure network architectures for 5G networks to reduce security and privacy issues of the network [36-39]. The security mechanisms in 5G networks can be easily implemented with the use of quantum walks hash functions.

4. Post-Quantum Cryptography

This section is going to discuss various Post-Quantum Cryptography (PQC) and ciphers which increase the reliability of 5G communication network.

4.1 Quantum Impact on Cryptography

Shor[3], proposed an algorithm in 1994 which offers the efficient way to factor huge prime numbers on quantum computer reduces the security of RSA. Expansions discuss the trends to be utilized to beat discrete algorithms issues and subvert ECC ciphers. In 1996, Grover [8] proposed the symmetric key ciphers like AES can be exploited through quantum data structure.

Cipher	Key Size	Classical	Quantum
RSA	1024	80	0
RSA	2048	112	0
ECC	256	128	0

ECC	384	256	0
AES	128	128	64
AES	256	256	128

Table1: Difference between classical ciphers and quantum ciphers

Table 1 sums up some common ciphers, their comparable symmetric key quality utilizing classical algorithms and quantum ciphers [40].

4.2 Post-Quantum Ciphers (PQC)

PQC is having different components from the classical public key cryptography. In PQC no key agreement is available which works on the principle of Diffie-Hellman algorithm. So, there is no requirement of 1:1 correspondence of tradition ciphers to the PQC domain. This section discusses some of the PQC categories used to encrypt the data.

4.2.1 Lattice Cryptography:

Lattice is referred to the all integer set which is arranged as a linear group of basis vector set. The main problem in mathematics is the shortest vector problem which is used to observe non-zero vectors from the vector space which traverse with basis vector. Lattice cryptography is considered NP-hard type problem. NTRU(Nth Degree Truncated Polynomial Ring) is the most popular lattice based cryptography which is an open source and comes under the category of public key encryption techniques. NTRU have the features of encryption as well as signature formulation. Encryption task is performed using NTRUEncrypt algorithm while signature formulation is handled using NTRUSign algorithm. It performs the operation within the area of truncated polynomial ring. Moreover, its security not only based on the complexity of discrete log type problem solving, but also to cracking this technique is similar to solve shortest vector lattice problem. Although it is not completely implemented mathematically using lattice, but its security proof is similar as that of solution obtained from shorted vector problem. Hoffstein & Silverman [41], in their study proposed the technique NTRU in and this techniques undergoes several studies. All this way lots of issues identified in this and resolved over the years. There are several other techniques available which works on different principle and offers several benefits. The other techniques includes, GGH(Goldreich-Goldwasser-Halevi)[42], is based on closest vector problem while recent algorithm Bimodal lattice signature scheme(BLISS) is a message authenticity technique to identify the person who sent the data. Of these methodologies, a refreshed rendition of NTRU has been endorsed as IEEE Standard 1363.1 and ANSI standard X9.98.

4.2.2. Hash-Based Cryptography:

The ongoing danger of blockchain innovation has restored center around hash-based cryptography. In light of the Merkle has trees, this methodology can be utilized as an option in contrast to customary computerized marks. The eXtended Merkle Signature Scheme (XMSS) has been distributed as an instructive record by the IETF as RFC 8391.

4.2.3 Code-Based Cryptography.

Code-put together cryptography is based with respect to the trouble of interpreting a general straight code. The McEliece plot was presented in 1978 and depends on registering arbitrary straight changes of a mistake adjusting code's generator network, and just the private key holder knowing the variables of that framework [44]. The figure has been suggested for thought in a PQC domain, yet requires amazingly long key lengths [45]. There are a couple of other code-based plans, outstandingly Niederreiter's methodology that additionally bolsters computerized marks.

4.**2.4 Supersingular Elliptic Curve Isogeny Cryptography.**

While the figures examined so far offer reciprocals to encryption and mark conspires, a key understanding convention with forward mystery is prominently inadequate. In 2012, analysts demonstrated that supersingular elliptic bends and supersingular isogeny diagrams can be utilized to make a post-quantum Diffie-Hellman-type figure, yet these methodologies remain moderately beginning and unstudied in scholastic writing.

5. Conclusion

The primary component of 5G systems is that they will play a focal job in our day by day life. Besides, as they use many promising correspondence advancements and will bolster a colossal number of associated gadgets this will without a doubt bring huge difficulties for the trust, security and protection. In this manner, secure instruments also, conventions are required as the reason for 5G systems to address this issue and follow security-by-plan yet in addition security-by- activities rules. Enlivened by the confinements of the old style cryptosystems and the upsides of quantum strolls, in this paper we compares new developments of cryptosystems to accomplish secure data sharing and information assurance which are based on quantum advances. To begin with, two the study discussed post quantum cryptography and cryptographic ciphers instruments for 5G applications dependent on QWs, in particular. At that point, in view of the two hash work proposition, two productive security conventions for making sure about the information in 5G systems situation have been presented. Directed execution investigations and reenactment results demonstrated that the proposed approaches are portrayed with high security, proficiency, and heartiness against a few notable assaults which make them reasonable for use inside different 5G applications.

References

1. Abd EL-Latif, A. A., Abd-El-Atty, B., Venegas-Andraca, S. E., & Mazurczyk, W. (2019). Efficient quantum-based security protocols for information sharing and data protection in 5G networks. Future Generation Computer Systems, 100, 893-906.
2. Ahmed, S. H., & Rani, S. (2018). A hybrid approach, Smart Street use case and future aspects for Internet of Things in smart cities. Future Generation Computer Systems, 79, 941-951.
3. Al-Turjman, F. (2019). 5G-enabled devices and smart-spaces in social-IoT: an overview. Future Generation Computer Systems, 92, 732-744.
4. Arapinis, M., Mancini, L., Ritter, E., Ryan, M., Golde, N., Redon, K., & Borgaonkar, R. (2012, October). New privacy issues in mobile telephony: fix and verification. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 205-216).
5. Arkko, J., & Haverinen, H. (2006). Extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA). RFC 4187, January.
6. Arkko, J., Lehtovirta, V., & Eronen, P. (2009). Improved extensible authentication protocol method for 3rd generation authentication and key agreement (EAP-AKA'). Network Working Group Request for Comments, 5448, 1-29.
7. Baldi, M., Santini, P., & Cancellieri, G. (2017, September). Post-quantum cryptography based on codes: State of the art and open challenges. In 2017 AEIT International Annual Conference (pp. 1-6). IEEE.
8. Bello, O., & Zeadally, S. (2019). Toward efficient smartification of the Internet of Things (IoT) services. Future Generation Computer Systems, 92, 663-673.
9. C. H. Tseng, S. Wang and W. Tsaur, "Hierarchical and Dynamic Elliptic Curve Cryptosystem Based Self-Certified Public Key Scheme for Medical Data Protection," in IEEE Transactions on Reliability, vol. 64, no. 3, pp. 1078-1085, Sept. 2015.
10. C. K. Williams, "Configuring enterprise public key infrastructures to permit integrated deployment of signature, encryption and access control systems," MILCOM 2005 - 2005 IEEE Military Communications Conference, Atlantic City, NJ, 2005, pp. 2172-2175 Vol. 4.
11. Chaudhary, R., Kumar, N., & Zeadally, S. (2017). Network service chaining in fog and cloud computing for the 5G environment: Data management and security challenges. IEEE Communications Magazine, 55(11), 114-122.
12. Cheng, C., Lu, R., Petzoldt, A., & Takagi, T. (2017). Securing the Internet of Things in a quantum world. IEEE Communications Magazine, 55(2), 116-120.
13. Daniel, A., & Lejla, B. (2015). Initial recommendations of long-term secure post-quantum systems. (PDF). PQCRYPTO.
14. Dao, N. N., Park, M., Kim, J., Paek, J., & Cho, S. (2019). Resource-aware relay selection for inter-cell interference avoidance in 5G heterogeneous network for Internet of Things systems. Future Generation Computer Systems, 93, 877-887.
15. Ducas, L., Durmus, A., Lepoint, T., & Lyubashevsky, V. (2013, August). Lattice signatures and bimodal Gaussians. In Annual Cryptology Conference (pp. 40-56). Springer, Berlin, Heidelberg.
16. Fan, K., Gong, Y., Du, Z., Li, H., & Yang, Y. (2015, August). RFID secure application revocation for IoT in 5G. In 2015 IEEE Trustcom/BigDataSE/ISPA (Vol. 1, pp. 175-181). IEEE.
17. Fan, K., Gong, Y., Liang, C., Li, H., & Yang, Y. (2016). Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G. Security and Communication Networks, 9(16), 3095-3104.
18. Fan, K., Song, P., & Yang, Y. (2017). ULMAP: Ultralightweight NFC mutual authentication protocol with pseudonyms in the tag for IoT in 5G. Mobile Information Systems, 2017.
19. Goldreich, O., Goldwasser, S., & Halevi, S. (1997, August). Public-key cryptosystems from lattice reduction problems. In Annual International Cryptology Conference (pp. 112-131). Springer, Berlin, Heidelberg.
20. Grover, L. K. (1996, July). A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing (pp. 212-219).
21. Grover, L. K. (1997). Quantum mechanics helps in searching for a needle in a haystack. Physical review letters, 79(2), 325.
22. Hoffstein, J., Pipher, J., & Silverman, J. H. (1998, June). NTRU: A ring-based public key cryptosystem. In International Algorithmic Number Theory Symposium (pp. 267-288). Springer, Berlin, Heidelberg.
23. IoT: number of connected devices worldwide 2012-2025 | Statista. (2020). Retrieved 30 April 2020, from https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
24. Jover, R. P. (2017). Some key challenges in securing 5G wireless networks. Electronic Comment Filing System, Jan.
25. Khan, A. S., Abdullah, J., Khan, N., Julahi, A. A., & Tarmizi, S. (2017). Quantum-Elliptic curve Cryptography for Multihop Communication in 5G Networks. International Journal of Computer Science and Network Security (IJCSNS), 17(5), 357-365.

26. Li, S., Da Xu, L., & Zhao, S. (2018). 5G Internet of Things: A survey. Journal of Industrial Information Integration, 10, 1-9.
27. M. Dyakonov. The case against quantum computing. IEEE Spectrum, 56(3):24–29, March 2019.
28. Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The impact of quantum computing on present cryptography. arXiv preprint arXiv:1804.00200.
29. McEliece, R. J. (1978). A public-key cryptosystem based on algebraic. Coding Thv, 4244, 114-116.
30. Message Level Encryption. (n.d.). Retrieved from https://developer.visa.com/pages/encryption_guide
31. Miller V.S. (1986) Use of Elliptic Curves in Cryptography. In: Williams H.C. (eds) Advances in Cryptology — CRYPTO '85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science, vol 218. Springer, Berlin, Heidelberg
32. Ni, J., Lin, X., & Shen, X. S. (2018). Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT. IEEE Journal on Selected Areas in Communications, 36(3), 644-657.
33. Nkenyereye, L., Liu, C. H., & Song, J. (2019). Towards secure and privacy preserving collision avoidance system in 5G fog based Internet of Vehicles. Future Generation Computer Systems, 95, 488-499.
34. Omondi, A. R. (2020). Elliptic-Curve Cryptosystems. In Cryptography Arithmetic (pp. 243-252). Springer, Cham.
35. Palattella, M. R., Dohler, M., Grieco, A., Rizzo, G., Torsner, J., Engel, T., & Ladid, L. (2016). Internet of things in the 5G era: Enablers, architecture, and business models. IEEE Journal on Selected Areas in Communications, 34(3), 510-527.
36. R. L. Rivest, A. Shamir, and L. Adleman. 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21, 2 (February 1978), 120–126. DOI:https://doi.org/10.1145/359340.359342
37. R. R. Jueneman, "Electronic document authentication," IEEE Network, vol. 1, no. 2, pp. 17-23, Apr. 1987.
38. RFC 3156 - MIME Security with OpenPGP. (2020). Retrieved 30 April 2020, from https://tools.ietf.org/html/rfc3156
39. Schinianakis, D. (2017). Alternative security options in the 5G and IoT era. IEEE Circuits and Systems Magazine, 17(4), 6-28.
40. Schneier, B. (2007). Applied cryptography: protocols, algorithms, and source code in C. john wiley & sons.
41. Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In Proceedings 35th annual symposium on foundations of computer science (pp. 124-134). Ieee.
42. The MobileBroadband Standard. (n.d.). Retrieved from https://www.3gpp.org/specifications-groups/sa-plenary/sa3-security
43. The Transport Layer Security (TLS) Protocol Version 1.3. (n.d.). Retrieved from https://tools.ietf.org/html/rfc8446
44. Tseng, C. H., Wang, S. H., & Tsaur, W. J. (2015). Hierarchical and dynamic elliptic curve cryptosystem based self-certified public key scheme for medical data protection. IEEE Transactions on Reliability, 64(3), 1078-1085.
45. W. Diffie and M. Hellman, "New directions in cryptography," in IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, November 1976.
46. Wang, Q., Chen, D., Zhang, N., Qin, Z., & Qin, Z. (2017). LACS: A lightweight label-based access control scheme in IoT-based 5G caching context. IEEE Access, 5, 4018-4027.
47. Yan, Z., Xie, H., Zhang, P., & Gupta, B. B. (2018). Flexible data access control in D2D communications. Future Generation Computer Systems, 82, 738-751.
48. Yanofsky, N. S., & Mannucci, M. A. (2008). Quantum computing for computer scientists. Cambridge University Press.