Cryptography in 5G - Mini Research Paper

Research · March 2022

CITATIONS
0

READS
954

4 authors, including:

Aakif Kuhafa
Sri Lanka Institute of Information Technology
3 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Gihan Niroshan
Sri Lanka Institute of Information Technology
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Nadeesha Rajakarunaratne
Sri Lanka Institute of Information Technology
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Cryptography in 5G

Aakif Kuhafa
Cybersecurity
Faculty of Computing
Sri Lanka Institute of Information Technology
Sri Lanka
IT19967226

Gihan Niroshan
Cybersecurity
Faculty of Computing
Sri Lanka Institute of Information Technology
Sri Lanka
IT19994024

Nadeesha Rajakarunaratne
Cybersecurity
Faculty of Computing
Sri Lanka Institute of Information Technology
Sri Lanka
IT19191034

Raneesha Pomodh
Cybersecurity
Faculty of Computing
Sri Lanka Institute of Information Technology
Sri Lanka
IT19177724

ABSTRACT

The fifth generation of mobile broadband networks have used many cryptography techniques and theories. Earlier generations used symmetric key cryptography for their privacy and security principals and 5G used some advanced techniques for same functions. Basically, in 5G, engineers used PKI-based trust model. This advanced move was happened because of quantum computing threatens to disclose the protection of earlier techniques such as ECC and RSA.

KEYWORDS

5G technology, post-quantum cryptography, quantum computing

INTRODUCTION

5G is the 5th generation of technology standard for broadband cellular network in telecommunication organizations. With the technological advancement in the telecommunication industry organizations discovered this technique to improve the speed, increase the bandwidth, reduce the latency, and so more. In 2019 cellular phone companies began to implement 5G technology to gain more benefits and improve the security of the networks and services [1].

5G technology has started a revolution in most of the companies. The download speed in 5G reaches up to 10 gigabits per second, which is 100 times faster than 4G. 5G uses network slicing improve the performance; it splits the network to tailor speed, capacity, coverage, security, and encryption by reassessing the resources from one slice to another. The delay between sending and receiving information is significantly low, the latency in 5G is 1 millisecond. 5G has high level security standards to protect data from violating confidentiality, integrity, and availability. Because of these features in 5G networks, most IoT (Internet of Things) uses have begun to use 5G technology to improve their services and operations.

With the growth of quantum cryptography 5G networks are secured when transmitting data. 5G uses public-key infrastructure (PKI) for user equipment authentication and to manage plane services securely. The density of qubits in quantum computers have matched Moore's law curve which doubles every 18 months. Increasing the key size would only provide an additional 18 months of key lifetime. These advancement of quantum cryptography has made cryptographers anxious about the longevity of ciphers like Rivest -Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC).

The National Institute of Standards and Technology (NIST) has been working on post-quantum cryptography and found a cipher which do not rely on RSA and ECC, and as a result it is immune to advancement of quantum computing. Various concern over quantum computing advances has motivated cryptographers to lead to standardize cipher suites by 2022.

In this paper we mainly discuss about post quantum cryptography, NIST standards, Subscribe and Access network Security in 5G and control plain security.

POST-QUANTUM CRYPTOGRAPHY)

Post-Quantum cryptography is a term used to imply that the implemented algorithms are resistant to quantum computing structure. The main objective in quantum cryptography is to securely distribute the key in a network. A bit string is agreed between the two parties using BB84 protocol and establishes a common key sequence using polarized photons. Therefore, eavesdropping is impossible because a qubit cannot be copied according to no-cloning theorem [2].

In mid 90's AES, RSA, and ECC symmetric key cipher security was questionable with the findings of Shor's and Grover's quantum algorithms [3]. The below table summarizes the common ciphers, their equivalent symmetric key strength using classical algorithms, and the equivalent security using quantum computers.

Table 1 : Comparison of classical and quantum security levels for ciphers

Cipher	Key Size	Effective Strength	
		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

1. Post-Quantum Cipher

Post-quantum cryptography referred to cryptographic ciphers that provide secure against cryptographic attacks by both quantum computers and classic computers. Most of the public-key algorithms currently in use, which can be broken in the future by using large quantum computers. This would be a huge effect of violating the confidentiality and integrity of 5G communication on the internet and other communication protocols [4]. There are six types of post-quantum cryptography methods currently in use.

1. Lattice-based cryptography
2. Multivariate cryptography
3. Hash-based cryptography
4. Code-based cryptography
5. Supersingular elliptic curve isogeny cryptography
6. Symmetric key quantum resistance

2. NIST Standards

The competition for post-quantum cryptography standards now on its 3rd round NIST expects to publish the final documents by 2024. In 5G standards, mainly focus on cryptographic agility of post-quantum cryptography. Also implement algorithms for RSA and ECC as 'drop-in replacement' by considering challenges of alternative auxiliary functions, signature size and especially public-key size [2].

5G SECURITY

The current generation of the telecommunication system is based on 5G radio networks. Mainly it focuses on to extreme mobile broadband, massive capacity on communication, and ultra-low latency to manage the scale of devices prognosticated for the mobile internets of things. To enable 5G network within the devices and the network via virtual and containerized environment, it uses multi-level of services and multi-connectivity network capabilities. 5G network has implemented with new security control measures to overcome the issues raised from 4G.3G, and 2G networks [5]. mainly it uses control mechanisms such as extreme subscriber identity security, mutual authentication, and other security mechanisms. 5G provides security to limit impact to known attacks.

1. Subscriber device, and network protection

5G network protect the confidentiality of Non-Access Stratum (which is a set of protocols in the evolved packet system) messages in between device and the network. It will be more secure to face and protect the device data from the man in the middle attacks, why because it is no longer to catch the data or the user details using such kinds of attacks. On the other hand, it introduced a security control mechanism called home control. It senses after verifying the authentication control of the device on the home network, the verification of the final device on the end network is completed.

To protect the data integrity, 5G introduced a network architecture element called Security Edge Protection Proxy (SEPP). It protects the network edge by acting as security gateway on intercommunication between home network and visited networks. SEPP provide application security for the network and prevent various attacks such as eavesdropping attacks. By introducing key management mechanisms, it implements the necessary encryption key processing and security capabilities discussion procedures [6]. SEPP uses signature and encryption of HTTP/2 roaming messages to ensure their authentication, integrity, and confidentiality.

2. Control Plane Security

"Control Plane" is the term that used to describe all signals that support the dot functions used in mobile telecommunication process. In earlier generations, core network is dwell of a set of static functions, that arranged together as a part of rack-mount software. In 5G technology assume a cloud native contact to root network systems. This network is re-predicting as a collection of small services. All these existing as an app in cloud and broadcast by using web service APIs with some other factors over a HTTPS [7]. These Virtualized Network Functions needs a public/private key and digitalized certificates to verify transactions. For this process Transport Layer Security (TLS) and HTTPS add the authentication and OAuth2.0 protocols are used to enable interactions. Addition to that, when the core network from one network carrier starts communicating with another network carrier some additional layers of security layers are used including IPsec.

FUTURE DEVELOPMENT

Need of 5G standards is a critical requirement and future implementation of post-quantum cryptography of public-key ciphers. A new definition will be added for cipher suite in transport layer security by satisfying the main focus of drop-in replacement. The need for an infrastructure for Certification Authorities (CA) to control the keys of post-quantum cryptography. Transition to new keys and ciphers can be done effectively by adopting public-key approaches and it will enable trust and authentication in 5G technology.

CONCLUSION

As the 4G chapter closes, a new generation signals which requires more safe networking technology to face pre generations issues and to be ready for next-generation services and demand. As a result, 5G network era has begun. This report shows the various aspects of the 5G wireless technology and secure key distribution techniques. Throughout this report, post-quantum cryptography shows the longevity of current ciphers with the help of various new cryptographic algorithms like Shor's algorithm and how it impacts on modern 5G cryptography. According to the cryptographic technics, there are some basic security mechanisms implemented to overcome different attacks or threats occurred in previous eras. This 5G technology helps in security sector of the country many securities high profile organization are now relaying on the wireless network system

to save their huge data. That's why 5G network security is more effective in current business world than previous technologies. This report can make things better for the technology sector in the future.

REFERENCES

[1] "5G," [Online]. Available: https://en.wikipedia.org/wiki/5G.

[2] M. Sharbaf, "Quantum cryptography: An emerging technology in network security," in *2011 IEEE International Conference on. IEEE*, 2011.

[3] L. Grover, "A fast quantum mechanical algorithm for database search," Bell Labs, New Jersey, 1996.

[4] "Post-quantum cryptography," [Online]. Available: https://en.wikipedia.org/wiki/Post-quantum_cryptography.

[5] "Securing the 5G Era," [Online]. Available: https://www.gsma.com/security/securing-the-5g-era/.

[6] H. Y. Youm, "5G security activities and future," Soonchunhyang University, Korea, 2018.

[7] E. Guttman and I. Ali, "Path to 5G: A Control Plane Perspective," *Journal of ICT*, vol. Vol 6.1&2, pp. 87-100, 2018.

[8] "Post-Quantum Cryptography PQC," NIST.