Asian Journal of Scientific Research and Innovations
ISSN: 2715-xxxx (online) | IF: 10.23 | Vol: 1, issue 1
Available: http://asiansciencejournal.org

THE ROLE OF CRYPTOGRAPHY IN NEW TECHNOLOGIES (IoT, Blockchain, 5G, 6G, Cloud and Fog Computing)

AKHRAROV ODILJON ALIMJONOVICH
Lecturer at the Military Security and Defense University of the Republic of Uzbekistan

Abstract: Cryptography plays a central role in ensuring the security, confidentiality, and integrity of data in modern and future technological systems. With the development of technologies such as the Internet of Things (IoT), blockchain, 5G, 6G, cloud computing, and fog computing, cryptography faces new challenges related to scalability, mobility, and the processing of enormous volumes of data. In IoT, cryptographic methods are required to protect data transmitted between billions of connected devices with limited computing power. In blockchain systems, cryptography ensures data immutability and transaction security in decentralized environments. In 5G and 6G networks, cryptography is used to protect traffic and to preserve the confidentiality and integrity of information transmitted under conditions of high speed and high device density. In cloud and fog computing, cryptography protects both data and computing resources, ensuring secure access and reliable data processing in distributed environments. This article examines cryptographic solutions used to protect data and systems in the context of emerging technologies. It also highlights current challenges and the future development of cryptographic methods that will help ensure security in a rapidly changing digital world.

Keywords: Internet of Things (IoT), blockchain, 5G, 6G, cloud computing.

Introduction

Cryptography is a fundamental discipline in the field of information security. As new technologies such as the Internet of Things (IoT), blockchain, 5G, 6G, cloud computing, and fog computing continue to develop, its role becomes increasingly important. These technologies radically transform the ways in which devices interact, data is processed, and communications are organized. As a result, new approaches and solutions are required to protect information at every level.

The main purpose of cryptography is to ensure the confidentiality, integrity, and availability of data. It helps protect information from unauthorized access, verify authenticity, prevent data forgery, and support the authentication and authorization of participants in digital interaction. In the context of rapidly growing data volumes, diverse information flows, and emerging cyber threats, cryptography has become a key instrument for ensuring security in distributed and multi-network systems.

Cryptography in the Internet of Things (IoT)

The Internet of Things is a future technological revolution in computing and communications based on the concept of continuous and ubiquitous connectivity of various

devices. Even at its current stage of development, IoT has changed the interaction between organizations, consumers, and surrounding objects.

Figure 1. Examples of devices connected within the Internet of Things.

IoT is also a network of physical objects connected to the Internet, including nanotechnologies, consumer electronics, household appliances, sensors, embedded systems, and personal mobile devices. An IoT system generally consists of several layers:

- End IoT devices such as sensors, controllers, and other modules that collect small amounts of data from industrial equipment or household appliances and transmit them to the network.
- Data transmission channels, including wired and wireless network protocols such as Serial, RS-485, MODBUS, CAN bus, OPC UA, BLE, Wi-Fi, Bluetooth, LoRaWAN, Sigfox, and others, which deliver information from end devices to intermediate gateways.
- Network gateways and hubs, including routers that integrate end devices and connect them to a cloud-based IoT platform.

Modern cryptographic methods are used to protect data transmission channels and software applications from information leakage. These methods include symmetric algorithms such as DES, AES, GOST 28147-89, Camellia, Twofish, Blowfish, IDEA, and RC4; asymmetric algorithms such as RSA and ElGamal; digital signatures; hash functions such as MD4, MD5, MD6, SHA-1, SHA-2, and GOST R 34.11-2012; key management mechanisms; and quantum cryptography.

There are also cryptographic protocols used in IoT systems. IPsec provides authentication, integrity checking, and encryption of IP packets, as well as secure key exchange on the Internet. TLS (Transport Layer Security) protects data transmission between Internet nodes by combining asymmetric cryptography for authentication, symmetric encryption for confidentiality, and message authentication codes to preserve integrity. Kerberos is a network protocol that provides mutual authentication of the client and server before communication is established.

Figure 2. Smart home as an example of IoT-based infrastructure.

Cryptography in Blockchain Technology

Blockchain, from the English words block and chain, means a chain of blocks. The blocks contain information and are linked to one another in chronological order. A new block is created whenever new information is added or changes are recorded. Information stored in a blockchain cannot be easily deleted or falsified. This is achieved because the chain of blocks is not controlled by a single person or company, but by all participants in the system. Any participant can join the system and become one of its maintainers.

Blockchain has three key characteristics: decentralization, security, and scalability. These characteristics are closely connected, and in most blockchain systems only two of them can be achieved at a high level at the same time. Strengthening one characteristic may weaken another. This problem is known as the blockchain trilemma: it is extremely difficult for a decentralized system to achieve equally high levels of decentralization, security, and

scalability simultaneously.

Figure 3. The blockchain trilemma: decentralization, scalability, and security.

There are three main forms of decentralization in blockchain systems. Architectural decentralization refers to the number of computers, nodes, or servers that make up the system and how many of them can fail at any moment without disrupting the entire network. Political decentralization refers to how many people or organizations control the computers that form the system. Logical decentralization determines whether, if the system is divided into two parts - including both providers and users - the two parts can continue to operate as independent units.

Cryptography lies at the foundation of blockchain technology by ensuring the integrity and security of transactions. It allows participants to interact with the blockchain while keeping personal information confidential. Cryptographic methods protect the authenticity of transactions and prevent fraud and forgery. Digital signatures, hash functions, and public-key cryptography play an important role in securing blockchain transactions [3].

Digital signatures verify the authenticity and integrity of transactions, ensuring that changes cannot be made without being detected. Hash functions create unique digital fingerprints for each block, making it practically impossible to modify one block without changing the entire chain. Public-key cryptography allows participants to exchange information securely and create a trusted network even without prior knowledge of one another. It supports secure encryption, decryption, and digital identification, thereby increasing confidentiality and trust in the blockchain environment.

In addition, the use of cryptographic keys in blockchain technology provides a secure way to manage access and permissions within the network. These keys, which are securely generated and stored by participants, act as digital credentials that authenticate and authorize transactions, adding another layer of security to the blockchain ecosystem.

Cryptography in 5G Networks

With the growth of Internet user needs, fifth-generation mobile technology has attracted attention worldwide. A key feature of 5G is its new network architecture, in which the main functions of telecommunications equipment are implemented at the software level and do not require specialized hardware solutions.

The 5G network architecture is designed to support the exchange of different types of data and the provision of diverse services using technologies such as Network Function Virtualization (NFV) and Software Defined Networking (SDN) [2]. The main innovations of fifth-generation mobile networks include enhanced Mobile Broadband (eMBB), Ultra-Reliable and Low-Latency Communications (URLLC), and massive Machine Type Communications (mMTC) for large-scale connection of sensors and IoT devices.

Figure 4. Main service areas and application domains of 5G technology.

Cryptography in 5G provides several key security functions:

• Confidentiality - protecting data from unauthorized access through encryption algorithms.

- Data integrity - ensuring that data has not been altered during transmission.
- Authentication - verifying the identity of users and devices connected to the network.
- Protection against replay attacks - using unique keys and timestamps to prevent repeated unauthorized use of intercepted data.

Some of the key cryptographic technologies used in 5G include encryption, authentication, and key management. AES (Advanced Encryption Standard) is a symmetric encryption algorithm used to protect user data on communication channels. AES provides a high level of security while allowing relatively fast data processing [2]. Public-key cryptography, such as RSA and ECC, is used for authentication and the creation of secure communication channels between the user and the network. Elliptic Curve Cryptography (ECC) is widely used in 5G because it provides strong security with lower computational costs.

Based on the security approaches of the fifth-generation standard, several protection solutions can be identified. A key component of 5G is authentication and key management. Secure context transfer mechanisms make it possible to exchange cryptographic information safely between devices and the infrastructure, which is important for ensuring the confidentiality and integrity of data during base-station switching or roaming. TLS and IPsec are used to protect data transmission at the network and Internet layers, especially over open communication channels.

Protection against identity attacks is also important. In 4G and earlier networks, IMSI (International Mobile Subscriber Identity) was used to identify subscribers. In 5G, improved authentication methods and IMSI pseudonymization are introduced to provide better protection against attacks and to reduce the risk of personal data leakage.

To protect 5G networks from intrusion, cybersecurity technologies must be improved in accordance with the conditions of mobile Internet and communication technologies. High bandwidth and other advantages of 5G require a reassessment of traditional protection methods. The expanded capabilities of 5G networks can simultaneously increase security risks.

Many IoT devices used in fifth-generation mobile networks are not sufficiently equipped with cybersecurity mechanisms. 5G creates new opportunities for IoT, but as the variety and number of network connections increase, the threat landscape also expands. For example, smart televisions, door locks, and refrigerators may become vulnerable points within a network. The absence of unified security standards and methods for IoT can lead to active and large-scale cybercrime.

Figure 5. A simplified 5G architecture with IoT and edge components.

The main types of attacks associated with vulnerable connected devices include:

- Botnets that control connected devices for large-scale cyberattacks.
- DDoS attacks that overload a network or website and block access to Internet resources.
- Man-in-the-middle attacks, in which messages exchanged between two parties are

silently intercepted and modified.

- Location tracking and call interception.

Cryptography in 6G Networks

6G is the sixth generation of wireless communication networks and is expected to implement a number of technological innovations compared with previous generations. These innovations may include the use of the terahertz band for communication or gesture recognition, additional frequencies between 7 and 24 GHz, integration of communication and sensing, artificial intelligence and machine learning, and reconfigurable intelligent surfaces.

One of the goals of 6G is to achieve maximum data transmission rates of up to 1 Tbit/s. To reach such speeds, bandwidth expansion to 10 GHz or more will be necessary. Such wide bandwidths are mainly available at higher frequencies, including the terahertz range.

Cryptography in 6G will be necessary for protecting personal data and preventing information leakage under conditions of increasingly intensive data transmission; ensuring confidentiality and authentication of users and devices in high-speed and high-load networks; integrating with new technologies and creating secure communication channels for innovative services such as autonomous vehicles, smart cities, and massive IoT systems; and protecting against quantum attacks, because future quantum computers may be able to break many current cryptographic schemes.

The main cryptographic technologies for 6G include quantum cryptography, post-quantum cryptography, zero-knowledge proofs, distributed ledgers, multifactor authentication, biometrics, and intelligent cryptography.

Quantum cryptography will become one of the most relevant areas for 6G. As quantum computing develops, traditional cryptographic methods such as RSA and ECC may become vulnerable to quantum attacks, because quantum computers can efficiently solve problems that are currently computationally difficult for classical computers.

Quantum Key Distribution (QKD) is a technology that will enable the exchange of cryptographic keys through quantum communication channels while providing a high level of security. The use of the quantum state of light for key transmission makes eavesdropping detectable, because any intervention in a quantum system changes its state [5].

Post-Quantum Cryptography (PQC) refers to cryptographic algorithms designed to resist quantum attacks. New encryption algorithms, such as lattice-based and hash-based algorithms, are already being developed and may be used in 6G [5].

Zero-Knowledge Proofs (ZKP) can help solve one of the key problems of 6G: preserving user privacy in networks that process large volumes of personal data. ZKP allows users to prove authenticity or compliance with a condition without disclosing the underlying information. This technique can be used in 6G authentication, allowing users to verify their identity without revealing sensitive identification data.

Blockchain and other distributed ledger technologies can support security at the infrastructure and device levels in 6G. Blockchain can be used to secure authentication and identity management, ensure the integrity of data transmitted across the network, prevent

unauthorized modification, and manage security in IoT devices and wireless sensor networks.

As the number of devices and users increases in 6G, multifactor authentication will become even more important. It combines several authentication methods, such as passwords, biometric data, tokens, and cryptographic certificates. Biometrics, including face recognition, fingerprints, and iris recognition, may be used to strengthen security and protect user data.

With the integration of artificial intelligence and machine learning into 6G networks, cryptography will also evolve. AI can be used to detect anomalous traffic, identify attack patterns, support adaptive key management, predict threats, and automate the selection of appropriate security mechanisms for specific network conditions.

Cryptography in Cloud Computing

Cloud computing is a model that provides on-demand network access to a shared pool of configurable computing resources such as networks, servers, storage, software, and services. These resources can be rapidly provisioned and released with minimal management effort or service-provider interaction [1]. In cloud computing, resources are abstracted and virtualized from the IT infrastructure of a cloud service provider and made available to clients.

Figure 6. Example of a cloud service access and protection architecture.

Cloud infrastructure provides various advantages for cloud users and other stakeholders. These advantages include access to data stored in the cloud regardless of location, pay-on-demand models, and economic benefits resulting from reduced need to purchase hardware and other IT infrastructure [2].

Despite these advantages, cloud computing raises significant concerns. Security is one of the main issues in the cloud computing industry [3]. The first and most obvious concern is confidentiality, because users cannot always be absolutely certain that data stored in the cloud is safe and secure. Attackers may exploit vulnerabilities in cloud computing and compromise cloud security. Using various malicious programs and techniques, they can harm organizations by stealing data, conducting man-in-the-middle attacks, and violating data integrity.

Figure 7. Protection of data and keys in a cloud computing environment.

There are two main types of encryption algorithms in cloud cryptography: symmetric and asymmetric encryption algorithms. Symmetric encryption, also called secret-key cryptography, uses one key for both encryption and decryption. DES is a data encryption standard that uses a single secret key for encryption and decryption. It uses a 64-bit secret key, 56 bits of which are generated randomly, while the remaining 8 bits are used for error detection. It is based on the Data Encryption Algorithm (DEA), a secret-key block cipher operating with a 56-bit key and 64-bit blocks [3].

AES (Advanced Encryption Standard) is a symmetric-key algorithm in which both encryption and decryption are performed using the same key. It is an iterative block cipher that works by repeatedly applying defined transformation steps. AES has a 128-bit block size and key sizes of 128, 192, and 256 bits for AES-128, AES-192, and AES-256 respectively.

Asymmetric encryption, also known as public-key cryptography, was introduced to

solve key management problems [3]. It uses both a public key and a private key. The public key is available to users, while the private key is kept secret by its owner. RSA is a public-key cryptosystem used for encryption and authentication on the Internet. It uses modular arithmetic and elementary number theory to perform calculations based on two large prime numbers [1].

Elliptic Curve Cryptography (ECC) is a modern public-key cryptographic approach designed to reduce the need for very long cryptographic keys. This asymmetric cryptosystem is based on number theory and mathematical elliptic curves, allowing the generation of short, fast, and reliable cryptographic keys [2].

Cryptography in Fog Computing

Fog computing is a technology that creates an intermediate layer between the cloud and the end user. Users can deploy fog computing nodes at different points within their network.

Figure 8. Interaction between cloud, fog, and end-user levels.

The main function of the end-user layer in fog computing is to collect data about events occurring in the physical environment and transmit the accumulated data to fog nodes at a higher level for processing and storage. Fog computing makes it possible to connect a large number of different devices to the network. However, in this technology, operations are not performed in a centralized environment, but in a complex decentralized and distributed environment of endpoints. This approach helps identify potential threats before they affect the entire network.

Cryptography in fog computing serves several important purposes:

- Ensuring data confidentiality by protecting data from unauthorized access both during transmission and storage.
- Guaranteeing data integrity by preventing or detecting changes that may occur during transmission through the network.
- Authenticating users and devices to confirm the identity of communication participants and prevent unauthorized access.
- Ensuring availability and protection against attacks by using cryptographic methods to resist DoS attacks and infrastructure-level attacks.

The cryptographic methods and technologies used in fog computing include encryption, key exchange, and digital signatures. Encryption is a critical element of security in fog computing because it protects data both in transit and while stored on intermediate nodes. Symmetric encryption, such as AES, is used to encrypt large amounts of data because it is relatively fast and efficient. However, symmetric keys must be transmitted and protected securely [2].

Asymmetric encryption, such as RSA or ECC, is used for more secure authentication and key exchange. In fog computing, efficient and secure exchange of encryption keys between nodes is essential, including edge devices, IoT devices, fog nodes, and central cloud servers. Key exchange protocols such as Diffie-Hellman can be used to exchange keys securely between nodes.

Digital signatures are used in fog computing to ensure data integrity and authentication. A digital signature confirms that data has not been changed during transmission and that it was sent by a legitimate source. RSA and ECDSA (Elliptic Curve Digital Signature Algorithm) are widely used to create digital signatures that verify the authenticity of data.

Conclusion

Cryptography remains a fundamental tool for protecting data and ensuring security in a rapidly developing digital world, where technologies such as the Internet of Things, blockchain, 5G, 6G, cloud computing, and fog computing are becoming integral parts of everyday life. Each of these technologies creates unique challenges and threats that require innovative cryptographic solutions aimed at protecting the confidentiality, integrity, and availability of information.

Cryptography for emerging technologies is not limited to the application of existing security methods. It also involves dynamic development and adaptation to new challenges. In an environment characterized by continuous growth in data volumes, new threats, and new technological capabilities, cryptography continues to play a key role in ensuring security and trust in modern and future technological systems. The development of cryptographic methods such as quantum cryptography, zero-knowledge cryptography, and other innovative approaches will determine the reliability and security of the digital world in the coming decades.

REFERENCES

1. Babenko, L. K., and Ishukova, E. A. Modern Block Cipher Algorithms and Methods of Their Analysis. Moscow: Gelios ARV Publishing House, 2015. 376 p.
2. Welschenbach, M. Cryptography in C and C++. Textbook. Moscow: Triumph, 2014. 462 p.
3. Stallings, W. Cryptography and Network Security: Principles and Practice. 8th ed. Pearson, 2021. 912 p.
4. Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C. Moscow: Triumph, 2012. 518 p.
5. Kerschbaum, F., and Großschädl, J. Post-Quantum Cryptography: Current State and Future Directions. Springer, 2021. 343 p.
6. Au, M. H., and Zhou, J. Cryptographic Algorithms and Protocols. CRC Press, 2020. 480 p.