11TH INTERNATIONAL SCIENTIFIC CONFERENCE
ON DEFENSIVE TECHNOLOGIES
OTEH 2024
Serbia, Tara, 9-11 October 2024

CONTEMPORARY CRYPTOGRAPHY: RECENT ACHIEVEMENT AND RESEARCH PERSPECTIVES

BORIŠA JOVANOVIĆ
University of Defence Belgrade, Military Academy and
Applied Mathematics and Electronics Centre, Belgrade, borisa.jovanovic@vs.rs

IVAN TOT
University of Defence Belgrade, Military Academy, ivan.tot@va.mod.gov.rs

SILVANA ILIĆ
Applied Mathematics and Electronics Centre, Belgrade, silvana.ilic@vs.rs

Abstract: *In modern times, cryptography has been considered as a branch of both mathematics and computer science, and is tightly related to information security. With the accelerated progress of the Internet and the increase of digital communication, the need for stronger and more effective methods of cryptographic protection has become more pronounced. With the rapid increase in computing power, the potential for breaking cryptographic algorithms also increases. This fact in modern cryptography creates a need for stronger and more advanced cryptographic algorithms. One development direction of modern cryptography is post-quantum cryptography, which can withstand the attacks of quantum computers. In addition to the potential threats to traditional cryptographic techniques, there is also the potential to integrate artificial intelligence tools with the process of developing and implementing cryptographic algorithms. For instance, advanced machine learning algorithms can be used to identify potential vulnerabilities in cryptographic systems and algorithms and improve their security. As technology continues to evolve, new techniques are being developed in the field of cryptography in order to stay one step ahead of new threats. In this paper, the current achievements of modern cryptography are explored and the research perspectives in this field are explained.*

Keywords: *post-quantum cryptography, algorithms, homomorphic encryption, quantum-resistant encryption, lightweight cryptographic algorithms.*

1. INTRODUCTION

Cryptography is a science that studies techniques for converting information into an unreadable format in order to protect confidential messages from unauthorized access[1]. The earliest known cryptographic techniques date back to ancient civilizations, where methods such as simple transposition and substitution ciphers were used to conceal messages and prevent unauthorized people from reading and understanding messages. These techniques evolved over time to include more complex ciphers, such as the Caesar and Vigenere ciphers, which were used during the Middle Ages. The development of the typewriter and the subsequent increase in literacy rates led to the need for more secure encryption techniques, leading to the development of more complex ciphers such as the Playfair Cipher and Enigma.

Symmetric cryptographic algorithms are one of the oldest and most widely used types of encryption. Their work is based on the concept of using the same key to encrypt and decrypt a message. The history of symmetric cryptographic algorithms dates back to ancient times, where simple substitution ciphers were used to encrypt messages. Over time, more complex algorithms such as the Hill cipher and the Data Encryption Standard (DES) were developed. The development of the Advanced Encryption Standard (AES) at the end of the twentieth century marked a significant improvement in the field of symmetric cryptographic algorithms as it provided stronger encryption and faster processing times.

An important component of modern cryptography are hash functions. A hash function is a mathematical function that takes an input (or message) and produces an output (or hash, or message fingerprint) of a fixed length [2]. Hash functions are primarily used to ensure data integrity because any change to the content of the original message will result in a different hash value.

Closely related to the application of the hash function is the digital signature technology. The goal of applying a digital signature is to provide a reliable method for user authentication and to ensure non-repudiation in digital communications. Digital signature technology is a mathematical scheme for demonstrating the authenticity of a digital message or electronic document. The development of digital signature technology dates back to the early 1980s, when the concept of asymmetric cryptographic algorithms was first introduced. Recently, various algorithms such as Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm

Corresponding author: B.Jovanović;
E-mail borisa.jovanovic@vs.rs
DOI: 10.5937/OTEH24067J

(ECDSA) have been developed [3].

Major historical events and technological advances have driven the evolution of cryptographic algorithms. The emergence of the Internet and its development has resulted in an increase in digital communication, which further causes an increased need for strong, reliable and more efficient cryptographic algorithms. With the ever-increasing computing power, the potential for cracking encryption algorithms is ever-increasing. This has led to the need for stronger and more advanced cryptographic algorithms, such as post-quantum cryptography, that can withstand quantum computer attacks.

In addition to the potential threats to the security of cryptographic algorithms, there is also the potential for integrating artificial intelligence tools into the design and evaluation processes of cryptographic algorithms. For example, machine learning algorithms can be used to identify potential vulnerabilities in the design of a cryptographic algorithm and thus to define procedures for improving their security.

As digital communications continue to rapidly evolve, the importance of maintaining superiority in the application of cryptographic techniques cannot be overstated. This paper explores the future of cryptography, including developments in post-quantum cryptography, blockchain based cryptography, modern lightweight cryptographic algorithms, and other emerging technologies. The future of cryptography holds great promise as researchers work to develop new homomorphic and quantum-resistant encryption techniques, new methods for securing block chain technology, new generations of lightweight cryptographic algorithms, and modern multiparty computing systems.

The main contribution of this paper is its aspiration to help in understanding the basic principles and postulates of modern cryptography. If we properly understand the principles and applications of modern cryptography, we will be better able to preserve the privacy and security of our communications and to protect our digital assets.

2. MODERN CRYPTOGRAPHY – DIRECTIONS OF DEVELOPMENT

Modern cryptography develops in the environment of the comprehensive use of quantum computers and the increasing need to make the content of communication inaccessible to uninvited participants. This is where cryptography comes into play: it is a key tool for building quality solutions for cyber security. To that end, cryptographic algorithms are used in a large number of applications that surround us; examples range from social networks, smartphones and cloud servers to embedded systems such as medical implants, car keys and passports. New advanced technology systems such as autonomous cars and electronic voting will rely even more heavily on strong security mechanisms. Moreover, the number of applications for cryptography have increased dramatically, as new cryptographic techniques are invented and proven secure. For example, securely transacting with cryptocurrencies such as bitcoin requires modern cryptography. As another example, hospitals may now share information about patients in a way that protects patient privacy while allowing the hospitals to apply statistical methods assessing the effectiveness of new treatments on the aggregate of the patients [4].

Such an environment influences the further development of cryptography, so the future of cryptography can be easily guessed. The most important research directions in modern cryptography are: research and development of new homomorphic and quantum-resistant encryption techniques; research and development of new methods for securing block chain technology; research and development of new generations of lightweight cryptographic algorithms and research and development of modern multiparty computer systems. In the following text of this paper, each of the mentioned directions of development of modern cryptography will be analyzed and explained in more detail.

2.1. Homomorphic encryption

Homomorphic encryption is a type of encryption that allows computation to be performed on ciphertext, meaning that data can be encrypted and manipulated without having to be decrypted first[5]. In other words, it allows performing various types of calculations on the data without revealing the data itself. This is a significant advance in modern cryptography as it enables secure computation and analysis over large data sets without compromising their confidentiality[6]. Homomorphic encryption technologies have numerous applications in a wide variety of fields such as healthcare, finance, and cloud computing[7]. For example, homomorphic encryption can be used to perform secure data analysis on sensitive data, such as medical records, without the need to disclose the data to unauthorized parties. It can also be used in cloud computing to protect data privacy while enabling secure cloud computing[8].

It is relatively easy to construct partially homomorphic encryption schemes, which are constructions that allow one mathematical operation to be performed on the ciphertext, typically multiplication or addition. Unfortunately, one mathematical operation is not sufficient for the majority of practical applications. For a long time finding a fully homomorphic encryption scheme that allows arbitrary operations was considered the holy grail of cryptography. The first such scheme was proposed by in [9] in 2009, which is based on lattices. This original system was quite impractical but since then numerous improvements have taken place. At the time of writing this paper, many competing schemes exist and use in practice is within reach[4].

In military applications, the homomorphic encryption technique can enable secure data processing in the cloud or other untrusted environments, preserving data confidentiality.

2.2. Quantum-resistant cryptography

The term post-quantum cryptography was coined to describe modern types of cryptosystems that are assumed

to be able to withstand attacks using large-scale quantum computers. Shor's algorithm[10] showed that cryptographic algorithms that are based on the hardness of factoring the product of two primes, or that are based on the hardness of computing discrete logarithms, are vulnerable to polynomial-time attacks using quantum computation. If and when quantum computers become available, cryptographic methods such as RSA or elliptic-curve cryptosystems will become vulnerable. While this seems to be a problem to be solved in the future, we already need to equip today's applications with cryptography that is resistant to quantum computer attacks in order to defend against "store now, decrypt later" adversaries[4].

In traditional cryptography (cryptography before the advent of quantum computers), the security of cryptographic systems relies on the complexity of mathematical algorithms, while in post-quantum cryptography, security relies on the laws of physics. Specifically, quantum cryptography uses the principle of quantum entanglement, which is based on the correlation of quantum states between two particles.

Today, post-quantum cryptography is an active field of research and several schemes have already been standardized. The National Institute of Standards and Technology has selected standardized, quantum-resistant digital signature algorithms including Crystals-Dilithium, Falcon, and Sphincs+. Also, the National Institute of Standards and Technology has chosen lattice-based KIBER as the key encapsulation mechanism for key establishment based on the encryption scheme. It was chosen as a result of a trade-off between assumed security and efficiency over conventional public-key schemes.

International standardization bodies have already compiled the first portfolio of standardized quantum-secure schemes for key encapsulation and digital signatures, which is currently still being expanded. In fact, with a large variety of standardized post-quantum cryptography schemes we will be ready to provide confidentiality and authentication services even in the era of powerful quantum computers[4].

From the available literature, it can be seen that quantum computing leads to both opportunities and risks for military communication systems. Quantum technologies such as post-quantum cryptography offer advanced methods for protecting military communications from potential quantum attacks. However, the same quantum capabilities can also be used to break traditional cryptographic methods, meaning that there is an urgent need for advances in quantum-resistant cryptographic solutions.

2.3. Block chain cryptography

Blockchain-based cryptography is a critical component of blockchain technology, which is widely used in various fields such as healthcare, finance, and supply chain management. It is a distributed ledger that records transactions in a secure and transparent manner. Cryptography is used in the blockchain to ensure the confidentiality, integrity and authenticity of the data stored in the blockchain network[11].

One of the basic cryptographic techniques used in blockchain is digital signature. A digital signature is a mathematical scheme that confirms the authenticity and integrity of a message or data. Digital signatures are used to verify transactions in the blockchain network, ensuring that the sender is the actual owner of the funds and preventing any unauthorized use of the data. Another critical cryptographic technique used in blockchain is cryptographic compression functions, better known as hash functions. Hash functions are used to create a unique digital fingerprint of the data stored in the blockchain network. This unique digital fingerprint, also known as a hash value, ensures that the data is protected from unauthorized access and cannot be changed without detection[11].

Blockchain-based cryptography plays a vital role in ensuring the security and transparency of data stored in the blockchain network. As blockchain technology continues to evolve, we can expect to see new cryptographic techniques and algorithms that will further enhance the security and efficiency of blockchain-based applications[12].

The development of blockchain technology brings with it increased data confidentiality and improved data availability that can help shape future military logistics and planning. Also, their development will make military communications more secure. In the long term, the application of blockchain technologies in the military will be a revolution if implemented well and many more military applications are found, in addition to being used wisely and affordably.

2.4. Lightweight cryptographic algorithm

Lightweight cryptography refers to a subset of cryptographic algorithms specifically designed to work efficiently on low-resource devices such as smart cards, RFID tags, and wireless sensor nodes. These devices often have limited processing power, memory and energy resources, making it a challenge to implement traditional cryptographic algorithms on them. Lightweight cryptography aims to address these challenges by developing cryptographic algorithms that have low computational and memory requirements while still providing a reasonable level of security.

The development of lightweight cryptography has become increasingly important with the proliferation of the Internet of Things (IoT) and other low-power, low-cost devices. These devices are becoming more and more present in our daily lives, and many of them require secure communication and authentication. Lightweight cryptography can provide a practical and effective solution for securing these devices, without sacrificing security. Some examples of lightweight cryptography algorithms include the SIMON and SPECK block ciphers, designed by the National Security Agency (NSA) for use in restricted environments. Another example is a lightweight version of the Advanced Encryption Standard (AES), known as AES-Lite. These algorithms have been adopted by various standardization bodies and are widely used in the industry to provide low-resource devices[13].

Embeddable cryptographic processors used for crypto modernization enable a range of new military communications applications, such as smartphones and rugged tablet computers for tactical use on the front lines, as well as secure tactical Wi-Fi, unmanned vehicle control and real-time targeting . Almost everyone has a feeling that embedded computing technology is constantly getting more powerful and efficient, while getting smaller and lighter. However, the need to preserve the power source while at the same time achieving satisfactory security of transmitted data opens the door to the application of light cryptographic algorithms in military communications.

2.5. Multiparty computation

Multiparty computation is a cryptographic technique that allows a group of parties to jointly compute a function on their private inputs, without revealing those inputs to each other or any third party. This technique allows parties to collaborate and calculate a result without sharing their individual data, which can be particularly useful in scenarios where data privacy is critical, such as financial transactions or medical research[14].

In multiparty computation, several parties provide input values and together compute a function from the input. Interestingly, when the protocol is completed, participants only know their input and response, but nothing about the input of other participants[15]. A standard example is a situation where three people want to know the highest salary in the group without revealing their individual salaries. Another application is determining the outcome of an election, i.e. electronic voting, or the highest bid at an auction based on encrypted data. Related to multiparty computation is secret sharing. The idea of (general) secret sharing is that out of n participants t must collaborate to compute a secret, e.g., a cryptographic key. A real-world scenario is that at least 2 out of 3 managers of a bank must get together to generate the secret code for opening a safe[4].

One possible application of the mentioned technologies in military communication systems is that, for example, to make a strategic decision in a specific situation, at least 5 out of 8 military decision-makers must gather to generate a secret code that is used to initiate special procedures.

3. CONCLUSION

Cryptography is a critical aspect of modern information security. It has evolved significantly over time, from basic substitution ciphers to sophisticated algorithms that ensure secure communication and transactions. Today, we have various types of cryptographic schemes, including symmetric and asymmetric encryption, hash functions, digital signatures, homomorphic encryption, post-quantum cryptographic algorithm, lightweight cryptography and multiparty computation. The development of lightweight cryptography has also enabled secure communication and transactions on low-power devices such as IoT devices. As technology continues to advance, the field of cryptography will play an increasingly important role in ensuring secure communication and transactions in an interconnected world. The future of cryptography is exciting and promising, and we can expect to see more innovations that will improve the security and privacy of military communication systems.

References

[1] BRUCE,S.: *Applied cryptography: protocols, algorithms, and source code in C. 2nd ed.* Hoboken, New Jersey: John Wiley & Sons; 1996

[2] SOBTI,R., GEETHA,G.: *Cryptographic hash functions: A review.* International Journal of Computer Science Issues (IJCSI). 2012;9:461

[3] MENEZES,A.J., VAN OORSCHOT,P.C., VANSTONE,S.A.: *Handbook of applied cryptography (202101 ed.).* 2021;1:1-810

[4] CRISTOF,P., JAN,P., TIM,G.: *Understanding cryptography From established symmetric and asymmetric ciphers to post-quantum cryptography*, Second Edition, Springer-Verlag Gmbh DE, 2024

[5] LAUTER,K.E., DAI,W., LAINE,K.: *Protecting privacy through homomorphic encryption*. Cham, Switzerland: Springer 2022

[6] DOAN,T.V.T., MESSAI,M-L., GAVIN,G., DARMONT,J.: *A survey on implementations of homomorphic encryption schemes*. The Journal of Supercomputing. 2023 vol. 79 p. 15098-15139

[7] CHATTERJEE,A., AUNG,K.M.M.: *Fully homomorphic encryption in real world applications*. Singapore: Springer; 2019

[8] VIAND,A., KNABENHANS,C., HITHNAWI,A.: *Verifiable fully homomorphic encryption*. arXiv Preprint arXiv:2301.07041. 2023

[9] CRAIG,G.: *Fully homomorphic encryption using ideal lattices*. In In Proc. STOC, pages 169–178, 2009

[10] SHOR,W.P.: *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.* SIAM Journal on Computing, 26(5):1484–1509, 1997.

[11] BOLFING,A.: *Cryptographic Primitives in Blockchain Technology: A Mathematical Introduction.* New York, USA: Oxford University

Press; 2020

[12] ZHENG,Z., XIE,S., DAI,H., CHEN,X., WANG,H.: *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*, 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, USA, 2017, pp. 557-564,

[13] DUTTA,I.K., GHOSH,B., BAYOUMI,M.: *Lightweight Cryptography for Internet of Insecure Things: A Survey*, 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2019, pp. 0475-048

[14] GOLDREICH,O.: *Secure multi-party computation. Manuscript. Preliminary version.* 1998 78 pages 1-78

[15] RONALD,C., IVAN,D.: *Multiparty Computation, an Introduction*, Birkhauser Basel, Basel, 2005. pages 41–87