Proceedings of the 2023 International Conference on Mathematical Physics and Computational Simulation
DOI: 10.54254/2753-8818/10/20230304

Application of modern algebra in cryptography

Yuling Qian

Sino-Canada School, SUZHOU, JIANGSU Province, 215027, China

sophieqian0512@gmail.com

Abstract. With the rapid development of the digital age, information security, from personal data to national security, is becoming increasingly crucial. Information security primarily refers to the computation and processing of diverse information in computer systems and information exchange networks in order to safeguard information security. Cryptography is the technical foundation for achieving these objectives. In the early stages of education, advanced mathematics, linear algebra, probability theory, and other fundamental disciplines must be studied, although the practical application of modern algebra, cryptography, number theory, and mathematical knowledge will vary. This study explores the application of current algebra in cryptography, including both traditional and modern cryptographic applications, using a literature review approach. By comparing images from various eras, the researchers discovered that images were classed as "traditional" and "modern" at various times. Moreover, the likelihood of both traditional and modern images being identified throughout the modern era is comparatively higher.

Keywords: modern algebra, cryptography, information security.

1. Introduction

Currently, the application of artificial intelligence (AI) in the fields of banking and insurance is expanding, while the application of blockchain technology is still in the exploratory phase [1]. Blockchain is a peer-to-peer network-based decentralised distributed ledger database that stores and processes data. Since blockchain is a database with a high level of credibility, it can be used for a variety of financial transactions, including payments, lending, and insurance. In conventional finance, financial institutions document each transaction prior to its exchange and liquidation. Nevertheless, blockchain technology enables decentralised storage and transaction data, eliminating the need for financial institutions to maintain records and enabling them to update them in unusual ways.

As an unique trust mechanism and method of value transfer, blockchain has reached a relatively mature state of implementation in the financial sector. The system of financial services based on blockchain technology offers security, efficiency, and transparency. The new technologies embodied by blockchain + Internet of Things permit the expansion of financial services beyond transactions to all links of the value chain. Blockchain +Internet of Things can realise the digitalization, automation, and intelligence of business processes; The business relationship between traditional financial institutions such as banks and insurance companies and customers can be shared via blockchain; It can provide customers with multi-dimensional information disclosure and risk assessment services; It can automatically assess and intelligently classify risks in order to improve risk identification capabilities.

DOI: 10.54254/2753-8818/10/20230304

In order to improve the application efficiency and dependability of blockchain technology in the financial sector, it is essential to validate and categorise blockchain transactions [2]. In this paper, the researchers classified cryptographic images using machine learning techniques, or Modern Algebra in Cryptography.

2. Brief introduction to cryptography

The study of cryptography, often known as cryptology, was created in response to the demands of secure communication. In addition, it is the ability to analyse information encryption and decryption technologies, as well as password-cracking technologies. There are two distinguishing aspects of cryptography: a long history and excellent mathematical abilities. In secure communication, the following processes occur during the sending and receiving of information: the sender sends out the original information - known as plaintext, executes various changes or transformations - known as encryption, and encrypts the information - ciphertext; the receiver receives the ciphertext, and the ciphertext is converted back to clear text, which is known as decryption. The decoded ciphertext is the message's original form. During transmission, the ciphertext may be intercepted by an eavesdropper. The thief cannot read the original information straight from the ciphertext that has been intercepted. Without understanding the algorithm for encryption, he attempted to retrieve the plaintext from the ciphertext, a process known as breaking or decrypting [3].

Cryptography belongs to the fields of mathematics and specialisation. It is divisible into the following classes: The first is to provide communication security methods, that is, to study how to encrypt the original information sent, making it difficult for intruders to crack it; this is known as encryption. The second is to steal the ciphertext information of others and decrypt it to obtain useful original information; this is known as cryptographic analysis. The first aspect is known as cryptography or coding. The second aspect is known as cryptanalysis. These two components constitute cryptography as a whole. Coding and cryptanalysis are referred to as twin or reciprocal sciences on occasion. In terms of function, the both are complementary. The objective of the first category is to develop cryptographic approaches that enhance the encryption's security. The second step is to disclose the secret. Both are mutually contradictory, complimentary, and co-evolve. The term "cryptosystem" refers to an encryption algorithm and the collection of equipment used to accomplish it. From the standpoint of the evolution of passwords, there are primarily five typical password systems:

1)Literature replaces cryptography, a system of encryption in use before to the Renaissance. Its encryption employs images, symbols, or numbers instead of text and is manually encrypted. 2) Mechanical cryptosystem, which was in operation prior to World War Two. Its cryptography algorithm is essentially a replacement for sophisticated multi-meters that is encrypted via mechanical manipulation. 3) The Serial port cryptosystem, which was established after the 1950s, continues to employ a cryptosystem. Typically, information is transmitted as binary sequences. Encryption is accomplished through electronic equipment. 4) Block cypher system, a private key cryptosystem that groups and encrypts plaintext information group by group. 5) Public key cryptosystem, also referred to as public key cryptosystem, is a new cryptosystem that arose in the mid-1970s and is distinguished by the ability to publish some keys. This is also the most significant development in modern cryptography. Public key system is a very promising cryptosystem that possesses notable properties in data encryption, user information verification, key management, and digital signature [4].

3. Cryptographic applications

3.1. Traditional cryptographic applications

Prior to the 1949 release of Shannon's "Secure System Communication Theory," the transmission of passwords was primarily accomplished through simple substitution and replacement of characters, therefore simple types of encryption largely fell under the purview of classical cryptography. Replacement cyphers encrypt plaintext by rearranging its characters, whereas replacement cyphers include the fundamental principles of modular operations, modular inverses, and Euler functions in

DOI: 10.54254/2753-8818/10/20230304

affine coding. Affine and Hill cyphers are examples of conventional cryptography applications. In this essay, Hill algebra is used to encrypt plaintext letters and Hill alphanumeric characters, and its encryption concepts are briefly described. In 1929, Lester Hill, a mathematician, introduced the Hill cypher in the American Mathematical Monthly. The basic idea is to employ linear substitution to replace n consecutive plaintext letters with the same number of ciphertext characters. The substitution key is a transformation matrix, and the inverse transformation requires just encrypted information.

3.2. Modern Cryptographic applications

Cryptography was created as a result of research into the secure transmission of information. In a nutshell, cryptography is the science of securing communication in hostile circumstances. It has grown as a result of a protracted and ceaseless battle for the "spear" and "shield" of cryptographic coding and analysis [5]. As a result of the use of modern science and technology, it has evolved into a cutting-edge science and technology that integrates and develops many fields. Currently, numerous domestic and international colleges offer cryptology courses. Due to the military application of cryptography, cryptography itself is shrouded in secrecy, and secret technology is utilised in numerous facets of daily life and work. Because to the mathematical abstraction underlying cryptography, it is difficult to acquire and comprehend its fundamental concepts and principles. Specifically, one-way functions, deception gate replacement, public key cryptography, etc., are quite inconsistent with the standard mathematical thinking model, which creates a number of teaching challenges for students. To improve the efficiency of these knowledge comprehension in the teaching process, students must be analysed in a "turn around" fashion from formal algorithms during the process of comprehending cryptographic concepts.

3.2.1. Applications in the mathematical courses of cryptography. Typical cryptographic mathematics courses include probability theory, rudimentary number theory, and abstract algebra, among other topics. These courses have unique algorithmic elements, particularly in the areas of elementary numbers and abstract algebra. Several abstract mathematical topics, such as groups, rings, fields, factorization, congruences, Chinese residual theorems, and quadratic residuals, are required for teaching cryptography. In the classroom, traditional teaching continues to be used to explain concepts, evaluate and prove theorems, and assign homework. After hearing an abstract topic, students are unable to comprehend its practical application, historical context, and relevance. Students can only memorise abstract mathematical ideas by rote memorization. "They work diligently during the questioning process but become trapped in set forms and conventions, unable to fully comprehend, learn, and apply them, making it impossible to dig into the more advanced areas of cryptography" [6]. As long as students learn these findings through conventional methods such as homework, it is evident that they will not attain higher results. Thus, in the process of studying cryptography based on mathematics, it is required to combine the qualities of these knowledge with the thinking mode of algorithms and modular techniques, and to supply fundamental concepts and algorithm ideas in related concepts from abstract algebra. Programming thinking, solving complex problems, examining its connotation based on its functional modules, and applying its extension from a theoretical standpoint will help students develop a greater knowledge of its concepts and methods. From the perspective of password application, it is necessary to increase interest in teaching abstract mathematics [6].

3.2.2. Application in the field of computer science and security protocols. The formal approach of algorithms in computer science and security protocols is based on mathematical integrated description technology, which is ideal for the description, development, and verification of connected systems. Formal methods are employed in these computer domains to further assess the performance of these systems in a safe and dependable manner; it is anticipated that this will increase the reliability and robustness of the designed algorithms and systems in a more scientific manner. This article focuses on the study of challenges in the teaching of cryptography's fundamental principles and combines the formalisation of algorithms with an emphasis on the analysis and comprehension of fundamental

DOI: 10.54254/2753-8818/10/20230304

concepts in public key cryptography. In public key cryptosystems, RSA cryptographic algorithms are the first to come to mind. Several instructors and college students are contemplating how to develop RSA to address the challenge of big data. This cryptosystem is neither officially defined nor formally described in sufficient detail. As an illustration, consider the decryption public key encryption technique. Public key cryptography is one of the most scientific sciences that can encapsulate modern cryptography in modern cryptography systems. Once Edifier and Hellman of Stanford University proposed a novel notion for public key cryptosystems in 1976, not only may their encryption methods be published, but the confidentiality of encrypted keys (primarily public keys) can also be disclosed without information reduction. The key management concerns of earlier cryptosystems have also been partially resolved.

First, a thorough discussion of the formal definition of public key cryptography follows. Second, it examines which portions of RSA are public key cryptography functions. Thirdly, evaluate the algorithm's potential security flaws. Finally, a concrete numerical example is provided. Specifically, public key cryptosystems can be formalised as triples from an algorithmic perspective (K, E, D). K is a key generation method, whose formal job is to generate a matching pair of public and private keys in preparation for the encryption and decryption algorithms E and D. K can be a probabilistic algorithm; E is an encryption algorithm whose functional module is to encrypt a message, and the algorithm can also be probabilistic; D is a decryption algorithm, and the function of the conversion algorithm is to implement ciphertext decryption operations [7]. The RSA key generation algorithm, encryption algorithm, and decryption algorithm are then detailed. Lastly, researchers officially define the relevant functional components and investigate potential security concerns in depth. The attacker may have mastered the resources and exposed the mathematical foundation of the RSA encryption algorithm's security. Lastly, a numerical example is provided to demonstrate the efficacy of the algorithm and enhance comprehension of the technique. The application of formal model analysis to describe public key cryptosystems and specific instances further explains the concept of public key cryptography and provides the key to comprehending the procedure and security performance of RSA algorithm encryption algorithms. It conforms to the thinking model of assessing and solving problems in contemporary learning processes and is capable of achieving twice as much with half the effort. This algorithm's formal method is also applicable to other cryptographic knowledge [8].

3.2.3. Applications in the cryptosystem design using modular thinking. In the process of cryptographic block cypher systems, blocks are subdivided into several components based on the functions of the cypher system, the design principles and objectives of each block are described, and methods are provided for achieving the blocks. In conclusion, the combination and analysis of each function block is provided. The combination of these traits will not influence their safety attributes. This section's structure and "overall scenario" must be comprehended in order to methodically examine the methods and rules of cryptographic system design and earn knowledge points for deriving analogous results. The following block cypher instruction is an illustration. In developing block cyphers, the topic can be separated into three stages based on the preceding analysis. First, the necessary security features for block cyphers are considered in light of their security needs. Using the algorithm's modular concept and based on these security criteria, functional blocks are then assigned according to their implementation qualities. Lastly, implementation algorithms corresponding to the various implementation approaches are provided [9].

Plaintext assaults are the primary threat to block cyphers since the block cipher's key z is utilised repeatedly, i.e. several times and once. Since a password is required to withstand this assault, it is important to design a password: 1) Confusion: A password's design should make the relationship between plaintext, ciphertext, and key so complicated that it cannot be exploited for password analysis. 2) Diffusivity: The design of a password should make each bit of the key affect each bit of the ciphertext to prevent the key from being decoded one bit at a time; each bit of plaintext should affect each bit of ciphertext to conceal the plaintext as explicitly as possible. 3) Containing a significant amount of nonlinearity. The modular design concept is to modularize block cyphers into computing

DOI: 10.54254/2753-8818/10/20230304

components, computing component combinations, SPNs (replacement/replacement networks), numerous iterations, and recurrent functions based on these security needs. Various modules implement different security qualities while ensuring that the interactions between the components of a function are not offset, but rather stacked, so that they only boost security performance and do not decrease it. The implementation procedure of a particular block cypher algorithm, such as DES, IDEA, AES, etc., is then examined in detail [10].

4. Conclusion

By comparing images from various eras, the researchers discovered that images were classed as "traditional" and "modern" at various times. In addition, throughout the modern era, the likelihood of both traditional and contemporary photographs being classed is rather high. In addition, the machine learning techniques utilised for various image classifications are constantly evolving. As for the limitations of this study, it only discusses the Application of Modern Algebra to Cryptography, and no empirical research has been conducted; this will be addressed in future research.

References

[1] Victor Shoup. A Computational Introduction to Number Theory and Algebra. Cambridge University Press, 2015.
[2] Neal Koblitz. Algebraic Aspects of Cryptography. Springer, 1998.
[3] J.-J. Quisquater and L. Guillou. How to Explain Zero-Knowledge Protocols to Your Children. [3]Advances in cryptology—CRYPTO'89 Proceedings, Springer, 1989, pp. 628-631.
[4] David Joyner. Adventures in Group Theory: Rubik's Cube, Merlin's Machine, and Other Mathematical Toys. The Johns Hopkins University Press, 2002.
[5] Serge Vaudenay. A Classical Introduction to Cryptography: Applications for Communications Security, Springer, 2005.
[6] Michiel Kosters. Algorithmic Number Theory: 7th International Symposium, ANTS-VII, Berlin, Germany, July 23-28, 2006, Proceedings. Springer-Verlag, Berlin, Heidelberg, 2006.
[7] Scott Aaronson. Quantum Computing, post-quantum cryptography, and the quest for quantum supremacy. National Science Review, Volume 4, Issue 3, May 2017, Pages 293–299.
[8] Gary L. Mullen and Daniel Panario. Handbook of Finite Fields. CRC Press, 2013.
[9] Tanja Lange, Daniel J. Bernstein, and Peter Schwabe. Post-Quantum Cryptography. Springer, 2009.
[10] Nigel P. Smart. Cryptography: An Introduction. McGraw-Hill, Springer, 2004, pp 50.