Mathematics and Computer Science
2022; 7(2): 18-23
http://www.sciencepublishinggroup.com/j/mcs
doi: 10.11648/j.mcs.20220702.11
ISSN: 2575-6036 (Print); ISSN: 2575-6028 (Online)

A Survey of Commercial Password Detection Methods

Zhou Yue[1], Ren Fengli[1], Shao Yong[2, *]

[1]Beijing Software Testing and Quality Assurance Center, Beijing, China

[2]Faculty of Information Technology, Beijing University of Technology, Beijing, China

Email address:

zhouyue@kw.beijing.gov.cn (Zhou Yue), renfl@kw.beijing.gov.cn (Ren Fengli), shaoyong@bjut.edu.cn (Shao Yong)

[*]Corresponding author

To cite this article:

Zhou Yue, Ren Fengli, Shao Yong. A Survey of Commercial Password Detection Methods. *Mathematics and Computer Science*. Vol. 7, No. 2, 2022, pp. 18-23. doi: 10.11648/j.mcs.20220702.11

Received: March 16, 2022; **Accepted**: April 9, 2022; **Published**: April 14, 2022

Abstract: Commercial password has been widely used in China's information services, and their role and importance in information security are gradually increasing. In recent years, as the application of quantum computing in computer technology becomes more and more extensive, the performance of computers continues to improve, and cryptographic penetration technology has emerged in an endless stream. Some known cryptographic algorithms are no longer secure in the new environment, such as the MD5 cryptographic algorithm with obvious security risks and the cracked RSA public key password algorithm, etc. Therefore, it is essential to detect and evaluate the security of commercial passwords. Based on a large number of literature at home and abroad and the practical work experience of Beijing Software Testing and Quality Assurance Center, this study comprehensively analyzes and combs the commercial password detection technology and forms a relatively complete research review on commercial password detection methods. The specific contents include traditional cryptanalysis methods, key penetration attack methods, side-channel attack methods, quantum computing cryptanalysis, etc. The research results provide important theoretical support for the commercial password security detection of the Winter Olympic information system, enhance the technical ability of the inspectors to the commercial password detection, and ensure the comprehensiveness of the information system security detection.

Keywords: Information Safety, Commercial Password, Detection Method

1. Introduction

A Commercial password is a cryptographic algorithm for encrypting information that does not involve state secrets. Its significance to the development of national information security is no less than the core password and ordinary password used for the insured state secret information [1]. The main commercial cryptographic algorithms popularized in China include symmetric cryptographic algorithms, asymmetric cryptographic algorithms, and cryptographic hash algorithms. When these cryptographic algorithms are designed, the encryption and anti-decryption effects are sound, and the security is very high. However, with the development of computers in recent years, especially the wide application of quantum computing in the field of computers, the number of cryptographic cases is gradually increasing, the difficulty of deciphering is significantly reduced, and the means of cryptographic attack are progressively enriched. Thus, some traditional cryptography believes that secure cryptographic algorithms are no longer safe in the new environment [2]. In 2013, the famous "Snowden incident" exposed large-scale monitoring events in the United States, a typical case of decoding passwords by non-mathematical means, that is, algorithm substitution attack. The algorithm substitution attack embeds the key information into the algorithm output by tampering with the algorithm deployment to obtain the encrypted data information, bringing new challenges to password security detection. With the emergence of side-channel cryptanalysis technology, the attacker can obtain the cryptographic key without complex mathematical theory derivation. The attacker can obtain the electromagnetic energy and other information leaked during the operation of cryptographic encryption equipment by some means and deduce the key information from this information. With the development of quantum computing technology, the application of quantum computing to crack keys has also

appeared in cryptography. All kinds of password attack algorithms bring significant challenges to the security of password algorithms but provide new technology for commercial password detection.

Commercial cipher detection detects the correctness and consistency of the cipher system, the quality of key generation and the security of key management through technical means. Corresponding national standards can judge the correctness and consistency of the key system; To evaluate the security of the cryptosystem, we need to consider whether the attacker can obtain the information encrypted by the password by some means [3].

At present, there are mainly two ways to attack the cryptosystem. One is the traditional method of cracking the ciphertext directly to get the encrypted information based on complex mathematical problems. Traditional commercial cryptographic detection methods are based on mathematical problems to restore ciphertext, including differential cryptanalysis, truncated differential cryptanalysis, impossible differential cryptanalysis, linear cryptanalysis, algebraic cryptanalysis, etc [4]. Traditional cryptanalysis has certain limitations. Its designers believe that the execution process of a cryptographic algorithm is safe; that is, if the ciphertext information cannot be solved by mathematical derivation, the cryptographic system is considered to be safe. This is not the case. The execution process of the cryptographic algorithm can be attacked now. In this case, the traditional cryptographic analysis method is no longer applicable. In terms of known plaintext and ciphertext information, traditional cryptanalysis can be divided into four categories: ciphertext only attack, known plaintext attack, selective plaintext attack and selective ciphertext attack. The above differential cryptanalysis attack belongs to the selective plaintext attack.

The other is the emerging key attack method, which obtains the key information generated by the cryptographic algorithm by unconventional means, and then crack the plaintext information contained in the ciphertext. One is side-channel analysis, which mainly analyzes the side information generated during the operation of cryptographic equipment, such as current, electromagnetic and other information. The side information is associated with the data generated during the operation of the cryptographic algorithm. By analysis of the side information, we can get the key information generated during the operation of the cryptographic algorithm or the intermediate value generated during the process and then crack the ciphertext information. The other is algorithm substitution attack. The idea of this method is "algorithm substitution attack," that is, unsafe factors are added during the the algorithm’s operation, resulting in the ciphertext information with key when the cipher algorithm outputs. The enemy can restore the ciphertext information according to the key in the ciphertext, thus damaging the security of the cipher system, However, the traditional commercial password detection method still believes that this is a secure password algorithm, so the traditional commercial password detection method is not suitable for detecting this new password attack [5]. The new commercial password detection method mainly obtains the key and restores the ciphertext information by embedding the back door, using the algorithm substitution attack. In addition to the above cryptographic algorithms, quantum computing attack methods have not been widely used. This cryptographic attack algorithm depends on quantum computing technology and is also a threat to cryptographic algorithms.

2. Traditional Commercial Cryptanalysis

Traditional commercial cryptanalysis follows the kerckhoffs criterion, which holds that even if the attacker has all the information except the key, the cryptosystem is still secure; that is, the security of the cryptosystem is based on the fact that the attacker cannot obtain its key. The traditional cryptanalysis method is based on complex mathematical problems to crack the password, combined with strong cracking to realize the cryptographic algorithm's analysis. Typical strong cracking methods include key exhaustive attack and table lookup attack. The more general traditional cryptanalysis methods based on complex mathematical problems include differential cryptanalysis, truncated differential cryptanalysis, impossible differential cryptanalysis, linear cryptanalysis, algebraic cryptanalysis, square attack, etc. Several typical cryptographic algorithm analysis techniques will be introduced below.

2.1. Differential Cryptanalysis

Many cryptographic algorithms are encrypted through iterative groups; a strong encryption algorithm is composed of multiple iterations of weak encryption algorithm. Among them, weak encryption algorithm has simple implementation and poor security. After the input of the last layer is determined, the output of the last layer is determined. This kind of password is usually called an iterative cryptosystem. Differential cryptanalysis is a cryptanalysis method for iterative cryptosystems proposed by Biham and Shamir in 1991. Differential cryptanalysis is a selective plaintext attack that uses statistical methods to analyze the influence characteristics of plaintext, ciphertext and difference to recover the key. The basic idea of differential cryptanalysis is to recover some key bits by examining the influence of the difference between plaintext pairs on the difference between ciphertext pairs. Differential cryptanalysis can crack DES passwords with less than 8 rounds in a few minutes, which is excellent progress compared with the key exhaustive attack. DES passwords with 15 rounds are still faster than key exhaustive attacks, but the time complexity required to crack DES with 16 rounds is 2^n, slightly higher than that of strong cracking. Although differential cryptanalysis is a selective plaintext attack, it is worth noting that it can be cracked only when enough plaintext information is available [6]. And with the complexity of cryptographic algorithm design, the general differential cryptanalysis method has been challenging to crack the key information in a reasonable time range.

2.2. Truncated Differential Cryptanalysis

Truncated differential cryptanalysis was proposed by Knudsen. Different from differential cryptanalysis, truncated differential cryptanalysis can reduce the number of rounds of cryptanalysis and only need to predict a part of bits in the differential path. In contrast, differential cryptanalysis requires fully predicting all differential values on the differential path [7]. This means that in the same case, truncated differential cryptanalysis needs less plaintext information than differential cryptanalysis to crack the ciphertext successfully. In some exceptional cases, cryptographic algorithms that can resist differential cryptographic attacks may not be able to resist truncated differential cryptanalysis.

2.3. Impossible Differential Cryptanalysis

Impossible differential cryptanalysis is a cryptanalysis method proposed by Biham, Biryukov and Shamir in 1999 [8]. Differential cryptanalysis is to find the difference with the highest probability and judge whether the difference is the correct difference. Impossible differential cryptanalysis is a variant of differential cryptanalysis. The difference with zero probability is called the impossible difference. This cryptanalysis method is called impossible differential cryptanalysis. The impossible differential cryptanalysis uses impossible differential path to eliminate the wrong key and get the correct key. If the plaintext pair satisfies the input difference of the path and restores the ciphertext with the correct key, it is impossible to get the wrong output difference. The realization of impossible difference analysis is mainly to construct an impossible difference path. The construction method of impossible difference path: find two difference paths with a probability of 1 and conflicting intermediate values, and connect the two paths to form a difference path with the likelihood of 0. This method is called a middle impossible encounter. The wrong keys can be excluded through the impossible differential path. Filtering these wrong keys can significantly reduce the number of guessing keys to find the correct key with lower complexity.

Impossible differential analysis has become a common technical means in commercial password detection. By eliminating the wrong key through impossible differential analysis, combined with differential cryptanalysis or truncated differential cryptanalysis, the efficiency of cryptanalysis can be improved.

2.4. Linear Cryptanalysis

Linear cryptanalysis was proposed by Japanese scholar Matsui at the European annual conference on cryptography in 1993 [9]. Linear cryptanalysis is a known-plaintext attack that uses the linear relationship between plaintext, ciphertext and key to recover some key bits. For iterative block ciphers, differential cryptanalysis uses some differential features of the previous n-1 round to recover the subkey of the last round. Linear cryptanalysis is the same idea, but linear cryptanalysis is to find a linear expression to recover the subkey of the last round. The purpose of linear cryptanalysis is to obtain the approximate linear expression of a given cryptographic algorithm. Firstly, a linear path based on statistics is constructed between the input and output of each S-box, and then this path is extended to the whole algorithm. Finally, an approximate linear expression without any intermediate value is obtained.

The 16 round DES cryptosystem has been deciphered by linear cryptanalysis but facing the 16 round cryptosystem, whether differential cryptanalysis or linear cryptanalysis, it needs a lot of plaintext information.

2.5. Algebraic Cipher Attack

The concept of algebraic cryptographic attack was formally proposed by Courtois and Meierl in 2003 [10]. Algebraic cipher attack is mainly aimed at sequence cipher. Its main idea is to deduce the unknown key by solving the nonlinear equations containing messages, ciphertexts, and keys. There are many similar methods for algebraic attacks on sequence ciphers. The main difference between these methods is the type of equation used, and the type of equation used usually determines the solution method of a cipher. At present, algebraic cryptanalysis has become another general cryptanalysis method after differential cryptanalysis and linear cryptanalysis. Whether it can resist algebraic attacks has also been used as a new standard to measure the security of cryptographic algorithms. An algebraic cryptographic attack first constructs the equations about the unknown key and solves the equations according to the current key information. Therefore, algebraic cryptographic attack is essentially a known-plaintext attack method. To implement an algebraic cryptography attack, the attacker must construct a certain number of multivariate equations. The specific number of equations to be constructed depends on the method used. Finally, the unknown key bits are obtained by solving the equations.

2.6. Square Attack

The most commonly used methods of block cryptanalysis are differential cryptanalysis and linear cryptanalysis. Still with the development of cryptographic technology, these two cryptanalysis methods can not efficiently attack new cryptographic algorithms. The square algorithm is a cryptographic algorithm used to resist differential cryptanalysis and linear cryptanalysis. The square algorithm was proposed by Joan Daemen et al in 1997, and square attack method was proposed when the block cipher square algorithm was proposed. It is used to attack the square cipher algorithm. The square attack is a particular plaintext attack method [11].

3. Algorithm Substitution Attack

In 2013, the famous "Snowden incident" revealed that the security agencies represented by the US National Security Agency (NSA) monitored internet users on a large scale by controlling the formulation of standards for cryptographic algorithms and tampering with the software and hardware

deployment of relevant algorithms in cryptographic products. The method used is to implant a password back door or subvert the password algorithm to obtain the user's private key and destroy the user's communication privacy. After the "Snowden incident," a "post-Snowden cryptography" has been formed in the international cryptography circle, which focuses on the research of the back door embedding form, working principle and prevention technology of cryptographic algorithm. At the 2014 US secret meeting, Bellare and others proposed an "algorithm substitution attack," which is used to describe an unique attack method of key leakage caused by the tampering of symmetric encryption algorithm during actual deployment. Huang Xinyi and others call the attack method of tampering with the algorithm deployment and embedding the key information into the algorithm's output to achieve the purpose of key penetration a "key penetration attack." The algorithm substitution attack methods based on embedding backdoor and subverting cryptographic algorithm mainly include setup, partial ciphertext attack, etc.

3.1. SETUP

Setup is an attack mechanism of embedded backdoor named general protection against black-box cryptosystem proposed by Young et al. in 1996. This mechanism can be embedded into the user's encryption device, allowing the attacker to obtain the user's key information without being noticed by the cryptographic device and the user, and can resist the attack on this mechanism. In the setup mechanism, the attacker can also modify the cryptographic algorithm to make the cryptographic device disclose the key information when outputting [12].

3.2. Partial Ciphertext Attack

According to the idea of algorithm substitution attack in the literature, Bellare et al. Proposed IV substitution attack, partial ciphertext attack, and other attack methods.[13]. Compared with the IV substitution attack, the partial ciphertext attack applies to a broader range of cipher algorithms, because the IV substitution attack is only suitable for the "operation manual" cipher system, that is, the published and transparent cipher system. It does not apply to the non-public encryption scheme. The partial ciphertext is a more general cipher attack method.

4. Side Channel Analysis

Traditional cryptography follows the Kerckhoffs criterion and believes that a cryptosystem is secure if the attacker cannot recover the key through mathematical calculation. Therefore, it cannot effectively cope with physical attacks, namely, the attack method of recovering the key through electromagnetic and electric current information. The implementation of cryptographic algorithms is divided into software implementation and hardware implementation. The software implementation of a computer processor is simple and low cost, but its computing ability is poor, and its security is low. When hardware devices such as FPGA are implemented, they will obtain higher running speed and higher security. Still, its universality is not as good as the cryptographic algorithm implemented by software. The implementation of a cryptographic algorithm depends on hardware equipment The hardware equipment of cryptographic system will leak various types of physical information such as energy and electromagnetism in the actual encryption process. Side-channel analysis technology can use this information to directly or indirectly recover the key of ciphertext information to crack the encrypted plaintext information in ciphertext. There are two primary analysis technologies for side-channel analysis: energy analysis technology and fault analysis technology. At present, various side-channel analysis methods and attack models have been fully developed. Side-channel analysis methods mainly include template attack, differential energy analysis, correlation energy analysis, simple fault analysis, differential fault analysis, photon side-channel analysis method, side-channel watermarking method, correlation collision analysis method, etc [14]. This paper will introduce several classical and general side-channel analysis methods.

4.1. Template Attack

When the cryptographic device performs an encryption operation, it completes the operation through the level conversion of internal nodes. Asteady stream of acquisition current will be generated in level conversion. Due to the existence of internal resistance, the voltage corresponding to the opposition will fluctuate when the equipment is running, and the change of voltage is directly proportional to the energy consumption of the microcontroller. The equipment will continue to generate energy. At the same time, the energy consumption depends on the encryption operation and encrypted data so that a particular relationship can be established between energy consumption and encryption. Energy analysis convert the voltage and current information generated during the operation of cryptographic equipment into energy information for analysis to obtain the key or data information related to the key [15].

Template attack is a simple energy analysis attack technology that constructs a template by collecting the energy curve of the cryptographic chip to complete the attack on the cryptographic chip. The principle of template attack is that the energy consumption depends on the data being processed by the cryptographic device. The key to a template attack is that the attacker and the attacker have the same cryptographic device. Template attack usually consists of two parts. The first step is template construction, and the second step is template matching. Thetemplate construction method is to collect the energy curve and select the information leakage point and energy model. The template is a data pair of mean vector m and covariance matrix C. It will make (m, c) a template. The attacker can determine the template of some instruction sequences through template creation. Template matching is when the attacker uses the created template and the energy consumption data obtained from the attacked device to recover the key information.

Template attack is a compelling side-channel analysis technology that can completely use various side-channel technologies to classify. However, a template attack requires the same device as the attacked device, which is also the weakness of a template attack. If the attacked device has the functions of data interference and key bit shielding, the effectiveness of the template attack will be significantly reduced.

4.2. Correlation Energy Analysis

There are two main ways in the research field of energy attacks on cryptographic devices by using side-channel information. The first is the differential energy analysis proposed by Paul Kocher et al. And the second is the attack method using the correlation between energy samples and Hamming distance. Correlation energy analysis was proposed by Brier et al. in 2004 [16]. This method is based on Hamming distance model. Due to the observability of the side-channel information and the predictability of the intermediate variables, the analysis method uses the statistical approach to analyze the correlation degree between the intermediate value obtained by the guessed key and the actual energy, and the absolute value of the correlation coefficient is positively correlated with the correct probability of the guessed key. However, the correlation energy analysis method has some limitations. The cryptographic algorithm can use effectively use a mask to resist the correlation energy attack. It is almost impossible to successfully obtain the key through the traditional correlation energy analysis method in many scenarios.

4.3. Differential Fault Analysis

Eli Biham and others proposed differential fault analysis in 1999. It is a powerful cryptanalysis method combining fault analysis and differential analysis [17]. It is suitable for most key cryptosystems on the market. The main idea of differential cryptanalysis is to induce the failure in the process of cipher encryption, generate the wrong ciphertext, and make differential analysis between the wrong ciphertext and the correct ciphertext to obtain the right key or part of the key. Differential cryptanalysis can crack not only the key of a known cryptographic algorithm, but also the key of an unknown cryptographic system. Differential cryptanalysis introduces an asymmetric fault model, which can also obtain the key in tamper-proof cryptographic equipment without knowing the structure and encryption mode of the cryptographic system.

Differential fault analysis has two key steps: fault induction and differential analysis. Differential cryptanalysis can be referred to in the literature for detailed understanding. Fault induction introduces fault in the key-encryption process, resulting in the wrong ciphertext. In the literature, Eli Biham et al. first assumed to use the instantaneous fault model, but this fault model has not been verified physically, and there are many disputes. Then they proposed a more practical and straightforward fault model. During the operation of the cryptographic equipment, use a narrow laser beam to cut off a wire or permanently destroy a storage unit in the cryptographic equipment. This model allows ciphertext-only attacks, and only a tiny amount of ciphertext information corresponding to unknown plaintext is needed to recover the key. This is a highly efficient attack method, which poses a significant threat to the security of cryptographic devices. Therefore, it is necessary to strengthen the protection of cryptographic devices to prevent attackers from attacking the cryptographic system.

5. Quantum Computation Cryptanalysis

IMany research works have combined some quantum algorithms to achieve more efficient quantum attacks in cryptanalysis in recent years. The most widely used is the nested use of the Grover algorithm and the Simon algorithm [18]. For example, Leander and May combine the Grover algorithm and the Simon algorithm to crack FX-based block ciphers, using the Simon algorithm as the internal decision function and the Grover algorithm as the internal search algorithm.

The Grover-meet-Simon algorithm is not a simple combination of the Grover algorithm and the Simon algorithm. This is an entirely new quantum algorithm, although at a higher level, it is a simple matter to combine Grover's algorithm with Simon's algorithm [19]. The main obstacle to combining the Grover algorithm and the Simon algorithm is the difference in the initial design of the two algorithms: the Simon quantum algorithm extracts the information of the cryptographic algorithm cycle bit by bit. In contrast, the Grover quantum search algorithm requires that all information can be used immediately. It solves this problem by executing multiple Simon algorithms in parallel.

6. Conclusion

This paper introduces the current, more mature commercial cryptanalysis methods. According to the classification of cryptanalysis technology and the way of cryptanalysis, this paper expounds on cryptanalysis technology’s specific principle and corresponding execution steps. It analyzes the adaptation scenarios, advantages and disadvantages of each cryptanalysis technology. The traditional cryptanalysis algorithm has been developed for a long time. The improvement of computer computing power provides more possibilities for the traditional password cracking methods based on mathematical problems. However, the traditional cryptanalysis algorithm will consume many resources, and the efficiency is not high if it wants to crack the new password algorithm. After more than 20 years of development, the side channel cryptanalysis technology has also matured. Energy analysis technology and fault analysis technology have high efficiency in cryptanalysis, and the key information can be obtained without mathematical derivation. The attack of side-channel analysis technology is not considered in the early design of

cryptographic algorithms. The cryptographic equipment is not protected, so it is easy to disclose the key information through the side channel information of cryptographic equipment. In recent years, new cryptographic devices have been resistant to side-channel analysis, and classical side-channel analysis techniques cannot effectively crack key information unless further unknown details are found in cryptographic devices. The rapid development of quantum computing has injected new impetus into the development of cryptography. Quantum computing provides a computational power guarantee for cryptanalysis and can greatly improve the efficiency of cryptanalysis. Some cryptographic algorithms that cannot be deciphered by traditional cryptanalysis or need to consume many computing resources are easily broken under quantum computing attacks; at least, they can significant shorten the time required to break the cryptographic algorithm. The research focus in cryptography is the post-quantum cryptography algorithm, also known as the anti-quantum cryptography algorithm. Anti-quantum cryptography algorithm is a cryptographic algorithm that can resist traditional cryptographic attacks and quantum computing attacks in theory. Still, there is no complete set of standards on anti-quantum cryptography. NIST (National Institute of Standards and Technology) has carried out several anti-quantum cryptography algorithm solicitation activities in 2016. It can be seen that the development of anti-quantum cryptography is of great significance to the security of cryptographic systems and is the focus of cryptography research in the future.

Acknowledgements

I would like to thank the Beijing Science and technology plan task (Z201100005820006) for our financial support. At the same time, I would also like to thank the authors of references and relevant researchers. Their research has given me essential concerns and helpful and provided a good connection for completing my thesis.

References

[1] Yao Jian, Domestic Commercial Cryptographic Algorithm and Its Performance Analysis. Computer Applications and Software, Vol 36, 2019, pp. 327-333.

[2] Xie Zongxiao, Dong Shengxiang, Zhen Jie, Nternational Standardization of Domestic Commercial Cryptographic Algorithms and Their Corresponding Relations. China Standards Review, Vol 5, 2021, pp. 20-23, 29.

[3] Wang Rong, Xie Wei, Cao Yan, Lu Peng, A Study on the Current Situation and Development Countermeasures of Commercial Cryptography Management in China. Information Security and Communications Privacy, Vol 3, 2020, pp. 83-90.

[4] Chen Hong, Zhao Hongrui, Construction of legal system of commercial password information security with Chinese characteristics from the perspective of national security. Information Security And Communications Privacy, Vol 6, 2020, pp. 29-35.

[5] Huo Wei, Thoughts on Several Issues of Commercial Cryptography Application and Innovation Development. Journal of Information Securyity Research, Vol 6, 2020, pp. 958-965.

[6] Chen Weijian, Differential fault attack on LiCi ciphe. Chinese Journal of Network and Information Security, Vol 7, 2021, pp. 104-109.

[7] He Yeping, Wu Wenling, Qin Sihan, Truncated Differential-Linear Cryptanalysis. Journal of Software, Vol 11, 2000, pp. 1294-1298.

[8] Wu Wenling, Zhang Lei, Research progress of impossible differential cryptanalysis. Journal of Systems Science and Mathematics Sciences, Vol 28, 2008, pp. 971-983.

[9] Liu Zhengbin, Differential-linear cryptanalysis of Prince ciphe. Chinese Journal of Network and Information Security, Vol 7, 2021, pp. 131-140.

[10] Tang Yonglong, The Study of Algebraic Attacks on Stream Ciphers. Computer CD Software and Applications, Vol 8, 2010, pp. 50-51, 55.

[11] Wang Zhe, Zhang Wenying, Meet-in-Middle Attack on 5-Round Squar. Computer Technology and Development, Vol 21, 2011, pp. 132-135, 139.

[12] Beth. Dempsey VOTERS SEPUP. Library Journal, Vol 135, 2010, pp. 62-73.

[13] Bellare M, Paterson K G, Rogaway P. Security of Symmetric Encryption against Mass Surveillance. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.

[14] Gu Dawu, Zhang Chi, Progress of and some comments on the research of side-channel attack for cryptosystems. Journal of Xidian University (Natural Science), Vol 48, 2021, pp. 14-21, 49.

[15] Sun Jiayi, Wei Yongzhuang, Template Attacks Against Lightweight Block Cipher Algorithm DoT. Computer Engineering, Vol 47, 2021, pp. 155-159, 165.

[16] Chen Ping, Wang Ping, Dong Gaofeng, Hu Honggang, SincNet-based Side Channel Attack. Journal of Cryptologic Reseatch, Vol 7, 2020, pp. 583-594.

[17] Xie Min, Li Jiaqi, Tian Feng, Differential Fault Attack on GOST. Journal of Cryptologic Reseatch, Vol 8 (4), 2021, pp. 630-639.

[18] Jake Tibbetts, Quantum Computing and Cryptography: Analysis, Risks, and Recommendations for Decisionmakers. Information Security and Communications Privacy, Vol 1, 2021, pp. 61-69.

[19] Wang Chao, Yao Haonan, Wang Baonan, Hu feng, Zhang Huanguo, Ji Xiangmin, Progress in Quantum Computing Cryptography Attacks. Chinese Journal of Computers, Vol 43, 2020, pp. 1691-1707.