ISSN: 2710-0588

Research on Fault Attacks of Lightweight Cryptographic Algorithms

Shukai Niu[1,2,*], Shuaiyu Huang[1,2], Shitong Zhang[1]

[1] Information Engineering College, Henan University of Science and Technology, China

[2] Henan International Joint Laboratory of Cyberspace Security Applications, Luoyang 471000, China

[*]Corresponding Author

Abstract

Fault attacks exploit fault injection techniques to compromise cryptographic systems, compromising device operations and leaking secret keys. Lightweight block cipher algorithms are suitable for resource-constrained environments, ensuring security while reducing hardware and software overhead. This paper summarizes the current research status of fault attacks on some lightweight cryptographic algorithms, including block ciphers, stream ciphers, etc. These studies are crucial for addressing system vulnerabilities, protecting personal privacy, and enhancing the stability of embedded systems. The aim of this paper is to provide comprehensive references for cryptographers, assisting in selecting suitable algorithms and defense strategies.

Keywords

Fault Attacks; Lightweight Cryptography; Block Ciphers; Attack Models; Security.

1. Introduction

With the development of digital technology, the Internet of Things (IoT) platforms are continuously evolving, and modern society's dependence on computer systems and embedded devices is becoming increasingly significant. These systems are not only responsible for storing and processing vital information but also undertake many important tasks in daily life. Alongside this, there is a growing demand for reliability and security of systems. Cryptography plays an irreplaceable role in this process, as IoT platforms, embedded devices, and computer systems rely heavily on cryptographic techniques. Consequently, cryptographic algorithms that play a primary role become the focus of our research. When it comes to cryptographic algorithms, many different algorithms and protocols are being used in various applications. For instance, AES and ECC are used in network communications, data storage, and IoT devices, 3DES is utilized in the financial sector, and RSA is employed for digital signatures, key exchange, and encrypted communication. In this context, fault analysis, as a crucial research area, is becoming an indispensable tool for ensuring system reliability and resilience against malicious attacks.

This paper aims to study and summarize the fault attacks on some lightweight cryptographic algorithms currently in use, hoping to provide direction and reference for current research on lightweight cryptography. We will primarily focus on the research status of fault attacks on cryptographic algorithms and highlight what we consider to be the most valuable aspects.

ISSN: 2710-0588

2. Research Status of Fault Attacks on Lightweight Block Cipher Algorithms

Block cipher algorithms are cryptographic algorithms that process input data in blocks. They divide the input data into fixed-size blocks and apply a series of encryption operations to each data block. The encryption process for each data block involves keys and rounds, transforming plaintext data into ciphertext data through multiple rounds of encryption transformations.

Common block cipher algorithms include DES, AES, and 3DES, among others. These algorithms employ different encryption techniques and key lengths to provide varying levels of security.

In 2015, JUNKO TAKAHASHI et al. conducted a differential fault analysis by examining the characteristics of the AND operation in SIMON's nonlinear function. They then assessed the number of fault injections required to obtain the secret key. They were the first to demonstrate how to extract the complete secret key for all parameters of the SIMON series using a real fault model based on random faults. This research provided new insights into the field of fault analysis.

In 2016, Zhang Wenwen et al. proposed a method for conducting impossible differential fault attacks on the LED algorithm using a half-byte fault model for the first time. They successfully injected faults before the last three rounds, thereby expanding the scope of fault injection. The research results demonstrated the vulnerability of the LED algorithm to impossible differential fault attacks. While in 2017, Li Wei et al. introduced a novel statistical fault analysis method for the LED algorithm. They utilized a half-byte fault model and conducted statistical analysis using SEI differentiator, GF differentiator, and GF-SEI combined differentiator. This attack method not only could be achieved under chosen ciphertext attack conditions but also improved the efficiency of fault attacks and reduced the number of faults.

In 2018, Wang Yongjuan et al. utilized the differential non-uniformity of the S-box to inject two faults in the last round of MIBS. By establishing relationships between plaintext differentials, ciphertext differentials, and candidate input values, they were able to rapidly recover the final round key and subsequently obtain all the keys.

In 2019, DUC-PHONG LE et al. proposed a simplified Grobner basis algorithm to address fault systems. They demonstrated that this method could fully crack the SIMON cipher with only 3 to 5 injected faults. They combined fault attacks with modern SAT solvers. By guessing some key bits and injecting a single fault only in the T-th round (where T is the number of rounds in the SIMON cipher), this combined attack successfully recovered the master key of the cipher. Also in the same year, PATRANABIS et al. proposed the first practically feasible fault attack assisted by side-channel information. This attack targets any block cipher employing position permutation with optimal diffusion. It can efficiently retrieve round keys using random half-byte faults. Their experimental results showed that a combined attack could recover the last round keys of PRESENT-80 and GIFT-128 using 4 random half-byte fault injections optimally. On average, the number of random half-byte faults required for PRESENT-80 and GIFT-128 was 9-18 and 6-9, respectively. In the same year, WANG Tao et al. established correspondences for the LBlock algorithm, enabling the rapid and intuitive narrowing down of input value ranges and subsequently determining corresponding expanded keys. They applied this optimization scheme to the LBlock lightweight block cipher algorithm. Injecting 2 faults with a width of 16 bits at the input of the last round could recover the last round key. Then, they pushed the state back one round and injected 2 faults with a width of 16 bits at the input of the second-to-last round to recover the second-to-last round key. This method reduced the computational complexity of key recovery to 219.At the same year, LI Wei et al. proposed a new ciphertext-only fault analysis method for the MIBS cipher system. Attackers could use a new fault model of double AND and two new differentiators, Parzen-HW and Parzen-HW-MLE, to crack MIBS.

ISSN: 2710-0588

This method further reduces fault injection and time, effectively improving attack efficiency. This indicates that ciphertext-only fault analysis poses a serious threat to the security of MIBS.

In 2020, XIE Min proposed and discussed a differential fault attack method against the FeW algorithm. This method employs a single-byte random fault model, introducing a single-byte random fault on the right side of the FeW algorithm's last round. It utilizes the characteristics of the linear diffusion function to obtain differential information and achieves key recovery based on the statistical distribution of S-box differentials. This method effectively attacks the FeW algorithm.

In 2021, LI Wei et al. studied the security of the TWINE cipher under chosen ciphertext attack conditions. They analyzed using a series of differentiators such as SEI, MLE, HW, and GF and could recover the TWINE cipher's master key with at least a 99% success rate.Also in 2021, LI Wei et al. proposed the security analysis of the Piccolo cipher under statistical fault analysis. They employed a series of differentiators including SEI, HW, ML, GF, and MAP under chosen ciphertext conditions to recover the Piccolo cipher's master key. Experimental results showed that the Piccolo algorithm could not resist attacks from statistical fault analysis. The newly proposed differentiators ML-MAP, MM-HW, and MM-HW-ML required only 164 and 262 faults to recover 80-bit and 128-bit master keys, respectively, effectively reducing the number of faults and enhancing attack efficiency. **Table 1** summarizes the research on block cipher.

Table 1. Fault Attacks on Block Ciphers

Cipher Algorithm	Fault Model	Fault Injection Position	Fault Injection Count	Key Recovery Method
SIMON	Random Fault	Last Round	7.82	Differential Fault Analysis
SIMON	Single Byte Fault	T-th Round	3-5	Groebner Basis Algorithm and SAT Solver
LED	Semi-Byte Fault	Last Fouth Round	48-96	Impossible Differential Fault Attack
LED	Semi-Byte Fault	Last Third Round	99	Statistical Fault Analysis
TWINE	Semi-Byte Fault	Last Third Round	8-18	Differential Fault Attack
TWINE	Semi-Byte Fault	Last Fourth Round	72	Ciphertext-Only Fault Analysis
MIBS	Double AND Fault	Last Round	2	Differential Fault Analysis
MIBS	Double AND Fault	Last Fouth Round	72	Ciphertext-Only Fault Analysis
FeW	Single Byte Fault	Right of Last Round	47.73-79.55	Differential Fault Analysis
PRESENT	Semi-Byte Fault	Last Fouth Round	4-9	Side-Channel Assisted
LBlock	16-bit Fault	Last Twice Round	4	Differential Fault Analysis
Piccolo	Semi-Byte Fault	Last Fouth Round	164-262	Statistical Fault Analysis

In recent years, fault analysis on block ciphers has primarily focused on widely-used algorithms such as PRESENT. In 2022, Huang Xiangshu et al. targeted the PRESENT algorithm and designed a multi-byte fault model. They injected random faults at arbitrary positions in the 30th and 29th rounds of the PRESENT algorithm. The number of injected bytes was not fixed. By leveraging the fault propagation paths of the PRESENT algorithm, they established relationships between

ISSN: 2710-0588

output differentials and possible input values. Through the proposed parallel S-box analysis method, they obtained the correct inputs and subsequently obtained the correct round subkeys. Finally, by analyzing the key scheduling scheme, they only needed two correct round subkeys to deduce the initial 80-bit master key. This method reduced the attack complexity from 29 to 218 and significantly reduced the average duration of round key attacks. Meanwhile, the proposed method improved the single-byte, fixed-position fault model to a multi-byte, arbitrary-position fault model, which better reflects real-world attack scenarios and reduces the requirements on fault injection devices, thereby enhancing the practicality of the method.

In 2022, Gao Yang et al. conducted research on the SLIM algorithm using a half-byte fault attack model. They analyzed the algorithm's differential diffusion patterns, combined with key expansion schemes, and proposed a fault injection strategy. They injected faults ranging from 1 to 4 half bytes in width from the 2nd to the 32nd round. Injecting a minimum of 62 sets of faults reduced the computational complexity of recovering the master key to 23.Also in the same year, Kong Man et al. utilized the characteristics of the permutation layer structure and the basic idea of differential faults to propose a differential fault attack method against the ESF algorithm. They injected 1-bit faults multiple times in the 30th round. Based on the differential characteristics of the S-box, they obtained different sets of input values for different input-output differentials and determined the unique possible input values of the S-box by taking their intersection. They analyzed and obtained the last round subkey. Using the same method, they injected 1-bit faults multiple times in the 29th and 28th rounds, combined with the last round subkey. Similarly, by exploiting the differential characteristics of the S-box, they analyzed and obtained the subkeys of the second-to-last and third-to-last rounds, requiring approximately 10 faulty ciphertexts in total. After recovering the 3-round subkeys, the computational complexity of recovering the master key was reduced to 222.

Table 2. Research on Block Ciphers After 2022

Cipher Algorithm	Key Length	Rounds	Fault Model	Injection Position	Attack Complexity
PRESENT	80/128	31	Multi-byte Random Fault	At any position in Round 30/29	218
SLIM	80	32	Half-byte Fault	At any position in Rounds 2 to 32	23
ESF	80/128	31	Single-bit Fault	At any position in Rounds 30/29/28	222
FeW	80/128	31	Single-bit Fault	Subkey in Round 30/29	225
DEFAULT	80/128	32	Cross confusion and linear code	Any position	/

In 2023, Li Wei et al. combined the design structure and implementation characteristics of the PRESENT cipher. They proposed a middle-meet statistical fault analysis method based on statistical analysis and middle-meet analysis strategy. They designed differentiators such as Pearson correlation coefficient Hamming weight, Kullback-Leibler divergence Hamming weight, and Jaccard similarity coefficient Hamming weight maximum likelihood estimator, which could break all versions of 80-bit and 128-bit original keys of the PRESENT cipher. This method attacks deeper rounds with fewer faults and less time consumption. In the same year, Yan Linyang et al. addressed the problem of the DEFAULT lightweight block cipher algorithm's vulnerability to differential fault attacks. They proposed a method to resist differential fault attacks using cross confusion and linear codes. This method implements cross confusion in redundant parts of the algorithm implementation against the algorithm structure, and protects each S-box by combining the 1-bit error correction and 4-bit error detection capabilities of

ISSN: 2710-0588

linear codes. Compared to existing protection methods, their method has significant advantages in terms of generality, fault detection effectiveness, and implementation cost. Also in 2023, Haiyan Xiao et al. considered differential fault analysis on the FeW algorithm's key scheduling algorithm. By injecting faults into the 30th and 29th round subkeys, approximately 69% of the master key bits could be recovered. Then, by brute-force searching for the remaining bits, the complete master key could be obtained. **Table 2** summarizes the research conducted after 2022.

3. Current Research Status on Fault Attacks of Lightweight Stream Cipher Algorithms

Stream cipher is a type of encryption algorithm, contrasting with block ciphers. In stream ciphers, the encryption key stream is XORed bit by bit with the plaintext stream to produce the ciphertext stream. In other words, stream ciphers encrypt data by applying the key stream to each plaintext bit individually, unlike block ciphers that process data in blocks.In 2011, SANDIP KARMAKAR et al. demonstrated that Grain-128 could also be attacked by introducing faults in the NFSR (Non-linear Feedback Shift Register). This attack required approximately 56 fault injections into the NFSR and had a computational complexity of about 221.

In 2012, Guan Jie et al. conducted a differential fault attack on the stream cipher algorithm LEX based on a bit-oriented random fault model. They concluded that it required either 96 pairs of correct/incorrect output key streams and 232 computations, or 120 pairs of correct/incorrect output key streams and 216 computations, to fully recover the 128-bit initial key. The results indicated that LEX was vulnerable to the differential fault attack.

In 2013, Jimson Mathew et al. proposed a system design approach that integrates concurrent error detection and correction with unified switching activity units for fault-tolerant cryptographic hardware design. They investigated the effectiveness of Hamming code-based error correction schemes as fault-tolerant methods in stream ciphers. The encoding was applied to stream cipher implementations based on Linear Feedback Shift Registers (LFSR). This method was implemented on industry-standard stream ciphers such as RC4 (WEP) and W7.

In 2013, Chen Hao et al. investigated the security of the LILI-128 algorithm against differential fault attacks. The attack utilized a bit-oriented fault model and combined both differential and algebraic analysis techniques. Random single-bit faults were injected into the LFSRd of the LILI-128 algorithm, resulting in an algebraic system of equations regarding the internal state of the LILI-128 algorithm. The Crypto MiniSAT solver was then employed to solve and recover the 128-bit initial key. Experimental results demonstrated that the security of the LILI-128 cipher implementation was vulnerable to the threat of differential fault attacks. Thus, countermeasures against fault attacks on encryption devices are necessary to enhance the security of the LILI-128 implementation.

In 2014, Chen Hao et al. introduced an algebraic fault attack method for the first time against the Helix stream cipher algorithm. By combining algebraic attacks with differential fault attacks, they proposed a general algebraic fault attack model targeting the modular addition operation structure in the Helix algorithm. By selecting plaintexts and injecting faults, they constructed algebraic equations for Helix under this model and used the CryptoMiniSAT solver to solve the equation system and recover the key information.

In 2015, Liu Huiying et al. addressed the issue of existing fault attack methods on the Decimv2 stream cipher, which failed to effectively utilize the Decimv2 nonlinear Boolean function differential characteristics, resulting in high attack complexity. They proposed an improved differential fault attack method by injecting bit-oriented random faults into the linear feedback shift register (LF-SR) of Decimv2. This method constructed a system of linear equations for the internal state of the algorithm and solved the equations to recover the initial key K.

ISSN: 2710-0588

Experimental results showed that the overall attack complexity was reduced from the existing O(242.5) to O(238.95).

In 2016, F.E.POTESTAD-ORDOEZ et al. presented experimental fault injection attacks on the FPGA implementation of the Trivium stream cipher. In the same year, Zhang Zhongya, Guan Jie, et al. conducted a differential fault attack on Phelix using a bit-oriented fault induction model. Theoretically, this attack only required 652 single-bit faults to fully recover the 256-bit working key, with a computational complexity of O(220). Experimental results demonstrated that the Phelix algorithm was vulnerable to differential fault attacks.

In 2021, Qiao Qinglan borrowed from Banik et al.'s proposed location identification algorithm for the Grain algorithm and introduced a signature vector-based fault location detection method suitable for Fruitv2 and Fruit-80. Experimental results demonstrated that Fruitv2, Fruit-80, and Fruit128 were easier to determine the injected fault positions compared to Sprout and Plantlet.**Table 3** summarizes the research of Stream Cipher Algorithms.

Table 3. Fault Attack Research on Stream Cipher Algorithms

Algorithm	Attack Method	Attack Result
Grain-128	Fault Injection Attack	Approximately 56 fault injections are needed, with a computational complexity of about 2^21.
LEX	Differential Fault Attack	280 single-bit fault injections can completely recover the 128-bit key in less than 1 minute.
Helix	Algebraic Fault Attack	Recovery of key information using a general algebraic fault attack model.
Decimv2	Improved Differential Fault Attack	On average, 2 fault injections can recover the entire 80-bit initial key, with reduced computational complexity.
Trivium	Experimental Fault Insertion Attack	Vulnerable to attacks, and fault positions cannot be estimated through time analysis.
Phelix	Differential Fault Attack	Theoretically, only 652 single-bit fault injections are needed to completely recover the 256-bit working key.
Fruit Series (Fruitv2, Fruit-80, Fruit128)	Signature Vector-based Fault Location Detection	Easier determination of injected fault locations.

4. Research Status of Fault Attacks on Lightweight Hybrid Cipher Algorithms

Hybrid cryptography refers to the combination of multiple cryptographic techniques of different types to enhance overall security and efficiency. Hybrid ciphers typically combine symmetric and asymmetric encryption technologies to balance the convenience of key management with the security of data transmission.

In hybrid cryptography systems, asymmetric encryption techniques are typically used to address key distribution and exchange issues, while symmetric encryption techniques are employed for actual data encryption and decryption processes. In a typical hybrid cryptography system, the sender encrypts a symmetric key with the recipient's public key and then sends the encrypted symmetric key along with the data encrypted using the symmetric key to the recipient. The recipient decrypts the symmetric key using their private key and then uses the symmetric key to decrypt the data.

Hybrid cryptography systems are widely used in areas such as secure communication, e-commerce, digital signatures, and more, providing crucial technical support for safeguarding the security and integrity of data.

ISSN: 2710-0588

In 2013, Zhang Kai, Guan Jie, Zhang Zhongya, et al. addressed the security issues in the sequence design of the SCB (senior cross breed) algorithm. With known sequence-generated keystream, they recovered the algorithm's seed key with a computational complexity of O(244). To obtain the keystream required for the sequence part attack, based on a single-bit random fault model, they conducted a differential fault attack on the grouping part of the SCB algorithm. With the introduction of 640 faults, the success rate of the attack algorithm reached 99.4%. The computational complexity required for recovering the 256-bit seed key was O(244).

5. Conclusion

This paper provides a summary of recent research on fault attacks on lightweight cryptography, aiming to offer a comprehensive reference for cryptographers, aiding their understanding of the development status and future trends of fault attacks and lightweight block cipher algorithms. It also aims to assist in selecting appropriate algorithms and defense strategies in different scenarios. The paper acknowledges that fault attacks and lightweight block cipher algorithms are two significant directions in the field of cryptography, with wide-ranging applications and challenges in areas such as the Internet of Things, embedded devices, and network security. It emphasizes the importance of further in-depth research and exploration in these areas.

Acknowledgments

This work was supported by Undergraduate Training Program for Innovation and Entrepreneurship of Henan University of Science and Technology (No. 2023128),Joint Fund Project of Science and Technology Research and Development Plan of Henan Province (Application Research) (No. 232103810042), Program for Henan Province Key Science and Technology (No. 222102210177, 232102211060, 242102211077, 242102210140), Research and Practice Project of Higher Education Teaching Reform (No. 2024BK174).

References

[1] JUNKO TAKAHASHI, TOSHINORI FUKUNAGA. Fault Analysis on SIMON Family of Lightweight Block Ciphers[C]. //Information security and cryptology: ICISC 2014, 17th International Conference, Seoul, South Korea, December 3-5, 2014, Revised Selected Papers.:Springer, 2015:175-189.

[2] Li W, Ge C Y, Gu D W, et al. Statistical Fault Analysis of LED Lightweight Cipher Algorithm in Internet of Things Environment[J]. Journal of Computer Research and Development, 2017, 54(10): 2205-2214. DOI:10.7544/issn1000-1239.2017.20170437.

[3] Wang Y J, Zhang S Y, Wang T, et al. Differential Fault Attack on MIBS Block Cipher[J]. Journal of University of Electronic Science and Technology of China, 2018, 47(4): 601-605. DOI:10.3969/j.issn.1001-0548.2018.04.020.

[4] DUC-PHONG LE, YEO, SZE LING, KHOO, KHOONGMING. Algebraic Differential Fault Analysis on SIMON Block Cipher[J]. IEEE Transactions on Computers,2019,68(11):1561-1572. DOI:10.1109/TC.2019.2926081.

[5] PATRANABIS, SIKHAR, DATTA, NILANJAN, JAP, DIRMANTO, et al. SCADFA: Combined SCA+DFA Attacks on Block Ciphers with Practical Validations[J]. IEEE Transactions on Computers, 2019, 68(10):1498-1510. DOI:10.1109/TC.2019.2913644.

[6] Wang T, Wang Y J, Gao Y, et al. Differential Fault Attack on Lightweight Block Cipher Algorithm LBlock[J]. Journal of Cryptologic Research, 2019, 6(1): 18-26. DOI:10.13868/j.cnki.jcr.000279.

[7] Li W, Cao S, Gu D W, et al. Chosen Ciphertext Fault Analysis of MIBS Lightweight Cipher in Internet of Things[J]. Journal of Computer Research and Development, 2019, 56(10): 2216-2228. DOI:10.7544/issn1000-1239.2019.20190406.

ISSN: 2710-0588

[8] Xie M, Li J, Tian F. Differential Fault Attack on FeW[J]. Journal on Communications, 2020, 41(4): 143-149. DOI:10.11959/j.issn.1000-436x.2020077.

[9] Li W, Wang M, Gu D, et al. Only Ciphertext Fault Analysis of Lightweight Cryptographic Algorithm TWINE[J]. Journal on Communications, 2021, 42(3): 135-149. DOI:10.11959/j.issn.1000-436x. 2021039.

[10] Li W, Li JY, Gu DW, et al. Statistical Fault Analysis of Lightweight Cryptographic Algorithm Piccolo[J]. Chinese Journal of Computers, 2021, 44(10): 2104-2121. DOI:10.11897/SP.J.1016.2021.02104.

[11] Huang X, Wang M, Du Z, et al. Random Differential Fault Attack Against Lightweight Block Cipher Algorithm PRESENT[J]. Journal of Chengdu University of Information Technology, 2022, 37(1): 8-15. DOI:10.16836/j.cnki.jcuit.2022.01.002.

[12] Kong M, Tan L, Wang Y, et al. Improved Differential Fault Attack Based on ESF Cipher Algorithm[J]. Journal of Computer Systems and Applications, 2022, 31(10): 288-294. DOI:10.15888/j.cnki.csa. 008764.

[13] Li W, Zhu X, Gu D, et al. Midway Collision Statistical Fault Analysis of the PRESENT Lightweight Cipher[J]. Chinese Journal of Computers, 2023, 46(2): 353-370. DOI:10.11897/SP.J.1016.2023. 00353.

[14] Yan L, Hao J, Li L. A New Method for Resisting Differential Fault Attacks on DEFAULT Cipher Algorithm[J]. Journal of Guilin University of Electronic Technology, 2023, 43(3): 223-230. DOI:10.3969/j.issn.1673-808X.2023.03.008.

[15] Haiyan Xiao, Lifang Wang, Jinyong Chang. The differential fault analysis on block cipher FeW[J]. Journal of Cyberspace Security Science and Technology, 2023, 6(2): 62-74.

[16] Sandip Karmakar, Dipanwita Roy Chowdhury. Fault Analysis of Grain-128 by Targeting NFSR[C]. In: Progress in Cryptology - AFRICACRYPT 2011. Springer, 2011: 298-315.

[17] Jimson Mathew, Saraju P. Mohanty, Shibaji Banerjee, et al. Attack tolerant cryptographic hardware design by combining error correction and uniform switching activity. Computers and Electrical Engineering, 2013, 39(4): 1077-1087. DOI: 10.1016/j.compeleceng.2013.01.001.

[18] Zhang Zhongya, Guan Jie. Differential fault attack on stream cipher algorithm LEX. Journal of Shanghai Jiaotong University, 2012, 46(6): 865-869, 875.

[19] Chen Hao, Wang Tao, Liu Huiying. Differential fault attack on stream cipher LILI-128. Journal of Computer Applications Research, 2013, 30(11): 3396-3399. DOI:10.3969/j.issn.1001-3695.2013. 11.049.

[20] Chen Hao, Wang Tao, Liu Huiying, et al. Algebraic fault attack on stream cipher Helix. Computer Engineering and Design, 2014, 35(2): 445-450. DOI:10.3969/j.issn.1000-7024.2014.02.017.

[21] Chen Hao, Wang Tao, Liu Huiying, et al. Differential fault attack on stream cipher Decimv2. Journal of Chinese Computer Systems, 2015, 36(1): 150-155.

[22] F. E. Potestad-Ordóñez, C. J. Jiménez-Fernández, M. Valencia-Barrero. Experimental and timing analysis comparison of FPGA Trivium implementations and their vulnerability to clock fault injection. In: 2016 Conference on Design of Circuits and Integrated Systems (DCIS), November 23-25, 2016, Granada, Spain. Institute of Electrical and Electronics Engineers, 2016: 1-6.

[23] Zhang Zhongya, Guan Jie. Differential Fault Attack on Stream Cipher Algorithm Phelix. In: Proceedings of the 8th National Conference on Technical Process Fault Diagnosis and Security, 2016: 1131-1136, 1142.

[24] Qiao Qinglan. Differential Fault Attack on Lightweight Stream Cipher Family Fruit. [Dissertation]. Shaanxi: Xidian University, 2021.

[25] Zhang Kai, Guan Jie, Zhang Zhongya, et al. Key Recovery Attack on Hybrid Cipher SCB Algorithm. [J]. Journal of Peking University (Natural Science Edition), 2013, 49(3): 397-403.

[26] Zhang Wenwen. Fault Attack Research on Lightweight Block Ciphers LED and TWINE Algorithm [D]. Shanghai: Donghua University, 2016.

[27] Gao Yang, Wang Yongjuan, Gao Guangpu, et al. Differential Fault Attack on Lightweight Block Cipher SLIM[J]. Journal of Cryptologic Research, 2022, 9(2): 223-236. DOI:10.13868/j.cnki.jcr.000514.