sensors

MDPI

Article

# An Effective Simulation Analysis of Transient Electromagnetic Multiple Faults

**Liang Dong [1,2], Hongxin Zhang [1,*], Shaofei Sun [1], Lei Zhu [2], Xiaotong Cui [1] and Bablu K. Ghosh [3]**

1 School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China; dongliang@163.com (L.D.); sfsun@bupt.edu.cn (S.S.); cuixiaotong@bupt.edu.cn (X.C.)
2 Communication and Electronic Engineering Institute, Qiqihar University, Qiqihar 161006, China; zhuzhubutterfly@163.com
3 Faculty of Engineering, University Malaysia Sabah, Kota Kinabalu 88400, Malaysia; ghoshbab@ums.edu.my
* Correspondence: hongxinzhang@bupt.edu.cn

Received: 20 February 2020; Accepted: 30 March 2020; Published: 1 April 2020

**Abstract:** Embedded encryption devices and smart sensors are vulnerable to physical attacks. Due to the continuous shrinking of chip size, laser injection, particle radiation and electromagnetic transient injection are possible methods that introduce transient multiple faults. In the fault analysis stage, the adversary is unclear about the actual number of faults injected. Typically, the single-nibble fault analysis encounters difficulties. Therefore, in this paper, we propose novel ciphertext-only impossible differentials that can analyze the number of random faults to six nibbles. We use the impossible differentials to exclude the secret key that definitely does not exist, and then gradually obtain the unique secret key through inverse difference equations. Using software simulation, we conducted 32,000 random multiple fault attacks on Midori. The experiments were carried out to verify the theoretical model of multiple fault attacks. We obtain the relationship between fault injection and information content. To reduce the number of fault attacks, we further optimized the fault attack method. The secret key can be obtained at least 11 times. The proposed ciphertext-only impossible differential analysis provides an effective method for random multiple faults analysis, which would be helpful for improving the security of block ciphers.

**Keywords:** transient electromagnetic injection; ciphertext-only fault analysis; Midori; random multiple fault attacks; differential attack

## 1. Introduction

With the rapid growth of Internet of Things (IoT) applications, people's productivity and daily lives have changed. People are enjoying the convenience of intelligent sensor network services; simultaneously, information security is essential. The potential attacks in IoT networks are increasing. The most exposed and vulnerable devices in IoT are routers, cameras, network attached storage (NAS) and printers, as shown in Figure 1. The private data collected by the intelligent sensor networks are carried by the underlying chips and transmitted to networks for data exchanges and data analysis. However, the attacker can obtain the secret key from the chip by performing physical attacks on the target chip. After the fault attacks are injected into the chip, the attackers can steal users' private data; maliciously attack the network terminal nodes; and monitor and tamper with the sensitive data in the network. Therefore, physical attacks cause considerable harm to smart sensors and embedded encryption devices in the IoT.

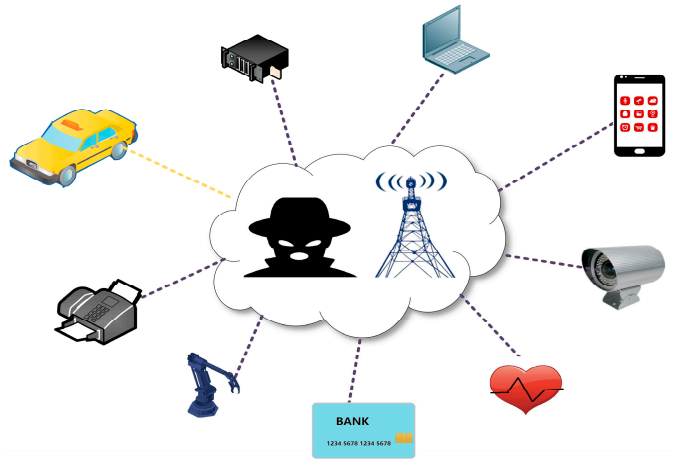


**Figure 1.** Attack scenario in the Internet of Things (IoT).

Physical attacks have attracted widespread attention in lightweight block ciphers. One method to analyze lightweight block ciphers is directly through electromagnetic radiation using methods such as simple electromagnetic analysis (SEMA) [1], correlation electromagnetic analysis (CEMA) [2] and differential electromagnetic analysis (DEMA) [3]. Other methods involve using clock disturbance, electromagnetic fault injection and laser fault injection [4–6] on the specified data registers by analyzing the fault ciphertext to obtain the secret key. Laser fault injection can inject bit-level faults in the specified data register, but the instrument for fault injection is more expensive. However, the manufacturing cost of the electromagnetic fault injection probe is lower. Dehbaoui et al. [7] and S. Ordas et al. [8] designed electromagnetic probes and used electromagnetic attacks to implement bit set or bit reset of data in the chip. Accurately injecting the fault into the encryption device is a prerequisite for obtaining the secret key. After the fault is injected, a proper fault analysis method is required to further obtain the secret key. Since Boneh et al. [9] used fault attacks to break RSA, effective fault analysis methods have become research hotspot. In lightweight block encryption analysis, fault attacks have been extended to impossible differential fault attack (IDFA) [10], impossible differential attack (IDA) [11,12], algebraic fault attack (AFA) [13], impossible meet-in-the-middle attack (IMMA) [14], differential fault attack (DFA) [15] and blind fault attack [16]. These methods mainly analyze the characteristic relationship between the data of the cryptosystem after the injection fault and obtain the secret key by means of solver and mathematical analysis.

The secret key can be quickly obtained by an appropriate fault analysis model. The proposed fault attack models mainly include the random single-byte [17], random single-nibble model [15], one-bit model [18] and diagonal model [19]. In addition to the fault analysis models proposed above, several novel fault attack models, such as persistent fault attack (PFA) [20] and rebound attack (RA) [21], were proposed. The proposed fault analysis models include a few random multiple fault attack models. However, transient multiple fault attacks occur during an electromagnetic transient fault injection [22,23]. Therefore, studying the random multiple fault attack model has important practical significance for fault analysis.

Single bit fault [24] and single nibble fault analysis models are widely used in high precision laser fault attacks. However, the attackers can use less sophisticated electromagnetic fault injection to attack sensors in IoT. An electromagnetic fault attack firstly introduces a transient fault [7,8] to the working chip by an electromagnetic probe. The correct key is obtained by collecting and analyzing the relationship between the fault and the correct data. During actual fault injection, the number and location of faults in the data register are affected by the precision of the injection equipment and the electromagnetic interference during the injection. At this time, the output electromagnetic wave injects multiple faults to the target data register. Therefore, the number and locations of random faults in the

data register cannot be predicted by the attacker. If a single nibble or single byte model is still used for analysis, the fault attack analysis fails.

Thus, IoT device security can be achieved with a lightweight cryptosystem. Midori is an energy-efficient lightweight cryptosystem proposed by Banik et al. [25]. Midori has broad application prospects in wireless sensor networks. To assess the security of Midori, many researchers developed various attack techniques on Midori. Cheng et al. [15] presented a cell-oriented fault propagation patterns on Midori. Chen et al. [11] designed 10 rounds of impossible differential paths to attack Midori-128. Shahmirzdi et al. [12] conducted three impossible differential attacks on Midori-64 with 10, 11 and 12 rounds. Nozaki et al. [26] distinguished the correct key from the error key by Hamming distance. Todo et al. [27] found a nonlinear invariant Boolean function G to distinguish the secret key.

The differential fault attack (DFA) [15,17–19] is a widely applied cryptanalysis technique. The correct and the faulty value are different at the fault point, and the attacker can obtain the secret key by analyzing differential faults. Impossible differential analysis is a powerful analysis method proposed by Knudsen [28] and Biham et al. [29]. By analyzing fault propagation paths, the elements that are absolutely impossible to exist in the key space are eliminated. As such, the correct key is obtained step by step. Differential fault attacks combine well with other attack methods, and the attack effect is significant. Many scholars applied this method to their issues. Combing differential fault analysis with algebraic attack, Jovanovic et al. [30] and Zhao et al. [13] successfully attacked LED-64 with a single fault injection. Li et al. [10] presented a novel impossible differential fault analysis on LED-64. To the best of our knowledge, a random multiple fault attack model on lightweight Midori against the impossible differential fault attack (IDFA) has not been proposed. We further optimized the proposed scheme of fault attacks during the experiment.

The major contributions of the paper are as follows:

(1) We propose an analysis model on lightweight Midori that can be used to analyze most of the random multiple fault attacks. We increase the number of analysis faults from one to six. The random multiple fault attack model can effectively analyze complex fault attacks.
(2) Through experimental simulation analysis, a linear function relationship between the number of fault attacks and the remaining key information content is obtained.
(3) The ciphertext-only fault attack is the attack method with the least known information. In this paper, the secret key is obtained by combining the impossible attack and the differential fault attack. Using the secret key invariant subspace, the secret key can be obtained by intersection of the subspace.

We summarize the results of the best-known attack on Midori-64 in Table 1. Li et al. [31] used six distinguishers to analyze the security of Midori-64. Among them, the hamming weight (HW) distinguisher provides the most effective fault analysis. However, the method can only analyze a random-nibble fault in the 15th round, and the number of fault injections is high. Cheng et al. [15] injected a random-nibble fault into the data register. By analyzing the differential fault propagation path of Midori, they found four invariant fault differential patterns. By analyzing these patterns to estimate the location where the fault was injected, they obtained the secret key. However, Cheng et al. [15] were only able to recover 80% of the secret key, and they did not discuss multiple fault injections. Our proposed method can be used not only analyze multiple random faults but also requires fewer fault injections. At least 11 fault injections are required to obtain the secret key. At present, the problem of multiple faults in data registers has been ignored by researchers. Analyzing the propagation of multiple fault differentials and using the combination of impossible fault attacks and differential fault attacks to improve the security of the lightweight cryptosystem in the case of multiple faults were the motivations of this study.

**Table 1.** Comparison of this work with previous fault attacks on Midori-64.

| Reference | Fault Model | | | | | Number of Faults |
|---|---|---|---|---|---|---|
| | Method | Probability | Round | Value | Distinguish multiple- nibble fault | |
| [31] | HW | 100% | R = 15 | 1 Nibble | No | 280 |
| [15] | DFA | 80% | R = 14 | 1 Nibble | No | 2 |
| this paper | IDFA | 100% | R = 14 | 1–6 Nibble(s) | Yes | 11 |

The rest of this article is divided into the following sections. In Section 2, we briefly describe Midori. In Section 3, we propose a random multiple fault attack model. In Section 4, we provide a detailed calculation for the model. In Section 5, we describe the experimental results. In the last section, we conclude this paper.

## 2. Specifications of Midori and Symbol Description

### 2.1. Midori

Midori is an energy-optimized, lightweight cryptosystem that can be used in resource-constrained circuits. Midori-64 and Midori-128 are two cryptosystems with 16 and 20 rounds, respectively. The round function of Midori is KeyAdd, SubCell (SB), ShuffleCell (SC), MixColumn (MC) and Round Constants (RC) in sequence, as shown in Figure 2.

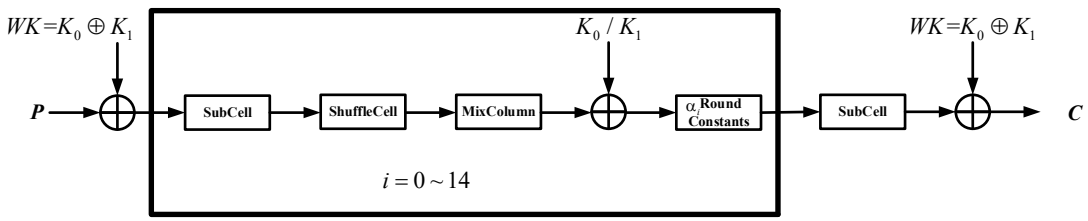


**Figure 2.** Overall structure of Midori-64.

(1) The KeyAdd operation uses the XOR operator with the key. The key of the first round and the last round is the key whitening operation. From the 2nd to the 15th round, $K_0$ and $K_1$ alternately XORed with the round function in the cryptosystem.
(2) SubCell transform is the only non-linear operation. SubCell operation minimizes the bit flip between input and output. Forward and inverse S-boxes are the same mathematical form.
(3) ShuffleCell rearranges the cell position in a fixed order.
(4) The MixColumn and inverse MixColumn operations are multiplied by the following matrix:

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

(5) Round Constants operation is XORed by the form of $4 \times 4$ binary matrices.

### 2.2. Symbol Description

The following notation is used to describe the analysis of Midori. Let $C$ be the right ciphertext and $C^*$ be the faulty ciphertext. Let $X^L \in (\{0,1\}^4)^{16}$, $Y^L \in (\{0,1\}^4)^{16}$, $Z^L \in (\{0,1\}^4)^{16}$ and $W^L \in (\{0,1\}^4)^{16}$ denote the output value of the Round Constants, SubCell, ShuffleCell and MixColumn layers in the $L$-th round with $1 \leq L \leq 16$, respectively. Let $\Delta X^L$, $\Delta Y^L$, $\Delta Z^L$ and $\Delta W^L$ denote the output difference of

$X$, $Y$, $Z$ and $W$ in the $L$-th round, respectively. Equation (1) denotes each nibble in $\Delta X^L$, $\Delta Y^L$, $\Delta Z^L$ and $\Delta W^L$, respectively.

$$\begin{cases} \Delta X^L = (\Delta x^L_{\{1,1\}}, \Delta x^L_{\{i,j\}}, \cdots, \Delta x^L_{\{4,4\}}) \\ \Delta Y^L = (\Delta y^L_{\{1,1\}}, \Delta y^L_{\{i,j\}}, \cdots, \Delta y^L_{\{4,4\}}) \\ \Delta Z^L = (\Delta z^L_{\{1,1\}}, \Delta z^L_{\{i,j\}}, \cdots, \Delta z^L_{\{4,4\}}) \\ \Delta W^L = (\Delta w^L_{\{1,1\}}, \Delta w^L_{\{i,j\}}, \cdots, \Delta w^L_{\{4,4\}}) \\ \qquad i = 1 \cdots 4 \ , \qquad j = 1 \cdots 4. \end{cases} \tag{1}$$

Let $\{i, j\}$ denote the $i$-th row and the $j$-th column. $\oplus$ denotes bitwise exclusive-or operation. We denote the inverse operations of Round Constants, SubCell, ShuffleCell, MixColumn by INVRC, INVSB, INVSHC and INVMC, respectively. Let $\varnothing_{\{i,j\}}$ and $\varnothing_{\{j\}}$ denote the set of $Y^{16}_{\{i,j\}}$ and $Y^{16}_{\{j\}}$ when the estimated $\Delta Z^{15}_{\{i,j\}} = 0$ and $\Delta Z^{15}_{\{j\}} = 0$, respectively. Let $\theta$ denote the intersection of $\rho$.

## 3. Random Multi-Fault Attack Model

Space particle radiation, aging of electronics and electromagnetic interference can disturb the current inside a chip. Faults are classified into intentional injection faults and unintentional injection faults. Faults can also be classified as transient faults, permanent faults and persistent faults. Compared with persistent fault injection [20], transient fault injection causes less damage to the chip. Therefore, most of the fault attacks are transient fault attacks. Although the position of the internal bit flip is related to the accuracy of the fault injection tool, the faults mentioned above have more random faults in the actual fault injection and attackers do not know. The electromagnetic waves radiated by the probe can disturb the clock circuit and the surrounding registers. Data transmission and data exchange in the chip are clock synchronized. In data transmission, setup-time and hold-time must be stable. In the process of electromagnetic fault injection, clock stability rapidly decreases, so setup-time and hold-time deviate, as shown in Figure 3. The occurrence of random multiple faults is complicated and ubiquitous. In the process of actual fault attacks analysis, we encounter very complex problems.

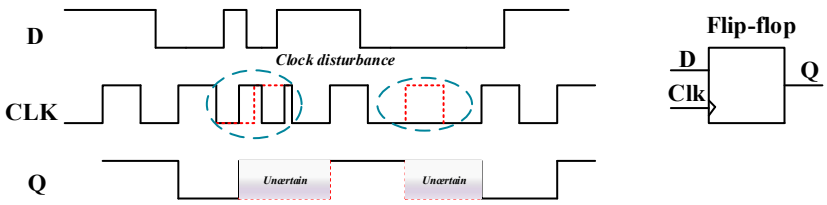


**Figure 3.** Clock disturbance of D flip-flop.

A suitable attack model is important for security analysis. If a fault attack model cannot effectively analyze actual faults, the analysis of a cryptosystem will encounter many difficulties. At present, models for multiple fault attacks are lacking. Liao et al. [32] proposed a multiple fault attack model with no more than three bytes. Using matrix diagonals, Saha et al. [19] analyzed multiple byte faults, but with relatively few types of faults. To the best of our knowledge, no random multiple fault attack model against Midori has yet been proposed. From the perspective of engineering, in this paper, a general random multiple fault model is proposed. The random multiple fault analysis model can be applied to most of the random fault attacks and improve the security of lightweight cryptosystems in IoT networks.

### *3.1. Fault Attacks Hypothesis*

This paper does not deal with the physical implementation of the attack. Fault attacks against Midori can be implemented based the following assumptions: An attacker is able to inject faults in the 14th round data register of Midori-64 and the number of the faults is no more than six. There is no fault injection in other memory elements of the crypto-hardware. After fault injection, the value of

fault registers changes and the fault location is unknown. The attacker can obtain the correct and the faulty ciphertexts after each fault injection. The attacker does not need to know the correct plaintext, so this is a ciphertext-only attack. An attacker injects multiple random faults in the 14th round of cryptosystem. As can be seen from Figure 2, the fault injection is the same in SubCell, ShuffleCell, and Round Constants. Assuming an electromagnetic fault is injected, there are four to six nibble faults. Random faults in data registers are shown in Figures 4–6. The black circle indicates the fault point. Figures 4–6 describe the distributions of four to six faults. The faults in Figures 4–6 indicate that the probability of fault occurrence of each position of the column is the same; there are zero-four faults in each column.

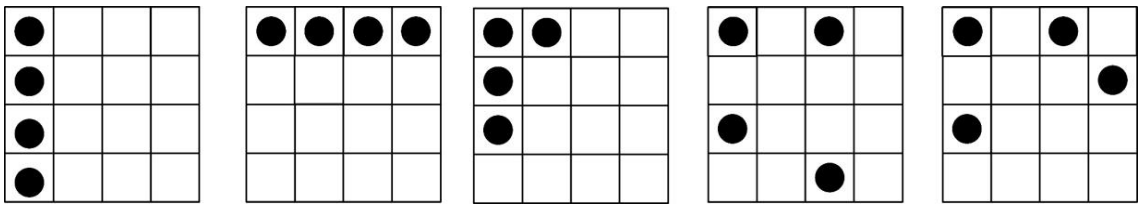

**Figure 4.** Four random faults.

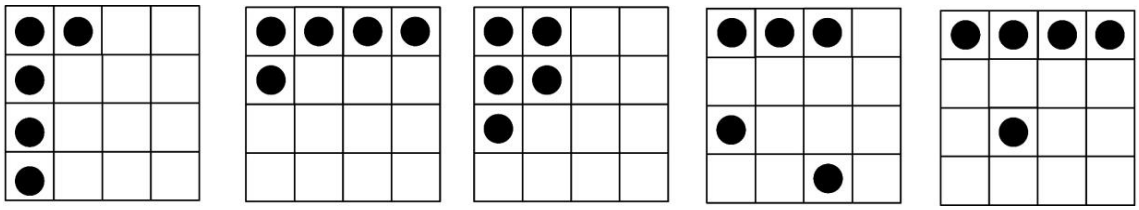

**Figure 5.** Five random faults.

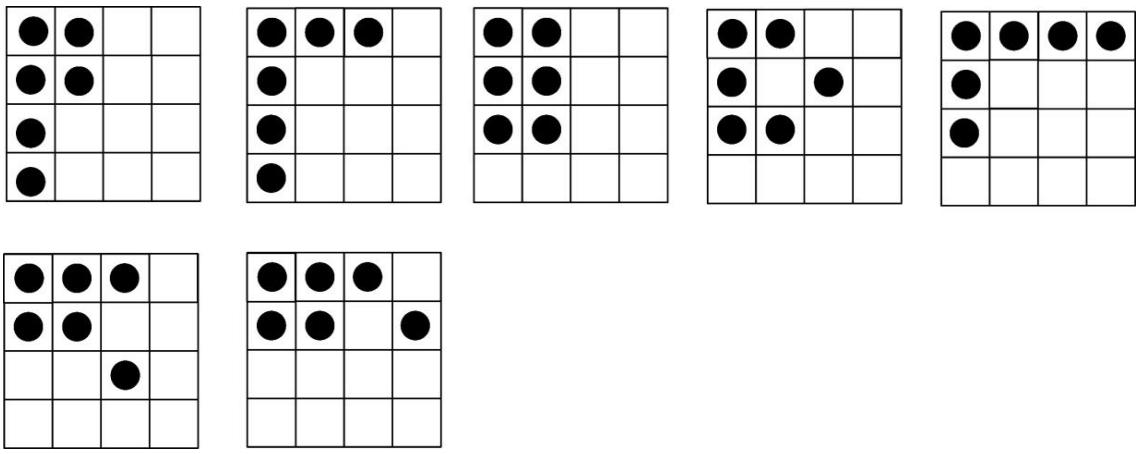

**Figure 6.** Six random faults.

### 3.2. Analysis of Random Multiple Fault Attack Models

Figure 7 shows how faults propagate when random multiple faults are injected into the 14th round. The fault state in the dashed box can be replaced by any state in Figures 4–6. According to the fault injection assumption mentioned above, the number of random faults in each column of the $\Delta X^{15}$, $\Delta Y^{15}$ and $\Delta Z^{15}$ is 0 to 4. To successfully implement random multiple fault attacks, we explain the two problems.

1. Problem 1: The location of no faults in each column of $\Delta X^{15}$, $\Delta Y^{15}$ and $\Delta Z^{15}$ is unknown. There are four positions in a column. We estimate all four fault positions as fault-free, and then take the union of the estimated invariant space in the column.

2. Problem 2: As the location and number of each fault injection are unknown, there may be 0–4 faults in a certain column of $\Delta Z^{15}$. After injecting random multiple faults two or three times into the cryptosystem, an adversary takes a fault-free union at each position of $\Delta Z^{15}$. It is possible that the number of faults in a column is four. If the adversary predicts this column as fault-free, an error will occur. To avoid mistakes, the adversary can inject faults two or three times into the cryptosystem. In other words, the adversary avoids mistakes by taking the unions multiple times. We provide a detailed explanation using the following differential fault attack equations.

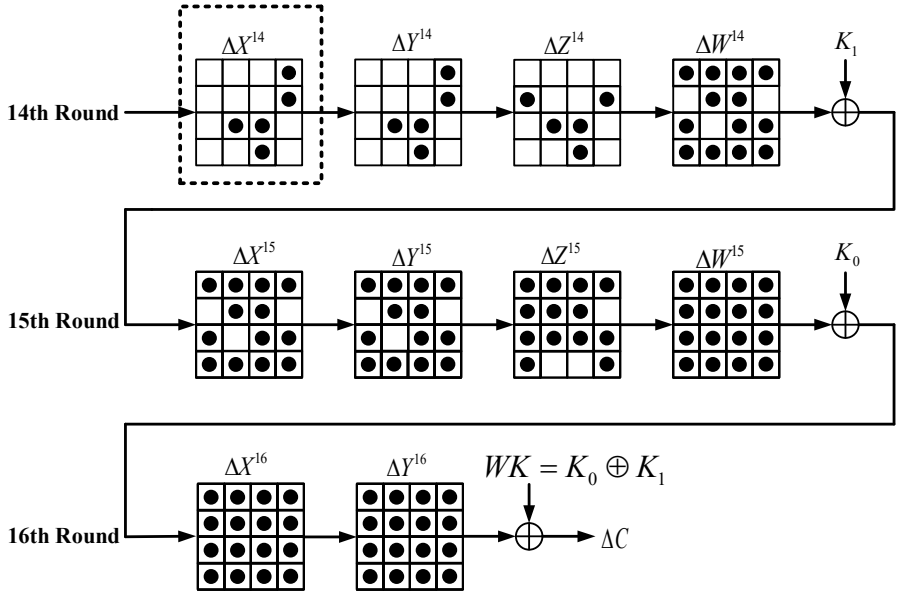


**Figure 7.** Random multiple faults' propagation paths.

## 4. Analysis of Fault Difference Equations

The analysis of the multiple differential fault path is shown in Figure 7. We perform the inverse operation through the inverse output differential of the 16th round S-box.

$$\Delta Y^{16} = \Delta C^{16} \tag{2}$$

By observing the Figure 7, we obtain the following differential equations:

$$\Delta W^{15} = \Delta X^{16} = \mathrm{INVSB}\left(\Delta Y^{16}\right) \tag{3}$$

$$\Delta Z^{15} = \mathrm{INVMIX}\left(\Delta W^{15}\right) \tag{4}$$

We can further obtain Equations (5)–(8) by expanding Equation (4).

$$\Delta Z^{15}_{\{1,1+l\}} = \mathrm{INVSB}\left(\Delta C^{16}_{\{2,1+l\}}\right) \oplus \mathrm{INVSB}(\Delta C^{16}_{\{3,1+l\}}) \oplus \mathrm{INVSB}(\Delta C^{16}_{\{4,1+l\}}) \tag{5}$$

$$\Delta Z^{15}_{\{2,1+l\}} = \mathrm{INVSB}\left(\Delta C^{16}_{\{1,1+l\}}\right) \oplus \mathrm{INVSB}(\Delta C^{16}_{\{3,1+l\}} \oplus \mathrm{INVSB}(\Delta C^{16}_{\{4,1+l\}}) \tag{6}$$

$$\Delta Z^{15}_{\{3,1+l\}} = \mathrm{INVSB}\left(\Delta C^{16}_{\{1,1+l\}}\right) \oplus \mathrm{INVSB}(\Delta C^{16}_{\{2,1+l\}} \oplus \mathrm{INVSB}(\Delta C^{16}_{\{4,1+l\}}) \tag{7}$$

$$\Delta Z^{15}_{\{4,1+l\}} = \mathrm{INVSB}\left(\Delta C^{16}_{\{1,1+l\}}\right) \oplus \mathrm{INVSB}(\Delta C^{16}_{\{2,1+l\}}) \oplus \mathrm{INVSB}(\Delta C^{16}_{\{3,1+l\}}) \tag{8}$$

$$\varnothing_{\{j\}} = \varnothing_{\{1,j\}} \cup \varnothing_{\{2,j\}} \cup \varnothing_{\{3,j\}} \cup \varnothing_{\{4,j\}} \tag{9}$$

where $j = 1, 2, 3, 4$ and $l = 0, 1, 2, 3$.

The relationship between $\Delta Z^{15}$ and $\Delta Y^{15}$ is shown in Table 2.

**Table 2.** The inverse differential of Midori.

| $\Delta Y_0^{15}$ | $\Delta Y_1^{15}$ | $\Delta Y_2^{15}$ | $\Delta Y_3^{15}$ | $\Delta Y_4^{15}$ | $\Delta Y_5^{15}$ | $\Delta Y_6^{15}$ | $\Delta Y_7^{15}$ | $\Delta Y_8^{15}$ | $\Delta Y_9^{15}$ | $\Delta Y_{10}^{15}$ | $\Delta Y_{11}^{15}$ | $\Delta Y_{12}^{15}$ | $\Delta Y_{13}^{15}$ | $\Delta Y_{14}^{15}$ | $\Delta Y_{15}^{15}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\Delta Z_0^{15}$ | $\Delta Z_7^{15}$ | $\Delta Z_{14}^{15}$ | $\Delta Z_9^{15}$ | $\Delta Z_5^{15}$ | $\Delta Z_2^{15}$ | $\Delta Z_{11}^{15}$ | $\Delta Z_{12}^{15}$ | $\Delta Z_{15}^{15}$ | $\Delta Z_8^{15}$ | $\Delta Z_1^{15}$ | $\Delta Z_6^{15}$ | $\Delta Z_{10}^{15}$ | $\Delta Z_{13}^{15}$ | $\Delta Z_4^{15}$ | $\Delta Z_3^{15}$ |

For the differential characteristics of the inverse S-box, as shown in Table 3, one input difference corresponds to multiple output differences. However, in a fault attack, the plaintext and secret key are always the same; that is, we can uniquely determine $Y^{16}$ and $Y^{15}$ by the estimation of S-box outputs.

**Table 3.** Difference distribution of Midori inverse S-box.

| γ | β |
|---|---|
| 1 | 1 2 4 5 6 8 14 |
| 2 | 1 4 9 12 |
| 3 | 4 6 7 8 9 13 15 |
| 4 | 1 2 3 4 5 8 11 |
| 5 | 1 4 7 9 10 12 |
| 6 | 1 3 7 8 12 13 15 |
| 7 | 3 5 6 11 13 14 |
| 8 | 1 3 4 6 9 11 12 14 |
| 9 | 2 3 5 8 9 11 12 |
| 10 | 5 10 13 15 |
| 11 | 4 7 8 9 11 13 15 |
| 12 | 5 6 8 9 12 14 |
| 13 | 3 6 7 10 11 14 |
| 14 | 1 7 8 12 13 14 15 |
| 15 | 3 6 10 11 14 15 |
| 0 | 0 |

$\gamma$ and $\beta$ represent inverse input and output difference, respectively.

The adversary estimates $\Delta W^{15}$ are listed in Table 2. Predicting the locations of multiple faults is impossible due to the complexity of random multiple fault injection. When the differential faults propagate to $\Delta Z^{15}$, the adversary estimates the fault-free position of $\Delta Z^{15}$, using Equations (5)–(9). Invariant space $Y^{16}$ is reduced by excluding non-zero nibbles in each column of $\Delta Z^{15}$. According to the explanations of Problems 1 and 2 above, when the adversary injects faults two or three times, the fault-free difference must exist in some columns of $\Delta Z^{15}$. After a fault attack, each column of candidate $Y^{16}$ can be expressed by the Equations (10)–(12). According to Problems 1 and 2 discussed above, the attackers independently induce faults two or three times at the 14th round and take the union of $\varnothing$, as shown in Equation (10).

$$\rho_m = \varnothing_{3m-2} \cup \varnothing_{3m-1} \cup \varnothing_{3m} (m = 1, 2, 3) \tag{10}$$

where $3m - 2$, $3m - 1$ and $3m$ represent the number of fault attacks and $m$ represents the number of $\varnothing$ unions. The attacker can obtain the set of estimated $Y^{16}$, as shown in Equations (11) and (12).

$$\theta_p = \rho_{2p-1} \cap \rho_{2p} \qquad (p = 1, 2, \cdots) \tag{11}$$

$$\omega_q = \theta_{2q-1} \cap \theta_{2q} \qquad (q = 1, 2, \cdots) \tag{12}$$

where $p$ and $q$ are the number of intersections. The attacker injects faults repeatedly until the element in $\omega_q$ is unique. During fault attacks, the elements of the set $\theta$ may be an empty set for various reasons. When $\theta$ is empty, the attacker cancels $\rho$ and re-injects random faults. Therefore, the adversary will eventually obtain a unique $Y^{16}$ by constantly injecting faults.

$$\mathrm{SB}(Y^{16}) \oplus K_0 \oplus K_1 = C \tag{13}$$

Then, $WK$ can be obtained according to the following formula:

$$WK = K_0 \oplus K_1 = C \oplus \mathrm{INVSB}(Y^{16}). \tag{14}$$

According to the key schedule of Midori, the adversary makes further derivations to obtain $K_0$. The equations are shown in Equations (15) to (19).

$$\Delta Y^{15} = \mathrm{INVSHC}(\mathrm{INVMIX}(\Delta X^{16})) \tag{15}$$

$$\Delta X^{16} = \mathrm{INVSB}(C \oplus WK) \oplus \mathrm{INVSB}(C^{*} \oplus WK) \tag{16}$$

With the method proposed above, we do not need to inject the fault again; the unique $Y^{15}$ can be recovered by the same fault attack data.

$$W^{15} = \mathrm{MC}(\mathrm{SHC}(\mathrm{SB}(Y^{15}))) \tag{17}$$

$$\mathrm{SB}\Big(\mathrm{RC}(W^{15} \oplus K_0)\Big) \oplus WK = C \tag{18}$$

$K_0$ can be obtained using Equation (19).

$$K_0 = W^{15} \oplus \mathrm{INVRC}(\mathrm{INVSB}(C \oplus WK)) \tag{19}$$

## 5. Experimental Analysis and Results

The random multiple fault attacks experiments were performed on a PC with a Core$^{\mathrm{TM}}$ i3 CPU with 4GB of RAM, using MATLAB language.

Information entropy is a method used to measure the estimation of source data. Sakiyama et al. [33] theoretically analyzed information entropy of the key leakage on S-box. However, in the multi-fault analysis for lightweight Midori, reports are absent on the secret key leakage relationship between the number of fault attacks and leak information content. To determine the relationship between the number of fault attacks and information content, we simulated 32,000 random multiple faults. Figure 8 shows a total of 32,000 curves, each colored line representing a fault attack process of the recovery secret key. Midori-64 initially needed to determine the 64-bit secret key without fault injection. With our proposed algorithm, when the intersection of the secret key space was taken about 10 times, the amount of undefined information content was reduced to five. We continued to intersect the secret key space set $\rho$; the remainder of the information content gradually reduced until all the secret keys were recovered.

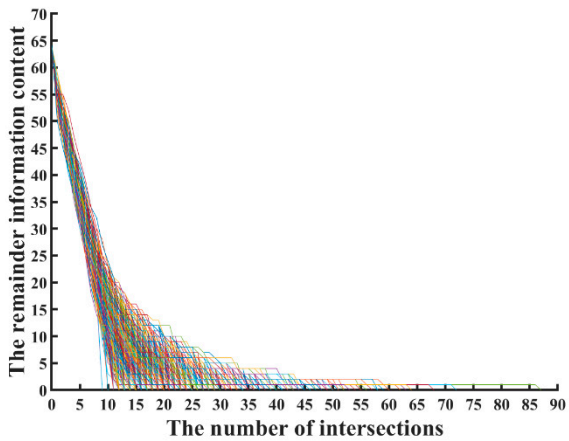


**Figure 8.** The remaining information content in 32,000 fault attacks.

To identify the relationship between predicted fault injection and the amount of information to be predicted, we took the mode (black dot) simulation fitting during 32,000 fault attacks and obtained

the functional relationship as shown below. Compared with Figure 8, the fitted graph in Figure 9 perfectly depicts the entire fault analysis process. The red curve in Figure 9 shows the boundary values of the data during the prediction process. The relationship between the number of intersections and remaining information content secret key bits is shown in Figure 9. We obtained the following formula by computer fitting:

$$y = \begin{cases} a \cdot e^{-\left(\frac{n-b}{c}\right)^2} & 0 \le n \le 26 \\ [0,3] & n \ge 27 \end{cases}, \tag{20}$$

where $y$ is the remaining information content; $n$ is the number of intersections; and $a$, $b$ and $c$ are constants. The ranges of $a$, $b$ and $c$ are: $a = 105.4\ (78.25,\ 132.6), b = -10.85\ (-14.56, -7.142)$ and $c = 14.9\ (13.18, 16.63)$.

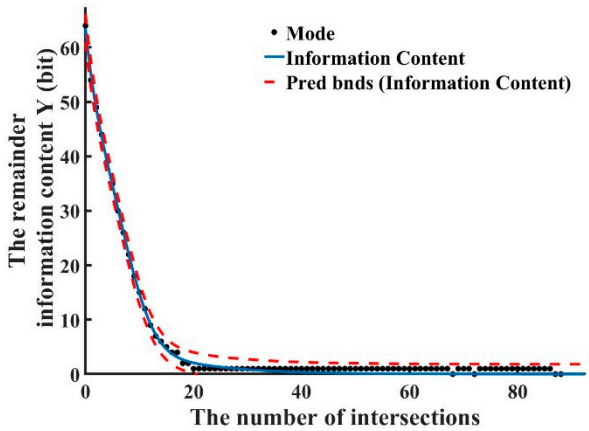


**Figure 9.** The relationship between the remaining information content and the number of intersections.

Therefore,

$$y = \begin{cases} 105.4 \cdot e^{-\left(\frac{n+10.58}{14.9}\right)^2} & 0 \le n \le 26 \\ [0,3] & n \ge 27 \end{cases} \tag{21}$$

Equation (20) shows good agreement with the experimental results. The adversary can obtain the remaining information content by taking the number of intersections into Equation (20). The remaining information content shrinks with the intersection, as shown in Figure 9. When the remaining information content is 1 bit, more faults need to be injected to make the information content 0 bit. To further explain the existence of a large number of 1-bits, we counted the remaining information content of each column during the attacks. As shown in Figure 10, the number of intersections is around 20.

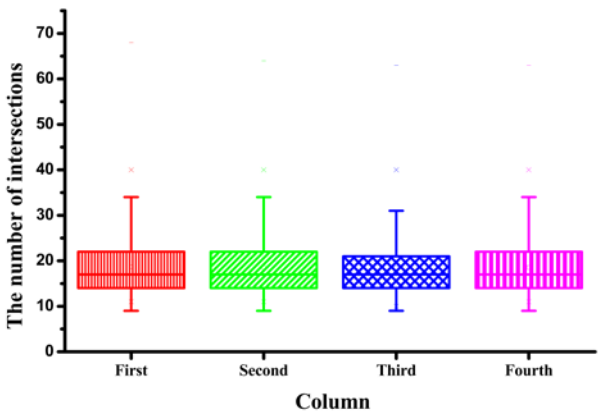


**Figure 10.** The number of attacks of each column.

To reduce the number of fault injections and improve attack efficiency, the attacker stops fault injection when there is 1 bit left. We took the undetermined secret key into Midori-64 for verification.

As shown in Figure 11, we counted the number of fault attacks before and after optimization. After optimization, the number of fault attacks reduced considerably, and most of attacks could be implemented within 20 times. Figure 12 shows the time distribution of fault attack. Most of the security keys can be recovered within 80 s. The efficiency after optimization greatly improved compared to before optimization.

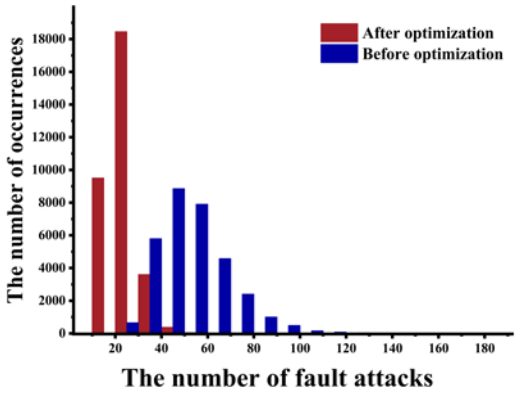


**Figure 11.** The relationship between the remaining information content and the number of intersections.

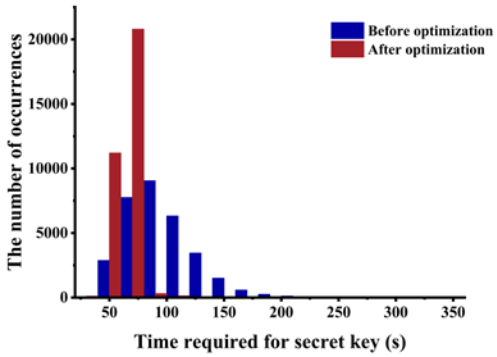


**Figure 12.** The distribution of the attack time.

## 6. Conclusions

In IoT networks, the data security of each sensor node faces severe challenges. The scattered distribution of a large number of nodes is convenient for attackers. In this paper, a novel random multiple fault attack method on Midori is proposed. The fault attack method can successfully recover the secret key in Midori with at least 11 attacks. Using computer simulation, we obtain the leakage relationship between the number of fault attacks and information content, which provides a theoretical basis for quickly obtaining the secret key. An adversary can use this function to judge the range of the remaining secret key. The random multiple fault attack method, provided in this paper is applicable to many fields. We present the random multiple fault analysis method, which provides a theoretical model for the analysis of unknown location and the number of fault injections. The proposed attack model can be applied to most of the laser fault attacks and electromagnetic fault attacks. We further optimized the attack scheme, reduced the number of fault attacks and decreased the time of fault attacks. The method proposed in this paper is helpful for analyzing the gradual process for obtaining secret keys under multiple faults. We expect that the multiple fault attacks will improve the security of lightweight cryptosystems.

**Author Contributions:** L.D., S.S. and L.Z. conceived and designed the experiments; L.D. and X.C. performed the experiments; L.D., S.S. and H.Z. analyzed the data; L.D. wrote the paper. H.Z. and B.K.G. reviewed the paper. H.Z., L.D. and L.Z. obtained funding. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was supported in part by the National Natural Science Foundation of China under grants 61571063 and 61701141; in part by the Natural Science Foundation of Beijing under grant 3182028; in part by the Fundamental Research Funds for the Central Universities (BUPT project grant numbers: 2019XD17 and 2019PTB-001); in part by the China Postdoctoral Science Foundation under grant 2017M611357; in part by the Postdoctoral Science Foundation of Heilongjiang Province of China under grant LBH-Z17045; in part by the Technology Bureau of Qiqihar City of Heilongjiang Province of China (grant number GYGG-201905); in part by the Heilongjiang Province Intelligent Machine Research Institute project (grant number 135409610); and in part by the Young Creative Talents Training Plan of General Universities of Heilongjiang Province of China under grant UNPYSCT-2017152; China Postdoctoral Science Special Foundation (2018T110274); and in part by the Science Foundation Project of Heilongjiang Province of China (QC2015073).

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Jean-Jacques, Q.; David, S. Simple electromagnetic analysis for smart cards: New results. In Proceedings of the Crypto 2000, Santa Barbara, CA, USA, 20–24 August 2000.
2. Ding, G.L.; Chu, J.; Yuan, L.; Zhao, Q. Correlation Electromagnetic Analysis for Cryptographic Device. In Proceedings of the Pacific-Asia Conference on Circuits, Communications and Systems, Chengdu, China, 16–17 May 2009.
3. De Mulder, E.; Ors, S.B.; Preneel, B.; Verbauwhede, I. Differential Electromagnetic Attack on an FPGA Implementation of Elliptic Curve Cryptosystems. In Proceedings of the World Automation Congress, Budapest, Hungary, 24–26 July 2006.
4. Selmke, B.; Brummer, S.; Heyszl, J.; Sigl, G. Precise Laser Fault Injections into 90 nm and 45 nm SRAM-cells. In Proceedings of the Smart Card Research and Advanced Application (CARDIS 2015), Bochum, Germany, 4–6 November 2015.
5. Van Woudenberg, J.G.J.; Witteman, M.F.; Menarini, F. Practical Optical Fault Injection on Secure Microcontrollers. In Proceedings of the Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2011), Nara, Japan, 28 September 2011.
6. Dutertre, J.M.; Beroulle, V.; Candelier, P.; De Castro, S.; Faber, L.B.; Flottes, M.L.; Philippe, G.; David, H.; Regis, L.; Paolo, M.; et al. Laser Fault Injection at the CMOS 28 nm Technology Node: An Analysis of the Fault Model. In Proceedings of the Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2018), Amsterdam, The Netherlands, 13 September 2018.
7. Dehbaoui, A.; Dutertre, J.M.; Robisson, B.; Orsatelli, P.; Maurine, P.; Tria, A. Injection of Transient Faults Using Electromagnetic Pulses Practical Results on a Cryptographic System. Available online: https://eprint.iacr.org/2012/123.pdf (accessed on 5 March 2012).
8. Ordas, S.; Guillaume-Sage, L.; Maurine, P. EM Injection: Fault Model and Locality. In Proceedings of the Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2015), St. Malo, France, 13 September 2015.
9. Boneh, D.; DeMillo, R.A.; Lipton, R.J. On the Importance of Checking Cryptographic Protocols for Faults. In Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques, Konstanz, Germany, 11–15 May 1997.
10. Li, W.; Zhang, W.; Gu, D.; Cao, Q.; Tao, Z.; Zhou, Z.; Liu, Y.; Liu, Z. Impossible differential fault analysis on the LED lightweight cryptosystem in the vehicular ad–hoc networks. *IEEE Trans. Dependable Secur. Comput.* **2016**, *13*, 84–92. [CrossRef]
11. Chen, Z.; Chen, H.; Wang, X. Cryptanalysis of Midori128 Using Impossible Differential Techniques. In Proceedings of the 12th International Conference, ISPEC 2016, Zhangjiajie, China, 16–18 November 2016.
12. Shahmirzadi, A.R.; Azimi, S.A.; Salmasizadeh, M.; Mohajeri, J.; Aref, M.R. Impossible differential cryptanalysis of reduced-round midori64 block cipher. *ISC Int. J. Inf. Secur.* **2018**, *10*, 3–13.
13. Zhao, X.; Guo, S.; Zhang, F.; Shi, Z.; Ma, C.; Wang, T. Improving and Evaluating Differential Fault Analysis on LED with Algebraic Techniques. In Proceedings of the Workshop on Fault Diagnosis Tolerance Cryptography (FDTC 2013), Santa Barbara, CA, USA, 20 August 2013.

14. Li, W.; Rijmen, V.; Tao, Z.; Wang, Q.; Chen, H.; Liu, Y. Impossible meet-in-the-middle fault analysis on the LED lightweight cipher in VANETs. *Sci. China Inf. Sci.* **2018**, *61*, 32110. [CrossRef]
15. Cheng, W.; Zhou, Y.; Sauvage, L. Differential Fault Analysis on Midori. In Proceedings of the Information and Communications Security (ICICS 2016), Singapore, 29 November–2 December 2016.
16. Korkikian, R.; Pelissier, S.; Naccache, D. Blind Fault Attack Against SPN Ciphers. In Proceedings of the 2014 Workshop on Fault Diagnosis and Tolerance in Cryptography, Busan, South Korea, 23 September 2014.
17. Li, W.; Gu, D.W.; Xia, X.L.; Zhao, C.; Liu, Z.Q.; Liu, Y.; Wang, Q.J. Single byte differential fault analysis on the LED lightweight cipher in the wireless sensor network. *Int. J. Comput. Intell. Syst.* **2012**, *5*, 896–904. [CrossRef]
18. Vasquez, J.D.C.G.; Borges, F.; Portugal, R.; Lara, P. An Efficient One-Bit Model for Differential Fault Analysis on SIMON Family. In Proceedings of the Workshop on Fault Diagnosis Tolerance Cryptography (FDTC), St. Malo, France, 13 September 2015.
19. Saha, D.; Mukhopadhyay, D.; Chowdhury, D.R. A Diagonal Fault Attack on the Advanced Encryption Standard. Available online: https://eprint.iacr.org/2009/581.pdf (accessed on 30 November 2009).
20. Zhang, F.; Lou, X.; Zhao, X.; Bhasin, S.; He, W.; Ding, R.; Qureshi, S.; Ren, K. Persistent fault analysis on block ciphers. *IACR Trans. Cryptol. Hardw. Embed. Syst.* **2018**, *3*, 150–172.
21. Mendel, F.; Rechberger, C.; Schläffer, M.; Thomsen, S.S. The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl. In Proceedings of the Fast Software Encryption (FSE), Leuven, Belgium, 22–25 February 2009.
22. Moro, N.; Dehbaoui, A.; Heydemann, K.; Robisson, B.; Encrenaz, E. Electromagnetic Fault Injection: Towards a Fault Model on a 32-bit Microcontroller. In Proceedings of the Workshop on Fault Diagnosis Tolerance Cryptography (FDTC 2013), Santa Barbara, CA, USA, 20 August 2013.
23. Gandolfi, K.; Mourtel, C.; Olivier, F. Electromagnetic analysis: Concrete results. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems, Paris, France, 14–16 May 2001.
24. Agoyan, M.; Dutertre, J.M.; Mirbaha, A.P.; Naccache, D.; Ribotta, A.L.; Tria, A. Single-Bit DFA Using Multiple-Byte Laser Fault Injection. In Proceedings of the 2010 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 8–10 November 2010.
25. Banik, S.; Bogdanov, A.; Isobe, T.; Shibutani, K.; Hiwatari, H.; Akishita, T.; Regazzoni, F. Midori: A Block Cipher for Low Energy. In Proceedings of the Advances in Cryptology—ASIACRYPT 2015, Auckland, New Zealand, 29 November–3 December 2015.
26. Nozaki, Y.; Yoshikawa, M. Statistical Fault Analysis for a Lightweight Cipher Midori. In Proceedings of the International Conference on Information and Automation (ICIA 2017), Macau, China, 18–20 July 2017.
27. Todo, Y.; Leander, G.; Sasaki, Y. Nonlinear invariant attack: Practical attack on full scream, iscream, and midori64. *J. Crypt.* **2019**, *32*, 1383–1422. [CrossRef]
28. Knudsen, L. DEAL-A 128-bit cipher. *Complexity* **1998**, *258*, 216.
29. Biham, E.; Shamir, A. Differential Fault Analysis of Secret Key Cryptosystems. In Proceedings of the 17th Annual International Cryptology Conference Advances in Cryptology (CRYPTO 1997), Santa Barbara, CA, USA, 17–21 August 1997.
30. Jovanovic, P.; Kreuzer, M.; Polian, I. An Algebraic Fault Attack on the LED Block Cipher. Available online: https://eprint.iacr.org/2012/400.pdf (accessed on 17 July 2012).
31. Li, W.; Liao, L.; Gu, D.; Cao, S.; Wu, Y.; Li, J.; Zhou, Z.; Guo, Z.; Liu, Y. Ciphertext-only fault analysis on the Midori lightweight cryptosystem. *Sci. China Inf. Sci.* **2020**, *63*, 1–3. [CrossRef] [PubMed]
32. Liao, N.; Cui, X.; Liao, K.; Wang, T.; Yu, D.; Cui, X. Improving DFA attacks on AES with unknown and random faults. *Sci. China Inf. Sci.* **2017**, *60*, 210–215. [CrossRef]
33. Sakiyama, K.; Li, Y.; Iwamoto, M.; Ohta, K. Information-theoretic approach to optimal differential fault analysis. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 109–120. [CrossRef]


© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).