Research on Fault-Electromagnetic Attack on Block Cipher
Chunhui Sun, Hui Li, Yang Yang, Jie Chen

Key Laboratory of Computer Network & Information Security Ministry of Education, Xidian University, Xi’an 710071, China
{sunch, lihui, yang.yang, jchen}@mail.xidian.edu.cn

Abstract
It is one of the important factors in iterative block ciphers design that proper rounds are used to resist differential analysis, linear analysis and many other kinds of attack. Block ciphers usually adopt loop codes in software and repetition structures in hardware in order to reduce complexity and cost. This paper presents an effective fault-electromagnetic attack which can change the rounds of block ciphers in running process, by inducing appropriate fault to the cryptographic chip. The executing rounds of the attacked block cipher can be detected from the electromagnetic radiation track of cryptographic chip. Then the secret key can be deduced directly or with simple mathematical analysis. The simulation result of lightweight block cipher PRESENT shows that the suggested attack is feasible and efficient, when it is implemented with single chip microcomputer. Furthermore, countermeasures are given to resist this kind of attack.

Keywords: Block Cipher, Side Channel Attack, Fault-Electromagnetic Attack

1. Introduction
There are two types of attacks in cryptanalysis. One is the traditional analysis method making use of the possible flaws in algorithm design itself, such as differential analysis [2], linear analysis [3, 4], algebraic analysis [4, 6], related-key attack [7], statistical saturation attack [5] and so on. The other is taking advantage of information during the algorithm implementation process. Side channel attack is the second type of cryptanalysis, with side channel information retrieved from cryptographic devices. Side channel attack is a powerful attack method by exploiting the information leaked during realistic cryptographic device operations. This leakage information includes timing [8], power consumption [10], electromagnetic radiation [13] and other features. Compared with the traditional cryptanalysis, side channel attack brings great threat to the cryptosystem with more efficiency and lower cost. Recently, some attacks are proposed, which combine side channel with traditional analysis. For instance, side channel-cube attack [12] and chosen plaintext-time attack [9] are put forward in order to enhance the effect of attack.

Fault attack is first proposed by Boneh, Demillo and Lipton [11] which is one of the most powerful methods of side channel attacks. Cryptographic device would result in wrong output when certain fault is induced by the attacker, then the secret key will be obtained by analysis. E. Biham and A. Shamir [14] improved the fault attack and brought it to analyze block ciphers (such as DES). Feistel and SPN network are classic architectures in the designation of block cipher. Feistel network is utilized in the implementation of DES, Blowfish, CAST-256 and so on. SPN network is used in the designation of AES, Serpent, PRESENT [1] and so on. DES is appointed as data encrypt standard by American National Standard Institute in 1976. In 2001, AES take the place of DES as the advanced encryption standard appointed by National Institute of Standards and Technology (NIST). PRESENT is proposed by A. Bogdanov and L.R. Knudsen on the Workshop Cryptographic Hardware and Embedded Systems (CHES 2007), which is an ultra lightweight block cipher utilizing SPN network and suitable for extremely resource constrained environment, such as RFID tags and sensor networks. In recent years, side channel attacks on PRESENT are proposed which include side channel-cube attack [12], differential-fault attack [15], and differential-fault analysis on key schedule of PRESENT [16].

This paper presents a method of fault-electromagnetic attack, by analyzing two kinds of overall structure in block cipher. The effect of injected fault can be estimated from observing the electromagnetic radiation track when cipher equipments operate, by inducing appropriate...
fault to the cryptographic chip. Finally, the sub-key of the first or the last round can be obtained, or executing rounds can be greatly reduced even to stop which is suitable for mathematical analysis. Through this method, we can see different implementations of cryptographic algorithms have distinct influence on the resistance of this attack. At last, countermeasures are given to resist this kind of attack.

The rest of the paper is organized as follows. In Section 2, we briefly review the main two architectures of block cipher and analyze feasibility of the fault attacks on them. Section 3 discusses the PRESENT (AES-like) cipher and analyzes the fault-electromagnetic attack on PRESENT in detail. Section 4 describes the experiment configuration of fault-electromagnetic attack on PRESENT. In section 5, we present our result and analyze the effect of the cryptographic algorithm implementation. Section 6 gives out the countermeasure. Section 7 concludes the paper.

2. Fault attacks on the architecture of block cipher

Feistel and SPN network are two main structures in iterative block ciphers. We describe the DES in the Feistel network and the AES as an example of the SPN network as follows respectively.

2.1. DES with Feistel network

In the implementation of DES algorithm, we use a Feistel network with 16 rounds. After the first \( IP \) initial permutation, plaintext \( P \) is divided into left and right two parts of 32 bits respectively. Then both of the half parts go through 16 rounds of Feistel network. Then the ciphertext \( C \) is able to be obtained after the \( IP^{-1} \) permutation which is the inverse permutation of \( IP \). Pseudocode of DES is presented as follows:

\[
\text{GenerateRoundKeys}(K) \\
\text{IP}(P) \\
\text{for } i = 1 \text{ to } 16 \\
\quad L_i = R_i \\
\quad R_i = L_{i-1} \oplus f(R_i, k_i) \\
\text{end for} \\
\text{IP}^{-1}(C')
\]

where \( k_i \) is the round key and \( C' \) is the output of plaintext \( P \) after 16 rounds permutations of Feistel network. Ciphertext \( C \) is obtained by the \( IP^{-1} \) permutation after \( C' \). With DES, it is possible to use the same function to decrypt the ciphertext. The only difference is that the round keys must be used in reverse order. It is one of the important factors that appropriate round number is the guarantee of security for DES. Below the proper number of rounds, it would not resist differential attack, linear attack and so on.

2.2. AES with Substitution-Permutation network

AES is composed of 10 rounds of substitution-permutation networks (SPN) and each round consists of bytes substitution, shifting rows, mixing columns and adding round key. Pseudocode of AES is presented as follows:
Compared with SPN structure, the Feistel structure has an advantage of similarity in encryption and decryption, which requires fewer components of software and hardware.

2.3. Fault attack on block cipher

From the above two kinds of structure can be seen, the appropriate number of rounds is an important factor to ensure the security of block cipher algorithm except S-box and key length. Many reduced round block ciphers are analyzed by mathematical cryptanalysis [2,3,6,7]. Fault attack is a method of extracting information from the secret key by injecting errors, during the operation process of the cryptographic algorithm. In general, an attacker gets fault ciphertexts by giving external impact on a device with voltage variation, glitch, clock jitter, laser [14,17,18,19], etc. Fault generated as an effect on the attack can be divided into permanent fault and transient fault. According to the fault caused by internal changes in the different, fault roughly is divided into single bit failure, single byte failure or multiple bytes fault. According to the difference of internal structure and physical properties in cipher chip, some inner bits are likely to change from 1 to 0, some are likely to change from 0 to 1, or some bits or bytes (word or double-word) change at random, when different fault is injected. For example, Biham and Shamir [14] have pointed out that the EEPROM cells are more likely to change from 1 bit to 0 bit during faults injecting errors.

From the two main structures of iterative block cipher can be seen, they perform in series rather than in parallel. Usually, iterative block ciphers adopt loop codes in software taking into account the code reusability and saving the memory resources, and have common structure circuits in hardware in order to save hardware resources and reduce circuit complexity. The number of iteration round can be easily attacked in block ciphers, when the round number \( i \) or the judgment of loop condition have changed as a result of the attack such as in the reading value \( i \) into fault. In the worst condition, 0 round or 1 round will be executed and the security of block cipher will be tragically destroyed. In the next section, we combine the fault attack and the electromagnetic attack method into one - the fault-electromagnetic attack. It will be demonstrated in detail and PRESENT algorithm will be focused as an example.

3. Fault-electromagnetic attack on PRESENT

3.1. Description of the PRESENT

PRESENT is an ultra lightweight block cipher consisting of 31 rounds with SPN network. The block length is 64 bits and two key lengths of 80 and 128 bits are supported. However, we focus on the version with 80-bit keys. Pseudocode of PRESENT is presented as follows.
In this pseudocode, $K$ is the 80-bit initial key and 32 rounds subkey with 64-bit in every round generated after key schedule. When PRESENT algorithm is prepared to load value $i$ for the 31 rounds iteration operations, the value of round number $i$ will change if this time injecting faults. When $i > 31$, the iteration round operations are skipped and directly go to the last operation of adding round key. Then, an attacker can get ciphertext $C = P \oplus k_{n}$. If plaintext is chosen for all zeros, the ciphertext is the 64-bit round key $k_{31}$ immediately. The 64-bit initial key can be deduced from $k_{31}$ by the key schedule and the rest of 16-bit initial key can be obtained by exhaustive attack. The hardware schematic of PRESENT is shown in Figure 1.

As shown in Figure 1, PRESENT has cycle structure of multiple rounds in hardware implementation. When fault is injected into cryptographic device lead to perform single or less round of encryption, the round key of block cipher can be obtained directly or with simplified mathematic attack by analyzing the false output.

It can be seen that the power consumption and electromagnetic radiation characteristic are similar in each round of iteration block cipher, which is more intuitive and accurate than the execution time for determination whether the iteration round have changed.

According to the above pseudocode, the following gives C codes of the circular part in PRESENT algorithm and a portion of the disassembling codes.

It can be seen from the disassembling codes that the round number $i$ is initiated in register A (accumulator) and stored in external SRAM with address 0x012F. The value $i$ is read out from this address when it is used. And update it in SRAM after $i$ is used and changed. The judgment of loop statement consists of three assembly codes. Firstly, clear the 1-bit register carry flag C (CLR C). Then read out the value of round in SRAM which subtracts immediate number 31 and the C flag from A (SUBB A, #0x1F). Finally, judge whether the C flag is reset to 0 (JNC C:15F3). If the C flag is set to 1, the loop body is considered as finished and jump to C:15F3.

---

**Figure 1. Hardware implementation of PRESENT-80**
which means turn into the procedure of the last add round key. Otherwise, go into the loop body. From the above analysis, it is not necessary to hit the device at the very moment it initializes the round value $i$. The opportunity to change the value $i$ includes that the initialization of $i$, store and read out $i$ from SRAM. There are several other ways to skip the loop body except the change of $i$. For example, set C flag when it is should be reset or reset C flag by injecting fault during subtraction operation.

There are several moments and positions to reduce or skip the round operations by injecting fault in the software implement. Different moments and positions require distinct fault types. For example, sometimes they need to reset the register, and sometimes they need to set the register. All of these factors bring more opportunities to inject faults with different ways and places during the operation of cryptographic device. Consequently, probability of success is increased.

3.2. Steps of fault-electromagnetic attack on PRESENT

The steps of fault electromagnetic attack are listed as follows.

1. We put all zero plaintext to the cryptographic device.
2. We observe the electromagnetic radiation track by oscilloscope in careful, and find characteristic wave form of multi-round structure. If not observed, adjust the position of coil over cipher chip until the characteristic wave form appears.
3. According to the wave form in step 2 and period of crystal oscillator, we attempt to adjust the injecting fault before current round operation.
4. We observe the electromagnetic radiation track, and check the variation of the round to determine whether it is satisfied with the desired round.
5. To achieve the required number of rounds, go to the next step. Otherwise, get back to step (3).
6. According to the round number, the secret key of block cipher can be obtained directly or with simple mathematic analysis.

4. Experiment configuration

The encryption and decryption of PRESENT are programmed with C language according to [1]. To simulate the process of fault injection, we induce a random number to operate on the round value and then download the output to the microcontroller. The plaintext and ciphertext are transmitted and received through the serial port of PC, respectively. The handmade coil is hanged over the microcontroller and the coil is connected to the difference probe (TDP1000) of digital oscilloscope (MSO4104) to show the electromagnetic radiation track. The difference probe is hold by a magnet stand for stable, as shown in Figure 2.

![Figure 2. The configuration of FEA experimentation platform](image)

We can monitor the electromagnetic radiation emitted by a microcontroller which runs cryptographic algorithm through oscilloscope, and analyze the effect of fault injected.
5. Results and Analysis

Adjusting the position of coil over microcontroller, we get the electro-magnetic radiation track of microcontroller during the operation of PRESENT block cipher as shown in Figure 3(a). The 31 distinct peaks show that similar structures in each round have similar electromagnetic radiation characteristics. Simulations shown in Figure 3(b, c, d) reflect the traces of electromagnetic radiation in the round of 6, 1 and 0, respectively, when faults inject the in PRESENT block cipher.

![Figure 3. The traces of electromagnetic radiation in different rounds of PRESENT-80 during encryption process](image)

Let the plaintext to be 0x000000000000 and the initial key to be 0x11223445567899AA in PRESENT. The subkeys of 32 rounds and ciphertext are shown in Table 1.

<table>
<thead>
<tr>
<th>32 round keys</th>
<th>ciphertext</th>
<th>rounds</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 0x1123345567788</td>
<td>0x4272734D26C8590C</td>
<td>31</td>
</tr>
<tr>
<td>2 0x7798224668AACC</td>
<td>0x32C1C84E69A4D1</td>
<td></td>
</tr>
<tr>
<td>3 0x39DE20EF3448CC</td>
<td>0xB16246583909C9C4</td>
<td></td>
</tr>
<tr>
<td>4 0x322AA73BC41DE09</td>
<td>0x3693562C84CB0728</td>
<td></td>
</tr>
<tr>
<td>5 0xB7982C44A6C8A9E</td>
<td>0x17AC8A4E9DA4D52</td>
<td></td>
</tr>
<tr>
<td>6 0x4216F305885C9A</td>
<td>0x9642558395C9C10</td>
<td></td>
</tr>
<tr>
<td>7 0x232264554E77881</td>
<td>0x7C9562C84AB072A0</td>
<td></td>
</tr>
<tr>
<td>8 0x7B982C44E4A9A2</td>
<td>0x91CA984E0B24D547</td>
<td></td>
</tr>
<tr>
<td>9 0x9E2165305808C9C</td>
<td>0x242572395309C169</td>
<td></td>
</tr>
<tr>
<td>10 0xB2164105828C9A</td>
<td>0x75507C4AE1F2A6FC</td>
<td></td>
</tr>
<tr>
<td>11 0x3AA693C42A60B4</td>
<td>0x75507C4AE1F2A6FC</td>
<td></td>
</tr>
<tr>
<td>12 0xE3272754D2788592</td>
<td>0x75507C4AE1F2A6FC</td>
<td></td>
</tr>
<tr>
<td>13 0x9A69362C820B76</td>
<td>0x75507C4AE1F2A6FC</td>
<td></td>
</tr>
<tr>
<td>14 0x082C1C64E4A9A49</td>
<td>0x75507C4AE1F2A6FC</td>
<td></td>
</tr>
<tr>
<td>15 0xB2164105828C9A</td>
<td>0x75507C4AE1F2A6FC</td>
<td></td>
</tr>
<tr>
<td>16 0x9A69362C820B76</td>
<td>0x75507C4AE1F2A6FC</td>
<td></td>
</tr>
</tbody>
</table>

As shown in Table 1, the ciphertext is $k_{32}$ when the input of PRESENT is all 0s and the number of round is 0. Then, the 64-bit initial key can be deduced from $k_{32}$ by the key schedule and the rest of 16-bit initial key can be obtained by exhaustive attack. When a fault makes the round of PRESENT to reduce certain rounds, the ability of resistance to attack in the algorithm...
design will decrease or even to lose. The attacks include differential attack, linear attack, and so on. Then mathematical cryptanalysis can be used to analyze the secret key simply.

For the pseudocode of PRESENT shown in Section 3.1, algorithm will execute at least 0 round when fault attack is implemented. When other forms of pseudocode are used, the minimum number of rounds is not always 0. For example, to achieve the 31 rounds using do-while should execute at least 1 round, because a round has executed before judging the loop condition.

By the same principle, when fault electro-magnetic analysis attacks the round value of AES, the minimum number of rounds is at least 1 which can be deduced from the pseudocode of AES in Section 2.2. In this condition, the ciphertext is the output of the plaintext and $k_i$ XOR then going through Substitution Byte, Shift Row, XOR with $k_{11}$, where the last round the Mix Column is omitted. The initial key could be easily obtained through mathematical analysis. If the loop statement is of the do-while form, algorithm will execute at least 2 round for the fault attack. In a similar way, mathematical cryptanalysis can be used to analyze the secret key simply.

According to pseudocode of DES in Section 2.1, the minimum number of rounds can achieve to 0 when a fault is introduced into to the value of round number $i$. The plaintext directly output ciphertext after substitution $IP$ and $IP^{-1}$ without any operation about subkey. When the round value $i$ is changed to 1 by faulty attack, there is only one operation about subkey that is $k_1$. Thus, $k_1$ can be easily deduced. When the value of round $i$ is changed to $1 < i < 16$, mathematic attack can be utilized to recover the initial key. Similarly, when the loop statement is changed to the do-while form, algorithm will execute at least 1 round.

In addition, different influence on attack can be deduced from the code implementation details. Here we focus on the PRESENT algorithm. When the loop statement in C language has the form of for($i = 0; i < 31; i += 1$){...} and the error induced to 8-bit microcontroller is stochastic, the loop body will be skipped if $i$ is changed to $i \geq 31$ with probability $\frac{225}{256}$. Similarly, when the loop statement in C language has the form of for($i = 31; i > 0; i --$){...}, the loop body will be skipped if $i$ is changed to 0 with probability $\frac{1}{256}$. While a value of round $i$ is greater than 31 which is even more than standard PRESENT, this can be observed by electromagnetic radiation traces.

From the analysis above, the different implementation of cipher algorithm will come into being distinct influence to the fault attack. In practice, the characteristics of hardware and the properties of operation with error should be taken into accounts when a fault is injected.

### 6. Countermeasures

From different faults injected, the available counter measures in hardware are as follows.

1. Lowering the electromagnetic radiation by metal shields in the cryptographic chip, also the metal shields should reduce the susceptibility to fault injection, but not eliminate it completely.

2. Active protection grid is added to increase the difficult of decapsulation. On the other hand, we can use new material to encapsulate the cryptographic chip.

3. We bury the sensitive registers or SRAM underneath other layers that contain less sensitive information.

4. We add sensors to detecting voltage glitch, clock glitch or add filter circuit to eliminate the glitch. When glitch is injected by an attacker, the detecting circuit will reset cryptographic chip or the filter would eliminate the glitch. And other sensor are also deployed to measure relevant environment variables such as light, temperature, induced voltage, infrared, X-ray.

5. Furthermore, internal shield clock can be directly used to prevent the attack aimed at clock.

6. We add duplicate circuit to run the cryptographic algorithm twice simultaneous, and then check the results. If the results not correspond, it will not output. Also it can do the encryption twice in series, or encryption once, and decryption once to verify it. But the last two manners need to consume two times as much time.
Compared with hardware counter measures, software counter measures have better flexibility and expansibility along with lower cost. When different types of faults are introduced, different influence on attack can be deduced from different software implementation and hardware support. Thus software design should be based on the characteristic of hardware support. From the pseudocode of AES and PRESENT, there direct uses the mark number of last subkey in the last add round key operation. If there don’t uses the mark number in direct but use a value which is related to the previous number of round in the loop body, the last add round key will make use of invalid subkey when the number of round makes change owing to a injected fault. For example, the loop statement in PRESENT has the form of for(\(i = 0; i < 31; i ++\)){…}. After 31 rounds, \(i = 31\) and \(i\) is direct used to the mark number of subkey in the last add round key operation. If \(i\) is changed to \(i > 31\) due to the injected fault, the last add round key will make use of invalid subkey which increases the difficulty of the attack. In addition, the form of do-while can increase the difficulty of the attack.

Intuitively, the hardware and software should adopt cascade connection with many same procedures rather than loop structure. Thereby, it is almost impossible to skip or reduce the number of round when a fault is injected. For hardware implementation it increases the cost and complexity, and for software implementation it needs more storage. But in some special security application scenario, it is necessary indeed.

7. Conclusion

Based on the characteristics of iterative block ciphers, we present an effective fault-electromagnetic attack which can reduce or even skip the rounds of iterative block ciphers. Then the secret key can be obtained directly or with simple mathematic analysis. The simulation result of lightweight block cipher PRESENT shows that the suggested attack is feasible and effective, when it implements in single chip microcomputer. Furthermore, we analyze the assembly codes and give countermeasures in software and hardware according to the principle of fault-electromagnetic attack.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant No. 61003300), the Fundamental Research Funds for the Central Universities (Grant Nos. K50510010012, K50510010018, K50510010030, JY10000901021) and the Natural Science Basic Research Plan in Shaanxi Province of China (Grant No. 2011JQ8042).

References