applied sciences

MDPI

Article

Chosen Plaintext Combined Attack against SM4 Algorithm

Jintao Rao [1,2,*] and Zhe Cui [1,2]

[1] Chengdu Institute of Computer Application, Chinese Academy of Sciences, Chengdu 610081, China
[2] University of Chinese Academy of Sciences, Beijing 100049, China
* Correspondence: raojintao17@mails.ucas.ac.cn

Abstract: The SM4 algorithm is widely used to ensure the security of data transmission. The traditional chosen plaintext power attacks against SM4 usually need to analyze four rounds power traces in turn to recover the secret key. In this paper, we propose a new combined chosen plaintext power analysis, which combines the chosen plaintext power attack and the differential characteristics of the substitution box (S-box) in SM4. In our attack, only the second and fourth round S-box outputs of SM4 algorithm are used as attack points, and some sensitive fixed intermediate values are obtained by power analysis when inputting specific plaintext. Then the differential analysis of these sensitive intermediate values is carried out to calculate the difference between the input and output of the S-box, and the key can be recovered from the differential characteristics of S-box. Compared with the traditional chosen plaintext power analysis, which requires four rounds of analysis, our analysis reduces the number of attack rounds into two rounds, and adopts the nonlinear S-box with obvious leakage information as the attack intermediate value, which effectively improves the feasibility of attack. Finally, a practical attack experiment is carried out on a Field Programmable Gate Array (FPGA) based implementation of SM4 algorithm, and the results show that our method is feasible and effective for real experiments.

Keywords: SM4; power analysis attack; differential cryptanalysis; combined attack

Citation: Rao, J.; Cui, Z. Chosen Plaintext Combined Attack against SM4 Algorithm. *Appl. Sci.* **2022**, *12*, 9349. https://doi.org/10.3390/app12189349

Academic Editors: Leandros Maglaras, Helge Janicke and Mohamed Amine Ferrag

Received: 10 August 2022
Accepted: 13 September 2022
Published: 18 September 2022

1. Introduction

Since Kocher et al. proposed differential power analysis (DPA) in Crypto '1999 [1], power analysis has rapidly become a research hotspot for cryptographic algorithm implementation security. The basic principle of power analysis is to collect power leakage information such as time, power consumption and electromagnetic radiation in the process of cryptographic equipment performing sensitive operations (such as encryption and decryption operation and key transmission), and build the Hamming weight or Hamming distance leakage model of key/sensitive information. Finally, the relationship between the model and the power leakage information is calculated by statistical methods to extract the key/sensitive information. Power analysis methods mainly include DPA attack, Correlation Power Analysis (CPA) [2–4], Template attack (TA) [5–8], and Mutual Information Analysis (MIA) [9] etc.

The SM4 cryptographic algorithm is a commercial block cipher algorithm published in China in 2006 [10]. It officially became an ISO/IEC international standard in 2021 and is widely used in government departments, power, finance and other network information systems to ensure the security of data transmission. Therefore, it is very important to analyze its implementation security.

1.1. Related Works

At present, the analysis of implementation security against SM4 algorithm mainly includes differential fault analysis [11] and power analysis [12–17]. Zhang Lei et al. proposed the differential fault analysis method on SM4 for the first time [11]. The fault attack induces some fault injections against the last four rounds of SM4 encryption to obtain some faulty

output. With the fault output and the differential characteristics of S-box, the attacker can recover the secret key. After that, Hu et al. conducted a traditional power analysis on SM4 algorithm [12]. They used the Hamming weight model to analyze the first four rounds of S-box output of SM4 encryption to obtain the round key, and then deduced the encryption key. The above study shows that, to recover the whole initial key, the attacker must analyze the first 4 rounds of encryption or the last 4 rounds of decryption of SM4 algorithm one by one. Moreover, the output of S-box as the only nonlinear operation is commonly chosen as the sensitive intermediate value. Just as introduced in [18], the power analysis with the leaked affine transformation included in S-box (i.e., the sensitive intermediate value) is almost the most powerful under the Gaussian noise assumption.

There also exist other attacks based on different known conditions, such as unknown plaintext attack and chosen plaintext attack. When the general S-box has low leakage and there is a need to find some new leaked intermediate value in an algorithm, or some intermediate value is needed to be fixed for attack, plaintext attack is often chosen as the most effective one. For example, in the literature [13–16], different intermediate values are chosen as attack points, and specific plaintext is input to obtain some sensitive fixed intermediate values for power attacks. First, Wang [13] and Du et al. [14] proposed the chosen plaintext power attack on SM4. Then Shan [15] and Chen et al. [16] expanded the power attack on SM4 by selecting specific plaintext. In addition, Hu et al. [17] proposed a general adaptively chosen-plaintext attack to improve the correlation in power analysis. Moreover, Maamar O et al. [19] further improved the method to be both non-adaptive and adaptive by choosing appropriate plaintexts. Both the methods can be applied to analyze grouping algorithms, such as AES [20–24] and SM4. There are also many attacks on other algorithms. For example, Clavier [20] proposed the chosen plaintext power attack on AES; Ding [21] expanded the chosen plaintext collision attack on masked AES; Zheng [22] improved chosen plaintext collision attack for masked AES. Guo [25] proposed the chosen plaintext power attack on HMAC-SM3, and Takemoto [26] proposed the chosen plaintext power attack on PRINCE. Further, chosen plaintext attacks also can be applied to public key cryptology. For example, Li [27] proposed a chosen plaintext power attack on CRT_RSA and Melissa [28] proposed a chosen plaintext power attack on post-quantum authenticated encryption. More generally, Nicolas et al. [29] showed that a generic strategy can be applied to any differential power or electromagnetic analysis attack, against unprotected or protected devices and exploiting profiled or non-profiled leakage models. To sum up, chosen plaintext power attacks have already been applied to many algorithms, especially AES and SM4.

However, the above chosen plaintext power attacks (here we just discuss the attacks against SM4) still require analysis of four rounds of SM4 one by one. That is, it is necessary to know the previous round's key value when analyzing the current round. Moreover, different special plaintexts are required for CPA/DPA to recover the different round's key. Hence, it is necessary to collect power consumption curves four times to recover the initial key. (Each time, the power curve of the next round can be collected only after the key value of the previous round is determined by the power analysis.) Reducing the rounds of this type of analysis means the attack will fail. Moreover, the attacks are mainly aimed at the linear operations and lack the analysis of the nonlinear S-box (strong leakage point). The problems above will make the attack more complicated and it may fail (because of the lower leakage of linear operations). Hence, we think that there is still room for further improvement.

1.2. Contributions

In this paper, we propose a new round-reduced chosen plaintext power analysis against SM4 which combines chosen plaintext attack and differential analysis. After two rounds of analysis, the initial 128-bit key of SM4 can be completely recovered. Compared to the traditional chosen plaintext attacks [13–16], our attack has the following advantages:

(1) Our attack can recover two round keys in one round of analysis simultaneously. For the previous chosen plaintext power analysis, only one round key can be recovered in one round of analysis and requires the analysis of rounds 1–4 in total. However, in our attack, only the S-box outputs of round 2 (or 4) are selected as the attack intermediate values to carry out the chosen plaintext attack by inputting special plaintexts. It can determine some fixed value about the first and second round keys (or the 3rd and 4th round keys). Then, by employing the differential characteristics of S-box, we can further determine 2^4 candidates for the two round keys with near 100% probability in one round of analysis.

(2) Our attack is more feasible and simpler for experiments. As mentioned above, our attack reduces the rounds of analysis. Correspondingly, we just need to collect power traces for twice, while the traditional attacks need 4 times. Furthermore, if we improve the method (see Section 3.3), i.e., guess all the 2^4 candidates of round keys derived by differential analysis and recalculate the correlation coefficients to distinguish the correct ones, the required number of traces will decrease by one third and the key search space complexity will be reduced. This makes the attack experiments more feasible.

(3) The target selected in our attack has stronger power leakage. All of the previous attacks targeted the linear operations such as the XOR operation before a round outputting as the leaked points, but our attack targets the nonlinear operation, i.e., the output of S-box. Under the same and unprotected implementation, the leakage of the S-box is obviously greater than the linear operations. This means our attack experiments can succeed more easily due to the stronger power leakage.

2. Preliminaries

This section mainly introduces the SM4 algorithm, the current chosen plaintext power analysis and differential analysis methods for the SM4 algorithm.

2.1. SM4 Algorithm

As shown in Figure 1, the encryption operation is carried out in the unit of 32-bit wide word, and an iteration operation is called a round, with a total of 32 iterations. Assume that the input $(X_0, X_1, X_2, X_3) \in Z_2^{32}$, round key $rk_i \in Z_2^{32}$.

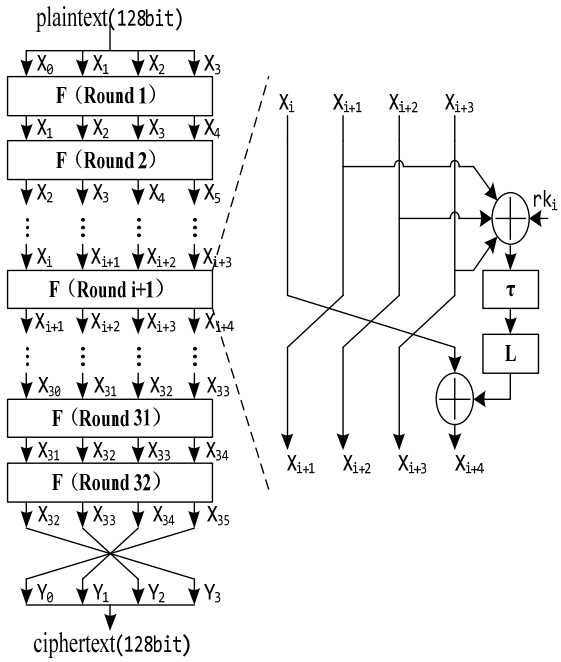

Figure 1. SM4 encryption process.

The round function F can be expressed as follows.

$$F(X_i, X_{i+1}, X_{i+2}, X_{i+3}) = X_i \oplus \mathrm{T}(X_{i+1} \oplus \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i) \quad (1)$$

Round transformation T: $Z_2^{32} \to Z_2^{32}$ is an invertible transformation, which is composed of nonlinear transformation τ and linear transformation L, and can be expressed as T(.) = L(τ(.)). Nonlinear transformation τ:τ is composed of 4 parallel S-boxes, and S-boxes are the permutation of 8-bit input and 8-bit output, denoted as Sbox (.). Assume the input is $A = (a_0, a_1, a_2, a_3) \in (Z_2^8)^4$, and the output is $B = (b_0, b_1, b_2, b_3) \in (Z_2^8)^4$. Then B can be expressed as follows.

$$B = (b_0, b_1, b_2, b_3) = \tau(A) = (Sbox(a_0), Sbox(a_1), Sbox(a_2), Sbox(a_3)) \quad (2)$$

Linear transformation L: The output of the nonlinear transformation τ is the input of the linear transformation L. Let the input be $B \in (Z_2^{32})$ and the output $C \in (Z_2^{32})$, then C can be expressed as follows.

$$C = L(B) = B \oplus (B \ll 2) \oplus (B \ll 10) \oplus (B \ll 18) \oplus (B << 24) \quad (3)$$

The SM4 key extension algorithm is basically the same as the encryption algorithm. Set the initial key of SM4 as $MK = (MK_0, MK_1, MK_2, MK_3)$, $MK_i \in Z_2^{32} (i = 0, 1, 2, 3)$. The round input in the iteration can be represented as $K_i \in Z_2^{32} (i \in \{0, 1, \ldots, 35\})$, $(K_0, K_1, K_2, K_3) = (FK_0 \oplus MK_0, \ldots, FK_3 \oplus MK_3)$, $K_{i+4} = K_i \oplus L(\tau(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i))$, where $CK = (CK_0, \ldots, CK_{31})$ and $FK = (FK_0, \ldots, FK_3)$ are fixed parameters of the system (see reference [10] for details). Then the round key $rk_i = K_{i+4}$ ($i \in \{0, 1, \ldots, 31\}$).

2.2. Chosen Plaintext Power Analysis for SM4

Reference [14] describes the chosen plaintext attack of SM4, and the details are described as below: First, select special plaintext with certain constraints, so that the output *res* after L transformation is fixed. Then, the round output X_{i+4} is selected as the attack object ($X_{i+4} = X_i \oplus res$, where X_i is the known random value and *res* is the fixed unknown value), and the fixed value *res* is obtained through power analysis, and then the round key can be deduced. The key of SM4 can be recovered by executing the chosen plaintext attack on the first four rounds successively. The attack of the first round is taken as an example:

1. Let $res = T(X_1 \oplus X_2 \oplus X_3 \oplus rk_0)$, choose some constraint special plaintext, make sure $X_1 \oplus X_2 \oplus X_3$ is fixed, so make sure *res* is fixed;
2. The output $X_4 (X_4 = X_0 \oplus res)$ of the first round is chosen as the attack point to perform CPA analysis and recover *res*;
3. Derive the round key rk_0.

The attack on round 2–4 is similar to the first round mentioned above, one round key is recovered each time, and the initial key is finally recovered through key extension.

2.3. Differential Characteristics of SM4 Algorithm S-box

In reference [11], a differential fault attack based on random bytes was proposed for SM4 by using the S-box differential characteristics of SM4. The differential characteristics of S-box are described as follows. For the SM4 algorithm, let $A_i = (a_{0,i}, a_{1,i}, a_{2,i}, a_{3,i})$ as the s-box input of round I, $B_i = (b_{0,i}, b_{1,i}, b_{2,i}, b_{3,i})$ as the s-box output of round i, and $C_i = (c_{0,i}, c_{1,i}, c_{2,i}, c_{3,i})$ (i = 1,2, … 32) as the output of L transformation in the i th round, where $a_{j,i}, b_{j,i}, c_{j,i} \in Z_2^8$, $j \in \{0, \ldots, 4\}$ and $i \in \{0, \ldots, 31\}$. At the same time, let $\triangle A_i = (\triangle a_{0,i}, \triangle a_{1,i}) \triangle a_{2,i} \triangle a_{3,i}$ as the input difference of S-box in round i. (Note: Different from the difference definition in reference [11], the difference in this paper is defined as the XOR value of S-box input in round i when two different plaintexts are input for encryption operation.) Similarly, $\triangle B_i = (\triangle b_{0,i}, \triangle b_{1,i} \triangle b_{2,i} \triangle b_{3,i})$ is defined as the output difference of S-box in round i, and let $\triangle C_i$=($\triangle c_{0,i}, \triangle c_{1,i}, \triangle c_{2,i}, \triangle c_{3,i}$) denote the output difference of L transformation in round i. where $\Delta a_{j,i}, \Delta b_{j,i}, \Delta c_{j,i} \in$

Z_2^8. For $j \in \{0,\ldots,4\}$ and $i \in \{0,\ldots,31\}$, the set $\Phi(\triangle a_{j,i}, \triangle b_{j,i})$ is defined to satisfy: $\Phi(\triangle a_{j,i}, \triangle b_{j,i}) = \{|x_{j,i} \in Z_2^8 | Sbox(x_{j,i}) \oplus Sbox(x_{j,i} \oplus \triangle a_{j,i}) = \triangle b_{j,i}\}$, that is the set of input values of S-box when the difference between input and output of S-box in round i is $\triangle a_{j,i}$ and $\triangle b_{j,i}$ respectively. In addition, let the inverse transform of L be L^{-1}. If $\triangle A_i$ and $\triangle C_i$ are known, $\triangle B_i$ can be derived through $\triangle B_i = L^{-1}(\triangle C_i)$, and $\Phi(\triangle a_{j,i}, \triangle b_{j,i})$ can also be constructed. As mentioned in reference [11], if $\Phi(\triangle a_{j,i}, \triangle b_{j,i})$ is a non-empty set and the attacker knows $\triangle a_{j,i}$ and $\triangle b_{j,i}$, then $x_{j,i}$ has at most 4 known candidate values. Moreover, the probability is 99.2% when there are 2 candidate values, and the probability is 0.8% is when there are 4. Based on the above differential characteristics, it can be seen that the input difference and output difference values of two pairs of different S-boxes need to be known to recover the round key of SM4 algorithm by using the differential characteristics.

3. Methodologies

It can be seen from Section 2.2 that chosen plaintext power analysis can only obtain one round key in each round of analysis. To recover the initial key of SM4, four rounds of analysis are needed to obtain four round keys. In order to improve the chosen plaintext power analysis, we utilize the differential characteristics of SM4 (see Section 2.3 for details). Thereby, it is only necessary to analyze the 2nd and 4th round of SM4 encryption to recover the whole initial key. The whole combined attack can be divided into two parts. Firstly, the intermediate value of the second and fourth round is obtained by round reduction chosen plaintext power analysis. Then the initial key is determined by differential analysis using S-box differential characteristics. The following two parts of the combined attack are introduced in turn.

3.1. Round Reduction-Based Chosen Plaintext on SM4

Step 1: Chosen plaintext

For N encryption operations, the plaintext input in each encryption operation must meet the requirement that X_0 is a random value and $X_1 \oplus X_2 \oplus X_3 = M_0$ (M_0 is a fixed value). That is, the first four bytes of plaintext grouping in each encryption operation are random, and the last 12 bytes are divided into three groups, and the XOR result is fixed.

According to the round operation of SM4, the round input $A_1 = (a_{0,1}, a_{1,1}, a_{2,1}, a_{3,1})$ and round output of the first round meet the following conditions:

$$A_1 = M_0 \oplus rk_0 \tag{4}$$

$$X_4 = X_0 \oplus T(A_1) \tag{5}$$

For the second round iteration, it can be obtained that the round input $A_2 = (a_{0,2}, a_{1,2}, a_{2,2}, a_{3,2})$ and the S-box output B_2 of the second round meet the following conditions:

$$A_2 = X_2 \oplus X_3 \oplus X_0 \oplus T(A_1) \oplus rk_1 \tag{6}$$

$$B_2 = \tau(A_2) \tag{7}$$

Step 2: Power analysis

Let $V_1 = T(A_1) \oplus rk_1$, then V_1 is a fixed value. The output B_2 of S-box in the second round of N group encryption operation is selected as the attack object (intermediate value) to conduct CPA (where the value of N, that is, the number of encryption operations, should make CPA analysis successful). The value of V_1 can be obtained, and then the equation for rk_0 and rk_1 is expressed as follows.

$$V_1 = T(M_0 \oplus rk_0) \oplus rk_1 \tag{8}$$

Since there are two unknowns in V_1, the key byte cannot be determined.

Step 3: Repeat steps 1 and 2 twice.

1. Repeat for the first time.

Reselect N groups of plaintext for encryption, input plaintext such that X_0' (the first 4 bytes of plaintext) is a random value,$M_0'(M_0' = X_1' \oplus X_2' \oplus X_3')$ is still fixed and $M_0' \neq M_0$. Let the S-box input of round 1 and round 2 be A_1' $(A_1{}' = (a'_{0,1}, a'_{1,1}, a'_{2,1}, a'_{3,1}))$ and A_2', X_4' be the round output of round 1, B_2' be the round output of round 2 S-box, then

$$A_1' = M_0{}' \oplus rk_0 \tag{9}$$

$$X_4' = X_0' \oplus T(A_1') \tag{10}$$

$$A_2' = X_2' \oplus X_3' \oplus X_0' \oplus T(A_1') \oplus rk_1 \tag{11}$$

$$B_2' = \tau(A_2') \tag{12}$$

Let $V_2 = T(A_1') \oplus rk_1$ (a fixed value) and $X_2' \oplus X_3' \oplus X_0'$ be a random known value, select the output of S-box as the attack object, and conduct CPA on the above N groups of data to recover the value of V_2.

2. Repeat for the second time.

Similarly, the following formula can be obtained by choosing the plaintext input:

$$A_1'' = M_0'' \oplus rk_0 \tag{13}$$

$$X_4'' = X_0'' \oplus T(A_1'') \tag{14}$$

$$A_2'' = X_2'' \oplus X_3'' \oplus X_0'' \oplus T(A_1'') \oplus rk_1 \tag{15}$$

$$B_2'' = \tau(A_2'') \tag{16}$$

where $M_0''(M_0{}'' = X_1'' \oplus X_2'' \oplus X_3'')$ is still fixed and $M_0{}'' \neq M_0' \neq M_0$. A_1'' and A_2'' are the input values of S-box in round 1 and round 2, and B_2'' is the output of S-box in round 2. Then $V_3 = T(M_0'' \oplus rk_0) \oplus rk_1$ can be recovered by chosen plaintext CPA.

To sum up, three equations about rk_0 and rk_1 can be obtained by collecting different plaintext inputs for the chosen plaintext power analysis.

$$\begin{cases} V_1 = T(M_0 \oplus rk_0) \oplus rk_1 \\ V_2 = T(M_0' \oplus rk_0) \oplus rk_1 \\ V_3 = T(M_0'' \oplus rk_0) \oplus rk_1 \end{cases} \tag{17}$$

3.2. Differential Analysis

Differential analysis of the above selected plaintext data includes three different plaintext inputs. It is known that the first round S-box input difference (the S-box input XOR value obtained from the XOR between the first plaintext input and the second plaintext input) $\triangle A_1$ satisfies the following formula:

$$\triangle A_1 = M_0 \oplus rk_0 \oplus M_0' \oplus rk_0 = M_0 \oplus M_0' \tag{18}$$

Similarly, the difference $\triangle A_1{}'$ of the first round S-box input obtained by XOR of the first plaintext input and the third plaintext input satisfies $\triangle A_1{}' = M_0 \oplus M_0''$.

Accordingly, Equation (17) shows that the differences $\triangle C_1$ and $\triangle C_1{}'$ of the first round of L transformation meet the following formula respectively.

$$\triangle C_1 = T(A_1) \oplus T(A_1{}') = V_1 \oplus V_2 \tag{19}$$

$$\triangle C_1{}' = T(A_1) \oplus T(A_1{}'') = V_1 \oplus V_3 \tag{20}$$

The output difference $\triangle B_1$ and $\triangle B_1{}'$ of S-box in the first round can be obtained by conducting L^{-1} inverse operation on $\triangle C_1$ and $\triangle C_1{}'$, and the formula is as follows.

$$\triangle B_1 = \tau(A_1) \oplus \tau(A_1 \oplus \triangle A_1) = L^{-1}(V_1 \oplus V_2) \tag{21}$$

$$\triangle B_1' = \tau(A_1) \oplus \tau(A_1 \oplus \triangle A_1') = L^{-1}(V_1 \oplus V_3) \tag{22}$$

According to the differential definition of S-boxes in Section 2.3, given the input and output differences $(\triangle A_1, \triangle B_1)$ and $(\triangle A_1', \triangle B_1')$ of the four S-boxes in the first round, for the input $(M_0 \oplus rk_0)$ and $(M_0' \oplus rk_0)$ of the four S-boxes, where M_0 and M_0' are known values, then the number of candidate values of every byte $rk_{j,0}(j = 0, 1, 2, 3)$ could be two or four. The probability is 99.2% for two values and is 0.8% for four values. In the following analysis, suppose that the round key has two candidate values. In case there exist four candidate values (very low probability), the attack is seen to fail and is carried out with different inputs again. For the differential analysis results of the above two times, the correct key is the intersection of the two, that is, two sets of key candidate values (99.2% probability) are obtained by the two analyses, respectively, and there is a same value in the two sets, that is, the correct round key byte $rk_{j,0}$. The next step is to analyze and recover the four bytes of rk_0 in turn, and then recover rk_1 from V_1. Finally, the correctness of rk_0 and rk_1 can be further verified by substituting rk_0 and rk_1 into equations set (17).

After rk_0 and rk_1 are recovered, the same method as above is adopted to select plaintext input so that the 12 bytes (3 words) after the third round of input are XOR fixed, that is, $M = X_3 \oplus X_4 \oplus X_5$ is a fixed value, and the first 4 bytes X_2 are random values, where X_3 and X_4 meet the following formulas.

$$X_4 = T(X_1 \oplus X_2 \oplus X_3 \oplus rk_0) \oplus X_0 \tag{23}$$

$$X_5 = T(X_2 \oplus X_3 \oplus X_4 \oplus rk_1) \oplus X_1 \tag{24}$$

The chosen plaintext input can be determined through derivation. For example, if X_2 is selected as random, $X_0 = X_1 = X_2$, and X_3 is a fixed value, then the round input of the third round can be ensured to meet the condition. Similarly, combining the above Sections 3.1 and 3.2 for power analysis and differential analysis based on chosen plaintext, respectively, can restore the values of rk_2 and rk_3 in turn.

In summary, by selecting different plaintext inputs, taking the S-box output of the second and fourth rounds as the attack objects, and combining with differential analysis, the key of the first four rounds of SM4 encryption algorithm can be obtained. Finally, the initial key of SM4 can be recovered by the key expansion algorithm.

3.3. Complexity Analysis and Further Improvement

As mentioned above, there are two steps for our attack. In the first step, i.e., the chosen plaintext attack, to determine the round keys in one round of analysis, three CPAs in one round of analysis are carried out to construct two differential relations of the input and output of S-box. There are 2^8 candidate values for each byte of the sensitive intermediate value, and 3 groups of curves need to be analyzed for attack. Hence, the sum key search space complexity for recovering the four round keys is $6 \times 4 \times 2^8$. Meanwhile, the number of traces needed for our attack is $6 \times N$, where N is the number of traces needed for each CPA.

To make our attack more feasible for experiments, we have made the following improvement. We first discuss the 2nd round of analysis. Since CPA is byte-wise carried out, each byte of rk_0 has two candidate values with near 100% probability. Alternatively, we carry out not three but two CPAs. Consequently, there are 2^4 candidate values for rk_0. Moreover, rk_1 also has 2^4 candidate values corresponding to rk_0 one by one, since rk_1 is determined by rk_0. Unlike the analysis of Section 3.1, we continue to analyze the 2nd round and guess the 2^4 candidate values of rk_0 and rk_1. Based on the guessed round keys, we recalculate the correlation coefficients between the S-box output and the traces. The round key corresponding to the maximum coefficient is the correct one. Then, we carry out another two CPAs in the 4th round of analysis with known rk_0 and rk_1. Likewise, the similar differential analysis is carried out in the 4th round, and 2^4 candidate values of rk_2 and rk_3 are recovered. The correct values of rk_2 and rk_3 can be picked out corresponding

to the maximum coefficient when guessing the candidate values and recalculating the correlation coefficients.

From the improvement, only 4 main CPAs are carried out and the number of traces for analysis has been reduced into $4 \times N$. Moreover, the key search space complexity decreases to $\left(4 \times 2^8 + 2^4\right) \times 2$. To sum up, our attack has obvious advantages at not only the number of traces needed for our attack but also the time complexity. This makes our attack more practical and feasible for experiments.

3.4. Limitations

As mentioned in Section 3.3, although our attack combines the new differential technology and is more feasible for experiments, there still exist some limitations.

Firstly, as introduced in Section 3.2, we only suppose that the round key has two candidate values. Actually, the round key byte has four candidates. For the case that there exist four candidate values, the attack is viewed to fail and is carried out with different inputs again. Furthermore, if we guess the four candidates in the analysis, the complexity analysis will increase. This is also what we will study and verify in the future. Secondly, when the implementation of SM4 has masking countermeasures and the S-box is masked with random numbers (this case is very common), our attack will fail. For the masking implementation, we will further consider to combine template attack and collision attack.

4. Experiments

For the above combined attacks, we carried out experimental verification on the SM4 algorithm implemented in FPGA chip, mainly verifying the feasibility and effect of the attack.

4.1. Experimental Environment

The FPGA chip used in the experiment (implementing SM4 algorithm) is SAKURA-G FPGA test board, and the Riscure suite about power analysis attack is used for our attack, including analysis of Software Inspector and hardware oscilloscope for acquisition. The whole analysis process is shown in Figure 2, including the following three steps. (1) PC delivers plaintext to SAKURA-G FPGA test board, and the test board performs SM4 encryption operation and generates trigger signal at the same time. (2) The PC sends control instructions to the oscilloscope to collect the power consumption curves leaked by the SM4 encryption operation, and sends the information to the PC for saving. (3) The collected SM4 power leakage curves are combined and analyzed by Riscure power analysis Software Inspector.

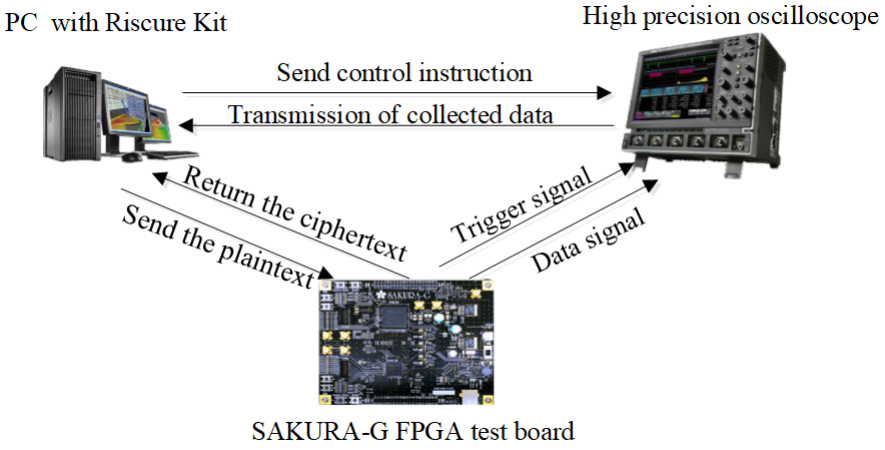

Figure 2. Measurement environment.

4.2. Attack Instances

In the experiment, the second round (the input of the first round needs to be controlled, so that rk_0 and rk_1 are recovered) is selected as the analysis object for attack examples. The analysis of the fourth round (the input of the third round needs to be controlled) is similar to that of the second round.

Based on the above experimental environment, three groups of power leakage curves A, B and C (1000 for each group) are collected, and the plaintext input of the curves need to satisfy the following requirements:

Group A: $M_0 = X_1 \oplus X_2 \oplus X_3$ is a fixed value, X_0 is a random value;

Group B: $M_0' = X_1' \oplus X_2' \oplus X_3'$ is a fixed value, X_0' is a random value;

Group C: $M_0'' = X_1'' \oplus X_2'' \oplus X_3''$ is a fixed value, X_0'' is a random value.

where $M_0 \neq M_0' \neq M_0''$.

As shown in Figure 3, the power curve of data collection in group A includes plaintext input, 32 obvious peaks, and ciphertexts output; each peak represents the round operation of SM4. The second peak (corresponding intermediate value is the output of the second round S box) is selected for attack. When the number of the power consumption curves is 1000, the correlation coefficient results of the attack are shown in Figures 4–7. There are four obvious peaks, which respectively represent the correlation between the correct guess value of V_1 four bytes and the power consumption curve sample points. Therefore, the correct V_1 can be determined. Similarly, the power consumption curves of group B and C are analyzed successively to recover V_2 and V_3. Using V_1, V_2, V_3 and chosen input plaintext values, the input and output difference of S-box is calculated, the round key rk_0 of the first round is recovered, and then rk_1 is deduced. Meanwhile, we can use two of the three values V_1, V_2, V_3, and chosen input plaintext values, calculate 16 candidate values for rk_0, and recalculate the correlation coefficients between the S-box output and the traces; the round key corresponding to the maximum coefficient is the correct rk_0, and then rk_1 is deduced.

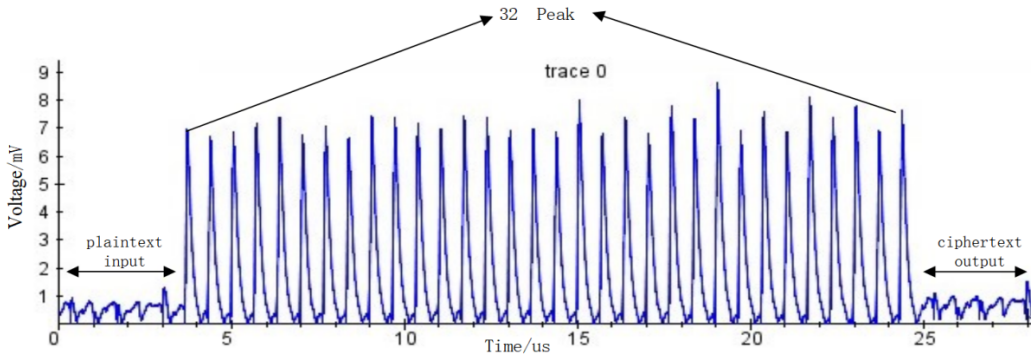

Figure 3. The power traces of SM4 encryption process.

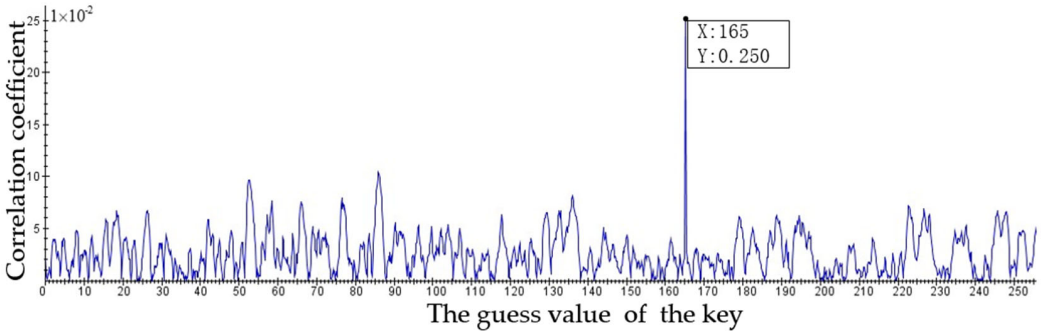

Figure 4. The first byte of V_1 CPA attack result.

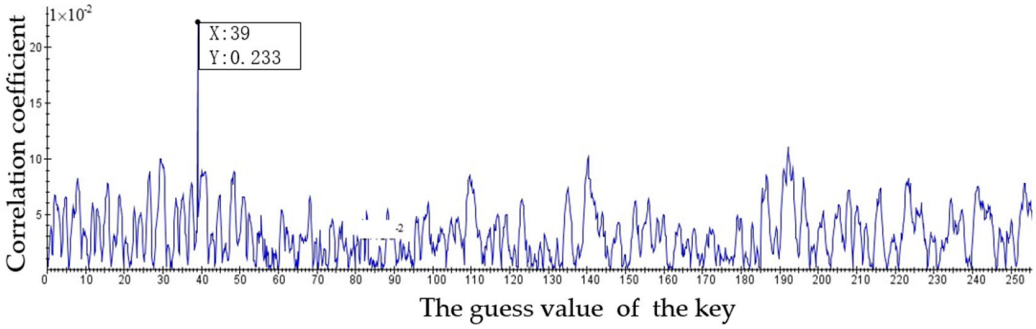

Figure 5. The second byte of V_1 CPA attack result.

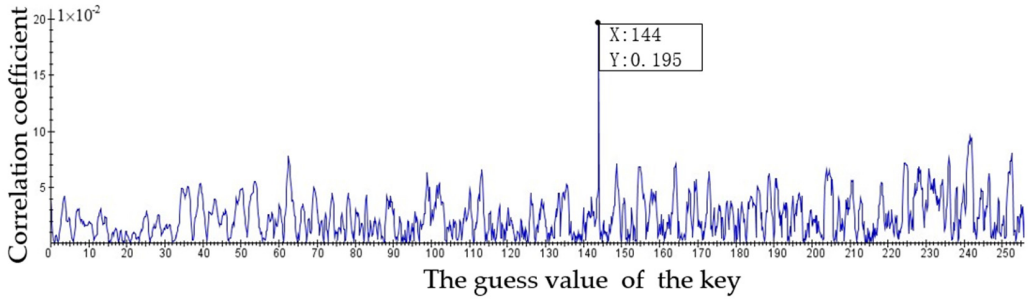

Figure 6. The third byte of V_1 CPA attack result.

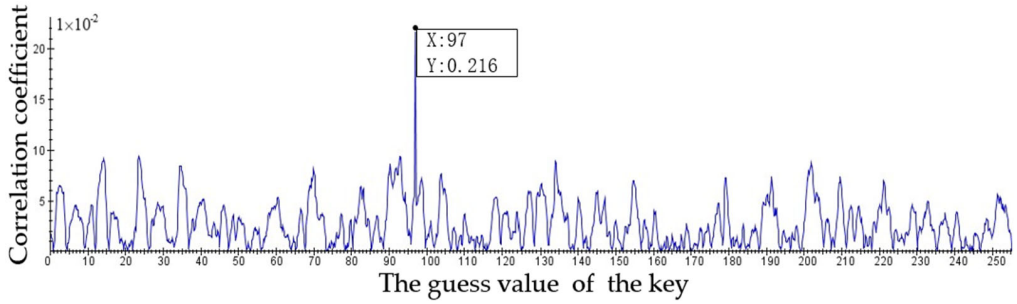

Figure 7. The fourth byte of V_1 CPA attack result.

Based on the keys rk_0 and rk_1 of the first and second rounds of the above attack, the input plaintext can make the input of the third round meet the attack conditions. The three groups of curves are collected again, and the output of the fourth round S-box on the curve is selected as the attack object to attack, and the round key rk_2 and rk_3 are obtained. Finally, the 128-bit initial key is completely recovered by the SM4 key extension algorithm.

4.3. Comparison with other Attack Methods

Compared with the previous chosen plaintext attack, the combined round reduction attack in this paper has obvious advantages on the number of rounds needed for attack, the selection of attack points and the number of times for collecting traces. The SM4 encryption attack is used as an example for comparison.

As shown in Table 1, our combined attack reduces the number of attack rounds by half, and our attack only needs to collect traces twice, which is significantly less than the number of plaintext selections in previous attacks, thus improving the efficiency of attack. In addition, compared with the previous linear XOR or L transformation and round output, our attack chooses the output of S-box as the attack point, which effectively improves the SNR and success rate of the attack. Furthermore, the sum number of traces, i.e., $4 \times N$, (N is the number of traces for a single successful attack) required for recovering the round keys of the first four rounds in our attack is obviously less than those ($16 \times N$) for the previous

chosen-plaintext attacks [13,15,16]. Although the sum number of traces in Reference [14] is $4 \times N$, needing to collect traces four times, our combined attack only needs to attack 2 times and collect traces twice, reducing collection time and attack time. Finally, key search space complexity is smaller than previous chosen-plaintext attacks [13–16].

Table 1. Comparison of four attack methods' features.

Attack Methods	The Rounds of Chosen Plaintext	The Intermediate Value of Power Attack	The Number of Times for Collecting Traces	The Sum Number of Traces	Key Search Space Complexity
Reference [13]	1, 2, 3, 4	L transformation for rounds 1, 2, 3, and 4	16	$16 \times N$	$4 \times 4 \times 2^8$
Reference [14]	1, 2, 3, 4	Round output of rounds 1, 2, 3, and 4	4	$4 \times N$	$4 \times 4 \times 2^8$
Reference [15]	1, 2, 3, 4	Round output of rounds 1, 2, 3, and 4	16	$16 \times N$	$4 \times 4 \times 2^8$
Reference [16]	1, 2, 3, 4	Round output of rounds 1, 2, 3, and 4	16	$16 \times N$	$4 \times 4 \times 2^8$
Our attack	2, 4	The S-box output of 2th and 4th rounds	2	$4 \times N$	$(4 \times 2^8 + 2^4) \times 2$

5. Conclusions

In this paper, we proposed a method that uses chosen plaintext power analysis for SM4 to improve the efficiency existing power analysis for SM4. The method reduces the number of attack rounds, the number of plaintext selections, and the search space of the key, and it selects the nonlinear s-box output as the attack point. This method is not only applied to analyze the first four rounds of SM4 encryption, but also effective to the first four rounds of SM4 decryption. Moreover, this method can also be directly applied to other grouping cipher attacks with similar differential features of S-box, such as AES. Meanwhile, we also can carry out our attack on the first four rounds on SM4 decryption. Another possibility for future work is to combine other cryptanalysis and side channel attacks, such as combining power analysis and algebraic analysis.

Author Contributions: Conceptualization, J.R. and Z.C.; methodology, J.R.; software, J.R.; investigation, J.R.; resources, Z.C.; writing—original draft preparation, J.R.; writing—review and editing. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by Sichuan Sciences and Technology Program (No.2018ZDZX0015), Sichuan Sciences and Technology Program (NO: 2019ZDZX0005), Sichuan Sciences and Technology Program (NO: 2022ZHCG0007).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: I would like to thank my supervisor, for his guidance through each stage of the process.

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

References

1. Kocher, P.; Jaffe, J.; Jun, B. Differential power analysis. In Proceedings of the 19th Annual International Cryptology Conference, Santa Barbara, CA, USA, 15–19 August 1999.
2. Eric, B.; Christophe, C.; Francis, O. Correlation power analysis with a leakage model. In Proceedings of the 6th International Workshop, Cambridge, MA, USA, 11–13 August 2004.

3. Tunstall, M.; Hanley, N.; McEvoy, R.P.; Whelan, C.; Murphy, C.C.; Marnane, W.P. Correlation power analysis of large word sizes. In Proceedings of the IET Irish Signals and Systems Conference, Derry, Ireland, 13–14 September 2007; pp. 145–150.
4. Pan, W.; Marnane, W. A Correlation Power Analysis Attack against Tate Pairing on FPGA. In Proceedings of the International Conference on Reconfigurable Computing: Architectures Tools and Applications, Belfast, UK, 23–25 March 2011.
5. Suresh, C.; Josyula, R.; Pankaj, R. Template Attacks. In Proceedings of the 4th International Workshop, Redwood Shores, CA, USA, 13–15 August 2003.
6. Rechberger, C.; Oswald, E. Practical Template Attacks. In Proceedings of the 5th WISA 2004 International Workshop, Jeju Island, Korea, 23–25 August 2004.
7. Archambeau, C.; Peeters, E.; Standaert, F.X.; Quisquater, J.J. Template attacks in principal subspaces. In Proceedings of the 8th International Conference on Cryptographic Hardware and Embedded Systems, Yokohama, Japan, 10–13 October 2006.
8. Fan, H.P.; Yuan, Q.J.; Wang, X.Y.; Wang, Y.J.; Wang, T. Key Advantage Template Attack against AES-128 Algorithm. *Acta Electonica Sin.* **2020**, *48*, 2003–2008.
9. Batina, L.; Gierlichs, B.; Prouff, E.; Rivain, M.; Standaert, F.X.; Veyrat-Charvillon, N. Mutual Information Analysis: A Comprehensive Study. *J. Cryptol.* **2011**, *24*, 269–291. [CrossRef]
10. Block Cipher for WLAN Products-SMS4. Available online: http://www.oscca.gov.cn/UpFile/200621016423197990.pdf (accessed on 1 January 2006).
11. Zhang, L.; Wu, W.L. Differential Fault Analysis on SMS4. *Chin. J. Comput.* **2006**, *029*, 1596–1602.
12. Hu, W.J.; Wang, A.; Wu, L.J.; Xie, X.J. Power Attack of SM4 Hardware Implementation Based on SAKURA-G Board. *Microelectron. Comput.* **2015**, *4*, 15–20.
13. Wang, S.; Gu, D.; Liu, J.; Guo, Z.; Wang, W.; Bao, S. A Power Analysis on SMS4 Using the Chosen Plaintext Method. In Proceedings of the Ninth International Conference on Computational Intelligence & Security, Sichuan, China, 16 October 2013.
14. Du, Z.B.; Wu, Z.; Wang, M.; Rao, J.T. Chosen-plaintext power analysis attack against SMS4 with the round-output as the intermediate data. *J. Commun.* **2015**, *36*, 146–152.
15. Shan, W.; Wang, L.; Li, Q.; Guo, L.; Liu, S.; Zhang, Z. A chosen-plaintext method of CPA on SM4 block cipher. In Proceedings of the 2014 Tenth International Conference on Computational Intelligence and Security, Yunnan, China, 15–16 November 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 363–366.
16. Jia, Z.; He, X.; Bei, B. Improved chosen-plaintext DPA on block cipher SM4. *J. Tsinghua Univ. (Sci. Technol.)* **2017**, *57*, 1134–1138.
17. Hu, W.; Wu, L.; Wang, A.; Xie, X.; Zhu, Z.; Luo, S. Adaptive chosen-plaintext correlation power analysis. In Proceedings of the 2014 Tenth International Conference on Computational Intelligence and Security, Yunnan, China, 15–16 November 2014; IEEE: Piscataway, NJ, USA, 2014; pp. 494–498.
18. Heuser, A.; Rioul, O.; Guilley, S. Good is not good enough, deriving optimal distinguishers from communication theory. In Proceedings of the International Workshop on Cryptographic Hardware and Embedded Systems–CHES 2014, Busan, Korea, 23–26 September 2014; Volume 8731, pp. 55–74.
19. Ouladj, M.; Guillot, P.; Mokrane, F. Chosen message strategy to improve the correlation power analysis. *IET Inf. Secur.* **2019**, *13*, 304–310. [CrossRef]
20. Clavier, C.; Isorez, Q.; Wurcker, A. Complete SCARE of AES-like block ciphers by chosen plaintext collision power analysis. In Proceedings of the International Conference on Cryptology in India, Mumbai, India, 7–10 December 2018; Springer: Cham, Switzerland, 2013; pp. 116–135.
21. Ding, Y.; Shi, Y.; Wang, A.; Zheng, X.; Wang, Z.; Zhang, G. Adaptive chosen-plaintext collision attack on masked AES in edge computing. *IEEE Access* **2019**, *7*, 63217–63229. [CrossRef]
22. Zheng, D.; Wang, L.; Zhao, B.; Zhang, M. Improved chosen-plaintext collision attack on masked AES. *J. Xi'an Univ. Posts Telecommun.* **2021**, *6*, 57–65.
23. Zhang, B.; Wang, A.; Zhu, L.; Xu, R.; Jia, X. Bitwise chosen plaintext power analysis on AES. *Cyberspace Secur.* **2019**, *3*, 93–98.
24. Deng, G.; Zhang, P.; Wu, H.; Zou, C. Adaptive chosen plaintext template analysis against cipher chips. *J. Huazhong Univ. Sci. Technol. (Nat. Sci. Ed.)* **2010**, *11*, 55–59.
25. Guo, L.; Wang, L.; Liu, D.; Shan, W.; Zhang, Z.; Li, Q.; Yu, J. A chosen-plaintext differential power analysis attack on HMAC-SM3. In Proceedings of the 2015 11th International Conference on Computational Intelligence and Security (CIS), Shenzhen, China, 19–20 December 2015; IEEE: Piscataway, NJ, USA, 2015; pp. 350–353.
26. Takemoto, S.; Nozaki, Y.; Yoshikawa, M. Differential power analysis using chosen-plaintext for unrolled PRINCE. In Proceedings of the 2018 International Conference on Robotics, Control and Automation Engineering, Beijing, China, 26–28 December 2018; pp. 152–155.
27. Li, Z.; Peng, G.; Shi, R.; Li, C.; Ma, Z.; Li, H. Chosen Plaintext Attacks on CRT-RSA. *J. Cryptologic Res.* **2016**, *3*, 447–461.
28. Azouaoui, M.; Kuzovkova, Y.; Schneider, T.; van Vredendaal, C. Post-Quantum Authenticated Encryption against Chosen-Ciphertext Side-Channel Attacks. Cryptology ePrint Archive, Report 2022/91. 2022. Available online: https://eprint.iacr.org/2022/916 (accessed on 1 January 2022).
29. Veyrat-Charvillon, N.; Standaert, F.X. Adaptive chosen-message side-channel attacks. In Proceedings of the International Conference on Applied Cryptography and Network Security, Beijing, China, 22–25 June 2010; Springer: Berlin/Heidelberg, Germany, 2010; pp. 186–199.