PROCEEDINGS OF SCIENCE

FPGA Implementation of AES Algorithm Resistant Power Analysis attacks

Lang Li[1]
College of Computer Science and Technology, Hengyang Normal University
HengYang, 421002, China
E-mail: `lilang911@126.com`

Yi Zou[2]
College of Computer Science and Technology, Hengyang Normal University
HengYang,421002, China
E-mail: `zou_zouyi@163.com`

Ge Jiao[3]
College of Computer Science and Technology, Hengyang Normal University
HengYang, 421002, China
E-mail: `jiaoge@126.com`

In order to be more effectively resist differential power analysis attacks, the improved fixed value masking algorithm is proposed for resource-constrained smart card based on fixed value masking and random masking. Firstly, a number of random numbers are selected and prestored in on-chip ROM for generating the corresponding byte-substitution table. It does not increase much power and hardware resources because the byte-substitution table is pregenerated. Finally, experiments in terms of the second-order differential power analysis attacks have been carried outon the improved fixed masking. The experimental results show that the proposed AES algorithm can be effectively resistant to the side-channel attacks with lower computing expenses and higher security.

CENet2017
22-23 July 2017
Shanghai, China

[1] Lang Li(1971-), Ph.D., his research interests include the embedded computing and the information security.

[2] This research is supported by the National Natural Science Foundation of China under Grant No.:61572174, the Scientific Research Fund of Hunan Provincial Education Department with Grant No.: 15A029, the Scientific Research fund of Hengyang Normal University with Grant No.: 16CXYZ01, the Science and Technology Plan Project of Hunan Province No.: 2016TP1020, Hunan Provincial Natural Science Foundation of China with Grant No.: 2015JJ4011, 2017JJ4001.

[3] Correspongding Author: lilang911@126.com

1.Introduction

At present, the password security of all kinds of smart cards have achieved the people's concerns and attention.SCA(Side Channel Attacks) was proposed in one paper[1], which completely broke the traditional way of cipher algorithm algebra brute force Attacks. The SCA depends on the leakage power consumption during the process of encryption, time and physical information such as electromagnetic radiation, which can decipher the key at a very low cost. The safety smart card needs to enhance the protection method in the design and technical research of implementation against the side channel attacks [2].

2. Improvement of the Fixed Value by Masking AES algorithm and the Optimized Implementation

2.1 Mathematical Proof of the Masking AES Algorithm Resistant to the ide-Channel Attacks

Plaintext P_t masks by using the random number *m*, key represents the encryption key to mask the keys with random number m_k. The byte substitution operation in AES algorithm needs a corresponding amendment, satisfies the new byte substitution:

$$SubBytes'(x+m) = SubBytes(x) + m' \tag{2.1}$$

After the mask, key and plaintext are output from the changing S-box:

$$S'[(P_t+m)+(key+m_k)] = S'[P_t+key+m+m_k] = S[p_t+key]+m_s \tag{2.2}$$

where m_s=m+ m_k

Without the masking byte substitution operation, if there is a guessed value *k* of the key, there is output byte substitution $S[P_t] + k$. With the output of the No.b value as the classification function, *n* power curves V_{ij} can be divided into two groups as follows:

$$V_0(S[P_t+k]) = \{V_{ij} \mid D_b(S[P_t+k])=0\} \tag{2.3}$$

$$V_1(S[P_t+k]) = \{V_{ij} \mid D_b(S[P_t+k])=1\} \tag{2.4}$$

Due to the randomicity of plain text input, each digit probability of 1s and 0s is 50%. You can think of the two groups of size *n / 2*. For each group, on average, after subtracting the received *j** time differential curve for the power consumption of the DPA:

$$T[j^*] = \frac{2}{n}\{\sum_{V_{ij}\in V_0(S[P_t\oplus key])} V_{ij} - \sum_{V_{ij}\in V_1(S[P_t\oplus key])} V_{ij}\} \tag{2.5}$$

Set the probability that the No.d bit value of a number x is 0 as $\beta_d(x)$. As the exclusive-OR with 0 does not change the original value, the probability that the No.d bit of $S[p_t] + k$ equals to the No. d of $S[p_t] + k + m_s$ is $\beta_d(m_s)$. Rewrite the equation above:

$$\begin{aligned} T[j^*] = {} & \frac{2}{n}\{\beta_d(m_s)\sum_{V_{ij}\in V_0(S[P_t\oplus k]\oplus m_s)} V_{ij} + (1-\beta_d(m_s))\sum_{V_{ij}\in V_1(S[P_t\oplus k]\oplus m_s)} V_{ij} - \\ & \beta_d(m_s)\sum_{V_{ij}\in V_1(S[P_t\oplus k]\oplus m_s)} V_{ij} - (1-\beta_d(m_s))\sum_{V_{ij}\in V_1(S[P_t\oplus k]\oplus m_s)} V_{ij}\} \\ = {} & \frac{2(2\beta_d(m_s)-1)}{n}\{\sum_{V_{ij}\in V_0(S[P_t\oplus k]\oplus m_s)} V_{ij} - \sum_{V_{ij}\in V_1(S[P_t\oplus k]\oplus m_s)} V_{ij}\} \end{aligned} \tag{2.6}$$

From Equation (2.6), if $\beta_d (m_s)$ is 0.5, i.e. The probability of an arbitrary number of 0 is 0.5, the peak amplitude $T^*[j]$ is 0, which prove that a random number masking method can resist side channel attacks by means of mathematical formalization.

2.2 Design Idea about Optimization

There are many added methods of random masking AES algorithm, including fixed value look-up table method, the improved fixed value look-up table method, multiplicative masking method, simplified multiplication masking method, embedded multiplication mask, etc. Partial methods are still not completely resistance to side channel attack, such as multiplication masking method with security risk of an attack by zero value, at meanwhile, the majority masking added methods have higher resource usage and are not suitable for resource-constrained smart card equipment safety. This paper proposes the improved fixed value look-up table method based on the fixed value look-up table method [3].

For the disadvantage of the look-up table method, that there are 256 values of the random number “m” with eight bits, and there are 256 new byte substitution form accordingly. If the encryption by using a random number each time is not fixed, the corresponding byte substitution must be quickly provided. If the method of fixed generation is used, you must store these tables to improve the computing speed. There are 256 kinds of tables, each table contains 256 values, the area consumption in the smart card development design is not acceptable. If the look-up table is generated randomly, it will consume speed and power and decryption time is basically spent in byte substitution table generation, which is clearly unacceptable by smart card producers and consumers.

With these defects, we put forward an improved fixed value masking algorithm, in which we chose a few fixed random numbers at the outset to produce a few bytes substitution tables stored in advance, then selected number randomly from the several fixed possible values during encryption. As the byte substitution tables are generated in advance, the area consumption is not too much and the speed of fixed value masking look-up table is fast. The diagram of the implementation in this way is shown as follows:

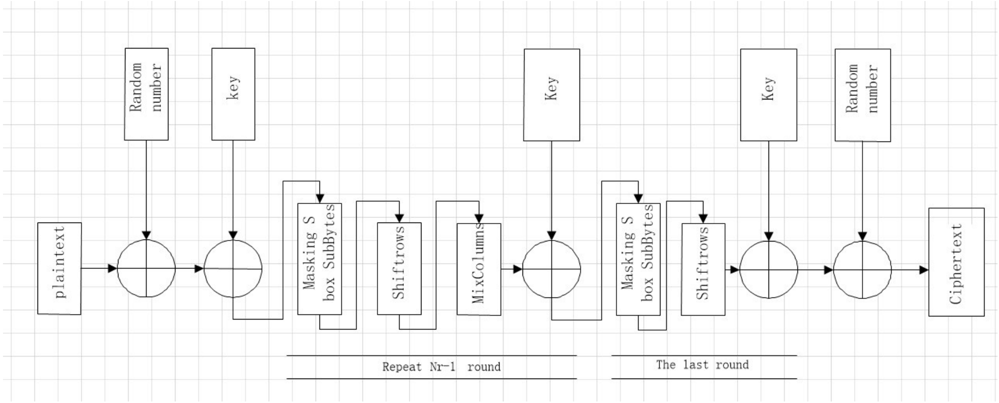
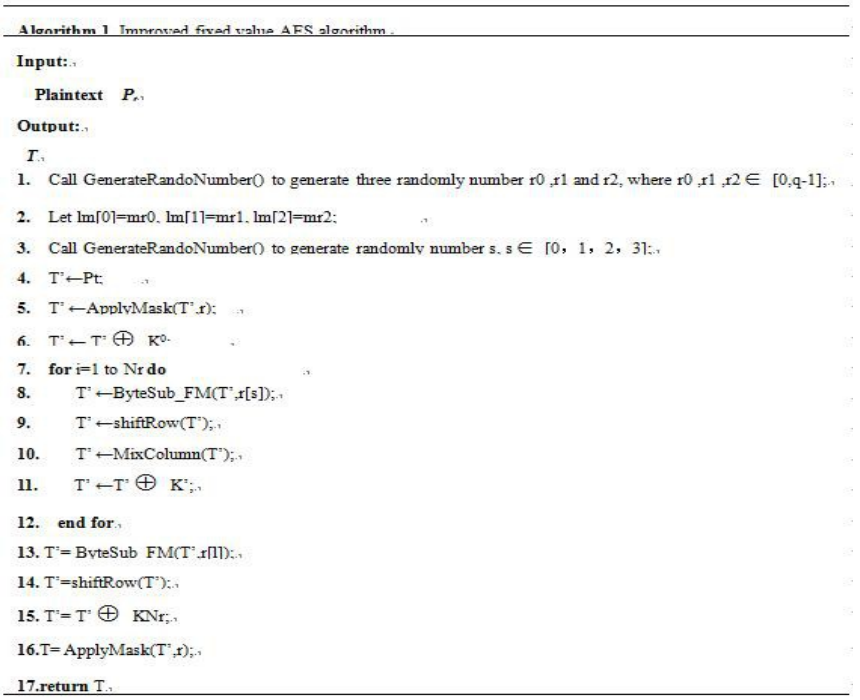


Figure 1: Framework of the Improved Fixed Value Masking Algorithm

The implementation method of the fixed value masking algorithm is described in detail as follows. Extract a few fixed values mask from a random number according to the strength of encryption key chip. The following is the implementation method of masking algorithm [4-6] in which three random Numbers are extracted as the fixed value:



Algorithm 1 Improved fixed value AES algorithm

```
Input:
  Plaintext  P
Output:
  T
Call GenerateRandoNumber() to generate three randomly number r0 ,r1 and r2, where r0 ,r1 ,r2 ∈ [0,q-1];
Let lm[0]=mr0, lm[1]=mr1, lm[2]=mr2;
Call GenerateRandoNumber() to generate randomly number s, s ∈ [0，1，2，3];
T'←Pt;
T' ←ApplyMask(T',r);
T' ← T' ⊕ K0
for i=1 to Nr do
    T' ←ByteSub_FM(T',r[s]);
    T' ←shiftRow(T');
    T' ←MixColumn(T');
    T' ←T' ⊕ K';
end for
T'= ByteSub FM(T',r[1]);
T'=shiftRow(T');
T'= T' ⊕ KNr;
T= ApplyMask(T',r);
return T
```

2.2 Generation of S-box

To effectively and correctly generate the S-boxes, you need to write the program to automatically generate a new S box. The flow diagram of S-boxes generation is as follows in Figure 2:

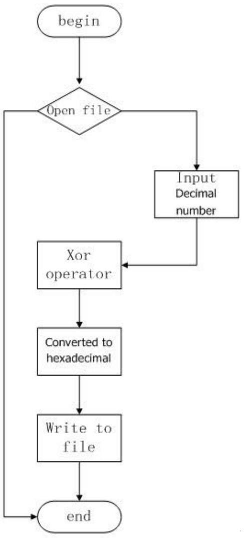


Figure 2: Framework of S-box

2.3 Core Code of AES Algorithm

Keep the original basic framework of AES algorithm code, the ciphertext XOR mask, select the corresponding mask S-box for the S-box, do exclusive-OR of the state and mask at last input so as to recover the standard cipher text.

input：

```
always @(posedge clk) sa33 <= #1 ld_r ? text_in_r[007:000]^ w3[07:00]^ 8'h11: sa33_next;
……
always @(posedge clk) sa00 <= #1 ld_r ? text_in_r[127:120]^w0[31:24]^ 8'h11: sa00_next;
```

the output：

```
always @(posedge clk) text_out[127:120] <= #1 (dcnt==0)?text_out[127:120]^ 8'h11:sa00_sr ^ w0[31:24] ;
……
always @(posedge clk) text_out[007:000] <= #1 (dcnt==0)?text_out[007:000]^ 8'h11:sa33_sr ^ w3[07:00] ;
```

With the random algorithm, the amended S box added corresponding mask can achieve the standard implementation of fixed value algorithm.

2.4 Experiment Results

The improved fixed value masking AES algorithm can be simulated with modelsim6.1f function correctly, the result of simulation waveform is shown as follows in Figure 3.

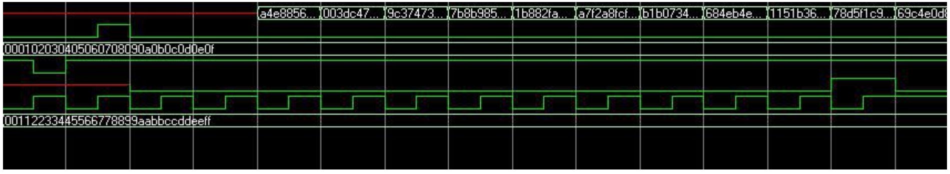
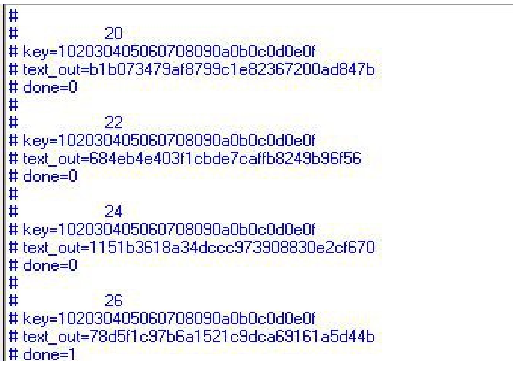


Figure 3: Waveform of the Improved Fixed Value Masking AES Algorithm

The simulation results are shown in Figure 4.



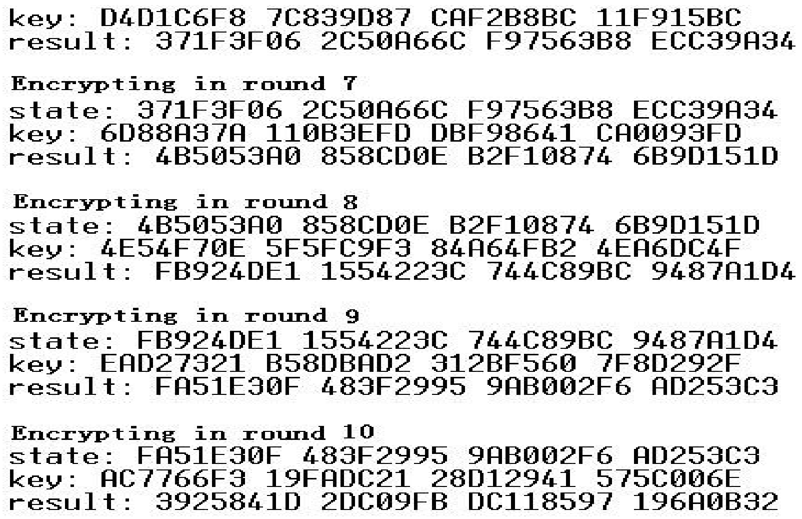
```
#
#             20
# key=102030405060708090a0b0c0d0e0f
# text_out=b1b073479af8799c1e82367200ad847b
# done=0
#
#             22
# key=102030405060708090a0b0c0d0e0f
# text_out=684eb4e403f1cbde7caffb8249b96f56
# done=0
#
#             24
# key=102030405060708090a0b0c0d0e0f
# text_out=1151b3618a34dccc973908830e2cf670
# done=0
#
#             26
# key=102030405060708090a0b0c0d0e0f
# text_out=78d5f1c97b6a1521c9dca69161a5d44b
# done=1
```

Figure 4: Output of the Improved Fixed Value Masking AES Algorithm

3.The implementation of the improved fixed value of masking AES algorithm on FPGA

3.1 The FPGA Implementation

After the hardware language of the improved fixed value masking AES algorithm, it is downloaded to the FPGA. The final running results are shown in Figure 5.



```
key: D4D1C6F8 7C839D87 CAF2B8BC 11F915BC
result: 371F3F06 2C50A66C F97563B8 ECC39A34

Encrypting in round 7
state: 371F3F06 2C50A66C F97563B8 ECC39A34
key: 6D88A37A 110B3EFD DBF98641 CA0093FD
result: 4B5053A0 858CD0E B2F10874 6B9D151D

Encrypting in round 8
state: 4B5053A0 858CD0E B2F10874 6B9D151D
key: 4E54F70E 5F5FC9F3 84A64FB2 4EA6DC4F
result: FB924DE1 1554223C 744C89BC 9487A1D4

Encrypting in round 9
state: FB924DE1 1554223C 744C89BC 9487A1D4
key: EAD27321 B58DBAD2 312BF560 7F8D292F
result: FA51E30F 483F2995 9AB002F6 AD253C3

Encrypting in round 10
state: FA51E30F 483F2995 9AB002F6 AD253C3
key: AC7766F3 19FADC21 28D12941 575C006E
result: 3925841D 2DC09FB DC118597 196A0B32
```

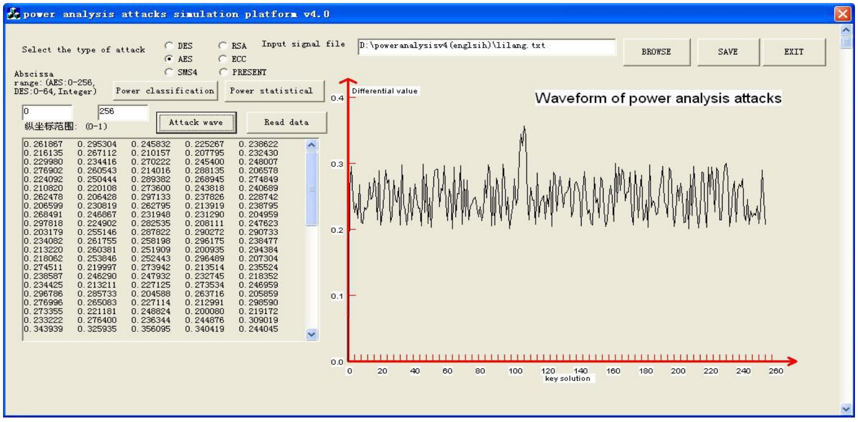
Figure 5 : Improved Fixed Value Masking AES Algorithm on FPGA

The downloaded operation figure can verify that the results of the corresponding design are correct.

3.2 Experiments of Resistance to Power Analysis Attack

The experiments of resistance to the second-order differential power attack have been carryied out with the improved fixed value mask AES algorithm and a fixed value masking algorithm respectively. As the basic idea of experiment, first of all, the IP core of the fixed value mask and the improved one are implemented respectively to simulate the function operation of IP core, then extract the inversion of 1-0 and 0-1. The inversion directly corresponds to the change of the power curve during encryption key chip operation. By means of software programming and automatic statistical analysis according to the principle of the bypass attack, we conclude the results in Figure 6 and Figure 7.

The experimental results of a fixed value mask second-order differential power attack are shown in Figure 6.



power analysis attacks simulation platform v4.0

Select the type of attack ○ DES ● AES ○ SMS4 ○ RSA ○ ECC ○ PRESENT

Input signal file D:\poweranalysisv4(englsih)\lilang.txt

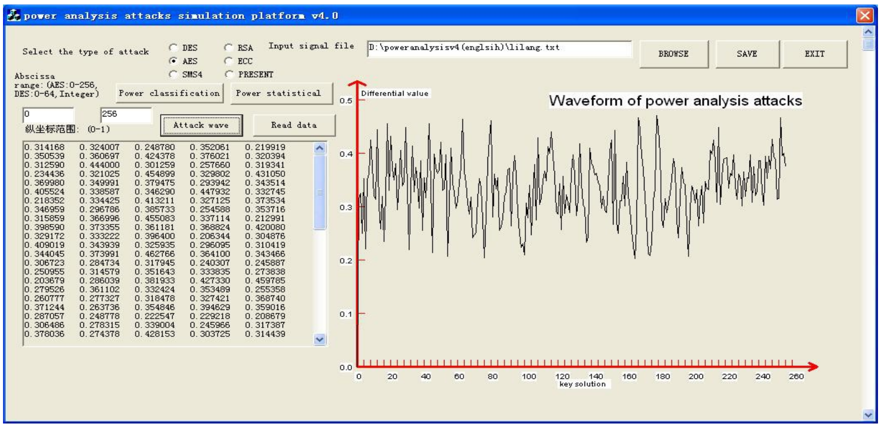
Abscissa range:(AES:0-256, DES:0-64,Integer) 0 256

纵坐标范围: (0-1)

```
0.261867   0.295304   0.245832   0.225267   0.238622
0.216135   0.267112   0.210157   0.207795   0.232430
0.229980   0.234416   0.270222   0.245400   0.248007
0.276902   0.260543   0.214016   0.288135   0.206578
0.224092   0.250444   0.289382   0.268945   0.274849
0.210820   0.220108   0.273600   0.243818   0.240689
0.262478   0.206428   0.297133   0.237826   0.228742
0.206599   0.230819   0.262795   0.213919   0.238795
0.268491   0.246867   0.231948   0.231290   0.204959
0.297818   0.224902   0.282535   0.208111   0.247623
0.203179   0.255146   0.287822   0.290272   0.290733
0.234082   0.261755   0.258198   0.296175   0.238477
0.213220   0.260381   0.251909   0.200935   0.294384
0.218062   0.253846   0.252443   0.296489   0.207304
0.274511   0.219997   0.273942   0.213514   0.235524
0.238587   0.246290   0.247932   0.232745   0.218352
0.234425   0.213211   0.227125   0.273534   0.246959
0.296786   0.285733   0.204588   0.263716   0.205859
0.276996   0.265083   0.227114   0.212991   0.298590
0.273355   0.221181   0.248824   0.200080   0.219172
0.233222   0.276400   0.236344   0.244876   0.309019
0.343939   0.325935   0.356095   0.340419   0.244045
```

Figure 6 : Attack's Results of A Fixed Value Mask Order DPA

The experimental results of the improved fixed value mask second-order differential power consumption attack are shown in Figure 7.



power analysis attacks simulation platform v4.0

Select the type of attack ○ DES ○ RSA ● AES ○ ECC ○ SMS4 ○ PRESENT

Input signal file: D:\poweranalysisv4(englsih)\lilang.txt

Abscissa range:(AES:0-256, DES:0-64, Integer): 0 256

纵坐标范围：(0-1)

```
0.314168    0.324007    0.248780    0.352061    0.219919
0.350539    0.360697    0.424378    0.376021    0.320394
0.312590    0.444000    0.301259    0.257660    0.319341
0.234436    0.321025    0.454899    0.329802    0.431050
0.369980    0.349991    0.379475    0.293942    0.343514
0.405524    0.338587    0.346290    0.447932    0.332745
0.218352    0.334425    0.413211    0.327125    0.373534
0.346959    0.296786    0.385733    0.254588    0.353716
0.315859    0.366996    0.455083    0.337114    0.212991
0.398590    0.373355    0.361181    0.368824    0.420080
0.329172    0.333222    0.396400    0.206344    0.304876
0.409019    0.343939    0.325935    0.296095    0.310419
0.344045    0.373991    0.462766    0.364100    0.343466
0.306723    0.284734    0.317945    0.240307    0.245887
0.250955    0.314579    0.351643    0.333835    0.273838
0.203679    0.286039    0.381933    0.427330    0.459785
0.279526    0.361102    0.332424    0.353489    0.255358
0.260777    0.277327    0.318478    0.327421    0.368740
0.371244    0.263736    0.354846    0.394629    0.359016
0.287057    0.248778    0.222547    0.229218    0.208679
0.306486    0.278315    0.339004    0.245966    0.317387
0.378036    0.274378    0.428153    0.303725    0.314439
```

Figure 7: The 2-order DPA Results of the Improved Fixed Value Masking

From Figure 6 and Figure 7, we know the result that a fixed value mask is unable of resisting the second-order differential power consumption attack, which is consistent with the validated results in other literature, while the improved fixed value mask can resist the second-order DPA.

4. Conclusion

The mask method resistant to the side-channel attack is profoundly studied in this paper. With the widespread use of smart card, its security has attracted the people's wide attention and research. A smart card is resource-constrained device, and its size and operation ability are limited. This paper proposes an improved method of fixed value mask based on the fixed value mask, describes the specific hardware implementation in detail, and verifies the corresponding experimental results. Based on the experiment results, we can conclude that the improved fixed value mask algorithm highlights better performance than the fixed value mask algorithm in resistance to side-channel attack with less increase of resource consumption.

References

[1]P Kocher, J Jaffe, B Jun. *Differential power analysis*[A].Advanced in Cryptology–CRYPTO '99[C]. California, USA: Springer Verlag.1999:388-397.

[2]Li Lang, Li Renfa, Tong Yuanman. *Development on Power Analysis Attack and Defense of Embedded Cipher Chip*[J].Journal of Computer Research and Development, 2010, 47(4): 595- 604.

[3]Yoshikawa M, Nozaki Y. *Power Analysis Attack and Its Countermeasure for a Lightweight Block Cipher Simon*[M]// Information Technology: New Generations. Springer International Publishing, 2016.

[4]Li Lang. *The block cipher chip, power attack and defense research* [D]. Changsha: hunan university, Ph.D. Thesis,2010.12.

[5]Masoumi M, Rezayati M H. *Novel Approach to Protect Advanced Encryption Standard Algorithm Implementation Against Differential Electromagnetic and Power Analysis*[J]. IEEE Transactions on Information Forensics & Security, 2015, 10(2):256-265.

[6]Eldib H, Wang C, Taha M, et al. *Quantitative Masking Strength: Quantifying the Power Side-Channel Resistance of Software Code*[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2015, 34(10):1558-1568.