An Improved AES Masking Method Smartcard Implementation for Resisting DPA Attacks

Xiaoan Zhou[1] , Juan Peng[1,2], Liping Guo[2,3]

[1]Information and engineering institution, Shenzhen University, Shenzhen, Guangdong 518060, China

[2]Security IC laboratory, Nationz Technologies Inc., Shenzhen, Guangdong 518057, China

[3]Computer Sciences and Technology Institution, University of Science and Technology of China, Hefei, Anhui 230022, China

Abstract

To improve the DPA (Differential Power Analysis) resistance of a cryptographic device such as a smartcard and facilitate the implementation of hardware, the paper proposes an improved masking method on AES for resisting DPA. The paper uses a multiplicative inversion in finite field GF (2^4) instead of GF (2^8) to reduce the complexity of the operation. The key of the presented method is to make each intermediate result being masked by random numbers multiplexing and corresponding affine transformation to eliminate the vulnerabilities to power analysis attacks in the implementation of AES. The experimental results show that the scheme is efficient and security against the DPA attacks, and the masking algorithm have already been implemented on the smartcard.

Keywords: *DPA, AES, masking, security, random numbers multiplexing, smartcard.*

1. Introduction

Currently, side-channel analysis has become a hotspot of cryptographic analyses. Different from conventional cryptographic security analyses, side-channel analyses monitors the changes in the electronic features of the IC, and exploit the information leakage with side channel characteristics (E.g. Power and EM). With modern statistics, now engineers and attackers are able to reveal sensitive data with side channel analyses. Side-channel analysis, especially the power analysis attacks, on software or hardware implementations of various crypto-systems aim at recovering the secret key information from power consumption performed on the smart card [5, 6]. Power Mask has caught wide attention since its implementation has not imposed much change in both cost and IC operation. Document [2] is the first broadcast that describes the DPA countermeasure using power masking. This method makes DPA very difficult by introducing Masking for the middle results of algorithm operation. With the power masking, correlation becomes very difficult. Document [7, 8] describes the method which uses asynchronous circuit and executive pipeline to strengthen the S-box capability. Nevertheless, the above methods mostly focus on S-box, while ignore all other calculation steps.

In this paper we present a practical implementation of 128-AES in the smartcard combined with improved idea masking method based on [1] which make each intermediate result being masked. This method has advantage of easy hardware implementation, less IC resources consumption, and most importantly, it removes the DPA spike corresponding to the round key and breaks the correlation between power consumption and hamming weight distance. This method is very effective to be used in smartcards or other security products.

The paper is organized as follows. Section 2 introduces the principle of an improved AES Masking Method, which included the process of encryption and decryption of AES, and the implementation on AES Masking Method for resisting DPA attacks. The security analysis of DPA attacks and experimental results are given in section 3, followed by the conclusion.

2. Masking Method

2.1 The process of AES encryption and decryption

AES [3](Advanced Encryption Standard) is a symmetric cryptographic algorithm released in 2001 by National Institute of Standards and Technology (NIST), the purpose is to replace DES, now it is extensively used. Its operation process is mainly composed of four parts, including one confusion and three substitutions:

(1) SubBytes: Transformation in the Cipher that process the State using a non-linear byte substitution table (S-box) that operates on each of the State bytes independently.

(2) ShiftRows: Transformation in the Cipher that process the State by cyclically shifting the last three rows of t-he State by different offsets.
(3) MixColumns: Transformation in the Cipher that takes all of the columns of the State and mixes their data (in dependently of one another) to produce new columns.
(4) AddRoundKey: Transformation in the Cipher and Inv-erse Cipher in which a Round Key is added to the St-ate using an XOR operation.

About the process of 128-AES en-decryption, start from AddRoundKey, and then implement nine round iterative, which contain the above four parts, finally implement the last round contains only the above three parts.

2.2 DPA resistant implementation of AES

The power masking method discussed in this paper, the masking mainly to 128-AES encryption (or decryption) process and its key extension operation is the same as conventional AES. The figure 1 shows its specific flow. The idea is following:

① Selection Random Number r

Mask technology use attacker who impossible access to random number r to masking the intermediate variable m, get masking the intermediate variable $m'(m'=m'\oplus r)$, the attacker who each time gets power consumption information is different, and therefore the attacker who unable to real gets the relationship between power consumption and key information by the intermediate variable m[4,5].

This paper select one byte random number r_0 , and duplicate fifteen times to become the 128 bits random number r , r[16]={ r_0, r_0, r_0, r_0, r_0, r_0, r_0, r_0, r_0, r_0, r_0, r_0, r_0, r_0, r_0, r_0}.

② Affine transformation f

Only the random number r_0 is affine transformation, and set r_0 [8] = {r_{00}, r_{01}, r_{02}, r_{03}, r_{04}, r_{05}, r_{06}, r_{07}}. With the affine transformation, we can obtain the following result where r_1 is the 8-bit value which r_1 [8] = {r_{10}, r_{11}, r_{12}, r_{13}, r_{14}, r_{15}, r_{16}, r_{17}}. Then make r_1 multiplex 15 times by the affine transformation f that results from the random number ra .

③ SubByte transformation

Use the S-box mask method for SubByte [1], the first part of an AES round is the SubByte transformation which is the only non-linear part of the AES. It is an S-box which is contains two transformations for a multiplicative inversion in GF (2^8) and an affine transformation f . The add operation is the bitwise XOR, the multiplication in GF (2^8) using the irreducible polynomial m(x) = x8+x4+x3+x+1 as modulus. In order to optimize efficiency of multiplication and inverse operation, we use a multiplicative inversion and square in finite field GF (2^4) instead of GF (2^8), and the square of the finite field operation treatment alone [9]. The mask transformation is obtained as follows (fig.2). Where:

M is plain value without mask, during all stages of the transformation, intermediary values are independent of M$\oplus$ r :

(a) we multiply with a non-zero 8-bit random r ,

(b) and we XOR with $r \otimes r$.

After the inversion in GF (28) we have a multiplicative mask and to reestablish the Boolean mask we use values independent of M$\otimes$ r :

(a) we XOR with 1,

(b) and we multiply with r .

Where the affine transformation f_1 as follows:

$$\begin{pmatrix} x1_0 \\ x1_1 \\ x1_2 \\ x1_3 \\ x1_4 \\ x1_5 \\ x1_6 \\ x1_7 \end{pmatrix} = \begin{pmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

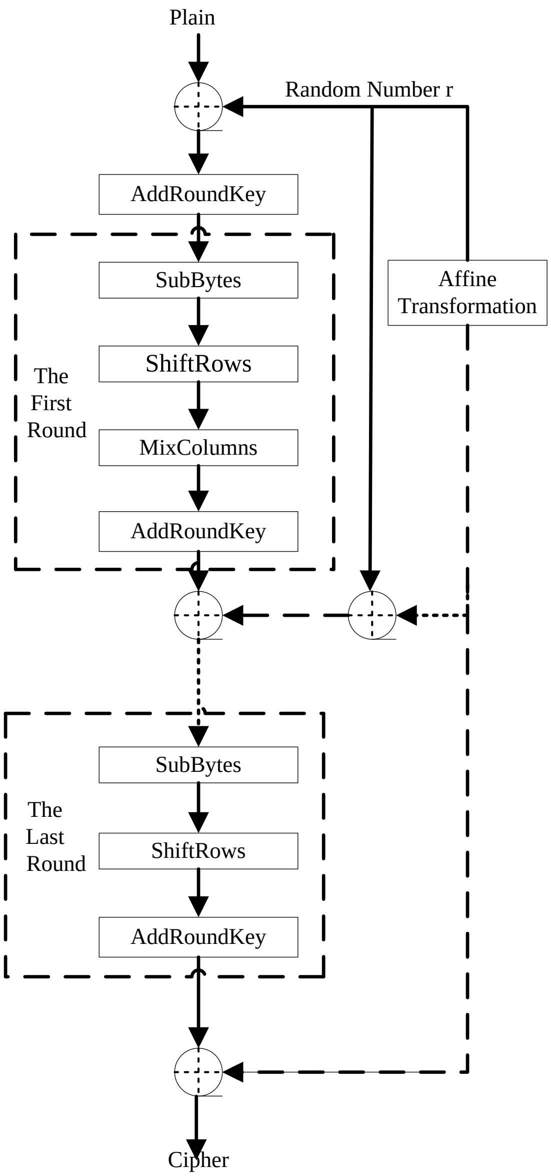

Fig.1: The process of masking of AES encryption

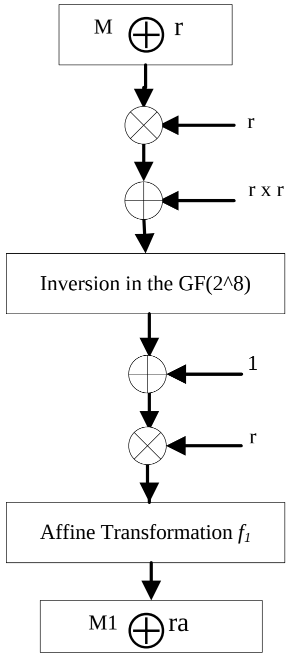

Fig.2: The SubByte transformation with masking countermeasure

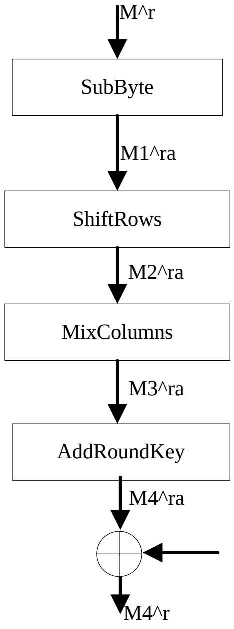

Fig.3: The round i of the AES with masking countermeasure

Now, let us see the process of a round of the AES with masking countermeasure (fig.3).Where:

- r represents the mask applied;
- every byte of ra are equal which results from r_1 multiplex 15 times by affine transformation f of SubByte, where $r_1 = f(r)$;
- M2^ ra =ShiftRows(M1^ ra), it is linear operation

which can ShiftRows(M1) and ShiftRows(ra) respectively and each byte of ra is equal;

- M3^ ra =MixColumns(M2^ ra), it is also linear operation and similar with ShiftRows;
- M4^ ra =AddRoundKey (M3^ ra), ra ^ r represents the random masking.

With this, it is possible to compute an AES and to keep the same random mask at each round. So, the AES mask algorithm can accurately realize.

3. Against DPA security analysis

We will simply consider the following fact: an ordinary DPA analysis for AES is based on related analysis of S-box and AddRoundKey when determining to set intermediate value related operations specific happen the position. Based on this fact, from the beginning of the AES which is input message to the end of it which is output cipher text none of the “real” intermediate values appear by this our masking scheme.

The masking method has been applied to the smart card, which adopts HHNEC EF130 SCS8LP Low Power technology and comprehensive clock constraint is 50MHz (ClkAes). We have used the Rescure’s Inspector 4.2 side channel analysis platform to analyze the FPGA implementation, chose the Altera StratixII Series of FPGA as an implementation tool, internal voltage set at 1.2V, adopt 90nm technology. The mask algorithm implemented area of FPGA is about 8080 gates, compared with traditional method [10], the performance of the mask algorithm implementation slightly lower to the traditional method.

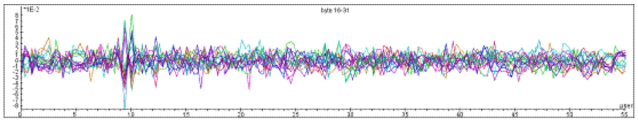

Fig.4: The differential power consumption for AES without masking countermeasure.

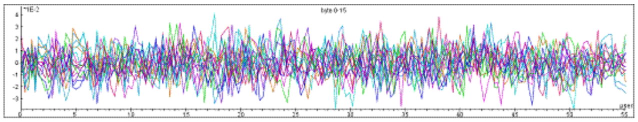

Fig.5: The differential power consumption for AES with masking countermeasure.

The above shows the testing results of AES, perform AES encryption for 100K times of AES random clear texts, the curve for alignment and sampling process and select the first round result correlation analysis, utilizes DPA to extract hidden information from a large sample of power traces obtained during cryptographic computations for AES without masking countermeasure (Fig.4), DPA spike is clear show, namely the attack is successful. On the other hand, with this design, the DPA spike is invisible and successful hidden.

4. Conclusions

We have described mask design method for a practical implementation of 128-AES (as well as apply to 196-AES and 256-AES), which contain multiplex 15 times random number r and the affine transformation f. As is seen from the experimental result of our implementations, these countermeasures against DPA can be implemented in a smart-card environment where obtains good technical effect: 1) hardware implementation is in low complexity and low other extra cost; 2) Simple software implementation. It has the advantage of comprehensive in comparison with other typical countermeasures.

Acknowledgments

This work was supported by Technology Research and Creative Design Sub-item Capital of Shenzhen Nanshan (No.KC2012JSYB0035A), and the State Development and Reform Commission of China (No. [2010]3044).

References

[1] Akkar M, Giraud C. An implementation of DES and AES Secure against Some Attacks [G] // LNCS2162: CHES 2001. Berlin: Spring, 2001:309–318.

[2] Chari S, Jutla C, Rao J R, Rohatgi P. A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards[C]//Proc.of the 2nd AES CandidateConference, Rome, Italy, 1999: 133-147.

[3] National Institute of Standards and Technology. FIPS 197 Advanced Encryption Standard [S]. 2001-11.

[4] Itoh K, Takenaka M, Torii N. DPA countermeasure based on the masking method[C]//LNCS 2288: Proceedings of the 4th International Conference Seoul on Information Security and Cryptology, 2002:440-456.

[5] Zhang Yiwei, Gong Bingbing, Liu Lie-en, Tang You. AES Dual-path Masking implementation Method for Resisting Side-channel Analysis[J].Computer Engineering, 2012,38(13):108-111.

[6] Jiang Huiping, Mao Zhigang. Advanced DESalgorithm anaginst differential power analysis and its hardware implementation [J]. Chinese Journal of Computers, 2004, 27(3):334-338.

[7] Han Jun, Zeng Xiaoyang, Zhao Jia. VLSI implementation of AES algorithm against differential power attack and differential fault attack [J]. Journal on Communications, 2010, 31(1):20-29.

[8] Arrag S, Hamdoun A, Tragha A, Khamlich S. Several AES Variants under VHDL Language in FPGA [J]. International Journal of Computer Science Issues, 2012, v9, n55-3, p135-141.

[9] Wolkerstorfer J, Oswald E, and Lamberger M. An ASIC implementation of the AES SBoxes. in Proc. Cryptography Trck at RSA Conf.2002, pp.67-78.

[10] Mohan H.S, Raji Reddy A. Performance analysis of AES and MARS encryption algorithms [J]. International Journal of Computer Science Issues, 2011,v8, n44-1, p 363-368.

Xiaoan Zhou, born in 1968, Ph.D., associate professor, master supervisor. He is working as a vice dean in the Information and engineering institution at ShenZhen University. He is IEEE communication association member and Shenzhen science and technology committee evaluation expert. His research interests include communication information processing and information security. He has published and presented in journal, international and national level conferences.

Juan Peng, born in 1988, master candidate. Her research interest is information security.

Liping Guo, born in 1987, master candidate. His research interest is Cryptography.