Hardware Implementation of Compact Reconfigurable AES/SM4 Encryption Circuit Against Differential Power Attact

Yaoping Liu [1], Huichao Zhao[1]

1156332965@qq.com

[1]High-tech institute, Fan Gong-ting South Street on the 12th, Qingzhou, Shandong, China

Abstract: In order to resist differential power attacks (DPA) effectively, a compact implementation of the whole masked reconfigurable AES/SM4 encryption circuit is proposed. Firstly, the general design of whole masked reconfigurable AES/SM4 encryption circuit is introduced. Secondly, the detailed design of masked reconfigurable S-box, masked mixcolumns and masked linear transformation is emphasized. Thirdly, the safety of the circuit is analyzed theoretically and verified by the attack experiment of the DPA platform. Finally, in the SMIC 0.18μm library, compared with the synthesized results of the whole masked AES and SM4 encryption circuits, the area and power consumption of the whole masked reconfigurable AES/SM4 encryption circuit are reduced by 11.67% and 24.48%, respectively.

Keywords: AES, SM4, Masking, Differential Power Attact

1 INTRODUCTION

AES was released by the US National Bureau of Standards in 2001. It is the latest international standard of block cryptographic algorithm and widely used in information security fields[5]. SM4 is a self-developed block cipher algorithm, published by the National Cryptography Administration in 2006 and approved as an industry standard in 2012, mainly used to protect the security of WLAN products[10]. As the only nonlinear arithmetic unit in AES and SM4 cryptography algorithms, S-box is mainly used in SubBytes and key expansion modules, which is the core to realize AES and SM4 cryptography algorithms.

The implementations of S-box mainly include Look-up Table (LUT) and Composite Field Arithmetic (CFA). LUT method is simple to implement, but the area cost is very large and the application flexibility is low. CFA computes a higher-order finite field as a composition of two or more lower-order finite fields, which is widely used in cryptography. The AES S-box is defined as the MI over GF(2^8) and affine transformation. The SM4 S-box mainly includes pre-affine operation, MI over GF(2^8) and post-affine operation. It can be see that both AES S-box and SM4 S-box involve the MI over GF(2^8). Wolkerstorfe proposed to convert the multiplicative inverse (MI) over GF(2^8) to the operations over GF(2^4) to realize S-box[11]. In the paper [4], the MI over GF(2^8) was decomposed into the composite field GF(($(2^2)^2$)^2), and the S-box with small area was implemented. Among these implementations proposed in previous papers, the S-box based on CFA occupies the smallest area[3]. In order to reduce

ICIDC 2023, June 02-04, Nanchang, People's Republic of China
Copyright © 2023 EAI
DOI 10.4108/eai.2-6-2023.2334594

hardware complexity, based on CFA, a reconfigurable AES/SM4 encryption circuit architecture with small area and low power consumption is proposed in the paper [8].

However, in the process of cryptographic chip design, in addition to considering the circuit performance such as area and power consumption, so as to ensure information security, the research on the security of the cryptographic chip has become an important branch of the field of cryptographic algorithm, which has been widely concerned at home and abroad. Power attack uses the power dissipation generated during the encryption/decryption process of the cipher chip and the correlation between the key and the intermediate data to crack the key. Currently, there are Simple Power Attack (SPA) and Differential power attack(DPA) and High-Order Differential Power Attack (HO-DPA) [6]. Among them, DPA is the main attack method because of its simple implementation, low cost and small key search space.

The intermediate data is randomized using the random masking technique in the encryption process, so the attacker is difficult to collect the effective power curve, and unable to obtain correlation between the key and power curve. In these papers [7,12], based on CFA, masked AES and SM4 S-box is designed, which can resist DPA effectively. The random masking method proposed in the paper [9] is used to mask the input and output of all modules in AES encryption circuit to achieve the effect of resisting DPA.

For ensuring the security of the encryption algorithm, the whole masked technology is the most commonly used method. The application of whole masked technology can resist DPA effectively, but the mask is added to each operation of the encryption, so the hardware complexity of the circuit is increased significantly. How to reduce the circuit area under the condition of ensuring the safety of the circuit is the key research content. Therefore, a design of reconfigurable AES/SM4 encryption circuit with small area and low power consumption is proposed to resist DPA.

2 The implementation of whole masked reconfigurable AES/SM4 encryption circuit

The whole masked reconfigurable AES/SM4 encryption circuit proposed in this paper is mask-protected at every step to make sure the security of the entire encryption process.

2.1 The design of whole masked reconfigurable AES/SM4 encryption circuit

The structure of whole masked reconfigurable AES/SM4 encryption circuit is shown in Figure 1. As shown in Figure 1, the circuit mainly includes masked AddRoundKey (ARK), masked reconfigurable SubBytes, masked ShiftRows (SR), masked MixColumns (MC), masked Linear Transform (LT), masked Reverse, whole masked key expansion and mask correction. Among them, as the only nonlinear operation module of the whole encryption circuit, the masked reconfigurable SubBytes is the key to realize the circuit, and the masked reconfigurable S-box based on CFA is the core of the design of masked reconfigurable SubBytes.

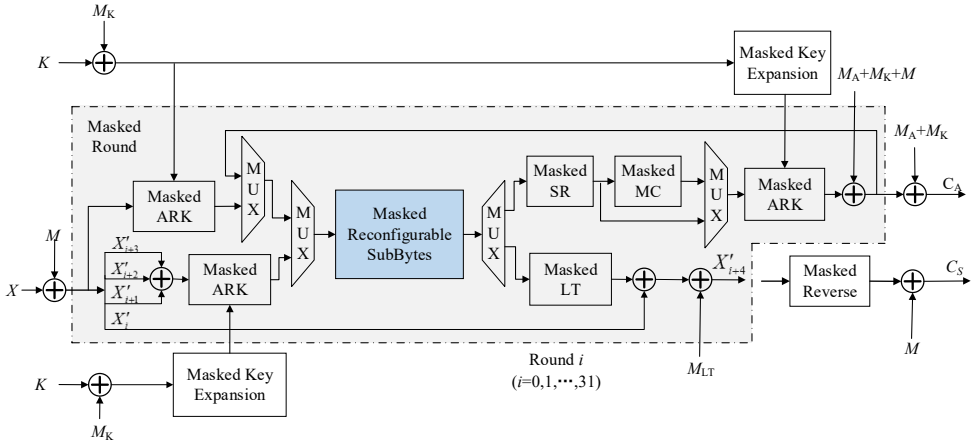

Fig. 1. The new architecture of S-Box using the CFA technique

The AES encryption process is as follows: firstly, the plaintext and the initial key are performed ARK operation. The output is used as the input of the first round transformation. Then the operations of SubBytes, SR and MC are executed successively. The result is performed ARK operation with the output of key expansion, and the output is used as the input of the second round transformation..... And execute them in sequence. The only difference is that the tenth round transformation does not include the MC operation, and directly adds the output of the SR to the round key to get the ciphertext of this encryption.

The SM4 encryption process is as follows: 128 bits plaintext X is divided into four 32 bits data (X_0, X_1, X_2, X_3) as the input of the first round transformation. The data after XOR operation of X_1, X_2 and X_3 are combined with the output of key expansion for ARK, SubBytes and LT operations. The output results are XOR with X_0 to obtain X_4. Then, the combination of X_1, X_2, X_3 and X_4 is 128 bits as the input of the second round transformation. And so on until the thirty-second round is over. The output of the last four round transformation is transformed in reverse order, and the output is ciphertext.

2.2 The optimization of whole masked reconfigurable AES/SM4 encryption circuit

2.2.1 The implementation of masked reconfigurable S-Box

The masked reconfigurable S-box is composed of masked MI over GF(2^8) and masked matrix multiplication, which is shown in Figure 2. The input of masked reconfigurable S-box is X+m, and its mask is m. The output masks after AES S-box and SM4 S-box are m_a and m_s respectively, and their expressions are shown in (1).

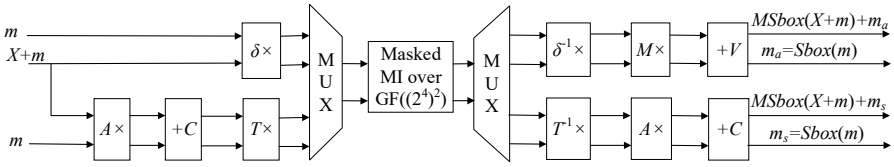

Fig. 2. The architecture of masked reconfigurable S-Box using the CFA technique

$$\begin{cases} m_a = M\left(\delta^{-1}\left(\delta m\right)^{-1}\right) + V = Sbox(m) \\ m_s = A\left(T^{-1}\left(T\left(Am + C\right)\right)^{-1}\right) + C = Sbox(m) \end{cases} \tag{1}$$

In order to reduce hardware complexity, the MI over GF(2^8) is decomposed into composite field GF((2^4)^2) adopting the irreducible polynomials as shown in (2) based on the CFA technology.

$$\begin{cases} GF\left(\left(2^4\right)^2\right): f_1\left(y\right) = y^2 + y + \upsilon \\ GF\left(2^4\right): f_2\left(x\right) = x^4 + x^3 + x^2 + x + 1 \end{cases} \tag{2}$$

Where υ=$\{0010\}_2$. In order to ensure the mask protection in the reconfigurable S-box operation, the masked MI over GF((2^4)^2) is directly implemented by the optimized masked operation over GF(2^4). The masked MI over GF((2^4)^2) includes two masked additions over GF(2^4), a masked square over GF(2^4), a masked constant multiplication over GF(2^4), three masked multiplications over GF(2^4) and a masked MI over GF(2^4). The masked addition over GF(2^4) needs 8 XOR gates. The masked constant multiplication and masked square over GF(2^4) can be combined into a single block and the masked block $()^2\times$v over GF(2^4) does not consume hardware resources.

The masked multiplication and MI over GF(2^4) can be expressed as (3) and (4) separately. In this paper, the DACSE algorithm[13] was used to optimize the masked multiplication over GF(2^4) and the optimization requires 47 XOR gates and 32 AND gates with a reduction of 59.22% in the number of equivalent gates compared to the direct implementation, which requires 117 XOR gates and 75 AND gates.

$$\begin{aligned} c = ab &= \left(a' + m_a\right)\left(b' + m_b\right) \\ &= a'b' + a'm_b + m_a b' + m_a m_b \end{aligned} \tag{3}$$

$$\begin{aligned} f &= \left(a'^2 + m_a{}^2\right)\left(a'^2 + m_a{}^2\right)^2\left(\left(a'^2 + m_a{}^2\right)^2\right)^2 \\ &= \left(a'^2 + m_a{}^2\right)\left(a'^4 + m_a{}^4\right)\left(a'^8 + m_a{}^8\right) \\ &= a'^{14} + a'^{12}m_a{}^2 + a'^{10}m_a{}^4 + a'^8 m_a{}^6 \\ &\quad + a'^6 m_a{}^8 + a'^4 m_a{}^{10} + a'^2 m_a{}^{12} + m_a{}^{14} \end{aligned} \tag{4}$$

The masked MI over GF(2^4) optimized by GA[1] and DACSE[13] algorithm requires 157.5 equivalent gates. Compared with the direct implementation that requires 105 XOR gates and 81 AND gates, the optimized circuit gives 279(63.92%) gates reduction in total area occupancy.

Based on the optimization of masked operations over GF(2^4), the masked MI over GF((2^4)^2) needs 772.5 equivalent gates, whose area is reduced by 62.79% compared to the direct implementation, which requires 514 XOR gates and 356 AND gates,

Except the masked MI based on CFA, matrix multiplications are also masked in the design of the masked reconfigurable S-box. Taking AES masked mapping matrix as an example, the

masked mapping matrix operation is actually mapping the masked input and the input mask respectively, which consumes twice the hardware resources of the mapping matrix circuit. Similarly, the area cost of masked affine-inverse mapping operation and masked affine operation is twice that of the corresponding operation without mask. Therefore, the masked matrix operations optimized in this paper require 156 XOR gates.

The number of equivalent gates required by the masked reconfigurable S-box is listed in Table 1. As shown in Table 1, the direct implementation of the masked reconfigurable S-box requires 768 XOR gates and 356 AND gates, which is equal to 2838 gates. The masked reconfigurable S-box optimized by GA-DACSE algorithm needs 1240.5 gates, which gives 1597.5(56.29%) gates reduction in total area cost.

Table 1. The area cost required by the masked reconfigurable S-Box.

Modules	Direct			Optimized						
	XOR	AND	Gates	NAND	NOR	AND	OR	XOR	XNOR	Gates (Reduction)
Masked MI Over GF($(2^4)^2$)	514	356	2076	7	2	119	4	191	2	772.5（62.79%）
Maked matix	254	—	762	—	—	—	—	156	—	468(38.58%)
Masked Reconfigurable S-Box	768	356	2838	7	2	119	4	347	2	1240.5 (56.29%)

2.2.2 The design of Masked MC and Masked LT

In the masked MC operation, the equal random mask corresponding to each byte is defined as m. The key operation in the MC is the double multiplication over GF(2^8), which is denoted as xTime2. By adding mask to it, the form shown in (5) can be obtained.

$$\begin{aligned} Mask\_xTime2:\ a' &= 2(a+m) = 2a+2m \\ &= xTime2(a)+xTime2(m) \end{aligned} \tag{5}$$

Both the masked LT and its mask operation can be realized by (6). Assuming the input random mask is m, the output mask can be derived as shown in (7).

$$\begin{aligned} L = LT(B) = B &+ (B <<< 2) + (B <<< 10) \\ &+ (B <<< 18) + (B <<< 24) \end{aligned} \tag{6}$$

$$\begin{aligned} m' = LT(m) = m &+ (m <<< 2) + (m <<< 10) \\ &+ (m <<< 18) + (m <<< 24) \end{aligned} \tag{7}$$

Where <<<i indicates that the 32-bit data loop moves i bits to the left.

The masking method of the whole masked key expansion is the same as that of the whole masked round transformation, that is, the corresponding masking process is carried out on the key, which will not be explained in detail.

2.3 The theoretical analysis of circuit safety

The security of random masking technology is that the median value of the mask is independent of the original median and mask. There is no dependence between the power of

the masked median and the original median, so that the circuit has the ability to resist DPA. Based on the lemma of proof of intermediate value security proposed in these papers [2,4], the security of whole masked reconfigurable AES/SM4 encryption circuit is analyzed theoretically.

Lemma 1: If u$\in F_{2^8}$, v is independent of u and in {0, 1, 2... , 2^{8-1}} follows uniform distribution, then Z=u+v also follows uniform distribution (Blomer 2004, Canright 2008).

In this paper, two 8bits random evenly distributed masks M and M_K are selected to mask the reconfigurable encryption circuit, and M and M_K are independent of plaintext and key. Take the security of masked intermediate value in AES encryption as an example to analyze. At the beginning of AES encryption, mask M and M_K are added to plaintext and key respectively. According to Lemma 1, plaintext and key with mask follows uniform distribution, and output still follows uniform distribution after initial ARK. The reconfigurable SubBytes is implemented based on reconfigurable S-boxs, so its output follows uniform distribution. The masked SR only shifts each row of data accordingly and does not change the distribution law of data, so its output follows uniform distribution. The masked MC is constant matrix multiplication, and the input follows uniform distribution, so based on matrix theory knowledge, its output also follows uniform distribution. According to Lemma 1, the output of masked key expansion follows uniform distribution. The masked variables in the masked correction are uniformly distributed, according to Lemma 1, we can see that the input data of the next round is uniformly distributed. The above analysis shows that the whole masked reconfigurable AES/SM4 encryption circuit can ensure its theoretical security in the AES encryption process. In the same way, the whole masked reconfigurable AES/SM4 encryption circuit can ensure its theoretical security during the SM4 encryption process.

3 COMPARISONS AND RESULTS

In the SMIC 0.18μm 1.8V cell library, the designs of the whole masked AES encryption circuit, the whole masked SM4 encryption circuit and the whole masked reconfigurable AES/SM4 encryption circuit are synthesized. The results are listed in Table 2.

Table 2: The synthesized results of the implementations.

Implementations	Area (μm^2)	Power (mW)
Whole Masked AES encryption circuit	179764.48	7.1848
Whole Masked SM4 encryption circuit	162421.67	5.6385
Whole Masked Reconfigurable AES/SM4 encryption circuit	302262.69	9.6836

Compared to the independent implementations of the whole masked AES and SM4 encryption circuit, whose total area and power are severally 342186.15μm^2 and 12.8233mW, the area and power of the whole masked reconfigurable AES/SM4 encryption are respectively reduced by 11.67% and 24.48%, which are 302262.69μm^2 and 9.6836mW.

In addition, the DPA experiment is carried out. In the whole masked AES encryption circuit, the output of the first round of S-box is selected as the attack position. Taking the high 8 bits in the 128-bit data as an example, the real key is 8'h2b. The guess key corresponding to the maximum peak value of the attack position is 8'h80 when 100,000 power curves are collected, which is different from the correct key. So 100,000 power curves cannot successfully attack the key value. In the process of whole masked SM4 encryption, the output of the S-box of round transformation is selected as the attack position. Taking the high 8 bits in the 32-bit key data of the first round as an example, the real key is 8'hf1. When 100,000 power curves are collected, the guess key corresponding to the maximum peak value of the attack position is 8'h9c. It is different from the correct key. It can be seen that the whole masked reconfigurable AES/SM4 encryption circuit designed in this paper can resist DPA effectively.

4 CONCLUSIONS

This paper focuses on the design of masked reconfigurable S-box, masked MC, masked linear transformation and whole masked reconfigurable key expansion using random masking technology, and implements a whole masked reconfigurable AES/SM4 encryption circuit with small area and low power consumption. In 180nm 1.8V COMS technology, compared with the independent designs of whole masked AES and SM4 encryption circuits, the area and power consumption of the proposed whole masked reconfigurable AES/SM4 encryption circuit are reduced by 11.67% and 24.48% severally. So the proposed circuit is suitable for applications with limited resources. In addition, the security of the circuit is analyzed theoretically, and is verified by DPA attack experiment. With the development of information technology, especially the development of artificial intelligence technology, HO-DPA make encryption algorithms easier to crack. Therefore, based on the proposed whole masked reconfigurable AES/SM4 encryption circuit, how to resist HO-DPA is the focus of future research.

REFERENCES

[1] Bao, Z. G. & T. Watanabe (2009) . A Novel Genetic Algorithm with Cell Crossover for Circuit Design Optimization. Circuits and Systems, 2009. ISCAS 2009. IEEE International Symposium on, Taipei, Taiwan, May 24-27, 2009, pp.2982- 2985, 2009.

[2] Blomer, J. , Guajardo, J. & V. Krummel (2004). Provably Secure Masking of AES. In LNCS, editor, Proceedings of SAC'04, volume 3357, pages 69–83. Springer, August 2004. Waterloo, Canada.

[3] Canright D (2005). A very compact S-box for AES. 2005 Cryptographic Hardware and Embedded Systems (CHES 2005), Springer Berlin Heidelberg, pp. 441-455, 2005.

[4] Canright, D. & Batina, L (2008). A Very Compact "Perfectly Masked" S-Box for AES. 2008 Workshop on Cryptographic Hardware and Embedded Systems (CHES 2008), Volume of LNCS 5037, 2008. 446-459.

[5] Fu, L. , Shen, X. , Zhu, L. & Wang, J (2014). A Low-Cost UHF RFID Tag Chip with AES Cryptography Engine. Security and Communication Networks, 7(2), 365-375.

[6] Kocher, P. C. , Jaffe, J. & Jun, B (1999). Differential power analysis. In CRYPTO'99, LNCS 1666, pp:388-397. Santa Barbara, CA, USA, Aug. 1999.

[7] Liang, H. , Wu, L. , Zhang, X. & Wang, J (2014). Design of a Masked S-box for SM4 Based on Composite Field. 2014 Tenth International Conference on Computational Intelligence and Security, 2014: 387-391.
[8] Liu, Y. P., Wu, N. , Zhang, X.Q. & Zhou, F (2017). A new compact hardware architecture of S-Box for block ciphers AES and SM4. IEICE Electronics Express, 2017, 14(11):20170358-20170358.
[9] Mangard S, Oswald E. & Popp T (2007). Power Analysis Attacks: Revealing the Secrets of Smart Cards. Graz University of Technology, Austria, Springer, 2007: 1-306.
[10] Wang, C. G. , Qiao, S. S. & Yong, H (2013). Low Complexity Implementation of Block Cipher SM4 Algorithm. Computer Engineering, 39(7), 177-180.
[11] Wolkerstorfer, J. , Oswald, E. & Lamberger, M (2002). An ASIC implementation of the AES SBoxes. Topics in Cryptology—CT-RSA 2002. Springer Berlin Heidelberg, 2002: 67-78.
[12] Zakeri, B. , Salmasizadeh, M. , Moradi, A. , Tabandeh, M. & Shalmani, M (2007). Compact and Secure Design of Masked AES S-Box. 2007 9th International Conference on Information and Communications Security, ICICS 2007, Springer, LNCS 4861, pp. 216-229.
[13] Zhang X, Wu N, Zhou F & et al (2014). An optimized delay-aware common subexpression elimination algorithm for hardware implementation of binary-field linear transform. IEICE Electronics Express, 11(22), pp. 1-8.