ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

A Countermeasure Circuit for Secure AES Engine against Differential Power Analysis

V.S.Subarsana[1], C.K.Gobu[2]

PG Scholar, Member IEEE, SNS College of Engineering, Coimbatore, India[1]

Assistant Professor Department of EEE, SNS College of Engineering, Coimbatore, India[2]

ABSTRACT— In cryptography, the Advanced Encryption Standard (AES) is one of the most popular algorithms used in symmetric key cryptography. It is available in many different encryption packages. AES is a 128 bit Symmetric block cipher which is based on a design principle known as a Substitution permutation network. Power analysis is a form of side channel attack in which the attacker studies the power consumption of a cryptographic hardware device (such as a smart card, tamper-resistant "black box", or integrated circuit). The attack can non-invasively extract cryptographic keys and other secret information from the device. Differential power analysis (DPA) is a side-channel attack which involves statistically analyzing power consumption from a cryptosystem. Several methods have been proposed in literatures to resist the DPA attack in cryptographic device, but they largely increase the hardware cost and severely degrade the throughput. In existing system, the security problem is resolved by a new architecture with self-generated true random sequence. DPA countermeasure circuit can effectively reduce the area overhead and throughput degradation.

KEYWORDS—Advanced Encryption Standard (AES), cryptography, differential power analysis (DPA), ring oscillators, true random number generator.

I. INTRODUCTION

The differential power analysis (DPA) attack proposed by Kocher et al. in 1999 [9] has become a serious issue when designing cryptographic circuits. The DPA attack can efficiently disclose the secret key by the power consumption information leaked from cryptographic devices. It has been proven that the secret key of an Advanced Encryption Standard (AES) chip can be disclosed. Accordingly, the DPA resistance has become the most important consideration for hardware-based cryptographic devices.

Several methods have been proposed to counteract the DPA attack, either in the algorithm or in the circuit level. Some of them use a data masking method to randomize the data processed in cryptographic circuits [4]. The data being processed is changed by an internally generated random mask before the en-/decryption process. As a result, a corresponding mask should be used to recover the actual output data at the end of the process. In this way, the power consumption of cryptographic circuits will be independent of the predicted power consumption. Some proposals balance the power consumption of different operations by using new logic cells or wave dynamical differential logic (WDDL) [8]. Standard cells are replaced by this new logic family and then the power consumption of different patterns would be almost the same. Some proposals isolate the power supply and cryptographic circuits by switching capacitors [3]. However, the increased security level results in extra hardware cost and throughput degradation.

Ring-oscillator-based DPA countermeasure circuits [6] can effectively reduce the area overhead and throughput degradation. Details of the ring oscillator based DPA countermeasure circuit such as inversion stages and number of oscillators have been discussed in [7]. However, random bytes from the pseudo random number generator would be the same after the system is reset. Therefore, the additional power consumption added by the DPA countermeasure circuit in each cycle would be the same if the attacker resets the system before recording power traces.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

To solve the reset problem, a different architecture that incorporates a true random number generator is proposed not only to counteract the DPA attack but also to self generated a true random sequence. With the proposed architecture, the security level of AES engines can be further enhanced while the area overhead can be also reduced. The AES - based cryptographic engine is explained in section II. The DPA attack flow is briefly introduced in Section III. The architecture and the analysis of the proposed DPA countermeasure circuit are given in Section IV. Section V shows the implementation result. At last, the conclusion is given in Section VI.

II. AES-BASED CRYPTOGRAPHIC ENGINE

In cryptography, the Advanced Encryption Standard (AES) is an encryption standard that comprises three block ciphers, AES-128, AES-192 and AES-256, adopted for different applications. AES is one of the most popular algorithms used in symmetric key cryptography. It is available in many different encryption packages. AES is based on a design principle known as a Substitution permutation network. It is fast in both software and hardware, is relatively easy to implement, and requires little memory. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits, whereas Rijndael can be specified with block and key sizes in any multiple of 32 bits, with a minimum of 128 bits and a maximum of 256 bits. Assuming one byte equals 8 bits, the fixed block size of 128 bits is 16 bytes. AES operates on a 4×4 array of bytes, termed the state (versions of Rijndael with a larger block size have additional columns in the state). Most AES calculations are done in a special field. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain-text into the final output of cipher-text. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform cipher-text back into the original plain-text using the same encryption key.

III. DPA ATTACK

The DPA attack utilizes the statistical analysis to calculate the correlation between the leaked power information and the predicted power consumption. Irrelative noises can be eliminated by statistical analysis and therefore, the DPA attack can still be successfully conducted even in a noisy environment. The secret key of a cryptographic circuit can be disclosed from the correlation index of the analysis result. The attacker prepares N different patterns for en-/decryption and records the power trace of these patterns. At the same time, these N patterns are also applied to a power prediction model to obtain predicted power values. The power prediction model is a method to determine possible power consumption, either in the behavior or in the algorithm level. For the AES algorithm, the 128-bit secret key can be divided into 16 8-bit subkeys, and the attacker can disclose each 8-bit subkey at one time. As a result, the array would consist of $2^8 = 256$ columns for all key hypotheses.

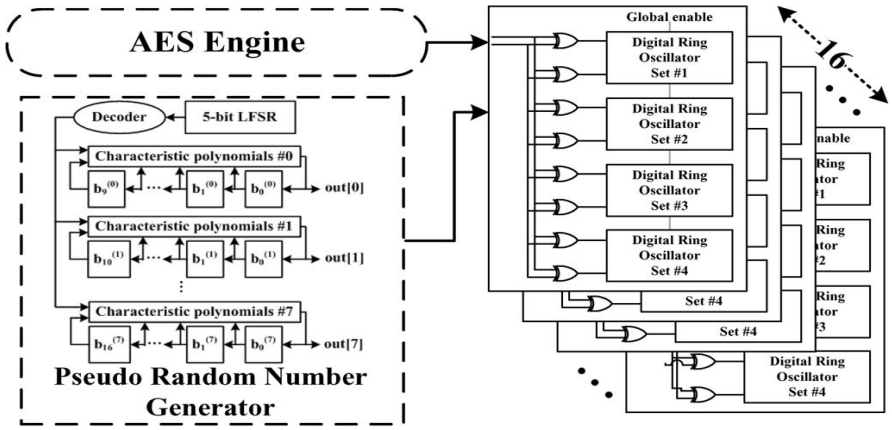

Fig. 1: Architecture of the pseudo random-based DPA countermeasure circuit.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IV. DPA COUNTERMEASURE CIRCUIT

To resist the DPA attack, both the pseudo and the true random-based DPA countermeasure circuits are presented in this section. The pseudo random-based architecture is introduced first and then the improved architecture with self-generated random sequence is presented. The effective countermeasure circuit is designed using Linear Feedback Shift Register.

A. Pseudo Random-Based DPA Countermeasure Circuit

The main purpose of the DPA countermeasure circuit is to break the dependency between the measured power traces and the predicted power values. As shown in Fig. 1, the proposed DPA countermeasure circuit consists of 16 identical subcircuits. Each subcircuit, which is composed of 12 digitally controlled ring oscillators, is controlled to randomly enable different number of ring oscillators. A global enable signal is also applied to turn off the subcircuit to reduce power consumption. As shown in Fig. 1, the random number generator is designed based on linear feedback shift registers (LFSRs) with dynamic feedback configuration to make the random sequence more unpredictable. Each subcircuit is controlled by a data byte of the AES data block and the random byte from the pseudo random number generator.

To demonstrate the effect of the DPA countermeasure circuit, power traces recorded by SPICE simulation are illustrated in Fig. 1 This figure shows power traces of an unprotected AES circuit with the same input pattern but two different secret keys. The same input data is repeatedly encrypted for 100 times, and power traces are recorded for further analysis. The two secret keys are randomly generated and used as a running example for this brief. Note that any two random secret keys would also lead to similar results.

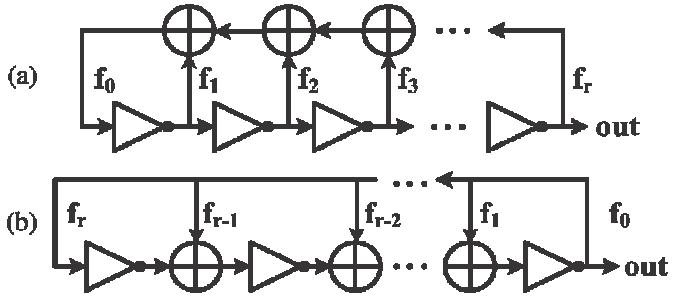

Fig. 2: (a) FiRO. (b) GaRO.

B. True Random-Based DPA Countermeasure Circuit

To solve the security weakness in the pseudo random-based architecture, a true random sequence for the DPA countermeasure circuit is required. However, most true random number generators are analog circuits with much higher power consumption. Goli proposed a digital method to generate random data by using ring oscillators in Fibonacci and Galois configurations. The proposed DPA countermeasure circuit that can generate a true random sequence of itself. Since the DPA countermeasure circuit is composed of several digital ring oscillators, these oscillators can be shared as random sources of the true random number generator after some modifications. Notice that the proposed DPA countermeasure circuit consists of four Fibonacci ring oscillator sets (FiRO), four Galois ring oscillator sets (GaRO), and eight postprocessing circuits. The FiRO and GaRO are composed of four Fibonacci and Galois ring oscillators, respectively. The DPA countermeasure circuit in consists of 12 3-stage ring oscillators directly controlled by random and data bytes to dynamically change the power consumption. As a result, an additional random number generator is required. For the DPA countermeasure circuit based on our previous work, ring oscillators with a simple structure are passively controlled by a random number generator. How ever, the DPA

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

countermeasure circuit in this work can actively generate random bits and feedback to control ring oscillators.

The proposed architecture incorporates a true random number generator into the DPA countermeasure circuit to resist the DPA attack and the *reset problem* mentioned earlier. The combination of two FiROs and two GaROs is used as the random source to generate one random sequence. In order to generate eight independent random bits for each data byte, a total of 32 ring oscillators (including Fibonacci and Galois ring oscillators) are required in the DPA countermeasure circuit. These eight random sources are sampled by flip-flops for further postprocessing. After postprocessing, these eight random bits are XORed with data bytes from the cryptographic circuit to dynamically enable oscillators in the FiRO and GaRO. The FiRO and GaRO now work not only as random sources in [5] to generate random data but also as the digitally controlled ring oscillators in [9] to counteract the DPA attack.

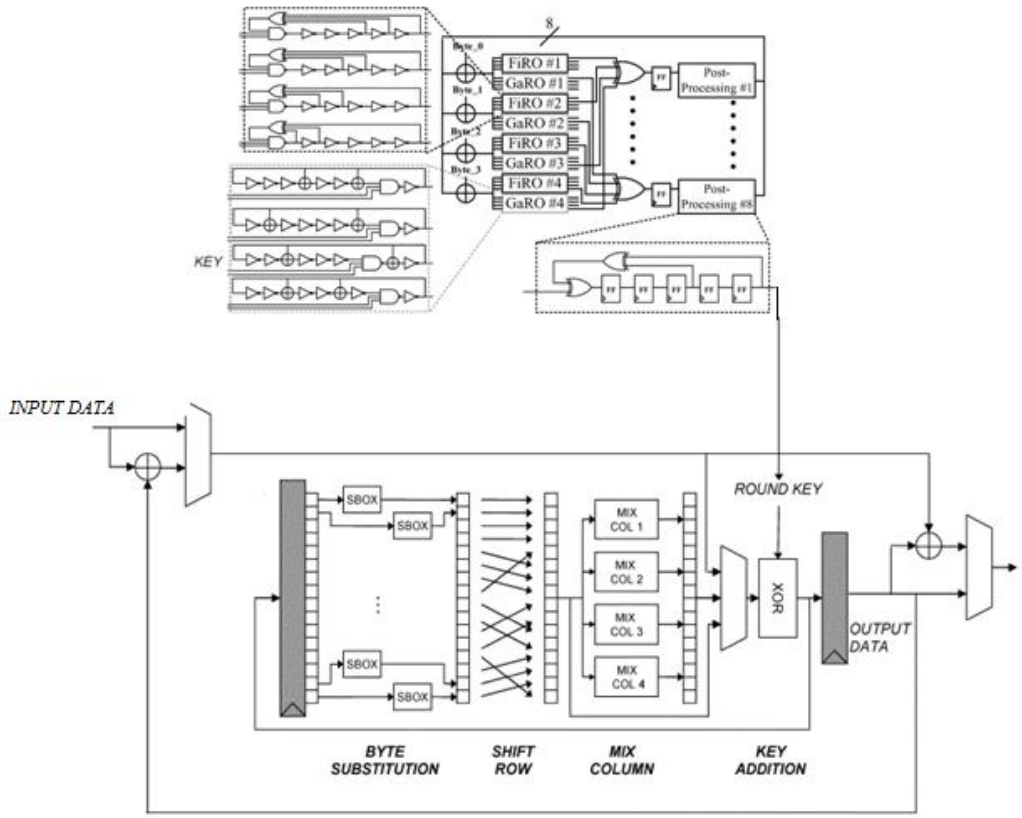

Fig. 3: Architecture of the DPA countermeasure circuit with self-generated true random sequence.

The postprocessing circuits are composed of LFSRs with different initial seeds. The purpose of the postprocessing circuit is to remove the bias of the random source. In each postprocessing circuit, the feedback value is XORed with that from the random source. In this way, even the postprocessing circuit starts from a deterministic state after the system is reset, the generated random sequence would not be the same because the random source is added into the feedback of the LFSR. Fig. 3 shows the architecture of the DPA countermeasure circuit with self-generated true random sequence. The mean value show that the random sequence would be VDD/2, and the standard deviations show that the generated sequence is true random after a warm-up time. For pseudo random sequences after system reset, the standard deviations would be always zero because the same sequence would be generated. For true random sequences generated with the proposed architecture, although the standard deviations are zero in the first few cycles, which means the generated bits in these cycles would be always the same after the system is reset. However, after the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

warm-up time, standard deviations would significantly increase and the random number generator would enter the true random state because the generated bit could be logic 0 or logic 1 with the same probability.

V. RESULTS

The DPA attack result for the proposed DPA resistant AES engine is shown in Fig. 3. The traditional DPA attack exploits the dynamic power consumption to disclose the secret key. As a result, the leakage power analysis has become an unavoidable issue for chip security. Since the DPA countermeasure circuit does not induce any extra delay in the original AES circuit, the throughput of the protected AES circuit is not affected. This is also a significant improvement compared with related works in terms of throughput degradation. Since the DPA countermeasure circuit is independent of the system clock, the additional power consumption will be the same for different AES implementations. The simulation result shows that area, time and speed are same in both the AES engine and proposed countermeasure circuit against DPA attack in AES engine. Thus using MODELSIM 6.3f the coding for AES engine and proposed countermeasure circuit against DPA attack in AES engine is simulated and synthesized using XILINX 8.1e. The compared results show that the area overhead is reduced due to hardware sharing of ring oscillators for generating random sequence without throughput degradation. Thus the security level of an AES engine can be improved by the proposed DPA countermeasure circuit without throughput degradation.

VI. CONCLUSION

The DPA resistance has become the most important consideration for hardware-based cryptographic devices. Although the pseudo random-based method has the advantage of easy implementation, the DPA resistance is largely reduced if the system is reset before recording the power trace accordingly, a true random-based architecture utilizing ring oscillators is proposed to resolve the reset problem by the self generated true random sequence. The major contribution is that the security level of an AES engine can be improved by the proposed DPA countermeasure circuit. In addition, another minor improvement is that the area overhead can be reduced due to hardware sharing of ring oscillators for generating random power and random sources. The true random-based architecture is implemented with an Advanced Encryption Standard (AES) crypto engine for both encryption and decryption. The proposed DPA countermeasure circuit has only minimum area and power overhead without throughput degradation.

REFERENCES

1. C. Tokunaga and D. Blaauw, (2010) "Securing encryption systems with a switched capacitor current equalizer," IEEE J. Solid-State Circuits, vol. 45, no. 1, pp. 23–31.
2. D. Hwang, K. Tiri, A. Hodjat, B.-C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, (2006) "AES-based security coprocessor IC in 0.18- µmCMOS with resistance to differential power analysis side-channel attacks," IEEE J. Solid-State Circuits, vol. 41, no. 4, pp. 781–792.
3. D. Suzuki, M. Saeki, and T. Ichikawa, (2004) "Random switching logic: A countermeasure against DPA based on transition probability," Cryptology Archive, Rep. 2004/346.
4. E. Oswald, S. Mangard, N. Pramstaller, and V. Rijmen, (2005) "A side-channel analysis resistant description of the AES S-Box," in Proc. 12th Int. Workshop, pp. 413–423.
5. E. Brier, C. Clavier, and F. Olivier, (2004) "Correlation power analysis with a leakage model," in Proc. CHES, pp. 16–29.
6. E. Trichina, T. Korkishkoand, and K. H. Lee, (2005) "Small size, low power, side channel-immune AES coprocessor: Design and synthesis results," in Proc. AES, vol. 3373, Lecture Notes in Computer Sciencepp. 113–127.
7. P.-C. Liu, H.-C. Chang, and C.-Y. Lee, (2010) "A low overhead DPA countermeasure circuit based on ring oscillators," IEEE Trans. Circuits Syst. II, Exp. Briefs, vol. 57, no. 7, pp. 546–550,.
8. K. Tiri, M. Akmal, and I. Verbauwhede,(2006) "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in Proc. 28th Eur. Solid-State Circuits Conference, pp. 403–406.
9. P. Kocher, J. Jaffe, and B. Jun, (1999) "Differential power analysis," in Proc. 19th Annu. Int. Cryptology Conf. Adv. Cryptology, pp. 388–397.
10. M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, (2010) "Leakage power analy- sis attacks: A novel class of attacks to nanometer cryptographic circuits," IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 57, no. 2, pp. 355–367,