# Design and Implementation of a DPA Resistant AES Coprocessor

Xinjian Zheng, Yiwei Zhang
Xi'an Microelectronics Technology Institute,
Xi'an 710054, China
addoil_zh@163.com

Bo Peng
ZTEIC Corporation,
ShenZhen 510087, China

*Abstract* **To improve the DPA resistance of cryptographic device in intellectual cards, a power analysis platform is constructed for AES. After analyzed the AES encrypt process, a MASK circuit, disturbance circuit for clock and disturbance circuit for power are designed and implemented in an AES coprocessor of ZTEIC Corporation's intellectual card. The AES coprocessor can process data with 900Mbps at 100 MHz frequency. The DPA test result shows the proportion of best DPA results is less than 5%, and with mask information. The AES coprocessor can defend DPA better than other products with a higher throughput.**

***KeyWords：AES; SPA; DPA; Sbox; Mask; WDDL***

## I. INTRODUCTION

As more security applications migrate to the wireless device, resistance to attacks on the PDA or cellophane will become a necessity. If the attacker extract the encryption keys, all the wireless communications will be insecure. Nowadays, most modern cryptographic devices are implemented using semiconductor logic gates, which are constructed out of transistors. Electrons flows across the silicon substrate when charge is applied to (or removed from) a transistor's gate, consuming power and producing electromagnetic radiation. Two types of power consumption leakage can be observed. The transition count leakage gives information about the number of changed bits, while the Hamming weight leakage is related to the number of 1 bits being processed simultaneously. If the attacker can measure these two power information, the cryptographic device is under power analysis attack.

Two types of power analysis attacks are distinguished [1]. In a simple power analysis (SPA) attack, an attacker uses the side-channel information from one or several measurement directly to determine the secret key. Another analysis is differential power analysis (DPA) attacks, which the attackers use many measurements to filter out noise.

### *A. Simple Power Analysis*

Simple Power Analysis[2] (SPA) is a technique that involves directly interpreting power consumption measurements collected during cryptographic operations. SPA can yield information about a device's operation as well as key material.

In SPA attacks, an attacker directly observes a system's power consumption. The amount of power consumed varies depending on the operation the circuit performed. Large features such as AES rounds, RSA operations, etc. may be identified, since the operations performed by the circuit vary significantly during different parts of these operations. At higher magnification, individual operations can be differentiated. SPA analysis can, for example, be used to break RSA implementations by revealing differences between multiplication and squaring operations. Similarly, many AES implementations have visible differences within permutations and shifts.

### *B. Diferential Power Analysis*

A DPA attack is more powerful than a SPA attack because the attacker does not need to know as many details about how the algorithm was implemented[6]. The technique also gains strength by using statistical analysis to help recover side channel information. The objective of the DPA attacks is to determine the secret key used by a smartcard running the DES/AES algorithm. These techniques can also be generalized to attack other similar cryptographic algorithms.

A DPA attacker begins by running the encryption algorithm for N random values of plain-text input. For each of the N plain-text inputs, $P_i$, a discrete time power signal, $S_{ij}$, is collected and the corresponding cipher-text output, $C_i$, may also be collected. The power signal $S_{ij}$ is a sampled version of the power consumed during the portion of the algorithm that is being attacked. The $i$ index corresponds to the $P_i$ that produced the signal and the $j$ index corresponds to the time of the sample. The attacker guess a sub key, The $S_{ij}$ are split according the differential sub keys. If $S_{ij}$ are spitted correctly, the sub key is the correct sub key, else turn to guess the next sub key.

The remainder of this article is organized as follows. In Section 2, we briefly introduce AES and the power analysis platform. After that we attacked the traditional AES coprocessor succeeded. In Section 3, a MASK circuit, disturbance circuit for clock and disturbance circuit for power are designed and implemented in an AES coprocessor of ZTEIC Corporation's intellectual card. In Section 4, we discuss the performance of our coprocessor and its countermeasure for DPA attack.

978-1-4244-2108-4/08/$25.00 © 2008 IEEE

## II. SPA AND DPA ATTACK ON AES COPROCESSOR

### A. Introduction to AES

The AES[3] algorithm is a symmetric block cipher that operates on 128-bit data blocks. It uses a cipher key to encrypt a 128-bit data block. The length of the cipher key can be 128 bits, 192 bits, or 256 bits.

Like most symmetric ciphers, AES encrypts an input data-block by applying the same round function iteratively. The round function alters the input data-block, which is called State, by applying non-linear and linear functions. The linear functions are RoundKeyAdd, ShiftRows, and MixColumns. The non-linear function is the Sbox.

Figure1 shows the process of 128bit AES encryption.

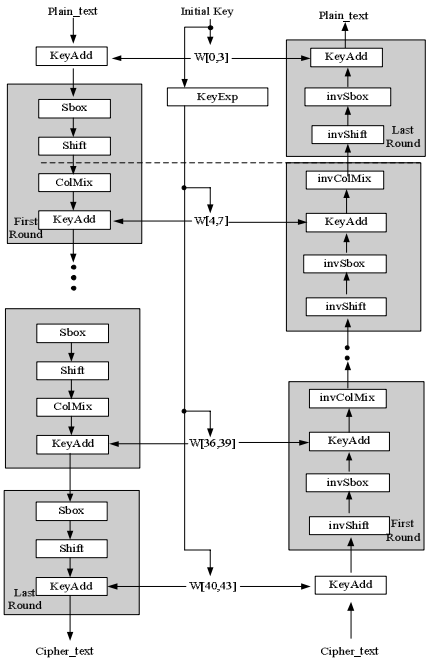


Fig.1 the process of 128bit AES encryption

### B. the DPA analysis platform

The DPA analysis platform is as figure 2.

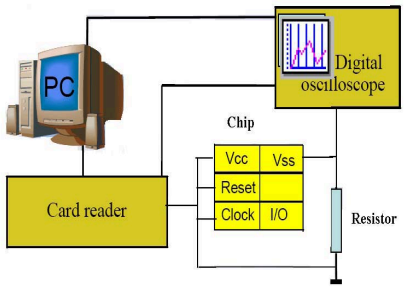


Fig.2 the DPA plat form

Power dissipated by the smartcard can be monitored at the ground pin of the smartcard by using a small resistor in series between the VSS pin on the card and the true ground. Current moving through the resistor creates a time varying voltage that can be sampled by a digital oscilloscope. The current flows out of the smartcard through a bond wire that acts as an inductor. The values of the inductor and the capacitors will determine the shape of the power signal that is observed at oscilloscope. The PC software receives the data from oscilloscope and computes the differences of the $S_{ij}$, the detail DPA process will be introduced in the next section.

### C. DPA on the traditional AES coprocessor

#### 1) SPA analysis on AES

Figure3 shows the AES encrypt process, the section between the two lines is the encrypt rounds of AES. There are 10 rounds for 128bit AES. We select the first round to see the detail operation of a round as Figure4.

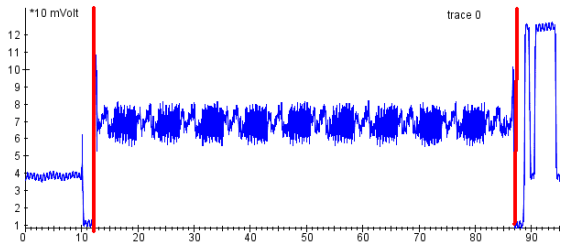


Fig.3 SPA analysis on AES

We can see from Figure4, the four operations in AES are executed sequentially. So we can attack the Sbox operation in first round with DPA analysis.

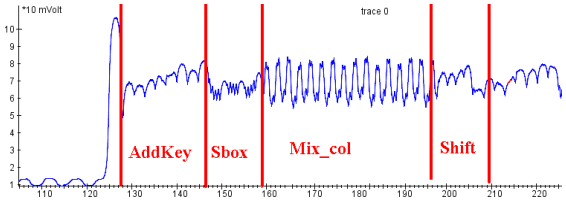


Fig.4 operations in an AES round

#### 2) DPA analysis on AES

After the SPA analysis, we execute AES encryption for k times, and record the plain-text and the cipher-texts. Then we use power consumption measurements to determine whether a key block guess *Ks* is correct. First we computes a k-sample differential trace $\Delta_D[1..k]$ by finding the difference between the average of the traces for which *D(C, b, Ks)* is one and the average of the traces for which *D(C, b, Ks)* is zero. The $\Delta_D[j]$ is the average over $C_{1..:m}$ of the effect due to the value represented by the selection function *D* on the power consumption measurements at point *j*. In particular,

$$\Delta_D[j] = \frac{\sum_{i=1}^{m} D(C_i, K_s)T_i}{\sum_{i=1}^{m} D(C_i, K_s)} - \frac{\sum_{i=1}^{m} (1 - D(C_i, K_s))T_i[j]}{\sum_{i=1}^{m} (1 - D(C_i, K_s))} \approx 2\left(\frac{\sum_{i=1}^{m} D(C_i, K_s)T_i[j]}{\sum_{i=1}^{m} D(C_i, K_s)} - \frac{\sum_{i=1}^{m} T_i(j)}{m}\right) \quad (1)$$

If *Ks* is incorrect, the bit computed using *D* will differ from the actual target bit for about half of the cipher texts *Ci*. The selection function *D(Ci, b,Ks)* is thus effectively uncorrelated

to what was actually computed by the target device. If a random function is used to divide a set into two subsets, the difference in the averages of the subsets should approach zero as the subset sizes approach infinity. Thus, if *Ks* is incorrect,

$$\lim_{m\to\infty} \Delta_D[j] \approx 0 \qquad (2)$$

Because trace components uncorrelated to *D* will diminish with $1/\sqrt{m}$, causing the differential trace to become flat.

If *Ks* is correct, however, the computed value for *D* ($C_i$, *b*, *Ks)* will equal the actual value of target bit b with probability 1, and there will be a peak in the differential trace.

We differ the recorded samples using the model in figure 5. Figure6.1 shows the correct sub-key with the DPA traces. Figure6.2 shows the incorrect sub-key with the DPA traces

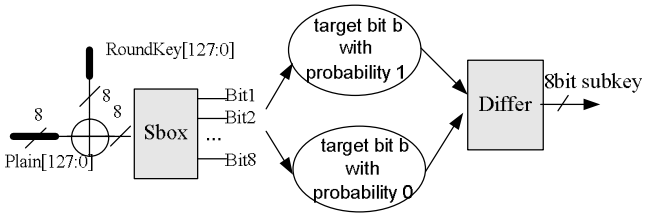


Fig.5 DPA model for AES

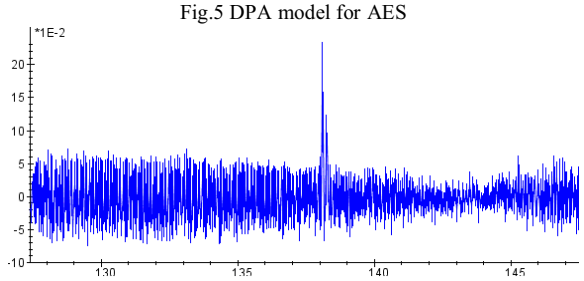


Fig.6-1 DPA analysis with correct key

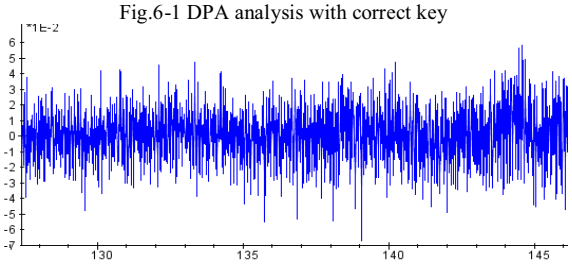


Fig.6-2 DPA analysis with incorrect key

### *D. DPA analysis result*

After analyzed all the Sboxes, we obtained the roundkey for an AES round. So we can calculate the initial key for AES.

## III. DESIGN OF THE DPA RESISTANT AES COPROCESSOR

### *A. Masking Design*

The goal of every countermeasure is to make the power consumption of a cryptographic device independent[5] of the intermediate values of the cryptographic algorithm. Masking can achieves this by randomizing the intermediate values processed by the cryptographic device. In a masked implementation, each intermediate value *V* is concealed by a random value *m* which is generated by the random number generator (RNG) in the Soc chip. The masked value $V_m$ = v*m. The operation * is defined as xor operation in AES. We applied the Masking technique to our AES coprocessor as figure 7.

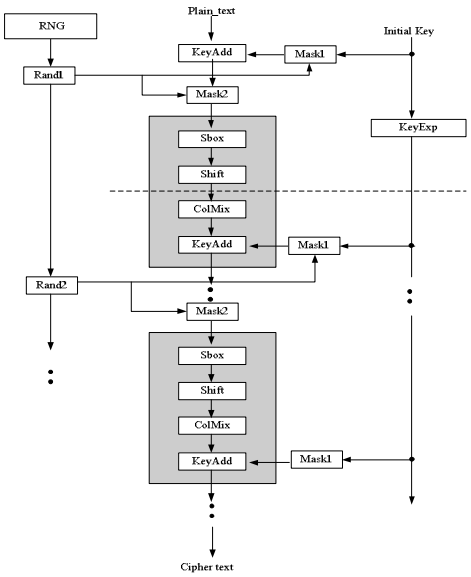


Fig.7 Masking the AES

### *B. Clock disturbance*

When applying DPA attack on AES process, the power consumption of each operation should be located at the same position in each recorded power trace. Otherwise, DPA attacks require significantly more power traces. This observation is the motivation of clock disturbance. If we removed some clock edge in the process of AES encryption using the random number generator (RNG), the power consumed with the same operation will not take place at the same time. The total time of the encryption will be change by the RNG, attackers can't align the operation in different encryption rounds, and the countermeasure of the AES coprocessor will be improved.

Figure 8 shows how to use the clock disturbance. A signal named DisEna is generated from the RNG module in the Soc chip. Most of the time the DisEna is disable, and the clock is the normal clock, when the DisEna is enabled the clock of the module AES will be closed, all the logic in AES coprocessor will be held. As the clock is disturbed, the AES coprocessor's performance will be decreased by 10%.

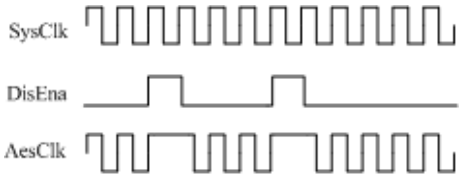


Fig.8 the Clock disturbance

### *C. Power disturbance*

Instead of concealing or de-correlating the side-channel information, the power disturbance techniques pursue the effect of not creating any side-channel information. The goal of these countermeasures is to balance the power consumption of the logic gates. This approach is correct by construction, is

independent of the cryptographic algorithm or arithmetic implemented, and is a distributed measure.

The wave dynamic differential logic [10][11] (WDDL) is used in our AES coprocessor design. A WDDL gate consists of a parallel combination of two positive complementary gates, one calculating the true output using the true inputs, the other the false output using the false inputs. A positive gate produces a zero output for an all zero input. It can certain that whenever the output out does not switch, the differential output out switches. So the power consumption is independent of the processing data.

Figure 9 shows a WDDL cell with pre-charge circuit.

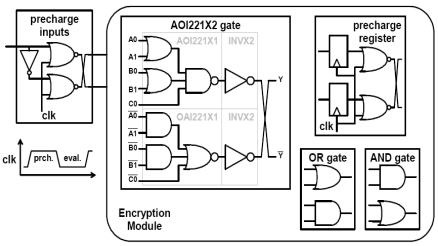


Fig.9 the WDDL cell

## IV. IMPLEMENTATION AND RESULTS

Based on the power analysis of the traditional AES coprocessor, this paper applied several techniques to defend SPA and DPA analysis. We design and implemented a novel DPA resistant AES coprocessor. The processor is implemented in TSMC0.18um process, with the synthesis result 49k gates. The AES coprocessor can process data with 900Mbps at 100 MHz frequency. The DPA test result shows the proportion of best DPA results is less than 5%, and with mask information. The AES coprocessor can defend DPA better than other products with a higher throughput. It has been used in ZTEIC corporation's IC cards. The full layout of the IC card and the AES in it is showed in Figure 10.

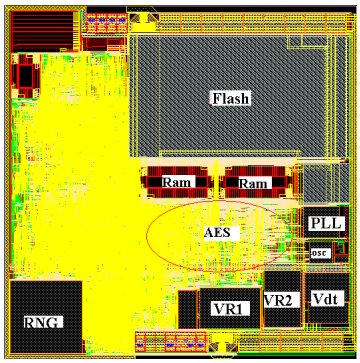


Fig.10 Layout of the SOC chip

Table I shows the comparison of our design with several DPA resistant coprocessors. It can be concluded that our design can defend DPA better than other products with a higher throughput.

Table I comparison of our design and several references

| reference | year | Algorithm | Area | Frequency | Countermeasures |
|---|---|---|---|---|---|
| Jiang's | 2004 | DES | -- | -- | Mask |
| Han's | 2005 | DES | -- | -- | WDDL |
| Kris's | 2006 | AES | 245K | 85Mhz | WDDL |
| proposed | 2007 | AES | 49K | 100Mhz | Mask, Clock disturbance, Paritial WDDL |

## REFERENCE


[1] S. Mangard. A simple power-analysis attack (SPA) attack on implementations of the AES key expansion. In P. J. Lee and C. H. Lim, editors, Proceedings of 5th International Conference on Information Security and Crytography (ICISC), number 2587 in Lecture Notes in Computer Science, pages 343–358, Seoul, Korea, November 2002. Springer-Verlag.

[2] P. Kocher, J. Jaffe, and B. Jun. Differential power analysis. In M. Wiener, editor, Advances in Cryptology: Proceedings of CRYPTO'99, number 1666 in Lecture Notes in Computer Science, pages 388–397, Santa Barbara, CA, USA, August 15-19 1999. Springer-Verlag.

[3] National Institute of Standards and Technology. FIPS 197: Advanced Encryption Standard, November 2001.

[4] N. P. Smart. Physical Side-Channel Attack on Cryptographic Systems. Software Focus. 2000.

[5] Jiang Hui—Ping Mao Zhi—Gang, Advanced DES Algorithm Against Differential Power Analysis and Its Hardware Implementation, Chinese Journal of Computers, Mar, 2004, pp.334~338

[6] K.Itoh M.Takenaka, N.Torii "DPA countermeasure based on the masking method", LNCS 2288, 2002,pp.440-456.

[7] H.Saputra, etal. "Masking the energy behavior of DES encryption", Proceedings of DATE 2003.

[8] J.Coron, L.Goubin "On Boolean and arithmetic masking against differential power analysis", CHES 2000.

[9] J. Coron, P. Kocher, and D. Naccache, "Statistics and secret leakage," in Financial Cryptography (FC), Anguilla, British West Indies, Feb. 2000, vol. 1962, Lecture Notes in Computer Science, pp. 157–173.

[10] Han J un , Zeng Xiaoyang , and Tang Ting'ao, VLSI Design of Anti Attack DES Circuits, Chinese Journal Of Semiconductors, Aug, 2005, pp:1646~1652

[11] Kris Tiri, Ingrid Verbauwhede, A Digital Design Flow for Secure Integrated Circuits, IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN OF INTEGRATED CIRCUITS AND SYSTEMS, VOL. 25, NO. 7, JULY 2006 1197~1208

[12] K. Tiri, and I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation", Design, Automation and Test in Europe Conference, February 2004,pp. 246-251,

[13] A. Hodjat, D. Hwang, B. Lai, K. Tiri, and I. Verbauwhede "A 3.84 Gbits/s AES Crypto Coprocessor with Modes of Operation in a 0.18-µm CMOS Technology", accepted at Great Lakes Symposium on VLSI (GLSVLSI 2005), April 2005.

[14] J. Daemen and V. Rijmen, "Resistance against implementation attacks:A comparative study of the AES proposals," in Proc. 2nd Advanced Encryption Standard (AES) Candidate Conf., Rome, Italy, 1999, pp. 122–132.

[15] N. Pramstaller, F. Gürkaynak, S. Häne, H. Kaeslin, N. Felber, and W. Fichtner, "Towards an AES crypto-chip resistant to differential power analysis," in 30th Eur. Solid-State Circuits Conf. (ESSCIRC), Leuven, Belgium, Sep. 2004, pp. 307–31

[16] E. Oswald, S. Mangard, and N. Pramstaller, "Secure and efficient masking of AES—A mission impossible?" IACR Cryptology ePrint Archive, Santa Barbara, CA, Rep. 2004/134, Jun. 2004