A Low Overhead DPA Countermeasure Circuit Based on Ring Oscillators

Po-Chun Liu, Hsie-Chia Chang, *Member, IEEE*, and Chen-Yi Lee, *Member, IEEE*

***Abstract*—Side-channel attacks, particularly differential power analysis (DPA) attacks, are efficient ways to extract secret keys of the attacked devices by leaked physical information. To resist DPA attacks, hiding and masking methods are commonly used, but it usually resulted in high area overhead and performance degradation. In this brief, a DPA countermeasure circuit based on digital controlled ring oscillators is presented to efficiently resist the first-order DPA attack. The implementation of the critical S-box of the advanced encryption standard (AES) algorithm shows that the area overhead of a single S-box is about 19% without any extra delay in the critical path. Moreover, the countermeasure circuit can be mounted onto different S-box implementations based on composite field or look-up table (LUT). Based on our approach, a DPA-resistant AES chip can be proposed to maintain the same throughput with less than 2K extra gates.**

***Index Terms*—Advanced encryption standard (AES), differential power analysis (DPA), hiding, masking, ring oscillator, S-box.**

I. Introduction

SIDE-CHANNEL attacks exploit the leaked physical information from chips to analyze the possible key and have become efficient ways to attack cryptographic devices. In 1996, Kocher proposed attacks that utilize the timing or power information with controlled data from the attacked devices [1]. Since the power information can easily be obtained by existing equipment, power analysis has become the most common attacking method.

In simple power analysis (SPA) [2], attackers observe a single power trace of the attacked device to guess a part of the secret key. Because SPA utilizes the key-dependent characteristic of power trace, this kind of attack is more suitable to attack asymmetric encryption algorithms. However, in symmetric encryption algorithms, such as advanced encryption standard (AES) [3], the characteristic of the power trace is independent of the secret key. The differential power analysis (DPA) introduced by Kocher *et al.* [2] collects numerous power traces of different encryption or decryption operations. These traces can be analyzed by statistic calculations to find the possible key used by cryptographic devices. Today, AES [3] has become the most popular symmetric encryption algorithm because of its high performance and high security. As a result, several countermeasure methods are proposed to protect an AES chip from DPA attacks.

Hiding and masking are two widely used methods to secure an AES chip against DPA attacks. The main concept of hiding methods is to make the power consumption of different transitions a constant value. Hiding methods use techniques such as wave dynamic differential logic (WDDL) [4] to make the power consumption of different transitions the same as possible. In addition, the main concept of masking methods is to break the relationship between the power consumption and the hypothetic power modeled by attackers. Internally generated random masks are *added* into the data at the beginning of encryption operations and *removed* at the end of encryption operations. However, removing these masks from the processed data is a tough problem due to the nonlinear transformation, i.e., the *subbyte* (S-box), in the AES algorithm. Several modified *subbyte* transformations have been proposed for the masked AES algorithm [5]–[7].

Although hiding and masking methods can efficiently improve the DPA resistance of cryptographic devices, the hardware cost is at least two times larger, and the throughput is degraded by at least 50%. In this brief, we propose a countermeasure circuit that resists DPA attacks in the circuit level by utilizing the concept of digital controlled ring oscillators. The main feature is that the countermeasure circuit is directly mounted onto the S-box module. Thus, there is no extra delay induced in the critical path. Since our proposed design adopts simple logic gates to counteract DPA attacks, the hardware cost overhead could be significantly reduced.

A brief review of DPA attacks is introduced in Section II. The proposed countermeasure circuit and the analysis against DPA attacks are given in Section III. Section IV shows the implementation results, and Section V concludes this brief.

II. Review of DPA Attacks

DPA is a very powerful method to eliminate the effects of irrelative noises; therefore, DPA attacks can still be conducted successfully even in an extremely noisy environment. The key to DPA attacks is the dependency between the power consumption of the attacked devices and intermediate values of encryption algorithms. Note that intermediate values can be any time instance within the encryption operation. Once the algorithm of the attacked device is recognized, intermediate values of the controlled input data can be obtained based on different key hypotheses. At the same time, the power consumption of such controlled input data can be recorded for further analysis. Since

Manuscript received November 10, 2009; revised January 27, 2010; accepted February 23, 2010. Date of publication June 3, 2010; date of current version July 16, 2010. This work was supported in part by the National Science Council under Grant NSC98-2220-E-009-005 and in part by the Ministry of Economic Affairs under Grant 98-EC-17-A-03-S1-005. This paper was recommended by Associate Editor G. Grassi.

The authors are with the Department of Electronics Engineering and Institute of Electronics, National Chiao Tung University, Hsinchu 300, Taiwan (e-mail: pcliu@si2lab.org; hcchang@si2lab.org; cylee@si2lab.org).

Digital Object Identifier 10.1109/TCSII.2010.2048400

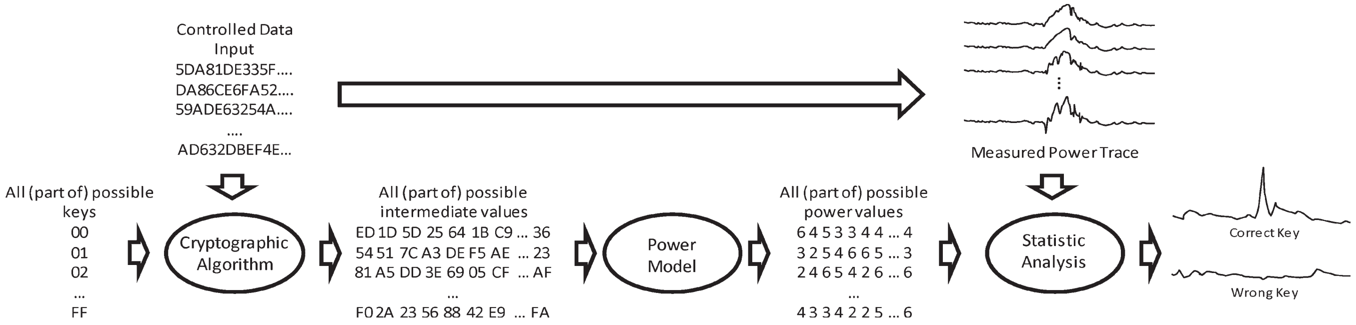

Fig. 1. DPA flow.

intermediate values can be translated into power values (PVs) by appropriate modeling, attackers can analyze the dependency between the PVs and the real power consumption to extract the secret key.

Fig. 1 shows the flow of DPA attacks [8]. The power consumption of the attacked device with controlled input data is recorded. At the same time, attackers use the same input data to calculate intermediate values for all possible key hypotheses (usually a small part of the secret key). Once intermediate values are obtained, attackers need to translate these intermediate values into PVs by some power models, which significantly affect the efficiency of DPA. The Hamming distance (HD) model, which is most often used for hardware implementations, translates intermediate values into PVs by counting the HD between two successive intermediate values. The HD model is suitable for hardware implementations because in CMOS technology, the power consumption highly corresponds to the number of signal transitions.

To extract the key information, attackers analyze the dependency between PVs and power traces by statistic calculations, such as difference of means or correlation coefficient. In the difference-of-means method, power traces are divided into two groups based on PVs. The difference-of-means of these two groups can thus indicate the dependency between PVs and power traces. The closer the difference approaches zero, the less the dependency between these two variables. Thus, if the key hypothesis is correct, then the dependency between PVs and power traces should be higher, and thus the difference of these two groups would lead to a peak. On the other hand, the correlation coefficient method considers not only the difference of means but also corresponding variances, which leads to fewer power traces required. The equation for calculating correlation coefficients is

$$r_{i,j} = \frac{\sum_{d=1}^{D}(h_{d,i}-\bar{h_i})\cdot(t_{d,j}-\bar{t_j})}{\sqrt{\sum_{d=1}^{D}(h_{d,i}-\bar{h_i})^2\cdot\sum_{d=1}^{D}(t_{d,j}-\bar{t_j})^2}} \quad (1)$$

where $h_{d,i}$ is the PV with possible key i for the dth input pattern, $t_{d,j}$ is the power trace at time index j for the dth input pattern, and $\bar{h_i}$ and $\bar{t_j}$ are mean values of $h_{d,i}$ and $t_{d,j}$ for total D input patterns. The closer the correlation coefficient approaches ±1, the higher the dependency between these two variables. If the key hypothesis is wrong, then the correlation coefficient should be zero; otherwise, there would be a peak in the analysis result. As a result, attackers can easily identify the secret key from the analysis result.

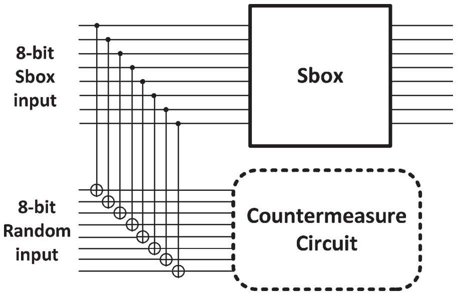

Fig. 2. Block diagram of DPA-resistant S-box.

III. DPA RESISTANT S-BOX

The fundamental idea of a DPA resistance circuit is to break the dependency between intermediate values and power traces. Several methods [4]–[7] based on masking or hiding have been proposed to change the power consumption characteristic of the attacked devices with redundant or additional circuits. However, modifications to the S-box are necessary in these proposals. Fig. 2 shows the block diagram of our proposed DPA-resistant S-box. The countermeasure circuit is designed to work in parallel along with the S-box module without any modification to the S-box. To dynamically change the power consumption of the S-box, an internally generated random mask and the input data of the S-box are used to control the countermeasure circuit.

A. Proposed DPA Countermeasure Circuit

Fig. 3 shows the architecture of our proposed DPA countermeasure circuit. The countermeasure circuit consists of 12 ring oscillators, each of which can be enabled or disabled independently. When a ring oscillator is enabled, it will consume additional power to change the power consumption characteristic. An 8-bit input is obtained by XORing one data byte with a random mask, and eight ring oscillators are directly controlled by this 8-bit input. The random mask can be generated by an internally designed random number generator, whose randomness dominates the DPA resistance of our proposed countermeasure circuit. The remaining four oscillators are controlled by pairs of these eight inputs, which is shown in Fig. 3. This way,

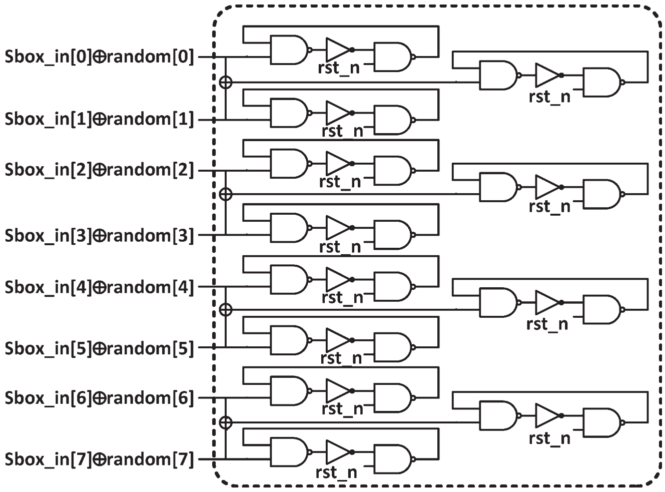

Fig. 3. Architecture of oscillator-based countermeasure circuit.

the amount of power consumption added to the whole chip corresponds to the masked data.

There are two design considerations for our proposed DPA countermeasure circuit: 1) the number of inversion stages in each ring oscillator and 2) the number of ring oscillators required for the S-box. The main consideration for the number of inversion stages is the hardware cost overhead, so the ring oscillator must be as short as possible. As shown in Fig. 3, only two NAND gates and one inverter are used in each ring oscillator. The first NAND gate is used to enable or disable the ring oscillator. When the input is logic 0, the ring oscillator remains idle with any feedback value, and no additional power is consumed. When the input is logic 1, the ring oscillator starts to oscillate and consumes additional power. The last NAND gate is designed to initialize the ring oscillator by system reset.

The number of ring oscillators in the DPA countermeasure circuit is also an important issue. The most intuitive way is to adopt eight ring oscillators because the input of an S-box is 8 bits. However, it is still vulnerable to DPA attacks. From (1), the correlation of $h_{d,i}$ and $t_{d,j}$ would be zero if these two variables are independent. Hence, the power consumption of ring oscillators must dominate over S-box to make the PVs and power traces independent. An LUT-based S-box, which is the most power consumptive one, consumes around 150 μW in 90-nm technology, but a single ring oscillator consumes only around 90 μW. Thus, the power consumption of ring oscillators cannot dominate over S-box if only one ring oscillator is enabled. As a result, we adopt two levels of hierarchy to make at least two ring oscillators be enabled with any control input except all zeros.

For the sake of illustration, the input of the S-box module is controlled to switch between two randomly chosen patterns, i.e., $1d_h$ and 93_h. The power trace is recorded and shown in Fig. 4. The intervals between solid lines in Fig. 4(a) are the power consumption characteristic switching from $1d_h$ to 93_h, and the intervals between dotted lines are that switching from $1d_h$ back to 93_h. As shown in Fig. 4(a), the power characteristic and the amount of power consumed are quite similar for the same input transition, and this gives the chance of conducting DPA attacks. When same patterns are applied to the S-box module with our proposed countermeasure circuit, the power trace is shown in Fig. 4(b). The power characteristic and the amount of power consumed for the same input transition are different now, and detailed analysis results are shown in Section III-B.

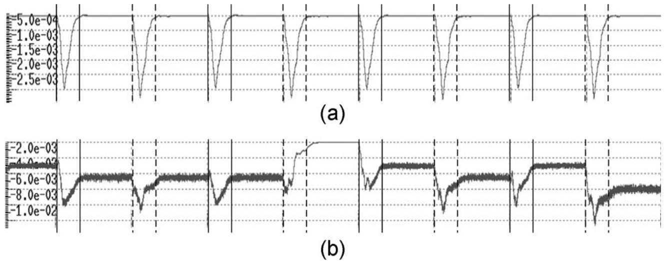

Fig. 4. (a) Power trace without countermeasure circuit. (b) Power trace with countermeasure circuit.

B. DPA Resistance Analysis

The proposed DPA-resistant S-box is simulated in SPICE to obtain simulated power traces. One million random input patterns with the same key are simulated, and all the power traces are recorded. These simulated power traces are then used to conduct DPA attacks using the analysis flow in Fig. 1. In this brief, the PVs are obtained by the HD model, and the correlation coefficient method is used for statistic calculation.

In the HD model, the PVs are modeled by the transition number between two successive intermediate values. The equation to obtain PVs can be written as PV $= a \times HW(v_{i-1} \oplus v_i) + b$, where a and b are real numbers and the function $HW()$ returns the 1's number of its input, and v_{i-1} and v_i are two successive intermediate values. The value of a and b is determined by the maximum and minimum power consumption of an S-box. If the HD of two successive values is zero, then PV is equal to b and can be determined by the minimum power consumption. Note that the intermediate values at the output of the S-box are used to model PVs.

The statistic analysis result of an LUT-based S-box without DPA countermeasure circuits is shown in Fig. 5. In Fig. 5(a), the correlation coefficients of all possible key hypotheses are plotted over time, and that of the correct key hypothesis is plotted as the bold line. The correct key hypothesis results in a significant peak at 6 ns, indicating that the correlation of the correct key is higher than all the other key hypotheses at this time instance. Then, attackers can assume the key hypothesis with the maximum correlation coefficient as the correct key. Since the correlation of the correct key between PVs and power traces is the highest at 6 ns, we now want to analyze how many traces are needed to obtain a peak at this time instance. Fig. 5(b) shows the correlation coefficients of all key hypotheses over the number of traces. Again, the correlation coefficient of the correct key is plotted as the bold line. As shown in Fig. 5(b), the more traces are used, the easier the attackers can distinguish the correct key from all the other key hypotheses. In this case, once more than 4000 traces are used, the correlation of the correct key at 6 ns will be higher than all the other key hypotheses, and the correct key can be found easily.

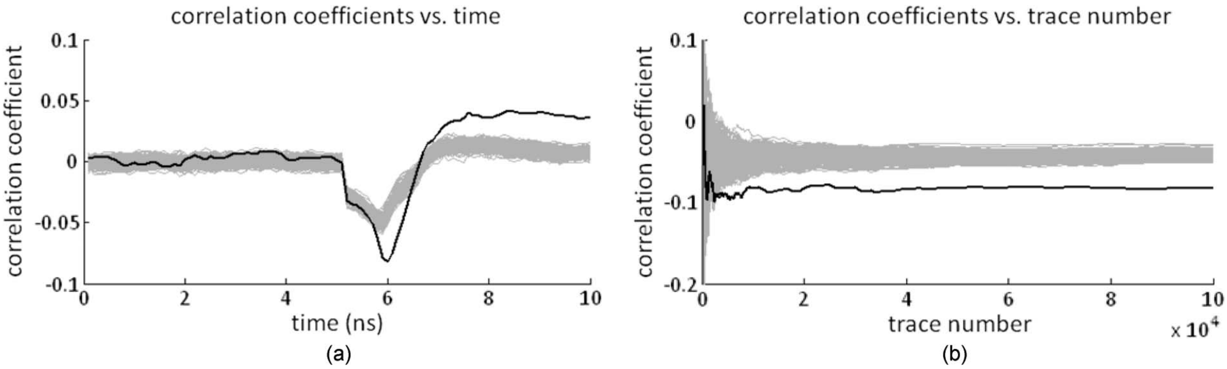

Fig. 5. Original S-box. (a) Correlation coefficients versus time. (b) Correlation coefficients versus trace number.

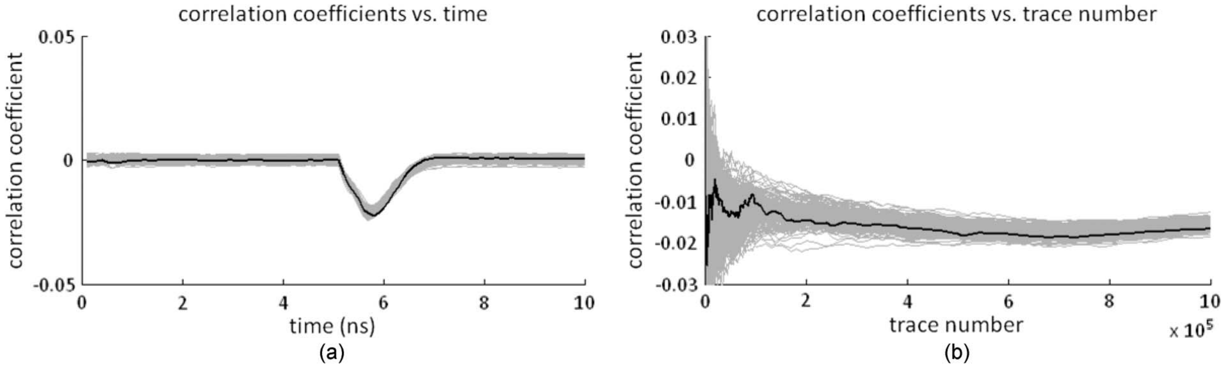

Fig. 6. LUT-based S-box with DPA countermeasure circuit. (a) Correlation coefficients versus time. (b) Correlation coefficients versus trace number.

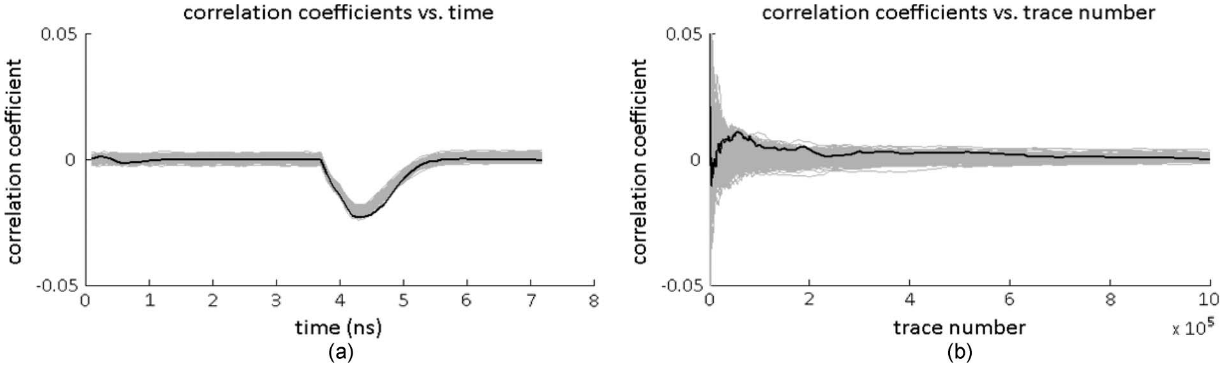

Fig. 7. Composite field-based S-box with DPA countermeasure circuit. (a) Correlation coefficients versus time. (b) Correlation coefficients versus trace number.

Fig. 6 shows the analysis result of an LUT-based S-box along with our proposed countermeasure circuit. There is still a peak at around 6 ns, but the peak value in Fig. 6(a) is much smaller than that in Fig. 5(a). Furthermore, the correct key now does not result in the highest correlation at this time instance. The correct key is now hidden in the analysis result. Therefore, even if attackers can find a peak in the analysis result, they still cannot find the correct key. As shown in Fig. 6(b), the correlation of the correct key is still lower than some other key hypotheses after one million traces are used to analyze. In addition, our proposed DPA countermeasure circuit can also efficiently counteract DPA attacks along with a composite field-based S-box, as shown in Fig. 7(a). The correlation of the correct key is lower than some other key hypotheses around 4.5 ns, so the correct key can also be hidden under the protection of our DPA countermeasure circuit. Fig. 7(b) shows that the correct key again cannot be found even if one million power traces are used.

From the above analysis results, our proposed DPA countermeasure circuit can resist DPA attacks by changing the power characteristic of the S-box. Thus, the correlation between PVs and power traces can be effectively broken to hide the correct key. In addition, since the DPA resistance of our approach is independent of the operating frequency, the proposed countermeasure circuit can provide better protection over decoupling capacitors [11].

IV. Implementation Results

Our proposed DPA countermeasure circuit is implemented in UMC 90-nm CMOS technology. Table I gives the synthesized results and the comparison between different DPA

TABLE I
COMPARISONS WITH RELATED DESIGNS

Method	Designs	Tech.	Area	Gates	Area Overhead	Critical Path	Delay Overhead	**Overhead Factor
Lookup Table	LUT S-box	90 nm	1784 μm^2	637	-	1.70 ns	-	-
	LUT S-box with ***DCO	90 nm	2123 μm^2	758	19%	1.70 ns	0%	1.19
Finite Field	Composite S-box	90 nm	638 μm^2	228	-	3.07 ns	-	-
	Composite S-box with DCO	90 nm	977 μm^2	349	53.13%	3.07 ns	0%	1.53
	Akkar [5]	90 nm	3017 μm^2	1078	372.88%	7.99 ns	160.26%	12.31
	Trichina [6]	90 nm	1821 μm^2	650	185.42%	7.97 ns	159.61%	7.41
	Pramstaller [9]	0.25 μm	n/a	n/a	*200%	n/a	*150%	7.50
WDDL	Hwang [10]	0.18 μm	n/a	n/a	*210%	n/a	*285.86%	11.96

*Estimated values based on [9] and [10]
**Overhead factor: ((Area Overhead)+100%) × ((Delay Overhead)+100%)
***DCO: Digital controlled ring oscillator

countermeasure methods. The LUT and the composite field S-box without DPA countermeasure are also shown for the overhead comparison. We also reimplemented Akkar and Giraud's [5] and Trichina *et al.*'s [6] methods using the same technology for further comparison. When our approach works along with an LUT-based S-box, the area overhead is 19% with no additional critical path delay, which is a big advance over traditional hiding and masking methods.

As for a low-cost AES design, the composite field-based S-box [12], [13] is widely adopted. Because the hardware cost of a composite field-based S-box is much lower than an LUT-based one, the area overhead to a single S-box is increased to 53.13% without lengthening the critical path delay. Since our design is an add-on circuit, the proposed countermeasure circuit can directly be mounted onto a composite field-based S-box to resist DPA attacks. The area overhead of Akkar and Giraud's [5] masked S-box is 372%, and the critical path is lengthened by 160%. Trichina *et al.*'s method [6] can efficiently reduce the area overhead to 185%. Oswald *et al.*'s method [7] is implemented by Pramstaller *et al.* in 0.25-μm technology [9]. As reported by Pramstaller *et al.*, the estimated area overhead of a single S-box is about 200%, and the estimated delay overhead is about 150%. The WDDL method proposed by Tiri and Verbauwhede [4] is implemented by Hwang *et al.* [10]. This algorithm-independent method can be directly applied to any encryption algorithm counteracting DPA attacks.

The overhead factor is defined to consider the area and delay overhead together. As listed in Table I, our proposal can achieve the lowest overall overhead among available solutions. Based on our implementation of the AES core [14], the overall area overhead is around 2K gates.

V. CONCLUSION

DPA attacks have become an important threat against cryptographic chips. The area overhead of hiding or masking methods is still too high for area-constrained applications. The throughput degradation also limits a DPA-resistant design for high-throughput systems. In this brief, we proposed a cooperative DPA countermeasure circuit based on ring oscillators working in parallel along with the S-box. The countermeasure circuit can be easily mounted on different implementations of the S-box to resist DPA attacks. No throughput degradation and low area overhead, 19% overhead for an LUT S-box and 53% overhead for a composite field S-box, can be achieved by the proposed countermeasure circuit. Because the area overhead of a single S-box is 121 gates, the overall overhead for an AES chip is less than 2K gates. The analysis results of our proposed countermeasure circuit showed that the correct key byte still cannot be found even when 10^6 random patterns are used to conduct DPA attacks.

REFERENCES

[1] P. Kocher, "Timing attacks on implementations of Diffie–Hellman, RSA, DSS, and other systems," in *Proc. 16th Annu. Int. Cryptology Conf. Adv. Cryptology*, 1996, pp. 104–113.

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. 19th Annu. Int. Cryptology Conf. Adv. Cryptology*, 1999, pp. 388–397.

[3] *Federal Information Processing Standards Publication 197—Advanced Encryption Standard*, Nat. Inst. Standards Technol., Gaithersburg, MD, Nov. 2001.

[4] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proc. Des., Autom. Test Eur. Conf. Exhib.*, Feb. 2004, vol. 1, pp. 246–251.

[5] M.-L. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks," in *Proc. CHES*, 2001, pp. 309–318.

[6] E. Trichina, D. D. Seta, and L. Germani, "Simplified adaptive multiplicative masking for AES," in *Proc. CHES*, 2002, pp. 71–85.

[7] E. Oswald, S. Mangard, N. Pramstaller, and V. Rijmen, "A side-channel analysis resistant description of the AES S-box," in *Proc. 12th Int. Workshop FSE*, 2005, pp. 413–423.

[8] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards*. New York: Springer Science+Business Media, LLC, 2007.

[9] N. Pramstaller, E. Oswald, S. Mangard, F. K. Gürkaynak, and S. Häne, "A masked AES ASIC implementation," in *Proc. Austrochip*, 2004, pp. 77–82.

[10] D. Hwang, K. Tiri, A. Hodjat, B.-C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "AES-based security coprocessor IC in 0.18-μm CMOS with resistance to differential power analysis side-channel attacks," *IEEE J. Solid-State Circuits*, vol. 41, no. 4, pp. 781–792, Apr. 2006.

[11] A. U. Danis and B. Ors, "Differential power analysis attack considering decoupling capacitance effect," in *Proc. Eur. Conf. Circuit Theory Des.*, Aug. 2009, pp. 359–362.

[12] D. Canright, "A very compact S-box for AES," in *Proc. CHES*, 2005, vol. 3659, pp. 441–455.

[13] A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A compact Rijndael hardware architecture with S-box optimization," in *Proc. Adv. Cryptography—ASIACRYPT*, 2001, vol. 2248, pp. 239–254.

[14] P.-C. Liu, H.-C. Chang, and C.-Y. Lee, "A 1.69 Gb/s area-efficient AES crypto core with compact on-the-fly key expansion unit," in *Proc. ESSCIRC*, Sep. 2009, pp. 404–407.