A True Random-Based Differential Power Analysis Countermeasure Circuit for an AES Engine

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

***Abstract*—The differential power analysis (DPA) has become a big threat to crypto chips since it can efficiently disclose the secret key without much effort. Several methods have been proposed in literatures to resist the DPA attack, but they largely increase the hardware cost and severely degrade the throughput. In this brief, a security problem based on ring oscillators is resolved by a new architecture with self-generated true random sequence. The true random-based architecture is implemented with an Advanced Encryption Standard (AES) crypto engine using UMC 90-nm CMOS technology. The DPA-resistant AES engine can achieve 2.97-Gb/s throughput at an operating frequency of 255 MHz with a 0.104-mm^2 cell area. The proposed DPA countermeasure circuit has only 6.2% area and 18.5% power overhead without throughput degradation.**

***Index Terms*—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 [1] 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 within 10,000 measurements [2], [3]. 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]–[7]. 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 called sense amplify based logic [8] or wave dynamical differential logic (WDDL) [9]. 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]. The current is charged to a capacitor array, and the current consumed by cryptographic circuits is then supplied by the capacitor array instead of the power supply. However, the increased security level results in extra hardware cost and throughput degradation. For example, the WDDL method can increase the security with 3 times larger silicon area and 75% throughput degradation [2]. The switching capacitor method can reduce the area overhead to 27%, but the performance is still degraded by 50% [3]. A ring-oscillator-based DPA countermeasure circuit [10] 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 [10]. 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.

To solve the *reset problem* in [10], a different architecture that incorporates a true random number generator is proposed not only to counteract the DPA attack but also to self-generate 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 DPA attack flow is briefly introduced in Section II. The architecture and the analysis of the proposed DPA countermeasure circuit are given in Section III. Section IV shows the implementation result and comparison to state-of-the-art designs. At last, the conclusion is given in Section V.

II. 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. These N power traces, which consist of T sample points, are firstly arranged as an N-by-T measured power array for further processing. At the same time, these N patterns are also applied to a power prediction model to obtain predicted power values. The power

Manuscript received August 30, 2011; revised November 13, 2011; accepted November 24, 2011. Date of publication January 23, 2012; date of current version February 23, 2012. This work was supported by the National Science Council under Grant NSC100-2220-E-009-062. This paper was recommended by Associate Editor Z. Wang.

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).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSII.2011.2180094

1549-7747/$31.00 © 2012 IEEE

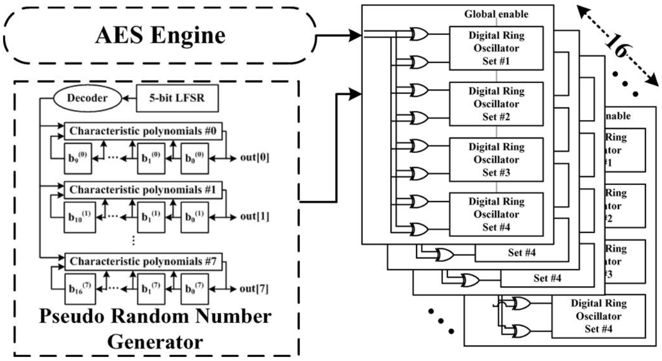
AES Engine
Decoder
5-bit LFSR
Characteristic polynomials #0
$b_9^{(0)}$
$b_1^{(0)}$
$b_0^{(0)}$
out[0]
Characteristic polynomials #1
$b_{10}^{(1)}$
$b_1^{(1)}$
$b_0^{(1)}$
out[1]
Characteristic polynomials #7
$b_{16}^{(7)}$
$b_1^{(7)}$
$b_0^{(7)}$
out[7]
Pseudo Random Number Generator
Global enable
Digital Ring Oscillator Set #1
Digital Ring Oscillator Set #2
Digital Ring Oscillator Set #3
Digital Ring Oscillator Set #4
Set #4
Set #4
Digital Ring Oscillator Set #4
16

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

prediction model is a method to determine possible power consumption, either in the behavior or in the algorithm level. Since the power consumption in the CMOS technology is induced by the logic level transition, the Hamming distance can somewhat represent the power consumption. Therefore, the Hamming distance of a specific point (for example, the registers that store the intermediate data) in two consecutive cycles can be used as the power value. These power values are secondly arranged as an N-by-K predicted power array, where N is the number of patterns, and K is the number of all possible key hypotheses. Each column of this array stands for the predicted power consumption of all N patterns with one key hypothesis. 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.

After the measured and the predicted power arrays are available, the secret key can be disclosed by the statistical analysis. Each column of the predicted power array is used to find a correlation index with every column of the measured power array. If the key hypothesis matches the secret key used by the cryptographic circuit, the correlation index would be higher than that of other key hypotheses. Notice that the correlation index can be obtained by statistical analysis using difference-of-means [1] or correlation [11].

III. 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.

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 [10]. 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 [12]. Each subcircuit is controlled by a data byte of the AES data block and the random byte from the pseudo random number generator.

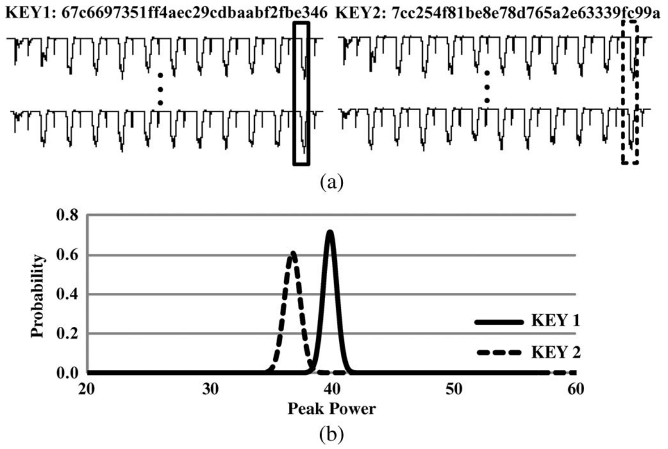

Fig. 2. (a) Simulated power traces of the same pattern with different secret keys. (b) Power distributions for the unprotected AES with different secret keys. The X-axis is the peak power consumption, and the Y-axis is the normalized probability density.

To demonstrate the effect of the DPA countermeasure circuit, power traces recorded by SPICE simulation are illustrated in Fig. 2(a). 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. The distribution of the power consumption at a specific time instance is shown in Fig. 2(b). The standard deviations for both keys are relatively small, and the normal distributions are quite centralized. Since the normal distribution of different secret keys can be easily distinguished, the DPA attack can use the statistical analysis to disclose the secret key with such kind of distribution. Since the statistical analysis requires both the means and standard deviation to calculate the correlation coefficient, the standard deviation is used as a criterion for the DPA resistance. Higher standard deviations would result in lower correlation coefficients and therefore, the correct key is harder to be disclosed.

The normal distribution of the same secret keys and data block for the pseudo random-based architecture is shown in Fig. 3(a). The standard deviation is largely increased compared with the unprotected AES circuit, leading to more flattened distributions. However, there is still a security weakness with this architecture. The random byte 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. Fig. 3(b) shows the normal distribution of power traces when the system is reset before every operation. The distributions with two different secret keys become easily distinguishable again, indicating the DPA resistance suffers.

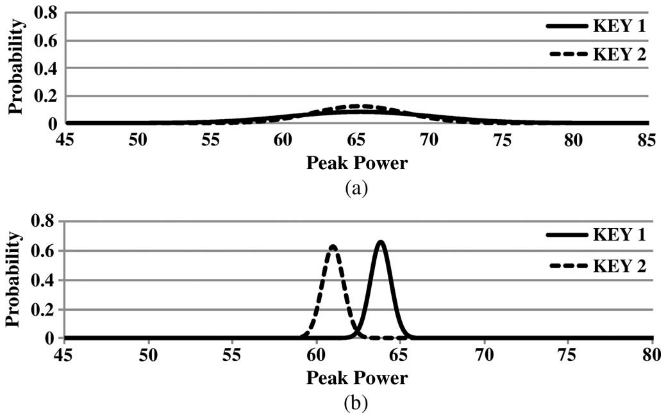

Fig. 3. (a) Normal distributions for the protected AES circuit with different secret keys. (b) Normal distributions for the protected AES circuit with different secret keys, reset is asserted before every operation.

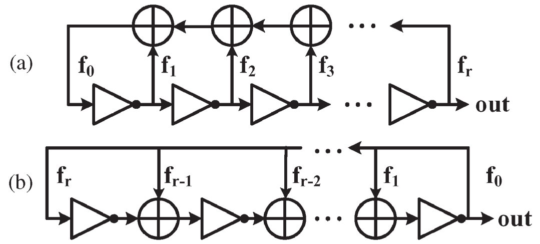

Fig. 4. (a) FiRO. (b) GaRO.

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 [13]. As shown in Fig. 4, the Fibonacci and the Galois ring oscillator consists of a series of inverters connected with feedback polynomial $f(x) = \sum_{i=0}^{r} f_i x^i$, where $f_0 = f_r = 1$. The coefficient $f_i = 1$ indicates that the path is connected, whereas $f_i = 0$ indicates no connection.

Instead of designing an extra true random number generator, Fig. 5 shows 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 [10] 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. However, the DPA countermeasure circuit in this work can actively generate random bits and feedback to control ring oscillators.

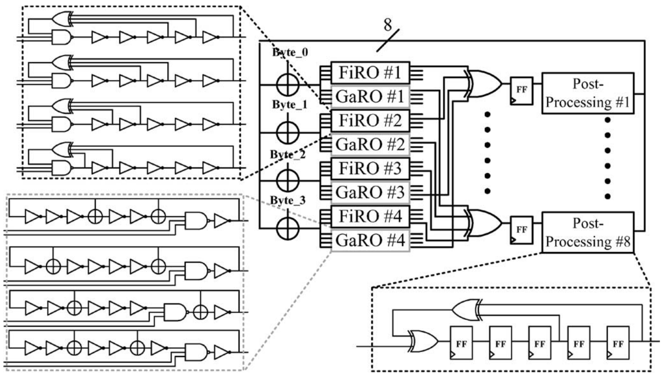

Fig. 5. Architecture of the DPA countermeasure circuit with self-generated true random sequence.

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 [13] to generate random data but also as the digitally controlled ring oscillators in [10] to counteract the DPA attack.

As discussed in [13], the FiRO will not have a *fixed point* if and only if $f(x) = (1 + x)h(x)$ and $h(1) = 1$, where $f(x)$ is the polynomial presentation of the feedback configuration for FiRO, and $h(x)$ is a primitive polynomial. Note that a fixed point is a state that the output vector of inverters is an alternating string of 1 and 0 ($\{01010\cdots\}$ or $\{10101\cdots\}$). Since each random source is from the combination of four different ring oscillators, at least four different $h(x)$ are required. To have four different forms of $h(x)$, the minimum degree of $f(x)$ for the FiRO is 6. Similarly, the condition for the GaRO, having no fixed point, is $f(1) = 0$, and the degree of $f(x)$ must be odd [13]. Again, in order to have four different configurations, the minimum degree of $f(x)$ for GaROs must be 7. The selected four Fibonacci and Galois ring oscillators are shown in Fig. 5 for minimum hardware cost consideration.

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. 6 shows the means and deviations of one generated random bit after 100 system reset. The means 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

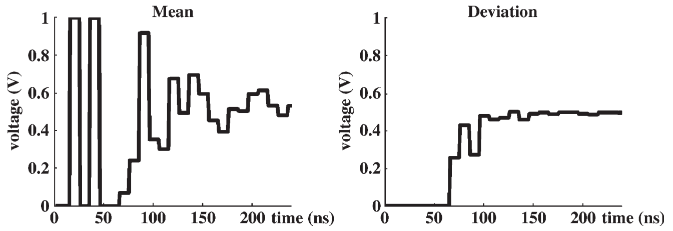

Fig. 6. Randomness analysis of one generated random bits.

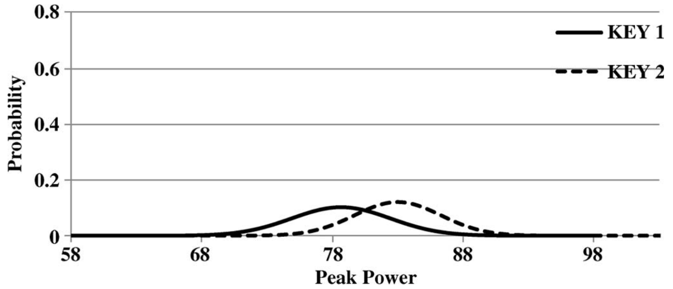

Fig. 7. Power distribution for the protected AES with true random-based DPA countermeasure circuit. The system reset is asserted before every operation.

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 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.

Normal distributions shown in Fig. 7 become flattened again as compared with Fig. 3(b) due to the true random sequence. These two distributions cannot be easily distinguishable and therefore, the DPA resistance of the true random-based architecture is increased even if the system is reset before every operation. Although distributions in this figure are not overlapped as that in Fig. 3(a), it is still not easily distinguishable and is secure enough as shown in the following section. In addition, the mean value of KEY1 becomes lower than that of KEY2. Therefore, the differences of means are also changed by the DPA countermeasure circuit. The quantitative analysis result is shown in the following.

IV. Implementation Results

A. DPA Attack Results

The DPA attack result for the proposed DPA-resistant AES engine is shown in Fig. 8. Note that the system reset is asserted before every encryption operation to demonstrate the effect of the true random-based architecture. Fig. 8(a) shows correlation coefficients of all key hypotheses with 10^7 measurements. The correlation coefficient of the correct key hypothesis is plotted in black, whereas others are plotted in gray. The correlation coefficient of the correct key hypothesis does not lead to a significant peak and therefore, the attacker cannot disclose the correct key byte from this analysis result.

The measurement to disclosure (MTD) can be used as a quantitative criterion for the DPA resistance. The MTD for the unprotected AES engine is around 9200 measurements, indicating that 9200 measurements are sufficient to disclose the secret key. For the protected AES engine, Fig. 8(b) shows correlation coefficients of all key hypotheses with different number of measurements. This figure shows that the correct key byte cannot be disclosed with 10^7 measurements.

The traditional DPA attack exploits the dynamic power consumption to disclose the secret key. However, for the deep submicrometer technology, the leakage power becomes more important particularly for low-power circuits. As a result, the leakage power analysis [14] has become an unavoidable issue for chip security.

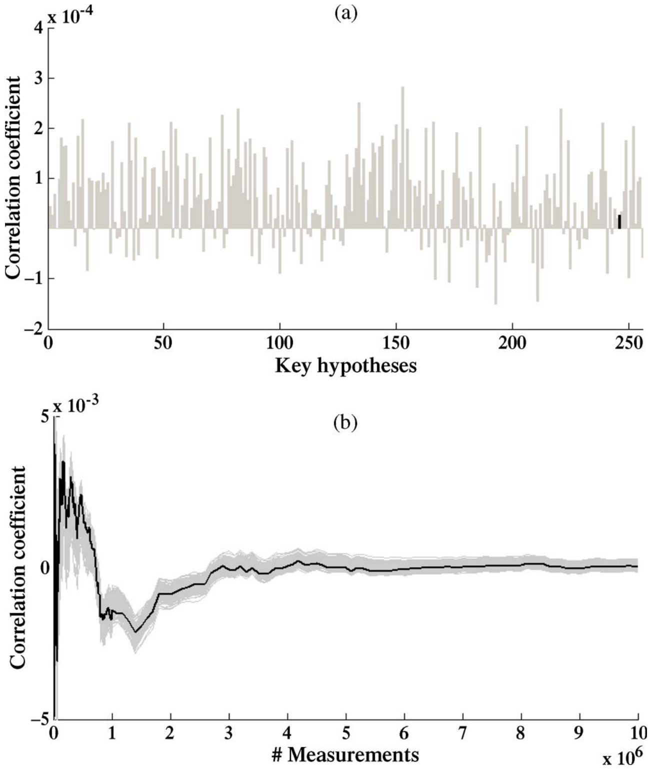

Fig. 8. (a) Correlation coefficients of all key hypotheses with 10^7 measurements. (b) Correlation coefficients with different number of measurements.

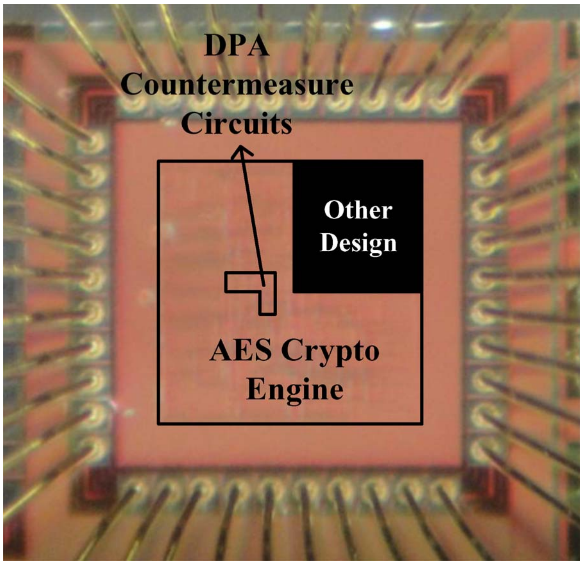

Fig. 9. Die photo of the DPA-resistant AES engine. The test chip contains another irrelative design for pin sharing.

TABLE I
IMPLEMENTATION RESULTS AND COMPARISON

	This Work		JSSC'06 [2]		JSSC'10 [3]	
Technology	90 nm		0.18 μm		0.13 μm	
Method	digital ring oscillator		WDDL		switching capacitor	
Design	Unprotected Core	Protected Core	Unprotected Core	Protected Core	Unprotected Core	Protected Core
Cell area	0.0979 mm^2	0.104 mm^2	0.79 mm^2	2.45 mm^2	0.35 mm^2	0.443 mm^2
Gates	35k	37.1k	79k	245k	70k	88.6k
Overhead$_A$	-	6.2%	-	210.1%	-	27.1%
Frequency	255 MHz	255 MHz	330 MHz	85.5 MHz	200 MHz	100 MHz
Throughput	2.97 Gb/s	2.97 Gb/s	3.84 Gb/s	0.99 Gb/s	2.56 Gb/s	1.28 Gb/s
Degradation	-	0%	-	74.2%	-	50%
Power	5.99 mW	7.10 mW	54mW	200mW	33.32mW	44.34mW
Condition	1V@200MHz	1V@200MHz	1.8V@50MHz	1.8V@50MHz	1.2V@100MHz	1.2V@100MHz
Overhead$_P$	-	18.5%	-	270.4%	-	33%
Figure of merit	-	1.26	-	20.01	-	2.54
MTD	9200	$> 10^7$	8168	1276186	4000	$> 10^7$

B. Chip Measurement Results

The die photo of the proposed DPA-resistant AES engine is shown in Fig. 9. Implementation results and that of the other two related works are listed in Table I. The cell area of our unprotected AES engine is 0.0979 mm^2 and that of the DPA countermeasure circuit is 0.0061 mm^2 in UMC 90-nm CMOS technology, indicating that the area overhead for our AES engine is around 6.2%. Note that the area overhead based on [10] is around 10.2%. Since the WDDL cells are usually 2–3 times larger than the standard cells, the protected AES proposed by Hwang et al. [2] results in 210% larger silicon area. The switching capacitors proposed by Tokunaga and Blaauw still result in 27.1% area overhead. The implementation result shows that the proposed architecture can outperform related works in terms of area overhead.

The maximum measured operating frequency of our AES engine is 255 MHz, and the maximum throughput would be 2.97 Gb/s. Since the DPA countermeasure circuit does not induce any extra delay in the original AES circuit, the maximum operating frequency of the protected AES circuit is not affected. This is also a significant improvement compared with related works in terms of throughput degradation.

The power consumption of our unprotected AES circuit is 5.99 mW with 1-V supply voltage running at 200 MHz. The extra power required by the proposed DPA countermeasure circuit is 1.11 mW, which is around 18.5% compared with the AES engine. Note that, since the DPA countermeasure circuit is independent of the system clock, the additional power consumption will be the same for different AES implementations.

To consider the effect of DPA countermeasure methods on area overhead, throughput degradation, and power overhead, the figure of merit is defined as $(\text{Overhead}_A + 100\%) \times (\text{Degradation} + 100\%) \times (\text{Overhead}_P + 100\%)$. Our proposal outperforms others in terms of this figure of merit.

V. CONCLUSION

The DPA attack utilizing the statistical analysis can efficiently disclose secret keys of cryptographic devices. In this brief, the statistical analysis of power traces with both the pseudo and the true random-based architecture circuit is discussed. 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.

REFERENCES

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

[2] 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.

[3] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE J. Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, Jan. 2010.

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

[5] D. Suzuki, M. Saeki, and T. Ichikawa, "Random switching logic: A countermeasure against DPA based on transition probability," Cryptology ePrint Archive, Rep. 2004/346, 2004. [Online]. Available: http://eprint.iacr.org

[6] 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.

[7] E. Trichina, T. Korkishkoand, and K. H. Lee, "Small size, low power, side channel-immune AES coprocessor: Design and synthesis results," in *Proc. AES*, vol. 3373, *Lecture Notes in Computer Science*, 2005, pp. 113–127.

[8] K. Tiri, M. Akmal, and I. Verbauwhede, "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 Conf.*, Sep. 2002, pp. 403–406.

[9] 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.

[10] P.-C. Liu, H.-C. Chang, and C.-Y. Lee, "A low overhead DPA countermeasure circuit based on ring oscillators," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 57, no. 7, pp. 546–550, Jul. 2010.

[11] E. Brier, C. Clavier, and F. Olivier, "Correlation power analysis with a leakage model," in *Proc. CHES*, 2004, pp. 16–29.

[12] R. Mita, G. Palumbo, S. Pennisi, and M. Poli, "A novel pseudo random bit generator for cryptography applications," in *Proc. 9th Int. Conf. Electron., Circuits Syst.*, 2002, vol. 2, pp. 489–492.

[13] J. D. Goli, "New methods for digital generation and postprocessing of random data," *IEEE Trans. Comput.*, vol. 55, no. 10, pp. 1217–1229, Oct. 2006.

[14] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage power analysis attacks: A novel class of attacks to nanometer cryptographic circuits," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 57, no. 2, pp. 355–367, Feb. 2010.