ISSN 2348-375X

Unique Journal of Engineering and Advanced Sciences

Available online: www.ujconline.net

Research Article

A LOW POWER COUNTERMEASURE CIRCUIT FOR HIGHLY SECURE AES ALGORITHM AGAINST DPA ATTACK

Preshy NP*, Ershad SB

University of Calicut, Nehru College of Engineering Research Centre Pampady, Kerala, India

Received: 07-03-2014; Revised: 05-04-2014; Accepted: 03-05-2014

*Corresponding Author: **Preshy NP**

University of Calicut, Nehru College of Engineering Research Centre Pampady, Kerala, India Email: preshy_snosh@yahoo.com

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. But the power overhead is high. To reduce this power overhead Bit Swapping LFSRs was introduced in the True Random Based Architecture. The proposed Low Power DPA countermeasure circuit reduces the power consumption upto 75% without throughput degradation.

Keywords: Advanced Encryption Standard (AES), cryptography, differential power analysis (DPA), ring oscillators, true random number generator, Bit Swapping LFSRS.

INTRODUCTION

The differential power analysis (DPA) attack proposed by Kocher et al. in 1999 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. 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. 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 or wave dynamical differential logic (WDDL). 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. 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. The switching capacitor method can reduce the area overhead to 27%, but the performance is still degraded by 50%. A ring-oscillator-based DPA counter measure circuit can effectively reduce the area overhead and throughput degradation. 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, 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. But the Power

overhead is still high. To overcome this power overhead, the Bit swapping LFSRs is introduced in the proposed architecture. Normal LFSRs are changed to BS-LFSRs. The proposed Low Power DPA countermeasure circuit reduces the power consumption 75% without throughput degradation.

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 Experimental result and comparison to state-of-the-art designs. At last, the conclusion is given in Section V.

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 prediction model is a method to determine possible power consumption, either in the behaviour 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 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 or correlation.

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.Fig.1 shows the complete architecture of proposed Low Power DPA Countermeasure circuit with AES Engine.

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. 2, 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 Bit swapping 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.

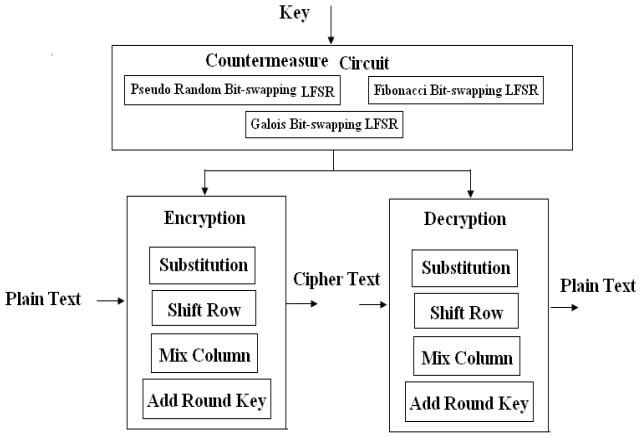

Figure 1: Architecture of Proposed Low Power DPA counter measure circuit with AES Engine.

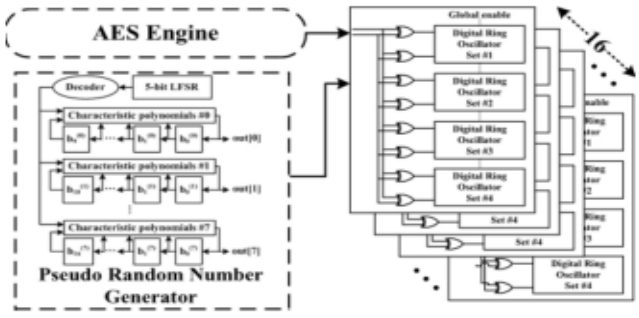

Figure 2: Architecture of the pseudorandom based DPA counter measure circuit.

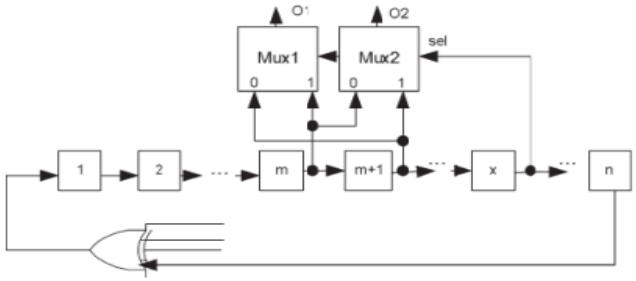

Figure 3: Swapping arrangement for an LFSR.

Here in Pseudorandom Bit LFSRs are used to generate the random bits. Bit-swapping LFSR (BS-LFSR), is composed of an LFSR and a 2 × 1 multiplexer. When used to generate test patterns for scan-based built-in self-tests, it reduces the number of transitions that occur at the scan-chain input during scan shift operation by 50% when compared to those patterns produced by a conventional LFSR. Hence, it reduces the overall switching activity in the circuit under test during test applications. The usage of this BS-LFSR reduces the power overhead.

To demonstrate the effect of the DPA countermeasure circuit, power traces recorded by SPICE simulation are illustrated in Fig.4 (a).This figure shows power trace so fan 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. 4(b). The standard deviations for both keys are relatively small, and the normal distributions are quite centralized.

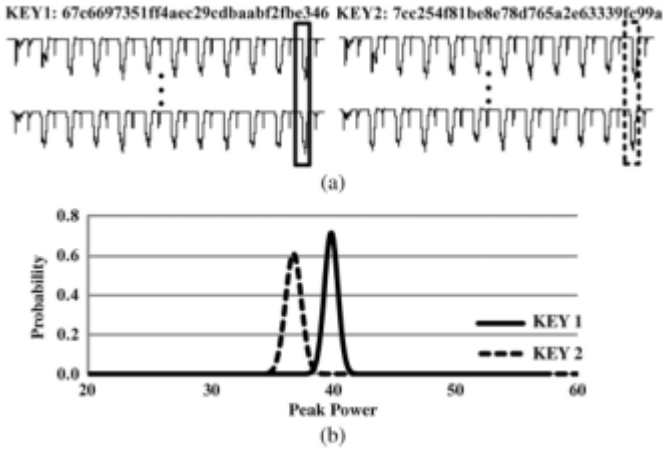

Figure 4: (a) Simulated power traces of the same pattern with different secret keys. (b) Power distributions for the unprotected AES with different secret keys. The X-axis is the peak power consumption, and the Y-axis is the normalized probability density.

The distribution of the power consumption at a specific time instance is shown in Fig. 4(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.

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.

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. As shown in Fig. 5, 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.

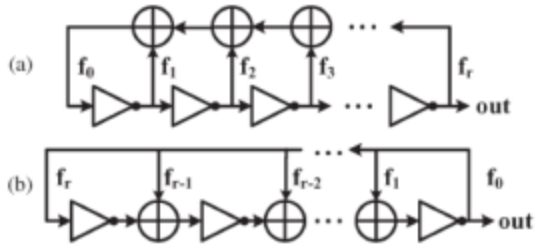

Figure 5: (a) FiRO. (b) GaRO

Instead of designing an extra true random number generator, Fig. 6 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 Bit Swapping ring oscillators, respectively. The DPA countermeasure circuit 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. 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 BS-FiROs and two BS-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 post processing. After, post processing 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 to generate random data but also as the digitally controlled ring oscillators to counteract the DPA attack.

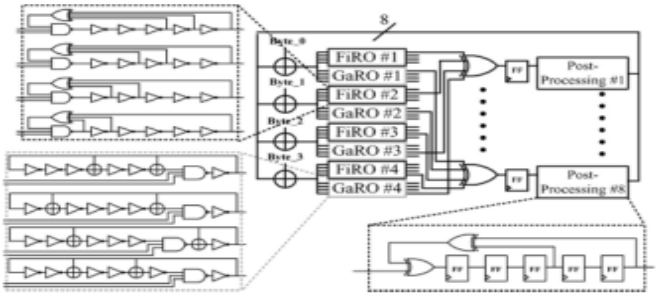

Figure 6: Architecture of the DPA countermeasure circuit with self-generated true random sequence.

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 1and0 ({01010⋯} or {10101⋯}). 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. 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. 6 for minimum hardware cost consideration.

The postprocessing circuits are composed of BS-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 BS-LFSR.

RESULTS

Simulation Results

The Low Power DPA Countermeasure Circuit was simulated using simulation tool ModelSim. Fig 7 shows the simulation results of the countermeasure circuit using normal LFSR. Fig 8 shows the simulation results of the countermeasure circuit using BS-LFSR. And fig 9 shows the simulation results of countermeasure circuit using BS-LFSR with AES Engine. And highly secured encryption/decryption process take place in the AES Engine using this Low Power DPA Countermeasure Circuit.

Power Consumption Analysis Results

The power consumption of the countermeasure circuit with normal LFSR and BS-LFSR are analyzed using the tool XPOWER analyzer in the Xilinx ISE8.1i. 1000MHz clock frequency applied to the countermeasure circuit with normal LFSR and gets the power consumption 490mW. And also applied 1000MHz clock to the countermeasure circuit with BS-LFSR and the power consumption is 164mw. By comparing these two circuits, the power consumption is reduced to 75% using BS-LFSR in the countermeasure circuit. Fig 10 shows the power analysis result of countermeasure circuit with normal LFSR and Fig 11 shows the power analysis result of countermeasure circuit with BS-LFSR.

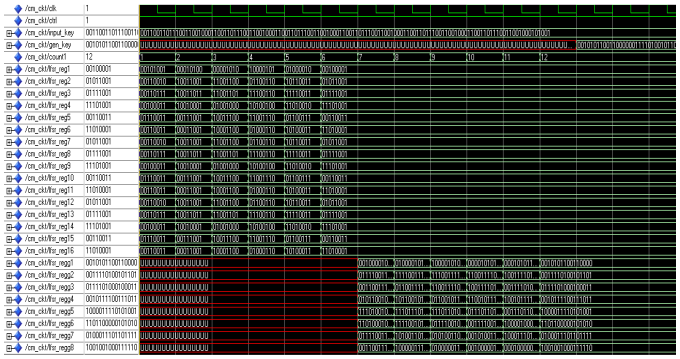

Figure 7: Simulation result of countermeasure circuit using normal LFSR

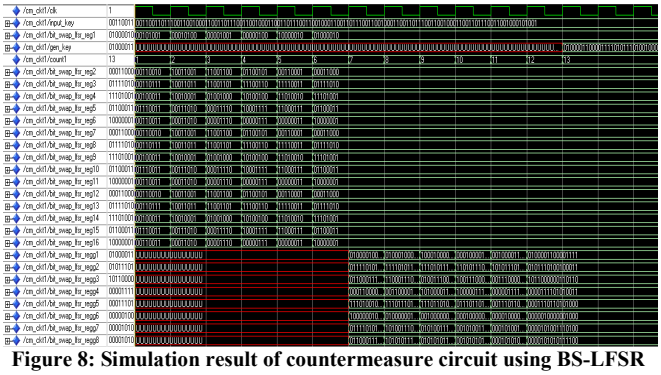

Figure 8: Simulation result of countermeasure circuit using BS-LFSR

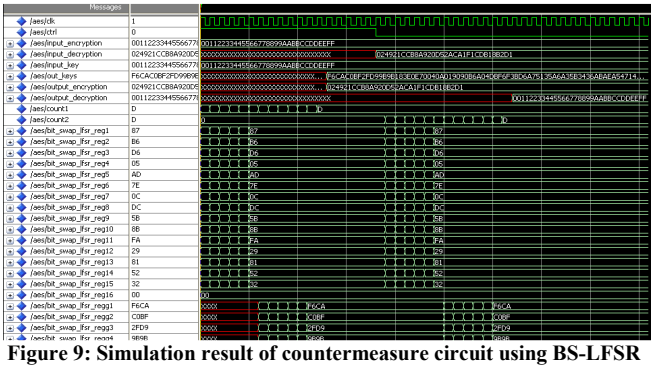

Figure 9: Simulation result of countermeasure circuit using BS-LFSR with AES Engine

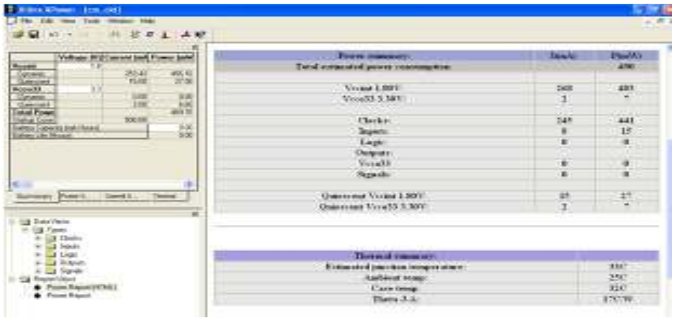

Figure 10: Power analysis result of countermeasure circuit using normal LFSR

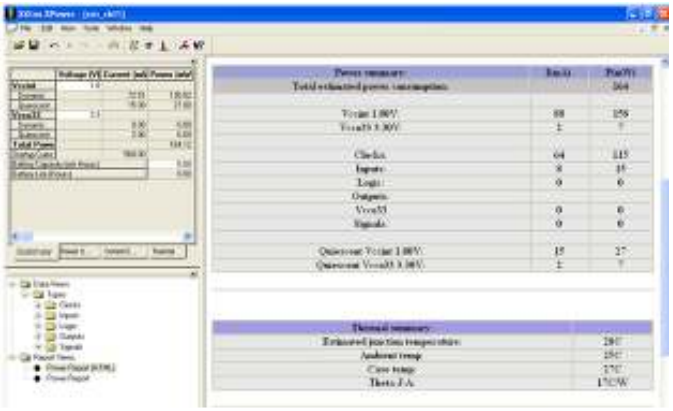

Figure 11: Power analysis result of countermeasure circuit using normal LFSR

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. The proposed DPA countermeasure circuit has only minimum area and power overhead without throughput degradation.

ACKNOWLEDGEMENT

The authors would like to thank Prof.H.S.Divakara Murthy, Dean&HOD of ECE department for his constructive comments and suggestions.

REFERENCES

1. Po-Chun Liu, Changko HC, A True random based differential power analysis countermeasure circuit for an AES Engine, 2nd ed., R. IEEE Transactions on circuits and Systems—II: Express Briefs, 2012; 59(2).
2. Kocher P, Jaffe J, and Jun B, Differential power analysis, in Proc. 19th Annu. Int. Cryptology Conf. Adv. Cryptology, 1999; 388–397.
3. Tokunaga C and Blaauw D, Securing encryption systems with a switched capacitor current equalizer, IEEE J. Solid-State Circuits, 2010; 45(1): 23–31.
4. Alioto M, Giancane L,Scotti G,andTrifiletti A,Leakagepoweranalysis attacks: A novel class of attacks to nanometer cryptographic circuits, IEEE Trans. Circuits Syst. I, Reg. Papers, 2010; 57(2):355–367.
5. Hwang D, Tiri K, Hodjat A, Lai BC, Yang S, Schaumont P, and Verbauwhede I, AES-based security coprocessor IC in 0.18- µm CMOS with resistance to differential power analysis side-channel attacks, IEEE J. Solid-State Circuits, 2006; 41(4): 781–792.
6. Goli JD,New methods for digital generation and postprocessing of random data," IEEE Trans. Comput., 2006; 55(10): 1217–1229.
7. Oswald E, Mangard S, Pramstaller N, and Rijmen V, A side-channel analysis resistant description of the AES S-Box, in Proc. 12th Int. Workshop FSE, 2005; 413–423.
8. Trichina E, Korkishkoand T, and Lee KH, Small size, low power, side channel-immune AES coprocessor: Design and synthesis results, in Proc.AES, Lecture Notes in Computer Science, 2005; (337 3): 113–127.
9. Suzuki D, Saeki M, and Ichikawa T, Random switching logic: A countermeasure against DPA based on transition probability, Cryptology ePrint Archive, Rep. 2004/346, 2004. [Online]. Available:http://eprint.iacr.org
10. Tiri K and Verbauwhede I, A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation, in Proc. Des.,Autom. Test Eur. Conf. Exhib., 2004; 1: 246–251.
11. Brier E, Clavier C, and Olivier F, Correlation power analysis with a leakage model, in Proc. CHES, 2004;16–29.
12. Tiri K, Akmal M, and Verbauwhede I, 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., 2002; 403–406.
13. Mita R, Palumbo G, Pennisi S, and Poli M, A novel pseudo random bit generator for cryptography applications, in Proc. 9th Int. Conf. Electron., Circuits Syst.,2002; l(2): 489–492.

Source of support: Nil, Conflict of interest: None Declared