Side-channel Power Analysis of Different Protection Schemes Against Fault Attacks on AES

Pei Luo[1], Yunsi Fei[1], Liwei Zhang[2], and A. Adam Ding[2]

[1] Department of Electrical and Computer Engineering, Northeastern University, Boston, MA 02115
silenceluo@coe.neu.edu, yfei@ece.neu.edu
[2] Department of Mathematics, Northeastern University, Boston, MA 02115
mathliwei@gmail.com, a.ding@neu.edu

Abstract. A protection circuit can be added into cryptographic systems to detect both soft errors and injected faults required by Differential Fault Analysis (DFA) attacks. While such protection can improve the reliability of the target devices significantly and counteract DFA, they will also incur extra power consumption and other resource overhead. In this paper, we analyze the side-channel power leakage of AES protection methods against fault attacks and quantify the amount. We implement six different schemes and launch correlation power analysis attacks on them. The results show that the protection circuits have all increased the power leakage and therefore make the system more vulnerable to power analysis attacks. We further compare different protection schemes in terms of power consumption, area, fault coverage, and side-channel leakage. Our results demonstrate trade-offs among multiple design metrics, and suggest that reliability, security, and costs have to be all considered together in the design phase of cryptographic systems.

Keywords: AES, differential fault analysis, side-channel attacks

1 introduction

Cryptographic operations have been the security engine for many critical systems and infrastructure. However, their reliability and security are subject to unintentional soft errors and intentionally introduced transient faults which can either disrupt the important security operations or even be used to infer the secret key to crack the entire system. As the process technology keeps shrinking and the supply voltage scales down, the probability of transient errors in circuits, including Single Event Transients (SETs) and Single Event Upsets (SEUs), is rapidly increasing [1]. These soft errors reduce the reliability of systems significantly. If these errors and other faults can be controlled by attackers to impose on cryptographic circuits, statistical analysis can be performed on the correct and faulty outputs to retrieve the key, which is called Differential Fault Analysis Attack [2].

DFA was first introduced by Biham *et. al.* on the Data Encryption Standard (DES) algorithm [2]. It was applied to the AES later and work [3] shows that only two pairs of correct and faulty ciphertexts are needed to break the AES-128, if a single byte fault occurs anywhere between the 8-th round and 9-th round MixColumn operations. The fault model is relaxed to be a random fault anywhere in one of the four diagonals of the state matrix at the input of the 8-th round of the cipher [4].

Meanwhile there are many different methods developed to physically inject faults into circuits. In [5], the authors used magnetic pulses to inject transient faults into an RISC micro-controller running AES. Other commonly used fault injection methods alter the supply voltage or system clocks. Work [4] shows that clock glitches can be used to inject faults into cryptographic devices. The work in [6] demonstrates the effectiveness of frequency injection attacks on both a microcontroller and an FPGA chip.

To protect cryptographic devices from such DFA attacks or improve the reliability of the system, many fault detection and correction schemes have been presented [1,7,8,9,10,11,12,13,14,15]. Some of them exploit the algebraic feature of the cryptographic algorithms. For example, some linear error detection codes are added to the AES system to detect the injected faults [11,12]. Other work relies on a redundant copy of the AES to detect random faults on the working copy [1]. Because DFA attacks inject faults

only into the last several rounds of the AES for possible cryptanalysis, some works propose to implement reverse operations of encryption/decryption to check the results [10].

As any error detection scheme adds some circuit to the original cryptographic system, such protection circuit would increase the power consumption, area, or latency of the system. Such addition may incur extra power leakages in cryptographic systems, which means while designing a scheme for protecting against a given attack (fault injection attacks), the implemented countermeasure would also affect other types of side-channel attacks. This problem was first discussed in [16]. The authors analyzed the impact of four error detection codes on the power analysis resistance. Their gate-level simulation results show that the power analysis vulnerability depends on the particular error detection code used.

In [17,18], the authors ran SPICE simulations of several protection schemes to obtain power consumption estimations, and then ran correlation power analysis (CPA) on their data. They showed that the presence of a parity check circuitry has a negative impact on the resistance of the device to CPAs, and the resistance decreases with the number of check bits used for error detection.

In [19], the authors employed information-theoretic measures to evaluate the relationship between reliability enhancements and the induced side-channel effects. They demonstrated that different EDC/ECC schemes impose different effects on memory security under statistical power analysis.

All the previous works [16,17,18,19] rely on simulation results instead of real implementation results for analysis. However, power simulations are based on simplified models compared to real implementations and do not precisely reflect power consumptions of crypto devices. What's more, previous works [17,18] only focus on simple protection schemes on S-Box, while many widely used protection schemes protect all steps in AES round operations and they are more efficient and complex. Therefore, we see the need of evaluating the power leakage of real implementations of protection schemes on AES, which will provide accurate results to secure system designers.

In this work, we perform a thorough analysis of the additional power leakage and quantify its effect on the success rate of power analysis attacks. We choose several different protection schemes that protect all steps of AES round operations instead of only S-Box. We implement all the schemes in real hardware systems (on FPGA) and measure the power consumption. Our analysis will provide a good understanding of the source and amount of the induced extra power leakages. The discussion and results of this work will provide good guidelines for designing secure and reliable AES implementation.

The rest of the paper is organized as follows. In Section 2, we introduce the protection methods on AES which we use to evaluate the side-channel leakages in this paper. In Section 3, we present the side-channel leakage model. In Section 4, we implement six different AES schemes and run side-channel attacks on them, and show the attack results. Finally we conclude the paper in Section 5.

2 Background: AES Protection Schemes

In this section, we give the background on the AES protection schemes that we have implemented. We introduce some commonly used error detection methods used in AES. The protection methods that we choose not only protect the S-Box, but also all other operations. They include both parity check codes and other complex ones.

One commonly used system protection method is redundancy, which duplicates critical components or functions of a system and compares their results at run-time to detect errors. In this paper, we denote the simple AES error detection scheme of a complete copy and comparison circuit after each step as *Duplicate*.

Other early error detection schemes exploit the inverse relationship existing between encryption and decryption at algorithm level. For example, work [10] performs a decryption after each encryption or computes the inverse operation after each step of the ciphering process. Many cryptographic engines already include both encryption and decryption modules, and therefore this scheme can make use of the hardware without introducing extra error detection hardware.

In [11], different error detection modules are added for the linear and nonlinear blocks of AES hardware implementation. For each of the linear modules, including the Affine transformation of the S-Box computation, ShiftRows, MixColumns, and AddRoundKey operations, error detection based on $(n+1, n)$

cyclic redundancy check (CRC) codes over $GF(2^8)$ (where $n \in \{4, 8, 16\}$) is implemented. CRC codes are demonstrated to be scalable and have very high fault coverage. The basic structure of CRC code error detection is shown in Fig. 1. An n-bit input message $S = \{s_0, s_1, \cdots, s_{n-1}\}$ is transformed into another message $\{t_1, t_2, \cdots, t_n\}$ by an AES operation, and t_0 is predicted from the parity of the message S and form a syndrome with $\{t_1, t_2, \cdots, t_n\}$. If the syndrome is not zero, there are errors happening in the operation and detected. In this paper, we implement CRC $(9, 8)$ and CRC $(5, 4)$ as described in [11] for all the four linear modules separately and denote them as *CRC8* and *CRC4*, respectively. In these implementations, the nonlinear module, the inverse computation of the S-Box operation, is protected by inverting the output of the module and comparing it with the original input to detect faults in the nonlinear module, utilizing the algebraic feature of the nonlinear (inverting) module in AES.

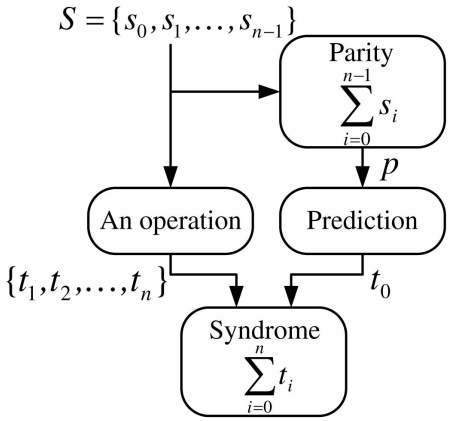

Fig. 1. The block diagram of CRC code error detection used in [11].

In [12], further improvement is done on protecting the linear modules. Instead of implementing CRC code error detection for each of the four linear modules separately, one single error detection is added for all the modules at once, as shown in Fig. 2. In this implementation, the linear compressor sums part of the round output (32-bit) to generate an 8-bit value, and the linear predictor generates an 8-bit signature for each 32-bit input. If these two 8-bit values do not match, an error is detected in the original linear computation module. [12] is actually a compressed and combined version of [11]. For every 32 bits, the scheme in [12] generates 8 bits for checking, while CRC $(5, 4)$ in [11] generates 1 extra bit for every 4 bits input for each linear module. We implement the scheme of [12] and denoted it as *Linear* in this paper, where the nonlinear module protection remains the same as in [11].

To improve the fault coverage, in [13], the authors proposed to use a new nonlinear error detection code and this method can significantly improve the fault coverage. Two cubic modules are added to increase the challenge for the attacker to inject a fault that can bypass the detection modules. We denote this method as *Robust* scheme in this paper.

Performance of various protection schemes has been evaluated and compared in previous works such as [1] and the metrics include fault coverage, execution time overhead, area and power overhead. In this paper, we choose several commonly used error detection schemes described above, implement them on an SASEBO-GII board [20,21], and analyze their side-channel power leakages in this paper. Note that the unprotected official implementation is from [22] with the S-Box implementation referred to [23,24,25]. For the induced error detection modules, we add them according to the details in [11,12,13] without modifying the original circuits. We sampled all the traces using an Agilent MSOX4104A oscilloscope with the AES system running at 3 MHz.

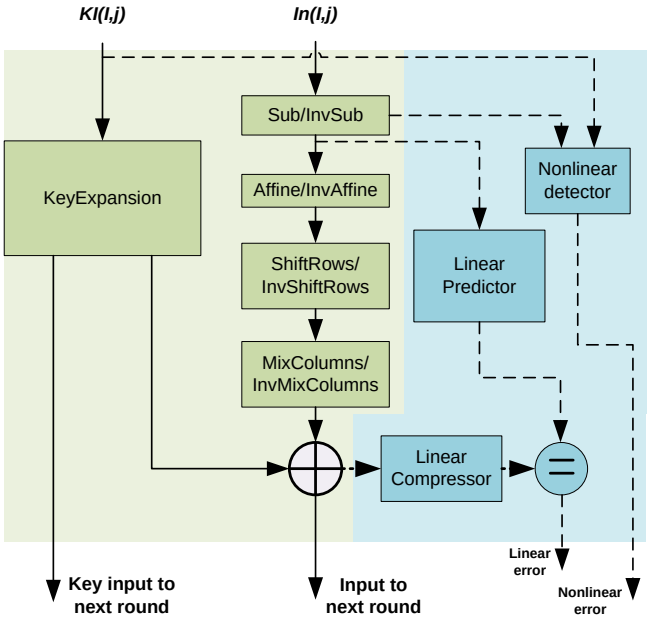

Fig. 2. *Linear* protection scheme of AES [12]

3 Power Leakage Model

For cryptographic devices, a commonly used linear Hamming-weight power leakage model is:

$$L = c + \epsilon V + \sigma r \tag{1}$$

where the power leakage L at a time point consists of a deterministic component and a random component. The deterministic power component is determined by the select function, $V = V(X, k_c)$, on the intermediate data Z that depends on the known input X and the secret key k_c. In many hardware systems, V is the Hamming weight (or distance) of Z. ϵ is the unit power consumption of one switching. The random power component is assumed to follow the Gaussian distribution, with a mean power c and a standard deviation σ. The constant mean power, c, is independent of both operations and data and represents the base level power consumption of the system. r is a standard Gaussian noise, $N(0, 1)$. σ represents the noise from both the measurement apparatus and other parts of the device that are not related to the intermediate data Z. The side-channel signal-to-noise ratio (SNR) is defined as $\delta = \epsilon/\sigma$ [26,27], which is a system-inherent side-channel leakage parameter.

Fig. 3 shows the hardware implementation of one AES round with protection circuits. Take the last round operation as example, at the edge of the 10^{th} round clock, the register's content is updated from D_{in} to D'_{in}. In the following cycle, the inputs to the combinational logic also change from D_{in} to D'_{in}, and will also incur extra power consumption in the error correction circuits with a possible delay comparing with the register's change.

For the AES hardware implementations without error detection circuits, V is the Hamming distance of the intermediate data stored in registers, denoted as $HW(D, D')$, in which D and D' are the content of the register before and after the clock edge. For the AES last round power analysis attack, the Hamming distance of register j, $(j = 0, 1, \cdots, 15)$ is:

$$HD_j = HD(SubBytes^{-1}(ShiftRows^{-1}(c_i \oplus k_i)), c_j) \tag{2}$$

in which c is the ciphertext and k is the last round key input while i and j are decided by the ShiftRows operation. We note here that the state register is divided into 16 bytes for power analysis in this paper.

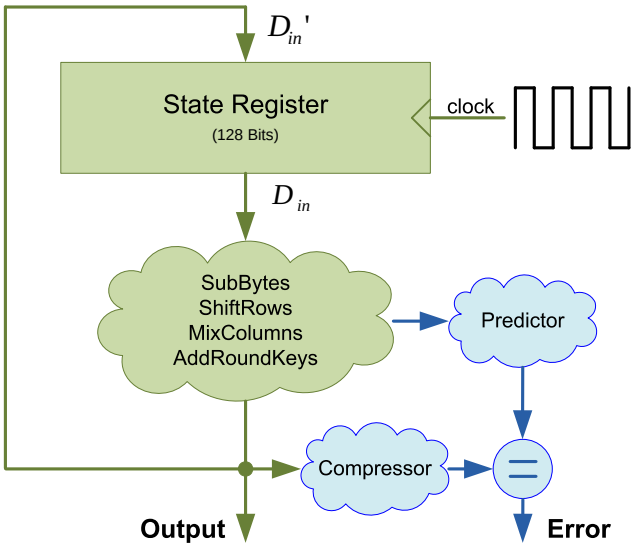

Fig. 3. Circuit model.

Simple error detection modules are mainly composed of combinational logic. To evaluate the power leakages of the error detection circuits, we assume the protection circuits incur extra noise and leakage and denote them as σ_d and ϵ_d, respectively, and the power model becomes:

$$L' = c + \epsilon V + \sigma r + c_d + \epsilon_d V + \sigma_d r = c' + \epsilon' V + \sigma' r \tag{3}$$

The new SNR is redefined as:

$$\delta = (\epsilon + \epsilon_d)/(\sigma + \sigma_d) = \epsilon'/\sigma'. \tag{4}$$

According to [27], the success rate (SR) of side-channel attacks and the number of traces needed for attack are directly determined by the SNR of a system. The addition of the protection circuits will therefore affect the SR of power analysis attacks on the protected AES. In Section 4.1, we will implement side-channel attacks based on power signals to verify the above assumptions.

4 Power Analysis Attacks on Protected AES Implementations

4.1 Side-Channel Attacks Results

In this section, we run CPA on the last round of the AES circuits with different protection circuits described in Section 2 and analyze the attack results. Besides *Duplicate*, *Linear*, *Robust*, *CRC8* and *CRC4* schemes described in Section 2, we denote the original AES implementation without protection circuits as *Original* and will use it as the baseline for comparison.

The above 6 schemes have different circuits and would incur different amount of side-channel power leakages. The CPA results are shown in Fig. 4. From the results we can see that:

- The SR curves of *Duplicate* and *Original* are very close. This is because the *Duplicate* scheme has another copy of every module in *Original* scheme. Both the leakage and noise are doubled and therefore the SNR is not changed.
- The SR curves of the other four schemes, *Linear*, *Robust*, *CRC4* and *CRC8*, are higher than the *Original* and *Duplicate* schemes. We therefore anticipate higher SNRs introduced by the protection circuits.

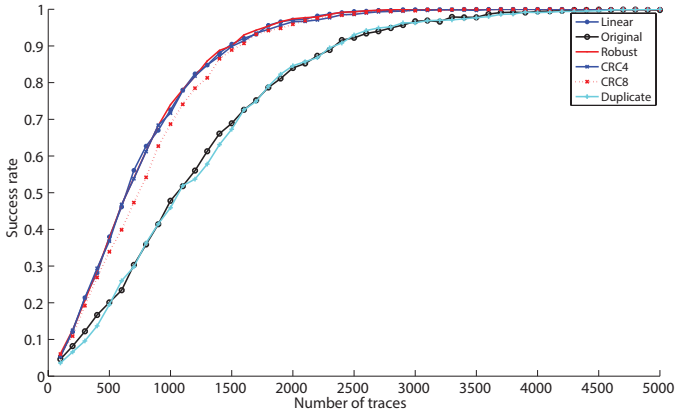

Fig. 4. Success rate of different protection implementations.

Table 1. Comparison between different protection schemes

Protection Schemes	FPGA implementation results (number)				ASIC implementation results		Fault Coverage	SNR	ϵ (10^{-5})
	Slice	Slice Regs	LUTs	LUT FFs	Area(um^2)	Power(mW)			
Original	872	748	2206	2481	13987.9	20.4	0%	0.0615	6.95
Duplicate	1341	742	3449	3760	25893.0	65.18	100%	0.0618	6.96
Linear	1303	744	3267	3558	18299.5	30.61	$90\% - 99\%$	0.0774	9.96
Robust	1578	764	3998	4308	36711.2	136.7	$1 - 2^{-56}$	0.0788	9.12
CRC4	1415	745	3436	3771	19504.5	52.01	$97.5\% - 100\%$	0.0771	9.03
CRC8	1503	764	3386	3735	19804.5	52.97	$97.5\% - 100\%$	0.0717	8.40

– The success rate of *CRC8* is a little lower than other three, *Linear*, *Robust* and *CRC4*. This is caused by the size of the protection circuits. For *CRC8*, the redundancy is 1 bit for each 8 bits while this ratio is 1 bit for each 4 bits in *Linear*, *Robust* and *CRC4* schemes. The compression rate of *CRC8* is higher and the width of the protection circuit is smaller. Thus the amount of additional leakage is smaller than the other protection circuits.

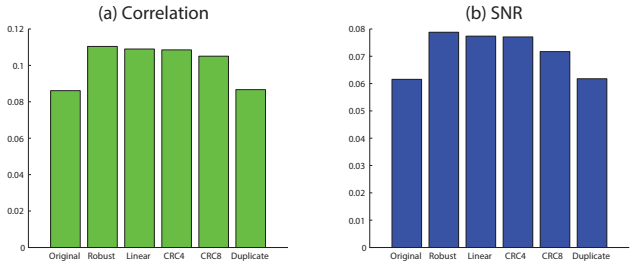

Fig. 5. Comparison of different protection implementations in terms of correlation, and SNR.

The above analysis can also be verified using the Pearson correlation and SNR results shown in Fig. 5(a), (b). The Pearson correlation factor is between the power measurements at the leakage point and the Hamming distances of the 16th byte of the last round state register calculated with $100,000$ traces. We run regression analysis on the power measurements using the model given in Equation (3)

and obtain the signal strength ϵ and noise level σ to calculate the SNR. Similarly, Fig. 5(a) and Fig. 5(b) show that the results can be categorized into three groups: *Original* and *Duplicate* schemes have the smallest correlation and SNR, *Linear*, *Robust* and *CRC4* schemes have the highest, and *CRC8* is in the middle.

While σ almost keeps the same for these schemes, the results of ϵ are presented in the last column of Table 1. ϵ in *Original* and *Duplicate* schemes are similar and much smaller than the value in *Linear*, *Robust* and *CRC4*, *CRC8*. *CRC8* has a smaller ϵ than the other three schemes. The ϵ results show that for the same number of switching activities, the dynamic power consumption is different for the above schemes. *CRC8* has lower dynamic power consumption at the leakage point because the width of its protection circuits is smaller than the other 3 schemes.

4.2 Metrics for the Selection of Protection Schemes

We also evaluate different protection methods in terms of power consumption, area, and fault coverage. We use Xilinx ISE 14.6 to implement the above 6 schemes and get the resource results shown in Table 1. The results include the number of slices, slice registers (slice Regs), slice look-up tables (LUTs) and the number of slice LUT-Flip Flop pairs (LUT FFs). To better understand the incurred extra power leakages, the six AES implementations (with or without protections) are also modeled in Verilog and synthesized in Cadence Encounter RTL Compiler with the NanGate 45nm Opencell library version v2009_07 [28]. The designs were placed and routed using Cadence Encounter. The power and area overhead of the protection schemes were estimated using Concurrent Current Source (CCS) model under typical operation conditions assuming a supply voltage of 1.1V and a temperature of 25 Celsius degree. The synthesis results for the schemes (area and power) are also shown in Table 1 and Fig. 6. The fault detection coverage results are from [1,11,12,13].

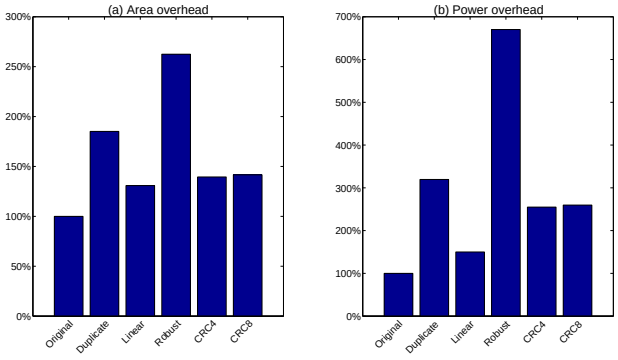

Fig. 6. ASIC implementation overhead comparison of protection schemes.

We note here that the implementations include control logic, interconnections and other overhead, thus the size of *Duplicate* is not just the double of *Original*. Meanwhile, the power includes both dynamic power and static power, thus the power consumption of *Robust* scheme is much higher than other schemes. We also note here that fault coverage results shown in Table 1 are based on random fault model, which means the faults are all randomly generated. For fault models in which the attackers can control the injected faults and injection positions, the fault coverage results will be very different, and *Robust* scheme will have much higher fault coverage than the other schemes.

The results show that no one is better than others in terms of all the design metrics. Take *Linear* and *Robust* protection schemes as example, they have similar side-channel power leakages, but the *Robust* scheme has higher fault detection coverage at the cost of more power and area than the *Linear* protection

scheme. For *CRC8* and *CRC4*, *CRC4* has a higher fault detection coverage and a little lower resource overhead, but also has a higher power leakage.

This demonstrates that no scheme dominates others, because one scheme can have a higher security level under one attacker models while has higher vulnerability under other attacker models. Therefore, when designing AES systems with protection, the trade-off among multiple aspects has to be explored so as to strike a balance between resource overhead, reliability, and side-channel attack resilience. At the same time, countermeasures against power analysis attacks can be applied to improve the side-channel resistance of the system. Countermeasures such as modified S-Box [29] and random masking [30,31] have been evaluated in previous papers and it's shown that they can effectively increase the difficulty of side-channel attacks.

5 Conclusion

This paper is motivated by the fact that protection circuits used to detect faults in cryptographic systems normally incur extra power consumption. Such power consumption may contain secret-related information, i.e., leakage, and results in increasing the vulnerability of cryptosystems against power analysis attacks. We analyze such extra power leakage, implement different protection schemes of the AES on FPGA, and run power based CPA attacks on them. The results show that protection circuits all increase the power leakage and the amount of leakage is related to the type of codes used and the number of checking bits of the protection circuits. Our analysis and experimental results provide guidelines for system designers to choose the best protection scheme, so as to meet requirements of multiple design considerations, including resource constraint, reliability, and resilience to both power analysis attacks and DFAs.

References

1. P. Maistri and R. Leveugle, "Double-data-rate computation as a countermeasure against fault analysis," *IEEE Transactions on Computers*, vol. 57, no. 11, pp. 1528–1539, Sept. 2008.
2. E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," in *Advances in CryptologyCRYPTO'97*. Springer, Aug. 1997, pp. 513–525.
3. G. Piret and J.-J. Quisquater, "A differential fault attack technique against SPN structures, with application to the AES and KHAZAD," in *Cryptographic Hardware & Embedded Systems*. Springer, Sept. 2003, pp. 77–88.
4. D. Saha, D. Mukhopadhyay, and D. R. Chowdhury, "A diagonal fault attack on the Advanced Encryption Standard," *IACR Cryptology ePrint Archive*, vol. 2009, p. 581, 2009.
5. A. Dehbaoui, J.-M. Dutertre, B. Robisson, P. Orsatelli, P. Maurine, and A. Tria, "Injection of transient faults using electromagnetic pulses-practical results on a cryptographic system," *IACR Cryptology ePrint Archive*, vol. 2012, p. 123, 2012.
6. S. Skorobogatov, "Synchronization method for SCA and fault attacks," *Cryptographic Engineering*, vol. 1, no. 1, pp. 71–77, April 2011.
7. R. Karri, G. Kuznetsov, and M. Goessel, "Parity-based concurrent error detection of substitution-permutation network block ciphers," in *Cryptographic Hardware & Embedded Systems*. Springer, Sept. 2003, pp. 113–124.
8. L. Breveglieri, I. Koren, and P. Maistri, "Incorporating error detection and online reconfiguration into a regular architecture for the advanced encryption standard," in *IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems*, Oct. 2005, pp. 72–80.
9. M. M. Kermani and A. Reyhani-Masoleh, "Parity-based fault detection architecture of S-box for advanced encryption standard," in *Defect & Fault Tolerance in VLSI Systems*. IEEE, Oct. 2006, pp. 572–580.
10. R. Karri, K. Wu, P. Mishra, and Y. Kim, "Concurrent error detection schemes for fault-based side-channel cryptanalysis of symmetric block ciphers," *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, vol. 21, no. 12, pp. 1509–1517, Nov. 2006.
11. C.-H. Yen and B.-F. Wu, "Simple error detection methods for hardware implementation of advanced encryption standard," *IEEE Transactions on Computers*, vol. 55, no. 6, pp. 720–731, June 2006.
12. M. Karpovsky, K. J. Kulikowski, and A. Taubin, "Differential fault analysis attack resistant architectures for the advanced encryption standard," in *Smart Card Research and Advanced Applications VI*. Springer, Aug. 2004, pp. 177–192.

13. ——, "Robust protection against fault-injection attacks on smart cards implementing the advanced encryption standard," in *2004 International Conference on Dependable Systems and Networks*. IEEE, June 2004, pp. 93–101.
14. M. Mozaffari-Kermani and A. Reyhani-Masoleh, "A low-power high-performance concurrent fault detection approach for the composite field S-box and inverse S-box," *IEEE Transactions on Computers*, vol. 60, no. 9, pp. 1327–1340, Sept. 2011.
15. ——, "Concurrent structure-independent fault detection schemes for the advanced encryption standard," *Computers, IEEE Transactions on*, vol. 59, no. 5, pp. 608–622, May 2010.
16. V. Maingot and R. Leveugle, "Error detection code efficiency for secure chips," in *13th IEEE International Conference on Electronics, Circuits and Systems*. IEEE, Dec. 2006, pp. 561–564.
17. F. Regazzoni, T. Eisenbarth, L. Breveglieri, P. Ienne, and I. Koren, "Can knowledge regarding the presence of countermeasures against fault attacks simplify power attacks on cryptographic devices?" in *IEEE International Symposium on Defect and Fault Tolerance of VLSI Systems*. IEEE, Oct. 2008, pp. 202–210.
18. F. Regazzoni, T. Eisenbarth, J. Grossschadl, and L. Breveglieri, "Power attacks resistance of cryptographic S-boxes with added error detection circuits," in *22nd IEEE International Symposium on Defect and Fault-Tolerance in VLSI Systems*. IEEE, Sept. 2007, pp. 508–516.
19. J. Dai and L. Wang, "A study of side-channel effects in reliability-enhancing techniques," in *24th IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems*. IEEE, Oct. 2009, pp. 236–244.
20. "Evaluation environment for side-channel attacks," http://www.risec.aist.go.jp/project/sasebo/.
21. A. Satoh, T. Katashita, and H. Sakane, "Secure implementation of cryptographic modules," *Development of a standard evaluation environment for side channel attacks. Synthesiology-English Edition*, vol. 3, no. 1, pp. 86–95, July 2010.
22. "AIST RCIS: SASEBO-GII," http://www.rcis.aist.go.jp/special/SASEBO/SASEBO-GII-en.html.
23. A. Satoh, S. Morioka, K. Takano, and S. Munetoh, "A compact rijndael hardware architecture with S-box optimization," in *ASIACRYPT 2001, Advances in Cryptology*. Springer, Dec. 2001, pp. 239–254.
24. D. Canright, "A very compact Rijndael S-box," DTIC Document, Tech. Rep., 2005.
25. E. N. Mui, R. Custom, and D. Engineer, "Practical implementation of Rijndael S-box using combinational logic," *Custom R&D Engineer Texco Enterprise Pvt. Ltd*, 2007.
26. S. Mangard, E. Oswald, and T. Popp, *Power analysis attacks: Revealing the secrets of smart cards*. Springer Publishing Company, 2010.
27. Y. Fei, Q. Luo, and A. A. Ding, "A statistical model for DPA with novel algorithmic confusion analysis," in *Cryptographic Hardware & Embedded Systems*. Springer, Sept. 2012, pp. 233–250.
28. "NanGate FreePDK45 Generic Open Cell Library," https://www.si2.org/openeda.si2.org/projects/nangatelib.
29. E. Oswald, S. Mangard, N. Pramstaller, and V. Rijmen, "A side-channel analysis resistant description of the AES S-box," in *Fast Software Encryption*. Springer, Feb. 2005, pp. 413–423.
30. A. Ding, L. Zhang, Y. Fei, and P. Luo, "A statistical model for higher order DPA on masked devices," in *Cryptographic Hardware and Embedded Systems CHES 2014*, 2014, vol. 8731, pp. 147–169.
31. M.-L. Akkar and C. Giraud, "An implementation of DES and AES, secure against some attacks," in *Cryptographic Hardware & Embedded Systems*. Springer, May 2001, pp. 309–318.