Implications of Noise Insertion Mechanisms of Different Countermeasures Against Side-Channel Attacks

Weize Yu
Department of Electrical Engineering
University of South Florida
Tampa, Florida 33620
Email: weizeyu@mail.usf.edu

Selçuk Köse
Department of Electrical Engineering
University of South Florida
Tampa, Florida 33620
Email: kose@usf.edu

***Abstract*—In this paper, the security implications of the noise insertion characteristics of different countermeasures against power analysis attacks are investigated. Through optimizing the selection of the type and sequence of the inserted noise, the security of a cryptographic circuit that has multiple countermeasures with varying noise insertion mechanisms can be improved. As demonstrated in this work, if the additive non-white noise and multiplicative noise are sequentially inserted into a cryptographic circuit, the correlation coefficient between the actual power dissipation of the cryptographic circuit and monitored power dissipation can be reduced over 37.6% under the same amount of inserted noise.**

I. Introduction

Power analysis attacks (PAA) can be quite effective to obtain the secret keys from cryptographic circuits with a high success rate and low cost [1], [9-11]. Various countermeasures [2-7,14,15] have been proposed against PAA that inject noise into the power profile of cryptographic circuits. The injected power noise can be categorized into two general types: multiplicative noise (MN) and additive noise (AN). Although these two noise insertion mechanisms have been extensively studied individually, to the best of the authors' knowledge, literature seldom exploited the impact of different implementations of multiple noise insertion mechanisms to further improve the security of cryptographic circuits against PAA.

Dynamic power dissipation P_d of a cryptographic circuit can be denoted as $P_d = \alpha f_c V_{dd}^2$ where f_c is the clock frequency, V_{dd} is the supply voltage, and α is the input data dependent parameter [7]. Some examples of the countermeasures that insert multiplicative noise to scramble the power consumption profile are the voltage/frequency scaling based countermeasures [12,13]. Countermeasures such as random dynamic voltage and frequency scaling (RDVFS) [5], random dynamic voltage scaling (RDVS) [6], and aggressive voltage and frequency scaling (AVFS) [7] have been proposed to insert multiplicative power noise into the cryptographic circuit by randomly altering the clock frequency or supply voltage. Alternatively, two types of additive power noise can be inserted into the power profile of a CC. When extra power is consumed to insert power noise to side-channel signature such by utilizing random power grids [2] as shown in Fig. 1(a), the inserted power noise would have a non-zero mean value and therefore can be categorized as non-white noise. As shown in Fig. 1(b), when a circuit component such as an on-chip decoupling capacitor is used to store a portion of the charge from the power supply and randomly discharge the energy to the cryptographic circuit in the next couple of cycles [3, 4], the inserted additive noise can be categorized as white noise due to the zero mean value. Please note that some of the existing countermeasures are orthogonal to each other can therefore can be implemented seamlessly together to increase the security of an integrated circuit.

In this paper, a cryptographic circuit that houses two orthogonal countermeasures with different noise insertion mechanisms is studied. After optimizing the type and sequence of the noise insertion, it is statistically demonstrated that the correlation coefficient between the actual power consumption and the monitored side-channel power can be decreased over 37.6%.

The rest of the paper is organized as follows. The effects of different noise insertion mechanisms on the power dissipation profile are investigated in Section II. The security evaluation and comparison of combining different countermeasures are discussed in Section III. Conclusions are provided in Section IV.

II. Monitored power dissipation of a cryptographic circuit (CC) with different noise insertion mechanisms

As mentioned in the *Introduction*, countermeasures can generate and insert three different types of noise to a cryptographic circuit: multiplicative noise (MN), additive white noise (AWN), and additive non-white noise (ANWN). If two noise insertion mechanisms are used sequentially to inject

This work is supported in part by the National Science Foundation CAREER award under Grant CCF-1350451, by a Cisco Research Award, and by a seed grant from Florida Center for Cybersecurity.

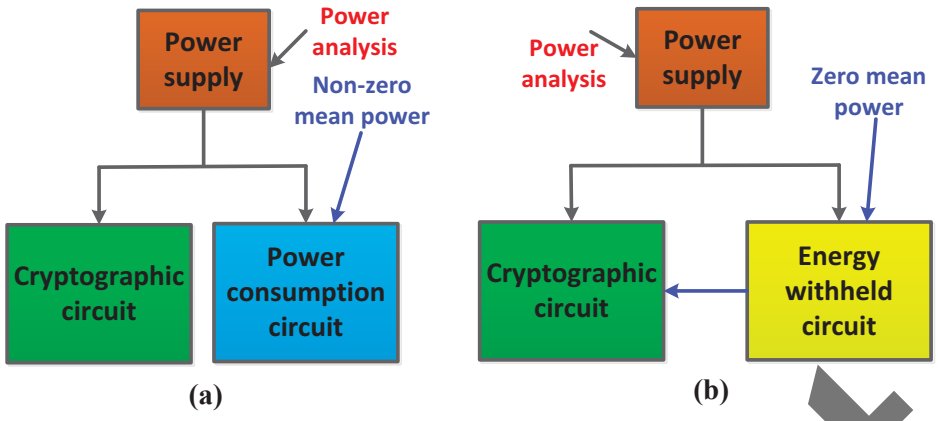

Fig. 1. Two types of additive power noise. (a) Additive non-white noise (ANWN). (b) Additive white noise (AWN).

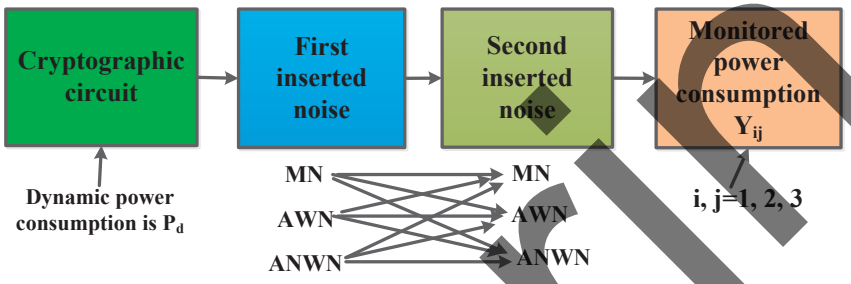

Fig. 2. Implementation of two noise insertion mechanisms into a CC. There are nine different noise implementations. First inserted noise/second inserted noise: MN/MN, MN/AWN, MN/ANWN, AWN/MN, AWN/AWN, AWN/ANWN, ANWN/MN, ANWN/AWN, and ANWN/ANWN.

noise into a cryptographic circuit, as shown in Fig. 2, there are nine different realizations of the resulting noise profile. Since both the dynamic power consumption and power noise of a cryptographic circuit conform to a normal distribution [8], the dynamic power consumption P_d of the cryptographic circuit can be written as

$$P_d = \mu_0 + \hat{P}_d, \tag{1}$$

where μ_0 is the mean value of the dynamic power consumption and $\hat{P}_d$ represents the power variation of the CC. If two independent MNs are inserted into a CC, the total monitored power dissipation Y_{11} can be denoted as

$$\begin{aligned} Y_{11} &= a_{21} \times a_{11} \times P_d = (\mu_{21} + \hat{a}_{21}) \times (\mu_{11} + \hat{a}_{11}) \times \\ &(\mu_0 + \hat{P}_d) = \mu_0\mu_{11}\mu_{21} + \mu_0(\mu_{11}\hat{a}_{21} + \mu_{21}\hat{a}_{11} + \hat{a}_{11}\hat{a}_{21}) \\ &+ (\mu_{11}\mu_{21} + \mu_{11}\hat{a}_{21} + \mu_{21}\hat{a}_{11} + \hat{a}_{11}\hat{a}_{21})\hat{P}_d, \end{aligned} \tag{2}$$

where a_{11} and a_{21}, respectively, represent the first and second injected MN signals, as listed in Table 1. μ_{11} (μ_{21}) and $\hat{a}_{11}$ ($\hat{a}_{21}$) are, respectively, the mean and variation of the first (second) inserted MN.

When an MN and AN are inserted into a CC, four different implementations can be chosen, as listed in Table 1. The corresponding monitored power dissipation for these four

TABLE I
MONITORED POWER DISSIPATION OF A CRYPTOGRAPHIC CIRCUIT WITH DIFFERENT NOISE INSERTION MECHANISMS AND SEQUENCE $(Y_{ij}, (i, j = 1, 2, 3))$.

First / Second	MN $\times a_{11}$	AWN $+ b_{11}$	ANWN $+ b_{12}$
MN $\times a_{21}$	Y_{11}	Y_{12}	Y_{13}
AWN $+ b_{21}$	Y_{21}	Y_{22}	Y_{23}
ANWN $+ b_{22}$	Y_{31}	Y_{32}	Y_{33}

implementations (Y_{12}, Y_{13}, Y_{21}, and Y_{31}) can be expressed as follows

$$\begin{aligned} Y_{12} &= a_{21} \times (P_d + b_{11}) = (\mu_{21} + \hat{a}_{21}) \times (\mu_0 + \hat{P}_d + \hat{b}_{11}) \\ &= \mu_0\mu_{21} + \hat{a}_{21}\mu_0 + \hat{a}_{21}\hat{b}_{11} + \mu_{21}\hat{b}_{11} + (\hat{a}_{21} + \mu_{21})\hat{P}_d, \end{aligned} \tag{3}$$

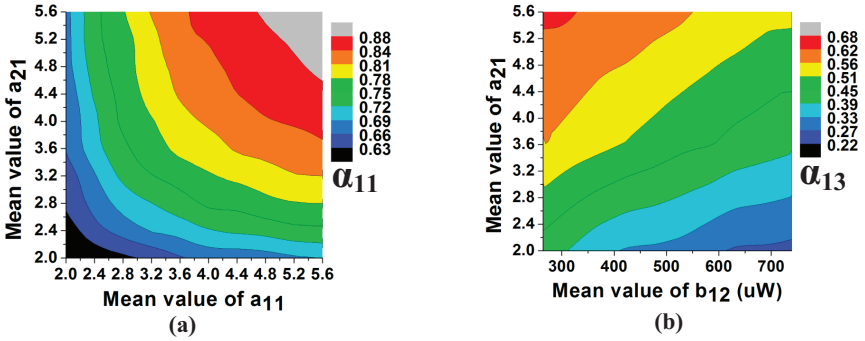

Fig. 3. Correlation coefficients (α_{11} and α_{13}) versus the mean value of the inserted noise (In (a) and (b), different colors represent different correlation coefficient values).

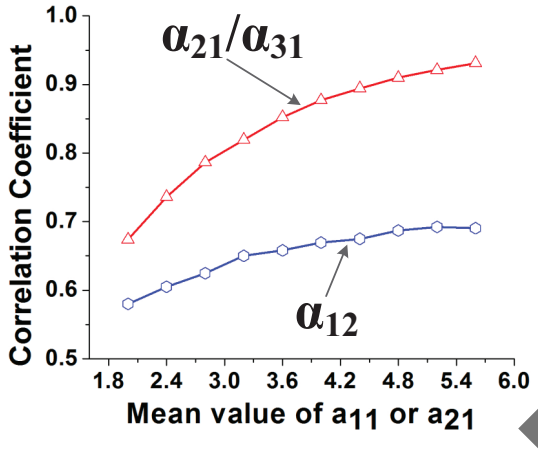

Fig. 4. Correlation coefficients (α_{12}, α_{21} and α_{31}) versus the mean value of the inserted noise.

$$Y_{13} = a_{21} \times (P_d + b_{12}) = (\mu_{21} + \hat{a}_{21}) \times (\mu_0 + \hat{P}_d + \beta_1 + \hat{b}_{11}) = \mu_{21}\mu_0 + \mu_{21}\beta_1 + \mu_{21}\hat{b}_{11} + \hat{a}_{21}\mu_0 + \hat{a}_{21}\beta_1 + \hat{a}_{21}\hat{b}_{11} + (\mu_{21} + \hat{a}_{21})\hat{P}_d, \quad (4)$$

$$Y_{21} = a_{11} \times P_d + b_{21} = (\mu_{11} + \hat{a}_{11}) \times (\mu_0 + \hat{P}_d) + \hat{b}_{21} = \mu_0\mu_{11} + \hat{b}_{21} + \mu_0\hat{a}_{11} + (\mu_{11} + \hat{a}_{11})\hat{P}_d, \quad (5)$$

$$Y_{31} = a_{11} \times P_d + b_{22} = (\mu_{11} + \hat{a}_{11}) \times (\mu_0 + \hat{P}_d) + \beta_2 + \hat{b}_{21} = \mu_0\mu_{11} + \beta_2 + \hat{b}_{21} + \mu_0\hat{a}_{11} + (\mu_{11} + \hat{a}_{11})\hat{P}_d, \quad (6)$$

where b_{11} (b_{12}) and b_{21} (b_{22}) are, respectively, the first and second inserted AWNs (ANWNs). $\hat{b}_{lk}, (l, k = 1, 2)$ is the corresponding variation of the inserted noise and $\beta_1(\beta_2)$ is the mean value of the first (second) inserted ANWN ($b_{l2} = \beta_l + \hat{b}_{l1}$).

When two independent ANs are injected into a CC, as listed in Table 1, the corresponding monitored power dissipation (Y_{22}, Y_{23}, Y_{32}, and Y_{33}) becomes

$$Y_{22} = P_d + b_{11} + b_{21} = \mu_0 + \hat{b}_{11} + \hat{b}_{21} + \hat{P}_d, \quad (7)$$

$$Y_{23} = P_d + b_{12} + b_{21} = \mu_0 + \beta_1 + \hat{b}_{11} + \hat{b}_{21} + \hat{P}_d, \quad (8)$$

$$Y_{32} = P_d + b_{11} + b_{22} = \mu_0 + \beta_2 + \hat{b}_{11} + \hat{b}_{21} + \hat{P}_d, \quad (9)$$

$$Y_{33} = P_d + b_{12} + b_{22} = \mu_0 + \beta_1 + \beta_2 + \hat{b}_{11} + \hat{b}_{21} + \hat{P}_d. \quad (10)$$

III. Security Evaluation

A 130nm CMOS cryptographic substitution-box (S-box) is designed and simulated in Cadence. The corresponding mean value and the standard deviation of the dynamic power consumption of the S-box are, respectively, 264 uW and 26.8 uW. The correlation coefficient between the actual power consumption and monitored power dissipation is a widely used security metric [6-8]. The correlation coefficient $\alpha_{ij}, (i, j = 1, 2, 3)$ between the actual power consumption P_d of the S-box and monitored power consumption Y_{ij} is statistically simulated in Matlab.

When the mean value of the multiplicative noise a_{11} or a_{21} increases, the correlation coefficient $\alpha_{11}/\alpha_{12}/\alpha_{13}/\alpha_{21}/\alpha_{31}$ would also increase, as shown in Fig. 3 and Fig. 4. The intuitive explanation is that the mean value of the multiplicative noise has a positive impact on amplifying the power variation $\hat{P}_d$ of the CC, as derived in (2)-(6). However, if the mean value of the additive noise b_{12} increases, the correlation coefficient α_{13} would decrease. The reduction in α_{13} is induced by multiplying the non-zero mean of ANWN with an MN noise that increases the effect of the ANWN, as derived in (4). Additionally, since the mean value of the additive noise b_{12} and b_{22} has no impact on the variation of $Y_{23}/Y_{32}/Y_{33}$, as shown in (8)-(10), the correlation coefficients $\alpha_{23}/\alpha_{32}/\alpha_{33}$ would not be affected by the mean value of additive noise [8].

As shown in Fig. 5, if the standard deviation of the multiplicative noise a_{11}/a_{21} or the additive noise $b_{11}/b_{12}/b_{21}/b_{22}$ increases, the correlation coefficient α_{ij} would reduce, meaning that the standard deviation of noise has a positive impact on enhancing the role of noise in a cryptographic circuit when two different noise profiles are sequentially inserted. The correlation coefficient α_{13} exhibits the lowest value among all the correlation coefficients under the same amount of inserted noise. The reason is that the impact of the additive noise b_{12} can be further utilized by the multiplicative noise a_{21} to form another additive noise $\hat{a}_{21}\beta_1$ that decreases the

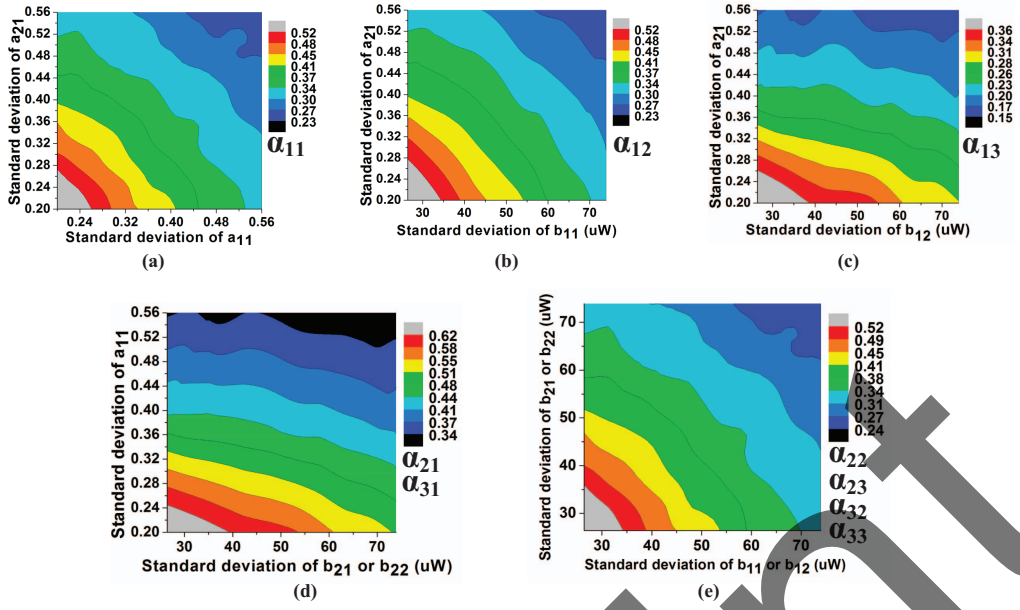

Fig. 5. Correlation coefficient $\alpha_{ij}, (i, j = 1, 2, 3)$ versus the standard deviation of the inserted noise (The standard deviation is normalized with the same ratio of mean value for both MN and ANWN).

correlation coefficient α_{13}, as shown in (4). Additionally, correlation coefficients α_{21} and α_{31} are the highest among all the correlation coefficients under the same amount of inserted noise. The intuitive reason is that the impact of the additive noise b_{21} or b_{22} is limited when inserted after the multiplicative noise, as shown in (5)-(6). Through optimizing the type and sequence of the noise insertion, the correlation coefficient between the actual and monitored power consumption of a cryptographic circuit can be reduced over 37.6%, as shown in Fig. 5.

IV. Conclusion

Security implications of the noise insertion characteristics of different countermeasures against power analysis attacks are explored in this paper. Increasing the mean value of the multiplicative noise has a negative impact on enhancing the security of a cryptographic circuit in the presence of two noise insertion mechanisms, whereas increasing the mean value of the additive noise may have a positive effect on improving the security. Through optimizing the type and sequence of the noise insertion, the correlation coefficient between the actual power consumption and monitored power consumption can be reduced over 37.6% under the same amount of inserted noise.

References

[1] S. Mangard, E. Oswald, and T. Popp, "Power analysis attacks revealing the secrets of smart cards (advances in information security)," Springer, New York, 2007.

[2] X. Wang, W. Yueh, D. B. Roy, S. Narasimhan, Y. Zheng, S. Mukhopadhyay, D. Mukhopadhyay, and S. Bhunia, "Role of power grid in side channel attack and power-grid-aware secure design," *in Proc. Design Automation Conference (DAC)*, Jun. 2013, pp. 1-9.

[3] W. Yu and S. Köse, "Charge-withheld converter-reshuffling (CoRe): A countermeasure against power analysis attacks," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 63, no. 5, pp. 438-442, May 2016.

[4] M. Mayhew and R. Muresan, "On-chip nanoscale capacitor decoupling architectures for hardware security," *IEEE Transactions on Emerging Topics in Computing*, vol. 2, no. 1, pp. 4-15, Mar. 2014.

[5] S. Yang, W. Wolf, N. Vijaykrishnan, D. N. Serpanos, and Y. Xie, "Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach," *in Proc. Design, Automation and Test in Europe (DATE)*, Mar. 2005, pp. 64-69.

[6] K. Baddam and M. Zwolinski, "Evaluation of dynamic voltage and frequency scaling as a differential power analysis attacks," *in Proc. VLSI design*, Jan. 2007, pp. 854-862.

[7] N. D. P. Avirneni and A. K. Somani, "Countering power analysis attacks using reliable and aggressive designs," *IEEE Transactions on Computers*, vol. 63, no. 6, pp. 1408-1420, Jun. 2014.

[8] F.-X. Standaert, E. Peeters, G. Rouvroy, and J.-J. Quisquater, "An overview of power analysis attacks against field programmable gate arrays," *Proceedings of the IEEE*, vol. 94, no. 2, Feb. 2006.

[9] M. Alioto, L. Giancane, G. Scotti, and A. Trifiletti, "Leakage power analysis attacks: A novel class of attacks to nanometer cryptographic circuits," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 57, no. 2, pp. 355-367, Feb. 2010.

[10] D. D. Huang, K. Tiri, A. Hodjat, B.-C. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "AES-based security coprocessor IC in 0.18-um CMOS with resistance to differential power analysis side-channel attacks," *IEEE Journal of Solid-State Circuits*, vol. 41, no. 4, pp. 781-791, Apr. 2006.

[11] M. Avital, H. Dagan, I. Levi, O. Keren, and A. Fish, "DPA-secured quasiadiabatic logic (SQAL) for low-power passive RFID tags employing S-boxes," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 62, no. 1, pp. 149-156, Jan. 2015.

[12] W. Yu and S. Köse, "Exploiting Voltage Regulators to Enhance Various Power Attack Countermeasures," *IEEE Transactions on Emerging Topics in Computing*, (in press).

[13] W. Yu and S. Köse, "Security-Adaptive Voltage Conversion as a Lightweight Countermeasure Against LPA Attacks," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, (in press).

[14] W. Yu and S. Köse, "A Voltage Regulator-Assisted Lightweight AES Implementation Against DPA Attacks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, no. 8, pp. 1152–1163, August 2016.

[15] W. Yu and S. Köse, "Time-Delayed Converter-Reshuffling: An Efficient and Secure Power Delivery Architecture," *IEEE Embedded Systems Letters*, vol. 7, no. 3, pp. 73–76, September 2015.