Implications of noise insertion mechanisms of different countermeasures against side-channel attacks

Journal:	*Electronics Letters*
Manuscript ID	ELL-2016-0480
Manuscript Type:	Letter
Date Submitted by the Author:	09-Feb-2016
Complete List of Authors:	Yu, Weize; University of South Florida, Electrical Engineering Kose, Selcuk; University of SOuth Florida, Electrical Engineering
Keywords:	SECURITY
Note: The following files were submitted by the author for peer review, but cannot be converted to PDF. You must view these files (e.g. movies) online.	
EL-Yu-kose.rar	

Implications of noise insertion mechanisms of different countermeasures against side-channel attacks

Weize Yu and Selçuk Köse

In this letter, 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 noise insertion mechanisms can be improved. As demonstrated in this work, if the additive non-white noise and multiplicative noise are inserted into a cryptographic circuit sequentially, 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.

Introduction: Power analysis attacks (PAA) can be quite effective to obtain the secret keys from cryptographic circuits (CCs) with a high success rate and low cost [1]. Various countermeasures [2-7] have been proposed against PAA that inject noise into the power profile of CCs. 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 our knowledge, literature seldom exploited the impact of different implementations of multiple noise insertion mechanisms to further improve the security of CCs against PAA.

Dynamic power dissipation P_d of a CC 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]. Techniques 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 CC 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 in side-channel 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 charge from the power supply and randomly discharge the energy to the CC in the next couple of cycles [3, 4], the inserted additive noise can be categorized as white noise due to the zero mean value.

In this letter, a CC that houses two 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%.

Monitored power dissipation of a cryptographic circuit (CC) with different noise insertion mechanisms: As mentioned in *Introduction*, three different types of noise: multiplicative noise (MN), additive white noise (AWN), and additive non-white noise (ANWN) can be inserted into a CC. If two noise insertion mechanisms are used sequentially to inject noise into a CC, 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 CC conform to a normal distribution [8], the dynamic power consumption P_d of the CC 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.

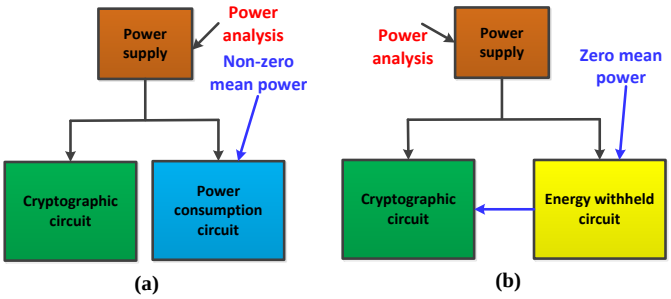

Fig. 1 *Two types of additive power noise. (a) Additive non-white noise (ANWN). (b) Additive white noise (AWN).*

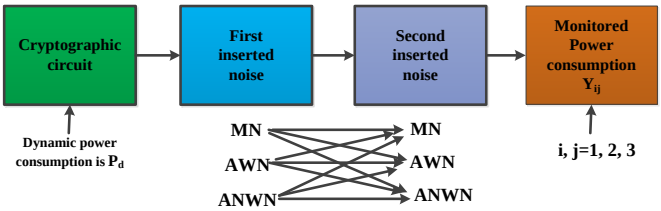

Fig. 2 *Implementation of two noise insertion mechanisms into a CC. There are nine different noise implementations. First inserted noise/second inserted noise: MN/MN, MN/AWN, MN/ANWN, AWN/MN, AWN/AWN, AWN/ANWN, ANWN/MN, ANWN/AWN, and ANWN/ANWN.*

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

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

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

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

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

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

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

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

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

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

Security Evaluation: A 130nm CMOS cryptographic 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.

Table 1: Monitored power dissipation of a CC with different noise insertion mechanisms and sequence ($Y_{ij}, (i,j=1,2,3)$).

First / Second	MN × a_{11}	AWN + b_{11}	ANWN + b_{12}
MN × 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}

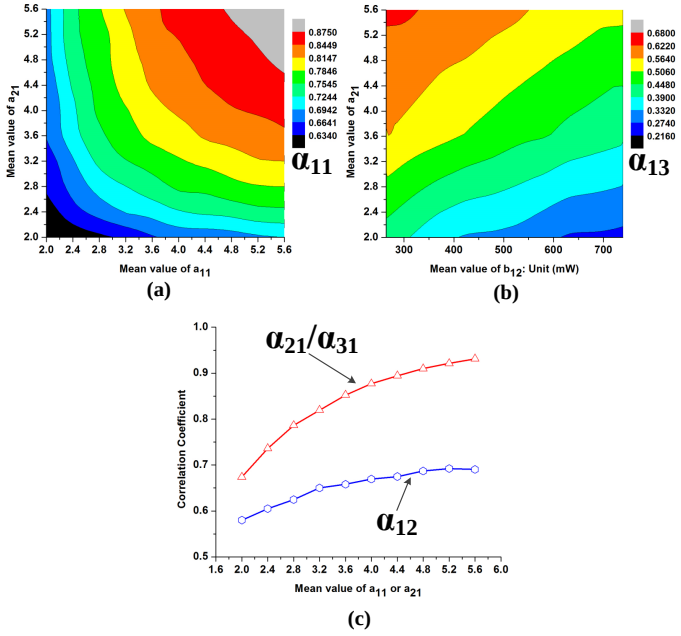

Fig. 3 *Correlation coefficients ($\alpha_{11}, \alpha_{12}, \alpha_{13}, \alpha_{21}$, and α_{31}) versus the mean value of the inserted noise (In (a) and (b), different colors represent different correlation coefficient values).*

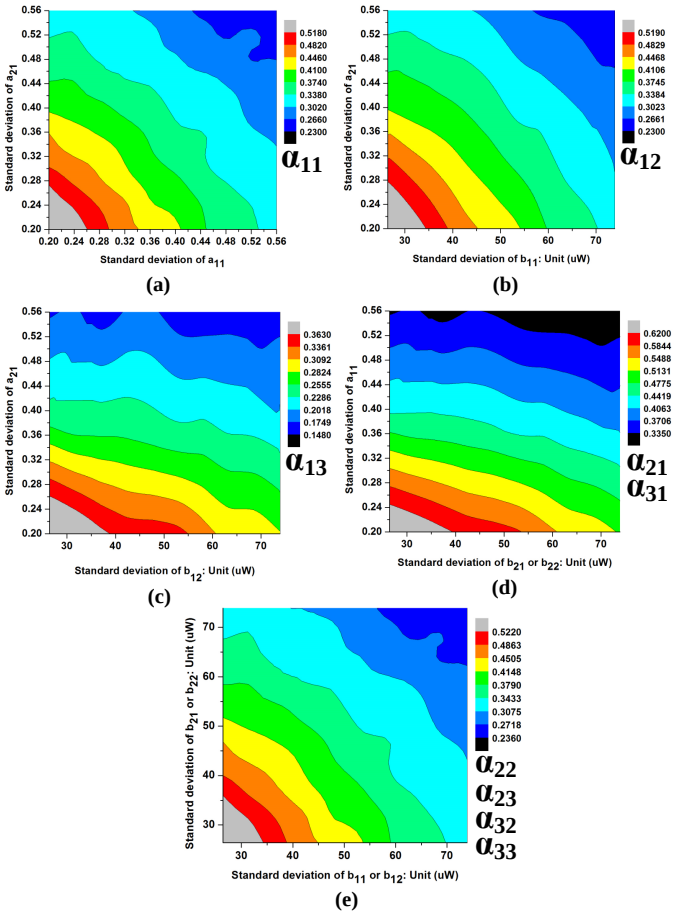

Fig. 4 *Correlation coefficient $\alpha_{ij}, (i,j=1,2,3)$ versus the standard deviation of the inserted noise (The standard deviation is normalized with the same ratio of mean value for both MN and ANWN).*

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. 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. 4, 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 CC 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 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 CC can be reduced over 37.6%, as shown in Fig. 4.

Conclusion: Security implications of the noise insertion characteristics of different countermeasures against power analysis attacks are explored in this letter. Increasing the mean value of the multiplicative noise has a negative impact on enhancing the security of a CC 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.

Acknowledgment: This work was supported in part by the National Science Foundation CAREER award under Grant no. CCF-1350451.

Weize Yu and Selçuk Köse (*Department of Electrical Engineering, University of South Florida, 4202 E. Fowler Avenue, Tampa, FL 33620, United States*)

E-mail: weizeyu@mail.usf.edu

References

1 Mangard, S., Oswald, E., and Popp, T.: 'Power analysis attacks revealing the secrets of smart cards (advances in information security)' (Springer, New York, 2007)

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

3 Yu, W., and Köse, S.: 'Charge-withheld converter-reshuffling (CoRe): A countermeasure against power analysis attacks', *IEEE Trans. Circuits Syst.-2: Express Briefs*, in early access

4 Mayhew, M., and Muresan, R.: 'On-chip nanoscale capacitor decoupling architectures for hardware security', *IEEE Trans. Emer. Topics Comput.*, 2014, **2**, (1), pp. 4-15

5 Yang, S., Wolf, W., Vijaykrishnan, N., Serpanos, D.-N., and Xie, Y.: 'Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach'. Proc. Design, Automation and Test in Europe, March 2005, pp. 64-69

6 Baddam, K., and Zwolinski, M.: 'Evaluation of dynamic voltage and frequency scaling as a differential power analysis attacks'. Proc. VLSI design, January 2007, pp. 854-862

7 Avirneni, N.-D.-P., and Somani, A.-K.: 'Countering power analysis attacks using reliable and aggressive designs', *IEEE Trans. Comput.*, 2014, **63**, (6), pp. 1408-1420

8 Standaert, F.-X., Peeters, E., Rouvroy, G., and Quisquater, J.-J.: 'An overview of power analysis attacks against field programmable gate arrays', *Proc. IEEE*, 2006, **94**, (2), pp. 383-394