False Key-Controlled Aggressive Voltage Scaling: A Countermeasure Against LPA Attacks

Weize Yu and Selçuk Köse, *Member, IEEE*

***Abstract*—A false key-controlled aggressive voltage scaling (AVS) technique is proposed as a countermeasure against leakage power analysis (LPA) attacks. A random number of false keys are utilized to control the supply voltage scaling to mask the possible leakage of the information related to the correct key to a malicious attacker. Contrary to the random AVS technique, false key-controlled AVS technique can guarantee that the added false keys always exhibit higher correlation coefficients than that of the correct key even if sufficient number of plaintexts (>10 million) are enabled. As demonstrated with the simulation results, the measurement-to-disclose (MTD) value of a cryptographic circuit can be enhanced over ten million against LPA attacks by utilizing the proposed technique, while the MTD values of a conventional cryptographic circuit without countermeasure and one with random AVS are, respectively, less than 500 and 100,000.**

***Index Terms*—Aggressive voltage scaling (AVS), false-key controlled, leakage power analysis attacks, measurement-to-disclose (MTD).**

I. Introduction

The critical information in modern integrated circuits can be leaked to a malicious attacker through power analysis attacks [1]–[3], [12]. Leakage power analysis (LPA) attacks are successfully implemented on cryptographic circuits in circuit level simulations [4]. However, when executed against an actual circuit (i.e., field-programmable gate array), LPA attacks seem to be ineffective [5]. The main reason is that the amplitude of the leakage power dissipation of a cryptographic circuit is typically quite lower than the dynamic power dissipation. The measurement noise therefore becomes more critical in LPA attacks, possibly making LPA attacks inefficient [5]. The measurement noise can, however, be filtered by utilizing techniques such as average sampling analysis. LPA attacks can therefore become effective if the attacker has the ability to significantly lower the operating frequency of the cryptographic circuit to perform average sampling analysis [6].

In a practical LPA attack, the correct key is typically determined based on the correlation coefficient between the predicted leakage power dissipation and actual leakage power dissipation after applying a sufficient number of plaintexts to the cryptographic circuit (i.e., the highest correlation coefficient corresponds to the correct key). Therefore, if a countermeasure can guarantee that the correlation coefficients of the false keys are always higher than the correlation coefficient of the correct key even after sufficient number of plaintexts are applied, the potential threats from LPA attacks can be eliminated.

Manuscript received October 17, 2016; revised January 5, 2017 and February 23, 2017; accepted March 3, 2017. Date of publication March 14, 2017; date of current version November 20, 2017. This work was supported in part by the National Science Foundation CAREER Award under Grant CCF-1350451, in part by the USF Presidential Fellowship, and in part by the Cisco Systems Research Award. This paper was recommended by Associate Editor S. Bhunia.

The authors are with the Department of Electrical Engineering, University of South Florida, Tampa, FL 33620 USA (e-mail: weizeyu@mail.usf.edu; kose@usf.edu).

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/TCAD.2017.2682113

Zhu *et al.* [11] proposed symmetric dual-rail logic (SDRL) as a countermeasure against LPA attacks. A cryptographic circuit built with SDRL can achieve an approximately constant leakage power dissipation under different input data. However, this countermeasure would double both the power consumption and the area of the cryptographic circuit since the SDRL requires more area than the conventional CMOS gates and consumes more power to flatten the input power profile. Random dynamic voltage and frequency scaling (RDVFS) with switched-capacitor voltage converters was proposed in [7] as a countermeasure against LPA attacks since the leakage power dissipation of a cryptographic circuit strongly correlates with the supply voltage. However, the power noise generated by randomly altering the supply voltage level can be filtered by an attacker by increasing the number of measurements.

An adaptive false key-controlled aggressive voltage scaling (AVS) is proposed as a countermeasure against LPA attacks. When LPA attacks are sensed by a cryptographic circuit, the input plaintexts are added to a false key to generate a signal that controls the supply voltage scaling. Since supply voltage strongly correlates with the actual leakage power dissipation of a cryptographic circuit [7], there is a strong correlation between the added false key and actual leakage power dissipation. If the correlation coefficient of the added false key is higher than the correlation coefficient of the correct key, the attacker may regard the added false key as the correct key.

Since the single added false key strongly correlates with the scaling behavior of the supply voltage, if the attacker realizes that the key with the highest correlation coefficient is the added false key and utilizes the added false key to unriddle the scaling behavior of the supply voltage, the correct key can still be leaked to attacker. To further scramble the leakage power trace, a random number of false keys are added to the plaintexts in every clock period to prevent the attacker from unriddling the supply voltage scaling pattern.

The rest of this paper is organized as follows. The basic architecture of the proposed false key-controlled AVS technique is introduced in Section II. LPA attacks are modeled and the security evaluation of the proposed technique is analyzed in Sections III and IV, respectively. LPA attack simulations are demonstrated in Section V. Overhead discussions and comparison with previous works are provided, respectively, in Section VI and Section VII. Conclusions are offered in Section VIII.

II. Proposed False Key-Based Countermeasure

A. Architecture of Single False Key-Controlled Aggressive Voltage Scaling

The basic architecture of the SFKC AVS technique is shown in Fig. 1. The n-bit input plaintext $A = (a_1, a_2, \ldots, a_n)_2$ is added to the correct key $K_c = (k_{c,1}, k_{c,2}, \ldots, k_{c,n})_2$ to generate the input data of the cryptographic circuit $X^I = (x_1^I, x_2^I, \ldots, x_n^I)_2$. If the cryptographic circuit is under an LPA attack, the attacker lowers the clock frequency f_c to mitigate the measurement noise [6]. When the clock frequency

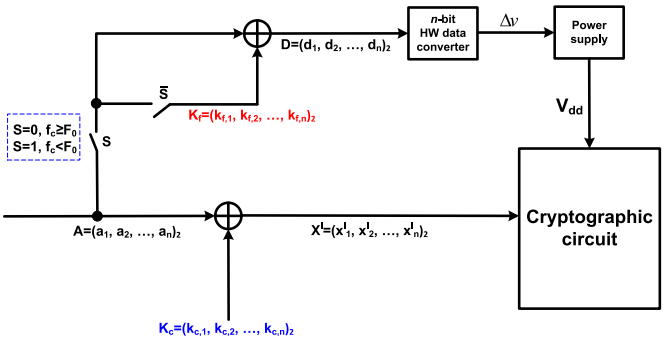

Fig. 1. Basic architecture of the proposed SFKC AVS technique ($S = 0$ represents the switch S is in off-state and the complementary switch $\overline{S}$ is in on-state, and vice versa).

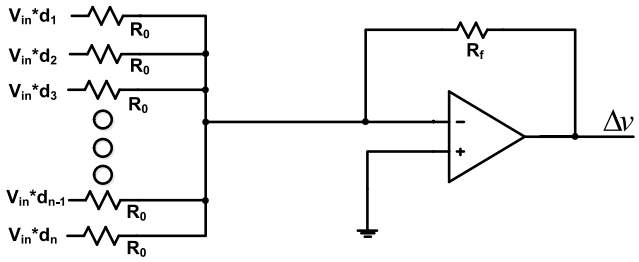

Fig. 2. Circuit schematic of n-bit HW data converter.

f_c is lowered below the critical clock frequency F_0,[1] the switch S is turned-on and the complementary switch $\overline{S}$ is turned-off. As a result, the input plaintext $A = (a_1, a_2, \ldots, a_n)_2$ is also added to the false key $K_f = (k_{f,1}, k_{f,2}, \ldots, k_{f,n})_2$ to generate the false key related data $D = (d_1, d_2, \ldots, d_n)_2$, $(D = A \oplus K_f)$. As illustrated in Fig. 1, the digital false key related data D is converted into an analog voltage signal Δv by an n-bit hamming-weight (HW) data converter.

Circuit schematic of the n-bit HW data converter is shown in Fig. 2. The relationship between input data D and output voltage Δv of the HW data converter can be written as

$$\Delta v = \left(\sum_{i=1}^{n} d_i\right) \times \left(-\frac{V_{\text{in}} R_f}{R_0}\right) = \left(\sum_{i=1}^{n} d_i\right) v_0 = \left(\sum_{i=1}^{n} a_i \oplus k_{f,i}\right) v_0 \quad (1)$$

where V_{in} is the voltage when the logic bit is equal to 1. R_f and R_0 are, respectively, the feedback resistance and weight resistance as shown in Fig. 2. v_0 can be considered as the output voltage resolution of the n-bit HW data converter.

The generated analog voltage Δv which strongly correlates with the false key K_f is used to control the scaling of the supply voltage V_{dd}. The modulated supply voltage V_{dd} can be denoted as

$$V_{\text{dd}} = V_{\text{dd},0} + \Delta v = V_{\text{dd},0} + \left(\sum_{i=1}^{n} a_i \oplus k_{f,i}\right) v_0 \quad (2)$$

where $V_{\text{dd},0}$ is the DC operating voltage of the cryptographic circuit without any voltage scaling.

When a cryptographic circuit is working in the normal mode (no LPA attack), the clock frequency f_c is significantly higher than the critical frequency F_0, the switch S is in off-state and the complementary switch $\overline{S}$ is in on-state. Under this condition, the digital data D becomes $(0, 0, \ldots, 0)_2$, $(K_f \oplus K_f = (0, 0, \ldots, 0)_2)$.

[1]Critical clock frequency F_0 is the slowest frequency which can prevent the attacker from filtering the measurement noise and make LPA attacks inefficient.

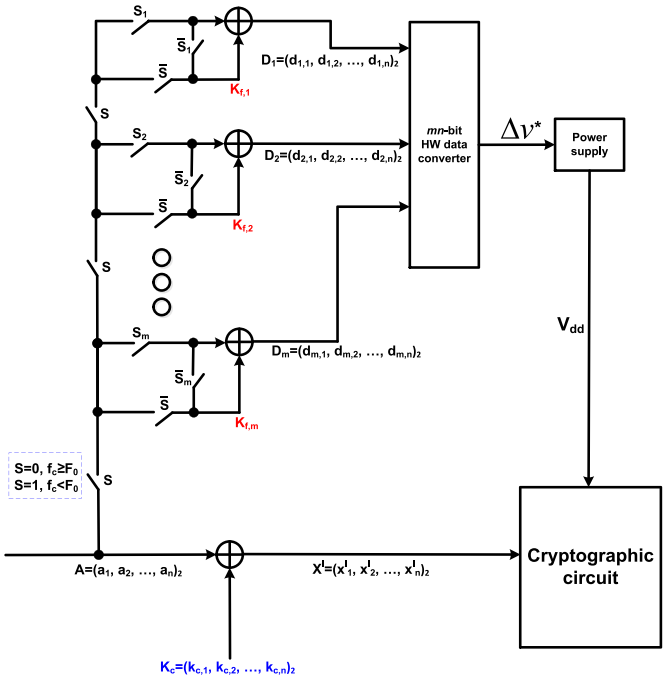

Fig. 3. Basic architecture of the proposed MPFKC AVS technique ($\overline{S}, \overline{S}_1, \overline{S}_2, \ldots, \overline{S}_m$ are the complementary switches of $S, S_1, S_2, \ldots, S_m$, respectively. $S, S_1, S_2, \ldots, S_m = 1$ represent they are in on-state while $S, S_1, S_2, \ldots, S_m = 0$ mean the off-state).

As a result, the output voltage of the HW data converter becomes $\Delta v \approx 0$, indicating that the supply voltage V_{dd} is fixed as $V_{\text{dd},0}$ and the cryptographic circuit is working in a normal mode.

AVS is a low overhead technique, which only reduces the performance of the cryptographic circuit by 5% [10]. Therefore, even if the proposed false key-controlled AVS is turned-on when the cryptographic circuit employs dynamic frequency scaling, the performance impact is negligible.

B. Architecture of Multiple Parallel False Keys-Controlled Aggressive Voltage Scaling

SFKC AVS technique masks the correct key with a single added false key that exhibits the highest correlation coefficient. However, the pattern of the supply voltage scaling may be unriddled to recover the correct key if the attacker utilizes that single added false key. In the proposed multiple parallel false keys-controlled (MPFKC) AVS technique, a random number of false keys are added to the plaintexts in every clock period, making it significantly more difficult to determine the voltage supply scaling pattern.

The architecture of the MPFKC AVS technique is shown in Fig. 3. Assume that the maximum number of added false keys in every clock period is m, $(m \geq 2)$ and all the possible added false keys are $K_{f,1}, K_{f,2}, \ldots, K_{f,m}$. Switches $S_1, S_2, \ldots, S_m$ are randomly turned-on and turned-off in every clock period to alter the number of added false keys in each clock period. An mn-bit HW data converter is utilized to convert the digital false keys related data $D_1, D_2, \ldots, D_m$ into an analog voltage signal. The corresponding output voltage of the mn-bit HW data converter Δv^* is

$$\Delta v^* = \sum_{j=1}^{m} S_j \sum_{i=1}^{n} d_{j,i} \times \left(-\frac{V_{\text{in}} R_f}{R_1}\right) = \sum_{j=1}^{m} S_j \sum_{i=1}^{n} d_{j,i} v_1 = \left(\sum_{j=1}^{m} S_j \sum_{i=1}^{n} a_i \oplus k_{f,j,i}\right) v_1 \quad (3)$$

where $S_j \in \{0, 1\}$, R_1 is the weight resistance of the mn-bit HW data converter, $k_{f,j,i}$ and $d_{j,i}$ are the i^{th} bit of the j^{th} added false key and the added false key related data, respectively, and v_1 is the output voltage resolution of the mn-bit HW data converter. As a result, the modulated supply voltage for the MPFKC AVS technique becomes $V_{\text{dd}} = V_{\text{dd},0} + \Delta v^*$.

V_w is the scaling width of supply voltage which is defined as the maximum value of $|V_{\text{dd}} - V_{\text{dd},0}|$. When V_w is the same for the SFKC AVS and MPFKC AVS techniques, (4) should be satisfied

$$V_w = \left| n \times \left(-\frac{V_{\text{in}} R_f}{R_0} \right) \right| = \left| mn \times \left(-\frac{V_{\text{in}} R_f}{R_1} \right) \right|. \tag{4}$$

Therefore, the relationship between the weight resistances R_0 and R_1 is $R_1 = mR_0$.

III. Threat Model and Modeling LPA Attacks

LPA attacks explore the correlation between the input data and the actual leakage power dissipation of a cryptographic circuit. Assume an LPA attack on a conventional cryptographic circuit,[2] x is the predicted leakage power dissipation of the cryptographic circuit by an attacker after combining the input data and correct key with a suitable power model. If the actual leakage power dissipation of the cryptographic circuit is y, the relationship between x and y can be denoted as

$$y = \alpha x + \beta \tag{5}$$

where α and β can be considered as the multiplicative and additive noise, respectively. Since both multiplicative noise and additive noise may exist in a cryptographic circuit, it is quite difficult to quantify the signal-to-noise ratio (SNR) from (5).

Fortunately, since the SNR of a system strongly correlates with the correlation coefficient [8], the SNR of a conventional cryptographic circuit can be determined by calculating the correlation coefficient. If an attacker applies m_1, (m_1 is sufficiently large) number of data to a conventional cryptographic circuit, the corresponding predicted leakage power and actual leakage power are, respectively, $x_1, x_2, \ldots, x_{m_1}$ and $y_1, y_2, \ldots, y_{m_1}$. The correlation coefficient $\gamma(x, y)$ between the predicted and actual leakage power is

$$\gamma(x, y) = \frac{\sum_{i_1=1}^{m_1} (x_{i_1} - \bar{x})(y_{i_1} - \bar{y})}{\sqrt{\sum_{i_1=1}^{m_1} (x_{i_1} - \bar{x})^2 \sum_{i_1=1}^{m_1} (y_{i_1} - \bar{y})^2}} \tag{6}$$

where $\bar{x}$ and $\bar{y}$ are, respectively, the mean values of $x_1, x_2, \ldots, x_{m_1}$ and $y_1, y_2, \ldots, y_{m_1}$. The SNR of a conventional cryptographic circuit can be determined as [8]

$$\text{SNR} = \frac{1}{\frac{1}{(\gamma(x,y))^2} - 1}. \tag{7}$$

Since the security of a cryptographic circuit is determined by the SNR value [8], a similar system with the same SNR can be used to evaluate the security of the actual conventional cryptographic circuit. When an equivalent additive noise $\xi \sim N(\mu_0, \sigma^2)$ is utilized to simulate a conventional cryptographic circuit against LPA attacks, the relationship between x and y can be modified as

$$y = \alpha_0 x + \xi \tag{8}$$

where α_0 is the mean value of α. Since

$$\frac{1}{m_1} \sum_{i_1=1}^{m_1} y_{i_1} = \alpha_0 \frac{1}{m_1} \sum_{i_1=1}^{m_1} x_{i_1} + \frac{1}{m_1} \sum_{i_1=1}^{m_1} \xi_{i_1} \tag{9}$$

where ξ_{i_1} is the corresponding equivalent additive noise due to the i_1^{th} input data, α_0 can be written as $\alpha_0 = (\bar{y} - \mu_0)/\bar{x}$.

[2]Throughout this paper, *conventional cryptographic circuit* is used to represent a circuit without any countermeasure against LPA attacks.

Since the new system has the same SNR as a conventional cryptographic circuit, (10) is satisfied

$$\frac{1}{\frac{1}{(\gamma(x,y))^2} - 1} = \frac{D(\alpha_0 x)}{\sigma^2} \tag{10}$$

where $D(\alpha_0 x)$ represents the variance of $\alpha_0 x$. The variance σ^2 of the equivalent additive noise ξ can therefore be obtained as

$$\sigma^2 = \left(\frac{\bar{y} - \mu_0}{\bar{x}} \right)^2 D(x) \left(\frac{1}{(\gamma(x, y))^2} - 1 \right). \tag{11}$$

IV. Security Evaluation

A. Single False Key-Controlled Aggressive Voltage Scaling Against LPA Attacks

The actual leakage power dissipation y of a conventional cryptographic circuit can be expressed as

$$y = V_{\text{dd},0} I_{\text{leak}} = V_{\text{dd},0} F(V_{\text{dd},0}) I_l = \omega_0 I_l \tag{12}$$

where I_{leak} is the actual leakage current of the cryptographic circuit, I_l is the leakage component which is independent of supply voltage, and $F(V_{dd,0})$ is the leakage component which is determined by supply voltage. By substituting (8) into (12), I_l can be written as

$$I_l = \frac{\alpha_0 x + \xi}{\omega_0}. \tag{13}$$

When the SFKC AVS technique is enabled on a cryptographic circuit, the actual leakage power dissipation $y^*(\Delta v, x)$ can be modeled as

$$\begin{aligned} y^*(\Delta v, x) &= (V_{\text{dd},0} + \Delta v) F(V_{\text{dd},0} + \Delta v) I_l \\ &= (V_{\text{dd},0} + \Delta v) F(V_{\text{dd},0} + \Delta v) \frac{\alpha_0 x + \xi}{\omega_0}. \end{aligned} \tag{14}$$

$F(V_{\text{dd},0} + \Delta v)$ can be approximated with the polynomial expansion as

$$F(V_{\text{dd},0} + \Delta v) \approx g_0 + \sum_{i_2=1}^{m_2} g_{i_2} (V_{\text{dd},0} + \Delta v)^{i_2} \tag{15}$$

where m_2 is the degree of the approximated polynomial and g_{i_2}, ($i_2 = 0, 1, \ldots, m_2$) is the corresponding coefficient of $(V_{\text{dd},0} + \Delta v)^{i_2}$. Accordingly, $(V_{\text{dd},0} + \Delta v) F(V_{\text{dd},0} + \Delta v)$ can be approximated as

$$\begin{aligned} &(V_{\text{dd},0} + \Delta v) F(V_{\text{dd},0} + \Delta v) \\ &\quad \approx g_0 (V_{\text{dd},0} + \Delta v) + \sum_{i_2=1}^{m_2} g_{i_2} (V_{\text{dd},0} + \Delta v)^{i_2+1} \\ &\quad = c_0 + \sum_{i_3=1}^{m_2+1} c_{i_3} (\Delta v)^{i_3} \end{aligned} \tag{16}$$

where c_{i_3}, ($i_3 = 0, 1, \ldots, m_2 + 1$) is the corresponding coefficient of $(\Delta v)^{i_3}$.

If a certain constant input data (the predicted leakage power is x_0) is applied to a cryptographic circuit and $(m_2 + 3)$ number of different supply voltages $V_{\text{dd},0}, V_{\text{dd},0} + \Delta v_1, \ldots, V_{\text{dd},0} + \Delta v_{m_2+2}$ are enabled, the corresponding actual leakage power dissipation of the cryptographic circuit becomes, respectively, $y^*(0, x_0), y^*(\Delta v_1, x_0), \ldots, y^*(\Delta v_{m_2+2}, x_0)$. Through solving the following equation:

$$\frac{y^*(0, x_0)}{c_0} \begin{pmatrix} 1 & \Delta v_1 & \cdot & \cdot & \cdot & (\Delta v_1)^{m_2+1} \\ 1 & \Delta v_2 & \cdot & \cdot & \cdot & (\Delta v_2)^{m_2+1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 1 & \Delta v_{m_2+2} & \cdot & \cdot & \cdot & (\Delta v_{m_2+2})^{m_2+1} \end{pmatrix}$$

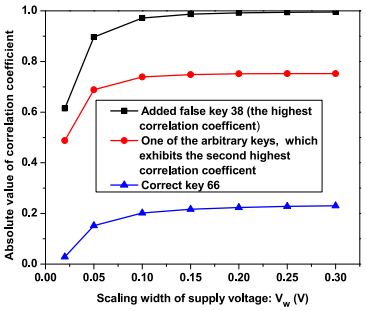

Fig. 4. Scaling width V_w of supply voltage versus absolute values of correlation coefficient of different keys for an S-box employs SFKC AVS technique against LPA attacks if HW model is utilized by the attacker ($K_f = 38$).

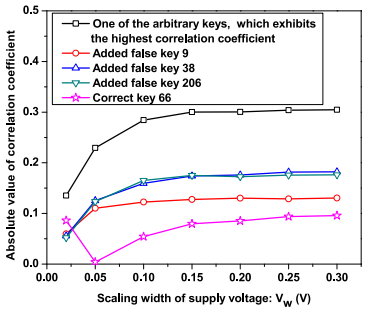

Fig. 5. Scaling width V_w of supply voltage versus absolute values of correlation coefficient of different keys for an S-box employs MPFKC AVS technique against LPA attacks if HW model is utilized by the attacker ($m = 3$, $K_{f,1} = 9$, $K_{f,2} = 38$, and $K_{f,3} = 206$).

$$\begin{pmatrix} c_0 \\ c_1 \\ \cdot \\ \cdot \\ \cdot \\ c_{m_2+1} \end{pmatrix} = \begin{pmatrix} y^*(\Delta v_1, x_0) \\ y^*(\Delta v_2, x_0) \\ \cdot \\ \cdot \\ \cdot \\ y^*\left(\Delta v_{m_2+2}, x_0\right) \end{pmatrix} \tag{17}$$

the coefficients $c_0, c_1, \ldots, c_{m_2+1}$ can be determined. When another m_3, (m_3 is sufficiently large) number of different supply voltages $V_{\mathrm{dd},0} + \Delta v_1', \ldots, V_{\mathrm{dd},0} + \Delta v_{m_3}'$ are enabled to the cryptographic circuit, the corresponding actual leakage power dissipation of the cryptographic circuit becomes, respectively, $y^*(\Delta v_1', x_0), \ldots, y^*(\Delta v_{m_3}', x_0)$. By minimizing the matching error $\sum_{i_4=1}^{m_3}((y^*(0, x_0)/c_0)(c_0 + \sum_{i_3=1}^{m_2+1} c_{i_3}(\Delta v_{i_4}')^{i_3}) - y^*(\Delta v_{i_4}', x_0))^2$, the optimum value of m_2 can be determined. $y^*(\Delta v, x)$ can therefore be approximately written as

$$y^*(\Delta v, x) \approx \left(c_0 + \sum_{i_3=1}^{m_2+1} c_{i_3}(\Delta v)^{i_3}\right)\frac{\alpha_0 x + \xi}{\omega_0}. \tag{18}$$

If the HW model is utilized by the attacker to predict the leakage power dissipation of the cryptographic circuit, x and Δv can also, respectively, be denoted as

$$x = \sum_{i=1}^{n} a_i \oplus k_{c,i} = \sum_{i=1}^{n} x_i \tag{19}$$

$$\Delta v = \left(\sum_{i=1}^{n} a_i \oplus k_{f,i}\right) v_0 = \left(\sum_{i=1}^{n} x_i \oplus k_{f,i} \oplus k_{c,i}\right) v_0. \tag{20}$$

If one of the arbitrary keys[3] $K_o = (k_{o,1}, k_{o,2}, \ldots, k_{o,n})$, the correlation coefficients of correct key K_c, added false key K_f, and that particular arbitrary key K_o are, respectively, $\gamma(\sum_{i=1}^{n} x_i, y^*(\Delta v, x))$, $\gamma(\sum_{i=1}^{n} x_i \oplus k_{f,i} \oplus k_{c,i}, y^*(\Delta v, x))$, and $\gamma(\sum_{i=1}^{n} x_i \oplus k_{o,i} \oplus k_{c,i}, y^*(\Delta v, x))$.

For a 130-nm CMOS substitution-box (S-box) [9] with SFKC AVS technique, as shown in Fig. 4, the added false key 38 shows the highest correlation coefficient by controlling the scaling of supply voltage. The correlation coefficient of correct key 66 is also lower than the second highest correlation coefficient with the impact of the added false key 38. In addition, when V_w exceeds 0.1 V, the variations of the correlation coefficient of different keys start converging.

[3]All of the possible keys can be categorized as the correct key, added false key, or an arbitrary key. We use *arbitrary key* to define any key other than the correct key and the added false key.

B. Multiple Parallel False Keys-Controlled Aggressive Voltage Scaling Against LPA Attacks

In order to prevent the attacker from unriddling the scaling behavior of supply voltage, a random number of false keys are added to plaintext in every clock period in the proposed MPFKC AVS technique. As a result, the actual leakage power dissipation of a cryptographic circuit that employs MPFKC AVS technique $y^{**}(\Delta v^*, x)$ is

$$y^{**}(\Delta v, x) \approx \left(c_0 + \sum_{i_3=1}^{m_2+1} c_{i_3}\left(\Delta v^*\right)^{i_3}\right)\frac{\alpha_0 x + \xi}{\omega_0} \tag{21}$$

where Δv^* is

$$\begin{aligned}\Delta v^* &= \left(\sum_{j=1}^{m} S_j \sum_{i=1}^{n} a_i \oplus k_{f,j,i}\right) v_1 \\ &= \left(\sum_{j=1}^{m} S_j \sum_{i=1}^{n} x_i \oplus k_{f,j,i} \oplus k_{c,i}\right) v_1\end{aligned} \tag{22}$$

when HW model is utilized by the attacker.

Note in Fig. 5 that neither the added false keys nor the correct key exhibit the highest correlation coefficient with the MPFKC AVS technique. The primary reason is that leakage power dissipation of the cryptographic circuit contains information about all of the added false keys when MPFKC AVS technique is enabled. Each added false key exhibits a high correlation with a portion of the leakage power dissipation induced by itself, but it may have a low correlation with the portion of the leakage power dissipation induced by other added false keys. However, an arbitrary key may have a high correlation with the components of the leakage power dissipation induced by different added false keys, resulting in a high correlation with the overall side-channel signal, as shown in Fig. 6(d). Another observation is that when V_w approaches 0.05 V, the critical signal that is leaked from the correct key is significantly attenuated by the noise due to the added false keys. This is due to the fact that the added multiple false keys start to become more effective when V_w exceeds 0.05 V.

V. LPA Attacks Simulation

A 130-nm CMOS S-box [9] that employs different countermeasures against LPA attacks are simulated in Cadence. Only 500 plaintexts are sufficient to leak the correct key 66 to the attacker from an S-box without countermeasure, as shown in Fig. 6(a). If an S-box employs random AVS technique, as shown in Fig. 6(b), after inputting 100 thousand plaintexts, the random power noise is filtered and the correct key 66 is also leaked to the attacker. As shown in Fig. 6(c), if an S-box employs SFKC AVS technique, the added false

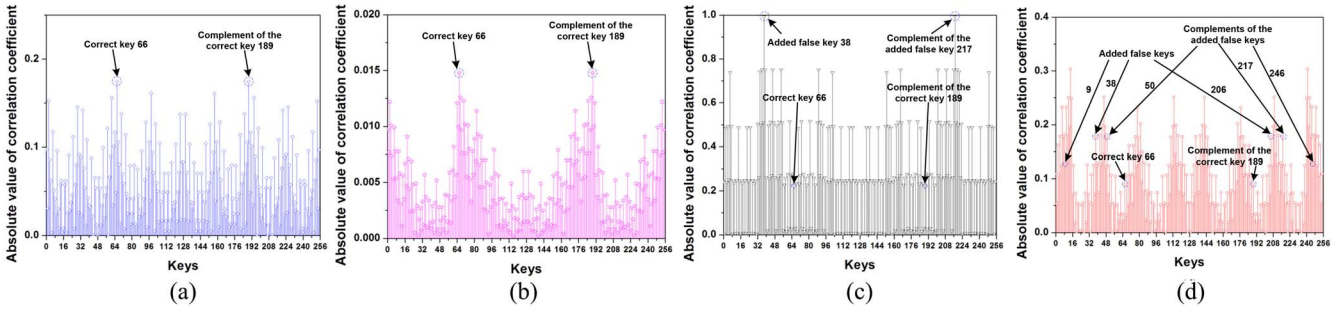

Fig. 6. Different keys versus absolute values of correlation coefficient under LPA attacks simulation ($V_W = 0.2$ V, if HW model is utilized by the attacker, polarity of the correlation coefficient can be used to discriminate the correct key and complement of the correct key [4]). (a) *S*-box without countermeasure after inputting 500 plaintexts. (b) *S*-box employs random AVS technique after inputting 100 thousand plaintexts. (c) *S*-box employs SFKC AVS technique after inputting ten million plaintexts. (d) *S*-box employs MPFKC AVS technique after inputting ten million plaintexts.

TABLE I
COMPARISON WITH PREVIOUS WORKS (X_a, X_d, AND X_l ARE, RESPECTIVELY, THE AREA, DYNAMIC POWER, LEAKAGE POWER OF A CONVENTIONAL CRYPTOGRAPHIC CIRCUIT)

	Area	Dynamic Power	Leakage power	MTD value
SDRL [11]	$2X_a$	$2X_d$	$2X_l$	—
SC converter +RDVFS [7]	X_a	$0.746X_d$	$0.7116X_l$	≥ 1 million
This work	$1.064X_a$	$0.5X_d$	$0.9039X_l$	≥ 10 million

key 38 exhibits the highest correlation coefficient even if ten million plaintexts are enabled. But the added false key 38 may be utilized by the attacker to unriddle the scaling behavior of supply voltage to leak the correct key 66. Alternatively, for an *S*-box with MPFKC AVS technique, the correct key 66 is masked from an LPA attack even if ten million plaintexts are utilized, as shown in Fig. 6(d).

VI. OVERHEAD ANALYSIS

If the average leakage power dissipation of a conventional *S*-box [9] without countermeasure is X_l and $V_W = 0.2$ V, the average leakage power dissipation of the *S*-box that employs random AVS technique, SFKC AVS technique, and MPFKC AVS technique, respectively, are $0.8160X_l$, $0.8162X_l$, and $0.9039X_l$. In MPFKC AVS technique, a smaller variance of the supply voltage scaling causes a slightly higher average leakage power dissipation on the *S*-box, as compared to random AVS and SFKC AVS techniques. The proposed MPFKC AVS technique bears approximately 6.4% area overhead, which consists of 3.4% area overhead induced by the inserted control circuit and 3% area overhead induced by the duplication of the registers to fix the circuit contamination delay.

VII. COMPARISON WITH PREVIOUS WORKS

When an LPA attack is not detected by the cryptographic circuit and the cryptographic circuit is working at the normal clock frequency, random AVS can be utilized to reduce dynamic power dissipation of the cryptographic circuit by 50%, as listed in Table I. When the clock frequency becomes lower than the critical frequency F_0, MPFKC AVS technique is activated against LPA attacks. As compared to the random voltage scaling technique in [7], the MTD value of the proposed MPFKC AVS technique can be enhanced over ten times against LPA attacks.

VIII. CONCLUSION

An adaptive false key-controlled AVS technique is proposed as a countermeasure against LPA attacks. The proposed technique can enhance the correlation between the added false keys and actual leakage power dissipation of the cryptographic circuit. The MTD value of a cryptographic circuit against LPA attacks is enhanced over ten million with the proposed technique that inserts a random number of false keys to control the scaling behavior of the supply voltage in every clock period.

REFERENCES

[1] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks Revealing the Secrets of Smart Cards* (Advances in Information Security). Berlin, Germany: Springer-Verlag, 2007.
[2] W. Yu and S. Köse, "A voltage regulator-assisted lightweight AES implementation against DPA attacks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 8, pp. 1152–1163, Aug. 2016.
[3] W. Yu and S. Köse, "Charge-withheld converter-reshuffling: A countermeasure against power analysis attacks," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 63, no. 5, pp. 438–442, May 2016.
[4] 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.
[5] A. Moradi, "Side-channel leakage through static power-should we care about in practice?" in *Cryptographic Hardware and Embedded Systems*. Heidelberg, Germany: Springer, 2014, pp. 562–579.
[6] S. M. D. Pozo, F.-X. Standaert, D. Kamel, and A. Moradi, "Side-channel attacks from static power: When should we care?" in *Proc. Design Autom. Test Europe (DATE)*, Grenoble, France, Mar. 2015, pp. 145–150.
[7] W. Yu and S. Köse, "Exploiting voltage regulators to enhance various power attack countermeasures," *IEEE Trans. Emerg. Topics Comput.*, to be published. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/7605440/, doi: 10.1109/TETC.2016.2620382.
[8] F.-X. Standaert, E. Peeters, G. Rouvroy, and J.-J. Quisquater, "An overview of power analysis attacks against field programmable gate arrays," *Proc. IEEE*, vol. 94, no. 2, pp. 383–394, Feb. 2006.
[9] N. Ahmad and S. M. R. Hasan, "Low-power compact composite field AES S-Box/Inv S-Box design in 65 nm CMOS using novel XOR gate," *Integr. VLSI J.*, vol. 46, no. 4, pp. 333–344, Sep. 2013.
[10] N. D. P. Avirneni and A. K. Somani, "Countering power analysis attacks using reliable and aggressive designs," *IEEE Trans. Comput.*, vol. 63, no. 6, pp. 1408–1420, Jun. 2014.
[11] N.-H. Zhu, Y.-J. Zhou, and H.-M. Liu, "Employing symmetric dual-rail logic to thwart LPA attack," *IEEE Embedded Syst. Lett.*, vol. 5, no. 4, pp. 61–64, Dec. 2013.
[12] M. Kar *et al.*, "Exploiting fully integrated inductive voltage regulators to improve side channel resistance of encryption engines," in *Proc. ISLPED*, San Francisco, CA, USA, Aug. 2016, pp. 130–135.