A Lightweight AES Implementation Against Bivariate First-Order DPA Attacks *

Weize Yu
University of South Florida
Tampa, Florida
weizeyu@mail.usf.edu

Selçuk Köse
University of South Florida
Tampa, Florida
kose@usf.edu

ABSTRACT

Aggressive voltage scaling (AVS) technique is an efficient and lightweight countermeasure for cryptographic circuits against conventional first-order (CFO) differential power analysis (DPA) attacks. However, in this paper, it is demonstrated that AVS technique is vulnerable against bivariate first-order (BFO) DPA attacks since the noise inserted by the random scaling of the voltage can be filtered easily under BFO DPA attacks. To protect a cryptographic circuit that utilizes voltage scaling against BFO attacks, a lightweight implementation of the advanced encryption standard (AES) is proposed. In the proposed technique, even if the noise inserted by the random voltage scaling is filtered, a significant amount of random power noise can still be present in the side-channel leakage obtained by BFO DPA attacks. As demonstrated with the simulation results, when BFO DPA attacks are implemented on the proposed lightweight random AES engine with AVS technique, the measurement-to-disclose (MTD) value is enhanced over 1 million. Alternatively, the MTD value is less than 6,000 under BFO DPA attacks for a conventional AES engine with AVS technique.

Keywords

Aggressive voltage scaling, bivariate first-order, differential power analysis attacks, advanced encryption standard

1. INTRODUCTION

Side-channel attacks (SCAs) have become important security concerns for modern integrated circuits (ICs) since the physical leakage mechanisms (such as power consumption, electro-magnetic emissions, and timing information) are difficult to control and mitigate [1–7]. Differential power analysis (DPA) attacks are widely studied SCAs, which can leak the secret key of a cryptographic circuit (CC) through exploiting the correlation between the input data and dynamic power consumption of the CC [8–11]. In order to protect CCs against DPA attacks, various countermeasures [1, 12–18] have been proposed to weaken the correlation between the input data and monitored dynamic power dissipation of the CC.

All of the existing DPA attack countermeasures can be categorized into two types: masking and hiding. The dynamic power consumption P_{dyn} of a CC can be denoted as $P_{dyn} = \beta_{0\rightarrow1} f_c V_{dd}^2 C_L$ [19] where $\beta_{0\rightarrow1}$ is the number of $0 \rightarrow 1$ transitions that occur within the CC under different input data, f_c is the clock frequency, V_{dd} is the supply voltage, and C_L is the load capacitance. Plaintext masking technique [13] is an effective masking countermeasure that inserts a large amount of intermediate random data values to mask the plaintexts, breaking the strong correlation between the input data and $\beta_{0\rightarrow1}$. However, the area overhead of plaintext masking technique for the look-up table (LUT) increases significantly due to the large amount of inserted random data values [13].

One of the techniques used in hiding countermeasures is to make P_{dyn} constant under any input data value (*i.e.,* constant hiding countermeasures). Therefore, balanced logic gate such as wave dynamic differential logic (WDDL) has been proposed in [1] which uses the complementary output and pre-charge stage to achieve a constant $\beta_{0\rightarrow1}$ regardless of the input data values. Alternatively, a constant P_{dyn} also can be achieved when a switched-capacitor current equalizer countermeasure [12] is enabled to discharge the residual charge which may leak the critical information. Unfortunately, constant hiding countermeasures induce significant power/area/performance overhead [12, 15].

Another technique used in hiding countermeasures is to make P_{dyn} as a random value (*i.e.,* random hiding countermeasures). Therefore, random power grid [14] and power profile scrambling [15] have been proposed by inserting additional random power consumption circuits to hide the actual power consumption of the CC. However, the inserted additional random power consumption circuits also cause non-negligible power/area/performance overhead [14, 15].

Random voltage/frequency scaling (VFS) techniques also belong to random hiding countermeasures, which have been proposed in [16–18] to reduce the correlation between the input data and P_{dyn} by randomly altering the clock frequency f_c or supply voltage V_{dd}. Aggressive voltage scaling (AVS) technique is a VFS-based countermeasure, which has high security (*i.e.,* MTD>1 million) against conventional first-order (CFO) DPA attacks with low overhead [18]. Since the scaling frequency of V_{dd} is significantly lower than the input

*This work was supported in part by the National Science Foundation CAREER grant under contract No. CCF-1350451 and a research award from Cisco Systems.

HASP '17, June 25, 2017, Toronto, ON, Canada
 ISBN 978-1-4503-5266-6/17/06...$15.00
DOI: http://dx.doi.org/10.1145/3092627.3092628.

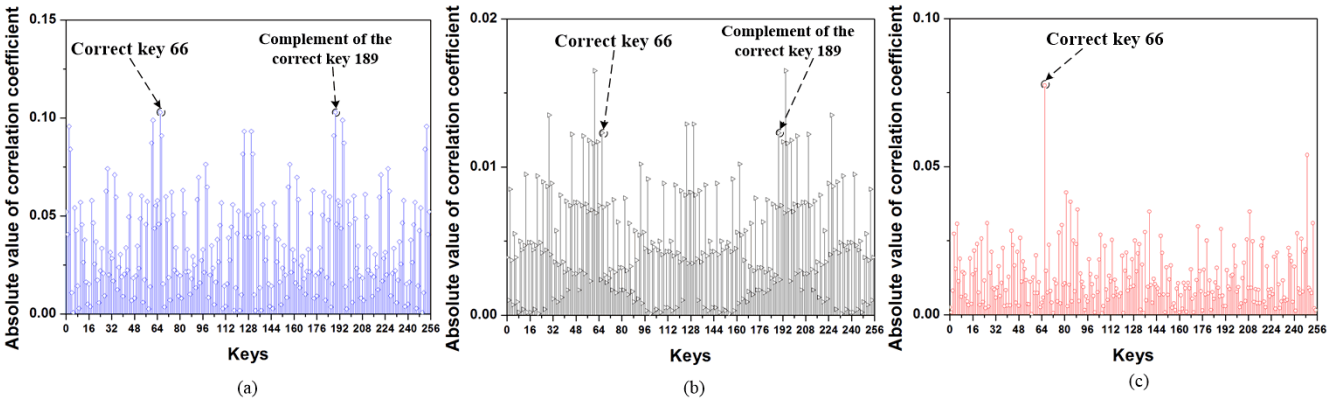

Figure 1: DPA attacks simulation ($f_c = 200MHz$ and $f_v = 2MHz$. $V_{DD2} - V_{DD1} = 1.0V$ where V_{DD1} and V_{DD2} are the minimum and maximum supply voltage values, respectively. For CFO DPA attacks, if HW model is utilized, polarity can be used to distinguish the correlation coefficients of the correct key and complement of the correct key [20]). (a) Absolute values of correlation coefficient of different keys for an S-box without countermeasure after inputting 1,000 plaintexts when CFO DPA attacks are implemented. (b) Absolute values of correlation coefficient of different keys for an S-box with AVS technique after inputting 100 thousand plaintexts when CFO DPA attacks are implemented. (c) Absolute values of correlation coefficient of different keys for an S-box with AVS technique after inputting 6,000 plaintexts when BFO DPA attacks are implemented.

data frequency (the same as the clock frequency f_c) [18], the attacker can filter the power noise generated by randomly altering V_{dd} by implementing bivariate first-order (BFO) DPA attacks. For instance, assume $P_{dyn}^{'}$ and $P_{dyn}^{''}$ are the dynamic power dissipation of a CC induced by two adjacent input data $data_1$ and $data_2$, respectively. $\beta_{0\rightarrow1}^{'}$ ($\beta_{0\rightarrow1}^{''}$) is the number of $0 \rightarrow 1$ transitions that occur in a CC induced by $data_1$ ($data_2$). Since $P_{dyn}^{'}$ and $P_{dyn}^{''}$ may share the same V_{dd} value due to the slow supply voltage scaling frequency, the attacker may use $P_{dyn}^{'}/P_{dyn}^{''} = \beta_{0\rightarrow1}^{'}/\beta_{0\rightarrow1}^{''}$ which is independent of V_{dd} as the new power data to implement BFO DPA attacks on the CC with AVS technique. As a result, a CC with AVS technique may be vulnerable to BFO DPA attacks.

Advanced encryption standard (AES) engine is a widely used CC to securely store critical data [1,3]. In an n-bit AES engine, $n/8$ number of substitution-boxes (S-boxes) are utilized to process the secret data. When DPA attacks are implemented on one of the $n/8$ number of S-boxes, the attacker can dynamically alter the plaintext of the specific S-box that is under DPA attack and maintain the plaintext as constant for the other S-boxes which are not under DPA attack. As a result, only the S-box under DPA attack exhibits a high dynamic power dissipation while other S-boxes exhibit a quite low leakage power dissipation. Recently, Yu et al. [3] proposed a lightweight AES engine to ensure that all of the S-boxes exhibit a high dynamic power dissipation even if a constant plaintext is enabled. Accordingly, $n/8$ number of invert boxes are placed in front of the $n/8$ number of S-boxes, respectively, to guarantee that all of the S-boxes have a high dynamic power dissipation by altering the constant input data periodically.

Although the S-boxes which are not under DPA attacks in the lightweight AES engine [3] can generate a high amplitude of side-channel power noise, due to lack of randomness, the attacker still can filter the noise easily when BFO DPA attacks are performed on the lightweight AES [3] with AVS technique as demonstrated in Section 4.2. Therefore, in this paper, a lightweight random AES is proposed to secure the CC that houses a VFS-based countermeasure against BFO DPA attacks. One of the differences between the lightweight AES [3] and proposed lightweight random AES is that the invert boxes in the lightweight AES invert the input data periodically while the invert boxes in the lightweight random AES invert the input data randomly. As a result, when BFO DPA attacks are implemented on a lightweight random AES engine with AVS technique, the large amount of random power noise generated by the other S-boxes (i.e., that are not under DPA attacks) due to the randomly inverting behavior can be utilized against BFO DPA attacks even if the random voltage scaling noise is filtered.

The rest of the paper is organized as follows. BFO DPA attacks are implemented on an S-box with AVS technique in Section 2. Working principle of the lightweight random AES engine is introduced in Section 3. Security of the lightweight random AES engine with AVS technique against BFO DPA attacks is evaluated in Section 4. Conclusions are offered in Section 5.

2. BFO DPA ATTACKS ON AN S-BOX WITH AVS TECHNIQUE

Assume that an attacker inputs data $I_j, (j = 1, 2, ...)$ to a CC and measures the corresponding dynamic power dissipation $P_{dyn,j}$ of the CC induced by the input data I_j. When the attacker analyzes the correlation between the input data I_j and $P_{dyn,j}$, the type of DPA attacks is categorized as a CFO DPA attack. Alternatively, the attacker may utilize a mathematical operation to convert two samples of the dynamic power dissipation profile $P_{dyn,j}$ and $P_{dyn,j+k}, (k \geq 1)$ as a new sample of the power data $P_{dyn,j}^{*}$. When the attacker exploits the correlation between the input data (I_j, I_{j+k}) and $P_{dyn,j}^{*}$, the corresponding DPA attacks are categorized as the BFO DPA attacks [21].

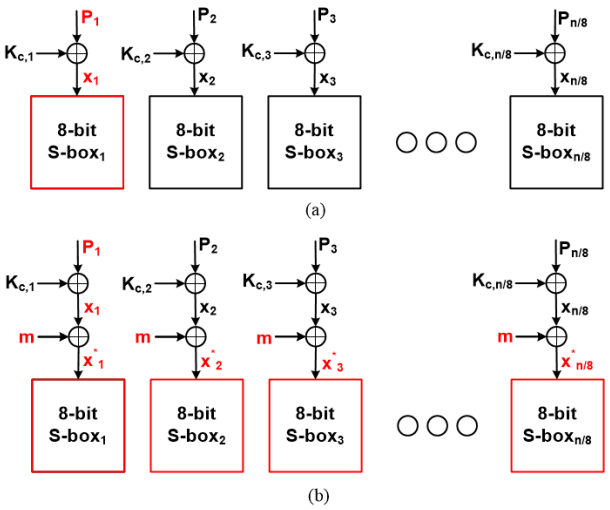

Figure 2: (a) Substitute bytes operation in the 1^{st} encryption round of an n-bit conventional AES engine. (b) Substitute bytes operation in the 1^{st} encryption round of an n-bit lightweight AES engine.

For an S-box that employs AVS technique, assume that the clock frequency f_c is h times of the supply voltage scaling frequency f_v ($f_c = hf_v$) where $h >> 1$ [18]. The dynamic power dissipation $P_{dyn,j}$ and $P_{dyn,j+1}$ of an S-box with AVS technique induced by the j^{th} and $(j+1)^{th}$ input data can be, respectively, denoted as

$$P_{dyn,j} = \beta_{0\to1,j} f_c V^2_{dd,[\frac{j}{h}]} C_L, \quad (1)$$

$$P_{dyn,j+1} = \beta_{0\to1,j+1} f_c V^2_{dd,[\frac{j+1}{h}]} C_L, \quad (2)$$

where $\beta_{0\to1,j}$ ($\beta_{0\to1,j+1}$) is the number of $0 \to 1$ transitions induced by the j^{th} ($(j+1)^{th}$) input data. $V_{dd,[\frac{j}{h}]}$ and $V_{dd,[\frac{j+1}{h}]}$ are the scaled supply voltage values, which, respectively, correspond to the j^{th} and $(j+1)^{th}$ input data. However, when $j \in [ih, (i+1)h-2]$, $(i = 1, 2, ...)$, the following equation (3) which is independent of the supply voltage is satisfied

$$\frac{P_{dyn,j+1}}{P_{dyn,j}} = \frac{\beta_{0\to1,j+1}}{\beta_{0\to1,j}}. \quad (3)$$

For CFO DPA attacks, if the predicted dynamic power dissipations by utilizing the j^{th} and $(j+1)^{th}$ input data with a suitable power model are, respectively, X_j and X_{j+1}, BFO DPA attacks may be implemented by the attacker to exploit the correlation between X_{j+1}/X_j and $P_{dyn,j+1}/P_{dyn,j}$ to leak the secret key.

If hamming-weight (HW) model is utilized by the attacker to implement the DPA attack when an 8-bit binary input data $I_j = (I_{j,1}, I_{j,2}, ..., I_{j,8})_2$ is enabled on an S-box, the predicted dynamic power dissipation of the S-box can be written as

$$X_j = \sum_{i_1=1}^{8} I_{j,i_1}. \quad (4)$$

As a result, the value range of X_j is $X_j \in [0, 8]$. If X_{j+1}/X_j is used as the predicted dynamic power dissipation of the S-box for executing BFO DPA attacks as explained above,

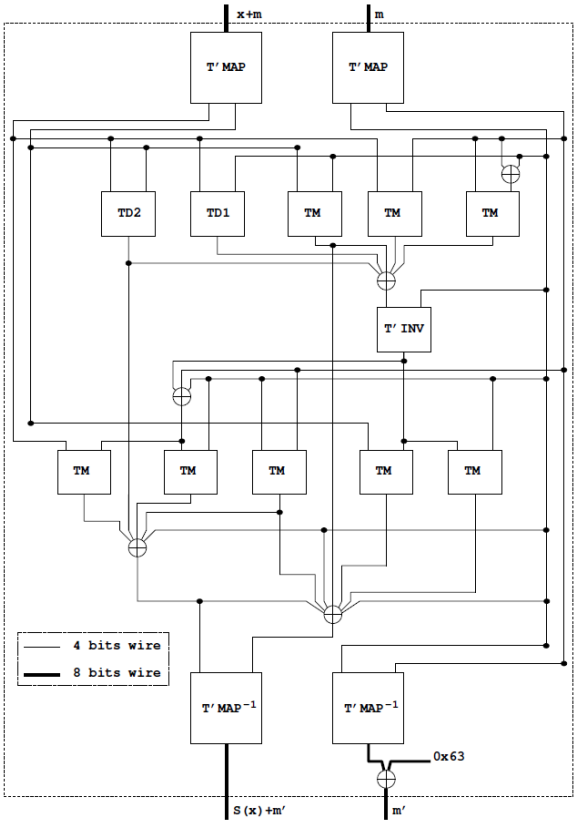

Figure 3: Architecture of the modified S-box from [13] (+ represents xor operation and S(x) is the substituted byte of x).

X_{j+1}/X_j would become infinity when $X_j = 0$ and $X_{j+1} \neq 0$. Therefore, in order to avoid the predicted dynamic power dissipation of the S-box having the risk of becoming infinity, $(X_{j+1}+1)/(X_j+1)$ is utilized as the predicted dynamic power dissipation of the S-box to perform BFO DPA attacks.

Two S-boxes [22], one without any countermeasure and one with AVS technique, are implemented with 130 nm CMOS and simulated in Cadence. As shown in Fig. 1(a), when a CFO DPA attack is implemented on an S-box without countermeasure, the correct key 66[1] is leaked to the attacker after inputting 1,000 plaintexts. When a CFO DPA attack is executed on an S-box with AVS technique, the correct key 66 cannot be obtained by the attacker even if 100 thousand plaintexts are enabled, as shown in Fig. 1(b). This result indicates that AVS technique is efficient against CFO DPA attacks. Alternatively, when a BFO DPA attack is implemented on an S-box with AVS technique, the correct key 66 is leaked to the attacker after inputting only 6,000 plaintexts, as shown in Fig. 1(c). AVS technique is therefore quite vulnerable against BFO DPA attacks.

3. PROPOSED LIGHTWEIGHT RANDOM AES ENGINE

The substitute bytes operation in the 1^{st} encryption round of a conventional n-bit AES engine is shown in Fig. 2(a). $n/8$ number of S-boxes reside in a conventional n-bit AES

[1]66 is chosen arbitrarily as the correct key.

engine. If the attacker intends to implement a DPA attack on S-box$_1$, only plaintext P_1 is dynamically altered while plaintexts $P_2, P_3, ..., P_{n/8}$ can be kept constant. Since the $l^{th}, (l = 1, 2, ..., n/8)$ input data of S-box$_l$ is $x_l = P_l \oplus K_{c,l}$ where $K_{c,l}$ is the secret key of S-box$_l$, only S-box$_1$ exhibits a high dynamic power dissipation due to the variable input data x_1. Alternatively, S-box$_2$, S-box$_3$, ..., S-box$_{n/8}$ generate a low leakage power dissipation due to the constant input data.

For the n-bit lightweight AES engine that is proposed in [3], the substitute bytes operation in the 1^{st} encryption round is illustrated in Fig. 2(b). The 8-bit mask data m generated by the invert boxes is added with $x_1, x_2, ..., x_{n/8}$, respectively, to generate the corresponding input data $x_1^*, x_2^*, ..., x_{n/8}^*$ to each S-box. Since the mask data m alters periodically between the two values such as $m = (00000000)_2, (11111111)_2, (00000000)_2, ...$, the input data $x_1^*, x_2^*, ..., x_{n/8}^*$ are periodically inverted to guarantee that all of the S-boxes exhibit a high dynamic power dissipation even if $x_1, x_2, ..., x_{n/8}$ are constant ($x_l^* = x_l \oplus m$). At the end of the encryption, the residue of the related mask component is removed to recover the correct cipher data in the n-bit lightweight AES engine [3]. However, since the S-box performs a non-linear operation, the mask data m would be tangled with the encryption data to make it difficult to remove at the end of encryption. In order to remove the mask data m easily at the end of encryption, the architecture of S-box needs to be modified. The modified S-box used in [3] is shown in Fig. 3. The encryption data x is linearly separated from the mask m after finishing the substitute byte operation if the modified S-box is utilized. The six transforming tables in Fig. 3 are summarized as follows [13, 23]

$$TD1 : ((y+g), g) \rightarrow y^2 \times p_0 + g, \tag{5}$$

$$TD2 : ((y+g), (z+g^{'})) \rightarrow ((y+g) + (z+g^{'})) \times (z+g^{'}), \tag{6}$$

$$TM : ((y+g), (z+g^{'})) \rightarrow (y+g) \times (z+g^{'}), \tag{7}$$

$$T^{'}INV : ((y+g), g)) \rightarrow TINV(y) + g, \tag{8}$$

where y, z, g, and $g^{'}$ are 4-bit data which corresponds to the input side of each transforming table. p_0 is the coefficient of y^2. $TINV$, $TMAP$, and $TMAP^{-1}$ are the inverse operation, mapping operation, and inverse mapping operation in the conventional S-box, respectively.

As compared to the aforementioned n-bit lightweight AES engine, in the proposed n-bit lightweight random AES engine, all of the invert boxes perform the invert operation randomly in every clock period to make the 8-bit mask data m generate a random pattern with the two possible masks; $(00000000)_2$ and $(11111111)_2$. As a result, S-boxes that are not under DPA attack (S-box$_2$, S-box$_3$, ..., S-box$_{n/8}$) would generate a large mount of uncertain power noise to protect S-box$_1$ against BFO DPA attacks.

In the conventional masked AES engine [13], a large amount of random mask data values are inserted to break the strong correlation between the plaintexts and input data of S-boxes, which leads to significant area and performance overhead due to the large size of the look-up table (LUT). However, in the proposed lightweight random AES engine, the area and performance overheads are negligible, which are approximated the same as [3] since only two mask data values $(00000000)_2$ and $(11111111)_2$ are inserted.

4. SECURITY EVALUATION AGAINST BFO DPA ATTACKS

The security of the conventional AES engine, the lightweight AES engine, and the proposed lightweight random AES engine is evaluated in this section against BFO DPA attacks when these AES engines employ AVS technique.

4.1 Conventional AES Engine with AVS Technique Against BFO DPA Attacks

For an S-box implemented with modern CMOS technology, the leakage power dissipation P_{leak} can be approximated as [24]

$$P_{leak} \approx V_{dd} I_{leak} e^{aV_{dd}}, \tag{9}$$

where I_{leak} is the component of the leakage current of the S-box which is controlled by the input data and is independent of the supply voltage whereas a is the CMOS technology dependent parameter.

As shown in Fig. 2(a), when S-box$_1$ in a conventional n-bit AES engine is under a DPA attack, only S-box$_1$ exhibits a high dynamic power dissipation while other S-boxes show a low leakage power dissipation. Therefore, if AVS technique is enabled on all of the S-boxes (assuming all of the S-boxes are controlled by the same voltage scaling pattern), the total monitored power dissipation $P_{tot,j}$ and $P_{tot,j+1}$ of the conventional n-bit AES engine with AVS technique induced by the j^{th} and $(j+1)^{th}$ input data, respectively, are

$$P_{tot,j} \approx \beta_{0\rightarrow1,1,j} f_c V_{dd,[\frac{j}{h}]}^2 C_L + V_{dd,[\frac{j}{h}]} e^{aV_{dd,[\frac{j}{h}]}} \sum_{s=2}^{n/8} I_{leak,s}, \tag{10}$$

$$P_{tot,j+1} \approx \beta_{0\rightarrow1,1,j+1} f_c V_{dd,[\frac{j+1}{h}]}^2 C_L + V_{dd,[\frac{j+1}{h}]} e^{aV_{dd,[\frac{j+1}{h}]}} \sum_{s=2}^{n/8} I_{leak,s}, \tag{11}$$

where $\beta_{0\rightarrow1,1,j}$ ($\beta_{0\rightarrow1,1,j+1}$) is the number of $0 \rightarrow 1$ transitions in S-box$_1$ induced by the j^{th} ($(j+1)^{th}$) input data and $I_{leak,s}, (s = 2, 3, ..., n/8)$ is the component of the leakage current of S-box$_s$ induced by the corresponding constant input data.

4.2 Lightweight AES Engine with AVS Technique Against BFO DPA Attacks

In the n-bit lightweight AES engine, as shown in Fig. 2(b), when S-box$_1$ is under DPA attacks, plaintexts $P_2, P_3, ..., P_{n/8}$ are maintained as constant. However, with the impact of mask data m, the input data x_s^* of S-box$_s$ would become $x_s^* = x_s, \overline{x_s}, x_s, ...$ when x_s is constant. When the input data x_s^* makes a transition from x_s ($\overline{x_s}$) to $\overline{x_s}$ (x_s), the number of $0 \rightarrow 1$ transitions in S-box$_s$ is $\beta_{0\rightarrow1,s}^*$ ($\beta_{0\rightarrow1,s}^{**}$). The total monitored power dissipation $P_{tot,j}^*$, $P_{tot,j+1}^*$, and $P_{tot,j+2}^*$ of the n-bit lightweight AES engine with AVS technique induced by the j^{th}, $(j+1)^{th}$, and $(j+2)^{th}$ input data, respectively, can therefore be written as

$$P_{tot,j}^* = \beta_{0\rightarrow1,1,j} f_c V_{dd,[\frac{j}{h}]}^2 C_L + f_c V_{dd,[\frac{j}{h}]}^2 C_L \sum_{s=2}^{n/8} (mod(j,2)\beta_{0\rightarrow1,s}^* + mod(j+1,2)\beta_{0\rightarrow1,s}^{**}), \tag{12}$$

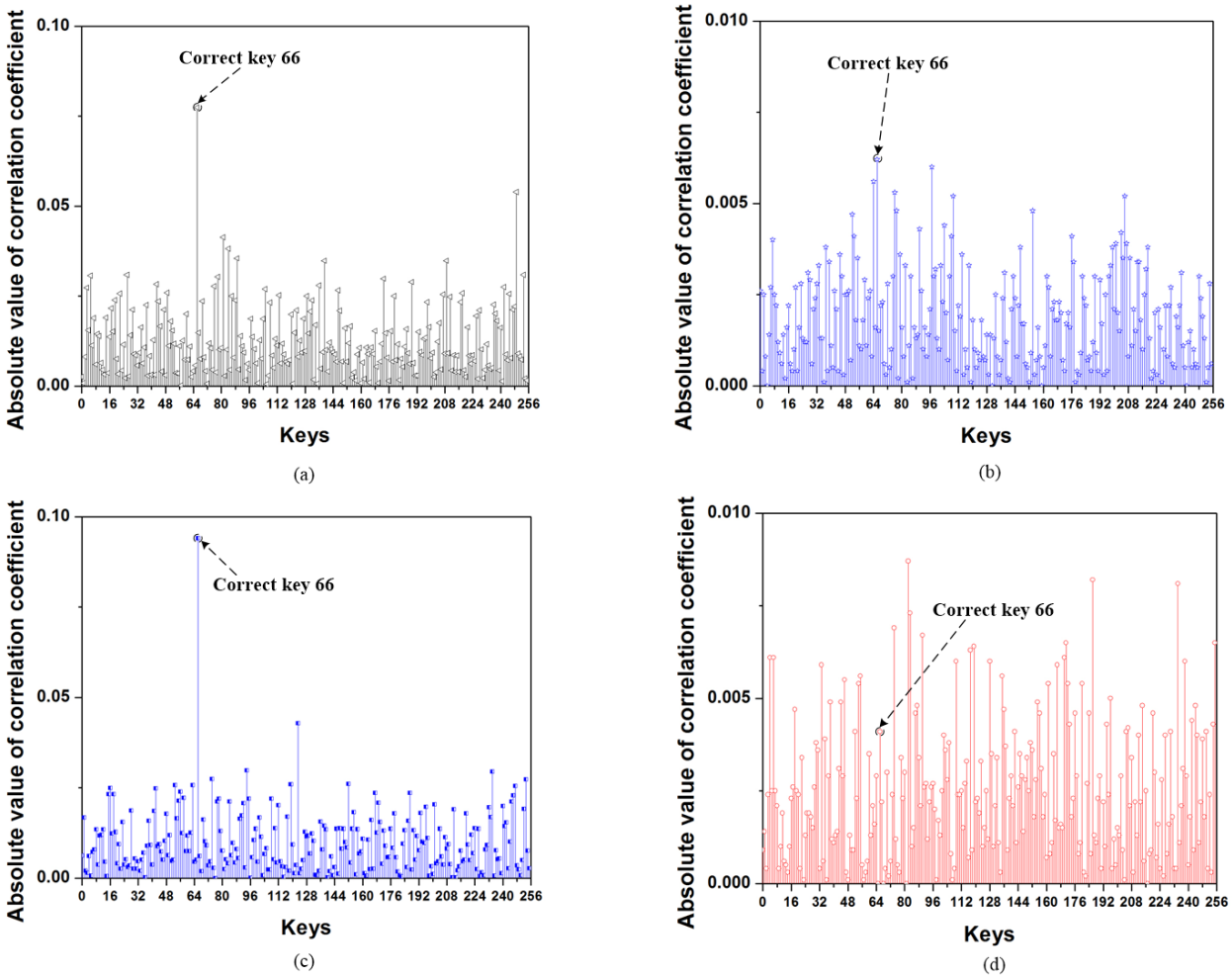

Figure 4: BFO DPA attacks simulation ($f_c = 200MHz$ and $f_v = 2MHz$. $V_{DD2} - V_{DD1} = 1.0V$). (a) Absolute values of correlation coefficient of different keys for a 128-bit conventional AES engine with AVS technique after inputting 6,000 plaintexts. (b) Absolute values of correlation coefficient of different keys for a 128-bit lightweight AES engine with AVS technique after inputting 500 thousand plaintexts (the attacker utilizes $P^*_{tot,j+1}/P^*_{tot,j}$ to perform BFO DPA attacks). (c) Absolute values of correlation coefficient of different keys for a 128-bit lightweight AES engine with AVS technique after inputting 20 thousand plaintexts (the attacker utilizes $P^*_{tot,j+2}/P^*_{tot,j}$ to perform BFO DPA attacks). (d) Absolute values of correlation coefficient of different keys for a 128-bit lightweight random AES engine with AVS technique after inputting 1 million plaintexts.

$$P^*_{tot,j+1} = \beta_{0\to1,1,j+1} f_c V^2_{dd,[\frac{j+1}{h}]} C_L + f_c V^2_{dd,[\frac{j+1}{h}]} C_L \times \sum_{s=2}^{n/8} (mod(j+1,2)\beta^*_{0\to1,s} + mod(j+2,2)\beta^{**}_{0\to1,s}), \quad (13)$$

$$P^*_{tot,j+2} = \beta_{0\to1,1,j+2} f_c V^2_{dd,[\frac{j+2}{h}]} C_L + f_c V^2_{dd,[\frac{j+2}{h}]} C_L \times \sum_{s=2}^{n/8} (mod(j,2)\beta^*_{0\to1,s} + mod(j+1,2)\beta^{**}_{0\to1,s}). \quad (14)$$

As shown in (12)-(14), if the attacker selects $P^*_{tot,j}$ and $P^*_{tot,j+1}$ to perform BFO DPA attacks, the large variance of dynamic power dissipation from the S-boxes, which are not under attack, reduces the signal-to-noise ratio (SNR) of the S-box that is under attack. However, when the attacker selects $P^*_{tot,j}$ and $P^*_{tot,j+2}$ to perform BFO DPA attacks, the dynamic power dissipation from other S-boxes may become constant which can be filtered by the attacker easily.

4.3 Proposed Lightweight Random AES Engine with AVS Technique Against BFO DPA Attacks

In Fig. 2(b), if the 8-bit mask data m generates a random pattern with the two values $(00000000)_2$ and $(11111111)_2$, when S-box$_1$ is under DPA attacks, the total monitored power dissipation $P^{**}_{tot,j}$ and $P^{**}_{tot,j+1}$ of the proposed n-bit lightweight random AES engine with AVS technique induced by the j^{th} and $(j+1)^{th}$ input data, respectively, are

$$P^{**}_{tot,j} = \beta_{0\to1,1,j} f_c V^2_{dd,[\frac{j}{h}]} C_L + f_c C_L V^2_{dd,[\frac{j}{h}]} u_j \times \sum_{s=2}^{n/8} (mod(\sum_{j_1=1}^{j} u_{j_1}, 2)\beta^*_{0\to1,s} + (1 - mod(\sum_{j_1=1}^{j} u_{j_1}, 2))\beta^{**}_{0\to1,s}), \quad (15)$$

$$P^{**}_{tot,j+1} = \beta_{0\to1,1,j} f_c V^2_{dd,[\frac{j+1}{h}]} C_L + f_c C_L V^2_{dd,[\frac{j+1}{h}]} u_{j+1} \times \sum_{s=2}^{n/8} (mod(\sum_{j_1=1}^{j+1} u_{j_1}, 2)\beta^*_{0\to1,s} + (1 - mod(\sum_{j_1=1}^{j+1} u_{j_1}, 2))\beta^{**}_{0\to1,s}), \quad (16)$$

where random parameter $u_{j_1} \in \{0, 1\}, (j_1 = 1, 2, ..., j + 1)$.

To evaluate the security benefit of the proposed lightweight random AES engine, it is compared against the other two implementations. Accordingly, i) a conventional 128-bit 130 nm CMOS AES engine with AVS technique, ii) a lightweight AES engine with AVS technique [3], and iii) the proposed lightweight random AES engine with AVS technique are simulated in Cadence. Moreover, a BFO DPA attack is individually implemented on these implementations by exploring the correlation between the input data and $P_{tot,j+1}/P_{tot,j}$, $P^*_{tot,j+1}/P^*_{tot,j}$, $P^*_{tot,j+2}/P^*_{tot,j}$, and $P^{**}_{tot,j+1}/P^{**}_{tot,j}$, respectively. As shown in Fig. 4(a), the correlation coefficient of the correct key of the conventional AES engine with AVS technique is almost the same as the correlation coefficient of the correct key of an S-box with AVS technique (in Fig. 1(c)). The primary reason is that the leakage power dissipation P_{leak} of an S-box is quite lower than the corresponding dynamic power dissipation P_{dyn} ($P_{leak}/P_{dyn} \approx 0.1\%$ in 130nm CMOS technology [3,24]). Therefore, the total leakage power dissipation of the other 15 S-boxes which are not under a DPA attack (S-box$_2$, S-box$_3$, ..., S-box$_{16}$) is about 1.5% (negligible) of the dynamic power dissipation of S-box$_1$ which is under the DPA attack. As a result, the input power profiles of an S-box with AVS technique and the 128-bit conventional AES engine with AVS technique under DPA attacks are almost the same.

In Fig. 4(b), if the attacker utilizes $P^*_{tot,j+1}/P^*_{tot,j}$ to perform BFO DPA attacks, the large variance of dynamic power dissipation from the other 15 S-boxes (S-box$_2$, S-box$_3$, ..., S-box$_{16}$) which are not under a DPA attack reduces the correlation coefficient of the correct key and enhances the MTD value to 500 thousand. However, due to the lack of randomness of the high dynamic power dissipation generated by these 15 S-boxes which are not under a DPA attack, the correct key 66 can still be leaked to the attacker after inputting 20 thousand plaintexts if the attacker utilizes $P^*_{tot,j+2}/P^*_{tot,j}$ to perform BFO DPA attacks, as shown in Fig. 4(c).

As shown in Fig. 4(d), when a BFO DPA attack is implemented on a 128-bit lightweight random AES engine with AVS technique, the random high power noise generated by the other 15 S-boxes can reduce the correlation coefficient of the correct key further as compared to the 128-bit lightweight AES engine with AVS technique. As a result, even if 1 million plaintexts are enabled, the correct key 66 can be prevented from leaking to the attacker.

5. CONCLUSION

A lightweight random AES is proposed as a countermeasure to significantly improve the security of AVS technique against BFO DPA attacks. The random power noise generated by randomly altering the invert operations in the lightweight random AES engine significantly reduces the correlation between the predicted and monitored power dissipation profiles. The MTD value of the proposed lightweight random AES engine with AVS technique is enhanced over 1 million against a BFO DPA attack whereas the conventional AES engine with AVS technique can be cracked after applying merely 6,000 plaintext inputs with a BFO DPA attack.

6. REFERENCES

[1] 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.

[2] W. Yu, O. A. Uzun, and S. Köse, "Leveraging on-chip voltage regulators as a countermeasure against side-channel attacks," *in Proc. Design Automation Conference (DAC)*, pp. 1–6, Jun. 2015.

[3] 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, Aug. 2016.

[4] 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*, doi: 10.1109/TVLSI.2017.2670537.

[5] W. Yu and S. Köse, "False key-controlled aggressive voltage scaling: A countermeasure against LPA attacks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, doi: 10.1109/TCAD.2017.2682113.

[6] W. Yu and S. Köse, "Security implications of simultaneous dynamic and leakage power analysis attacks on nanoscale cryptographic circuits," *IET Electronics Letters*, Vol. 52, No. 6, pp. 466–468, March 2016.

[7] O. A. Uzun and S. Köse, "Converter-gating: A power efficient and secure on-chip power delivery system," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, Vol. 4, No. 2, pp. 169–179, Jun. 2014.

[8] M. Avital, H. Dagan, I. Levi, O. Keren, and A. Fish, "DPA-secured quasi-adiabatic 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.

[9] M. Alioto, S. Bongiovanni, M. Djukanovic, G. Scotti, and A. Trifiletti, "Effectiveness of leakage power analysis attacks on DPA-resistant logic styles under process variations," *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 61, No. 2, pp. 429–442, Feb. 2014.

[10] W. Yu and S. Köse, "Charge-withheld converter-reshuffling: A countermeasure against power analysis attacks," *IEEE Transactions on Circuits and Systems II: Express Briefs*, Vol. 63, No. 5, pp. 438–442, May 2016.

[11] 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, Sep. 2015.

[12] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE Journal of Solid-State Circuits*, Vol. 45, No. 1,

pp. 23–31, Jan. 2010.

[13] F. Regazzoni, Y. Wang, and F.-X. Standaert, "FPGA implementations of the AES masked against power analysis attacks," *Constructive Side-Channel Analysis and Secure Design (COSADE)*, pp. 56–66, Feb. 2011.

[14] 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)*, pp. 1–9, Jun. 2013.

[15] P.-C. Liu, H.-C. Chang, and C.-Y. Lee, "A true random-based differential power analysis countermeasure circuit for an AES engine," *IEEE Transactions on Circuits and Systems II: Express Briefs*, Vol. 59, No. 2, pp. 103–107, Feb. 2012.

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

[17] K. Baddam and M. Zwolinski, "Evaluation of dynamic voltage and frequency scaling as a differential power analysis countermeasure," *in Proc. VLSI Design*, pp. 854–862, Jan. 2007.

[18] 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.

[19] 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, pp. 383–394, Feb. 2006.

[20] 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.

[21] A. Moradi and O. Mischke, "How far should theory be from practice?," *in Proc. Cryptographic Hardware and Embedded Systems (CHES)*, pp. 92–106, 2012.

[22] 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," *Integration, the VLSI Journal*, Vol. 46, No. 4, pp. 333–344, Sep. 2013.

[23] Z. Yuan, Y. Wang, J. Li, R. Li, and W. Zhao, "FPGA based optimization for masked AES implementation," *in Proc. International Midwest Symposium on Circuits and Systems (MWSCAS)*, pp. 1–4, Aug. 2011.

[24] W. Yu and S. Köse, "Exploiting voltage regulators to enhance various power attack countermeasures," *IEEE Transactions on Emerging Topics in Computing*, doi: 10.1109/TETC.2016.2620382.