A Lightweight Masked AES Implementation for Securing IoT Against CPA Attacks

Weize Yu and Selçuk Köse, *Member, IEEE*

***Abstract*— A false key-based advanced encryption standard (AES) technique is proposed to prevent the stored secret key leaking from the substitution-box under correlation power analysis (CPA) attacks without significant power and area overhead. Wave dynamic differential logic (WDDL)-based XOR gates are utilized during the reconstruction stage to hide the intermediate data that may be highly correlated with the false key. After applying the false key and designing the reconstruction stage with the WDDL, the minimum measurement-to-disclose value for the proposed lightweight masked AES engine implementation becomes over 150 million against CPA attacks. As compared to an unprotected AES engine, the power, area, and performance overhead of the proposed AES implementation is negligible.**

***Index Terms*— IoT security, false key-based masking, correlation power analysis attacks, wave dynamic differential logic.**

I. Introduction

EMERGENCE of internet of things (IoT) devices is challenging the conventional design targets for integrated systems such as energy efficiency, cost, noise, and performance. With the prospected proliferation of IoT devices with 5G networks, ensuring safe margins for these design targets will become even more crucial due to the limited battery life and significant physical constraints [1]. Additionally, IoT devices are quite vulnerable to hardware attacks since they are typically more accessible to an attacker as compared to the other general purpose computing devices. The limitations when combined with the cost constraints make the design of security measures for the IoT devices quite challenging. Regardless of these constraints, IoT devices still need to perform a certain level of secure computation by utilizing encryption algorithms such as advanced encryption standard (AES) [2], [3]. Various modifications have previously been proposed to make the hardware implementation of encryption algorithms more secure against side-channel attacks [4]–[11], such as using different logic styles and masking the actual stored key with random data. All of the existing countermeasures lead to significant power/area/performance overhead. Existing countermeasures utilized in general purpose computing devices are therefore typically not feasible for IoT devices. Novel power efficient and low-area overhead countermeasures are required to secure IoT devices against side-channel attacks (SCAs).

Lightweight cryptography is a critical requirement to efficiently protect the secret data that is being processed and/or stored within IoT devices from leaking to malicious attackers [12]–[14]. However, the secret key stored in an unprotected AES engine can be obtained by a malicious attacker with SCAs by exploiting certain physical leakage channels (*i.e.*, power dissipation, electromagnetic emissions, acoustics, temperature, and timing information) from the AES engine [15], [16]. Correlation power analysis (CPA) attacks are a type of SCAs to extract the secret key from an encryption engine efficiently and effectively by exploring the correlation between the input data and the power consumption profile [17]–[20]. For example, only 5,000-20,000 plaintexts would be sufficient to leak the secret key through CPA attacks from an unprotected AES engine [18], [20].

To protect an AES engine against CPA attacks, several masked AES[1] hardware implementation techniques have been proposed [21]–[24]. In masked AES implementations, random intermediate data are continuously added to the plaintexts during the encryption process to mask the side-channel leakage from substitution-boxes (S-boxes) which process the secret data. At the end of the encryption, the random intermediate data which are generated as a result of the masking operation are removed from the correct cipher data. A conventional masked AES engine, however, requires large look-up tables (LUTs) and the performance is significantly reduced due to the large amount of random masking data values [22], [23].

Alternatively, another countermeasure against CPA attacks can be performed by using balanced logic gates such as the wave dynamic differential logic (WDDL) [16], [25], sense amplifier-based logic (SABL) [26], [27], and dual-rail circuits [28], [29] to hide the dynamic power dissipation of the AES engine. Although perfectly balancing the dynamic power dissipation of logic circuits is challenging due to the mismatch of the load capacitance, delay-based technique [30] and time-enclosed logic (TEL) [31] have been proposed to minimize the mismatch of load capacitance with promising results. Unfortunately, balanced logic gates also impose significant area and performance overhead to the AES engine [16], [32].

In this paper, a false key-based AES technique is proposed by utilizing a single constant intermediate data I_c that is to be added to all of the correct round keys $K_{c,0}, K_{c,1}, \ldots, K_{c,m}$

[1] Throughout the paper, *masked AES* is used for *boolean masked AES.*

Manuscript received December 6, 2016; revised March 30, 2017; accepted May 1, 2017. Date of publication May 31, 2017; date of current version October 24, 2017. This work is 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 Research Award. This paper was recommended by Associate Editor M. Alioto. *(Corresponding author: Weize Yu.)*

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/TCSI.2017.2702098

1549-8328 © 2017 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.

(m is the number of AES encryption rounds) to generate false round keys $K_{f,0}, K_{f,1}, \ldots, K_{f,m}$ ($K_{f,i} = K_{c,i} \oplus I_c$ where $i = 0, 1, \ldots, m$). The generated false round keys $K_{f,0}, K_{f,1}, \ldots, K_{f,m}$ replace the corresponding correct round keys $K_{c,0}, K_{c,1}, \ldots, K_{c,m}$ during the encryption. At the end of the encryption, the mask is removed from the output, generating the correct cipher data. The primary difference between the conventional masked AES technique [21]–[24] and the proposed false key-based AES technique is the location of the masking operation. In the conventional masked AES technique, random intermediate data are utilized to mask the plaintexts only before the 1^{st} encryption round, whereas the masking operation is performed at all of the encryption rounds (see Fig. 5) in the proposed false key-based AES technique. When an attacker implements a CPA attack on the proposed false key-based AES technique, the attacker needs to perform the attack in two separate stages to be successful. In the first stage, the attacker needs to implement a regular CPA attack on the corresponding S-boxes to obtain the stored key, which in this case is the false round key $K_{f,i}$. In the second stage, the attacker needs to implement a CPA attack on the XOR gates which are used to remove the I_c-based mask to unriddle the correct round key $K_{c,i}$ within the reconstruction block. In the first stage, the attacker can obtain the false round key $K_{f,i}$ with relatively small effort since there exists no countermeasure in the S-boxes. However, when the attacker executes a CPA attack on the XOR gates within the reconstruction block, the high dynamic power dissipation of the S-boxes will act as noise that will significantly reduce the signal-to-noise ratio (SNR) of the side-channel dynamic power leakage from the XOR gates.

Although the relatively high dynamic power consumption of the S-boxes can act as power noise to reduce the SNR of these XOR gates under CPA attacks, the reduction in the SNR may not be sufficient to guarantee the security of the false key-based AES technique. To further reduce the SNR of the dynamic power that leaks from these XOR gates, WDDL-based XOR gates are utilized within the reconstruction block to remove the I_c-based mask in the proposed AES technique.

As compared to the conventional masked AES technique and fully WDDL implemented AES technique, the benefits of the proposed false key and WDDL assisted AES technique can be summarized as follows:

- The large area and performance overhead induced by the large size of the intermediate masking data can be eliminated since only one intermediate data value I_c is used for masking the correct round key $K_{c,i}$
- The large area and performance overhead of the AES technique that is fully WDDL implemented can be significantly reduced since only those XOR gates that are used within the reconstruction block are replaced with the WDDL gates

The rest of the paper is organized as follows. Related background on the conventional masked and fully WDDL implemented AES techniques is offered in Section II. Architecture and working principle of the false key and WDDL assisted AES technique are described, respectively, in Section III and Section IV. Security evaluation and circuit level verification of the proposed AES technique are provided, respectively, in Section V and Section VI. CPA attacks simulation is performed in Section VII and test vector leakage assessment (TVLA) simulation is provided in Section VIII. Comparisons with the state-of-the-art are summarized in Section IX, potential improvements against higher-order power analysis attacks are discussed in Section X. Conclusions are offered in Section XI.

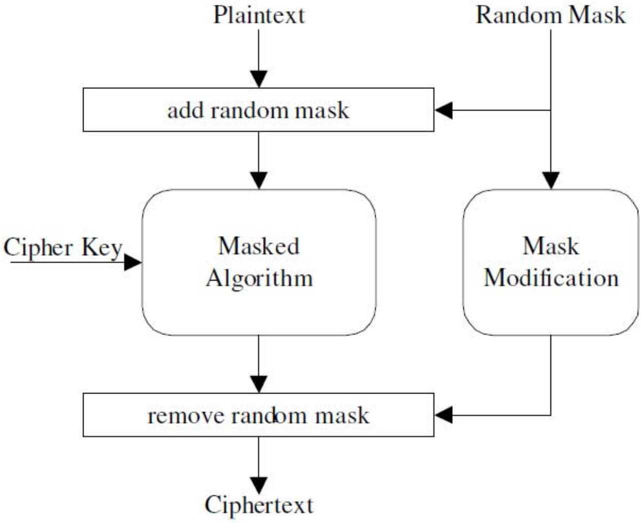


Fig. 1. Basic working principle of the conventional masked AES technique [21].

II. Background

A. Review of Conventional Masked AES Technique

In a conventional masked AES technique, the random mask data are added to the input plaintext at the beginning of the encryption, as shown in Fig. 1. When the encryption ends, the random mask component needs to be removed to generate the correct cipher data at the output. Since the S-boxes in an AES engine perform a non-linear data transformation, the random mask is intertwined with the plaintext after the non-linear transformations that occurs in the S-boxes. For example, if the plaintext is X and the random mask is B, since S-box($X \oplus B$)$\neq$S-box(X)$\oplus$S-box(B), the mask component would be quite difficult to remove when the encryption ends. To easily remove the mask component at the end of the encryption, in a conventional masked AES engine, the architecture of the S-boxes is modified to have the mask component separated from the encryption data after going through the non-linear transformations within the S-boxes (S-box($X\oplus B$)=S-box(X)$\oplus$S-box(B)). The architecture of the modified S-box is shown in Fig. 2 where the six distinct transforming tables in Fig. 2 are summarized as follows[2] [22], [33], [34]

$$T_{d1}: \ ((x_1^* + b_1^*), b_1^*) \rightarrow (x_1^*)^2 \times p_0 + b_1^*, \tag{1}$$

$$\begin{aligned} T_{d2}: \ & ((x_1^* + b_1^*), (x_2^* + b_2^*)) \\ & \rightarrow ((x_1^* + b_1^*) + (x_2^* + b_2^*)) \times (x_2^* + b_2^*), \end{aligned} \tag{2}$$

[2] "+" represents xor operation.

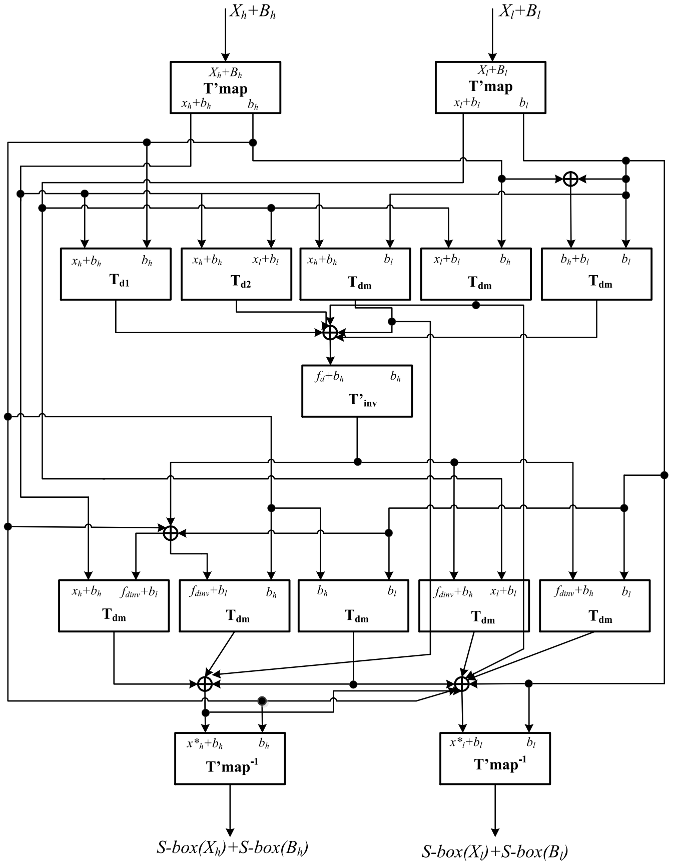


Fig. 2. Architecture of the reconstructed S-box from [22], [23] (X_h (X_l) and B_h (B_l) represent the high (low) 4-bit of the encryption data and the high (low) 4-bit of the masking data at the input side of the reconstructed S-box, respectively. S-box(X_h) (S-box(X_l)) and S-box(B_h) (S-box(B_l)) denote the high (low) 4-bit of the encryption data and the high (low) 4-bit of the masking data at the output side of the reconstructed S-box, respectively).

$$T_m: ((x_1^* + b_1^*), (x_2^* + b_2^*)) \rightarrow (x_1^* + b_1^*) \times (x_2^* + b_2^*), \quad (3)$$

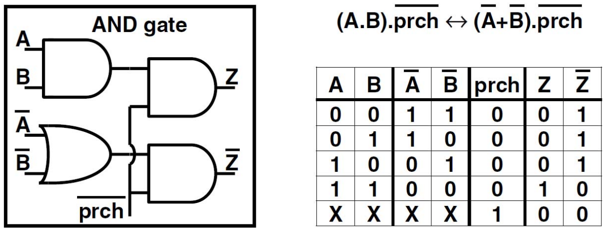
$$T_{inv}^{'}: \ ((x_1^* + b_1^*), b_1^*)) \rightarrow T_{inv}(x_1^*) + b_1^*, \quad (4)$$

$$T^{'}map: \ ((x_1^* + b_1^*), b_1^*)) \rightarrow Tmap(x_1^* + b_1^*), \quad (5)$$

$$T^{'}map^{-1}: \ ((x_1^* + b_1^*), b_1^*)) \rightarrow Tmap^{-1}(x_1^* + b_1^*), \quad (6)$$

where x_1^* (b_1^*) and x_2^* (b_2^*) are the 4-bit encryption (masking) data which are linked with the input of each table. p_0 is the binary coefficient of the 4-bit data $(x_1^*)^2$. T_{inv}, $Tmap$, and $Tmap^{-1}$ are, respectively, the inverse operation, mapping operation, and inverse mapping operation which occur in the conventional S-box. Please note that T_{inv} performs a non-linear operation, while $Tmap$ and $Tmap^{-1}$ perform linear operations.

Although the conventional masked AES engine is an effective countermeasure against first-order CPA attacks, the large size of data to perform the random masking impose significant area and performance overhead. For example, a 128-bit masked AES engine that is implemented in a field-programmable gate array (FPGA) leads to 60.1% area and 11% performance overhead [24].


AND gate
A
B
$\overline{A}$
$\overline{B}$
prch
Z
$\overline{Z}$
$(A.B).\overline{prch} \leftrightarrow (\overline{A}+\overline{B}).\overline{prch}$

A	B	$\overline{A}$	$\overline{B}$	prch	Z	$\overline{Z}$
0	0	1	1	0	0	1
0	1	1	0	0	0	1
1	0	0	1	0	0	1
1	1	0	0	0	1	0
X	X	X	X	1	0	0

Fig. 3. Architecture of the SDDL-based AND gate (left) and the corresponding truth table (right) [35].

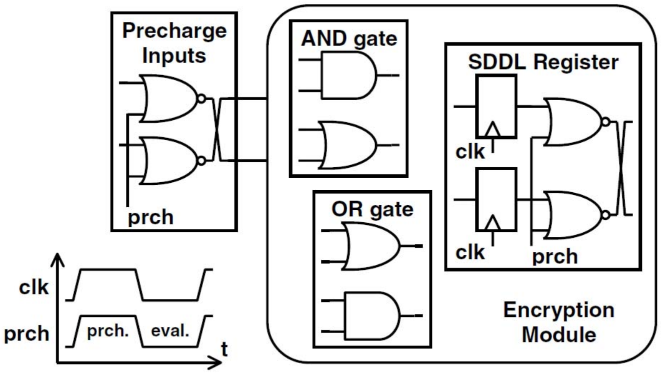


Fig. 4. Architecture of the WDDL-based AND and OR gates [35].

B. Fully WDDL Implemented AES Technique

In CMOS logic circuits, the dynamic power dissipation occurs only when the output logic state makes a transition from 0 to 1 [28], [35]. The architecture of a simple dynamic differential logic (SDDL) based AND gate is shown in Fig. 3. If the precharge signal $prch$ is set to 1, the output logic Z and the complementary output logic $\overline{Z}$ of the SDDL-based AND gate are both 0. When $prch$ makes a transition from 1 to 0, either Z or $\overline{Z}$ has a one time $0 \rightarrow 1$ transition under any input data. As a result, the SDDL-based AND gate exhibits the same dynamic power dissipation regardless of the input data.

Although the dynamic power consumption of the SDDL-based logic gates is independent of the input data, the time delay between the input data and the precharge signal can be observed in the dynamic power consumption [35]. Therefore, in order to eliminate the signature of the time delay difference from the dynamic power consumption profile, WDDL-based logic gates have been proposed [35] by using an SDDL register to synchronize the input data with the precharge signal, as shown in Fig. 4. An AES engine that is implemented completely with the WDDL leads to significant area and performance overhead. For example, a 128-bit AES engine that is implemented completely with the WDDL results in 210.1% area and 74.2% performance overhead [16], [32].

III. Architecture of the Proposed Lightweight AES Technique

The architecture of a false key-based n-bit AES engine is illustrated in Fig. 5. A constant intermediate data[3]

[3] $I_c \neq (000\ldots0)_2$. Since $K_{f,i} = K_{c,i} \oplus (000\ldots0)_2 = K_{c,i}$, the false round key $K_{f,i}$ is equal to the correct round key $K_{c,i}$ if $I_c = (000\ldots0)_2$.

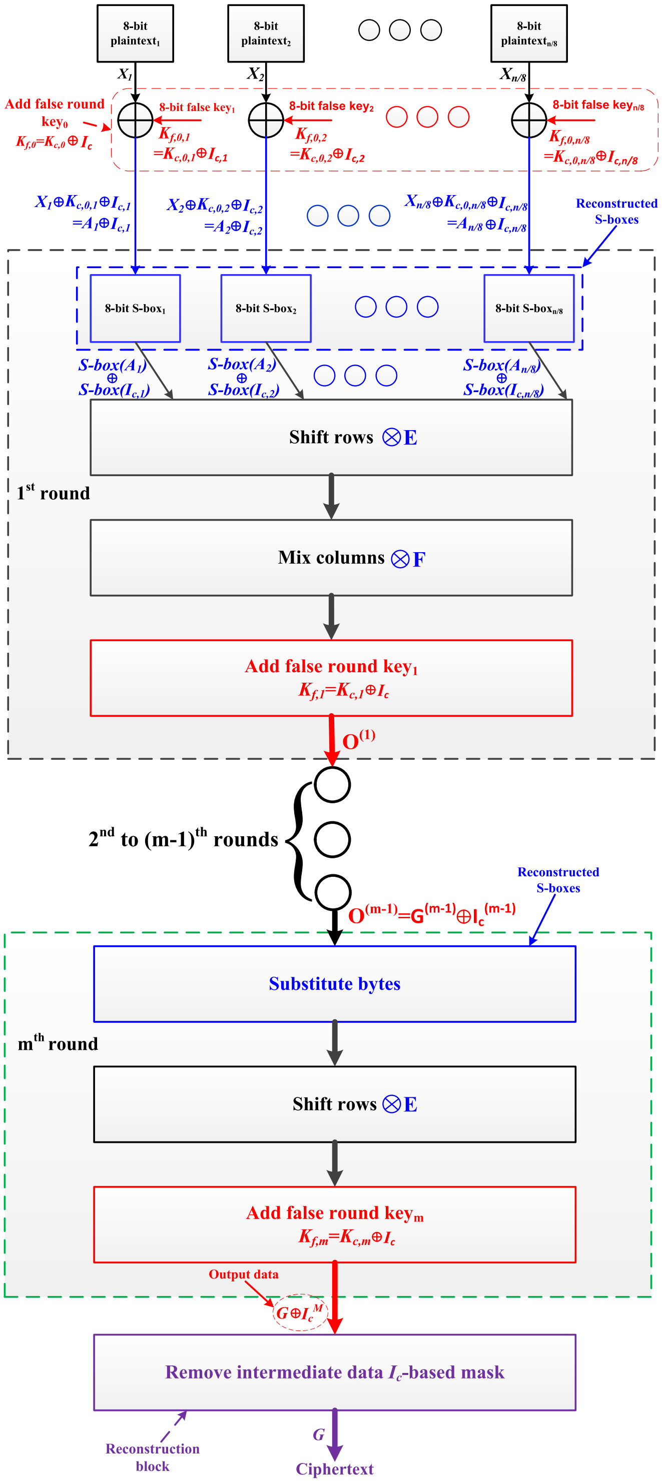

8-bit plaintext$_1$
8-bit plaintext$_2$
8-bit plaintext$_{n/8}$
X_1
X_2
$X_{n/8}$
Add false round key$_0$
$K_{f,0}=K_{c,0}\oplus I_c$
8-bit false key$_1$
$K_{f,0,1}=K_{c,0,1}\oplus I_{c,1}$
8-bit false key$_2$
$K_{f,0,2}=K_{c,0,2}\oplus I_{c,2}$
8-bit false key$_{n/8}$
$K_{f,0,n/8}=K_{c,0,n/8}\oplus I_{c,n/8}$
$X_1\oplus K_{c,0,1}\oplus I_{c,1}=A_1\oplus I_{c,1}$
$X_2\oplus K_{c,0,2}\oplus I_{c,2}=A_2\oplus I_{c,2}$
$X_{n/8}\oplus K_{c,0,n/8}\oplus I_{c,n/8}=A_{n/8}\oplus I_{c,n/8}$
Reconstructed S-boxes
8-bit S-box$_1$
8-bit S-box$_2$
8-bit S-box$_{n/8}$
$S\text{-}box(A_1)\oplus S\text{-}box(I_{c,1})$
$S\text{-}box(A_2)\oplus S\text{-}box(I_{c,2})$
$S\text{-}box(A_{n/8})\oplus S\text{-}box(I_{c,n/8})$
Shift rows $\otimes$E
1st round
Mix columns $\otimes$F
Add false round key$_1$
$K_{f,1}=K_{c,1}\oplus I_c$
$O^{(1)}$
2nd to (m-1)th rounds
$O^{(m-1)}=G^{(m-1)}\oplus I_c^{(m-1)}$
Reconstructed S-boxes
Substitute bytes
mth round
Shift rows $\otimes$E
Add false round key$_m$
$K_{f,m}=K_{c,m}\oplus I_c$
Output data
$G\oplus I_c^M$
Remove intermediate data I_c-based mask
Reconstruction block
G
Ciphertext

Fig. 5. Architecture of the proposed n-bit false key-based AES engine.

$I_c = (I_{c,1}, I_{c,2}, \ldots, I_{c,n/8})$ is added to the correct round key $K_{c,i} = (K_{c,i,1}, K_{c,i,2}, \ldots, K_{c,i,n/8})$ to generate the false key $K_{f,i} = K_{c,i} \oplus I_c = (K_{c,i,1} \oplus I_{c,1}, K_{c,i,2} \oplus I_{c,2}, \ldots, K_{c,i,n/8} \oplus I_{c,n/8})$. In the 1^{st} encryption round, when the input plaintext is $X = (X_1, X_2, \ldots, X_{n/8})$, the input data of the $j^{th}(j = 1, 2, \ldots, n/8)$ S-box is $X_j \oplus K_{c,0,j} \oplus I_{c,j} = A_j \oplus I_{c,j}$ where A_j is the standard encryption data and $I_{c,j}$ can be considered as the corresponding mask ($A = (A_1, A_2, \ldots, A_{n/8}) = X \oplus K_{c,0}$). In order to remove the I_c-based mask without significant effort at the end of the encryption, the reconstructed S-boxes from the conventional masked AES engine [23], [34] are used to separate the mask from the encryption data, as shown in Fig. 2. As a result, the output data of the j^{th} S-box in the 1^{st} encryption round become S-box$(A_j)\oplus$ S-box$(I_{c,j})$, as shown in Fig. 5. In the remaining encryption rounds, the false round keys $K_{f,1}, K_{f,2}, \ldots, K_{f,m}$ are also implemented to mask the leakage of correct round keys $K_{c,1}, K_{c,2}, \ldots, K_{c,m}$.

When the encryption process ends (after the m^{th} encryption round), the output data of the false key-based AES engine can be denoted as $G \oplus I_c^M$ where G is the correct cipher data and I_c^M is the residue of the intermediate I_c-based mask. Please note that the intermediate data I_c has a constant value, so the I_c-based mask I_c^M also has a constant value. The constant mask data can be linearly separated from the encryption data. Therefore, after the 1^{st} round of encryption, as shown in Fig. 5, the output data $O^{(1)}$ becomes

$$\begin{aligned}
&O^{(1)}\\
&= (S - box(A) \oplus S - box(I_c)) \otimes E \otimes F \oplus K_{c,1} \oplus I_c\\
&= S - box(A) \otimes E \otimes F \oplus K_{c,1} \oplus S - box(I_c) \otimes E \otimes F \oplus I_c,
\end{aligned} \tag{7}$$

where E and F are, respectively, the matrices to perform the shift rows and mix columns operations, as shown in Fig. 5. $I_c^{(1)}$=S-box$(I_c) \otimes E \otimes F \oplus I_c$ is the mask component after the 1^{st} round of encryption. Let us assume the output data of the $\gamma^{th}, (\gamma = 2, 3, \ldots, m-1)$ encryption round is $O^{(\gamma)} = G^{(\gamma)} \oplus I_c^{(\gamma)}$ where $G^{(\gamma)}$ is the encryption data and $I_c^{(\gamma)}$ is the mask component. Since from the 2^{nd} encryption round to the $(m-1)^{th}$ encryption round, the encryption processes are repeated. The relationship between $I^{(\gamma)}$ and $I_c^{(\gamma-1)}$ can therefore be written as

$$I_c^{(\gamma)} = S - box(I_c^{(\gamma-1)}) \otimes E \otimes F \oplus I_c. \tag{8}$$

However, since the final (m^{th}) encryption round does not have the mix columns operation, the relationship between I_c^M and $I_c^{(m-1)}$ is

$$I_c^M = S - box(I_c^{(m-1)}) \otimes E \oplus I_c. \tag{9}$$

The last step is to remove the mask I_c^M to recover the correct ciphertexts when the encryption ends with a reconstruction block, as shown in Fig. 5. The $y^{th}, (y = 1, 2, \ldots, n)$ bit of the output data of the false key-based AES engine $G_y \oplus I_{c,y}^M$ needs to be added with the y^{th} bit of I_c^M to recover the y^{th} bit of the correct ciphertexts G_y $(G_y \oplus I_{c,y}^M \oplus I_{c,y}^M = G_y)$. As shown in Fig. 6, WDDL-based XOR gates are selected for achieving the operation of removing the residual mask related data I_c^M.

IV. Practical CPA Attacks on the Proposed AES Engine

A successful CPA attack against the proposed false key and WDDL assisted AES implementation needs to contain two steps. In the first step, a regular CPA attack should be performed on the S-boxes. The attacker applies a series of

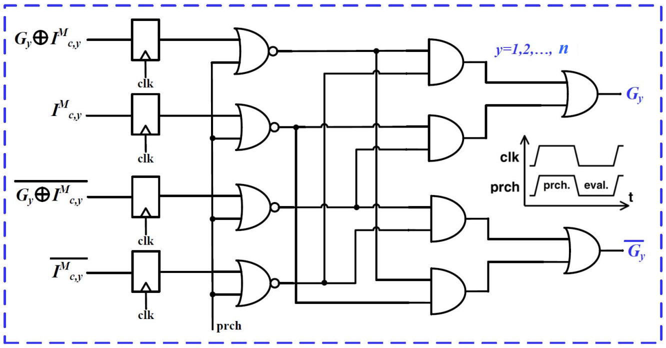


Fig. 6. Architecture of the reconstruction block to remove the intermediate data I_c-based mask I_c^M at the end of the m^{th} encryption round (implemented with the WDDL-based XOR gates).

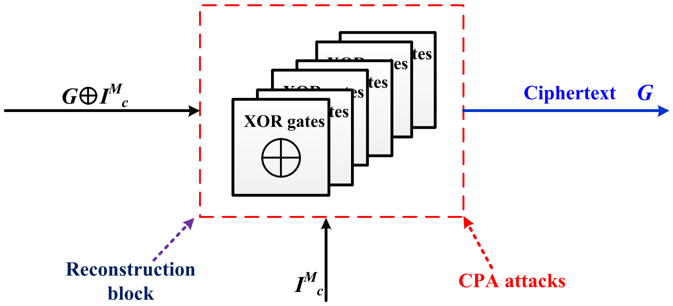


Fig. 7. CPA attacks on the reconstruction block while it removes the intermediate data I_c-based mask I_c^M from the ciphertext.

plaintexts that consider all of the possible combinations of the stored secret key and develops a suitable power model to estimate the resulting power consumption profiles. The attacker then measures the resulting dynamic power consumption profile for each plaintext and performs a correlation analysis to calculate the correlation coefficient between the predicted and measured power profiles. After analyzing a sufficient number of power consumption data, the hypothesized key with the highest correlation coefficient is identified as the correct key by the attacker. In the proposed false key-based AES engine, for instance, if the attacker performs a regular CPA attack on the S-boxes of the 1^{st} encryption round, only the false round key $K_{f,0}$ can be obtained since the false round key $K_{f,0}$ is added to the input plaintext X before the 1^{st} encryption round as shown in Fig. 5.

In the second step, the attacker needs to obtain the intermediate data I_c to distinguish the correct round key $K_{c,i}$ from the false round key $K_{f,i}$. Therefore, the attacker needs to implement a CPA attack on the reconstruction block, shown in Fig. 5 and Fig. 7, to determine the intermediate data I_c. Since the false round key $K_{f,i}$ can be obtained in the first step, the attacker can determine the output data of the false key-based AES engine $G \oplus I_c^M$ by using $K_{f,i}$. Therefore, the attacker can combine the output data $G \oplus I_c^M$ with all of the possible I_c^M to predict the dynamic power consumption of the XOR gates by using a hypothetical power model. After measuring the dynamic power consumption of the XOR gates within the reconstruction block with CPA attacks, the hypothesized I_c^M with the highest correlation coefficient is likely to be the correct I_c^M. The intermediate data I_c and correct round key $K_{c,i}$ can be unriddled when the attacker determines the correct I_c^M.

When the attacker measures the dynamic power dissipation of those XOR gates within the reconstruction block, the high dynamic power consumption of the S-boxes acts as additional power noise that reduces the SNR of the related power dissipation of the XOR gates. This additional power noise may, however, not be sufficient to reduce the SNR of the XOR gates to eliminate the risk of a successful CPA attack. Therefore, as shown in Fig. 6, WDDL-based XOR gates are utilized in the reconstruction block to further decrease the SNR. Since no countermeasure exists within the S-boxes, the security of the reconstruction block determines the security of the proposed false key and WDDL assisted AES implementation.

V. Security Evaluation

For a WDDL-based XOR gate, although the output logic and the complementary output logic have one 0 → 1 transition under any input data, the capacitance mismatch between the output and complementary output may leak some information in the form of power variation from the WDDL-based XOR gate [35]. The corresponding power variation ΔP_w that is induced by the capacitance mismatch of the WDDL-based XOR gate can be denoted as

$$\begin{aligned}\Delta P_w &= P_{w,1} - P_{w,0} = C_{L,1} f_c V_{dd}^2 - C_{L,2} f_c V_{dd}^2 \\ &= (C_{L,1} - C_{L,2}) f_c V_{dd}^2 = \Delta C_L f_c V_{dd}^2,\end{aligned} \tag{10}$$

where $P_{w,1}$ and $P_{w,0}$ are, respectively, the dynamic power dissipation of the WDDL-based XOR gate when the output logic and complementary output logic make transitions from 0 → 1. $C_{L,1}$ and $C_{L,2}$ are, respectively, the load capacitance of the output and complementary output. ΔC_L is the mismatch capacitance, f_c is the clock frequency, and V_{dd} is the supply voltage.

In an n-bit false key and WDDL assisted AES engine, if the attacker performs a CPA attack on the WDDL-based XOR gates to obtain the I_c^M, the attacker can choose k bits out of the n-bit I_c^M each time to perform a CPA attack ($1 \leq k \leq n$). Let's assume that x, ($x = 0, 1, 2, \ldots, k$) out of k number of WDDL-based XOR gates make a transition from 0 → 1 in the output. Since x conforms to a binomial distribution, as illustrated with the simulation result in Fig. 8(a), the corresponding mean value $E(x)$ and variance $D(x)$ can be obtained as

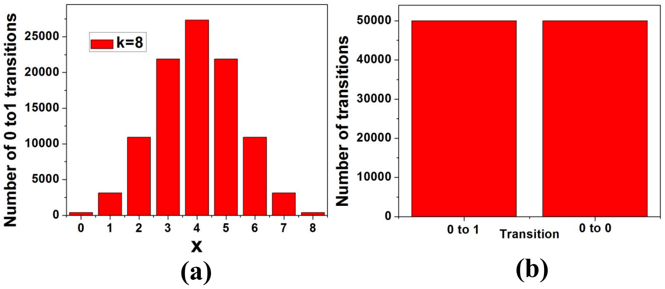
$$E(x) = k \times p = \frac{1}{2}k, \tag{11}$$

$$D(x) = k \times p \times (1 - p) = \frac{1}{4}k, \tag{12}$$

where p is the probability that the output logic makes a transition from 0 → 1 and p is equal to 1/2 as shown with the simulation result in Fig. 8(b).

The variance $D(kP_{w,0} + x\Delta P_w)$ of the power dissipation of k number of WDDL-based XOR gates under CPA attacks can be determined as

$$D(kP_{w,0} + x\Delta P_w) = 0 + D(x) \times (\Delta P_w)^2 = \frac{1}{4}k(\Delta P_w)^2. \tag{13}$$



(a) (b)

Fig. 8. (a) Number of 0 → 1 transitions versus x for eight WDDL-based gates (under 100, 000 tests). (b) Numbers of 0 → 1 and 0 → 0 transitions at the output of a WDDL-based gate (under 100, 000 tests).

When the attacker applies variable plaintexts to the false key-based AES engine, all of the S-boxes in the false key-based AES engine would exhibit high dynamic power consumption. The dynamic power consumption generated by these S-boxes acts as power noise to protect the WDDL-based XOR gates against CPA attacks. Note that the dynamic power consumption of cryptographic circuits conforms to a normal distribution [36]. The mean and variance of the dynamic power consumed by the false key-based AES engine are, respectively, μ_{ar} and σ_{ar}^2. The SNR of the power profile of the k number of WDDL-based XOR gates in reconstruction block under CPA attacks SNR_k can be written as

$$SNR_k = \frac{\sigma_S^2}{\sigma_N^2} = \frac{\sigma_k^2}{\sigma_{ar}^2 + \sigma_{n-k}^2} = \frac{\frac{1}{4}k(\Delta P_w)^2}{\sigma_{ar}^2 + \frac{(n-k)}{4} \times (\Delta P_w)^2}, \tag{14}$$

where σ_S^2 and σ_N^2 are, respectively, the variance of the signal and noise. σ_k^2 is the variance of the power dissipated by the k number of WDDL-based XOR gates that are under CPA attacks while σ_{n-k}^2 is the variance of the $(n - k)$ number of the WDDL-based XOR gates that are not targeted by the CPA attacks in the reconstruction block.

The corresponding correlation coefficient γ_k and the MTD value MTD_k of the k number of WDDL-based XOR gates that are under CPA attacks can be estimated as [36]

$$\gamma_k = \frac{1}{\sqrt{1 + \frac{1}{SNR_k}}}, \tag{15}$$

$$MTD_k \simeq c \times \frac{1}{\gamma_k^2}, \tag{16}$$

where c is the success rate dependent coefficient [36]. By substituting (14) and (15) into (16), MTD_k can be written as

$$MTD_k = c \times (1 + \frac{\sigma_{ar}^2 + \frac{(n-k)}{4} \times (\Delta P_w)^2}{\frac{1}{4}k(\Delta P_w)^2}). \tag{17}$$

For each attack when the attacker selects k bits of the n-bit I_c^M to perform a CPA attack, 2^k possible values need to be hypothesized. However, if the attacker implements a CPA attack on one of the 8-bit S-boxes, 2^8 possible keys need to be considered. Since the attacker can choose a variable number of bits to perform the CPA attack on I_c^M, in order to compare with the CPA attacks on S-boxes, the total normalized MTD value MTD_{nor} to perform a CPA attack on the n-bit I_c^M is defined as (assuming that n/k is an integer)

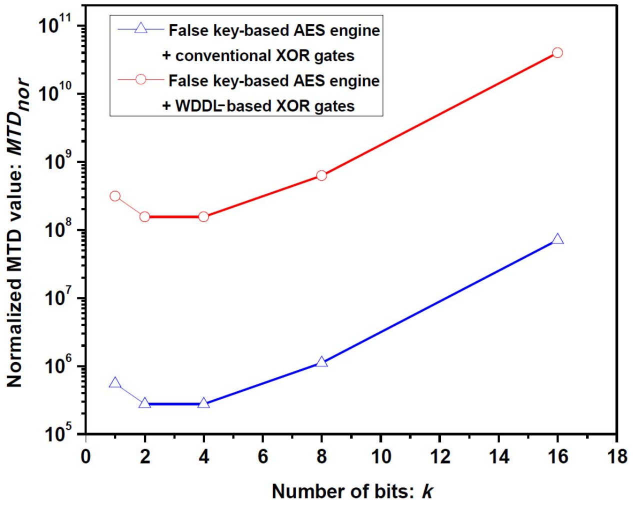


Fig. 9. Normalized MTD value versus k number of bits of I_c^M under CPA attacks against a 128-bit false key-based AES engine with WDDL-based XOR gates within the reconstruction block and a 128-bit false key-based AES engine with conventional XOR gates.

$$MTD_{nor} = \frac{2^k}{2^8}\frac{n}{k} \times c \times (1 + \frac{\sigma_a^2 + \frac{(n-k)}{4} \times (\Delta P_w)^2}{\frac{1}{4}k(\Delta P_w)^2}). \tag{18}$$

A. Proposed False Key and WDDL Assisted AES Engine Against CPA Attacks

The proposed 128-bit false key and WDDL assisted AES engine is designed at 130 nm CMOS technology node and simulated in Cadence. The standard deviation of the dynamic power dissipation of the false key-based AES engine is $\sigma_{ar} = 107.2\ uW$. Since no complementary output exists in a conventional XOR gate to balance the power dissipation, the power variation of a conventional XOR gate is significantly larger than the power variation of a WDDL-based XOR gate. Note that when the power signature has more variation that is correlated with the operation, the amount of information leakage may increase. The corresponding power variations of a WDDL-based XOR gate and a conventional XOR gate under process-voltage-temperature (PVT) Monte Carlo simulation are, respectively, $0.038\ uW$ and $1.054\ uW$.

The relationship between MTD_{nor} and k number of bits of I_c^M under CPA attacks is shown in Fig. 9. The minimum MTD value of a 128-bit false key-based AES with WDDL-based XOR gates to remove the mask is around 1.59×10^8 when the number of bits is $k = 4$. Alternatively, the corresponding minimum MTD value of a 128-bit false key-based AES with conventional XOR gates for removing the mask is about 2.07×10^5. Utilizing the WDDL only in the reconstruction block still increases the MTD value by more than 768 times.

B. Impact of Technology Scaling on the Proposed Technique Against CPA Attacks

The load capacitance C_L of a CMOS logic gate can be denoted as [37]

$$C_L \approx n^* C_{ox}^* (L_g W_n + L_g W_p), \tag{19}$$

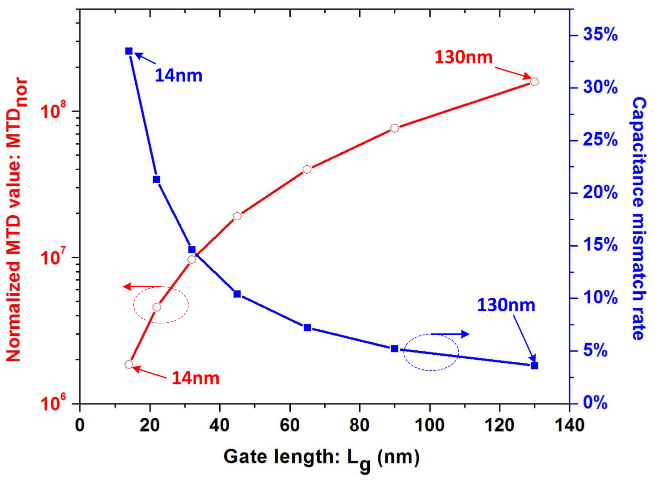


Fig. 10. Scaled gate length L_g versus normalized MTD value and capacitance mismatch rate for a 128-bit false key-based AES engine with WDDL-based XOR gates within the reconstruction block.

where C_{ox}^* is the gate capacitance density of NMOS and PMOS. L_g is the gate length of NMOS and PMOS. W_n (W_p) is the gate width of NMOS (PMOS).

Assuming that the feature size of the CMOS logic gate scales with a scaling factor s, the scaled load capacitance $C_L(s)$ of the CMOS logic gate becomes

$$C_L(s) \approx sC_{ox}^*(\frac{L_g}{s}\frac{W_n}{s} + \frac{L_g}{s}\frac{W_p}{s}) = \frac{C_{ox}^*(L_g W_n + L_g W_p)}{s} = \frac{C_L}{s}. \tag{20}$$

When the load capacitance mismatch of a WDDL-based XOR gate induced by the process-voltage-temperature (PVT) variations is ΔC_L, the capacitance mismatch ratio of the WDDL-based XOR gate ω_0 can be written as

$$\omega_0 = \frac{\Delta C_L}{C_L}. \tag{21}$$

Assuming that the feature size of the WDDL-based XOR gate is also scaled with the same scaling factor s, the scaled capacitance mismatch ratio $\omega(s)$ and power variance of the scaled AES engine, respectively, become

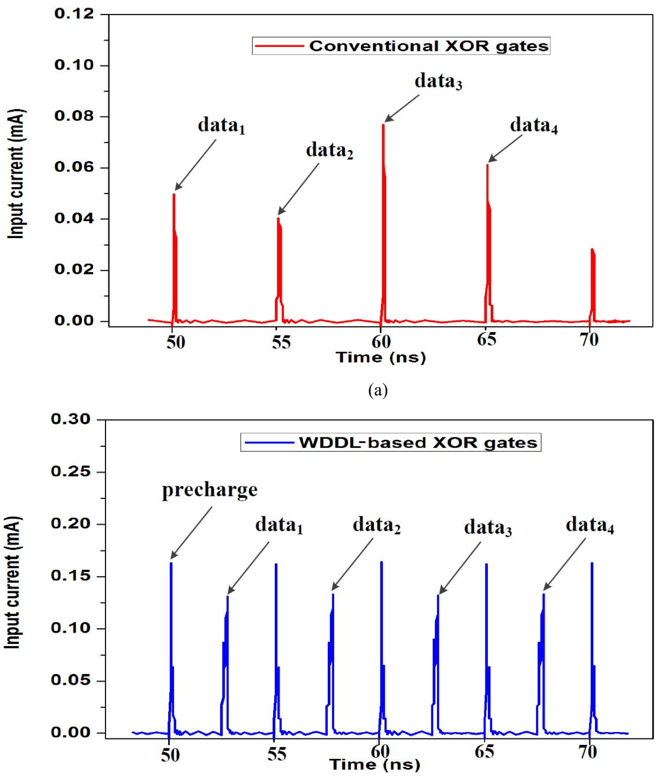
$$\omega(s) = s\frac{\Delta C_L}{C_L} = s\omega_0, \tag{22}$$

$$\sigma_{ar}^2(s) = \frac{\sigma_{ar}^2}{s^2}. \tag{23}$$

By using (18), when the feature size of the false key and WDDL assisted AES engine is scaled from 130 nm to 14 nm, the load capacitance mismatch rate of the WDDL-based XOR gate is increased from 3.6% to 33.5%, as shown in Fig. 10. Moreover, if the number of bits $k = 4$, the minimum MTD value of the proposed 128-bit false key and WDDL assisted AES engine decreases from 1.59×10^8 to 1.85×10^6 when the feature size is scaled from 130 nm to 14 nm.

VI. Circuit Level Evaluation

In the false key-based AES engine, if the attacker chooses $k = 4$ bits of the mask I_c^M in the reconstruction block for each CPA attack sample, the input current profile of four conventional XOR gates and WDDL-based XOR gates under CPA attacks are shown in Fig. 11(a) and Fig. 11(b), respectively. The input current of conventional XOR gates varies significantly when the input data change, as shown in Fig. 11(a). Alternatively, the input current of WDDL-based XOR gates has a negligible variation under different input data, as shown in Fig. 11(b). Furthermore, as compared to the false key-based AES engine with conventional XOR gates within the reconstruction block, the false key-based AES engine with WDDL-based XOR gates within the reconstruction block has a negligible power overhead, as shown in Fig. 12.



(a)

(b)

Fig. 11. (a) Input current profile of four conventional XOR gates under different input data. (b) Input current profile of four WDDL-based XOR gates under different input data.

VII. CPA Attacks Simulation

CPA attacks are performed on the following four implementations: i) 128-bit unprotected AES engine, ii) conventional masked AES engine, iii) false key-based AES engine with conventional XOR gates to remove the mask I_c^M, and iv) the proposed false key and WDDL assisted AES engine. All of these different encryption engines are implemented with 130 nm CMOS technology node in Cadence. A hamming-weight (HW) based power prediction model is used in the simulations. In this model, the polarity of the correlation coefficient can be used to distinguish the correct key (data) and the complement of the correct key (data) [38]. For a 128-bit unprotected AES engine, when one of the 16 S-boxes is targeted by CPA attacks – assuming the attacker

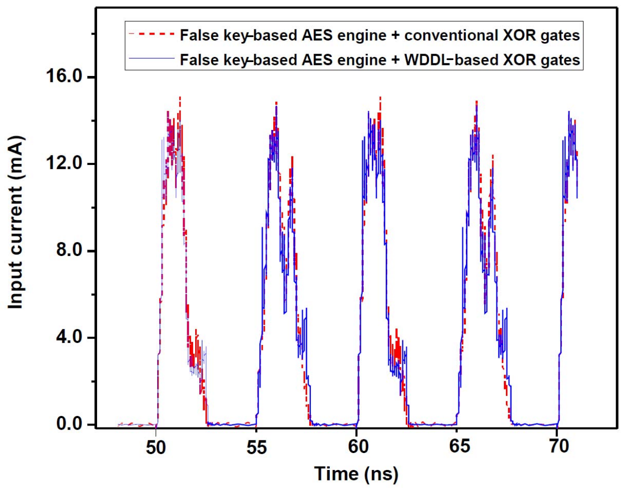


Fig. 12. Input current profile of a 128-bit false key-based AES engine that has WDDL-based XOR gates in the reconstruction block and a 128-bit false key-based AES engine with conventional XOR gates.

TABLE I

SUMMARIZED SIMULATION RESULTS OF CPA ATTACKS

	AES technique without countermeasure	Conventional masked AES technique	False key- based AES technique	False key and WDDL assisted AES technique
MTD value	$\approx 1.6\times10^5$	$>1.6\times10^7$	$\approx 9\times10^5$	$>3\times10^7$

inputs variable plaintexts to the AES engine – the correct key[4] $(92)_{10}$ can be leaked to the attacker after inputting a mere 10,000 plaintexts, as shown in Fig. 13(a). Alternatively, when the attacker performs CPA attacks on one of the 16 S-boxes in the 128-bit conventional masked AES engine, the correct key $(92)_{10}$ is prevented from leaking to the attacker even if 1 million plaintexts are enabled, as shown in Fig. 13(b). Although the conventional masked AES technique can enhance the MTD value over 100 times, the related overheads of 60.1% area increase and 11% performance degradation make the conventional masked AES implementation quite challenging [24].

As explained previously, XOR gates are typically utilized to remove the mask I_c^M in masked AES implementations. Let's assume that the CPA attacks are performed on those XOR gates in the false key-based AES engine that houses conventional XOR gates. When the attacker selects $k = 4$ bits of the mask I_c^M while performing the CPA attacks, the correct data[5] $(3)_{10}$ can be leaked to the attacker after inputting 450,000 plaintexts due to the large side channel power leakage from the conventional XOR gates, as shown in Fig. 13(c).

Alternatively, when $k = 4$ number of WDDL-based XOR gates are utilized to remove the mask I_c^M in the proposed 128-bit false key and WDDL assisted AES engine, the correct data $(3)_{10}$ is masked from leaking to the attacker implementing CPA attacks even after inputting 15 million plaintexts, as shown in Fig. 13(d). This over 30× increase in the MTD value is primarily due to the tiny power leakage from the WDDL-based XOR gates as compared to the large power leakage from the conventional XOR gates. In order to compare the security of the proposed 128-bit false key and WDDL assisted AES engine with the 128-bit unprotected AES engine against CPA attacks, the normalized MTD value of the proposed 128-bit false key and WDDL assisted AES engine can be obtained – by utilizing equation (18) – as follows

$$(2^4/2^8) \times (128/4) \times 1.5 \times 10^7 = 3 \times 10^7. \tag{24}$$

Please note that the MTD value for a successful attack on a single S-box of the unprotected AES engine is about 10,000 as demonstrated in Fig. 13(a). The total MTD value that is required to successfully disclose the secret keys within all the 16 S-boxes of the 128-bit unprotected AES engine would therefore be around 160,000. As a result, the MTD value can be enhanced over 187.5 times after employing the proposed false key and WDDL assisted AES technique. The summarized simulation results of the CPA attacks are shown in Table I.

VIII. TEST VECTOR LEAKAGE ASSESSMENT (TVLA) SIMULATION

To validate the reliability of the CPA attacks simulation on the proposed false key and WDDL assisted AES technique in Section VII, the test vector leakage assessment (TVLA) is performed. The objective of a TVLA is to study the impact of the input data pattern on the security of the proposed technique [39]. TVLA is achieved by utilizing Welch's t-test. Two different types of input data: fixed input data and random input data need to be used for verification. Assuming that the number of fixed plaintexts is n_1 and the number of random plaintexts is n_2, the t-test value α can be defined as [39]

$$\alpha = \frac{\overline{y}_1 - \overline{y}_2}{\sqrt{\frac{\sigma_1^2}{n_1} + \frac{\sigma_2^2}{n_2}}}, \tag{25}$$

where $\overline{y}_1$ ($\overline{y}_2$) is the average power dissipation induced by fixed (random) plaintexts and σ_1^2 (σ_2^2) is the variance of the power dissipation induced by fixed (random) plaintexts. When $|\alpha| < 4.5$, the input data pattern can be considered to have negligible impact on the security of the proposed technique [39]. However, if $|\alpha| > 4.5$, it can be considered that the attacker can leak a higher amount of critical information from the device by selecting different input data patterns [39].

As shown in Fig. 14, the t-value α is always within the t-threshold ($-4.5 < \alpha < 4.5$) even if the number of input plaintexts is over 15 million. Therefore, the proposed false key and WDDL assisted AES technique leaks negligible critical information through selecting the pattern of the input data.

IX. COMPARISON WITH PREVIOUS WORKS

The proposed false key and WDDL assisted AES technique is compared with the following techniques: switching capacitor countermeasure [20], WDDL countermeasure [16], ring oscillator countermeasure [32], conventional masking technique [24], and DPA resistant encryption by construction (DRECON) technique [40], [41]. As shown in Table II,

[4] $(92)_{10} = (01011100)_2$ is selected as the correct key for the 8-bit S-box of the 128-bit AES engine under CPA attacks.

[5] $(3)_{10} = (0011)_2$ is chosen as the correct data for the 4 bits of the mask I_c^M under CPA attacks.

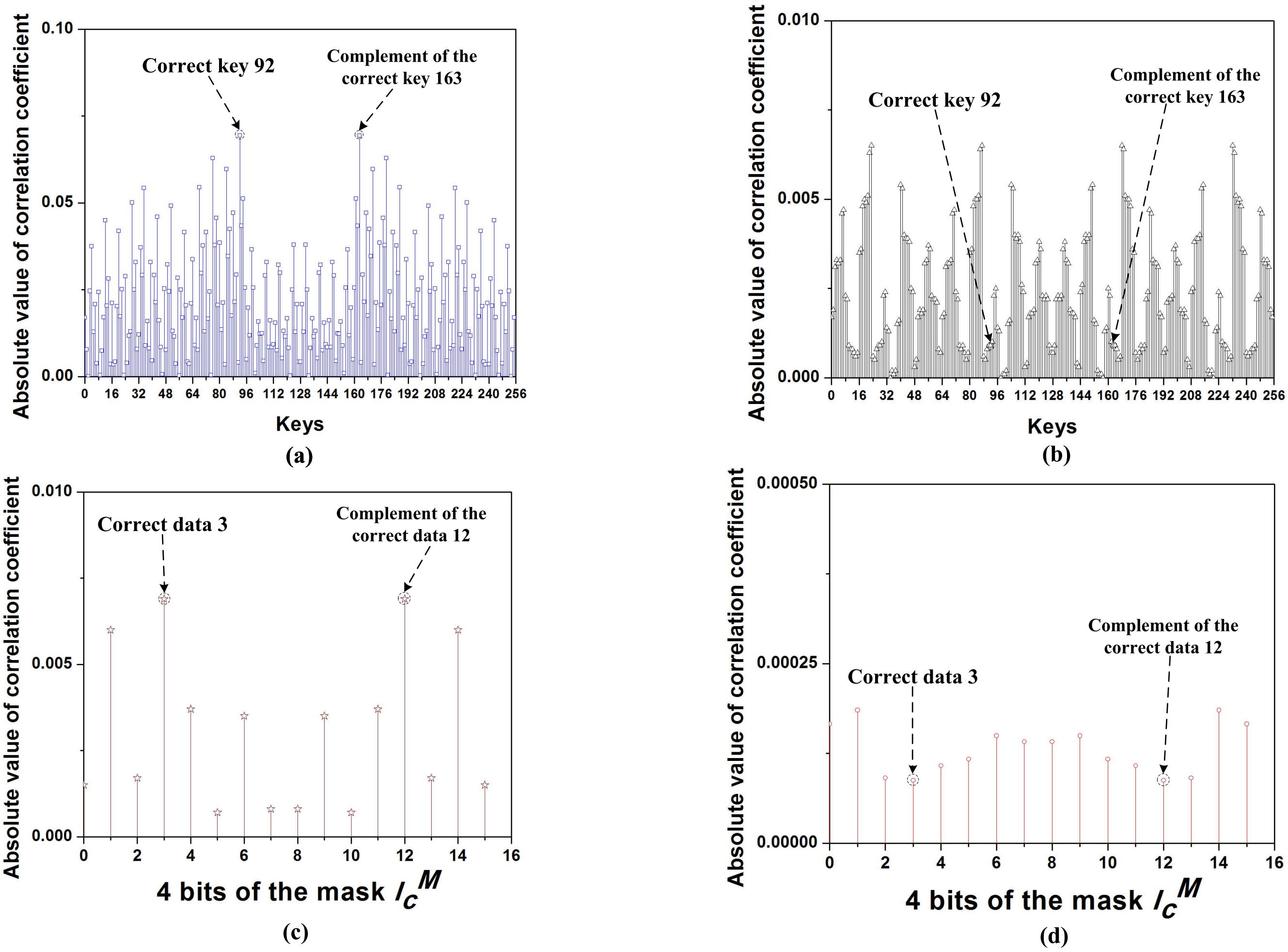


Fig. 13. CPA attacks simulation. (a) All of the possible keys of an 8-bit S-box versus absolute value of the correlation coefficient when one of the 16 S-boxes in a 128-bit unprotected AES engine is under CPA attacks after inputting 10,000 plaintexts. (b) All of the possible keys of an 8-bit S-box versus absolute value of the correlation coefficient when one of the 16 S-boxes in a 128-bit conventional masked AES engine is under CPA attacks after inputting 1 million plaintexts. (c) All of the possible data of 4 bits of the mask I_c^M versus absolute value of the correlation coefficient when 4 bits of the mask I_c^M in a 128-bit false key-based AES engine with conventional XOR gates are under CPA attacks after inputting 450,000 plaintexts. (d) All of the possible data of 4 bits of the mask I_c^M versus absolute value of the correlation coefficient when 4 bits of the mask I_c^M in the proposed 128-bit false key and WDDL assisted AES engine are under CPA attacks after inputting 15 million plaintexts.

the area overhead of the proposed AES technique is about 2.61%. 0.24% of the area overhead is induced by LUTs and 2.37% of the area overhead is induced by WDDL-based XOR gates. The power overhead of the proposed AES technique is about 0.24%, which is due to the higher power consumed by the WDDL-based XOR gates as compared to the conventional XOR gates. The throughput degradation and the maximum frequency of the proposed AES technique are about 1.81% and 196.4 MHz, respectively. Since the WDDL-based XOR gates in the proposed AES technique need to be synchronized to eliminate the power delay, the proposed AES technique has about 2.55 ns timing delay. Additionally, as demonstrated in Section VII, the MTD value of the proposed AES technique is enhanced over 187.5 times as compared to the AES technique without any countermeasure.

X. Discussion on Higher-Order Power Analysis Attacks

A conventional masked AES implementation is vulnerable against higher-order power analysis attacks. To make a conventional masked AES implementation secure against higher-order power analysis attacks, the number of the masks should be either equal to or greater than the order of the attack. For example, $H, (H = 1, 2, \ldots)$ number of random mask data is effective against $(H)^{th}$-order power analysis attacks and not effective against $(H+1)^{th}$-order attacks [42].

Since the false key and WDDL assisted AES technique is based on the conventional masked AES implementation, an additional constant mask data can be added as a countermeasure against second-order power analysis attacks. However, as compared to the conventional masked AES technique, if H number of mask data is utilized against $(H)^{th}$-order power analysis attacks, the size of the LUTs in the proposed technique would be reduced by $1/2^{8H}$.

Another method is combining with another existing countermeasure together against higher-order power analysis attacks. In an actual implementation, many countermeasures are combined together to prevent power analysis attacks since no single countermeasure can completely provide protection against power analysis attacks [43]. A conventional masked AES technique causes 60.1% area overhead and 11% performance overhead [24], making it quite expensive to

TABLE II

COMPARISON WITH PREVIOUS TECHNIQUES (MTD VALUE REPRESENTS THE NUMBER OF MEASUREMENTS TO DISCLOSE THE SECRET KEY UNDER FIRST-ORDER POWER ANALYSIS ATTACKS. X^* IS THE MTD VALUE OF AN AES ENGINE WITHOUT ANY COUNTERMEASURE)

	0.13 um switching capacitor [20]	0.18 um WDDL [16]	90nm ring oscillator [32]	FPGA masking technique [24]	FPGA DRECON technique [40,41]	This work
Area overhead	27.1%	210.1%	6.2%	60.1%	60.1%	2.61%
Power overhead	33%	270.4%	18.5%	0%	0%	0.24%
Maximum frequency	100MHz	85.5MHz	255Hz	97MHz	92.7MHz	196.4MHz
Delay	———	———	———	———	———	2.55ns
Throughput degradation	50%	74.2%	0%	11%	0%	1.81%
MTD value	>2500X*	≈156X*	>1087X*	>100X*	>100X*	>187.5X*

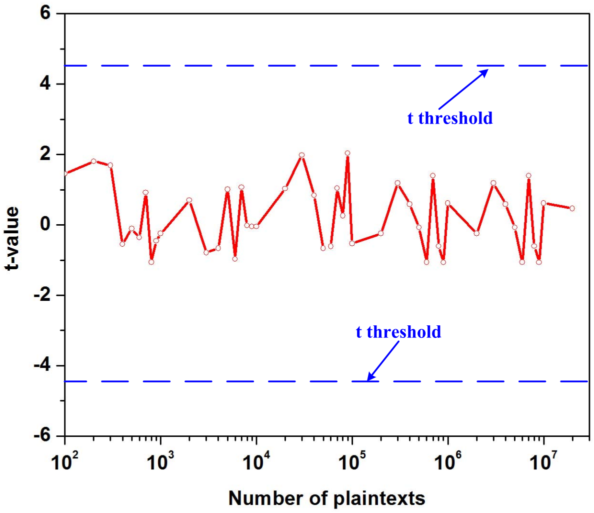


Fig. 14. TVLA simulation of the proposed false key and WDDL assisted AES technique ($n_1 = n_2$).

implement. Alternatively, the proposed false key and WDDL assisted AES technique only induces 2.61% area overhead and 1.81% performance overhead. Therefore, the proposed false-key and WDDL assisted AES technique provides a lightweight alternative to combine together with other techniques against higher-order power analysis attacks.

XI. CONCLUSION

A false key and WDDL assisted AES technique is utilized as a countermeasure against CPA attacks. False round key is added in each encryption round to reduce the correlation between the dynamic power consumption profile and the actual key. Concurrently, WDDL-based XOR gates are utilized in the reconstruction block to remove the mask at the end of the encryption process. Since during the whole encryption process, from the beginning to the end, the side-channel dynamic power consumption profile is correlated with the false key, an attacker needs to apply a CPA attack in two separate stages. After implementing the false key and WDDL assisted AES technique, the MTD value becomes over 1.5×10^8. The power, area, and performance overhead of the proposed technique is negligible, as compared to an unprotected AES engine.

REFERENCES

[1] S. Ray, Y. Jin, and A. Raychowdhury, "The changing computing paradigm with Internet of Things: A tutorial introduction," *IEEE Des. Test*, vol. 33, no. 2, pp. 76–96, Apr. 2016.

[2] Z. Bohan, W. Xu, and Z. Kaili, "Encryption node design in Internet of Things based on fingerprint features and CC2530," in *Proc. Green Comput. Commun. (GreenCom)*, Aug. 2013, pp. 1454–1457.

[3] K. N. Prasetyo, Y. Purwanto, and D. Darlis, "An implementation of data encryption for Internet of Things using blowfish algorithm on FPGA," in *Proc. 2nd Int. Conf. Inf. Commun. Technol. (ICoICT)*, May 2014, pp. 75–79.

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

[5] O. A. Uzun and S. Köse, "Converter-gating: A power efficient and secure on-chip power delivery system," *IEEE J. Emerg. Sel. Topics Circuits Syst.*, vol. 4, no. 2, pp. 169–179, Jun. 2014.

[6] W. Yu and S. Köse, "Time-delayed converter-reshuffling: An efficient and secure power delivery architecture," *IEEE Embedded Syst. Lett.*, vol. 7, no. 3, pp. 73–76, Sep. 2015.

[7] 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.

[8] 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.

[9] W. Yu and S. Köse, "Exploiting voltage regulators to enhance various power attack countermeasures," *IEEE Trans. Emerg. Topics Comput.*, to be published, doi: 10.1109/TETC.2016.2620382.

[10] W. Yu and S. Köse, "Security-adaptive voltage conversion as a lightweight countermeasure against LPA attacks," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, to be published, doi: 10.1109/TVLSI.2017.2670537.

[11] W. Yu and S. Köse, "False key-controlled aggressive voltage scaling: A countermeasure against LPA attacks," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, to be published, doi: 10.1109/TCAD.2017.2682113.

[12] X. Yao, Z. Chen, and Y. Tian, "A lightweight attribute-based encryption scheme for the Internet of Things," *Elsevier Future Generat. Comput. Syst.*, vol. 49, pp. 104–112, Aug. 2015.

[13] M. B. Shemaili, C. Y. Yeun, K. Mubarak, and M. J. Zemerly, "A new lightweight hybrid cryptographic algorithm for the Internet of Things," in *Proc. Int. Conf. Internet Technol. Secured Trans.*, Dec. 2012, pp. 87–92.

[14] A. M. Nia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Trans. Emerg. Topics Comput.*, to be published, doi: 10.1109/TETC.2016.2606384.

[15] P. Luo, L. Zhang, Y. Fei, and A. A. Ding, "Towards secure cryptographic software implementation against side-channel power analysis attacks," in *Proc. Appl.-Specific Syst., Architectures Processors (ASAP)*, Jul. 2015, pp. 144–148.

[16] D. D. Huang *et al.*, "AES-based security coprocessor IC in 0.18-μm CMOS with resistance to differential power analysis side-channel attacks," *IEEE J. Solid-State Circuits*, vol. 41, no. 4, pp. 781–792, Apr. 2006.

[17] N. Benhadjyoussef, H. Mestiri, M. Machhout, and R. Tourki, "Assessing CPA resistance of AES with different fault tolerance mechanisms," in *Proc. Design Autom. Conf. (ASP-DAC)*, Jan. 2016, pp. 661–666.

[18] N. Benhadjyoussef, H. Mestiri, M. Machhout, and R. Tourki, "Implementation of CPA analysis against AES design on FPGA," in *Proc. Int. Conf. Commun. Inf. Technol. (ICCIT)*, Jun. 2012, pp. 124–128.

[19] C. Wang, M. Yu, J. Wang, P. Jiang, and X. Tang, "A more practical CPA attack against present hardware implementation," in *Proc. Cloud Comput. Intell. Syst. (CCIS)*, Oct. 2012, pp. 1248–1253.

[20] C. Tokunaga and D. Blaauw, "Securing encryption systems with a switched capacitor current equalizer," *IEEE J. Solid-State Circuits*, vol. 45, no. 1, pp. 23–31, Jan. 2010.

[21] M. Nassar, Y. Souissi, S. Guilley, and J.-L. Danger, "RSM: A small and fast countermeasure for AES, secure against 1st and 2nd-order zero-offset SCAs," in *Proc. Design, Autom. Test Eur. Conf. Exhibit. (DATE)*, Mar. 2012, pp. 1173–1178.

[22] Y. Wang and Y. Ha, "FPGA-based 40.9-Gbits/s masked AES with area optimization for storage area network," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 60, no. 1, pp. 36–40, Jan. 2013.

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

[24] N. Kamoun, L. Bossuet, and A. Ghazel, "Correlated power noise generator as a low cost DPA countermeasures to secure hardware AES cpher," in *Proc. Signals, Circuits Syst. (SCS)*, Nov. 2009, pp. 1–6.

[25] S. Guilley, L. Sauvage, P. Hoogvorst, R. Pacalet, G. M. Bertoni, and S. Chaudhuri, "Security evaluation of WDDL and SecLib countermeasures against power attacks," *IEEE Trans. Comput.*, vol. 57, no. 11, pp. 1482–1497, Nov. 2008.

[26] K. Tiri, M. Akmal, and I. Verbauwhede, "A dynamic and differential CMOS logic with signal independent power consumption to withstand differential power analysis on smart cards," in *Proc. Eur. Solid-State Circuits (ESSCIRC)*, Sep. 2002, pp. 403–406.

[27] Y. Zhang, P. Wang, and L. Hao, "Design of resistant DPA three-valued counter based on SABL," in *Proc. Int. Conf. ASIC*, Oct. 2011, pp. 9–12.

[28] D. Sokolov, J. Murphy, A. Bystrov, and A. Yakovlev, "Design and analysis of dual-rail circuits for security applications," *IEEE Trans. Comput.*, vol. 54, no. 4, pp. 449–460, Apr. 2005.

[29] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "Three-phase dual-rail pre-charge logic," in *Proc. Cryptograph. Hardw. Embedded Syst. (CHES)*, 2006, pp. 232–241.

[30] M. Bucci, L. Giancane, R. Luzzi, G. Scotti, and A. Trifiletti, "Delay-based dual-rail precharge logic," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 19, no. 7, pp. 1147–1153, Jul. 2011.

[31] S. Bongiovanni, F. Centurelli, G. Scotti, and A. Trifiletti, "Design and validation through a frequency-based metric of a new countermeasure to protect nanometer ICs from side-channel attacks," *J. Cryptograph. Eng.*, vol. 5, no. 4, pp. 269–288, Nov. 2015.

[32] P.-C. Liu, H.-C. Chang, and C.-Y. Lee, "A true random-based differential power analysis countermeasure circuit for an AES engine," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 59, no. 2, pp. 103–107, Feb. 2012.

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

[34] E. Oswald and K. Schramm, "An efficient masking scheme for AES software implementations," in *Proc. Int. Workshop Inf. Security Appl. (WISA)*, 2005, pp. 292–305.

[35] K. Tiri and I. Verbauwhede, "A logic level design methodology for a secure DPA resistant ASIC or FPGA implementation," in *Proc. Design, Autom. Test Eur. Conf. Exhibit.*, Feb. 2004, pp. 246–251.

[36] O.-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.

[37] R. T. Howe and C. G. Sodini, *Microelectronics: An Integrated Approach*. Upper Saddle River, NJ, USA: Prentice-Hall, 1996.

[38] 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.

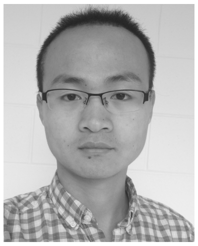
[39] S. Saab, A. Leiserson, and M. Tunstall, "Key extraction from the primary side of a switched-mode power supply," in *Proc. Asian Hardw.-Oriented Security Trust (AsianHOST)*, Dec. 2016, pp. 1–7.

[40] S. Hajra *et al.*, "DRECON: DPA resistant encryption by construction," in *Proc. AFRICACRYPT*, 2014, pp. 420–439.

[41] S. Patranabis, D. B. Roy, and D. Mukhopadhyay, "Using tweaks to design fault resistant ciphers," in *Proc. VLSI Design*, Jan. 2016, pp. 585–586.

[42] B. Gierlichs, S. Guilley, and D. Mukhopadhyay, *Security, Privacy, and Applied Cryptography Engineering*. Heidelberg, Germany: Springer-Verlag, Oct. 2013.

[43] A. Moradi, M. Kirschbaum, T. Eisenbarth, and C. Paar, "Masked dual-rail precharge logic encounters state-of-the-art power analysis methods," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 9, pp. 1578–1589, Sep. 2012.



Weize Yu received the B.S. degree in electrical engineering from the University of Electronic Science and Technology of China, Chengdu, China, in 2009, and the M.S. degree in electrical engineering from the Institute of Microelectronics of Chinese Academy of Sciences, Beijing, China, in 2012. He is currently pursuing the Ph.D. degree with the University of South Florida.

His current research interests include on-chip power management and hardware security.

Selçuk Köse (S'10–M'12) received the B.S. degree in electrical and electronics engineering from Bilkent University, Ankara, Turkey, in 2006, and the M.S. and Ph.D. degrees in electrical engineering from the University of Rochester, Rochester, NY, in 2008 and 2012, respectively.

He was with the VLSI Design Center of the Scientific and Technological Research Council, Ankara, Turkey, the Central Technology and Special Circuits Team in the enterprise microprocessor division of Intel Corporation, Santa Clara, CA, USA, and the RF, Analog, and Sensor Group, Freescale Semiconductor, Tempe, AZ, USA. He is currently an Assistant Professor with the Department of Electrical Engineering, University of South Florida, Tampa, FL, USA. His current research interests include the analysis and design of high-performance integrated circuits, on-chip dc–dc converters, and hardware security.

Prof. Köse has served on the Technical Program and Organization Committees of various conferences. He is a recipient of the NSF CAREER Award, the Cisco Research Award, the USF College of Engineering Outstanding Junior Researcher Award, and the USF Outstanding Faculty Award. He is an Associate Editor of the *Journal of Circuits, Systems, and Computers* and *Microelectronics Journal*.