A Comprehensive Evaluation of Integrated Circuits Side-Channel Resilience Utilizing Three-Independent-Gate Silicon Nanowire Field Effect Transistors-Based Current Mode Logic

Yanjiang Liu, Jiaji He, Haocheng Ma, Tongzhou Qu, and Zibin Dai

***Abstract*—Side-channel attack (SCA) is one of the physical attacks, which will reveal the confidential information from cryptographic circuits by statistically analyzing physical manifestations. Various circuit-level countermeasures have been proposed as fundamental solutions to eliminate the correlations between side-channel information and circuit's internal operations. The existing solutions, however, will introduce nonnegligible power and area overheads, making them difficult to be deployed in resource-constrained applications. In this article, a novel three-independent-gate silicon nanowire field effect transistor (TIGFET) with the intrinsic SCA-resilience characteristics is introduced to balance the tradeoffs among cost, performance, and security of cryptographic implementations. We construct six TIGFET-based current mode logic (CML) gates that can retain lower power variation under all possible transitions compared to the CMOS counterparts. As a proof of concept, advanced encryption standard (AES), SM4 block cipher algorithm (SM4), and lightweight cryptographic algorithm PRESENT are implemented utilizing the TIGFET-based CML gates. Correlation power attack is performed to evaluate the improvement of SCA resilience. Simulation results verify that the TIGFET-based cryptographic implementations decrease 42.37% area usage, lower 61.16% energy efficiency, reduce 5.35× power variation, and achieve a similar level of SCA resistance compared to the CMOS counterpart, which is applicable for the resource-constrained applications.**

Manuscript received 17 May 2021; revised 17 August 2021 and 19 October 2021; accepted 10 November 2021. Date of publication 16 November 2021; date of current version 20 September 2022. This work was supported in part by the China Postdoctoral Science Foundation under Grant 2019TQ0167, and in part by the National Natural Science Foundation of China under Grant 62004112. This article was recommended by Associate Editor Y. Makris. *(Yanjiang Liu and Jiaji He contributed equally to this work.) (Corresponding author: Yanjiang Liu.)*

Yanjiang Liu, Tongzhou Qu, and Zibin Dai are with the School of Cryptographic Engineering, Information Engineering University, Zhengzhou 450000, China (e-mail: yanjiang_liu@tju.edu.cn; qutongzhou@outlook.com; daizb2004@126.com).

Jiaji He and Haocheng Ma are with the School of Microelectronics, Tianjin University, Tianjin 300072, China (e-mail: dochejj@tju.edu.cn; hc_ma@tju.edu.cn).

Digital Object Identifier 10.1109/TCAD.2021.3128364

***Index Terms*—Circuit-level countermeasures, CMOS transistors, cryptographic implementations, side-channel attack (SCA), three-independent-gate silicon nanowire field effect transistors (TIGFETs).**

I. Introduction

ALTHOUGH cryptographic algorithms are proved mathematically secure, their hardware implementations are facing side-channel attacks (SCAs) which try to recover the secret information by analyzing the physical manifestations such as timing, power, electromagnetic, etc. The SCA was proposed by Kocher in 1996 using power information. After that, numerous SCA approaches, including simple power analysis (SPA) [1], differential power analysis (DPA) [2], correlation power analysis (CPA) [3], and template attack (TA) [4] have been explored to reveal the sensitive information of cryptographic implementations.

SCAs recover the key of cryptographic circuits due to the side-channel information is related with logic/circuit-level operations. To improve the resistance against SCAs, numerous circuit-level SCA countermeasures, including the current mode logic (CML) [5]–[7], FinSAL [8], EE-SPFAL [9], D3C [10], PGM [11], and so on, have been developed to reduce the internal correlations between the power consumption and logic operations. Although all the existing circuit-level countermeasures enhance the security level of hardware implementations, it introduces nonnegligible power and area overheads, which make them difficult to be deployed in resource-constrained applications. Therefore, circuit-level SCA countermeasures have always been criticized for its applicability.

Recently, emerging devices have already shown their potentials in hardware security applications relying on their unique and unconventional properties. Some SCA-resistant circuits based on the emerging transistors are proposed to achieve the goals of high security and low cost, including the flip-flops based on the three-independent-gate silicon nanowire field effect transistors (TIGFETs) [12], [13], CML gates based on the tunnel FETs (TFETs) [5], [7], [14]–[16], XOR/XNOR gate based on the TIGFETs [17], and so on. To the best of our knowledge, the TIGFET is the only one transistor with two symmetric polarity gates, which has the symmetric I–V behavior. The symmetrical I–V characteristics of TIGFET decrease the power differences under two transitions (0→1 and 1→0), which provide inherent resilience to the SCA. Furthermore, several TIGFET-based compact gates (e.g., NAND, XOR, and multiplexer) can be designed with less transistors compared to the other emerging transistors. Of all the existing emerging transistors, the TIGFET is the only candidate for the high-security and high-performance cryptographic circuits design.

In this article, we will leverage the symmetric I–V characteristics of TIGFETs to design SCA-resistant circuits which can achieve all desired properties with improved metrics of power, area, and security. Specifically, we set up an SCA-resistant library based on the TIGFETs, including the INV, AND, OR, XOR, Latch, and Flip-Flop. The performance and security characteristics of these logic gates are evaluated under all possible logic transitions. Then, simplified advanced encryption standard (AES), SM4, and PRESENT circuits are implemented with this library, and CPA is then performed on the proposed design to prove its SCA-resilience. The main contributions are listed as follows.

1) The SCA-resistance characteristics of TIGFET are analyzed, and the CML and TIGFETs are combined to design low-cost and high-security gates.
2) An SCA-resistant library based on the TIGFET is built. To the best of our knowledge, this is one of the first pioneer attempts to cover all basic SCA-resistant logic gates upon TIGFETs.
3) All designed gates are compatible with the traditional integrated circuit design process, and three cryptographic circuits using this library retain the SCA-resistance characteristics without sacrificing the main performance metrics, e.g., area and power.

The following of this article is organized as follows. Section II introduces the circuit-level SCA countermeasures. Section III presents the major vulnerabilities of CML and its low-cost solutions. Section IV gives the SCA-resistant library based on the TIGFET and its security evaluation. Section V describes three cryptographic implementations with the SCA-resistant library and analyzes the CPA attack results. Section VI concludes this article.

II. Related Work of Circuit-Level SCA Countermeasures

Concerning the catastrophic consequences caused by SCA in the cryptosystems, numerous side-channel prevention methods have been proposed over the past few decades. Of all the existing methods, circuit-level SCA countermeasures have become the most promising SCA prevention approaches. From [18], gate-level masking method is first presented to make the power consumption independent of the processed data by redesigning the basic logic gates. Furthermore, Trichina *et al.* [19] introduced several masked circuits, and De *et al.* [20] proposed a path-balanced masked dual-rail precharge circuit based on binary decision diagram. However, first-order masking schemes cannot thwart the high-order DPA attack; thus, high-order masking techniques are heavily focused in [21]. More specifically, a random switching logic presented in [22] is proposed to resist the second-order SCA. Nevertheless, the outputs' transitions of masked logic gates are still dependent on the input transitions when clock or power supply glitch is injected [23]. Several works described in [24] and [25] perform a successful attack on the masked hardware implementations with glitches.

To prevent the glitches attack, numerous transistor-level hiding approaches have been investigated to hide the processed data of cryptographic implementations. Tiri and Verbauwhede proposed a complementary logic SABL in [26], and its improvement WDDL [27]. To further improve the security level, masking schemes are applied into the WDDL and several improvements have been presented, including the EE-SPFAL [9], SC-DDPL [28], RO-BDD [29], ADDL [30], and so on. Although the WDDL and its improvements are compatible with the design process of the integrated circuit, it still leaks side-channel information due to the asymmetric routing and unbalanced load conditions. Therefore, full-custom differential logic styles, which are well designed, placed and routed, are proposed to enhance the weaknesses of the masking schemes. In [31] and [32], a delay-based dual-rail precharge logic is presented, which is insensitive to unbalanced load conditions. Besides, Bucci *et al.* [33] proposed a three-phase dual-rail precharge logic and Badel *et al.* [34] built some generic standard cells based on the CML. Concerning the low latency and stable power consumption, CML has been widely recognized by researchers. Hassoune *et al.* [35] introduced a low-swing CML, and Cevrero *et al.* [36] proposed a standard cell library PG-MCML to reduce the static power consumption of MCML-based cryptographic circuits.

Furthermore, the existing circuit-level SCA countermeasures based on the emerging devices are also explored to reduce the power consumption of cryptographic circuits. More specifically, the TFETs and TIGFETs are utilized to reduce the area overhead and power consumption of cryptographic circuits. Bi *et al.* design a TFET-based library for the DPA-resilient block cipher design [5], [7], [14]–[16]. But the secure flip-flop is still not described. Furthermore, a true single-phase clock (TSPC) flip-flop based on the TIGFETs [13] and modified TSPC [12] are introduced. Besides, several secure combinational cells based on the TIGFETs are presented [17]. However, these schemes still introduce nonnegligible area overheads, which make the CML difficult to be deployed in the resource-constrained applications.

III. Current Mode Logic Vulnerabilities and Their Solutions Based on TIGFETs

As shown in [5]–[7], the CML provides a constant current value with 2× area overheads, which has been proven as an effective way against SCA among all the existing circuit-level countermeasures. Therefore, the CML is introduced to design the SCA-resilience circuits in this article.

The general structure of CML is illustrated in Fig. 1(a), which is mainly composed by the pull-up network, the pull-down network, and the tail current source. The pull-up network

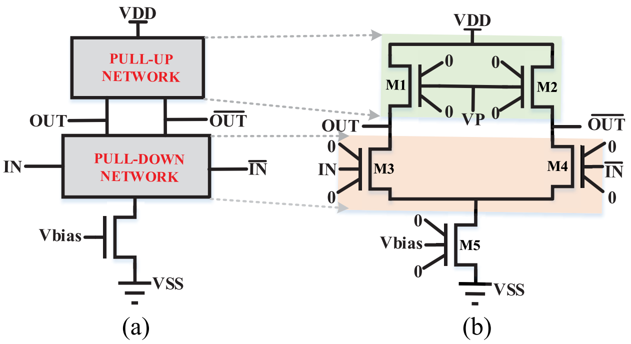


Fig. 1. CML. (a) Basic structure of the CML. (b) Structure of the TIGFET-based CML inverter/buffer.

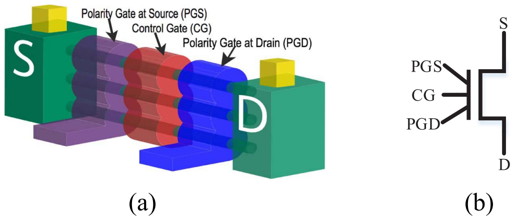


Fig. 2. (a) Structure and (b) symbol of a TIGFET.

works as the load resistor and achieves a voltage swing on the output, i.e., OUT and $\overline{\text{OUT}}$, and the load resistance value R determines the output voltage swing. The pull-down network implements the differential logic function according to the differential inputs, i.e., IN and $\overline{\text{IN}}$, and provides a complementary output in every clock cycle. The n-type transistor operates in the saturation region as a tail current source and the voltage value of the gate (denoted as Vbias) determines the amplitude of a current flowing to ground.

Considering the differential structure, such a logic style offers high robustness to the ambient noises, e.g., cross talk noise and power/ground noise. But the current of pull-up and pull-down networks is not the same that can be used to infer the internal transitions. Besides, such a differential structure uses more than twice as much the area footprints of the traditional gates and the tail current source results in a significant increment of static power [7]. Note that the symmetric I–V characteristics of TIGFETs can balance the current flowing through the pull-up and pull-down networks, and its low leakage characteristics and complex Boolean function configurations can realize the low-cost scheme for a cryptographic design [17]. Therefore, we exploit the TIGFETs to balance the tradeoffs among area footprints, power overheads, and security characteristics of CML for the cryptographic implementations.

Fig. 2 shows the structure of TIGFET [37]. Source gate (denoted as S) and drain gate (denoted as D) connect with three vertically stacked silicon nanowires, and three gate contacts [polarity gate at the source (PGS), polarity gate at the drain (PGD) and control gate (CG)] exist between the S and D. Compared to the traditional CMOS transistor, the TIGFET has two additional independent gates that control the device's electrical characteristics. The CG controls the channel conduction or not, and the PGS and PGD jointly determine electrons or holes flowing through the channel. A TIGFET can realize several complex Boolean logic functions by combining the bias configurations of CG, PGD, and PGS, e.g., two series n-type/p-type FETs and XOR, and the detailed bias gate conditions are presented in [38]. For a complex circuit, it requires a smaller number of TIGFETs compared with the CMOS counterparts. For example, a 32-bit adder based on TIGFETs has 2.05× lower total area and 3.83× lower energy-delay product [39]. Thus, the TIGFET presents an appealing option for area-constrained cryptographic systems.

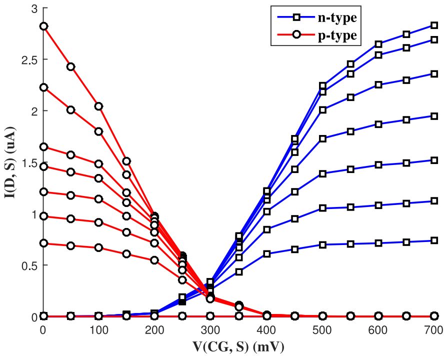


Fig. 3. I–V curves of TIGFET with the different drain–source voltages.

Furthermore, the TIGFET can be configured as a p-type FET and n-type FET with the default bias gate conditions, and its DC transfer characteristics with the different of drain–source voltage ($V(D, S)$) are shown in Fig. 3. The red and blue lines represent the drain–source current ($I(D, S)$) of p-type FET and n-type FET, respectively, $V(D, S)$ scales from 0 to 0.7 V, and the sweep voltage of $V(D, S)$ is 0.1 V. The $I(D, S)$ varies with $V(D, S)$ and V(CG,S). Regarding Fig. 3, the $I(D, S)$ of p-type FET decreases with the increase in V(CG, S), while the $I(D, S)$ of n-type FET increases with the increase in V(CG, S). Besides, two I–V curves of each $V(D, S)$ are symmetrical to each other and the vertical symmetry axis is $V(\text{CG, S}) = 0.3$ V. The symmetric I–V characteristics show that the p-type FET and n-type FET have the same power dissipation process; thus, the TIGFETs consume the same amount of power under all possible input transitions. Although the CML retains extremely low-power variations for all transitions, such structure based on the CMOS are vulnerable to SCA due to the current of pull-up and pull-down networks is not the same. The symmetric I–V characteristics of TIGFET can help to balance the power variations of all transitions. Therefore, we build CML based on TIGFETs' symmetric properties such that we can achieve a high SCA-resistance level without sacrificing area cost and power overhead.

IV. TIGFET-Based SCA-Resilience Library Design and Security Evaluation

For the logic gates in cryptographic circuits, the power consumption under different input transitions (e.g., 0→1, 1→0, 0→0, and 1→1) differs from each other, and these power differences can be exploited to reveal the data transitions using the power attack model. The total power consumption of cryptographic circuits is the sum of all the switching logic gates, and the power variation of each logic gate directly determines the SCA-resilience of cryptographic circuits. Therefore,

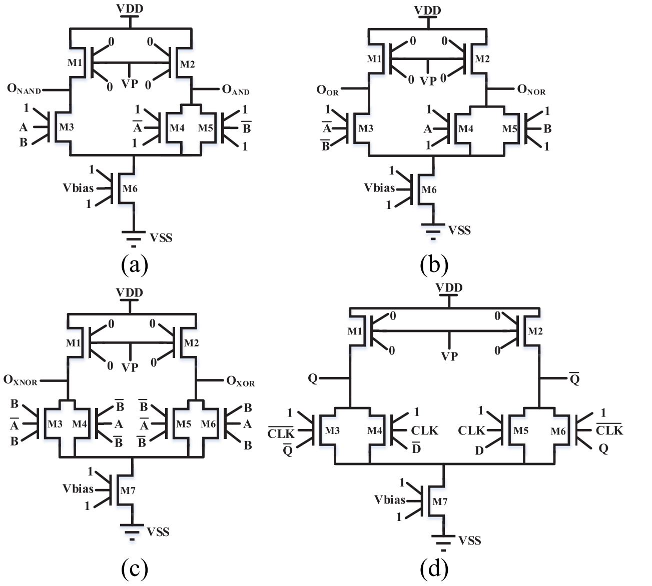


Fig. 4. Structure of four TIGFET-based CML gates: (a) AND; (b) OR; (c) XOR; and (d) Latch.

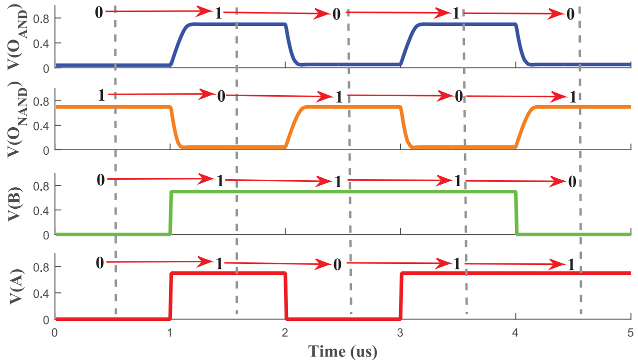


Fig. 5. Timing waveforms of AND based on the TIGFET.

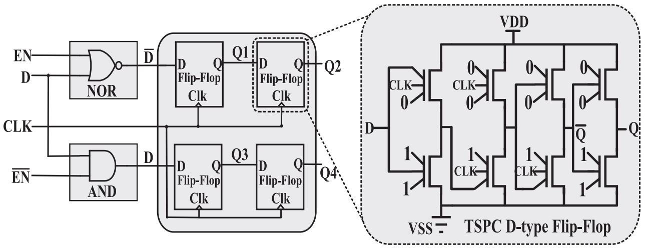


Fig. 6. Structure of TIGFET-based sMSFF.

we design several TIGFET-based basic gates that can enable low-power variations with all types of input transitions and maintain high performances (e.g., area overhead and power consumption) compared to the CMOS counterparts, and evaluate the SCA-resilience characteristics of these basic gates in this section.

A. Development of TIGFET-Based Standard Cells

As introduced in [39], *p*-type FETs and *n*-type FETs are obtained by configuring different bias gate conditions, and various logic circuits can be built with these TIGFETs. The structure of TIGFET-based inverter/buffer (denoted as INV) is depicted in Fig. 1(b). Two *p*-type TIGFETs (M1 and M2) form the pull-up network and both M1 and M2 work in the amplification region. The CG of M1 and M2 (denoted as VP) determines the voltage swing. Meanwhile, two *n*-type TIGFETs (M3 and M4) perform the differential function, and M5 provides a constant current *I*. The voltage value of CG (denoted as Vbias) determines the magnitude of *I*. When the IN and $\overline{\text{IN}}$ are logic "1" and "0," respectively, M3 is turned on, the current *I* flows through the left-handed branch of INV, and the voltage value of OUT and $\overline{\text{OUT}}$ are VDD$-I\times R$ and VDD, respectively. The voltage value of OUT and $\overline{\text{OUT}}$ are VDD and VDD$-I\times R$, respectively, when the IN and $\overline{\text{IN}}$ are logic "0" and "1." Note that $I\times R$ is the voltage swing value, and VDD and VDD$-I\times R$ represent the logic "1" and "0," respectively.

Furthermore, four other TIGFET-based CML gates are designed and its structure is shown in Fig. 4. For the TIGFET-based CML AND shown in Fig. 4(a), M3 is turned on and the output O_{NAND} is logic "0" when the input *A* and *B* are logic "1." Otherwise, M4 or M5 is turned on, and the output O_{NAND} and O_{AND} are logic "1" and "0," respectively. The timing waveform of TIGFET-based CML AND is shown in Fig. 5 and the results are consistent with the AND's logic function. Moreover, the OR, XOR, and Latch, respectively, shown in Fig. 4(b)–(d) are also simulated and the timing results are accord with the corresponding logic function.

In sequential circuits, the flip-flop is the main source of side-channel information leakage due to the side-channel information of the sequential circuit is synchronized on a rising/falling clock edge [40]. In order to eliminate the internal relationship between the data transitions and side-channel information, a TIGFET-based single master–slave flip-flop (sMSFF) is constructed in this article. The structure of sMSFF is illustrated in Fig. 6, which is composed by one NOR gate, one AND gate, and four TSPC Flip-Flops.

For the sMSFF, three dummy TSPC Flip-Flops are added to ensure a 0→1 and 1→0 transition in each transition. Traditionally, a Flip-Flop can be formed by two D-type Latches; thus, the CML-based Flip-Flop needs 14 TIGFETs. To further reduce the area, a TSPC Flip-Flop presented in [38] formed by eight TIGFETs is used as the Flip-Flop of sMSFF. The period of enable signal (denoted as EN) is four times that of the clock signal (denoted as CLK). When the EN keeps at the logic "1," sMSFF stays in the precharge stage, and the output Q1 and Q3 remain at logic "0." When the EN keeps at the logic "0," sMSFF enters in the evaluation stage and the value of D propagates to the output. Q1 and Q3 are assigned by $\overline{\text{D}}$ and its opposite value D, respectively, at the rising edge of CLK, while Q2 and Q4 capture the value of Q1 and Q3 at the next rising edge of CLK, respectively. The NOR and AND gates are utilized to generate a differential signal pair (D and $\overline{\text{D}}$) at the evaluation stage and keep the outputs at logic "0" at the precharge stage. The simulated timing waveform of sMSFF is shown in Fig. 7.

B. Performance and Security Evaluation of Standard Cells

In this article, 10-nm TIGFET and CMOS device SPICE models are used to evaluate the performance and security

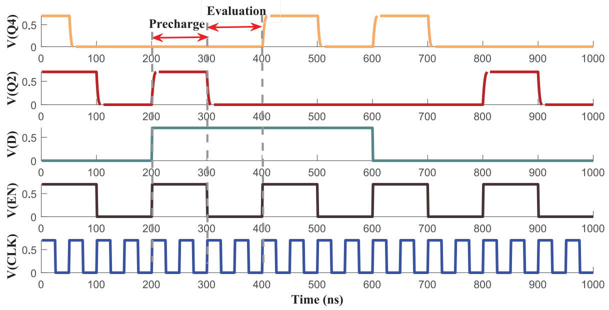


Fig. 7. Timing waveforms of TIGFET-based sMSFF.

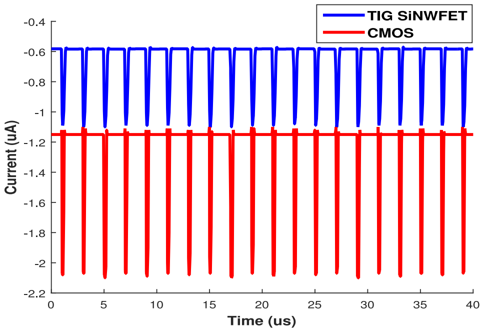


Fig. 8. Supply current of CML AND gate based on the TIGFET and CMOS technology.

characteristics of the proposed standard cells. As described above, VP and Vbias determine the power variations of CML-based logic gates. Therefore, voltage sweeping analysis on VP and Vbias is performed and the transistor size is also adjusted to ensure the relatively low-power variations under all possible transitions. When the VP and Vbias of TIGFET-based CML gates are set to 0.25 and 0.5 V, respectively, the variation of power dissipation reaches the minimum value.

The normalization energy deviation (NED) and maximum current variation (MCV) are widely used to evaluate the power variations under all possible transitions [6], which are described in (1) and (2), where $E_i(t)$ and $E_j(t)$ are the consumed energy under the ith and jth transitions, and $\mathbf{E}$ and $\mathbf{I}$ are the consumed energy matrix and maximum supply current matrix for all possible transitions, and $I_i(t)$ and $I_j(t)$ are the maximum supply current under the ith and jth transitions

$$\text{NED} = \underset{E_i(t),E_j(t)\in\mathbf{E}(t)}{\arg\max} \frac{E_i(t)-E_j(t)}{\max(\mathbf{E})} \times 100\% \tag{1}$$

$$\text{MCV} = \underset{I_i(t),I_j(t)\in\mathbf{I}(t)}{\arg\max} \frac{I_i(t)-I_j(t)}{\max(\mathbf{I})} \times 100\%. \tag{2}$$

Fig. 8 compares the power variations of TIGFET-based and CMOS-based CML AND gate. As shown in Fig. 8, the maximum supply current of TIGFET-based CML AND gate ranges from 1087.8 to 1098.5 nA, while the CMOS-based CML AND gate falls within the range of 2066.7–2087.5 nA. The TIGFET-based CML AND gate reduces 1.9× supply current compared to the CMOS counterparts. The NED and MCV of TIGFET-based CML AND gate are 0.42% and 0.97%, respectively, while the CMOS-based CML AND gate are 0.9% and 0.99%, respectively.

Moreover, other standard cells are simulated under the same bias conditions, and the average energy under all possible transitions is calculated to quantify the energy efficacy. For the average energy result shown in Fig. 9(a), the average energy of TIGFET-based logic is smaller than the corresponding CMOS-based counterpart. More specifically, the TIGFET-based logics lower 55.96% energy compared to the CMOS counterparts. Furthermore, the MCV and NED between the TIGFET-based and CMOS-based logics are used to evaluate the power variations and the results are shown in Fig. 9(b) and (c). The NED and MCV of TIGFET-based logics, respectively, are less than 1% and 3.5%, which shows that these basic logic gates maintain a constant power dissipation under various transitions.

Overall, the TIGFET-based basic logic achieves stable power consumption with lower energy compared to the CMOS-based logic. It is worth noting that the invariant power consumption provides no information about the data transitions. Therefore, it is extremely difficult to retrieve the secret information of the cryptographic implementation using the SCA. Although we only present six basic logic gates in the library, more complex logic functions can be obtained using these standard cells. In the next section, cryptographic circuits are implemented with these TIGFET-based standard cells and CPA is performed to evaluate their SCA-resilience.

V. SCA-Resilience Evaluation of Cryptographic Circuits

A. Performance Analysis

AES, SM4, and PRESENT have been widely applied in the critical applications and sensitive fields, such as communication, finance, Internet of Things, and so on. To better assess the SCA-resilience efficacy of the proposed design, a 16-bit cryptographic datapath instead of a full cryptographic circuit is adopted using this library [41]. However, the other cryptographic datapaths, modules, and experimental noises will reduce the signal-to-noise ratio of a 16-bit cryptographic datapath, and the SCA results of the 16-bit cryptographic datapath cannot reflect the SCA-resilience efficacy of a cryptographic implementation. In [43], the authors use random noise to overcome the absence of noise in simulations. Similarly, a Gauss noise is added to the simulated current traces for emulating the influences of other modules and environmental noises in this article. In general, other modules of design and experimental noise easily mask the power consumption of the cryptographic datapath. For the AES, the supply current of CML_CMOS ranges from 650 to 1010 μA. Therefore, the mean and variance of Gauss noise are 1 mA and 0.05, respectively, which can mask the total power dissipation of the 16-bit cryptographic datapath. Where the design using the conventional CMOS technology denoted as Basic_CMOS, and the CML circuits utilizing the CMOS and TIGFET technology denoted as CML_CMOS and CML_TIGFET, respectively. As described above, a TIGFET device has two additional gates compared to the CMOS device, thus the area of a TIGFET device is

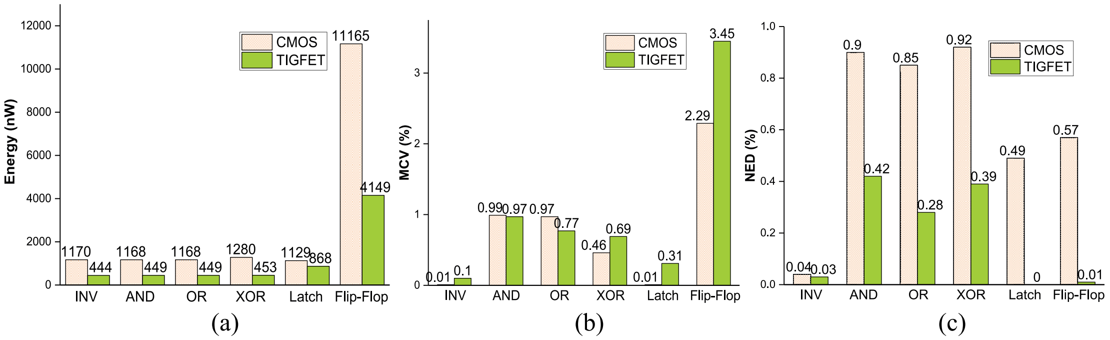


Fig. 9. Comparison of (a) energy, (b) MCV, and (c) NED between TIGFET-based and CMOS-based CML gates.

TABLE I
Performance Comparison Between Design Utilizing TIGFET and CMOS Technology

Circuits \ Performance		Area Estimation (UST)	Average Energy (uW)	Delay Overhead (ps)	Maximum Current Variation (%)
AES	Basic_CMOS	6032	20.26	299	97.12
	CML_CMOS	10908	636.1	182.2	8.71
	CML_TIGFET	7170	231.1	1920	3.48
SM4	Basic_CMOS	11372	40.8	59.91	95.84
	CML_CMOS	18438	819.33	167.4	35.26
	CML_TIGFET	11790	376.9	1897.9	2.6
PRESENT	Basic_CMOS	1240	0.82	655.28	99.16
	CML_CMOS	5052	188.6	513.3	10.17
	CML_TIGFET	2184	64.5	3045.96	3.4

* TIGFET area = 1.5 × # of CMOS.

approximately 1.5 × larger than a single CMOS [12], [13]. For consistency, the equivalent unit size transistors (USTs) is used to estimate the area usage of TIGFET-based cryptographic circuits. The area estimation of CML_TIGFET implementations is 1.5 times the number of required TIGFETs. The area estimation results are shown in the second column of Table I. The 16-bit AES datapath of CML_TIGFET and CML_CMOS occupies 3585 and 5454 transistors, and the 16-bit SM4 datapath requires 5895 and 9219 transistors, while the 16-bit PRESENT datapath requires 2184 and 5052 transistors. From the area perspective, the simplified AES, SM4, and PRESENT of the CML_TIGFET reduces 34.27%, 36.06%, and 56.77% area overhead compared with the CML_CMOS, respectively. Overall, we achieve a significant reduction in area overhead compared with the CMOS counterparts and the averaged area reduction is 42.37%.

Simulations of the simplified AES, SM4, and PRESENT are performed using the HSPICE. With the consideration that SCA reveals the key byte by byte, the possible key scales from 16’h0000 to 16’h00FF. Moreover, the 16-bit plaintext scales from 16’h0000 to 16’h01FF are exploited during the simulation. The supply current (I_{supply}) of the 16-bit AES datapath under 512 input transitions is shown in Fig. 10. The first and last 50 sample points represent the I_{supply} at the precharge and evaluation stage, respectively. As shown in Fig. 10, the I_{supply} of the CML_CMOS is much larger than the CML_TIGFET. More specifically, the I_{supply} of CML_CMOS ranges from 650 to 1010 μA, while the I_{supply} of CML_TIGFET falls within the range of 330 to 416 μA. The TIGFET-based cryptographic designs reduce at least 2.2× dynamic current compared to the CMOS-based circuits. Moreover, the average energy is also calculated to contrast the power consumption of the cryptographic circuits between the CMOS and TIGFET technology. The average energy of CML_CMOS and CML_TIGFET, respectively, are 636.1 and 231.1 μW, then, the CML_TIGFET of the simplified AES consumes only 63.67% energy compared to the

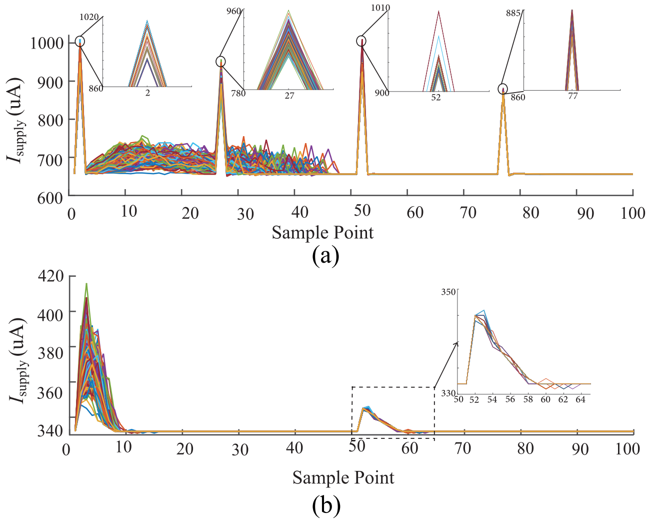


Fig. 10. Comparisons of I_{supply} of 16-bit AES datapath implementation under all 512 input transitions. (a) CML_CMOS; (b) CML_TIGFET.

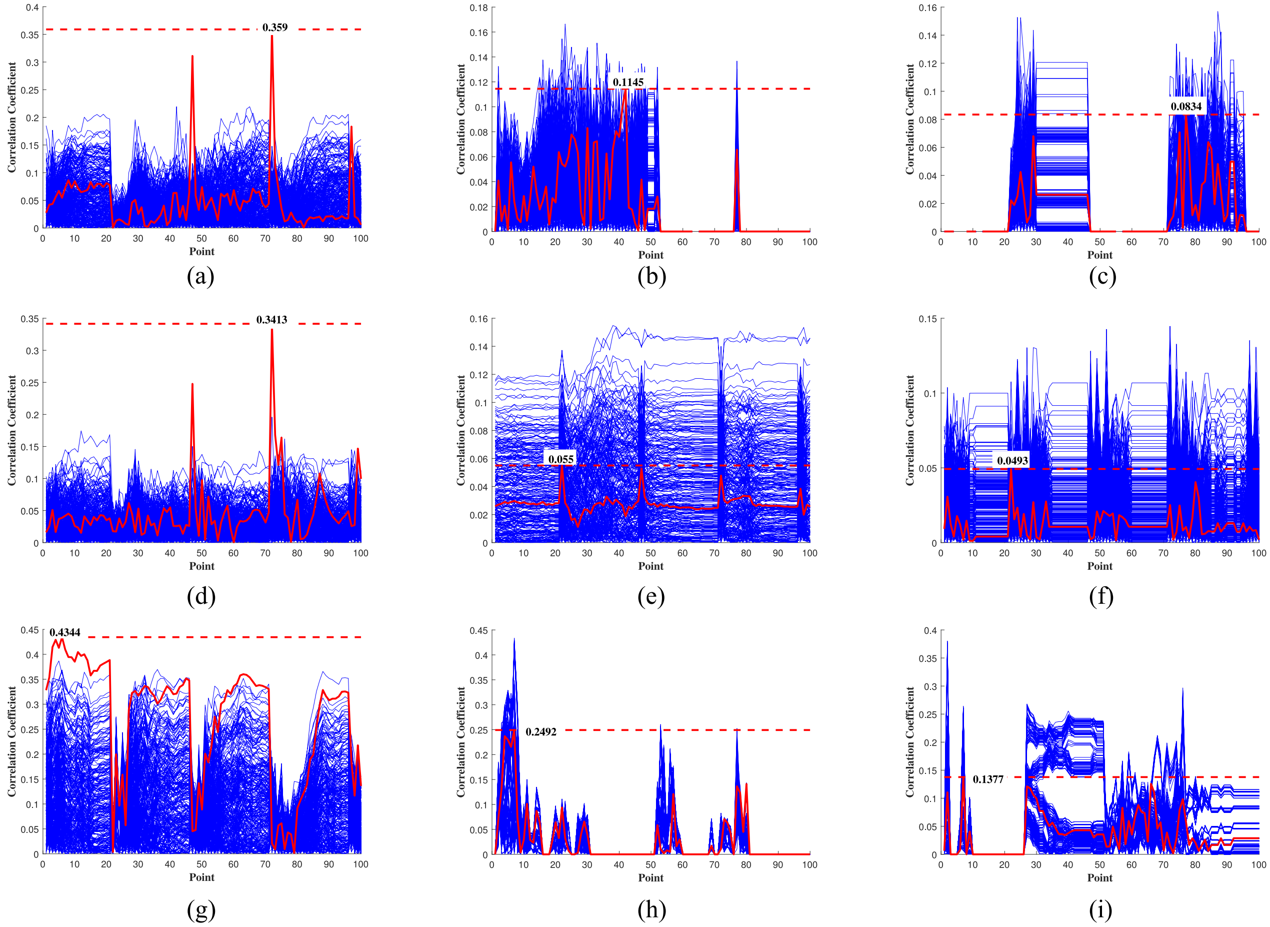
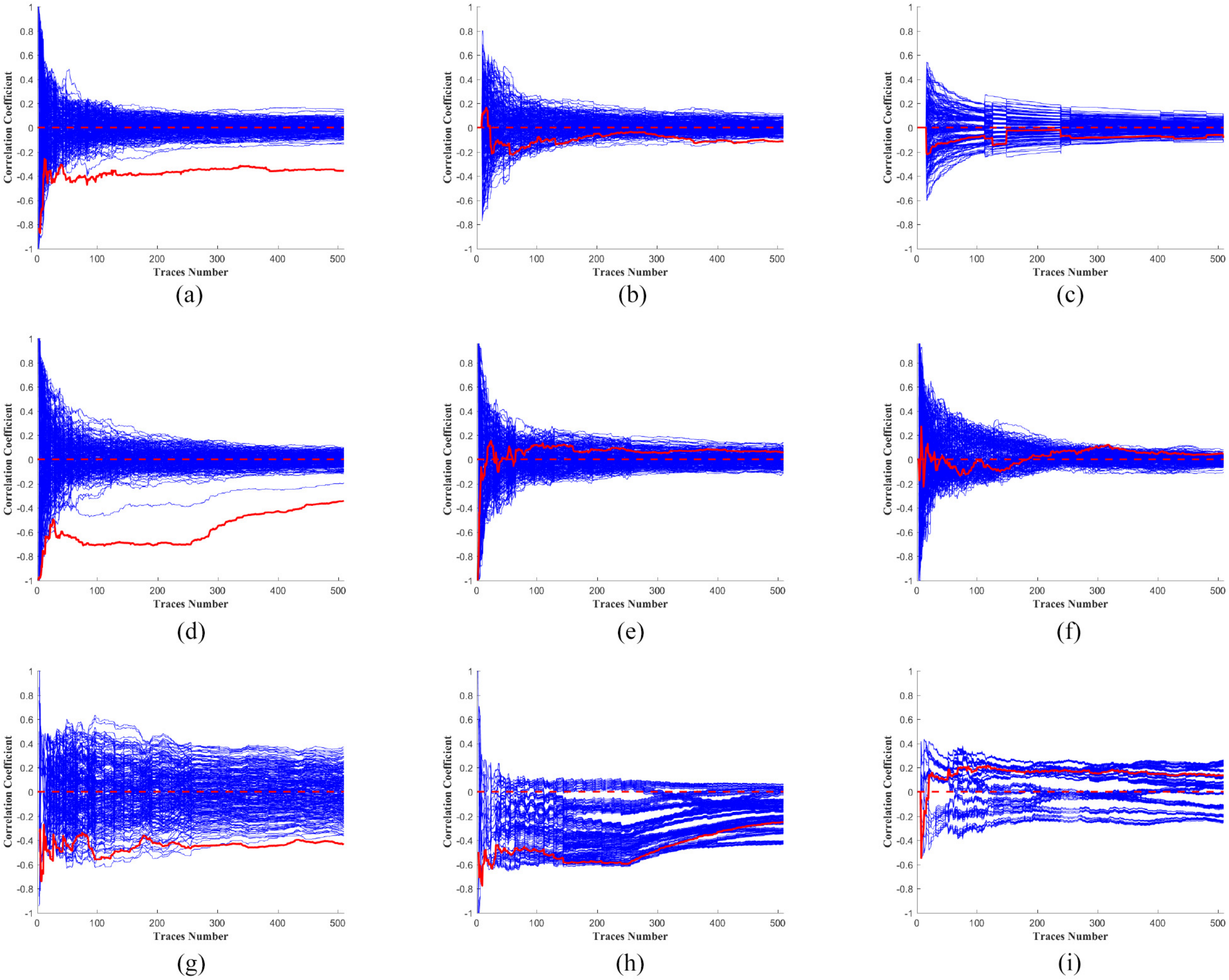


Fig. 11. CPA results of AES, SM4, and PRESENT using CMOS and TIGFET technology. (a) CPA results of Basic_CMOS of AES. (b) CPA results of CML_CMOS of AES. (c) CPA results of CML_TIGFET of AES. (d) CPA results of Basic_CMOS of SM4. (e) CPA results of CML_CMOS of SM4. (f) CPA results of CML_TIGFET of SM4. (g) CPA results of Basic_CMOS of PRESENT. (h) CPA results of CML_CMOS of PRESENT. (i) CPA results of CML_TIGFET of PRESENT.

CML_CMOS. Meanwhile, the average energy of the simplified SM4 and PRESENT is also calculated and the results are shown in Table I. Regarding the Table I, the CML_TIGFET of the simplified SM4 and PRESENT, respectively, reduce 54% and 65.8% energy compared to the CML_CMOS. In summary, the CML_TIGFET decreases 61.16% energy on average over the CML_CMOS, which shows that the TIGFETs are efficient to be applied to the resource-constrained fields.

The delay results are also depicted in Table I and the simulation time step is 1 ps. The delay of CML_TIGFET is greater than the Basic_CMOS and CML_CMOS. More specifically, the delay value of CML_TIGFET of AES, SM4, and PRESENT, respectively, are 1.92, 1.89, and 3.05 ns, while the CML_CMOS of AES, SM4, and PRESENT, respectively, are only 182.2, 167.4, and 513.3 ps. The CML_TIGFET of AES, SM4, and PRESENT increases 10.53×, 11.36×, and 4.93× delay compared to the CML_CMOS. Such nonnegligible delay overhead of TIGFET-based cryptographic implementations is mainly contributed by Flip-Flops. Because the proposed TIGFET-based Flip-Flop increases 10.29 × delay cost compared with the CMOS-based counterpart. Moreover, the TIGFET-based INV, AND, and OR increase 24.7%, 11.9%, and 26.3% compared to the CMOS-based counterparts. In the future, the Flip-Flop and other three combinational gates are redesigned to further reduce the delay overhead. Although the maximum working frequency of TIGFET-based cryptographic circuits is smaller than the CMOS-based counterparts, it still could reach 328 MHz; thus, it will be sufficient for the IoT devices [42].

Furthermore, the MCV is calculated to measure the information leakage capability of the proposed design under all transitions. Note that the smaller the MCV value, the less the power fluctuates, and fewer information cryptographic design leaks. As shown in Table I, the MCV of Basic_CMOS can be achieved as large as 95.84%, and the CML_CMOS and CML_TIGFET offer a low MCV under various transitions compared to the Basic_CMOS, and the CML_TIGFET has a minimum MCV value. More specifically, the CML_TIGFET of the simplified AES, SM4, and PRESENT decreases 1.5×, 12.57×, and 1.99× compared to the CML_CMOS counterparts, and the averaged power fluctuation improvement is 5.35×. In summary, the power consumption of the TIGFET-based implementation is more constant than the CMOS-based under 512 transitions. To sum up, the TIGFET-based implementations achieve lower area/power consumption and higher delay overhead compared to the CMOS-based design. If only comparing the area usage and power consumption, we can



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Fig. 12. Minimum number of traces to the disclosure of AES, SM4, and PRESENT using CMOS and TIGFET technology. (a) MTD results of Basic_CMOS of AES. (b) MTD results of CML_CMOS of AES. (c) MTD results of CML_TIGFET of AES. (d) MTD results of Basic_CMOS of SM4. (e) MTD results of CML_CMOS of SM4. (f) MTD results of CML_TIGFET of SM4. (g) MTD results of Basic_CMOS of PRESENT. (h) MTD results of CML_CMOS of PRESENT. (i) MTD results of CML_TIGFET of PRESENT.

already claim that the TIGFET-based circuit is more suitable to resource-constrained applications.

B. SCA-Resilience Analysis

Based on the above power simulation results, CPA is used to evaluate the SCA-resilience efficacy of cryptographic implementations. For the CPA, the correlation coefficient σ between the power attack model (**HC**) and simulated current traces I_{supply} for each hypothetical key is calculated, and the secret key is inferred by looking for the highest level of correlation coefficients. The **HC** is presented in (3), where **HC** is the matrix among adjacent outputs [e.g., $f(P_{i-1}\oplus k_x)$ and $f(P_i\oplus k_x)$] for a hypothetical key (k_x), the value of column x and row y of **HC**, respectively, represent the size of hypothetical keys and input transitions, P_{i-1} and P_i are the $(i-1)$th and ith plaintext of cryptographic algorithms, f represents the function of cryptographic algorithms executing, and HD is the power attack model function

$$\mathbf{HC}(y,x) = HD(f(P_{i-1} \oplus k_x), f(P_i \oplus k_x)). \qquad (3)$$

It is worth noting that the quality of the power attack model determines the efficiency of SCA. The Hamming distance model computed based on the number of flipped bits can represent the power dissipation process of cryptographic circuits accurately, and the CPA using this model has performed many successful attacks on the cryptographic circuits. Therefore, the Hamming distance model is used as the power attack model in this article.

Note that the predicted Hamming distance model corresponding with the correct key is strongly correlated with the supply current of cryptographic circuits. Thus, the maximum correlation coefficient corresponds to the guessed key is always considered as the correct key. The correlation coefficients of CMOS-based and TIGFET-based circuits are shown in Fig. 11. The red and blue lines are the correct and other 255 incorrect hypothetical keys, respectively. Regarding Fig. 11(a), (d), and (g), the correlation coefficients correspond with the correct key reach to the peak value which indicates that obvious information leakage could be observed at this sample point, and the CPA perform a successful attack on the unprotected design with the conventional CMOS technology. For Fig. 11(b), (c), (e), (f), (h), and (i), all the correlation coefficients are lower than 0.3, and the correlation coefficients corresponding to the correct key are hidden within the wrong keys. It means that CPA fails to reveal the correct key of CML_TIGFET and CML_CMOS implementations with 512 traces. Moreover, the maximum correlation coefficient of CML_TIGFET implementations is smaller than CML_CMOS implementations. More specifically, the highest correlation coefficient of CML_TIGFET of AES, SM4, and PRESENT is 0.0834, 0.0493, and 0.1377, while the corresponding results of CML_CMOS are 0.1145, 0.055, and 0.2492, respectively. Therefore, we can claim that the CML_TIGFET implementations leak less information than CML_CMOS implementations.

Furthermore, the minimum number of traces to disclose the correct key (denoted as MTD) based on the highest correlation coefficient is calculated and the MTD results are shown in Fig. 12. The red and blue lines show the traces of correct key and other 255 incorrect hypothetical keys, respectively. As shown in Fig. 12(a), (d), and (g), the red lines are clearly separated from the others which indicate there exists obvious key-related information leakage, and the Basic_CMOS of cryptographic circuits (e.g., AES, SM4, and PRESENT) is not resilient to the CPA attack, and the correct key was successfully retrieved with less than 250 traces. For Fig. 12(b), (c), (e), (f), (h), and (i), the correlation coefficients do not increase after the increasing number of traces reaches 100, and the correlation coefficient corresponds to the correct key is mixed with the other wrong keys which show that neither the CML_CMOS nor CML_TIGFET failed to attacked with 512 traces. Note that the smaller the MTD results, the fewer information cryptographic design leaks and the higher the SCA-resilience efficacy. Ideally, the MTD results of the proposed design should reach 0. From Fig. 12, all the MTD results slightly fluctuate around 0. The Euclidean distance is an effective variation measurement method and, thus, we use the Euclidean distance to determine the variations between MTD results and 0. Considering the trend of MTD results, we remove the first 100 points of MTD results and calculate the Euclidean distance of the remaining sample points. The Euclidean distance of CML_TIGFET of AES, SM4, and PRESENT is 1.528, 1.2698, and 3.3113, while the corresponding results of CML_CMOS are 1.923, 1.5672, and 9.4092, respectively. Overall, the trend of proposed CML_TIGFET circuits is farther from the boundaries than CML_CMOSi circuits, and the Euclidean distance of the proposed CML_TIGFET circuit is smaller than the CML_CMOS counterpart. Therefore, we can conclude that it is easier to reveal the correct key of CML_CMOS implementations with the increasing number of traces than CML_TIGFET implementations. Besides, an 8-bit cryptographic datapath is built and utilized to further validate the SCA-resilience efficacy of the proposed design. The SCA results and MTD results of 8-bit cryptographic are consist with the 16-bit cryptographic datapath. Therefore, we can conclude that CML_TIGFET circuit is superior for SCA-resistance than the CML_CMOS circuit. In summary, the cryptographic circuits using TIGFETs are well suitable for resource-constrained applications given its low power and area overhead combined with its comparable security levels compared to CMOS-based implementations.

VI. Conclusion

In this article, TIGFETs are leveraged to the circuit-level SCA countermeasures. Circuit designs using TIGFETs maintain a similar security-level against SCA without sacrificing the power consumption and area overhead compared to CMOS counterparts. A library with six basic logic gates based on the TIGFET was designed and optimized based on the performance evaluation. Three cryptographic circuits were built using this library and CPA was performed to evaluate the SCA-resilience. Experimental results proved that the TIGFETs have an advantage in the hardware security applications compared to CMOS transistors.

In the future, we will develop a generic standard cell library with different driving strengths for large-scale designs. The SCA-resilience of other cryptographic implementations will also be evaluated. Furthermore, low-power techniques will be explored to further reduce the power consumption for power-constrained devices such as IoT devices. Finally, the structure of our proposed TIGFET-based logics are optimized to achieve several all desired properties with improved metrics of power, area, delay, and security.

References

[1] C. Zhang, Z. Liu, Y. Chen, J. Lu, and D. Liu, "A flexible and generic Gaussian sampler with power side-channel countermeasures for quantum-secure Internet of Things," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8167–8177, Sep. 2020.

[2] M. Masoumi, "Novel hybrid CMOS/memristor implementation of the AES algorithm robust against differential power analysis attack," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 7, pp. 1314–1318, Jul. 2020.

[3] D. Bellizia, S. Bongiovanni, P. Monsurro, G. Scotti, A. Trifiletti, and F. B. Trotta "Secure double rate registers as an RTL countermeasure against power analysis attacks," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 7, pp. 1368–1376, Jul. 2018.

[4] M. O. Choudary and M. G. Kuhn, "Efficient, portable template attacks," *IEEE Trans. Inf. Forensics Security*, vol. 13, pp. 490–501, 2018.

[5] B. Yu, P. E. Gaillardon, X. S. Hu, M. Niemier, J.-S. Yuan, and Y. Jin, "Polarity-controllable silicon nanoWire FET-based security," in *Security Opportunities in Nano Devices and Emerging Technologies*. Boca Raton, FL, USA: CRC Press, 2017, p. 143.

[6] J. Shen, L. Geng, and F. Zhang, "Dynamic current mode logic based flip-flop design for robust and low-power security integrated circuits," *Electron. Lett*, vol. 53, no. 18, pp. 1236–1238, 2017.

[7] Y. Bi, K. Shamsi, J.-S. Yuan, Y. Jin, M. Niemier, and X. S. Hu, "Tunnel FET current mode logic for DPA-resilient circuit designs," in *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 3, pp. 340–352, Jul./Sep. 2017.

[8] S. D. Kumar, H. Thapliyal, and A. Mohammad, "FinSAL: FinFET-based secure adiabatic logic for energy-efficient and DPA resistant IoT devices," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 37, no. 1, pp. 110–122, Jan. 2018.

[9] S. D. Kumar, H. Thapliyal, and A. Mohammad, "EE-SPFAL: A novel energy-efficient secure positive feedback adiabatic logic for DPA resistant RFID and smart card," *IEEE Trans. Emerg. Topics Comput.*, vol. 7, no. 2, pp. 281–293, Apr.–Jun. 2019.

[10] S. Kaedi, M. A. Doostari, and M. B. Ghaznavi-Ghoushchi, "A DPA attack on IOA data-dependent delay countermeasure based on an inherent tempo-spatial data dependency," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 66, no. 8, pp. 1341–1345, Aug. 2019.

[11] A. Roohi and R. F. DeMara, "PARC: A novel design methodology for power analysis resilient circuits using spintronics," *IEEE Trans. Nanotechnol.*, vol. 18, pp. 885–889, Aug. 2019.

[12] M. M. Sharifi, *et al.*, "A novel TIGFET-based DFF design for improved resilience to power side-channel attacks," in *Proc. Design Autom. Test Europe Conf. Exhibit. (DATE)*, 2020, pp. 1253–1258.

[13] X. Tang, J. Zhang, P.-E. Gaillardon, and G. De Micheli, "TSPC flip-flop circuit design with three-independent-gate silicon nanowire FETs," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, 2014, pp. 1660–1663.

[14] B. Yu, P.-E. Gaillardon, X. S. Hu, M. T. Niemier, J.-S. Yuan, and Y. Jin, "Leveraging emerging technology for hardware security-case study on silicon nanowire fets and graphene symfets," in *Proc. IEEE 23rd Asian Test Symp.*, 2014, pp. 342–347.

[15] Y. Bi, K. Shamsi, J.-S. Yuan, F.-X. Standaert, and Y. Jin, "Leverage emerging technologies for DPA-resilient block cipher design," in *Proc. Design Autom. Test Europe Conf. Exhibit. (DATE)*, 2016, pp. 1538–1543.

[16] Y. Bi *et al.*, "Emerging technology-based design of primitives for hardware security," *ACM J. Emerg. Tech. Comput. Syst.*, vol. 13, no. 1, pp. 1–19, 2016.

[17] E. Giacomin and P. Gaillardon, "Differential power analysis mitigation technique using three-independent-gate field effect transistors," in *Proc. IFIP/IEEE Int. Conf. Very Large Scale Integr. (VLSI-SoC)*, 2018, pp. 107–112.

[18] Y. Ishai, A. Sahai, and D. Wagner, *Private Circuits: Securing Hardware Against Probing Attacks* (Lecture Notes in Computer Science 2729). Berlin, Germany: Springer, 2003, pp. 463–481.

[19] E. Trichina, D. De Seta, and L. Germani, "Simplified adaptive multiplicative masking for AES," in *Proc. Inf. Conf. Cryptogr. Hardw. Embedded Syst.*, 2002, pp. 187–197.

[20] P. De, U. Parampalli, and C. Mandal, "Secure path balanced BDD-based pre-charge logic for masking," *IEEE Trans. Circuits Syst. I, Reg. Paper*, vol. 67, no. 12, pp. 4747–4760, Dec. 2020.

[21] L. Zhang, A. A. Ding, Y. Fei, and P. Luo, "Efficient nonprofiling 2nd-order power analysis on masked devices utilizing multiple leakage points," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 5, pp. 843–855, Sep./Oct. 2019.

[22] T. Ichikawa, D. Suzuki, and M. Saeki, "Random switching logic: A new countermeasure against DPA and second-order DPA at the logic level," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. 90, no. 1, pp. 160–168, 2007.

[23] T. E. Pogue and N. Nicolici, "Incremental fault analysis: Relaxing the fault model of differential fault attacks," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 3, pp. 750–763, Mar. 2020.

[24] A. Chakraborty, B. Mazumdar, and D. Mukhopadhyay, "A combined power and fault analysis attack on protected grain family of stream ciphers," *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, vol. 36, no. 12, pp. 1968–1977, Dec. 2017.

[25] M. Alam, S. Ghosh, M. J. Mohan, D. Mukhopadhyay, D. R. Chowdhury, and I. S. Gupta, "Effect of glitches against masked AES S-box implementation and countermeasure," *IET Inf. Security*, vol. 3, no. 1, pp. 34–44, 2009.

[26] K. Tiri and I. Verbauwhede, "Securing encryption algorithms against DPA at the logic level: Next generation smart card technology," in *Proc. Int. Conf. Crypto. Hardw. Embedded Syst.*, 2003, pp. 125–136.

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

[28] D. Bellizia, S. Bongiovanni, M. Olivieri, and G. Scotti, "SC-DDPL: A novel standard-cell based approach for counteracting power analysis attacks in the presence of unbalanced routing," *IEEE Trans. Circuits Syst. I, Reg. Paper*, vol. 67, no. 7, pp. 2317–2330, Jul. 2020.

[29] P. De, C. Mandal, and U. Prampalli, "Path-balanced logic design to realize block ciphers resistant to power and timing attacks," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 5, pp. 1080–1092, May 2019.

[30] M. Nassar, S. Bhasin, J.-L. Danger, G. Duc, and S. Guilley, "BCDL: A high speed balanced DPL for FPGA with global precharge and no early evaluation," in *Proc. Design Autom. Test Europe Conf. Exhibit.*, 2010, pp. 849–854.

[31] B. Fadaeinia and A. Moradi, "3-phase adiabatic logic and its sound SCA evaluation," *IEEE Trans. Emerg. Topics Comput.*, early access, Feb. 27, 2020, doi: 10.1109/TETC.2020.2976711.

[32] 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.

[33] M. Bucci, L. Giancane, R. Luzzi, and A. Trifiletti, "A flip-flop for the DPA resistant three-phase dual-rail pre-charge logic family," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 11, pp. 2128–2132, Nov. 2012.

[34] S. Badel *et al.*, "A generic standard cell design methodology for differential circuit styles," in *Proc. Design Autom. Test Europe*, 2013, pp. 843–848.

[35] I. Hassoune, F. Mace, D. Flandre, and J.-D. Legat, "Low-swing current mode logic (LSCML): A new logic style for secure and robust smart cards against power analysis attacks," *Microelectron. J.*, vol. 37, no. 9, pp. 997–1006, 2006.

[36] A. Cevrero, F. Regazzoni, M. Schwander, S. Badel, P. Ienne, and Y. Leblebici, "Power-gated MOS current mode logic (PG-MCML): A power aware DPA-resistant standard cell," in *Proc. 48th ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, 2011, pp. 1014–1019.

[37] P.-E. Gaillardon, M. Hasan, A. Saha, L. G. Amarù, R. Walker, and B. S. Rodriguez, "Digital, analog and RF design opportunities of three-independent-gate transistors," in *Proc. IEEE Int. Symp. Circuits Syst.*, 2016, pp. 405–408.

[38] J. Zhang, X. Tang, P.-E. Gaillardon, and G. De Micheli, "Configurable circuits featuring dual-threshold-voltage design with three-independent-gate silicon nanowire FETs," *IEEE Trans. Circuits Syst. I, Reg. Paper*, vol. 61, no. 10, pp. 2851–2861, Oct. 2014.

[39] J. Romero-GonzáLez and P.-E. Gaillardon, "BCB evaluation of high-performance and low-leakage three-independent-gate field-effect transistors," *IEEE J. Explor. Solid-State Computat. Devices Circuits*, vol. 4, no. 1, pp. 35–43, Jun. 2018.

[40] B. Vaquie, S. Tiran, and P. Maurine., "Secure D flip-flop against side channel attacks," *IET Circuits Devices Syst.*, vol. 6, no. 5, pp. 347–354, 2012.

[41] X. Wang *et al.*, "Role of power grid in side channel attack and power-grid-aware secure design," in *Proc. ACM/EDAC/IEEE Des. Autom. Conf.*, 2013, p. 78.

[42] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

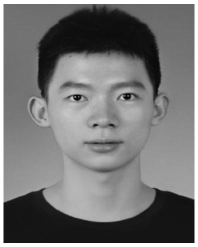
[43] D. Poggi, T. Ordas, A. Sarafianos, and P. Maurine, "Checking robustness against EM side-channel attacks prior to manufacturing," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, early access, Jun. 25, 2021, doi: 10.1109/TCAD.2021.3092297.

Yanjiang Liu received the Ph.D. degree from the School of Microelectronics, Tianjin University, Tianjin, China, in 2020.

He is currently working as a Postdoctoral Research Fellow with Information Engineering University, Zhengzhou, China, in 2020. His current research interests include cryptographic chips design, side-channel prevention, anti-physical attack techniques, and hardware Trojan detection.

Jiaji He received the B.S. degree in electronic science and technology and the M.S. and Ph.D. degrees in microelectronics from Tianjin University, Tianjin, China, in 2013, 2015, and 2019, respectively.

From 2016 to 2018, he was supported by the China Scholar Council to work as a Visiting Scholar with the University of Central Florida, Orlando, FL, USA, and the University of Florida, Gainesville, FL, USA. He worked as a Postdoctoral Research Fellow from 2019 to 2021 with the School of Integrated Circuits, Tsinghua University, Beijing, China. He is currently an Associate Professor with the School of Microelectronics, Tianjin University. His research interests are digital circuit design, cryptographic chip design, hardware security, on-chip security primitive design, side-channel vulnerabilities mitigation, and formal verification.



Haocheng Ma received the M.S. degree in electronic science and technology from Tianjin University, Tianjin, China, in 2017, where he is currently pursuing the Ph.D. degree with the School of Microelectronics.

His current research interests include digital circuit design and hardware security.

Tongzhou Qu received the M.S. degree from Information Engineering University, Zhengzhou, China, in 2019, where he is currently pursuing the Ph.D. degree.

His research interests include coarse-grained reconfigurable array, cryptographic arithmetic, and cryptographic processing element.

Zibin Dai received the Ph.D. degree from Information Engineering University, Zhengzhou, China, in 2008.

He became a Full Professor with Information Engineering University in 2006. His research interests are VLSI design of crypto-ICs, energy-efficient SoC platform, and cryptographic arithmetic for security applications.