# A Novel TIGFET-based DFF Design for Improved Resilience to Power Side-Channel Attacks

Mohammad Mehdi Sharifi*, Ramin Rajaei*, Patsy Cadareanu†, Pierre-Emmanuel Gaillardon†
Yier Jin◇, Michael Niemier*, X. Sharon Hu*
*Department of Computer Science and Engineering, University of Notre Dame, USA
†Department of Electrical and Computer Engineering, The University of Utah, USA
◇Department of Electrical and Computer Engineering, University of Florida, USA

***Abstract*—Side-channel attacks (SCAs) represent a significant security threat, and aim to reveal otherwise secret data by analyzing a relevant circuit's behavior, e.g., its power consumption. While all circuit components are potential power side channels, D-flip-flops (DFFs) are often the primary source of information leakage to an SCA. This paper proposes a DFF design based on the three-independent-gate field-effect transistor (TIGFET) that reduces side-channel vulnerabilities of sequential circuits. Notably, we find that the I-V characteristics of the TIGFET itself leads to inherent side-channel resilience, which in turn enables simpler and more efficient cryptographic hardware. Our proposed design is based on a prior TIGFET-based true single-phase clock (TSPC) DFF design, which offers high performance and reduced area. More specifically, our modified TSPC (mTSPC) design exploits the symmetric I-V characteristics of TIGFETs, which results in pull-up and pull-down currents that are nearly identical. When combined with additional circuit modifications (made possible by the unique characteristics of the TIGFET), the mTSPC circuit draws almost the same amount of supply currents under all possible input transitions (less than 1% variation for different transitions), which can in turn mask information leakage. Using a 10nm TIGFET technology model, simulation results show that the proposed TIGFET-based DFF circuit leads to decreased power consumption (up to 96.9% when compared to the prior secured designs), has a low delay (15.2 ps), and employs only 12 TIGFET devices. Furthermore, an 8-bit S-box whose output is sampled by a group of eight mTSPC DFFs was simulated. A correlation power analysis attack on the simulated S-box with 256 power traces shows that the key is not revealed, which confirms the SCA resiliency of the proposed DFF design.**

***Index Terms*—three-independent-gate FET (TIGFET); side-channel attack (SCA); correlation power analysis (CPA) attack; true single-phase clock D-flip-flop (TSPC DFF).**

## I. Introduction

With the growth of integrated circuits (ICs) and the internet of things (IoT), computing devices are used in numerous aspects of daily life, e.g., to scan credit cards, in smart homes, in mobile devices, etc. The hardware required for the aforementioned applications frequently stores, processes, and transmits sensitive information such as credit card numbers, social security numbers, passwords, etc., which can be targeted in adversarial attacks. Hardware infrastructure can be protected against software attacks using cryptographic algorithms such as the Data Encryption Standard (DES) and Advanced Encryption Standard (AES) [1], [2], and it is difficult to attack said algorithms directly, as significant compute power and/or compute time is required for "brute force" methods [3].

Still, cryptographic algorithms can leak information through hardware side channels such as timing delay [4], power signatures [5], and electromagnetic radiation [6]. Said leakages make it possible for an attacker to decipher and infer encrypted information that may be stored in an IC. Among different SCAs, a correlation power analysis (CPA) attack [7] is an effective method that employs an oscilloscope to monitor the power traces of an IC, and a workstation to analyze the oscilloscope data. This attack relies on the fact that the power traces from the circuits in security-centric compute units are highly dependent on input transitions. Prior work [8]–[10] has sought to minimize power signatures associated with a given transition (i.e., to make all transitions uniform, and minimize information leakage). However, in exchange for improved side-channel resilience, all of the aforementioned circuits also suffer from higher power consumption during normal operation, as well as increased area which makes said circuits expensive to deploy in actual systems.

In sequential circuits, D-flip-flops (DFFs) can leak more information than other parts of a circuit to a given power attack [11]. This is primarily due to the fact that DFFs sample their output on a rising/falling clock edge, which synchronizes power consumption. Also, when there is a transition on input data to a DFF, data is more likely to be revealed as **(i)** CMOS devices do not have symmetric I-V characteristics for *p*-type and *n*-type devices, and therefore the pull-up and pull-down network currents are not the same in a given design and **(ii)** there are two transition types – "change" and "no change" – and during a change transition ($0 \rightarrow 1$ and $1 \rightarrow 0$) the supply current is considerably higher than that of a no-change transition ($0 \rightarrow 0$ and $1 \rightarrow 1$).

Three-independent gate field-effect transistors (TIGFETs) [12] have recently been proposed as a substitute for FinFET technology. This device can be reconfigured dynamically as an *n*-type or *p*-type transistor using the three input gates. TIGFETs also have symmetrical I-V characteristics. We aim to exploit this characteristic of TIGFET devices to design circuits (e.g., DFFs) that are inherently resilient to SCAs, i.e., **the device's symmetrical I-V characteristics provide inherent resilience**. Furthermore, TIGFETs can also be used to design compact NAND gates, XOR/XNOR gates [13], etc. that also offer symmetric switching signatures and resiliency to SCAs (although no system-level analysis was reported). TIGFET devices also have inherently low leakage, and when combined

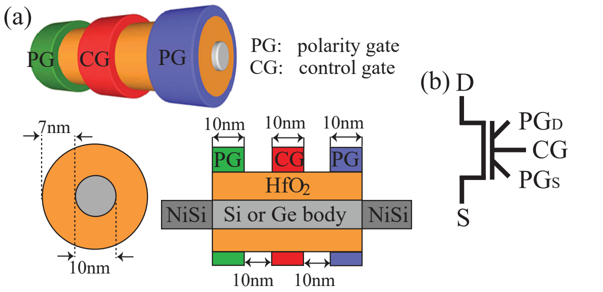

Fig. 1: **(a)** The structure of the designed device with 10 nm gate lengths and gate spacings. The total channel length is 50 nm; **(b)** The TIGFET schematic symbol; $D$ refers to the drain, $S$ to the source, $PG_D$ and $PG_S$ to the respective polarity gates, and $CG$ to the control gate.

with proper circuit designs lead to lower leakage circuits [14].

In this paper, we leverage TIGFET device symmetry in conjunction with circuit-level techniques to design a novel, low-overhead, and SCA resilient DFF, that enables extremely low maximum current variation across all types of input transitions. We have implemented a TIGFET-based, 8-bit S-box circuit to show its resiliency to CPA attacks. Moreover, through detailed circuit level simulations, we show that the proposed TIGFET-based DFF circuit decreases power consumption by up to 96.9% when compared to prior designs, and has a low delay of 15.2 ps.

The rest of the paper is organized as follows: Sec. II provides relevant background on the TIGFET device and CPA attacks, and also reviews other secure DFF designs. Sec. III proposes a novel TIGFET-based secure DFF design. Sec. IV describes evaluations of the proposed DFF. Sec. V concludes.

## II. Background

Here, we review TIGFET devices, CPA SCAs, and existing secure DFF designs that form the basis of comparisons to be presented in Sec. IV.

### A. Three-Independent-Gate Field-Effect Transistors

The TIGFET is a multiple-independent-gate reconfigurable device, which has been experimentally demonstrated using silicon [12], [15], and 2-D channel materials such as tungsten diselenide [16]. A TIGFET device consists of a semiconducting channel, metallic source and drain contacts, and three gate electrodes: the *Control Gate* (CG), and two symmetric *Polarity Gates* (PG) at the source and drain to act as electrostatic doping means at the Schottky barrier interfaces. The general device structure is illustrated in Fig. 1a.

Table I provides a summary of TIGFET device operation based on the transistor symbol seen in Fig. 1b. The selected PG voltage determines the dominant carrier in the channel, effectively choosing if the device will act as $n$-type (electron-dominated) or $p$-type (hole-dominated). (If the PGs are increased to the supply voltage, the device will be $n$-type, and if the PGs are grounded, the device will be $p$-type.) The CG acts as a standard transistor gate in that the state of the CG determines whether the dominant carriers will pass through from source-to-drain.

TABLE I: Gate Biases for Different TIGFET Configurations

| **Dominant carrier** | **Device State** | **Applied Potentials (V)** | | |
|---|---|---|---|---|
| | | $V_{PG_S}$ | $V_{CG}$ | $V_{PG_D}$ |
| $n$-type | OFF | $V_{DD}$ | 0 | $V_{DD}$ |
| | ON | $V_{DD}$ | $V_{DD}$ | $V_{DD}$ |
| $p$-type | OFF | 0 | $V_{DD}$ | 0 |
| | ON | 0 | 0 | 0 |

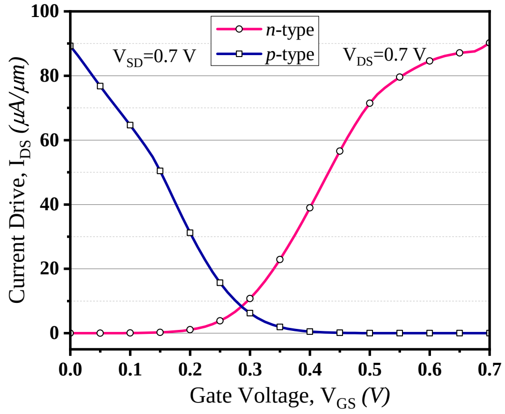

Fig. 2: $I_D$-$V_G$ characteristics of the simulated device at $V_{DD}$= 0.7 V. The switching is centered around $V_{GS}$= 0.3 V.

To validate the performance of TIGFET devices at advanced nodes, Synposys Sentaurus was used to perform TCAD simulations based on a 10 nm diameter silicon-nanowire TIGFET device with gates of 10 nm and separations of 10 nm. Nickel silicide-to-silicon is the assumed Schottky barrier contact and the dielectric layer is $HfO_2$ with a thickness of 8 nm.

The maximum current drive at the nominal supply voltage of 0.7 V for $n$-type operation is 90.20 $\mu$A/$\mu$m, and for $p$-type is 89.25 $\mu$A/$\mu$m as seen in Fig. 2. The <1% asymmetry between $n$-type and $p$-type operation seen in this simulation is a significant improvement over the previously published 22 nm TIGFET circuit model [12] which exhibited almost 10% asymmetry. The loss in current drive compared to the previous model is due to the lowering of the supply voltage from 1.2 V to 0.7 V which was done to provide for fair comparisons at the 10 nm CMOS technology node.

### B. Correlation Power Analysis (CPA) Attack

In this work, we study the efficacy of our proposed DFF against CPA attacks. CPA attacks can be more effective than other attacks such as differential power analysis (DPA), and can also decrease the number of power samples required. CPA attacks are performed by monitoring the power traces associated with cryptographic hardware. The goal of a CPA attack is to craft a power model of the device under attack, which can be used to find the correlation between predicted power consumption and actual power consumption [17]. After collecting enough power traces from the power supply of the cryptographic hardware, an adversary can infer the secret key by looking for the highest level of correlation, using the power model.

### C. Secure DFFs

Conventional DFF designs are usually based on a master/slave structure which employs two consecutive latches controlled by a clock signal. Conventional designs typically have different charge/discharge currents, i.e., for "change" $\{0 \rightarrow 1, 1 \rightarrow 0\}$ and "no-change" $\{0 \rightarrow 0, 1 \rightarrow 1\}$ transitions. As a result, these designs are vulnerable to SCAs like the CPA attack. This is because the CPA attack power model is computed based on the number of bits flipped in the output due to an input change. Thus, having different power consumptions for "change" and "no-change" transitions in DFFs can leak information that can be exploited in a CPA attack. To address this issue, a number of secure DFFs have been proposed. Common characteristics associated with previous secure DFF designs include **(i)** circuits that employ static storage elements, and as such, have higher delays when compared to dynamic storage elements (e.g., similar to SRAM and DRAM memories); **(ii)** designs that employ various "dummy" transistors to insert redundant node transitions to balance supply currents associated with different input transitions.

For example, in [8], a sense amplifier based logic FF (SABL-FF) was proposed. The SABL-FF design is based on a sense amplifier circuit. The circuit is sensitive to the voltage difference between its inputs and amplifies the difference in the output (a positive difference results in "1" and a negative difference results in "0" at the output). The SABL-FF requires both the input data and its complementary value ($D$ and $\bar{D}$) and outputs $Q$ and $\bar{Q}$. As the SABL-FF is symmetric, it uses and produces differential data, and has almost the same current variations for an input "change" transition. However, this circuit does not have the same current variation for an input "change" and "no change". This results in non-symmetric supply currents for various input transitions, which can adversely impact the maximum current variation (MCV) of the design, which is defined in Eq. 1.

$$MCV = \frac{I_{max} - I_{min}}{I_{max}} \tag{1}$$

When a circuit has a higher MCV, it is more susceptible to SCAs [18], [13]. In Eq. 1, $I_{max}$ and $I_{min}$ denote the maximum and minimum supply currents of the circuit, respectively, when measured at the rising edge of the clock over 4 different transitions including $\{0 \rightarrow 0, 0 \rightarrow 1, 1 \rightarrow 0, 1 \rightarrow 1\}$.

In [9], a dynamic current mode logic (DyCML) secure DFF design is proposed. Similar to the SABL-FF design, the DyCML-FF design is a differential, master/slave, and precharge sense amplifier-based circuit. This circuit requires three clock domains and two complementary data inputs. Though DyCML-FF produces symmetric current variation for all transitions, it requires a large number of transistors. Furthermore, it is not technology node scaling friendly. Our simulations show that when the DyCML-FF is implemented assuming a 10nm FinFET model, an appropriate pull-down path cannot be realized due to decreased capacity of the dynamic current source, and the circuit does not function properly. To combat this problem, the transistors that serve as the capacitor require large sizes, which adversely affects area.

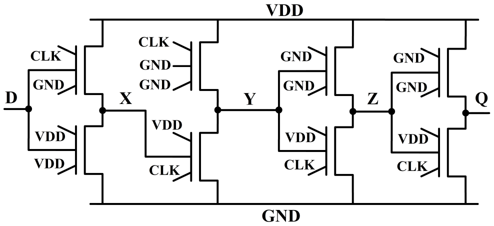

Fig. 3: The original TIGFET TSPC design transistor level schematic.

### D. TIGFET DFF designs

In [14], a TIGFET-based TSPC-DFF design is proposed and Fig. 3 shows its circuit diagram. For simplicity, the set and reset signals and the associated transistors are removed. Unlike the SABL-FF and DyCML-FF designs, the TSPC-DFF design only requires the input data and does not need the input complement. It also only needs a single clock phase and has a smaller area when compared to other conventional DFFs. The area of the TSPC-DFF can be further reduced by using one TIGFET device to realize two serial CMOS devices. TIGFET-based TSPC DFFs have lower leakage when compared to a FinFET TSPC-DFF, due to the inherent low-power and low-leakage property of the TIGFET device. However, the TSPC-DFF cannot offer a low MCV for all input transitions. In fact, our simulation results show that the current variation can be as large as 24.7%. We will introduce a modified TSPC-DFF, denoted as mTSPC-DFF to overcome this MCV problem.

## III. Proposed Secure TIGFET-based DFF

Our proposed TIGFET-based mTSPC DFF for power attack resiliency is illustrated in Fig. 4a. This circuit is comprised of 12 TIGFETs and as will be seen, offers a low MCV across all input transitions. In this section, we describe the design itself and explain how its structure should enable low MCV, as well as reduced design complexity when compared to other designs. Specific gains will be quantified in Sec. IV.

We first discuss **circuit functionality**. Per Fig. 4a, the proposed mTSPC design includes two states: pre-charge (when $CLK$ is '0') and evaluate (when $CLK$ is '1'). In the precharge state, devices Tp1 and Tn1 act as an inverter and provide the complementary state of $D$ at $X$. At the same time, nodes $Y$ and $Z$ go high through their active pull-up networks. Specifically, Tp2 and Tp3 are ON and bring node $Y$ to a high state. The evaluate state occurs at the rising edge of $CLK$, when $CLK$ changes from '0' to '1'. In this state, all the pull-up networks of the circuit switch OFF, and depending on the input value, the output node either remains high or goes down. (That is, Tp2 and Tp3 turn OFF and based on the value of $X$, $Y$ stays high or goes to a low state.) Comparing the design shown in Fig. 4a with that in Fig. 3, one can see that the number transistors are increased from 8 to 12. The additional transistors are essential to minimize MCV. Fig. 4b shows the regular operation waveform of the proposed mTSPC design.

TABLE II: Node charges/discharges of mTSPC vs. input transitions

| Nodes of the mTSPC design | | CLK=0 | | | | CLK=1 | | | | Total Number of Charges/Discharges |
|---|---|---|---|---|---|---|---|---|---|---|
| | | X | Y | Z | Q | X | Y | Z | Q | |
| Output Transition | $0 \rightarrow 0$ | ↑ | — | ↑ | — | — | ↓ | — | ↓ | 2↑ + 2↓ |
| | $0 \rightarrow 1$ | ↓ | ↑ | — | ↑ | — | — | ↓ | — | 2↑ + 2↓ |
| | $1 \rightarrow 0$ | — | ↑ | — | — | — | ↓ | — | ↓ | 2↑ + 2↓ |
| | $1 \rightarrow 1$ | — | — | ↑ | — | — | — | ↓ | — | 1↑ + 1↓ |

The original TSPC design will not lead to acceptably low MCV metrics (see Sec. IV-A). This is because it has more internal node charges/discharges during "change" transitions when compared to "no change" transitions. As such, the supply currents for $\{0 \rightarrow 1$ and $1 \rightarrow 0\}$ transitions will be significantly higher than for $\{0 \rightarrow 0$ and $1 \rightarrow 1\}$ transitions, and the MCV metric will be high for this design. To address this challenge, we added extra transitions to nodes $Z$ and $Q$ to increase the supply currents of "no change" transitions. To do so, we changed the pull-up network at node $Z$, which provides the inverse of logic signal $Y$. In the mTSPC design, transistors Tp4 and Tp5 bring node $Z$ to a precharge state when $CLK$ is low. Similarly, the pull-up network of node $Q$ is also altered in the mTSPC design to add a precharge state at this node as well. Therefore, per Table II, there is one transition at $Z$ or $Q$ in all input transitions. To balance the supply currents of all transitions, we also re-design the pull-up and pull-down networks of node $Y$. Section IV-A quantitatively evaluates the charge currents of mTSPC design and measures the MCV.

We now further discuss how the mTSPC design delivers **symmetric switching signatures** and inherent resilience to SCAs. As noted earlier, we aim to minimize MCV in order to provide resilience to SCAs. For each input transition of the DFF – $\{0 \rightarrow 0,\ 0 \rightarrow 1,\ 1 \rightarrow 0,\ 1 \rightarrow 1\}$ – the current variations should be as close as possible, and ideally identical. To this end, the symmetric I-V characteristics of TIGFET devices enable a simplified design. Table II shows the state changes of the intermediate nodes when $CLK$ transitions from '0' to '1' for all four possible input transitions. As shown in the table, except for the $1 \rightarrow 1$ transition, there are exactly 2 charges and 2 discharges for each transition. The $1 \rightarrow 1$ transition, however, has 1 discharge and 1 charge. This would make the current during the $1 \rightarrow 1$ transition different from the other three. To reduce this current variation, we added transistor Tn5 to the circuit. One may point out that similar "charge/discharge" balances can also be applied to FinFET based designs. This is true and would help to improve a FinFET circuit's MCV. However, as the I-V characteristics of FinFET devices are not symmetric, balancing the number of charge/discharge nodes is not sufficient. This is due to the fact that the pull-up and pull-down currents of the FinFET are different, and reducing MCV requires balancing the currents in charge and discharge paths, which is much more challenging to do with FinFET designs than TIGFET designs.

When compared to other secure DFF designs **structurally**, the mTSPC design has additional advantages. First, per Fig. 4a, the mTSPC design is comprised of just 12 transistors, while a DyCML design (for example) requires as many as 30 transistors. (Even if one assumes that a TIGFET device has an increased area footprint of 1.5× [14] to account for extra gate signals, circuit area would still be reduced.) Furthermore, the mTSPC design requires only one clock signal, while designs such as the DyCML FF require three, i.e., $CLK$, $\overline{CLK}$ and a third, delayed clock signal, in order to function correctly. Moreover, as will be seen in Sec. IV, since the mTSPC design does not require static storage elements, the clock-to-output delay is lower.

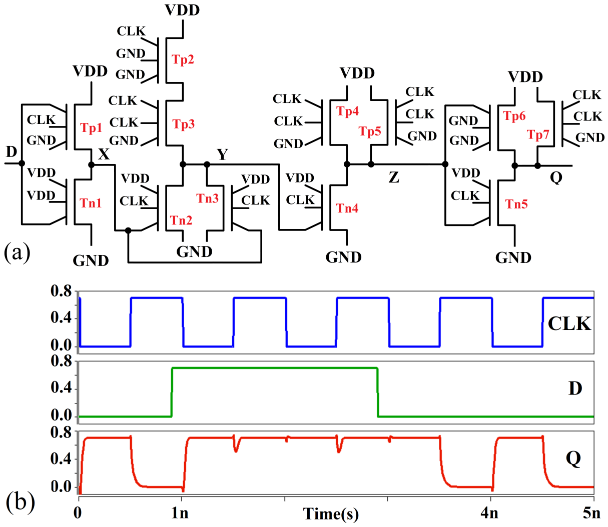

Fig. 4: The TIGFET mTSPC design: **(a)** transistor level schematic; **(b)** output waveform.

# IV. Evaluation

We have implemented our proposed design using 10nm TIGFET and FinFET device models to evaluate the security of the proposed design against SCA attacks as well as other figures of merit. To better assess our design with compared to FinFET technology, we considered both the high performance (HP) and low leakage (LL) PTM models in our analyses. For fairness, HSPICE simulations were carried out using the nominal supply voltage for each of the FinFET and TIGFET devices, 0.75 V and 0.7 V for the FinFET and TIGFET models respectively. A clock frequency of 1 GHz is assumed in all DFF circuit level simulations.

## A. Circuit Level Analysis

Table III compares our proposed mTSPC design with prior designs discussed in Sec. II-C. Specifically, we compare our design with the secure SABL-FF [8] and DyCML-FF [9] (considering both the HP and LL FinFET models). We also included the original TIGFET TSPC design in Table III to show the SCA resiliency benefits achieved by the circuit-level design techniques discussed in Sec. II. Furthermore, we also included a FinFET-based equivalent circuit of TSPC and mTSPC designs to show the specific contribution from TIGFET *devices* in improving the SCA resiliency. For this, the LL-FinFET PTM model which consumes lower power/energy and offers lower MCV is used.

TABLE III: Comprehensive comparison

| FF Design | SABL | | DyCML | | Original TSPC | | mTSPC | |
|---|---|---|---|---|---|---|---|---|
| | 10nm HP FinFET | 10nm LL FinFET | 10nm HP FinFET | 10nm LL FinFET | 10nm TIGFET | 10nm LL FinFET | 10nm TIGFET | 10nm LL FinFET |
| Maximum Current Variation (%) | 62.2% | 56.4% | 1.37% | 2.07% | 24.76% | 85.18% | 0.11% | 6.8% |
| Area Estimation (UST) | 17 | 17 | 30 | 30 | 12 | 11 | 18 | 14 |
| Avg. Energy/Cycle (aJ) | 316.6 | 206.79 | 3279.7 | 931.6 | 51.5 | 90.1 | 103.2 | 573 |
| Clock-to-output (ps) | 8.7 | 21.8 | 4.7 | 9.16 | 54.15 | 14.79 | 15.2 | 4.05 |
| Number of Clock Domains | 2 | 2 | 3 | 3 | 1 | 1 | 1 | 1 |

We first compare the SCA resiliency of our design with its counterparts. To quantitatively compare SCA resiliency of the proposed DFF with prior designs, we use maximum current variation (MCV) which is defined in Eq. 1.

We can use data from the second row of Table III to assess the contribution of the TIGFET device as well as the circuit-level approach employed in the design of the TIGFET mTSPC. Quantitatively:

- The MCV of TIGFET mTSPC is only 0.11% (6.70 $\mu$A for $\{0 \rightarrow 0$ and $1 \rightarrow 0\}$ transitions and 6.71 $\mu$A for $\{0 \rightarrow 1$ and $1 \rightarrow 1\}$ transitions) while the MCV of a FinFET equivalent circuit is no better than 6.8%. This suggests that the TIGFET device symmetry can considerably improve the resiliency of the mTSPC design. Note that, the FinFET equivalent mTSPC circuit is optimized for the lowest obtainable MCV via transistor resizing.
- When the original TIGFET TSPC design is compared to the mTSPC design, the mTSPC design offers a substantially better MCV metric (24.76% to 0.11%). This implies the contribution of the proposed circuit to the obtained SCA resiliency of TIGFET mTSPC. Furthermore, the MCV of the TIGFET mTSPC design is >10× lower than that of the DyCML design (0.11% vs. 1.37%) – as will be seen, the TIGFET design also offers improvements in other figures of merit.

The third row of Table III considers circuit area. As stated earlier, the TIGFET device has three independent programmable gates, and will have a footprint that is approximately 1.5× larger than a single FinFET device [14]. As such, when we estimate circuit area, we assume equivalent unit size transistors (UST). As shown, the UST area of the proposed TIGFET mTSPC is 40% smaller than a DyCML-FF, 33.3% larger than TIGFET TSPC (which has a much higher MCV metric), and is comparable with SABL-FF.

We now compare the average energy per cycle (AEpC) of the different DFFs. To measure AEpC, energy consumption is measured over the 4 different transitions. For each transition group, 3 cases are considered: (1) input data does not change over the clock period, (2) input data changes when the clock is in a low state, and (3) input data changes when the clock period is high. AEpC results are reported in the 4th row of Table III. As shown, the TIGFET mTSPC has an AEpC of only 103.2 aJ while an LL-FinFET equivalent has an AEpC of 573 aJ. Therefore, for the same circuit topology a FinFET design has an AEpC that is 5.6× higher than a TIGFET equivalent. Additionally, LL-FinFET and HP-FinFET DyCML based designs have AEpC metrics that are 9× and 32× higher than the TIGFET mTSPC design, respectively. When comparing the TIGFET mTSPC design with the original TIGFET TSPC design, the mTSPC design doubles the energy consumption. However, the original TSPC is not comparable with the mTSPC design in terms of MCV.

Next, we compare the performance of DFF circuits. The 5th row of Table III compares the clock-to-output delay which is the duration of the rising edge of clock to the output update. Generally, FinFET designs are faster than TIGFET designs and this is reflected in the delays of TIGFET TSPCs (mTSPC) when compared with FinFET TSPCs (mTSPC) (as well as HP-FinFET SABL-FF and FinFET DyCML-FF). However, the mTSPC design assumes dynamic logic and also does not include static storage. Consequently, the TIGFET mTSPC offers 71.9% and 30.3% delay improvements when compared to original TSPC (which is not dynamic) and LL-FinFET SABL-FF (which includes a static storage), respectively.

The last row of Table III compares the number of clock domains required for each design. This comparison also provides a sense of design complexity as more clock domains suggest more complex layouts and area overhead. Thus, another advantage of our mTSPC design is that it requires one clock domain (similar to the TSPC design) while SABL-FF and DyCML-FF need 2 and 3 clock domains, respectively.

### B. *System Level Analysis*

To study the efficacy of the proposed TIGFET mTSCP-DFF with respect to SCAs, we have implemented an 8-bit AES S-Box in [19] using TIGFET devices. (The AES S-Box is a nonlinear function which maps an input byte to an output byte. The input of the S-Box is the XORed results of an 8-bit plaintext and an 8-bit key; the goal of the CPA attack is to leak the 8-bit key.) We present two simulations, where the output of the S-box is sampled by a group of eight TIGFET mTSPC DFFs and original TIGFET TSPC DFFs. The logic gates (i.e., NAND, NOR, INV, etc.) used to implement the S-Box are simple conventional logic gates implemented with TIGFET devices. As DFFs are the major information leakage points in power attacks [11], we do not employ secure logic gates in the 8-bit S-Box implementation. Thus, by showing that the TIGFET mTSPC DFF-based S-Box is CPA resilient when using conventional gates and a *secure* DFF, it validates the utility of our design. (As we use TIGFET devices for said gates, there may be some inherent SCA resiliency due to device symmetry, e.g., TIGFET NAND (NOR) has MCVs of 25.7% (27.2%) compared to FinFET NAND (NOR) which

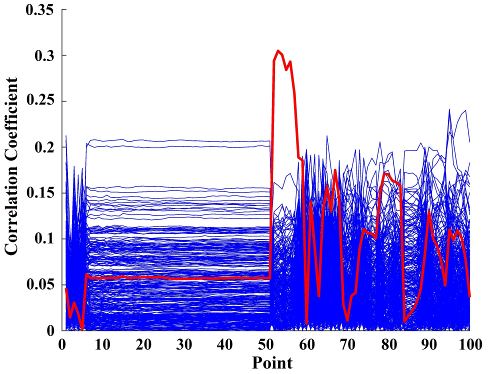

Fig. 5: CPA attack results on original TIGFET TSPC

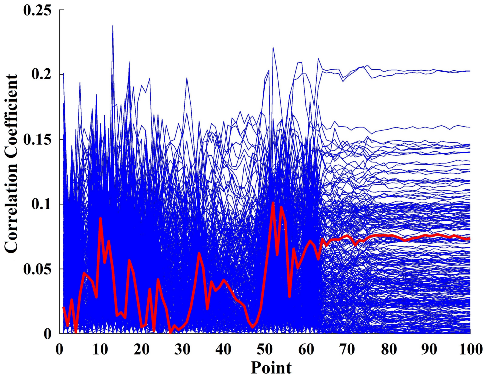

Fig. 6: CPA attack results on TIGFET mTSPC

has MCVs of 49.9% (46.1%), but the TIGFET gates are not further optimized to reduce MCV.

For both simulations, all possible 256 input value combination were injected to the S-Box, and the power traces of these inputs (sampled from HSPICE simulations) were used to perform the CPA attack. Results are shown in Fig. 5 and Fig. 6 for the original TIGFET TSPC and mTSPC TIGFET DFF, respectively. For each key guess, the computed correlation coefficient of the circuit's power consumption against the predicted power model is depicted as a line in Fig. 5 and Fig. 6. Blue lines show the correlation of incorrect keys, and red lines show the correlation of the correct key. Per Fig. 5, when the correct key is guessed there is a pronounced correlation in the power trace which indicates information leakage, and the original TIGFET TSPC-DFF is not resilient to the CPA attack. Per Fig. 6, the correct key trace does not have the strongest correlation, and the mTSPC TIGFET DFF *is resilient* to CPA attacks/does not reveal the secret 8-bit key.

## V. Conclusion

This paper proposes an SCA resilient, but simple and low-cost, DFF circuit based on the emerging TIGFET device. The DFF design exploits the symmetric behavior of a TIGFET in combination with circuit-level design techniques. We show that the inherent symmetric I-V characteristic of the TIGFET device simplifies circuit design and improves SCA resiliency. Additional circuit-level modifications enhance current balance over various input transitions to further boost SCA resiliency. The proposed design also leads to simplified layouts (e.g., due to the reduction in required clock domains) when compared to other proposed designs. Simulation results confirm that the proposed DFF leads to ultra low MCV (just 0.11%) while prior designs cannot offer MCVs below 1.37% (and require greater overhead). Furthermore, the new TIGFET DFF can be 5× to 32× more energy efficient than prior works. As TIGFETs are CMOS compatible, this suggests that they may be an ideal candidate for realizing side-channel resilient cryptographic hardware. This is further supported by the CPA attack results based on circuit-level simulations of a TIGFET based 8-bit S-box implementation. This will be explored in future work.

## Acknowledgment

This work was supported by Intel.

## References

[1] E. Biham et al. *Differential cryptanalysis of the data encryption standard*. Springer Science & Business Media, 2012.

[2] J. Daemen et al. *The design of Rijndael: AES-the advanced encryption standard*. Springer Science & Business Media, 2013.

[3] R. A. E. B. L. Knudsen. Serpent: A proposal for the advanced encryption standard. In *First Advanced Encryption Standard (AES) Conference, Ventura, CA*, 1998.

[4] P. C. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In *Annual International Cryptology Conference*, pages 104–113. Springer, 1996.

[5] P. Kocher, et al. Differential power analysis. In *Annual International Cryptology Conference*, pages 388–397. Springer, 1999.

[6] K. Gandolfi, et al. Electromagnetic analysis: Concrete results. In *International workshop on cryptographic hardware and embedded systems*, pages 251–261. Springer, 2001.

[7] E. Brier, et al. Correlation power analysis with a leakage model. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 16–29. Springer, 2004.

[8] K. Tiri, et al. A dynamic and differential cmos logic with signal independent power consumption to withstand differential power analysis on smart cards. In *Proceedings of the 28th European solid-state circuits conference*, pages 403–406. IEEE, 2002.

[9] J. Shen, et al. Dynamic current mode logic based flip-flop design for robust and low-power security integrated circuits. *Electronics Letters*, 53(18):1236–1238, 2017.

[10] D. D. Hwang, et al. Aes-based security coprocessor ic in 0.18-$muhboxm$ cmos with resistance to differential power analysis side-channel attacks. *IEEE J. of Solid-State Circuits*, 41(4):781–792, 2006.

[11] B. Vaquie, et al. Secure d flip-flop against side channel attacks. *IET Circuits, Devices Systems*, 6(5):347–354, Sep. 2012.

[12] J. Zhang, et al. Configurable circuits featuring dual-threshold-voltage design with three-independent-gate silicon nanowire fets. *IEEE T. on Circuits and Systems I: Regular Papers*, 61(10):2851–2861, 2014.

[13] E. Giacomin et al. Differential power analysis mitigation technique using three-independent-gate field effect transistors. In *2018 IFIP/IEEE International Conference on Very Large Scale Integration (VLSI-SoC)*, pages 107–112. IEEE, 2018.

[14] X. Tang, et al. Tspc flip-flop circuit design with three-independent-gate silicon nanowire fets. In *2014 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1660–1663. IEEE, 2014.

[15] M. De Marchi, et al. Polarity control in double-gate, gate-all-around vertically stacked silicon nanowire fets. In *2012 International Electron Devices Meeting*, pages 8–4. IEEE, 2012.

[16] G. V. Resta, et al. Doping-free complementary logic gates enabled by two-dimensional polarity-controllable transistors. *ACS nano*, 12(7):7039–7047, 2018.

[17] O. Lo, et al. Power analysis attacks on the aes-128 s-box using differential power analysis (dpa) and correlation power analysis (cpa). *Journal of Cyber Security Technology*, 1(2):88–107, 2017.

[18] I. Levi, et al. A survey of the sensitivities of security oriented flip-flop circuits. *IEEE Access*, 5:24797–24809, 2017.

[19] J. Daemen et al. Specification for the advanced encryption standard (aes). *Federal Information Processing Standards Publication*, 197, 2001.