Abstract—Hardware security vulnerabilities are a major concern for embedded computing devices which are now used in many applications such as credit cards, SIM cards, or financial systems, putting sensible data at risk. Such systems are often targeted by differential power attacks, where the power trace can be monitored in order to get access to the sensible data. To alleviate this issue, a possible technique proposed in literature is to use a complementary gate (e.g., computing both XOR and XNOR operations in parallel) in order to have a symmetrical power trace for all possible input combinations. However, this technique results in a large area and power overhead since it approximatively requires twice the number of transistors. Recently, novel technologies such as Three-Independent-Gate Field Effect Transistors (TIGFETs) have been shown to be able to realize compact logic gates using less transistors when compared to Complementary Metal Oxide Semiconductor (CMOS) technology. In this paper, we investigate the benefits of using TIGFETs in terms of hardware security. First, we show that using the complementary gate technique with TIGFETs can reduce the transistor count, the power trace variation, the switching power and leakage by $2\times$, $57\%$, $36\%$ and $8\times$ respectively, when compared to CMOS. In addition, we show that for the same transistor count and similar switching power, using TIGFETs can reduce the power trace variation and the leakage by $81\%$ and $6.7\times$ respectively when compared to CMOS.

I. INTRODUCTION

With the fast development of the semiconductor industry and the Internet of Things in the past few years, many critical applications now rely on the use of Integrated Circuits (ICs): credit cards, SIM cards, electronic banking, e-commerce, etc. Such systems are generally used to deal with important data such as credit card or social security numbers, insider markets information, making them a target for attackers. As a protection, the data is usually encrypted through a circuit which can be subject to hardware security vulnerabilities, threatening the successful deployment of such computing devices. Indeed, circuits may leak some important information, such as timing delay [1], power [2] or electromagnetic radiation [3], making them vulnerable to external attacks.

Attacks using information leaking from the cryptographic circuits are known as Side Channel Attacks (SCAs) and were first introduced by Kocher in 1996 [1]. In particular, Differential Power Analysis (DPA) [2] exploits the correlation between the power trace of the circuit and the cipher encryption technique. This is based on the fact that logic gates such as XOR, which are widely used in cryptographic algorithms [4], have a power trace that strongly depends on the input data [2]. As a result, such attacks have since been shown to be successful at extracting the cryptographic key of several algorithms running on different kind of digital circuits [5], [6], making hardware security a major concern for modern ICs. To this end, some work proposed to use complementary output for logic gates (e.g., computing both XOR/XNOR or OR/NOR operations in parallel) [7]–[9] in order to make the power consumption more independent from the input values. However, it requires many more transistors, considerably increasing the area footprint and the overall power consumption of the circuit.

Recently, novel technologies such as Three-Independent-Gate Field Effect Transistors (TIGFETs) [10] have been proposed as an alternative to FinFETs. By having three independent gate terminals, TIGFETs present richer switching capabilities for a given transistor. They have been shown to be able to realize compact logic gates, such as XOR or XNOR that only require 4 transistors instead of 8 for conventional CMOS gates [10]. As a result, when using the complementary gate technique to reduce the power trace variation against DPAs, the area and power consumption overhead can be greatly reduced with TIGFET devices. In this paper, we investigate the benefits of using TIGFET technology in term of hardware security with the complementary gate technique using XOR and XNOR gates. We evaluate the benefits of our circuits at the 22nm technology node by comparing Silicon NanoWire TIGFETs (TIG SiNWFTETs) with CMOS FinFET Low-Standby Power (LSTP) structures [11]. The contributions of this paper are:

- We propose a new organization for the gate inputs of the TIGFET XOR cell, leading to a reduction of the input current gate variation by $1.87\times$ when compared to the conventional design.
- When compared to CMOS, using the proposed TIGFET XOR and XNOR gates can reduce the transistor count, the power trace variation, the switching power and the leakage by $2\times$, $57\%$, $26\%$ and $8\times$ respectively.
• We show that for the same number of transistors and a similar switching power, using TIGFETs decreases the power trace variation and the leakage by 81% and 6.7 × respectively, when compared to CMOS.

The rest of this paper is organized as follows: In Section II, we provide the technical background about TIGFET technology and review some side channel attack protection techniques. Section III presents the proposed TIGFET-based design. Section IV shows experimental results. Section V concludes this paper.

II. TECHNICAL BACKGROUND

In this section, we first present the necessary background on TIGFET technology and review some generalities about side channel attacks and possible mitigation techniques.

A. Operations of TIGFET

Fig. 1 shows a scanning electron microscopy view of a fabricated TIGFET device [12] with its three independent gate contacts: the Control Gate (CG) which controls the potential barrier in the channel and the Polarity Gate at Source (PGS) and the Polarity Gate at Drain (PGD) which modulate the Schottky barriers at source and drain. Depending on the three gate voltage biasings, a TIGFET can be configured in 4 modes: low-\( V_T \) n-type, high-\( V_T \) n-type, low-\( V_T \) p-type and high-\( V_T \) p-type. In addition to polarity control, a unique feature of TIGFET technology is their ability to act as two series or parallel transistors by biasing one input and controlling the two others. Therefore, by using TIGFET, more compact logic gates can be built. More details on this feature of TIGFETs can be found in [10].

![Fig. 1: Scanning Electron Microscopy image of a fabricated TIGFET device using four vertically stacked silicon nanowires [12]. The three gates are surrounding the silicon nanowires in a gate-all-around fashion.](image)

TIGFET devices have been successfully fabricated with several channel technologies such as FinFET [13], 2D [14] or SiNWFET [10]. In this paper, we will consider the latter since it provides better electrostatic control over the channel and better scalability properties than FinFETs [15] while being fully compatible with CMOS. Being based on Schottky barriers, TIGFET devices exhibit very low leakage compared to their CMOS counterpart [10], as it will be demonstrated in Section IV. In the considered TIGFET structure, the nanowires have a diameter \( d \) of 15nm while the length of the gates are both 24nm long. The dielectric layer is HfO\(_2\) with a thickness of 5.1nm and an equivalent oxide thickness of 0.8nm. These materials were selected to ensure full compatibility with standard CMOS processes. The dual-\( V_T \) I-V curves of a single nanowire TIGFET, simulated with TCAD Sentaurus [16], are shown in Fig. 2. The solid lines are the low-\( V_T \) configurations and the dashed lines are the high-\( V_T \) configuration. The extracted on-current is about 33.5\( \mu \)A. While the current drive is lower than CMOS (51.5\( \mu \)A), TIGFET devices unlock new circuits opportunities and bring very competitive advantages in terms of standby energy or energy-delay product when compared to CMOS [17]. In addition, even though the required \( V_{DD} \) for the considered TIGFET technology (1.2V) is higher than the nominal voltage of the 22nm FinFET technology node (0.9V), TIGFET can still achieve a significant power reduction, as it will be demonstrated in Section IV.

![Fig. 2: Simulated I-V curve of a TIG SiNWFET for \( V_{DS} = 1.2V \) in logarithmic scale [10].](image)

B. TIGFET Based Compact Logic Gates

Due to their richer switching capabilities, TIGFETs can be used to design compact logic gates. For instance, a TIGFET-based XOR can be realized with only 4 transistors [10], as shown in Fig. 3 (a), while a CMOS XOR requires 8 transistors. In the same manner, other compact logic gates such as tristate inverter [18], used to build multiplexers or majority gates, proven to be very promising operators [19], can be realized using TIGFETs, as depicted in Fig. 3 (b) and (c) respectively.

![Fig. 3: TIGFET compact logic gates: (a) 2-input XOR; (b) tristate inverter; (c) 3-input majority gate.](image)
C. Side Channel Attacks and Mitigation Techniques

To protect the data at the hardware level against DPAs, several works proposed [20], [21] to randomize the correlation between the power trace and the input combination. While such kind of technique was proven to be efficient against DPAs, later works showed that it was still at threat against template attacks [22], [23]. Another possible technique is to reduce the dependency between the power trace and the input combination, considerably increasing the number of trace measurements required to get the private key and thus the cost required for an external attack to be successful [24]. The first technique of this kind was proposed by Tiri et al. [7] where they showed that by having a constant output load capacitance, the power trace was more independent of the input values. To do so, they proposed a sense amplifier based logic where each gate was redesigned to produce the regular output (such as AND or OR) as well as the complementary output (such as NAND or NOR). While the power trace variation was greatly reduced compared to conventional CMOS logic gates, this technique came at the price of twice the area of the power, making it difficult to expand for large circuits. On the other hand, using TIGFETs with this kind of technique can reduce the overall area overhead as well as the power consumption since they require less transistors to build logic gates when compared to CMOS, as explained in Section II-B.

III. TIGFET-based Power Trace Variation Mitigation Technique

The origin of the power trace variation in conventional logic gates is due to two factors: (i) the input and output loads of the gate seen for each transition; (ii) the current characteristic of n-type or p-type transistors. Symmetrizing both current and capacitances ensure that the same energy is consumed/dissipated for each transition and hence leads to the same power trace. In this section, we first show how to rearrange the gate inputs for the TIGFET XOR in order to symmetrize the input loads. Without loss of generality, we focus in this paper on the XOR operator since it is widely used in cryptography for its mathematical properties (such as the ability to realize an addition modulo 2) [4]. Then, we present how to reduce the output power trace with the complementary gate technique by using TIGFET XOR and XNOR gates.

A. Symmetrical TIGFET XOR Design

As for the CMOS structure, the conventional TIGFET XOR [10], depicted in Fig. 4 (a), presents different power traces coming from the different input loads on the polarity and control gates. To mitigate this effect, the inputs can be rearranged in a certain way in order to symmetrize the input gate load, without changing the XOR functionality, as depicted in Fig. 4 (b). With this configuration, each input (A, B, \( \overline{A} \) and \( \overline{B} \)) sees one control gate and two polarity gates so the same equivalent input gate capacitance. We will see in the experimental section that this technique leads to a lower input gate power variation when compared to the conventional design.

B. Complementary TIGFET XOR/XNOR Circuit

In Section II-C, we reported that using complementary gates (AND and NAND or XOR and XNOR) was a possible mitigation scheme against side channel attack by balancing the output load between the different possible input combinations. Fig. 5 (a) shows CMOS XOR and XNOR gates. By having complementary outputs, if A is switching from 0 to 1, one output will switch from 0 to 1 and the other one from 1 to 0. As a result, one gate is loading while the other is discharging, so the power output trace is less dependent on the input values, making it harder for external attackers to find a correlation with the private key. While it helps reducing the power trace variation, it comes roughly at twice the cost in term of area and power consumption [7]. Thanks to their ability to realize compact logic gate as reviewed in Section II-B, TIGFET-based logic gates can take advantage of this technique without leading to a large area and power overhead. As shown in Fig 5 (a) and (b), CMOS XOR and XNOR cells require a total of 16 transistors while TIGFET XOR and XNOR gates only requires 8 transistors. Therefore, by having twice less transistors, TIGFET XOR and XNOR gates are expected to reduce the power consumption when compared to CMOS XOR and XNOR gates since the datapath goes...
through less diffusion capacitances. In addition, a standalone CMOS XOR gate requires the same number of transistors (8) than a TIGFET using the complementary gate technique (XOR and XNOR gates combined). As a result, for the same number of transistor, TIGFET can reduce the output power trace variation, leading to more robust designs against side channel attacks. Both of those predictions will be verified in Section IV.

IV. EXPERIMENTAL RESULTS

In this section, we demonstrate the benefits of using TIGFETs to realize robust logic gates against DPAs. We first introduce our experimental methodology and then show the benefits of the proposed symmetrical TIGFET design. Then, we compare the power trace as well as the switching and leakage power of TIGFET and CMOS XOR and XNOR gates.

A. Experimental Methodology

For circuit-level simulations, the VerilogA table model from [10] has been used for the TIGFET model. Its equivalent RC circuit of is depicted in Fig. 6. The current values were extracted from TCAD Sentaurus [16] simulations under the assumptions discussed in Section II-A. Capacitance values have been extracted from TCAD simulations as an average value under all possible bias configurations to model intrinsic capacitances of the device. The supply voltage used for the TIG SiNW FETs is 1.2V. The Predictive Technology Model (PTM) 20nm-FinFET Low-Standby-Power (LSTP) [11] is used in the circuits of the CMOS logic gates. They have a nominal supply voltage $V_{DD} = 0.9V$. Current and power values are extracted from HSPICE simulations [25].

B. Conventional and Symmetrical TIGFET XOR Cells Comparison

As explained in Section III-A, TIGFET XOR inputs can be rearranged in order to symmetrize the gate loads without changing the XOR functionality. In that way, each input sees the same equivalent input capacitance, reducing the overall power trace variation. To evaluate the benefits of this re-arrangement, we evaluated the gate current values for each possible input combinations. To do so, we monitored the total output current coming from the input inverters, which is also the input gate currents, as shown in Fig. 7(a). $A_{pre}$ and $B_{pre}$ denotes signals $A$ and $B$ before conditioning. As illustrated in Fig. 7(b), there are some "positive" (denoted as $I_{gate,pos}$) and "negative" (denoted as $I_{gate,neg}$) current peaks depending on the input transition. In order to study the current gate variation for the conventional and symmetrical TIGFET XOR gates, we report the minimum and maximum input currents for both $I_{gate,pos}$ and $I_{gate,neg}$ for each transition in Fig. 7(c). As predicted, the symmetrical design can reduce the input gate currents, up to 1.87× compared to the conventional implementation. In the rest of this paper, we will only consider symmetrical TIGFET XOR and XNOR cells.

C. CMOS and TIGFET Complementary Gates (XOR and XNOR) Comparison

To evaluate the power trace of both CMOS and TIGFET circuits, we evaluate the minimum peak current $I_{supply,min}$ for every possible transitions, as shown in Fig. 8(a) on the orange curve. From this, we compute the minimum and maximum $I_{supply}$ peak values ($I_{supply,min}$ and $I_{supply,max}$ respectively) and derive the $I_{supply}$ variation for both architectures. The supply voltage being constant, monitoring $I_{supply}$ peak values is the same as monitoring the total power trace values. For
the rest of this paper, we refer to current trace variation by power trace variation. Here, we first compare \( I_{\text{supply}} \) peak values for both CMOS and TIGFET circuits using the complementary gate technique with XOR and XNOR cells, whose simulation schematics are shown in Fig. 8 (b) and (c) respectively. For the rest of this paper, we denote XOR and XNOR gates by XOR/XNOR. As shown in Table I, the maximum power variation for TIGFET is 12.5\% lower than CMOS, making TIGFET-based design more robust against DPAs. Note that the power trace variation could be further improved against CMOS, by using an engineered TIGFET device with a high level of symmetry between n-type and p-type configurations, as presented in [26]. In addition, the TIGFET circuit only requires 8 transistors while the CMOS circuit requires 16, decreasing the overall area and reducing the power consumption, as it will be shown in Section IV-E.

D. TIGFET Complementary Gates (XOR and XNOR) Comparison with Standalone CMOS XOR Gate

As anticipated in Section II-A, due to their richer switching capabilities, TIGFET can realize smaller logic gates in term of transistor count when compared to CMOS. As we saw, the technique of using a complementary gate to reduce the power trace variation can be applied with TIGFETs, without compromising the overall area. More particularly, the TIGFET XOR and XNOR cells require the same number of transistors (8) as a standard CMOS XOR. Fig. 9 (a) shows the power trace values for different input combinations for the TIGFET XOR/XNOR gates and the CMOS XOR gate. While the CMOS XOR has a maximum power trace variation of 64\%, the symmetrized TIGFET XOR/XNOR circuit only presents a 12\% variation, leading to a power trace variation reduction of 81\%, as shown in 9 (b). Note that this reduction is realized with the same number of transistors between both structures.

E. Summary and Power Consumption Evaluation

In this part, we summarize the power trace variation for 4 architectures: CMOS XOR, CMOS XOR/XNOR, TIGFET XOR and TIGFET XOR/XNOR. As explained before, the power trace variation denotes the maximum variation on the power trace for every possible input combinations. In addition, for each architecture, we evaluated the switching and leakage power (as the average value of all switching and leakage power values for each input combinations respectively), as well as the transistor count, as shown in Table II. By using the complementary gate technique with both XOR/XNOR, TIGFET circuits can reduce the power trace variation by 57\%, the transistor count by 2\times, the switching power by 26\% and the leakage by 8\times against CMOS XOR/XNOR. In addition, when compared to a standalone CMOS XOR, using the TIGFET XOR/XNOR circuit can reduce the power trace variation by 81\% and the leakage by 6.7\times for the same transistor count and switching power.

V. CONCLUSION

In this paper, we investigated the benefits of using TIGFET technology in term of hardware security. We showed that TIGFET can reduce the power trace variation when compared to CMOS, making TIGFET-based designs more robust against

---

(a) Transient curves of CMOS XOR/XNOR for different input combinations and \( I_{\text{supply}} \) evaluation methodology; Simulation setup schematics of: (b) CMOS XOR/XNOR and (c) TIGFET XOR/XNOR.

![Fig. 8](image-url)

### TABLE I: \( I_{\text{supply}} \) current values comparison between CMOS XOR/XNOR and symmetrical TIGFET XOR/XNOR, for different input combinations.

<table>
<thead>
<tr>
<th>AB</th>
<th>out</th>
<th>( I_{\text{supply}} ) CMOS (( \mu \text{A} ))</th>
<th>( I_{\text{supply}} ) TIGFET (( \mu \text{A} ))</th>
</tr>
</thead>
<tbody>
<tr>
<td>00 → 01</td>
<td>0 → 1</td>
<td>-76.361</td>
<td>-26.571</td>
</tr>
<tr>
<td>01 → 1</td>
<td>1 → 0</td>
<td>-76.392</td>
<td>-29.047</td>
</tr>
<tr>
<td>11 → 0</td>
<td>0 → 1</td>
<td>-92.779</td>
<td>-28.400</td>
</tr>
<tr>
<td>00 → 0</td>
<td>0 → 1</td>
<td>-92.957</td>
<td>-29.703</td>
</tr>
<tr>
<td>00 → 1</td>
<td>0 → 1</td>
<td>-72.760</td>
<td>-28.881</td>
</tr>
<tr>
<td>01 → 1</td>
<td>1 → 0</td>
<td>-82.251</td>
<td>-26.605</td>
</tr>
<tr>
<td>11 → 0</td>
<td>0 → 1</td>
<td>-92.670</td>
<td>-29.861</td>
</tr>
<tr>
<td>01 → 0</td>
<td>1 → 0</td>
<td>-92.698</td>
<td>-28.275</td>
</tr>
</tbody>
</table>

\( \min (I_{\text{supply}}) \) (\( \mu \text{A} \)) = -92.957 \( \mu \text{A} \) \( \max (I_{\text{supply}}) \) (\( \mu \text{A} \)) = -72.760 \( \mu \text{A} \)

\( \text{V} \text{ariation} \) (\%): 28\% 12\%

(1) The red logical value denotes which input is switching.
TABLE II : Switching power, power trace variation, transistor count and leakage for the different circuits.

<table>
<thead>
<tr>
<th>Design</th>
<th>Switching Power (µW)</th>
<th>Power Trace Variation (%)</th>
<th>Transistor Count</th>
<th>Leakage (nW)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMOS XOR</td>
<td>9.192</td>
<td>64</td>
<td>8</td>
<td>5.738</td>
</tr>
<tr>
<td>CMOS XOR/XNOR</td>
<td>12.611</td>
<td>28</td>
<td>16</td>
<td>6.918</td>
</tr>
<tr>
<td>TIGFET XOR</td>
<td>6.604</td>
<td>75</td>
<td>4</td>
<td>0.594</td>
</tr>
<tr>
<td>TIGFET XOR/XNOR</td>
<td>9.299</td>
<td>12</td>
<td>8</td>
<td>0.854</td>
</tr>
</tbody>
</table>

DPAs attacks. In particular, we showed that when using the complementary gate technique with XOR and XNOR gates, TIGFET circuits can reduce the power trace variation by 57%, the transistor count by 2×, the switching power by 26% and the leakage by 8× against CMOS. When compared to a standalone CMOS XOR, using the TIGFET XOR/XNOR circuit can reduce the power trace variation by up to 81% and the leakage power by 6.7× for the same transistor count and a similar switching power. This work shows that emerging technology such as TIGFET can bring novel advantages beyond traditional power and area performances when compared to regular CMOS, here as improved hardware security features.

ACKNOWLEDGMENTS

This work was supported by the NSF Career Award number 1751064, the IMEC core partners’ CMOS program and the SRC Contract 2018-IN-2834. The authors would like to acknowledge Michael Niemer and Sharon Hu from The University of Notre Dame for the fruitful discussion.

REFERENCES