True-PolyTronik: Securing Circuits Against Laser Logic State Imaging Attack Using RFET

Sajjad Parvin[ᗐ], Chandan Kumar Jha[ᗐ], Frank Sill Torres[‡], and Rolf Drechsler[ᗐ,†]
[ᗐ] Institute of Computer Science, University of Bremen, Germany
[†] Cyber-Physical Systems, DFKI GmbH, Germany
[‡] Institute for the Protection of Maritime Infrastructures, German Aerospace Center, Germany
{parvin, chajha, drechsler}@uni-bremen.de, frank.silltorres@dlr.de

***Abstract*—It has been shown that an adversary equipped with *Optical Probing* (OP) capabilities can modulate the power supply of a design with a low frequency and low amplitude signal, and extract the static state of transistors in a design. This OP technique, known as *Laser Logic State Imaging* (LLSI), has been successfully exploited to extract the data in SRAM blocks, combinational circuits, and more. Several mitigation techniques exist against LLSI attacks, however, they are often power-hungry, require large amplitude modulation of the power supply to function effectively, or necessitate the inclusion of a laser light sensor detection on the chip, making them costly solutions. Additionally, other techniques require a change in the transistor fabrication steps, making them costly to integrate into the CMOS fabrication process. In this work, we explore *Reconfigurable Field Effect Transistor* (RFET) technology, which can be reconfigured at runtime to function as either a PMOS or NMOS transistor to mitigate LLSI attacks on chips. Additionally, the RFET technology is compatible with CMOS fabrication and it has been shown to integrate seamlessly into existing CMOS technology. We demonstrate that with the aid of RFET technology, we can design effective logic cells capable of detecting even small power supply modulation which is a prerequisite for LLSI attack. This enables us to configure logic cells in a manner that corrupts their static state upon LLSI attack. We implement this mitigation technique against LLSI attacks by biasing the program pins of RFET-based logic cells such that, when the supply voltage drops, the logic cell alters its original intended behavior and generates gibberish data. We demonstrate our approach on several combinational logic cells and D-latch cells. Next, we propose an RFET-based biasing circuitry design that produces stable voltage for the program pins of RFETs, upon LLSI attack on the chip. Finally, we also evaluate the performance of our approach by comparing the logic cells when they are protected using our proposed technique versus when they are unprotected.**

***Keywords*—Reconfigurable Field Effect Transistor, emerging technologies, LLSI, Optical Probing, Contactless Probing.**

I. Introduction

As Moore's law reaches its limit, new devices emerge to push the boundaries of packing more functionality and computational power to computer chips [1]–[3]. One such emerging and promising device is *Reconfigurable Field Effect Transistor* (RFET), where the transistor can be configured on the fly to operate as N-type or P-type transistors [1]. The reconfigurability of RFETs allows the designing of multifunctional logic circuits that can be configured at runtime [2]. Therefore, due to the reconfigurability of RFET-based designs, they substantially occupy a lower area in comparison to the traditional CMOS-based designs [1], [2]. Many works in the literature have explored area-efficient logic cell design based on RFET technology [1]–[3].

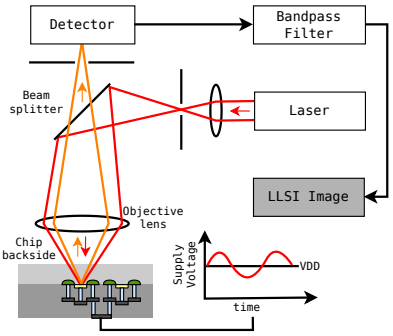


Fig. 1: LLSI setup schematic

Another, less explored application of RFET-based design is in the development of secure *Integrated Circuits* (ICs) [9]–[11]. The RFET-based designs are explored to prevent power *Side-Channel Analysis* (SCA) attack by exploiting reconfigurability and adding randomness to the power trace of the design [9], designing reconfigurable and delay-invariant logic cells to prevent delay SCA attacks by masking the delay trace of the reconfigurable logic cell, etc. Additionally, RFET-based designs are also explored for efficient and robust logic-locking schemes to secure ICs with a much lower area than the traditional CMOS-based logic locking schemes, watermarking the ICs, layout camouflaging [11], etc. Thus, the reconfigurability of RFET-based designs makes them ideal for security-critical applications. Hence, in this work, we explore the applicability of RFET in designing secure ICs against novel attacks.

Recently, a novel non-invasive laser-assisted SCA-based attack, namely *Optical Probing* (OP) attack is shown effective in retrieving chips stored/processed information [12], especially an extension of OP attack that can probe the static state of transistors in a design which is called *Laser Logic State Imaging* (LLSI) attack [13], [14]. For an LLSI attack, an adversary freezes the clock at the desired time step and lowers the nominal supply voltage (V_{dd}). Next, the adversary modulates the V_{dd} with a sinusoidal signal which has an amplitude, and a frequency of 100 mV, and 100 kHz, respectively. Then, using a *Near-InfraRed* (NIR) laser, probe the backside of the IC to retrieve the static state of each transistor in the design.

In this work, we utilize RFET-based designs, to mitigate the above-mentioned LLSI attack. We explored an approach where when the voltage drops only by 100 mV in the supply voltage, the RFET-based logic cells disrupt their previous functionality

TABLE I: Comparison of various LLSI mitigation techniques

LLSI Attack Countermeasure	CFS	C	FC
Nanopyramid [4]	✓	€€€	Not compatible with CMOS technology fabrication
Backside Protection [5]	✓	€€	Security measures can be bypassed by disabling sensor unit
TOPRC [6]	✗	€	Redesign of logic cells' layout is required
Twofold [7]	✗	€€	High area cost for clock and voltage sensor
Self-Destructive Logic Cell [8]	✗	€	Requires significant drop in supply voltage to function properly
True-Polytronik	✗	€	RFET is compatible with CMOS fabrication technology, inherently provides reconfigurability, low area solution

CFS: change in fabrication step, **C**: Cost, **FC**: further comment, **€**: relative price

and erase the previously computed data.

The contributions of this work are as follows:

- Investigating RFET-based designs as a mitigation technique against LLSI attack
- Thorough investigation of several RFET-based combinational and sequential logic cells against LLSI attack
- Investigating a biasing circuitry that generates stable program pin voltage despite supply voltage drops
- Evaluate the performance of our proposed protected against unprotected RFET-based logic cells

II. Related Works

Several countermeasures against the LLSI attack are implemented at the circuit and technology levels. At the technology level, researchers have demonstrated that modifying the fabrication process of CMOS transistors and introducing nanopyramid structures into the transistors' channel can scramble the incoming OP laser light, thereby preventing such attacks [4]. Introducing nanopyramid structures to scramble the incoming laser light is novel, yet it remains a costly solution for many applications. Another technology-level solution involves coating the backside of the chip with an opaque material and using an on-chip light emitter and sensor to detect the removal of the opaque layer [5]. An adversary can bypass this method by removing the opaque layer and disabling the sensor unit.
At the circuit level, several LLSI mitigation techniques have been investigated which are sensor-based solutions. In [7], a twofold clock and voltage-based detection method are proposed to counteract LLSI attacks on a chip, specifically when an adversary freezes the clock and reduces the supply voltage. This twofold technique is costly to implement, in terms of occupied area on chip. In [8], a self-destructive polymorphic logic cell is proposed which is based on CMOS. This CMOS-based polymorphic logic cell changes its behavior based on the level of supply voltage applied to the logic cell. However, for the proposed CMOS-based polymorphic logic cells, the supply voltage must drop to half of the nominal supply voltage to change their functionality, and then it can thwart the LLSI attack [8]. Another mitigation technique at the layout level is to design differential logic cells and keep the regions of the layout that carry complementary signals juxtaposed [6]. By juxtaposing regions carrying complementary signals, due to the limited resolution of OP setup, an attacker cannot probe the state of transistors. In Table I, we compared available LLSI mitigation techniques against our work.

III. Preliminaries & Background

A. Optical Probing Methodology

OP employs *Laser Scanning microscope* (LSM), in which a focused laser beam is controlled via galvanometric mirrors or statically pointed at a single point on a chip. At the same time, a detector collects the reflected light (see Fig. 1). Since silicon is limpid to light in the *NIR* spectrum, performing OP on an IC through its backside is possible without thinning or preparation of the chip. As shown in Fig. 1 the laser light focused on a region of the die area of IC passes the bulk silicon and travels through the active areas of transistors. A portion of incident light is reflected, for instance, when the incident light hits the first metal layer, then it travels back through the silicon into the microscope lens. Afterward, the beam splitter directs the reflected light to an optical detector, which converts its intensity into a voltage. Based on the voltage present at each terminal of a transistor, more or less scattering of incident light occurs, as shown in Fig. 1. This is because of the modulated electrical field inside the transistor upon applying a voltage to the transistor's terminals and creating more surface that the light can scatter from [15].

B. Optical Probing for Data Extraction

Voltage differences applied to a transistor can be detected using *Electro-Optical Probing* (EOP), enabling the extraction of data processed on an IC by parking the laser at one spot of the design. To identify paths carrying periodic signals, *Electro-Optical Frequency Mapping* (EOFM) scans the chip, producing a gray-scale image where bright spots indicate areas with switching activity, which can then be probed using EOP. An extension to EOFM, called LLSI, allows even the extraction of static logic states by modulating the power supply of the device by a signal of 100mV with the frequency of 100KHz [13]. By modulating the power supply with low amplitude, and low-frequency sinusoidal signal, upon freezing the clock at the desired clock signal, an adversary can retrieve the static state of each transistor in the design, because the sinusoidal is imposed on the active region of the transistor. As a result, the adversary can scan the laser over the area of interest, filter the reflected light at the detector according to the modulated signal's frequency, and thereby retrieve the state of each transistor in the design.

C. RFET

RFETs are a type of transistor that can be configured as either a PMOS or an NMOS on the fly [1], [16]. One type of RFET is called *Three-Independent-Gate Field-Effect Transistor* (TIGFET) which is shown in Figure 2. The IV curve

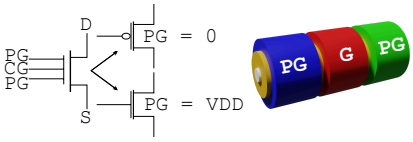


Fig. 2: TIGFET structure

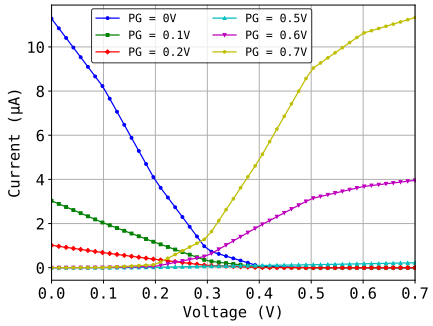


Fig. 3: IV Curve of TIGFET for various program pin voltages

of TIGFET is shown in Figure 3 for various applied voltages to the *PG* pin of TIGFET. It can be seen that from Figure 3 when the applied voltage at *PG* pins exceeds 300 mV, the TIGFET switches its behavior from a P-type transistor to an N-type transistor. This reconfigurability nature of the RFETs in the runtime makes them attractive for designing dense circuits, i.e. RFET-based logic cell has less number of transistors and can be configured to compute multiple functions on the fly [2], and for security applications due to their configurable nature [11].

IV. True-PolyTronik Flow

The premise of *True-PolyTronik* is to design circuits using RFETs that leverage their reconfigurability for designing secure ICs against LLSI attack. In *True-PolyTronik* methodology, upon detecting a drop in supply voltage—a prerequisite for LLSI attack— *True-PolyTronik* actively corrupts the data to safeguard the static state of logic cells. The conventional flow of the LLSI attack is shown in Figure 4, where an adversary freezes the clock, and modulates the power supply of an unprotected chip, and then by performing the OP attack through backside the chip which leads to retrieving the sensitive information on the chip. However, in the case of *True-PolyTronik* chips, if an adversary lowers and modulates the power supply, it triggers the RFET-based logic cells to corrupt their stored information as shown in Figure 4. *True-PolyTronik* takes advantage of controlling and biasing the program pin of RFET (the *PG* pin, as shown in Figure 2), such that when a voltage drop due to an LLSI attack is detected, the RFET-based logic cell design changes its functionality and overwrites the previously computed data. As a result, the adversary after probing the chip using the laser through its backside retrieves gibberish data from the *True-PolyTronik* chip. Based on the latter description, we designed and evaluated the functionality of *True-PolyTronik* RFET-based INV, NAND/NOR2, *Full Adder* (FA), D-latch in terms of data corruption capabilities. In addition, we utilize a reference voltage generator circuit to bias the RFET-based logic cell designs, to provide stable program pin biasing even under supply voltage drop, and allow the RFET-based logic cell designs to corrupt their previous data.

TABLE II: Truth table for the polytronic TIGFET-based INV logic cell, detailing its behavior in both normal operation and attack mode

In	Normal	Under Attack
	Out	Out
0	1	0
1	0	0

V. Experimental Result

In this section, we discuss the experimental results of *True-PolyTronik* logic cells. The simulations are done using TIGFET model [16] in Cadence Virtuoso. The nominal supply voltage of TIGFET is 700 mV. All the results are obtained on a machine with Intel Xeon E3-1240 V2 which runs at 3.4 GHz, and 32 GB of memory.

A. INV

Figure 5a shows the schematic of RFET-based INV logic cell. In Figure 5a, P_u and P_d refer to the program pin of RFET for *Pull-Up Network* (PUN) and *Pull-Down Network* (PDN), respectively. In order to find the proper bias voltage for P_u and P_d that results in the corruption of computed output upon supply voltage drop of 100 mV, we performed a parametric analysis on the P_u and P_d bias voltages under both nominal and attack mode conditions (supply voltage drops to 600 mV). In our parametric analysis, the RFET-based INV logic cell corrupts its functionality when the supply voltage drops 100 mV below the nominal value, when the P_u and P_d are set to 360 mV, and 480 mV, respectively. The truth table for both normal operation, and under LLSI attack of the INV logic cell is shown in Table II. The outputs that differ between the attack mode and normal operation are highlighted in Table II. Additionally, the output waveform for both normal operation and under LLSI attack of the INV logic cell is shown in Figure 6a and Figure 6b, respectively. The red vertical line used in Figure 6a and Figure 6b demonstrate the time that input switches its value. We can see that when the attack is mounted the output stays at 0 irrespective of the input.

B. NAND2/NOR2

Figure 5b shows the schematic of the RFET-based NAND2/NOR2 logic cell which can be configured to be both NAND2 or NOR2 based on the applied program voltage to the program pin (*P*) [17]. RFET-based NAND2/NOR2 logic cell's program pin (*P*, and the inverted version of this signal P_b) is controlled by an INV logic cell to configure the NAND2/NOR2 logic cell's functionality. Since we do not have direct access to these pins, we try to achieve data corruption of this logic cell through the biasing program pin of the INV logic cell at a point that upon supply voltage drop alters the functionality of this NAND2/NOR2 logic cell. To determine the appropriate bias voltages for P_u, and P_d for the INV logic cell that generates program signal for the

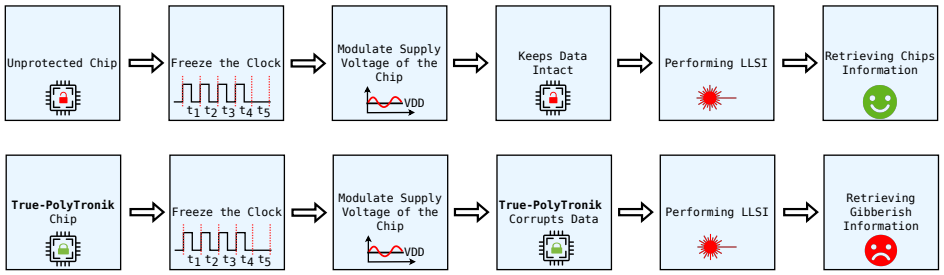
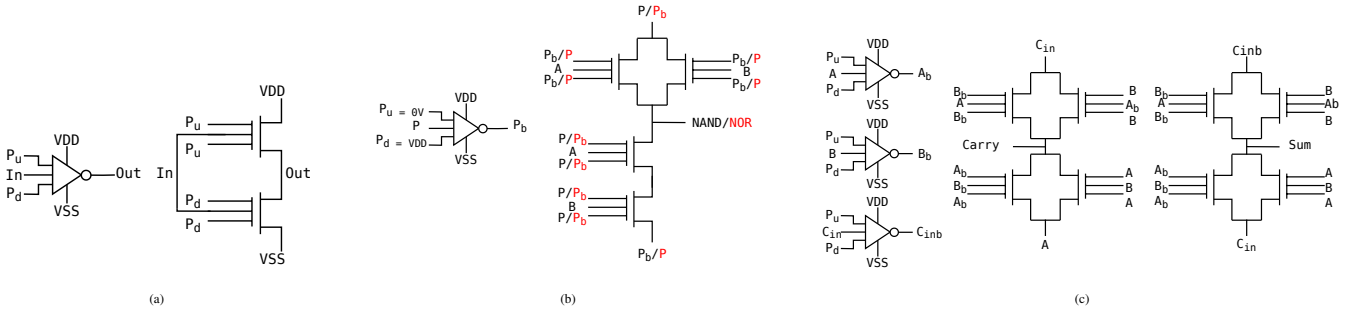
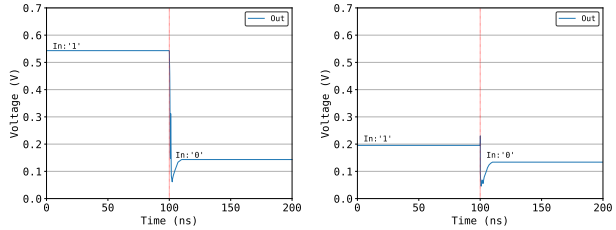


Fig. 4: LLSI attack flow for both unprotected chips and True-PolyTronik-based chips



(a) (b) (c)

Fig. 5: a) schematic of TIGFET-based INV logic cell b) schematic of TIGFET-based reconfigurable NAND2/NOR2 logic cell c) schematic of TIGFET-based FA



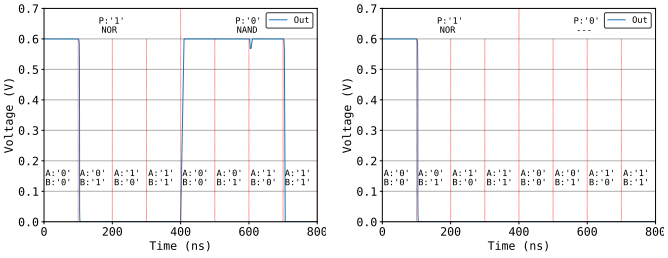
(a) Supply voltage at 700 mV (b) Supply voltage at 600 mV

Fig. 6: TIGFET-based INV logic cell's output waveform when supply voltage drops from 700 mV to 600 mV

NAND2/NOR2 logic cell that leads to the corruption of the computed output, we conducted a parametric analysis of the P_u, and P_d bias voltages under both nominal and attack mode conditions. In our parametric analysis, the RFET-based INV logic cell, which configures the NAND2/NOR2 logic cell, corrupts its output when the supply voltage drops 100 mV below the nominal value with P_u and P_d set to 360 mV and 480 mV, respectively. The truth table for both normal operation, and under LLSI attack of the NAND2/NOR2 logic cell is shown in Table III. The outputs that differ between the attack mode and normal operation are highlighted in Table III. Additionally, the waveform for both nominal operation and under LLSI attack mode of the NAND2/NOR2 logic cell is shown in Figure 7a, and Figure 7b, respectively. The vertical red line used in Figure 7a, and Figure 7b demonstrate the time that input switches input value. Figure 7b demonstrates that for under attack mode, NAND2/NOR2 logic cell works correctly as a NOR2 logic cell, while NAND2 functionality of this reconfigurable logic cell is corrupted. For this simulation, we used a signal with a period of 100 ns, and we computed the NAND2/NOR2 logic cell's output for all possible input combinations for both nominal and under LLSI attack mode.

TABLE III: Truth table for the polytronic TIGFET-based NAND2/NOR2 logic cell, detailing its behavior in both normal operation and attack mode

A	B	Normal		Under Attack	
		P = VSS	P = VDD	P = VSS	P = VDD
		NAND2	NOR2	NAND2	NOR2
0	0	1	1	0	1
0	1	1	0	0	0
1	0	1	0	0	0
1	1	0	0	0	0



(a) NAND2/NOR2 normal operation (b) NAND2/NOR2 under LLSI attack

Fig. 7: TIGFET-based NAND2/NOR2 output waveform when supply voltage drops from 700 mV to 600 mV.

C. FA

Figure 5c shows the schematic of an RFET-based FA logic cell which utilizes only 8 RFETs [3]. Since we do not have direct access to the program pins of RFET-based FA, we try to achieve data corruption of this logic cell through the biasing program pin of the INV logic cell which generates the inverted version of the input signals. To identify the correct bias voltages for P_u and P_d that result in output corruption, we analyzed the P_u and P_d bias voltages in both normal and under LLSI attack modes. In our parametric analysis, the RFET-based INV logic cell that generates the inverted version of the input signal which is required for the RFET-based FA circuit corrupts the functionality of the FA logic cell's output when the supply voltage drops 100 mV below

TABLE IV: Truth table for the polytronic TIGFET-based FA logic cell, detailing its behavior in both normal operation and attack mode

A	B	Cin	Normal		Under Attack	
			Sum	Carry	Sum	Carry
0	**0**	**0**	0	0	0	0
0	**0**	**1**	1	0	1	1
0	**1**	**0**	1	0	0	0
0	**1**	**1**	0	1	0	1
1	**0**	**0**	1	0	0	1
1	**0**	**1**	0	1	1	1
1	**1**	**0**	0	1	0	1
1	**1**	**1**	1	1	1	1

the nominal value, when the P_u and P_d are set to 360 mV, and 480 mV, respectively. The truth table for both normal operation, and under LLSI attack of the FA logic cell is presented in Table IV. The outputs that differ between the attack mode and normal operation are highlighted in Table IV. We could not generate the output waveform of the FA for all the possible input combinations due to the convergence problems associated with the used TIGFET model. Hence, we performed transient simulation for all the input combinations separately in both nominal and under LLSI attack mode, as shown in Table IV.

D. D-Latch

Figure 8 shows the schematic of the RFET-based transmission gate-based D-latch logic cell [18]. The D-latch is based on a CMOS circuit that, we converted into RFET-based D-latch. In order to achieve data corruption of this logic cell, we bias the program pin of both INV logic cells in the loop which acts as a memory element, as shown in Figure 8. We analyzed the bias voltages for P_u and P_d both normal and under attack conditions to determine the settings that would corrupt the computed output. In our parametric analysis, the RFET-based INV logic cell that generates the inverted version of the input signal which is required for the RFET-based D-latch circuit corrupts the functionality of the D-latch logic cell's output when the supply voltage drops 100 mV below its nominal value, when the P_u and P_d are set to 360 mV, and 480 mV, respectively. The truth table for both normal operation, and under LLSI attack of the D-latch logic cell is presented in Table V. The outputs that differ between the attack mode and normal operation are highlighted in Table V. For D-latch, we first activated the clock, and let the D-latch sample the input signal (D), and after 230 ns operating at nominal supply voltage, we dropped the supply voltage from nominal to 600 mV. The results are shown in Figure 9a, and Figure 9b for the case when the D-latch stores logic '0' and '1', respectively. The red dotted lines in Figure 9a and Figure 9b indicate the moment the supply voltage was dropped from nominal 700 mV to under LLSI attack mode at 600 mV. According to Figure 9a, and Figure 9b when the D-latch is under attack mode, it always outputs logic '0' which is similar to the case when we reset the D-latch.

E. RFET Program Pin Biasing Circuitry

To ensure the self-destructive behavior of RFET-based logic cell designs investigated in previous sections, the program

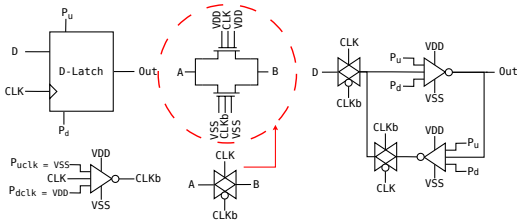


Fig. 8: Schematic of TIGFET-based transmission-based D-Latch

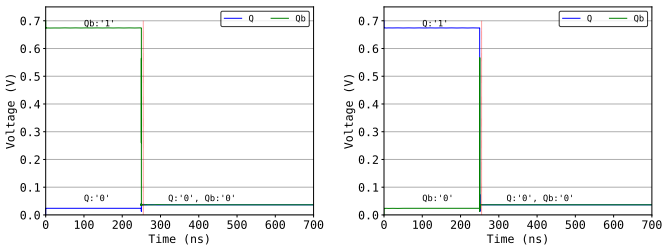
TABLE V: Truth table for the polytronic TIGFET-based D-latch logic cell, detailing its behavior in both normal operation and attack mode

CLK	D	Normal		Under Attack	
		Q	Qb	Q	Qb
0	0	Q'	Qb'	0	0
0	1	Q'	Qb'	0	0
1	0	0	1	0	0
1	1	1	0	1	0

pins of the RFET must be biased at a voltage that remains stable or undergoes only minimal change, even when the supply voltage level drops. To generate such a bias voltage, one potential candidate circuitry is voltage reference circuits, as shown in Figure 10. An ideal reference voltage operates independent of process variation, change in supply voltage, and temperature [19]. For the voltage reference circuit shown in Figure 10, we biased the pins P_u and P_d at 0 V, and 700 mV, respectively. This enables the voltage reference circuit shown in Figure 10 to act as a MOSFET-only reference voltage circuit [19]. Since the current of both transistors is equal as shown in Figure 10, we can write the output of the voltage reference circuit as follows:

$$V_{ref} = \frac{V_{dd} - V_{TH_u} + \sqrt{\frac{\beta_d}{\beta_u}} \times V_{TH_d}}{\sqrt{\frac{\beta_d}{\beta_u}} + 1} \tag{1}$$

where β, V_{TH}, and V_{dd} refer to the transistor's fabrication parameters, threshold voltage, and supply voltage, respectively. Hence, we can generate the reference voltage by changing the transistor's fabrication parameters such as sizing of the transistors. Table VI reports the reference voltage generated by the circuit shown in Figure 10 for various sizing of TIGFET (n is the number of nanowires for the TIGFET). We can see that upon supply voltage dropping the generated reference voltage



(a) D-latch storing 0

(b) D-latch storing 1

Fig. 9: TIGFET-based D-latch waveform when supply voltage drops from 700 mV to 600 mV for both cases where the D-latch stores logic "0", and logic "1".

TABLE VI: Reference voltage generation for various sizing of transistors

V_ref Output (mV)		N_u														
		1			25			50			75			100		
		V_{dd}: 0.7 V	V_{dd}: 0.6 V	ΔV	V_{dd}: 0.7 V	V_{dd}: 0.6 V	ΔV	V_{dd}: 0.7 V	V_{dd}: 0.6 V	ΔV	V_{dd}: 0.7 V	V_{dd}: 0.6 V	ΔV	V_{dd}: 0.7 V	V_{dd}: 0.6 V	ΔV
N_d	**1**	284.5	230.4	19%	388.4	232.0	40%	407.8	344.4	16%	418.9	354.8	15%	425.0	364.0	14%
	25	200.0	143.1	28%	284.5	230.4	19%	305.9	246.4	19%	318.0	256.2	19%	326.0	264.3	19%
	50	166.9	122.8	26%	261.4	216.7	17%	284.5	230.4	19%	296.9	240.1	19%	305.9	246.4	19%
	75	150.4	114.6	24%	247.6	209.7	15%	273.6	221.9	19%	284.5	230.4	19%	296.9	237.8	20%
	100	140.6	108.9	23%	239.4	204.8	14%	261.3	216.7	17%	273.6	223.6	18%	284.5	230.4	19%

ΔV: change in reference voltage after supply voltage drop from nominal value

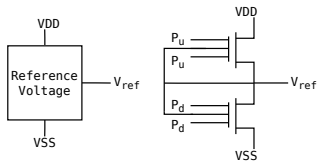


Fig. 10: Schematic of reference voltage circuit using only TIGFETs

changes on average 19 % of reference voltage generated when operating at nominal supply voltage.

VI. Performance Evaluation & Discussion

In this study, we evaluated the effectiveness of protecting RFET-based logic cells by biasing their program pins at a level where a 100 mV drop in supply voltage can corrupt the previously computed value. To evaluate the performance of our mitigation technique against LLSI attack, we analyze the performance of the self-destructive RFET-based INV logic cell described in Section V-A, and compare it with a traditional INV logic cell. For our comparison, we utilize a fan-out of 4 INV logic cells in simulation. For the conventional and unprotected INV logic cell, when operating at 700 mV supply voltage with an input signal of period 100 ns, it exhibits a power consumption of 19.18 pW and a delay of 1.3 ns. However, for the protected RFET-based INV logic cell (top transistor biased at 360 mV, bottom transistor biased at 480 mV), the performance is significantly affected, with the power consumption increasing to 128.52 pW, and the delay extending to 68 ns.

The performance drop of our self-destructive RFET-based logic cell design is significant, however, this scheme can be used to protect selective logic cells in a design. Since, in a large design upon LLSI attack, the RFET-based protected logic cells are connected to unprotected logic cells, hence the corrupted data from RFET-based logic cells will propagate to the unprotected logic cells. Consequently, the data of the unprotected logic cells will be corrupted without the need to protect all the logic cells in the design using RFET-based logic cells which have significantly higher power, and delay penalty. Hence, selectively replacing unprotected logic cells with our proposed RFET-baed logic cells can still thwart the LLSI attack, and keep the overall power and performance penalty at a negligible level.

VII. Conclusion

In this work, we explored RFET-based logic cell design as a mitigation technique against one extension of OP attack, namely the LLSI attack. We demonstrated that logic cells designed with RFETs can corrupt the computed data when an adversary modulates the power supply rail of a chip, a prerequisite for an LLSI attack. These RFET-based logic cells achieve this self-destructive behavior by reconfiguring themselves into different logic cells upon power supply rail modulation. We designed several self-destructive RFET-based logic cells, including an INV, FA, NAND2/NOR2, and D-latch logic cells, and evaluated their effectiveness against LLSI attacks. We also provided a bias circuitry for biasing the program pins of RFETs, which provides a robust voltage even when the supply voltage drops. As of our future work, we will investigate RFET-based logic cell designs that are more efficient in terms of performance and power consumption.

Acknowledgment

The work described in this paper has been supported by the Deutsche Forschungsgemeinschaft (DFG – German Research Foundation) under the priority programme SPP 2253 – 439918011 in project DR 287/38-1 and SPP 2253 - 535696594 in project DR 287/43-1.

References

[1] T. Mikolajick *et al.*, "The rfet—a reconfigurable nanowire transistor and its application to novel electronic circuits and systems," *SST*, 2017.
[2] S. Rai *et al.*, "Designing efficient circuits based on runtime-reconfigurable field-effect transistors," *TVLSI*, 2019.
[3] S. Parvin *et al.*, "Hidden cost of circuit design with rfets," in *DATE*, 2024.
[4] H. Shen *et al.*, "Nanopyramid: An Optical Scrambler Against Backside Probing Attacks," in *ISTFA*, 2018.
[5] E. Amini *et al.*, "Assessment of a chip backside protection," in *JHSS*, 2018.
[6] S. Parvin *et al.*, "Toward optical probing resistant circuits: A comparison of logic styles and circuit design techniques," in *ASP-DAC*, 2022.
[7] T. Farheen *et al.*, "A twofold clock and voltage-based detection method for laser logic state imaging attack," *TVLSI*, 2022.
[8] A. Cannon *et al.*, "Protection against physical attacks through self-destructive polymorphic latch," in *ICCAD*, 2023.
[9] N. Kavand *et al.*, "Redcap: Reconfigurable rfet-based circuits against power side-channel attacks," in *DATE*, 2024.
[10] G. Galderisi *et al.*, "Robust reconfigurable field effect transistors process route enabling multi-v t devices fabrication for hardware security applications," in *DRC*, 2022.
[11] N. Kavand *et al.*, "Securing hardware through reconfigurable nanostructures," in *ICCAD*, 2022.
[12] S. Tajik *et al.*, "On the power of optical contactless probing: Attacking bitstream encryption of FPGAs," in *CCS*, 2017.
[13] B. Niu *et al.*, "Laser Logic State Imaging (LLSI)," in *ISTFA*, 2014.
[14] T. Krachenfels *et al.*, "Automatic extraction of secrets from the transistor jungle using laser-assisted side-channel attacks," in *USENIX*, 2021.
[15] U. Kindereit, "Investigation of laser-beam modulations induced by the operation of electronic devices," Doctoral Thesis, Technische Universität Berlin, Fakultät IV - Elektrotechnik und Informatik, Berlin, 2009.
[16] G. Gore *et al.*, "A predictive process design kit for three-independent-gate field-effect transistors," in *VLSI-SoC)*, 2019.
[17] G. Galderisi *et al.*, "Reconfigurable field effect transistors design solutions for delay-invariant logic gates," *ESL*, 2022.
[18] N. Weste and D. Harris, *CMOS VLSI Design: A Circuits and Systems Perspective*, 4th ed. USA: Addison-Wesley Publishing Company, 2010.
[19] R. J. Baker, *CMOS: circuit design, layout, and simulation*. John Wiley & Sons, 2019.