Securing Hardware through Reconfigurable Nano-structures

(Invited Paper)

Nima Kavand*, Armin Darjani*, Shubham Rai, Akash Kumar
Chair of Processor Design, TU Dresden, Germany
{nima.kavand, armin.darjani, shubham.rai, akash.kumar}@tu-dresden.de
*Both authors contributed equally to this research.

ABSTRACT

Hardware security has been an ever-growing concern of the integrated circuit (IC) designers. Through different stages in the IC design and life cycle, an adversary can extract sensitive design information and private data stored in the circuit using logical, physical, and structural weaknesses. Besides, in recent times, ML-based attacks have become the new de facto standard in hardware security community. Contemporary defense strategies are often facing unforeseen challenges to cope up with these attack schemes. Additionally, the high overhead of the CMOS-based secure add-on circuitry and intrinsic limitations of these devices indicate the need for new nano-electronics. Emerging reconfigurable devices like Reconfigurable Field Effect transistors (RFETs) provide unique features to fortify the design against various threats at different stages in the IC design and life cycle. In this manuscript, we investigate the applications of the RFETs for securing the design against traditional and machine learning (ML)-based intellectual property (IP) piracy techniques and side-channel attacks (SCAs).

KEYWORDS

HW Security, Reconigurable Nano-structures, RFET, IP Protection, Side-channel Attacks

ACM Reference Format:
Nima Kavand*, Armin Darjani*, Shubham Rai, Akash Kumar. 2022. Securing Hardware through Reconfigurable Nano-structures: *(Invited Paper).* In *IEEE/ACM International Conference on Computer-Aided Design (ICCAD '22), October 30-November 3, 2022, San Diego, CA, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3508352.3561116

1 INTRODUCTION

Hardware security is a new metric that hardware designers should consider, along with the circuit's area, power, performance, and cost. In hardware security both the sensitive data and the design itself should be preserved against various threats. This information can be leaked at different stages in the life-cycle of a circuit from manufacturing phase to end user usage.

In recent years, there has been a rapid increase in the use of highly interconnected computing devices in many applications, including credit card scanners, smartphones, and autonomous vehicles. These devices generally deal with sensitive data like passwords and personal information. Cryptography algorithms such as Advances Encryption Standard (AES) are mainly used to encode these data and preserve their integrity and confidentiality against unauthorized access. However, these algorithms may leak secret information due to the vulnerabilities of the underlying hardware to SCAs. SCAs are a class of attacks in which the attacker tries to extract sensitive data like the secret encryption key or the circuit function by analyzing the physical behavior of hardware like power, delay, or electromagnetic radiation [27].

From the first time that Kocher [18] introduced these attacks, many complex countermeasures like masking the intermediate logic transitions or balancing the circuit's power consumption under different inputs have been proposed [40]. However, SCA still remains threatening because of the high overheads of the countermeasures or other limitations in traditional CMOS-based design.

Beside leaking of the sensitive information, the design itself is prone to attacks. Today, IP piracy is one of the biggest challenges for hardware design vendors. The term "IP piracy" refers to the illegal usage of hardware intellectual properties without the permission of the true owner. The main goal of the malicious entities here can range from reverse engineering the IP to illegal usage of the IP through overproducing. The ever-growing complexity of the IC has steeply increased the cost of IC manufacturing which propelled companies to go fabless over the years. As a result, the different parts of the IC manufacturing flow may be carried out by various entities from different regions of the globe. This outsourcing and globalization have brought so many perils regarding the integrity and confidentiality of IPs, resulting in the loss of several billions of dollars each year.

Adding protection units at the silicon layer seems inevitable for designers in order to safeguard the IP. For this purpose, many design-for-trust (DFT) techniques like layout camouflaging [38], split manufacturing [54], watermarking, and logic locking (LL) [39, 44] have been proposed. Split manufacturing and layout camouflaging protect the design against reverse engineering. Watermarking is a technique to prevent illegal usage of the IP. LL is the most holistic DFT technique that can stop both reverse engineering and illegal usage of the IC by locking the design. Each DFT technique has been subject to an everlasting cat-and-mouse game between the attackers and the defenders. Every new threat requires a more sophisticated countermeasure that would bring more overhead in terms of power, performance, and area or increase the cost of the circuit production based on the DFT technique. Moreover, advancements in ML have shifted the competition in favor of attackers. ML has introduced new tools that attackers can utilize to break protection add-on circuitries that were deemed to be unbreakable. These tools can detect traces of security add-ons by which the attackers can break or circumvent the security technique more straightforwardly than ever.

Considering the limitations of CMOS scaling and the lack of security-specific properties in CMOS technology, new radical solutions should be considered at the silicon layer to propel the

ICCAD '22, October 30-November 3, 2022, San Diego, CA, USA

ACM ISBN 978-1-4503-9217-4/22/10.
https://doi.org/10.1145/3508352.3561116

emerging threats with acceptable overheads in terms of performance, delay, and area. Intrinsic properties of reconfigurable nanotechnologies like RFETs and spintronics provide HW security designers with new tools that can compensate for shortcomings of CMOS technology. In this paper, we show that utilizing RFETs can result in more compact and sophisticated security add-ons that help the designers to shield the design to protect both IP and data at different levels of IC life cycle. The rest of the paper is organized as follows. In Section 2, we provide a brief background about RFETs. Section 3 investigates the benefits of RFET to provide SCA resilient HW. In Section 4 we discuss IP protection techniques against IP piracy. We show that utilizing RFETs can benefit the security designers for implementing various DFT techniques. Finally, Section 5 concludes the paper.

2 BACKGROUND

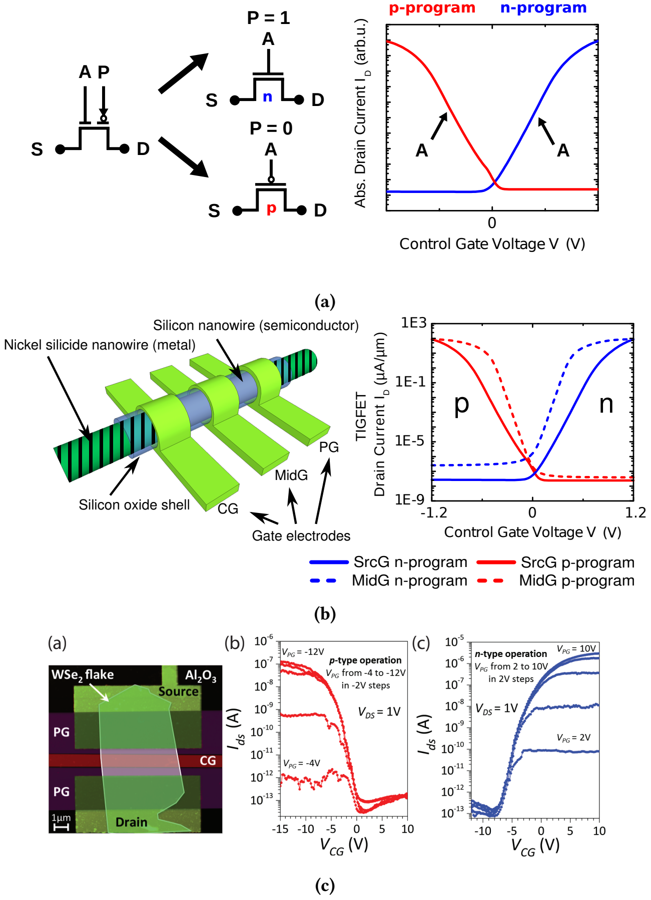
Recently, various emerging nanotechnology have been demonstrated that enable hardware security features by virtue of their exciting properties [37, 48, 35]. This manuscript focuses on RFETs, that allow the implementation of secure circuits due to their device-level reconfigurable properties.

In RFETs, individual devices exhibit electrical conduction for both types of charge carriers – electrons or holes, on the application of an external bias potential [13, 8]. Hence, a transistor can be tuned either as a p- or n-type device. This device-level reconfigurability is a manifestation of a physical phenomenon called *ambipolarity*. Ambipolarity refers to the movement of both types of charge carriers through the channel. Ambipolarity can be either due to chemical doping (via materials or impurities) or electrostatic doping (application of external potential to generate charge carriers) [23].

RFETs are characterized by two types of gate terminals – a program gate (PG) and a control gate (CG). The PG controls the type of charge carriers flowing through the channel to enable the device to function either as p- or n-type, while the CG controls the flow of charge carriers by allowing them to accumulate within the channel. This is shown in Figure 1a where the red and blue lines show the electrical symmetry in p- and n-type, respectively. One can notice how the value of P at PG determines the behavior of the device.

In terms of geometry of devices, RFETs can be realized with existing contemporary geometries in 1-dimension or 2-dimension. 1D devices are those that are realized using nanowire, nanoribbon or nanotube structures such as silicon nanowires (SiNW) [13, 8], germanium nanowires (GeNW) [51], graphene nanoribbons [12], carbon nanotubes FETs (CNTFETs) [19]. Figure 1b shows a 1D nanowire geometry demonstrating device-level reconfigurability [30]. Similarly, various 2D geometries (or planar geometry) have also been demonstrated made of channel materials such as silicon [43], graphene [24] or other Transition Metal Decalchogenide (TMD) materials such as $MoTe_2$ [25], WSe_2 [42]. WSe_2 device with reconfigurable properties are shown in Figure 1c.

Since RFETs are enabled mostly by channel materials such as silicon or germanium, their manufacturing process overlaps with contemporary CMOS technology [23]. Additionally, as shown above, RFETs can be realized by multiple parallel technologies and geometries, which make them a feasible technology to complement CMOS technologies to alleviate the issues of Moore's law [21, 22]. They have well-established EDA flows proposed in works like [29, 33]. More details about the physics of such technology and similarity to the fabrication process can be found in [23, 21].



(a)

(b)

(c)

Figure 1: (a) Representative figure of an RFET showing how it can be reconfigured to either as a p- or n-type device [30]. (b) 1D SiNW RFET with multi-independent gates [36]. (c) 2D WSe_2 RFET whose properties demonstrated in [42].

The device-level reconfigurability offered is beneficial in enabling bottom-up hardware security features for electronic circuits [31, 35, 45]. Various security features enabled by such technologies are described in the subsequent sections.

3 DATA SECURITY AGAINST SCA

Preserving data security is one of the most crucial aspects of HW security. There are various types of data theft attacks, such as microprobing and SCAs [11], in which attackers try to access sensitive information. The encryption algorithms are designed to scramble data and prevent unauthorized people from directly accessing confidential information. Although these algorithms are assumed to be secure mathematically, their careless implementation may make them vulnerable to SCAs. Data-dependent information leaked through side channels like power consumption and execution time can reveal the internal secrets of the cryptographic circuit. In this section, we describe the power SCAs and discuss the CMOS limitations and RFET benefits to provide countermeasures against them.

3.1 Power SCA

Power SCA is a physical attack that needs proximity to the victim HW [9]. This attack is based on the dependency between input data and circuit power consumption. In other words, power consumption relies on internal operations and signal transitions, which are highly related to the input data. The attacker can exploit dynamic and leakage power traces [16]; however, most of the works in the literature focus on dynamic power. A power SCA generally consists of two phases: Gathering power traces from the device and analyzing the traces using different methods to extract the secret information. Simple power analysis (SPA), differential power analysis (DPA), and correlation power analysis (CPA) are the most well-known classical power SCAs.

SPA tries to find the secret key from the raw power traces straightforwardly. Revealing the key of the RSA protocol by analyzing the temporal power trace of the device during the RSA exponentiation is an example of such attacks [26]. In DPA [17], the attacker guesses a part of the secret key (subkey) and calculates the intermediate result for different plaintexts. Then the power traces of the device are split into two subsets, P_0 and P_1, based on the value of a single bit of the guessed intermediate result. At last, the guessed subkey is assessed by differentiating the means of P_0 and P_1. Only a good guess of the subkey leads to a high difference between the two means. DPA is more complicated than SPA and requires more power traces. The adversary can perform a power attack more efficiently using CPA [5]. For this aim, he or she needs to assume a power leakage model like hamming weight or hamming distance. The correlation between the model and the actual power trace determines the accuracy of the guessed key.

As data-dependency of power consumption is the common point in the mentioned attacks, all the countermeasures aim to reduce this link. SCA countermeasures are divided into two categories: hiding and masking. In hiding, we want to decrease the Signal to Noise Ratio (SNR) of the leakage information to make the data extraction difficult. This can be achieved by making power consumption constant (signal reduction) or parallel execution of independent operations (noise addition) [27]. On the other hand, masking intends to make the power consumption not only depend on the input data but also on a random mask unknown to the attacker [20].

There are serious limitations in the CMOS-based design for thwarting power SCAs:

(1) The said countermeasures are complex and burden large area and power overheads to the HW. Limited power budget in many applications such as embedded systems hinder us to employ SCA countermeasures for a large portion of a chip. Besides, dedicating a lot of space to security elements means reducing the effective area of the chip and increasing the manufacturing cost. The CMOS scaling limitations make the situation even more challenging.

(2) Some fundamental features of COMS-based circuits make them vulnerable to the power SCAs. Asymmetric I-V characteristics of p- and n-type transistors and different structures of the pull-up and pull-down networks in CMOS-based design lead to a significant power trace variation during different transitions.

Unique features of the RFET enable us to address these problems. We can design compact and low-power logic cells thanks to the reconfigurability and multi-input support of the RFET. It allows employing more complex countermeasures against the SCA while meeting the area and power constraints. Besides, RFETs have an inherent SCA resiliency because, firstly, most RFETs provide near identical I-V characteristics in p- and n-type configurations [52], and secondly, RFETs can merge two or more transistors in series into a single device, which helps design circuits with more similar pull-up and pull-down networks. In the following, we explain two works that provide power SCA resilience using RFET.

Using complementary gates (e.g., NAND-AND or XOR-XNOR gates) to equalize dynamic power consumption during charging and discharging the output capacitance is a well-known and effective power SCA countermeasure. However, this technique leads to a large area and power overhead because it almost doubles the number of required transistors. Using RFET, compact and low-power logic gates can be realized with fewer transistors, enabling us to afford the complementary gate technique. For this reason, [10] proposes an RFET-based 2-input XOR-XNOR gate using RFET to decrease the power trace variation. In addition to balancing the output capacitance by using complementary gates, the inputs are rearranged (compared to the naive RFET-based implementation [58]) to equalize the input capacitances. The authors show that their design can reduce the power trace variation and switching power by 57% and 26% with half number of transistors compared to the CMOS counterpart. Besides, it consumes 8× less leakage power due to the lower leakage current of the RFET. As the XOR gate is widely used in cryptographic circuits, the authors claimed that the proposed method increases the robustness of the circuit against the DPA attack.

In contrast to [10], which focuses on the combinational logic gates, [47] targets the sequential elements in the cryptographic circuits. The authors in [47] propose a modified true single-phase clock D-flipflop (mTSPC DFF) using RFET. Based on the results, RFET-based mTSPC DFF can achieve much lower power trace variation compared to the CMOS one. The higher resiliency of the RFET-based mTSPC DFF comes from the symmetrical characteristic of RFET. For security evaluation, a CPA attack has been performed on an 8-bit S-box whose output is sampled by a group of proposed DFFs. The key was not revealed with 256 power traces.

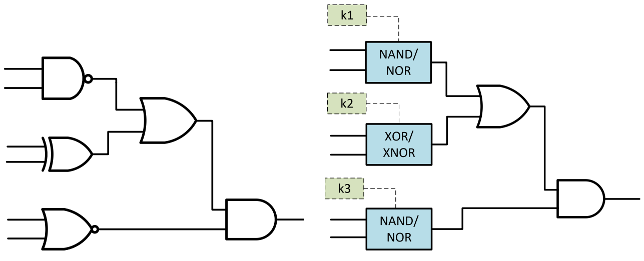
4 IP PROTECTION

To protect their legitimate interests, IP designers should consider adding a set of DFT techniques to their design, considering the overheads they are willing to bear in terms of power, area, performance, and the level of protection they deem to provide. In this section, we discuss the DFT techniques and investigate the benefits RFET devices provide for such techniques based on their intrinsic electrical and structural properties.

4.1 Logic Locking

Logic locking (LL) is a holistic DFT technique that can shield the IP through different stages of the IC supply chain. This technique locks the design by adding new logic elements to the circuit, hiding the true functionality of the design. The locked design only functions correctly upon receiving a true set of key bits stored in a tamper-proof on-chip memory.

Preliminary LL techniques [39, 44] utilized XOR/XNOR gates or multiplexers to bring the most corruption to the output of the circuit if the wrong key is in place. However, these early approaches were



(a) Original circuit **(b) Locked circuit**

Figure 2: RFET-based LL

broken by Boolean satisfiability (SAT)-based attack [49]. The SAT attack suffers two weaknesses. Firstly it requires access to a functional golden chip (Oracle) which is not always possible. Secondly, it is not scalable for large circuits with complex structures such as multipliers, cryptography algorithms, huge AND trees, and routing modules. Harnessing these weaknesses, security designers have proposed anti-sat schemes like point-function [57] and stripped functionality logic locking (SFLL) [56] techniques. Although effective, the protection techniques for thwarting SAT attacks infer large overheads regarding area, power, and performance when implemented utilizing CMOS-based logic.

In recent years a new class of attacks dubbed structural attacks has been introduced that can break large complex circuits without the need for an oracle. The most powerful structural attacks utilize ML [6, 4, 2, 1] to find the structural traces that protection logic brings to the original design. Most of these attacks use the locked circuit for training the ML models; To prevent them, the attacker can hide the structural traces of the LL scheme [7] or lock a large portion of the circuit to minimize the attacks' training accuracy.

In this section, we discuss the benefits of transistor level reconfigurability of RFETs for thwarting SAT and structural attacks.

4.1.1 Threat Model. The attacker has access to the locked netlist and can distinguish between primary inputs and key inputs. Moreover, the attacker is aware of the underlying locking scheme. In the case of SAT attack, the attacker has access to an oracle.

4.1.2 Benefits of RFETs for LL. In CMOS-based circuits, locking the design requires additional logic cells like XOR/XNORs, look-up Tables (LUTs), and multiplexers. The intrinsic reconfigurability of RFET cells can omit the need for bringing additional cells to lock the circuits. Using RFETs alongside CMOS in a circuit leads to a drastic decrease in the area and power overhead of the LL technique by simply replacing some of the existing CMOS logic cells in the design with RFET counterparts [34]. Figure 2 shows a small circuit locked with RFET cells. Locking this circuit with CMOS cells requires one extra XOR cell, one extra NOR cell, one extra nand cell and two multiplexers, while the RFET version only needs three INV cells for providing programming signals for PGs.

Knowing RFET's potential, [3] presented an anti-sat LL scheme based on RFET gates. The authors also showed that utilizing RFETs results in less overheads for their anti-sat scheme. Moreover, they showed that replacing CMOS cells with reconfigurable RFET cells connected to key bits decreases the area overhead of LL by a factor of 4 while it infers less performance penalty comparing CMOS only based XOR/XNOR LL technique. Moreover, the locked circuit's overall power stays almost the same as the original circuit.

Table 1: The security and overhead of XOR/XNOR based LL scheme

Benchmark	**Accuracy (%)**		**Area overhead (%)**	
	OMLA	SCOPE	CMOS	RFET
C1355	42	48	123.0	10.2
C1908	47	44	84.5	7.0
C7552	51	43	44.4	3.7
C5315	50	49	39.6	3.3

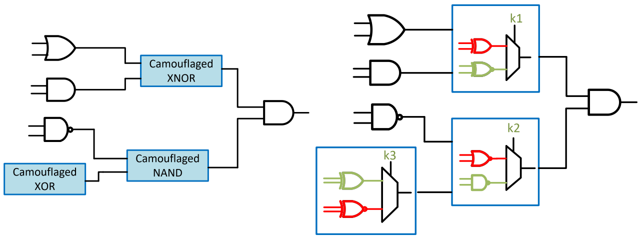
To evaluate the benefits of using RFET cells in LL against ML-based structural attacks, we locked various circuits from *ISCAS-85* benchmarks. Here we lock all XOR and XNOR cells of the original design by replacing them with RFET XOR/XNOR cells. Locking an XOR (XNOR) cell using CMOS requires 12 transistors (two INV cells and an XOR cell), while locking the same cell using RFETs requires only six transistors by replacing the XOR gate with an XOR/XNOR RFET cell and using an inverter for connecting key bit to the cell. However, based on [50] each RFET transistor is roughly 1.5x bigger than a CMOS transistor. So, to calculate the area overhead, we multiply the number of RFET transistors by 1.5. Table 1 shows the area overhead (based on the number of transistors) and the accuracy results from OMLA [4] and SCOPE [1] attacks in such a scheme. The results show that this scheme can thwart both attacks by decreasing their accuracy to less than 50%, meaning they guess the values of the key bits randomly. Moreover, the table shows that the area overhead of implementing such scheme can be drastically decreased using RFET devices.

4.2 Layout Camouflaging

Layout camouflaging is a DFT technique that is added to the circuit at the fabrication stage by replacing some common logic gates with camouflaged ones. This way, malicious entities cannot access the true design using simple imaging tools. Layout camouflaging can be implemented as static and dynamic [40] where the first needs devices that carry on multiple functionalities in the pre-fabrication stage, and in the latter, devices should support dynamic functionality at the run-time.

Equipped with advanced imaging, de-packaging, and de-layering tools, the attackers can easily extract the CMOS-based camouflaged netlist of an IP. By accessing the gate-level library, attackers can map the camouflaged circuit to a logic-locked circuit considering functionality control signals as key bits connected to multiplexers. Figure 3 shows the mapping of camouflaged circuit with XOR/XNOR and AND/NAND camouflaging primitives to a logic locked circuit. Guarding the IP against state-of-the-art attacks requires using many camouflaging primitives in the same chip area. Power and area-hungry CMOS-based camouflaging primitives limit the camouflaged portion of the circuit. Emerging nanotechnologies like RFET devices can compensate for this limitation by bringing transistor level reconfigurability.

4.2.1 Threat Model. Here, the attacker can provide multiple copies of the functional chip. The attacker also has access to reverse engineering tools for de-packaging, de-layering, and imaging that can extract the camouflaged netlist. Besides, the attacker has access to the gate-level library and it is not possible for the attacker



(a) Camouflaged circuit **(b) Mapped to logic locked circuit**

Figure 3: Mapping camouflaged circuits to logic locked circuit

to resolve voltage and current assignments with advanced invasive read-out attacks. After extracting the camouflaged netlist, the attacker utilizes SAT to attacks the circuit.

4.2.2 Static camouflaging. As mentioned, pre-fabrication reconfigurability is the main demand for static camouflaging [40]. Here, devices with a lower area and power, and more functionality implemented using the same layout, are preferable. Lower power and area overhead lead to having more camouflaged primitives within the tolerable overhead span, and more functionality brings more complexity per primitive regarding SAT attack.

Emerging nanotechnologies have been exploited in recent years for developing compact and low-power camouflaging primitives. In [28], the authors proposed a static camouflaging primitive leveraging the giant spin-hall effect (GSHE) switch. This single primitive can implement all 16 possible boolean functions for two inputs. By bringing the highest number of possible functions per primitive, this cell can replace all two input logics in the design. The authors showed that the run-time of the SAT attack increases exponentially by increasing the number of camouflaging primitives in the design.

4.2.3 Dynamic Camouflaging. Changing the functionality of the logic gates on-the-fly in the functional circuit is a promising way to thwart SAT attacks. In this technique, based on the state and inputs of the circuit, some of the outputs of the circuit would be set to the wrong values in functional chips. Although this technique is not a good choice for deterministic processing systems, it can be utilized to secure approximate circuits. Having wrong values for some outputs in various conditions leads the SAT solver to a wrong key or a UNSAT problem [41].

Emerging nanotechnologies like magnetic domain-wall [14], magnetoelectric spin-Orbit (MESO) [41], and RFETs can be utilized in dynamic reconfiguration. During dynamic camouflaging, the delay of switching primitive functionality is as important as power, area, and performance overheads. In [41] authors presented a MESO gate capable of implementing eight different functionalities. Using an image processing error tolerant IP, the authors showed that dynamic camouflaging could thwart a range of attacks in various IC manufacturing stages.

Although, the current works for camouflaging seem promising their shortcomings should be addressed. Considerably higher delay of GSHE and MESO devices compared to CMOS gates can limit their usage to the design's non-critical paths. As an example [6], in a large-scale circuit, only 5 to 15 percent of the gates can be replaced by GSHE gates. Moreover, the delay of switching the MESO gates' function is very high compared to conventional CMOS gates' delay.

Table 2: Comparison of camouflaging primitives

Publication	Primitive Function	Energy (fJ)	Power (μW)	Cell Delay	Switching Delay
DWM [14]	AND/OR	67.72	60.46	1.12 ns	N/A
MESO [41]	XOR, XNOR, AND, OR NAND,NOR,INV,BUF	0.01	0.06	0.26 ns	258 ps
GSHE [28]	All 16 functions	0.33	0.21	1.55 ns	N/A
RFET	NAND/NOR	0.01	1.5	6.7 ps	14.3 ps
RFET	XOR/XNOR	0.04	3.4	10.9 ps	10.5 ps

This shows that having more functionalities per camouflaging primitive should not be the only consideration when choosing emerging nanotechnologies for camouflaging. Future works should consider high performance compact and low-power devices. RFET devices seem promising for this purpose. These devices provide the security designer with compact, low-power, and high-performance camouflaging primitives with very fast functional switching. While, the number of functionality per primitive is not high in these devices; they can replace a higher number of CMOS gates in the original circuit with a minimum performance penalty. Table 2 shows the comparison of emerging-devices camouflaging primitives. In this table we used 14nm GeNW RFET Verilog-A model based on [53] for implementing RFET cells.

4.3 Watermarking

Watermarking is an effective IP protection measure against false ownership claims. The designer can insert secret signature or watermarks within the circuit to prove the ownership against a falsely claimed IC. Device-level reconfigurability can be utilized to insert watermarks in circuits as shown in [32]. The authors used RFETs-based inverters, which are polymorphic from a schematic point of view as shown in Figure 4. The inverter functionality can be realized with different values of PG inputs.

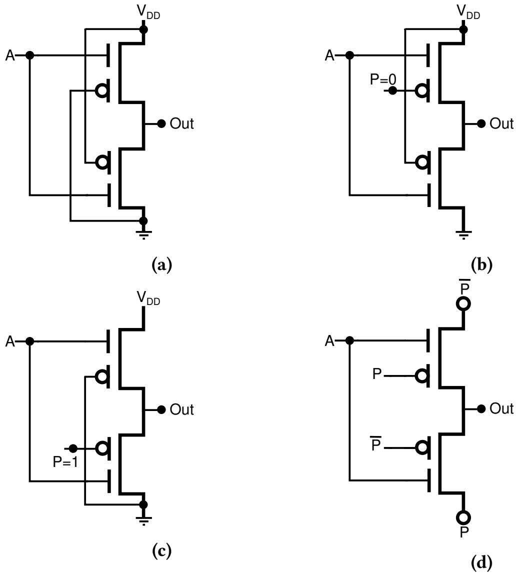


Figure 4: Polymorphic inverters (a) Static design – drain, source and PG are fixed to V$_{dd}$ and V$_{ss}$ respectively (b) Transistor's PG terminal connected to logic 0 (c) Transistor's PG terminal connected to logic 1 (d) Fully reconfigurable design where both logic 0 and logic 1 can be used for inverter functionality. This design also has an additional inverter to drive P and $\overline{P}$.

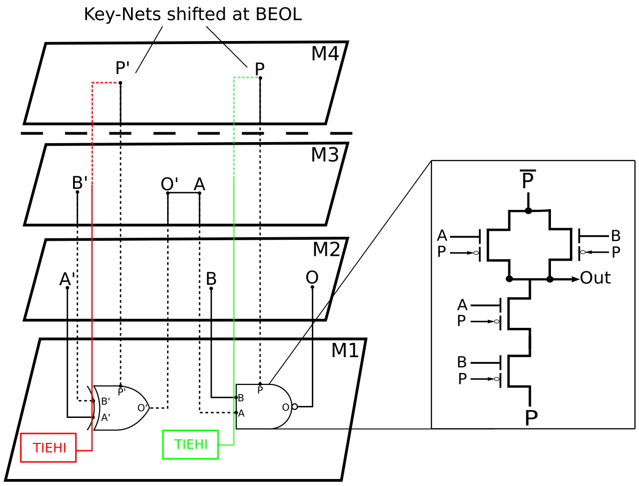


Figure 5: An example of SM using RFET-based reconfigurable cells [34]

Such inverter designs can be used by the designer to insert watermarking by encoding digital signature with the type of polymorphic inverters used. Additionally, using the inverter design as shown in Figure 4d, one can also design a strong watermarking scheme by using imperfections in RFETs-based logic gates [32]. With these imperfections in individual RFETs, logic gates can be shorted to drive outputs to only logic 1 or logic 0. These outputs can be specifically selected at don't care nodes within the logic graph and drive the inverters (Figure 4d). Using don't care nodes and specific values of logic (0 or 1) to drive the inverters, the designer can embed strong watermark within the IC. However, one shortcoming of such a watermark technique is that it requires invasive techniques to prove ownership claims.

4.4 Split Manufacturing

As mentioned, due to globalization, the security of the chip can be threatened at various manufacturing stages. In a scenario, IP may be attacked by malicious persons in an untrusted foundry. Split Manufacturing (SM) can help us to defeat such attacks. SM is a method in which the manufacturing process is split up into front-end-of-line (FEOL) and back-end-of-line (BEOL). FEOL contains all transistors, passive elements, and one or a few metal layers, mainly for intra-cell interconnections, and BEOL includes higher metal layers, mainly for inter-cell interconnections. While SM was first introduced in [15] to enhance yield by separately testing FEOL and BEOL, it was later considered a means to increase HW security [54]. The high cost of keeping fabrication equipments up-to-date is one of the main reasons design houses are fabless. With SM, it is possible to outsource the FEOL to an untrustworthy high-end fab and keep the BEOL process in a trusted fab (e.g., in the design house) with older technology. As the attackers in the untrustworthy fab have access only to the FEOL layout, they cannot easily infer the whole design due to missing interconnects. Hence, SM can preserve IP protection against trojan insertion and IP piracy. Since lifting wires to the higher metal layers affects the performance and power consumption of the chip, it is crucial to decide which wires should be lifted to gain acceptable security with minimum performance and power penalty. Although SM hides some interconnects from the attacker, they may be able to extract missing parts with the help of *design constraint based attacks* [55]. These attacks exploit logic and physical hints in the FEOL layout alongside design constraints to guess the connections in the BEOL. The hints include the proximity of cells, direction of the dangling nets in the FEOL, allowable load capacitance for a driver, the non-formation of combinational loops, and timing constraints [34]. Thus, designers must be careful not to leave such traces in the FEOL.

4.4.1 Threat Model. Here, the design house, designers, packaging and testing group, and the BEOL foundry are trustworthy, and only the FEOL foundry is considered untrustworthy. The attacker cannot acquire a functional chip from the open market because the end-user is trusted (a common assumption for sensitive and military applications). The attacker aims to infer the missing BEOL connections from the incomplete FEOL layout.

4.4.2 RFET benefits for SM. Due to the functional polymorphism provided by RFETs, the idea of LL can be leveraged in SM. In this method presented in [34], only the PG signals must be lifted to the BEOL, and the other wires can be routed freely based on the design constraints and goals. The concept of the proposed RFET-based SM method is shown in Figure 5. Similar to the LL, in the proposed SM, the actual functionality of polymorphic gates is not apparent to the attackers; hence, they are not able to extract the entire netlist from the FEOL layout. The main difference between this method and LL is that, here, keys are implemented via connections in the BEOL with the help of TIE cells instead of a tamper-proof memory. Although the seminal idea of this method was first introduced in [46] for CMOS, additional key gates were required in their approach. In contrast, the inherent polymorphism of RFET enables us to implement the SM without adding extra logic gates. The main reasons why the design constraint based attacks do not work on this SM approach are as follows:

(1) Randomizing the placement of TIE cells can eliminate the proximity between TIE cells and corresponding PG signals.
(2) As TIE cells provide constant '0' and '1' for RFET programming, the hint of load capacitance and timing constraints are not applicable.
(3) Since TIE cells are not driven by any other logic gate, the hint of non-formation of combinational loops does not help the attacker.

5 CONCLUSION

In this paper, we investigated the application of RFET as a reconfigurable device in different aspects of HW security. Intrinsic features of RFETs like reonfiguriblity, symmetrical characteristic, and multi-input support can be utilized to provide more robust HW security solutions with considerably less overhead comparing CMOS-based approaches. Moreover, we expect novel HW security solutions to be proposed based on inherent device-level reconfigurability provided by RFET.

ACKNOWLEDGMENTS

This work was financially supported by the German Federal Ministry of Education and Research BMBF under the framework of VE-CirroStrato.

REFERENCES

[1] Abdulrahman Alaql et al. "SCOPE: Synthesis-based constant propagation attack on logic locking". In: *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* (2021).

[2] Abdulrahman Alaql et al. "Sweep to the secret: A constant propagation attack on logic locking". In: *2019 Asian Hardware Oriented Security and Trust Symposium (AsianHOST)*. IEEE. 2019.

[3] Qutaiba Alasad et al. "Strong logic obfuscation with low overhead against IC reverse engineering attacks". In: *ACM Transactions on Design Automation of Electronic Systems (TODAES)* (2020).

[4] Lilas Alrahis et al. "OMLA: An oracle-less machine learning-based attack on logic locking". In: *IEEE Transactions on Circuits and Systems II: Express Briefs* (2021).

[5] Eric Brier et al. "Correlation power analysis with a leakage model". In: *International workshop on cryptographic hardware and embedded systems*. Springer. 2004.

[6] Prabuddha Chakraborty et al. "SAIL: Analyzing structural artifacts of logic locking using machine learning". In: *IEEE Transactions on Information Forensics and Security* (2021).

[7] Armin Darjani et al. "ENTANGLE: An Enhanced Logic-locking Technique for Thwarting SAT and Structural Attacks". In: *Proceedings of the Great Lakes Symposium on VLSI 2022*. 2022.

[8] Michele De Marchi et al. "Polarity control in double-gate, gate-all-around vertically stacked silicon nanowire FETs". In: *2012 International Electron Devices Meeting*. 2012.

[9] Abhijitt Dhavlle. "Adversarial Learning Inspired Emerging Side-Channel Attacks and Defenses". In: *arXiv preprint arXiv:2104.04054* (2021).

[10] Edouard 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)*. IEEE. 2018.

[11] Basel Halak. "Cist: A threat modelling approach for hardware supply chain security". In: *Hardware Supply Chain Security*. Springer, 2021, pp. 3–65.

[12] Naoki Harada et al. "A polarity-controllable graphene inverter". In: *Applied Physics Letters* (2010).

[13] André Heinzig et al. "Reconfigurable silicon nanowire transistors". In: *Nano Letters* (2012).

[14] Kejie Huang et al. "Magnetic domain-wall racetrack memory-based nonvolatile logic for low-power computing and fast run-time-reconfiguration". In: *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* (2016).

[15] Richard Wayne Jarvis et al. *Split manufacturing method for advanced semiconductor circuits*. US Patent 7,195,931. 2007.

[16] Shaminder Kaur et al. "Stratification of Hardware Attacks: Side Channel Attacks and Fault Injection Techniques". In: *SN Computer Science* (2021).

[17] Paul Kocher et al. "Differential power analysis". In: *Annual international cryptology conference*. Springer. 1999.

[18] Paul C Kocher. "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems". In: *Annual International Cryptology Conference*. Springer. 1996.

[19] Yu-Ming Lin et al. "High-performance Carbon Nanotube Field-effect Transistor with Tunable Polarities". In: *IEEE transactions on nanotechnology* (2005).

[20] Rubén Lumbiarres López et al. "Faking countermeasure against side-channel attacks". In: (2017).

[21] T Mikolajick et al. "20 Years of reconfigurable field-effect transistors: From concepts to future applications". In: *Solid-State Electronics* (2021).

[22] T Mikolajick et al. "Reconfigurable field effect transistors: A technology enablers perspective". In: *Solid-State Electronics* 194 (2022), p. 108381.

[23] T Mikolajick et al. "The RFET—a reconfigurable nanowire transistor and its application to novel electronic circuits and systems". In: *Semiconductor Science and Technology* (2017).

[24] Sandeep Miryala et al. "A Verilog-A model for reconfigurable logic gates based on graphene pn-junctions". In: *2013 Design, Automation Test in Europe Conference Exhibition (DATE)*. 2013.

[25] Shu Nakaharai et al. "Electrostatically Reversible Polarity of Ambipolar α-MoTe2 Transistors". In: *ACS Nano* (2015).

[26] Roman Novak. "SPA-based adaptive chosen-ciphertext attack on RSA implementation". In: *International Workshop on Public Key Cryptography*. Springer. 2002.

[27] Maamar Ouladj and Sylvain Guilley. *Side-Channel Analysis of Embedded Systems*. Springer, 2021.

[28] Satwik Patnaik et al. "Advancing hardware security using polymorphic and stochastic spin-hall effect devices". In: *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE. 2018.

[29] Shubham Rai et al. "A physical synthesis flow for early technology evaluation of silicon nanowire based reconfigurable FETs". In: *2018 Design, Automation Test in Europe Conference Exhibition (DATE)*. 2018.

[30] Shubham Rai et al. "Designing Efficient Circuits Based on Runtime-Reconfigurable Field-Effect Transistors". In: *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* (2019).

[31] Shubham Rai et al. "Emerging Reconfigurable Nanotechnologies: Can They Support Future Electronics?" In: *Proceedings of the International Conference on Computer-Aided Design*. ICCAD '18. San Diego, California: ACM, 2018.

[32] Shubham Rai et al. "Hardware Watermarking Using Polymorphic Inverter Designs Based On Reconfigurable Nanotechnologies". In: *2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. 2019.

[33] Shubham Rai et al. "Preserving Self-Duality During Logic Synthesis for Emerging Reconfigurable Nanotechnologies". In: *2021 Design, Automation Test in Europe Conference Exhibition (DATE)*. 2021.

[34] Shubham Rai et al. "Security promises and vulnerabilities in emerging reconfigurable nanotechnology-based circuits". In: *IEEE Transactions on Emerging Topics in Computing* (2020).

[35] Shubham Rai et al. "Vertical IP protection of the next-generation devices: Quo vadis?" In: *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE. 2021, pp. 1905–1914.

[36] Michael Raitza et al. "Exploiting transistor-level reconfiguration to optimize combinational circuits". In: *Design, Automation Test in Europe Conference Exhibition (DATE), 2017*. 2017.

[37] Jeyavijayan Rajendran et al. "Nano Meets Security: Exploring Nanoelectronic Devices for Security Applications". In: *Proceedings of the IEEE* (2015).

[38] Jeyavijayan Rajendran et al. "Security analysis of integrated circuit camouflaging". In: *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 2013.

[39] Jeyavijayan Rajendran et al. "Security analysis of logic obfuscation". In: *Proceedings of the 49th Annual Design Automation Conference*. 2012.

[40] Nikhil Rangarajan et al. *Next Era in Hardware Security*. Springer, 2021.

[41] Nikhil Rangarajan et al. "Opening the doors to dynamic camouflaging: Harnessing the power of polymorphic devices". In: *IEEE Transactions on Emerging Topics in Computing* (2020).

[42] Giovanni V. Resta et al. "Polarity control in WSe2 double-gate transistors". In: *Scientific Reports* (2016).

[43] Maximilian Reuter et al. "From MOSFETs to Ambipolar Transistors: Standard Cell Synthesis for the Planar RFET Technology". In: *IEEE Transactions on Circuits and Systems I: Regular Papers* (2021).

[44] Jarrod A Roy et al. "Ending piracy of integrated circuits". In: *Computer* (2010).

[45] Ansh Rupani et al. "Exploiting Emerging Reconfigurable Technologies for Secure Devices". In: *2019 22nd Euromicro Conference on Digital System Design (DSD)*. 2019.

[46] Abhrajit Sengupta et al. "A new paradigm in split manufacturing: Lock the FEOL, unlock at the BEOL". In: *Cryptography* (2022).

[47] Mohammad Mehdi Sharifi et al. "A Novel TIGFET-based DFF Design for Improved Resilience to Power Side-Channel Attacks." In: *2020 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. 2020.

[48] Ozgur Sinanoglu et al. *The Next Era in Hardware Security: A Perspective on Emerging Technologies for Secure Electronics*. Springer, 2021.

[49] Pramod Subramanyan et al. "Evaluating the security of logic encryption algorithms". In: *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE. 2015.

[50] Xifan 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)*. IEEE. 2014.

[51] Jens Trommer. *Towards Reconfigurable Electronics by Functionality-Enhanced Circuits and Germanium Nanowire Devices*. BoD–Books on Demand, 2017.

[52] Jens Trommer et al. "Functionality-enhanced logic gate design enabled by symmetrical reconfigurable silicon nanowire transistors". In: *IEEE Transactions on Nanotechnology* (2015).

[53] Jens Trommer et al. "Material prospects of reconfigurable transistor (rfets)–from silicon to germanium nanowires". In: *MRS Online Proceedings Library (OPL)* (2014).

[54] Kaushik Vaidyanathan et al. "Building trusted ICs using split fabrication". In: *2014 IEEE international symposium on hardware-oriented security and trust (HOST)*. IEEE. 2014.

[55] Ranga Vemuri et al. "Split Manufacturing of Integrated Circuits for Hardware Security and Trust: Methods, Attacks and Defenses". In: (2021).

[56] Muhammad Yasin et al. "Provably-secure logic locking: From theory to practice". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 2017.

[57] Muhammad Yasin et al. "SARLock: SAT attack resistant logic locking". In: *2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. IEEE. 2016.

[58] Jian Zhang et al. "Configurable circuits featuring dual-threshold-voltage design with three-independent-gate silicon nanowire FETs". In: *IEEE Transactions on Circuits and Systems I: Regular Papers* (2014).