Design Enablement Flow for Circuits with Inherent Obfuscation based on Reconfigurable Transistors

J. Trommer*, N. Bhattacharjee, T. Mikolajick
NaMLab gGmbH
Nöthnitzer Str. 64a, 01187 Dresden, Germany
jens.trommer@namlab.com

S. Huhn, M. Merten, M.E. Djeridane, M. Hassan, R. Drechsler
Arbeitsgruppe Rechnerarchitektur, University of Bremen
Bibliothekstr. 5, 28359 Bremen, Germany

S. Rai, N. Kavand, A. Darjani, A. Kumar
Chair of Processor Design, TU Dresden
Helmholtzstraße 10, 01062 Dresden, Germany

V. Sessi, M. Drescher, S. Kolodinski, M. Wiatr
GlobalFoundries Fab 1
Wilschdorfer Landstraße 101, 01109 Dresden, Germany

***Abstract*—Reconfigurable transistors are a new emerging type of device, which offer the promise to improve the resistance of electronic components against know-how theft. In order to enable a product development of such an emerging device, a cross-layer design enablement strategy is needed, as emerging technologies are not necessarily compatible withstandard tools used in the industry. In 'CirroStrato', we aim on the development of such a complete flow enabling CMOS co-integration of reconfigurable transistors, ranging from process adjustments, device modeling, library characterization, physical and logical synthesis up towards sophisticated hardware security tests. In this multi-partner-project (MPP) paper, our aim is to elucidate the overall design enablement flow, as well as current research challenges on the individual stages.**

***Index Terms*—Emerging devices, reconfigurable circuits, EDA, modelling, CMOS co-integration, hardware security**

I. Introduction

Today's society relies, to a critical extent, on trust in electronic systems. Over the last few years, the security of these systems has been repeatedly threatened by hardware-level attacks [1]–[3] that can bypass software-based security solutions. Theft and unauthorized replication of integrated circuits poses a particular problem. Cheap but faulty or even trojanized replicas can lead to severe failures in mission-critical areas, such as self-driving cars or industrial plants, with high collateral damage up to personal injury. The direct and indirect financial damage caused by *Intellectual Property* (IP) piracy is estimated at several hundred billion euros annually. CMOS-based technologies already offer various security mechanisms to protect the subject-specific IP ('know-how') of electronic components. However, such protection circuits based on classical CMOS technology have proven to be cost-inefficient in terms of higher chip area as well as high power consumption. Moreover, these solutions often lack comprehensive protection of proprietary designs along the entire value chain. Several emerging nanotechnologies, like memristors, carbon nanotubes and spintronic devices, have been proposed to increase the security level due to their inherent resilience against various attacks. Among them, Reconfigurable Field-effect Transistors (RFETs) represent one of the most promising nanotechnological solution to protect against know-how theft [4], [5]. This type of transistor with electrically adjustable p- or n-conductivity [6] offers a variety of inherent device properties that make them ideal for the realization of trustworthy electronics (Fig. 1). Thanks to their inherent polymorphic nature, RFETs enable reversible electrical programmability of digital circuit blocks without the need to change the layout or physical structure [7]. Manufacturers can therefore program the actual or desired functionality following contract manufacturing and defect testing. Neither the manufacturer (foundry) nor external test centers have access to the actual functionality of the design. Unlike in standard CMOS electronics, the actual circuit or function remains hidden in the layout since it cannot be distinguished from other combinations by either simple physical microanalysis (reverse engineering). Being a charge-based device, RFETs hold the potential to be integrated seamlessly into CMOS technology [8]. Due to geometric similarities, Fully-Depleted Silicon-On-Insulator (FDSOI) technology are particularly suitable for such co-integration [9]. Recently, also a co-integration schema for bulk-CMOS has been proposed [10].

In order to enable product development for such platforms, a cross-layer design enablement strategy is needed, as emerging technologies are not necessarily compatible with standard tools used in industry. In the 'CirroStrato' project, started in March 2021, we aim on the development of such a complete flow enabling reconfigurable transistors as CMOS add-on. The objectives are ranging from process co-integration, device modeling, library characterization, physical and logical synthesis up towards sophisticated hardware security tests. In this intermediate multi-partner project (MPP) paper, our aim is to elucidate on the overall targeted design enablement flow, as well as research challenges on the individual stages.

II. Background

A. Attack Models and IP Protection Strategies

In the heart of a major semiconductor crisis caused by technological acceleration and also by demand outstripping supply, the globalization of the semiconductor business model is more important than ever as it offers highly specialized expertise at lower cost. However, third party involvement in the process

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

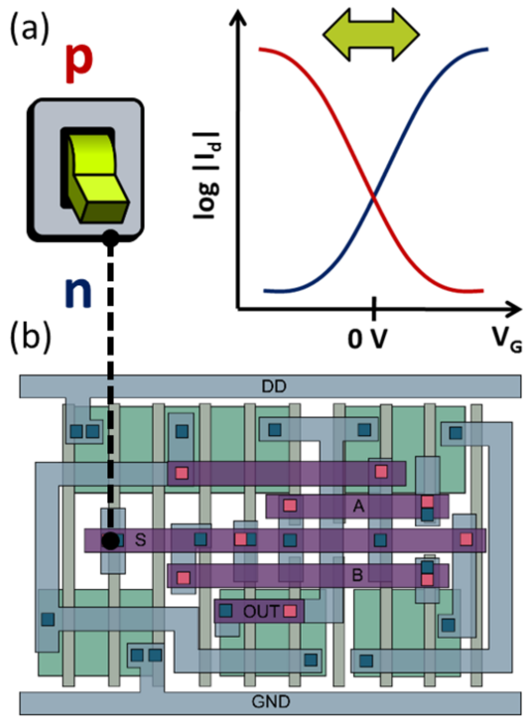

Fig. 1: Generic representation of Reconfigurable Field Effect Transistor (RFET) functionality. (a) Dynamic device level polymorphism by switching p- to n-operation. (b) Dynamic gate level obfuscation of a layout with electrically selectable NAND or NOR functionality.

increases the risk of intentional temperament by misusing or inserting Trojans, IP infringement, reverse engineering or overproducing circuits to be sold in the black market [11], [12]. Many solutions were suggested to deal with these issues, namely watermarking, fingerprinting, split-manufacturing, camouflaging, and logic locking. Each solution targets specific threats [12]. While watermarking and fingerprinting only allow the identification of the infraction after it took place. The remaining solutions aim to stop these threats from happening. However, split-manufacturing does not protect from the most critical threat: reverse engineering.

In the literature, the threat model, in the context of hardware security, is aspired from Kerckhoffs's principle. It is, therefore, reasonable to assume that the attacker has full access to the netlist (often acquired through reverse engineering), and a working circuit known as an Oracle. Second party entities like foundries or design test centers are perfectly capable of overproducing, and through reverse engineering, commit all the aforementioned infractions. Reverse engineering is mainly possible through probing, structural analysis, and side channel attacks. These three can be thwarted using camouflaging.

However, the leading defense technique against IP theft is *Logic Locking* [13], [14]. It consists of adding supplementary logic driven by additional primary inputs known as *key_inputs* to ensure that the proper circuit operation is only obtained when the correct key pattern is assigned, otherwise, the added logic would corrupt the output. Logic locking can protect against overproduction. One of the drawbacks of the logic locking is the high area, delay, and power overhead that this technique infers to the circuit. Also classical logic locking approaches have been shown to be weak against powerful satisfiability (SAT)-based attacks [15].

B. Reconfigurable Transistors

The unique device level reconfigurability of RFETs is based on the requirement of having a minimum of independent two gates: one *Program Gate* (PG), which switches the transistor between the p-type and n-type behavior and one *Control Gate* (CG) which turns the transistor ON/OFF. In the framework of 'CirroStrato', two device variants become highly interesting for a co-integration to CMOS: the Back-Bias RFET [8] and the *Three-Independent-Gate* (TIG)-RFET [17] as illustrated in Figure 2(a,c). In the Back-Bias RFET, the substrate contact below the *Buried Oxide* (BOX) creates electrostatic doping in the SOI channel, which controls the charge type (electrons or holes) that is injected through the Nickelsilicide (NiSi) Schottky contacts into the channel. The device features the smallest possible RFET implementation but comes at the expense of the program voltage being higher than the typical supply voltage V_{DD}. On the contrary, in TIG-RFETs the individual PGs overlap the Si-NiSi interface from the front, thereby controlling the band bending to choose the majority carriers being injected into the channel. The carrier injection is, therefore, governed by thermionic field emission across this metal-semiconductor interface, while the CG forms a thermal barrier, thereby governing the charge transport across the channel. This device variant is larger, but it facilitates a higher expressive capability and is operational with a single supply voltage. More details of device physics and the background of RFETs are given in Ref. [6].

The feature of reconfigurability between p- and n-modes and the feature of multiple independent gates can be exploited to design electrical reconfigurable polymorphic logic gates, whose functionality can not be reverse engineered by simple visualization of the gate layout. Typical examples are NAND/NOR or XOR/XNOR gates. Utilizing those logic gates, RFETs can combine the techniques like logic locking and camouflaging to obfuscate the layout of a given circuit [4]. The main difference here is that instead of adding key logic gates to the design, existing NAND, NOR, or XOR gates can be replaced by polymorphic RFET gates, which will behave as intended by the designer by considering the PG as a *key_input*. Based on this, advanced concepts like dynamic camouflaging are conceivable, which are claimed to be more resilient against SAT-attacks [18]. Another huge advantage of using RFETs is their inherent electrical symmetry with respect to n/p-operation, which is also relevant in terms of power and delay, which can be utilized by circuit designers to propose low overhead countermeasures against side-channel attacks and probing. Thus, offering an extra layer of protection above logic locking [19], [20].

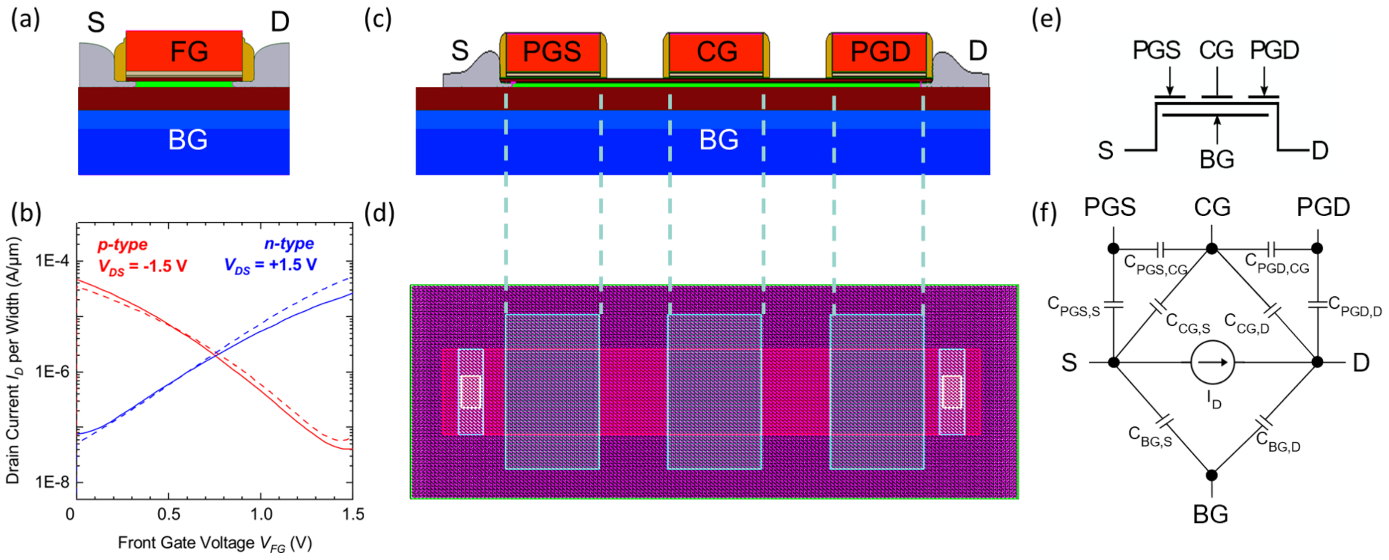

Fig. 2: Model development from TCAD to SPICE for Reconfigurable Field Effect Transistors on an 22 nm SOI platform. (a) Process simulated Back-Bias RFET device structure with front-gate (FG), back-gate (BG), source (S) and drain (D) and (b) simulated electrical characteristics (dotted lines) fitted to the measured data from [16] (straight lines). (c) Three-Independent-Gate RFET structure with control gate (CG), program gates at source (PGS) and drain (PGD) derived from (d) TIG-RFET layout files. (e) Symbol for the resulting TIG-RFET device table model for circuit schematic and (f) equivalent circuit showing the most important current and capacitance relations to be stored in the table.

III. Design Enablement Flow

A crucial component for bringing RFETs into mainstream electronics is to enable a design automation flow that can be utilized to develop RFETs-based circuits and make them able to co-exist on-chip with CMOS. Our targeted EDA flow is shown in Fig. 3. In the remainder of the paper, we discuss the key steps required as well as their associated challenges.

A. 22nm FDSOI Baseline and RFET Co-Integration

The yellow colored boxes in Fig. 3 indicate the standard CMOS EDA flow, in which we aim to integrate RFET devices. At its heart, the foundry provides a *Process Design Kit* (PDK), which is a set of files used to describe the fabrication process of the integrated circuit. It already comprises all physical and geometrical parameters, like gate line width, contacted poly pitch and channel doping. From this set of rules, a circuit library can be derived either by the foundry or the customer itself. Using this set of circuit blocks, the netlist of the actual IP can be generated. After logical synthesis, the layout information of the gate is used in physical synthesis to yield the final circuit layout, which will be brought to tape-out on a set of lithographic masks. One of the important features of modern PDKs is that CMOS technology is no longer limited to a single n- and p-type device. Both types manifest themselves in a multitude of versions, ranging from low V_{DD} core devices with different V_{TH} flavors to high V_{DD} i/o devices. On the one hand, this gives a great degree of freedom to circuit designers, on the other hand, it is a challenge for design automation, as models, libraries, and tools have to be capable of working with all of those device variants seamlessly.

In our current work, we target to supply RFETs as an additional device flavor to the 22FDX® technology platform [9] offered by GlobalFoundries, wherever their unique properties are needed. RFETs are superior with respect to CMOS co-integration as compared to other emerging front-end devices. There is no need for the introduction of new materials or processes. Technologically, planar RFETs mainly differentiate themselves from classical MOSFETs by the $NiSi_X$ Schottky contacts, which align directly inside the FDSOI channel instead on top of the raised source and drain areas [8]. In addition, different layout versions with one, two, or three front-gates have to be considered. The main challenge for fabrication is to prevent a silicide formation between the multiple front-gates while also keeping the number of additional masks as low as possible. To ensure this, a set of dedicated RFET PDK rules is derived, which is not influencing the 22 nm FDSOI baseline process. Based on these rules a single TIG-RFET layout (Fig. 2(d)) was established from which a library of TIG-RFET standard cells can be generated to supplement the CMOS gate library in terms of security functionality.

B. Modeling and Library Characterization

Device modeling plays a crucial part in bridging the gap from device development to circuit design. In order to make the RFET standard cells accessible to VLSI designers, *Liberty* files are needed, which contain high-level information about the security cells, including logic behavior, area, timing information, power consumption, and inputs capacitances. Details about the physical information of the cells are largely neglected.

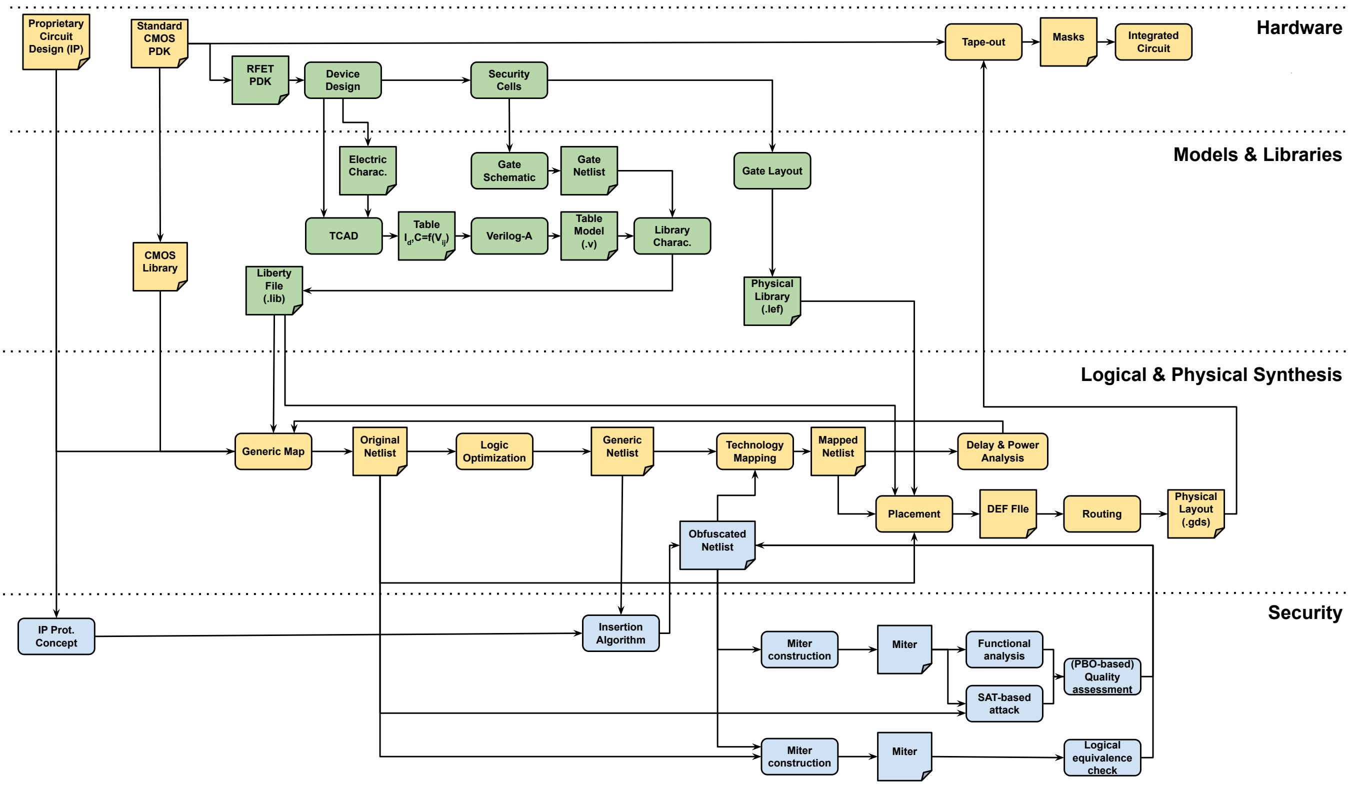

Fig. 3: Design enablement flow for RFETs as an add-on for CMOS technology across four layers of abstraction. Key steps (rounded boxes) and datasets (file shaped boxes) are indicated. Yellow colour indicates standard CMOS flow, green indicates EDA enablement for RFETs; blue indicates additional design for IP protection.

To create a *Liberty* file, all the standard cells should be characterized by analog circuit simulations. This can be done automatically using industrial characterization tools or manually using a SPICE circuit simulator. As most characterization tools are not set up for the extended functionality that the program gate offers to RFETs, we need to define the logic function and delay and power arcs of each cell for the tool by developing proper TCL scripts. Cell netlists and device models are essential for the characterization process. Generally, compact models, which rely on a formula-based description of the device behavior, would be preferred. However, the currently available models only cover the DC part of the devices and typically cannot reflect the behavior of more than two independent gates [21]–[23]. Thus, in ‘CirroStrato’, we target the development of TCAD-based table models as an intermediate step towards the full circuit design enablement. In the present approach, RFET structures are modeled by Sentaurus TCAD SPROCESS, inspired by the fabrication steps of the underlying FDSOI platform [8], [9]. Electrical measurements of test structures such as the Back-Bias RFET shown in Fig. 2(a,b) become the reference for parameter extraction such as mobilities for electrons μ_e and holes μ_h, tunneling masses and gate metal work function [16]. Combining the gathered parameter-set with layout information, predictive characteristics for other device flavors can be derived and verified by electrical measurements. Following an optimization of the TCAD model, voltage sweeps are performed across all the terminals, and the corresponding current, charge and capacitance distributions are extracted to form a look-up table. Finally, a Verilog-A based model is used to read the table data and therefore enable SPICE simulations in any analog circuit simulator supporting Verilog-A. This process is illustrated for a TIG-RFET device in Fig. 2(c-f). The drawback of this approach is that a new table has to be generated with each device flavor or development iteration. Also, tables tend to become very large with a higher number of independent gates as the overall number of data points N scales with $N = G^{V_i}$, where G is the granularity of the voltage sweep and V_i is the number of independent electrodes. In addition, the capacitive relations of the multigate structures can be quite complex, also leading to a large data table size [24]. Finally, for each standard cell, an additional LEF library is created to comprise layout information of the cells, like the coordinates of the pins or the number of metal layers.

C. *Logic and Physical Synthesis*

Once the technology model and library files are available, the next step is to generate a circuit netlist using RFET-based standard cells. This process basically comprises two main steps: *Logic* and *Physical synthesis*. Both these steps abstract away the technological aspects and focus on circuit integration by breaking it down into multiple stages, as shown in Fig. 3. To conduct logic synthesis just the Liberty file is required, while for physical synthesis, both Liberty and LEF library are needed.

Logic synthesis deals with optimizing a logic representation of a given circuit in terms of a cost function to typically reduce the overall area, delay, or power consumption of the circuit. Here, it is important that in principle both static as well as dynamic reconfigurable designs can be built with RFETs. From a conventional standpoint, existing logic synthesis approaches [25], [26] provide acceptable solutions for circuits made exclusive from RFETs. It has been shown recently that RFETs-specific logic abstraction can be integrated within logic synthesis to yield even better results in terms of area [27], [28]. However, dynamic reconfigurable logic gates often have a higher area or delay overhead as compared to their static implementation [29]. Existing CMOS synthesis tools are often sub-optimal in terms of truly utilizing this dynamic reconfigurable property. Suitable strategies to partition the circuit into static and reconfigurable components have to be devised. In 'CirroStrato', we aim to deliver techniques and methodology targeting such solutions. Particularly partitioning approaches help to mitigate the area and delay overheads. They are integral for our targeted security applications, where both transistor types are integrated in a single circuit. RFET-based standard cells should just be chosen, if they offer a benefit to the system like higher security, or less overhead. This approach is not limited to security, but can be also beneficial for general computing as demonstrated for 1-bit full adder designs [30]. Once logic synthesis is done, the logic representation undergoes technology mapping to generate a gate-level netlist based on the standard cells available in the library.

Physical synthesis takes this netlist from the technology mapping stage and uses various algorithms to realize the circuits in terms of metal wires and actual technology-characterized standard cells. Exact measures of delay and area are calculated in this stage. The main challenge for integrating RFET-based circuits in physical synthesis flow is to care for the additional gate terminal (program gate) of transistors within the standard cell boundary. This leads to more usage of routing resources [31]. An early-level physical synthesis for RFETs using an open-source tool flow with only few standard cells has been proposed in [32]. A more elaborate study with dynamic reconfigurable gates has been shown in [31], where the authors explored the standard *Power Shut-off* (PSO) approach to accommodate all reconfigurable standard cells within a single portion of the die. For a real co-integration of RFET and CMOS standard cells, synthesis will be more challenging, as both cell types have to be placed intermixed on the chip. Here, additional constraints like different sizes of both standard cell libraries must be considered if area-minimized designs are targeted.

Further, the design flow for security within the 'CirroStrato' framework adds additional challenges as contemporary algorithms have to bring in security considerations at various stages of their implementation. For example, conventional security approaches such as logic locking and camouflaging schemes are primarily implemented over the mapped netlist and are abstracted away from the synthesis algorithms. In 'CirroStrato', we aim at embedding security bindings deep within the synthesis paradigms for RFETs-based circuits to enable efficient security solutions with low overhead. One option to achieve this is explained in more detail in the next section.

D. Security Qualification

In order to maximize the resulting security while retaining the intended functional behavior, the placement of the polymorphic RFET cells is crucial. A smart placement can yield higher security with fewer elements, thus also reducing power and delay overheads. To ensure the functional equivalence of the protected circuit and the original circuit, a miter-based logical equivalence check is proposed as part of our design flow. The mechanisms' security assessment is of utmost importance to reinforce the newly introduced protection mechanism and, hence, avoid any weak logic structures. Various assessment techniques can be used for the quality assessment of RFET-based logic locking mechanisms. Simple simulation-based approaches, e.g., the approximate *Hamming Distance* (HD)-based assessment techniques, have been used for a simple evaluation of the protection quality. This approach uses HD-based measurements to differentiate two outputs of a circuit x and y [33]–[35]. The result is considered optimal if the HD is 50% of the maximal HD. The formal approach proposed in [36] shows the limitations of simulation-based approaches, unveiling further weaknesses in the protection mechanisms. In particular, formal techniques are orchestrated to analyze the circuit's state space to determine whether any incorrect keys exist that unintentionally unlock and expose the circuit's correct functional behavior. At first, an inverted miter circuit is generated from the *Circuit under Assessment* (CuA) while considering the a-priori known *correct* key. The CuA is unrolled for N clock cycles since sequential elements – meaning *Flip-Flops* (FFs) – have to be considered for an exact assessment in terms of sequential circuits' unrolling [37]. The primary inputs are equally driven for both unrolled instances of the CuA and are kept constant during the unrolling. After the inverted miter has been added, the key is constrained for both instances of the unrolled CuA. The entire model is stored as one SAT instance and processed by a state-of-the-art SAT solver. If the SAT instance is unsatisfiable, the correct key is considered as stable. If a satisfiable solution is determined, a corrupting key has been determined to yield a functional equivalent behavior of the CuA given at least one stimulus. For a qualitative assessment of the discovered security threat, every detected corrupting key is evaluated against the number of possible stimuli leading to this breach. This framework was improved in [38]. More precisely, the framework is enhanced to calculate the most intimidating corrupting keys based on the concept of a SAT-based attack. In contrast to other techniques, the corrupting keys are calculated based on *Distinguishing Input Patterns* (DIPs), maximizing the number of equivalent behaving stimuli. This improves the quality of the assessment of potential security threats using logic locking mechanisms. The detected security breach can be analyzed to determine the structural reason for the threat. The information can be used in an iterative reinforcement process of the mapped netlist, minimizing the weaknesses of the introduced protection mechanism until a maximum level of security is reached for a given overhead.

IV. Conclusion

We have presented a disruptive design enablement flow for integrating emerging reconfigurable field effect transistors as security elements into an existing 22 nm FDSOI technology. Challenges in the realization of this application, from hardware co-integration, modeling, library characterization, synthesis, and quality assessment of the security function, have been discussed. The overall flow will accelerate the design of emerging RFET-based applications for hardware security and beyond.

References

[1] Y. Kim, R. Daly, J. Kim, C. Fallin, J. H. Lee, D. Lee, C. Wilkerson, K. Lai, and O. Mutlu, "Flipping bits in memory without accessing them: An experimental study of dram disturbance errors," *ACM SIGARCH Computer Architecture News*, vol. 42, no. 3, pp. 361–372, 2014.

[2] P. Kocher, J. Horn, A. Fogh, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, *et al.*, "Spectre attacks: Exploiting speculative execution," *Communications of the ACM*, vol. 63, no. 7, pp. 93–101, 2020.

[3] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, *et al.*, "Meltdown: Reading kernel memory from user space," *Communications of the ACM*, vol. 63, no. 6, pp. 46–56, 2020.

[4] Y. Bi, P.-E. Gaillardon, X. S. Hu, M. Niemier, J.-S. Yuan, and Y. Jin, "Leveraging emerging technology for hardware security-case study on silicon nanowire fets and graphene symfets," in *2014 IEEE 23rd asian test symposium*, pp. 342–347, IEEE, 2014.

[5] J. Knechtel, "Hardware security for and beyond cmos technology: an overview on fundamentals, applications, and challenges," in *Proceedings of the 2020 International Symposium on Physical Design*, pp. 75–86, 2020.

[6] T. Mikolajick, G. Galderisi, S. Rai, M. Simon, R. Böckle, M. Sistani, C. Cakirlar, N. Bhattacharjee, T. Mauersberger, A. Heinzig, *et al.*, "Reconfigurable field effect transistors: A technology enablers perspective," *Solid-State Electronics*, p. 108381, 2022.

[7] J. Trommer, A. Heinzig, T. Baldauf, S. Slesazeck, T. Mikolajick, and W. M. Weber, "Functionality-enhanced logic gate design enabled by symmetrical reconfigurable silicon nanowire transistors," *IEEE Transactions on Nanotechnology*, vol. 14, no. 4, pp. 689–698, 2015.

[8] V. Sessi, M. Simon, S. Slesazeck, M. Drescher, H. Mulaosmanovic, K. Li, R. Binder, S. Waidmann, A. Zeun, A.-S. Pawlik, *et al.*, "Back-bias reconfigurable field effect transistor: A flexible add-on functionality for 22 nm fdsoi," in *2021 Silicon Nanoelectronics Workshop (SNW)*, pp. 1–2, IEEE, 2021.

[9] R. Carter, J. Mazurier, L. Pirro, J. Sachse, P. Baars, J. Faul, C. Grass, G. Grasshoff, P. Javorka, T. Kammler, *et al.*, "22nm fdsoi technology for emerging mobile, internet-of-things, and rf applications," in *2016 IEEE International Electron Devices Meeting (IEDM)*, pp. 2–2, IEEE, 2016.

[10] S. H. Lee, S. H. Kim, S. Jung, J. W. Park, T. M. Roh, W. Lee, and D. Suh, "Demonstration of reconfigurable fet and logic gates on epitaxial lateral overgrowth silicon platform," *IEEE Transactions on Electron Devices*, vol. 69, no. 10, pp. 5443–5449, 2022.

[11] S. Dupuis, P.-S. Ba, G. Di Natale, M.-L. Flottes, and B. Rouzeyre, "A novel hardware logic encryption technique for thwarting illegal overproduction and hardware trojans," in *2014 IEEE 20th International On-Line Testing Symposium (IOLTS)*, pp. 49–54, 2014.

[12] M. Rostami, F. Koushanfar, and R. Karri, "A primer on hardware security: Models, methods, and metrics," *Proceedings of the Institute of Radio Engineers*, vol. 102, pp. 1283–1295, Aug. 2014.

[13] A. Chakraborty, N. Jayasankaran, Y. Liu, J. Rajendran, O. Sinanoglu, A. Srivastava, Y. Xie, M. Yasin, and M. Zuzak, "Keynote: A disquisition on logic locking," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, pp. 1952–1972, Oct. 2020.

[14] M. Yasin, J. Rajendran, and O. Sinanoglu, *Trustworthy Hardware Design: Combinational Logic Locking Techniques*. Springer Publishing Company, Incorporated, 1st ed., 2019.

[15] P. Subramanyan, S. Ray, and S. Malik, "Evaluating the security of logic encryption algorithms," in *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pp. 137–143, 2015.

[16] M. Simon *et al.*, "Three-to-one analog signal modulation with a single back-bias-controlled reconfigurable transistor," *Nature communications*, 2022.

[17] J. Zhang, M. De Marchi, D. Sacchetto, P.-E. Gaillardon, Y. Leblebici, and G. De Micheli, "Polarity-controllable silicon nanowire transistors with dual threshold voltages," *IEEE Transactions on Electron Devices*, vol. 61, no. 11, pp. 3654–3660, 2014.

[18] N. Rangarajan, S. Patnaik, J. Knechtel, R. Karri, O. Sinanoglu, and S. Rakheja, "Opening the doors to dynamic camouflaging: Harnessing the power of polymorphic devices," *IEEE Transactions on Emerging Topics in Computing*, 2020.

[19] G. Galderisi, T. Mikolajick, and J. Trommer, "Reconfigurable field effect transistors design solutions for delay-invariant logic gates," *IEEE Embedded Systems Letters*, vol. 14, no. 2, pp. 107–110, 2022.

[20] S. Rai, S. Patnaik, A. Rupani, J. Knechtel, O. Sinanoglu, and A. Kumar, "Security promises and vulnerabilities in emerging reconfigurable nanotechnology-based circuits," *IEEE Transactions on Emerging Topics in Computing*, vol. 10, no. 2, pp. 763–778, 2022.

[21] J. Zhang, P.-E. Gaillardon, and G. De Micheli, "A surface potential and current model for polarity-controllable silicon nanowire fets," in *2015 45th European Solid State Device Research Conference (ESSDERC)*, pp. 48–51, IEEE, 2015.

[22] C. Roemer, G. Darbandy, M. Schwarz, J. Trommer, A. Heinzig, T. Mikolajick, W. M. Weber, B. Iñíguez, and A. Kloes, "Physics-based dc compact modeling of schottky barrier and reconfigurable field-effect transistors," *IEEE Journal of the Electron Devices Society*, vol. 10, pp. 416–423, 2021.

[23] W. Ni, Z. Dong, B. Huang, Y. Zhang, and Z. Chen, "A physic-based explicit compact model for reconfigurable field-effect transistor," *IEEE Access*, vol. 9, pp. 46709–46716, 2021.

[24] P. Cadareanu, J. Romero-Gonzalez, and P.-E. Gaillardon, "Parasitic capacitance analysis of three-independent-gate field-effect transistors," *IEEE Journal of the Electron Devices Society*, vol. 9, pp. 400–408, 2021.

[25] R. K. Brayton and A. Mishchenko, "ABC: an academic industrial-strength verification tool," in *CAV*, 2010.

[26] M. Soeken, H. Riener, W. Haaswijk, E. Testa, B. Schmitt, G. Meuli, F. Mozafari, and G. De Micheli, "The epfl logic synthesis libraries," *arXiv preprint arXiv:1805.05121*, 2018.

[27] S. Rai, M. Raitza, S. S. Sahoo, and A. Kumar, "Discern: Distilling standard-cells for emerging reconfigurable nanotechnologies," in *2020 Design, Automation Test in Europe Conference Exhibition (DATE)*, pp. 674–677, 2020.

[28] S. Rai, A. T. Calvino, H. Riener, G. D. Micheli, and A. Kumar, "Utilizing xmg-based synthesis to preserve self-duality for rfet-based circuits," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, pp. 1–1, 2022.

[29] S. Rai, M. Raitza, and A. Kumar, "Technology mapping flow for emerging reconfigurable silicon nanowire transistors," in *2018 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 767–772, 2018.

[30] G. Gore, P. Cadareanu, E. Giacomin, and P.-E. Gaillardon, "A predictive process design kit for three-independent-gate field-effect transistors," in *2019 IFIP/IEEE 27th International Conference on Very Large Scale Integration (VLSI-SoC)*, pp. 172–177, IEEE, 2019.

[31] A. Krinke, S. Rai, A. Kumar, and J. Lienig, "Exploring physical synthesis for circuits based on emerging reconfigurable nanotechnologies," in *2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD)*, pp. 1–9, 2021.

[32] S. Rai, A. Rupani, D. Walter, M. Raitza, A. Heinzig, T. Baldauf, J. Trommer, C. Mayr, W. M. Weber, and A. Kumar, "A physical synthesis flow for early technology evaluation of silicon nanowire based reconfigurable fets," in *2018 Design, Automation Test in Europe Conference Exhibition (DATE)*, pp. 605–608, 2018.

[33] Q. Alasad, J.-S. Yuan, and Y. Bi, "Logic locking using hybrid CMOS and emerging SiNW FETs," *Electronics*, vol. 6, no. 3, 2017.

[34] Q. Alasad, Y. Bi, and J.-S. Yuan, "E_2LEMI: Energy-efficient logic encryption using multiplexer insertion," *Electronics*, vol. 6, 2017.

[35] J. Rajendran, H. Zhang, C. Zhang, G. S. Rose, Y. Pino, O. Sinanoglu, and R. Karri, "Fault analysis-based logic encryption," *IEEE Transactions on Computers*, vol. 64, no. 2, pp. 410–424, 2015.

[36] M. Merten, S. Huhn, and R. Drechsler, "Quality Assessment of RFET-based Logic Locking Protection Mechanisms using Formal Methods," in *IEEE European Test Conference (ETS)*, pp. 1–2, 2022.

[37] R. Arora and M. Hsiao, "Enhancing SAT-based bounded model checking using sequential logic implications," in *International Conference on VLSI Design*, pp. 784–787, 2004.

[38] M. Merten, D. E. Mohammed, S. Huhn, and R. Drechsler, "SAT-based Key Determination Attack for Improving the Quality Assessment of Logic Locking Mechanisms," in *International Workshop on Boolean Problems (IWSBP)*, pp. 1–13, 2022.