Formal Analysis of Camouflaged Reconfigurable Circuits

Steffen Märcker, Michael Raitza, Shubham Rai, Giulio Galderisi,
Thomas Mikolajick, Jens Trommer and Akash Kumar
Technische Universität Dresden, Germany
E-mail: {steffen.maercker, michael.raitza, shubham.rai, akash.kumar}@tu-dresden.de
Namlab gGmbH, Germany
E-mail: {giulio.galderisi, thomas.mikolajick, jens.trommer}@namlab.com

***Abstract*—Reconfigurable field effect transistors are an emerging device technology. Reconfigurability between P- and N-type polarity and multiple (control) gates per device make them well suited for static and dynamic layout camouflaging as well as logic locking, watermarking and similar IP protection techniques. In contrast to classical transistors, the devices can provide fully symmetrical I-V characteristics between P- and N-type polarity with equal device geometry. In this paper, we explore logic gate variants and analyze their delay invariance using a fully automated design space exploration backed by probabilistic model checking. We evaluate how this invariance carries over to more complex combinational circuits and latches. Our analysis shows that effective camouflaging using reconfigurable logic gates is indeed achievable and identifies the most promising designs.**

***Index Terms*—Camouflaging, circuit analysis, device models, formal verification, reconfigurable logic, timing analysis**

I. Introduction

In our increasingly digitally driven world, computer systems face various threats not only at the software but also at the hardware level. Side-channel attacks and hardware trojans target the data and try to extract sensitive information such as encryption keys or manipulate the computation [1], [2]. Attacks on hardware designs aim to pirate the IP of components or to support the execution of other attacks. The attacker can be both an untrustworthy foundry or a customer of the chip. Several countermeasures have been proposed to hide the true functionality of a design: *Layout camouflaging* [3] uses special cell layouts that look identical for two or more logic functions. *Logic locking* [4], *delay locking* [5] and *split manufacturing* [6] use key bits to unlock the correct functionality. Keys are stored in tamper-proof memory or encoded in the back-end of line. *Wave Pipelining* [7] secretly spreads the computation of some signals over multiple clock cycles to camouflage the timing.

Circuits secured with these techniques can be attacked with SAT attacks, as they are an effective technique to derive the correct configuration, i. e., cell function, key bits, cell interconnects and timing constraints without complete knowledge of the physical design and secret keys [8], [9]. Since the complexity increases exponentially in the number of key bits and connections, an attacker aims to rule out impossible/improbable configurations in order to cut down the search space and to increase the chances of success. Besides logical analysis, the circuit's timing parameters can be analyzed and provoking timing violations through dysfunctional configurations by increasing the clock speed can yield additional information via timing error patterns. Thus, the most effective way to harden designs against SAT attacks is to increase the search space, i. e., the number of key bits, and to invalidate underlying assumptions of timing analysis [7].

First, the number of locked cells and thus key bits can be increased if circuit reconfiguration can be achieved with only little extra costs. Reconfigurable nano devices and especially reconfigurable field effect transistors (RFETs) lend themselves to this task, whereas classic CMOS designs bear significant overheads. Reconfiguration facilitates the implementation of two or more functions with the same cell layout which are selected by the key bits. This results in significantly less overhead while still achieving decent performance, see [10] for an overview. Second, the information gained from timing analysis and induced timing errors can be minimized if the reconfigurable logic cells do not show significant performance variations between their configurations. Hence, delay invariance for logic cell reconfiguration was identified as a desirable property [11]. It can also aid in delay locking, wave pipelining and hardening against side-channel attacks. Here, we focus on the delay invariance of RFET-based reconfigurable logic cells in the context of IP protection via logic locking.

1) Threat model: We assume an invasive attack where the attacker gets access to the locked/camouflaged netlist and identifies the primary and the key inputs either through imaging techniques or directly in the fab. He also has access to a functional chip, the so-called oracle, to conduct a SAT attack.

2) Contributions: In this paper, we show an investigation into hardening logic cells against delay variance that can be reconfigured between the basic logic functions NAND and NOR. We also take transistor device performance variations into consideration and show that certain designs show an outstanding resilience against high drain current variations. The identified designs are put to test in the C17 benchmark circuit and in SR latches to show the camouflaging effectiveness in larger combinational designs and in sequential circuits. Based on our

This research was supported in part by the German Research Foundation (DFG), Project DART (PN: 500109949) and Project SecuReFET (PN: 439891087) in the framework of a special priority program on Nano Security (SPP 2253). Thanks to Joram Brenz for supporting the experiments.

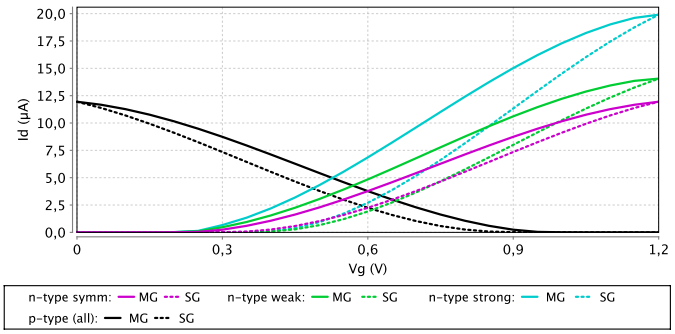

Fig. 1. I-V characteristics of 24 nm 3-gated GeNW RFETs with symmetric, weak and strong asymmetric currents. MG: middle gate SG: source (SB) gate

findings, we propose a new camouflage-able SR latch design that allows a configurable output polarity while maintaining a stable input sensitivity.

II. Device Model

A reconfigurable field effect transistor is a device with at least two gates that can be dynamically configured to either PMOS or NMOS operation mode using one of its gates, the so-called polarity control gate [12]–[14]. According to the selected mode, the remaining gates open the channel if and only if all of them are opened, i. e., they form a wired-AND which enables the compression of serial circuit paths [15], [16]. The two outer gates control the Schottky barriers (SB) whereas additional middle gates exploit thermal barriers. This results in devices that feature both high-V_T (steered at the source gate) and low-V_T (steered at the middle gate) switching characteristics as shown in the I-V Diagrams in Figure 1. This is typically achieved by an alignment of the Schottky contact metal work function close to the middle of the semiconductor band-gap. In contrast to classic CMOS technology, the transfer characteristics of the devices can be tuned during fabrication without changing the device geometry such that PMOS and NMOS currents are highly symmetric [17]. A fine-tuning of the symmetry can be done by strain-incorporation [18], [19]. However, due to process variability a certain unwanted symmetry might still be there in a given process.

In this paper, we consider a family of 24 nm Germanium-nanowire based devices with up to four gates. We use behavioral models [20] that are parametrized according to a projection of the FEM simulation of the device presented in [21]. Compared to [20], [22], we refined our model of this RFET family. Most importantly, the model now incorporates the increase of the channel resistance in the number of gates. This impacts the trade-off between low-V_T switching and the (increased) channel length. We also consider device performance variations and perform our investigations using three different devices, a fully symmetric, a weak asymmetric and a strong asymmetric device. Figure 1 shows the I-V characteristics of each variant.

In Section III, we analyze discretized charge-transport models of the circuits using probabilistic model checking [23] as proposed in [20], [22]. With this flow we explore a comprehensive set of circuit variants, verify their functional correctness, and query performance metrics, such as circuit delays, that are proven correct and accurate with respect to the model precision, instead of relying on simulation.

TABLE I
Relative comparison of NAND vs. NOR worst-case delay.

	Δ of worst-case delay in %					
	symm.		weak		strong	
Variant	rise/fall	WCD	rise/fall	WCD	rise/fall	WCD
2b [11]	0.9	0.0	1.1	0.0	1.5	0.9
2c [11]	0.0	0.0	0.0	0.0	0.0	0.0
1i	0.3	0.0	0.3	0.0	0.4	0.3
1s	0.3	0.0	0.3	0.3	0.3	0.3
2i	16.3	0.0	16.3	16.3	16.3	16.3
2s	20.3	0.0	20.2	12.8	20.2	20.2
3i	16.8	0.0	27.7	16.8	16.8	16.8
3s	32.9	0.0	35.5	19.4	32.9	32.9
4i	61.7	0.0	69.7	2.7	70.5	24.1
4s	58.0	0.3	68.2	6.6	69.0	21.0
5i	0.6	0.6	0.0	0.0	0.6	0.0
5s	16.1	0.6	15.6	15.6	15.6	15.6
6i	0.0	0.0	0.0	0.0	0.0	0.0
6s	16.1	0.0	16.1	16.1	16.1	16.1
7i	0.0	0.0	0.0	0.0	0.0	0.0
7s	0.0	0.0	0.0	0.0	0.0	0.0

III. Experiments

In this section we explore how reconfiguration, multiple-independent gates and PMOS/NMOS symmetry enable delay-camouflaged circuits. For this purpose, we focus on the 50-50 propagation delay, also worst-case delay (WCD), and assume an output load of $H = 1$. In our first experiment, we consider a logic cell that can be reconfigured between NAND and NOR, the two fundamental functions in logic design. We compare both configurations with respect to their WCD for all sensible implementations of such a reconfigurable cell.

In our second experiment, we consider the impact on a combinational circuit build of such cells, i. e., a circuit where each gate can be reconfigured between NAND and NOR. In our last experiment, we build reconfigurable latches from these cells and analyze their delay sensitivity to reconfiguration. In all our experiments, we drive the inputs to the circuits using artificial signals with a 1 ps slope. All experiments are performed for the three transistor devices shown in Figure 1.

A. Reconfigurable NAND-NOR

The 3-minority function characterizes circuits that can be configured to NAND or NOR via an input signal P:

$$\text{3-MIN}(P, A, B) = \overline{P} \wedge \text{NAND}(A, B) \vee P \wedge \text{NOR}(A, B).$$

This means, P selects between the cofactors NAND and NOR. We assume P and its inverse $\overline{P}$ will be connected directly to V_{DD} and V_{SS} as done in split manufacturing and logic locking. To protect gates connected to the supply voltages from surges/glitches, both are also provided via tie-cells in practice if necessary. Since 3-MIN is fully *self-dual*, its circuit implementations can exploit transistor reconfiguration using pass-gate transistors [20]. To achieve optimal performance in

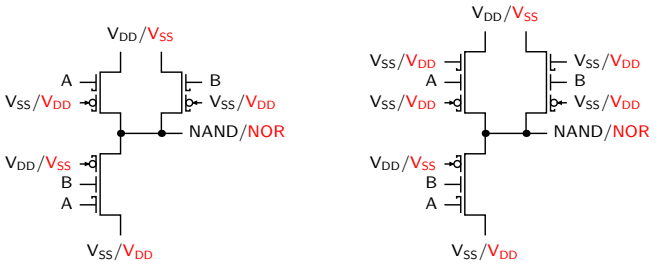

Fig. 2. 3-MIN variant 2s and fine-tuned variant 2b [11] demonstrating the benefit of using identical devices for camouflaging.

our application, these pass-gate transistors should be driven by P and $\overline{P}$, i. e., V_{DD} and V_{SS}. This is possible for all implementations that use only one input signal for transistor reconfiguration because 3-MIN is symmetric in all inputs. If a circuit requires an inverted signal other than $\overline{P}$, we integrate the necessary inverter into the cell to take its delay into account.

In our experiments, we consider all the principal implementation variants of 3-MIN using RFETs with up to 4 gates obtained from an automatic design space exploration as described in [20]. They differ in their topology (1–7) and whether inputs are connected only to the faster middle gates (i) or to the slower SB gates (s), too. For comparison, we add the designs (b) and (c) proposed in [11] which are variants of topology 2. In this paper, they are called 2b and 2c, respectively.

Table I pairs the NAND and NOR configuration of each implementation and lists the relative differences between their rise/fall delays and their WCDs. Each circuit is evaluated with the three device variants exhibiting symmetric, weak asymmetric and strong asymmetric drain currents. In the context of camouflaging, we focus on the delay difference between both configurations relative to their maximum delay rather than absolute values. Please refer to [24] for a much more detailed performance analysis of the circuits 1–7(i/s). We observe that all circuits exhibit virtually no difference between the WCD of NAND and NOR in the symmetric RFET scenario. This is expected, since the slowest (serial) branch is equally slow in PMOS and NMOS mode. However, in certain implementations (2, 3, 4, 5s, and 6s) the rise and fall delays differ up to 62 %. In these circuits, the pull-down network for NAND, which is pull-up for NOR, uses an RFET with at least one more gate than its counterpart. Drive strength differs significantly between these devices, which causes imbalances between both networks and hence asymmetry between NAND and NOR. This is most obvious when comparing 2s to 2b. Both are based on the same topology but the latter uses only 3-gated RFETs resulting in balanced networks, see Figure 2.

If the RFET's PMOS and NMOS modes are asymmetric, structural imbalances are emphasized, as shown in the weak and strong asymmetric columns in Table I. This affects the WCDs, because the different currents counteract imbalances in NAND configurations but increase them in NOR configurations. An attacker could exploit this in a timing violation attack. Implementations with no or only little imbalances (2b, 1i/s, and 5i) are not affected. Also, the fine-tuned variant 2c has only little advantage over its sibling 2b. Whether the imbalances of some circuits such as 5s or 6s can be leveled, too, is out of the scope of this paper.

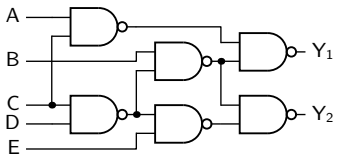

Fig. 3. C17 benchmark circuit [25] in NAND configuration

TABLE II
RELATIVE COMPARISON OF C17 NAND VS. C17 NOR WORST-CASE DELAY.

	Δ of worst-case delay in %					
	symm.		weak		strong	
Variant	rise/fall	WCD	rise/fall	WCD	rise/fall	WCD
2b [11]	7.2	0.0	11.4	2.3	12.1	3.4
2c [11]	7.0	0.0	13.0	1.2	14.0	6.9
2s	10.6	0.0	20.5	6.9	20.8	13.4
5i	1.3	0.0	3.4	3.4	3.4	3.4
6i	1.0	0.0	2.7	2.7	3.2	3.2
7i	1.9	0.0	4.6	3.6	10.0	10.0
7s	0.5	0.0	6.9	6.5	9.7	5.6

B. Reconfigurable Combinational Circuit

We use circuit C17 from the logic synthesis benchmark established in [25] to evaluate the 3-MIN cells in a combinational circuit. Due to space restrictions, we have to limit our presentation to a single circuit from the benchmark suite. We instantiate each C17 implementation with all gates configured once to NAND once to NOR. The analysis in [11] used logical effort [19] which gives high-level structural performance estimates. Here, we compute the actual end-to-end delays when capturing the whole C17 circuits as one large transistor circuit.

Table II shows the relative differences in rise/fall times and WCDs over all outputs for promising designs and 2s for comparison. If the transistors are perfectly symmetric, we notice no difference in the WCD of all circuits. However, a pronounced difference in the rise/fall delays can be spotted in 2b, 2c and even more in 2s. For asymmetric devices, the differences in rise/fall times increase and WCDs are also affected. As expected, 2s is most sensitive to the asymmetry with up to 21 % difference in rise/fall times and 13 % in the overall WCD. Surprisingly, 7i exhibits differences up to 10 % and 2c up to 7 %. The other variants are much less affected. Overall, except for variant 2s, these differences are smaller than the deviations that arise from using asymmetric devices compared to symmetric devices for both NAND and NOR. This means, any differences measured can also be attributed to production variations and hence, an attacker cannot draw firm conclusions about the configuration of the basic cells from the combinational circuit's WCD. As all configurations are similarly affected by timing-violation attacks, designers may pick the most suitable cell according to other relevant parameters like expected energy consumption or drive strength, without compromising the camouflaging.

C. Reconfigurable Latch

The reconfigurable 3-MIN circuit lends itself as an implementation vehicle for the latch, a ubiquitous component of VLSI designs. Reconfigurability between NAND and NOR enables the designer to disguise the latch's input sensitivity or, as we show with a new circuit design, store the register value inverted. For this investigation, we focus on hold delay differences rather than absolute performance. Still, our results show multiple viable implementations. The reconfigurable latch, just like the common implementations, uses two cross-coupled logic gates one of which is connected to S and Q_1 and the other to R and Q_2, see Figure 4. A program signal P is connected to the third input of both 3-MIN circuits and selects between NAND and NOR latch functionality and thereby changes the input sensitivity. So, when programmed the wrong way, the circuit will never actually store its input but will perform the opposite of set and reset or enter the forbidden state.

In the context of circuit camouflaging, one step of revealing the functionality of synchronous circuits is to look for hold violations in various configurations. Yet, camouflaging is most effective when different configurations all implement plausible or not-obviously-broken circuits. Thus, providing a latch that can camouflage its input sensitivity is a valuable prospect. Based on our findings for the 3-MIN circuit variants, we investigate the circuit behavior in the SR latch. Table III shows the most promising variants when implemented with the three different transistor devices. For a symmetric device, circuit topology does not matter much, yielding a wide range of implementation options. The weak asymmetric device favors the very small fully reconfigurable variant 1s and the partially reconfigurable variant 6s, which is also the best performing implementation for the strong asymmetric device. It turns out to be very resistant to device asymmetry.

D. 2-NMUX Latch

The previously shown latch design exchanges the illegal input combinations when being reconfigured with the one that stores the output value. As this almost always breaks the circuit function in obvious ways, it may not be the implementation of choice for camouflaging. The NMUX circuit, shown in Figure 4, can be used to solve this issue, since it can be rewritten as:

$$\mathrm{NMUX}(P,S,B) = \overline{P} \wedge \mathrm{NAND}(\overline{S},B) \vee P \wedge \mathrm{NOR}(S,B)$$

Used as a building block for an SR latch, it implements a high-active NAND latch in the configuration $P = 0$ and a high-active NOR latch for $P = 1$. This effectively yields a latch that stores its input either direct or inverted, but where the illegal input combination remains the same. Thus, circuit reconfiguration only inverts the output without affecting the controlling circuitry, yielding a plausible, but wrong, alternative implementation. Additionally, the S / R input is used direct and inverted in the transistor circuit, which means its logic can be inverted by exchanging the connections. Thus, the circuit can also be used to implement a low-active latch with similar performance characteristics.

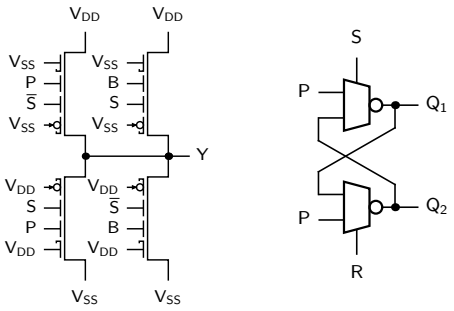

Fig. 4. NMUX circuit and its application in an SR latch. S / R selects between the "active" signal, represented by P, or the feedback, thus storing $\overline{\mathrm{P}}$.

TABLE III
HOLD TIME DIFFERENCES BETWEEN NAND- AND NOR-CONFIGURED SR LATCHES IMPLEMENTED WITH THREE DIFFERENT TRANSISTOR MODELS.

	symm.		weak		strong	
Variant	Δ_{ps}	$\Delta_{\%}$	Δ_{ps}	$\Delta_{\%}$	Δ_{ps}	$\Delta_{\%}$
2b [11]	0.0	0.0	1.9	5.3	2.0	6.5
2c [11]	0.0	0.0	1.9	4.7	2.1	6.0
1i	0.1	0.1	0.7	**0.9**	5.2	7.4
2i	0.0	0.0	3.8	9.6	4.1	11.9
2s	0.0	0.0	3.2	9.6	3.6	12.4
3i	0.0	0.0	4.7	9.3	5.1	11.6
4s	0.0	0.0	6.1	8.6	1.1	1.7
5i	0.0	0.0	4.9	9.7	5.3	12.0
6s	0.0	0.0	**0.5**	**0.9**	**0.5**	**1.1**
7i	0.0	0.0	5.8	9.4	6.4	11.9
NMUX	10.5	18.0	13.8	21.2	7.1	14.3

NMUX is not self-dual and, thus, does not make use of transistor-level reconfiguration and has only one principle implementation, but it benefits greatly from multi-gate devices. Its structure is similar to variant 2s with the added drawback that the inverter at the S / R input adds real cost. In Table III, the circuit shows significant imbalances between NAND and NOR operation. Still, by providing two plausible implementations, the circuit "only" incurs a performance penalty which can be worked around during VLSI design.

IV. Conclusion

We analyzed the delay invariance of all principle RFET-based implementations of logic cells reconfigurable between NAND and NOR. Delay invariant designs are achievable and deliver key bits for logic locking and camouflaging at only minor additional costs. These two properties are important to defend against SAT attacks, and RFETs enable practical implementations. Our end-to-end delay analysis of the C17 benchmark circuit has shown the impact of delay invariance on this combinational circuit. Lastly, we have demonstrated that delay invariant latches are achievable and that 2-NMUX is a promising candidate to improve the camouflaging of SR latches. In the future, we plan to address other reconfigurable circuits, like the 3-XOR, shown in [22], which is of great importance to computation-intensive and cryptographic circuits, for which effective camouflaging may be of even greater importance.

References

[1] P. C. Kocher, "Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems," in *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, N. Koblitz, Ed., ser. Lecture Notes in Computer Science, vol. 1109, Springer, 1996, pp. 104–113.

[2] L. Lin *et al.*, "Trojan side-channels: Lightweight hardware trojans through side-channel engineering," in *Cryptographic Hardware and Embedded Systems - CHES 2009, 11th International Workshop, Lausanne, Switzerland, September 6-9, 2009, Proceedings*, C. Clavier *et al.*, Eds., ser. Lecture Notes in Computer Science, vol. 5747, Springer, 2009, pp. 382–395.

[3] J. Rajendran *et al.*, "Security analysis of integrated circuit camouflaging," in *2013 ACM SIGSAC Conference on Computer and Communications Security, CCS'13, Berlin, Germany, November 4-8, 2013*, A. Sadeghi *et al.*, Eds., ACM, 2013, pp. 709–720.

[4] J. A. Roy *et al.*, "Ending piracy of integrated circuits," *Computer*, vol. 43, no. 10, pp. 30–38, 2010.

[5] Y. Xie *et al.*, "Delay locking: Security enhancement of logic locking against IC counterfeiting and overproduction," in *Proceedings of the 54th Annual Design Automation Conference, DAC 2017, Austin, TX, USA, June 18-22, 2017*, ACM, 2017, 9:1–9:6.

[6] K. Vaidyanathan *et al.*, "Building trusted ics using split fabrication," in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust, HOST 2014, Arlington, VA, USA, May 6-7, 2014*, IEEE Computer Society, 2014, pp. 1–6.

[7] G. L. Zhang *et al.*, "Timingcamouflage+: Netlist security enhancement with unconventional timing," *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, vol. 39, no. 12, pp. 4482–4495, 2020.

[8] J. Backes *et al.*, "The analysis of cyclic circuits with boolean satisfiability," in *2008 IEEE/ACM International Conference on Computer-Aided Design*, 2008, pp. 143–148.

[9] A. Chakraborty *et al.*, "Evaluating the security of delay-locked circuits," *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, vol. 40, no. 4, pp. 608–619, 2021.

[10] N. Kavand *et al.*, "Securing hardware through reconfigurable nano-structures," in *Proceedings of the 41st IEEE/ACM International Conference on Computer-Aided Design, ICCAD 2022, San Diego, California, USA, 30 October 2022 - 3 November 2022*, T. Mitra *et al.*, Eds., ACM, 2022, 130:1–130:7.

[11] G. Galderisi *et al.*, "Reconfigurable field effect transistors design solutions for delay-invariant logic gates," *IEEE Embed. Syst. Lett.*, vol. 14, no. 2, pp. 107–110, 2022.

[12] A. Heinzig *et al.*, "Reconfigurable silicon nanowire transistors," *Nano Letters*, vol. 12, no. 1, pp. 119–124, 2011.

[13] M. De Marchi *et al.*, "Polarity control in double-gate, gate-all-around vertically stacked silicon nanowire fets," in *Electron Devices Meeting, IEDM '12, 2012 IEEE Int.*, 2012, pp. 8–4.

[14] J. Zhang *et al.*, "Dual-threshold-voltage configurable circuits with three-independent-gate silicon nanowire fets," in *Circuits and Systems, ISCAS '13, IEEE Int. Symp.*, 2013, p. 2111.

[15] J. Trommer *et al.*, "Reconfigurable nanowire transistors with multiple independent gates for efficient and programmable combinational circuits," in *Proc. 2016 Design, Automation & Test in Europe Conf. & Exhib., DATE '16*, Mar. 2016, pp. 169–174.

[16] M. Simon *et al.*, "A wired-and transistor: Polarity controllable fet with multiple inputs," in *2018 76th Device Research Conf. (DRC'18)*, Jun. 2018, pp. 1–2.

[17] A. Heinzig *et al.*, "Dually active silicon nanowire transistors and circuits with equal electron and hole transport," *Nano Letters*, vol. 13, no. 9, pp. 4176–4181, 2013.

[18] T. Baldauf *et al.*, "Tuning the tunneling probability by mechanical stress in schottky barrier based reconfigurable nanowire transistors," *Solid-State Electronics*, vol. 128, pp. 148–154, 2017, Extended papers selected from EUROSOI-ULIS 2016.

[19] J. Trommer *et al.*, "Functionality-enhanced logic gate design enabled by symmetrical reconfigurable silicon nanowire transistors," *IEEE Transactions on Nanotechnology*, vol. 14, no. 4, pp. 689–698, 2015.

[20] M. Raitza *et al.*, "Quantitative characterization of reconfigurable transistor logic gates," *IEEE Access*, vol. 8, pp. 112 598–112 614, 2020.

[21] J. Trommer *et al.*, "Enabling energy efficiency and polarity control in germanium nanowire transistors by individually gated nanojunctions," *ACS Nano*, vol. 11, no. 2, pp. 1704–1711, 2017.

[22] M. Raitza *et al.*, "Exploring standard-cell designs for reconfigurable nanotechnologies: A formal approach," in *2022 Design, Automation & Test in Europe Conference & Exhibition, DATE 2022, Antwerp, Belgium, March 14-23, 2022*, C. Bolchini *et al.*, Eds., IEEE, 2022, pp. 23–28.

[23] M. Kwiatkowska *et al.*, "PRISM 4.0: Verification of probabilistic real-time systems," in *Proc. 23rd Int. Conf. on Computer Aided Verification, CAV '11*, vol. 6806, 2011, pp. 585–591.

[24] S. Rai *et al.*, "Discern: Distilling standard-cells for emerging reconfigurable nanotechnologies," in *Proc. 2020 Design, Automation & Test in Europe Conf. & Exhib., DATE '20*, IEEE, 2020, xx–yy.

[25] J. M. Matos *et al.*, "A benchmark suite to jointly consider logic synthesis and physical design," in *Proceedings of the 2015 Symposium on International Symposium on Physical Design, ISPD 2015, Monterey, CA, USA, March 29 - April 1, 2015*, A. Davoodi *et al.*, Eds., ACM, 2015, pp. 185–192.