

Hardware Security Challenges Beyond CMOS: Attacks and Remedies

Kaveh Shamsi*, Wujie Wen[†], and Yier Jin*

*Department of Electrical and Computer Engineering, University of Central Florida

[†]Department of Electrical and Computer Engineering, Florida International University
kaveh@knights.ucf.edu, wwen@fiu.edu, yier.jin@eecs.ucf.edu

Abstract—The globalization of Integrated Circuits (ICs) supply chain has raised security concerns on how to ensure the integrity and the trustworthiness of fabricated circuits. While existing attack and protection methods are developed for CMOS based circuits, the introduction of emerging transistors acts as a double-sided sword. The usage of emerging devices introduces new security issues which the attackers can leverage to launch hardware attacks. On the other hand, the unique properties of emerging devices also provides a great opportunity for defenders to develop innovative hardware security primitives and to construct resilient hardware platforms for cybersecurity. In this paper, we will summarize the previous work in both directions, attacks and remedies with a focus on the authors' previous work in this domain. We will also discuss the research trends so that the emerging devices can better help secure our computing systems, besides their roles in extending the Moore's Law.

I. INTRODUCTION

Maintaining device performance and integration density relative to Moore's law has been the main incentive for vast efforts in research and development on electron devices over the past decades. Researchers from academia and industry have developed numerous non-CMOS devices [1]. Although the mainstream role of CMOS cannot yet be replaced by any of the novel computing devices, there is the possibility that their capabilities can be exploited for special applications.

Therefore, research efforts that try to utilize non-conventional properties or develop novel VLSI design techniques for optimizing non-CMOS logic or memory circuits are quite prevalent in today's hardware and circuit design literature. The leading example among these applications is hardware based security. Hardware security in the context of emerging devices includes both, instances where the security and integrity of the system can be enhanced by the non-conventional capabilities, as well as cases where vulnerabilities arise from the non-CMOS device infrastructure.

In this paper we intend to present an overview of the state-of-art with respect to beyond CMOS devices in hardware security applications with a focus on the authors' previous research in this domain. The paper encapsulates two main circuit based security topics: 1) Side-channel attacks that directly relate to circuit architectures and data-dependent power-consumption profiles in conventional CMOS circuits. 2) Intellectual Property and integrated circuit integrity enhancement through circuit encryption and obfuscation techniques. The paper is organized in the following fashion. Section II presents a brief technical background of the nano-devices that are discussed throughout the paper as well as the device models

that are used. Section III presents work in the intellectual property (IP) protection domain using novel nano-transistors. Section IV discusses emerging device based side-channel resiliency improvement. The paper concludes with Section VI.

II. EMERGING DEVICES

This paper discusses both memory devices and logic devices. The state of emerging memory technologies is competitive to CMOS with a number of industries launching commercial beyond-CMOS memories, e.g., Spin Transfer Torque Magnetic Random Access Memories (STT-MRAMs).

STT-MRAMs: The spin-transfer torque (STT) process allows the polarity of nano-magnets to be altered through charge-current [2]. Furthermore the Giant Magnetoresistance effect causes a magnet-insulator-magnet nano-pillar to have different resistance levels based on the relative polarity of the two magnetic layers [2]. These two properties are exploited in STT-MRAMs, where a magnetic tunneling junction (MTJ) is switched through a charge current application that can alter its states, performing write operations to the memory. Reading the MTJ is performed by comparing its resistance to a reference resistance. Modern STT-MRAMs have access times of a few nanoseconds which is compatible with last-level SRAM caches.

With respect to transistor and logic technologies FinFET CMOS is the mainstream technology in deeply scaled geometries near 10nm [1]. Promising non-CMOS transistors that are referred to in this paper are listed as follows.

Tunneling FETs: Charge-transport through the channel in Tunneling-FETs (TFETs) is dominated by tunneling current. The highly asymmetric drain and source doping creates a tunneling barrier, allowing charge carriers to tunnel through the channel. A conceptual view of an N-TFET is depicted in Fig. 1a. Modulating the barrier thickness through the gate voltage creates a steep-slope sub-threshold operation reaching below the 60mV/decade theoretical limit of MOSFETs. This is the most promising feature of TFETs as it allows for voltage scaling while maintain low leakage operation. III-V TFETs show the highest saturation current due to the presence of high mobility carriers in III-V material. GaSb-InAs hetero-junction [3] TFETs and InAs homo-junction [4] TFETs are the dominant devices in the research domain. For our experiments we use a Verilog-A model from [3] for heterojunction TFETs and a model from [4] for homo-junction TFETs. The models are based on table-files extracted from TCAD simulations with the addition of parasitic capacitances and resistors.

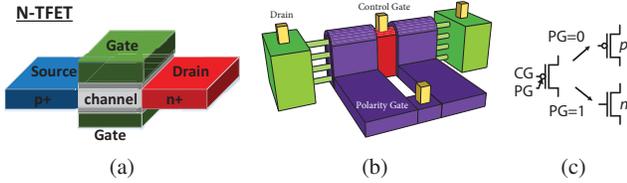


Fig. 1: (a) Tunnel FET conceptual view [7] vs. (b) Double-gate SiNWFET 3D structure (c) SiNWFET circuit symbol and polarity control.

Silicon nanowire FETs: Schottky barrier FETs were proposed originally to overcome the source/drain (D/S) ohmic contacts' conductance limitation in deeply scaled transistors. Recent research has revealed that by controlling the barrier heights at the metallic source and drain Schottky contacts both types of carriers can be injected into the channel. This allows the polarity of the transistor (p-type/n-type) to be altered dynamically. In this paper we utilize polarity control, Schottky barrier silicon nano-wire FETs (SiNWFET) [5]. A number of intrinsic Silicon nanowires are stacked vertically as the channel while gate-all-around (GAA) structures modulate conductance and polarity. Fig. 1b illustrates the 3D structure of the SiNWFET used throughout this paper. The double-GAAs in the D/S vicinity modulate the Schottky barrier heights and therefore control the polarity of the device. The control gate (CG) controls the conductance of the transistor similar to conventional MOSFETs. We use a Verilog-A model adopted from [5], [6] for the simulations in this paper. The model is calibrated to a 22nm process node with a 1.2V nominal voltage.

III. IP/IC PROTECTION

With the globalization of the IC supply chain, the fabless business model has dominated the state-side semiconductor industry where design and verification is decoupled from the fabrication facilities. A critical concern for many fabless design-houses is protecting their hardware intellectual properties (IP). Moreover, the success and advancement of reverse engineering techniques and industries intensifies the security and privacy concerns [8]–[10]. A number of different methods at the design stage have been proposed in literature for thwarting reverse engineering attacks on IP/IC. In this section we discuss how emerging nano-devices can contribute to more efficient implementations of circuit protection and obfuscation methodologies.

A. Polymorphic and Programmable Logic for Circuit Obfuscation

Logic-encryption is one of the main techniques for protecting hardware intellectual property [11]–[13]. The idea is to have a circuit produce incorrect results unless a certain “key” is loaded into the circuit. Formally a circuit $C(\vec{X})$ is transformed to $C(\vec{X}, \vec{K})$ such that $\exists \vec{K}_c^* \text{ s.t. } \forall \vec{X} C(\vec{X}, \vec{K}_c^*) = C(\vec{X})$. One method for logic encryption is to insert elements into the circuit to create additional inputs and then using the extra inputs as the key vector [11] to corrupt the output. Another

method is to replace parts of the circuit with polymorphic or programmable logic [12]. Polymorphic logic gates [14] can implement a number of different functionalities based on an additional input and can be programmed to one of their possible functionalities whereas fully programmable logic can implement any possible function with a fixed number of inputs. For instance, [14] presented gates that can change their functionality based on the supply voltage level.

In this work we discuss how basic logic blocks implemented using polarity-controllable FETs can be used to implement area efficient polymorphic or programmable functions with very low area overhead. Fig. 2.a demonstrates a NAND/NOR gate implementation in SiNWFET technology. The polarity gates are configured so that the pull-down network is programmed to NMOS logic while the pull-up circuit is PMOS. It can be seen that the structure is similar to a static CMOS NAND or NOR gate, however, the functionality can be altered through the supply pins without disrupting full-swing operation. The XOR/XNOR gate (Fig. 2.c) and the XOR/XNOR transmission block (Fig. 2.d) have a light-weight implementations in SiNWFET technology. Furthermore, a 3-input look-up-table (LUT) can be efficiently built with polarity control FETs as seen in Fig. 2.a. Table I demonstrates the design metric improvements for these blocks over CMOS counterparts.

B. Security Analysis

In order to provide a security analysis of the encrypted circuit we assume a threat-model widely used in the logic-encryption literature [9], [16]: An attacker can purchase an unlocked IC and use it to obtain correct input output pairs. The attacker can also delayer the chip and scan the circuit structure, therefore, the attacker has knowledge of the structure of the circuit. Given access to correct input-output pairs and the structure of the IC [9], [16] presented a SAT-based approach for finding the key in less than a minute even for large circuits. The SAT-based attack is based upon finding input patterns that would result in different outputs for different keys. These input patterns are referred to as *discriminating inputs*. Then the unlocked circuit is queried using the discriminating inputs, and the observations are recorded as constraints in a boolean satisfiability (SAT) problem. Once no more discriminating inputs can be found the key can be extracted from the SAT formula.

Although the SAT based attack proves to be very powerful, certain circuit structures demonstrate greater resiliency to the attack compared to others. For instance, a comparator that compares an input to a key value with a single output that transitions on a match, requires exponential number of input/output patterns with respect to the number of inputs in order to find the key. This is due to the fact that the output of the comparator only transitions when the key value is entered and therefore, most of the accumulated observations do not help the algorithm get closer to a correct key guess. Based upon this intuition, a SAT-resilient logic-encryption has to utilize structures with very low controllability at their outputs with respect to the key inputs. Such a structure implemented

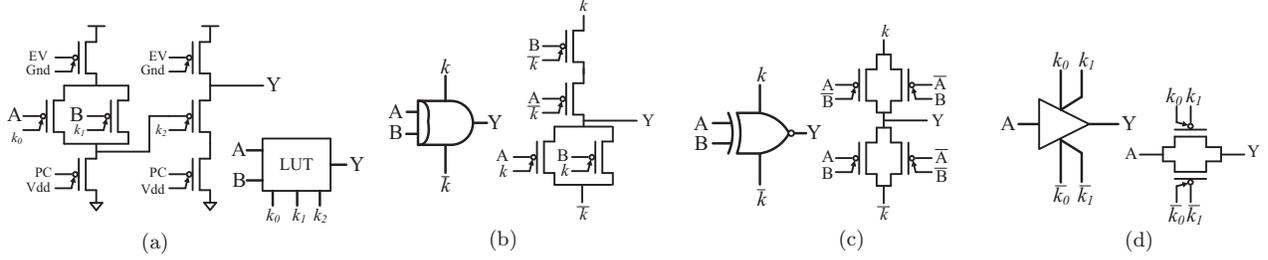


Fig. 2: (a) Mini-LUT with 3 key inputs [15] vs. (b) NAND/NOR gate (c) XOR/XNOR gate. (d) XOR/XNOR pass logic.

TABLE I: Simulation Results for NAND/NOR Gates

Gate	Static Power (pW)	Average Dynamic Power for output switching at 1GHz (uW)	Delay Averaged on different transitions (ps)
FinFET 22nm LSTP NOR	52.19	0.19	28
FinFET 22nm HP NOR	30360	0.67	23.5
FinFET 22nm LSTP NAND	27.19	0.15	23
FinFET 22nm HP NAND	1650	0.652	15.5
SiNWFET 20nm NAND/NOR	8.037	1.77	30
SiNWFET 20nm XOR/XNOR	48	0.58	8

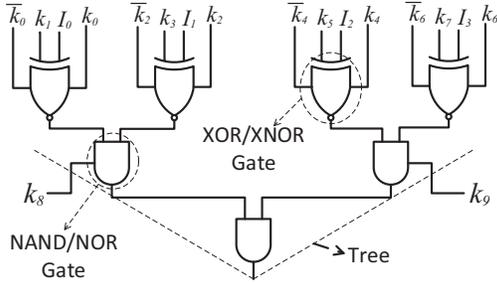


Fig. 3: XOR/XNOR based low-controllability structure. The tree gates can also be NAND/NOR which adds to the complexity

in SiNWFET technology is shown in Fig. 3 which is based on an AND-tree. We verify the resiliency of this structure by adding the circuit to a number of the ISCAS benchmarks and profiling a C++ implementation of a SAT logic-decryption algorithm. An AND-tree of more than 10 inputs proves sufficient resiliency against such attacks as seen in Fig. 4.

IV. SIDE CHANNEL ATTACKS

Given physical access to cryptographic hardware, side-channel information emitted from the integrated circuit can be used to break the encryption. Power side-channel attacks were presented in [17] and are based on measuring the real-time power consumption of a circuit implementation of an encryption algorithm and extracting the key based on this observation. Power side-channel attacks are surprisingly powerful against a myriad of different encryption algorithms.

During a power side-channel attack an attacker builds a set of hypothetical power consumptions for different keys or plain-

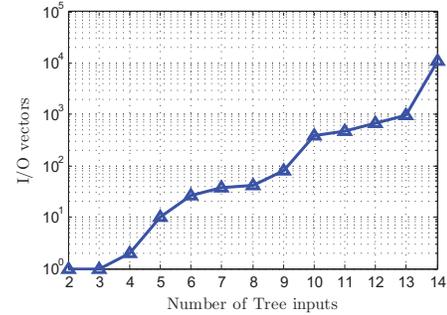


Fig. 4: SAT Based logic decryption complexity in terms of number of discriminating inputs required. Multiple trees with 16-inputs in a large circuit can effectively thwart the attack.

texts by analyzing the algorithm. Often times, the number of bit flips inside the circuit is analyzed to construct hypothetical power traces and then the measured power trace is correlated with the hypothesis to classify the computation and find the correct key. Therefore, power consumption that is related to the number of bit-flips is the source of the information leakage. In this section we examine circuit level design techniques that can help thwart power-analysis attacks.

A. CML Logic Circuits

Static CMOS logic design is based on pull-up and pull-down networks that drive a single ended output. The single-output nature of static CMOS logic results in data-dependent power consumption. If the output of the circuit makes a transition the power consumption is drastically different compared to when no transition occurs at the output. On the other hand, it is believed that double-ended CMOS logic styles as well as pre-charge logic styles are more resilient to DPA due to

the fact that the circuit consumes a certain amount of energy regardless of whether the output transitions or not. Current Mode Logic (CML) [18] is a constant power consumption logic style and Dynamic CML (DyCML) [19] is a pre-charge based logic style, both of which demonstrate extra resiliency against DPA.

CML circuits were originally used for noise-resistance high-speed communication interfaces due to their high switching speed and the fact that double-ended logic extends the noise-margin for signals [20]. However, the logic style was then adopted by researchers to reduce side-channel information leakage [21]. A generic CML gate and the voltage allocation are depicted in Fig. 5. A tail transistor is biased in saturation so that it operates as a current source. The unbalanced NMOS network routes this current to a pull-up network that comprises of resistive loads. The unbalance in the NMOS-tree causes all the current to switch to one branch causing the corresponding output to lower while the other output end is left high. The voltage difference at the output can be transferred to another differential gate allowing direct cascading of logic gates.

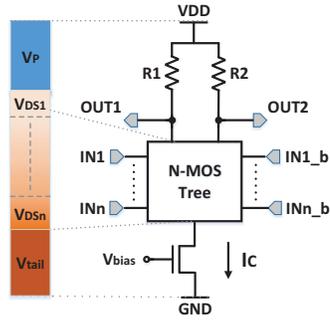


Fig. 5: CML gate and its voltage allocation [22].

B. CML Standard Cells with TFET and SiNWFET

Based on the described circuit structure the high and low voltage levels in the CML gate depend on the current source value as well as the resistive loads. The resistive loads are generally implemented using p-type FETs that are biased in the triode resistive region. Using p-type FETs allows the resistance to be tuned using the gate-bias as well as consuming less area than on-chip resistors with smaller process variation. Based upon these design guidelines, we developed a minimal standard library of CML gates using SiNWFETs and TFETs and 22nm FinFET. The gates were optimized for delay power product by tuning the current tail and the resistive load bias and the simulation results for the gates' design metrics can be seen in Fig. 10.

C. Security Analysis

In order to verify the security of the current mode gates we monitor the power profile of single gates through different input transitions. Fig. 8 depicts how the transient power consumption of the gates shows symmetric power consumption with little AC information in the power trace. Fig. 9

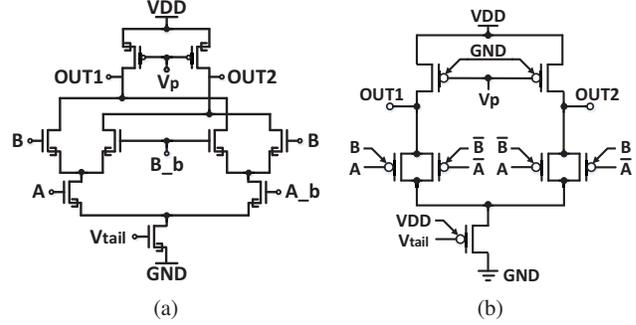


Fig. 6: CML XOR schematics using (a) TFET (b) SiNWFET [22].

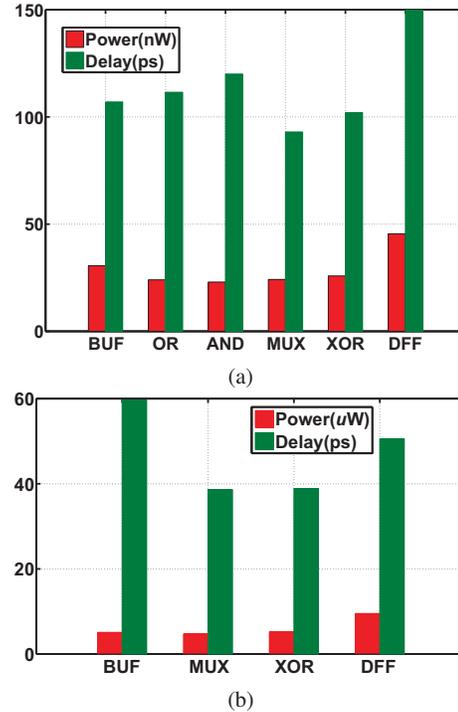


Fig. 7: Power and delay profiles of CML standard cells using (a) TFET (b) SiNWFET. [22]

demonstrates the power consumption of an 8-bit logic with respect to the number of bit-flips in the computation. It can be observed that while the power consumption of the static logic increases drastically with respect to the hamming weight, for CML logic the difference is quite smaller requiring extra accuracy. A case study of an entire cipher implementation of TFET CML is presented in [22].

V. SYMMETRIC OPERATION STT-MRAMS

Novel Non-volatile memory technologies have been on the rise over the past decade [23]. STT-MRAMs were successfully commercialized [2]. The ability to switch the magnetic orientation of the MTJ by passing charge current through it is key to the operation of STT-MRAMs. STT-MRAMs can be arranged in different configurations to build memory circuits. A common memory architecture is the 1Transistor-

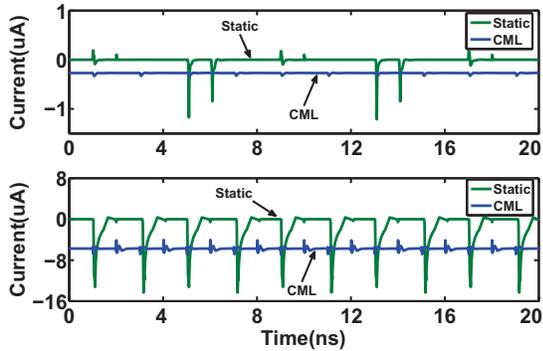


Fig. 8: The power traces between static XOR and CML XOR using TFET (top) and SiNW FET (bottom). [22]

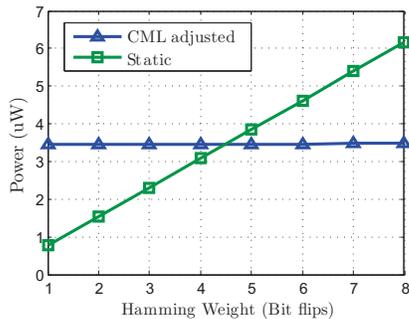


Fig. 9: Power difference with respect to hamming weight (number of bit-flips) for static and CML TFET.

1Resistor (1T-1R) architecture which is depicted in Fig. 10a. The 1T1R bit cells are arranged in a 2D grid where the BLs and SLs are connected together. By setting the BL/SLs to the corresponding data values and asserting a voltage on the WL a write operation can be performed. For read operations the WL is asserted and the BLs are routed to sense-amplifiers that detect the state of the cell by comparing its resistance to a reference value.

Inherent to the 1T1R architecture is asymmetric write performance for writing a ‘1’ or ‘0’. The asymmetry is primarily due to two factors: 1) The n-type transistor in the bitcell is under weak bias conditions when in one of the write cases while it operates with full V_{gs} in the other case. This is depicted in Fig. 10b; 2) The STT switching process is less efficient for the P→AP transition, therefore, a longer time or larger current is required for this transition. As both these processes are related to the device parameters it is rather difficult to control this asymmetry. Other solutions such as [24] rely on negative bit-line architectures. However, these architecture reduce the performance of the strong write operation to balance the write performance.

In this work we present how SiNWFET polarity controllable devices can be utilized for eliminating the weak-write scenario from the operation of STT-MRAMs [25]. If the n-type transistor is switched to p-type mode during the weak-write and the gate-voltage for the p-type device is set to 0 this will allow the p-type device to operate with full-bias.

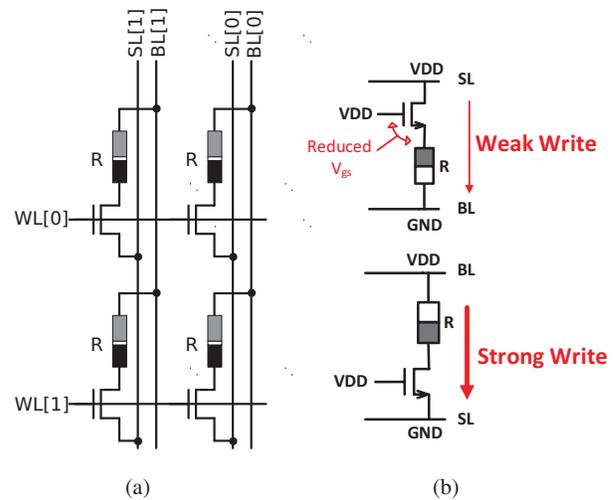


Fig. 10: (a) 1T1R STT-MRAM (b) Write asymmetry due to transistor bias degradation. [22]

This effectively eliminates the source-degeneration effect that degrades the weak write performance.

Although the dynamic configuration of the bit-cell transistor can improve the bottleneck of the write-time, it is difficult to implement such a switching style in a 1T1R architecture with a single supply. This is due to the fact that the WL is shared among bit-cells that are performing different write operations. It can be shown that no configuration of the BL/SL and WL of the the STT array can result in data-dependent polarity switching for each bit-cell.

While a single-step STT-MRAM cannot easily incorporate the polarity switching, double-step STT-MRAMs such as Multi-Level Cell (MLC) STT-MRAMs can adopt this scheme. MLC STT-MRAMs were built in [26] by stacking two MTJs in series creating 4 resistance states in the same cell. Fig. 11 depicts the operation of such a memory architecture in 2-steps with polarity control FETs. The 2-step process eliminates weak-writes and the performance improvements are reported in Table II. In addition to significant write performance improvements balanced write architectures can thwart power-side channel attacks on the memory.

VI. CONCLUSION

A set of emerging device based circuit design techniques where presented and evaluated to enhance the security of computing systems that utilize such devices. IP protection, side-channel attacks and dis-order based security are topics in the security domain that directly relate to circuit architectures. As for realization of these techniques seems that spin-based devices and low power transistor technologies are the most promising, and therefore, investigating their design techniques, and evaluating their use in non-conventional applications such as security is a reasonable investment.

REFERENCES

- [1] “International technology roadmap for semiconductors(itrs),” in <http://www.itrs.net>.

TABLE II: MLC STT-RAM single cell write comparison using different technologies and strategies

Technology	CMOS 45nm		FinFET 22nm		SiNW-FET			
					Polarity Switching		n-mode only	
	AP→P	P→AP	AP→P	P→AP	AP→P	P→AP	AP→P	P→AP
Transistor Area	90×45nm ²		2 fins		2 fins		2 fins	
Switching Time	2.83ns	37.4ns	2.5ns	14.4ns	2.24ns	6.47ns	2.24ns	31.7ns
WL Pulse Width	37.4ns	37.4ns	14.4ns	14.4ns	6.47ns	6.47ns	31.7ns	31.7ns
Write Energy	0.46pJ	2.03pJ	0.45pJ	1.41pJ	0.44pJ	0.88pJ	0.44pJ	2.6pJ
Average Current	119uA	57.3uA	133uA	69.8uA	146uA	98uA	146uA	57.3uA

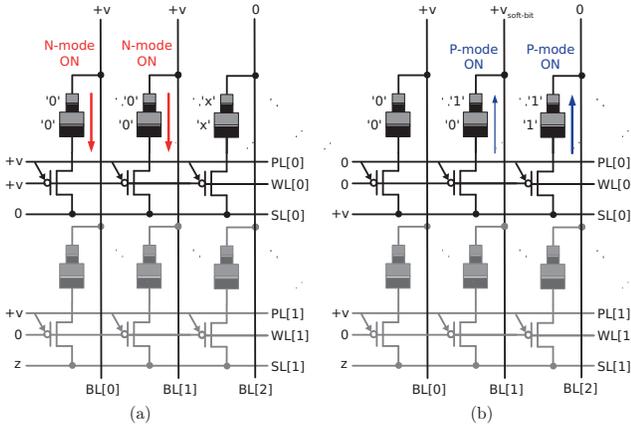


Fig. 11: (a) Write step-1 (b) Write step-2.

- [2] K. Roy, M. Sharad, D. L. Fan, and K. Yogendra, "Computing with spin-transfer-torque devices: Prospects and perspectives," *Very-large-scale integration (VLSI), 2014 IEEE International Symposium on*, July 2014.
- [3] G. Zhou, R. Li, T. Vasen, M. Qi, S. Chae, Y. Lu, Q. Zhang, H. Zhu, J.-M. Kuo, T. Kosel, M. Wistey, P. Fay, A. Seabaugh, and H. Xing, "Novel gate-recessed vertical inas/gasb tfets with record high ion of 180 $\mu\text{a}/\mu\text{m}$ at $v_{\text{ds}}=0.5$ v," in *Electron Devices Meeting (IEDM), 2012 IEEE International*, Dec 2012, pp. 32.6.1–32.6.4.
- [4] U. Avci, R. Rios, K. Kuh, and I. Young, "Comparison of performance, switching energy and process variations for the tfet and mosfet in logic," in *VLSI Technology (VLSIT), 2011 Symposium on*, June 2011, pp. 124–125.
- [5] M. De Marchi, D. Sacchetto, S. Frache, J. Zhang, P. Gaillardon, Y. Leblebici, and G. De Micheli, "Polarity control in double-gate, gate-all-around vertically stacked silicon nanowire fets," in *Electron Devices Meeting (IEDM), 2012 IEEE International*, Dec 2012, pp. 8.4.1–8.4.4.
- [6] J. Zhang, P.-E. Gaillardon, and G. De Micheli, "Dual-threshold-voltage configurable circuits with three-independent-gate silicon nanowire fets," in *Circuits and Systems (ISCAS), 2013 IEEE International Symposium on*, May 2013, pp. 2111–2114.
- [7] B. Sedighi, X. Hu, H. Liu, J. Nahas, and M. Niemier, "Analog circuit design using tunnel-fets," *Circuits and Systems I: Regular Papers, IEEE Transactions on*, vol. 62, no. 1, pp. 39–48, Jan 2015.
- [8] [Http://www.chipworks.com/](http://www.chipworks.com/).
- [9] P. Subramanian, S. Ray, and S. Malik, "Evaluating the security of logic encryption algorithms," in *Hardware Oriented Security and Trust (HOST), 2015 IEEE International Symposium on*. IEEE, 2015, pp. 137–143.
- [10] W. Li, A. Gascon, P. Subramanian, W. Y. Tan, A. Tiwari, S. Malik, N. Shankar, and S. Seshia, "Wordrev: Finding word-level structures in a sea of bit-level gates," in *Hardware-Oriented Security and Trust (HOST), 2013 IEEE International Symposium on*, 2013, pp. 67–74.
- [11] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, "Logic encryption: A fault analysis perspective," in *Proceedings of the Conference on Design, Automation and Test in Europe*, ser. DATE '12, 2012, pp. 953–958.
- [12] A. C. Baumgarten, "Preventing integrated circuit piracy using reconfigurable logic barriers," 2009.
- [13] F. Koushanfar and G. Qu, "Hardware metering," in *Design Automation Conference, 2001. Proceedings, 2001*, pp. 490–493.
- [14] A. Stoica, R. Zebulum, D. Keymeulen, M. Ferguson, and V. Duong, "Taking evolutionary circuit design from experimentation to implementation: some useful techniques and a silicon demonstration," *IEE Proceedings-Computers and Digital Techniques*, vol. 151, no. 4, pp. 295–300, 2004.
- [15] M. De Marchi, J. Zhang, S. Frache, D. Sacchetto, P.-E. Gaillardon, Y. Leblebici, and G. De Micheli, "Configurable logic gates using polarity-controlled silicon nanowire gate-all-around fets," *Electron Device Letters, IEEE*, vol. 35, no. 8, pp. 880–882, 2014.
- [16] M. El Massad, S. Garg, and M. V. Tripunitara, "Integrated circuit (ic) decamouffaging: Reverse engineering camouflaged ics within minutes," in *NDSS*, 2015.
- [17] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Advances in Cryptology – CRYPTO'99*, 1999, pp. 789–799.
- [18] M. Yamashina and H. Yamada, "An MOS current mode logic (MCML) circuit for low-power sub-ghz processors," *IEICE Trans. on Electronics*, vol. E75-C, no. 10, pp. 1181–1187, 1992.
- [19] M. Allam and M. Elmasry, "Dynamic current mode logic (DyCML): a new low-power high-performance logic style," *IEEE Journal of Solid-State Circuits*, vol. 36, no. 3, pp. 550–558, 2001.
- [20] A. Bellaouar, "Current mode logic gates for low-voltage high speed applications," Jul. 24 2001, uS Patent 6,265,898.
- [21] A. Cevrero, F. Regazzoni, M. Schwander, S. Badel, P. Ienne, and Y. Leblebici, "Power-gated mos current mode logic (pg-mcml): A power aware dpa-resistant standard cell library," in *Proceedings of the 48th Design Automation Conference*, ser. DAC '11, 2011, pp. 1014–1019.
- [22] Y. Bi, K. Shamsi, J.-S. Yuan, F.-X. Standaert, and Y. Jin, "Leverage emerging technologies for dpa-resilient block cipher design," in *2016 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2016, pp. 1538–1543.
- [23] *International Technology Roadmap for Semiconductors*, 2013 Edition. Emerging Research Devices.
- [24] D. Lee, S. K. Gupta, and K. Roy, "High-performance low-energy stt mram based on balanced write scheme," in *Proceedings of the 2012 ACM/IEEE international symposium on Low power electronics and design*. ACM, 2012, pp. 9–14.
- [25] K. Shamsi, Y. Bi, Y. Jin, P.-E. Gaillardon, M. Niemier, and X. S. Hu, "Reliable and high performance stt-mram architectures based on controllable-polarity devices," in *Computer Design (ICCD), 2015 33rd IEEE International Conference on*. IEEE, 2015, pp. 343–350.
- [26] T. Ishigaki, T. Kawahara, R. Takemura, K. Ono, K. Ito, H. Matsuoka, and H. Ohno, "A multi-level-cell spin-transfer torque memory with series-stacked magnetotunnel junctions," in *VLSI Technology (VLSIT), 2010 Symposium on*. IEEE, 2010, pp. 47–48.