electronics

MDPI

Article

Design of VGSOT-MTJ-Based Logic Locking for High-Speed Digital Circuits

Divyanshu Divyanshu, Rajat Kumar, Danial Khan, Selma Amara and Yehia Massoud *

Innovative Technologies Laboratories (ITL), King Abdullah University of Science and Technology (KAUST), Thuwal 23955-6900, Saudi Arabia
* Correspondence: yehia.massoud@kaust.edu.sa

Abstract: Emerging spintronics devices in recent research have received much interest in various fields. Their unique physical aspects are being explored to keep Moore's law alive. Therefore, the hardware security aspects of system-on-a-chip (SoC) designs using spintronics devices becomes important. Magnetic tunnel junctions (MTJ) are a potential candidate in spintronics-based devices for beyond-CMOS applications. This work uses voltage-gated spin-orbit torque-assisted magnetic tunnel junction (VGSOT-MTJ) based on the Verilog-A behavioral model to design a possible logic-locking system for hardware security. Compared with the SOT MTJ, which uses a heavy metal strip below the MTJ stack, VGSOT-MTJ has an antiferromagnetic (AFM) strip that utilizes the voltage-controlled magnetic anisotropy (VCMA) effect to significantly reduce the $J_{SOT,critical}$. To design the logic-locking block, we performed a Monte Carlo analysis to account for the effect of process variation (PV) on critical MTJ parameters. Eye diagram tests and mask designing were performed, which included the effect of thermal noise and PV for high-speed digital circuit operations. Finally, transient performance was analyzed to demonstrate the VGSOT-MTJ's ability to design logic-locking blocks from the circuit operation perspective.

Keywords: hardware security; magnetic tunnel junction (MTJ); spintronics; voltage-gated spin-orbit torque (VGSOT); voltage-controlled magnetic anisotropy (VCMA)

Citation: Divyanshu, D.; Kumar, R.; Khan, D.; Amara,S.; Massoud, Y. Design of VGSOT-MTJ-Based Logic Locking for High-Speed Digital Circuits. *Electronics* **2022**, *11*, 3537. https://doi.org/10.3390/electronics11213537

Received: 13 September 2022
Accepted: 26 October 2022
Published: 30 October 2022

1. Introduction

In the last two decades, unprecedented growth in embedded systems has globalized custom integrated circuit (ICs) design. The cost of creating and maintaining the cutting-edge facilities required to manufacture these devices has increased dramatically as technology has advanced. As a result, many design companies have gone fabless, heavily relying on untrusted and unaffiliated foundries to fabricate their ICs. This results in hardware security concerns and financial losses, as an unreliable foundry can lead to counterfeiting, reverse engineering, IC overbuilding, hardware Trojan insertion, or IP piracy [1,2]. Recently, advancement in various emerging technologies (spintronic devices, memristors, carbon nanotubes (CNTs), nanowire FETs (NWFETs), etc.) has played a vital role in improving the notion of beyond-CMOS applications. For instance, using spin as a state variable instead of charge for logic operations [3] and several other emerging spintronics phenomenon-based applications [4] have shown great potential in recent research. The general prospect of utilizing various spintronics phenomena for security is discussed in [5]. In the context of hardware security, logic locking is one of the promising obfuscation methodologies for next-generation hardware security [6]. Logic locking protects ICs from overbuilding and IP piracy by inserting a key along with the primary inputs to drive the design. A correct key ensures the functionality of the design, while the wrong key corrupts the functionality. The key is stored on the chip's tamper-proof memory for life and remains there even if the power is removed [7]. Figure 1 shows the basic overall flow of IC design in system-on-a-chip (SoC) design. The idea is to use a specialized foundry to insert a logic-locking

block during manufacturing to create a locked netlist. More details about key storage and protection are discussed in Section 3.1.

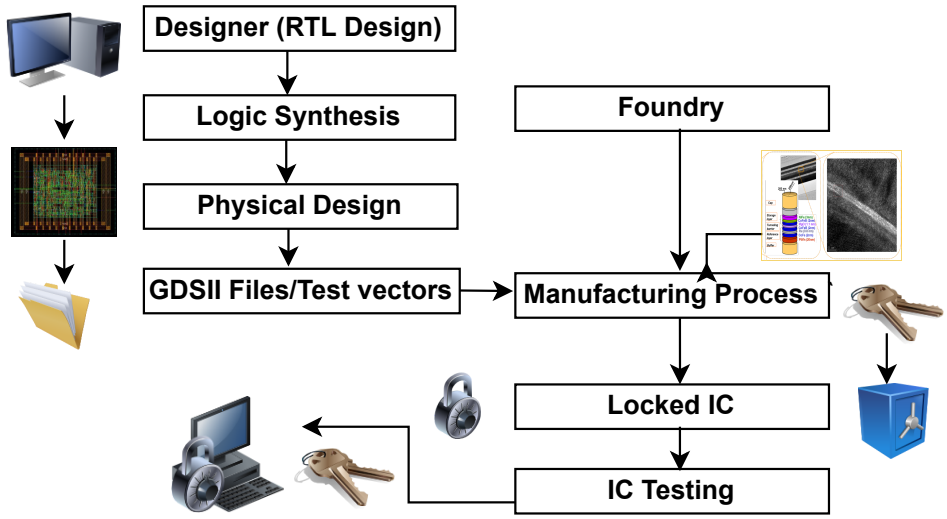


Figure 1. Overall IC design flow and logic locking with keys.

MTJs have been utilized in implementing many aspects of hardware security such as true random number generators (TRNG) [8], physically unclonable functions (PUF) [9], logic locking [10], hardware Trojans [11], etc. Spin torque effects, such as spin transfer torque (STT) and spin orbit torque (SOT), have significantly boosted the development of spintronics. Two terminal MTJs are electrically driven by STTs resulting from spin-polarized current pulses, where free layer (FL) magnetization is nearly collinear with the spin polarization [12]. Therefore, such torques are weak, and FL magnetization only absorbs the required switching energy. Consequently, two terminal STT-MTJ is slow due to its incubation time and energetically inefficient due to the large write current across the MTJ stack [13]. Recently, current-induced SOTs operating at low energy levels have been exploited for high-performance spintronic applications [14]. A three-terminal MTJ-SOT is fast and energy efficient with perpendicular-to-the-plane magnetization, where read and write paths are separated. This isolation significantly improves the device's reliability, since the write current flows through the heavy metal (HM) rather than the tunneling barriers, which are sensitive to electrical breakdown. Recent experiments have revealed that by replacing the HM with an antiferromagnetic (AFM) metal, field-free SOT switching can be achieved, since the AFM metal creates not only an SOT, but also provides an in-plane exchange bias (H_{EX}) [15]. Another emerging write mechanism is the voltage-controlled magnetic anisotropy (VCMA) effect, which, during switching, temporarily modulates the energy barrier when voltage is applied across the MTJ [16]. Recently, a new write mechanism, called voltage-gated SOT (VGSOT), has been introduced using the VCMA effect with AFM/FM/oxide structure to modulate the SOT current [17]. Reference [18] provides a comprehensive overview with all levels of hardware infrastructure for hardware security. The authors of [19] discuss the modeling of the VCMA-MTJ for high speed MRAM applications. By solving a modified Landau–Lifshitz–Gilbert (LLG) equation, the magnetic dynamics of the VCMA-MTJ's free layer are first investigated. A VCMA-MTJ electrical model is then built by integrating the Brinkman resistance model, Slonczewski STT model, VCMA effect, and tunnel magnetoresistance model. Finally, three MTJ switching strategies including STT-assisted thermally-activated VCMA, STT-assisted precessional VCMA, and precessional VCMA are investigated for MRAM applications.

This work explores a voltage-gated spin-orbit torque-assisted magnetic tunnel junction (VGSOT-MTJ) based on the Verilog-A behavioral model [20] to design a possible logic locking [6] system for hardware security. References [21–29] evaluate the performance

and reliability of CNT bundles for on-chip interconnect applications due to their large conductivity and current carrying capabilities. References [30–34] report modeling and minimizing on-chip inductive effects. Authors in [35] discuss a comprehensive model for the resistance in graphene nanoribbon (GNR) interconnects. One of our future goals is to explore spintronics devices for interconnects due to their low-power consumption, non-volatility, and competitive bit area cell. The rest of the paper is organized as follows. Section 2 demonstrates the proposed work based on VGSOT-MTJ. The experimental results are presented in Section 3. The paper is finally concluded in Section 4.

2. Proposed Work

2.1. Background of VGSOT-MTJ

The MTJ circuit can be utilized to perform logic operations and to implement polymorphic gates [16]. The ability to obtain polymorphic gate behavior allows the IC chip to have an extra layer of security. It becomes difficult to obtain exact an logic implementation by reverse-engineering the layout. The magnetic dynamics of the free layer are governed by the modified Landau–Lifshitz–Gilbert (LLG) equation [20]:

$$\begin{aligned}\frac{\partial \overrightarrow{m}}{\partial t} = &-\gamma \overrightarrow{m} \times \overrightarrow{H}_{eff}(\mathrm{V_{MTJ}}) + \alpha \overrightarrow{m} \times \frac{\partial \overrightarrow{m}}{\partial t} + \gamma \mathrm{H_{STT}^{DL}} \overrightarrow{m} \times \overrightarrow{m}_p \times \overrightarrow{m} + \gamma \mathrm{H_{STT}^{FL}} \overrightarrow{m} \times \overrightarrow{m}_p \\ &+ \gamma \mathrm{H_{SOT}^{DL}} \overrightarrow{m} \times \overrightarrow{m}_\sigma \times \overrightarrow{m} + \gamma \mathrm{H_{SOT}^{FL}} \overrightarrow{m} \times \overrightarrow{m}_\sigma \end{aligned} \quad (1)$$

$$\mathrm{H_{STT}^{DL}} = \frac{\hbar P J_{\mathrm{STT}}}{2e\mu_0 M_{\mathrm{S}} T_{\mathrm{SL}}} \quad (2)$$

$$\mathrm{H_{SOT}^{DL}} = \frac{\hbar \theta_{SH} J_{\mathrm{SHE}}}{2e\mu_0 M_{\mathrm{S}} T_{\mathrm{SL}}} \quad (3)$$

$$\vec{H}_{eff} = \vec{H}_{PMA} + \vec{H}_{VCMA} + \vec{H}_D + \vec{H}_{ex} + \vec{H}_{th} \quad (4)$$

$$R_{MTJ}(V_{MTJ}) = \frac{R_p\left[1 + \left(V_{MTJ}/V_h\right)^2 + TMR\right]}{1 + \left(V_{MTJ}^2/V_h^2\right) + TMR[0.5(1 + \cos\theta)]} \quad (5)$$

$$TMR_{\mathrm{Real}(V_{MTJ})} = \frac{TMR}{1+\left(V_{MTJ}^2/V_h^2\right)} \quad (6)$$

Here, $\overrightarrow{m}$ is the magnetization of the free layer, γ is the gyromagnetic ratio, μ_0 is the vacuum permeability, and $\overrightarrow{H}_{eff}$ is the effective magnetic field with different contributing terms such as perpendicular magnetic anisotropy (PMA), voltage-controlled magnetic anisotropy (VCMA), demagnetization field, exchange bias, and thermal noise, as shown in Equation (5). α is the Gilbert damping coefficient, P is the polarization factor, J_{STT} and J_{SHE} are the STT and SOT current densities applied to the MTJ device, $\overrightarrow{m}_p$ is the polarization direction of the spin current injected in the free layer by the STT, and $\mathrm{H_{SOT}^{FL}}$ and $\mathrm{H_{SOT}^{DL}}$ are the current-dependent proportionality constants for the FL torque and DL torque, respectively, of the SOT. $\overrightarrow{m}_\sigma$ is the pure spin current induced by the spin-orbit coupling, θ_{SH} is the spin Hall angle, T_{SL} is the free layer thickness, TMR is the tunnel magnetoresistance ratio of the MTJ when there is V_{MTJ} applied across the MTJ, and V_h is the applied voltage across the MTJ. θ is the angle between magnetization of the free layer and the fixed layer, and the other symbols have their usual meanings.

2.2. Design of Logic-Locking Block Using VGSOT-MTJ

Figure 2 shows a logical implementation of the AND/NAND gate based on a hybrid CMOS-MTJ approach. The gate can be used in the logic-locking mechanism for hardware security applications. The MOS logic consists of NMOS transistors MN11-MN13. Two complimentary three-terminal MTJs are present in both branches of the PCSA. A reset

signal is used to reset the MTJs to their default states. The write enable signal should be HIGH to write the MTJs with the key values. The write enable signal should be high when: (1) the clock pulse is LOW and (2) the reset signal is not HIGH. The reset path, read path, and write path of MTJs are highlighted in the circuit diagram. Figure 3 shows the logical AND operation obtained for the schematic of Figure 2 for both the VGSOT- and SOT-based MTJs for comparison. The fall time is more for VGSOT-MTJ, which is highlighted in the figure. The dotted region indicates the read interval for the logic state. Table 1 contains key parameters set during electrical simulation. Parameters such as Gilbert damping coefficient, saturation magnetization, etc. are MTJ technology parameters that depend on the material composition and the device parameters such as oxide-layer and free-layer thickness. AFM dimensions are masked and process design parameters can be adjusted. During process-variation simulation, the reference-point data must be selected so that the introduced deviation lies between the allowed range of operation in the compact model. The testing of parameters is thus limited by the degree of sophisticated modeling of the compact model. A more realistic and scaled compact model will therefore allow a better logic-locking system using MTJ devices.

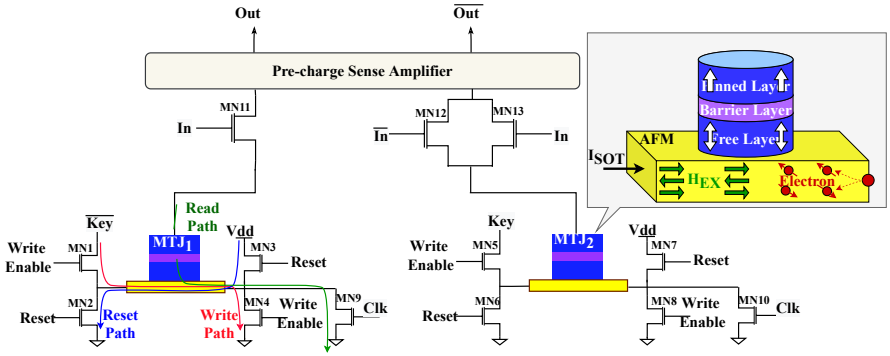


Figure 2. Logic-locking block schematic using VGSOT-MTJ.

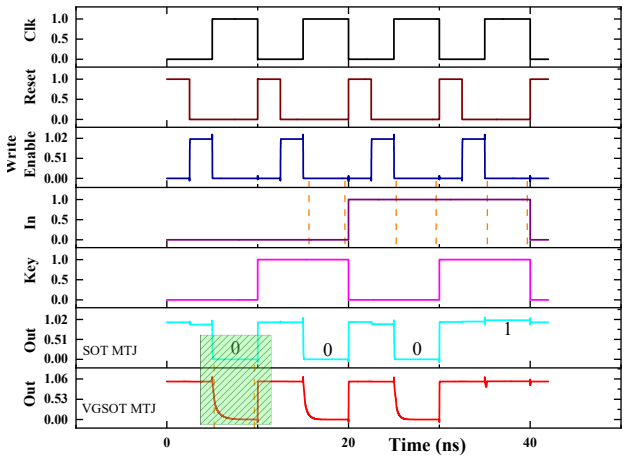


Figure 3. VGSOT and SOT logical AND operation block waveforms.

Table 1. MTJ parameters set during electrical simulation.

Parameter	Magnitude	Unit
MTJ dimension	50*50	nm
MTJ surface area	π*D^2/4	-
AFM dimension (L, W, H)	60*50*3	nm
Damping coefficient and TMR	0.05, 1.2	-
Oxide- and free-layer thickness	1.4, 1.1	nm
Saturation magnetization and H_{EX}	6.25*10^5, −50	A/m, Oe
Polarization factor and spin Hall angle	0.58, 0.25	-
VCMA coefficient	60	fJ/V.m
Gyromagnetic ratio	2.2127*10^5	m/(A.s)

3. Experimental Results

3.1. Logic-Locking Mechanism and Monte Carlo Simulations

We performed electrical simulations in a TSMC 40 nm CMOS generic process design kit using the Cadence spectre simulator with W/L ratio = 3, the temperature of 300 K,, and simulation steps of 1 ps. In Figure 4a, the designed logic-locking block is used to lock the netlist of the desired operation with Y = AB + BC + CA. The key is stored in tamper-proof memory and the correct logic is produced only when the correct key combination is inserted, as shown in Figure 4b. To account for the effect of process variation (PV) that may arise during fabrication and the robustness of the design, we performed 250 Monte Carlo (MC) simulations. Table 2 contains the variation data for both the MTJ of Figure 2 under the different values of PV and the obtained success ratio for the correct operation. The critical parameters such as TMR and free- and oxide-layer thickness were varied following a Gaussian distribution. With increasing process variations, the amount of standard deviation (SD) observed in MTJ resistance was increased, resulting in incorrect output. The low-discrepancy sequence (LDS) method was used during MC simulation, in which a deterministic sequence is used to obtain uniform coverage of the sampling space, and the convergence accuracy $\approx 1/pow(N, 2/3)$ is faster than the random sampling method, which has convergence accuracy = 1/sqrt(N).

Figure 5 shows the transient variation of MTJ_1 and MTJ_2 of the logic-locking block under the different PV values. A more significant deviation in the resistance value of MTJs due to PV can cause incorrect operation; thus, the tolerance to device imperfection needs to be considered. Table 3's data is taken from [20], which compares critical parameters for traditional SOT MTJ and VGSOT-MTJ. Thus, VGSOT switching requires less current and energy, but has more delay than traditional SOT MTJ. This delay in switching characteristics may cause a significant challenge in designing logic-locking blocks when operated in high-speed digital circuit operation. Thus, in this work, we focus more on analyzing the VGSOT-MTJ for high-speed circuits by using some standard circuit tests mentioned in Sections 3.2 and 3.3.

Table 2. 250 Monte Carlo simulation results (LDS method) for VGSOT-MTJ

PV	R_{MTJ1} SD(KΩ)	R_{MTJ2} SD(KΩ)	Success Ratio
5%	155.5	53.11	42.85%
10%	159.95	56.75	38.57%

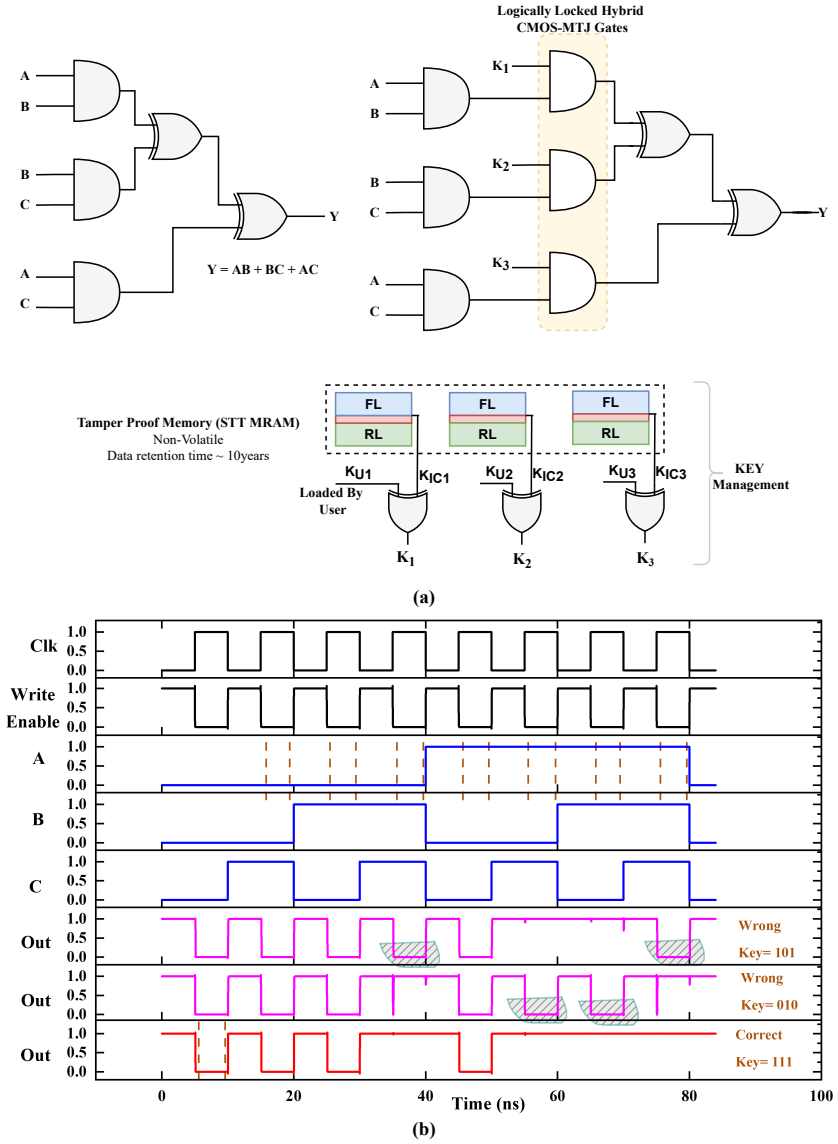
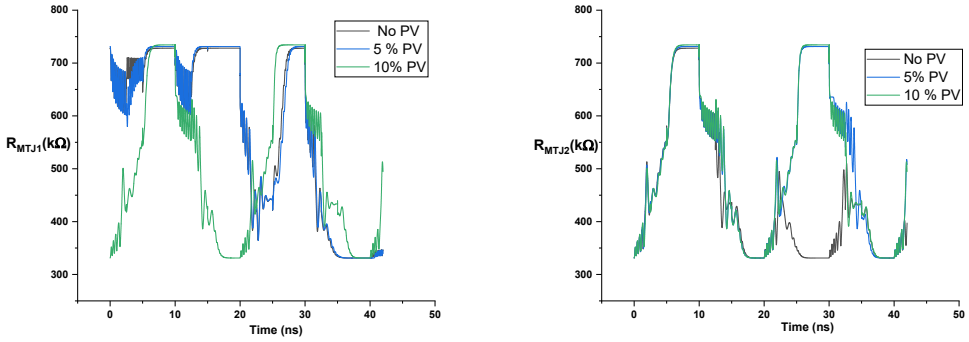


Figure 4. (**a**) Logic-locked netlist with keys. (**b**) Logic-lock operation with correct and incorrect key values with error highlighted.



(**a**) (**b**)

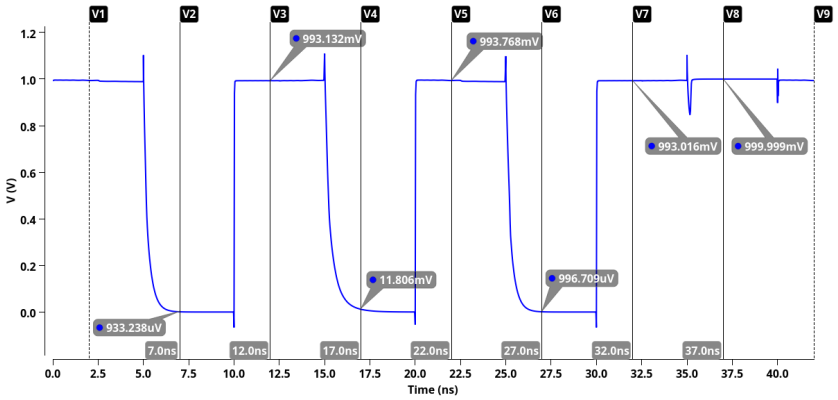
Figure 5. MTJ resistance variation for different PV % for (**a**) MTJ_1 and (**b**) MTJ_2.

Table 3. Performance comparison: SOT vs. VGSOT [20].

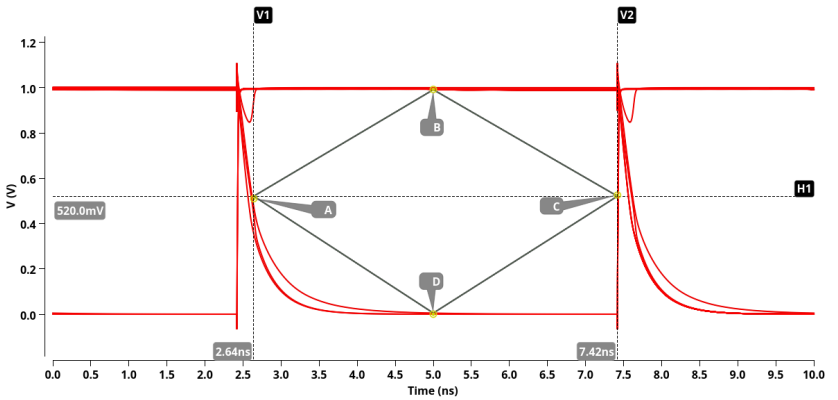
	Traditional SOT MTJ	VGSOT-MTJ
I_{SOT}	−98 uA	−6.2619 uA
Switching delay	2.5 ns	3 ns
Switching error rate	0.225	0
Switching energy	10.68 fJ/bit	0.08 fJ/bit

3.2. Eye Diagram: Mask Design and Optimization

In this work, we perform an eye-diagram analysis to check the quality of the signal in high-speed digital transmission. The logic-locking block must perform satisfactorily in high-speed transmission to ensure proper operation. In the eye diagram test, the signal is split into sections, which are overlaid on top of each other, giving information about the distribution of the timing of the transitions between the Low and High levels. Eye Diagram analysis helps keep track of some crucial parameters such as signal duration, synchronization with the system clock pulse, noise effect, undershoot and overshoot, etc. If any of the parameters are degraded, the eye-opening is affected and, thus, eye-mask tests become difficult to perform. In Figure 6a, the one-cycle operation of the logic-locking block is split into several sections with a unit interval (UI) of 5 ns to capture the transitions properly. V1 (at 2 ns) represents the start of the interval and V9 (at 42 ns) represents the end.



(**a**)



(**b**)

Figure 6. (**a**) Defining UI for the logic-locking block. (**b**) Obtained eye diagram for Case 1.

A centered eye-diagram was created as shown in Figure 6b, highlighted in red. The eye period is set to $2 * UI = 10$ ns and the threshold is at 520 mV. To evaluate the performance,

the eye diagram is tested across the following eye masks: HDMI compliance, HDMI 2.0 TP2EQ (data rate 3.4G to 3.712G and 5.94G to 6G), MIPI M-phy R_x and T_x compliance, PCI express Gen 3 compliance, and SFP + PCB compliance. The logic-locking block did not pass any of the masks mentioned. Thus, a personalized diamond-shaped mask was created as shown in Figure 6b. The vertices are marked from A to D.

When the effect of thermal noise (NON = 1) on eye parameters is included, the mask designed fails due to the shifting of the eye diagram, as shown in Figure 7a. A detailed eye diagram analysis was performed to account for the effect of process variation (uniform distribution and Gaussian distribution) and the effect of thermal noise, and an optimized eye mask was created with vertices A (2.72 ns, 520 mV), B (5 ns, 985 mV), C (7.4 ns, 520 mV), and D (5 ns, 10 mV), as shown in Figure 7b. The eye performance metrics were calculated; the data are tabulated in Table 4 using the NRZ (non-return to zero) modulation scheme. The eye performance was measured in five different cases, which included different PV with different types of random variation (RV)(RV = 0 is for constant device parameters, RV = 1 is for a uniform distribution of parameters, and RV = 2 is for a Gaussian distribution) in the MTJ parameters such as TMR ratio, free- and oxide-layer thickness, and effect of thermal noise (NON). All simulations were performed considering the effect of VCMA and the exchange bias field, as described in Equations (1)–(4). Equations (7)–(9) represents some of the equations used for calculating the metrics of Table 4. More details on parameter evaluation are available in the Cadence manual.

$$\text{Random Jitter} : \sqrt{\sum_i p_i (x_i - \mu)^2} \tag{7}$$

$$\text{Eye S/N} : \text{(Level1 Mean} - \text{Level 0 Mean) / (Level 1 SD} + \text{Level 0 SD)} \tag{8}$$

$$\text{Eye Height = (Level 1 Mean -3* Level 1 SD)} - \text{(Level 0 Mean + 3* Level 0 SD)} \tag{9}$$

where μ is the mean of the histogram distribution of the crossing point at the threshold value (here 20% threshold), x is the value on the x-axis from the tail of the distribution, and p is the value of the corresponding height of the histogram. SD stands for standard deviation.

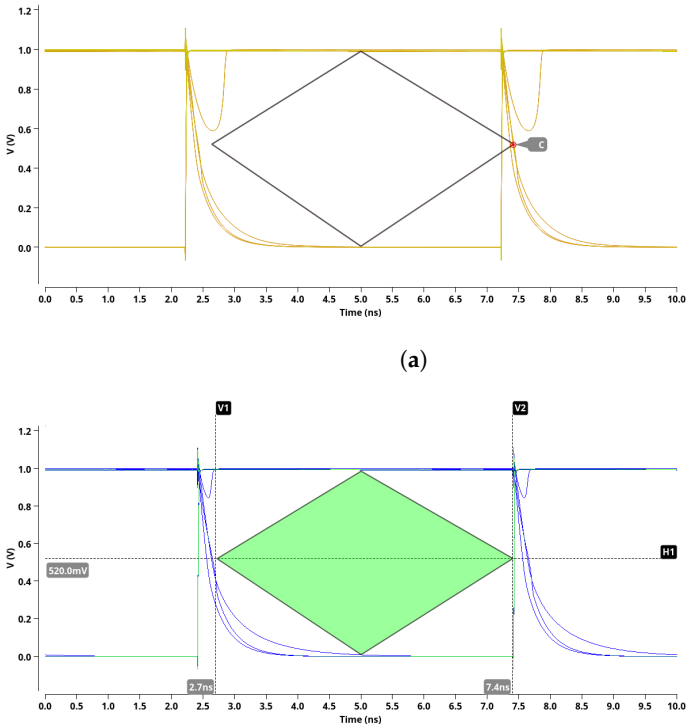


Figure 7. (**a**) Eye mask designed for Case 1 failed when NON = 1. (**b**) Optimized eye diagram to counter the effect of PV and the thermal effect.

Table 4. Eye diagram performance results for NRZ modulation.

Parameters	Case 1 (PV = 0, NON = 0, RV = 0)	Case 2 (PV = 0 , NON = 1, RV = 0)	Case 3 (PV = 3% , NON = 0, RV = 1)	Case 4 (PV = 3%, NON = 1, RV = 1)	Case 5 * (PV = 3%, NON = 1, RV = 2)
Level 0: Mean	7.573 mV	4.782 mV	6.216 mV	12.44 mV	12.96 mV
Level 0: SD	8.744 mV	5.099 mV	6.709 mV	10.51 mV	15.72 mV
Level 1: Mean	994.3 mV	994.3 mV	994.3 mV	994.6 mV	994.3 mV
Level 1: SD	2.804 mV	2.74 mV	3.042 mV	2.702 mV	2.77 mV
Eye Amplitude	986.8 mV	989.5 mV	988.1 mV	982.2 mV	981.3 mV
Eye height	952.1 mV	966 mV	958.8 mV	942.6 mV	925.9 mV
Eye width	4.513 ns	4.504 ns	4.366 ns	4.436 ns	4.423 ns
Eye S/N	85.45	126.2	101.3	74.34	53.08
Eye rise time	14.01 ps	14.05 ps	14.03 ps	13.93 ps	13.93 ps
Eye fall time	364.2 ps	361.2 ps	379.2 ps	432.7 ps	398.2 ps
Random jitter	53.80 ps	54.84 ps	78.84 ps	61.56 ps	64.87 ps
Deterministic jitter	164.3 ps	166.7 ps	161.2 ps	194.4 ps	188.2 ps

Case 5 *-Due to significant variation in resistance, the success ratio is less than 100%. The worst case is considered for successful simulation only.

3.3. Transient Measurements

Transient measurements are critical in evaluating circuit designs. In Table 5, the transient measurement data are tabulated where 20% and 80% thresholds with respect

to the baseline and top line are used. Electrical simulations are performed for the five cases, and important transient parameters are calculated to evaluate the performance of the logic-locking block. Due to the parameter variation, we observe a slight variation in some of the transient behavior, indicating that the selected MTJ can show tolerance to a certain extent for any practical applications. Figure 8 shows the transient capture of the data for Case 2.

Table 5. Data for transient measurement under various conditions.

Parameters	Case 1	Case 2	Case 3	Case 4	Case 5 *
Average rise time	14.04 ps	14.04 ps	14.04 ps	14.03 ps	14.04 ps
Average fall time	359.96 ps	386.06 ps	382.96 ps	451.17 ps	404.16 ps
Undershoot	6.30%	6.30%	6.29%	6.32%	6.30%
Overshoot	10.91%	10.87%	10.91%	10.91%	10.97%
Average slew rate—rising edge	42.56 V/ns	42.56 V/ns	42.56 V/ns	42.60 V/ns	42.56 V/ns
Average slew rate—falling edge	1.68 V/ns	1.57 V/ns	1.58 V/ns	1.38 V/ns	1.54 V/ns
Duty cycle (first cycle)	51.70%	51.66%	51.71%	52.15%	51.79%
RMS value	802.4 mV	801.2 mV	802.9 mV	803.7 mV	803.1 mV

Case 5 *-Due to significant variation in resistance, the success ratio is less than 100%. The worst case is considered for successful simulation only.

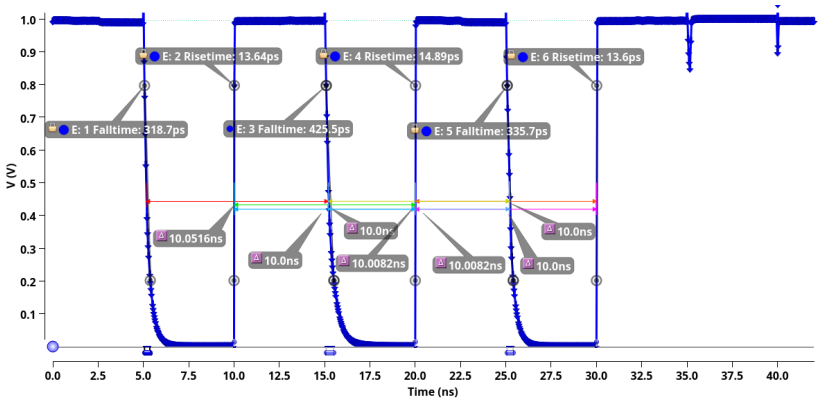


Figure 8. Transient calculation performed on the logic lock block output (Case 2).

4. Conclusions

As SoC design flow depends on multiple untrusted entities to reduce the time to produce ICs, securing hardware becomes a challenge. The challenge increases if the attacker intelligently utilizes emerging devices in the SoC design flow. With the development of fabrication abilities beyond CMOS devices, one cannot simply ignore the importance of such devices for defense, attack mechanisms, and hardware security. In this work, we used VGSOT-MTJ because it is a three-terminal structure offering certain advantages such as high endurance, separate read and write paths, etc. Additionally, it has better switching characteristics in terms of energy and error rate compared to the traditional SOT-MTJ. However, it has poor switching delay, which could be a potential challenge for designing a better logic-locking block using MTJ, especially in high-speed digital circuits. In this paper, we investigated how PV can affect simulations by using standard MC simulations. Furthermore, thermal noise can be tolerated and the optimized eye-mask diagram is designed to ascertain the proper range of operation for the block. Transient simulations are

performed considering some critical points in the VGSOT-MTJ model. This work addresses the challenges in designing the logic-locking block from the circuit-design perspective of high-speed digital circuits. However, the current work does not address how secure this structure is to intelligent attacks based on algorithms, side-channel attacks, etc. The performance of the proposed design for such attacks can be analyzed in future work.

Author Contributions: Conceptualization, D.D.; methodology, D.D. and R.K.; software, D.D. and R.K.; validation, D.D., R.K., D.K., and Y.M.; formal analysis, D.D.; investigation, D.D., R.K., and D.K.; resources, D.K., S.A., and Y.M.; data curation, D.D. and R.K.; writing—original draft preparation, D.D. and D.K.; writing—review and editing, D.K. and S.A.; visualization, D.D. and R.K.; supervision, Y.M.; project administration, Y.M.; funding acquisition, Y.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hu, W.; Chang, C.-H.; Sengupta, A.; Bhunia, S.; Kastner, R.; Li, H. An Overview of Hardware Security and Trust: Threats, Countermeasures, and Design Tools. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2021**, *40*, 1010–1038.
2. Chakraborty, A.; Jayasankaran, N.G.; Liu, Y.; Rajendran, J.; Sinanoglu, O.; Srivastava, A.; Xie, Y.; Yasin, M.; Zuzak, M. Keynote: A Disquisition on Logic Locking. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2020**, *39*, 1952–1972.
3. Srinivasan, S.; Sarkar, A.; Behin-Aein, B.; Datta, S. All-Spin Logic Device With Inbuilt Nonreciprocity. *IEEE Trans. Magn.* **2011**, *47*, 4026–4032.
4. Mishra, R.; Yang, H. Emerging Spintronics Phenomena and Applications. *IEEE Trans. Magn.* **2021**, *57*, 1–34.
5. Ghosh, S. Spintronics and Security: Prospects, Vulnerabilities, Attack Models, and Preventions. *Proc. IEEE* **2016**, *104*, 1864–1893.
6. Kamali, H.M.; Azar, K.Z.; Farahmandi, F.; Tehranipoor, M. Advances in Logic Locking: Past, Present, and Prospects. *Future Hardware Security Research Series.* **2022.**
7. Limaye, N.; Kalligeros, E.; Karousos, N.; Karybali, I. G.; Sinanoglu, O. Thwarting All Logic Locking Attacks: Dishonest Oracle With Truly Random Logic Locking. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2021**, *40*, 1740–1753.
8. Onizawa, N.; Mukaida, S.; Tamakoshi, A.; Yamagata, H.; Fujita, H.; Hanyu, T. High-Throughput/Low-Energy MTJ-Based True Random Number Generator Using a Multi-Voltage/Current Converter. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2020**, *28*, 2171–2181.
9. Divyanshu, D.; Kumar, R.; Khan, D.; Amara, S.; Massoud, Y. Physically Unclonable Function using GSHE driven SOT assisted p-MTJ for next generation hardware security applications. *IEEE Access* **2022**, *10*, 93029–93038.
10. Divyanshu, D.; Kumar, R.; Khan, D.; Amara, S.; Massoud, Y. Logic Locking Using Emerging 2T/3T Magnetic Tunnel Junctions for Hardware Security. *IEEE Access* **2022**, *10*, 102386–102395.
11. Kumar, R.; Divyanshu, D.; Khan, D.; Amara, S.; Massoud, Y. Spin Orbit Torque-Assisted Magnetic Tunnel Junction-Based Hardware Trojan. *Electronics* **2022**, *11*, 1753.
12. Kazemi, M.; Rowlands, G.E.; Ipek, E.; Buhrman, R.A.; Friedman, E.G. Compact Model for Spin–Orbit Magnetic Tunnel Junctions. *IEEE Trans. Electron Devices* **2016**, *63*, 848–855.
13. Wang, Z.; Zhou, H.; Wang, M.; Cai, W.; Zhu, D.; Klein, J.O.; Zhao, W. Proposal of Toggle Spin Torques Magnetic RAM for Ultrafast Computing. *IEEE Electron Device Lett.* **2019**, *40*, 726–729.
14. Lee, S.-W.; Lee, K.-J. Emerging three-terminal magnetic memory devices. *Proc. IEEE* **2016**, *104*, 1831–1843.
15. Liu, Y.; Zhou, B.; Zhu, J.-G. Field-free magnetization switching by utilizing the spin Hall effect and interlayer exchange coupling of iridium. *Sci. Rep.* **2019**, *9*, 325.
16. Zhang, H.; Kang, W.; Wang, L.; Wang, K.L.; Zhao, W. Stateful reconfigurable logic via a single-voltage-gated spin Hall effect driven magnetic tunnel junction in a spintronic memory. *IEEE Trans. Electron Devices* **2017**, *64*, 4295–4301.
17. Lee, K.; Kan, J.; Kang, S.H. Spin-orbit-torque magnetoresistive random access memory with voltage-controlled anisotropy. U.S. Patent No 9,589,619, 7 March 2017.
18. Bhunia, S.; Tehranipoor, M. *Hardware Security: A Hands-On Learning Approach*, 1st ed.; Computer and Technology: Cambride, United States, 2019.
19. Kang, W.; Ran, Y.; Zhang, Y.; Lv, W.; Zhao, W. Modeling and Exploration of the Voltage-Controlled Magnetic Anisotropy Effect for the Next-Generation Low-Power and High-Speed MRAM Applications. *IEEE Trans. Nanotechnol.* **2017**, *16*, 387–395.
20. Zhang, K.; Zhang, D.; Wang, C.; Zeng, L.; Wang, Y.; Zhao, W. Compact Modeling and Analysis of Voltage-Gated Spin-Orbit Torque Magnetic Tunnel Junction. *IEEE Access* **2020**, *8*, 50792–50800.
21. Massoud, Y.; Nieuwoudt, A. Modeling and design challenges and solutions for carbon nanotube-based interconnect in future high performance integrated circuits. *Acm J. Emerg. Technol. Comput. Syst.* **2006**, *2*, 155–196.

22. Nieuwoudt, A.; Massoud, Y. Predicting the Performance of Low-Loss On-Chip Inductors Realized Using Carbon Nanotube Bundles. *IEEE Trans. Electron Devices* **2008**, *55*, 298–312.
23. Massoud, Y.; Ismail, Y. Grasping the Impact of On-Chip Inductance in High Speed ICs. *IEEE Circuits Devices Mag.* **2001**, *17*, 14–21.
24. Eachempati, S.; Nieuwoudt, A.; Gayasen, A.; Narayanan, V.; Massoud, Y. Assessing Carbon Nanotube Bundle Interconnect for Future FPGA Architectures. In Proceedings of the IEEE Design Automation and Test in Europe, Nice, France, 16–20 April 2007.
25. Nieuwoudt, A.; Ragheb, T.; Nejati, H.; Massoud, Y. Increasing Manufacturing Yield for Wideband RF CMOS LNAs in the Presence of Process Variations. In Proceedings of the IEEE Symposium on Quality Electronic Design, Washington, DC, USA, 26–28 March 2007.
26. Nieuwoudt, A.; Mondal, M.; Massoud, Y. Predicting the Performance and Reliability of Carbon Nanotube Bundles for On-Chip Interconnect. In Proceedings of the IEEE ASP Design Automation Conference, Yokohama, Japan, 23–26 January 2007.
27. Nieuwoudt, A.; Massoud, Y. Accurate Resistance Modeling for Carbon Nanotube Bundles in VLSI Interconnect. In Proceedings of the IEEE Conference on Nanotechnology, Cincinnati, OH, USA, 17–20 July 2006.
28. Nieuwoudt, A.; Massoud, Y. Assessing the Implications of Process Variations on Future Carbon Nanotube Bundle Interconnect Solutions. In Proceedings of the IEEE Symposium on Quality Electronic Design, San Jose, CA, USA, 26–28 March 2007.
29. Nieuwoudt, A.; Massoud, Y. Performance Implications of Inductive Effects for Carbon Nanotube Bundle Interconnect. *IEEE Electron Devices Lett.* **2007**, *28*, 305–307.
30. Massoud, Y.; Majors, S.; Bustami, T.; White, J. Layout techniques for minimizing on-chip interconnect self-inductance. In Proceedings of the 35th ACM/IEEE-CAS/EDAC Design Automation Conference (Cat. No.98CH36175), San Francisco, CA, USA, 15–19 June 1998; pp. 566–571.
31. Massoud, Y.; Kawa, J.; MacMillen, D.; White, J. Modeling and analysis of differential signaling for minimizing inductive crosstalk. In Proceedings of the 38th Design Automation Conference (IEEE Cat. No.01CH37232), Las Vegas, NV, USA, 22 June 2001; pp. 804–809.
32. Massoud, Y.; White, J. FastMag: A 3-D magnetostatic inductance extraction program for structures with permeable materials. In Proceedings of the IEEE/ACM International Conference on Computer Aided Design, 2002. ICCAD 2002., San Jose, CA, USA, 10–14 November 2002; pp. 478–484.
33. Massoud, Y.; Majors, S.; Kawa, J.; Bustami, T.; MacMillen, D.; White, J. Managing on-chip inductive effects. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2002**, *10*, 789–798.

34. Massoud, Y.; White, J. Simulation and modeling of the effect of substrate conductivity on coupling inductance and circuit crosstalk. *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **2002**, *10*, 286–291.
35. Ragheb, T.; Massoud, Y. On the modeling of resistance in Graphene Nanoribbon (GNR) for future interconnect applications. In Proceedings of the 2008 International Conference on Computer-Aided Design (ICCAD'08), San Jose, CA, USA, 10–13 November 2008.