Logic Locking Using Emerging 2T/3T Magnetic Tunnel Junctions for Hardware Security

DIVYANSHU DIVYANSHU©, RAJAT KUMAR©, DANIAL KHAN©, SELMA AMARA©, (Member, IEEE), AND YEHIA MASSOU©, (Fellow, IEEE)
Division of Computer, Electrical and Mathematical Sciences and Engineering, King Abdullah University of Science and Technology, Thuwal 23955, Saudi Arabia
Corresponding author: Yehia Massoud (yehia.massoud@kaust.edu.sa)

ABSTRACT With the advancement of beyond CMOS devices, a new approach to utilize the inherent physics of such emerging structures for various applications is of great interest in recent research. Spintronics-based devices offer key advantages like ease of fabrication with Si-substrate, non-volatile memory, low operational voltage, and non-linear device characteristics, which have shown potential for several emerging fields of study. Hardware security is one of the key interest areas which heavily relies on CMOS-based ICs, and the defense and attack mechanism is mostly based on CMOS-based structures. This work explores several emerging structures based on 2T/3T magnetic tunnel junctions (MTJ) for possible logic locking applications in hardware security systems. We demonstrate the effect of MTJ-based devices to implement logic locking even in the presence of process variations, and its ability of robustness to device imperfections has been evaluated using monte carlo simulations for practical applications.

INDEX TERMS CMOS technology, hardware security, logic locking, magnetic tunnel junction (MTJ), spintronics, spin-orbit torque (SOT), spin-transfer torque (STT), voltage-controlled magnetic anisotropy (VCMA).

I. INTRODUCTION
The integrated circuits (ICs) are commonly recognized as a source of trust in Internet-of-Things (IoT) applications. The billions of devices are expected to be connected through IoT, covering a broad range of applications by 2025. However, globalization of integrated circuit (IC) design and fabrication has led to growing cost and design complexity that resulted in severe security concerns. As a result, most IC design companies have gone fabless due to their heavily relying on untrusted foundries to fabricate their ICs [1], [2], [3]. In the semiconductor sector, insertion of hardware Trojans, reverse engineering attacks, side-channel attacks, piracy of intellectual property (IP), counterfeiting of chips, overbuilding, and others have raised both hardware security threats and financial losses [4]. Recently, the development of various emerging technologies has played a vital role in improving the notion of hardware security [5], [6], [7]. The main purpose of the emerging technologies is to overcome the fundamental limitations of scaling and power consumption of the CMOS technology. For example, spintronic is a promising contender for logic devices and information storage due to its non-volatility, low power consumption, and high endurance [8].

Researchers have investigated utilizing the unique inherent properties of the emerging devices (memristors, carbon nanotubes (CNTs), and nanowire FETs (NWFETs), etc.) to lower the performance overhead of CMOS-based security approaches such as hardware obfuscation. References [9], [10], [11], [12], [13], [14], [15], [16], [17] evaluate the performance and reliability of CNT bundles for on-chip interconnect applications due to their large conductivity and current carrying capabilities. Authors in [18] report a comprehensive model for the resistance in graphene nanoribbon (GNR) interconnects. One of our future goals is to explore spintronics devices for memory and/or logic applications and even for interconnects due to their low-power consumption, non-volatility, and competitive bit area cell. A technique named “ProbLock” in [19] can be applied to both combinational and sequential circuits using a filtering process to select the best location of key gates based on various constraints. The algorithm is tested on 40 benchmarks from the ISCAS ‘85 and ISCAS ‘89 suites and the ProbLock is evaluated against a SAT attack. The hardware obfuscation alters the structure or description of a circuit to make it more difficult for an attacker
to reverse engineer it. Currently, IC camouflaging [20], split manufacturing [21], and logic locking [22] are popular obfuscations methodologies in research. IC camouflaging and split manufacturing rely on a reliable foundry, whereas logic locking with an active key gives greater protection against a wider threat space.

II. BACKGROUND
A. LOGIC LOCKING IN HARDWARE SECURITY
Logic locking (LL) is a technique that inserts new key inputs and logic mechanisms into the circuit, causing the circuit to behave incorrectly until the correct key combination is provided. Logic locking is sub-divided into two categories: combinational logic locking [23] and sequential logic locking [24]. In combinational logic locking, the output of the circuit is corrupted until and unless the correct key combination is applied. In contrast, additional states are inserted in sequential logic locking, causing the circuit to be locked until the correct sequence is provided.

Various logic locking techniques have been proposed to protect the privacy and integrity of the ICs. Random logic locking [23] obfuscates the outputs by randomly inserting XOR/XNOR gates in the gate-level netlist but is broken by the sensitization attacks. Strong logic locking [25], which is supposed to be immune to sensitization attacks, can be broken by SAT attacks. Cycle logic locking [26] creates a logical loop in the circuit to thwart the SAT attack. Stripped functionality logic locking—Hamming distance (SFLL-HD) and Tenacious and traceless logic locking (TTL) [27] are resilient to both removal and SAT attacks.

B. 2T/3T MAGNETIC TUNNEL JUNCTION (MTJ)
Fig. 1 shows a typical MTJ structure comprising two relatively thick ferromagnetic layers (a fixed layer and a free layer) separated by a relatively thin tunnel barrier layer [28]. When the fixed layer and the free layer have the same magnetic direction (parallel, denoted by P), the MTJ shows a lower resistance (R_P). On the contrary, when the magnetic directions of both layers are opposite (Anti-parallel, denoted by AP), the MTJ shows a higher resistance (R_AP). In this work, we have divided the structures based on the number of terminals for the MTJ block. We have considered the spin-transfer torque (STT) phenomenon for the 2T structure and field-free spin-orbit torque (SOT) assisted switching for the 3T structure for designing the logic locked circuit. For deterministic switching characteristics, the energy barrier height must be sufficient to overcome the thermal energy to have a higher data retention time. The tunnel magnetoresistance (TMR) ratio characterizes the resistance difference and is defined by the following equation:

\[
TMR = \frac{R_{AP} - R_P}{R_P} \times 100
\]

If the difference between the resistances in parallel and anti-parallel is larger, it shows higher TMR and higher readability.

When a bidirectional current greater than the critical current (I_C0) flows through an MTJ cell, it can switch between parallel and anti-parallel states. The MTJ cell switches from parallel to anti-parallel state when the passing current (>I_C0) flows from the fixed layer to the free layer. On the contrary, when passing current flows from the free layer to the fixed layer, the MTJ cell switches from anti-parallel to parallel state. The magnetic dynamics of the free layer are governed by modified Landau Lifshitz Gilbert (LLG) equation [34], which is given by:

\[
\begin{align*}
\frac{\partial \bar{m}}{\partial t} &= -\gamma \bar{m} \times \vec{H}_{\text{eff}} (\text{MTJ}) + \alpha \bar{m} \times \frac{\partial \bar{m}}{\partial t} \\
&+ \gamma H_{\text{DL}} \bar{m} \times \bar{m}_p \times \bar{m} + \gamma H_{\text{STT}} \bar{m} \times \bar{m}_p \\
&+ \gamma H_{\text{SOT}} \bar{m} \times \bar{m}_\sigma \times \bar{m} + \gamma H_{\text{SHE}} \bar{m} \times \bar{m}_\sigma \\
&\quad (2)
\end{align*}
\]

Here, \(\bar{m}\) is the magnetization of the free layer, \(\gamma\) is the Gyromagnetic ratio, \(\mu_0\) is the vacuum permeability, \(\vec{H}_{\text{eff}}\) is the effective magnetic field having different contributing terms like perpendicular magnetic anisotropy (PMA), voltage-controlled magnetic anisotropy (VCMA), demagnetization field, exchange bias and thermal noise as shown in equation (5). \(\alpha\) is the Gilbert damping coefficient, \(P\) is the polarization factor, \(J_{\text{STT}}\) and \(J_{\text{SHE}}\) are the STT and SOT current density applied to the MTJ device, \(\bar{m}_p\) is the polarization direction of the spin current injected in the free layer by the STT, \(H_{\text{SOT}}\) and \(H_{\text{SHE}}\) are respectively the current-dependent proportionality constants for the FL torque and DL torque of the SOT, \(\bar{m}_\sigma\) is the pure spin current induced by the spin-orbit coupling, \(\theta_{\text{SH}}\) is the spin Hall angle, \(T_{\text{SL}}\) is the free layer thickness and other symbols have their usual meaning.

The MTJ has been utilized in implementing many aspects of hardware securities such as True Random Number Generators (TRNG), Physically Unclonable Functions (PUF) [6], logic and future memory [8], hardware Trojan [35], Poly-morphic Logic [30], Logic Obfuscation [31], etc. In this work, we use different MTJ devices and perform logic locking applications to explore the viability and applicability of such devices for future hardware security applications. Fig. 2(a)-(b) represents switching characteristics for 2T MTJ
We have performed electrical simulations in tsmc 40nm CMOS generic process design kit using the cadence spectre simulator with W/L ratio = 3, temperature at 300K, and simulation steps of 1 ps.

III. PROPOSED WORK

The MTJ circuit can be utilized to perform the logic operation and to implement polymorphic gates [31]. The ability to obtain polymorphic gate behavior allows the IC chip to have an extra layer of security. It becomes difficult to obtain exact logic implementation by reverse-engineering the layout. The PMA STT compact model [32] consists of, from the substrate side, Ta(5)/Ru(10)/Ta(5)/Co$_{20}$Fe$_{60}$B$_{20}$(x)/MgO(y)/Co$_{20}$Fe$_{60}$B$_{20}$(z)/Ta(5)/Ru(5), where the dimensions are in nm and x, y, and z values are selected during the electrical simulation as mentioned in Table 1. The Voltage-controlled magnetic anisotropy effect (VCMA) is utilized in various two-terminal MTJ models like STT assisted Precessional model and STT assisted thermally activated MTJ model, as described in [33]. In the 3T SOT MTJ structure, MTJ with Heavy metal (HM) is used, where the switching mechanism requires both SOT and STT current. The requirement of STT current passing through the MTJ stack is reduced, and thus more reliability in operation is achieved. Furthermore, the model developed in [28] does not require an external magnetic field to change the state of the MTJ. On the other hand, the VGSOT p-MTJ can also switch without needing a magnetic field. Instead of the HM, the anti-ferromagnetic (AFM) strip provides spin-orbit torque along with an exchange bias and VCMA effect, allowing it to have reduced critical current density for switching, as mentioned in Table 5, thus paving the way for more practical applications.

A. 2T MTJ CIRCUIT DESCRIPTION

The switching takes place in a 2-terminal MTJ structure because of the STT switching mechanism. Fig. 3(a) shows the block diagram representation of a gate based on 2T MTJ providing output in true as well as in complementary form. The elaborated design of the block diagram is present in Fig. 3(b). It consists of a pre-charge sense amplifier, a MOS logic, two complimentary MTJs, and a writing circuit to write the MTJ state. A precharge sense amplifier works in two phases: the precharge and the evaluation phase. Both outputs are precharged to the supply voltage when the clock pulse is LOW, hence known as the precharge phase. When the clock
pulse is HIGH, outputs are evaluated depending on the MOS logic tree and states of MTJs, hence known as the evaluation phase. The writing circuit shown in Fig. 3(b) is used to write both MTJs together, providing a path from Vdd to ground through P1-MTJ1-MTJ2-N2 or P2-MTJ2-MTJ1-N1.

The circuit in Fig. 3(b) shows the implementation of a two-input AND/NAND hybrid CMOS-MTJ gate for logic locking. One gate input is applied in the MOS logic present above complimentary MTJs, and another input is applied in the writing circuit. Presently, the MOS transistors have the ON
TABLE 1. MTJ parameters set during electrical simulation.

| MTJ Types      | Parameter                        | Magnitude | unit  |
|---------------|----------------------------------|-----------|-------|
| STT-MTJ       | MTJ dimension and shape          | 32 x 32, circular | nm    |
|               | Gilbert damping coefficient and TMR₀ | 0.025, 200% |       |
|               | Oxide and free layer thickness   | 0.85, 1.3   | nm    |
|               | Saturation magnetization         | 15.800     | Oersted |
|               | Polarization factor and Spin Hall angle | 0.52  |       |
|               | Functional Variation (Gaussian distribution) | |       |
| Pre-VCMA MTJ  | MTJ dimension and shape          | 50 * 50, circular | nm    |
|               | Damping coefficient and TMR      | 0.05, 1.2   |       |
|               | Saturation magnetization         | 6.25e05     | A/m   |
|               | Polarization factor and MgO barrier height | 0.58, 0.5 | V     |
| SOT-MTJ       | MTJ dimension and shape          | 40 * 40, circular | nm    |
|               | Heavy metal dimension (L, W, H) and resistance | 60 * 40 * 3, 1000 | nm, Ω  |
|               | Damping coefficient and TMR      | 0.03, 1.2   |       |
|               | Saturation magnetization         | 8e05        | A/m   |
|               | Asymmetry factor and field like torque component | 1.1, 0.8 |       |
|               | Functional Variation (Gaussian distribution) | |       |
| VG-SOT MTJ    | MTJ dimension and shape          | 50 * 50     | nm    |
|               | Heavy metal dimension (L, W, D)  | 60 * 50 * 3 | nm    |
|               | Damping coefficient and TMR      | 0.05, 1.2   |       |
|               | Saturation magnetization         | 6.25e05     | A/m   |

resistance ($R_{ON}$) in $kΩ$ and OFF resistance ($R_{OFF}$) in $GΩ$. When the value of In is low, the resistance of the left branch of PCSA is in $GΩ$, and the resistance of the right branch is in $kΩ$. Therefore, the Out is pulled to 0V much faster than $\overline{Out}$, giving Out as 0 whenever In=0. When the value of In is high, both the branches have resistance in $kΩ$. When In=1 and Key=0, the resistance of left branch is $R_{ON} + R_{AP}$ and right branch is $R_P$, therefore Out is pulled to 0V much faster because $R_{AP} > R_P$. When In=1 and Key=1, the resistance of left branch is $R_{ON} + R_P$ and right branch is $R_{AP}$. For proper operation in this case, the MTJ parameters are adjusted such that $R_{ON} + R_P < R_{AP}$.

Fig. 3(c) shows the required operation for the 2T MTJ devices. The In and Key are the two primary inputs of the block diagram. When Clk is high (evaluation phase), the Out of STT and Pre-VCMA MTJ are plotted for all possible combinations of In and Key. The Key is applied in the writing circuit to write the MTJ states, which can only be done when Clk is low. Hence $W_{En}$ signal is set as $\overline{Clk}$. For considering the effect of process variation (PV), some key parameters are varied following the Gaussian distribution as mentioned in Table 1. Fig. 3(d)-(e) shows the variation in the parameters of MTJ₁ and MTJ₂ of Fig. 3(b) when 250 times Monte-Carlo simulations were performed. The STT MTJ-based structure showed great robustness to device imperfections and had a 100% success ratio for the considered case. Fig. 3(f)-(g) shows the Monte-Carlo results for parallel resistance of MTJ₁ and MTJ₂. Currently, the Precessional VCMA MTJ compact model does not have a process variation option for analyzing the variation effect.

B. 3T MTJ CIRCUIT DESCRIPTION

In a 3-terminal MTJ structure, the switching can occur because of STT as well as SOT switching mechanism. Fig. 4(a) shows a logical implementation of the AND/NAND gate based on a hybrid CMOS-MTJ approach. The circuit outputs are analyzed in the same way as those for the 2T MTJ circuit, as mentioned in section III-A. The gate can be used in the logic locking mechanism for hardware security applications. The block diagram of the circuit is shown in Fig. 4(b). The MOS logic consists of a single NMOS transistor MN11. Two complimentary 3-terminal MTJs are present in both branches of PCSA. A reset signal is used to reset the MTJs to the 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. Fig. 4(c) shows the plots of all input and output pins of the 3T logic locking block (both SOT and VG-SOT) for all the combinations of In and Key. The $W_{En}$ signal is used to write the MTJ state with Key. It is made high only when both Clk and Reset signals are low. During process variation simulation, the reference point data needs to be selected so that the introduced deviation must lie between the allowed range of operation in the compact model.
The testing of parameters thus is limited by the degree of sophisticated modeling of the compact model. A more realistic and scaled compact model will thus allow a better logic locking system using MTJ devices. Fig. 4(d)-(e) shows the variation in some key parameters for SOT MTJ in the presence of process variations and 250 times Monte Carlo simulations for the parameters mentioned in Table 1. Table 2 contains Monte-Carlo simulation results for SOT and VG-SOT MTJ. With increasing process variations, the amount of standard deviation (SD) observed in MTJ resistance was increased, resulting in incorrect output. Thus, for designing a logic locking system, the circuits need to be optimized to include process variations.

### IV. EXPERIMENTAL RESULTS AND DISCUSSION

#### A. LOGIC LOCKING CIRCUIT OPERATION

In logic locking-based hardware security, key management is an important aspect as the attacker aims to obtain the key by any means. Therefore, the key is stored in a tamper-proof memory and fabricated on a chip in such a way that its value is not known to the outside foundry [23]. However, even with tamper-proof memory, attacks to obtain keys are known, and the most significant one is by using Power Attack (PA) analysis [27]. Spintronics-based tamper-proof memory is also vulnerable to this attack because of the write and read current difference. Due to their specific advantages mentioned earlier, they are also an ideal choice for storing the key.
TABLE 3. Truth table for all possible outcomes for 2T STT based logic locking circuit implementing \( Y = AB + BC + CA \).

| A | B | C | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |

STT-MRAM device are a good alternative because of their less area consumption. The endurance problem is reduced as the data needs to be written only once, and with an energy barrier height of around 60 kT, the data retention time is around 10 years. The implemented circuit is shown in Fig. 5(a). An extra layer of security is added by including user-defined keys, which act as a prevention for PA-based attacks. Several ways of securing keys are investigated in the key management aspect of hardware security. As the LL block operates as AND/NAND logic, we have selected them to operate in AND operation, and the key value is marked from 0-7, where 0 represents the pattern \( K_1K_2K_3 = 000 \) and 7 represents \( K_1K_2K_3 = 111 \). Fig. 5(b) represents the operation for STT MTJ when implemented for the circuit shown in Fig. 5(a) under some specific key values. Table 3 contains all the combinations and obtained results for this operation, with the correct key value being \( K_1K_2K_3 = 111 \). Similar results are obtained using all other MTJ models. Suppose an attacker can decipher the possible gate functionality by reverse-engineering the IC chip, consisting of MTJ-based logic locked block. In that case, the attack algorithm will still need to simulate \( 2^{26} \) patterns to narrow it down to a single key value. The Hamming distance (HD) for logic locking block needs to be ideally 50% [27] to introduce difficulty for SAT attacks. For the correct waveform in this design, the HD is 25%. So, this circuit will be more vulnerable to algorithm-based attacks.

B. LOGIC LOCKING: ADVANTAGES AND CHALLENGES FOR MTJ DEVICES

The goal of an attacker is to obtain the secret key used for logic encryption. The attacker is assumed to have access to the encrypted netlist and working IC chip. The attacker can simulate the attack patterns from the encrypted netlist, infers key response from it and, is successful in its attack. A detailed description of the evolution of logic locking and the evolution of attack and defense mechanisms is presented in [22]. It is becoming important to analyze dynamic threat models and new attack patterns in such emerging technologies. With increasing interest in alternative hardware, it is important to look towards the security aspects of such emerging devices. The ever-increasing need for scaling also requires a thorough understanding of new security challenges arising from such requirements. The attacker can understand the functionality of a chip by using a microscopic image of the layout to determine the netlist and type of logic being implemented and then simulate it by using a test pattern. The possibility of obtaining multiple logic functionality by using the same structure and a select signal makes it extremely difficult to specify the logic functionality of such multi-layer stacked nanopillars. So, having the layout pattern itself will not be sufficient. The complex switching mechanism applied needs to be decoded for attacking multi-staged logic locking units, making it more difficult to reverse engineer than CMOS-based logic locking.

The main disadvantage of such emerging beyond CMOS devices is that conventional logic locking based mechanism considers that the foundry and the user both are untrusted, so the locking of the netlist and storing of a key is done before sending to the foundry. Beyond CMOS devices are limited currently since specialized fabrication techniques are required to implement logic locking blocks. To overcome this difficulty, either the foundry needs to be trusted, or the circuit needs to contain a more significant number of such blocks.
FIGURE 6. (a) MTJ composition. (b) Device stack deposited by magnetron sputtering TEM image showing multi nanolayers. (c) Free layer magnetization vs applied external field and temperature for a specific input for SOT MTJ model.

TABLE 5. Performance comparison for SOT vs VG-SOT.

|                  | Traditional SOT MTJ | VG-SOT MTJ |
|------------------|---------------------|------------|
| $I_{sot}$        | -98 UA              | -6.2619 UA |
| Switching delay  | 2.5 ns              | 5 ns       |
| Switching error rate | 0.225           | 0          |
| Switching Energy | 10.68 fJ/bit        | 0.08 fJ/bit|

based on the emerging devices in the ICs to make it difficult to reverse engineer at a particular point. Another aspect is that MTJ devices have unique physical characteristics and dependence on certain external parameters like temperature and magnetic field. Any fluctuations in such parameters can cause operation failure even in the activated chips. Fig. 6(c) demonstrates the dependence of free layer magnetization dynamics for the SOT MTJ model on temperature and magnetic field. A parametric sweep needs to be performed to obtain the critical value for them, and the design needs to be optimized to operate below the critical values for any future practical applications. Reference [36] analyzes the effect of the magnetic field on the MOS device characteristics. The reference concluded that the high magnetic field of up to 7T did not cause any significant performance degradation. So, the CMOS-based structure is practically immune to magnetic fields for general applications, and the logic locked circuit needs to be designed in such a way as to ensure sufficient tolerance to stray magnetic fields. The thermal stability factor needs to be optimized to ensure proper operation during temperature sweep tests in the system-on-chip (SoC) design flow. In [29], a hybrid CMOS/MTJ circuit for low power design has been discussed with significant improvement in circuit parameters.

Adding a logic locking block using an MTJ-based AND gate will cause an area overhead, but MTJ devices have competitive bit area cell, and improvement in scaling for such devices in the future may decrease the required area overhead. Also, the ICs contain many transistors, and the requirement of such MTJ-based logic locking block can be limited to a few places; thus, a small area trade-off for higher security can be achieved. Table 4 compares the various parameters of Magnetic Non-Volatile memory for different MTJ structures [37]. The best energy-delay product is obtained for the VCMA-assisted STT model. The recently reported VG-SOT model, which contains the anti-ferromagnetic strip instead of the conventional HM layer, has an extra $H_{ex}$ as illustrated in equation (2), providing an additional effect on its characteristic based on the modified LLG expression. Performance

TABLE 6. Eye diagram test analysis for signal integrity for the selected MTJ devices for high speed digital circuits applications.
comparison of VG-SOT MTJ is made with 3T SOT MTJ and presented separately in Table 5 [34]. Thus, emerging structures with different switching mechanisms and materials are being developed rapidly, and improvements in circuit parameters are expected in the future. An MTJ with much higher endurance is preferred for the Logic Locking application. Due to the lower requirement of critical $J_{SHE}$ in VG-SOT MTJ, as described in Table 5, it can be a better alternative for future logic locked circuits. The performance of emerging MTJ-based Logic locking circuits needs to account for the signal integrity tests to analyze its behavior in high-speed digital integrated circuits. Fig 7 shows the Eye diagram test result performed on VG-SOT MTJ, and Table 6 contains the comparison data of eye diagram analysis for all the selected MTJ.

V. CONCLUSION

Spintronics’ growing and emerging technology is a prime candidate for information storage and logic devices due to its significant advantages over traditional CMOS technology, such as low-power consumption, non-volatility, and high endurance. Hardware security heavily relies on CMOS-based structures for defense and attack mechanisms. Several emerging structures based on 2T/3T magnetic tunnel junctions have been explored in the proposed work for possible logic locking applications in hardware security systems. The effect of MTJ-based devices been evaluated using Monte Carlo simulations in the presence of process variations to implement the logic locking and its ability of robustness to device imperfections. Furthermore, we tried to present a general outline for the design consideration, advantages, and challenges of such emerging structures for future logic locking applications and their signal integrity performance by using eye-diagram analyses for applications in high-speed digital circuits.

REFERENCES

[1] A. Chakraborty, N. G. Jayasankaran, Y. Liu, J. Rajendran, O. Sinanoglu, A. Srivastava, Y. Xie, M. Yasin, and M. Zurasak, “Keynote: A disquisition on logic locking,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 39, no. 10, pp. 1952–1972, Oct. 2020.
[2] K. Shamshi, M. Li, K. Pfaks, S. Fazzari, and D. Z. Pan, “IP protection and supply chain security through logic obfuscation: A systematic overview,” ACM Trans. Des. Automat. Electron. Syst., vol. 24, p. 5, Sep. 2019.
[3] M. Rostami, F. Koushanfar, and R. Karri, “A primer on hardware security: Models, methods, and metrics,” Proc. IEEE, vol. 102, no. 8, pp. 1283–1295, Aug. 2014.
[4] W. Hu, C.-H. Chang, A. Sengupta, S. Bhunia, R. Kastner, and H. Li, “An overview of hardware security and trust: Threats, countermeasures, and design tools,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 40, no. 6, pp. 1010–1038, Jun. 2021.
[5] Y. Bi, K. Shamshi, J.-S. Yuan, P.-E. Gaillardon, G. D. Micheli, X. Yin, X. S. Hu, M. Niemier, and Y. Jin, “Emerging technology-based design of primitives for hardware security,” ACM J. Emerg. Technol. Comput. Syst., vol. 13, no. 1, pp. 1–19, Dec. 2016.
[6] S. Ghosh, “Spintronics and security: Prospects, vulnerabilities, attack models, and preventions,” Proc. IEEE, vol. 104, no. 10, pp. 1864–1893, Oct. 2016.
[7] M. Khan and S. Ghosh, “Comprehensive study of security and privacy of emerging non-volatile memories,” J. Low Power Electron. Appl., vol. 11, no. 4, p. 36, 2021.
[8] S. Bhatti, R. Shiaa, A. Hirohata, H. Ohno, S. Fukami, and S. N. Piramanyan, “Spintronics based random access memory: A review,” Mater. Today, vol. 20, no. 9, pp. 530–548, 2017.

[9] Y. Massoud and A. Nieuwoudt, “Modeling and design challenges and solutions for carbon nanotube-based interconnect in future high performance integrated circuits,” ACM J. Emerg. Technol. Comput. Syst., vol. 2, no. 3, pp. 155–196, Jul. 2006.
[10] A. Nieuwoudt and Y. Massoud, “Predicting the performance of low-loss on-chip inductors realized using carbon nanotube bundles,” IEEE Trans. Electron Devices, vol. 55, no. 1, pp. 298–312, Jan. 2008.
[11] Y. Massoud and Y. Ismail, “Grasping the impact of on-chip inductance in high speed ICs,” IEEE Circuits Devices Mag., to be published.
[12] S. Eachempati, A. Nieuwoudt, A. Gayasen, N. Vijaykrishnan, and Y. Massoud, “Assessing carbon nanotube bundle interconnect for future FPGA architectures,” in Proc. Design, Autom. Test Eur. Conf. Exhib., Apr. 2007, pp. 1–6.
[13] A. Nieuwoudt, T. Ragheb, H. Nejati, and Y. Massoud, “Increasing manufacturing yield for wideband RF CMOS LNAs in the presence of process variations,” in Proc. 8th Int. Symp. Quality Electron. Design (ISQED), Mar. 2007, pp. 801–806.
[14] A. Nieuwoudt, M. Mondal, and Y. Massoud, “Predicting the performance and reliability of carbon nanotube bundles for on-chip interconnect,” in Proc. Asia South Pacific Design Autom. Conf., Yokohama, Japan, Jan. 2007, pp. 708–713.
[15] Y. Massoud and A. Nieuwoudt, “Accurate resistance modeling for carbon nanotube bundles in VLSI interconnect,” in Proc. 6th Int. Conf. Nanotechnol., Jul. 2006, pp. 288–291.
[16] A. Nieuwoudt and Y. Massoud, “Assessing the implications of process variations on future carbon nanotube bundle interconnect solutions,” in Proc. 8th Int. Symp. Quality Electron. Design (ISQED), Mar. 2007, pp. 119–126.
[17] A. Nieuwoudt and Y. Massoud, “Performance implications of inductive effects for carbon-nanotube bundle interconnect,” IEEE Electron Device Lett., vol. 29, no. 4, pp. 305–307, Apr. 2007.
[18] T. Ragheb and Y. Massoud, “On the modeling of resistance in graphene nanoribbon (GNR) for future interconnect applications,” in Proc. IEEE/ACM Int. Conf. Computer-Aided Design, San Jose, CA, USA, Nov. 2008, pp. 593–597.
[19] M. Yue and S. Tehranipoor, “A novel probability-based logic-locking technique: ProbLock,” Sensors, vol. 21, no. 23, p. 8126, Dec. 2021.
[20] M. Yasin, “CamoFurturb: Secure IC camouflaging for minterm protection,” in Proc. IEEE/ACM Int. Conf. Computer-Aided Design (ICCAD), 2016, pp. 1–8.
[21] K. Xiao, D. Forte, and M. M. Tehranipoor, “Efficient and secure split manufacturing via obfuscated built-in self-authentication,” in Proc. IEEE Int. Symp. Hardware Oriented Secur. Trust (HOST), May 2015, pp. 14–19.
[22] H. Kamali, K. Azar, F. Farahmandi, and M. Tehranipoor, “Advances in logic locking: Past, present, and prospects,” Cryptol. ePrint Arch., Tech. Rep., 2022.
[23] J. A. Roy, F. Koushanfar, and I. L. Markov, “EPIC: Ending piracy of integrated circuits,” in Proc. Design, Autom. Test Eur., Mar. 2008, pp. 1069–1074.
[24] R. S. Chakraborty and S. Bhunia, “HARPOON: An obfuscation-based SoC design methodology for hardware protection,” IEEE Trans. Comput.-Aided Design Integr. Circuits Syst., vol. 28, no. 10, pp. 1493–1502, Oct. 2009.
[25] J. Rajendran, Y. Pino, O. Sinanoglu, and R. Karri, “Security analysis of logic obfuscation,” in Proc. 49th Annu. Design Autom. Conf. (DAC), 2012, pp. 83–89.
[26] K. Shamshi, M. Li, T. Meade, Z. Zhao, and D. Z. Pan, “Cyclic obfuscation for creating SAT-unresolvable circuits,” in Proc. Great Lakes Symp. VLSI, Ottawa, ON, Canada, May 2017, pp. 173–178.
[27] M. Yasin, A. Sengupta, M. T. Nabeel, and M. Ashraf, “Provably-secure logic locking: From theory to practice,” in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Dallas, TX, USA, Oct. 2017, pp. 1601–1618.
[28] Z. Wang, W. Zhao, E. Deng, J.-O. Klein, and C. Chappert, “Perpendicular-anisotropy magnetic tunnel junction switched by spin-Hall-assisted spin-transfer torque,” J. Phys. D. Appl. Phys., vol. 48, no. 6, Feb. 2015, Art. no. 065001.
[29] S. D. Kumar, Z. Kahleifeh, and H. Thapliyal, “Novel secure MTJ/CMOS logic (SMCL) for energy-efficient and DPA-resistant design,” Social Netw. Comput. Sci., vol. 2, no. 2, p. 92, Apr. 2021.
[30] A. Roohi, R. Zand, and R. F. DeMara, “Logic-encrypted synthesis for energy-harvesting-powered spintronic-embedded datapath design,” in Proc. Great Lakes Symp. VLSI, Chicago, IL, USA, May 2018, pp. 9–14.
[31] J. Yang, X. Wang, Q. Zhou, Z. Wang, and H. Li, “Exploiting spin-orbit torque devices as reconfigurable logic for circuit obfuscation,” *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 38, no. 1, pp. 57–69, Jan. 2019.

[32] Y. Zhang, B. Yan, W. Kang, and Y. Cheng, “Compact model of subvolume MTJ and its design application at nanoscale technology nodes,” *IEEE Trans. Electron Devices*, vol. 62, no. 6, pp. 2555–2565, Jun. 2015.

[33] H. Zhang, W. Kang, L. Wang, K. L. Wang, and W. Zhao, “Stateful reconfigurable logic via a single-voltage-gated spin Hall-effect driven magnetic tunnel junction in a spintronic memory,” *IEEE Trans. Electron Devices*, vol. 64, no. 10, pp. 4295–4301, Oct. 2017.

[34] K. Zhang, D. Zhang, C. Wang, L. Zeng, Y. Wang, and W. Zhao, “Compact modeling and analysis of voltage-gated spin-orbit torque magnetic tunnel junction,” *IEEE Access*, vol. 8, pp. 50792–50801, 2020.

[35] R. Kumar, D. Divyanshu, D. Khan, S. Amara, and Y. Massoud, “Spin orbit torque-assisted magnetic tunnel junction-based hardware trojan,” *Electronics*, vol. 11, no. 11, p. 1753, May 2022.

[36] L. Hebrard, D. V. Nguyen, D. Vogel, J.-B. Schell, C. Po, N. Dumas, W. Uehling, and J. Pascal, “On the influence of strong magnetic field on MOS transistors,” in *Proc. IEEE Int. Conf. Electron., Circuits Syst. (ICECS)*, Dec. 2016, pp. 564–567.

[37] W. Kang, Y. Ran, W. Lv, Y. Zhang, and W. Zhao, “High-speed, low-power, magnetic non-volatile flip-flop with voltage-controlled, magnetic anisotropy assistance,” *IEEE Magn. Lett.*, vol. 7, 2016, Art. no. 3106205.

**DIVYANSHU DIVYANSHU** received the B.Tech. degree in electronics system engineering from the National Institute of Electronics and Information Technology, Aurangabad, Maharashtra, India, in 2018, and the M.Tech. degree in VLSI from the Indian Institute of Technology (IIT) Mandi, Mandi, India, in 2021. He is currently pursuing the Ph.D. degree with the Innovative Technologies Laboratories (ITL), King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia. He has worked as a Visiting Student at the Integrated Circuits and System Group (ICS), CEMSE, and at the ITL, CEMSE, KAUST. His research interests include spintronic based devices for hardware security applications, spintronic based VLSI circuit design, and other emerging spintronic based computing paradigms.

**RAJAT KUMAR** received the B.Tech. degree in electronics and communication engineering from the National Institute of Technology (NIT) Hamirpur, Himachal Pradesh, India, in 2019, and the M.Tech. degree in electrical engineering with specialization in very large scale integration (VLSI) from the Indian Institute of Technology (IIT) Mandi, Himachal Pradesh, India, in 2021. He is currently pursuing the Ph.D. degree with the Innovative Technologies Laboratories (ITL), Computer, Electrical and Mathematical Science and Engineering (CEMSE) Division, King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia. His research interest includes spintronics domain, from circuit-level simulation of spintronic devices in various applications like hardware security and logic designing to fabrication of the devices.

**DANIAL KHAN** received the B.S. degree in electrical engineering from the University of Engineering and Technology (UET), Peshawar, Pakistan, in 2011, and the combined M.S. and Ph.D. degrees in electronic and electrical engineering from Sungkyunkwan University, Suwon, South Korea, in 2020. From October 2020 to December 2021, he worked as a Postdoctoral Fellow at Sungkyunkwan University. He is currently working as a Postdoctoral Fellow with the Department of Computer, Electrical and Mathematical Sciences and Engineering, King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia. His research interests include spintronics, analog IC designs, RF energy harvesting systems, wireless power transfer (WPT) systems, and power management IC designs.

**SELMA AMARA** (Member, IEEE) received the Ph.D. degree in micro and nano electronics specialty from the Spintec-CEA Laboratory, Joseph Fourier University. She has research and industrial experiences at different teams and has competences in nanofabrication in clean room, thanks to Spintec Laboratory, which offers such a specialized training of the nanofabrication. She has taught some undergraduate and graduate courses in physics: electronics, optics, magnetisms, and mechanics. She was a Postdoctoral Researcher with the Novel Magnetic Devices (NoMaDe) Group—A joint research team between Institut d’Electronique Fondamentale (IEF), Paris Sud University, and the Ecole Normale Supérieure (ENS). She is currently working as a Postdoctoral Fellow in nanofabrication of TMR sensors at KAUST. She has attended various specialized international conferences and published articles in prestigious international journals. Her main research interests include the spintronics and related applications going from electrical engineering to biotechnology. Her research interests include the design, implementation, electrical characterization, preparation, and instrumental analysis of samples.

**YEHIA MASSoud** (Fellow, IEEE) received the Ph.D. degree in electrical engineering and computer science from the Massachusetts Institute of Technology (MIT), Cambridge, USA. He has held several positions at leading institutions of higher education and the industry including Rice University, the Stevens Institute of Technology, Worcester Polytechnic Institute (WPI), UAB, the SLAC National Accelerator Laboratory, and Synopsys Inc. From January 2018 to July 2021, he was the Dean of the School of Systems and Enterprises (SSE), Stevens Institute of Technology, USA. Prior to Stevens, he served as the Head of the Department of Electrical and Computer Engineering (ECE), WPI, between 2012 and 2017. In 2003, he joined Rice University, as an Assistant Professor, where he became one of the Fastest Rice Faculty to be granted tenure in electrical and computer engineering and computer science, in 2007. He is currently the Director of the Innovative Technologies Laboratories (ITL), King Abdullah University of Science and Technology (KAUST). He has published more than 400 papers in leading peer-reviewed journals and conference publications. His research interests include design of state-of-the-art innovative technological solutions with a broad range of technical areas including smart cities, autonomy, smart health, smart mobility, embedded systems, nanophotonics, and spintronics. His research group was responsible for developing the world’s first realization of compressive sensing systems for signals, which provided an unprecedented one order of magnitude savings in power consumption and significant reductions in size and cost and has enabled the implementation of self-powered sensors for smart cities and ultra-low-power biomedical implantable devices.

Dr. Massoud was selected as one of ten MIT Alumni Featured by MIT’s Electrical Engineering and Computer Science Department, in 2012. He was a recipient of the Rising Star of Texas Medal, the National Science Foundation CAREER Award, the DAC Fellowship, the Synopsys Special Recognition Engineering Award, and the several best paper awards. He has been a PI or a Co-PI on more than $30 Million of funded research from the NSF, DOD, SRC, and the industry. He has served on the IEEE CAS Award Nomination Committee, IEEE Mac Valkenburg Award Committee, IEEE CAS Fellow Committee, IEEE Rebooting Computing Steering Committee, and IEEE Nanotechnology Council. He also served as the 2016 IEEE MWS/CAS Technical Program Co-Chair, as well as the 2009 General Program Co-Chair and the 2007 Technical Program Co-Chair for the ACM Great Lakes Symposium on VLSI. He was also named a Distinguished Lecturer by the IEEE Circuits and Systems Society. He has served as an Editor for the *Mixed-Signal Letters*—the Americas, as an Associate Editor for the IEEE Transactions on Very Large Scale Integration Systems, and the IEEE Transactions on Circuits and Systems—I, as well as a Guest Editor for a Special Issue of the IEEE Transactions on Circuits and Systems—I.  

* * *

**VOLUME 10, 2022**  
102395