Cybersecurity Regulation of Smart Mobility Hardware Systems: Case Assessment for Spin-Based MTJ Devices

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 (email: yehia.massoud@kaust.edu.sa)

***Abstract*—Smart mobility refers to optimizing transportation and communications to integrate new safety, efficiency, sustainability, and air quality standards. It interrelates various solutions, including improved health due to better air quality, less traffic congestion, and fewer victims in road accidents. However, the reliability and cybersecurity aspects of these systems raised serious concerns. A mobility infrastructure may be vulnerable to information leakage and denial of service (DoS) attacks from intelligent attackers. Therefore, hardware security plays a critical role in the computing systems. Globalization of integrated circuit (IC) design flow has increased the complexity, resulting in severe security concerns. Hardware Trojan (HT) insertion, Intellectual property (IP) theft, and many such attacks can pose significant challenges from untrusted entities, and conventional secure hardware mechanisms may not hold with emerging devices. Recent developments in beyond-CMOS devices have resulted in several novel hardware-level attacks and defenses, which motivates us to comprehensively assess the need for cybersecurity regulation for next-generation intelligent and secure hardware systems focussed on spintronic devices. These spin-based devices are potential candidates among emerging devices due to their low power consumption, ease of fabrication in the silicon substrate, and inherent spatial and temporal randomness.**

***Index Terms*—Cybersecurity, smart mobility, secure hardware system, spintronics, magnetic tunnel junction (MTJ)**

I. Introduction

A. Motivation

Smart mobility, in short, is a network of intelligent transportation and mobility. It re-imagines the transportation systems utilized in daily life and business, integrating many aspects of technology and mobility [1]. This covers not only using conventional motor vehicles, electric vehicles, and public transportation networks but also entirely new forms of transportation, including car-sharing programs and on-demand ride-sharing services. The decline in private vehicle ownership and the emergence of totally new mobility options are two examples indicate how consumer behavior changes are accelerating the transformation of the way people travel. This concept has gained hold in the fleet industry in recent years due to worries about traffic congestion, pollution, productivity loss, and (of course) money. Artificial Intelligence (AI), the Internet of Things (IoT), and Big Data will play a fundamental role in new solutions in the coming years [2].

Cybersecurity is the defense against cyber attacks on internet-connected systems, including hardware, software, and information [3]. Cyberattacks may take the form of IP theft, denial-of-service (DoS) attacks, Trojan horses, and control system attacks [4]. A cybersecurity policy is required to safeguard computer systems and information technology to oblige various businesses and organizations to defend their systems and data from cyberattacks. Fig. 1 shows the popular Confidentiality, Integrity, and Availability (CIA) triad used to model policies and security aspects in an organization [5]. It is clear from Fig. 1 that the hardware component is a key pillar in any organizational security infrastructure. Smart mobility system has a lot of electronic sensors and ICs at the core of the hardware system. The security measures can take the shape of additional hardware/design changes with extra cost. Hardware security is emerging as a significant design consideration while designing the ICs. With the advancement in emerging technologies, researchers in hardware security have immense opportunities to transform the current passive role of CMOS devices in security applications. Various emerging technologies have significantly improved the hardware security paradigm recently. The main goal of these technologies is to overcome CMOS technology's fundamental restrictions on scaling and power consumption. For instance, spin-based MTJ [6] devices have unique security aspects for hardware security primitives [7] and other important applications [8]. This will be discussed in detail in Section I-B. This emerging paradigm can

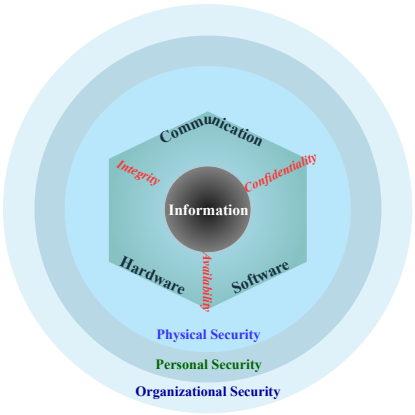

Fig. 1. The CIA triad model for policies and information security [5].

pose a requirement for assessing cybersecurity policy regulation as the framework needs to be adapted based on emerging hardware alternatives. This work provides a case assessment for Spin-based MTJ devices in an intelligent mobility hardware system and cybersecurity regulation approach.

B. Spin-Based Devices for Hardware Security

The ability to electrically control the magnetization dynamics and fabrication of MTJ stack at sub-10nm regime [9] has given rise to various interest in different applications like shared write channel-based high-density memories [10] and all-spin logic [11]. Fig. 2 shows the overall road map of utilizing MTJ devices at the hardware level in a smart mobility infrastructure. Any attack at the hardware level has more impact as another security mechanism is built on top of it. This section briefly describes various security primitives being developed using MTJ devices.

1) True Random Number Generator (TRNG): Random numbers are used in cryptographic key generation, Monte Carlo simulations, and various other security applications. TRNGs utilizes entropy from physical phenomena like jitter, the randomness of various electrical parameters, and metastability to generate statistically independent and secure keys. Various spintronics-based TRNGs have been investigated in the last decade due to the randomness in the physical characteristics of the MTJs. For the first time, a TRNG based on the random switching probability of MTJs with conditional perturb was experimentally demonstrated [12]. Recent works explore TRNGs using MTJ devices [13], [14] show promising results and can be used for cryptographic applications in hardware security.

2) Physical unclonable function (PUF): It is a special hardware identifier that uses inherent fabrication variations of the device technology to produce an electronic response (fingerprint) when subjected to specific challenges [15]. PUFs have emerged as useful solutions for preventing semiconductor counterfeiting, chip identification, resistance to side-channel attacks, and malicious Trojans [16]. PUFs are used in cryptographic key generation access and authentication, which are difficult to replicate. The challenge response of the PUF creates a cryptographic key for a particular device. Several PUF architectures have been proposed in the literature in recent years using spin-based devices [17]- [19]. Fig. 3 shows a typical circular MTJ stack that can be used for PUF-based hardware [19]. Equation (1)-(2) describes the commonly used PUFs performance evaluation metrics.

$$Uniqueness = \frac{2}{k(k-1)} \sum_{i=1}^{k=1} \sum_{j=i+1}^{k} \frac{HD(R_i, R_j)}{n} \times 100\% \tag{1}$$

$$Robustness = \frac{1}{x} \sum_{y=1}^{x} \frac{HD(R_i, R_{i,j})}{n} \times 100 \tag{2}$$

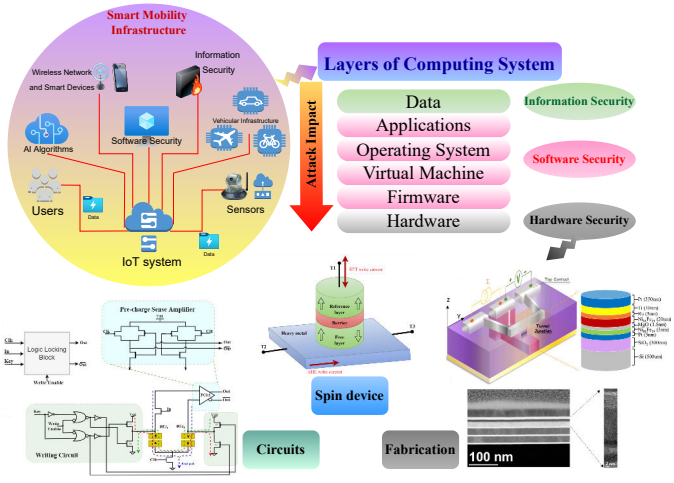

Fig. 2. A road-map for using spin-based devices in smart mobility infrastructure for hardware security.

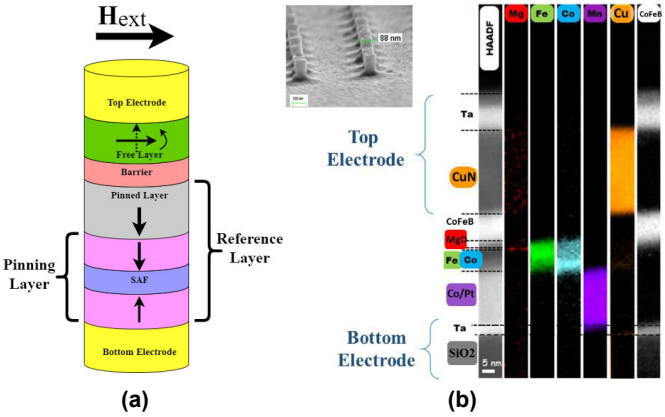

Fig. 3. (a) Pictorial representation of the circular MTJ. An SEM image of the patterned MTJs is inset. (b) The MTJ stack composition and the TEM image of the multi-layers [19].

3) Logic Locking (LL): It is a method in which KEY inputs are inserted to enable new logic mechanisms into the circuit, which causes the circuit to perform incorrect operation unless the correct KEY values is fed. A vast number of LL methods have been proposed to protect the integrity, and privacy of the ICs [20]. In Fig. 4, using a three-terminal voltage-gated spin-orbit torque MTJ, an LL block is created [21]. Interest has grown in developing LL mechanisms using emerging 2T, and 3T MTJ devices [22]. Fig. 5 shows the use of thermally stable shape-anisotropy assisted-perpendicular magnetic anisotropy based double layer MTJ (s-PMA DMTJ) for LL block and the polymorphic logic behavior for camouflaged layout [23].

The output corruption measurement can be evaluated by the following general equations where Equation (3) determines the average Hamming Distance (H.D.) [24]:

$$\frac{1}{y \times N_I \times N_K} \sum_{i=1}^{N_K} \sum_{j=1}^{N_I} H.D.\left(Y_L\left(I_j, K_i\right), Y_o\left(I_j\right)\right) \times 100\% \tag{3}$$

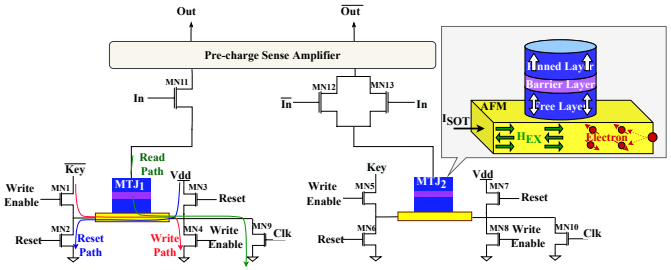

Fig. 4. LL block circuit schematic using VGSOT-MTJ [21].

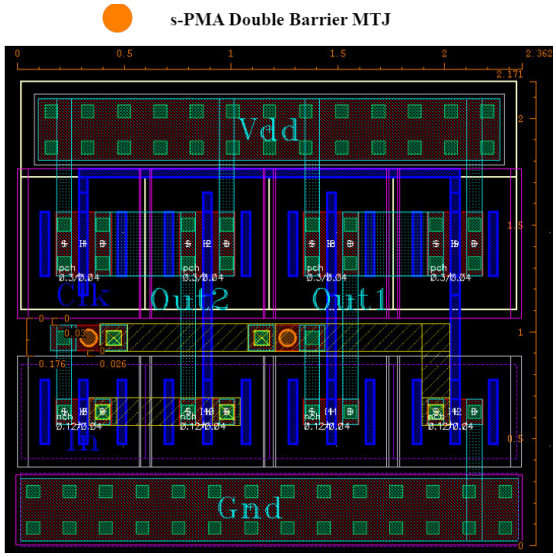

Fig. 5. Layout Camouflage diagram indicating the polymorphic logic for s-PMA DMTJ block as a counter to RE based attacks in an LL system.

Where, N_K is the KEY values, each with N_I input combinations, y is the number of output bit, Y_L is the locked output, and Y_o represents the original circuit output.

Output error rate [25], which is the probability of erroneous bit(s) at the output vector of Y_L is given by:

$$\frac{1}{N_I \times N_K} \sum_{i=1}^{N_K} \sum_{j=1}^{N_I} z \times 100\% \tag{4}$$

Here,

$$z = \begin{cases} 1, & \text{if } H.D.\left(Y_L\left(I_j, K_i\right), Y_o\left(I_j\right)\right) \geq 1 \\ 0, & \text{else} \end{cases} \tag{5}$$

4) Watermarking: Watermarking is a Passive method of ensuring hardware security that is used to prevent the counterfeiting of IPs by generally embedding digital image and video watermarks. With the evolution of hardware watermark, beyond CMOS devices as an alternative hardware solution was proposed to utilize the unique physical characteristic of such devices. Researchers in [26] demonstrated the hardware watermark generation using the photo-response of MoS_2 memtransistor. Recently, researchers in [27] designed an approach towards generating hardware watermark at the circuit level in

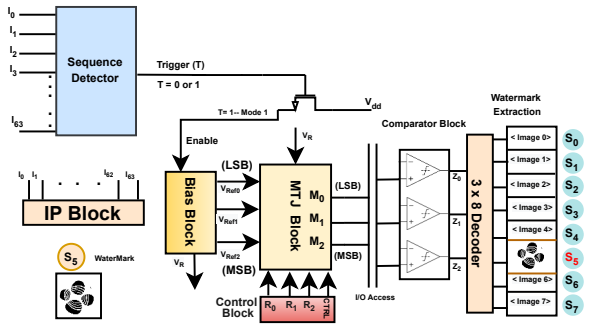

Fig. 6. Watermark generation circuit using field assisted SOT-MTJ [27].

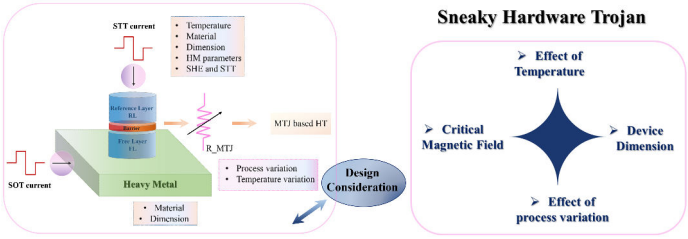

Fig. 7. Modelling of sneaky HT for field sensitive SOT-MTJ.

an FSM-inspired approach, where the magnetic sensitivity of the MTJ was used as a passive method to guide the MTJ through a specific state sequence as shown in Fig. 6.

C. Current Threats: Magnetic Tunnel Junction Based Hardware Trojan

Malicious modification at the hardware level can cause altered IC functionality, leading to disastrous results concerning the security of the system. Usual design-time verification and post-fabrication methods may not be sufficient to counter emerging HTs using emerging beyond-CMOS devices such as spin-based MTJs [28], which can cause DoS in smart mobility systems. Fig. 7 demonstrates the approach to model a sneaky HT. Fig. 8 shows the insertion of such structure in a typical system-on-chip (SoC) design flow [28]. In Fig. 9, the DoS operation is demonstrated for the MTJ-based HT where the application of external $B_{Ext} \approx 10$ mT can cause malfunctioned behavior at the circuit simulation level.

II. Assessment of International Regulation on Hardware Systems

Fig. 10 demonstrates the cybersecurity framework with highlighted blocks indicating additional regulation for MTJ devices [29]. All cyber systems are constructed using the physical hardware of the IC chips in modern computers, electronics, and communications networks in smart mobility. A compromised physical component severely affects the system's cybersecurity by undermining all additional layers. Therefore, hardware security focuses on safeguarding systems from vulnerabilities at the devices' physical layer. Hardware security must be given more attention to maintain the health

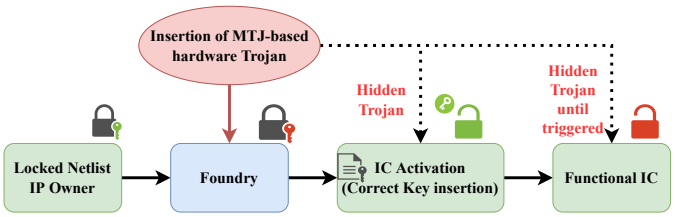

Fig. 8. Insertion of SOT-MTJ based HT in LL SoC design flow.

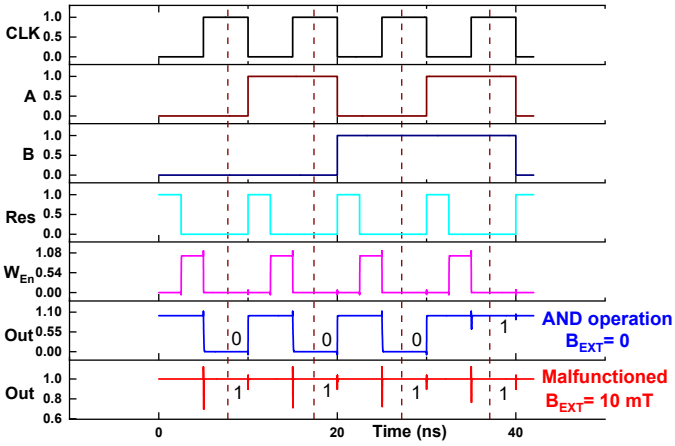

Fig. 9. Normal and DoS behaviour of SOT-MTJ based HT based AND logic block [24].

of our increasingly interconnected world in light of recent globalization in industry, technology, and geopolitics.

A. Current CMOS based devices

The semiconductor industry has been transformed globally over the past few decades. As a result, a 90% decline has been experienced in the number of companies with cutting-edge manufacturing capabilities leaving behind only three companies (Intel, Samsung, and TSMC) conducting state-of-the-art foundries [30]. Low power consumption and high operational speed of ICs resulted in reduced device feature size making the semiconductor industry encounter a limit in the underlying physics. As the size is further reduced, undesirable quantum mechanical effects will become increasingly prominent. Therefore, emerging technologies such as spintronics promise alternatives to CMOS devices due to their low power consumption, non-volatility, ease of fabrication in the silicon substrate, high endurance, etc.

B. Roadmap for Spin-based devices

Fig. 10 shows the cybersecurity framework as mentioned in [29]. The highlighted blocks in Fig. 10 are directly affected by emerging hardware like MTJs when considered for security mechanisms like cryptography, secure architectures, physical security, and Infrastructure security. Threat management, like specialized HTs and other attacks, are possible, and updates

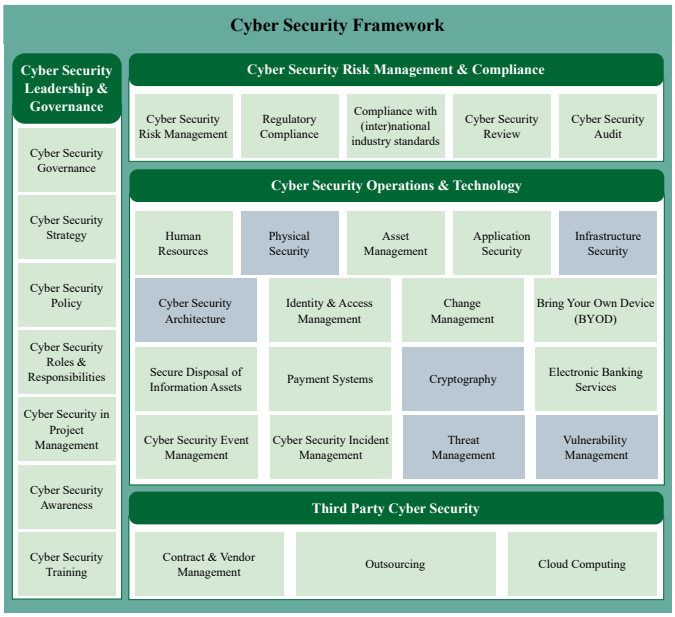

Fig. 10. Cybersecurity framework [29] with highlighted blocks indicating extra regulation for MTJ devices.

become essential. Also, as new hardware security primitives are employed using MTJ devices, specific vulnerabilities may arise for those structures that need to be addressed in the Vulnerability management block. Other blocks' design remains more or less the same, and depending on the application, some improvements may be required in the future. The cybersecurity regulation for hardware systems thus will need in the future to incorporate the physical characteristic of the emerging hardware paradigms and amendment in corresponding software and information security paradigms arising due to such novel device implementation.

III. Conclusion

With the world moving towards smart mobility systems, many electronic devices have been connected for information exchange and computation. The reliability and cybersecurity aspects of these systems have become a big concern. Intelligent attackers can leak information and threaten the denial of service of connected systems in a mobility infrastructure. In various layers of computing systems, the importance of hardware security is paramount. Globalization of IC design and fabrication has led to growing cost and design complexity, resulting in severe security concerns. Hardware Trojans, IP theft and various other attacks can offer serious problems from untrusted third parties. Recent advancements in beyond-CMOS devices have developed several novel attacks and defense mechanisms at the hardware level. In this study, we present a comprehensive assessment of and need for cybersecurity regulation for next-generation intelligent and secure hardware systems based on spintronic MTJ devices due to a growing interest in utilizing them for various active and passive security primitives.

REFERENCES

[1] M. Wallin, "What is smart mobility and why is it important?," *Verizon Connect.* [Online]. Available: verizonconnect.com/resources/article/smart-mobility.

[2] "Smart mobility: definition, solutions and all you need to know," *Tomorrow.city.* [Online]. Available: tomorrow.city/a/smart-mobility-definition-solutions-and-all-you-need-to-know.

[3] J. Srinivas, A. K. Das, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Future Gener. Comput. Syst.,* vol. 92, pp. 178–188, 2019.

[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 des. integr. circuits syst.*, vol. 40, no. 6, pp. 1010–1038, 2021.

[5] Wikipedia contributors, "Information security," *Wikipedia, The Free Encyclopedia,* 23-Jan-2023.

[6] J.-G. (jimmy) Zhu and C. Park, "Magnetic tunnel junctions," *Mater. Today (Kidlington),* vol. 9, no. 11, pp. 36–45, 2006.

[7] S. Ghosh, "Spintronics and Security: Prospects, Vulnerabilities, Attack Models, and Preventions," *in Proceedings of the IEEE,* vol. 104, no. 10, pp. 1864-1893, Oct. 2016.

[8] R. Mishra and H. Yang, "Emerging Spintronics Phenomena and Applications," *IEEE Trans. Magn.,* vol. 57, no. 1, pp. 1–34, 2021.

[9] M. Stone *et al.,* "Anomalous properties of sub-10-nm magnetic tunneling junctions," *in 2015 Fourth Berkeley Symposium on Energy Efficient Electronic Systems (E3S),* 2015.

[10] R. Mishra, T. Kim, J. Park, and H. Yang, "Shared-write-channel-based device for high-density spin-orbit-torque magnetic random-access memory," *Phys. Rev. Appl.,* vol. 15, no. 2, 2021.

[11] S. Srinivasan, A. Sarkar, B. Behin-Aein, and S. Datta, "All-spin logic device with inbuilt nonreciprocity," *IEEE Trans. Magn.,* vol. 47, no. 10, pp. 4026–4032, 2011.

[12] W. H. Choi *et al.,* "A Magnetic Tunnel Junction based True Random Number Generator with conditional perturb and real-time output probability tracking," *in 2014 IEEE International Electron Devices Meeting,* 2014.

[13] Z. Fu *et al.,* "An overview of spintronic True Random Number Generator," *Front. Phys.,* vol. 9, 2021.

[14] N. Onizawa, S. Mukaida, A. Tamakoshi, H. Yamagata, H. Fujita and T. Hanyu, "High-Throughput/Low-Energy MTJ-Based True Random Number Generator Using a Multi-Voltage/Current Converter," *in IEEE Transactions on Very Large Scale Integration (VLSI) Systems,* vol. 28, no. 10, pp. 2171-2181, Oct. 2020.

[15] G. Suh *et al.,* "Physical unclonable functions for device authentication and secret key generation," *IEEE DAC,* Jun. 2007, pp. 9–14.

[16] C. Herder, M. Yu, F. Koushanfar and S. Devadas, "Physical Unclonable Functions and Applications: A Tutorial," *Proceedings of the IEEE,* vol. 102, no. 8, pp. 1126-1141, Aug. 2014.

[17] G. Finocchio *et al.,* "Spin–orbit torque based physical unclonable function,"*J. Appl. Phys.,* vol. 128, no. 3, p. 033904, 2020.

[18] S. Lee *et al.,* "Spintronic physical unclonable functions based on field-free spin-orbit-torque switching," *Adv. Mater.,* vol. 34, no. 45, p. e2203558, 2022.

[19] D. Divyanshu, R. Kumar, D. Khan, S. Amara, and Y. Massoud, "Physically unclonable function using GSHE driven SOT assisted p-MTJ for next generation hardware security applications," *IEEE Access,* vol. 10, pp. 93029–93038, 2022.

[20] A. Chakraborty *et al.,* "Keynote: A Disquisition on Logic Locking," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,* vol. 39, no. 10, pp. 1952-1972, Oct. 2020.

[21] D. Divyanshu, R. Kumar, D. Khan, S. Amara, and Y. Massoud, "Design of VGSOT-MTJ-based logic locking for high-speed digital circuits," *Electronics (Basel),* vol. 11, no. 21, p. 3537, 2022.

[22] D. Divyanshu, R. Kumar, D. Khan, S. Amara, and Y. Massoud, "Logic locking using emerging 2T/3T magnetic tunnel junctions for hardware security," *IEEE Access*, vol. 10, pp. 102386–102395, 2022.

[23] D. Divyanshu, R. Kumar, D. Khan, S. Amara, and Y. Massoud, "An Approach towards Designing Logic Locking Using Shape-Perpendicular Magnetic Anisotropy-Double Layer MTJ," *Electronics (Basel),* vol. 12, no. 3, p. 479, Jan. 2023.

[24] J. Rajendran *et al.,* "Fault analysis-based logic encryption," *IEEE Trans. Comput.,* vol. 64, no. 2, pp. 410–424, 2015.

[25] A. Sengupta, M. Nabeel, N. Limaye, M. Ashraf, and O. Sinanoglu, "Truly stripping functionality for logic locking: A fault-based perspective," *IEEE Trans. Comput.-aided Des. Integr. Circuits Syst.,* vol. 39, no. 12, pp. 4439–4452, 2020.

[26] Aaryan Oberoi, Akhil Dodda, He Liu, Mauricio Terrones, and Saptarshi Das, "Secure Electronics Enabled by Atomically Thin and Photosensitive Two-Dimensional Memtransistors", *ACS Nano*, 2021, 15 (12), 19815-19827.

[27] D. Divyanshu, R. Kumar, D. Khan, S. Amara, and Y. Massoud, "FSM inspired unconventional hardware watermark using field-assisted SOT-MTJ," *IEEE Access,* vol. 11, pp. 8150–8158, 2023.

[28] R. Kumar, D. Divyanshu, D. Khan, S. Amara, and Y. Massoud, "Spin orbit torque-assisted magnetic tunnel junction-based hardware Trojan," *Electronics (Basel)*, vol. 11, no. 11, p. 1753, 2022.

[29] Saudi Arabian Monetary Authority, "Cyber Security Framework," 2017. [Online]. Available: https://www.sama.gov.sa/en-US/RulesInstructions/CyberSecurity/Cyber20Security20Framework.pdf.

[30] E. V. Levine, and A. Pipikaite, "Hardware is a cybersecurity risk. Here's what we need to know," *World Economic Forum.* [Online]. Available: https://www.weforum.org/agenda/2019/12/our-hardware-is-under-cyberattack-heres-how-to-make-it-safe/.