IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 4 January 2023, accepted 18 January 2023, date of publication 23 January 2023, date of current version 26 January 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3238807

RESEARCH ARTICLE

FSM Inspired Unconventional Hardware Watermark Using Field-Assisted SOT-MTJ

DIVYANSHU DIVYANSHU, RAJAT KUMAR, DANIAL KHAN, SELMA AMARA, (Member, IEEE), AND YEHIA MASSOUD, (Fellow, IEEE)

Computer, Electrical and Mathematical Sciences and Engineering, King Abdullah University of Science and Technology, Thuwal 23955-6900, Saudi Arabia

Corresponding author: Yehia Massoud (yehia.massoud@kaust.edu.sa)

ABSTRACT The globalization of the Integrated Circuits supply chain has increased threats from untrusted entities involved in the process. Several mechanisms, such as logic locking, watermarking and split manufacturing, are widely used to ensure hardware security. This study describes a novel method for creating hardware watermarks inspired by finite-state machines. It makes use of the unique physical property of magnetic tunnel junctions that are based on spin-orbit torque. The design strategy is described in detail, including the use of an EDA tool to analyze and take advantage of the unique switching properties of MTJ, their non-volatility, and their reliance on an external magnetic field to direct information through a predetermined order of states in a manner akin to an FSM. Furthermore, the performance prospects are analyzed using Monte Carlo simulations. For the 5% and 10% of process variation in the key MTJ parameters, the accuracy of 100% and 99.80%, respectively, are achieved. In control signal voltage variation, a tolerance of 9% (0.91V) is observed. The required state transition is not altered, demonstrating a tolerable sensitivity to temperature variation from 250K to 350K. The security aspects and methodology for the approach are explained to ensure a more robust and practical application, and finally, a comparison is made with other FSM-based watermarks.

INDEX TERMS Hardware watermarks, hardware security, spintronics, spin-orbit torque (SOT), magnetic tunnel junction (MTJ), finite-state machine (FSM).

I. INTRODUCTION

Over the past decades, intellectual property (IP) based System-on-Chip (SoC) design has attracted significant attention in the semiconductor industry. IP cores are recycled to accelerate time-to-market while preserving low design costs. However, these benefits of the design-reuse paradigm have compromised security and raised severe concerns about IP infringements. Various untrusted and unreliable third-party agents, who participate at different stages of the SoC design cycle, often misuse these IPs. IP infringement can take various forms, such as overbuilding, IP cloning, and counterfeit ICs [1]. To address these security concerns, Design-for-Security (DfS) has emerged as a crucial and integral part of the IC design that can further be classified into two categories: (a) Active methods and (b) Passive methods. Logic locking, split-manufacturing, and IC camouflaging are active methods that can prevent IP piracy, while passive methods like Fingerprinting and Watermarking are employed to detect IP piracy.

Security measures come with an expense in some form, like different hardware/design changes. Intelligent attackers may decipher the security mechanism using several techniques like reverse engineering, Machine-Learning based attacks, and side-channel analysis [2]. Spintronics devices offer several security aspects for applications in hardware security [3], [4], and other important applications [5], [6], [7]. MTJ is a widely investigated spintronic device and has been used for different hardware security primitives in recent research [8], [9], [10], [11], [12]. The use of emerging beyond CMOS devices for watermark generation currently needs to be well explored and thus provides many opportunities for utilizing the unique physical characteristic of such devices for generating watermark solutions. In the context of 2D materials-based novel watermarking generation,

The associate editor coordinating the review of this manuscript and approving it for publication was Santosh Kumar.

photo-response of MoS_2 mem-transistor [13] is described. A timeline of the evolution of watermarking and anti-counterfeiting techniques is mentioned in [14]. Passive methods like watermarking in hardware security are still in the early stages of research interest. This work provides a unique approach to generating the hardware watermark using the magnetic sensitivity of the SOT-MTJ device at the circuit level. This work explores a three-terminal SOT-MTJ device for secure watermark generation considering various design parameters, PVT variation, and security analysis. Instead of using spin-transfer torque (STT) current, an external magnetic field is used as a critical element for deterministic switching along with SOT current, which is usually not used because of the requirement of the magnetic fields.

The rest of the paper is organized as follows: Section II explains the background of watermarking and magnetic tunnel junctions. Section III discusses the circuit operation for the proposed secure watermarking generation. Experimental results are discussed in Section IV. Finally, Section V concludes the paper.

II. BACKGROUND

A. WATERMARKING

Watermarking is a technique that allows the IP designer to conceal authorship information inside the design without affecting the functionality of the design. This watermark is used for IP ownership authentication against suspected IP infringements in legal proceedings [15]. An ideal watermarking method is simple to insert, verifiable, and well integrated into the design, and yet does not suffer from high overhead and removal attacks [16]. The following characteristics are necessary for a watermarking strategy [17], [18].

- The functionality of the original design must not be changed by the watermarked design.
- The overhead incurred should be minimal due to the watermark's insertion.
- The watermark needs to be resilient to various modification and removal attacks.
- Credible authorship proof is essential to be presented in the court as strong evidence for claiming the authorship.

IP watermarking techniques can be sub-divided into five categories: (a) Constrained-based watermarking, (b) Side channel-based watermarking, (c) Test structure-based watermarking, (d) Digital signal processing (DSP)-based watermarking, and (e) Finite state machine (FSM) watermarking. The constrained-based watermarking strategy consists of system-level, behavior-level, logic-level, and physical-level synthesis. It is a complex optimization problem with exponential growth in the acceptable solutions concerning the input size, and IP can be considered the solution to the optimization problem [19]. Side channel-based watermarking can exploit a cryptographic device that has leaked physical information and is widely used to recover the secret keys [20]. With a side-channel-based watermark, a watermarking signal is embedded within the side channel instead of secret information being leaked out. The central concept is to incorporate a watermark into an IP core using a side channel, such as power consumption. The verifier then extracts the watermark and certifies ownership using that side-channel information. Test structure-based watermarking embeds a watermark at the behavior level into a test sequence. The test signals must be traceable once the IPs have been integrated into the complete SOCs. Using this advantage, the authors combined the watermark generating circuit with this test sequence to observe and test any IP in the chip even after packaging the chip [21]. In the test mode, the watermark sequences and the output test patterns are sent by the selected IP, and the IP provider identity can be determined based on the watermark sequence. Digital signal processing (DSP)-based watermarking is implemented at the algorithmic or system level [22] to allow designers to slightly alter the decibel (dB) specifications of the filters without sacrificing their performance. A high-level digital filter encodes a single character (7 bits) as a watermark. The filter design is then divided into seven segments, each used as a modulation signal for one of the bits. The FSM-based watermark is incorporated at the behavioral level while remaining inoffensive to chip functionality courtesy of adding additional FSM transitions or states. FSM-based watermarking can be divided into two types: state-based watermarking [23] and transition-based watermarking [24]. State-based watermarking techniques require encoding a changing state or adding additional states. In contrast, transition-based watermarking techniques employ unused transitions or introduce new ones to the FSM.

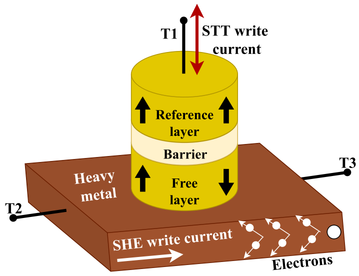

FIGURE 1. SOT-MTJ device structure.

B. MAGNETIC TUNNEL JUNCTION

In the SOT-MTJ device, an MTJ stack that consists of a barrier layer sandwiched between two ferromagnetic layers is placed on a heavy metal (HM), as shown in Fig. 1. Depending on the magnetization orientation of the free layer with respect to pinned layer, the state of MTJ is determined. Several switching mechanisms are possible, like STT switching, SOT-assisted STT switching, and thermally and field-assisted switching. Field-assisted switching is generally less used in MTJ-based memory and logic circuits because of the difficulty of generating a magnetic field; Therefore, magnetization control via electric current is preferred.

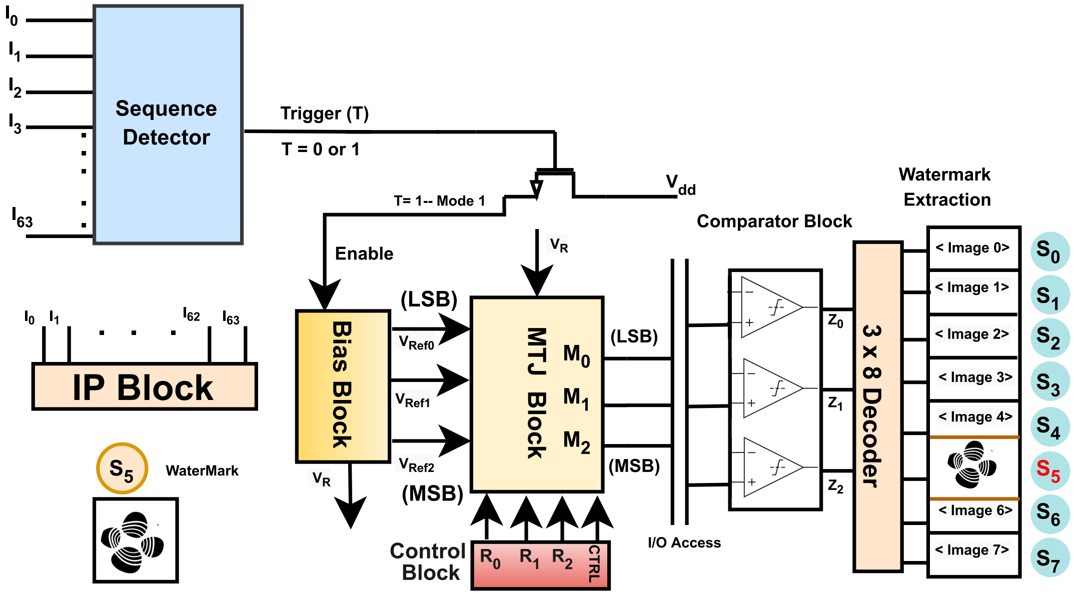

FIGURE 2. Block Diagram of the proposed watermark generation.

However, this work uses a magnetic field to generate a watermark because proof of authentication is not frequent. Magnetic field-assisted switching can enhance security to a very high degree against various threats generally encountered in watermark design. Equation 1 is the Landau-Lifshitz-Gilbert (LLG) equation that governs the magnetic dynamics of the free layer, and equation 2 provides the MTJ resistance [25].

$$\frac{\partial \vec{m}}{\partial t} = -\gamma \mu_0 \vec{m} \times \vec{H}_{eff} + \alpha \vec{m} \times \frac{\partial \vec{m}}{\partial t} - \xi P J_{STT} \vec{m} \times (\vec{m} \times \vec{m}_r) - \xi \eta J_{SOT} \vec{m} \times (\vec{m} \times \vec{\sigma}_{SOT}) \quad (1)$$

$$R_{MTJ}\,(V_{MTJ}) = \frac{R_p\left[1 + (V_{MTJ}/V_h)^2 + TMR_0\right]}{1 + \left(V_{MTJ}^2/V_h^2\right) + TMR_0[0.5(1+\cos\theta)]} \quad (2)$$

Here, $\vec{m}$ and $\vec{m}_r$ are the unit vector along with magnetization of the free layer and the pinned layer, respectively, γ is the Gyromagnetic ratio, μ_0 is the vacuum permeability, $\vec{H}_{eff}$ is the effective magnetic field, α is the Gilbert damping coefficient, P is the polarization factor, J_{STT} and J_{SOT} are the STT and SOT current density and $\vec{\sigma}_{SOT}$ is the polarization direction of the spin current injected in the free layer. TMR_0 is the TMR ratio at zero bias, V_h is the bias when TMR is divided by half, θ is the spin hall angle, and R_p is the parallel state resistance of the MTJ. $J_{STT} = 0$ is set so that $\vec{m}$ is dependent upon J_{SOT} and $\vec{H}_{eff}$ as input parameters.

III. CIRCUIT OPERATION

A. WATERMARK GENERATION CIRCUIT

The proposed watermark is embedded in the design, and it is suggested to insert post-synthesis to avoid optimization constraints. The working operation of watermark generation does not interfere with regular circuit operation and provides credible and secure proof of ownership. The watermark is designed in such a way that even with a machine learning-based approach employing trial and error, the likelihood of the watermark being detected and generated by an untrusted entity is very low. The block diagram of the overall strategy adopted in this work is shown in Fig. 2. It consists of a 64-bit sequence detector (SD), which receives input from the IP block to ensure the watermark inputs are distributed in the design. A trigger signal (T) is generated, with a very low probability of triggering, i.e., 2^{-64}. The signal T=0 disables the watermark generation process, and T=1 provides specific input to the MTJ block (3 bits) with different values. The control block consists of different control signals to guide the state of the MTJs. Comparators with reference at 0 V are used to ensure proper selection of logic levels (Z_2 (MSB) to Z_0). Finally, the watermark extraction block in each state stores a specific image, and the correct watermark image is stored in one of the states from S_0 to S_7. The IP owner designed the watermark extraction block, and information related to the watermark is confidential and can be used as a 'golden model' during proof of ownership. The watermark extraction block and comparators can also be inserted before the I/O access interface. With intelligent design, it will be possible to avoid I/O access, which is currently a disadvantage. However, inserting the watermark extraction block and comparators before the I/O access will increase the fabrication cost for all the chips, reduce security advantage by becoming more prone to revealing information for reverse engineering-based attacks, and increase area consumption on a silicon substrate as a trade-off for removing the I/O access.

B. MTJ BLOCK OPERATION

In the MTJ block described in Fig. 3, the Verilog-A-based behavioral compact model of MTJ is used [19]. Three MTJ

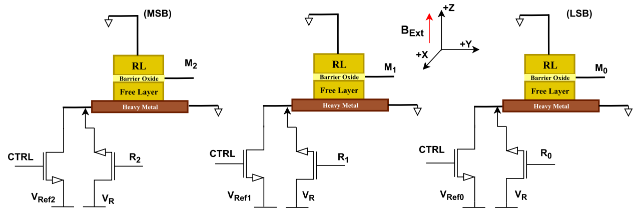

FIGURE 3. Internal structure of a MTJ block.

devices are used with different sets of input bias ($V_{Ref0} =$ 250 mV; $V_{Ref1} = 200$ mV; $V_{Ref2} = 150$ mV; $V_R = 400$ mV), thus requiring different magnetic fields (B_{Ext}) for switching ($B_{Ext,Critical}$ $[S_0 \rightarrow S_1] = 7$ mT; $B_{Ext,Critical}$ $[S_1 \rightarrow S_3] =$ 13 mT; $B_{Ext,Critical}$ $[S_3 \rightarrow S_7] = 18$ mT). The most significant bit (MSB) M_2 is given a lower bias and thus requires more torque for switching from B_{Ext}. The control block of Fig. 2 generates a CTRL signal (Rise time and Fall time = 10 ps, Pulse Width = 5 ns). This CTRL signal is used to write the MTJ from logic 0 to Logic 1 with the help of B_{Ext}. A significant reverse bias (V_R) is applied when (R_{0-2}) (Rise time and Fall time = 10 ps, Pulse Width (T_R) = 5 ns) is applied as the control signal to erase the magnetization information as shown in Fig. 4. This allows the designer to control the magnetization of the MTJ individually. The non-volatile nature of MTJ devices enables them to retain information once written, thus allowing controlled transitions between different states. The MTJ used here is a perpendicular magnetic anisotropy (PMA) MTJ, and thus its magnetic orientation is perpendicular (along the z-axis) to the x-y plane. B_{Ext} is applied along the +z direction to influence the magnetization. Table 1 contains the MTJ parameter used during the electrical simulations. All parameters are selected as the default values of the developed compact model. All the simulations are performed in a cadence spectre simulator in TSMC 40 nm technology with W/L = 3 and temperature at 300 K. State S_5 stores the watermark image, and Fig. 4 shows the transitions implemented to converge to S_5. $T_S \approx$ 3.36 ns is the settling time after erasing the data. The designer provides the control signals, and $B_{Ext} = 22$ mT is used as the magnetic key for this specific transition. Any other transition sequence will be invalid during the proof of authentication. It is also important to note that the term fac_{fl} mentioned in Table 1, which indicates the field-like torque effect, will significantly affect the magnetization dynamics. More details about this are present in [26]. The default value $fac_{fl} = 0.8$ is used in this work; however, the state transition is correct from 0.5 to 1.25, as obtained by parametric analysis.

IV. RESULT AND DISCUSSION

A. EFFECT OF PVT

This section includes design robustness for the intended successful transition concerning different conditions. Firstly, the effect of process variation (PV) in specific MTJ parameters such as TMR ratio, free layer thickness, and oxide layer thickness is analyzed. 1000 times Monte-Carlo simulations are performed to include the variation from different levels of PV following Gaussian distribution in the above-mentioned MTJ parameters. Low-discrepancy sequence (LDS) sampling is used during the simulation, and the results are listed in Table 2. The correct sequence accuracy of 99.80% is achieved even with significant 10% variations indicating impressive tolerance to device imperfection, as shown in

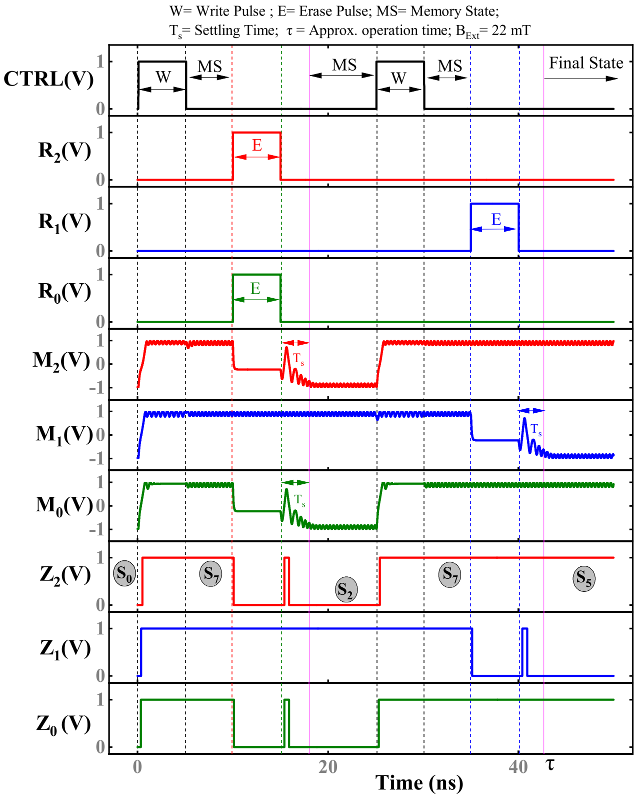

FIGURE 4. State Transition Waveform used to converge to state S_5.

TABLE 1. MTJ Device and Technology parameter used during simulation.

Parameter	Values
MTJ Dimension and Shape	40 nm × 40 nm, circular
Free Layer Thickness	0.7 nm
Oxide Layer Thickness	0.85 nm
HM Length, Width, and Height	60 nm × 40 nm × 3 nm
Gilbert Damping Coefficient	0.03
Saturation Magnetization	800,000 emu/cm^3
TMR, Anisotropy Field	120%, 88,000 A/m
Spin Hall Angle, Heavy Metal Resistance	0.3, 1000 Ω
Potential Barrier Height of MgO	0.5 V
Polarization Factor and fac_{fl}	0.61 and 0.8
Initial Configuration, Simulation Steps	Set at Parallel, 1ps

TABLE 2. Monte-Carlo simulation showing R_{M2} operating point shift with Process Variation in MTJ parameters.

PV %	Mean Value	SD	Skewness	Correct Transition
3 %	8.02 kΩ	0.485 kΩ	81.621 mΩ	100%
5 %	8.07 kΩ	0.819 kΩ	180 mΩ	100%
10 %	8.28 kΩ	1.695 kΩ	429.39 mΩ	99.80%

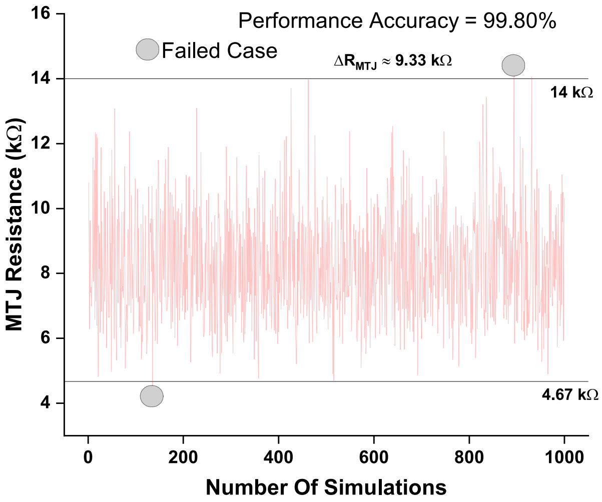

FIGURE 5. 1000 times Monte-Carlo simulation result with 10% PV in TMR, free layer and oxide layer thickness.

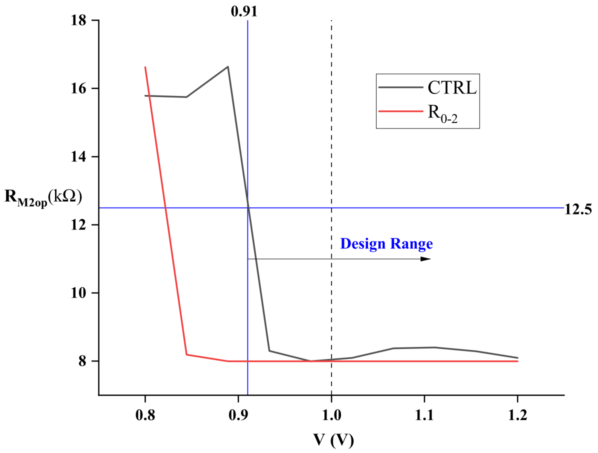

FIGURE 6. Variation in voltage of control signals and its effect on the MSB resistance.

Fig. 5. To further test the voltage level variation in the control signal pulse applied to the MTJ block, the voltage variation effect on the MSB operating point resistance (R_{M2op}) is observed, and a tolerance of 9% (0.91V) is obtained, as shown in Fig. 6. To see the effect of temperature variation, a temperature sweep from 250 K to 350 K is applied, and $\Delta R_{MTJ} = 0.334$ kΩ change is observed. However, no change in desired state transition is observed, indicating acceptable tolerance to temperature variation. The PVT simulation showed that the MTJ block has an acceptable tolerance to variation in various parameters. Thus, from the circuit design perspective, it shows possible practical applications.

B. SECURITY ANALYSIS

This section discusses some of the security aspects of the proposed work. Firstly, let us define some of the symbols used. Let the applied external magnetic field (B_{Ext}) lies in Γ, where $\Gamma_0 \in$ (-∞, 0 mT), $\Gamma_1 \in$ [0 mT, 6mT), $\Gamma_2 \in$ (7 mT, 12mT), $\Gamma_3 \in$ (13 mT, 17mT), $\Gamma_4 \in$ (18 mT, 25mT) and $\Gamma_5 \in$ (25 mT, ∞). Let S $\neq$ 0 be a finite set of states, S_i, $S_n \in$ S, where S_i is the current state with S_0 being the initial reset state and S_n being the next state, τ represents the overall time required in the correct state transition as designed and shown in Fig. 4, and χ represents the allowed control signals set by the designer. Let ψ represent the transition function which governs $S_i \rightarrow S_n$ under some specific condition.

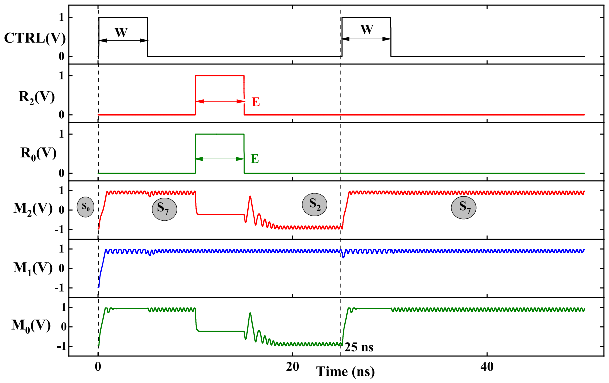

FIGURE 7. State transition waveform when CTRL is applied at t = 0 and t = 25 ns, desired state transition is obtained.

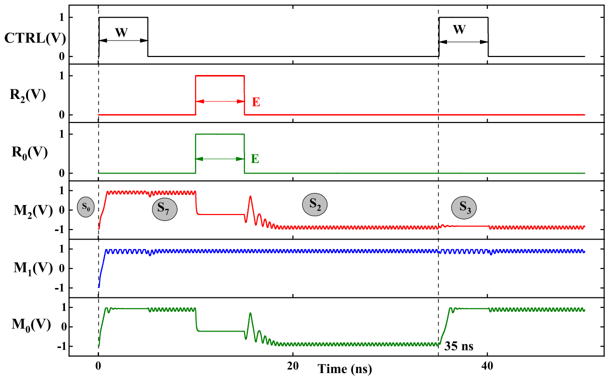

FIGURE 8. State transition waveform when CTRL is applied at t= 0 and t = 35 ns, incorrect state transition is obtained.

1) PROOF OF OWNERSHIP

The strength is ascertained by the probability of obtaining the same watermark while simultaneously having a low probability of false triggering. Here the triggering probability is very low and approximated as:

P<Correct State> $\approx 2^{-64}$ * <Analog Magnetic Key (Γ_4)> * <Correct Control Block Signals (χ) >

which has a very low probability of triggering as an external field is also used with specific control signal sequences. In Fig. 7 and Fig. 8, the control signal is applied at different instances of time, and different state transitions are observed; this behavior is per equation (1)-(2) and demonstrates that the state transition is also a function of the time instance of the control sequence. Algorithm 1 contains the methodology to obtain the desired operation.

TABLE 3. Eye-Diagram analysis for countering tampering and removal attacks.

MTJ bit	Level 0 Mean	Level 1 Mean	Eye Amplitude & Height	Eye Width	SNR	Deterministic Jitter
M_0 (LSB)	-0.685 V	0.882 V	1.567 V, 0.492 V	3.252 ns	4.372	586 ps
M_1	-0.683 V	0.894 V	1.578 V, 0.493 V	3.137 ns	4.364	525.7 ps
M_2 (MSB)	-0.684 V	0.882 V	1.566 V, 0.503 V	3.183 ns	4.42	531.9 ps

Algorithm 1 Proof of Ownership : Methodology

```
Step 1: Enable the watermark block
Ensure $T = 1$
while $T = 1$ do
    if $I_0$-$I_{63}$ Matches the owner data-sheet than
        Proceed to Step 2
    else
False Triggering: Hardware Trojan/Tampering In the IP
  Block/SD ⇒ Discard the chip/ Claim Counterfeiting
    end if
    Step 2:
     Ensure $S_i = S_0$ (Set Initial state)
      $R_{0\to2}|_{t=t_1} \cup$ Wait till $|_{t\geq t_1+T_R+T_S} \cup B_{Ext} \in \Gamma_1$
      if $S_i \neq S_0$ then
          CLAIM CLAIM: Tampering/Counterfeiting
      else
          Proceed to Step 3:
      end if
     Step 3:
      Ensure $S_n \Rightarrow S_0 \to S_7 \to S_2 \to S_7 \to S_5$
     if $S_n \not\Rightarrow S_0 \to S_7 \to S_2 \to S_7 \to S_5$ then
          CLAIM: Tampering/Counterfeiting
     end if
     while $S_n \Rightarrow S_0 \to S_7 \to S_2 \to S_7 \to S_5$ do
          if $B_{Ext} \in \Gamma_4 \cup$ t $\approx t_1 + \tau \cup$ CTRL,$R_{0\to2} \in \chi$
  then
  Perform Eye-Diagram Test/Transient Measurement
          if True then
              CLAIM: Ownership
          else
              CLAIM: Tampering/Counterfeiting
          end if
      end if
   end while
```

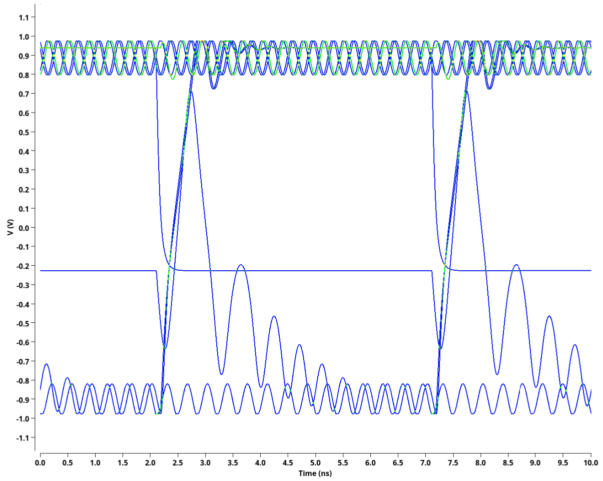

FIGURE 9. Eye diagram analysis for MSB bit.

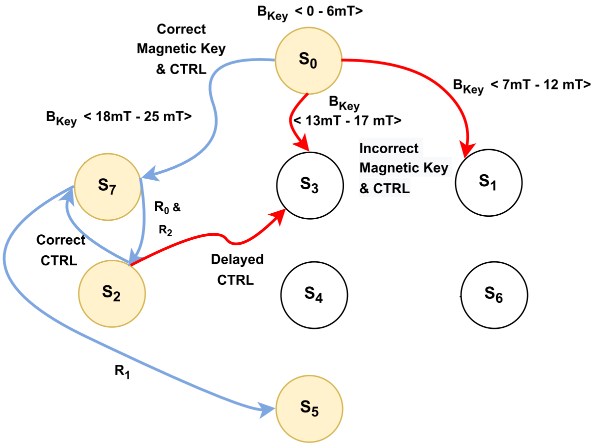

FIGURE 10. Overall state transition graph (STG) for the approach.

TABLE 4. Transient Analysis of MTJ bits for countering tampering and removal attacks.

MTJ bit	Rise Time(Max.)	Fall Time(Max.)	Delay(Max.)
M_0 (LSB)	501.6 ps	6.841 ns	49.11 ps
M_1	583.2 ps	6.84 ns	60.11ps
M_2 (MSB)	593.4 ps	6.839 ns	44.65 ps

2) REMOVAL ATTACKS AND TAMPERING

If the attacker removes the watermark block and replaces it with its watermark, proof of authentication can be easily verified; in the worst case, the attacker can implement the same hardware configuration to converge to the same state. To counter such rare cases, an Eye-Diagram test is performed with a Unit interval (UI) of = 5 ns and a Period of 2 * UI to create a centered eye diagram, as shown in Fig. 9. Eye diagram tests are used to test the signal integrity at a high data speed rate. It is challenging to clone the signal behavior of such an emerging device with great accuracy due to the complex and non-linear device characteristics. Table 3 contains eye-diagram results for each MTJ bit, and Table 4 contains information related to the transient behavior of the MTJs used here. These data can be used as a reference against cloning-based attacks. The approach used here is FSM inspired and not entirely based on the FSM watermarking approach used conventionally. Attacks like state re-encoding, circuit

TABLE 5. Comparison with other FSM-based watermarking techniques.

Type	Existing Technique	Performance Evaluation				Resistance to attack			
		Credibility	Overhead	Resiliency	Invisibility	Removal	Forging	Tampering	RE
State Based	Watermark as property [27]	Low	High	Low	Low	Low	Low	Medium	Low
	State Encoding based [23]	Medium	High	Medium	Low	Low	Low	Low	Low
Transition Based	Unused transition based [32]	Medium	Medium	Medium	Low	Medium	High	Medium	Low
	Existing Transition based [33]	Medium	Low	High	Medium	High	Low	Medium	Medium
	Robust watermarking [24]	High	Low	High	Medium	High	High	Medium	High
Hybrid	FSM and Test based [34]	High	Low	High	Medium	High	High	High	Medium
This Work	SOT-MTJ based	High	High	High	Low	Medium	High	High	High

RE: Reverse Engineering.

Re-timing, State Reduction [21] etc., are inefficient and can be easily detected.

3) TOLERANCE AGAINST MACHINE LEARNING (ML) BASED ATTACK AND REVERSE ENGINEERING

The complex device characteristic and dependence on different designs and external parameters to obtain the specific state is very unconventional, thus posing a solid resilience to conventional ML-based attacks. To demonstrate this idea, mathematical reasoning is provided where ML-based brute force attack will be computationally expensive compared to well-known binary decision diagrams to show this concept (BDD) [28], [29]. The state-transition diagrams (STGs) can be manipulated via ML-based attack if the transition relation and output functions are compromised by computing the image and pre-image of a set defined by its characteristic function and obtaining the set of reachable states. However, a detailed discussion on BDD properties, characteristics, and attacks on them is outside the scope of the work. However, a similar trend in Fig. 10 presents the STG diagram of this work. Where the highlighted states (S_0, S_2, S_5, and S_7) are the states of interest, and arrows highlighted in blue represents the desired state transition. The transition relation ψ for the STG shown in Fig. 10 is defined as follows:

$$\psi(S_i, \Gamma, \chi) \equiv f\{\frac{\partial \vec{m}}{\partial t} = -C_1\vec{m} \times \vec{H}_{eff} + C_2\vec{m} \times \frac{\partial \vec{m}}{\partial t} - C_3 J_{SOT}\vec{m} \times (\vec{m} \times \vec{\sigma}_{SOT}), MTJ_{D,Shape}, HM_{D,Res}\} \quad (3)$$

where C_1-C_3 are some constants. The ML-based attack thus will have to solve a highly non-linear vector-time-differential equation along with information related to other devices, circuits, and confidential watermark design parameters, which is computationally extremely expensive. In case no design information is leaked except for ψ and basic state transition information. Still, other parameters like the actual values of Γ, χ, and physical device dimension will be difficult to decipher using brute force ML algorithms compared to much simpler BDD-based FSM hardware watermarks. Thus this method, in general, is more robust to ML-based attacks. Another approach that an attacker can use is to deploy reverse-engineering attacks to obtain the device structure dimensions and material composition and then use an ML-based algorithm in conjugation. This method will be compelling, but Reverse Engineering is a destructive, time-consuming, and costly method, and de-packaging the chip can cause an error in the watermark structure. Also, keeping the comparator block and watermark extraction block described in section III-A outside the IC provides a counter against ML and reverse engineering-based attacks. These blocks are confidential property and add an extra layer of security at the cost of providing I/O access.

4) GENERAL SECURITY AND PERFORMANCE CONCERN

Application of a small amount of magnetic field ($B_{Ext} \approx$ 22 mT) does not affect the MOS transistors and can tolerate applied field up to 7T [31]. Thus, applying a magnetic key will not hinder the regular IP blocks. Even if a certain amount of information related to the design is leaked, it is still complicated for the attacker to copy the proof of authentication process. With the advancement of fabrication technology, the area overhead can be reduced significantly in the future, which is currently a clear disadvantage, along with the invisibility of the hardware watermark block, especially for smaller IP/ICs. Also, the complexity of design and fabrication compared to other methods is a significant concern for this approach. This approach of Hardware watermarking is not robust against several other threat models effectively, such as the insertion of Hardware Trojans, and can not detect skillfully inserted Trojans unless the Trojan changes the 64-bit input sequence required to trigger the watermarking operation. Table 5 gives a comparison with other FSM-based watermarking techniques. Emerging beyond CMOS devices for watermark generation is not well explored. Table 5 compares this work with other FSM-based approaches. This work has a clear disadvantage in overhead and needs to perform better in terms of invisibility.

V. CONCLUSION

SOT-MTJ is a non-volatile device with non-linear characteristics dependent on several external parameters. This article uses the external magnetic field as a passive method of generating the watermark. The designed circuit allows the user to converge and obtain the watermark, which helps to provide proof of authentication. This approach works satisfactorily with a higher security advantage but requires complex design, fabrication methodology, and extra hardware. Using an external magnetic field to guide the MTJ in an actual IP core properly and inserting the MTJ block with other CMOS devices in the SoC design is complex. Many aspects of hardware reliability, like aging and time dependent dielectric breakdown (TDBB), need to be ascertained for practical application. A detailed fabricated attempt for such analysis is currently out of the scope of this work. By utilizing SOT-MTJ compact model in EDA tools, this work offers a potential future use for hardware watermarks. Monte Carlo simulations are performed to show the robustness to the device imperfections. Using STG diagrams and security considerations, broad algorithmic approaches are used to build such unconventional watermarks, and eye-diagram tests are performed to counter removal and tampering effects.

REFERENCES

[1] 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.

[2] S. Ghosh, M. N. I. Khan, A. De, and J.-W. Jang, "Security and privacy threats to on-chip non-volatile memories and countermeasures," in *Proc. 35th Int. Conf. Comput.-Aided Design*, Nov. 2016, pp. 1–6.

[3] S. Ghosh, "Spintronics and security: Prospects, vulnerabilities, attack models, and preventions," *Proc. IEEE*, vol. 104, no. 10, pp. 1864–1893, Oct. 2016.

[4] A. Japa, M. K. Majumder, S. K. Sahoo, R. Vaddi, and B. K. Kaushik, "Hardware security exploiting post-CMOS devices: Fundamental device characteristics, state-of-the-art countermeasures, challenges and roadmap," *IEEE Circuits Syst. Mag.*, vol. 21, no. 3, pp. 4–30, 3rd Quart., 2021.

[5] R. Mishra and H. Yang, "Emerging spintronics phenomena and applications," *IEEE Trans. Magn.*, vol. 57, no. 1, pp. 1–34, Jan. 2021.

[6] 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, Oct. 2011.

[7] S. Dhull, A. Nisar, N. Bindal, and B. Kaushik, "Advances in magnetic domain walls and their applications," *IEEE Nanotechnol. Mag.*, vol. 16, no. 5, pp. 29–44, Oct. 2022.

[8] 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," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 28, no. 10, pp. 2171–2181, Oct. 2020.

[9] 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.

[10] 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.

[11] 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.

[12] D. Divyanshu, R. Kumar, D. Khan, S. Amara, and Y. Massoud, "Design of VGSOT-MTJ-based logic locking for high-speed digital circuits," *Electronics*, vol. 11, p. 3537, Oct. 2022.

[13] A. Oberoi, A. Dodda, H. Liu, M. Terrones, and S. Das, "Secure electronics enabled by atomically thin and photosensitive two-dimensional memtransistors," *ACS Nano*, vol. 15, no. 12, pp. 19815–19827, Dec. 2021.

[14] A. Wali and S. Das, "Hardware and information security primitives based on two-dimensional materials and devices," *Adv. Mater.*, Dec. 2022, Art. no. 2205365.

[15] M. Shayan, K. Basu, and R. Karri, "Hardware trojans inspired IP watermarks," *IEEE Design Test*, vol. 36, no. 6, pp. 72–79, Dec. 2019.

[16] L. Zhang and C.-H. Chang, "State encoding watermarking for field authentication of sequential circuit intellectual property," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2012, pp. 3013–3016.

[17] C.-H. Chang, M. Potkonjak, and L. Zhang, "Hardware IP watermarking and fingerprinting," in *Secure System Design and Trustable Computing*. Berlin, Germany: Springer, 2016, pp. 329–368.

[18] R. Karmakar, S. S. Jana, and S. Chattopadhyay, "A cellular automata guided finite-state-machine watermarking strategy for ip protection of sequential circuits," *IEEE Trans. Emerg. Topics Comput.*, vol. 10, no. 2, pp. 806–823, Jun. 2022.

[19] A. B. Kahng, J. Lach, W. H. Mangione-Smith, S. Mantik, I. L. Markov, M. Potkonjak, P. Tucker, H. Wang, and G. Wolfe, "Constraint-based watermarking techniques for design IP protection," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 20, no. 10, pp. 1236–1252, Oct. 2001.

[20] J. Ma, J. Lee, and M. Tehranipoor, "Layout-aware pattern generation for maximizing supply noise effects on critical paths," in *Proc. 27th IEEE VLSI Test Symp.*, May 2009, pp. 221–226.

[21] Y.-C. Fan, "Testing-based watermarking techniques for intellectual-property identification in SOC design," *IEEE Trans. Instrum. Meas.*, vol. 57, no. 3, pp. 467–479, Mar. 2008.

[22] R. Chapman and T. S. Durrani, "IP protection of DSP algorithms for system on chip implementation," *IEEE Trans. Signal Process.*, vol. 48, no. 3, pp. 854–861, Mar. 2000.

[23] M. Lewandowski, R. Meana, M. Morrison, and S. Katkoori, "A novel method for watermarking sequential circuits," in *Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust*, Jun. 2012, pp. 21–24.

[24] A. Cui, C.-H. Chang, S. Tahar, and A. T. Abdel-Hamid, "A robust FSM watermarking scheme for IP protection of sequential circuit design," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 30, no. 5, pp. 678–690, May 2011.

[25] 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.

[26] Y. Zhuo, W. Cai, D. Zhu, H. Zhang, A. Du, K. Cao, J. Yin, Y. Huang, K. Shi, and W. Zhao, "Mechanism of field-like torque in spin-orbit torque switching of perpendicular magnetic tunnel junction," *Sci. China Phys., Mech. Astron.*, vol. 65, no. 10, pp. 1–6, Oct. 2022.

[27] A. L. Oliveira, "Techniques for the creation of digital watermarks in sequential circuit designs," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 20, no. 9, pp. 1101–1117, Sep. 2001.

[28] S. B. Akers, "Binary decision diagrams," *IEEE Trans. Comput.*, vol. C-27, no. 6, pp. 509–516, Jun. 1978.

[29] R. E. Bryant, "Graph-based algorithms for Boolean function manipulation," *IEEE Trans. Comput.*, vol. C-35, no. 8, pp. 677–691, Aug. 1986.

[30] K. S. Brace, R. L. Rudell, and R. E. Bryant, "Efficient implementation of a BDD package," in *Proc. Conf. Proc. 27th ACM/IEEE Design Autom. Conf. (DAC)*, 1990, pp. 40–45.

[31] L. Hebrard, D. V. Nguyen, D. Vogel, J.-B. Schell, C. Po, N. Dumas, W. Uhring, 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.

[32] I. Torunoglu and E. Charbon, "Watermarking-based copyright protection of sequential functions," *IEEE J. Solid-State Circuits*, vol. 35, no. 3, pp. 434–440, Mar. 2000.

[33] A. T. Abdel-Hamid, S. Tahar, and E. M. Aboulhamid, "Finite state machine IP watermarking: A tutorial," in *Proc. 1st NASA/ESA Conf. Adapt. Hardw. Syst. (AHS)*, 2006, pp. 457–464.

[34] A. Cui, C.-H. Chang, and L. Zhang, "A hybrid watermarking scheme for sequential functions," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2011, pp. 2333–2336.

DIVYANSHU DIVYANSHU received the B. Tech. degree in electronics system engineering from the National Institute of Electronics and Information Technology (NIELIT), Aurangabad, Maharashtra, India, in 2018, the M. Tech. degree in electrical engineering with a 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), King Abdullah University of Science and Technology (KAUST), Saudi Arabia. He has worked as a Visiting Student at the Integrated Circuits and System Group (ICS), CEMSE, and the Innovative Technologies Laboratories (ITL), CEMSE, KAUST, from June 2021 to August 2022. His research interests include magnetic tunnel junction based circuits, systems, and algorithm designing for hardware security primitives. He is a recipient of the KAUST Fellowship, MHRD GATE Fellowship, and Bidhan-Lokmanya Scholarship.

RAJAT KUMAR received the Bachelor of Technology degree in electronics and communication engineering from the National Institute of Technology (NIT), Hamirpur, Himachal Pradesh, India, in 2019, and the Master of Technology degree in electrical engineering with a specialization in Very Large Scale Integration (VLSI) from the Indian Institute of Technology (IIT), Mandi, Himachal Pradesh, 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 current research interests include the hybrid integration of spin-based devices with CMOS circuits for hardware security and ultra-low power applications.

DANIAL KHAN received the B.S. degree in electrical engineering from the University of Engineering and Technology (UET), Peshawar, Pakistan, in 2011, 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, Saudia Arabia. His research interests include spintronics, analog IC designs, RF energy harvesting systems, wireless power transfer (WPT) systems, and power management ICs 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, magnetism, and mechanics. She was a Postdoctoral Researcher within the Novel Magnetic Devices (NoMaDe) Group—a joint research team between Institut d'Electronique Fondamentale, Paris Sud University (IEF) and Ecole Normale Supérieure (ENS). She is currently working as a Postdoctoral Fellow at KAUST in nanofabrication of TMR sensors. 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 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, MA, USA.

He has held several positions at leading institutions of higher education and the industry including Rice University, Stevens Institute of Technology, WPI, UAB, the SLAC National Accelerator Laboratory, and Synopsys Inc. From January 2018 to July 2021, he was the Dean at the School of Systems and Enterprises (SSE), Stevens Institute of Technology, USA. Prior to Stevens, he worked as the Head of the Department of Electrical and Computer Engineering (ECE) at the Worcester Polytechnic Institute (WPI), from 2012 to 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 with the Innovative Technologies Laboratories (ITL), at King Abdullah University of Science and Technology (KAUST). He has been a PI or a Co-PI on more than 30 Million dollar of funded research from the NSF, DOD, SRC, and the industry. 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 that span 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 several best paper awards. 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 MWSCAS Technical Program Co-Chair, the 2009 General Program Co-Chair, and the 2007 Technical Program Co-Chair of the ACM Great Lakes Symposium on VLSI. He has served as the Editor for the Mixed-Signal Letters-the Americas, as an Associate Editor of the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, and the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, and the Guest Editor of a special issue of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS. He was also named a Distinguished Lecturer by the IEEE Circuits and Systems Society.

• • •