IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 4 July 2022, accepted 18 August 2022, date of publication 1 September 2022, date of current version 9 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3203817

RESEARCH ARTICLE

Physically Unclonable Function Using GSHE Driven SOT Assisted p-MTJ for Next Generation Hardware Security Applications

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, Saudi Arabia

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

ABSTRACT The increasing threat of security attacks on hardware security applications has driven research towards exploring beyond CMOS devices as an alternative. Spintronic devices offer advantages like low power, non-volatility, inherent spatial and temporal randomness, simplicity of integration with a silicon substrate, etc., making them a potential candidate for next-generation hardware security systems. In this work, we explore the Giant Spin Hall effect driven spin-orbit torque magnetic tunnel junction implementing physically unclonable function. The effect of process variation is considered in key MTJ parameters like TMR ratio, free and oxide layer thickness following Gaussian distribution, and Monte-Carlo simulations to determine the effect of the process variations. A unique challenge-response pair is obtained utilizing the inherent variations in magnetization dynamics of the free layer due to process variations.

INDEX TERMS Giant spin hall effect, hardware security, magnetic tunnel junction, physical unclonable functions, spintronic, spin-orbit torque.

I. INTRODUCTION

Recently, the demand for lower power consumption and higher integrated circuits (ICs) operational speed led to a rapid reduction in device feature size. However, device shrinking is approaching its fundamental limits, raising several critical challenges to semiconductor manufacturing and process sectors [1], [2]. Therefore, innovative future technology is essential as an alternative to CMOS devices. The growing and emerging technology of spintronic 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 [3]. Spintronics uses both the spin and charge of electrons to create new devices, such as memory, sensors, and logic gates that have the same properties as the existing devices that use only the charge of electrons. This technology has two prospects: (1) zero energy emissions and (2) replacement of existing CMOS technology [4]. According to the first prospect, current flow by electron spin does not consume any energy in the form of heat, eliminating ICs' heating issues. According to the second prospect, devices beyond CMOS technology are needed to fabricate as CMOS devices are approaching their operational and integration limits. Spintronic has attracted researchers working on semiconductor devices based on these two critical problems solutions. This new technology can combine the functionalities of magnetic devices and semiconductor microelectronics into one IC.

The spin torque effects, such as spin-orbit torque (SOT) [5] and spin-transfer torque (STT) [6], have significantly boosted the development of spintronic. In general, robust switching is implemented in logic devices or memory applications, whereas stochastic properties are avoided [7]. However, physically inherent randomness or process-induced variations are vital in generating unique unclonable identification for the hardware security domain. Since the globalization of IC design and manufacturing has resulted in increased cost and design complexity, severe security concerns have been

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

TABLE 1. List of abbreviations used in this paper.

Abbreviation	Definition
GSHE	Giant Spin Hall Effect
MTJ	Magnetic Tunnel Junction
SOT	Spin-Orbit Torque
STT	Spin-Transfer Torque
PUF	Physically Unclonable Function
C-R	Challenge-Response
HM	Heavy Metal
TMR	Tunnel Mgnetoresistance
PMA	Perpendicular Magnetic Anisotropy
IMA	In-plane Magnetic Anisotropy
p-MTJ	PMA Magnetic Tunnel Junction
i-MTJ	IMA Magnetic Tunnel Junction

raised. As a result of their heavy reliance on untrustworthy foundries to fabricate their ICs, most IC design companies have gone fabless [8]. Recently, the development of various emerging technologies (memristors, carbon nanotubes (CNTs), nanowire FETs (NWFETs), etc.) have played a vital role in improving the notion of hardware security [9]. For example, physically unclonable functions [10], [11], and true random number generators (TRNGs) [12] take advantage of random physical properties in fabricated CMOS devices to achieve higher and more efficient information security. Spin-based PUFs and TRNGs have recently been proposed to expand the potential usage of spintronics while providing a proper mechanism to build hardware security devices with characteristics beyond traditional CMOS technology. Authors in [13] discuss a SOT-MTJ-based hardware Trojan. References [14], [15], [16], [17], [18], [19], [20], [21], [22] evaluate the performance and reliability of CNT bundles for on-chip interconnect applications due to their large conductivity and current carrying capabilities. Authors in [23] 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. Table 1 shows a list of abbreviations used in this paper.

II. BACKGROUND

A. PHYSICAL UNCLONABLE FUNCTION

Physical unclonable function is a unique hardware identifier that utilizes intrinsic fabrication variations of the CMOS technology to generate an "electronic fingerprint" (known as a response) when subjected to an input (known as a challenge) for a particular device [24]. PUFs have emerged as promising solutions for the prevention of chip identification, semiconductor counterfeiting, malicious Trojan insertion, and countering side-channel attacks [25], [26]. PUFs are used in access authentication and cryptographic key generation, which are difficult to predict and reproduce. The challenge-response of the PUF creates a cryptographic key for a particular device. The PUF should be capable of generating repeated responses for the same challenge with respect to aging and varying environmental conditions (electromagnetic interference, voltage noise, temperature). This attribute of the PUF is called intra-hamming distance, which should be near zero. Moreover, different PUFs generate different responses when subjected to the same challenge. This property is measured as inter-hamming distance, which should be near 50% [9]. In recent years, several PUF architectures have been proposed in the literature. The simplest PUF is a ring oscillator that generates a unique frequency for each IC it is fabricated on [27]. Delay-based arbiter is another example of a PUF that generates a fingerprint based on the propagation delay of the circuit [28]. Error Correction Codes (ECCs) have been widely employed as an effective means of smoothing noise response to improve PUF reliability but die area or design complexity is sacrificed [29]. PUFs based on non-volatile memory (NVM) devices such as spin torque effect, phase change memory (PCM), etc. are attracting considerable research interest due to their high scalability and low power consumption [3].

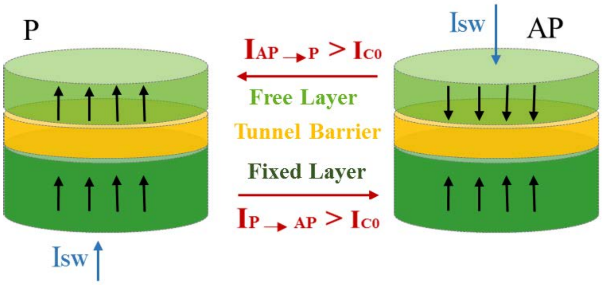

P
AP
Isw
$I_{AP \rightarrow P} > I_{C0}$
Free Layer
Tunnel Barrier
Fixed Layer
$I_{P \rightarrow AP} > I_{C0}$
Isw

FIGURE 1. p-MTJ structure and switching between the two states.

B. MAGNETIC TUNNEL JUNCTION

Fig. 1 shows a typical p-MTJ structure comprised of two relatively thick ferromagnetic layers (a fixed layer and a free layer) separated by a relatively thin tunnel barrier layer [30]. 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 GSHE-driven MTJ, a spin current is generated perpendicularly by passing a SHE write current through the heavy metal. This spin current exerts torque on the free layer, causing the switching of the MTJ state. The spin current is due to the directional and coherent motion of electron spin and is a rank-two pseudo-tensor quantity with multiple components. The TMR ratio characterizes the resistance difference and is defined by the following equation:

$$TMR = \frac{R_{AP} - R_P}{R_P} \times 100 \tag{1}$$

If the difference between the resistances in parallel and anti-parallel is larger, it shows higher TMR and 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 an anti-parallel to a parallel state. The magnetic dynamics of the free layer are governed by Landau Lifshitz Gilbert (LLG) equation [31], and the MTJ resistance is given by:

$$\frac{\partial \vec{m}}{\partial t} = -\gamma \mu_0 \vec{m} \times \vec{H}_{eff} + \alpha \vec{m} \times \frac{\partial \vec{m}}{\partial t} - \xi P J_{STT} \vec{m} \times (\vec{m} \times \vec{m}_r) - \xi \eta J_{SHE} \vec{m} \times (\vec{m} \times \vec{\sigma}_{SHE}) \tag{2}$$

$$R_{MTJ}\left(V_{MTJ}\right) = \frac{R_p\left[1 + (V_{MTJ}/V_h)^2 + TMR_0\right]}{1 + \left(V_{MTJ}^2/V_h^2\right) + TMR_0[0.5(1+\cos\theta)]} \tag{3}$$

Here, m and m_r are the unit vector along with magnetization of the free layer and the reference layer, respectively, γ is the Gyromagnetic ratio, μ_0 is the vacuum permeability, H_{eff} is the effective magnetic field, α is the Gilbert damping coefficient, P is the polarization factor, J_{STT} and J_{SHE} are the STT and SOT current density applied to the MTJ device and σ_{SHE} 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.

This paper proposes a PUF circuit using GSHE-driven SOT MTJ for next-generation hardware security applications. Here, we utilize the process variations in crucial parameters like TMR, free layer, and oxide layer thickness to obtain a unique C-R pair that is more difficult to clone and has higher endurance than other STT-based PUFs.

III. PROPOSED WORK

Fig. 2 represents the block diagram for the overall approach of utilizing a SOT-assisted MTJ device for PUF. The SOT current (I_SOT) and the STT current (I_STT) are injected into the MTJ device to check its performance. Fig. 3 demonstrates the overall simulation framework for the field-free SOT-assisted STT switching. This switching method has certain advantages, such as no external magnetic field is required, and in comparison to the STT-based switching mechanism, it requires less current to be passed from the thin oxide layer in the MTJ stack, thus more endurance and reliable operation. The resistance of the MTJ stack is dependent on the magnetization of the free layer, applied input current, material parameters, and device dimensions. All this information is needed for cloning the exact behavior, yet the presence of process variations and temperature variations make it extremely difficult to clone the behavior of the MTJ. Compared to STT MTJ-based PUF, the requirement of two current sources makes it more difficult for the attacker to copy the switching characteristics as the unique set of both the values is responsible for switching. The disadvantage of this approach lies in that this structure is a three-terminal device which makes it more complex, having a large area compared to STT MTJ-based PUFs. The compact model for the circular PMA MTJ selected is presented in [31] and the simulation parameters are selected based on the experimentally determined MTJ stack presented in section III C for a more realistic PUF simulation. The detailed switching mechanism for the model is provided in [32].

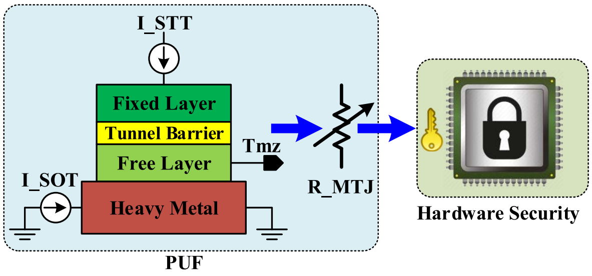


FIGURE 2. Block diagram for SOT assisted MTJ PUF for hardware security.

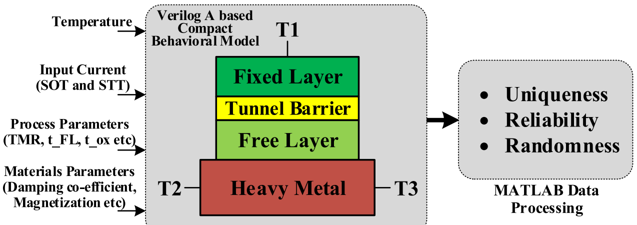

Temperature
Input Current (SOT and STT)
Process Parameters (TMR, t_FL, t_ox etc)
Materials Parameters (Damping co-efficient, Magnetization etc)
Verilog A based Compact Behavioral Model
T1
Fixed Layer
Tunnel Barrier
Free Layer
Heavy Metal
T2
T3
• Uniqueness
• Reliability
• Randomness
MATLAB Data Processing

FIGURE 3. Simulation framework for SOT assisted MTJ PUF.

A. p-MTJ WITH HIGH BARRIER HEIGHT ($\Delta \approx 60\ k_BT$)

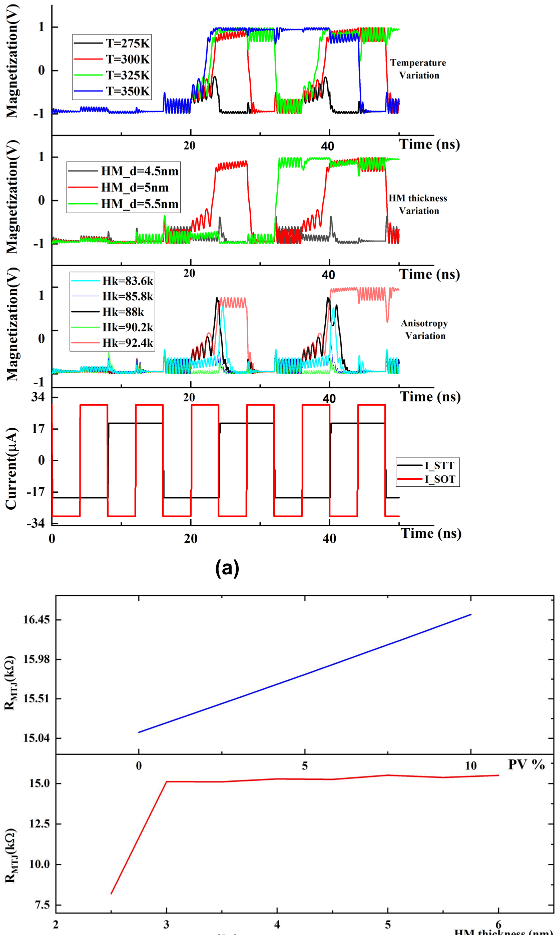
Fig. 1 shows the basic p-MTJ structure. When the magnetization is in the in-plane direction instead of the perpendicular direction, the MTJ stack is called IMA MTJ. This work explores p-MTJ-based PUF characteristics due to its faster and lower requirement of write current [33]. The MTJ barrier height is an important physical parameter that determines the energy difference in the two stable states and the probability of switching. With a high $\Delta \approx 60\ k_B$T, (where k_B is the Boltzmann constant and T is the temperature in Kelvin), the data retention time is around ten years and has deterministic switching characteristics which are utilized for non-volatile memory applications [31]. The simulation is performed with 5% process variation in TMR, free layer thickness, and oxide layer thickness. The parametric analysis in the spectre simulator is then performed for other parameters like temperature, heavy metal thickness, and anisotropy field value to demonstrate that other parameter variations can create a unique free layer magnetization response and thus a variable resistance behavior at the output side which can be utilized for generating unique C-R. As two identical device fabrication in such a multilayer structure is not possible, this leads to distinct input/output characteristics, and the ability

TABLE 2. SOT assisted MTJ parameters set for electrical simulations.

Parameter	Values
MTJ dimension and shape	40 nm * 40 nm, circular
Free layer thickness	1.4 nm
Oxide layer thickness	1.2 nm
HM length, width and height	60 nm * 40 nm * 5 nm
Gilbert damping coefficient	0.03
Saturation magnetization	800000 emu/cm^3
TMR	120%
Anisotropy field	88000 A/m
Spin Hall angle	0.3
Heavy metal resistivity	200 $\mu\Omega$ cm
Potential barrier height of MgO	0.5 V

TABLE 3. 200 times Monte Carlo simulation results for average free layer magnetization value under various process variations.

Process variation	Mean value	Standard Deviation
3 %	-18.6082 mV	118.836 mV
5 %	-33.6616 mV	168.113 mV
10 %	-81.97 mV	179.5 mV



(a)

(b)

FIGURE 4. (a) Spectre simulation indicating magnetization reversal with distinct characteristic indicating different possible sources of entropy. (b) MTJ resistance variations with some key parameters like heavy metal thickness and process variations.

to utilize such behavior in MRAM structure for hardware security is being explored in recent research [9]. For the selected compact model, 200 times Monte Carlo simulation is performed using random sampling. We considered variations of free layer thickness, the thickness of the oxide layer, and the TMR ratio following Gaussian distribution to consider the effect of the process variations of these key parameters in the free layer magnetization level of the MTJ. The simulation is performed for 50 ns at 300 K temperature with $B_{ext} = 0$, the applied SOT current density of 15 MA/cm^2 is passed through terminal T2 and T3, and the applied STT current of 1.59 MA/cm^2 is passed through terminal T1 and T3 of Fig. 3. A comprehensive study of current-induced spin-orbit torque and its physics in ferromagnetic and anti-ferromagnetic material is presented in [34]. The SOT-MTJ device is a three-terminal structure. Terminal T1-T3 in Fig 3 are the physical pins or the electrical contacts that pass the input parameters. Sense amplifier circuits can be used to properly sense the state of the MTJ-based PUF for more practical applications. The P to AP and AP to P switching are not symmetrical, so the asymmetrical factor is set at asy = 1.1. The field-like torque component, as mentioned in [35], is set at fac_fl = 0.8. Device parameters are obtained experimentally for the MTJ stack, as mentioned in Table 2. Table 3 contains the results for the Monte Carlo simulation with 3%, 5%, and 10% process variations in the mentioned parameters and the mean and standard deviation in the average value of the free layer magnetization.

Fig. 4(a) shows the variations of free layer magnetization dynamics with respect to temperature variation. The strong dependency on the temperature is a viable source of entropy that can provide a unique response to a specific challenge. It is thus important to test MTJ sensitivity to variation in temperature as the MTJ thermal stability factor is a function of temperature, as shown below:

$$\Delta = \frac{E_b}{k_B T} \tag{4}$$

where, E_b is the energy barrier height

In SOT-assisted MTJ switching, an extra heavy metal is required through which charge current is passed, generating a spin current in the perpendicular direction through the stack. The SOT mechanism assists in the switching. Any variation in heavy metal dimension would change the requirement of critical current density required for switching and thus will create a unique switching response as shown in Fig. 4(a) for the case of variation in heavy metal thickness. As it is not possible to fabricate an identical multilayered stack with some variation in dimensions is to be expected which can be utilized for generating unique C-R pair. Other physical parameters also result in variation in free layer magnetization dynamics along with variation in supply currents; thus, SOT-assisted MTJ offers a complex and rich source of entropy and non-linearity, making them an ideal candidate for PUFs.

TABLE 4. MTJ device parameters for LBM operation.

Parameter	Values
MTJ dimension and shape	14 nm * 14 nm, circular
Free layer thickness	0.5 nm
Oxide layer thickness	0.8 nm
HM length, width and height	30 nm * 14 nm * 3 nm
Gilbert damping coefficient	0.1
Saturation magnetization	240 emu/cm^3
TMR	120%
Spin Hall angle	0.3
Heavy metal resistivity	200 $\mu\Omega$ cm

Fig. 4(b) shows the MTJ resistance variation with respect to variation in Heavy metal thickness and process variation in TMR, Free layer, and Oxide layer thickness following Gaussian distribution. $\Delta\ R_{MTJ}$=1.4k Ω was observed when PV was varied from 0% to 10%.

B. p-MTJ WITH LOW BARRIER HEIGHT ($\Delta \approx 0\ k_BT$)

Stable magnets can be redesigned to have a low energy barrier [36]. In the absence of any input, the magnetization value fluctuates between the two stable states, and the probability of switching can be controlled using an applied current which is like a binary stochastic neuron behavior [37]. The energy associated with a magnet is given by:

$$E = 0.5\ H_{kp} M_s V(1 - m_z^2) + 0.5\ H_{ki} M_s V(1 - m_y^2) \quad (5)$$

where

$$H_{kp} = 2\ K_s/t - 4\pi M_s \quad (6)$$

where H_{kp} is the perpendicular anisotropy field along the z-axis, K_s is the surface anisotropy density, H_{ki} is the in-plane anisotropy along the y-axis, M_s is the saturation magnetization, and V is the volume of the magnet. LBM-based p-MTJ is designed, and the simulation parameter for the same is mentioned in Table 4 to obtain the required thermal stability factor based on:

$$\Delta_{PMA} = \frac{H_{ki} M_s V}{2} \approx 0 \quad (7)$$

Fig. 5(a) demonstrates the free layer magnetization reversal due to thermal energy without any applied input current. Fig. 5(b) shows the long-time averaged magnetization as a function of applied SOT current, which is utilized to create the SOT MTJ-based neural or other non-Boolean architectures. With careful designing, a unique PUF-like response like the one demonstrated in Section III-A can be obtained, which could be useful for advanced hardware security based on such spintronic devices as unique changes in magnetization value can alter the computational logic. A detailed investigation into the PUF circuits using low barrier regime-based p-MTJ and i-MTJ structure on such emerging computing paradigms is beyond the scope of the current work.

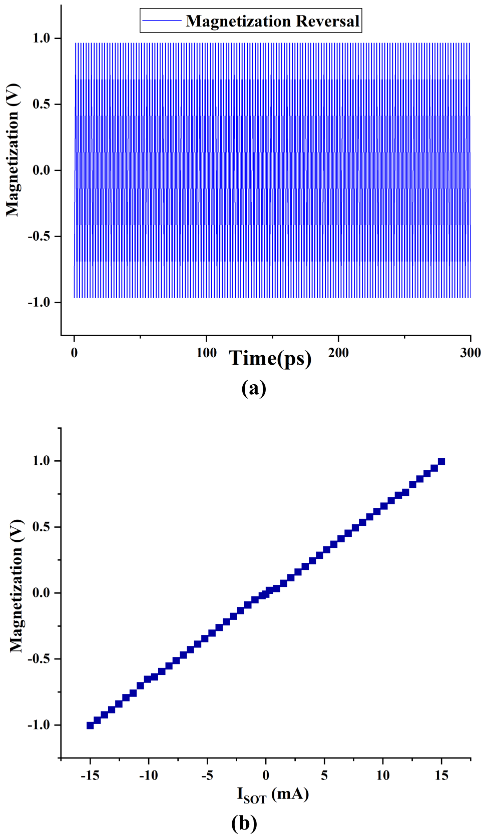


FIGURE 5. **(a) Magnetization reversal due to thermal energy for LBM. (b) Long time averaged magnetization as a function of applied SOT current.**

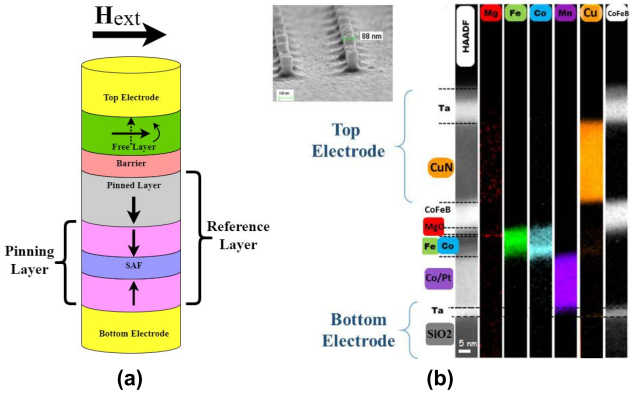


FIGURE 6. **(a). Representative image of the circular MTJ pillar with the magnetic layers and the top and bottom contact. An SEM image of the patterned MTJs is inset. (b) The MTJ stack composition and the TEM image of the multilayers.**

C. DEVICE FABRICATION AND MATERIAL PARAMETERS

Thin-film multilayer of our studied device is deposited on thermally oxidized Si substrates using Singulus DC/RF magnetron sputtering. The MTJ stacks is with the following composition: bottom electrode/[Co (0.5)/Pt (0.2)]$_6$/Ru (0.8)/[Co (0.6)/Pt (0.2)]$_3$/Ta (0.2)/Co (0.9)/W (0.25)/FeCoB (1)/MgO (0.8)/FeCoB (1.4)/ W (0.3)/FeCoB (0.5)/MgO (0.75)/top

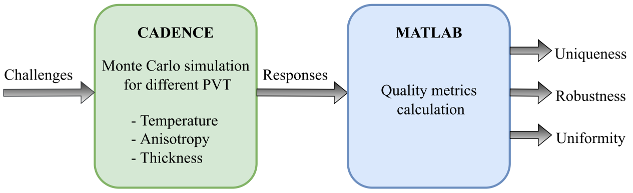


FIGURE 7. Block diagram for the performance characteristics evaluation step.

electrode (thickness in nm). MTJ devices are bottom pinned perpendicular magnetized. The free layer thickness is 1.4 nm to reorient its magnetization from in-plane (for thicker free layer) to out-of-plane (for free layer 1.4 nm) because of the competition between the interfacial perpendicular magnetic anisotropy (iPMA) at the FeCoB/MgO interface and the demagnetizing energy. The composite Co/W/FeCoB polarizing layer (PL) is characterized by a magnetization oriented out-of-plane due to the iPMA at the MgO interface and the interlayer exchange coupling to the $(Co/Pt)_6/Ru/(Co/Pt)_3$ synthetic antiferromagnet (SAF) structure shown in Fig. 6 with transmission electron microscopy (TEM) image. The magnetic stacks were patterned into circular nanopillars using e-beam lithography followed by Argon ion etching. The nominal diameters are 80 nm and 120 nm, which can be seen inset in the scanning electron microscopy (SEM) image in Fig. 6. Statistical measurements with a 4-points magnetic probe station set up on the fabricated devices at low bias voltages give a TMR of approximately 120%. The resistance area product of the MTJ stack is 10 $\Omega\mu m^2$. In our study, we used tungsten (W) as the bottom electrode material, which presents a relatively high resistance of Rs 200 Ω, which is in series with the MTJ resistance and independent of the device diameter. The (SAF) cancels the Fixed layer's dipolar influence on the free layer. This SAF layer is further pinned using additional antiferromagnet (Co/Pt, Pt/Mn, etc.), which is shown as the purple layer. Due to high non-linearity and process variation, different current pulses, Heavy metal dimensions, materials, etc., make it difficult to accurately decipher the PUF characteristics using the destructive reverse engineering method. Thus, an exact SOT MTJ PUF is difficult to reverse engineer.

IV. PUF PERFORMANCE METRICS AND GENERAL APPROACH

Fig. 7 depicts PUF performance metrics and a general approach. Several performance metrics for PUF characterization have been done previously [38], [39] and Machine Learning-based attack resilient PUFs using STT-MTJ are reported in [40]. The general approach for evaluating emerging PUF characteristics remains the same as for CMOS-based PUFs, which is briefly presented in this section. A detailed PUF evaluation of SOT-MTJ-based MRAM, which reported a Uniformity of 49.9236% and Uniqueness of 50.0428%, is presented in [41], which used a small capacity TRNG and high-reliability secure hash algorithm. Future work will include a detailed investigation into using these general performance metrics, Machine learning-based attack resilience, and NIST tests for evaluating and comparing the PUF characteristics with other emerging MTJ structures.

- **Uniqueness** – It determines the inter-chip variation. In the ideal case, different chips must have distinct outputs, and if the set of measurements is statistically independent, their Hamming Distance (HD) would be 50% [42]. The following equation calculates it:

$$Uniqueness = \frac{2}{k(k-1)} \sum_{i=1}^{k=1} \sum_{j=i+1}^{k} \frac{HD(R_i, R_j)}{n} \times 100\% \tag{8}$$

Algorithm 1 Pseudocode for Uniqueness Value

```
Compute number of PUFs (k)
Compute number of response bits (n)
Initialize Hamming Distance (Total_HD) to 0
Repeat
Compute Hamming Distance for all PUFs (Total_HD)
End Repeat
Uniqueness value = 2(Total_HD)/(n*k(k-1))*100
```

- **Robustness** – It is the intra-die variation which ideally is zero. It is measured by taking many measurements from a single IC, and the mean error rate is calculated based on the following formula [38]:

$$Robustness = \frac{1}{x} \sum_{y=1}^{x} \frac{HD(R_i, R_{i,j})}{n} \times 100 \tag{9}$$

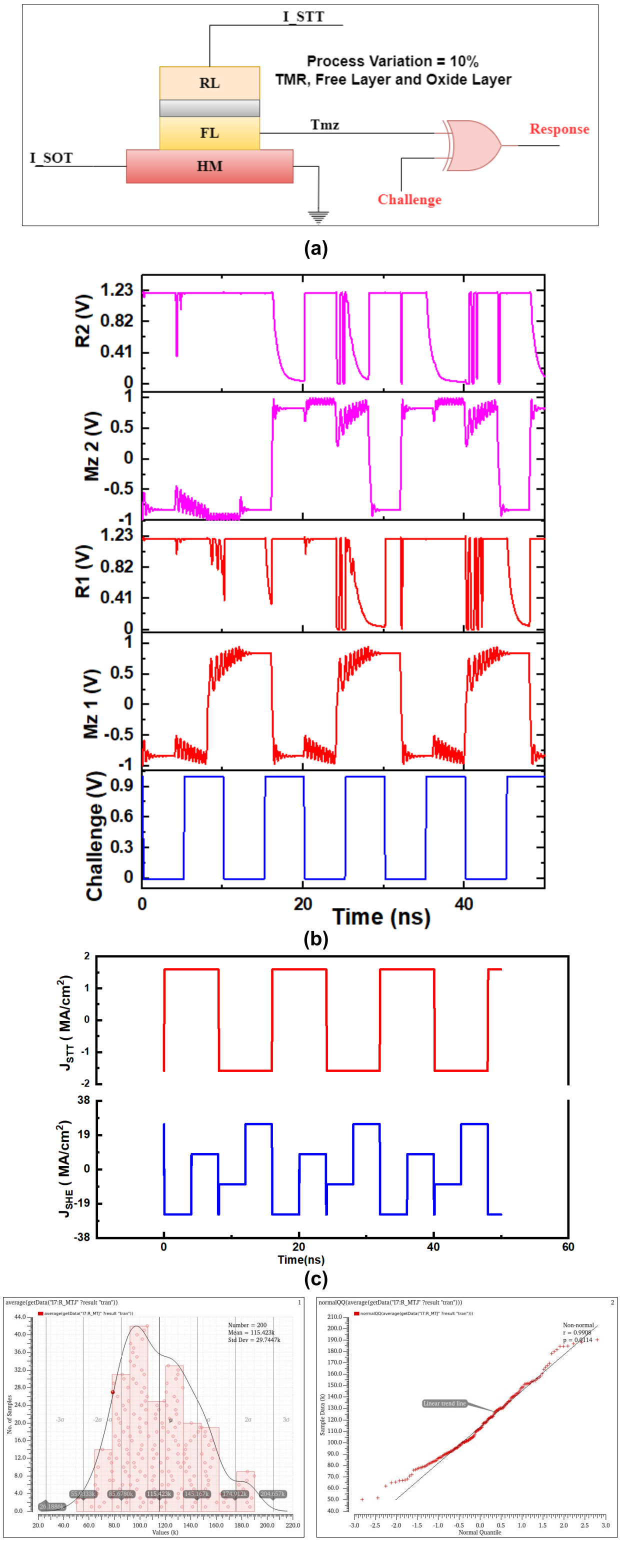
Algorithm 2 Pseudocode for Robustness Value

```
Compare the size of response A and response B
If (size(response A) $\neq$ size(response B)):
Display Error:
Else:
Compute number of bits per response (n)
Compute total number of samples (x)
Initialize Hamming Distance (Total_HD) to 0
Repeat
Compute Hamming Distance for each row (Total_HD)
End Repeat
Robustness value = (Total_HD)/(x*n)*100
```

- **Uniformity** – Estimates how uniform the proportion of "0" and "1" is in the response bits of a PUF.

Algorithm 3 Pseudocode for Uniformity Value

```
Compute response in integer form
Uniformity value = sum(response)/length(response)*100
```



(a)

(b)

(c)

(d)

FIGURE 8. (a) Schematic diagram for SOT assisted MTJ based PUF. (b) Monte Carlo simulation results with 10% process variations and C-R waveform with distinct characteristics due to variation in MTJ free layer. (c) Applied Current density waveform. (d) MTJ resistance variations representing distinct values due to uniform sampling method and process variations, Quantile plot for MTJ resistance with respect to linear trend line representing the amount of deviation.

V. MEASUREMENT RESULTS

A. SOT ASSISTED STT PUF CIRCUIT

The key requirement for PUF is high process variation and non-linearity to ensure enough randomness and uniqueness in the structure. An extra heavy metal for generating the spin-orbit torque creates more chaotic magnetization dynamics for the free layer than another non-volatile device-based PUF. The requirement of two sets of current sources will make it more difficult to reverse engineer systems based on such PUF.

Fig. 8(a) represents the schematic for generating the C-R pair. Fig. 8(b) represents the C-R implementation waveform based on the above PUF, in which we include process variation of 10% (TMR ratio = 1.2, free layer thickness = 1.4nm, and oxide layer thickness = 1.2 nm) in p-MTJ with high barrier height. We performed 200 times Monte Carlo simulations to generate C-R pair in TSMC 65nm technology node with CMOS W/L ratio = 10/3 and Vdd = 1.2 V. No process variation for the CMOS device was considered during the simulation, and other simulation parameters are the same as mentioned in Table 2 with simulation steps of 1 ps, asy = 1.1 and fac_fl = 2.5. In Fig. 8(b)-(c), due to process variation and the random sampling method used during simulation unique magnetization orientation of the free layer would lead to a unique response for a given challenge. Fig. 8(c) shows the applied current density to the PUF structure. In Fig. 8(d), MTJ resistance, a critical parameter, is obtained using Monte Carlo simulation for 200 points, and variation in resistance due to process variations is demonstrated. The energy per bit can be calculated according to the following equation:

$$E = \int_{0}^{tsw} V_{dd} * i_{dd}(t)\,\mathrm{d}t \qquad (10)$$

where t_{sw} is the switching delay, V_{dd} is the supply voltage, and $i_{dd}(t)$ is the total current from the power supply. The write current is set at a value larger than the critical current density required for obtaining a switching probability of 100%.

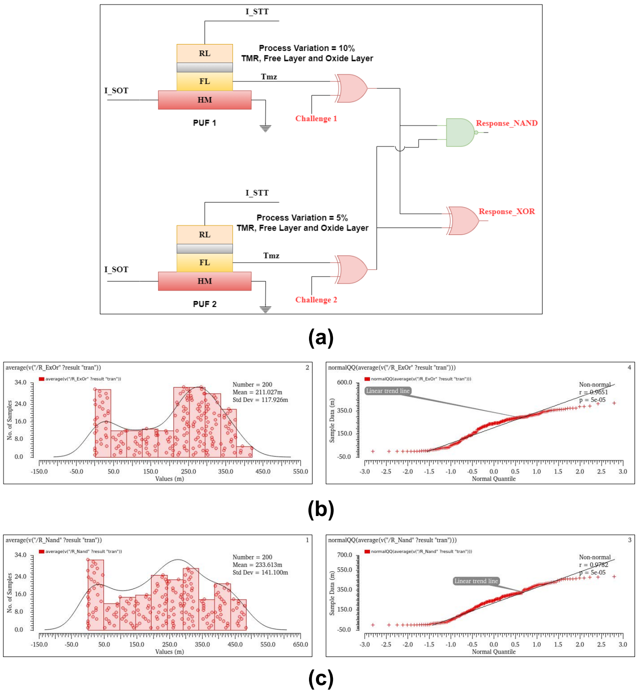
Table 5 contains the effect of different amounts of process variations in MTJ average resistance value. As the process variations that follow the Gaussian distribution increase, the variation in the range of minimum and maximum value of resistance increases, and the standard deviation increases. Thus, the higher the process variations, the more the difference in the expected value of MTJ resistance is exploited to obtain a unique device signature, which is one of the critical requirements of PUFs, thus making SOT-assisted MTJ a potential candidate for PUF implementation.

B. DUAL-PUF STRUCTURE

Dual PUF circuits are designed to enable unique responses, and a larger number of stages provide more degree of randomness in signature. The multistage PUF structure can be designed for a specific type of application and considering other design constraints. In Fig. 9 (a), we present a simple

TABLE 5. 200 times Monte Carlo simulation results for average MTJ resistance value under various process variations (PV).

PV	Min. value	Max. value	Mean value	Std. Dev.
3 %	86.48 kΩ	130.7 kΩ	111.6 kΩ	8.79 kΩ
5 %	74.47 kΩ	145 kΩ	112.3 kΩ	14.58 kΩ
10 %	50.22 kΩ	190.22 kΩ	115.42 kΩ	29.74 kΩ



(a)

(b)

(c)

FIGURE 9. (a) Schematic diagram for Dual PUF structure with different process variations. (b) 200-time Monte Carlo simulation to obtain the deviation in average value for XOR stage, and (c) NAND stage.

TABLE 6. 200 times Monte Carlo simulation result for average response value for circuit shown in Fig. 8(a).

Response	Min. value	Max. value	Mean value	Std. Dev.
NAND	200.2 nV	484.9 mV	233.6 mV	141.1 mV
XOR	4.952 μV	421.5 mV	211 mV	117.9 mV

approach where PUF 1 and PUF 2 have different process variations (10% and 5%, respectively), and we provide a specific set of challenges 1 and 2. Further, we create another logic stage for generating the unique response signature. In many previous works, the use of delay and toggle path is used to create unique C-R pair. In Fig. 9(b), we perform a similar analysis as done in section III-A for the Monte Carlo analysis of the circuit presented in Fig. 9 (a).

Table 6 shows that the standard deviation in the average value of the response is significant compared to the mean value, which is also clear from the Monte Carlo results in Fig. 9 (b)-(c). Added stage of logic and dual PUF structure enables more unique responses which can be differentiated from other responses more quickly. More uniqueness is important for the PUF performance characteristic metric.

VI. CONCLUSION

Physical unclonable function has emerged as a reliable solution to address security issues for next-generation hardware systems. This paper presents giant spin Hall effect driven spin-orbit torque magnetic tunnel junction based PUF for hardware security applications. Simulation results show that the proposed PUF structure generates a unique response for a specific challenge depending upon the magnetization variations. To satisfy the proposed work, Monte Carlo simulations for single and multiple PUF structures have been carried out.

REFERENCES

[1] M. H. Bhuyan, "History and evolution of CMOS technology and its application in semiconductor industry," *Southeast Univ. J. Sci. Eng. (SEUJSE)*, vol. 11, no. 1, pp. 28–42, Jun. 2017.

[2] H. Ilatikhameneh, T. Ameen, B. Novakovic, Y. Tan, G. Klimeck, and R. Rahman, "Saving Moore's law down to 1 nm channels with anisotropic effective mass," *Sci. Rep.*, vol. 6, no. 1, pp. 1–6, Aug. 2016, doi: 10.1038/srep31501.

[3] S. A. Wolf, J. Lu, M. R. Stan, E. Chen, and D. M. Treger, "The promise of nanomagnetics and spintronics for future logic and universal memory," *Proc. IEEE*, vol. 98, no. 12, pp. 2155–2168, Dec. 2010.

[4] A. Hirohata, K. Yamada, Y. Nakatani, I.-L. Prejbeanu, B. Diény, P. Pirro, and B. Hillebrands, "Review on spintronics: Principles and device applications," *J. Magn. Magn. Mater.*, vol. 509, Sep. 2020, Art. no. 166711, doi: 10.1016/j.jmmm.2020.166711.

[5] L. Liu, C.-F. Pai, Y. Li, H. W. Tseng, D. C. Ralph, and R. A. Buhrman, "Spin-torque switching with the giant spin Hall effect of tantalum," *Science*, vol. 336, no. 6081, pp. 555–558, May 2012.

[6] J. C. Slonczewski, "Current-driven excitation of magnetic multilayers," *J. Magn. Magn. Mater.*, vol. 159, nos. 1–2, pp. 1–7, Jun. 1996.

[7] K. Garello, F. Yasin, H. Hody, S. Couet, L. Souriau, S. H. Sharifi, J. Swerts, R. Carpenter, S. Rao, W. Kim, J. Wu, K. K. V. Sethu, M. Pak, N. Jossart, D. Crotti, A. Furnemont, and G. S. Kar, "Manufacturable 300 mm platform solution for field-free switching SOT-MRAM," in *Proc. Symp. VLSI Technol.*, Jun. 2019, pp. 194–195.

[8] 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.

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

[10] G. Selimis, M. Konijnenburg, M. Ashouei, J. Huisken, H. de Groot, V. van der Leest, G.-J. Schrijen, M. van Hulst, and P. Tuyls, "Evaluation of 90 nm 6T-SRAM as physical unclonable function for secure key generation in wireless sensor nodes," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, May 2011, pp. 567–570.

[11] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, "Silicon physical random functions," in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS)*, 2002, pp. 148–160.

[12] Y. Kim, X. Fong, and K. Roy, "Spin-orbit-torque-based spin-dice: A true random-number generator," *IEEE Magn. Lett.*, vol. 6, pp. 1–4, 2015.

[13] 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.

[14] 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.

[15] 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.

[16] Y. Massoud and Y. Ismail, "Grasping the impact of on-chip inductance in high speed ICs," *IEEE Circuits Devices Mag.*, vol. 17, pp. 14–21, Feb. 2001.

[17] 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. Exhibit.*, Apr. 2007, pp. 1–6.

[18] 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.

[19] 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.

[20] Y. Massoud and A. Nieuwoudt, "Accurate resistance modeling for carbon nanotube bundles in VLSI interconnect," in *Proc. 6th IEEE Conf. Nanotechnol.*, Jul. 2006, pp. 288–291.

[21] 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.

[22] A. Nieuwoudt and Y. Massoud, "Performance implications of inductive effects for carbon-nanotube bundle interconnect," *IEEE Electron Device Lett.*, vol. 28, no. 4, pp. 305–307, Apr. 2007.

[23] T. Ragheb and Y. Massoud, "On the modeling of resistance in graphene nanoribbon (GNR) for future interconnect applications," in *Proc. IEEE/ACM Int. Conf. Comput.-Aided Design*, San Jose, CA, USA, Nov. 2008, pp. 593–597.

[24] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th Annu. Design Autom. Conf.*, 2007, pp. 9–14.

[25] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[26] D. Puntin, S. Stanzione, and G. Iannaccone, "CMOS unclonable system for secure authentication based on device variability," in *Proc. ESSCIRC 34th Eur. Solid-State Circuits Conf.*, Sep. 2008, pp. 130–133.

[27] R. Maes and I. Verbauwhede, "Physically unclonable functions: A study on the state of the art and future research directions," in *Towards Hardware-Intrinsic Security* (Information Security and Cryptography). Berlin, Germany: Springer, 2010.

[28] D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 10, pp. 1200–1205, Oct. 2005.

[29] C. Bösch, J. Guajardo, A. Sadeghi, J. Shokrollahi, and P. Tuyls, "Efficient helper data key extractor on FPGAs," in *Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst.*, Washington, DC, USA, 2008, pp. 181–197.

[30] S. Ikeda, K. Miura, H. Yamamoto, K. Mizunuma, H. D. Gan, M. Endo, S. Kanai, J. Hayakawa, F. Matsukura, and H. Ohno, "A perpendicular-anisotropy CoFeB–MgO magnetic tunnel junction," *IEEE Trans. Electron Devices*, vol. 59, no. 3, pp. 819–826, 2010.

[31] 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.

[32] P. Barla, V. K. Joshi, and S. Bhat, "Design and analysis of SHE-assisted STT MTJ/CMOS logic gates," *J. Comput. Electron.*, vol. 20, no. 5, pp. 1964–1976, Aug. 2021.

[33] E. Kitagawa, S. Fujita, K. Nomura, H. Noguchi, K. Abe, K. Ikegami, T. Daibou, Y. Kato, C. Kamata, S. Kashiwada, N. Shimomura, J. Ito, and H. Yoda, "Impact of ultra low power and fast write operation of advanced perpendicular MTJ on power reduction for high-performance mobile CPU," in *Proc. Int. Electron Devices Meeting*, Dec. 2012, pp. 29.4.1–29.4.4.

[34] A. Manchon, J. Železný, I. M. Miron, T. Jungwirth, J. Sinova, A. Thiaville, K. Garello, and P. Gambardella, "Current-induced spin-orbit torques in ferromagnetic and antiferromagnetic systems," *Rev. Modern Phys.*, vol. 91, no. 3, Sep. 2019, Art. no. 035004.

[35] M. Wang, W. Cai, D. Zhu, Z. Wang, J. Kan, Z. Zhao, K. Cao, Z. Wang, Y. Zhang, T. Zhang, and C. Park, "Field-free switching of a perpendicular magnetic tunnel junction through the interplay of spin–orbit and spin-transfer torques," *Nature Electron.*, vol. 1, no. 11, pp. 582–588, Nov. 2018.

[36] P. Debashis, R. Faria, K. Y. Camsari, and Z. Chen, "Design of stochastic nanomagnets for probabilistic spin logic," *IEEE Magn. Lett.*, vol. 9, pp. 1–5, 2018.

[37] O. Hassan, R. Faria, K. Y. Camsari, J. Z. Sun, and S. Datta, "Low-barrier magnet design for efficient hardware binary stochastic neurons," *IEEE Magn. Lett.*, vol. 10, pp. 1–5, 2019.

[38] S. Su, M. Zhu, H. Wang, B. Yang, and L. Liu, "A survey on the security of PUFs," *J. Phys., Conf.*, vol. 1993, Aug. 2021, Art. no. 012031.

[39] Y. Tanaka, M. Goto, A. K. Shukla, K. Yoshikawa, H. Nomura, S. Miwa, S. Tomishima, and Y. Suzuki, "Physically unclonable functions with voltage-controlled magnetic tunnel junctions," *IEEE Trans. Magn.*, vol. 57, no. 2, pp. 1–6, Feb. 2021.

[40] R. Ali, D. Zhang, H. Cai, W. Zhao, and Y. Wang, "A machine learning attack-resilient strong PUF leveraging the process variation of MRAM," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 6, pp. 2712–2716, Jun. 2022.

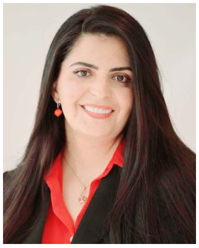
[41] Z. Hou, Z. Wang, C. Wang, M. Wang, Y. Wang, X. Wang, C. Duan, and J. Yang, "Reconfigurable and dynamically transformable In-Cache-MPUF system with true randomness based on the SOT-MRAM," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 69, no. 7, pp. 2694–2706, Jul. 2022.

[42] G. Komurcu and G. Dundar, "Determining the quality metrics for PUFs and performance evaluation of two RO-PUFs," in *Proc. 10th IEEE Int. NEWCAS Conf.*, Jun. 2012, pp. 73–76.

DIVYANSHU DIVYANSHU received the B.Tech. degree in electronics system engineering from the National Institute of Electronics and Information Technology, Aurangabad, Maharastra, 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, such as 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, 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 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. 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. Thanks to Spintec Laboratory, which offers such a specialized training of the nanofabrication. Her main research interests include the spintronics and related applications going from electrical engineering to biotechnology. Her current 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, USA.

He has held a 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, 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 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 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 the several best paper awards. He has been a PI or a Co-PI on more than 30 Million Doller 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 MWSCAS Technical Program Co-Chair, as well as the 2009 General Program Co-Chair for the ACM Great Lakes Symposium on VLSI, and the 2007 Technical Program Co-Chair for the ACM Great Lakes Symposium on VLSI. 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 the Guest Editor for a Special Issue for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I.