DOVA PRO: A Dynamic Overwriting Voltage Adjustment Technique for STT-MRAM L1 Cache Considering Dielectric Breakdown Effect

Kangwei Xu, Dongrong Zhang, Patrick Girard, Qiang Ren, Yuanqing Cheng

SD-PUF: A Novel Area Efficient and Highly Reliable PUF with Signature Improvement for Spin-Transfer Torque Magnetic Cell-Based Circuits

Kangwei Xu, Dongrong Zhang, *Student Member, IEEE,* Patrick Girard, *Fellow, IEEE,* Qiang Ren, *Member, IEEE*
Yuanqing Cheng, *Senior Member, IEEE*

***Abstract*—Physical Unclonable Function (PUF) attracts enormous attention in recent years to securely preserve confidential information in computing systems. The conventional PUFs require many independent PUF components and/or are incapable of generating multiple response-bit per cycle, resulting in significant area overhead and power consumption. Recently, spin-transfer torque magnetic cell (STT-mCell) has emerged as a promising spintronic device to be used in Computing-In-Memory (CIM) system. However, it is challenging to guarantee the hardware security of STT-mCell based circuits. In this work, we propose a novel STT-mCell Delay based PUF design (SD-PUF) exploiting the unique manufacturing process variation (PV) of STT-mCell that can overcome these issues. A methodology is used to select appropriate logic gates in the all-spin chip to generate a unique identification key. A linear feedback shift register (LFSR) initiates SD-PUF and simultaneously generates a 64-bit signature at each clock cycle. Bit generation in SD-PUF is stabilized using an automatic write-back technique. For uniqueness enhancements, a masking scheme is applied for signature improvement. The uniqueness of the improved SD-PUF is 49.61%. With ±20% supply voltage, and 5°C-105°C temperature variations, SD-PUF shows a strong resiliency. In comparison with the state-of-the-art PUFs, our approach can reduce hardware overhead and energy consumption effectively. Finally, the robustness of SD-PUF against various attacks is verified as well.**

***Index Terms*—Spin-Transfer Torque Magnetic Cell (STT-mCell); hardware security; physical unclonable function (PUF); automatic write-back; signature improvement.**

I. Introduction

Due to the performance gap between processor and main memory in big data and neural network computing, memory access becomes the bottleneck for further performance improvement of computing systems, which is called "Memory Wall". Computing-In-Memory (CIM) is a promising technique to solve this problem [1]. On the other hand, with the increasing integration density on-chip enabled by Moore's law, power consumption rockets up and results in severe thermal problem, which is known as the "Power Wall". In order to break through "power wall" problem, several emerging semiconductor devices are proposed to achieve better power efficiency compared to CMOS transistors [2] [3]. For example, the spintronic technology which exploits the spin polarization of electrons for information processing has been extensively studied in recent years [4]. STT-mCell is a kind of spintronic device supporting both data storage and computing. With STT-mCell technology, the all-spin circuit can be implemented and serves as a current-driven circuit. STT-mCell circuits have ultra-low power and fast computing speed making them suitable for IoT and mobile computing applications [5].

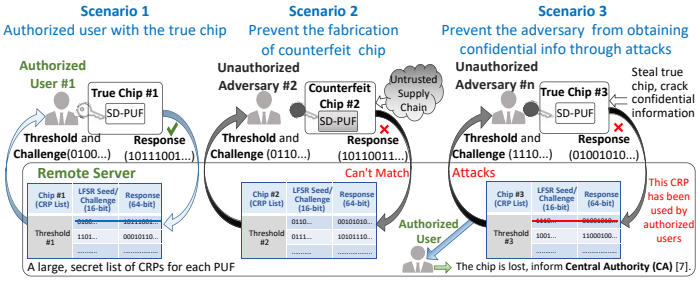


Fig. 1. Different scenarios of PUF application.

However, due to its non-volatility, hardware security has become a big concern for STT-mCell based all-spin circuits. After a growing number of attacks [6] [27], Physical Unclonable Function (PUF) has been proposed as an effective technique to enforce the data privacy and guarantee access permission of the confidential information. It harvests the intrinsic manufacturing process variations to produce a set of chip-unique responses from a set of challenges that are prohibitively hard to simulate, emulate or predict. The memory access delay can be exploited as a unique and unclonable "signature" of a chip [7]. For the application of PUF, as shown in scenario 1 of Figure 1, the Central Authority (CA) selects a challenge at random from challenge-response-pair (CRP) list in the remote server, and sends the challenge to the authorized user. The user #1 applies this challenge to the SD-PUF of the chip #1, after the user obtains the correct response of chip #1, and then use the chip. As shown in scenario 2 and 3 of Figure 1, the PUF helps in use cases such as prevention of semiconductor counterfeiting, chip authentication, and countering attacks.

Electronic PUFs are based on some electrical properties, such as transmission path delay and resistance value [7].

Kangwei Xu, Dongrong Zhang and Qiang Ren are with the School of Electronic and Information Engineering, Beihang University, Beijing, 100191 China (e-mail: xukangwei@buaa.edu.cn, dongrongzhang@buaa.edu.cn, qianren@buaa.edu.cn).

Patrick Girard is with the Laboratory of Computer Science, Robotics and Microelectronics of Montpellier, University of Montpellier, CNRS, 34095 Montpellier, France (e-mail: girard@lirmm.fr).

Yuanqing Cheng is with the School of Integrated Circuit Science and Technology, Beihang University, Beijing, 100191 China (e-mail: yuanqing@ieee.org).

The corresponding author is Yuanqing Cheng.

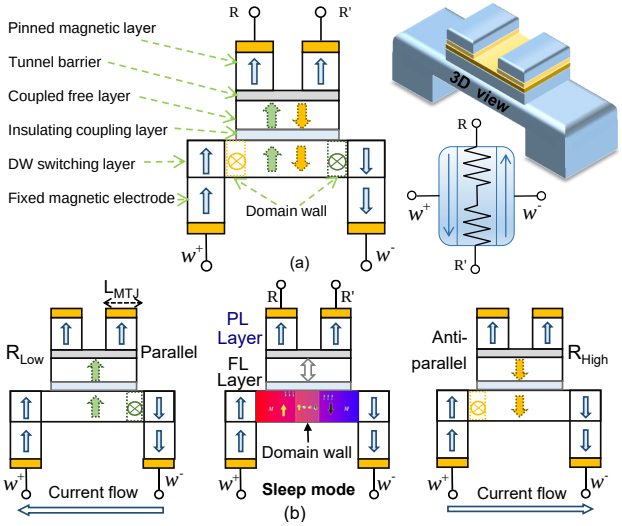


Fig. 2. (a) The symbol, 2D and 3D illustrations of a STT-mCell. (b) The low resistance (left) and high resistance (right) of a STT-mCell.

Many CMOS-based PUFs were proposed in the last decade to enhance the circuit security, such as Arbiter-PUF [8], ring-oscillator PUF [9], etc. However, the conventional CMOS PUFs have significant power consumption, and cannot be directly applied to all-spin circuits due to different logic switching mechanisms [6].

In this article, a novel area and energy-efficient PUF with high throughout is proposed based on STT-mCell's write delay variations. In addition, we also propose circuit-level design techniques that take advantage of the Design-for-Testability (DFT) structures, to enhance the reliability of our PUF. Compared to the state-of-the-art techniques, our design takes advantage of the intrinsic device characteristics, and avoids the use of techniques such as accelerated aging, ramping time adaption, and external effects that may degrade device performance and lifetime. The main contributions of our work can be summarized as follows.

- The proposed STT-mCell delay based PUF (SD-PUF) reuses existing components in the circuit to reduce area overhead and power consumption effectively. With a K-stage linear feedback shift register (LFSR), it can generate signatures of an arbitrary length smaller than $2^K - 1$ for a given challenge.
- To enhance the reliability of signature regeneration, we proposed an Automatic Write-Back (AWB) technique based on the DFT structure, fully utilizing the existing test components.
- A counter-based signature improvement technique is embedded in SD-PUF to enhance the signature's uniformity and uniqueness. And the SD-PUF is proven to be effective against to existing attacks.
- The throughout of signature generation is high (64 bits per clock cycle), i.e., multiple response-bits can be extracted with shorter test period. Moreover, the proposed PUF design methodology can be extended to other non-volatile CIM devices, such as magnetoelectric spin-orbit (MESO) device [10], Composite-Input Magnetoelectric-based Logic Technology (CoMET) device [11] and so on.

To the best of our knowledge, this is the first PUF design for STT-mCell based all-spin circuits. The rest of this paper is organized as follows. Section II presents the necessary preliminaries of STT-mCell and related works of advanced PUFs. Section III illustrates the PUF design challenges for STT-mCell based circuits. Section IV describes the implementation details of SD-PUF, AWB scheme and the counter-based signature improvement technique. Comprehensive evaluations of the proposed SD-PUF with extensive security analyses are given in Section V. Finally, we conclude the paper in Section VI.

II. Preliminaries and Related Work

This section firstly introduces a four-terminal magneto-electronic device named STT-mCell (referred to as "mCell") [5] and then describes the related work.

A. Introductin to STT-mCell

1) Basics of STT-mCell: The STT-mCell is a spintronic device with electrical insulation between the separated read and write paths. As shown in Fig. 2 (a), the four-terminals of the device form separated write path (w^+, w^-) and read path (R, R'). A magnetic tunnel junction (MTJ) is the basic storage element in STT-mCell. It is composed of a tunnel barrier sandwiched between a pinned magnetic layer (PL) and a coupled free layer (FL) as shown in Fig. 2 (b). The MTJ resistance R_{MTJ} is determined by the magnetization of the FL with respect to that of the PL. When the magnetization of the FL is the same as that of the PL (the input electron current flows from the w^- port to the w^+ port), the MTJ is in the parallel state and $R_{MTJ} = R_{Low}$ (low resistance). Otherwise, the MTJ is in the anti-parallel state and $R_{MTJ} = R_{High}$ (high resistance). The magnetization of the FL can be controlled by the domain wall motion underneath, which can be adjusted by injecting spin current as shown in Fig. 2 (b). In an MTJ, the resistance ratio between R_{Low} and R_{High} is defined as Tunneling Magnetoresistance Ratio (TMR), and is given by

$$TMR = \frac{R_{High} - R_{Low}}{R_{Low}} \tag{1}$$

The low and high resistances of a tunnel junction in an STT-mCell are given by (2) and (3) respectively [12].

$$R_{Low} = \frac{RA}{w * L_{MTJ}} \tag{2}$$

$$R_{High} = \frac{RA}{w * L_{MTJ}}(1 + TMR) \tag{3}$$

where w and L_{MTJ} are device width and MTJ length respectively, as shown in Fig. 2 (b).

2) Magnetic Memory with STT-mCell: Unlike conventional random access memory (RAM) chip technologies, data of STT-mCell are not stored as electric charge but instead stored by magnetic polarization of storage elements, which can be changed to represent either a '1' (i.e., PL is anti-parallel to FL) or '0' (i.e., PL is parallel to FL).

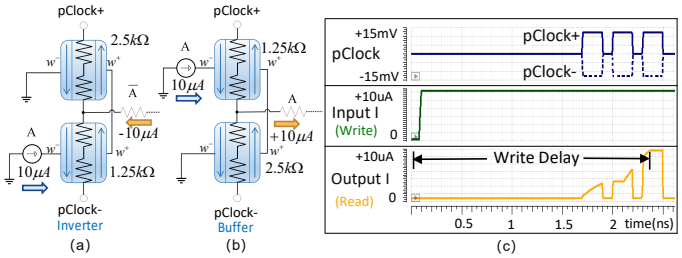


Fig. 3. (a) The schematic diagram of a STT-mCell based inverter. (b) The schematic diagram of a STT-mCell based buffer. (c) The logic gate level diagram of the buffer with pClk.

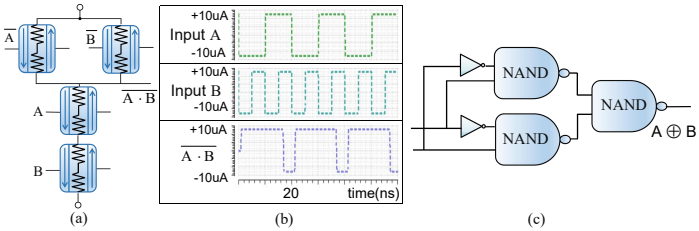


Fig. 4. (a) The schematic of a NAND gate based on STT-mCell. (b) Transient waveforms of operating the NAND gate. (c) An XOR gate based on NAND gates.

3) STT-mCell Based Logic: Similar to CMOS circuits, STT-mCells can be used to build various logic gates with pull-up and pull-down STT-mCell networks. As shown in Fig. 3(a) and (b), the STT-mCell based inverter/buffer can be constructed by two mCells, called pull-up mCell (UmC) and pull-down mCell (DmC). When the input is applied to the UmC (w^-), the DmC (w^-) becomes ground, UmC and DmC are complementary pairs [13]. The output current is

$$I = \frac{V(\frac{1}{R_{PU}} - \frac{1}{R_{PD}})}{k}, \quad k = 1 + R_{outpath}(\frac{1}{R_{PU}} + \frac{1}{R_{PD}}) \quad (4)$$

where V is the magnitude of the power supply. R_{PU} and R_{PD} are the resistances of the UmC and DmC in the gate.

An mCell is R_{Low} when the current is right ward (w^- to w^+) . An mCell is R_{High} when the current is left ward(w^+ to w^-). The generic buffer circuit is shown in Fig. 3(b). If the applied input is $I_{in} = +10\mu A$ in UmC of a buffer, R_{PU}= R_{Low}, R_{PD} = R_{High}, so the output current turns into a positive current (buffer: $I_{out} = +I_{in}$) by equation (4).

In addition to the buffer/inverter shown in Fig. 3, a variety of other logic gates can be constructed by STT-mCells [12]. For instance, a 2-input NAND gate and its functional simulation are illustrated in Figure 4(a) and (b), respectively. In the STT-mCell based circuit, since logic value is only based on the direction of the current flow, the positive current represents logic '1' and the negative current represents logic '0'. Based on the NAND gate, we can set up the XOR gate (Figure 4(c)) and so on. Furthermore, the implementation of SD-PUF is based on the current-driven property of STT-mCell, and the LFSR, scan chain, etc., can all be constructed by STT-mCell based gates.

4) The read/write operation of STT-mCell based logic gate: The isolated read and write paths make STT-mCell based all-spin circuit ultra low power and more reliable [12]. Similar to conventional MRAM, the STT-mCell is feasible for power gating by enabling/disabling clock signals. The clock signal is called $pClock$ in this paper. As shown in Fig. 3(b), it illustrates the function of $pClock$ and the read/write operations of a buffer. When the $pClock$ is disabled, the non-volatile circuit retains the state and enters a zero power sleep mode. When the $pClock$ is reactivated, the circuit instantaneously exits the sleep mode and logic computation continues as normal.

B. Related Work

Considering the existing PUFs, many area and energy-efficient designs have been proposed to enhance the uniqueness, reliability, security, and cost, which are summarized in Table I and presented as follows.

1) Reliability Improvement: Bhargava *et al.* used the accelerated aging effects to skew the bi-stable PUF cells so as to produce reliable bits [13] [14]. However, aging acceleration required dedicated circuit components or additional testing procedure, and also degraded the performance of the PUF when it worked as the normal memory [15]. Zhang *et al.* [16] proposed bit generation technique in an STT-MRAM-based MemPUF, which was stabilized with a novel automatic write-back scheme. But the PUF required an independent write-back module that resulted in larger area overheads.

The most common way to solve the reliability issue is to use Error Correction Code (ECC) [17] [18]. ECC stabilizes the noisy response-bits generated from the PUF. However, if the bit error rate (BER) of the raw response is high, the ECC overhead may be very costly. Circuit-level optimizations can be used to reduce the hardware overhead if they are properly applied.

2) Uniqueness Improvement: Zheng *et al.* took advantage of SRAM write-failure effect to produce random bits, and the supply voltage was used to increase the uniqueness (measured by Hamming Distance) of the PUF [19]. But it may be compromised if adversaries know the digital signals that can regulate the external effects (e.g., supply voltage [20] and electrical pulse [21]) for bit expansion, i.e., the adversaries may exploit the obtained information to predict the results of response-bit expansion to breakdown the PUF design. Another domain wall memory PUF (DWM-PUF) was proposed in [22]. This design provided additional knobs, e.g., shift pulse, number of access ports to expand the set of challenge-response pairs. The results showed excellent uniqueness. However, the domain wall can only be shifted forward and backward by injecting current from the left/right-shift contact. Read is performed by shifting the desired bit under the read head using spin polarized currents. For random access, the worst case latency is the summation of the number of shift latencies and the write/read latency.

3) Cost Improvement: Buskeeper PUF utilizes buskeeper cell, which is smaller than D flip-flop(DFF). However, the enhancement is for DFF PUFs and requires additional addressing circuit [23]. A system with the aging-resistant ring oscillator PUF (ARO-PUF) [24] offers a considerably smaller PUF footprint since it requires lighter ECC scheme than a system with the conventional RO-PUF. Although it shows less area overhead, the design is limited to custom layout implementations.

TABLE I
THE RELIABILITY, UNIQUENESS, COST AND SECURITY OF EXISTING PUF QUALITY IMPROVEMENT SCHEMES.

	Bi-stable PUF [13]	**MemPUF [16]**	**RESP [19]**	**DWM-PUF [22]**	**Buskeeper PUF [23]**	**ARO-PUF [24]**	**Non-Linear VTC [25]**	**CRC-PUF [26]**
Reliability	√	√	√	△	△	√	×	△
Uniqueness	△	√	√	√	△	△	√	√
Cost	×	×	×	×	√	√	△	√
Attack Resistance Analysis	Not Mentioned	Resistant to Side-Channel Attacks	Not Mentioned	Not Mentioned	Resistant to Reverse Engineering	Not Mentioned	Resistant to Modeling Attack	Resistant to Modeling Attack

(1) √ Indicates that the proposed scheme can improve the specific metric of PUFs' performance;
(2) △ Indicates that the proposed scheme may improve the specific metric of PUFs' performance;
(3) × Indicates that the proposed scheme may deteriorate the specific metric of PUFs' performance.

4) Resistance to Attack: In [25], a nonlinear voltage transfer function was instantiated to create a complex mapping between the challenge and response of each circuit module, which was impossible to attack. However, the nonlinear voltage transfer function varies with aging, and the error is accumulated at each stage, leading to low PUF reliability. A lightweight PUF construction, a Cyclic Redundancy Check (CRC) PUF was proposed in [26], which input challenges are de-synchronized from output responses to make a PUF model difficult to learn. However, its security evalution is only for modeling attacks and does not take other attacks into consideration.

Most of existing spintronic PUFs suffer from non-negligible area overhead. The arithmetic units of some improvements may be vulnerable to various attacks, and the operation phase requires long test time with low throughout. More importantly, the existing designs mainly target the memory security without considering the all-spin circuit design including both logic and memory for CIM architectures.

To this end, a spintronic PUF design with the following features is needed: 1) multi-response-bits can be extracted per clock cycle with inexpensively and effectively; 2) be able to generate signatures with satisfied uniqueness and low test cost; 3) can offer high reliability and resistance to adversal attacks.

III. PUF DESIGN CHALLENGES FOR STT-MCELL BASED CIRCUIT

In this section, the influence of process variation on STT-mCells electrical characteristics is first described, then the challenge-Response pair setting of SD-PUF is explored, and finally the reliability of response bit is analyzed.

A. Process Variation Impact on Write Delay of the STT-mCell

Process variations (PV) affect the characteristics of STT-mCells significantly. In this subsection, we firstly evaluated the process variation impact on STT-mCell. Then we explored the relationship between PV and the write delay of STT-mCell based logic gate.

The geometry of the STT-mCell structure, e.g., device width, MTJ length, TMR, and resistance area product (RA), may vary due to imperfections in the fabrication process [12] [27] [28]. During the fabrication of STT-mCell, one of the greatest challenges is to obtain high TMR with low RA of the MTJ. Low RA can reduce the power consumption of the circuit, but decreasing RA also results in a drop in TMR due to metallic conduction through the junction. Therefore, there is a trade-off between RA and TMR [29].

To successfully program the MTJ within a given delay, the current amplitude needs to be larger than a critical reference current (denoted as I_{ref}). As shown in Fig. 3 (b), a positive $10\mu A$ write current is injected to the buffer at $0ns$, and the buffer completely outputs $10\mu A$ at $2.5ns$. The time interval between them is called write delay of the mCell-based buffer. High TMR with low RA of the MTJ can reduce the write delay. The smaller L_{MTJ} is, the shorter the write delay is.

An etching step is required to fabricate and separate two MTJs that share the same free layer. The contact is difficult to fabricate because precisely etching the MgO barrier without damaging the magnetic free layer is challenging. In this paper, we consider the process variations of L_{MTJ}, RA and TMR simultaneously. When L_{MTJ}, RA and TMR change due to the process variations [12], the domain wall can have slightly different moving speeds, that can affect the write delay of each STT-mCell.

B. STT-mCell based Challenge-Response Pair Setup

Based on the observation of process variation impact on STT-mCell write delay, we can construct the all spin PUF. The Challenge-Response Pair (CRP) generation is described as follows.

1) Challenge generation: A PUF can be stimulated with external inputs, called challenges, upon which it generates with corresponding outputs, called responses. The generated response R_{Ci} depends on its internal physical disorder and the input challenge. As shown in Fig. 2, the STT-mCell is designed symmetrically for storing logic '0' and '1'. In actual manufacturing, due to the process variations, it is impossible to fabricate complete symmetrical left and right path (w^+, w^-). Moreover, the delay in writing '0'/'1' is slightly different, because the domain wall moves from the center to the left or right with slightly different distances due to process variations.

Therefore, the different logic '0' and '1' signal is equivalent to a challenge applied to each signature bit.

Meanwhile, the number of CRPs determine whether the PUF is strong or weak PUF. The number of CRPs (Challenge-Response Pairs) of a strong PUF must be very large, or it is exponential with respect to the number of components used for building the strong PUF [7]. A weak PUF can be stimulated by a very small number of fixed challenges C_i, and the number of responses generated by weak PUF is limited for each chip. However, the challenge bits designed from LFSR are different combinations of '1s' / '0s', which are considered as the exponential internal challenges applied to the SD-PUF. Therefore, the SD-PUF is designed with reference to strong PUF features

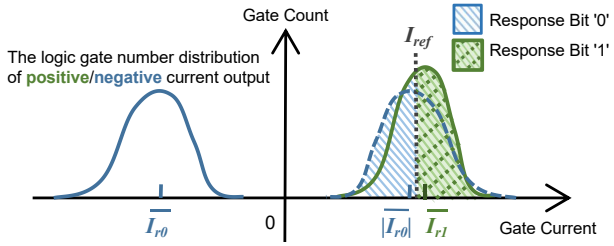


Fig. 5. Distribution of characteristic currents in the STT-mCell based buffers.

2) Extracting the Response-Bit: Read operations are performed by using a sense amplifier (SA) where the reading current I_r is compared against a reference value I_{ref}. Fig. 5 illustrates the distribution of the currents generated during read operations in case of outputing a positive current '1' (with average $\overline{I_{r1}}$) or outputing a negative current '0' (with average $\overline{I_{r0}}$). The reference current I_{ref} is generated by averaging the current flowing through all selected buffers during the read operation, and the reference current will be close to ($\overline{I_{r1}}$ + $|\overline{I_{r0}}|$)/2 [30]. If $I_r > I_{ref}$, this translates in a read '1' operation (shaded in green color), while if $I_r < I_{ref}$ it translates in a read '0' operation (shaded in blue color).

However, due to the unavoidable and unpredictable noise in the circuit, there is an uncertain sensing zone for the sense amplifier. The bits falling into the sensing margin, i.e. where $|I_r\text{-}I_{ref}|$ is smaller than the sensing margin of the SA, can induce a meta-stable state, which will be randomly stabilized to '0' or '1' depending on the noise in the circuit. To reduce the probability of such occurrences, we use a 3-stage sense amplifier (first stage for current sensing and the other two for voltage sensing), which can counteract the effect of read variability [30].

C. The Reliability of Response Bit Generation

Maintaining the reliability of response-bit generation under varying woking conditions is a major challenge for the spintronic PUFs [16]. The reliability of producing a response-bit is defined as the probability that bit b_t, generated from a selected logic gate at time point t, is reproduced as $b_{t+\delta t}$ at time $t + \delta t$ ($\delta t > 0$) (see Fig. 6).

On the one hand, the thermal fluctuation in the output current may cause the actual write delay vary over time due to the thermal noise (see Fig. 7 (a)). In 500 samples of STT-mCells's write

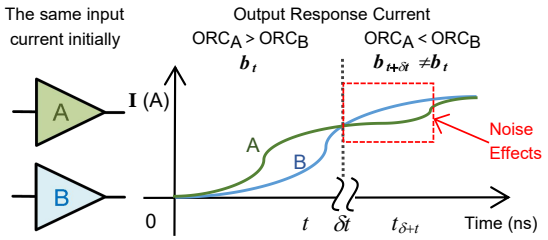


Fig. 6. Reliability model of SD-PUF. The reliability may be deteriorated by noise effects in STT-mCell, i.e., $b_{t+\delta t} \neq b_t$.

delay, there are a few mCells with larger variation from the standard value, which will degrade the reliability of signatures. When we designed SD-PUF, we tried to overcome the significant delay variations due to the small number of mCells that have large process variations. The masking scheme proposed in Section IV-D helps to improve the quality of a few biased bits. On the other hand, the bits generated from the cells may be disturbed sightly by external/neighbor magnetic field [16]. Assuming that θ (the angle between FL magnetization and PL magnetization) is distributed as in [31], Figure. 7 (b) plots the complementary reliabilities (represented by Bit-Error Rates or BERs) at different temperatures by our simulation (See Section IV for simulation setup details). It shows that the BERs increase with increasing ambient temperature and reaches 17% in the worst case.

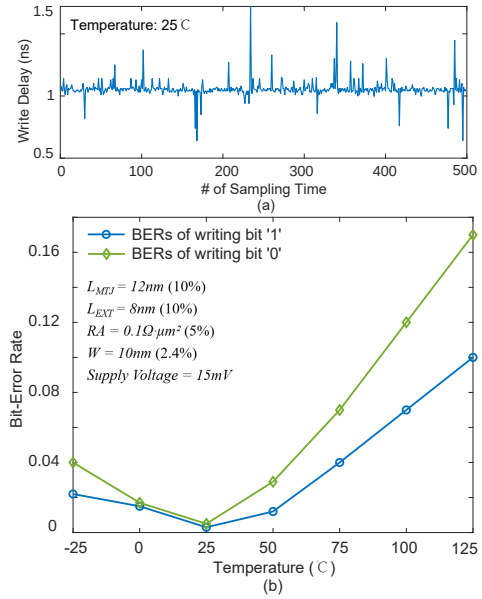


Fig. 7. (a) The distribution of the write delay of STT-mCells from 500 samples. Temperature is 25°C. (b) BERs at varying temperature points (from -25°C to 125°C) were calculated in the 500 samples that produce unreliable bits in consecutive 10 read-out operations. Nominal values and variations (shown in brackets) of the relevant process parameters used in the simulation are shown in the figure.

The effectiveness of PUF may be degraded if these fluctuations affect the bit generation process more than the other intrinsic mCell variations. Therefore, the STT-mCell based PUF design needs techniques to enhance reliability.

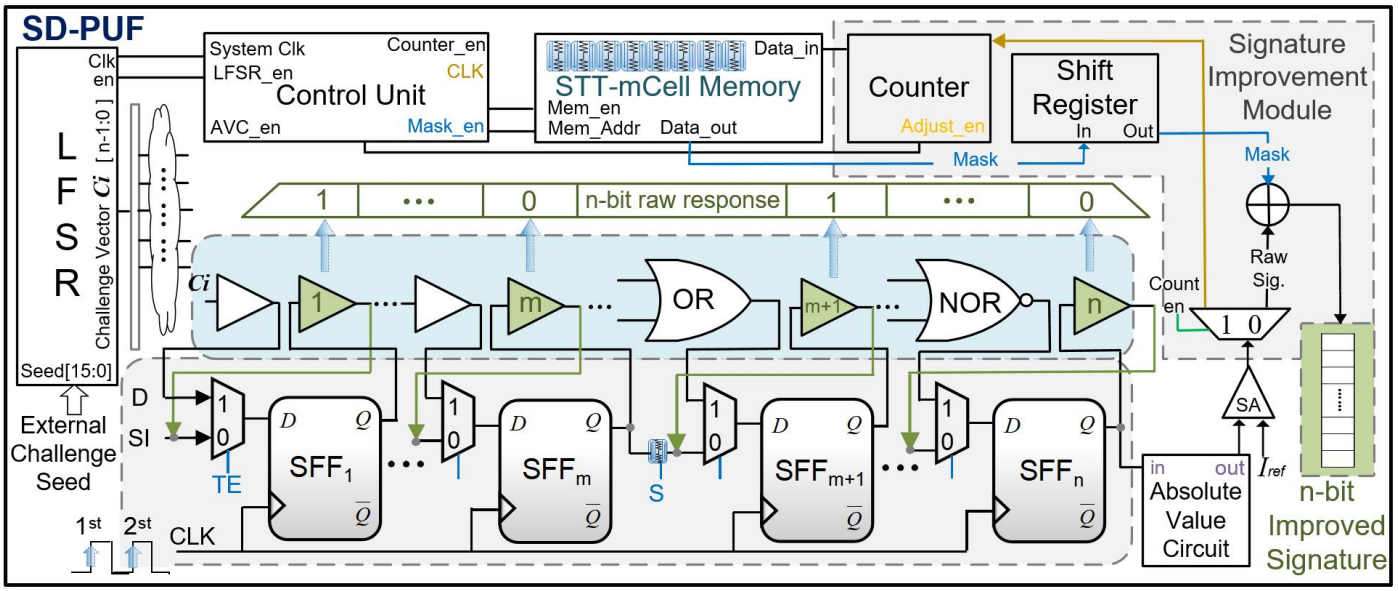


Fig. 8. The architecture of the proposed STT-mCell Delay based PUF (SD-PUF).

IV. Write Delay Based STT-mCell PUF Architecture

In this section, we present the implementation of a novel spintronic PUF in the STT-mCell based all-spin circuit.

A. Overview of SD-PUF Architecture

As shown in Fig. 8, all logic gates in the circuit are built by STT-mCells. Like conventional CMOS VLSI design, we assume the DFT structure is also embedded in the all-spin circuits, including scan flip flops and scan chains and we select the logic gates following the SFFs for delay characterization. Its principle is based on that their input can be controlled by scan flip-flops (SFFs) in the scan chain. That is, the challenges can simultaneously reach the inputs of logic gates by the SFFs. The working procedure of SD-PUF is as follows.

At the beginning, initialize all logic gates to zero voltage. An external challenge vector is provided as the initial seed of a linear feedback shift register (LFSR), which generates an internal challenge vector (C_i). C_i is propagated through the circuit to the D terminal of scan flip-flops (SFFs) in parallel, and then with the rising edge of clock signal arrives. C_i is simultaneously applied to the logic gates following the SFFs. In Fig. 8, we denote the selected gates for delay characterization with numbers $1, \cdots, m, m+1, \cdots, n$. The write delays of these gates are different due to process variations. Furthermore, the buffers selected under test, are controlled by the same SFF's clock to synchronize the write and read operations. The first buffer (labeled as '1' in the figure) has been written completely. As a result, the signature bit of this buffer is logic value '1'. However, the buffer labeled as 'm' in the figure may not receive enough current to reach the switching threshold within the same time period. So the signature bit corresponding to buffer 'm' is still logic value '0'. Then, these selected buffers can generate different digital signature bits of '0'/'1' simultaneously based on the process variations of each mCell-based all-spin chip.

B. The Detailed Implementation of SD-PUF

The proposed SD-PUF is composed of an LFSR, and the scan chain existing in the DFT structure. By utilizing the existing components as much as possible, SD-PUF can reduce the area and power overheads effectively. The main components and their functionalities are described as follows.

- *Linear Feedback Shift Register (LFSR):* An external challenge vector as an initial seed is provided to the LFSR, and it generates a 64-bit internal challenge vector (C_i) in each clock cycle. Note that the challenge length is determined by the number of selected gated under test, and any LFSR capable of producing a 64-bit pseudo-random number can be used for this work. The LFSR ensures the diversity of challenges for a 64-bit signature.
- *The scan chain structure:* Note that DFT techniques are widely used in contemporary ICs [32]. SD-PUF reuses the scan chain to implement its functionality. Fig. 8 shows SFFs are stitched together and form a scan chain. The outputs (internal challenge C_i) of the LFSR act as the inputs of the scan chain, and are written to the SFFs (triggered by the rising edge) in parallel.

Now we describe how to test the buffer write delay. The threshold current (I_{ref}) is assumed to be $9.56\mu A$ at $2.5ns$. The assumed switching threshold is generated by averaging the switching currents of 1000 STT-mCells considering process variations. After initializing the buffers to zeros, different positive $+10\mu A$ (logic value '1') write currents and negative $-10\mu A$ (logic value '0') write currents are injected to buffers. After the response is generated, it is shifted out by the scan chain, then passes through the absolute value circuit [33] and sense amplifier (SA) [34], where the response read current (I_r) is compared against to a reference threshold (I_{ref}). If the buffer output I_r exceeds the I_{ref}, we can get the logic value '1', otherwise, we get the logic value '0'.

In actual circuit design, a buffer/an inverter is generally placed behind the D flip-flop to improve driving capability.

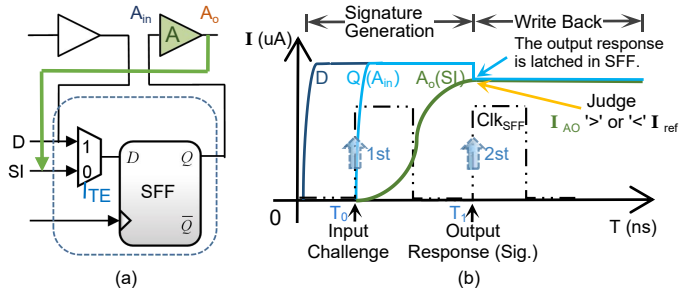


Fig. 9. (a) The schematic of the AWB scheme. (b) The transient timing diagram of latching a bit in the scan flip-flop.

Therefore, we selected buffer as the logic gate for the test in the experiment, rather than placing an arbitrary gate. It is convenient to use the unified clock to control the same logic gates. The more gates we can choose from, the higher randomness of the authentication signature is. If there are n logic gates to be chosen, less than $2^n - 1$ different response combinations can be generated.

In the following, we will introduce an automatic write-back (AWB) scheme to enhance the reliability of bit regeneration, and a counter-based signature improvement technique to improve the uniqueness and security of the SD-PUF further.

C. The Automatic Write-Back Scheme

We propose an automatic write-back (AWB) scheme, to exploit the non-volatility of the STT-mCell to improve the reliability of raw response. It aims to make the random bit reproducible thereafter. As shown in Fig. 8, in the write-back phase, the switch 'S' and the terminal 'TE' are set to 0, which means that the switch 'S' is open, and the response is written back to the 'SI' terminal, it prevents interference between every two stages of the SFFs. Note that when the circuit performs its normal logic operations (not in the PUF test phase), TE=1, the enabled D terminal is selected for transmission [7]. The write-back phase is independent of the other phases.

The principle of the AWB scheme is described below, as shown in Fig. 9, *when the write time of selected logic gate reaches the delay threshold T_1, all SFFs are triggered by the rising edge of the clock signal, the generated bit is automatically written back into the scan flip-flop (SFF).*

Due to the process variation of buffer 'A', the write delay between write (A_{in}) and read (A_{out}) is unique. Fig. 9(b) shows the timing diagrams of write-back process in the scan chain. Firstly, a current (line 'D') is injected to the SFF, after the first rising edge of the clock, the output current ("challenge", line 'Q') reaches A_{in} of the buffer 'A' at time T_0. Execute the write-back scheme, TE is set to 1 and the switch behind SFF is open. Then, the SFF is triggered by the second clock rising edge, the output response current is written to the SFF with a fixed current value at time T_1 (i.e., the response is latched in SFF via write-back wire). The time interval between two rising edges is the write delay threshold T_{ref} we set. Finally, the response can be shifted out by the scan chain for post-processing.

The security of AWB is guaranteed by its "spontaneous" execution upon the completion of read operation in the procedure mentioned above. Therefore, malicious write is prohibited during the write-back process. Note that our proposed AWB scheme may also be used in other PUFs based on other emerging non-volatile memory (NVM) technologies. Compared to other NVMs, the write endurance of STT-mCell is much higher [12] (e.g., FLASH [35] and Phase Change Memory [36]). Furthermore, STT-mCell has several advantages over other types of NVMs: 1) the density of STT-mCell is high, which makes it infeasible for tampering attacks such as probing the internal nodes or wires; 2) since the current required for successful STT-mCell switching is not as large as that used in MRAMs [37], the electro-magnetic coupling is too weak to be exploited by side-channel attacks [38].

Compared to the reliability improvement techniques proposed in the literature [13] [14] [39], our method is superior in several aspects. Firstly, unlike the approach in [16], generation of the response bits in our scheme does not necessarily require setting the two MTJs into complementary states to represent write-back value, which may add extra hardware overhead and the complexity of write-back operation. Secondly, our method does not rely on aging effects on the memory devices for reliability enhancement. Aging effects such as hot-carrier injection and negative-bias temperature instability may change the inherent properties of the devices permanently, and the stability of read/write operations will be significantly deteriorated [15].

More importantly, the traditional test structure requires more area on-chip, but we only need to add a write-back wire to the original DFT structure in our AWB scheme. Moreover, the scan chain is immune to security attacks because when the circuit is switched from PUF mode to normal logic check mode, SFFs in the scan chain will be reset (i.e., written by 0) before other read/write operations are performed. Even if the adversary understands our PUF test methodology, they cannot get the threshold value stored on off-chip authentication server of each PUF die. Therefore, the secret bit generated in the PUF mode cannot be reproduced or predicted.

D. Counter-Based Signature Improvement

In the actual circuit, logic gates may be interfered by the surrounding environment conditions or manufacturing process variations (PV), and a small portion of the '0'/'1' signature may be biased [40]. Meanwhile, with the modern semiconductor supply chain, the foundry may control the process parameter to bias the output signature, and ship out-of-spec/defective devices [7]. To improve the quality and security of signature, a counter-based signature improvement technique is proposed for SD-PUF as shown in Fig. 8.

The counter-based signature improvement module consists of a counter, a multiplexer and an XOR gate. A signature masking scheme is used to enhance the uniformity and uniqueness of SD-PUF. The control and processing unit initiates the mask generation circuit to generate the mask for each SD-PUF. An external 16-bit seed is applied to the LFSR and a 64-bit signature is used for mask generation. The multiplexer is used

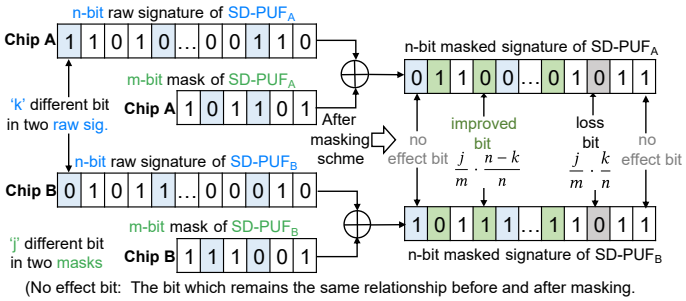


Fig. 10. The masking scheme diagram for improvements in signature uniformity and uniquenes.

to select the bit '1' in this new signature. The total occurrences of bit '1's in the signature are accumulated in the counter, and is converted to binary code as the m-bit mask, which is stored in STT-mCell. When SD-PUF is activated by the user, the control unit loads the m-bit mask value from memory into *the Shift Register*.

The XOR gate is used to XOR the raw signature with the mask. As shown in Fig. 10, controlled by the rising edge of clock signal of SFFs, the n-bit raw signature shifted in the scan chain is XORed with the m-bit mask shifted out by the shift register. That is, the m-bit mask is XORed with the m-bit of n-bit signature every cycle until all n-bit are XORed. The new n-bit masked signature is the final signature.

As shown in Fig. 10, with the masking scheme, the uniqueness of SD-PUF's signature can be improved. Assume that there are different k bits between two n-bit raw signatures, and different j bits between two m-bit masks for two SD-PUFs. Then, there are n-k same bits between two raw signatures.

With the masking scheme, only $\frac{j}{m} \times 100\%$ different mask bits can affect the raw signature bits. Among these affected bits, $\frac{n-k}{n} \times 100\%$ would be flipped compared to the raw signatures, which increases the uniqueness of the generated signature. However, there would be $\frac{k}{n} \times 100\%$ bits flipped to the same values, which reduces the uniqueness (because they were actually different in raw signatures). So the overall uniqueness enhancement can be represented as:

$$\Delta u = \frac{j}{m} \cdot \frac{n-k}{n} - \frac{j}{m} \cdot \frac{k}{n} = \frac{j}{m}(1 - \frac{2k}{n}) \qquad (5)$$

As shown in (4), the whole uniqueness is improved for cases with $\frac{k}{n} < 0.5$, and the lower the initial uniqueness

TABLE II
THE STATISTICAL PROBABILITY DISTRIBUTION OF UNIQUENESS IMPROVEMENT WITH THE MASKING SCHEME.

Two SD-PUFs	The probability of the same bit values in two signatures: $\frac{n-k}{n}$	The probability of the different bit values in two signatures: $\frac{k}{n}$
The probability of the different bit values in two masks : $\frac{j}{m}$	$\frac{j}{m} \cdot \frac{n-k}{n}$	$\frac{j}{m} \cdot \frac{k}{n}$
The probability of the same bit values in two masks : $\frac{m-j}{m}$	No effect	No effect

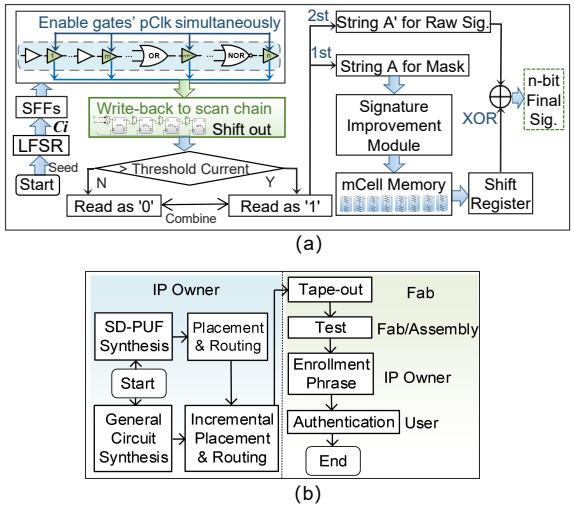


Fig. 11. (a) The structure diagram of SD-PUF; (b) The working flow of SD-PUF.

$\frac{k}{n}$ is, the more improvement Δu can be achieved. Also, it should be noted that an instable bit within m-bit mask can cause $\frac{n}{m}/n = \frac{1}{m}$ final signature bit error rate (BER) due to the repeated mask application scheme. Therefore, it is necessary to store the mask value in non-volatile STT-mCell, to improve its resiliency to attacks, which will be discussed in Section V-G. As shown in Fig. 8, the control and processing unit is used to control the activation of SD-PUF, enable counter-based signature improvement module, store and load mask/threshold values.

The proposed SD-PUF is scalable and can be extended to other non-volatile memory and computing devices, such as magnetoelectric spin-orbit (MESO) device [10], Composite-Input Magnetoelectric-based Logic Technology (CoMET) device [11] and so on. Meanwhile, the proposed SD-PUF structure with the two improved schemes mentioned above can also be used in CMOS-PUF design.

In summary, the structure and workflow diagrams of SD-PUF with signature improvement are shown in Fig. 11 (a) and (b), respectively. The main steps in the work flow is described as follows.

- *Challenge Generation:* Initialize all inputs to zero. Then, a 16-bit external seed is applied to a 16-stage LFSR, and a 64-bit long input challenge (seed) C_i is obtained.
- *The Mask Generation:* Enable the masking functionality. Controlled by the first rising edge of SFFs' clock, C_i simultaneously reaches the inputs of the logic gates following the SFFs. 64 bits signature (String A) is written back to the scan chain by the second rising edge, and then shifted out to the signature improvement module. The multiplexer is used to select bit '1's in this signature. The total occurrences of bit '1's in 'String A' are accumulated in the counter, and is converted to a binary code as an m-bit mask. Then, the m-bit mask value is stored in STT-mCell memory. When an XOR operation is performed, the mask is shifted out by the shift register.
- *The Raw Signature Generation:* The raw signature gen-

eration process is basically the same as the signature generation process used for the mask as mentioned above. First, the testing mode is enabled and a new 16-bit seed (different from the previous one) is applied to the LFSR. Then, a new 64-bit sequence of '0'/'1's can be generated as the raw signature ('String B').

- *The Improved Signature Generation:* Controlled by pClock, the n-bit raw signature is shifted out bit by bit through the scan chain and XORed with the m-bit mask in sequence. Finally, the n-bit masked signature can be served as the final masked signature.

V. Experimental Results

In this section, we evaluated the three most important metrics of SD-PUF, i.e., uniqueness, uniformity and reliability. The STT-mCell model that has been validated against experimental data was used in our simulations [46]. The area and energy consumption of our design were compared with the state-of-the-art works.

TABLE III
Paremeters Used in the Monte Carlo Simulation

Parameters	Nominal values	Process Variation (RSD)
Length of MTJ	L_{MTJ} = 12nm	10%
Distance of two MTJs	L_{EXT} = 8nm	10%
RA of the mCell	RA = 0.1Ω·μm²	5%
Width of the mCell	W = 10nm	2.4%
Supply Voltage	15mV	-
Temperature	25℃	-

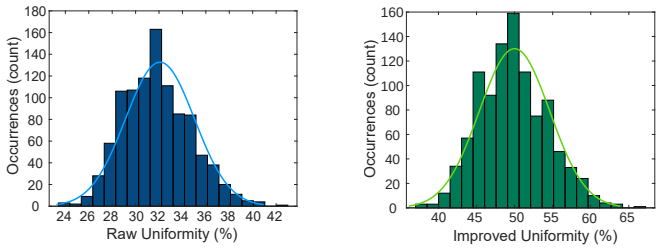
A. Experimental Setup

The standard logic modules are built based on the Verilog-A model of STT-mCell [46], and simulated in Cadence Spectre [41]. The simulation results are compared with the prototype in [46] to show the accuracy of the logic modules. The power consumption of each logic module was calculated in Virtuoso Calculator. Based on these logic modules, the circuit-level simulations of SD-PUF were performed with Cadence Spectre, the total area overhead and power consumption of SD-PUF were synthesized by Design Compiler.Parameters used for Monte Carlo simulation are given in Table III. During simulations, the same challenge set was applied to the LFSR of all 1000 SD-PUF samples at 25°C with $15mV$ supply voltage to produce the final 64-bit signature. Finally, the statistical data were generated and analyzed in Matlab. ITC99 [42], Gaisler [43], ISCAS [44], and OpenSPARCT2 [45] benchmarks were used for evaluations.

B. Uniformity Analysis

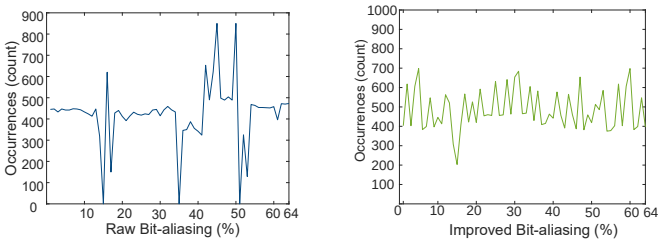
The uniformity denotes a good random distribution of logic values '0' and '1' in each PUF signature. The average uniformity of the raw signatures with the masking scheme is 49.03% (ideally 50%) as shown in Fig. 12 (b).

The bit-aliasing indicates a balanced random distribution of '0's and '1's for the same bit position in a PUF population. The bit-aliasing of the raw signatures and the masked signatures are



(a) (b)

Fig. 12. Uniformity reflecting the randomness among various bits within the same chip. (a) Uniformity of the raw signatures without masking scheme, μ = 32.08%. (b) Uniformity of the signatures with masking scheme, μ = 49.03%.



(a) (b)

Fig. 13. Bit-aliasing reflecting the randomness in the same bit among all signatures. (a) Bit-aliasing of raw signature, μ = 42.35%. (b) Bit-aliasing of the signatures with masking, μ = 48.47%.

shown in Fig. 13 (a) and (b), respectively. We can observe that the masking scheme reduces the bit-aliasing of the SD-PUF signature effectively.

C. Uniqueness Analysis

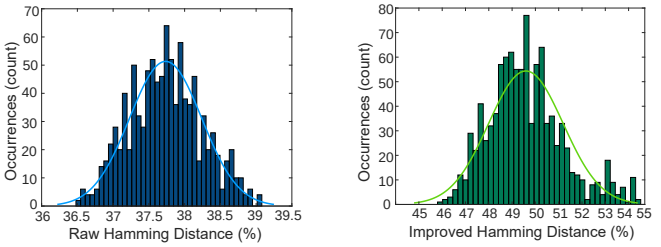
Uniqueness is often quantified as the average Hamming distance between the signatures to the same challenge obtained from all SD-PUF samples measured in the same environmental condition. Let R_u and R_v be the n-bit responses of two different chips, u and v, the uniqueness U for m chips is expressed as

$$U = \frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^{m} \frac{HD(R_u, R_v)}{n} \times 100\% \quad (6)$$

where the function HD computes the Hamming distance between two PUF values. The results are calculated based on 64-bit strings generated from SD-PUF. As shown in Fig. 14, the uniqueness of the improved signature approaches to 49.61% (ideally 50%), which indicates a high uniqueness of the produced bits.

D. Reliability Analysis

The reliability measures the stability of PUF responses to the same challenge under temperature and supply voltage variations. It was evaluated by comparing the response bits generated at different operating corners with those at the nominal corner (25°C, $15mV$). The proposed SD-PUFs were measured with the supply voltage, in the range of $15mV$±20% with a step of $1.5mV$. The thermal models for STT-Cell have also been thoroughly discussed in some studies [12] [47] [48].



(a) (b)

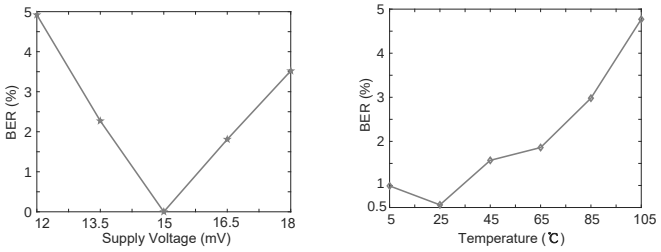
Fig. 14. The distribution of the Hamming Distance obtained from SD-PUF using N = 64 logic gates for 1000 chips. (a) HD of the raw signatures, μ = 37.73%. (b) HD of the improved signatures, μ = 49.61%.

To facilitate thermal analysis of STT-mCell at the circuit level, we added the temperature variable to the mCell Verilog-a file and varied it from 5°C to 105°C.

Let R_i be an n-bit response to an input challenge C produced by a PUF chip i under the nominal operating condition. The same set of challenges were then applied k times to obtain the response $R_{i,j}$ for $j = 1, 2, ...k$. The reliability S of chip i can be computed by

$$S = 1 - BER = 1 - \frac{1}{k}\sum_{j=1}^{k}\frac{HD(R_i, R_{i,j})}{n} \times 100\% \quad (7)$$

Fig. 15 illustrates the bit error rate (BER) with environmental variations. The average worst BERs tested with voltage and temperature variations are 4.92% and 4.77%, respectively. The BER$\leq$10% is acceptable for PUF designs since error-correcting codes can be used with a low cost [51]. The results demonstrate that SD-PUF is robust.



(a) (b)

Fig. 15. PUF reliability metrics estimated for 1000 SD-PUFs operating under supply voltage and temperature variations.

E. Optimal Sizes of Mask and Signature

Table IV summarizes the results obtained for the different signature and mask sizes. The minimal size, for which the conditions of unpredictable SD-PUF are met, is $length_{\_signature}$=32, $length_{\_mask}$=4 (marked in blue in Table IV). However, this size would be sensitive to additional noise that may affect its reliability. A better option, is $length_{\_signature}$=64 and $length_{\_mask}$=6 (marked in green in Table IV). This option guarantees the reliability of SD-PUF with sufficient margins for additional noise and relatively low BER. Moreover, this option has better signature uniqueness.

TABLE IV
PUF RELIABILITY AND UNIQUENESS WITH DIFFERENT LENGTHS OF THE RAW SIGNATURE AND THE MASK.

$l_{-sig.}$	l_{-mask}	No. of masking cycles	BER	fHD[%]		fHW[%]	
				μ	σ	μ	σ
8	2	4	4.56	35.77	10.6	48.65	5.5
16	2	8	9.19	38.95	9.1	48.33	9.2
16	3	6	11.42	41.78	9.4	48.51	7.3
32	4	8	12.72	48.02	5.4	49.31	5.4
32	5	7	10.03	45.55	8.6	48.20	6.9
48	5	10	7.81	49.41	3.1	48.98	4.8
64	4	16	6.85	49.58	1.6	49.19	4.6
64	6	11	5.14	49.61	1.5	49.03	5.0

F. Area Overhead

As mentioned above, the two parts: LFSR and scan chains are reused parts in the existing circuit without incurring extra hardware overhead. Therefore, the area overhead mainly comes from buffer, counter, multiplexer XOR gate, the absolute value circuit, the sensor amplifier, and STT-mCell memory.

Refer to the methods taken by peers, and the mCell manual [46] [49] to calculate the spin circuit area [50], we defined the area of various logic gates in the library file. The total area overhead of SD-PUF was synthesized in Design Compiler with those STT-mCell gates in 45nm technology node. And the area per bit $(area/bit)$ can be calculated by

$$area/bit = (total\ area - reused\ area)/n \quad (8)$$

where $total\ area$ is the area of SD-PUF, the $reused\ area$ includes the area of LFSR and scan chain, n is the number of response bits.

As shown in table VI, due to the reuse of LFSR and scan chain, SD-PUF has area benefits over other designs. We also evaluated the area overheads for some benchmarks (i.e., Gaisler, ITC99 and ISCAS) shown in Table V. We can observe that the area overhead is negligible, especially for large-scale circuits.

TABLE V
THE AREA OVERHEAD OF SD-PUF.

Benchmark	leon2	leon3mp	b22	s38584
Area Overhead(%)	0.0024	0.0031	0.09	0.26

G. Security Analysis

Some adversary-designed possible attacks against the SD-PUF are discussed as follows.

1) *Modeling Attack:* Adversarial machine learning-based modeling attack is an emerging threat to the security of the PUF design. Modeling attack is generally carried out in three steps: 1) the adversary collects lots of CRPs of a specific PUF; 2) the adversary uses large CRPs to train the predictive model; and 3) the adversary applies new challenges and uses the predictive model for the specific PUF to obtain the complete PUF CRPs, breaks its security. The effectiveness of modeling

attack is based on the principle that similar challenges tend to generate similar responses, because signal propagation delay can be well represented by an additive linear delay model with a limited number of unknown parameters [56].

However, the mCell-based circuit consists of nonlinear magnetic devices. There are complex dependencies between the related parameters, such as magnetic field variations inside the device. Meanwhile, the threshold current stored in the server in different SD-PUFs may be different, which also makes it difficult to perform modeling attacks.

To prove the security of SD-PUF under modeling attack, 16 one-hot challenges are applied, as shown in Fig. 16(a) and (b). The average HD of the 16 responses is 38.63%, indicating that SD-PUF is capable of yielding significantly diverged signatures for similar challenges. Therefore, it is difficult for adversaries to succeed in modeling attacks.

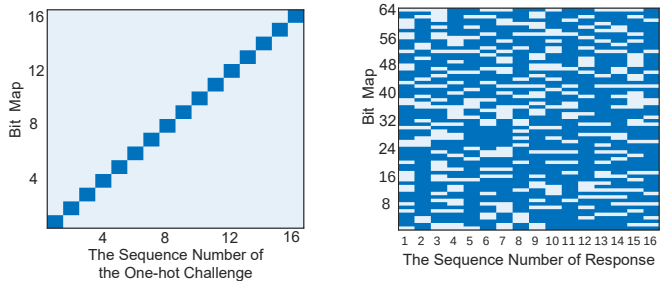


Fig. 16. The binary bitmaps of one-hot challenges and improved signatures in the modeling attack scenario. The '0's and '1's are represented by light blue pixels and dark blue pixels, respectively.

2) *Side-Channel Attack:* Side-channel attack is an effective way to gain the implementation information of a cryptosystem. Side-channel attack can be performed by extracting varied power profiles caused by the internal operations. For example, the traditional butterfly PUF is vulnerable to side-channel attack. With the power side-channel attack, the current and power can be collected from each current trace. Based on the extra power consumption of each response, the portion of '1' can be deduced. Although the LFSR within SD-PUF may be vulnerable to side-channel attacks, it leaks no information about the mapping between challenges and signatures. As the signature generated by SD-PUF depends on the variations of write delay with complex magnetic coupling dependence among associated parameters, it is almost impossible for the adversary to to find out the relationship between challenge vectors and each signature bit.

3) *Fault Injection Modeling Attack:* During fault injection modeling attack, the adversary deliberately changes environmental variations to collect reliable CRP set and reduce the dimension of CRP space to make modeling attacks easier [57]. However, identifying the reliable CRPs of SD-PUF in different environments is difficult, because environmental effects can not be used for reducing CRP space of SD-PUF with satisfying reliability. Furthermore, compared with MRAM [16], external/neighbor magnetic interference has little influence on STT based RAMs, the switching of STT-mCell is not driven by the external magnetic field, but a current going through the device instead [46].

4) *Memory Attack:* As we can see from the masking scheme above, the threshold read pulse setting stored in IP owner's server is not known to the adversary. Meanwhile, the mask is stored in STT-mCell memory. If the mask is stolen [58] [59], the adversary only knows the quantity of logic '1' values in the raw signature. To guess all bits in the raw signature by brute force, the hit probability is $\frac{1}{2^n}$, where n is the signature length. The time effort of guessing the whole signature with size larger than 32-bit is unacceptable.

5) *Deterministic Attack:* During tape-out of the SD-PUF in fab, the adversary can control the process variations of the logic gates following SFFs. The output raw signature may be biased toward '0' or '1', which severely deteriorates the randomness of the signature. If 20% process variation (σ_{L_MTJ}=2.4nm) is applied to all logic gates in the simulation, the uniqueness of the raw signatures is 4.95%. However, the poor uniqueness can be overcome by the masking scheme. Then, the uniqueness of the improved 64-bit signature is 42.11%. This proves that the loss of uniformity and uniqueness caused by deterministic attack can be improved by the proposed scheme effectively.

6) *Man-In-The-Middle Attack (MITM):* During the authentication process, a large list of CRPs and a threshold stored on a server list, the challenge sent to the user is chosen randomly from this list, and the response obtained from the user is verified for correctness against this list. The adversary in the middle involves eavesdropping on the communication between the PUF and authentication server. The adversary may collect a CRP set of an authentic PUF, and uses the CRP set to train the predictive model. The SD-PUF against the modeling attack is described in Section V-G (1).

For another, the adversary may directly attack the chip by collecting a threshold and a CRP. This method is useless in PUF authentication. For the reason that each CRP can only be used once, and the CRP-list on a server shrinks over time [7].

H. Comparison

Table VI compares the figures of merit among several state-of-the-art PUF designs with the proposed SD-PUF. SD-PUF shows satisfying security performance (see Section V-G). Compared with other PUFs in terms of design effort, the proposed SD-PUF reuses the scan chain to replace the PUF array that generates response. By using the existing all-spin circuit, the signature is reliable with high throughout (64 bits per clock cycle), and SD-PUF has significant area and power benefits over other designs.

VI. Conclusion

In this work, we propose a novel delay PUF (SD-PUF) design for the emerging STT-mCell based all-spin circuits. By incorporating the AWB scheme, the generation of raw response-bits produced from the SD-PUF can be stabilize under varying operating conditions. The uniformity and uniqueness of the signature are improved by signature masking. Simulation results

TABLE VI
COMPARISON OF THE PROPOSED SD-PUF WITH OTHER STATE-OF-THE-ART PUF DESIGNS.

Metrics	SD-PUF	Sym-PUF [52]	Com-PUF [53]	SRAM-PUF [54]	INV-PUF [54]	STT-RAM PUF [16]	Non-Linear VTC [25]	Arbiter-PUF [8]	Buskeeper [55]
Technology Node	45nm	65nm	65nm	65nm	65nm	45nm	45nm	180nm	65nm
Energy/bit(pJ)	5.65×10^{-3}	0.93	0.548	1.1	1.5×10^{-2}	0.69×10^{-3}	N/A	N/A	N/A
Uniqueness(%)	49.61	50.6	50.01	33.21	50.14	49.9	49.8	50.0	49.1
Temp. range(℃)	5-105℃	0-80℃	0-80℃	25-85℃	25-85℃	-40-85℃	0-90℃	-25-85℃	-40-85℃
BER per 10℃ (%)	1.07	0.68	0.44	6.67	0.47	2.16	0.9	1.4	1.14
BER per 10% volt (%)	2.10	1.82	0.13	>16.67	1.3	N/A	3.65	N/A	N/A
Area/bit(μm²)	2.46×10^{-3}	29.86	7.42	N/A	N/A	0.43	N/A	N/A	N/A
Design Effort	Counter, XOR, SA, Absolute circuit, MUX, Shift register. (low)	PUF array, Row Decoder, Read module. (high)	PUF array, Decorder, MUX,Comp. (relatively low)	PUF SRAM array, MUX Decorder. (high)	PUF INV array, MUX, Decorder. (relatively low)	PUF cell,SA, Row/Column Decorder, Write driver, MUX. (low)	Non-linear VTC block, Switch, SA, Reliability enhanced circuit. (low)	RF front-end, OTP memory, Multiplexer, Arbiter, LFSR. (relatively high)	Buskeeper, Register, Multiplexer, Fuzzy extractor. (high)
Security	As shown in Section V-G	Vulnerable to Modeling Attack	Vulnerable to Modeling Attack	Vulnerable to Modeling Attack	Resistant to Fault Injection Attack	Resistant to Side-channel Attack	Resistant to Modeling Attack	Resistant to Modeling Attack	Resistant to Fault Injection Attack

[1] N/A illustrate the data is not available; [2] Compared with the optimal value from published results;

considering process variations of STT-mCells show that SD-PUF is reliable to environmental variations. Additionally, the SD-PUF reuses the existing circuit components with minimal extra hardware overhead, and it simultaneously generates 64 bits signature with low power consumption compared to the state-of-the-art PUF designs. The security of SD-PUF against various attacks is also validated.

REFERENCES

[1] B. Yan, F. Chen, Y. Zhang, C. Song, H. Li and Y. Chen, "Exploring the opportunity of implementing neuromorphic computing systems with spintronic devices," 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, 2018, pp. 109-112.

[2] F. Oboril, R. Bishnoi, M. Ebrahimi and M. B. Tahoori, "Evaluation of Hybrid Memory Technologies Using SOT-MRAM for On-Chip Cache Hierarchy," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 34, no. 3, pp. 367-380, March 2015.

[3] R. Patel, X. Guo, Q. Guo, E. Ipek and E. G. Friedman, "Reducing Switching Latency and Energy in STT-MRAM Caches With Field-Assisted Writing," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 24, no. 1, pp. 129-138, Jan. 2016.

[4] Y. Xu, B. Wu, Z. Wang, Y. Wang, Y. Zhang and W. Zhao, "Write-Efficient STT/SOT Hybrid Triple-Level Cell for High-Density MRAM," in IEEE Transactions on Electron Devices, vol. 67, no. 4, pp. 1460-1465, April 2020.

[5] D. Morris, D. Bromberg, J. Zhu and L. Pileggi, "mLogic: Ultra-low voltage non-volatile logic circuits using STT-MTJ devices," DAC Design Automation Conference 2012, San Francisco, CA, 2012, pp. 486-491.

[6] S. Motaman, M. N. I. Khan and S. Ghosh, "Novel application of spintronics in computing, sensing, storage and cybersecurity," 2018 Design, Automation & Test in Europe Conference & Exhibition (DATE), Dresden, 2018, pp. 125-130

[7] Tehranipoor M , Wang C . Introduction to Hardware Security and Trust [M]. Springer New York, 2012.

[8] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and Implementation of PUF-Based "Unclonable"RFID ICs for Anti-Counterfeiting and Security Applications," in IEEE Int. Conf. on RFID, April 2008, pp. 58–64.

[9] G. E. Suh and S. Devadas, "Physical Unclonable Functions for Device Authentication and Secret Key Generation," in Design Automation Conf., June 2007, pp. 9–14.

[10] Z. Liang, M. G. Mankalale, J. Hu, Z. Zhao, J. Wang and S. S. Sapatnekar, "Performance Characterization and Majority Gate Design for MESO-Based Circuits," in IEEE Journal on Exploratory Solid-State Computational Devices and Circuits, vol. 4, no. 2, pp. 51-59, Dec. 2018.

[11] M. G. Mankalale, Z. Liang, Z. Zhao, C. H. Kim, J. Wang and S. S. Sapatnekar, "CoMET: Composite-Input Magnetoelectric- Based Logic Technology," in IEEE Journal on Exploratory Solid-State Computational Devices and Circuits, vol. 3, pp. 27-36, Dec. 2017.

[12] Bromberg D. Current-driven magnetic devices for non-volatile logic and memory [Ph.D. dissertation]. Carnegie Mellon University; 2014.

[13] M. Bhargava, C. Cakir, and K. Mai, "Reliability enhancement of bi-stable PUFs in 65 nm bulk CMOS,"in Proc. IEEE Symp. Hardw.-Oriented Secur. Trust, San Francisco, CA, USA, Jun. 2012, pp. 25–30.

[14] M. Bhargava and K. Mai, "A high reliability PUF using hot carrier injection based response reinforcement," in Proc. 15th Int. Workshop Crypotograph. Hardw. Embedded Syst., Santa Barbara, CA, USA, Aug. 2013, pp. 90–106.

[15] S. V . Kumar, C. H. Kim, and S. S. Sapatnekar, "Impact of NBTI on SRAM read stability and design for reliability," in Proc. IEEE 7th Int. Symp. Quality Electron. Design, Santa Clara, CA, USA, Mar. 2006, pp. 210–218.

[16] L. Zhang, X. Fong, C. Chang, Z. H. Kong and K. Roy, "Highly Reliable Spin-Transfer Torque Magnetic RAM-Based Physical Unclonable Function With Multi-Response-Bits Per Cell," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 8, pp. 1630-1642, Aug. 2015.

[17] Y . Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in Proc. EUROCRYPT, Interlaken, Switzerland, May 2004, pp. 523–540.

[18] C. Bösch, J. Guajardo, A. R. Sadeghi, J. Shokrollahi, and P . Tuyls "Efficient helper data key extractor on FPGAs," in Proc. 10th Int. Workshop Cryptograph. Hardw. Embedded Syst., Washington, DC, USA, Aug. 2008, pp. 181–197.

[19] Y . Zheng, M. S. Hashemian, and S. Bhunia, "RESP: A robust physical unclonable function retrofitted into embedded SRAM array," in Proc. 50th ACM/EDAC/IEEE Design Autom. Conf., Austin, TX, USA, Jun. 2013, pp. 1–9.

[20] Kursawe, A. Sadeghi, D. Schellekens, B. Skoric, and P . Tuyls,"Reconfigurable physical unclonable functions—Enabling

technology for tamper-resistant storage," in Proc. IEEE Int. Workshop Hardw. Oriented Secur. Trust, San Francisco, CA, USA, Jul. 2009, pp. 22–29.

[21] L. Zhang, Z. H. Kong, and C.-H. Chang, "PCKGen: A phase change memory based cryptographic key generator," in Proc. IEEE Int. Symp. Circuits Syst., Beijing, China, May 2013, pp. 1444–1447.

[22] A. Iyengar, K. Ramclam and S. Ghosh, "DWM-PUF: A low-overhead, memory-based security primitive," 2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), Arlington, VA, 2014, pp. 154-159.

[23] P. Simons, E. van der Sluis, and V . van der Leest, "Buskeeper PUFs, a promising alternative to D flip-flop PUFs," in Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust (HOST), Jun. 2012, pp. 7–12.

[24] M. T. Rahman, F. Rahman, D. Forte and M. Tehranipoor, "An Aging-Resistant RO-PUF for Reliable Key Generation," in IEEE Transactions on Emerging Topics in Computing, vol. 4, no. 3, pp. 335-348, July-Sept. 2016

[25] A. Vijayakumar and S. Kundu, "A novel modeling attack resistant PUF design based on non-linear voltage transfer characteristics," in Proc. Design, Automat. Test Eur. Conf. Exhibit. (DATE), Mar. 2015, pp. 653–658.

[26] E. Dubrova, O. Näslund, B. Degen, A. Gawell and Y. Yu, "CRC-PUF: A Machine Learning Attack Resistant Lightweight PUF Construction," 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS & PW), Stockholm, Sweden, 2019, pp. 264-271.

[27] J. Li, P . Ndai, A. Goel, S. Salahuddin, and K. Roy, "Design paradigm for robust spin-torque transfer magnetic RAM (STT MRAM) from circuit/architecture perspective," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 18, no. 12, pp. 1710–1723, Dec. 2010.

[28] X. Fong, S. H. Choday, and K. Roy, "Bit-cell level optimization for non-volatile memories using magnetic tunnel junctions and spin-transfer torque switching," IEEE Trans. Nanotechnol., vol. 11, no. 1, pp. 172–181, Jan. 2012.

[29] H. Maehara, K. Nishimura, Y. Nagamine, K. Tsunekawa, T. Seki, H. Kubota, A. Fukushima, K. Yakushiji, K. Ando, and S. Yuasa, "Tunnel Magnetoresistance above 170% and Resistance-Area Product of $1\Omega \cdot \mu m^2$ Attained by Insitu Annealing of Ultra-Thin MgO Tunnel Barrier," Applied Physics Express, vol.4, no.3, p. 033002, Mar.2011.

[30] E. I. Vatajelu, G. Di Natale, M. Indaco and P. Prinetto, "STT MRAM-based PUFs," 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE), Grenoble, 2015, pp. 872-875.

[31] N. N. Mojumder and K. Roy, "Proposal for switching current reduction using reference layer with tilted magnetic anisotropy in magnetic tunnel junctions for spin-transfer torque (STT) MRAM," IEEE Trans. Electron Devices, vol. 59, no. 11, pp. 3054–3060, Nov. 2012.

[32] R. Ma, S. Holst, X. Wen, A. Yan and H. Xu, "STAHL: A Novel Scan-Test-Aware Hardened Latch Design," 2019 IEEE European Test Symposium (ETS), Baden-Baden, Germany, 2019, pp. 1-6.

[33] M. Kumngern, "Absolute Value Circuit for Biological Signal Processing Applications," 2013 4th International Conference on Intelligent Systems, Modelling and Simulation, Bangkok, pp. 601-604, 2013.

[34] M. Elaakhdar, I. Adly and H. Ragai, "High Performance Time-Continuous Differential Sense Amplifier in Time Domain Sensing with 28 nm Technology for Automotive Applications," 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE), Southend, UK, 2018, pp. 262-265.

[35] K. Kim, "Future memory technology: Challenges and opportunities," in Proc. IEEE Int. Symp. VLSI Technol., Syst., Appl., Hsinchu, Taiwan, Apr. 2008, pp. 5–9.

[36] A. Pirovano et al., "Reliability study of phase-change nonvolatile memories," IEEE Trans. Device Mater. Rel., vol. 4, no. 3, pp. 422–427, Sep. 2004.

[37] 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.

[38] S. Ben Dodo, R. Bishnoi and M. B. Tahoori, "Secure STT-MRAM Bit-Cell Design Resilient to Differential Power Analysis Attacks," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 28, no. 1, pp. 263-272, Jan. 2020.

[39] M. Cortez, S. Hamdioui, V . van der Leest, R. Maes, and G.-J. Schrijen,"Adapting voltage ramp-up time for temperature noise reduction on memory-based PUFs," in Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust, Austin, TX, USA, Jun. 2013, pp. 35–40.

[40] L. Yu, X. Wang, F. Rahman and M. Tehranipoor, "Interconnect-Based PUF With Signature Uniqueness Enhancement," in IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 28, no. 2, pp. 339-352, Feb. 2020.

[41] Cadence Spectre. Accessed: Oct. 17,2020. [Online]. Available: https://www.cadence.com/en_US/home/tools/custom-ic-analog-rf-design/circuit-simulation/spectre-simulation-platform.html

[42] ITC99 Benchmark. Accessed: Oct. 17,2020. [Online]. Available: http://www.cerc.utexas.edu/itc99-benchmarks/bench.html

[43] Gaisler Benchmark. Accessed: Oct. 17, 2017. [Online]. Available: http://www.gaisler.com/index.php/downloads/leongrlib

[44] Opensparc Benchmark. Accessed: Oct. 17, 2017. [Online]. Available: http://www.oracle.com/technetwork/systems/opensparc

[45] ISCAS Benchmark. Accessed: Oct. 17, 2017. [Online]. Available: http://web.eecs.umich.edu/ jhayes/iscas.restore/benchmark.html

[46] Morris, Daniel H. "mLogic: Nonvolatile Pulsed-Current Logic and Memory Circuits," [J]. Dissertations & Theses - Gradworks, 2012.

[47] B. Wu, Y. Cheng, J. Yang, A. Todri-Sanial and W. Zhao, "Temperature Impact Analysis and Access Reliability Enhancement for 1T1MTJ STT-RAM," in IEEE Transactions on Reliability, vol. 65, no. 4, pp. 1755-1768, Dec. 2016.

[48] H. Zhao et al., "Spin-transfer torque switching above ambient temperature," IEEE Magn. Lett., vol. 3, 2012, Art. ID 3000304.

[49] STT-mCell Model Manual. Accessed: Oct. 2, 2019. [Online]. Available: https://nanohub.org/resources/21633/download.

[50] Z. Wang et al., "Current Mirror Array: A Novel Circuit Topology for Combining Physical Unclonable Function and Machine Learning," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 65, no. 4, pp. 1314-1326, April 2018.

[51] E. I. Vatajelu, G. Di Natale, M. Barbareschi, L. Torres, M. Indaco, and P. Prinetto, "STT-MRAM-based PUF architecture exploiting magnetic tunnel junction fabrication-induced variability," ACM J. Emerg. Technol. Comput. Syst., vol. 13, no. 1, 2016.

[52] Y . Su, J. Holleman, and B. P. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variations," IEEE J. Solid-State Circuits, vol. 43, no. 1, pp. 69–77, Jan. 2008.

[53] J. Li and M. Seok, "Ultra-compact and robust physically unclonable function based on voltage-compensated proportional-to-absolute-temperature voltage generators," IEEE J. Solid-State Circuits, vol. 51, no. 9, pp. 2192–2202, Sep. 2016.

[54] A. Alvarez, W. Zhao and M. Alioto, "14.3 15fJ/b static physically unclonable functions for secure chip identification with $<2\%$ native bit instability and 140× Inter/Intra PUF hamming distance separation in 65nm," 2015 IEEE International Solid-State Circuits Conference - (ISSCC) Digest of Technical Papers, San Francisco, CA, 2015, pp. 1-3.

[55] P. Simons, E. van der Sluis, and V . van der Leest, "Buskeeper PUFs, a promising alternative to D flip-flop PUFs," in Proc. IEEE Int. Symp. Hardw.-Oriented Secur. Trust (HOST), Jun. 2012, pp. 7–12.

[56] U. Rhrmair and J. Slter, "Puf modeling attacks: An introduction and overview," in 2014 Design, Automation Test in Europe Conference Exhibition (DATE), March 2014, pp. 1–6.

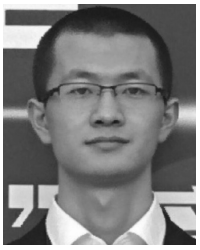
[57] J. Delvaux and I. Verbauwhede, "Fault injection modeling attacks on 65nm arbiter and ro sum pufs via environmental changes," IEEE Transactions on Circuits & Systems I Regular Papers, vol. 61, no. 6, pp. 1701–1713, 2014.

[58] G. Shi and J. Ru, "Research on classification of memory attack," in Proc. 2nd Workshop Adv. Res. Technol. Ind. Appl. (WARTIA). Paris, France: Atlantis Press, May 2016, pp. 392–397.

[59] J. Barrett, R. Colbeck, and A. Kent, "Memory attacks on device-independent quantum cryptography," Phys. Rev. Lett., vol. 110, no. 1, 2013.

[60] Xu, Xiaolin , and W. P. Burleson . "Hybrid side-channel/machine-learning attacks on PUFs: a new threat?" Design Automation and Test in Europe IEEE, 2014.

Kangwei Xu got his B.S. degree from Tiangong University, Tianjin, China, in 2019, where he is currently pursuing his master degree in CADET Lab., Beihang University, Beijing, China. His current research interest is high reliable physical unclonable function design with emergying spintronic technology. He got the first prize of 2017 Chinese Undergraduate Mathematical Contest in Modeling in Tianjin Division.



Dongrong Zhang received the B.S. degree from Beihang University, Beijing, China, in 2016, where he is currently pursuing the Ph.D. degree. He is currently with Beihang University, Beijing. His current research interests include on-chip monitoring, physical design, and on-chip dynamic adaptation methodologies. Mr. Zhang was a recipient of second and third places of the 25th Feng Ru Cup Competition of Academic and Technological by Inventing "ID Certification System Basing on Personal Movement Identification" and "Color Laser Projection System." He was honorably mentioned by 2015 International Mathematical Contest in Modeling.

Patrick Girard receiver the M.S. degree in electrical engineering and the Ph.D. degree in microelectronics from the University of Montpellier, Montpellier, France, in 1988 and 1992, respectively.

He is currently a Research Director with the French National Center for Scientific Research (CNRS), and a Chair with the Microelectronics Department, Laboratoire d'Informatique de Robotique et de Microelectronique de Montpellier, Montpellier. His current research interests include all aspects of digital testing and memory testing, reliability and fault tolerance, and test of 3-D integrated circuits. Dr. Girard holds the Technical Activities Chair of the Test Technology Technical Council (TTTC) of the IEEE Computer Society. He has served as a Vice-Chair of the European TTTC of the IEEE Computer Society, and also on numerous conference committees including ACM/IEEE Design Automation Conference (DAC), ACM/IEEE Design Automation and Test in Europe (DATE), IEEE International Test Conference (ITC). He is the founder and Editor-in-Chief of the *ASP Journal of Low Power Electronics* and an Associate Editor of the IEEE TRANSACITONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEM and the IEEE TRANSACTIONS ON COMPUTER-AIDED DESIGN (CAD) OF INTEGRATED CIRCUITS AND SYSTEMS.

Qiang Ren received the B.S. degree from Beihang University, Beijing, China, in 2008, the M.S. degree from the Institute of Acoustics, Chinese Academy of Sciences, Beijing, China, in 2011, and the Ph.D. degree from Duke University, Durham, NC, USA, in 2015, all in electrical engineering.

From 2016 to 2017, he was a Postdoctoral Researcher with the Computational Electromagnetics and Antennas Research Laboratory (CEARL), Pennsylvania State University, University Park, PA, USA. In September 2017, he joined the School of Electronics and Information Engineering, Beihang University, as an "Excellent Hundred" Associate Professor. His current research interests include numerical methods for multiscale and multiphysics modeling, inverse scattering, and parallel computing.

Yuanqing Cheng (S'11, M'13, SM'20) received his Ph.D. degree from the Key Laboratory of Computer System and Architecture, Institute of Computing Technology, Chinese Academy of Sciences, Beijing, China. After spending one year post-doc study at LIRMM, CNRS, France, he joined Beihang University, China as an assistant professor. His research interests include VLSI design for 3D integrated circuits considering thermal and defect issues, as well as spintronics computing system architecture design. He is an IEEE Senior member and ACM member.