STT-MRAM-Based Reliable Weak PUF

Yupeng Hu, *Senior Member, IEEE*, Linjun Wu, Zhuojun Chen, *Member, IEEE*, Yun Huang, Xiaolin Xu, *Member, IEEE*, Keqin Li, *Fellow, IEEE*, and Jiliang Zhang, *Senior Member, IEEE*

Abstract—In recent years, micro-nano device characteristics like ferroelectrics and resistive switching are being used to build important security primitives such as Physical Unclonable Function (PUF). The micro-nano device-based hardware security primitives, although with higher security, energy efficiency, and integration density, suffer from serious reliability issues caused by process scaling. To mitigate this issue, this paper introduces a reconfigurable weak PUF based on spin-transfer torque magnetoresistive random-access memory (STT-MRAM), which adopts the crossing switches implemented with simple demultiplexes (DEMUXs) to improve the flexibility and reliability. Moreover, two algorithms, `neighboring bit lines` and `top-`n, are proposed to enlarge the gap between two parallel reading currents, thus further enhancing the reliability of PUF responses. Experimental results demonstrate that the proposed PUF scheme achieves good uniqueness (50.64 percent), uniformity (50.02 percent), and bit-aliasing ($\approx$49.80%). Particularly, the proposed method significantly improves the PUF reliability, achieving low bit error rate (BER $\leq$ 2.13%) within the range of -20°C to 90°C.

Index Terms—Physical unclonable function, STT-MRAM, reliability, flexibility

1 Introduction

The development of modern semiconductor industry has been dependent on the increasingly globalized supply chain, in which the manufacturing of most semiconductor devices is outsourced to the off-shore, untrustworthy "one-stop-shop" foundries. Consequently, the security of the hardware devices is becoming a dominant concern of the modern IC industry [1]. For example, the market research firm IHS iSuppli revealed that the top five counterfeit electronics incurred around 169 billion revenue loss to the global semiconductor business [2]. More detailed, the outsourced electronic manufacturing brings various issues like overproduction, in which an untrusted foundry may fabricate more chips than contracted and sell them at a lower price. These issues are threatening the security and reliability of many critical infrastructures, such as the national defense system, as well as commercial electronics like medical devices [3].

Physical Unclonable Function (PUF) is a promising hardware security primitive that can effectively address these aforementioned security issues [31]. PUFs have attracted a plethora of attention in both academia and industry [4]. While the fabrication of conventional CMOS-based devices is approaching the material and physical limits, various emerging micro-nano devices [6] are being explored for higher performance. Given the significant potential of micro-nano devices, they have also been used to build hardware security primitives, like PUF [5]. Among these existing solutions, the PUFs based on spin-transfer torque magnetoresistive random access memory (STT-MRAM) are gaining a lot of attention with promising energy efficiency and integration density [7]. However, due to the scaling of the manufacturing process dimension, the STT-MRAM PUFs also suffer from severe reliability issues. For example, the storage states of the scaled memory cells are more sensitive to environmental disturbances, such as temperature, magnetic field noise, and supply voltage fluctuation, leading to significant bit error rates (BERs). Many methods have been proposed to mitigate these reliability issues, such as fuzzy extractors [8] or error correction codes (ECC) [9] (a.k.a. helper data [29]). Additionally, many reliability enhancing technologies for these emerging PUFs are also proposed at the cost of higher structural complexity and more strict control conditions [10], [11], [12].

The sensitivity of the sense amplifier (SA) [32] is also an essential factor affecting device reliability. In the previous works, the response bits are all extracted from the read current gap between a single magnetic tunneling junction (MTJ) cell and the reference current. Therefore, the current gap input to SA is small. It requires SA to have a higher resolution, which increases the difficulty of circuit design. Furthermore, there are two methods to provide reference current. The simple one is to use a pinned MTJ whose electrical resistance is close to all memory cells' average value. Another option is to compose a reference circuit with plenty of reference cells whose MTJ electrical characteristics are identical to the memory cells. The reference current obtains from the reference circuit is due to more reliability than from a single device. But the reference circuit increases the complexity and occupies a larger area.

- *Yupeng Hu, Linjun Wu, Yun Huang, and Jiliang Zhang are with the College of Computer Science and Electronic Engineering, Hunan University, Changsha 410012, China. E-mail: {yphu, wulinjun777, huangyun1996, zhangjiliang}@hnu.edu.cn.*
- *Zhuojun Chen is with the School of Physics & Electronic, Hunan University, Changsha 410012, China. E-mail: zjchen@hnu.edu.cn.*
- *Xiaolin Xu is with the Department of Electrical and Computer Engineering, Northeastern University, Boston, MA 02115 USA. E-mail: x.xu@northeastern.edu.*
- *Keqin Li is with the Department of Computer Science, State University of New York, New Paltz, NY 12561 USA. E-mail: lik@newpaltz.edu.*

*Manuscript received 3 Nov. 2020; revised 9 Apr. 2021; accepted 4 July 2021. Date of publication 13 July 2021; date of current version 9 June 2022. (Corresponding author: Jiliang Zhang.)
Recommended for acceptance by G. Di Natale.
Digital Object Identifier no. 10.1109/TC.2021.3095657*

To solve the existing problems associated with these STT-MRAM-based PUFs, we introduce a novel STT-MRAM-based reconfigurable weak PUF to improve reliability. The main contributions of this work are summarized as follows:

1) We propose a flexible, reconfigurable weak PUF structure based on STT-MRAM. It adopts the parallel currents of MTJ cells to generate response bits. The parallel current of a bit line is several times larger than the current of a single MTJ cell, and the large current value can resist signal noise fluctuations more effectively. Specifically, the structure inserts a novel crossing structure composed of multiple Demutiplexs (DEMUXs) into the conventional STT-MRAM. By adjusting the control signals of these DEMUXs in the proposed crossing structure, each MTJ cell could flexibly connect to different bit lines to construct optimized MTJs parallel structures, where any two parallel bit lines consisting of multiple MTJ cells can produce a 1-bit response. This structure can solve the drift issue caused by temperature or supply voltage since it does not require any reference cell/circuit.
2) Two algorithms, `neighboring bit lines` and `top-`n algorithms, are introduced to maximize the difference between the read currents of two bit lines for the proposed PUF structure, thus improving the reliability of the PUF responses. Based on the proposed parallel structure, these two algorithms accumulate multiple MTJ cell pairs' current gaps. Therefore, the current gap input to the SA is enlarged several times compared with the previous work. This method considers the enhancement of response reliability from the SA resolution, which is rarely explored in previous works.
3) We perform extensive experiments with Hspice simulation, which adopts the commonly used MTJ model [13]. The experimental results demonstrate that our proposed reconfigurable PUF can achieve $\leq 2.13\%$ bit error rate (BER), 50.64 percent uniqueness, $\approx 49.80\%$ bit-aliasing, and 50.02 percent uniformity.

The remainder of this paper is organized as follows. Background and related works are reviewed in Section 2. Section 3 introduces the preliminaries of PUFs. Section 4 presents the proposed reconfigurable and reliable weak PUF based on STT-MRAM. Section 5 presents comprehensive performance evaluations for the proposed STT-MRAM-based PUF designs and algorithms. Finally, Section 6 concludes this paper and points out future directions.

2 Related Work

Various reliability enhancing technologies are proposed to eliminate the bit errors of PUF responses. The authors of [8] defined a fuzzy extractor and store a string as the helper data to reproduce the correct responses. The temporal majority voting method collects the results of multiple PUFs and chooses the bits that appear most frequently as the final output [30], [33]. The dark-bit masking scheme detects and marks the location of the unstable PUF bits and then discards these bits further in the application [30]. Other dominant approaches are more focused on the bit errors caused by the aging effect of transistors [30]. Burn-in reinforcement such as biased-temperature instability (BTI) [32] and hot-carrier injection (HCI) [31] are all used to enhance the stability of the SRAM PUF cells. The breakdown position BD-PUFs [30] utilize the position of oxide breakdown in CMOS to improve the reliability of responses.

This section reviews the state-of-the-art reliability optimizing technologies for emerging PUFs, which could be classified into structural optimization and read-write optimization.

Structural Optimization. Structural optimization technologies employ extra circuit structures to weaken the current fluctuations caused by environmental disturbances. The extra circuits are at the cost of higher design complexity and hardware overhead. The Xbar PUF [14] employs XORing and column shuffling techniques to resist the environmental disturbances with an extra elaborating structure. Even for a small-scale CRPs set, the Xbar PUF consumes a large amount of energy to generate a single response bit. In [7], [15], the active cells and reference cells are manufactured in the same way, therefore the drift is consistent between the read currents and reference currents under the same conditions. The stability of the reference current of these solutions is affected by the size of the reference array. The authors of [10] adopted multiplexers to enlarge the time gap between the delay paths, thus enhancing the reliability of PUFs. Nanoscale ReRAM devices work as the main delay cells to improve the reliability of classic CMOS time delay PUF (TD-PUF) [34]. MUXs divert the racing pulse based on the input select bit to expand the difference between the delay paths. However, the main part of the TD-PUF is still using CMOS technology, so it has little effect on reducing power consumption.

Read/Write Optimization. The read-write optimization technologies strengthen the robustness of responses based on strict control conditions or complicated peripheral circuits. The masking technology outputs the response bits generated by the reliable cells while neglecting the unreliable cells [16]. In [16], the authors employed an MRAM to extract the raw PUF responses and an additional register to store the information on the location of unreliable cells. The authors of [12] utilized optimized forming conditions to set part of the cells into the certain low resistance state while other cells remain at the initial high resistance state. In [17] and [18], the output bits are written back to the memory cells to enhance the robustness of response regeneration. The authors of [11] sumed up the read-out currents of multiple RRAM cells to generate one response bit, which can statistically minimize the early-lifetime failure incurred by RRAM retention degradation under high temperature.

Different from previous work, we consider the enhancement of response reliability from the SA resolution based on the proposed parallel structure and the reconfigurable algorithms, which ensure the current gap input to the SA is enlarged several times compared with the existing work. Therefore, we can resolve the drift issue caused by temperature or supply voltage without any reference cell/circuit.

3 Preliminaries

3.1 Physical Unclonable Function

A physical unclonable function is a special hardware primitive characterized by its unique input (challenge) and output (response) behavior. Each PUF instance owns a unique mapping relationship between challenges and responses. This mapping relationship depicts the internal complex physical characteristics generated during the manufacturing process. Below are three commonly used metrics to evaluate the performance of PUFs [7], [19].

Uniqueness. When a set of challenges are applied to different PUF instances, their responses are expected to be different. Therefore, uniqueness is used as the parameter that indicates the difference between PUF instances, and this parameter is defined with Eq. (1)

$$HD(R_i, R_j) = \sum_{k=1}^{K} R_i[k] \oplus R_j[k], \tag{1}$$

where R_i and R_j denote the corresponding K-bits responses generated by PUF_i and PUF_j under the same challenges. Statistically, the ideal uniqueness is 50 percent for a group of PUF instances, which means half of the bits between R_i and R_j are expected to be different. Specifically, the normalized inter Hamming distance in Eq. (2) is commonly used to measure the uniqueness of N PUFs with K-bits responses

$$HD_{inter} = \frac{2}{N(N-1)} \sum_{i=1}^{K-1} \sum_{j=i+1}^{K} \frac{HD(R_i, R_j)}{K} \times 100\%. \tag{2}$$

Uniformity. Uniformity represents the statistical distribution of '1' and '0' in the PUF response. For example, the uniformity of a K-bit response r can be defined as follows:

$$Uni = \frac{1}{K} \sum_{k=1}^{K} r_k \times 100\%, \tag{3}$$

where r_k represents the kth bit of the response r. The ideal uniformity of a PUF is 50 percent, which indicates that 50 percent of the bits are data '1', and the rest is data '0'.

Bit-Aliasing. If a bit of response is '0' or '1' with the same probability, the bit is unbiased. Bit-aliasing is defined as

$$BA(k) = \frac{1}{N} \sum_{i=1}^{N} R_i(k), \tag{4}$$

where k is the kth response bit, N is the number of PUFs and $R_i k$ is the kth response bit of the ith PUF.

Reliability. PUF responses are expected to remain the same under the same challenge even under different environmental conditions [28]. In this paper, the reliability is measured by Rel, which is calculated as follows:

$$Rel = 1 - BER = 1 - \frac{1}{P \times K} \sum_{p=1}^{P} HD(r, r_p) \times 100\%. \tag{5}$$

A PUF obtains P responses from the same challenge over P runs. K is the length of each response, and $P \times K$ indicates the total response bits generated after P runs. r is the response generated under the standard condition, which works as a reference value. r_p is the pth response under different test conditions. Ideally, the BER of a PUF is expected to be zero, and reliability is 100 percent. Their reliability is usually affected by different environmental conditions, since PUFs leverage microscopic process variations.

3.2 STT-MRAM PUF

In the STT-MRAM, the data is stored in the magnetic tunneling junctions. An MTJ generally has a sandwich structure that consists of two ferromagnetic layers separated by a tunnel barrier. The lower layer is the pinned layer with a fixed magnetization direction. The upper layer has a freely rotating magnetic direction, namely the free layer. The magnetization direction of the free layer can be programmed by providing a sufficiently large spin-polarized current. The relative magnetization direction of the two ferromagnetic layers influences the resistance of an MTJ. When the relative direction of the two ferromagnetic layers is parallel, the MTJ device exhibits a low resistance state (LRS). Otherwise, the MTJ exhibits a high resistance state (HRS).

STT-MRAM PUFs have already been explored and demonstrated with higher security, energy efficiency, and integration density [35]. However, low reliability limits the applicability of the PUFs. In this work, we focus on improving the reliability of PUFs, which are based on typical STT-MRAM structure where each memory cell has an MTJ connected to a word line selecting transistor (1T1M) in series. For an $m \times n$ STT-MRAM PUF, the address of each memory cell $M_{i,j} (i \in [1, m], j \in [1, n])$ is the challenge input coded by the m word lines (WLs) and the n bit lines (BLs). Applying a small voltage to the corresponding bit line, the current $I_{i,j}$ flowing through the cell $M_{i,j}$ is proportional to its electrical resistance. The PUF response is generated by comparing the current $I_{i,j}$ with the reference current I_{ref} via a comparator. The original input signal is amplified by a sense amplifier as the output. For example, if $I_{i,j} > I_{ref}$, the response bit is set to '1'; otherwise, it is '0'.

3.3 Reliability Challenges for STT-MRAM PUF

Despite its security and efficiency, the STT-MRAM PUF should also handle the reliability issue in implementation. An MTJ can be considered as a voltage-controlled variable resistance. The parallel tunnel resistance R_P in the MTJ of the CoFeB/MgO/CoFeB structure [20], [21] is shown as follows:

$$R_P = \frac{t_{ox}}{F \times \varphi^{-\frac{1}{2}} \times Area} \times \exp(1.025 \times t_{ox} \times \varphi^{-\frac{1}{2}}), \tag{6}$$

where t_{ox} represents the free layer thickness, φ stands for the insulation barrier height, F denotes the multiplication factor (depending on the material composition of the magnetic tunnel junction), and $Area$ stands for the junction area of an MTJ. The anti-parallel state resistance R_{AP} is $R_{AP} = R_p \times (1 + TMR)$ [22]. According to the Slonzewski model [23], the tunnel magnetoresistance (TMR) can be modeled as follows:

$$TMR = \frac{TMR(0)}{1 + V_{bias}^2 / V_h^2}, \tag{7}$$

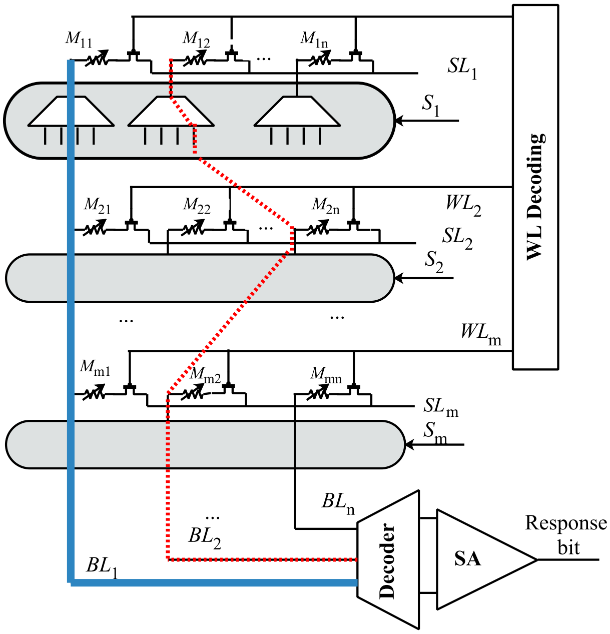


Fig. 1. The proposed STT-MRAM-based $m \times n$ PUF.

where TMR(0) denotes the TMR at 0 bias, V_{bias} is the bias on the MTJ, and the V_h represents the bias when the $TMR = 0.5 \times TMR(0)$. The value of the TMR is a key parameter for the reading operation of the memory circuits. A larger TMR can achieve higher reading accuracy, especially for the memory chips without error correction circuits. To avoid interfering with the data stored in the MTJ, a small bias is applied to the BL, resulting in a small read current. However, such a small voltage/current amplitude is not high enough to resist the environmental disturbance.

The first challenge for the STT-MRAM PUF is the random fluctuation of temperature and voltage/current that degrades the reliability. Additionally, the sensitivity of the comparator also affects the reliability of the PUF instance. To solve these problems, we need to enlarge the gap between the active and reference currents as much as possible, for example, making it to be larger than the comparator resolution.

4 STT-MRAM-Based Reconfigurable and Reliable Weak PUF

4.1 Structure Overview

We present the structure overview of the proposed STT-MRAM-based weak PUF in Fig. 1. The main contribution of the proposed STT-MRAM-based $m \times n$ weak PUF structure is inserting m dedicated n bits crossing switches S_i into the basic 1T1M STT-MRAM topology, to make these MTJ cells (denoted by the addresses $M_{i,j}$, $i \in [1, m]$, $j \in [1, n]$) reconfigurable along with the m WLs and n BLs. Specifically, the proposed PUF can generate n bits responses and maintain the regular connections between the WLs and the source lines (SLs). Instead of connecting to a fixed bit line, each MTJ cell can connect to any bit line through the well-designed crossing switches composed of the widely available DEMUXs. For instance, in Fig. 1, the cells M_{12}, M_{2n}, M_{m2} are connected to the same bit line BL_2 marked by the dash red line, while the cells M_{11}, M_{21}, M_{m1} remain connected to the original bit line BL_1 marked by the bold blue line.

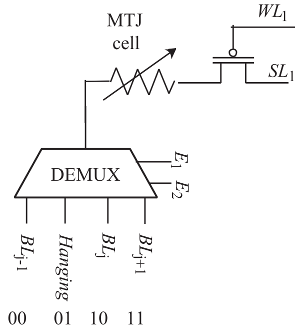


Fig. 2. Crossing switch implementation.

We implement the crossing switch S_i with n DEMUXs, as shown in Fig. 2. There are up to four connection options for each MTJ cell: default connection to bit line BL_j, the front bit line BL_{j-1}, the next bit line BL_{j+1}, and the hanging. It is worth mentioning that in the proposed scheme, the next bit line of BL_n is BL_1. The DEMUX's signal control state E_1E_2 of the cell M_{ij} is $E(M_{ij}) \in E = \{00, 01, 10, 11\}$, which indicates four possible outputs, i.e., $BL_{j-1}, Hanging, BL_j, BL_{j+1}$. The control signal distribution is determined by the designer during the manufacturing process according to the position of each line in the DEMUX.

Due to the flexible configuration of the 1:4 DEMUX, each MTJ cell can connect to different neighboring BLs to construct an optimized parallel combination, where any two bit lines can produce one response bit through current comparison. Particularly, we propose corresponding reconfigurable algorithms that search the appropriate MTJ combinations in parallel to achieve the intended current gap. If the SLs are grounded and the WLs are applied positive bias, the MTJ cells connected in the same bit line form a parallel sub-circuit, as shown in Fig. 3. Therefore, not only the parallel current obtained in a bit line is larger than the current from a single MTJ cell, but also the optimized the current gap between the corresponding two bit lines will be maximized, thus making the PUF reliable.

4.2 CRPs Generation Algorithms

In this section, we introduce two CRPs generation algorithms for the proposed reconfigurable PUF, i.e., `neighboring bit lines` and `top-`n , which can output optimized CRPs to improve the reliability of the proposed PUF. In the initial writing operation, these two algorithms set all cells in HRS, which can obtain a more random distribution of MTJ resistance to guarantee the uniqueness, unclonability, and unpredictability. Notably, the algorithms employ two essential functions to perform the optimized CRPs read/generate operation as follows.

Challenge$(A_j, A_{j'})$. $A_j, A_{j'}$ denote the addresses of the MTJ cells connected to bit lines BL_j and $BL_{j'}$ in parallel via DEMUX, respectively. The two sets generate response bits between BL_j and $BL_{j'}$, then they are returned as a challenge C_j in this function, where $i \in [1, m], j, j' \in [1, n]$.

Response$(I_j, I_{j'})$. This function compares the current of two bit lines (BL_j and $BL_{j'}$) and returns '1' as one bit response R_j, if $I_j > I_{j'}$; otherwise it returns '0', where I_j

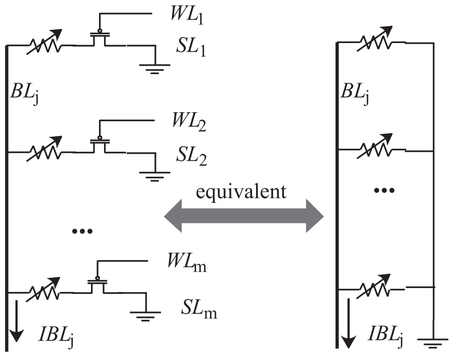


Fig. 3. Equivalent parallel circuit.

and $I_{j'}$ are the sum of the read current of all the parallel MTJ cells connected to the jth and j'th bit line.

Algorithm 1. Neighboring Bit Lines Reconfigurable Algorithm

```
Require:
    The set of all MTJ cells addresses, $A = \{M_{i,j}\}$;
    The set of the read current of all cells, $I = \{I_{i,j}\}$;
    The given current gap threshold, $T$;
Ensure:
    Challenge-Response Pair CRP;
 1: for $j = 1$ to $n$ do
 2:     if $|I_j - I_{j+1}| \geq T$ then
 3:         $R_j \leftarrow Response(I_j, I_{j+1})$;
 4:         $C_j \leftarrow Challenge(A_j, A_{j+1})$ ;
 5:     else
 6:         for $i = 1$ to $m - 1$ do
 7:             if $((I_{m,j} > I_{m,j+1}) \oplus (I_{i,j} > I_{i,j+1}) == 1$ then
 8:                 $E(M_{i,j}) \leftarrow 11, E(M_{i,j+1}) \leftarrow 10$;
 9:             end if
10:         end for
11:         $R_j \leftarrow Response(I_j, I_{j+1})$;
12:         $C_j \leftarrow Challenge(A_j, A_{j+1})$;
13:     end if
14: end for
15: $CRP \leftarrow \{\{C_1, R_1\}, \{C_2, R_2\}, \ldots, R_n\}\}$;
16: return CRP;
```

- *The Neighboring Bit Lines Reconfigurable Algorithm*

The proposed neighboring bit line algorithm is devoted to search for proper MTJ cells that are further reconnected along two neighboring bit lines, e.g., BL_j and BL_{j+1}. Thus, the current gap between the two neighboring bit lines $|I_j - I_{j+1}|$ is larger than the given current gap threshold T. It is worth noting that when it runs to the last bit line BL_n, the next bit line will be BL_1. The searching criteria for the intended MTJ cells is defined as follows:

$$\underset{cells \in A_j or A_{j+1}}{\arg} \{|I_j - I_{j+1}| \geq T\}, j \in [1, n]. \tag{8}$$

As illustrated in Algorithm 1, if the original current gap between the two neighboring bit lines is larger than T, then the algorithm will directly extract the CRPs. Otherwise, the key iterative searching and reconfiguration process (shown in lines 6-10) are conducted. Particularly, if there are inconsistency of comparisons as shown in line 7, then their bit line connections for cells $M_{i,j}$ and $M_{i,j+1}$ will be exchanged (code line 8) by resetting their signal control states $E(M_{i,j}) \leftarrow 11$ and $E(M_{i,j+1}) \leftarrow 10$ (see Fig. 2 as an example). For instance, when $i, j = 1$, if original $I_{m,1} > I_{m,2}$ and $I_{1,1} < I_{1,2}$, the code line 8 exchanges the bit line connections for $M_{1,1}$ and $M_{1,2}$. As a result, $M_{m,1}$ and $M_{1,2}$ connect to BL_1 while $M_{m,2}$ and $M_{1,1}$ connect to BL_2. Otherwise, if original $I_{m,1} > I_{m,2}$ and $I_{1,1} > I_{1,2}$, $M_{1,1}$ and $M_{1,2}$ keep in original connection. The operation in code line 8 can eliminate all inconsistencies and reconfigure the bit line connections to keep the current gap between two neighboring bit lines as large as possible. The optimized CRP is returned as the final result (code line 16).

The computing complexity of Algorithm 1 is $O(m \cdot n)$, while it depends on the accurate threshold T that is not easy to obtain concerning the different characteristics of various PUFs. We introduce another algorithm, top-n reconfigurable algorithm, that is more adaptive and practical.

Algorithm 2. Top-n Reconfigurable Algorithm

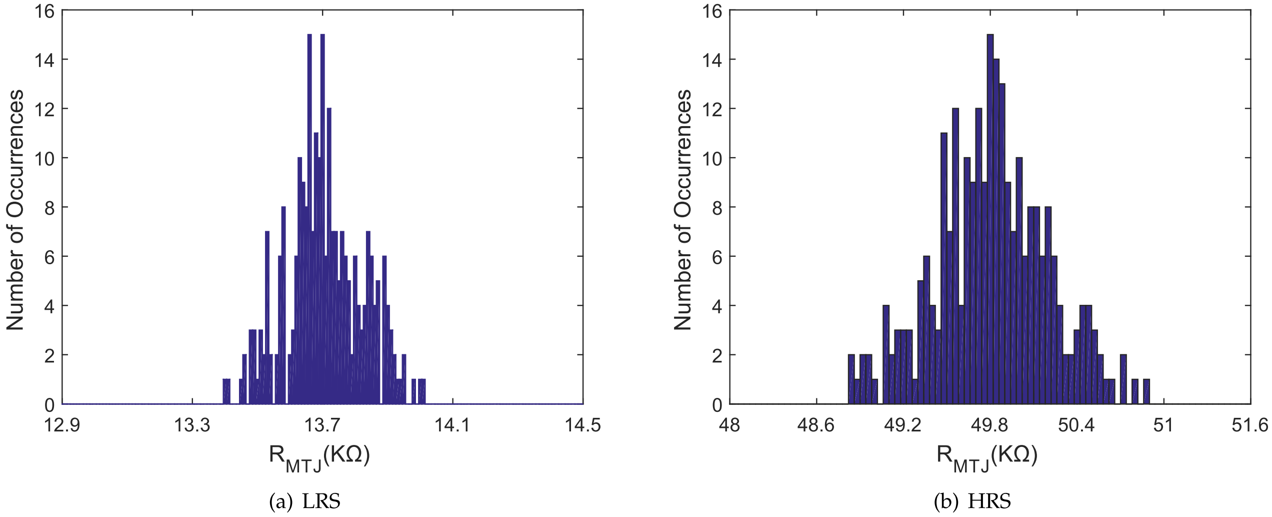
```
Require:
    The set of all MTJ cells addresses, $A = \{M_{i,j}\}$;
    The set of the read current of all cells, $I = \{I_{i,j}\}$;
    The number of response bits, $n$;
Ensure:
    Challenge-Response Pair CRP;
 1: $A_j \leftarrow \emptyset, j \in [1, n]; \Delta \leftarrow \emptyset; k \leftarrow 1$;
 2: for $i = 1$ to $m$ do
 3:     $CellSort(WL_i)$;
 4:     for $j = 1$ to $n$ do
 5:         $A_j \leftarrow A_j \cup M_{i,j}$;
 6:     end for
 7: end for
 8: for $j = 1$ to $n - 1$ do
 9:     for $j' = j + 1$ to $n$ do
10:         $\Delta_{j,j'} \leftarrow |I_j - I_{j'}|$;
11:         $\Delta \leftarrow \Delta \cup \Delta_{j,j'}$;
12:     end for
13: end for
14: for each $\Delta_{j,j'}$ in $Top_n(\Delta)$ do
15:     $C_k \leftarrow Challenge(A_j, A_{j'})$;
16:     $k \leftarrow k + 1$;
17: end for
18: $CRP \leftarrow \{\{C_1, R_1\}, \{C_2, R_2\}, \ldots, \{C_n, R_n\}\}$;
19: return CRP;
```

- *The Top-n Reconfigurable Algorithm*

The top-n reconfigurable algorithm searches for n pairs bit lines, which can obtain the largest n current gaps among all bit lines in the set P. The searching problem can be defined as follows:

$$\underset{A_k}{\arg\max} \{I_p - I_q\}, p, q \in [1, |P|], k \in [1, n], \tag{9}$$

where $A_k (k \in [1, n])$ indicates there are top n pairs of intended bit lines. However, the computing complexity of this searching is $|P| = O(n^m)$, which is unaffordable for a lightweight PUF application. To mitigate this issue, we further adopt a heuristic strategy in Algorithm 2 that can rapidly find out the n pairs intended bit lines, thus extracting



(a) LRS (b) HRS

Fig. 4. The resistance distribution under LRS and HRS.

the largest n current gaps. As shown in Algorithm 2, a cell can never be used in two bit lines simultaneously, thus for each word line $WL_i (i \in [1, m])$, we employ the function $CellCurrentSort(WL_i)$ to sort the n cells according to their current values, in descending order (code line 3). Consequently, the intended top n pairs bit lines can be heuristically achieved following code lines 4-5.

After calculating all the current gaps between any two selected bit lines (code lines 8-13), Algorithm 2 records the n largest gaps via function $Top_n(\Delta)$ and adopts the combination of corresponding cells for two bit lines to generate CRPs in code lines 14-17. The computing complexity of Algorithm 2 depends on the specific sorting algorithm with complexity $f(n) > n$ and thus is $O(f(n) \cdot m + n^2)$. The two CRPs generation algorithms only need to run once during the initialization phase and almost have no negative effects on the other functions of PUF.

4.3 Case Study

We illustrate the efficiency of the proposed algorithms with an example of a 4×4 STT-MRAM-based PUF, i.e., $A = \{MTJ_{i,j}\} (i, j \in [1, 4])$, which can generate 4-bits response. The set of the read current of each cell in the 4 bit lines is $I = \{\{8, 7, 8, 9\}, \{7, 6, 9, 8\}, \{9, 7, 7, 6\}, \{6, 9, 5, 8\}\} \mu A$, with

$$I_1 = 8 + 7 + 8 + 9 = 32,$$
$$I_2 = 7 + 6 + 9 + 8 = 30,$$
$$I_3 = 9 + 7 + 7 + 6 = 29,$$
$$I_4 = 6 + 9 + 5 + 8 = 28.$$

Based on the random location distribution of all MTJ cells, we assume that the original challenge combinations are $\{\{A_1, A_2\}, \{A_2, A_3\}, \{A_3, A_4\}, \{A_4, A_1\}\}$ and the responses are $\{1110\}$. The original $Challenge\{A_2, A_3\} = \{\{M_{12}, M_{22}, M_{32}, M_{42}\}, \{M_{13}, M_{23}, M_{33}, M_{43}\}\}$ obtains a current gap $|I_2 - I_3| = 1$. After performing Algorithm 1, the reconfigured challenges will become $Challenge\{A_2, A_3\} = \{\{M_{13}, M_{23}, M_{32}, M_{42}\}, \{M_{12}, M_{22}, M_{33}, M_{43}\}\}$, and the currents set of all cells in BL_2 and BL_3 is $\{\{9, 7, 9, 8\}, \{7, 6, 7, 6\}\}$, which can generate a larger current gap. As a result, the output response bits become $\{1100\}$.

If we perform the Algorithm 2, the reconfigured set of the MTJ cells read currents in the 4 bit lines becomes $I = \{\{9, 9, 9, 9\}, \{8, 7, 8, 8\}, \{7, 7, 7, 8\}, \{6, 6, 5, 6\}\}$, which can obtain a maximum current gap 13 and the response bits $\{1110\}$. In this way, the reconfigurable algorithms significantly improve the reliability of the proposed PUF, by enlarging the current gap between two bit lines. Besides, the reconfigurable PUF can be applied to some security protocols (e.g., multi-party communication), where many parties require to share the same key [19].

5 Performance Evaluations

According to the metrics mentioned in Section 3.2, this section presents the performance evaluations of the proposed PUF with HSpice simulation. In our experiment, we adopt the state-of-the-art MTJ simulation model [13], specifically, we set the free layer thickness as $l_z = 1.48nm$, the oxide insulating layer thickness as $t_{ox} = 0.85nm$, the saturation magnetization as $Ms_0 = 1020$, the polarization factor as $P_0 = 0.69$, and the magnetic damping factor as $\alpha = 0.006$. We choose three key parameters to introduce the process variations, the width of the free layer is $l_x = 65nm$ with relative deviation 5 percent; the length of the free layer is set as $l_y = 65nm$ with relative deviation 5 percent; and the resistance-area product $RA = 5/nm^2$ at absolute zero temperature with relative deviation 3 percent. All cells are set to HRS at $0.9V$ as the default, and the read voltage is $0.2V$.

5.1 Monte Carlo Analysis

If the statistical distribution of component parameters in a circuit is known, the Monte Carlo method can randomly and repeatedly extract the component parameters according to the distribution law [24]. Furthermore, it can randomly extract the circuit parameter for computer simulation, to reveal the statistical distribution of the circuit characteristics. This work makes use of the Monte Carlo function in HSpice to analyze the distribution of MTJs resistance. Figs. 4a and 4b provide 100 samples under LRS and HRS via Monte Carlo simulations, based on Eqs. (6) and (7). These simulation results demonstrate an obvious resistance difference between the two resistance states. As mentioned

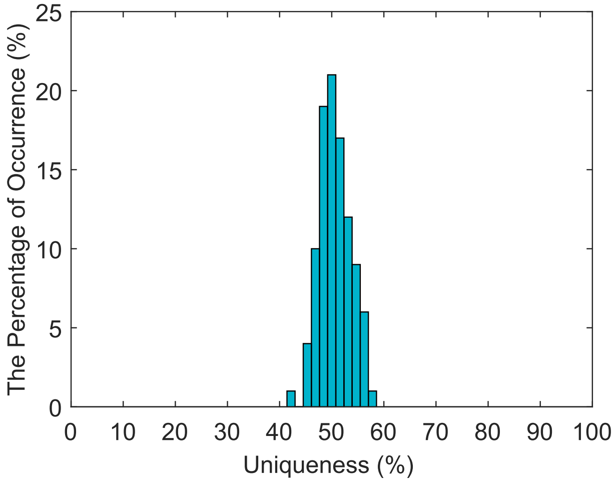


Fig. 5. Uniqueness.

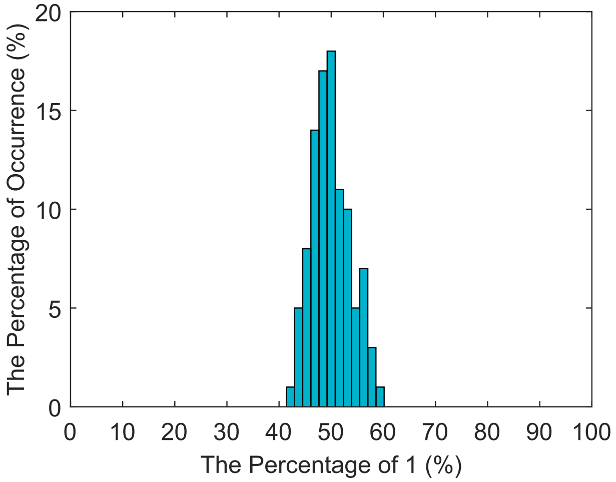


Fig. 6. Uniformity.

in Section 4.2, the samples under HRS have more random distribution than the under LRS, which ensures the unclonability of the proposed PUF scheme.

5.2 Uniqueness

Eq. (2) defines the uniqueness between different PUFs by the normalized inter Hamming distance. We perform the uniqueness evaluation of the 15 proposed 4-cells parallel reconfigurable PUFs, with the neighboring bit lines reconfigurable algorithm applied at $20^\circ C$. Each PUF generates a 64-bits response. In Eq. (2), $N = 15$, $K = 64$. Fig. 5 shows the uniqueness of approximately 100 pairs 64-bits responses generated by the 15 PUFs. Although the number of occurrences of 50 percent is 23, most of the uniqueness values approximate the optimal value 50 percent with the mean uniqueness value as 50.64 percent. And they are normally distributed around 50 percent, the worst case is about $50 \pm 8\%$.

5.3 Uniformity

Fig. 6 depicts the proportion of data ‘1’ in the 100 responses of 64-bits. The 100 responses are generated by the proposed 4 cells parallel reconfigurable PUF with the neighboring bit lines reconfigurable algorithm at $20^\circ C$. The average percentage of the occurrence of ‘1’ is 50.02 percent, which approximately equals to the ideal value. In our scheme, the response bits are generated by comparing the parallel currents of two bit lines. Due to the structure’s reconfigurable, the positions of the two bit lines can be exchanged, which means that the ratio of ‘0/1’ can be adjusted.

5.4 Bit-Aliasing

We perform the bit-aliasing evaluation of 6 groups (grp_1-grp_6) proposed 4×64 MTJ cells STT-MRAM-based PUF, Each group has 100 samples generated by Monte Carlo method. We extract the 64 bits response bit-aliasing values from the simulation results, and compute using Eq. (4). The results obtained are given in Fig. 7. The bit-aliasing of the 6 groups PUFS are in the range from 48.41 to 51.11 percent, and their average value is 49.80 percent.

5.5 Reliability

As depicted in Figs. 8 and 9, we evaluate the reliability of the PUF_1-PUF_{12} listed in Table 1 at the different environments through the bit error rate defined by Eq. (5). First we collect the PUF responses at the nominal condition as the reference (a.k.a., golden responses). Then we measure the same PUF again under varying temperature and supply voltage conditions. The reference values are generated at $25^\circ C$ and $0.2V$ read bias as the temperature varies from $-20^\circ C$ to $90^\circ C$ with a step of $10^\circ C$, and the supply voltage fluctuates within $\pm 10\%$ with a step of $4mv$.

- *Reliability of Group 1 (PUF_1-PUF_8)*

Here we compare the reliability of the proposed reconfigurable PUFs at varying sizes. All eight PUFs generate 128-bits responses and their bit lines are composed of 4, 8, 16, and 32 memory cells parallel structure, respectively. PUF_1, PUF_3, PUF_5, and PUF_7 adopt the neighboring bit lines reconfigurable algorithm, and the others adopt the top-n reconfigurable algorithm.

The experimental results show that the number of parallel cells on a bit line has a substantial effect on the PUF characteristics. As shown in Fig. 8a, there are no error bits for group 1 at nominal temperature, which indicates high reliability. PUF_1-PUF_4 show error bits at higher or lower

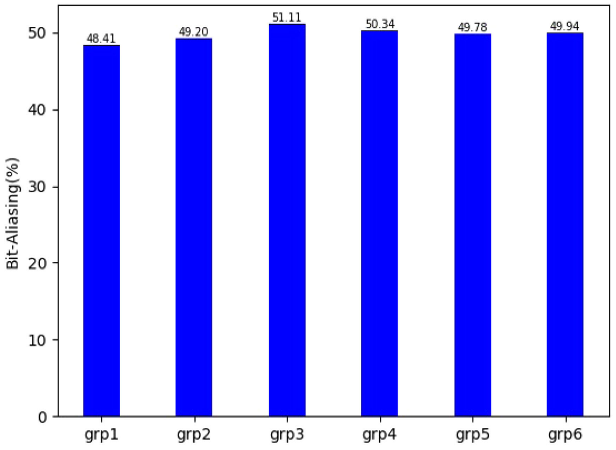
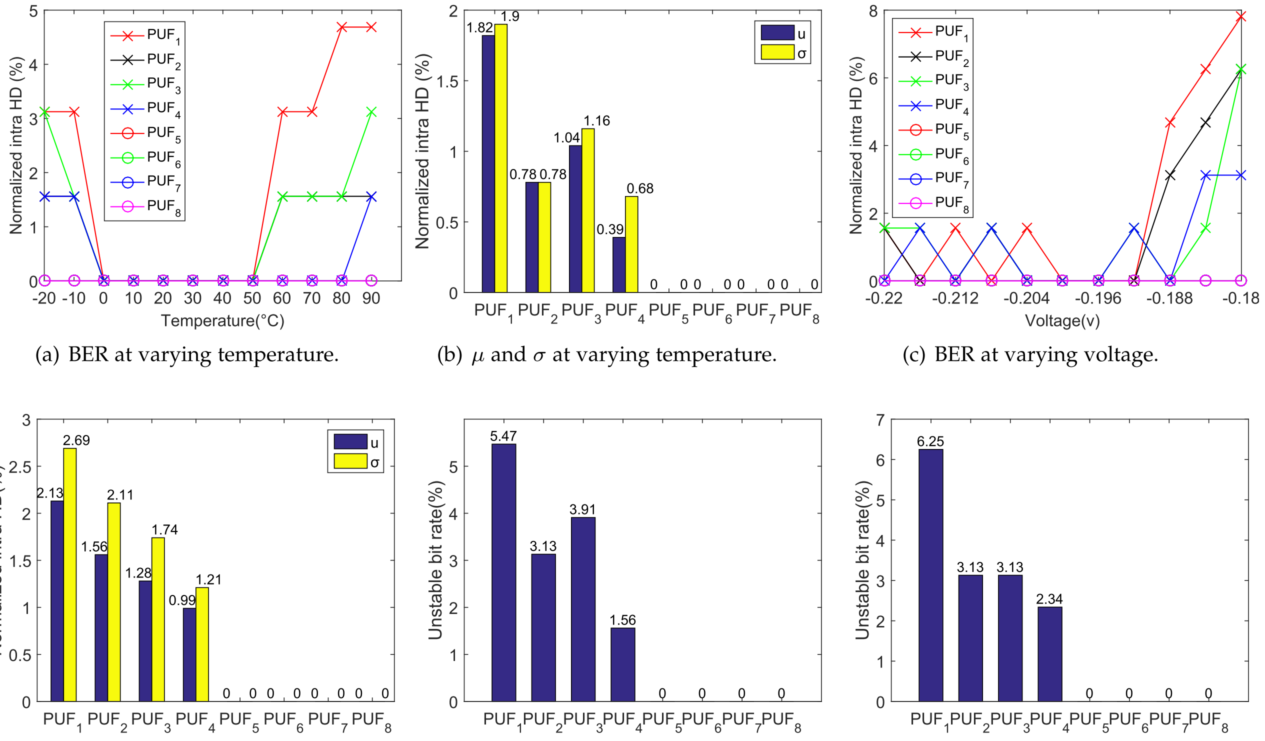


Fig. 7. The bit-aliasing of grp_1-grp_6.



(a) BER at varying temperature.

(b) μ and σ at varying temperature.

(c) BER at varying voltage.

(d) μ and σ at varying voltage.

(e) Unstable bit rate at varying temperature.

(f) Unstable bit rate at varying voltage.

Fig. 8. The reliability of group 1 (PUF_1-PUF_8) at varying temperature and voltage. The μ is the mean value and σ is the standard deviation of BER.

temperature conditions caused by the fluctuation of some device parameters, e.g., saturation magnetization and the polarization factor that vary with the temperature. When the number of parallel cells m exceeds 16 (i.e., PUF_5-PUF_8), there are no error occurrences. The increase of m improves the reliability of the PUF since a larger number of parallel cells leads to a broader current gap between two bit lines. As aforementioned in Section 3.2, the top-n reconfigurable algorithm performances better due to its adaptivity. For example, PUF_2 and PUF_4 outperform the PUF_1 and PUF_3 under a wide range of temperatures. Notably, the near-zero μ and σ in Fig. 8b further indicate that the proposed PUF scheme is stable and resistant to disturbance.

Figs. 8c and 8d present the reliability of group 1 at varying voltages. Since the supply voltage affects not only the MTJ devices but also the sensitivity of the sense amplifier, the reliability fluctuates slightly, and the BER decreases to 8 percent. However, the number of parallel cells m exceeds 16 in PUF_5-PUF_8, which can form a large enough parallel current difference. PUF_5-PUF_8 are still reliable under the voltage fluctuations. Figs. 8e and 8f present the unstable bit rate of group 1 at varying temperature and voltages. Bit errors do not always occur in the same location.

- *Reliability of Group 2 (PUF_9-PUF_{12})*

As shown in Fig. 9, we compare our PUFs with other PUF implementations in the same condition. The PUF_{11} uses one special MTJ as the reference, whose electrical resistance is equal to the average value of all active cells in an anti-parallel state. The PUF_{12} utilizes the reference current generation solution proposed in [7]. Owing to the reconfiguration algorithm, PUF_9 and PUF_{10} achieve much lower BER than PUF_{11} and PUF_{12}. The PUF_{10} is the most reliable, and its mean BER is merely 20 and 40 percent of that of PUF_{11} and PUF_{12}.

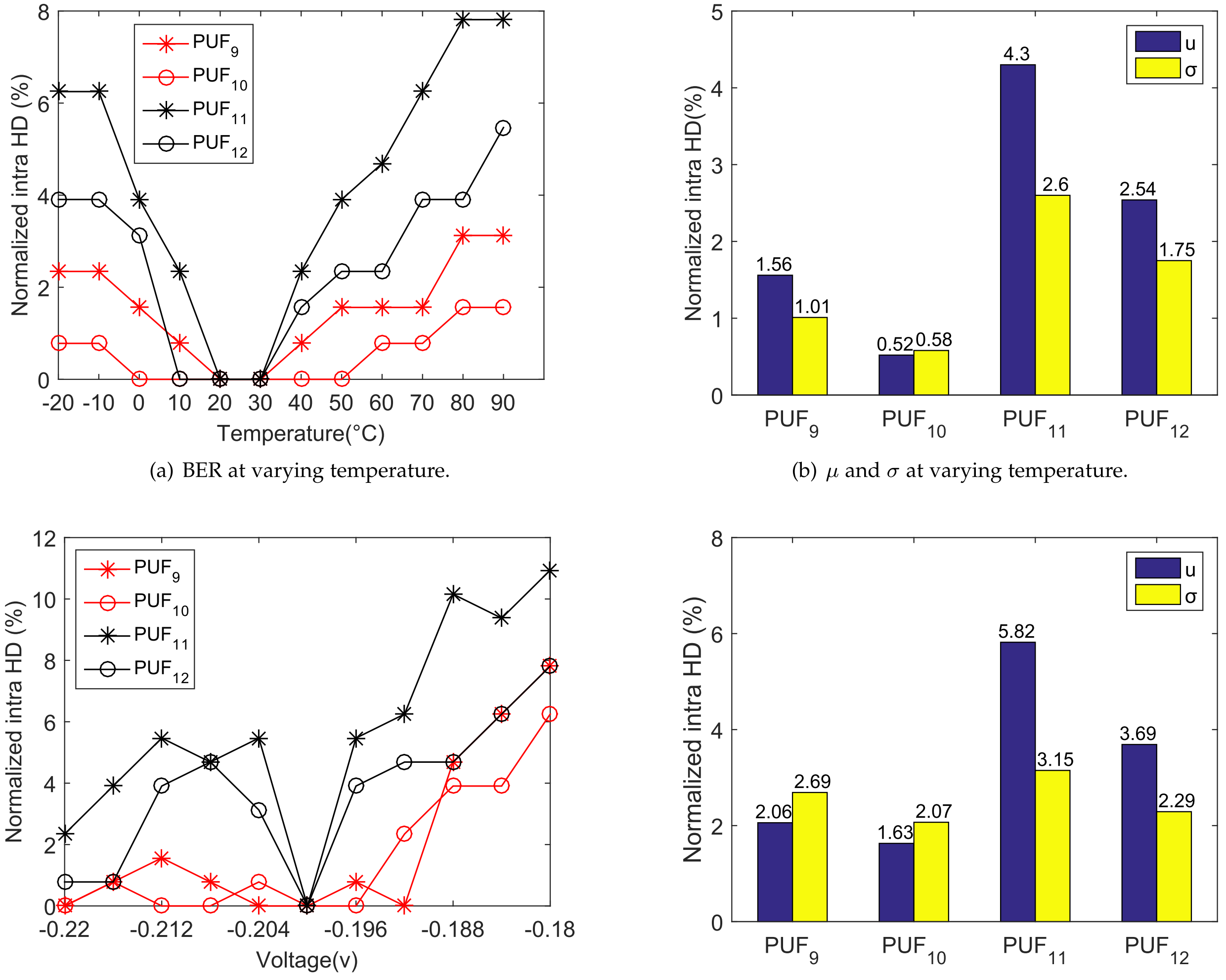
We summarize the three key metrics of our proposed reconfigurable PUFs and other state-of-the-art PUFs in Table 2, which shows that the proposed PUF outperforms all other schemes in terms of uniqueness and higher reliability.

5.6 Hardware Overhead

The proposed PUF scheme achieves higher reliability at the cost of reasonable hardware overhead. Since STT-MRAM is still in bench-scale research, we exploit simulation to evaluate the hardware overhead. We compare our proposed reconfigurable PUFs with other STT-MRAM-based PUFs in Table 3. Each MTJ memory cell is regarded as a separate unit. The MRAM arrays of the PUFs mentioned in Table 3 are all composed of 64 MTJ memory cells. Except for the MRAM array, we focus on the CMOS digital circuit overhead mainly arises from the DEMUXs and other gates.

[25] introduced the simplest STT MRAM PUF structure without any reliability enhancement measures, so the circuit overhead is minimal. Compared with [7], [25] requires additional 64 MTJ devices (without transistors) to form a reference current generation array. In [18] , since the memory cell structure is 2T2M, the MRAM array's hardware overhead is almost doubled. Additionally, the PUF needs extra write-back circuits.

J bit lines can produce up to $1/2 \times J \times (J-1)$ pairwise combinations at the most. For the proposed n-top solution, we divide the 64-cell array into 16 bit lines with 4-cell parallel, which can generate up to 120 combinations, and take the top 64 bit line pairs with the largest current gap to generate the 64-



(a) BER at varying temperature.

(b) μ and σ at varying temperature.

(c) BER at varying voltage.

(d) μ and σ at varying voltage.

Fig. 9. The reliability of group 2 (PUF_9-PUF_{12}) at varying temperature and voltage.

TABLE 1
Two Groups of the STT-MRAM-Based PUFs are at Varying Sizes

PUF	MRAM Size ($m \times n$ cells)	Algorithm
PUF_1	4×128	Neighboring bit lines
PUF_2	4×128	Top-n
PUF_3	8×128	Neighboring bit lines
PUF_4	8×128	Top-n
PUF_5	16×128	Neighboring bit lines
PUF_6	16×128	Top-n
PUF_7	32×128	Neighboring bit lines
PUF_8	32×128	Top-n
PUF_9	4×64	Neighboring bit lines
PUF_{10}	4×64	Top-n
PUF_{11}	8×8	/
PUF_{12}	8×8	/

PUF_1-PUF_8 generate the 128 bits responses, and PUF_9-PUF_{12} generates the 64 bits responses form groups 1 and 2, respectively.

bits response. Since in most micro-control system chips, the number of gates is usually more than 1000,000 [27]. Compared with the overall circuit, the increased hardware overhead of the proposed PUF is within 0.1%~0.5%.

6 Conclusion

In this paper, we propose a reconfigurable STT-MRAM-based weak PUF. Specifically, the proposed PUF achieves

TABLE 2
The Key Metrics Comparisons of Different MRAM PUFs With Our Solutions

PUF	Uniqueness	Uniformity	Reliability (BER)
Neighboring bit lines	**50.64%**	**50.02%**	**$\leq$ 2.13%**
top-n	**50.01%**	**49.99%**	**$\leq$ 1.56%**
[7]	49.9-51%	48.7-50%	4.2-5.1%
[18]	49.9-50.4%	-	$\leq 10^{-1} - 10^{-6}$
[25]	47%	-	2.25%
[26]	60.56%	-	7.76%

TABLE 3
The Hardware Comparisons of Different MRAM PUFs With Our Solutions

PUF	1T1M	LUT	response bits
top-n	**64**	**37**	**≥64**
[7]	**64+64MTJ**	**7**	**64**
[18]	**64 × 2**	**27**	**64**
[25]	**64**	**7**	**64**

higher reliability than state-of-the-art, which takes advantage of the DEMUXs-based crossing switches that is not explored before. In addition, two algorithms, neighboring bit-line reconfiguration and top-n reconfiguration, are proposed to further increase the difference between two parallel read currents, to enhance the reliability of responses. Our experimental results demonstrate that the proposed reconfigurable solution can significantly improve the PUF reliability. Additionally, the uniqueness, bit-aliasing, and uniformity are close to the ideal value of 50 percent. When there are more than 16 memory cells connected in parallel in one bit line, the bit error rate is almost equal to 0 within a large temperature range from $-20^{\circ}C$ to $90^{\circ}C$.

Although this work makes the first attempt to improve the reliability of weak PUF with a reconfigurable STT-MRAM, there still exist limitations of the proposed design. First, to obtain a more stable read current and a larger current gap, multiple memory cells are needed to generate one response bit, which introduces reasonable hardware overhead but could be further optimized. Second, the experimental results are based on Hspice simulation and MTJ model due to the lack of real implementation and measurement platforms. Future works will explore the implementation and optimization of the highly reliable reconfigurable weak PUF solution on real MRAM devices.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grants 62122023, 61872130, U20A20202, and 61874042, the Key R&D Projects of Changsha under Grant kq1907103, the Hunan Natural Science Foundation for Distinguished Young Scholars under Grant 2020JJ2010, Hu-Xiang Youth Talent Program under Grant 2018RS3041, the Key Research and Development Program of Hunan Province under Grant 2019GK2082.

References

[1] Y. Wang, P. Chen, J. Hu, G. Li, and J. Rajendran, "The cat and mouse in split manufacturing," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 26, no. 5, pp. 805–817, May 2018.

[2] Force, SIA Anti-Counterfeiting Task, "Winning the battle against counterfeit semiconductor products," *White Paper Semicond. Ind. Assoc.*, pp. 4–8, 2013.

[3] J. Zhang and G. Qu, "Recent attacks and defenses on FPGA-based systems," *ACM Trans. Reconfigurable Technol. Syst.*, vol. 12, no. 3, pp. 1–24, 2019.

[4] G. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. Des. Autom. Conf.*, 2007, pp. 9–14.

[5] J. Rajendran, G. S. Rose, R. Karri, and M. Potkonjak, "Nano-PPUF: A memristor-based security primitive," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI*, 2012, pp. 84–87.

[6] S. T. C. Konigsmark, L. K. Hwang, D. Chen, and M. D. F. Wong, "CNPUF: A carbon nanotube-based physically unclonable function for secure low-energy hardware design," in *Proc. Asia South Pacific Des. Autom. Conf.*, 2014, pp. 73–78.

[7] E. I. Vatajelu, G. Di Natale , M. Indaco, and P. Prinetto, "STT MRAM-based PUFs," in *Proc. Des. Autom. Test Eur. Conf. Exhib.*, 2015, pp. 872–875.

[8] Y. Dodis *et al.*, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–116, 2008.

[9] Y. Hu, S. Song, S. Xiao, Q. Xu, N. Xiao, and Z. Qin, "A dominating error region strategy for improving the bit-flipping LDPC decoder of SSDs," *IEEE Trans. Circuits Syst. II Exp. Briefs*, vol. 62, no. 6, pp. 578–582, Jun. 2015.

[10] K. Beckmann, H. Manem, and N. C. Cady, "Performance enhancement of a time-delay PUF design by utilizing integrated nanoscale ReRAM devices," *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 3, pp. 304–316, Third Quarter 2017.

[11] A. Shrivastava, P. Y. Chen, Y. Cao, S. Yu, and C. Chakrabarti, "Design of a reliable RRAM-based PUF for compact hardware security primitives," in *Proc. IEEE Int. Symp. Circuits Syst.*, 2016, pp. 2326–2329.

[12] P. Tseng *et al.*, "Error free physically unclonable Function with Programmed resistive random access memory using reliable resistance states by specific identification-generation method," *Japanese J. Appl. Phys.*, vol. 57, no. 4, pp. 1–6, 2018.

[13] J. Kim, A. Chen, B. Behin-Aein , S. Kumar, J. P. Wang, and C. H. Kim, "A technology-agnostic MTJ SPICE model with user-defined dimensions for STT-MRAM scalability studies," in *Proc. Custom Integr. Circuits Conf.*, 2015, pp. 1–17.

[14] M. Uddinl *et al.*, "Design considerations for memristive crossbar physical unclonable functions," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 14, no. 1, pp. 1–23, 2017.

[15] E. I. Vatajelu, G. Di Natale , L. Torres, and P. Prinetto, "STT-MRAM-based strong PUF architecture," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI*, 2015, pp. 467–472.

[16] E. I. Vatajelu, G. Di Natale, and P. Prinetto, "Zero bit-error-rate weak PUF based on spin-transfer-torque MRAM memories," in *Proc. Int. Verification Secur. Workshop*, 2017, pp. 128–133.

[17] Y. Pang *et al.*, "A reconfigurable RRAM physically unclonable function utilizing post-process randomness source with $6{\times}10^{-6}$ native bit error rate," in *Proc. IEEE Int. Solid State Circuits Conf.*, 2019, pp. 402–404.

[18] L. Zhang, X. Fong, C.-H. Chang, Z. H. Kong, and K. Roy, "Highly reliable spin-transfer torque magnetic RAM-based physical unclonable function with multi-response-bits per cell," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 8, pp. 1630–1642, Aug. 2015.

[19] J. Zhang and G. Qu, "Physical unclonable function-based key-sharing via machine learning for IoT security," *IEEE Trans. Ind. Electron.*, vol. 67, no. 8, pp. 7025–7033, Aug. 2020.

[20] W. F. Brinkman, R. C. Dynes, and J. M. Rowell, "Tunneling conductance of asymmetrical barriers," *J. Appl. Phys.*, vol. 41, no. 5, pp. 1915–1921, 1970.

[21] J. Hayakawa *et al.*, "Current-driven magnetization switching in CoFeB/MgO/CoFeB magnetic tunnel junctions," *Japanese J. Appl. Phys.*, vol. 44, no. 37–41, pp. 1–18, 2005.

[22] M. Julliere, "Tunneling between ferromagnetic films," *Phys. Lett.*, vol. 54, no. 3, pp. 225–226, 1975.

[23] J. C. Slonczewski, "Current driven excitation of magnetic multilayers," *J. Magnetism Magn. Mater.* vol. 159, no. 96, pp. 1–7, 1996.

[24] L. Tae-Hoon and C. Gyuseong, "Monte Carlo based time-domain Hspice noise simulation for CSA-CRRC circuit," *Nucl. Instrum. Methods Phys. Res.* vol. 505, no. 1/2, pp. 328–333, 2003.

[25] J. Das, K. Scott, andS. Burgett, "MRAM PUF: A novel geometry based magnetic PUF with integrated CMOS nanotechnology," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 13, no. 1, pp. 1–15, 2016.

[26] X. Zhang *et al.*, "A novel PUF based on cell error rate distribution of STT-RAM," in *Proc. Asia South Pacific Des. Autom. Conf.*, 2016, pp. 342–347.

[27] H. Huang, C. Fang, and C. Fan, "Very-large-scale integration design of a low-power and cost-effective context-based adaptive variable length coding decoder for H.264/AVC portable applications," *IET Image Process.*, vol. 6, no. 2, pp. 104–114, 2012.

[28] J. Zhang *et al.*, "A survey on silicon PUFs and recent advances in ring oscillator PUFs," *J. Comput. Sci. Technol.*, vol. 29, no. 4, pp. 664–678, 2014.

[29] J. Delvaux, D. Gu, D. Schellekens, and I. Verbauwhede, “Helper data algorithms for PUF-based key generation: Overview and analysis,” *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 34, no. 6, pp. 889–902, Jun. 2015.

[30] K.-H. Chuang, E. Bury, R. Degraeve, B. Kaczer, D. Linten, and I. Verbauwhede, “A physically unclonable function using soft oxide breakdown featuring 0% native BER and 51.8 fJ/bit in 40-nm CMOS,” *IEEE J. Solid-State Circuits*, vol. 54, no. 10, pp. 2765–2776, Oct. 2019.

[31] M. Bhargava and K. Mai, “An efficient reliable PUF-based cryptographic key generator in 65nm CMOS,” in *Proc. Des. Autom. Test Eur. Conf. Exhib.*, 2014, pp. 1–6.

[32] R. Maes and V. van der Leest, “Countering the effects of silicon aging on SRAM PUFs,” in *Proc. IEEE Int. Symp. Hardware Oriented Secur. Trust*, 2014, pp. 148–153.

[33] S. Mathew *et al.*, “A 4fJ/bit delay-hardened physically unclonable function circuit with selective bit destabilization in 14nm trigate CMOS,” in *Proc. IEEE Symp. VLSI Circuits*, 2016, pp. 1–2.

[34] K. Beckmann, H. Manem, and N. C. Cady, “Performance enhancement of a time-delay PUF design by utilizing integrated nanoscale ReRAM devices,” *IEEE Trans. Emerg. Topics Comput.*, vol. 5, no. 3, pp. 304–316, Third Quarter 2017.

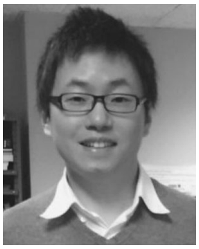
[35] M. Hosomi *et al.*, “A novel nonvolatile memory with spin torque transfer magnetization switching: Spin-Ram,” in *Proc. IEEE Int. Electron Devices Meeting*, 2005, pp. 459–462.

Yupeng Hu (Senior Member, IEEE) received the MS and PhD degrees in computer science from Hunan University, Changsha, China, in 2005 and 2008, respectively. He is currently a professor with the College of Computer Science and Electronic Engineering, Hunan University. He is the dean of the Department of Cyberspace Security. He was with the National University of Defense Technology as a postdoctoral from 2011 to 2016. He was with the Department of Computer Science and Engineering, UT-Arlington as a visiting scholar from 2015 to 2016. He was also with IBM China Development Laboratory as an academic visitor in 2012. His research interests include big data and storage systems security, erasure coding, AI security, and network and system security. He has published more than 60 journal articles, book chapters, and refereed conference papers. Several big data security detection, mobile codes audition, and vulnerability mining systems he developed have been adopted by National Administration of State Secrets Protection, Tencent Security Response Center, or productized by several security companies. He is a senior member of the ACM.

Linjun Wu is currently working toward the PhD degree in the College of Computer Science and Electronic Engineering, Hunan University, Changsha, China. Her current research interests include hardware security and AI security.

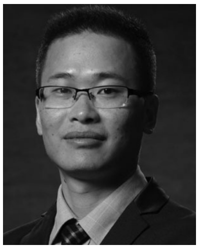
Zhuojun Chen (Member, IEEE) received the PhD degree in micro-electronics and solid-state circuits with emphasis in radiation-hardened integrated circuit design from the Institute of Shanghai Institute of Microsystem and Information Technology, Chinese Academy of Sciences, Beijing, China, in 2017. Presently, he is an associate professor at Hunan University. His research interests include high reliability integrated circuit and device design.

Yun Huang is currently working toward the graduate degree in the College of Computer Science and Electronic Engineering, Hunan University, Changsha, China. Her current research interests include machine learning and hardware security.



Xiaolin Xu (Member, IEEE) received the BS and MS degrees from the University of Electronic Science and Technology of China, Chengdu, China, in 2008 and 2011, respectively, and the PhD degree in electrical and computer engineering from the University of Massachusetts Amherst, Amherst, Massachusetts, in 2016. He was a postdoctoral fellow with the Florida Institute for Cybersecurity Research, Gainesville, Florida. He is an assistant professor with the Department of Electrical and Computer Engineering, Northeastern University, Boston, Massachusetts. His research interests include hardware security and trust, embedded systems, VLSI, and FPGA.

Keqin Li (Fellow, IEEE) is a SUNY distinguished professor of computer science with the State University of New York. He is also a distinguished professor with Hunan University, China. His current research interests include cloud computing, fog computing and mobile edge computing, energy-efficient computing and communication, embedded systems and cyber-physical systems, heterogeneous computing systems, big data computing, high-performance computing, CPU-GPU hybrid and cooperative computing, computer architectures and systems, computer networking, machine learning, intelligent and soft computing. He has authored or coauthored more than 770 journal articles, book chapters, and refereed conference papers, and has received several best paper awards. He has chaired many international conferences. He is currently an associate editor of *ACM Computing Surveys* and *CCF Transactions on High Performance Computing*. He has served on the editorial boards of *IEEE Transactions on Parallel and Distributed Systems*, *IEEE Transactions on Computers*, *IEEE Transactions on Cloud Computing*, *IEEE Transactions on Services Computing*, and *IEEE Transactions on Sustainable Computing*.



Jiliang Zhang (Senior Member, IEEE) received the PhD degree in computer science and technology from Hunan University, Changsha, China, in 2015. From 2013 to 2014, he worked as a research scholar with the Maryland Embedded Systems and Hardware Security Lab, University of Maryland, College Park. From 2015 to 2017, he was an associate professor with Northeastern University, China. He is currently a full professor with Hunan University. He is the director of Chip Security Institute of Hunan University, and the secretary-general of CCF Fault-Tolerant Computing Professional Committee. His current research interests include hardware security, hardware-assisted security, and microarchitecture security. He has authored more than 60 technical papers in leading journals and conferences. He is serving as a steering member for Hardware Security Forum of China and a guest editor of the *IEEE Transactions on Circuits and Systems II: Express Briefs*.