A Highly Reliable and Tamper-Resistant RRAM PUF: Design and Experimental Validation

Rui Liu[1], Huaqiang Wu[2*], Yachun Pang[2], He Qian[2], Shimeng Yu[1#]
[1]School of Electrical, Computer, and Energy Engineering, Arizona State University, Tempe, AZ 85287, USA
[2]Institute of Microelectronics, Tsinghua University, Beijing 100084, China
Email: [*]wuhq@tsinghua.edu.cn, [#]shimengy@asu.edu

***Abstract*—This work presents a highly reliable and tamper-resistant design of Physical Unclonable Function (PUF) exploiting Resistive Random Access Memory (RRAM). The RRAM PUF properties such as uniqueness and reliability are experimentally measured on 1 kb HfO_2 based RRAM arrays. Firstly, our experimental results show that selection of the split reference and offset of the split sense amplifier (S/A) significantly affect the uniqueness. More dummy cells are able to generate a more accurate split reference, and relaxing transistor's sizes of the split S/A can reduce the offset, thus achieving better uniqueness. The average inter-Hamming distance (HD) of 40 RRAM PUF instances is ~42%. Secondly, we propose using the sum of the read-out currents of multiple RRAM cells for generating one response bit, which statistically minimizes the risk of early retention failure of a single cell. The measurement results show that with 8 cells per bit, 0% intra-HD can maintain more than 50 hours at 150 °C or equivalently 10 years at 69 °C by 1/kT extrapolation. Finally, we propose a layout obfuscation scheme where all the S/A are randomly embedded into the RRAM array to improve the RRAM PUF's resistance against invasive tampering. The RRAM cells are uniformly placed between M4 and M5 across the array. If the adversary attempts to invasively probe the output of the S/A, he has to remove the top-level interconnect and destroy the RRAM cells between the interconnect layers. Therefore, the RRAM PUF has the "self-destructive" feature. The hardware overhead of the proposed design strategies is benchmarked in 64 × 128 RRAM PUF array at 65 nm, while these proposed optimization strategies increase latency, energy and area over a naive implementation, they significantly improve the performance and security.**

Keywords—RRAM, PUF, hardware security, reliability, tamper resistance, layout obfuscation

I. INTRODUCTION

Physical Unclonable Function (PUF) is a hardware security primitive that has been proposed for device authentication and key generation [1]. So far, several silicon PUF primitives have been reported including delay-based PUFs such as Arbiter or Ring Oscillator PUF and Memory based PUFs such as SRAM or Flip-Flop PUF [2-4]. However, the responses of these PUFs are sensitive to environmental variations [5]. Although a small percentage of response bit errors is tolerable by fuzzy extraction when the PUF is used for authentication, even a single bit error is unacceptable when PUF is used for key generation as the output is usually hashed. In order to achieve a reproducible output, error correction codes (ECC) along with helper data is generally used [5]. However, helper data partially leaks the secure information thus making PUF prone to attacks [6]. In addition, many of these existing PUF primitives are susceptible to different types of attacks. For example, the Arbiter PUF and its variants all suffer from the modeling attacks (e.g. the machine learning algorithms) [7], and the SRAM PUF can be characterized by photon emission analysis and cloned by Focused Ion Beam (FIB) Circuit Edit (CE) [8]. Therefore, developing new PUF primitives that mitigate the threats from these attacks is a very important research topic.

Recently, emerging non-volatile memory (NVM) based PUFs have been proposed [9], including phase change memory (PCM) PUFs [10], spin torque transfer magnetic random access memory (STT-MRAM) PUFs [11] and resistive random access memory (RRAM, or memristor) PUFs [12-16]. It should be noted that the NVM PUF may not follow the canonical definition of PUF, but it is more similar to a true random number generator with a (secure) NVM. Most of these prior works are based on simulations or single device measurement, which usually could not accurately reflect the statistics of variability and reliability in the memory arrays. To date there is limited experimental data available in literature about NVM based PUF's characteristics at array-level. In [10], PCM PUFs were experimentally evaluated on 1 Mb arrays, showing the mean value of inter-Hamming distance (HD) is around 30% without hash and intra-HD can be up to 10%. Many of the prior works [12, 13] use the probabilistic switching of RRAM as the entropy source. However, the cycling endurance degradation will eventually limit its lifetime, and the active switching in each cycle consumes much higher energy consumption than the static read-out of resistance. In this work, we focus on using RRAM resistance variability as entropy source for a *weak* PUF, aiming for super high reliability and tamper resistance for the key generation application. The contribution of this work include:

1) Realistic data of RRAM PUF properties such as uniqueness and reliability are experimentally measured from the fabricated 1 kb RRAM arrays.

2) Strategies to improve RRAM PUF's uniqueness by using dummy arrays for split reference generation and relaxing transistors size for split sense amplifier are proposed and experimentally validated, achieving ~42 % inter-HD.

3) Strategies to improve RRAM PUF's reliability by multiple-cell as one response bit are proposed and experimentally validated, achieving 0% intra-HD for a 50 hours at 150 °C, which may eliminate the necessity of additional ECC circuit.

4) Strategies to improve RRAM PUF's tamper resistance against invasive probing by layout obfuscation are proposed. The sense

978-1-4673-8826-9/16/$31.00 ©2016 IEEE

amplifiers (S/A) are randomly embedded into the array underneath a sea of uniformly distributed fake and real RRAM cells between M4 and M5. If the adversary tries to probe the response bits from S/A, RRAM cells will be destroyed.

The paper is organized as follows: Section II provides a brief introduction of the RRAM PUF implementation. Section III presents the measurement results of RRAM PUF properties on 1 kb RRAM arrays. Section IV describes the strategies to improve RRAM PUF's uniqueness, reliability and tamper resistance, as well as their associated overhead. Section V summarizes this work.

II. RRAM PUF AND PERFORMANCE METRICS

Oxide-based RRAM is an emerging NVM candidate currently under extensive industrial development [17]. It has a relatively large variability in resistance distribution, which is a significant design challenge for NVM applications. Nevertheless, hardware security applications generally embrace truly random variations. Here we leverage RRAM's resistance variability to design a weak PUF. The operation principle of RRAM is the reversible switching between a high resistance state (HRS, or "0") and a low resistance state (LRS, or "1") by voltage pulse. The physical mechanism of oxide-based RRAM is generally attributed to the formation and rupture of conductive filaments with oxygen vacancies between two metal electrodes. Due to the randomness of the oxygen vacancies' generation and annihilation, the dimension and composition of the conductive filament inevitably vary from cell to cell, and even from cycle to cycle within one cell. Thus RRAM variability is inherent in its physical mechanism instead of the solely manufacturing process variation. Since conduction in the HRS is dominated by the tunneling mechanism between the tip of the residual filament and the electrode, a small variation of tunneling gap distance results in a significant variation in HRS resistance, which provides a sufficient entropy for PUF application. Therefore the larger variability in HRS (than in LRS) is exploited in this work.

Firstly, we introduce the proposed circuit diagram of the RRAM PUF macro for the PUF construction phase (red part) and the PUF operation phase (green part), as shown in Fig. 1. In this work, the properties of RRAM are measured from fabricated 1

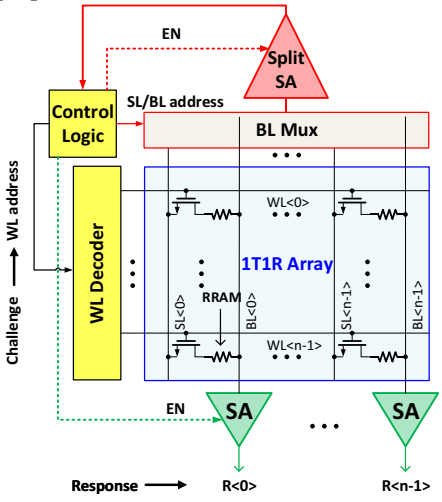

Fig. 1. Proposed RRAM PUF circuit macro for the PUF construction phase (red) and PUF operation phase (green).

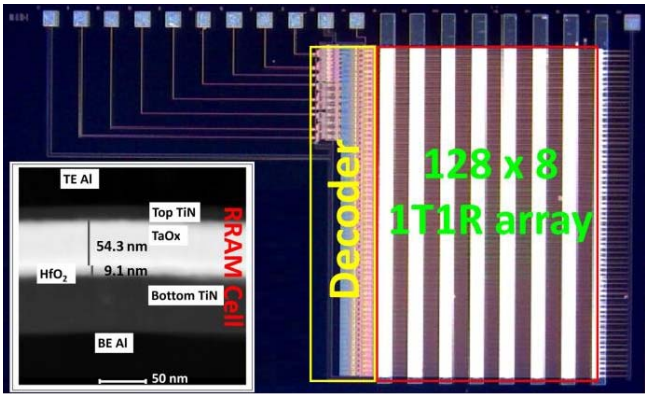

Fig. 2. Top view of the fabricated 128×8 1 kb 1T1R RRAM array with a built-in decoder under the microscope. The inset is cross-sectional microscopic image of $TiN/TaO_x/HfO_2/TiN$ RRAM device.

kb (128 rows × 8 columns) 1-transistor-1-resistor (1T1R) arrays. Fig. 2 shows the microscopic top view image of the RRAM array with a built-in decoder. The RRAM device structure is $TiN/TaO_x/HfO_2/TiN$ stack as shown in the cross-section microscopic image (inset of Fig. 2), which is integrated between the interconnect layers on top of the CMOS transistors. In the PUF construction phase, a pulse forming process is performed row by row in the RRAM array to initiate the subsequent switching. In our testing protocol, a verification criterion is enforced for forming that the RRAM's LRS read-out current should reach the same level by ramping up the transistor gate WL voltage and BL voltage. This ensures an almost uniform LRS distribution across cells to start with. Then all the cells in the array are attempted to RESET to HRS using the same pulse condition, thus the variation that occurs in the first-time RESET becomes the random source entropy for the RRAM PUF. Then

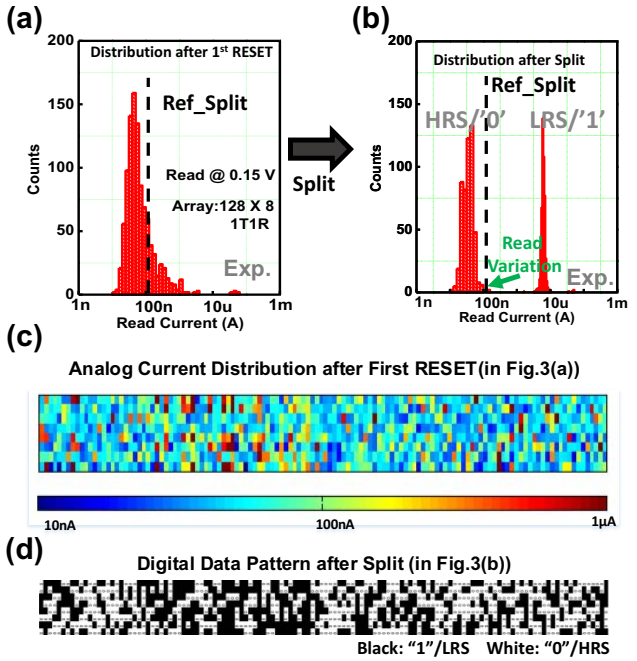

Fig. 3. (a) Distribution of read current after the first RESET in an RRAM array and (b) distribution after a part of cells are programmed into LRS according to the split reference. (c) Analog data pattern after the first RESET operation. (d) Digital data pattern after the split.

a read voltage is applied across each RRAM cell and the read current is measured. Fig. 3(a) shows the read current distribution after first-time RESET of the 1 kb array. A split reference current is chosen within the distribution. The cells with currents above the reference are SET into LRS, as shown in Fig. 3(b). This split process aims to digitize the randomness and improve the PUF's reliability against resistance fluctuations and read-out noises [14]. Fig. 3(c) presents the analog data pattern when the first RESET operation is performed. Fig. 3(d) shows the digital data pattern after split. The window between the two split states should be sufficiently large so that even minimum-sized sense amplifier can differentiate the read current. After this split process and the enrollment of challenge-response pairs (CRPs) in the database, the RRAM PUF construction is complete. During the normal operations when deployed in the field, only read operations are performed on the RRAM PUF: the address is given as the challenge, the digital read-out through a read sense amplifier is the response.

III. Performance Evaluation on 1 kb RRAM Arrays

To evaluate the uniqueness, 40 PUF instances are constructed from 5 1 kb 1T1R arrays with size of 128 × 8. By applying the same challenge inputs (activating all rows one by one), 128-bit responses are measured. Then the uniqueness is evaluated by inter-HD of the responses pair-wisely compared across the 40 PUF instances.

A. Impact of Split Reference on RRAM PUF's Uniqueness

One factor that affects the RRAM PUF's uniqueness is the split reference used in the split process. Ideally the reference should a read current that can make an equal 50% probability of generating "0" and "1", although this restriction will reduce the possible configurations of the response bit stream. In experiments, we used a dummy column to generate the split reference. Then the split reference is set as the median current of the 128 dummy cells in one column. We prepared 40 dummy columns. Hence we have 40 possible split references. Due to variations between column and column, the generated 40 possible references distribute in a wide range from (74 nA to 238 nA). We choose one with smallest deviation from the ideal reference and the other one with largest deviation from ideal reference to conduct the split process. Fig. 4 shows the fractional inter-HD distributions when using these two split references. When split with the most accurate reference, the average inter-HD is around 49.8% with a tight distribution. However, when split with the most inaccurate reference, the average fractional inter-HD is only 24.2%. This result shows the importance of choosing a good split reference for achieving a good uniqueness.

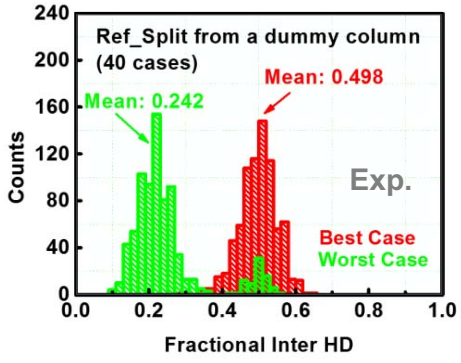

Fig. 4. Distribution of fractional inter-Hamming distance (HD) of 128-bit responses with split reference current obtained from a dummy column. The best and worst cases of 40 split references from 40 dummy columns are shown.

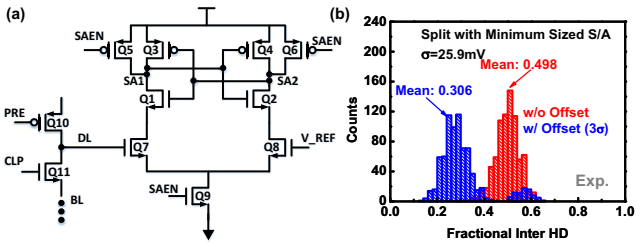

Fig. 5. (a) Schematic of a voltage mode sense amplifier (S/A) used in the split process as a comparator. (b) Distribution of fractional inter-HD of 128-bit responses without or with S/A offset (σ= 25.9 mV). Minimum sized transistors are used.

B. Impact of Split S/A Offset on RRAM PUF's Uniqueness

Sense amplifier (S/A) is used as the comparator in the split process. Under ideal conditions, an idea S/A should be able to amplify a very small input differential signals correctly. In reality, however, process variations in the transistors of an S/A introduce an input offset, which results in a skewed preference to generate "1" or "0". In this work, a voltage mode sense amplifier is employed in the split process, as shown in Fig. 5(a). The two differential inputs are V_DL and V_REF. At first, pre-charge transistor (Q10) is turned on and the BL is charged to V_read. Then Q10 is turned off and BL is being discharged through RRAM cell for a short period of time to develop a voltage sense margin. Depending on the RRAM cell's current, V_DL's decay can be fast or slow. Finally, SAEN is turned on and the difference between V_DL and V_REF is amplified by the latch based load and the digital output is generated in SA1 and SA2. In a naive implementation, all the transistors in S/A can be minimum sized. To assess the input offset of this S/A, 1000 Monte Carlo simulation runs were performed in Cadence Spectre in TSMC 65 nm node using library "TSMC65-GP-1p9m_6X1Z1U_ALRDL_2.0". The simulation shows that the S/A with minimum sized transistors has an offset voltage σ of 25.9 mV. If S/A with 3σ input offset voltage is used in the split process, it might have a much skewed preference to generate more "0"s or "1"s. As a result, the distribution of the fractional inter-HD decreases to 30.6% as shown in Fig. 5(b). Therefore, minimizing S/A offset voltage is necessary in the split process.

C. Impact of RRAM Retention Failure on PUF's Reliability

Reliability of RRAM PUFs requires an excellent data retention even at elevated temperature conditions. Once the retention

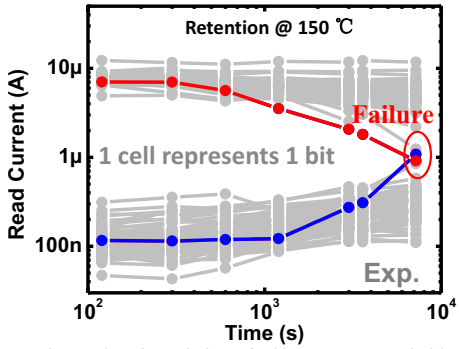

Fig. 6. Measured retention degradation of 1 kb RRAM array baking at 150 °C. Error occurs within 2 hours if a single cell represents a PUF response bit.

failure occurs in the RRAM cell, it will introduce an error in the response bits, thus increasing the intra-HD. To evaluate the RRAM's data retention, a high temperature (150 °C) is used to accelerate the failure in our measurement. Fig. 6 shows the 1 kb RRAM array's read current degradation without voltage bias a150 °C. The experimental result shows that the tail bits in HRS and tail bits in LRS crossed-over in less than 2 hours (or equivalently less than a 25 days at 85 °C), which means errors occur in the PUF's response if a PUF response bit is represented by a single RRAM cell. This experimental result illustrates the necessity of improving RRAM PUF's reliability.

IV. Improving RRAM PUF's Perfromance and Reliablity

In this section, we will propose design strategies to improve RRAM PUF's uniqueness and reliability issues as pointed out in the previous section. In addition, we will employ a layout obfuscation technique to enhance its tamper resistance.

A. Accurate Split Reference Generation by Dummy Array

In order to generate a more accurate split reference, more dummy cells are needed to average out the cell to cell variations. For example, the dummy cells can be obtained from an array (with 8 columns each array) instead of one column. We prepared 5 split references from 5 dummy arrays. Table I lists the mean values and standard deviations of the fractional inter-HD when using these 5 split references. The distribution of inter-HD is centered at 47.78% with a small σ of 5.563% in the worst case. In the practical design, there are two ways to obtain a good split reference. First, it can be obtained by off-chip pre-calibration. A dummy array (or a few dummy arrays) can be manufactured in same batch. The same programming conditions are performed on the dummy array. It is easy to find the median of read current by a simple sorting algorithm off-chip. Second, a dummy array are designed adjacent to the real array on-chip, and a custom circuit is needed to do the sorting. Since the split process is only done once in the PUF construction phase, finding a good split reference from off-chip pre-calibration is more efficient in terms of area and energy.

TABLE I. Uniqueness Evaluation with Ref_Split Generated From a Dummy Array (128 ×8)

Uniqueness	Ref_Split generated from Array No.				
	1st	2nd	3rd	4th	5th
μ(%)[a]	49.48	48.97	49.79	47.77	49.80
σ(%)[b]	4.90	5.06	4.87	5.56	4.86

[a] Mean

[b] Standard Deviation

B. Improve Uniqueness by Minimizing Split S/A Offset

As technology node scales down, the input offset of S/A increases due to the overall increase in local (i.e. within-die) process variation, e.g. random dopant fluctuation (RDF). It is known that the standard deviation of the transistor's threshold voltage (V_{th}) distribution is proportional to $1/(WL)^{1/2}$ [18]. Sizing the transistors is a flexible option and is employed in this work. The key contributor to the offset is from the input differential pair (Q7 and Q8 in Fig. 5(a)), thus their sizes should be increased most. Besides Q7 and Q8, Q1, Q2, Q3, Q4 in the latch based load and Q9 in the bottom current source are also critical transistors that should increase sizes. Table II and Table III list two sets of transistor's sizes that can reduce the offset σ to 7.868 mV and 6.511 mV respectively. In addition, in order to

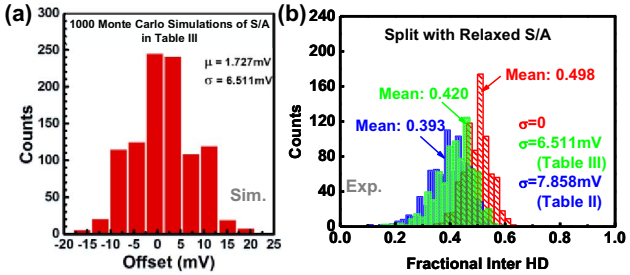

Fig. 7. (a) Distribution of split S/A voltage offset from 1000 Monte Carlo simulations. The transistor sizes are relaxed as in Table III. (b) Distribution of fractional inter-HD of 128-bit responses when using S/A different 3σ voltage offsets in the split process.

reduce the input offset from layout point of view, symmetrical and common centroid layout design is employed. Fig. 7 (a) is the distribution of input voltage offset obtained by running 1000 Monte Carlo simulations with transistor sizes listed in Table III. When the standard deviation of input offset is reduced to 6.511 mV, the average inter-HD can be improved to 42% as shown in Fig. 7 (b). Such a relaxed design of split S/A does not increase the total area of RRAM PUF macro too much because there is only one split S/A per PUF used in the construction phase, while other read S/A to generate response bits used in the operation phase can still be minimum sized.

TABLE II. S/A Transistors' Size to Reduce Offset σ to 7.858 mV

Transistor	Q1/Q2	Q3/Q4	Q5/Q6	Q7/Q8	Q9	Q10/Q11
Gate Length (nm)	60	60	60	180	60	60
Width (nm)	240	240	120	900	120	120

TABLE III. S/A Transistors' Size to Reduce Offset σ to 6.511 mV

Transistor	Q1/Q2	Q3/Q4	Q5/Q6	Q7/Q8	Q9	Q10/Q11
Gate Length (nm)	60	60	60	180	60	60
Width (nm)	240	240	120	1800	240	120

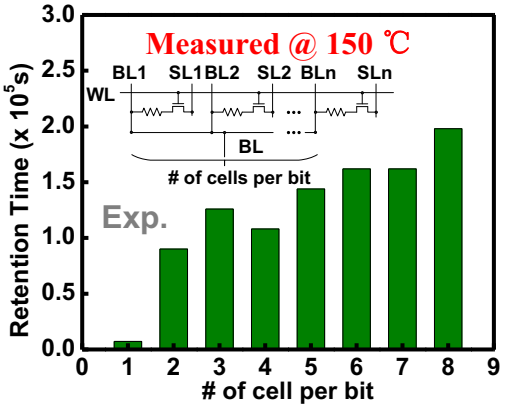

Fig. 8. Measured retention time when a PUF response bit is represented by different number of cells.

C. Multi-Cell-Per-Bit to Improve Reliablity

We propose improving the retention properties using multiple RRAM cells to represent a PUF response bit. The concept behind is that if multiple RRAM cells in parallel are wired as one group, the read-out current will be added up. Due to inherent cell to cell variations, some cells may fail later than others, and the redundancy can minimize the probability of early lifetime failure for the whole group. In the practical design, multiple BLs can be wired together before sending the BL current to the read S/A. In the PUF construction phase, we can program each cell

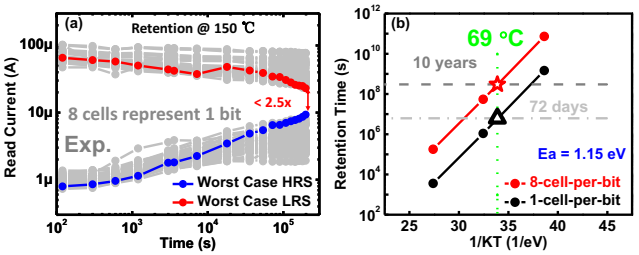

Fig. 9. (a) Measured retention degradation of 1 kb RRAM array baking at 150 °C if 8 cells represent one response bit. (b) Extrapolated retention time using Ea=1.15 eV. 8 cells per bit can possibly ensure 10-year lifetime at 69 °C.

(not including the redundant cells) individually using separate source lines (SLs). Then both the cell and redundant cells should be programmed to the same state as a group according to the comparison with the split reference. Therefore, we do not average out the variation by grouping the cells together. Fig. 8 shows the retention time for different number of RRAM cells representing one PUF response bit that is measured at 150 °C. In general, longer retention time can be achieved with more redundant cells as expected. When each response bit is represented by 8 parallel RRAM cells, it can be sustained for more than 50 hours at 150 °C for a given PUF instance with high reliability (Fig. 9(a)). The on/off ratio of readout the currents for the tail bits is larger than 2.5×, which can be reliably sensed by the read S/A. Fig. 9(b) shows the equivalent retention time extrapolated to 85 °C and 27 °C using the 1/kT extrapolation with activation energy (Ea=1.15 eV, determined in another experiment). 8 RRAM cells in parallel can possibly generate a highly reliable response for 1.75 years at 85 °C, and 10 years at 69 °C. In addition, we have examined that the multiple-cell-per-bit approach has negligible impact on the PUF's uniqueness.

D. Layout Obsfucation for Tamper Resistance

A basic requirement for a weak PUF is that the adversary should not have access to the response bits, as the number of CRPs in a weak PUF is limited. However, the adversary can perform semi-invasive or invasive tampering attacks to obtain the response bits. For example, the SRAM's data pattern can be seen under near-infrared imaging because the hot carriers in the transistors emit photons [8]. It is expected that RRAM's conduction in oxide does not emit photons under laser or X-ray scanning (at least not reported yet). However, the digital responses of RRAM PUF are still read out through the S/A. Hence, the read S/A might be a potential weak spot that an adversary can micro-probe to access the output and read the secret information out. Fig. 10 shows RRAM PUF architecture with 1T1R memory array. Eight cells are grouped together to generate one response bit. The conventional design places the read S/A at the edge of the array, thus they are easy to be identified under the microscope thus vulnerable to the probing attack.

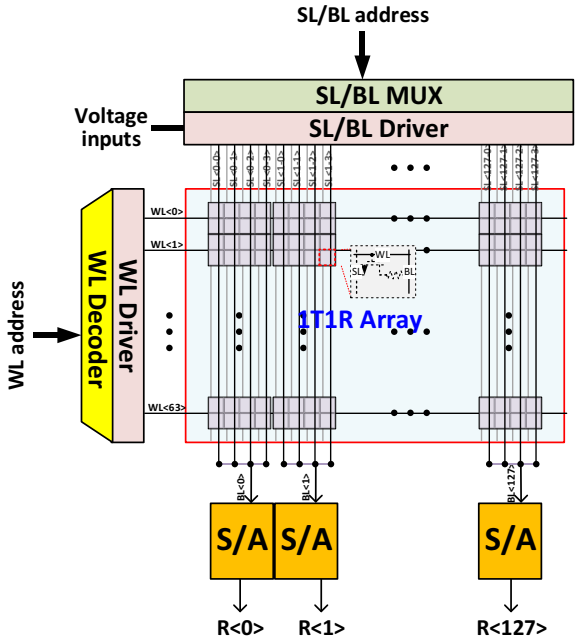

Fig. 10. RRAM PUF architecture with 1T1R memory array. Eight cells are grouped together to generate one response bit. The conventional design places read S/A at the edge of the array, thus vulnerable to the probing attack.

In order to obfuscate the adversary, we propose to hide the S/A within the 1T1R array and randomize the locations of S/A, as shown in Fig. 11 (a). Between M4 and M5, we uniformly place the RRAM contact vias across the array. Fig. 11 (b) shows the Cadence layout of a block including S/A, 8 real RRAM cells and 16 fake RRAM cells on top of S/A. The RRAM contact vias on

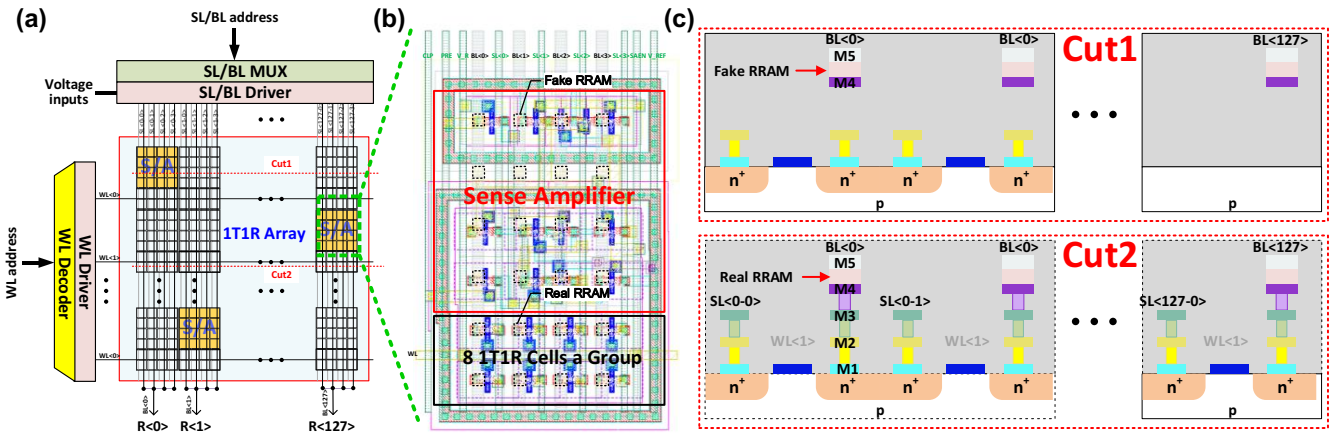

Fig. 11. (a) Tamper-resistant RRAM PUF architecture with read S/A randomly embedded into the array and hiding underneath a sea of real and fake RRAM cells. (b) Layout obfuscation of a block including read S/A, 8 real RRAM cells and 12 fake RRAM cells. Layout done by Cadence using TSMC 65 nm PDK. (c) Cross-section view for cutting through S/A and cutting through the real RRAM cells respectively.

top of the 1T1R are the real RRAM cells, while the RRAM contact vias on top of the S/A are fake RRAM cells. Fig. 11 (c) presents the cross-section of the die for a cut through S/A with fake RRAM cells and a cut through region with the real RRAM cells respectively. When an adversary attempts to probe the S/A's output underneath the uniformly distributed RRAM cells, it is difficult for him to differentiate between the real RRAM cells and the fake RRAM cells from the top-view. The real RRAM cells which implement a secure key storage might be permanently destroyed when the adversary tries to invasively probe, thus the proposed layout obfuscation enables a "self-destructive" feature for the RRAM PUF.

E. Area Cost and Peformance Overhead Analysis

All the proposed design strategies such as relaxing split S/A's transistor sizes, multiple-cell-per-bit, and layout obfuscation with S/A hiding are associated with hardware overhead including more area, larger latency and energy consumption. In order to evaluate the overhead, we use Cadence and HSPICE to evaluate the area cost and performance of a 64 × 128 RRAM PUF macro. Three designs are evaluated. The first one is 1-cell-per-bit without S/A hiding as the baseline, which has the poorest reliability and the lowest security. The second one is 8-cell-per-bit without S/A hiding, which is highly reliable but not tamper resistant. The last one is 8-cell-per-bit with S/A hiding, which is of highest reliability and tamper resistance. All the designs are benchmarked at TSMC 65 nm node using "TSMC65-GP-1p9m_6X1Z1U_ALRDL_2.0" library. Table IV shows the benchmark results. Compared to the baseline, the highly reliable design introduce 1.52× latency, 1.55× energy, and 4.70× area, and the highly reliable plus tamper-resistant design introduce 3.88× latency, 1.84× energy, and 24.53× area. Depending on the application scenarios, the designers can choose the appropriate design strategies. For example, if the security is a not topmost requirement but still 10-year lifetime is necessary, the highly reliable design but without S/A hiding may be sufficient.

TABLE IV. AREA AND PERFORMANCE OF 64 × 128 RRAM PUF ARRAY

Architecture	S/A hiding (w/ or w/o)	Latency (ns)	Energy (pJ)	Area (mm^2)[c]
1-cell-per-bit	w/o	4.24	9.59	0.0083
8-cell-per-bit	w/o	6.46	14.87	0.0390
	w/	16.45	17.69	0.2036

[c.] Including the peripheral circuits (e.g. row decoder, column MUX, write driver and S/A)

V. CONLUSION

In this paper, we experimentally evaluated RRAM PUF's characteristics such as uniqueness and reliability on 1 kb 1T1R arrays. Design strategies to improve uniqueness, reliability and security have also been proposed. The uniqueness of RRAM PUF can be improved by selecting a more accurate split reference from more dummy cells and minimizing the input offset of the split S/A with relaxed transistor's sizes. The reliability of RRAM PUF can be improved by using multiple RRAM cells to generate one response bit. The security in terms of tamper resistance can be improved by layout obfuscation of hiding S/A into the array and underneath fake RRAM cells. As these proposed strategies come with the expense of latency, energy consumption and area efficiency, trade-offs should be considered given the application's priorities. The realistic data measured from the RRAM arrays in this work will be valuable for system designers to develop the practical protocols using the RRAM PUF at the system level.

ACKNOWLEDGMENT

This work is in part supported by NSF-CCF-1449653.

REFERENCES

[1] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *44th IEEE/ACM Design Automation Conference (DAC)* pp. 9–14, Jun. 2007.

[2] B. Gassend, D. Clarke, M. van Dijk and S. Devadas, "Silicon physical random functions," In *Proc. of the 9th ACM Conf. on Comput. And Commun. Security (CCS),* pp. 148–160, Oct. 2002..

[3] J. Guajardo, S. S. Kumar, G. J. Schrijen, P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," in *Workshop on Cryptographic Hardware and Embedded Systems (CHES)*, pp.63-80, 2007..

[4] R. Maes, P. Tuyls and I. Verbauwhede, "Intrinsic PUFs from flip-flops on reconfigurable devices." in *Benelux Workshop on Information and System Security*, vol. 17, 2008.

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

[6] J. Delvaux and V. Ingrid, "Key-recovery attacks on various RO PUF constructions via helper data manipulation," in *Proc. of conf. on Design, Automation & Test in Europe (DATE),* p. 72. 2014.

[7] U. Rührmair, J. Solter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, "PUF modeling attacks on simulated and silicon data," in *IEEE Trans. Inf. Forens. Security*, vol. 8, pp. 1876-1891, Aug. 2013.

[8] C. Helfmeier, C. Boit, D. Nedospasov and J.-P. Seifert, "Cloning physically unclonable functions," in *IEEE Int. Hardware Oriented Security and Trust (HOST)*, 2013.

[9] L. Zhang, X. Fong, C.-H. Chang, Z. H. Kong, and K. Roy, "Feasibility study of emerging non-volatile memory based physical unclonable functions," in *Proc. 6th IEEE Int. Memory Workshop (IMW),* pp. 135–138, May 2014.

[10] L. Zhang, Z. H. Kong, C.-H. Chang, A. Cabrini, and G. Torelli, "Exploiting Process Variations and Programming Sensitivity of Phase Change Memory for Reconfigurable Physical Unclonable Functions," in *IEEE Trans. Inf. Forens. Security*, vol. 9, pp. 921-932, Jun. 2014.

[11] J. Das, K. Scott, S. Rajaram, D. Burgett, S. Bhanja, "MRAM PUF: A novel geometry based magnetic PUF with integrated CMOS," in *IEEE Trans. on Nano.*, vol. 14, no. 3, pp. 436-443, 2015.

[12] G. S. Rose, N. McDonald, L. K. Ya, B. Wysocki, "A write-time based memristive PUF for hardware security applications," in *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2013.

[13] P. Koeberl, U. Kocaba, A.-R. Sadeghi, "Memristor PUFs: A New Generation of Memory-based Physically Unclonable Functions," *in Design, Automation and Test in Europe (DATE)*, 2014.

[14] W. Che, J. Plusquellic, S. Bhunia, "A Non-volatile memory based physically unclonable function without helper data," in *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2014.

[15] A. Chen, "Utilizing the variability of resistive random access memory to implement reconfigurable physical unclonable functions," in *IEEE Electron Device Lett.*, vol. 36, no. 2, pp. 138-140, Feb. 2015.

[16] P.-Y. Chen, R. Fang, R. Liu, C. Chakrabarti, Y. Cao and S. Yu, "Exploiting Resistive Cross-point Array for Compact Design of Physical Unclonable Function," in *IEEE Int. Hardware Oriented Security and Trust (HOST)*, pp. 26-31, May 2015.

[17] H.-S. P. Wong, H.-Y. Lee, S. Yu, Y.-S. Chen, Y. Wu, P.-S. Chen, B. Lee, F.T. Chen, M.-J. Tsai, "Metal–oxide ReRAM," in Proc. IEEE, vol. 100, pp. 1951–1970, Jun. 2012.

[18] M. J. Pelgrom, H. P. Tuinhout and M. Vertregt, "Transistor matching in analog CMOS applications", in *IEEE International Electron Devices Meeting (IEDM)*, pp. 915-918, 1998