A Physical Unclonable Function with Redox-based Nanoionic Resistive Memory

Jeeson Kim, Student Member, IEEE, Taimur Ahmed, Hussein Nili, Jiawei Yang, Doo Seok Jeong, Paul Beckett, Sharath Sriram, Member, IEEE, Damith C. Ranasinghe, Member, IEEE, and Omid Kavehei, Senior Member, IEEE

Abstract—A unique set of characteristics are packed in emerging nonvolatile reduction-oxidation (redox)-based resistive switching memories (ReRAMs) such as their underlying stochastic switching processes alongside their intrinsic highly nonlinear current-voltage characteristic, which in addition to known nano-fabrication process variation make them a promising candidate for the next generation of low-cost, low-power, tiny and secure Physically Unclonable Functions (PUFs). This paper takes advantage of this otherwise disadvantageous ReRAM feature using a combination of novel architectural and peripheral circuitry. We present a physical one-way function, nonlinear resistive Physical Unclonable Function (nuPUF), potentially applicable in variety of cyber-physical security applications given its performance characteristics. We experimentally verified performance of Valency Change Mechanism (VCM)-based ReRAM in nano-fabricated crossbar arrays across multiple dies and runs. In addition to a massive pool of Challenge-Response Pairs (CRPs), using a combination of experimental and simulation, our proposed PUF shows a reliability of 98.67%, a uniqueness of 49.85%, a diffuseness of 49.86%, a uniformity of 47.28%, and a bit-aliasing of 47.48%.

Index Terms—Physical unclonable function, resistive random access memory, emerging nonvolatile memory.

1 INTRODUCTION

Redox based resistive memories (ReRAMs) are an emerging class of two-terminal nonvolatile memory technology. They are one of the most promising devices for conventional and unconventional information processing and memory applications [1]–[3]. They can be integrated on-chip with conventional CMOS technology. Thanks to their highly nonlinear resistance behavior, their read-out speed can be programmed to be fast or slow, with higher or lower power consumptions, respectively. As there are countless choices of material, these devices can also be fabricated with an aim for ultra-high density digital memories or behave like an analog memory with multiple stable states. Unlike SRAM, DRAM and FLASH technologies, these devices do not rely

- J. Kim, P. Beckett and O. Kavehei are with Nanoelectronic and Neuro-inspired Research Laboratory, RMIT University, VIC 3000, Australia. E-mails: {jeeson.kim, paul.beckett, omid.kavehei}@rmit.edu.au.
- T. Ahmed, S. Sriram, J. Kim and O. Kavehei are with the Functional Materials and Microsystems Research Group, RMIT University, VIC 3000, Australia. E-mails: {taimur.ahmed, sharath.sriram}@rmit.edu.au.
- H. Nili is with the Department of Electrical and Computer Engineering, University of California, Santa Barbara, CA 93106 USA. E-mail: hnnili@ece.ucsb.edu.
- J. Yang is with Wenzhou Medical University, China. E-mail: yangjw@wibe.ac.cn.
- D. S. Jeong is with the Electronic Materials Research Centre, Korea Institute of Science and Technology, 136-791 Seoul, Republic of Korea. E-mail: djsjeong@kist.re.kr.
- D. C. Ranasinghe and J. Kim are with the Auto-ID Labs, School of Computer Science, The University of Adelaide, SA 5005, Australia. E-mail: damith.ranasinghe@adelaide.edu.au.

Manuscript received ; revised . This work was supported by Australian Research Council under grant DP140103448 and National Natural Science Foundation of China under Grant 61501332.

on charge storage and retention on a capacitor, rather they exploit a new type of underlying physics that is based on a mixed ionic-electronic conduction mechanism and hence, it is a resistance retention-based technology. These memories have also surpassed nonvolatile FLASH technology in almost any aspect; They offer orders of magnitude higher endurance and write speed than FLASH, they have eliminated FLASH memory’s need for high voltage supply and cumbersome erase procedure, and they offer all these advantages at a potentially lower volume fabrication cost [4]–[9]. ReRAMs could be made potentially denser than FLASH and like FLASH they can go vertical (3D) and ensure zero-power consumption when on stand-by [10]–[12].

Security and privacy applications of such device as part of broader cyber-physical system industry ranging from nation-wide power grids, small scale health care system to Internet of Things (IoT) and solutions based on radio frequency identification (RFID) [13], [14]. For instance, IoT demands challenging security solutions with features such as interoperability, scalability and lightweight process [14], [15]. In such area, power and performance demanding environment, Physical Unclonable Functions (PUFs) could be a suitable solution [16]–[22].

A 19th century scientist, Auguste Kerckhoffs once stated, a system should be secure even if everything about the system, except the key, is a public knowledge [23]. Building on this principle, PUF’s very fundamental feature is the ability to remove the requirement of storing secrets and leave any other system feature as public knowledge [24], [25]. Secrets in PUF are intrinsically encrypted in physical implementation randomness – e.g. silicon fabrication
process, for which there is no way to reverse engineer the system but to characterize every single component of the system. It is therefore very difficult, if not impossible, to make an identical copy of the system even by the use of identical processes, facilities and material [26]. The basic idea of a PUF is to gain advantage of otherwise disadvantageous physical system manufacturing non-idealties. These non-idealties can be classified into spatial and temporal variations. Spatial variations include process variations such as dimensions, random dopant fluctuations, line-edge roughness, which manifest themselves as conventionally undesirable features such as threshold voltage variation and offset in CMOS and other electrical characteristics of solid-state devices. Temporal variation includes noise, supply power, temperature fluctuations, transient effects as common effects in both conventional and emerging technologies. One unique property that is unique to ReRAM devices, is their random oxygen vacancy profile.

Fig. 1(a) and (b), shows a direct evidence of oxygen vacancy profile in our devices (true for all ReRAMs) [27]. This pattern is likely to change with every switching as the formation and rupture of nano-filaments in certain location is an stochastic phenomenon. This pattern is also varying from device-to-device. The tricky part about this spatio-temporal random oxygen vacancy profile in ReRAMs is that once programming is finished, the profile stays fixed under no or small magnitudes of energy delivered to our Valency Change Mechanism (VCM)-based ReRAMs. Temporal and transient aspects of this nano-conductive filament pattern is more profound when the device is switching or is in its Low Resistance State (LRS). It can also be concluded that when a filament becomes the main path of conducting current between electrodes, ReRAM’s LRS’s conductance is almost independent of device contact sizes and tier variation, while in High Resistance State (HRS), the nano-conductive filament pattern is fixed, unique to each device, and their height are much less than LRS’s nanofilaments. Dimensional and line-edge roughness variations are also mainly effecting HRS. Therefore, oxygen vacancy profile could be consider as a perfectly spatial parameter when a ReRAM device is in its HRS. It is important to note that discussions around oxide-trap-induced effects such as burst or random telegraph noise are outside the scope of this paper due to the relatively low frequency nature of the phenomenon.

These systematic, random and spatial variations in CMOS has been harnessed to produce tiny differences in identical circuit and system performance. For instance, small differences in delay has been the source of spatial randomness in arbiter PUFs (Arb-PUFs) and ring-oscillator PUFs (RO-PUFs) [14], [28], [29]. SRAM-PUF is another example. SRAM’s metastability is widely used as another source of randomness. Process variation in implementation of SRAM’s latch and read-out/addressing transistors could make its switch to “1” or “0” more likely than the other after setting up a metastable condition [30]–[33]. While some CMOS PUFs are custom designed, many have been reported on field array logics such as Field-Programmable Gate Array (FPGA). That unfortunately created systematic bias issues as there is no ultimate control over interconnect length [34].

While silicon technology has started a new ground-breaking wave of security primitive solutions, the game is still on for true random key generators that are highly secure, cheap, small and energy-efficient [35]. The device-to-device randomly variant oxygen vacancy profile in VCM ReRAMs provides another dimension that if utilized appropriately could pave the way for
implementation of highly secure nonvolatile memory (NVM)-based PUFs. In this work, we propose a novel PUF architecture based on nonvolatile ReRAM crossbar arrays. Contributions of this work include:

- Introducing a nonlinear ReRAM-based PUF and presenting its full analysis.
  - This includes, assessment of important PUF metrics based on a mix of extensive experimental analysis and simulation.
- Employing the idea of dummy cells and arrays to strengthen nPUF against side-channel power monitoring attacks.

The paper is organized as follows: Section 2 discuss properties of ReRAMs and proposes nPUF and its circuit and architectural level operation. nPUF characterization and experimental results of fabricated ReRAM arrays are illustrated. Section 3 analyses nPUF performance metrics and discusses simulation results. Finally, Section 4 summarizes the work.

## 2 Nonlinear Resistive PUF

### 2.1 Electrical properties of ReRAM

Measured signature bipolar switching behavior of our VCM ReRAM devices is depicted in Fig. 2(a) at room temperature. Device switching characteristic becomes available when an irreversible electro-forming step is completed. An electro-forming step forces the device to switch from its pristine state to its LRS. Beyond that point the device is capable of switching between its LRS and HRS, when enough energy is delivered to the device in form of applied current. Our device SET (HRS→LRS) and RESET (LRS→HRS) switching thresholds are around 800 mV and -750 mV, respectively, as it is shown in Fig. 2(a). For electro-forming a maximum sweep voltage range of 2.5 to 3.2 V and current compliance range 100 to 500 µA was used. The switching behavior is known to be caused by the formation and rupture of one or more filamentary paths through the oxide layer between Top Electrode (TE) and Bottom Electrode (BE) [27], [36]. This is shown in Fig. 1 Switching sequence (1-4) is shown in Fig. 2(a) and the device was initially in its HRS. Electrical characterization and measurement data was gathered with Keithley 4200 Semiconductor Characterization System. It is worths noting that electo-forming and its impact on spatio-temporal characteristics of oxygen vacancy profile is an interesting topic which is outside the scope of this paper and underpins further investigation.

Using standard photolithography we designed and fabricated a stack of the following materials to implement our VCM ReRAM devices. A 20 nm Pt and its 5 nm Ti adhesion layer are deposited on a SiO$_2$/Si substrate as BE using electron-beam evaporation. An amorphous SrTiO$_3$, a-STO, (33 nm) film is subsequently sputtered through a shadow mask and in the next step, a 5 nm Pt as buffer metal layer is e-beam evaporated on the a-STO layer. Then, two layers of a-STO films were sputtered in different conditions; A 30 nm oxygen deficient (OD) a-STO layer on a normal 3 nm a-STO. Finally, a Pt/Ti (20 nm/10 nm) is formed by e-beam evaporated on the a-STO layer. Then, two layers of a-STO films were sputtered in different conditions; A 30 nm oxygen deficient (OD) a-STO layer on a normal 3 nm a-STO. Finally, a Pt/Ti (20 nm/10 nm) is formed by e-beam evaporation as TE. All deposition steps were processed at room temperature and a crossbar optical image and its material stack is shown in Fig. 2(b). The crossbar array consists of 8 columns of TEs and 6 rows of BEs. When a voltage below switching threshold (Fig. 2(a)'s inset), known as READ voltage, is applied to the TE, it produces a current that can be read-out from BE. Full details on fabrication process can be found in Refs. [27], [36]. ReRAM switching layer in our devices is an amorphous OD SrTiO$_{3-x}$ (a-STO), where $x$ represents the level of oxygen deficiency created by a combination of processes within
The material stack during fabrication and engineered by a detailed micro/nano-fabrication development recipe.

To highlight Fig. 3(a) shows one main device-to-device (D2D) variation of our VCM ReRAM HRS and LRS at different READ voltages. In this paper, we only use HRS. Measurements remark that HRS is widely distributed over a decade in the range of 100 kΩ to 1 MΩ. Fig. 3(b) demonstrates temperature dependence of the ReRAM cell. It shows thermal activation of current transport through the cells in the temperature range 275°C to 450°C K. Although measured resistance transition over multiple devices is substantial, the behavior suggests a trend that can be considered in our peripheral read-out circuitry for mPUF.

2.2 Circuit and Architecture

The proposed mPUF structure is shown in Fig. 4. The overall system architecture consists of multiple VCM ReRAM crossbars, two sense amplifiers and bit generators. The system accepts parallel streams of 64-bit inputs that each is called a challenge and produces 64-bit output that is called a response. Each challenge produces 1-bit response. Fig. 4(a) illustrates a modified StrongARM (mSAL) latch. We added transistors M₁₃, M₁₄ and M₁₅ to better control the flow of current when sensing is enabled using the signal, SenEn. The current mirror and control transistor in the left hand side and highlighted in red are serving dummy cells/arrays and are not part of the mSAL circuit and we discuss its effects on supply power signal-to-noise ratio (SNR) later in the paper. Original idea and full description of the sensing circuitry can be found in Refs. [37], [38]. The mSAL circuit consists of two identical parts, highlighted in green and blue that are competing to own the output, Vₓ and Vₚ. Assuming negligible mismatch between peer transistors (e.g. M₁ and M₂), the state of the latch should be identified by the mismatch between Iₚ and Iₚ. As Fig. 4(b) illustrates, these two currents are directly passing through a selection of multiple ReRAM devices which are all programmed in their HRS. Due to the randomly different oxygen vacancy profile of these devices, one of the currents will be higher than the other, which means voltages at nodes P and Q will not be identical. That causes an unbalance in the current that is drawn by M₁ and M₂ after a pre-charge mode (SenEn=0) that charged nodes P, Q, X and Y to V_DD. The unbalance will push the latch (transistors M₃₋₆) towards Vₓ=V_DD, Vₚ=0 or Vₓ=0, Vₚ=V_DD.

One of the most important systematic bias that needs to be mitigated is the offset generated as the result of mismatch between current mirror pairs, M₁₁ and M₁₂, and M₃₋₆ of the latch. It is known that in conventional StrongARM circuit, dominant contributors to the offset are M₁ and M₂ [37]. In this case, we need to extend that set to include M₁₁ and M₁₂. Due to the fact that our architecture uses only two mSAL circuits, as shown in Fig. 4(c), there are plenty of room for mitigating M₁₂ offset contribution. It is very well-known that such offset in a FET (field effective transistor) is the direct result of mismatch in threshold voltages which is the consequence of process variation. According to the renowned Pelgrom’s Law,

\[
\sigma_{V_T} \propto \frac{1}{\sqrt{WL}},
\]

where \( W \), \( L \) and \( \sigma_{V_T} \) representing length and width of transistor channel and standard deviation of threshold voltage mismatch, sampled from thousands of pairs [39], [40], to avoid creating a systematic bias in our CMOS, M₁₁, M₁₂ should be as large as possible.

In the proposed PUF, input challenge either directly or through a set of linear-feedback shift registers (LFSRs), which are not shown in Fig. 4(b) diagram, randomly activates 1, 2, 3, 4 or 5 columns out of \( M \) rows of each of the \( I_{P,Q,D} \) currents. In this paper, \( N=M=128 \), therefore, a massive pool of Challenge-Response-Pairs (CRPs) are expected as it is shown in Section 2. Other array characteristics such as sneak-current paths (array parasitic currents) are data and addressing pattern dependent, and hence, are included in our analysis but their individual role

Fig. 3: (a) Device-to-device (D2D) variation in HRS and LRS. State resistance variation of HRS and LRS are extracted from 58 devices at different READ voltages between 0.1 and 0.5 V. As Fig. 3(a)’s inset suggests, nonlinearity of I-V characteristics causes semi-exponential increase in HRS current with every 100 mV increase in voltage. Therefore, as READ voltage increases, \( R_{ON}/R_{OFF} \) ratio decreases. (b) Resistance systematic variation induced by temperature change from, near zero degree of Celsius, 275°C K, to 450°C K.
were not studied in this paper. Fig. 4(c) demonstrates that the input challenge (InC) is applied to two crossbar arrays A and B (CBA A and CBA B) and mSALs produce relevant output bits. For every operation, output bit of the first part, called Hidden Challenge (HiC) in this paper, influences selection of rows and columns in the second part. As its name suggests, it acts as a hidden challenge that participate in response bit generation and it could be multiple bits for different structures and requirements. While all parts are directly involved in response bit generation, the part highlighted in red, dummy, aim to confuse power consumption signal in order to reduce the adversarial chance in using side-channel power monitoring.

2.3 Operation

READ voltage of nrPUF operation is chosen from the set of READ voltages highlighted in Fig. 3. As our read-out is current based, we aim to choose the lowest READ voltage possible to guarantee no destruction to the stored state. Due to inherent variation of ReRAM crossbar arrays, conductances of cells are widely distributed and that variation is ultimately translated to read-out current. Selected output of ReRAM crossbars are set as:

\[ I_{row,i} = \sum_{k=1}^{CS} g_{i,j_k} V_{READ}, \]

where \( g_{i,j_k} \) denotes conductance of cell located at \((i,j_k)\) node, \(i\) represents a device row location selected by analog/current multiplexer (aMUX), \(j_k\) is a column location by decoder block and \(CS\) is total number of columns selected. The aMUX utilizes a group of transmission gates for passing analog current inputs to its output. For temperature considerations, a temperature sensing circuitry could be beneficial alongside Fig. 4(a). After read-out, current distribution is the root source of PUF uniqueness. In Section 2.1, we showed individual ReRAM cell resistance distribution, see Fig. 3(a). In this work, we fixed \( CS = 5 \). It utilizes a wider distribution than one or two column selection methods. Suppose \( I_1, I_2, \ldots, I_{CS} \) are \( CS \) number of independent random variables (a cell read-out current) with mean \( \mu_1, \mu_2, \ldots, \mu_{CS} \) and variance \( \sigma_1^2, \sigma_2^2, \ldots, \sigma_{CS}^2 \). Then the mean and variance of the linear combination \( I_{row} = \sum_{k=1}^{CS} I_k \) are defined as:

\[ \mu_{I_{row}} = \sum_{k=1}^{CS} \mu_k \]
respectively. This shows that $I_{row}$ distribution as well as its standard deviation increase with higher CS. This is shown in Fig. 5(a). Since nPUF deals with comparison of electrical characteristics (linear sum of CS number of cells’ read-out current), the wider variation distribution provides the advantage of reducing possibility that selected comparator objects are in indistinguishable range. The high CS method has another merit in that it increases the challenge space as well as prevents revealing of the PUF’s variation fingerprint to adversaries attempting to characterize the PUF. Column and row selection on CBA A is entirely driven by a $q$-bit challenge using decoder and aMUXs block, see Fig. 4(b) and (c).

A CMOS unit selects $2 \times l$ rows and each provides $I_{A,row}$, and performs $l$ pairs of current comparison in order to deliver $l$-bit HiC as an input of CBA B’s CMOS unit. In this work $l=1$, and hence two rows in each operation is selected. While column selection is based on $q$-bit challenge ideally through decoders and LFSRs, an internally generated $l$-bit HiC participates in selection of CBA B’s columns and rows in order to produce, $I_{B,row}$, and finally generates 1-bit final response for $n$PUF. The number of selection can be adjusted considering the size of ReRAM crossbar array and can be set as $\log_2 \left( \frac{M}{2} \right)$, where $M$ is the number of rows in CBA. Total number of CRPs ($N_{CRP}$) also depends on the size of ReRAM crossbar arrays and it can be estimated as:

$$N_{CRP} = \left( \frac{N}{CS} \right) \times \left( \frac{M}{2} \right) \times l,$$

(5)

where $M, N$ are the sizes of CBA ($M \times N$). It is worth recalling that CS is the number of selected columns and $l$ is the HiC bit length.

3 PERFORMANCE EVALUATION

3.1 Avalanche characteristic

A PUF should be a one-way function that ideally there is no link between its input and output. When this property is achieved, it becomes nearly impossible to guess challenge bits by observing corresponding response bits and vice versa [41]. CRPs should also be unrelated, so that knowing one CRP has no impact on predicting other unknown CRPs regardless of their similarity [42]. This can be better described as following:

1) Response bits should have similar probability over challenge space [43]. For each response bit, the probabilities of being “1” or “0” should likely to be equal, i.e, $P_{Prob}(r = 1) = P_{Prob}(r = 0) = 50\%$.

2) Response bit transition rate to a set of challenges with Hamming Distance (HD) = $i$ should be 50%, where $1 \leq i \leq q$ and $q$ is a length of a challenge. Consider $q$-bit reference challenge ($C_{Ref}$) and a challenge ($C_i$) with HD=1 from $C_{Ref}$. When $i \in \{1, \ldots, S\}$, all with HD=1 from $C_{Ref}$, we have a vector of size $S$ of responses to those challenges. To meet the strict avalanche criterion (SAC) requirement, $r_i \oplus r_{Ref}$, which represents whether a transition in $i^{th}$ response bit occurred compared to the reference response ($r_{Ref}$), should result in a balanced vector of $S$ responses. It means we should ideally observe a balanced (50%) number of “1”s and “0”s in the output vector. In other words, $P_{Prob}(r_S \oplus r_{Ref}=1)=50\%$ [44].
Although it is very difficult, if not impossible, to prove unclonability mathematically, literature has shown that some PUFs are predictable [34], [45]-[48]. For high immunity to these attacks, it is desirable to have the two properties mentioned above [14], [28]. In most PUFs, the first property may be obtained, but the second, avalanche behavior, is more difficult. This is particularly the case for linear Arb-PUF structure. The example utilizes sequence stages of four terminal switches with two inputs and two outputs. Each switch is controlled by a single bit which identifies the switch configuration. The fundamental idea is that, due to process variations, delays of an identical signal at the input arriving at two different output pins are slightly different. Every stage contains two multiplexers connecting inputs to outputs. In a low-throughput delay-based PUF architecture, independence among CRPs is hard to achieve. There exist attempts to design nonlinear PUF architectures and examples includes XOR PUF [14] and Feed-Forward Arb-PUFs (FF Arb-PUFs) [28], [29]. XORing in Arb-PUFs is a powerful method to randomize this irregular output to generate a balanced output. An XOR PUF consists of multiple Arb-PUFs and an XOR function which XORs the responses of Arb-PUFs. They show improvement on SAC after adding the XOR function [49]. Another example, FF Arb-PUFs, utilize one or few switch(es) that are independent of input. It means that feed-forward creates some hidden information and the PUF achieves a higher degree of complexity [29], [46].

In Fig. 5(c), a PUF with single crossbar array structure shows a biased output bit transition rate, and this is the particular case of low HD between row and column selections. Compared to single crossbar, the proposed \( nr \)PUF, dual crossbars, provides a significantly improved response bit stream balance and SAC.

### 3.2 Attacks

Possible attacks on PUFs are various both on software and hardware level [50]. For PUFs with limited number of CRPs, \( N_{CRP} \), such as SRAM-PUFs, it may be possible to characterize the entire structure by direct probing and/or side-channel power monitoring attack [51], [52].

It is also known that a high \( N_{CRP} \) makes model-building attacks possible more effective via machine learning analysis on large collection of output data. This immediately implies that PUFs with small throughputs will be less vulnerable to machine learning attacks. ReRAM-based PUFs may have the potential to mitigate these issues by providing adjustable throughput e.g. by adjusting sense amplifier, nanowire and overall parasitic capacitance at the output of each crossbar. Also, they adopt a random selection of a subset of memory cells and comparing the current passing through them in a total analog fashion [11], [53]. Using this method, a PUF with \( M \times N \) crossbar size obtains at least as \( N \) times as many challenges as RO-PUF with \( M \) number of RO stages [53].

### 3.2.1 Simple and differential power analysis attacks

One of effective security threat targeting system implementation of cryptographic algorithms is side-channel attacks. Power analysis has been effectively used against different sensitive items such as smart-card microprocessors [54], [55]. Differential Power Analysis (DPA) goal is to extract correlations between data and supply power fluctuations. Therefore, in systems that generating “1” and “0” in the output consume different current DPA will be an effective statistical tool that given enough traces is cable of extracting tiny correlations. Other power analysis techniques include correlation power analysis based on the Hamming distance model and partitioning power analysis [51], [56]-[59].

The proposed \( nr \)PUF is using differential current analysis as the means to generate output bit therefore therefore correlation between the total current consumption and output bit diminishes. Additionally, we have exploited dummy arrays (as explained in Section 2), in order to reduce any potential correlations even further. The relatively low-cost and effective performance of ReRAM technology offers the possibility of dummy array introduction to enable the capability of confusing power consumption pattern.

Power analysis attacks in general could be evaluated by signal-to-noise ratio (SNR) between the single-bit unit power consumption and the standard deviation of power leakage [59]. In \( nr \)PUF, we analyzed power consumption for generation of 2000 output bits. An input challenge dependent selection of 5 columns with 20 ReRAMs identifies the output bit, while one or more ReRAM on dummy arrays are randomly selected at the same time in order to achieve confusion. Due to random nature of selection of dummy arrays and devices involved in the process, invasive attacks such as laser cutting of interconnects would unlikely result in a functioning \( nr \)PUF without dummy devices.

Fig. 6 illustrates our SNR analysis result as a function of number of dummy devices involved in confusing power signal. As expected, the more the number of dummy devices are the lower SNR becomes and therefore it is possible to adjust such performance for different applications according to their sensitivity.

### 3.3 PUF metrics

We evaluated \( nr \)PUF against key PUF metrics in this part. Extensive circuit level Cadence simulations were followed up with rigorous Matlab analysis considering experimental data collected form a wide range of identical devices on same or different dies. Measured variations in current were fed into these simulations and devices were working under minimum READ voltage to be similar to experiments. There assumed noise and uncertainty on supply power line and existence of faulty devices (e.g. stuck-at-ON) in both crossbars. The following lists our considerations for analysis:
Fig. 6: Role of dummy ReRAMs in lowering Signal-to-Noise Ratio (SNR) in an attempt to make supply power signal unrecoverable and unrelatable to output bit generation. Number of dummy ReRAMs is directly relevant to the magnitude of $I_D$ in Fig. 4(a) and (b).

- There is 10% $3\sigma$ READ supply voltage variation at any READ voltages,
- A temperature fluctuation of $±10^6$ K at any working temperature,
- An undetectable current difference of $\Delta I=±20$ nA, where $\Delta I=I_{V1}−I_{V3}$,
- 90% of HRS programmed devices were successful, therefore, 10% of ReRAMs are assumed to be stuck-at-ON (in their LRS range, see Fig. 3(a)), and
- Measured ReRAM’s HRS variations have lognormal distribution, see Fig. 3(a). These data were imported into analytical analysis flow to evaluate $nr$ PUF.

3.3.1 Hamming Weight (HW) test

HW test calculates inter- and intra-PUF responses in order to detect bit bias toward “0” or “1”. HW tests include uniformity (UF) and bit-aliasing (BA). Average UF and BA results are shown in Fig. 4(a) and (b) and both are closely distributed near 50%.

Uniformity (UF) is an intra-response HW assessment to evaluate a balance of “0”s or “1”s in a response vector. Ideally, UF should show a perfect balance. UF is defined as:

$$UF = \frac{1}{n} \sum_{j=1}^{n} r_{i,j} \times 100\%,$$

where $r_{i,j}$ is $j^{th}$ bit of an $n$ bit response to $i^{th}$ challenge. In Fig. 4(a), red distribution curve represents the best-case UF of $nr$PUF when random challenges (zero or slightly larger than zero correlation between them) generate a response. It is closely distributed near to its ideal UF of 50%. The worst-case UF is when challenges are not random and have high similarities with HD$_{challenge} \leq 5$ considering a challenge length of 64-bit. Results shows the worst-case $nr$PUF, is normally distributed with $\mu$ of 47.28% and standard deviation of 11.09%. In contrast, UF of single crossbar structure is poorly centered and is rather uniformly distributed. This shows $nr$PUF could better satisfy desirable SAC behavior.

Bit-Aliasing (BA) is a measure that shows the degree of similarity across responses from different PUFs (inter-HW). Ideally, a PUF should avoid identical responses, hence, BA should be 50%. BA can be calculated as:

$$BA = \frac{1}{p} \sum_{i=1}^{p} r_{i,j} \times 100\%,$$

where $r_{i,j}$ is $j^{th}$ bit of an $n$ bit response from an $i^{th}$ PUF instance. It is shown that average BA of $nr$PUF is 47.48% with deviation of 5.03%.

3.3.2 Hamming Distance (HD) test

HD test calculates the HD of inter- and intra-PUF responses in order to assess how unique PUFs are. HD tests include uniqueness (UQ) and diffuseness (DF). Average UQ and DF results are shown in Fig. 7(c) and (d) and both are closely distributed near 50%.

Uniqueness (UQ) is an inter-PUF HD test and an indicator of the PUF’s information bits that can be extracted by evaluating a degree of difference between responses of different PUFs to identical challenges. Truly random PUF should achieve UQ close to the ideal value of 50%. Average UQ is defined as:

$$UQ = \frac{1}{(\binom{p}{2})} \sum_{i=1}^{p-1} \sum_{j=i+1}^{p} \frac{HD(R_i, R_j)}{n} \times 100\%,$$

where HD($R_i$, $R_j$) is the HD between $n$ bit responses to a challenge from a pair of $i^{th}$ and $j^{th}$ PUF instances.

Diffuseness (DF) is an intra-PUF HD measurement, is to analyze a degree of response difference from different sets of challenges applied to the same PUF. DF is defined as:

$$DF = \frac{1}{(\binom{c}{2})} \sum_{i=1}^{c-1} \sum_{j=i+1}^{c} \frac{HD(R_i, R_j)}{n} \times 100\%,$$

where HD($R_i$, $R_j$) is the HD between $n$ bit responses to a pair of $i^{th}$ and $j^{th}$ challenge from a PUF instance.

3.4 Reliability

PUFs are expected to demonstrate high reliability. Reliability shows PUF’s ability to reproduce same response to the same challenge over time and under significant spatio-temporal variations. In other words, it is defined as the probability that response bit $r_t$ that is generated at time $t$ to be reproduced at a $\Delta t$ later and $r_t = r_{t+\Delta t}$. An ideal PUF should provide 0% difference in its responses to identical challenges and this is represented by Bit
Fig. 7: nrPUF Performance evaluations. (a) Worst-case uniformity (UF) comparison of response bit-stream of a nrPUF and a single crossbar structure. Red curve shows ideal distribution for UF, and it is clear that nrPUF is closer to the ideal UF than single crossbar-based PUFs. nrPUF’s UF shows a well-balanced “0”s and “1”s in its response bit-stream. (b) nrPUF’s bit-aliasing is shown. Each bit of nrPUF responses are assessed by calculating BA over 1000 PUF instances. The result indicate a well-balanced ratio of “1”s and “0”s across responses. (c) Uniqueness (UQ) and (d) diffuseness (DI) of nrPUF are demonstrated under a number of extreme temporal and transient nature uncertainty, such as supply voltage, temperature and sensing margin fluctuations.

Error Rate (BER) definition below:

\[
BER = \frac{\frac{1}{2} \sum_{i=1}^{tr-1} \sum_{j=i+1}^{tr} \text{HD}(R_i, R_j)}{n} \times 100\%,
\]  

where \( \text{HD}(R_i, R_j) \) is the HD between responses to \( i^{th} \) and \( j^{th} \) application of a challenge to a PUF. Ideal reliability (RE) is 100% and is defined as:

\[
RE = 100\% - BER.
\]

Fig. 8: Bit Error Rate (BER) of nrPUF. (a) Reliability of nrPUF at a range of column number selection (CS) choices between 1 and 5 under supply voltage, temperature and sensing margin fluctuations. Reliability is significantly improved as CS increases. (b) Average BER over multiple nrPUF analysis is shown as a function of CS and mSAL error margin of \( \Delta I=\pm 10 \) to \( \pm 100 \) nA.

The reason for adopting a group of ReRAMs instead of a single device is to raise immunity against temporal variations. Although a single device comparison method has obvious advantages of consuming lower power, it has a poor reliability. When a PUF response stability is not guaranteed, the system requires an additional error correction module integrated with the PUF device and it increases costs, throughput and overall power consumption [66], [67].

Based on current distribution results, we evaluated reliability of nrPUF under different conditions. For each measurement set, we use 500 random challenges and each challenge is repeated for 50 trials in a PUF instance. Results clearly show the advantage of selecting multiple columns (CS=5) over one or two column(s) (CS=1 or 2) selection method. Scattered cross symbols in Fig. 8(a) represent average BER of 50 trials to 500 challenges. We assume SA margin for this work is 20 nA. Mean value of BER \( \mu_{BER} \), which is 3.45% for CS=1 reduces by increasing CS. This is 2.39%, 1.87%, 1.61% and 1.33% for CS=2, 3, 4 and 5, respectively. As CS and mSAL’s sensitivity increases, lower BER could be achieved (see Fig. 8(b)). Table 1 presents a comparison between different proposed ReRAM PUFs. As the Table suggests, the proposed nrPUF could potentially achieve a closer performance metrics to the ideal, while all cited works have used similar mix of experimental-simulation analysis.
TABLE 1: Comparison of crossbar PUFs.

| Reference     | NanoPPUF | M-PUF | MemristorPUF | mrSPUF | CPR-PUF | nrtPUF |
|---------------|----------|-------|--------------|--------|---------|--------|
| Crossbar      | 4×4      | 8     | 1MB cells    | 128×128| 1024×1024| 2×128×128|
| Minimum cell size | 6F²      | –     | 4F²         | 4F²    | 4F²     | 2×4F² |
| Memory state  | LRS/HRS  | LRS/HRS | –          | LRS    | HRS     | HRS    |
| Uniqueness (%)| 49%      | 49.85 | ~48/50/55    | 50.07  | ~49.95  | 49.85  |
| Reliability (%)| –        | –     | –           | 92.5   | ~98     | 98.67  |
| Diffuseness (%)| 49%      | –     | –           | 49.96  | –       | 49.86  |
| Uniformity (%)| 49%      | 49.99 | –           | 50.76  | –       | 47.28  |
| Bit-aliasing (%)| –       | 49.99 | –           | 49.99  | –       | 47.48  |
| CRPs calculation | –      | –     | –           | $\frac{N \times (M_i)^i}{2} \times (\frac{M-i}{2})$ | $\frac{N \times (M_i)^i}{2} \times (\frac{M-i}{2}) \times \log_2 \left( \frac{M}{2} \right)$ |
| Total CRPs$^1$ | –       | –     | –           | $\sim 3.7 \times 10^{18}$ | $\sim 10^6$ | $\sim 2.7 \times 10^{13}$ |

BC: Best-case
F: ReRAM feature size
Typ: Typical-case
WC: Worst-case
†: Calculated for $N=M=128$ and $i=5$ for mrSPUF
– Not mentioned

Excluding peripheral circuitry contribution, experimentally measured worst-case power consumption per ReRAM per response bit considering READ voltage of 100 mV results power consumptions as low as 100 nW. While simple estimation of power consumption based on this figure will be far from realistic total power consumption, specially by mSAL, it raises confidence in applicability of nrtPUF. It is worth noting ReRAM arrays consume almost zero power while on stand-by. Data retention at the mentioned READ voltages has also been guaranteed for years at 85° C. Unlike start-up issues with SRAM-PUF [68], we believe nrtPUF should provide a more reliable power-up phase thanks to their non-volatility and long data retention. According to our experimental observations of fastest pulse measurements using Keithley 4225-PMU, peripheral circuitry would dominate nrtPUF throughput, which can be designed to have a range of operational speeds including slow readouts as suggested in Ref. [69].

4 Conclusion

In summary, we present a novel nrtPUF based on measured data collected from a range of ReRAM devices on one or multiple dies, fabricated under identical conditions. nrtPUF utilizes a relatively simple ReRAM crossbar structure, minimizing its design phase to nanofabrication masks design. To improve unpredictability, nrtPUF utilizes two crossbars with a hidden challenge passing from the first part to the second. We demonstrated that such feature could improve avalanche behavior and uniformity while maintaining other performance metrics close to ideal. Various PUF performance metrics have been analyzed. A uniformity of 47.28%, bit-aliasing of 47.48%, diffuseness of 49.86% and uniqueness of 49.85% are found. The PUF’s multiple column selection flexibility also offered a reliability of 98.67% under extreme process, voltage, temperature and sensing margin fluctuations. Additionally, we utilized a set of dummy ReRAMs to reduce nrtPUF’s supply power SNR, although our read-out circuitry resulted in no meaningful relationship between power consumption and output bit generation of “1” or “0”. ReRAM devices in nrtPUF are programmed in their HRS to (1) take advantage of highly spatially driven variations in HRS and (2) reduces power consumption. Crossbar aspects such as resistance-pattern dependent sneak current paths (parasitic current via neighboring cells) are also intrinsically contributing to nrtPUF performance but their specific role in nrtPUF operation is currently under investigation.

References

[1] S. Choi, P. Sheridan, and W. D. Lu, “Data clustering using memristor networks,” *Scientific Reports*, vol. 5, 2015.
[2] R. Legenstein, “Computer science: Nanoscale connections for brain-like circuits,” *Nature*, vol. 521, no. 7550, pp. 37–38, 2015.
[3] M. Prezioso, F. Merrikh-Bayat, B. Hoskins, G. Adam, K. K. Likharev, and D. B. Strukov, “Training and operation of an integrated neuromorphic network based on metal-oxide memristors,” *Nature*, vol. 521, no. 7550, pp. 61–64, 2015.
[4] R. Waser and M. Aono, “Nanoionics-based resistive switching memories,” *Nature Materials*, vol. 6, no. 11, pp. 833–840, 2007.
[5] H.-S. P. Wong and S. Salahuddin, “Memory leads the way to better computing,” *Nature Nanotechnology*, vol. 10, no. 3, pp. 191–194, 2015.
[6] P. W. Coteus, J. U. Knickerbocker, C. H. Lam, and Y. A. Vlasov, “Technologies for exascale systems,” *IBM Journal of Research and Development*, vol. 55, no. 5, pp. 14–1, 2011.
[7] I. Valov, E. Linn, S. Tappertzohen, S. Schmelzer, J. Van den Hurk, F. Lentz, and R. Waser, “Nanobatteries in redox-based resistive switches require extension of memristor theory,” *Nature Communications*, vol. 4, p. 1771, 2013.
[8] R. Waser, R. Dittmann, G. Staiko, and K. Szot, “Redox-based resistive switching memories—nanionionic mechanisms, prospects, and challenges,” *Advanced Materials*, vol. 21, no. 25-26, pp. 2632–2663, 2009.
[9] D. B. Strukov, “Endurance-write speed tradeoffs in nonvolatile memories,” *Applied Physics A*, vol. 122, no. 4, pp. 1–4, 2016.
[50] M. Roel, “Physically unclonable functions: Constructions, properties and applications,” Ph.D. dissertation, Ph. D. thesis, Dissertation, University of KU Leuven, 2012.

[51] C. Helfmeier, C. Boit, D. Nedospasov, and J.-P. Seifert, “Cloning physically unclonable functions,” in IEEE International Symposium on Hardware-Oriented Security and Trust–HOST, 2013, pp. 1–6.

[52] U. Rührmair, H. Busch, and S. Katzenbeisser, “Strong PUFs: models, constructions, and security proofs,” in Towards Hardware-Intrinsic Security. Springer, 2010, pp. 79–96.

[53] L. Zhang, X. Fong, C.-H. Chang, Z. H. Kong, and K. Roy, “Optimizing emerging nonvolatile memories for dual-mode applications: Data storage and key generator,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 34, no. 7, pp. 1176–1187, 2015.

[54] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, “Introduction to differential power analysis,” Journal of Cryptographic Engineering, vol. 1, no. 1, pp. 5–27, 2011.

[55] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, “Examining smart-card security under the threat of power analysis attacks,” IEEE Transactions on Computers, vol. 51, no. 5, pp. 541–552, 2002.

[56] E. Brier, C. Clavier, and F. Olivier, “Correlation power analysis with a leakage model,” in International Workshop on Cryptographic Hardware and Embedded Systems, 2004, pp. 16–29.

[57] Y. Fei, Q. Luo, and A. A. Ding, “A statistical model for DPA with novel algorithmic confusion analysis,” in International Workshop on Cryptographic Hardware and Embedded Systems, 2012, pp. 233–250.

[58] Q. Luo and Y. Fei, “Algorithmic collision analysis for evaluating cryptographic systems and side-channel attacks,” in IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), 2011, pp. 75–80.

[59] Y. Fei, A. A. Ding, J. Lao, and L. Zhang, “A statistics-based fundamental model for side-channel attack analysis.” IACR Cryptology ePrint Archive, vol. 2014, p. 152, 2014.

[60] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, “Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs,” in IEEE International Conference on Reconfigurable Computing and FPGAs (ReConFig), 2010, pp. 298–303.

[61] J. Rajendran, G. S. Rose, R. Karri, and M. Potkonjak, “NANO-PUF: A memristor-based security primitive,” in IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2012, pp. 84–87.

[62] G. S. Rose, N. McDonald, L.-K. Yan, and B. Wysocki, “A write-time based memristive PUF for hardware security applications,” in IEEE/ACM International Conference on Computer-Aided Design (ICCAD), 2013, pp. 830–833.

[63] P. Koeberl, U. Kocabas , and A.-R. Sadeghi, “Memristor PUFs: a new generation of memory-based physically unclonable functions,” in Proceedings of the Conference on Design, Automation and Test in Europe, 2013, pp. 428–431.

[64] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, “Memristive crypto primitive for building highly secure physical unclonable functions,” Scientific Reports, vol. 5, 2015.

[65] ——, “mrPUF: A novel memristive device based physical unclonable function,” in Applied Cryptography and Network Security, 2015, pp. 595–615.

[66] M. D. Yu and S. Devadas, “Secure and robust error correction for physical unclonable functions,” IEEE Design Test of Computers, vol. 27, no. 1, pp. 48–65, 2010.

[67] Y. Oren, A.-R. Sadeghi, and C. Wachsmann, “On the effectiveness of the remanence decay side-channel to clone memory-based PUFs,” in International Workshop on Cryptographic Hardware and Embedded Systems, 2013, pp. 107–125.

[68] M. Cortez, A. Dargar, S. Hamdioui, and G.-J. Schrijen, “Modeling SRAM start-up behavior for physical unclonable functions,” in 2012 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2012, pp. 1–6.

[69] U. Rührmair, C. Jaeger, M. Bator, M. Stutzmann, P. Lugli, and G. Csaba, “Applications of high-capacity crossbar memories in cryptography,” IEEE Transactions on Nanotechnology, vol. 10, no. 3, pp. 489–498, 2011.