A Physical Unclonable Function with Redox-based Nanoionic Resistive Memory

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

Abstract—Emerging non-volatile reduction-oxidation (redox)-based resistive switching memories (ReRAMs) exhibit a unique set of characteristics that make them promising candidates for the next generation of low-cost, low-power, tiny and secure physical unclonable functions (PUFs). Their underlying stochastic ionic conduction behavior, intrinsic nonlinear current-voltage characteristics and their well known nano-fabrication process variability might normally be considered disadvantageous ReRAM features. However, using a combination of a novel architecture and special peripheral circuitry this paper exploits these non-idealities in a physical one-way function, nonlinear resistive PUF, potentially applicable to a variety of cyber-physical security applications. We experimentally verify the performance of valence change mechanism (VCM)-based ReRAM in nano-fabricated crossbar arrays across multiple dies and runs. In addition to supporting a massive pool of challenge-response pairs (CRPs), using a combination of experiment and simulation our proposed PUF exhibits a reliability of 98.67%, a uniqueness of 49.85%, a diffuseness of 49.85%, a uniformity of 47.38%, and a bit-aliasing of 47.48%.

Index Terms—Physical unclonable function, redox-based resistive switching memory.

I. INTRODUCTION

The 19th century cryptographer, Auguste Kerckhoffs stated, "...a system should remain secure even if everything about the system, except the secret key, is public knowledge." [1], a principle still adhered to by a majority of modern cryptosystems. Physical unclonable functions (PUFs) fundamentally fulfill this principle by removing the ability of adversaries to extract secrets stored in non-volatile memories (NVMs) while leaving the remaining system features as public knowledge [2-5]. Secrets in a PUF are hidden in the randomness of its physical implementation (e.g. the silicon fabrication process) making it extremely difficult, if not impossible to discover them using the types of physical attacks commonly used for extracting keys from NVMs. Hence, the basic idea of a PUF is to take advantage of otherwise undesirable manufacturing non-idealities to create a physical system that is extremely hard to copy even if it is fabricated using identical processes, facilities and materials [2, 3, 6].

Various materials, systems and technologies have been considered as a source of uncontrollable randomness for PUFs. CMOS (complementary metal-oxide-semiconductor) PUF models have already exploited non-idealities such as variations in dimensions, random dopant fluctuations and line-edge roughness that are unique to each circuit to encode secret information [2, 7-12]. While this technology has spawned many potential security solutions, for example ring oscillator PUFs (RO-PUFs), arbiter PUFs (Arb-PUFs) and SRAM PUFs, the search is still on for PUFs that are highly secure, cheap, small and energy-efficient [2, 13-18].

Recently, emerging solid-state memories have drawn significant attention due to their potential for lower power and cost. Of these, redox-based resistive memories (ReRAMs) are one of the most promising for conventional and unconventional information processing as well as for memory applications [19-21]. ReRAMs also offer a number of desirable device characteristics for constructing PUFs:

- They can achieve ultra-high information density in simple nano-crossbar architectures [22]. For instance, they can be fabricated in much denser arrays than SRAM configurations employed in SRAM PUFs [23].
- They provide several unique sources of non-idealities for constructing PUF primitives. One unique feature that can be considered as exclusive to the broader family of valence change memories (VCM), electrochemical metallization memories (ECM) and, potentially, phase change memories (PCM) is their random nano-conductive ionic filament patterns across devices and variable switching cycles of a given device.
- The randomly varying oxygen vacancy profile from device-to-device (D2D) in VCM ReRAMs provides another dimension for non-idealities that can be exploited for NVM-based PUFs.
- ReRAMs offer a potentially lower additional volume fabrication cost compared to other types of emerging NVMs and allows the use of a range of materials.
- ReRAM fabrication processes can be seamlessly integrated conventional CMOS processing [24-29].

In this work, we propose a novel PUF architecture based
on non-volatile ReRAM crossbar arrays (CBAs). The main contributions of this work are as follows:

- We introduce a new PUF primitive, a nonlinear ReRAM-based PUF (nPUF) architecture (Section II-B), capable of being realized at nano-scale dimensions and yielding a large number of response bits with respect to the overall size of the nPUF. As part of this architecture, we propose the concept of employing dummy ReRAMs to potentially strengthen nPUF against power monitoring side-channel attacks (Section IV-B).
- We fabricate and experimentally evaluate ReRAM CBAs (Section II-A) to validate our proposed nPUF.
- We present extensive evaluations of the ReRAM-based PUF architecture including the evaluation of key PUF performance metrics based on detailed experimental analysis that are fed into Cadence simulations (Section III and IV).

The remainder of the paper is organized as follows: Section II discusses characteristics of ReRAMs and proposes the nPUF. Experimental results of ReRAMs and the nPUF architecture and operation are also included in this section. Section III analyses nPUF performance using widely used measure for evaluating PUF primitives, including avalanche characteristics. Section IV presents a comparison with other nano PUF primitives, a discussion on possible vulnerabilities and summarizes the paper, while Section V concludes the article.

II. NONLINEAR RESISTIVE PUF

In this section, valency change mechanism (VCM)-based ReRAMs are investigated as a primary source of randomness in a PUF design. Fig. 1(a) and (b), show direct evidence of oxygen vacancy profiles in our devices (something that is true for all ReRAMs) [30]. This pattern varies significantly between devices. An important aspect of this spatio-temporal random oxygen vacancy profile in ReRAMs is that once programming is finished, the profile stays fixed under the condition of zero or small magnitudes of energy delivered to the VCM-based ReRAMs.

The temporal aspects of this nano-filament pattern are even more profound when the device is switching or is in its low resistance state (LRS). When a filament becomes the main path of conducting current between electrodes, the conductance of ReRAMs in LRSs is almost independent of device contact sizes and their variations. On the other hand, in the high resistance state (HRS) the nano-filament pattern is fixed, unique to each device and the filament heights are much less than those of ReRAMs in their LRS (see Fig. 1(b)). Further, variations due to dimensional and line-edge roughness (LER) are much more evident when the device in its HRS. As a result, this paper considers the devices only in their HRS for two reasons: (1) using HRS devices can reduce total power consumption and (2) the overall combination of oxygen vacancy profile, dimensional and LER variations means that spatial variation is stronger when it is in its HRS. It is also 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.

A. Electrical Properties of ReRAM

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 were deposited on a SiO2/Si substrate as the bottom electrode (BE) using electron-beam evaporation. An amorphous SrTiO3, α-STO, (33 nm) film was subsequently sputtered through a shadow mask and in the next step, a 5 nm Pt buffer metal layer was e-beam evaporated on the α-STO layer. Then, two successive layers of α-STO films were sputtered: firstly a normal 3 nm α-STO followed by a 30 nm oxygen deficient (OD) α-STO layer.

The ReRAM switching layer in our devices is an amorphous OD SrTiO3−x (α-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.

Finally, a Pt/Ti (20 nm/10 nm) is formed by e-beam evaporation as top electrode (TE). All deposition steps were processed at room temperature and a crossbar optical image and its material stack is shown in Fig. 2(a). The CBA consists of 8 columns of TE and 6 rows of BEs. Full details on fabrication process can be found in Refs. [30, 31].
The measured signature bipolar switching behavior of our VCM ReRAM devices at room temperature is depicted in Fig. 2(b). Device switching characteristics emerge when an irreversible electro-forming step is completed. This 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 sufficient energy is delivered to the device in the form of applied current. Our device SET (HRS→LRS) and RESET (LRS→HRS) switching thresholds are around 0.8 V and -0.75 V, respectively, as it is shown in Fig. 2(b). For electro-forming, a maximum sweep voltage range of 2.5 to 3.2 V and current compliance range 100 μA 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 the TE and BE [30, 31]. The switching sequence (1→4) is shown in Fig. 2(b) where the device was initially in its HRS. When a voltage below switching threshold (Fig. 2(b)’s inset), known as READ voltage, is applied to the TE, it produces a current that can be read from the BE.

The I–V nonlinearity is highly correlated to the applied bias and the state of the devices. It is also known that the nonlinearity strongly depends on the exponential ionic drift occurring as the result of applying external current or voltage stimulation [30–32]. An experimental demonstration of the conductive paths formed in our fabricated devices is shown in Fig. 1(a) and (b). The I–V nonlinearity of these devices can be used as a source of randomness in a ReRAM CBA [23] and is already known to enable realization of purely passive CBAs [33]. It is also known that higher nonlinearities minimize sneak-path current (i.e., the array’s data dependent parasitic currents) and hence reduce the pressure on CBA design parameters such as their sizes [33, 34]. We have included sneak-paths in our array analysis but their individual roles are not studied in this paper. It is also important to note that the impact of higher parasitic currents, where the current is passing through more than one element other than the main signal path, can be reduced significantly by careful circuit design. In this work we achieve this using differential current read-out and a high sensitivity modified strongARM latch (mSAL) in Fig. 4(b) in the read path.

Fig. 3(a) shows one main source of device to device variation in our VCM ReRAM in both their HRS and LRS at different READ voltages.

Electrical measurements and characterization of our fabricated cells were undertaken using a Keithley 4225-PMU Semiconductor Characterization System. The measurements indicate that the resistance values in the HRS are widely distributed over a decade in the range of 100 kΩ to 1 MΩ. Our study across a number of arrays and multiple rounds of fabrication using identical recipes has shown no evidence of a conductance gradient in any direction and hence we have observed no spatial bias associated with these arrays. The measured variation in resistance with temperature in these
cells, shown in Fig. 3(b), is also very large, exhibiting a greater than $\times 10$ change over the range 275$^\circ$ K to 450$^\circ$ K. Although a substantial temperature dependent resistance change was measured over multiple devices, the behavior suggests a trend that can be taken into account in our peripheral read-out circuitry for the nPUF.

As a final observation here, it is worth noting that electroforming and its impact on the spatio-temporal characteristics of the oxygen vacancy profile of an interesting topic in itself that, while outside the scope of this paper, would warrant further investigation.

B. Circuit and Architecture

The proposed nPUF 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 inputs (called a challenge), and produces a corresponding 61-bit output stream (called a response). As Fig. 4(a) illustrates, analog multiplexers accepting subsets of input challenge (InC) to select columns and rows, thereby activating multiple ReRAM cells.

The multiplexer circuits employ a group of transmission (pass-) gates to pass row current or READ voltage. These multiplexers are also capable of grounding or floating unselected rows and columns. An input challenge identifies which columns and rows and how many of them in which combination are selected. In the proposed PUF, therefore, InC activates a particular number of columns (CS) out of N total columns and exactly two rows out of M rows for each of the $I_{F-Q}$ currents. $I_{F-Q}$ are the results of ReRAM selections by InC, whereas $I_D$ is caused by dummy cells selected by an independent random number generator. In this paper, $M=128$, therefore, a massive pool of Challenge-Response-Pairs (CRPs) will be available, as is shown in Section II-C and Table I.

Note that ReRAM devices are all programmed in their HRS for the proposed nPUF as described in Section II-A. Due to the randomly different oxygen vacancy profile of these devices, one of the currents will be higher than the others, which means currents through nodes P, Q, and D (IP, IQ and IN) will not be identical in Fig. 4(a). As Fig. 4(b) illustrates, IP and IQ are connected to a modified strong ARM latch (mSAL) through current mirrors (CM) with gain of 1, while ID represents dummy cells current which does not contribute to response bit generation process, but to the total power consumption. The original idea and full description of the sensing circuitry can be found in Refs. [35, 36]. The mSAL circuit consists of two identical parts, highlighted in blue and green, which are competing to generate the output, Vx and Vy. Assuming negligible mismatch between peer transistors (e.g., M1 and M2), the state of the latch will be determined by the mismatch between IP and IQ.

A difference in IP and IQ causes an imbalance in the current that is drawn by M1 and M2 after the pre-charge period (SenEn=0) during which nodes P, Q, X and Y are charged to $V_{DD}$. The imbalance will push the latch (transistors M3-e) towards $V_X=V_{DD}$, $V_Y=0$ or $V_X=0$, $V_Y=V_{DD}$. Transistors M13, M14 and M15 have been included to better control the flow of current when sensing is enabled using the signal, SenEn.

One of the most important systematic biases that needs to be mitigated is the offset generated as a result of the mismatch between the current mirror pairs, M1,11 and M2,12, and M3,9 within the latch. It is known that in the conventional StrongARM circuit, the dominant contributors to the offset are M1 and M2 [35]. 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 is plenty of room for mitigating the M1,2 offset contribution. It is 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 well
known Pelgrom’s Law:
\[ \sigma_{\Delta V_T} \propto \frac{1}{\sqrt{W \cdot L}} \]

where \(W, L\) are the width and length of transistor channel and \(\sigma_{\Delta V_T}\) represents the standard deviation of the threshold voltage mismatch, sampled from thousands of pairs [37, 38]. To avoid creating a systematic bias in our CMOS circuits, \(M_{1,1,1,2,12}\) should be as large as possible.

As shown in Fig. 4(c), the result of the imbalance of part A (highlighted in gray), which is the hidden challenge (HiC) in this paper, influences the selections of rows and columns in part D (highlighted in yellow). As its name suggests, the HiC is the internally generated challenge, which we call it hidden challenge. It is fed to CBA B to generate a response. In this paper, the total 64-bit challenge contributes to operating the CBA B. Depending on the particular structure and system requirements, the challenge for CBA B can be entirely hidden or be partially derived from a the main InC.

While all parts are directly involved in the generation of the response bits, the dummy part highlighted in red aims to confuse the power consumption signal to reduce the chances of an attack using side-channel power monitoring. We discuss its effects on supply power signal-to-noise ratio (SNR) later in the paper (Section IV-B).

C. Operation

The READ voltage of the nPUF 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 possible READ voltage to guarantee no destruction to the stored state. Due to inherent variations of ReRAM devices in a CBA, the conductance of its cells are widely distributed and this variation is ultimately translated to read-out current. The output of selected ReRAMs is given by:
\[ I_i = \sum_{k=1}^{CS} g_{i,j_k} V_{READ}, \]

where \(g_{i,j_k}\) denotes the conductance of the cell located at node \((i,j_k)\), \(i\) represents a device row location selected by the current MUX, \(j_k\) is a similarly selected column location and \(CS\) is the total number of selected columns. In this work, we fixed \(CS = 5\), which increases the current output distribution compared to choosing values of (say) one or two. We can start the analysis by assuming that \(I_1, I_2, \ldots, I_{CS}\) form a total of \(CS\) independent random variables\(^1\) (i.e., cell read-out currents) 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:

\[ \mu_{I_{row}} = \sum_{k=1}^{CS} \mu_k \]

and

\[ \sigma_{I_{row}}^2 = \sum_{k=1}^{CS} \sigma_k^2, \]

respectively. This shows that the \(I_{row}\) distribution as well as its standard deviation increases with higher \(CS\). Since nPUF deals with a comparison of electrical characteristics (i.e., the linear sum of the read-out current from \(CS\) cells), the wider variation distribution provides the advantage of reducing the possibility that selected comparator objects are placed in an indistinguishable range. Using higher values of \(CS\) has further advantages in that it increases the challenge space while preventing the PUF’s variation fingerprint from being revealed to adversaries attempting to characterize the PUF. Although a single device method \((CS = 1)\) has obvious advantages of consuming lower power, adopting a group of ReRAMs raises immunity against temporal variation, which will be discussed in Section III-B. Therefore, setting \(CS = 5\) represents a reasonable compromise between MUX design complexity and total power consumption.

Column and row selection on CBA A is entirely driven by a \(q\)-bit challenge using analog multiplexers, via an array of transistor pass-gates (see Fig. 4(a)). Column and row selection in CBA B is also driven by almost the same peripheral circuitry. The only difference is the use of a linear-feedback shift register (LFSR) that accepts an internal bit, generated by CBA A output, to generate \(q\)-bit HiC that is applied to CBA B in order to generate 1-bit of final response for nPUF. This nonlinear structure of two concatenated CBAs reduces a direct

\^1This assumption is substantiated by experiments.

relationship between challenges and responses. The merits of nPUF’s nonlinear structure is evaluated by comparison with single crossbar method in Section III and discussed in Section IV B. The single crossbar method is highlighted in gray in Fig. 4(e), and referred to as the single crossbar in this paper.

The number of selections can be adjusted considering the size of ReRAM CBA and can be set as $\log_2\left(\binom{M}{2}\right)$, where $M$ is the number of rows in the CBA. The total number of CRPs ($N_{CRP}$) also depends on the size of ReRAM CBAs and can be estimated as:

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

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.

III. PERFORMANCE EVALUATION

We evaluated our proposed nPUF against key PUF metrics. Circuit-level simulations in Cadence® were followed by Matlab analysis considering experimental data collected from a wide range of ReRAM devices on the same or on different dies. Circuit simulation confirms response bit generation with a power supply voltage at 1 V and temperature variation from -25°C to 125°C. The measured variations in current were fed into these simulations and devices were operated under minimum READ voltage to be similar to our experiments. Noise and uncertainty were assumed to exist on supply power line as well as faulty devices (e.g. stuck-at-ON) in both CBAs. The following lists our considerations for analysis:

- There is 10% 3σ READ supply voltage variation at any READ voltages,
- A temperature fluctuation of $\pm 10^\circ K$ at any working temperature,
- An unacceptable current difference of $\Delta I = 20$ nA. where $\Delta I = I_{p} - I_{Q}$,
- 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 log-normal distribution, see Fig. 3(a). These data were imported into the analytical analysis flow to evaluate the nPUF.

We use the following notations and definitions for the nPUF evaluation:

- $p$ Number of PUF instances.
- $n$ Number of response bits.
- $tr$ Number of trials on the same PUF instance.
- $r_{ij}$ $j^{th}$ bit of $i^{th}$ response.
- $c$ Number of challenges.

Key PUF evaluation metrics include uniqueness, difficulty, bit-aliasing, uniformity, and reliability (Fig. 3). More detailed definitions of these evaluation metrics can be found in refs. [14, 39]. The first four are measures of stochasticity and quality of randomness in PUF(s), while reliability measures the robustness of a PUF against spatio-temporal variation.

Figure 6. nPUF performance evaluations. (a) Worst-case uniformity (UF) comparison of a nPUF and a single crossbar method. (b) Bit-aliasing (BA) of nPUF’s.

A. Hamming Weight (HW) Measures

The HW test calculates inter- and intra-PUF responses in order to detect bit bias toward “0” or “1” and includes measures of uniformity and bit-aliasing. The average uniformity and bit-aliasing results are shown in Fig. 6(a) and (b) and both are closely distributed near 50%.

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

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

where $r_{ij}$ is the $j^{th}$ bit of an $n$ bit response to the $i^{th}$ challenge. In Fig. 6(a), red distribution curve represents the best-case UF of nPUF. We refer to the red curve as the best-case UF because it is closely distributed around 50%. The red curve is calculated from the responses of the nPUFs to a random challenge set. To evaluate nPUF’s design strength, we compare the worst-case UF of nPUF to the single crossbar organization. In this paper, the worst-case UF is calculated using responses to the challenge set which has challenges only with HD$\text{\text{challenge}} \leq 5$. Note that total response length in the nPUF is 64. The results shows the worst-case nPUF is normally distributed with $\mu$ of 47.28% and standard deviation of 11.09%. In contrast, the worst-case UF of a single crossbar is poorly centered and is rather uniformly distributed.

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

$$BA = \frac{1}{p} \sum_{i=1}^{p} r_{ij} \times 100\%,$$
where $r_{ij}$ is the $j$th bit of an $n$ bit response from an $i$th PUF instance. Each bit of $n$PUF responses is assessed by calculating BA over 1000 PUF instances. It can be seen that average BA of the $n$PUF is 47.48% with a deviation of 5.03%.

**B. Hamming Distance (HD) Measures**

The HD test calculates the HD of inter- and intra-PUF responses in order to assess how unique PUFs are. HD tests include uniqueness and diffuseness. The average uniqueness and diffuseness results are shown in Fig. 7(a) and (b) 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 differences 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:

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

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, that analyzes a degree of response differences from different sets of challenges applied to the same PUF [14]. DF is defined as:

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

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.

**Reliability (RE):** shows the PUF’s ability to reproduce the same response to the same challenge under spatio-temporal variations. In other words, it is defined as the probability that a response bit, $r_{ij}$ (generated at time $t$), can be reproduced at a time $\Delta t$ later. An ideal PUF should provide 0% difference in its responses to identical challenges and this is represented by bit error rate (BER) definition below:

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

where $HD(R_i, R_j)$ is the HD between responses to $i$th and $j$th application of a challenge. Ideal RE is 100% and is defined as:

$$RE = 100\% - BER.$$

When the reliability of a PUF response is not guaranteed, the system requires an additional error correction module integrated with the PUF device, which increases costs and overall power consumption [40, 41].

Based on the current distribution results, we evaluated RE of $n$PUF under supply voltage, temperature and sensing margin fluctuations. For each measurement set, 500 random challenges were applied and each challenge repeated for 50 trials of a PUF instance. The results in Fig. 8 clearly show the advantage of selecting multiple columns ($CS = 5$) over selecting just one or two column(s) ($CS = 1$ or 2). For example, assuming the current sensing margin is 20 nA in Fig. 8, the mean value of BER is 3.45% for $CS = 1$. The BER significantly reduces as $CS$ is increased, exhibiting values of 2.39%, 1.87%, 1.61% and 1.33% for $CS = 2$, 3, 4 and 5, respectively at this sensing margin. It can also be seen that the average BER decreases steeply as the sensing margin reduces or, put another way, as the mSAL’s sensitivity increases. This implies that even lower BER could be achieved by further increasing the sensitivity of the mSAL.

**C. Avalanche characteristics**

The avalanche characteristic, in cryptography, is the desirable property where a slight change in input (for example, flipping a single bit) results the significant as well as unpredictable changes in output (for example, half the output bits flip). When this property is achieved in PUF, each CRP is unrelated, so that knowing one CRP has no impact on predicting other unknown CRPs regardless of their similarity [42].

Although it is very difficult, if not impossible, to analytically prove unclonability, it has been shown that some PUFs are predictable [50-54]. For high immunity to these attacks, avalanche behaviour is required, however difficult it might be to achieve [2, 7]. This is particularly the case for the linear Arb-PUF structure. In a low-throughput delay-based PUF architecture like Arb-PUF, independence among CRPs is hard to achieve. Attempts have already been made to design
Table I: Comparison of ReRAM CBA-based PUFs.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Crossbar</td>
<td>4X4</td>
<td>8 bits</td>
<td>1MB cells</td>
<td>128 x 128</td>
<td>1024 x 1024</td>
<td>256 x 256</td>
<td>2 x 128 x 128</td>
</tr>
<tr>
<td>Min. cell size</td>
<td>6F²</td>
<td></td>
<td>4F²</td>
<td>4F²</td>
<td>4F²</td>
<td>4F²</td>
<td>2 x 4F²</td>
</tr>
<tr>
<td>Memory state</td>
<td>LRS/IRRS</td>
<td>LRS/IRRS</td>
<td>LRS</td>
<td>LRS</td>
<td>LRS/IRRS</td>
<td>LRS/IRRS</td>
<td>LRS/IRRS</td>
</tr>
<tr>
<td>Uniqueness (%)</td>
<td>49</td>
<td>49.85</td>
<td>~48/50/55</td>
<td>50.07</td>
<td>49.95</td>
<td>46.2</td>
<td>49.85</td>
</tr>
<tr>
<td>Reliability (%)</td>
<td>~</td>
<td>~</td>
<td>~92.5 (WC)</td>
<td>~98</td>
<td>83.3 (WC)</td>
<td>98.67</td>
<td>98.67</td>
</tr>
<tr>
<td>Diffuseness (%)</td>
<td>49</td>
<td>~</td>
<td>~49.96</td>
<td>~</td>
<td>~</td>
<td>~</td>
<td>~</td>
</tr>
<tr>
<td>Uniformity (%)</td>
<td>~</td>
<td>49.99</td>
<td>~50.76</td>
<td>~</td>
<td>~</td>
<td>~</td>
<td>~</td>
</tr>
<tr>
<td>Bit-aliasing (%)</td>
<td>~</td>
<td>~</td>
<td>~49.99</td>
<td>~</td>
<td>~</td>
<td>~</td>
<td>~</td>
</tr>
<tr>
<td>CRPs calculation</td>
<td>~</td>
<td>~</td>
<td>~~N x (M) x (M/2)</td>
<td>~</td>
<td>~</td>
<td>~</td>
<td>~</td>
</tr>
<tr>
<td>Total CRPs</td>
<td>~</td>
<td>~</td>
<td>~3.7 x 10^18</td>
<td>~10^8</td>
<td>~2.3 x 10^37</td>
<td>~2.7 x 10^13</td>
<td>~2.7 x 10^13</td>
</tr>
</tbody>
</table>

F: ReRAM feature size; TYP: Typical-case; BC: Best-case; WC: Worst-case; * indicates it is not mentioned; | was mentioned but no specific distribution quantity was given; † are calculated for M x N CBA(n) of M=2^n=128; | uses x=5.

nonlinear PUF architectures and examples includes the XOR PUF [2] and Feed-Forward Arb-PUFs (FF Arb-PUFs) [7, 8]. An XOR PUF consists of multiple Arb-PUFs and an XOR function which combines the responses of the individual Arb-PUFs, thereby improving the avalanche behavior [55]. Another example, FF Arb-PUFs, utilizes one or few switch(es) that are independent of the input. The resulting feed-forward creates some hidden information and the PUF achieves a higher degree of complexity [8, 51].

To measure the avalanche characteristics of our nPUF, we compared its output bit transition rate with that for one of the single crossbar systems. The inputs were cycled between a reference pattern and a second stimulus pattern that depends on CS. For our nPUF, CS is fixed at five, so that the stimulus pattern is set such that all five selected columns are different from the reference input. Similarity, with CS = 1 only one column selection is different from the reference input selection. In Fig. 9, the color-map shows output transition rate for each choice of row and column transitions. The greener the map, the closer the outcome is to the ideal case of a balance response, i.e., a 50% output transition rate. A PUF with a single crossbar structure shows a biased output bit transition rate, and this is the case for all low row and column selections transitions. Compared to the single crossbar case, the proposed nPUF provides a significantly improved bit-stream balance, and therefore better avalanche characteristics.

D. Estimated Power Consumption

The worst-case power consumption per ReRAM per response bit was measured for our fabricated devices with the READ voltage set to 100 mV. Excluding the contribution of the peripheral circuitry, the power consumption figures in the range of 100 nW were observed. While simple estimates of total mSAL power consumption based on this figure will be far from realistic, it does support the idea of the nPUF as a low-power system element. It is worth noting here that ReRAM arrays consume almost zero power while on standby. Data retention at this range of READ voltages has also been guaranteed for years at 85°C. In contrast to the start-up issues experienced with volatile SRAM-PUFs [56] solutions, we believe that the nPUF should provide a more reliable power-up phase thanks to their non-volatility and long data retention.

According to our experimental observations using the fastest pulse measurements available on the Keithley 4225-PMU (200 MS/s), the performance of the peripheral circuitry would dominate the nPUF throughput, which can be designed to have a range of operational speeds including slow read-outs as suggested in [57] ensure the security of the SHIC PUF primitive.

IV. DISCUSSION

In this section, the structure, performance and NCRP of the proposed nPUF are compared against different alternative ReRAM based PUFs. The nPUF's design advantages such as hidden challenge and dummy cells are also explained in detail.

A. Comparison

nPUF is compared against evaluation data from different ReRAM based PUFs: Nano PUF [43], M-PUF [44], MemPUF [45], mSPUF [46, 47], CPR-PUF [48] and spPUF [49]. Note that PUF metrics results are the measures under typical environmental conditions unless otherwise mentioned. In Table I, the proposed nPUF could potentially achieve the ideal
reliability of 100% while uniqueness, diffuseness, uniformity, and bit-aliasing are close to the ideal of 50%. It can be observed that both uniformity and bit-aliasing are slightly lower than 50% in the m-PUF, which can be attributed to the m-SAL error margin when it is generating the biased bit. Under normal conditions, the diffuseness of the m-PUF and CRP-PUF are also similar and close to the ideal. Similarly, the uniqueness of all the PUF circuits examined here are near to the ideal 50%. On the other hand, the reliability of m-PUF can be seen to be slightly better than other PUFs.

As the table suggests, the proposed m-PUF could achieve performance metrics even closer to the ideal, given all cited works have used a similar mix of experimental and simulation analysis. Also, the works against which we are comparing have adopted a random subset of memory cells and compare the total current passing through them in an analog fashion [48, 58]. Using this method, a PUF with \( M \times N \) crossbar size obtains at least \( N \) times as many challenges as a RO-PUF with \( M \) RO stages [58].

B. Attacks

Given our focus on realizing a secure nano-scale PUF primitive implementation, we first explore the possibility of mounting an invasive attack to create a successful clone of a m-PUF. An invasive attack using direct probing of the m-PUFs may allow a skillful and highly resourced adversary to estimate the resistance of each ReRAM cell and thereby create a software or hardware clone. However, these invasive attempts are more likely to damage the m-PUF structure permanently given the level of skill and tools required to probe nano devices. In turn, damage to the m-PUF would change its challenge-response behavior [59]. Further, semi-invasive photon emission analysis on m-PUF would not work because ReRAMs do not emit photons [60].

Given the potentially large number of CRPs possible with the m-PUF, the proposed PUF primitive may be used in lightweight authentication mechanisms or in more advanced cryptographic protocols, for example in multi-party key exchange requiring the exposure of the PUF interface. Where a PUF interface is directly exposed to an adversary, linear additive delay PUFs such as Arb-PUFs are capable of yielding massive numbers of CRPs and have been shown to be vulnerable to model building attacks [52, 61] by passive adversaries capable of eavesdropping on the CRPs or being able to submit a chosen number of challenges and extract corresponding responses. This type of attack, using the relationship between challenge and response pairs to construct a software model of a PUF, remains the most feasible attack against PUF types with an exposed PUF read-out interface.

In the design of the m-PUF, we have deliberately used a nonlinear structure to reduce the direct relationship between the CRPs (see Fig. 4(b)) where the output from CBA A is hidden and integrated to generate the response from CBA B. Furthermore, it is known that a large \( N_{CRP} \) are required to build an accurate mathematical model of a PUF where the success of the model is determined by its ability to achieve a similar reliability to the PUF under attack. Therefore, simply limiting the rate at which CRPs can be interrogated from a PUF, as proposed in [57] for a simple CBA with diode-like devices at cross-points, can make model-building attacks less effective.

The proposed m-PUF demonstrates high reliability and the capability to lower throughput by employing the techniques discussed in [57], as well as for example, by adjusting sense amplifier capacitance at the output of each crossbar to increase the overall capacitance. Hence, CRP throttling can be used to make the m-PUF less vulnerable to machine learning attacks.

Power analysis attacks: One of the more effective security threats targeting the implementation of cryptographic algorithms is side-channel attacks. Power analysis has been effectively used against different cryptosystem implementation such as smart-card microprocessors [62, 63]. Differential power analysis (DPA) goal is to extract correlations between data and supply power fluctuations. Other power analysis techniques include correlation power analysis based on the Hamming distance model and partitioning power analysis [62, 64-67].

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 [67]. We analyzed the power consumption of our m-PUF resulting from the generation of 2000 output bits. An input challenge dependent selection of five columns with 20 ReRAMs identifies the output bit, while in addition, one or more ReRAM are randomly selected at the same time in order to achieve confusion.

The use of dummy cells alongside the differential read-out scheme (see Fig. 4(b)), provides the potential for significant reduction in the chance of a successful power monitoring side-channel attack. The insertion of dummy operations in software and hardware to mask activities during timing or power analysis attacks has been a well-known technique in hardware security and software cryptography. For instance, [68] reports multiple examples of using dummy structures, such as dummy buffers or dummy loops, as part of advanced encryption standard (AES) software and hardware implementation to thwart attackers.

Note that each CBA of m-PUF utilizes \( M \times N \) (\( M = N = 128 \)) ReRAMs. Fig. 10 illustrates our SNR analysis result as a function of number of dummy devices involved in confusing the power signal. As expected, the more the number of dummy devices, the lower the SNR becomes and therefore
it is possible to adjust performance for different applications according to their sensitivity.

V. CONCLUSION

In summary, we present a novel nPUF based on measured data collected from a range of ReRAM devices on one or multiple dies, fabricated under identical conditions. The nPUF utilizes a relatively simple ReRAM crossbar structure, minimizing design phase to nano-fabrication masks design compare to complex CMOS layout design process. To improve unpredictability, the nPUF 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.

A uniformity of 47.28%, bit-aliasing of 47.48%, diffuseness of 49.86% and uniqueness of 49.85% have been measured in our devices. The PUF’s multiple column selection flexibility also offered a reliability of 98.67% under extremes of process, voltage, temperature and sensing margin fluctuations.

Additionally, we have employed a set of dummy ReRAMS to reduce nPUF’s supply power SNR, although our read-out circuitry exhibited no meaningful relationship between power consumption and output bit generation of either “0” or “1”. ReRAM devices in the nPUF are programmed in their HRS to (1) take advantage of highly spatially driven variations in HRS and (2) reduce power consumption. The crossbar array aspects such as resistance-pattern dependent sneak current paths (parasitic current via neighboring cells) are also intrinsically contributing to nPUF performance but their specific role in nPUF operation is currently under investigation.

REFERENCES


[47] ——, “muPUF: A novel memristive device based physical unclonable function,” in *Applied Cryptography and...*


Hussein Nili received his B.Sc. degree in Electronics Engineering from University of Tehran, Tehran, Iran and Ph.D. degree from RMIT University, Melbourne, Australia, in 2010 and 2015, respectively. He is currently a Postdoctoral Scholar with the Electrical and Computer Engineering Department at University of California Santa Barbara, where his research interests include design and in-depth characterization of highly disordered and nano-engineered electronic materials platforms for novel computing/memory architectures.

Jiawei Yang received his B.Eng degree in Electrical Engineering from Zhejiang University (China) in 2004. From 2004 to 2007, he worked for Honeywell (China) as an electrical engineer. In 2011, he received his Ph.D degree in Electrical & Electronics Engineering from the University of Melbourne and National ICT Australia. Between 2011 and 2014, he was research fellow for the Centre for Neural Engineering (CINE) at the University of Melbourne, focusing on designing electronics for high acuity retinal prosthesis and other biomedical implants. Currently, he is principal investigator in Wenzhou Medical University (China).

Doo Seok Jeong is a senior scientist at the Korea Institute of Science and Technology (KIST), South Korea. He received his BS and ME in materials science from Seoul National University in 2002 and 2005, respectively. He received his PhD degree in materials science from RWTH Aachen, Germany, in 2008. Since 2008, he has worked for KIST. He is an Associate Editor of Journal of Electronic Materials (Springer). He has published more than 80 SCI papers that have been cited over 3800 times in total. His research interests focus on spiking neural networks for temporal learning, ranging from building block to online learning algorithm.

Paul Beckett (M’06, SM’08) received the B. Eng. degree in Communication Engineering, M. Eng. and Ph.D. degrees from RMIT University, Melbourne, Australia, in 1975, 1984, and 2007, respectively. He is currently an Associate Professor with the School of Engineering, RMIT University where his research interests include the design and simulation of nanoscale computer architecture and the mixed signal modeling of asynchronous reconfigurable circuits.

Sharath Sriram (S’04, G’05, M’09) is the joint leader of the Functional Materials and Microsystems Research Group at RMIT University, Melbourne, Australia, from where he was awarded his Ph.D. in 2009. He is the founding Deputy Director of the Universities Micro Nano Research Facility, a 1,200 sq.m. state-of-the-art macro/nanofabrication facility. Associate Professor Sriram’s expertise includes the synthesis of functional thin films and micro/nanostructures and devices. He has published over 120 peer-reviewed publications. He is the recipient of the 2010 Gold Medal for Excellence in Research from the Australian Institute of Nuclear Science and Engineering, a 2011-2014 Australian Postdoctoral Fellowship from the Australian Research Council, the 2012 NMI Prize for Measurement Excellence from the National Measurement Institute, Australia, a 2012 Victoria Fellowship, and the 2014 RMIT Vice-Chancellor’s Early Career Researcher Award.

Danith C. Ranasinghe received the Ph.D. degree in electrical and electronic engineering from The University of Adelaide, Australia, in 2007. From 2005 to 2006, he was a Visiting Scholar with the Massachusetts Institute of Technology and a Post-Doctoral Research Fellow with the University of Cambridge from 2007 to 2009. He joined The University of Adelaide in 2010, and is currently a Tenured Senior Lecturer with the School of Computer Science, where he leads the research group with the Adelaide Auto-ID Laboratory. His research interests include pervasive and ubiquitous computing, wearable computing, human activity recognition, geotechnology, lightweight cryptography for resource constrained devices, and physical cryptography.

Omid Kavehei (S’05, M’12, SM’16) received his Ph.D. degree in electronic engineering from The University of Adelaide, Australia, in 2012. He is currently a Lecturer at Royal Melbourne Institute of Technology in Melbourne, Australia. Prior to this appointment he was with Centre for Neural Engineering at The University of Melbourne as a Research Fellow in Microelectronics. Dr Kavehei was an executive member of the South Australian IEEE student chapter and the recipient of The University of Adelaide 2013 postgraduate university alumni medal and the South Australian Young Nanotechnology Ambassador award in 2011. His research interests include emerging solid-state memory devices, physical cryptography, novel computational paradigms based on nanotechnology and implantable electronics. He is a Senior Member of IEEE.