R$^3$PUF: A Highly Reliable MemRistive Device based Reconfigurable PUF

Yansong Gao† and Damith C. Ranasinghe†
†Auto-ID Labs, School of Computer Science, The University of Adelaide, SA 5005, Australia
{yansong.gao, damith.ranasinghe}@adelaide.edu.au

Abstract—We present a memristive device based R$^3$PUF construction achieving highly desired PUF properties, which are not offered by most current PUF designs: (1) High reliability, almost 100% that is crucial for PUF-based cryptographic key generations, significantly reducing, or even eliminating the expensive overhead of on-chip error correction logic and the associated helper on-chip data storage or off-chip storage and transfer. (2) Reconfigurability, while current PUF designs rarely exhibit such an attractive property. We validate our R$^3$PUF via extensive Monte-Carlo simulations in Cadence based on parameters of real devices. The R$^3$PUF is simple, cost-effective and easy to manage compared to other PUF constructions exhibiting high reliability or reconfigurability. None of previous PUF constructions is able to provide both desired high reliability and reconfigurability concurrently.

Index Terms—Reconfigurable PUF; High reliable; Memristive devices

I. INTRODUCTION

Physically Unclonable Functions (PUFs) exploit the static randomness resulting from uncontrollable process variations to extract instance-specific secrets. Unlike assigned storage digital secrets in a memory, the instance-specific secrets arise during the creation of PUF embedding devices. Attributing to inevitable randomness, PUFs cannot be reproducibly forged even by the original manufacturer. Various physical randomness sources have been utilized for building PUFs such as gate-delay [20], power-on state of the static random-access memory (SRAM) [8]. Among memory-based PUFs, SRAM PUFs gained the most attention since they are considered ‘for free’ due to memory availability in almost all commodity products. As the conventional silicon technology is continuously scaling down and approaching its most material and physical extents, there is a growing urge to look for memory elements for nanoelectronic applications.

The memristive device is one of promising candidates considering its faster speed, higher density, lower power and non-volatility. Moreover, its fabrication is compatible with current CMOS fabrication process. However, in nano region, currently, they suffer serious variations that somehow deteriorates their performance in memory applications. As the device engineers are always attempting to eliminate the variations. Security applications, for example, PUF constructions based on the memristive devices [18], [12], [19], [17], [14], [6], [5], actually embrace such prevalent physical variations, because truly prevalent randomness implies more entropy when extracting PUF secrets.

The response (output) given the same PUF is highly desired to be stable when it is re-evaluated upon the same challenge (input). This property is referred to as reliability. Besides that, there are other desirable properties such as reconfigurability and large challenge response pairs (CRPs) space—more entropy extracted within a compact area. Reconfigurability of a PUF is the capability of refreshing its CRPs—evolving the PUF itself into a new instance that exhibits different CRP behaviors, which is of great importance in many application scenarios such as updating electronic tokens—electronic tickets, and preventing downgrading software versions by binding software to hardware [13], [10], [7]. As the other intermediate benefit, the derived key from an rPUF can also be renovated whenever necessary. Moreover, it is indicated that the rPUF is capable of eliminating some potential attacks such as modeling attacks and reverse engineering [16]. We also note that the reconfigurability helps to mitigate security concerns that malicious contract manufacturers evaluate PUF secrets without authorization before PUF enrollment by a trusted party. In this context, the PUF secrets can be reconfigured before enrollment phase by the trust party, where the reconfigurability makes PUF secrets evaluated by malicious manufactures useless.

Motivated by these targets, we present a memory-based PUF construction, a highly Reliable memRistive element based Reconfigurable PUF (R$^3$PUF), termed as R$^3$PUF by leveraging peculiarities of memristive devices. Compared with memory PUFs based on CMOS, eg., SRAM, R$^3$PUF has higher density that enables a large CRP space within a compact area attributing to the small footprint of memristive devices. Most significantly, R$^3$PUF achieves both high reliability and reconfigurability, while most of current memory-based PUF constructions may achieve either one of them, but not both, at the cost of expensive additional logic. The main contributions of this work are summarized as follows:

**Highly reliable PUF.** We develop R$^3$PUF to generate highly reliable responses. As a consequence, error correction logic is less or even no more required resulting in a lightweight alternative that can be easily plugged into PUF based key generation applications. Based on our simulation results in Section IV-C R$^3$PUF achieves reliability of 100%.

**Reconfigurable PUF.** We endow R$^3$PUF with reconfigurability without incurring additional area overhead, so that its CRP(s) can be refreshed whenever necessary at no additional costs. We emphasize that the reconfiguration of R$^3$PUF is unpredictable and irreversible.
Evaluation. We validate $R^3$PUF performance using a public memristive device model guided with experimental data. We detail the rationale of improved $R^3$PUF performance in comparison with previous memristive device-based PUF constructs [18], [12], [19], [17], [14], [6], [5].

In next section, we present a background on memristive devices and their properties, followed by concisely survey of one memristive device based reliable PUF and two reconfigurable PUF constructions. We also introduce the important memristive device property unnoticed in previous PUF designs. In Section III, we outline $R^3$PUF design along with its operations. Section IV evaluates $R^3$PUF performance and compares it with other memristive device based PUFs. Section V concludes the paper.

II. MEMRISTIVE DEVICES BASED PUFs

A. Resistance Variation Sources

A memristive device is a two terminal non-volatile nano element. It switches between high resistance state (HRS) and low resistance state (LRS) by applying a negative/positive potential difference between the top electrode and bottom electrode. The growth and disruption of filamentary conductive paths inside the insulating dielectric are responsible for this switching behavior, illustrated in Fig. 1 (a). The switching from HRS to LRS is referred to as the SET operation, whereas the switching from LRS to HRS is referred to as the RESET operation. The HRS and LRS that are also changeably referred to as $R_{OFF}$ and $R_{ON}$ respectively to denote the two logic states for storing digital information. Attributing to its non-volatility, stored information (resistance) remains after power being cut-off.

The memristive device has a very small footprint. A special layer partially doped is sandwiched between two electrodes. The thickness is down to several nanometers. This enables super high content information storage capability in a compact area where memristive devices are integrated [21]. However, for memristive devices, resistance variations is inevitable and actually prevalent due to the hardness of fine fabrication control. Geometrical variations such as thickness, width, dopant density significantly impact the resistance in both HRS and LRS states, which has been experimentally measured in fabricated devices, see Fig. 1(b). This is obviously unwanted for memory-based applications because resistance variations deteriorate read margin when distinguishing between HRS and LRS states. However, this prevalent true randomness is of importance for PUF designs [18], [12], [19], [1], [2], [17], [14], [6], [5], [3].

Besides the geometric induced variations, the resistance in HRS and LRS is also determined by cycle-to-cycle (C2C) variation. C2C variation is an unique variation that is not exhibited by CMOS devices. It is caused by random locations of filaments in the memristive device when it is reprogrammed cycle by cycle—some of these metal filaments’ locations are formed and disrupted randomly during reprogramming [23], [22], [2]. Hence, the resistance observed in HRS or LRS states varies not only among devices but also among different programing cycles given the same device. The C2C variation adopted from measured data is illustrated in Fig. 2.

![Fig. 1. (a) RESET and SET operation of the memristive device. (b) Experimental resistance variation distribution on LRS and HRS state—corresponding to $R_{ON}$ and $R_{OFF}$ respectively—measured from 1600 memristive devices [11].](image)

![Fig. 2. Cycle-to-cycle (C2C) variations. $R_{OFF}$/HRS and $R_{ON}$/LRS variation for an individual memristive device for 1000 cycles, experimental data is adopted from [22].](image)

B. Reliable PUFs and Reconfigurable PUFs

1) A Reliable PUF: Che et al. [1] proposed a memristive device based PUF that generates highly reliable (error free) response. The PUF operations during enrollment are generalized in Fig. 3 and follow steps as: i) All of memristive devices in an array are initially programmed into LRS. This indicates the entropy of PUF response is from the resistance variance in $R_{ON}$, see Fig. 1(b). ii) The varied $R_{ON}$ resistance of each memristive device is digitalized. Then the the median of all digitalized values is determined. iii) The memristive device is programmed into LRS if the digitalized value of such a specific device is lower than the median value, otherwise the memristive device is programmed into HRS.

In general, in Fig 4, if the memristive device initial resistance is lower than the median of LRS ($R_{ON}$), its final state is LRS state. Otherwise, its final state is in HRS state. The regeneration of PUF response is simply reading out the
memristive device’s state, HRS/LRS is eg., ‘1’/’0’. The ratio of HRS to LRS is large enough to distinguish these two states, see Fig. 1(b), in other words, there is no overlap because of a large gap between bimodal resistance distributions. Thereupon, the reliable response regeneration is ensured.

Although this PUF capture certain desirable features from memristive devices such as substantial resistance variations in either HRS or LRS, high resistance ratio of HRS to LRS and non-volatility. The operation procedures during the enrollment is, however, complicated. Such a complicated enrollment phase results in higher cost due to the usage of analog-to-digital converter, counter, and also write-back circuits. As will be shown in the R³PUF, we require neither any extra hardware nor the write-back operation.

2) Reconfigurable PUFs: Gao et al. [5] and Chen et al. [2] noticed that unique C2C variations of memristive offers the feasibility to design rPUFs. In general, these two memristive device based rPUF constructions exploit either HRS or LRS resistance distributions as random source to extract responses. The response is produced based on comparisons of two (or more) memristive devices’ resistance when they are aligned to the same state (HRS/LRS). The response readout uses a small voltage without disturbing the resistance of memristive devices. Whenever reconfiguration is on demand, memristive devices are reprogrammed using a larger voltage that is able to SET/REST the devices.

C. Abrupt Switching Behavior

The abrupt switching behavior reacts with the threshold voltage phenomena [23]—illustrated in Fig. 3. For electric-field-induced bipolar switching in a memristive device, the applied electric field plays a dominant role. A small electric-field is inadequate to move ions in the device to change its resistance [23]. Therefore, in practice, the resistance of the memristive device stays unchanged or changes negligibly if the voltage drops across the memristive device falling within two threshold voltages $V_{\text{RESET}}$ and $V_{\text{SET}}$. Otherwise, it swiftly switches to HRS if the biased voltage reaches to $V_{\text{RESET}}$ or to LRS if the biased voltage goes to $V_{\text{SET}}$.

By exploiting C2C variations and abrupt switching behavior of memristive devices, our R³PUF achieves high reliability and reconfigurability concurrently with a very simple design and operations.

III. R³PUF DESIGN

In this Section, we detail the principles of R³PUF design by making most of all forgoing memristive device properties.

A. R³PUF construction

Topology of the R³ PUF is similar to popular memory-based PUFs [8], [24]. A memory-based PUF consists of a number of memory cells, each cell produces a response bit that is independent on others generated by other cells. The R³PUF, as illustrated in Fig. 5(b), has an alike topology, where the challenge is the address of the R³PUF cell in a high density array. The R³PUF cell is quite simple, where two memristive devices $M_1$, $M_2$ are connected serially. Its operation has two phases: response extraction and readout.

1) Response Extraction: Both memristive devices are set to LRS/$R_{\text{ON}}$ initially—also see visualized operation procedures depicted in Fig. 6. Then the applied voltage $V_{\text{in}}$ across two devices gradually increases to $2 \times |V_{\text{RESET}}|$—noting the polarity of memristive device. Due to inherent resistance variations, $R_{\text{ON1}}$ (LRS resistance of $M_1$) and $R_{\text{ON2}}$ are different. For the purpose of easing the description, we assume that $R_{\text{ON1}} > R_{\text{ON2}}$. As a consequence, $M_1$ will first reach to the RESET threshold voltage $V_{\text{RESET}}$ and start switching to the $R_{\text{OFF1}}$. This is because $M_1$ shares more applied voltage considering the fact that $M_1$ and $M_2$ eventually forms a voltage divider. Once $M_1$ starts switching to $R_{\text{OFF1}}$, its increasingly shared voltage further amplifies its switching and makes it switching to $R_{\text{OFF1}}$ even faster. At the meantime, $M_2$ is stuck
in $R_{ON2}$ because it cannot reach to its threshold voltage as the fact that the voltage dropped across it becomes even smaller once $M_1$ starts switching. In our R3PUF construction, this amplification alike voltage sharing behavior eventually serves as one basis of the high reliability.

2) Response Readout.: The readout is performed by simply applying a small voltage that does not disturbs resistance of memristive devices. Recall that at the end of response extraction phase, the $M_1$ is in $R_{OFF1}$ and the $M_2$ is in $R_{ON2}$. According to

$$V_{out} = V_{in} \times \frac{R_{ON2}}{R_{ON2} + R_{OFF1}}$$  

and $R_{OFF}/R_{ON}$ is usually large—1000 has been experimentally shown in [11]. We can see that the $V_{out}$ will close to 0 V. We further digitize $V_{out}$ to obtain a response by simply utilizing an inverter—acting as a voltage comparator. Hence, the response of ‘1’ is produced in this exemplary case.

Considering $M_1$ remains in HRS and $M_2$ in LRS even when the power is off, therefore, whenever the response is regenerated later, it will be stably reproduced. To sum it up, the exploitation of non-volatility of memristive device and high ratio of HRS to LRS enables robust response regeneration.

B. R3PUF Reconfiguration

To endow the R3PUF with reconfigurability, firstly, the $M_1$ is reprogrammed back to $R_{ON1}$ from $R_{OFF1}$—we follow the same motivating example in Section II-A—by applying $V_{in}$ that is smaller than $-V_{SET}$, again noting the polarity of memristive devices in Fig. 5. Now taking the C2C variation into consideration, the $R_{ON1}$ of $M_1$ after this SET operation is different from the previous value. As a result, the relationship between $R_{ON1}$ and $R_{ON2}$ becomes unknown—which one is higher is nondeterministic. Next, response extraction operations, step 2 to step 3 depicted in Fig. 6 are conducted to extract a refreshed response, where the response value is unpredictable.

We realize that the number of times that R3PUFs can be reconfigured is determined by the endurance of memristive devices. Endurance is the maximum cycles that the memristive device can be reprogrammed between HRS and LRS without suffering obvious read margin degradation. Specifically, the ratio of HRS/LRS still keeps higher enough to explicitly distinguish two logic states: ‘0’ and ‘1’. Luckily, the endurance usually is high, for example, experimental reports of $10^5$ in [9]. This number is adequate for most rPUF applications.

IV. R3PUF EVALUATIONS AND DISCUSSIONS

We evaluate and analyze the R3 PUF performance based on the below described public behavior model guided with experimental data as shown in Fig. 1 [11]. Then we fairly compare it with other memristive device based PUFs.

A. Memristive Device Model and Simulation Setup

1) Device Model: The memristive device model is adopted from [4]. It has a state variable $\omega$ $\subset$ [0, 1] corresponding to the value of its resistance $R_m$, which is a function as

$$R_m = R_{OFF}(R_{ON}/R_{OFF})^\omega$$  

According to Eq. 2 $R_m = R_{OFF}$ when $\omega = 0$, while $R_m$ is in the $R_{ON}$ state if $\omega = 1$.

The dynamic switching behavior of the memristive device is defined as:

$$\frac{dw}{dt} = \begin{cases} 
\alpha(v - V_{SET}), & (v \geq V_{SET}) \\
\alpha(v + V_{RESET}), & (v \leq V_{RESET}) \\
\beta v, & \text{otherwise}
\end{cases}$$  

where $v$ is the voltage drop through the memristive device. Although we consider a symmetrical threshold voltage for $V_{RESET}$ and $V_{SET}$, it will not affect the performance evaluation. The $\alpha$ and $\beta$ coefficients are switching rates. Here, we set $\beta = 0$ assuming that the smaller voltage does not alter the state variable as pointed out in [23]. The $\alpha = 10^5$ to fit the experimentally reported abruptly switching when $v > V_{SET}$ or $v < V_{RESET}$.

The developed behavioral model created in Verilog-A language is also adopted from [4]. Simulated I-V curve in Fig. 7 (a) shows well matching behavior as in Fig. 4.

2) Simulation Setup: The memristive device model is integrated into the R3PUF cell circuit as shown in Fig. 6. The inverter is implemented by standard 90nm technology. The simulation is conducted via Monte Carlo command in Cadence. Variations for different parameters are listed in Table I. Note the variance of $R_{ON}$ and $R_{OFF}$ is intentionally set smaller than the measured data in Fig. 2 in order to demonstrate that slightly variation is already able to lead a high reliable R3PUF.
B. Results

We carry out simulations according to the R³PUF operations depicted in Fig. 6. The R³PUF operation is simple that only involves with controlling the applied voltage $V_{in}$. Therefore, we depict the setting of $V_{in}$ and the corresponding output voltage $V_{out}$ between $M_1$ and $M_2$ in Fig. 7 to experimentally imply the entire operation procedures by an indirectly means. We first describe a specific validation of a single R³PUF cell before large population evaluations. The $M_1$ and $M_2$ are set to be LRS state initially, where $R_{ON1} = 5 \times 10^5 \, \Omega$ and $R_{ON2} = 4.99 \times 10^5 \, \Omega$ with a very small resistance difference of 0.2% compared with $R_{ON1}$.

Starts from shadowed area a in Fig. 7(b), $V_{in}$ is gradually increased from 0 V to 2.5 V. Both of $M_1$ and $M_2$ stay unchanged as $V_{in} << 2$ V considering that $V_{out}$ is linear increased as $V_{in}$ increases. Once the voltage approaches to $2 \, V = 2 \times |V_{RESET}|$, the $M_1$ starts switching first as it shares a larger voltage—recall $R_{ON1} > R_{ON2}$, hence, it reaches to $RESET$ threshold first. The resistance of $M_1$ switches from $R_{ON1}$ to $R_{OFF1}$ that is amplified by the abrupt switching behavior as the voltage dropped across $M_1$ becomes larger. Such a switching will be quickly finished, and later almost all applied voltage drops across $M_1$ according to Equation (1) and a large HRS/LRS ratio, thereof, $V_{out}$ goes down to near 0 V. The response readout is validated by applying a $V_{in}$ of 1 V as shown in area b of Fig. 7. As the $V_{out} \approx 0$ V, the response gives logic ‘1’ after digitalization by an inverter. 

Monte Carlo simulation runs 15,000 times taking all the variation sources in Table I into consideration. In other words, 15,000 R³PUF cells are simulated. Histograms of $V_{out}$ and response are shown in Fig. 7(c). We can see that the $V_{out}$ is close to 0 V or 1 V when the readout voltage $V_{in} = 1$ V is applied. The percentage of ‘1’ in response is 50.60%, which is close to the ideal value of 50% that implies good randomness/unpredictability.

C. Discussions

1) Reliability: Due to the unavailable memristive device temperature model [5], [19], the reliability performance under different temperatures cannot be evaluated. However, the high reliability can be envisioned because of the rationale: i) Once the step 3 of R³PUF operation is done, the resistance of $M_1$ and $M_2$ will remain constant even the power is off attributing to the non-volatility. ii) $V_{out}$ demonstrated in Fig. 7(c) shows a widely and clearly separation indicating that there is always one memristive device is in LRS state and the other one is in the opposite HRS state. iii) Seeing the high ratio of $R_{OFF}$ to $R_{ON}$, even right tail of $R_{ON}$ distribution and left tail of $R_{OFF}$ distribution still has magnitude difference. Foregoing facts guarantee that the later re-readout of response is robust. Actually, the histogram of $V_{out}$ from 15,000 R³PUF cells implies a reliability of 100%.

2) Reconfigurability: To reconfigure the R³PUF, SET both of $M_1$ and $M_2$ to LRS is needed. This is validated in the area c in Fig. 7 (b). After SET operation, both memristive devices are in LRS. Considering the physical means induced C2C variations, the response generated once the R³PUF is reconfigured cannot be predicted even the previous response value is known. This guarantees the forward security. Likewise, observing the later generated response after reconfiguration is unable to discover the previous response value, which ensures the backward security. Further, the reconfiguration by using C2C variation cannot be reversed by any party.

3) Comparisons: The results of R³PUF are from simulations, note other memristive device based PUF realizations [18], [12], [19], [11], [2], [17], [14], [6], [5] also evaluated from simulations. Therefore, it is reasonable to compare with them.

We are the first work to achieve both high reliability and reconfigurability, moreover, without extra area cost and complicated operations. These works [18], [12], [19], [17] do not take the inherent C2C variations into consideration, which may further degrade these PUF designs’ reliability performance. Two works consider the C2C variations to design rPUFs [2], [5] but without realizing high reliability. Given the only work shows high reliability [11] reviewed in Section II, it requires complex operation procedures and costs extra hardware overhead. All the aforementioned designs do not fully take advantage of the properties exhibited by the memristive devices. However, the reason that they cannot offer high reliability and reconfigurability simultaneously with a very simple circuit implementation. The R³PUF exploits more inherent properties from the memristive devices: process variations, C2C variations, abrupt dynamic switching behavior, high ratio $R_{OFF}/R_{ON}$, high endurance and the non-volatility. All of these exploited properties of memristive devices eventually lead to a simple R³PUF but equipped with better performance.

V. Conclusion

In this paper, we propose the R³PUF design and evaluate its performance by extensive simulations guided with existed memristive device model and parameters from experimental data. The R³PUF has higher reliability performance and also is reconfigurable without extra area cost and complicated operations, because we are able to capture peculiarities of memristive devices. Based on the simulation, it indicates that the reliability is almost to 100%, if not 100% as infinitely Monte Carlo runs cannot be achieved. Therefore, the ECC implementation overhead can be significantly reduced—or maybe omitted based on the error free response shown in the results—when the R³PUF is used for cryptographic key generations. In addition, The unique C2C variation is exploited to reconfigure the CRPs of the R³PUF, which enables updating the derived cryptographic keys on demand.

Our future work will experimentally evaluate R³PUF’s performance based on fabricated memristive devices.

REFERENCES

[1] W. Che, J. Plusquellic, and S. Bhumia. A non-volatile memory based physically unclonable function without helper data. In IEEE/ACM International Conference on Computer-Aided Design (ICCAD), pages 148–153. IEEE, 2014.
Fig. 7. (a) Simulated I-V (current-voltage) curve of a typical memristive device. The inset figure shows the same I-V curve but the y-axis is on a logarithmic scale. $V_{\text{RESET}} = -1$ V and $V_{\text{SET}} = 1$ V. (b) Validation of the R$^3$PUF operations. (c) Distribution of the $V_{\text{out}}$ and response of the R$^3$PUF.