

Threshold Voltage based Dual Memristor Crossbar PUF

Aref Al-Tamimi, Shawkat Ali, Yuan Cao, Amine Bermak

Item type

Journal Contribution

Terms of use

This work is licensed under a [CC BY-NC-ND 4.0](#) license

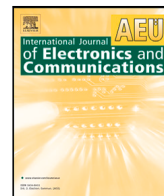
This version is available at

https://manara.qnl.qa/articles/journal_contribution/Threshold_Voltage_based_Dual_Memristor_Crossbar_PUF/26404060/1

Access the item on Manara for more information about usage details and recommended citation.

Posted on Manara – Qatar Research Repository on

2024-01-04



Threshold Voltage based Dual Memristor Crossbar PUF

Aref Al-Tamimi^{a,*}, Shawkat Ali^b, Yuan Cao^c, Amine Bermak^a

^a Hamad Bin Khalifa University, College of Science and Engineering, Qatar

^b King Abdullah University of Science and Technology, Saudi Arabia

^c Hohai University, College of Internet of Things Engineering, China

ARTICLE INFO

Keywords:

PUF
Crossbar
Memristors
IoT security

ABSTRACT

IoT security plays a crucial role where smart devices are interconnected and one of these can give an intrusion access to the network if they are not secured. Physical unclonable function (PUF) comes in handy as an emerging lightweight hardware security primitive for key management and device authentication. In this research work, we propose a new architecture of PUF hardware based on memristor threshold voltage variation. Memristor manufacturing variations are exploited for the threshold voltage variation which makes the device unique. The selection from the proposed crossbars forms two connected memristors. The selections connect the formed voltage divider network to the input and ground. The output is probed at the middle node, which is the selected rows of the two crossbars. Voltage (challenge) is applied at selected pair of memristors through the corresponding columns and rows, and output (response) is taken from the selected rows. We believe this work will set a new direction for the researchers to explore manufacturing errors for PUF applications.

1. Introduction

In the realm of interconnected smart devices, the significance of IoT security cannot be understated. Within this intricate network, a single unsecured device has the potential to breach the system's security, introducing an unwelcome intrusion. This is why safeguarding these interconnected devices is crucial in ensuring the integrity and protection of the entire network. Challenges to implementing security functions on a resource-constrained IoT device have led researchers to develop more advanced and lightweight solutions [1]. Physical unclonable function (PUF) comes in handy as an emerging lightweight hardware security primitive for key management and device authentication [2]. It surpasses the traditional cryptographic algorithms of storing confidential key information in a nonvolatile memory (NVM) [3]. PUF extracts a reliable unique fingerprint from devices and exploits unpredictable and uncontrolled device parameters that are due to process variations during manufacturing. The set of the input and output binary vectors of a PUF is called a challenge-response pair (CRP). The mapping of the CRPs of different PUF instances is expected to be different from each other. Since Pappu first introduced the PUF concept [4], many silicon-based PUFs have been proposed over the years [5,6]. One of the emerging PUF designs is based on memristors, due to its advantages of power, area, and security [7]. The Memristor, a device discovered by Chua [8], stores digital data in the form of two states, high resistance (R_{OFF}) and low resistance (R_{ON}). The states are triggered when the

applied voltage across the two terminals crosses its threshold value either in a forward or reverse direction. In literature, most memristor PUFs exploit the R_{ON} and R_{OFF} tolerated resistance errors to generate a random output bitstream.

Memristor crossbars are commonly used in artificial intelligence accelerator designs with high-density data storage and computing performance [9]. Fig. 1 shows a typical PUF design using memristor arrays [7]. This type of PUF requires two identical arrays, hence it occupies twice the physical area per output bit. When a voltage is applied to a selected cell of each array, the voltage at the output node of each array will differ due to the tolerated error in the resistivity of the selected memristors. The outputs of the array nodes are compared using a CMOS comparator that generates an output result depending on their voltage difference. The output of the CMOS is a binary $-v, +v$ which represents digital 1 and 0, respectively. The size of the PUF array per bit is proportional to the CRP bit size. A higher CRP bit size corresponds to a stronger PUF with higher entropy. For the $2[n \times n]$ crossbar PUF shown in Fig. 1, the challenge size is $4\log_2(n)$ bits. This type of PUF is prone to noise, offset error, and meta-stability error caused by the comparator, which ultimately contributes to the output error. The comparator also increases the area, complexity, and power consumption as the CRP bit size increases.

This work is an extension of the authors' published conference paper (ICM 2022) [10] which proposed a concept of utilizing threshold

* Corresponding author.

E-mail addresses: altamimi@hbku.edu.qa (A. Al-Tamimi), shaali@hbku.edu.qa (S. Ali), caoyuan0908@hhu.edu.cn (Y. Cao), abermak@hbku.edu.qa (A. Bermak).

<https://doi.org/10.1016/j.aeue.2023.155012>

Received 12 May 2023; Accepted 6 November 2023

Available online 30 November 2023

1434-8411/© 2023 The Author(s). Published by Elsevier GmbH. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

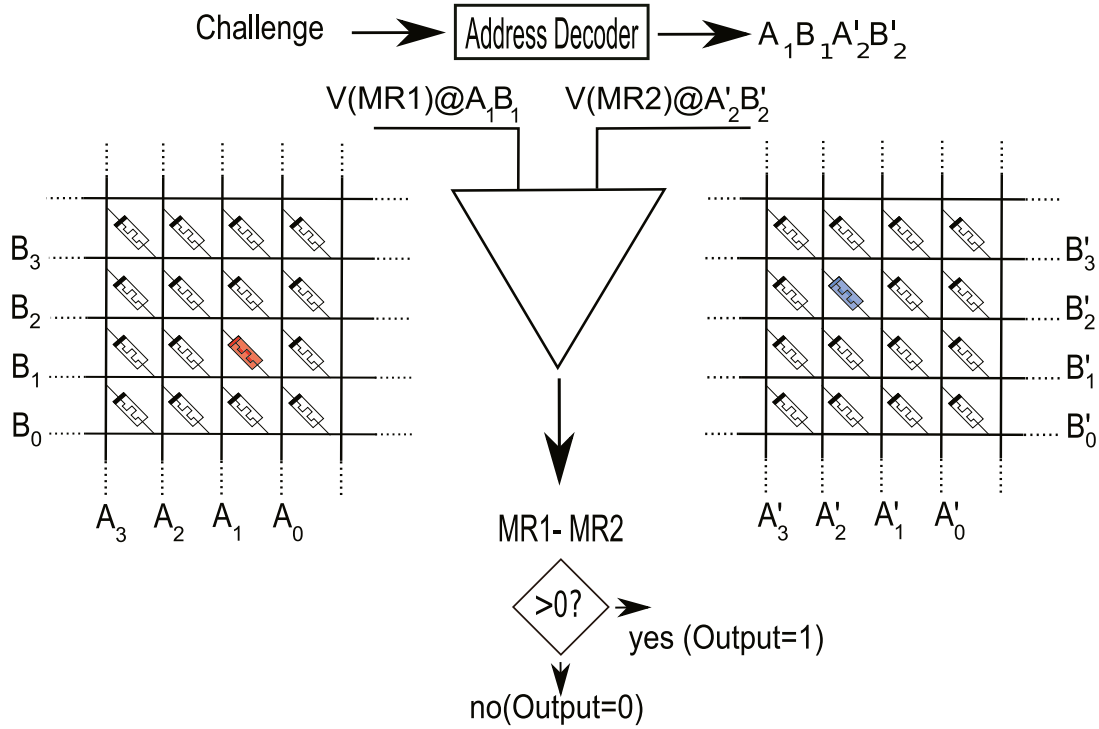


Fig. 1. Memristors crossbars PUF flow diagram.

voltage in memristors for PUF by exploiting the threshold voltage error of memristors. The novelty of the design is related to the use of comparator-free architecture enabling considerable savings in terms of power consumption. In addition, this extended version demonstrates a novel design that is based on dual memristor crossbar PUF, which is a sneak path resilient.

When applying a reading voltage for a memristor in a crossbar, part of the current flow through the neighboring memristors and create a parallel resistance, thereby causing it to be erroneously read. This is known as a Sneak Path (SP) effect. In PUF mode this error if not balanced causes biasing toward a group of memristors, and reduces uniformity. Although the problem of sneak paths is discussed in literature [11], previous crossbars PUF work [12,13] have not tackled the effect of SP in their design. The proposed unidirectional memristors' crossbars reduce SP by preventing the current from flowing through the neighboring memristors, by blocking reverse currents.

The dual memristor-based crossbar architecture in this extended work is hardware-friendly and realized by a simple rewiring arrangement of the memristor crossbars of Fig. 1. It provides the storage of a traditional memristor array in normal mode, and in PUF mode it avoids the use of comparators and solves the sneak path issue.

For the rest of this paper, the detailed structure of the proposed PUF will be discussed in Section 2. Section 3 presents the algorithm of the proposed Uni-directional memristor model, followed by the design and analysis of a 2[4×4] memristor array. Section 4 will conclude the paper.

2. Threshold Voltage based Dual Memristor Crossbar PUF

The proposed Threshold Voltage based Dual Memristor Crossbar (TvDuMXbar) PUF, shown in Fig. 5 exploits the non-uniformity of memristors' threshold voltages. The proposed PUF core consists of a cell of two memristors connected in series between the input and ground. Both memristors are identical except for manufacturing errors in their electrical and physical properties. The impurity that is targeted in this paper is the memristors' threshold voltages. The threshold voltage non-uniformity is introduced due to manufacturing process errors. The proposed idea is to capture the difference in threshold voltages of the

cell memristors and output it as a binary single bit. TvDuMXbar PUF leverages the memristor cell for its core, by scaling it into two identical left and right memristors crossbars (LXbar),(RXbar) respectively. The cell top and bottom memristors are selected from both LXbar and RXbar respectively. The cell selection is based on a given challenge address, and the PUF response is the cell's output. The selection mechanism connects the input source to one end of the selected Top memristor in LXbar, and connects the ground to one end of the selected Bottom memristor in the RXbar. The selection mechanism also connects the other ends of the selected top and bottom memristors together and forms the output node of the selected network. This dual memristor selection forms a single cell of the proposed PUF of Fig. 3. In the remainder of this section, the design and implementation of the proposed cell and TvDuXbar PUF are presented.

2.1. Memristor threshold voltage non-uniformity

The threshold voltage of a memristor depends mainly on its active thin film layer thickness. The process of building memristors does not maintain uniformity in the layer thickness. This makes the threshold voltages differ for different memristor instances. Fig. 2 presents an IV graph that illustrates such threshold voltage (v_{th}) variations among different memristor instances [14].

2.2. Dual memristor cell

The dual memristor cell consists of two identical memristors connected in series as depicted in Fig. 3. Assuming both memristors have similar specifications, the threshold voltages of the memristors still differ by a small fraction due to the error caused by the manufacturing process. Initiating both memristors to an *OFF* state, and applying a rising voltage v_{in} at the input port, causes the output at the middle node to form a pulse as demonstrated in Fig. 3. The formation of the pulse is due to the state-switching sequence of the two memristors due to the difference between their v_{th} values.

The process of generating the pulse starts by initiating top and bottom memristor states to *OFF* and then applying a rising voltage

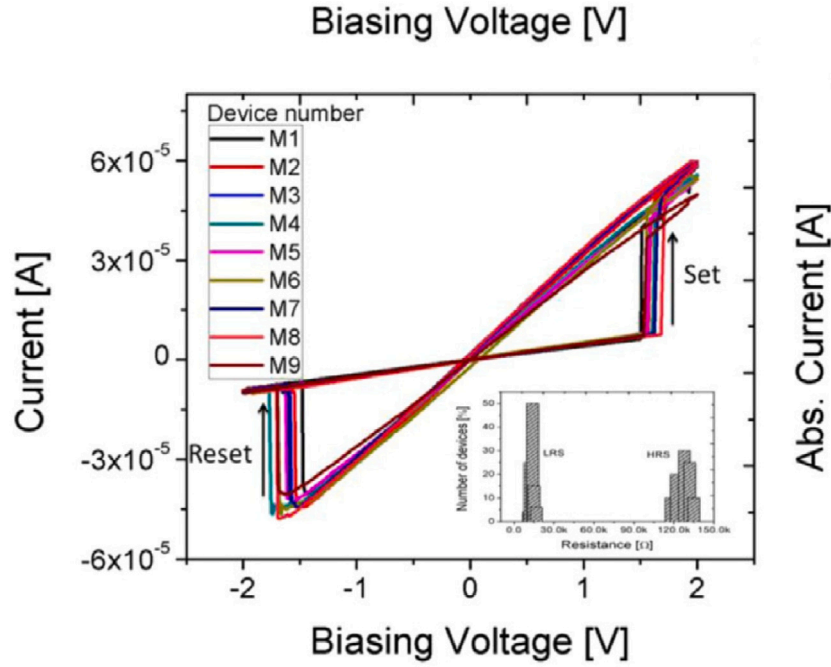


Fig. 2. IV graph demonstrates different threshold voltages for different memristors [14].

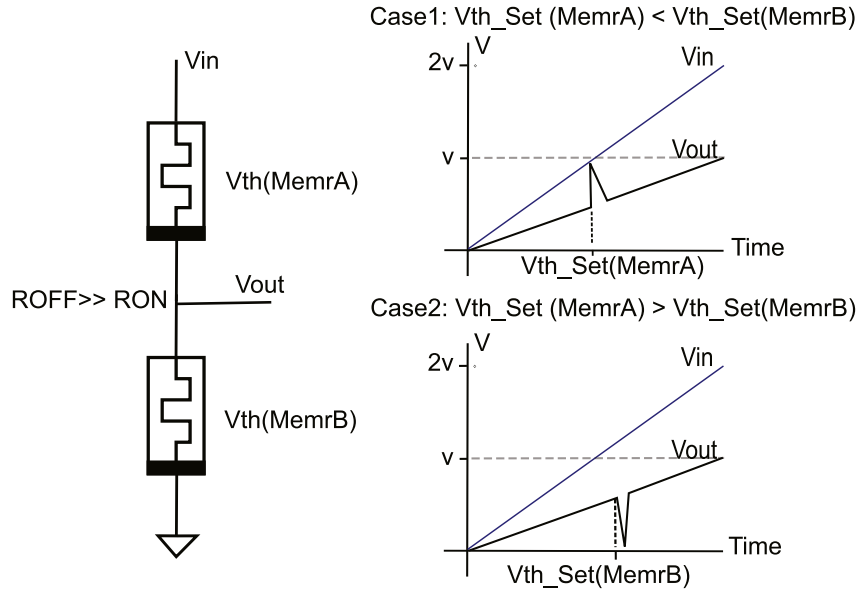


Fig. 3. Pulse generated while rising the applied voltage across the proposed memristors sub-circuit due to the memristors change of states, for $MR1_{vth} < MR2_{vth}$ and $MR1_{vth} > MR2_{vth}$.

at the input. Voltage division makes the voltage across each memristor rise at half the rate of the applied voltage until the voltage across the memristor with the lower threshold reaches its threshold and changes its state from *OFF* to *ON*, while the other memristor remains in the *OFF* state. The new state of the affected memristor reduces the voltage across it abruptly, which increases the voltage across the other memristor to reach and cross its *OFF* \rightarrow *ON* threshold and change its state to *ON*. Having both memristors in the *ON* state makes the voltage at the middle node revert back to $v_{in}/2$, which completes the formation of the pulse at the output.

The upward or downward shape of the pulse depends on which of the memristors turns *ON* first. If the top memristor, the one connected to the input v_{in} , turns *ON* first, the voltage at the output is pulled up to a value closer to v_{in} and when the other memristor turns *ON*

it returns back to $v_{in}/2$. This forms an upward pulse. On the other hand, if the bottom memristor's v_{th} is smaller than the top one, it turns *ON* first, and since it is connected to ground, its state changes, and the voltage at the output is pulled down towards the ground. That also changes the voltage across the other memristor and turns it *ON*, which sets the voltage at the output back to the original value of $v_{in}/2$. This process forms a downward-shaped pulse. The pulse shape at the output is captured and exploited. Both cases are presented in Fig. 4.

The error of the threshold voltage values that caused one memristor to turn *ON* before the other is exploited for a PUF, and the binary output is determined by the polarity of the pulse. The positive and negative polarity of the pulse is mapped to binary {0, 1}. The amplitude of the pulse at the output is reached when both memristors are in opposite states. For MRT and MRB representing the top and bottom

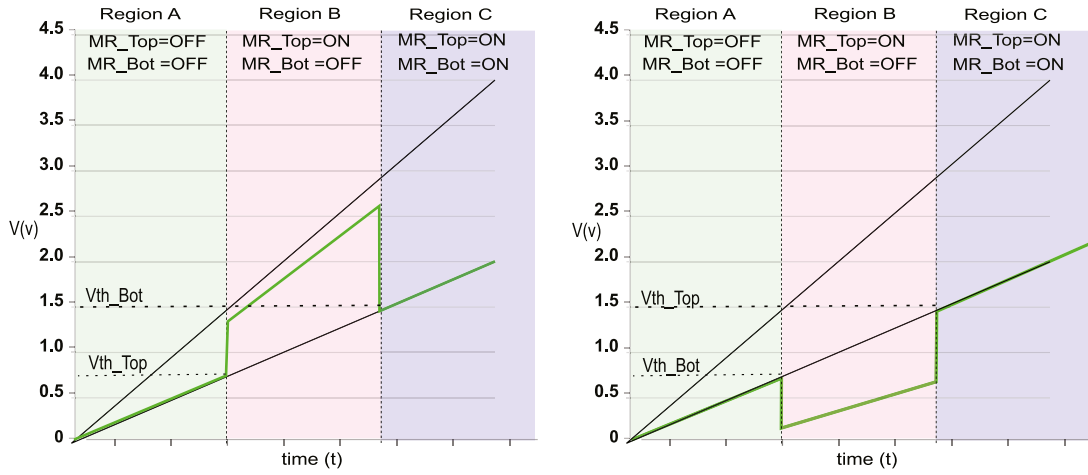


Fig. 4. Three regions of the dual memristors states that form a pulse shape at the output.

memristors respectively, and assuming their thresholds are not equal, i.e. $MRT_{vth} \neq MRB_{vth}$, one of two possible pulse shapes will form. Assuming R_{OFF}, R_{ON} represent the resistance values of *OFF*, *ON* states respectively, and the ratio of R_{OFF} to R_{ON} to be k , then by using voltage divider, the pulse amplitude of V_{out} for each case is:

$$V_{out} = \begin{cases} V_{in} * \frac{R_{OFF}}{R_{OFF} + \frac{1}{k} R_{OFF}} = \frac{k}{1+k} V_{in} & MRT_{vth} < MRB_{vth} \\ V_{in} * \frac{R_{ON}}{R_{ON} + k R_{ON}} = \frac{1}{1+k} V_{in} & MRT_{vth} > MRB_{vth} \end{cases} \quad (1)$$

2.3. Threshold voltage based dual memristor crossbar (TvDuXbar) PUF structure

The proposed TvDuMXbar PUF design uses two identical memristor crossbars, left and right crossbars represented by (LXbar) and (RXbar) respectively, such that, a dual memristor cell is formed by selecting one memristor from each crossbar. The two crossbars are connected such that the rows of the LXbar connect to a 90° rotated rows of RXbar. The orientation is such that every node of LXbar connects to a node with opposite polarity in the RXbar. The selected node between LXbar and RXbar represents the formed cell's output (OUT) which is considered the output of the PUF, as illustrated in Fig. 5. The system selection mechanism uses analog switching. An Analog demultiplexer (dmux) is used to direct the input to the selected column of LXbar, a router (WDM) is used to connect the selected rows of LXbar and RXbar together, and an analog multiplexer (mux) connects the columns of RXbar to ground. The output is read at the selected rows in the router. The selection components use transmission gates(TG) [15]. TG is a bidirectional switch that preserves the signal resolution. The *ON*–*OFF* resistance of TG is in the order of 10Ω and 10MΩ respectively. The resistance is controlled by the transistor geometrical W/L ratio. The pulse at the output is captured using a peak detector as shown in Fig. 5. The peak detector consists of a diode, switch, and, a capacitor. The size of the capacitor is proportional to the pulse width. A switch is added to reset the capacitor for the next output cycle.

2.4. PUF output generation process

The output generation process for $2[n \times n]$ PUF is as follows:

1. Initialize LXbar and RXbar memristors to R_{OFF} by applying a reversed bias *write* voltage.
2. Reset the peak detector capacitor.
3. Challenge is applied as an address of length $4 \times \log_2(n)$.
4. The address is partitioned to four equal sub-addresses (m_3, m_2, m_1, m_0) with m_3 and m_0 assigned to address's MSB and LSB respectively.

5. Each of the sub-addresses controls the selected left column, left row, right row, and right column respectively.
6. Apply rising voltage at v_{in} .
7. One of the selected memristors turns *ON* and then the other one follows.
8. A pulse is generated at the middle node of the formed cell circuit.
9. The peak detector and ADC digitize the signal to *high* or *low*.

As explained previously, the digital outcome at the output reflects the difference between the v_{th} values of the two selected memristors while both are in the *OFF* state. Due to the voltage divider, the rising voltage applied to both memristors is equal. This ensures fairness and prevents the memristor with high v_{th} from turning *ON* before the other one. The key factor of the process fairness is that both memristors are exposed to similar conditions. This needs to be further analyzed with the effect of crossbars sneak path current flow.

2.5. Sneak path

In crossbar structures, when a voltage is applied at the selected node, the current also flows on other paths besides the targeted element. Most of those currents flow through the neighboring elements. This is known as the Sneak Path effect. Sneak path (SP) is an ongoing challenge for crossbar memristors. The flow of the current through neighboring elements makes readings of the selected elements to be inaccurate. To see the effect of the sneak path on the proposed TvDuMXbar, an equivalent circuit of a general $2[n \times n]$ TvDuMXbar PUF with an address selection of (i, j, k, l) is presented in Fig. 6. For the selection of columns (i, l) of LXbar and RXbar respectively, $I(LXbarSP(i))$ and $I(RXbarSP(l))$ represent the SP current at LXbar and RXbar, and the total equivalent resistance parallel to the selected memristors represented by $R(LXbarSP(i))$ and $R(RXbarSP(l))$. The symmetry of $R(LXbarSP(i))$ and $R(RXbarSP(l))$, implies their value equivalence.

The effect of the SP on the proposed TvDuXbar $2[n \times n]$ crossbars is analyzed using the equivalent circuit presented in Fig. 6. Fig. 7(a) depicts a suppressed circuit, suppressing both LXbar and RXbar memristors, with the SP resistance of LXbar and RXbar presented as $R(LXbarSP(I))$, $R(RXbarSP(I))$ which represent the parallel resistance of the selected memristors. Assuming an address selection of (i, j, k, l) , which represents left columns, left row, right row, and right column respectively. In order to ensure equal current flow in the two selected memristors, the portion of the current $I(LXbarSP(i))$, $(RXbarSP(l))$ that flows in the two equivalent resistors $R(LXbarSP(I))$, $R(RXbarSP(l))$, which are parallel to the two selected memristors R_{kl} , L_{ji} , need to be minimized and equalized, i.e. $(I(LXbarSP(i)) = I(RXbarSP(l)))$.

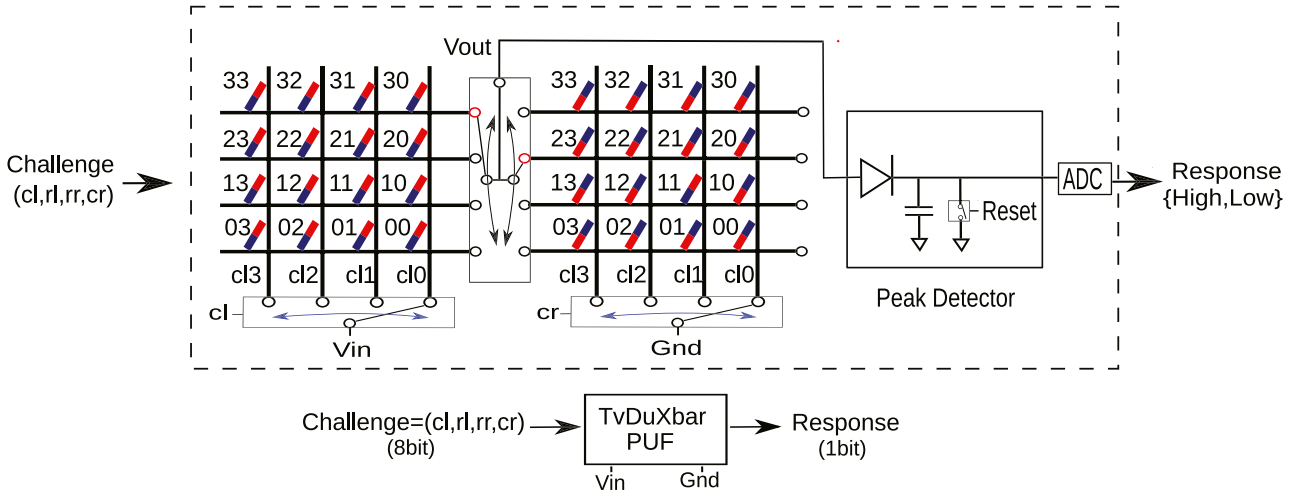


Fig. 5. Vth-based Dual Memristor Xbar PUF, with 8-bit challenge and one-bit response.

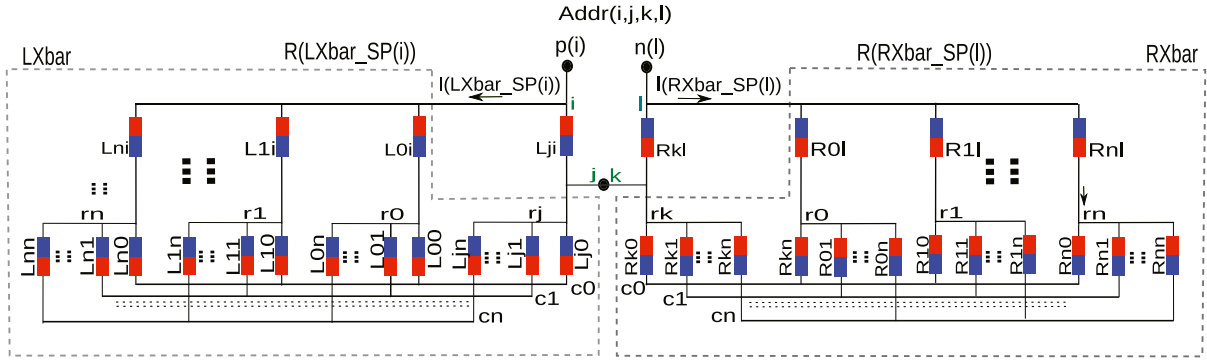


Fig. 6. TvDuMXbar equivalent circuit with address selection (i, j, k, l) , assuming the following switches resistance ($R_{ON} = 0$, $R_{OFF} = \text{inf}$).

Selecting the two memristors R_{kl} and L_{ji} with $v_{th}(R_{kl}) < v_{th}(L_{ji})$ as presented in Fig. 7(a), and applying a rising voltage at $p(i)$, the voltages across the selected memristors R_{kl} and L_{ji} are shown in Fig. 7(b) and [7(c)]. Fig. 7(b) represents the voltage rising across R_{kl} and L_{ji} when $I(LXbar_{SP}(i)) = I(RXbar_{SP}(l))$. Notice since $v_{th}(Bot) < v_{th}(Top)$ the rising voltage changes the state of the bottom memristor before the top one, as it should be. On the other hand, if $I(LXbar_{SP}(i)) < I(RXbar_{SP}(l))$ that makes $v(R_{kl})$ reaches $v_{th}(R_{kl})$ before $v(L_{ji})$, which makes the top memristor change states before the bottom one as shown in Fig. 7(c). Notice $t(V_{th}(Top)) < t(V_{th}(Bot))$. This produces a wrong reading for the PUF. If the current flow ratio in $R(LXbar_{SP}(i))$ and $R(RXbar_{SP}(l))$ are not equal, this impacts the current ratio flowing in the selected memristors. The current flow difference deviates the voltage at the output from $v_{in}/2$. So if the v_{th} difference of the selected memristors is smaller than the difference of voltages across, the one with the higher voltage across turns ON first, even if it is the one with bigger v_{th} as shown in Fig. 7(c). This deviation affects the fairness of the output decision, and it creates a bias towards the memristor with the higher current flow.

In the proposed design, while both selected memristors are in the same state, there is a symmetry in the parallel resistance of the two memristors as depicted in Fig. 6. This ensures similar current flow in the selected memristors and guarantees similar voltages across the two selected memristors when both are in the OFF state. This is true for any scaled $2[n \times n]$ circuit and for any arbitrary address selection. Note that as n increases, the SP current increases. Although this does not affect the ratio of the SP current of the two selected memristors, it increases the power consumption, due to an increase in the number of parallel resistances.

To reduce the SP current, a unidirectional memristor (UD) from a previous work demonstrated in [16], is used to minimize SP effect by blocking reversed current. Fig. 8a illustrates the IV graph of a unidirectional memristor showing asymmetric resistive switch, with a sweep between $-4V$ and $4V$; while Fig. 8b illustrates a micro photograph of the fabricated 3×3 unidirectional memristor crossbar. The unidirectional memristor's function is similar to an ideal diode, except for an additional memory feature. It only allows the passing of forward current and highly resists reverse current. A modified device with ON – OFF v_{th} set at $v = 0$ is used. The ON – OFF state change occurs at $v \leq 0$. The Uni-directional memristor (UD) symbol is drawn with red and blue to represent the polarity, where the positive port is at the red side.

With the UD memristors, all the SP currents are analyzed. Considering the same equivalent circuit of Fig. 6, and tracing the current flow in two arbitrary branches of LXbar and RXbar, since the memristors are connected back-to-back and front-to-front respectively, this ensures that all currents flowing through these branches are at least reverse-biased at one of the memristors, and hence blocked. The SP current $I(L_{1i})$ in the LXbar, for instance, is blocked by $L_{10}, L_{11}, \dots, L_{1n}$, since the memristors are connected back to back. Similarly, $I(R_{00}), I(R_{01}), \dots, I(R_{0n})$ in the RXbar are blocked by $R_{00}, R_{01}, \dots, R_{0n}$ respectively, since they are connected front-to-front. This is true for every SP branch in the left and right crossbars. Another situation that needs to be considered is at region B of Fig. 4. After the first memristor turns ON, the equivalent circuit is no longer of Fig. 7(a). Since the balancing is disrupted, the next concern is whether the second memristor of the cell turns on before any of the SP memristors. In other words, If R_{kl} is turned ON first, and short-circuited, then the concern is on whether L_{ji}

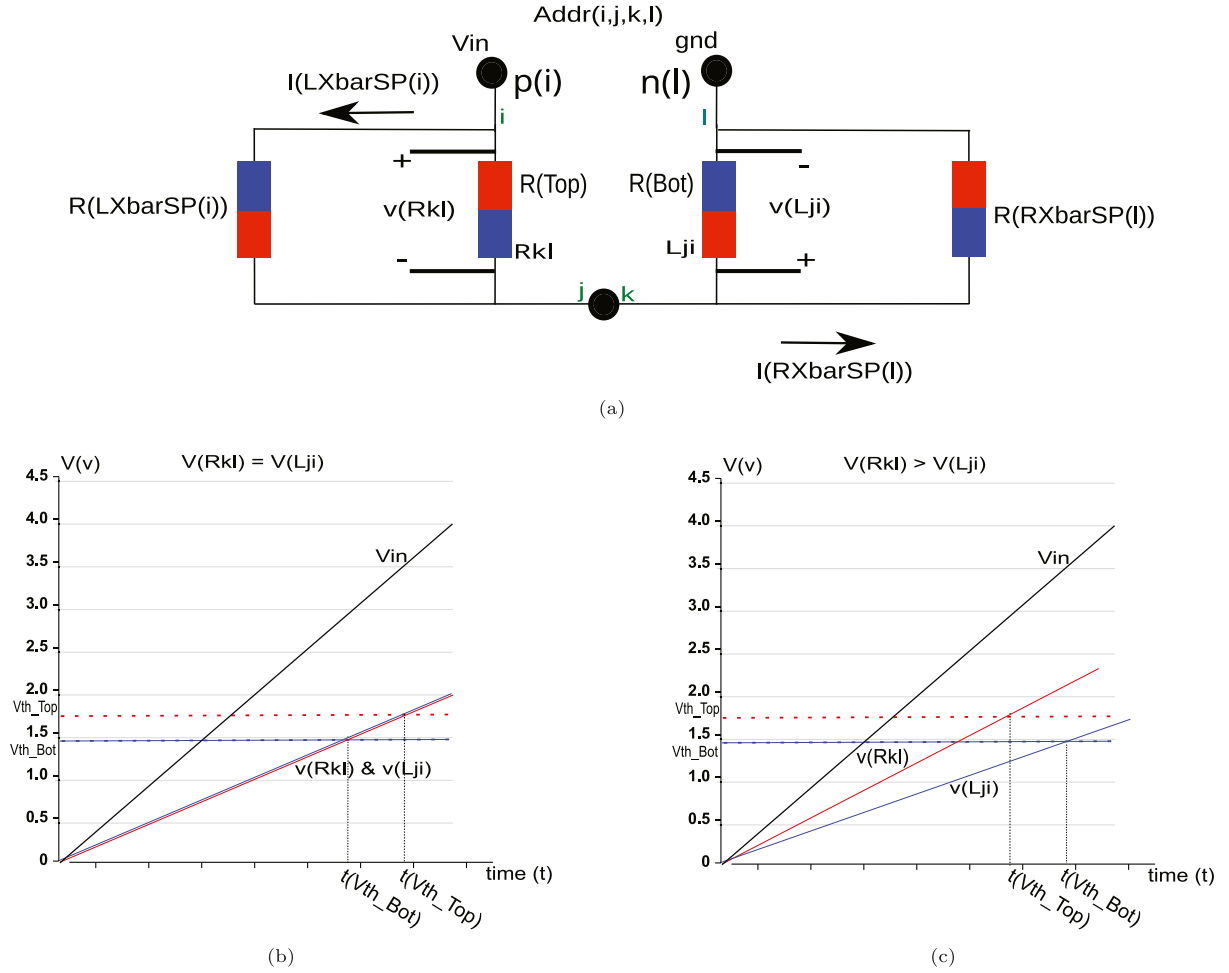
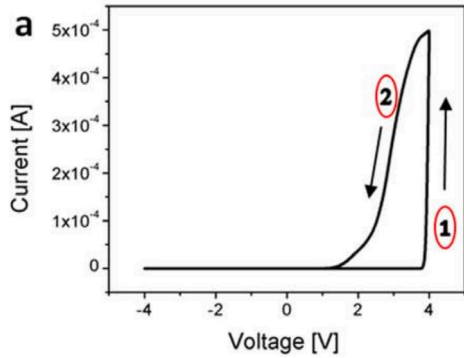
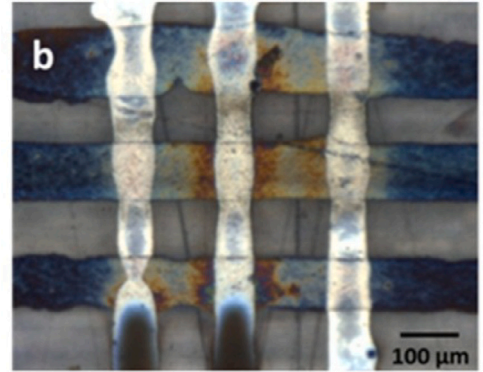


Fig. 7. (a) The proposed $2n \times n$ Xbars with suppressing LXbar and RXbar memristors, and i, j, k, l selection, $R_{SP}(Top), R_{SP}(Bot)$ representing the parallel resistance of the selected Top and Bottom memristors. (b)&(c) Plot of the voltage across the selected memristors when applying a rising voltage V_{in} for 2 cases: (b): $v(Rkl) = v(Lji)$, and (c): $v(Rkl) > v(Lji)$. Notice the impact of the voltage and the difference in the order of state change for the selected memristors.



(a) I-V curve of the Ag/ZnO/G-O/Ag 2×2 RRSD array



(b) 3×3 crossbar of the fabricated UD memristor.

Fig. 8. Resistive switching device with highly asymmetric current-voltage characteristics: a solution to backward sneak current in passive crossbar arrays [16].

turns ON before any of $R(RXbarSP(l))$ memristors. The cases at region B of Fig. 4 when the states of both memristors complement each other. i.e. ON, OFF and OFF, ON respectively are examined.

For the first case as shown in Fig. 6, assuming Lji to be ON and has very low resistance, part of the current $I(L)$ flows as $I(Rkl)$ and the rest shared equally as $I(Rk0, Rk1, \dots, Rk[n-1])$ through $Rk1, Rk2, \dots, Rkn$. Since the path of Rkl to $n(l)$ is shorter than the other memristors, and the fact that each of the other memristors ($Rk1, Rk2, \dots, Rkn$) is

connected back to back with a set of other memristors, and blocks all the $I(Rk1, Rk2, \dots, Rkn)$ currents, this guarantees that most of the current flow through Rkl , and hence it turns ON.

Similarly, when the bottom memristor Rkl is ON and has very low resistance, part of the current from the source $I(i)$ is distributed between $I(Lji)$ and the total sum of $I(L0i, L1i, \dots, Lni)$ through $Lji, L0i, \dots, Lni$. Since the current $I(Lji)$ through Lji has the shortest path to $n(l)$, and the fact that each of the other memristors $I(L0i, \dots, Lni)$ is

connected back to back with a set of other memristors, this guarantees a reversed bias that blocks all the $I(L0i, \dots, Lni)$ currents. Hence, most of the current flow through Lji , and it turns ON .

2.6. Masking multi output PUF

The proposed PUF binary output size is a single bit. This gives an adversary a 50% chance to predict the output. Improving the entropy requires more instances. For an n -bit output PUF, n instances of PUF need to be created. In practice, strong security key entropy size should be greater than 2^{80} . A strong PUF is one with a large CRP space. Since the challenge size is 120 bits which is brute force resilient and despite the possibility of collisions, the proposed PUF is considered as strong PUF since it can generate CRP space of size 2^{120} . Fig. 9 demonstrates a system of 120 instances of TvDuMXbar PUFs of size $2[4 \times 4]$. The input challenge for each instance is 8 bits, to be split into four 2-bit sub-addresses for the columns and rows. In general, as shown in previous sections, each $2[n \times n]$ PUF instance takes an input of size $4\log_2(n)$ and produces a 1-bit output. For a system specification of larger size challenge and response, more instances need to be created. PUF array enables an adversary to restructure its profile by applying a specific set of vectors that are needed to restructure the pattern and PUF signatures. By controlling and applying specific challenge vectors, it is possible to extract the table of each sub-PUF individually.

2.7. Extra security layer

The output of PUF system needs to be hidden to prevent the adversary from extracting its profile. A non-reversible non-linear function is needed to mask the output of the proposed PUF. Some literature [17] suggest XOR-ing the output of PUFs, while others suggest adding a hash function [18]. The first solution requires fewer resources but is not resilient against attacks, while the second solution requires higher resources. A better solution that is low-weight in both power and area, is to use a Non-Linear Feedback Shift Register (NLFSR). The suggested and proposed stream cipher is Lizard, which is known for its resilience and low weight [19]. Lizard utilizes 120-bit keys, 64-bit IVs, and a 121-bit inner state length as part of its core processes. As a result, it can generate up to 218 keystream bits per key/IV pair, which makes it suitable with currently used communication protocols, such as Bluetooth, WLAN, and HTTPS. LIZARD offers 80-bit security against key recovery attacks including Time-memory-data (TMD) trade-off attacks. The only attack that is known to weaken Lizard is the Differential Fault Attack (DFA) [20]. It is a very well-known technique to evaluate the security of a stream cipher. It is an invasive side-channel attack where an attacker injects a random fault using an invasive attack method such as a laser beam that is applied in to a cipher device to flip one or more bits in the cipher state. By observing and comparing the keystream generated from this altered internal state and the fault-free keystream, the attacker may identify the fault location, and then utilize the keystream together with the information of fault location to deduce the internal state. This invasive method has succeeded in crypto-analyzing many cipher streams besides Lizard, such as Grain v1, Trivium, and Mickey 2.0 [21,22]. However, since an invasive attack corrupts the memristors part of the PUF, this method is ineffective with the proposed PUF.

3. Simulation, analysis, and results

The typical evaluation key metrics for determining PUF performance are uniformity, uniqueness, unpredictability, and reliability. In this work, all specified metrics are analyzed. The unpredictability is analyzed post the NLFSR (Lizard) layer. Also, the effect of SP on output fairness and uniformity is examined.

3.1. Simulation setup

The relation between the crossbar array size and the challenge size in bits as demonstrated in previous sections is

$$\text{size}(\text{challenge}) = 4 \times \log_2(n)(\text{bits}).$$

For this simulation, it is chosen to optimize bit size with $n = \text{size}(\text{challenge}) = 16$ bits.

In this simulation, a $2[16 \times 16]$ TvDuMXbar PUF is modeled, implemented, and analyzed. The design is modeled and simulated using Systemc-AMS(TM) [23]. Systemc-ams is a free open-source system design and verification C++ library. Both traditional and UD memristors of Fig. 10 are modeled. The model's R_{ON} state is set to 10Ω , and R_{OFF} are checked in the range (1 k Ω -100 M Ω). R_{ON} value is chosen arbitrarily and kept unchanged while modifying R_{OFF} . The reason, as explained in Section 2.2, is due to the selected memristors which are initially OFF before applying the increased input voltage. Therefore, the value of R_{ON} will not affect the probability of which of the two selected memristors turns on first, since none of the two selected memristors are in the ON state. Even after one of the memristors turns on, R_{ON} has no other influences in the process until completion. The case of one ON memristor is discussed in Section 2.5. Furthermore, since in the simulation, smaller R_{ON} did not cause a wider sneak path, higher R_{ON} will not contribute to the sneak path either.

The algorithm of the memristor model is shown in Algorithm 1. The same algorithm is applied for a UD memristor by setting $vthL = 0$

Algorithm 1: Filament memristor model

```

1 Parameters;
2 vthL: Threshold voltage to set Roff;
3 vthR: Threshold voltage to set Ron;
4 initialization;
5 Ron=10;
6 Roff=1e7;
7 R=Roff; Initialize the state to Roff
8 Read v;
9 if v < vthL then
10   Rmem=Roff;
11   ;
12 else if v >= vthR then
13   Rmem=Ron;
14   ;
Result: Output Rmem

```

LXbar, and RXbar memristor vth parameters are stored in four arrays. LXbar memristors $vthL$ and $vthR$ are stored in two arrays $vthLL$ and $vthLR$ as follows:

$$vthLL_{n \times n} = \begin{bmatrix} vthll_{(n-1)(n-1)} & \dots & vthll_{(n-1)1} & vthll_{(n-1)0} \\ \vdots & \ddots & \vdots & \vdots \\ vthll_{1(n-1)} & \dots & vthll_{11} & vthll_{10} \\ vthll_{0(n-1)} & \dots & vthll_{01} & vthll_{00} \end{bmatrix},$$

$$vthLR_{n \times n} = \begin{bmatrix} vthlr_{(n-1)(n-1)} & \dots & vthlr_{(n-1)1} & vthlr_{(n-1)0} \\ \vdots & \ddots & \vdots & \vdots \\ vthlr_{1(n-1)} & \dots & vthlr_{11} & vthlr_{10} \\ vthlr_{0(n-1)} & \dots & vthlr_{01} & vthlr_{00} \end{bmatrix}$$

RXbar parameters are stored in $vthRL$ and $vthRR$ respectively. The DC value of the Vth is set to be fixed for LXbar and RXbar memristors.

Arrays vth error parameter initialization

The vth error matrix elements $e_{i,j}$ are assumed to be uniformly distributed. Each error set is carefully generated using a C++ random library. The set is then tested for uniformity using CHI^2 (χ^2) test. The parameter values ($\alpha = 0.05$, $n = 10$) which correspond to a critical value of 16.919 are usually used in the literature, we follow similar

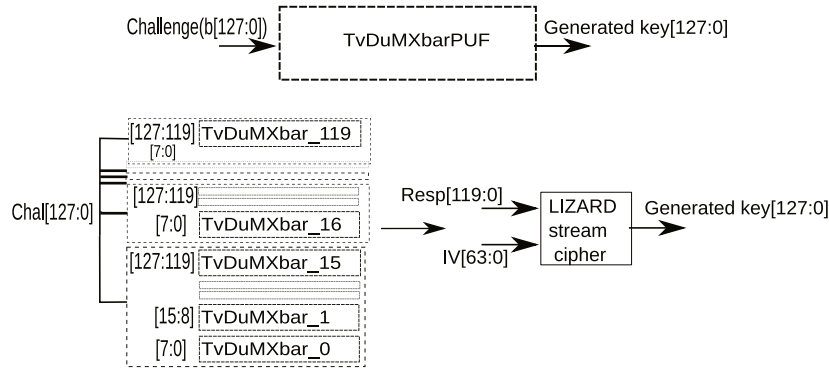


Fig. 9. The structure of TvDuMXbar PUF system that consists of 120 stacked TvDuMXbar instances, that accept a 128-bit challenge and generate a response of a 128-bit key stream. The challenge is repeated for every 16 TvDuMXbar instances. The LIZARD stream cipher is used to mask TvDuMXbar response. The seed consists of the response output with an IV vector, and it generates a 128-bit key stream.

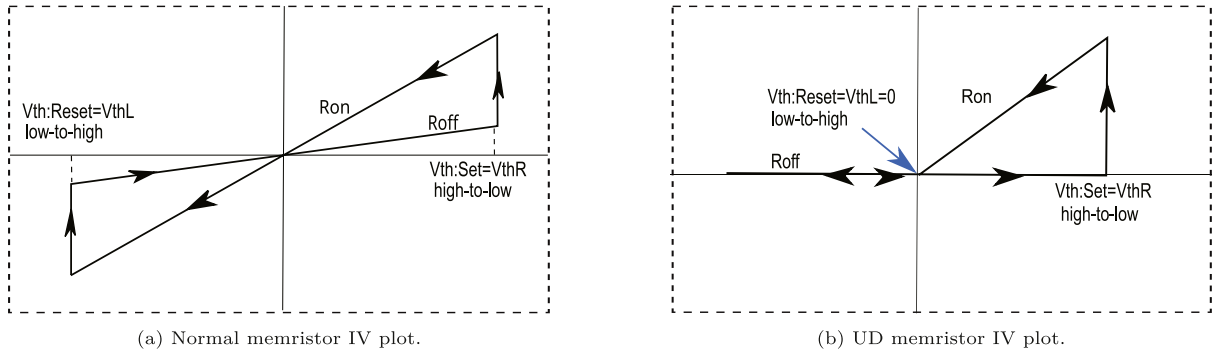


Fig. 10. A suppressed version of $2n \times n$ Xbars with i, j, k, l selection, at region 2, with (a) top memristor on, (b) bottom memristor on.

practice [24]. The generated sample sets are tested against (χ^2) critical value. To ensure higher accuracy, the set that passes the test are the one with value less than 20% of the critical value. The four passed sets are assigned to *ErrorLL*, *ErrorLR*, *ErrorRL*, *ErrorRR* matrices. Each of the matrices represents the negative and positive threshold parameters for each memristor in each crossbar respectively. The error arrays are then summed with the corresponding matrices that contain the nominal values $vthN$ to generate $vthLL_{n \times n}$, $vthLR_{n \times n}$, $vthRL_{n \times n}$, and $vthRR_{n \times n}$ parameter matrices. The representation of $ErrorLL_{n \times n}$ and $ErrorLR_{n \times n}$ of LXbar are as follow:

$$ErrorLL_{n \times n} = \begin{bmatrix} el_{(n-1)(n-1)} & \cdots & el_{(n-1)1} & el_{(n-1)0} \\ \vdots & \ddots & \vdots & \vdots \\ el_{2(n-1)} & \cdots & el_{21} & el_{20} \\ el_{1(n-1)} & \cdots & el_{11} & el_{10} \\ el_{0(n-1)} & \cdots & el_{01} & el_{00} \end{bmatrix},$$

$$ErrorLR_{n \times n} = \begin{bmatrix} er_{(n-1)(n-1)} & \cdots & er_{(n-1)1} & er_{(n-1)0} \\ \vdots & \ddots & \vdots & \vdots \\ er_{2(n-1)} & \cdots & er_{21} & er_{20} \\ er_{1(n-1)} & \cdots & er_{11} & er_{10} \\ er_{0(n-1)} & \cdots & er_{01} & er_{00} \end{bmatrix}$$

Similarly, *ErrorRL* and *ErrorRR* represent the negative and positive noise error matrices of RXbar. The vth arrays of LXbar and RXbar represent the sum of both nominal and the errors as follows:

$$[vth_{n \times n}] = [vthN_{n \times n}] + [Error_{n \times n}]$$

The TvDuMXbar PUF model is constructed using the dual memristor model of Fig. 3 as the core element. Initially, all the memristors are set to *OFF*. Note that both RXbar arrays $vthRL$, $vthRR$ are rotated 90° counterclockwise to match the orientation of Fig. 5. A selection of arbitrary challenges results in responses shown in the plots of Fig. 11. The result pulse shapes and output are verified to correspond to the

sign of the difference between the vth 's that correspond to LXbar and RXbar respectively.

3.2. Performance metrics

The performance metrics that are investigated are uniformity, uniqueness, unpredictability, and reliability.

The uniformity of PUF output depends on the random distribution of the error of the crossbar elements, which should result in a random output when taking the difference of two arbitrarily selected memristors from the two crossbars. It was explained in previous sections that SP creates a parallel resistance to each of the selected memristors. This affects the voltages across each of the selected memristors and hence influences the output fairness. Minimizing the difference of these voltages drastically reduces the biasing. Two methods are investigated to test the uniformity. The occurrence of '0's and '1's in response bits of 1000 PUFs when a common challenge is applied, and the occurrence of '0's and '1's in the response for randomly selected 1000 challenges when applied to a single PUF. Ideally the occurrence must be 50%.

The uniqueness is related to the PUF error signature. To test the uniqueness, a common challenge vector is applied to 100 instances of PUF core, and pre-Lizard responses are collected, and analyzed. Ideally, the occurrences of '1' and '0' must be equal (50%).

The unpredictability strength depends on the hardware that is connected to the PUF array as explained in Section 2.6. The ultra-lightweight stream cipher NLFSR/Lizard is used in the proposed PUF. In this simulation setup, an array of 120 instances of $2[16 \times 16]$ TvDuMXbar PUF ($n = 16$) is used, with an arbitrary 64-bit initialization vector (IV) are used as inputs to LIZARD stream cipher. After 256 clock cycles, the output is collected and a CRP is generated.

The reliability metric is defined as how efficient PUF is in reproducing the same response bits under different operating conditions. In this

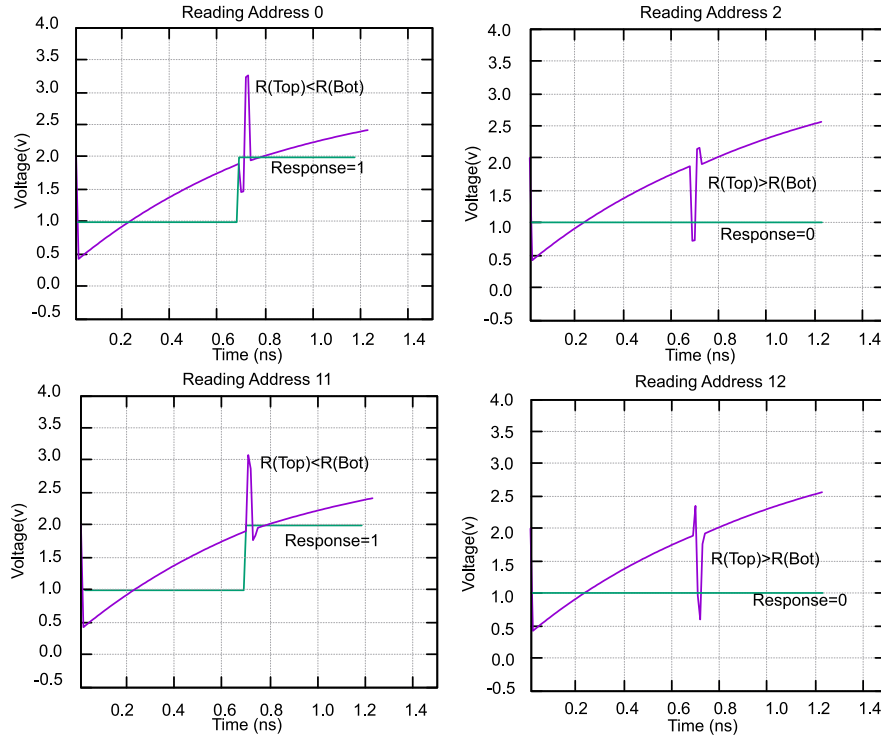


Fig. 11. PUF response for some selected array cells. The output (green) is biased at 1 volt. The peak detector gives a step increase in the output for positive pulses only. Note the small pulses due to the sneak path before and after the selected cell main pulse, which does not affect the decision.

work, the reliability is investigated within a temperature interval. In literature, it is reported that the memristor threshold voltage exhibits a deviation in an approximate interval of $[-0.6v_{th}, 0.6v_{th}]$ when varying temperature between $[1.5\text{ K}, 300\text{ K}]$ [25,26]. So it is a valid argument to assume that the threshold voltage is a function of temperature. For the reliability test purpose, the type of relationship between the temperature and the threshold voltage is not of importance as long as the mapping between the extreme temperatures and threshold voltages is known, since the purpose of the experiment is to test the output consistency for all ranges of threshold voltages that corresponds to the temperature interval. The applied temperature is assumed to be normally distributed with the nominal temperature to be the expected value. Since both crossbars occupy a considerably small area, the temperature divergence across them is considered negligible. So it is safe to assume that the temperature is constant across the two crossbars. The test strategy starts by finding the extreme threshold voltages that correspond to the extreme temperature. Then to mimic the temperature variation, it is sufficient to sweep the threshold voltages between these extreme values. The reliability is then found by varying the threshold voltages while applying the same challenges. The threshold voltage, and the response values which are represented by $v_{thN} + v_{th_err}[i, j]$, and $Resp_{ref}$ respectively, are considered as the nominal and are set as reference points at room temperature. Note in this experiment the manufacturing variation errors are included in the threshold nominal values. The threshold voltage that contributes to temperature change is represented by v_{th_T} , and it is added to all elements of both LXbar and RXbar arrays. v_{th_T} is then swept between the extreme thresholds with a step size of 0.1. These extreme thresholds are found in most literature not to exceed $[-0.6v_{th}, +0.6v_{th}]$ which correspond to the temperature interval of $[1.5\text{ K}, 300\text{ K}]$. At every iteration, Xbars arrays are updated with the new values of v_{th_T} , and the response for the tested challenge is compared with its counterpart reference. If at any of the iterations, the two responses do not match, the challenge is labeled as “unstable”. At the end of the experiment, the reliability is calculated as the ratio of the stable challenges to the total challenges. Listing 1 demonstrates the code for the reliability test. The experiment is tested

for randomly chosen 1000 challenges and has been conducted using 1000 PUF samples. Each sample is represented by different error arrays v_{th_err} . For this experiment, the challenge is applied at every iteration. For a nominal v_{thN} of 2.0, v_{th_T} is swept from $-0.6v_{thN}$ to $0.6v_{thN}$ or -1.2 to 1.2 and hence the net v_{th} sweep is $-3.2 + v_{therr}[i, j]$ to $3.2 + v_{therr}[i, j]$ for a step size of 0.1, which results in approximately 64 iterations.

Listing 1: Reliability verification while varying threshold voltage that is contributed by temperature variation

```
// Challenge address=(leftcol=i,leftrow=j,
    rightrow=k,rightcol=l)
vthN=2.0;// Design specification threshold
    voltage
vth_step=0.1;
left_bound=-0.6*vthN;
right_bound=0.6*vthN;

for all challenges
    for (float vth_T = left_bound; vth_T <
        right_bound; vth_T += 0.1) {
        //Updating vth matrices
        for all m,n
            vthL[m,n]=vthN+vthL_err[
                m,n]+vth_T
            vthR[m,n]=vthN+vthR_err[
                m,n]+vth_T
        \\Test Response for challenge (i
            ,j,k,l)
        Response=vthL[i,j] - vthR[k,l]
        //Response test
        if (Response !=ResponseRef(i,j,k
            ,l) )
            state[challenge(i,j,k,l)
                ]=unstable;
    }
```

Table 1

The difference of the voltage across both selected memristors with varying R_{OFF} for both traditional and UD memristors.

Memristor not UD		Memristors UD	
R(High) (Ω)	VMR(Top)-VMR(Bot) (v)	R(High) (Ω)	VMR(Top)-VMR(Bot) (v)
1.0E3	1.21E-2	1.0E3	1.83E-3
1.0E4	1.81E-2	1.0E4	2.31E-4
1.0E5	6.63E-2	1.0E5	2.70E-5
1.0E6	6.63E-2	1.0E6	2.71E-6
1.0E7	6.63E-2	1.0E7	3.8E-7

Table 2

The error due to SP for different R_{High} for both traditional and UD memristors for a sample of 100 CRP.

Memristor not UD		Memristors UD	
R(High) (Ω)	Output error (%)	R(High) (Ω)	Output error (%)
1.0E3	10%	1.0E3	7%
1.0E4	10%	1.0E4	0.01%
1.0E5	10%	1.0E5	0.001%
1.0E6	10%	1.0E6	1E-4%
1.0E7	10%	1.0E7	1E-7%

Table 3

Electrical and device parameters of Memristors M1, M2 for P1, P2 respectively [27].

Device	R_{High}	R_{Low}	V_{th+}	V_{th-}
P1	8 G Ω	8 k Ω	+4 V	-4 V
P2	10 G Ω	10 M Ω	+1.5 V	-1.5 V

3.3. Analysis and results

Table 1 shows an improvement in the output uniformity since the output biasing that is caused by the SP is reduced. The table demonstrates the difference in the voltages across the two selected memristors when input is applied. Ideally, the difference must be zero (unbiased). The simulation is performed for different values of R_{High} for both the traditional and UD memristors. By comparing the results, one observes that the increase of R_{High} for traditional memristors has a small improvement in minimizing SP current. On the other hand for UD memristors, the accuracy is proportional to the resistive values of R_{High} .

To find the biasing error caused by SP, an ideal output is generated which consists of just the difference of the selected memristors' threshold voltages, by using the array indices and comparing the result of TVDuMXbar PUF output. The test is performed using 100 randomly selected samples for different R_{High} of UD memristors. The results are presented in Table 2. It was found that the error rates improved for larger R_{High} . This is expected since the error rate is proportional to the probability of the two selected samples having v_{th} difference being less than the values shown in Table 1.

3.4. Performance metrics analysis

In this simulation, $n = 16$ is chosen and backed with a LIZARD stream NLFSR. 120 instances of $2[16 \times 16]$ memristors are used along with an arbitrary 64-bit initialization vector (IV) as input to LIZARD NLFSR to improve the unpredictability. After 256 clock cycles, the output is collected and a CRP set is generated as shown in Fig. 12.

The result is compared with PUFs P1, P2 that are selected from a previous work [27]. P1 and P2 are two different dual Xbar PUF setups with memristors M1, M2 respectively. M1, M2 electrical, and device parameters are shown in Table 3.

Table 4

Performance for $16 \times 16 \times 2$ PUF.

Performance	PUF P1	PUF P2	Proposed	Ideal
Reliability	95%	95%	94.4%	100%
Uniformity	48.5%	48%	50.6%	50%
Uniqueness	50.1%	50.17%	50.19%	50%

Table 5

Memristors-based crossbar PUFs power consumption range, compared to TvDuMXbar PUF.

References	Power consumption (uW)
[13]	417-453
[12]	564-1633
TvDuMXbar	0.9

Performance evaluation parameters of the proposed PUF along with the previous work P1, P2 in Table 4. The results are listed in Table 4. It can be observed that the performance of the proposed PUF is close to the ideal and satisfies the PUF evaluation criteria.

3.5. Power consumption

The power consumption for a read and write operation per memristor cell is 25 and 400 nW respectively [28]. Since the proposed PUF is a comparator-free design, the dominant power is consumed during the memristors' "write" operation, which is low in our case. Table 5 demonstrates the comparisons of the power consumption of the proposed TvDuMXbar with other designs found in the literature.

From Table 5, it is evident that the power consumption of memristor crossbar PUF from the previous art is significantly higher than that of our proposed TvDuMXbar. The ratio in power consumption, which is four orders of magnitude, is attributed to a specific factor in the design of the memristor-based PUF. The primary component that contributes to high power consumption in the other memristor crossbar PUFs is the CMOS comparators. The literature on memristor crossbar PUFs [29–32] indicates that these designs use at least one comparator.

The comparator is a crucial element for the decision-making process in the PUF. To generate the response during PUF operation, the selected memristor voltage is compared to either another selected memristor's voltage or a reference voltage. This additional CMOS component in the memristor-based PUF can substantially increase its overall power consumption. However, the dual-memristor cell in TvDuMXbar does not require a comparator. Few authors provided power analysis data for their memristor PUF crossbars [12,13]. Unfortunately, the authors of [29–31,33] have not discussed the power consumption of their PUF core design. However, since the comparators are the dominant factors in the memristor PUF designs in terms of power consumption, it is worth mentioning that the power consumption of a comparator as found in literature [34–36] is in the range of [29.7, 420] uW. On the other hand, for the TvDuMXbar, the power consumed for the "write" operation which depends on the R_{OFF} value, is $\frac{v^2}{R_{OFF}}$. For V_{in} of 3v, and R_{OFF} of 1e7 Ω , the power consumed is 0.9uW. The power consumption for the proposed PUF shown in Table 5, excludes the portion consumed by the Lizard hardware implementation which has an estimated power consumption of only 2.1 μ W, which is still way less compared to the other implementations [19].

4. Conclusions

In this paper, a novel fully passive Threshold-based Dual Memristor Crossbar PUF design, using a unidirectional memristors model, is presented. The proposed PUF exploits the randomness of device threshold voltage variation during the manufacturing process. The analysis shows that the symmetry structure and the use of unidirectional memristors improve the performance against SP current. In addition, our proposed

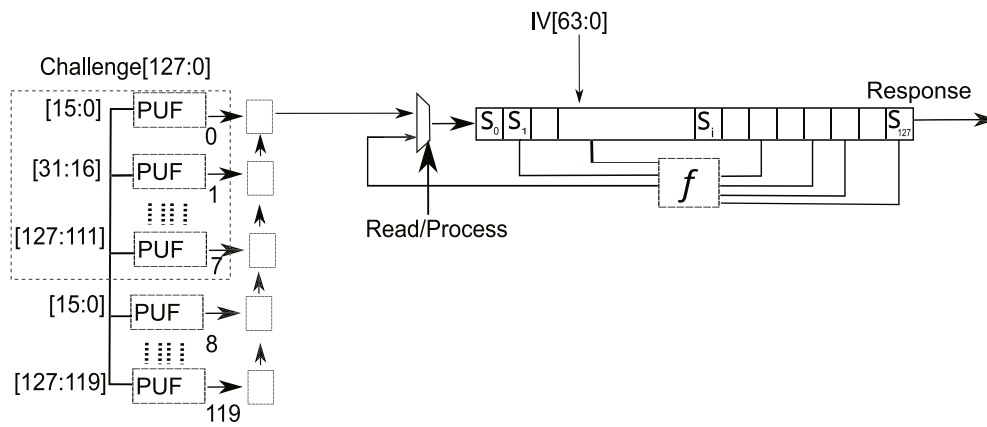


Fig. 12. A stack of 120 TvDuMXbar PUF instances is used with 64 bit IV as a seed to Lizard NLSR, to generate a 128-bit response. The challenge is distributed between every eight instances. The response is read after 256 clock cycles.

design is based on dual memristor crossbar PUF using a comparator-free design resulting in significantly lower power consumption and sneak path resiliency. The design uses less area compared to traditional crossbar PUF. The response of this proposed PUF as any other conventional 2D array PUF needs to be post-processed with a hash function to generate a cryptographic key with full bit entropy. A low-weight stream cipher “Lizard” uses fewer resources than a typical hash function. Unlike other crossbar PUFs, the proposed TVDUXbar PUF does not require an active comparator, which reduces the required resources.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

This work was supported by National Priorities Research Program (NPRP) under Grant NPRP13S-0212-200345 from the Qatar National Research Fund (a member of Qatar Foundation). The findings herein reflect the work and are solely the responsibility of the authors.

Furthermore, The work is an extended version of a previous paper entitled “Memristors Threshold Based Physical Unclonable Function” [10] which was presented at the 34th IEEE International Conference on Microelectronics (ICM 2022) in Casablanca in Dec. 7-10, 2022”.

References

- Li J, Seok M. Ultra-compact and robust physically unclonable function based on voltage-compensated proportional-to-absolute-temperature voltage generators. *IEEE J Solid-State Circuits* 2016;51(9):2192–202.
- Mispan MS, Halak B, Chen Z, Zwolinski M. TCO-PUF: A subthreshold physical unclonable function. In: 2015 11th conference on Ph. D. research in microelectronics and electronics. IEEE; 2015, p. 105–8.
- Kumar R, Burleson W. On design of a highly secure PUF based on non-linear current mirrors. In: 2014 IEEE international symposium on hardware-oriented security and trust. IEEE; 2014, p. 38–43.
- Pappu R, Recht B, Taylor J, Gershenfeld N. Physical one-way functions. *Science* 2002;297(5589):2026–30.
- Simons P, van der Sluis E, van der Leest V. Buskeeper PUFs, a promising alternative to D flip-flop PUFs. In: 2012 IEEE international symposium on hardware-oriented security and trust. IEEE; 2012, p. 7–12.
- Cao Y, Zhang L, Zalivaka SS, Chang C-H, Chen S. CMOS image sensor based physical unclonable function for coherent sensor-level authentication. *IEEE Trans Circuits Syst I Regul Pap* 2015;62(11):2629–40.
- Zhao X, Zhao Q, Liu Y, Zhang F. An ultracompact switching-voltage-based fully reconfigurable RRAM PUF with low native instability. *IEEE Trans Electron Devices* 2020;67(7):3010–3.
- Chua L. Memristor-the missing circuit element. *IEEE Trans Circuit Theory* 1971;18(5):507–19.
- Liu S, Wang Y, Fardad M, Varshney PK. A memristor-based optimization framework for artificial intelligence applications. *IEEE Circuits Syst Mag* 2018;18(1):29–44.
- Al-Tamimi A, Ali S, Cao Y, Bermak A. Memristors threshold based physical unclonable function. In: 2022 International conference on microelectronics. IEEE; 2022, p. 130–4.
- Gül F. Addressing the sneak-path problem in crossbar RRAM devices using memristor-based one Schottky diode-one resistor array. *Results Phys* 2019;12:1091–6.
- Rose GS, Meade CA. Performance analysis of a memristive crossbar PUF design. In: 2015 52nd ACM/EDAC/IEEE design automation conference. IEEE; 2015, p. 1–6.
- Uddin M, Majumder MB, Rose GS, Beckmann K, Manem H, Alamgir Z, et al. Techniques for improved reliability in memristive crossbar PUF circuits. In: 2016 IEEE computer society annual symposium on VLSI. IEEE; 2016, p. 212–7.
- Ali S, Bae J, Lee CH, Choi KH, Doh YH. All-printed and highly stable organic resistive switching device based on graphene quantum dots and polyvinylpyrrolidone composite. *Org Electron* 2015;25:225–31. <http://dx.doi.org/10.1016/j.orgel.2015.06.040>, URL <https://www.sciencedirect.com/science/article/pii/S1566119915300112>.
- Balaji GN, Aathira V, Ambhikavathi K, Geethiga S, Havin R. Low power and high speed synchronous circuits using transmission gates. *Asian J Res Soc Sci Humanit* 2017;7(2):713–20.
- Ali S, Bae J, Lee CH, Kobayashi NP, Shin S, Ali A. Resistive switching device with highly asymmetric current–voltage characteristics: a solution to backward sneak current in passive crossbar arrays. *Nanotechnology* 2018;29(45):455201. <http://dx.doi.org/10.1088/1361-6528/aad6f>.
- Zhou C, Parhi KK, Kim CH. Secure and reliable XOR arbiter PUF design: An experimental study based on 1 trillion challenge response pair measurements. In: Proceedings of the 54th annual design automation conference 2017. 2017, p. 1–6.
- Shamsoshoara A, Korenda A, Afghah F, Zeadally S. A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. *Comput Netw* 183:107593.
- Hamann M, Krause M, Meier W. LIZARD-A lightweight stream cipher for power-constrained devices. *IACR Trans Symmetric Cryptol* 2017;2017(1):45–79.
- Zhen M, Tian T, Wenfeng Q. Differential fault attack on the stream Cipher LIZARD. *Chin J Electron* 2021;30(3):534–41.
- Banik S, Maitra S, Sarkar S. Improved differential fault attack on MICKEY 2.0. *J Cryptogr Eng* 2015;5:13–29.
- Skorobogatov S. Optically enhanced position-locked power analysis. In: Cryptographic hardware and embedded systems-CHES 2006: 8th International workshop, Yokohama, Japan, October 10–13, 2006. Proceedings 8. Springer; 2006, p. 61–75.
- Vachoux A, Grimm C, Einwich K. Towards analog and mixed-signal SOC design with systemc-AMS. In: Proceedings. DELTA 2004. second IEEE international workshop on electronic design, test and applications. IEEE; 2004, p. 97–102.
- Wilson EB, Hilferty MM. The distribution of chi-square. *Proc Natl Acad Sci* 1931;17(12):684–8.

- [25] Beilliard Y, Paquette F, Brousseau F, Ecoffey S, Alibert F, Drouin D. Investigation of resistive switching and transport mechanisms of $\text{Al}_2\text{O}_3/\text{TiO}_2$ -x memristors under cryogenic conditions (1.5 K). *AIP Adv* 2020;10(2).
- [26] Han CY, Han ZR, Fang SL, Fan SQ, Yin JQ, Liu WH, et al. Characterization and modelling of flexible VO_2 Mott Memristor for the artificial spiking warm receptor. *Adv Mater Interfaces* 2022;9(19):2200394.
- [27] Khan MI, Ali S, Al-Tamimi A, Hassan A, Ikram AA, Bermak A. A robust architecture of physical unclonable function based on memristor crossbar array. *Microelectron J* 2021;116:105238.
- [28] Ali S, Bae J, Lee CH, Shin S, Kobayashi NP. Ultra-low power non-volatile resistive crossbar memory based on pull up resistors. *Org Electron* 2017;41:73–8.
- [29] Gao Y, Ranasinghe DC, Al-Sarawi SF, Kavehei O, Abbott D. Memristive crypto primitive for building highly secure physical unclonable functions. *Sci Rep* 2015;5(1):12785.
- [30] Nili H, Adam GC, Hoskins B, Prezioso M, Kim J, Mahmoodi MR, et al. Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors. *Nat Electron* 2018;1(3):197–202.
- [31] Gao B, Lin B, Pang Y, Xu F, Lu Y, Chiu Y-C, et al. Concealable physically unclonable function chip with a memristor array. *Sci Adv* 2022;8(24):eabn7753.
- [32] Singh J. Implementation of memristor towards better hardware/software security design. *Trans Electr Electron Mater* 2021;22(1):10–22.
- [33] Pang Y, Gao B, Lin B, Qian H, Wu H. Memristors for hardware security applications. *Adv Electron Mater* 2019;5(9):1800872.
- [34] Naik P. A new high precision dynamic comparator for low power high speed ADCs. *Int J Eng Trends Technol* 2015;22(5):225–9.
- [35] Singh S, et al. A novel CMOS dynamic latch comparator for low power and high speed. *Int J Microelectron Eng (IJME)* 2015;1(1):17–24.
- [36] Zhang S, Li Z, Ling B. Design of high-speed and low-power comparator in flash ADC. *Procedia Eng* 2012;29:687–92.