mrPUF: A Novel Memristive Device Based Physical Unclonable Function

Yansong Gao[1,2], Damith C. Ranasinghe[2], Said F. Al-Sarawi[1], Omid Kavehei[3], and Derek Abbott[1]

[1] School of Electrical and Electronic Engineering, The University of Adelaide, SA 5005, Australia, (yansong.gao,said.alsarawi,derek.abbott)@adelaide.edu.au,
[2] Auto-ID Labs, School of Computer Science, The University of Adelaide, SA 5005, Australia, damith.ranasinghe@adelaide.edu.au,
[3] Functional Materials and Microsystems Research Group, School of Electrical and Computer Engineering, Royal Melbourne Institute of Technology, Victoria 3001, Australia, omid.kavehei@rmit.edu.au

Abstract. Physical unclonable functions (PUFs) exploit the intrinsic complexity and irreproducibility of physical systems to generate secret information. They have been proposed to provide higher level security as a hardware security primitive. PUFs are an emerging and promising solution for establishing trust in an embedded system with low overhead with respect to energy and area. Most current PUF designs focus on exploiting process variations in CMOS (Complementary Metal Oxide Semiconductor) technology. In recent years, progress in nanoelectronic devices such as memristors has demonstrated the prevalence of process variations in scaling electronics down to the nano region. In this paper we exploit the extremely large information density available in the nanocrossbar architecture and the huge resistance variations of memristors to develop on-chip memristive device based PUF (mrPUF). Our proposed architecture demonstrates good uniqueness, reliability and improved number of challenge-response pairs (CRPs). The proposed mrPUF is validated using nanodevices characteristics obtained from experimental data and extensive simulations. In addition, the performance of our mrPUF is compared with existing memristor based PUF architectures. Furthermore, we analyze and demonstrate the improved security with respect to model building attacks by expounding upon the inherent nature of nanocrossbar arrays where we use the independence between nanocrossbar columns to generate responses to challenges.

Keywords: Physical unclonable function, PUFs, hardware security, memristor, nanocrossbar, model building attack.

1 Introduction

Modern security systems used to establish the authenticity of products or identity of users are based on the principle of protecting 'keys' required for securing systems and allowing solely authorized participants to be able to obtain secret keys. However, developments in invasive and non-invasive physical tampering methods such as micro-probing, laser cutting, and power analysis and monitoring have

made it possible to extract digitalized secret information from integrated circuits (ICs), and consequently compromising conditional access systems by using illegal copies of the secret information. Tamper proofing techniques used in smartcards to protect the secret keys such as cutting power or tripping tamper-sensitive circuitry that leaks the secret information have shown to be vulnerable to physical attacks [1]. For instance, an adversary can remove a smartcard package and reconstruct the layout of the circuit using chemical and optical methods. Even the data in some types of non-volatile memories, such as electrically erasable programmable read-only memory (EPROM) can be revealed by sophisticated tampering methods. To protect secret information, the emerging area of physical unclonable functions (PUFs) promise a reliable and highly-secure approach and is receiving increasing attention. PUFs express inherent and unclonable instance-specific features of physical systems and provide an alternative to storing keys on insecure hardware devices [2]. A PUF produces an output signal (response) to an external physical excitation signal (challenge). The response is a function of the physical properties of the system such as signal delay variations across identical integrated circuits and the applied challenge. A significant advantage in using PUFs is that the key is not digitally stored in the memory of a device (such as smart cards) but is extracted from device specific characteristics in response to an external stimulus. Besides the aforementioned device authentication and identification, PUFs can be used for cryptographic key generation and more complicated cryptographic protocols such as oblivious transfer (OT), bit commitment (BC), key exchange (KE) [3–7].

Conventional PUFs such as Ring Oscillator PUF, Arbiter PUF, SRAM (static random access memory) PUF exploit uncontrollable process variations in conventional CMOS fabrication technology. Although technological developments in CMOS devices such as FinFET enhanced device operations in ultra deep submicron technologies, such developments are expected to confront the physical limitation imposed by the continuing trend towards smaller feature sizes [43]. Consequently, CMOS based PUF designs will also face a roadblock in terms of providing secure physical unclonable functions in the future.

Recent developments in nanoelectronics demonstrated a potentially low-cost and high-performa nce nonionic nonvolatile resistive memory device called the memristor (in literatures, memristor and memristive device is used interchangeably) [8–10]. Memristors have inherent randomness due to fabrication process variations (i.e, thickness, cross-sectional area). This inherent randomness provides opportunities for building up physical unclonable functions with high performance. Furthermore, these nanodevices are easy to fabricate and are compatible with CMOS fabrication processes offering a potentially low cost security primitive.

The proposed mrPUF architecture, which combines nanocrossbars and current mirror controlled ring oscillators, and the proposed authentication mechanism are unique and have not been considered in the past to the best of our knowledge. Our architecture allows the extraction of secret information by exploiting the abundant variations in nanodevices and nanofabrication. A summary of our contributions in this paper are:

1. We propose a novel PUF architecture that exploits the fabrication variations inherent in nano-electronic devices. In particular we exploit the significant

variations in the resistance values on a nanocrossbar structure based resistive memory to build mrPUF.
2. We conduct extensive studies to evaluate mrPUF and demonstrate its superior performance with respect to key performance metrics: diffuseness; uniqueness; and reliability.
3. We show that mrPUF is resistant to model building attacks by exploiting characteristics inherent to nanocrossbar arrays, in particular the independence of information in individual columns, to develop a challenge selection strategy for a direct authentication mechanism using a mrPUF. We also demonstrate the significantly large number of challenge response pairs possible with our proposed architecture when compared to existing memristor based PUF designs.

The rest of this paper is organized as follows: Section 2 presents related work; The mrPUF architecture is presented in Section 3; Section 4 evaluates mrPUF's performance metrics and compares it with other PUF structures in the literature; Section 5 presents two applications of mrPUF with respect to key generation and challenge response pairs based authentication protocol, and analyses their security; Section 6 compares mrPUF with other memristor based PUFs and Section 7 concludes this paper.

2 Related Work

Over the years, a number of PUF structures have been proposed, built and analyzed. These include *time delay based* PUFs such as the Arbiter PUF [2, 11] (APUF), Feed-Forward APUF [12], An arbiter based PUF built on current starved inverters [13], Ring-Oscillator PUF [14] (RO-PUF), and Glitch PUF [15]; *Memory-based* PUFs leveraging device mismatch such as SRAM PUF [16, 17], Latch PUF [18], Flip-flop PUF [19, 20], Butterfly PUF [21]. A comprehensive review of different PUF architectures can be found in [22, 23].

Here we introduce the RO-PUF as our mrPUF will integrate it. In addition, we provide a brief review of nanocrossbar arrays and memristive devices which our PUF architecture utilizes. Furthermore, we briefly review previous memristor based PUF architectures.

2.1 RO-PUF

The RO-PUF is one of the leading microelectronic PUF designs because of its relatively high reliability. A typical RO-PUF circuit consists of k ring-oscillators, two k-to-1 multiplexers that select a pair of ring-oscillators, RO_i and RO_j, two counters and a comparator, as shown in Fig. 1. All the ring-oscillators in this structure are identical. Ideally, the frequency of each oscillator is unique, however, because the oscillating frequency is a function of the physical device parameters, which are subject to device process variation, the oscillation frequencies of each oscillator are not all identical. Therefore, the oscillation frequencies of each pair is compared by counting this frequency using a digital counter. If $f_i < f_j$ (where f_i and f_j are the oscillating frequencies of RO_i and RO_j, respectively) the digital comparator output will be '0', otherwise '1'. The pairing of oscillators is controlled using two digital multiplexers, each use a subset of the input challenge bits to select an oscillator.

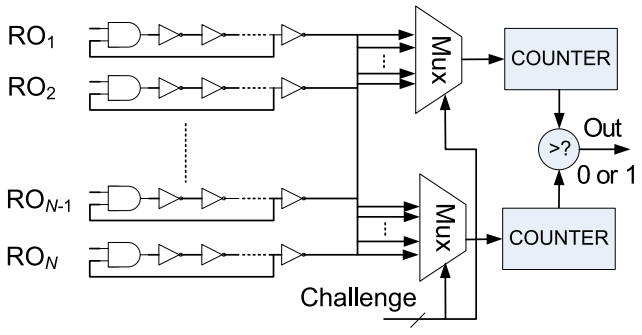

Fig. 1. A conventional ring-oscillator PUF (RO-PUF)

In order to avoid an extremely large number of bits in counters, it is important to design relatively slow oscillators with an oscillation frequency of the order of hundreds of MHz. Therefore, depending on the technology, 50–100 inverters are needed for one RO to produce a frequency in this range [22, 24]. This design constraint will increase costly area and power overhead. In contrast, we propose an ring oscillator design that slows the oscillating frequency by using only a fraction of the number of inverters used in a RO-PUF.

2.2 Nanocrossbar arrays and memristive devices

Crossbar arrays of metal-oxide based devices have attracted much attention in recent decades because of their high information density, compatibility with current CMOS technology, and simple implementation. The nanocrossbar array consists of parallel horizontal wires on top and perpendicular vertical wires at the bottom. At each junction, a two terminal device with or without a nonlinear selector element is formed and acts as a switch.

A nanocrossbar array structure is shown in Fig 2(a) where each nanodevice is located at the crosspoint of the top and bottom wires. When reading a targeted memristive device, reading voltage is applied to the selected word line and the current of the selected bit line is sensed to determine the state of the memristive device. For other unselected word lines and bit lines, they can be connected to ground or floating. Floating is preferred since it consumes much less power. During reading it is important to note that there also exists many sneak path currents (red line) besides the desired read current (blue line).

Recently, a number of nanoscale electronic device implementations have emerged that include resistive switching and memristive devices. Realization of a solid-state memristive device [8–10], namely the memristor, shown in Fig 2 (b), presents a new opportunity for realizing ultra high density memory arrays together with nanocrossbar structures [30]. The unique properties of such devices are the non-volatile memory and nanoscale dimensions.

In redox (reduction-oxidation) based resistive switching devices there are two major types of devices available: i) electrochemical metalization (ECM) memory; and ii) valence change memory (VCM) [45]. Both are examples of memristive device realizations. The memristor is a solid-state device consisting of a thin-film semiconductor sandwiched between two metal contacts. Inside a memristive element there is a built-in concentration gradient of anions (VCM systems) or

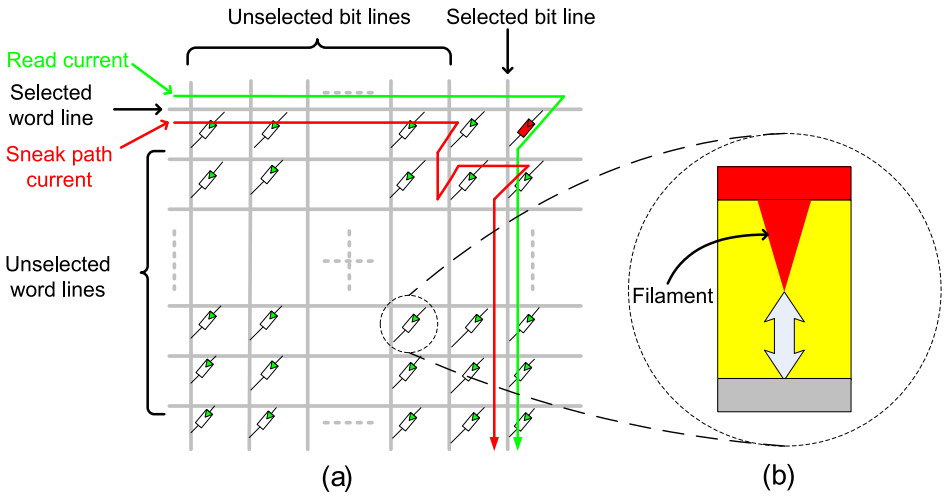

Fig. 2. (a) Nanocrossbar array of nanoionic memristive devices. (b) Illustrates the operation principles of a memristive device. The top electrode contains active ionic which stands for low resistance, while the bottom electrode is poor ionic region. Gray arrow indicates the ionic motion. The memristive device switches from OFF to ON with a positive potential difference between the top electrode and bottom electrode corresponding to 'SET' operation as one or more conductive filaments grow or form, while switches from ON to OFF with a negative potential difference between the top electrode and bottom electrode as the filaments disrupt.

cations (ECM systems) together with a temperature gradient which is a direct result of current passing through the conductive channel (conductive filament) and is known as Joule-heating. The ionic gradient consists of rich and poor ionic regions. The rich ionic region (top region in Fig. 2 (b)) gives rise to low resistance, R_{ON}, and the poor ionic region (bottom region in Fig. 2 (b)) is responsible for high resistance, R_{OFF}. The basic operating principle of the memristive device is shown in Fig. 2(b). A positive/negative voltage between two terminals of the memristive device will form/disrupt the filaments, and hence push the device in its ON/OFF state. Once memristive device has been programmed its memristance will remain unchanged even if its power supply is disconnected.

2.3 Memristor-based PUFs

Because of the interesting properties of memristors discussed earlier, researchers have started investigating the feasibility of memristors for building a PUF [32, 42, 29, 40]. Two of these studies [32, 42] employ a time and voltage constrained write mechanism (weak-write) to force each memristor to an undefined logic region (neither logic '1' or '0'). Subsequently, these memristors attain an unpredictable logic state due to process variations that influence memristance. Similar to SRAM PUF, a memristor PUF [32, 42] is only capable of producing a limited number of CRPs. More significantly, the PUF in [32, 42] requires a calibration procedure to determine the weak-write parameters (time and voltage) to force memristors into the undefined logic region.

In [41] the author leveraged sneak path currents inherent in memristor-based nanocrossbars and bidirectional features to build up a nano Public Physical Un-

clonable Functions (PPUF). Unlike PUFs, security of the PPUF no longer relies on the secrecy of its physical parameters that define its uncontrollable variations and the model of a PPUF that exactly matches the PPUF hardware behavior is publicly known to every one. The security of a PPUF is based on the time difference (several orders of magnitude) between fast execution time on PPUF hardware to acquire correct response and the much longer time required to compute the response correctly using the PPUF model. In fact, PUFs and PPUFs are hardware primitives with different requirements for authentication and other security services. Moreover, the nano PPUF always needs accurate measurements of its physical parameters to obtain through an accurate model of the nano PPUF that is inconvenient and expensive. Although the PPUF provides an alternative to securely storing challenge response pairs, the poor reliability of the nano PPUF designs still need to be addressed. We refer readers to [38] for a more comprehensive overview.

Our preliminary design of mrPUF was first outlined in [29] where we illustrated the possibility to use the significantly increased variations in high state and low state of memristor resistance in a nanocrossbar array together with an RO-PUF. In this paper we build on our initial concept outline. It should be noted that in this paper, we only exploit abundant resistance variations in R_{ON} state in individual memristors to achieve a more reliable PUF architecture. In addition, we evaluate key PUF performance metrics of mrPUF and analyze the security of the PUF based applications: key generation, and device authentication, which are not investigated in our previous work.

3 mrPUF

3.1 Concept

It has been shown that the memristor can be used to store digital states by utilizing the two distinct resistance values of the memristor, namely ON and OFF resistances, referred to as R_{ON} and R_{OFF}. These resistances are random variables with log-normal distribution values [9]. Fig. 3 illustrates the distribution of these resistances after an initial programming step of randomly selected binary values in a nanocrossbar array. As mentioned in Section 2.2, variations in memristors is prevalent when their dimensions approach the nano-scale region. These inherent variations can be effectively utilized to design a novel PUF architecture, as we will demonstrate in this article.

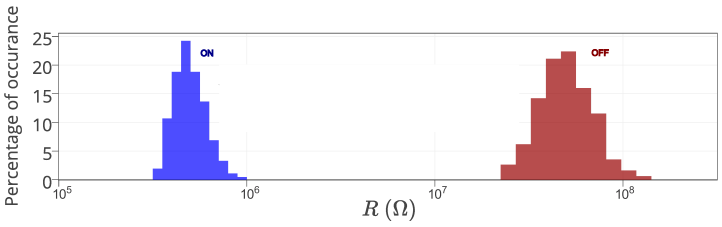

Fig. 3. Experimental resistance variation extracted from a 40×40 nanocrossbar array (1600 memristors) from the experimental data [9].

A memristor-based nanocrossbar architecture has the ability to combine large number of memristive devices in a compact area, and hence, has the ability to store a very large amount of information within a small physical size. When reading a targeted memristor resistance value, in addition to the current through the targeted memristor, there exist a number of other current paths that are commonly referred to as *sneak path* currents that result in an inaccurate reading of the targeted memristor device value (see Fig. 2). To suppress sneak path currents, a number of techniques are proposed [9]. Three of the leading techniques at the center of attention in today's industry and academic research community to suppress sneak path currents are; i) an intrinsic current-rectifying behavior [9, 47] which is translated into an extremely high current-voltage nonlinearity as shown in Fig. 4; ii) having a highly nonlinear series element with a transistor-like or a diode-like behavior; and iii) Complementary resistive switches (CRS) [35]. Presently, the first solution appears more promising than the two latter approaches due to its ability to maintain competing memory features such as small area and the highly nonlinear self-rectifying feature in these solid-state devices. As for CRS, the read operation is destructive and multilevel capability of the memristive device can not be used. In fact, sneak path current in nanocrossbar arrays mitigates the effect of process variations in individual memristors during readout. So intrinsic diode characteristic of the memristor helps maintain the process variations influence on resistance of memristor during readout; this is desirable for a PUF design aiming to exploit process variation.

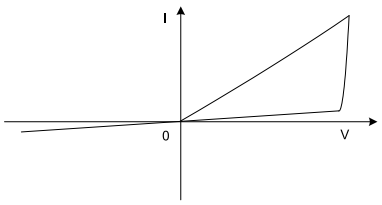

Fig. 4. Memristor with intrinsic diode characteristic.

In [39] the authors demonstrated that resistance variation is more prevalent in R_{ON} state than in R_{OFF} state due to the thickness of memristors. Furthermore, in [26] it was demonstrated that resistance is resilient to temperature and telegraph noise (refers to resistance fluctuations due to electrons captured or released again near or inside the filament) in R_{ON} state more than in R_{OFF} state. For these reasons only the R_{ON} state is used to construct the mrPUF architecture (i.e. we initially program the entire nanocrossbar to store the logic value '1') to reduce susceptibility to both temperature increases and telegraph noise and consequently increase the reliability of the PUF architecture. The sources of variations exploited in our mrPUF are listed below:

1. Memristor manufacturing variations: These variations are prevalent in the nanoscale region, and can be due to variation in device layer thicknesses, dimensions, or doping.
2. Programing variations: In the first programing operation (i.e, programming the state to '0' or '1'), it will introduce variations because the filament location and width in memristor are random.

3. CMOS device manufacturing variations: CMOS device properties due to inherent CMOS process variations, although CMOS process variations in CMOS components such as decoder, ring oscillators is very small compared with the first two listed sources.

3.2 mrPUF Architecture

The proposed mrPUF architecture shown in Fig. 5(a) comprises two key components: a $M \times N$ nanocrossbar array and two current mirror-controlled ring oscillators (CM-ROs), shown in Fig. 5(b). Individual memristor variations in the nanocrossbar array is the source of mrPUF's secrecy. While the CM-RO that has i (in this work, $i = 5$) inverters translates the analog resistance variations of a individual memristor into frequency for digitizing the analog variations to facilitate measurements.

Challenge bits are used to provide the address bits for both the analog multiplexer and the decoder. The decoder is used to select one column of the nanocrossbar array. Two analog $M \times 1$ multiplexers select two rows acting as bit lines. For example, we can select the red marked memristors (one memristor between Row_2 and Col_2 and the other memristor between Row_{M-1} and Col_2) after applying a single challenge. It should be noted that in this reading scheme the two randomly selected memristors have to be from the same column.

Each selected memristor is then used to control the current in the current mirror structure used to starve the current in each inverter in the ring oscillator loop, resulting in a *current starved ring oscillator* structure. So, the oscillation frequency is a direct function of this current which in turn is a direct function of the value of the memristor. The oscillation frequency of each oscillator is measured using a counter (as in RO-PUF). The outputs from the two counting circuits are compared and a response bit is generated accordingly. The reason only 5 inverters are used in one CM-RO is that the oscillation frequency is already down to decades of MHz (as illustrated in Fig. 7) by using 5 inverters due to a current starved ring oscillator structure.

A challenge is presented as an address to a decoder and a multiplexer as shown in Fig. 5. Subsequently, the outputs of CM-RO are compared to generate a response to the challenge. In the mrPUF architecture illustrated in Fig. 5 the number of possible challenge response pairs (CRPs) are $N \times \binom{M}{2}$. Where N and M are the number of columns and rows, respectively, in the nanocrossbar array.

In contrast to RO-PUF, which uses an array of ROs, the proposed mrPUF efficiently uses two 5-stage CM-ROs which are re-configured using the nanocrossbar and consequently result in a significant area reduction and ease of reading as the output frequency is substantially reduced to facilitate accurate counting. Also unlike the memristor-based PUF in [32] where the goal is to sense the value of the resistance to determine the binary value of a target element in nanocrossbar array, we translate a memristance value into a frequency through a CM-RO. The advantages of this approach are:

1. Use of significantly smaller number of ring oscillators and only 5 inverter stages to build each ring oscillator.
2. Mitigate some of the undesirable variations in responses caused by power supply and temperature fluctuations as we employ a differential structure to generate a response bit.

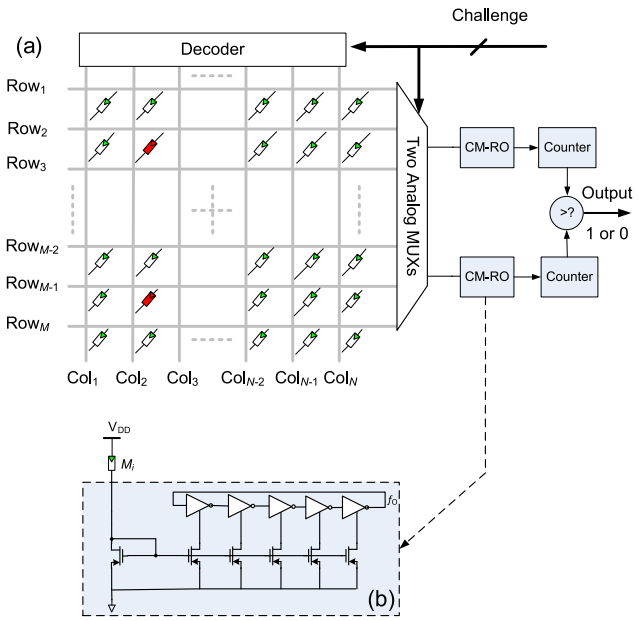

Fig. 5. Memristor-based nanocrossbar PUF architecture, mrPUF. (a) All memristors are in the ON state, the red color (or dark) marked memristors are selected memristors in the nanocrossbar array. (b) Current controlled RO (CM-RO). One current mirror configures all the inverters in a RO structure, M_i is the selected memristor in nanocrossbar array, Although variations in the oscillation frequency of each RO is slightly influenced by the threshold voltage variations in the CMOS transistor composing the starved inverter and current mirror structures, the overall variation in the oscillation frequency is primarily determined by the variations in memresistance of M_i if the supply voltage, V_{DD}, is kept constant.

3. Unlike in [32] we do not need complex circuitry to readout a memory cell and we do not directly expose full physical information (binary value in memory) at each junction of a nanocrossbar array.

4 mrPUF Evaluation

4.1 Simulation environment and settings

We conduct extensive experiments to evaluate our mrPUF architecture. The simulation was carried out using Cadence tools. In these simulations the mrPUF was built using a 40×40 nanocrossbar array with 1.25 Ω segment resistance for nanowires and two 5-stage CM-ROs as shown in Fig. 5. Each memristor is programmed to R_{ON} where the value of R_{ON} is selected from the log-normal distribution shown in Fig. 3. It should be noted here that the log-normal distribution values are extracted from the fabricated experimental data in [9]. Readout is achieved using a 1 V supply voltage. Our selected voltage ensures that we are operating below the memristor's threshold voltage and ensures the device memristance does not alter with respect to time. In these simulations we use the GPDK 90 nm standard CMOS technology in Cadence with a 1.0 V supply voltage. The memristor model is adapted from [46, 33] and written in Verilog-A language. The simulated results

of our memristor model shown in Fig. 6 agrees well with experimental results published in [9].

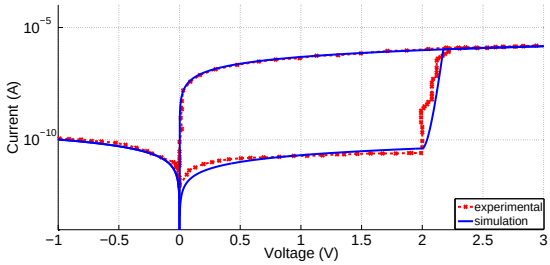

Fig. 6. Memristor with intrinsic diode characteristics. Red dash line is obtained from experimental data [9, 31] and the dot line depicts the accuracy of the simulated results produced by our memristor model written by Verilog-A language and used in generating the simulation results in our study.

We simulated a 40×40 nanocrossbar array architecture shown in Fig. 5 and obtained 31,200 CRPs using 15 bit length challenges.

4.2 Performance

There are a number of performance measures proposed in the literature for evaluating PUFs. We have selected fundamental metrics to demonstrate the performance of mrPUF using uniqueness, uniformity, diffuseness and reliability as proposed in [37] and [28]. Detailed definitions and explanations of these metrics for evaluating PUF architecture can be found therein. In addition to PUF performance we firstly investigate the frequency distribution of CM-RO to ensure that the frequency is indeed, mainly, a function of the resistance of the selected individual memristor.

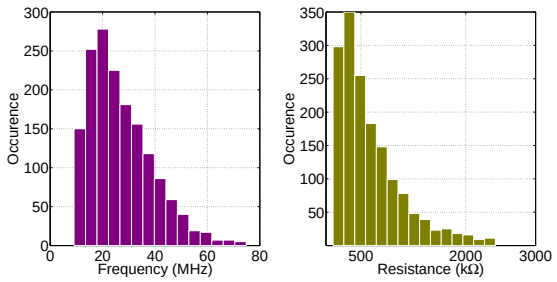

Fig. 7. The plot on the left shows the frequency distribution and the plot on the right shows the resistance distribution in a 40×40 nanocrossbar array. As expected, the frequency distribution agrees well with the resistance distribution.

Frequency distribution To test whether the frequency is determined by the variations from the resistance distribution of memristors in the nanocrossbar array, we readout all of the frequencies in one mrPUF instance from CM-RO configured by challenge bits, which select a target memristor in the nanocrossbar. The number of frequencies are equal to the number of memristors in nanocrossbar array (i.e. 1600). The frequency distribution is shown in Fig. 7. It can be seen that, as expected, the frequency distribution follows a log-normal distribution. For comparison, we show the resistance distribution in the nanocrossbar array in Fig. 7 as well. The close alignment of the frequency distribution and the resistance distribution plots illustrates that the dominant variation determining the mrPUF response is from the inherent random variations of individual memristors in the nanocrossbar array (which is more prevalent in the nano-region) instead of the CMOS technology variations in the peripheral CMOS circuitry. Detailed relationship between CM-RO's frequency and memristor's resistance is shown in Fig. 8 where we can see how the frequency of a CM-RO is determined by the resistance of a memristor.

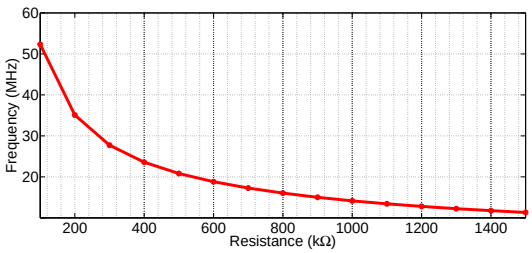

Fig. 8. The relationship between CM-RO's frequency and memristor's resistance. The circuit is shown in Fig. 5(b).

Uniformity Randomness or uniformity is an indicator of the balance of '0' and '1' in the response vector. An ideal PUF should show that a '0' or '1' response is equiprobable. For mrPUF our results show that the probability of a '0' or '1' response is very close to 50% (probability of '1' is 50.34% as shown in Fig. 9(a)).

Diffuseness measures the difference between responses for different challenges applied to the same PUF. Diffuseness quantifies the information content that can be extracted from a PUF. Diffuseness is measured by calculating the mean of Hamming Distance (HD) for all the possible responses generated by the PUF. Diffuseness for an ideal PUF is 50%.

Note the mrPUF, like the APUF, only produces a 1 bit response for a given challenge. To obtain a binary response vector, we apply a randomly selected set of challenges to the mrPUF, and then we concatenate these single response bits to a multiple bit response vector. Here, we use responses with 128 bits, therefore we apply 100 sets of 128 random challenges to the mrPUF. Subsequentially, we gain one hundred 128 bit responses to evaluate the diffuseness. The HD among these 100 responses is shown in Fig 9 (b). The mean of HD is 64.10 bits out of the 128 bit response, then the diffuseness is calculated as 50.08% close to the expected value of 50%.

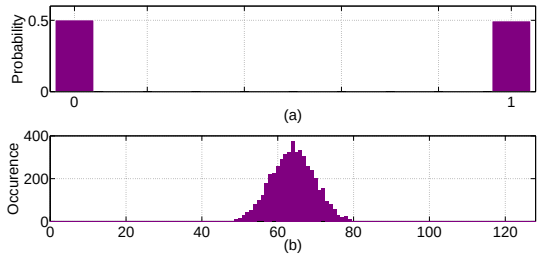

Fig. 9. (a) Uniformity or randomness of mrPUF: probability of output logic '1' and '0' are close to 50%, which are 50.34% and 49.66% for logic '1' and logic '0' respectively. (b) Diffuseness of the mrPUF: mean of HD among 100 randomly generated responses is 64.10 bits out of 128 bits (50.08%)

Uniqueness When applying the same challenge set to different PUFs, the responses from different PUFs are expected to be different due to intrinsic variations of each PUF. This is a highly desirable characteristic that be capable of distinguish one PUF from a large population. Uniqueness is the inter-device performance that can be measured by inter-HD. The mean of hamming distance is uniqueness expected to be 50 % as an ideal value.

We use 100 different mrPUF instances to evaluate the uniqueness and the result is shown in Fig 10. It can be observed that the mean of inter HD for the mrPUF is 64.22 bits out of the 128 bit response and this value agrees with that expected from an ideal PUF (i.e. 64 bits). The uniqueness is 50.17 %.

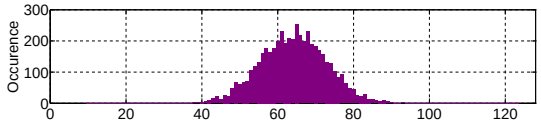

Fig. 10. Uniqueness evaluation: mean of inter HD among 100 responses generated from 100 PUF instances for the same given challenge is 64.22 bits out of 128 bits (50.17%).

Reliability Reliability or steadiness indicates stability of the PUF output bits, i.e. the ability to consistently generate the same response to a corresponding challenge. Reliability of an ideal PUF should be strong (100%). However, because noise (environmental variations, instabilities in circuit, aging) are unavoidable, there are always uncertain factors affecting the response. Reliability is measured by intra-chip HD among different samples of PUF response bits to the same challenge set applied to the same PUF instance.

A reference response Ref_i is recorded at normal operating condition (27°C and 1.0 V supply voltage for our simulation), then a response $\text{Ref}_i^{'}$ is extracted at a different operating condition but using the same set of challenges as before. After samples of $\text{Ref}_i^{'}$ are collected, the HD between Ref_i and $\text{Ref}_i^{'}$ is calculated. An ideal PUF's intra HD between Ref_i and $\text{Ref}_i^{'}$ should be 0 bits. Reliability can also

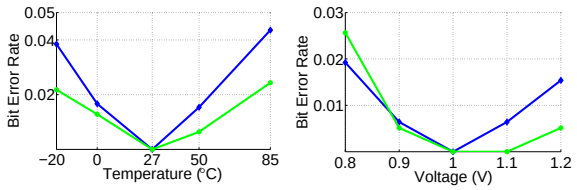

Fig. 11. Bit error rate (BER) under different temperature (left) and voltage (right) deviations.

be described by Bit Error Rate (BER), which is the percentage of flipped (error) bits (also called measurement noise) out of response bits due to noise.

Under simulation settings, we would always obtain the same responses for the same challenges if the temperature and voltage conditions do not change. In other words, the BER caused by measurement noise can not be evaluated. However, it is feasible to evaluate reliability under different temperature and supply voltages as discussed below.

We evaluate the reliability of two mrPUF instances and the results obtained are shown in Fig. 11. We obtained a 500 bit length response by repeatedly challenging mrPUFs under four different voltages: 0.8 V; 0.9 V; 1.1 V; and 1.2 V. The temperature settings used for the evaluation was 27°C. Worst-case BER is 2.6% under ±20% deviation and 0.65 % under ±10% deviation from nominal power supply voltage of 1.0 V.

The resistance temperature coefficient of memristive devices in ON state is similar to a metallic resistor [25, 34]. Therefore, we used metallic resistor temperature coefficient to conduct reliability evaluation under different temperature conditions. Reliability tests were repeated for four different ambient temperatures (-20°C, 0°C, 50°C, 85°C). The supply voltage used in these tests was 1.0 V. Worst BER of the two mrPUFs is 4.4% when the temperature is 85°C.

5 Applications and Security Analysis

5.1 Cryptographic key generation

It is impractical to use raw responses of a PUF as cryptographic keys directly because the BER is higher than the industrial standard of BER that is in the order of 10^{-6} (the industrial standard of BER for cryptographic key generation) [5]. As illustrate in [27], a fuzzy extractor can be used to correct the raw response and hash the corrected response to build a cryptographic key.

For example, to obtain 63 secret bits after the correction with BER rate lower than 10^{-6}, the BCH(255,63,61) code can be used. The mrPUF is expected to generate 11 unreliable bits out of a 255 bits response considering the worst-case BER of 4.4%. The BCH(255,63,61) code can correct up to 61/2 errors out of 255 bits. Therefore, the probability of reliably regenerating a response is 3.9×10^{-7} (lower than 10^{-6}) by using the BCH(255,63,61) code.

The syndrome generated reveals at most 192 bits (255–63) of information and therefore there are 63 secret bits can be used from the 255 bits response under the worst-case condition. Hence an attacker has to guess at least 63 bits to find the correct PUF response. In general, as proposed in [14], the regenerated response

can be hashed to obtain a fixed size key or serve as a seed for a key generation algorithm.

5.2 Authentication

Our PUF can also be directly used for device authentication using a simple challenge-response pairs based authentication protocol. The authentication protocol follows 5 steps:

First: A trusted party applies randomly chosen challenges to obtain responses and saves these CRPs in a database for future authentication (characterization of the PUF) before the PUF (as part of an integrated circuit) is sent to end-users. This is called the provision phase.

Second: Whenever an end-user needs to authenticate the authenticity of the product to which the PUF has been integrated, the user requests an authentication from the trusted party.

Third: The trusted party randomly selects a challenge from those stored securely in a database and sends it securely to the end-user. Subsequently, the end-user applies the challenge to their PUF and obtains a response.

Fourth: The user securely sends the obtained response to the trusted party.

Fifth: The trusted party compares the received response with the response stored. If they are close to each other, within an expected BER, authenticity of the product integrated with a PUF is established.

In order to prevent a replay attack by a passive attacker, a single CRP is only used once. This is possible because of large number of CRPs can be generated from the PUF.

To evaluate PUF security there are two analysis approaches: One is to evaluate the internal entropy of the PUF; The other one is to find out how many independent CRPs produced by the PUF, or in other words, how many CRPs needed to train the attacker's model to gain a high prediction accuracy of the physical PUF. In terms of the first approach, it has been demonstrated that the internal entropy of the PUF does not tell the attacker how to break a PUF, even the entropy is very low. In addition, it is not clear that the internal entropy is a good indicator of the PUF's security as highlighted in [44]. While the second approach is a better way to evaluate the security of a PUF [44]. So we use the second approach to evaluate the security of the mrPUF.

PUFs such as APUF, RO-PUF have been shown that after exposing a specific number of CRPs an attacker gains enough knowledge to build a model to predict responses for a given unused challenge [44, 12, 36]. This model building attack also threatens our mrPUF. In this section, we are going to illustrate how to avoid such a model building attack by leveraging the inherent property of our mrPUF architecture and a challenge selection strategy.

We assume the attacher does not have authority to physically access to the mrPUF. The CRPs they can acquire is only from eavesdropping. Consider the mrPUF shown in Fig. 5 with N columns and M rows. Each challenge will select one column and two rows. In other words, each challenge selects two memristors in the same column but from different rows, then the resistance of these two memristors are translated into frequencies by two CM-ROs to generate a single response bit. Now, if we only consider memristors in one column within the nanocrossbar array, we can model a mrPUF instance as a k ring oscillators PUF. From [44] we

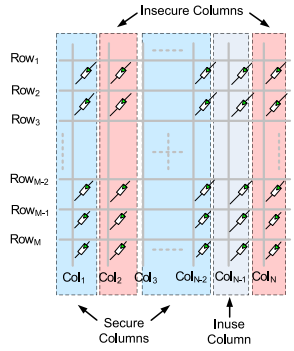

Fig. 12. mrPUF access mechanism resilient to model building attacks by using information from independent columns: firstly, we use CRPs generated from one randomly selected *Secure Column*, after N_{CRP} (number of CRPs required to train the attacker's model to acquire needed prediction accuracy) CRPs are used, this column becomes an *Insecure Column*. Secondly, we move to another randomly selected *Secure Column*. The column currently in use while its number of CPRs exposed is below N_{CRP} is labeled *Inuse Column*.

can obtain an estimate of the number of CRPs needed to train a machine learning based model to achieve an error rate of ϵ as

$$N_{\mathrm{CRP}} \approx \frac{k(k-1)(1-2\epsilon)}{2+\epsilon(k-1)} \tag{1}$$

where N_{CRP} is the number of CRPs needed to train a machine learning classifier and k is the number of RO in RO-PUF. The total number of CRPs in RO-PUF is NT_{CRP}, which is equal to $k \times (k-1)/2$. If an attacker wants to impersonate the PUF through building a predictive model, the error rate of the predictions of the model should be less than ϵ, or the trusted party can still distinguish the impersonated PUF from the original PUF. Based on Equation 1, to achieve a prediction accuracy of 1-ϵ, an adversary needs N_{CRP} CRPs to train a machine learning classifier.

It is noticeable that each challenge applied to mrPUF only selects two memristors in the same column, therefore information exposed in one column does not leak any information related to other columns. This property can be exploited to avoid machine learning based model building attacks through careful challenge selection.

In this paper, we propose a challenge selection strategy outlined in Fig. 12 to avoid model building attacks. The nanocrossbar columns are separated into three categories. If CRPs produced from one column have never been used, then this column is a *Secure Column*, since there is no information exposed to an adversary thus far. Under the condition that we only use CRPs from one column, the adversary needs N_{CRP} CRPs to train their machine learning classifier and build a model of the memristor related delays for a given column. Thus if N_{CRP} CRPs generated (obtained using Equation 1) from the *Inuse Column* has been used then this column becomes an *Insecure Column* because an adversary may have gathered enough CPRs to build a model and can potentially predict the response to future challenges with high accuracy. If the number of used CRPs generated from the column is still less than N_{CRP}, the column is an *Inuse Column*.

In our mrPUF, each column can be used to generate N_{CRP} secure CRPs because the attacker cannot predict the response with a high enough accuracy (1-ϵ) unless N_{CRP} CRPs are exposed. After more than N_{CRP} CRPs generated from the *Inuse Column* are exposed, the *Inuse Column* becomes an *Insecure Column*. We do not use CRPs generated from this *Insecure Column* again. Since each column is independent, the attacker is unable to use their existing knowledges to construct a model of the subsequent *Secure Columns*. This process can continue until all *Secure Columns* have been exhausted.

By using our proposed challenge selection mechanism in Fig. 12, we can make mrPUF more resilient to model building attacks. To increase security using our proposed mechanism above, it is better to set $N>M$. In this way, we are able to obtain more independent columns.

6 Comparison

Here we compare mrPUF with other memristor based PUFs. However, Comparison with nano PPUF is not presented because the nano PPUF has been developed to meet the requirements for a public PUF, where the need to build a model of a nano PPUF requires highly accurate measurements of each individual memristor in the nanocrossbar array in the provisioning phase. Furthermore, since the performance evaluations of RO-PUF, APUF and SRAM PUFs are acquired from experimental data, it is unfair to compare these with our simulated result. So here, we compare our mrPUF with existing memristor based PUFs where their results are also from simulation based studies.

Table 1. Comparison with memristor based PUFs

	[32]	[42]	mrPUF
Uniqueness	$\approx 50\%$	$\approx 50\%$	50.17%
Uniformity	—	$\approx 50\%$	49.66%
Crossbar	used	No	used
CRP Number	$M \times N$	M	$N \times \binom{M}{2}$

Since all the PUFs in Table 1 are based on large uncontrollable variations in nanofabrication and nanodevices, the uniqueness and uniformity are all close to the ideal value of 50%. We do not compare reliability performance because there is no such information presented in other memristor based PUFs. In Table 1, whether a nanocrossbar is used or not determines the circuit density. In terms of the CRP number, M and N denote the number of rows and columns, respectively, in a nanocrossbar array. In particular, for the PUF presented in [42], M denotes the number of memristors used in the PUF architecture. The number of CRPs of the other two memristor based PUFs is equal to the number of memristors. As for our mrPUF, it can be seen that it is capable of yielding a significantly larger number of CRPs.

In summary, we have evaluated the uniqueness, randomness performance of mrPUF. In addition, we also investigate the reliability under different temperature and voltage conditions. Such evaluation is missing in the currently published memristor based PUFs. Moreover, we have also analyzed the security of our mrPUF for two potential applications and proposed a challenge selection strategy

to avoid model building attacks when mrPUF is used directly for authentication applications.

7 Conclusion

In this paper, we present a novel PUF architecture named mrPUF. Our approach exploits the robustness of RO-PUFs and exploits the large variations in nanodevices as well as the high information density available in nanocrossbar structures to create a novel PUF. Our architecture not only achieves sound reliability, uniqueness, diffuseness, but also improves the number of available CRPs in comparison with other recent memristor based PUF architectures. In particular, we show that mrPUF achieves higher levels of security due to the inherent features of nanocrossbar arrays that the information in one column is independent from other columns. We also demonstrate a mechanism using mrPUF in an authentication protocol that is resistant to model building attacks by the proposed challenge selection strategy.

A limitation of our work is that our experiments are conducted based on device simulations, albeit using de-facto industry standard modelling tools and experimentally verified process variations, rather than physical realizations, Addressing this limitation forms the subject of our future work. Furthermore, in our future work we will investigate the possibility of building a re-configurable and strong memeristive device based PUF architecture [48] by exploiting the variations induced during re-programming and increasing the number of CRPs significantly.

8 Acknowledgment

This research was supported by a grant from the Australian Research Council (DP140103448). The authors also appreciate sponsorship from the China Scholarship Council, and the support from the Department of Further Education, Employment, Science and Technology (DFEEST) under the Collaboration Pathways Program, Government of South Australia.

References

1. O. Kömmerling and M. G. Kuhn. Design principles for tamper-resistant smartcard processors. In *Proceedings of the USENIX Workshop on Smartcard Technology*, pages 2–2. USENIX Association, 1999.
2. J. W. Lee, D. Lim, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas. A technique to build a secret key in integrated circuits for identification and authentication applications. In *Symposium on VLSI Circuits*, pages 176–179. IEEE, 2004.
3. R. Maes, A. Van Herrewege, and I. Verbauwhede. Pufky: A fully functional PUF-based cryptographic key generator. In *Cryptographic Hardware and Embedded Systems*, pages 302–319. Springer, 2012.
4. M. van Dijk and U. Rührmair. Physical unclonable functions in cryptographic protocols: Security proofs and impossibility results. *IACR Cryptology ePrint Archive*, 2012:228, 2012.
5. L. Zhang, Z. H. Kong, and C.-H. Chang. PCKGen: A phase change memory based cryptographic key generator. In *IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1444–1447, 2013.

6. U. Ruhrmair and M. van Dijk. Pufs in security protocols: Attack models and security evaluations. In *IEEE Symposium on Security and Privacy (SP)*, pages 286–300, 2013.
7. H. Kang, Y. Hori, T. Katashita, M. Hagiwara, and K. Iwamura. Cryptographie key generation from PUF data using efficient fuzzy extractors. In *16th International Conference on Advanced Communication Technology (ICACT)*, pages 23–26. IEEE, 2014.
8. D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams. The missing memristor found. *Nature*, 453(7191):80–83, 2008.
9. K.-H. Kim, S. Gaba, D. Wheeler, J. M. Cruz-Albrecht, T. Hussain, N. Srinivasa, and W. Lu. A functional hybrid memristor crossbar-array/CMOS system for data storage and neuromorphic applications. *Nano letters*, 12(1):389–395, 2011.
10. O. Kavehei, S. Al-Sarawi, K.-R. Cho, K. Eshraghian, and D. Abbott. An analytical approach for memristive nanoarchitectures. *IEEE Transactions on Nanotechnology*, 11(2):374–385, 2012.
11. B. Gassend, D. Lim, D. Clarke, M. Van Dijk, and S. Devadas. Identification and authentication of integrated circuits. *Concurrency and Computation: Practice and Experience*, 16(11):1077–1098, 2004.
12. D. Lim, J. W. Lee, B. Gassend, G. E. Suh, M. Van Dijk, and S. Devadas. Extracting secret keys from integrated circuits. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 13(10):1200–1205, 2005.
13. Kumar, Raghavan and Patil, Vinay C and Kundu, Sandip. Design of unique and reliable physically unclonable functions based on current starved inverter chain. *IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, pages 224–229, 2011.
14. G. E. Suh and S. Devadas. Physical unclonable functions for device authentication and secret key generation. In *Proceedings of the 44th Annual Design Automation Conference*, pages 9–14, 2007.
15. D. Suzuki and K. Shimizu. The glitch PUF: A new delay-PUF architecture exploiting glitch shapes. In *Cryptographic Hardware and Embedded Systems, CHES*, pages 366–382. Springer, 2010.
16. D. E. Holcomb, W. P. Burleson, and K. Fu. Initial SRAM state as a fingerprint and source of true random numbers for RFID tags. In *Proceedings of the Conference on RFID Security*, volume 7, 2007.
17. D. E. Holcomb, W. P. Burleson, and K. Fu. Power-up SRAM state as an identifying fingerprint and source of true random numbers. *IEEE Transactions on Computers*, 58(9):1198–1210, 2009.
18. Y. Su, J. Holleman, and B. P. Otis. A digital 1.6 pJ/bit chip identification circuit using process variations. *IEEE Journal of Solid-State Circuits*, 43(1):69–77, 2008.
19. R. Maes, P. Tuyls, and I. Verbauwhede. Intrinsic PUFs from flip-flops on reconfigurable devices. In *3rd Benelux Workshop on Information and System Security (WISSec 2008)*, volume 17, 2008.
20. V. van der Leest, G.-J. Schrijen, H. Handschuh, and P. Tuyls. Hardware intrinsic security from D flip-flops. In *Proceedings of the fifth ACM Workshop on Scalable Trusted Computing*, pages 53–62. ACM, 2010.
21. S. S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls. The butterfly PUF protecting IP on every FPGA. In *Hardware-Oriented Security and Trust, 2008. HOST 2008. IEEE International Workshop on*, pages 67–70. IEEE, 2008.
22. M. Roel. Physically unclonable functions: Constructions, properties and applications. PhD thesis, Dissertation, University of KU Leuven, 2012.
23. C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas. Physical unclonable functions and applications: A tutorial. 2014.
24. A. Maiti, J. Casarona, L. McHale, and P. Schaumont. A large scale characterization of RO-PUF. In *IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, pages 94–99, 2010.
25. J. Borghetti, D. B. Strukov, M. D. Pickett, J. J. Yang, D. R. Stewart, and R. S. Williams. Electrical transport and thermometry of electroformed titanium dioxide memristive switches. *Journal of Applied Physics*, 106(12):124504, 2009.

26. S. Choi, Y. Yang, and W. Lu. Random telegraph noise and resistance switching analysis of oxide based resistive memory. *Nanoscale*, 6(1):400–404, 2014.
27. Y. Dodis, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *Advances in Cryptology-Eurocrypt 2004*, pages 523–540. Springer, 2004.
28. Y. Hori, T. Yoshida, T. Katashita, and A. Satoh. Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs. In *International Conference on Reconfigurable Computing and FPGAs (ReConFig)*, pages 298–303. IEEE, 2010.
29. O. Kavehei, C. Hosung, DC. Ranasinghe, and S. Skafidas. mrPUF: A memristive device based physical unclonable function. *arXiv preprint arXiv:1302.2191*, 2013.
30. O. Kavehei, E. Linn, L. Nielen, S. Tappertzhofen, E. Skafidas, I. Valov, and R. Waser. An associative capacitive network based on nanoscale complementary resistive switches for memory-intensive computing. *Nanoscale*, 5(11):5119–5128, 2013.
31. K.-H. Kim, S. H. Jo, S. Gaba, and W. Lu. Nanoscale resistive memory with intrinsic diode characteristics and long endurance. *Applied Physics Letters*, 96(5):053106, 2010.
32. P. Koeberl, Ü. Kocabaş, and A.-R. Sadeghi. Memristor PUFs: a new generation of memory-based physically unclonable functions. In *Proceedings of the Conference on Design, Automation and Test in Europe*, pages 428–431. EDA Consortium, 2013.
33. S. Kvatinsky, K. Talisveyberg, D. Fliter, E. G. Friedman, A. Kolodny, and U. C. Weiser. Verilog-A for memristor models. Technical report, Citeseer, 2011.
34. D.-H. Kwon, K. M. Kim, J. H. Jang, J. M. Jeon, M. H. Lee, G. H. Kim, X.-S. Li, G.-S. Park, B. Lee, S. Han, et al. Atomic structure of conducting nanofilaments in TiO_2 resistive switching memory. *Nature Nanotechnology*, 5(2):148–153, 2010.
35. E. Linn, R. Rosezin, C. Kügeler, and R. Waser. Complementary resistive switches for passive nanocrossbar memories. *Nature Materials*, 9(5):403–406, 2010.
36. A. Mahmoud, U. Rührmair, M. Majzoobi, and F. Koushanfar. Combined modeling and side channel attacks on strong PUFs. *IACR Cryptology ePrint Archive*, 2013:632, 2013.
37. A. Maiti, V. Gunreddy, and P. Schaumont. A systematic method to evaluate and compare the performance of physical unclonable functions. In *Embedded Systems Design with FPGAs*, pages 245–267. Springer, 2013.
38. M. Potkonjak and V. Goudar. Public physical unclonable functions. *Proceedings of the IEEE*, 102(8):1142 – 1156, 2014.
39. J. Rajendran, R. Karri, and G. S. Rose. Improving tolerance to variations in memristor-based applications using parallel memristors. *IEEE Transactions on Computers*, 64(3):733 – 746, 2015
40. J. Rajendran, R. Karri, J. B. Wendt, M. Potkonjak, N. R. McDonald, G. S. Rose, and B. T. Wysocki. Nanoelectronic solutions for hardware security. *IACR Cryptology ePrint Archive*, 2012:575, 2012.
41. J. Rajendran, G. S. Rose, R. Karri, and M. Potkonjak. Nano-PPUF: A memristor-based security primitive. In *VLSI (ISVLSI), 2012 IEEE Computer Society Annual Symposium on*, pages 84–87. IEEE, 2012.
42. G. S. Rose, N. McDonald, L.-K. Yan, and B. Wysocki. A write-time based memristive PUF for hardware security applications. In *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 830–833, 2013.
43. M. Rostami, J. B. Wendt, M. Potkonjak, and F. Koushanfar. Quo vadis, PUF?: Trends and challenges of emerging physical-disorder based security. In *Proceedings of the Conference on Design, Automation & Test in Europe*, page 352. European Design and Automation Association, 2014.
44. U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber. Modeling attacks on physical unclonable functions. In *Proceedings of the 17th ACM conference on computer and communications security*, pages 237–249. ACM, 2010.

45. I. Valov, R. Waser, J. R. Jameson, and M. N. Kozicki. Electrochemical metallization memoriesfundamentals, applications, prospects. *Nanotechnology*, 22(25):254003, 2011.
46. I. Vourkas, A. Batsos, and G. C. Sirakoulis. SPICE modeling of nonlinear memristive behavior. *International Journal of Circuit Theory and Applications*, 2013.
47. S. Wu, L. Ren, J. Qing, F. Yu, K. Yang, M. Yang, Y. Wang, M. Meng, W. Zhou, X. Zhou, et al. Bipolar resistance switching in transparent ITO/$LaAlO_3$/$SrTiO_3$ memristors. *ACS Applied Materials & Interfaces*, 2014.
48. Y. Gao, D. Ranasinghe, S. Al-Sarawi, O. Kavehei, and DC. Abbott. Memristive crypto primitive for building highly secure nano-PUF. *Nature Scientific Reports*, in submission, 2015.