frontiers | Frontiers in Communications and Networks

TYPE Review
PUBLISHED 17 October 2022
DOI 10.3389/frcmn.2022.884874



OPEN ACCESS

EDITED BY
Oluwakayode Onireti,
University of Glasgow, United Kingdom

REVIEWED BY
Lukas Zimmermann,
Hahn-Schickard-Gesellschaft für angewandte Forschung, Germany
Filip Kodytek,
Czech Technical University in Prague, Czechia
Nafisa Noor,
North South University, Bangladesh
Siam Hussain,
University of California, San Diego, United States
Hanady Issa,
Technology and Maritime Transport (AASTMT), Egypt

*CORRESPONDENCE
Jeeson Kim,
jeesonkim@sejong.ac.kr

SPECIALTY SECTION
This article was submitted to IoT and Sensor Networks, a section of the journal Frontiers in Communications and Networks

RECEIVED 08 March 2022
ACCEPTED 20 July 2022
PUBLISHED 17 October 2022

CITATION
Kim J (2022), Nano-intrinsic security primitives with redox-based resistive memory.
*Front. Comms. Net* 3:884874.
doi: 10.3389/frcmn.2022.884874



# Nano-intrinsic security primitives with redox-based resistive memory

Jeeson Kim*

Department of Intelligent Mechatronics Engineering, Sejong University, Seoul, South Korea

Physical unclonable function (PUF) exploits advantages of otherwise undesirable non-idealities to create physical systems that are difficult to copy even with the same manufacturing process. Nano-intrinsic PUFs use the variability of nanotechnology per hardware instance as a source of cryptographic randomness. Among various emerging memories, redox-based resistive memory (ReRAM) is a promising candidate for providing next-generation low-cost, low-power, ultra-small PUF-based security solutions. This review shows various ReRAM-based PUF implementations and their key features. We compare their performance and discuss which properties of ReRAM to focus on for effective PUF implementation.

KEYWORDS

**hardware security, physical unclonable function, emerging non-volatile memory, redox-based resistive memory, hardware-security primitive**

## 1 Introduction

Security is a concept expressing resilience against potential harm or damage from external hostile forces. Beneficiaries of security may include objects, systems, persons, groups, and institutions vulnerable to unwanted changes in their environment. The term is also used to refer to a means to protect its beneficiaries. The means include, for example, protection systems (e.g., fence, lock, and carrier), detection systems (e.g., radar and security cameras), and policies for developing conditions (e.g., access control using photo identification). The need for secure communication is a topic of long history, with early examples dating back to about 2000 B.C. in Ancient Egypt. Egyptian hieroglyphics is a secret writing system hiding the meaning of a message. Likewise, secure military communication has been undoubtedly crucial in the past and, to some extent, today. In our vastly digitalized world, the need for digital information security has risen exponentially due to increased sensitive information processing and communication across various platforms, such as computers and smart mobile devices. Moreover, the explosive growth of the Internet of Things (IoT) introduces sensitive information communicated over the Internet at every moment of our lives. Unfortunately, keeping security is difficult, and we often witness security vulnerability or an entire breakdown in the worst case. In June 2010, Stuxnet demonstrated that a digitalized attack could interfere with the regular operation of a whole industrial plant is one profound example of a large number of similar occasions (Chen and Abu-Nimeh, 2011; Langner, 2011; Beyerer et al.,

2015; Junker, 2015). In many ways, our society has become inseparable from digital information, which places a high demand for reliable security and trust techniques.

As a subfield of security, cryptology deals with the science of constructing secret writing systems for information security (cryptography) and the science of breaking constructed cryptosystems (cryptanalysis) (Paar and Pelzl, 2009). Because cryptanalysis is the only way to assure that a cryptosystem is secure, cryptography and cryptanalysis are closely linked and often exercised by the same person. This is in agreement with Kerckhoffs' principle (Auguste, 1883), in which the most classical cryptographic approaches are based on the concept that cryptosystems can only be considered secure if the details of the system, except for the secure key, are disclosed and can successfully withstand cryptanalysis attempts. At the same instant, Kerckhoffs' principle emphasizes the importance of not exposing the secure key to the outside despite the elaborate cryptanalysis. Therefore, the degree of security is typically expressed by the required level of effort to break the cryptosystems without knowing the key.

When security came into the modern world, symmetric cryptography and asymmetric cryptography were widely used. Primarily, asymmetric cryptography has dominated the markets, whereas its cost has become a significant concern. Cost is measured regarding memory usage, power consumption, die size, and execution time, among others. On the contrary, authenticity and credibility are essential considerations in the financial and banking markets. Therefore, early cryptography focused on building security using steel or heavy hardware security modules. The later emergence of non-volatile memory (NVM) added flexibility for some applications. The current best practice for providing security in a mobile system is to place a secret key in a non-volatile electrically erasable programmable read-only memory (EPROM) or battery-backed volatile static random-access memory (SRAM). The key is used for hardware cryptographic operations, where the key lengths correspond to the level of security. However, another rule applies—the longer the key, the more resources—and computation are required. In other words, the increase in cost is inevitable for achieving a high level of security.

A software-based cryptographic implementation is often sufficient for applications where devices are less focused on security. For example, a bootloader verifying the authenticity of the embedded firmware is commonly used to prevent most threats to consumer and industrial devices using digital signature and hash functions. Software-based solutions are simple and do not pose significant cost concerns. However, when performing software encryption algorithms on platforms where other applications are running concurrently, there is a potential for information leaked from timing measurements or cached data to detect secret keys and cause solution failures. Furthermore, in some traditional situations, such as consumer products using small core or coreless chips, hardware-based cryptography is the only solution. For such consumer products, costs are under pressure, but security is not the selling advantage. These security practices demonstrate a constant struggle between the low implementation costs and the high-security levels.

Nonetheless, consumer products must be provided at the lowest possible cost with security features, and authentication is often used. Symmetric challenge/response-based validation works to prevent potential counterfeiting for the authentication. If it aims for truly random numbers, the cryptographic implementation in hardware is mandatory for the random number generation, whereas software post-processing ideally helps produce more numbers. In classical authentication, the secret binary key needs to be permanently stored on the NVM of the devices and remains unexposed. However, this is difficult to uphold in practice, as performing physical attacks such as invasive, semi-invasive, or side-channel attacks on NVM is relatively easy; when it succeeds, it can potentially expose the secret key (Anderson, 2001). In this context, this hardware vulnerability is one of the initial motivations for developing better key protection methods (van Dijk and Rührmair, 2012).

## 2 Background

Security is an important topic due to recent years' emerging hardware design objectives (Ravi et al., 2004). Hardware needs to be protected, as potential hardware vulnerabilities can cause attacks on the programs and contents running on it. For a similar reason, manufacturing integrated circuit (IC) by untrusted foundries and using these components should be avoided (Majzoobi et al., 2008). Current hardware security relies on conventional cryptographic protocols, in which the secret binary key is permanently stored on the hardware's memory device, but the contents remain confidential. However, this is difficult to uphold in practice, as performing physical attacks on NVM is relatively easy.

### 2.1 Physical unclonable function

The concept of physical unclonable function (PUF) can be expressed as "a fingerprint of an object." A human fingerprint is referred to measurable physical characteristics as part of human biometrics, and biometrics authentication is often used for identification and access control. Proper human biometrics are suitable for authentication due to the characteristics of inheritance, unclonability, and individuality, which are also applicable to the PUF concept in a similar manner (Maes, 2012).

In 2001, Pappu (2001) introduced a three-dimensional optical micro-structures PUF construction using coherent radiation and defined it as a "physical one-way function," a general concept of PUF. Immediately after that, Gassend et al.

(2002b) proposed a silicon-based PUF construction and described it as a "physical random function." Both acronyms, which stand for "physical unclonable function," are chosen for pronouncing convenience and avoiding confusion with the concept of a "pseudo-random function (PRF)." A PUF is not strictly a function in the mathematical sense because a single input can be related to more than a single output due to environmental noise on the response generation. Therefore, PUF can be described as a probabilistic function because it deals with parameter uncertainties or variabilities (Uryasev, 2000). Also, a PUF's output is considered a random variable with a probability distribution, not a deterministic value.

IC-based PUF security has major advantages thanks to its simple digital circuit-based structures. This includes a simple fabrication process, low power consumption, small area consumption, and potentially forming anti-tamper circuitry. Equally importantly, PUF applications do not require expensive cryptographic hardware as a secure hash algorithm (SHA) or public/private key encryption algorithms. PUF's secret is derived from the physical characteristics of the IC; therefore, the chip must be powered on for the secret to reside in digital memory. From the point of view of attacks to obtain the secret key, any physical attack attempting to extract digital information must be made while the chip is powered on.

## 2.2 Classification of PUFs

### 2.2.1 Weak and strong PUFs

In PUF, the possible input is called a challenge and the resulting output is called a response, in which the pair is defined as a challenge-response pair (CRP). For a set of PUF instances, the responses to the same challenge are expected to differ; therefore, the CRP is the key point to distinguishing one PUF instance from others. Weak and strong PUFs are classified based on a possible CRP or, more often, CRPs. Weak PUF stores secret binary key(s) in hardware memories, such as read-only memory (ROM), flash memory, and NVM, using the bit-to-cell mapping method. Therefore, the total number of CRPs is limited to the total number of cells, often only one CRP per PUF instance. The most popular implementation of weak PUF is static random-access memory PUF (SRAM-PUF), which exploits the threshold variability of the cross-coupled SRAM cells, and examples of SRAM-PUF and a few more memory-based weak PUF constructions will be discussed in Section 3.4.

In opposition to weak PUF, strong PUF provides a more complex challenge-response behavior that generates responses instead of simply reading out cells. It is often assumed that access to responses is publicly available. As a result of many possible challenges of strong PUF, even for the adversary holding physical possession of a PUF instance, a complete readout of all CRPs can be prevented because it is unlikely possible to enumerate all CRPs within a fixed time (ideally, exponential in the number of challenge bits).

### 2.2.2 Intrinsic PUFs

Intrinsic PUF is one of the most widely investigated classes of PUFs, although it does not fall into the type of the first attempt to describe PUF or PUF-like constructions that are introduced above (Pappu, 2001; Pappu et al., 2002). The intrinsic PUFs require two additional characteristics: first, the complete PUF construction should be fully integrated into the embedding device, including the measurement equipment; second, the integration should be completed using the standard manufacturing flow without processing specifically designed PUF-related features and components (Maes and Verbauwhede, 2010a). Because of these two characteristics, intrinsic PUF can provide cost-efficient solutions. For example, SRAM-PUF is favorable for building PUF as SRAM has been widely used in nearly all electronic applications.

### 2.2.3 PUF extensions

Rührmair et al. (2011) proposed super high information content PUF (SHIC-PUF) to maximize the extractable structural information of a physical system within the drastically reduced readout speed. Its highly dense information-based design increases the immunity against algorithmic attacks, including machine-learning techniques, and their security may even withstand attackers with unlimited computational power. Crossbar array (CBA) is typically used for SHIC-PUF due to its structural benefits of high-density information and easy integration on a chip. Its structure allows a large CRP space; therefore, all SHIC-PUFs are considered strong PUFs (Rührmair, 2010).

Gassend et al. (2002a) defined a new type of PUF, controlled PUF (CPUF), that can only be accessed *via* a physically bounded algorithm. Because of this characteristic, any attempt to break the link between the CPUF and the algorithm leads to destroying the CPUF. The inseparable algorithm of CPUF makes chosen-challenge-based model-building attacks more difficult because the algorithms generate challenges (Maes, 2012). Hence, turning PUF into CPUF could increase security (Maes and Verbauwhede, 2010a).

Public PUF (PPUF) was suggested to resolve classical public cryptography's conceptual and practical limitations. Beckmann and Potkonjak (2009) used PUFs' characteristics for creating a public key-based protocol. Reverse engineering, the complete extraction of the parameters from the PPUF's physical systems, is possible when the PUF model is publicly available. However, despite the full characterization of the structure, simulating input-output mapping of PPUF requires considerable time without owning the PPUF hardware. Thus, this approach is likely immune to side-channel attacks due to technological constraints that prevent PUF cloning. Later, Rührmair (2009) proposed the SIMulation Possible, but Laborious (SIMPL)

system, which is a similar concept to the one proposed by Beckmann and Potkonjak (2009).

Kursawe et al. (2009) were the first to define reconfigurable PUF in which its mechanism and configuration can be transformed into an entirely new PUF, such that even with the knowledge of CRPs from the previous PUF configuration, the challenge-response behavior of the new PUF cannot be predicted. It should be noted that reverting the configuration of reconfigurable PUF is a difficult task. In addition, the configuration mechanism should not be in the form of either changing a part of the challenge or altering the placement of PUF.

## 2.3 PUF preliminary

### 2.3.1 PUF properties

Over the past few years, many publications have introduced new PUF concepts and attempted to define the general PUF concept. Maes (2012) well formulated the crucial properties of PUFs using informal qualifiers such as easy or hard and low or high.

- Constructability describes how easy it is to construct a PUF instance of a particular type of PUF. The qualifier of "easiness" in this context includes the cost of production.
- Evaluability is described as "easy to evaluate" in the early publications (Gassend et al., 2002a; Gassend et al., 2004). The "easiness" in this context depends on the variant of PUF constructions. Theoretically, evaluability points to polynomial time and effort (Gassend et al., 2002a); from the practical point of view, it can also include area, power, energy, and cost budgets imposed by the application (Maes, 2012).
- Unpredictability is addressed as "hard to characterize or predict" (Gassend et al., 2002a; Gassend et al., 2004). Complete characterization of an entire PUF should be challenging to an adversary with only a polynomial amount of resources (time, measurement of CRPs, etc.). It can only extract a negligible amount of information about the response to a randomly chosen response challenge (Gassend et al., 2002b).
- Mathematical unclonability of PUF can be described as the extension of unpredictability with unlimited access. For a PUF that exhibits mathematical unclonability, PUF should still be unpredictable even when an adversary has unlimited physical access to the PUF.
- Physical unclonability means that producing (or manufacturing) two identical PUFs is technically impossible even for the manufacturer of the original (Gassend et al., 2002a).
- Reproducibility property concerns the response distribution to identical challenges over time. It means that PUF should generate the same response to the same challenge with a high probability.
- Uniqueness concerns the response distribution to identical challenges across PUF instances. A PUF should generate different responses to the same challenge with high probability.
- One-wayness property means that given a PUF instance and its random response, there is no efficient inversion algorithm finding a challenge that produces a response similar to the given response.
- Tamper evidence means that it is "hard" to physically alter a PUF instance without a noticeable effect on its pre-recorded CRPs.

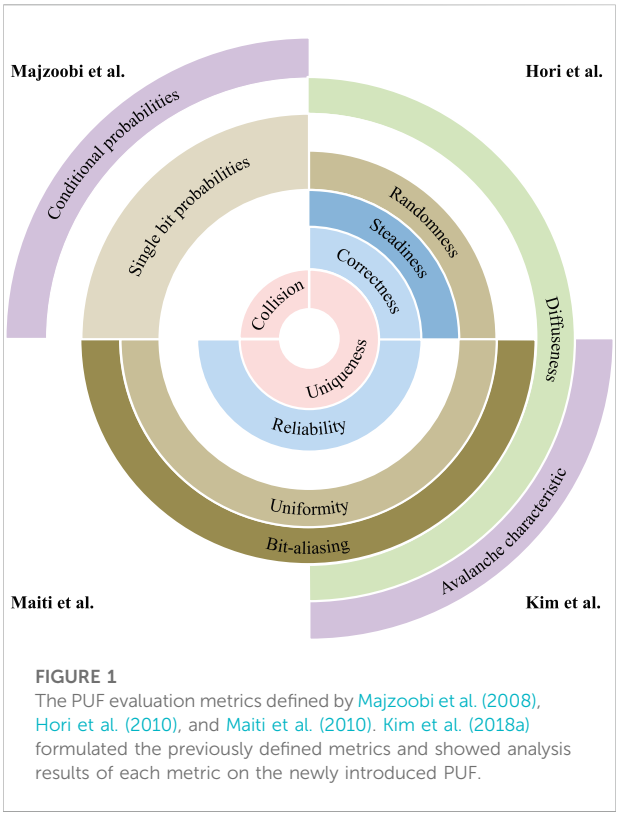


FIGURE 1
The PUF evaluation metrics defined by Majzoobi et al. (2008), Hori et al. (2010), and Maiti et al. (2010). Kim et al. (2018a) formulated the previously defined metrics and showed analysis results of each metric on the newly introduced PUF.

### 2.3.2 PUF evaluation metrics

As security primitive, PUF must produce random but device-specific responses that should be consistent under varying operating conditions, and for a fair evaluation, the specific PUF performance indicators and tools should be defined. Majzoobi et al. (2008) defined four metrics, predictability, collision, sensitivity, and reverse engineering, that can show PUF's resiliency against four broad classes of attacks, predictability, collision, fault-injection, and reverse engineering attacks, respectively. Hori et al. (2010) suggested the concept of five indicators: randomness, steadiness, correctness, diffuseness, and uniqueness. Maiti et al. (2010)

defined these PUF evaluation metrics using different terms, bit-aliasing, uniformity, uniqueness, and reliability, and presented evaluation results on ring oscillator PUF (RO-PUF). Kim et al. (2018a) formulated the defined metrics and showed the results in detail on the newly proposed PUF. These evaluation metrics are illustrated in Figure 1 (adopted from Kim (2019)).

The following notations are used to calculate the evaluation metrics.

| | |
|---|---|
| $p$ | Number of PUF instances |
| $C$ | Number of challenges |
| $T$ | Number of tries |
| $r$ | Response string |
| $r_{i,j}$ | $j$th bit of the $i$th response string $r$ |
| $L$ | Response bit length |

#### 2.3.2.1 Uniqueness

Uniqueness represents the capability of one PUF to distinguish itself from others. The value is calculated as a percentage by calculating Hamming distance (HD) between two responses from two PUFs when the same challenge is applied to them. Ideally, uniqueness is expected to be 50%. For example, ideal uniqueness can be achieved when responses from the two PUF instances (to the same challenge) have an average of a half-bit difference. When the number of PUF instances is more than two, the mean value of HDs from all possible combinations of two $\binom{p}{2}$ represents uniqueness. Therefore, uniqueness is the average inter-PUF HD and can be expressed as follows:

$$\text{Uniqueness} = \frac{1}{\binom{P}{2}} \sum_{i=1}^{P-1} \sum_{j=i+1}^{P} \frac{\text{HD}(r_i, r_j)}{L} \times 100\%, \quad (1)$$

where $r_i$ and $r_j$ are the response strings from $i$th and $j$th PUF instances, respectively.

#### 2.3.2.2 Diffuseness

Diffuseness represents the capability of one PUF to generate different responses. Similar to uniqueness, diffuseness is calculated as a percentage, yet it calculates HD between responses of one PUF to various challenges. Therefore, diffuseness shows the degree of difference among a single PUF's responses. Ideally, diffuseness is expected to be 50%. This can be expressed as follows:

$$\text{Diffuseness} = \frac{1}{\binom{C}{2}} \sum_{i=1}^{C-1} \sum_{j=i+1}^{C} \frac{\text{HD}(r_i, r_j)}{L} \times 100\%, \quad (2)$$

where $r_i$ and $r_j$ are the response strings to $i$th and $j$th challenges from a PUF instance.

#### 2.3.2.3 Reliability

Reliability represents the capability of a PUF to produce an identical response to the same challenge on two different occasions under varying operating conditions such as temperature or power supply voltage. Ideal reliability is 100%, which can only be obtained with a zero-bit error rate (BER). Reliability is expressed as follows:

$$\text{Reliability} = 100\% - \text{BER}. \quad (3)$$

An ideal PUF should provide zero response difference to the same challenge under varying operating conditions, and therefore, BER can be defined as follows:

$$\text{BER} = \frac{1}{\binom{T}{2}} \sum_{i=1}^{T-1} \sum_{j=i+1}^{T} \frac{\text{HD}(r_i, r_j)}{L} \times 100\%, \quad (4)$$

where $r_i$ and $r_j$ are $i$th and $j$th response strings to the same challenge of PUF instance.

#### 2.3.2.4 Uniformity

Uniformity represents the capability of PUF to produce balanced bits in response. It is expressed as a percentage by calculating Hamming weight (HW) in response, and the ideal uniformity is 50%. Uniformity can be calculated as follows:

$$\text{Uniformity} = \frac{1}{L} \sum_{j=1}^{L} r_{i,j} \times 100\%, \quad (5)$$

where $r_{i,j}$ is $j$th bit of a $L$ bit response from an $i$th PUF instance. The uniformity of bit-string can be evaluated through subtests of the statistical test suite provided by NIST.

#### 2.3.2.5 Bit-aliasing

Bit-aliasing represents the capability of a PUF to produce balanced bits across responses. It can be measured by calculating the total number of ones in a particular bit from different PUF responses to an identical challenge. Ideal bit-aliasing is 50%, and it can be expressed as follows:

$$\text{Bit}-\text{aliasing} = \frac{1}{P} \sum_{i=1}^{P} r_{i,j} \times 100\%, \quad (6)$$

### 2.3.3 PUF attacks

PUF can be subjected to various attacks. An adversary can attempt to duplicate (clone) or build a model of the original using various methods such as direct measurement and chosen challenge generation.

For cloning attacks, entire responses to corresponding challenges can be read out in an invasive manner. In this case, weak PUF can be read out, even though the response exists in the system only for a short time. Even if care is taken to prevent key readout over a standard on-chip channel, other threats using laser stimulation can reveal the key if weak PUFs are used. In an invasive attack, an adversary can reprogram

the tendency of a cell using focused ion beam circuit edit, thus effectively cloning the CRP behavior of the PUF. The cloning and invasive attacks appear less applicable to strong PUFs.

The most relevant method of attack for strong PUFs is modeling attacks. In this method, an adversary collects a large number of CRPs from a given PUF and tries to extrapolate the behavior of the PUF on unknown CRPs by numeric methods parametric model using collected CRPs. Machine learning (ML) algorithms are a powerful tool to this end. Indeed, if one could learn the basic delay parameters and model the interaction with the challenge bits, one could accurately predict the response bits for the random challenge, even without access to the PUF (Maes and Verbauwhede, 2010b).

# 3 PUF constructions

This section provides examples of different types of PUFs. In particular, the sources of randomness, configuration, and performance results are discussed.

## 3.1 Coating PUF

Posch (1998) proposed using an active coating to protect IC, and Tuyls and Škorić (2006) proposed further building a PUF integrating the coating layer into IC. The top of the IC is covered with a protective coating layer, doped with random dielectric particles of random sizes and shapes. The IC is equipped with an array of metal sensors beneath the coating layer. Each sensor locally probes the dielectric properties of the coating layer and measures the capacitance. For coating PUF, the selection of specific sensors is the challenge, and measured capacitance values by selected sensors become the response. The coating layer can physically protect the coating PUFs against physical attacks. Tamper evidence was also verified since the coating layer resides on the top of the IC. However, coating PUFs have limited challenge space because the number of sensors only can be limited, and mathematical cloning possibility exists.

## 3.2 Optical PUF

The concept of building PUF using the interaction of visible light with randomized micro-structure was firstly proposed by Pappu (2001) and Pappu et al. (2002). Optical PUF is constructed with optical micro-structure tokens, in which each token produces an irregular speckle pattern from refractive particles of the micro-structure when irradiated with a laser. Then, the patterns are processed into a binary vector using an image processing technique. The laser orientations are used as challenges, and the resulting feature vectors are responses. Optical PUF has the benefits of having a large challenge space and computational difficulty for predicting responses to unknown challenges (Tuyls et al., 2005). However, it exhibits relatively low reliability compared to conventional PUFs requiring a sensitive reader, which increases the cost of deploying these PUFs (Rührmair et al., 2011).

Jiang and Chong (2008) proposed different optical PUFs that exploit random patterns formed by scattering phosphor particles of random sizes and shapes. The pattern of phosphor PUF is then used for the anti-counterfeiting system.

## 3.3 Silicon PUF

Building PUF on silicon has a significant advantage in that the PUF feature can directly connect to standard digital circuity embedded on the same chip. This has led silicon-based PUFs to become the mainstream of modern PUF constructions. This section discusses examples of silicon-based PUFs and summarizes the source of randomness, configurations, and performance of each PUF.

### 3.3.1 Ring oscillator PUF

Ring oscillator PUF (RO-PUF) is a well-known silicon-based PUF, generally classified as an intrinsic PUF. RO-PUF can have various configurations with different randomness source, but all are based on the change in frequency of the oscillating circuit. Gassend et al. (2002b) proposed delay-based RO-PUF. Its architecture includes a delay circuit placed in the oscillator circuit loop with additional AND gates (Figure 2). The delay circuit consists of $n$–1 stages of switch components and a final multiplexer (MUX) (Figure 2B), where $n$ is the bit length of the challenge. Each switch component consists of two 2–to–1 MUXes and pairs of buffers (Figure 2C). At each switching stage, the input (rising or falling) edge can be crossly or straightly sent to its output terminal depending on the challenge bit of the stage. After the $n$–1 stages, one of the two edges is selected by MUX and fed into input through negative feedback to form oscillation. The frequency of the oscillating signal is then counted by an edge detector, and the counted value is PUF response. The main drawback of this PUF is that although the number of challenges is exponential, the challenges are not independent. This can lead to severe vulnerability to model-building attacks. As such, RO-PUF may have "physical unclonability" but not "mathematical unclonability" (Maes, 2012).

Suh and Devadas (2007) introduced another RO-PUF using more than one oscillation loop. They used identically implemented $n$ numbers of ring oscillator blocks that consist of series inverter chains (Figure 3). Challenge of PUF select a pair of the blocks using MUXes. Then, two counters separately count the frequencies of signals from selected oscillating blocks. Comparing the two counted values ($f_A$ and $f_B$) is the corresponding PUF's response bit. The number of possible

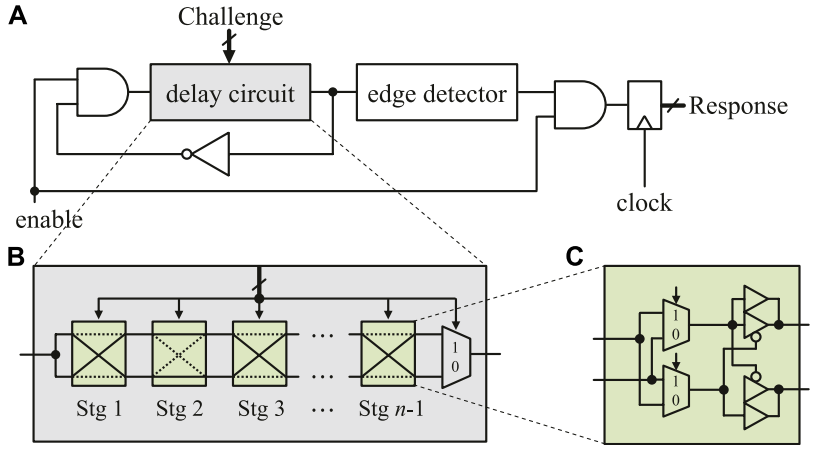


FIGURE 2
RO-PUF proposed by Gassend et al. (2002b). **(A)** RO-PUF architecture with **(B)** n-1 stage delay circuit. **(C)** 2-to-1 MUX-based switching stage.

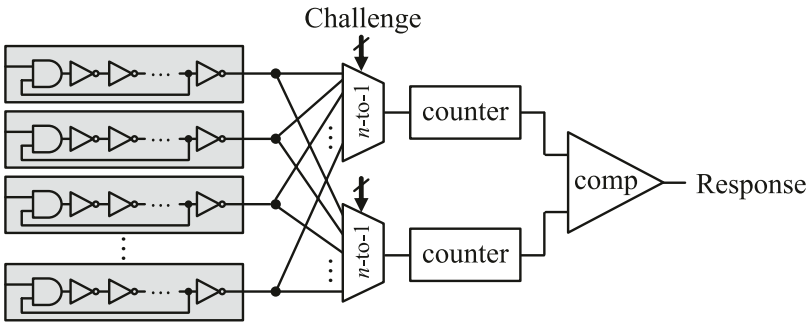


FIGURE 3
RO-PUF proposed by Suh and Devadas (2007).

challenges is calculated as $\binom{n}{2}$. However, not all these challenges are independent because there is an order of frequencies in the blocks. For using strictly independent challenges, the method where challenges only select two adjacent blocks can be used. This approach reduces the challenge space to n/2. The authors also proposed a 1–out–of–$k$ masking scheme, grouping $k$ oscillator blocks to enhance reliability. Note that this RO-PUF becomes a weak PUF because there is a limited number of challenges that can configure the PUF's operation.

Maiti and Schaumont (2009) and Maiti and Schaumont (2011) proposed reliability-enhanced RO-PUF. To reduce undesirable bias caused by variation concerning the locations of oscillators (spatial correlation), the group of oscillators is placed as close as possible, and the physically adjacent pair of oscillators are selected for the response bit generation. This shows improved uniqueness properties and reliability nearly ideally by sacrificing possible challenge space.

Yin and Qu (2010) suggested a group-based RO-PUF that leverages a subsequence grouping algorithm instead of dealing with spatial correlation. The PUF shows ×9.82 improved reliability compared to RO-PUF with 1–out–of–$k$ masking scheme ($k$ = 8) while keeping independent challenge space at $\lfloor \frac{n}{2} \rfloor$. Shortly after, Yin et al. (2013) suggested using a low complexity algorithm to replace the subsequence-based grouping algorithm for practicality.

### 3.3.2 Arbiter PUF

Arbiter PUF (Arb-PUF) is another well-known type of PUF that focuses on the delay feature in randomness sources. Gassend et al. (2004) firstly proposed PUF with arbiter circuits. Arb-PUF uses two delay paths as a form of concatenating $n$ number switch components (Figure 4A). The circuit for each stage consists of a switch component of two 2–to–1 MUXes and two buffers (Figure 4B). Similar to RO-PUF, the input (rising or falling)

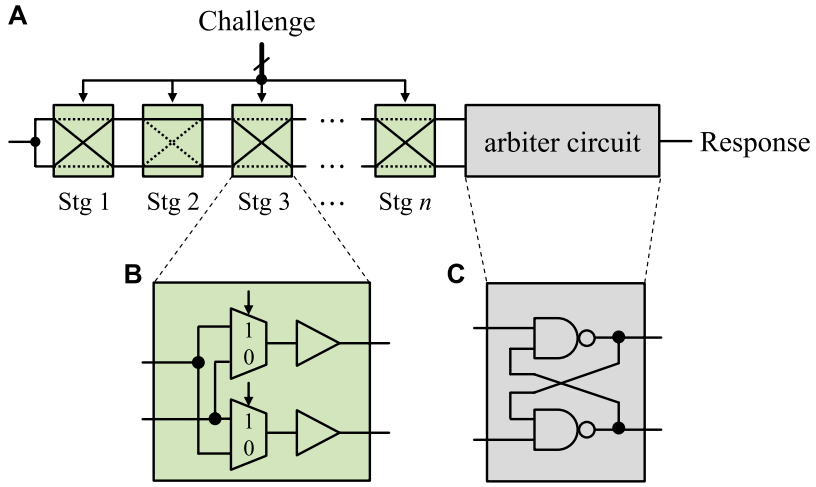


FIGURE 4
Basic structure of Arb-PUF. **(A)** Arb-PUF uses **(B)** multiple stages of switch components and **(C)** an arbiter circuit.

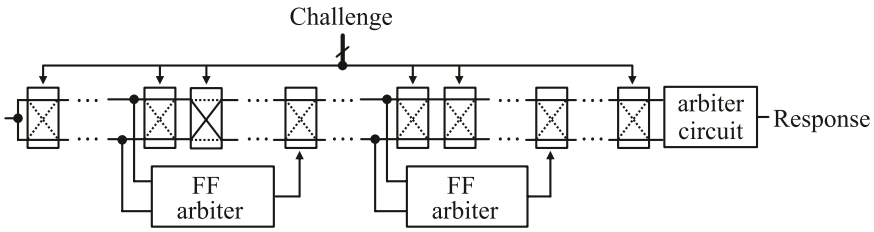


FIGURE 5
FF-Arb-PUF circuit as proposed by Lee et al. (2004) and Lim et al. (2005).

edge can be crossly or straightly sent to its output terminal. After the *n*th stage, an arbiter circuit is used for response bit generation, the winner of the race (Figure 4C). The response bit is decided by one out of $2^n$ possible delay paths (challenge bit). However, not all these delay paths are independent, which makes Arb-PUF vulnerable to modeling attacks. The lack of independence in responses is apparent in the achieved uniqueness results, which is 1%, far from the ideal value of 50%.

Lee et al. (2004) proposed a nonlinearity-based Arb-PUF, a PUF with integrated feed-forward (FF) arbiters[1]. The main structure is similar to the conventional Arb-PUF, but FF arbiters are added to some switching components (Figure 5). The effect of the added FF component is evident in the experiments of Lim et al. (2005) and Lim (2004). The results show a significant improvement in the uniqueness of 38%. However, including FF implementation sacrifices the reliability of PUF by 5%. This may be due to the increased noise probability due to the internal arbiters (Majzoobi et al., 2009). Nonetheless, the nonlinear behavior can complicate the reverse engineering process. Suh and Devadas (2007) proposed a PUF configuration with increased resistance to attacks by XORing the multiple outputs of the Arbiter circuit to obfuscate the outputs (response bits). However, later, it was shown that attacks using advanced ML techniques could effectively break the security of this PUF (Rührmair et al., 2010).

## 3.4 Memory-based PUF

One of the widely investigated types of silicon-based PUFs is memory-based PUFs. Memory devices such as D flip-flops and SRAM are composed of standard complementary metal-oxide-semiconductor (CMOS) components; thus, the memory-based PUF has the advantage that a separate manufacturing/fabrication

1 It was originally suggested by Gassend et al. (2004) in a rough manner.

process is not required to use the PUF feature on the chip. In addition to the manufacturing benefit, the response measuring circuits for memory-based PUFs can be intrinsically simpler than those for delay-based PUFs.

Flash memory cell consists of an array of floating gate transistors comprising stacked two gates (control gate and floating gate). The threshold voltage of each transistor without charge on its floating gate varies due to manufacturing process variations. It means that the amount of charge required to store logic value "0" varies from transistor to transistor.

Dynamic random-access memory (DRAM) was investigated for building PUF. DRAM cell consists of a capacitor and an access transistor. DRAM cell bit-line (BL) carries a logic value depending on the amount of charge in the capacitor. The capacitor of each cell has a different leakage charge level due to the non-ideality of the access transistors caused by, for example, sub-threshold leakage and gate-induced drain leakage.

Guajardo et al. (2007) proposed SRAM-PUF that exploits the randomness source from SRAM cells, often in an arrayed structure. The structure of an SRAM cell typically consists of six transistors[2] that are two access transistors controlled by a word-line (WL) signal and two cross-coupled inverters connecting the data lines ($\bar{Q}$ and Q) to bit-lines ($\overline{BL}$ and BL). The startup state of SRAM cells is used for building PUF. Due to the uncontrollable process variations, the startup state of each cell is independent. Therefore, for SRAM-PUF, the challenge is given as a selection of memory locations, and the response is the cell readout results.

Alternative memory-based PUFs using more advanced digital storage elements were also introduced. Su et al. (2007) proposed using a latch in which each memory cell consists of cross-coupled NOR gates. Like SRAM-PUF, latch PUF relies on randomness across the memory cells caused by threshold voltage mismatch. Kumar et al. (2008) presented Butterfly PUF, a method to emulate SRAM behavior while it can fix the need to reset memory cells on startup. It consists of two cross-coupled latches with clear/preset input that drives the cell to its instability. van der Leest et al. (2010) introduced a processing method to overcome the naturally presented startup value bias of D flip-flop cells of PUF.

Most memory devices are standard CMOS components that are freely distributed on ICs. In this context, memory-based PUFs benefit from no (or low) additional resources required for embedding security functions to the IC. Memory-based PUFs usually generate a limited number of CRPs; thus, they are generally suitable for security key generation. Although the uniqueness of most implementations is close to ideal (50%), no exceptionally high reliability is observed. Reliability is a critical attribute for secure key generation, and failure to achieve this will require some error correction process.

2 The type of SRAM cells varies, and other kinds use 4, 8, 10, or 12 transistors.

TABLE 1 Comparison of emerging NVMs.

| | FeRAM | PCRAM | MRAM | ReRAM |
|---|---|---|---|---|
| Endurance | ✓ | △ | ✓ | △ |
| Retention | ≥10 y | ≥10 y | ≥10 y | ≥10 y |
| Scalability | ✗ | △ | △ | △ |
| Write speed | ✓ | ✗ | ✓ | △ |
| Read speed | ✓ | ✓ | ✓ | ✓ |
| Power consumption | ✓ | ✓ | ✗ | ✓ |

✓, good; △, medium; ✗, poor.

# 4 Emerging non-volatile memory for PUF

## 4.1 Emerging non-volatile memory

Data storage is required in any functional information processing system. As consumer electronics is shifting toward pervasive and mobile applications, high-performance and additional hardware requirements such as lower power, lower cost, and compact become essential. Semiconductor memory can be split into two significant categories regarding data persistence: volatile and non-volatile memories (NVMs). Although volatile memories have numerous advantageous features such as dense structure (DRAM) and fast writing/reading speed (SRAM), they lose their stored data when power is switched off. On the contrary, for NVMs such as ROM or flash memory, their stored data can be preserved when power is switched off. Thus, for many decades, flash memory applications have grown explosively. However, flash memory is gradually approaching the physical limit of scalability. With CMOS scaling approaching the limits, some novel memory devices have been proposed. While the development of 3D flash memory will likely keep flash memories in an essential role in the market, the scalability limit of memory has led to the consideration of other "non-charge" memory technologies (called emerging NVM).

Emerging NVMs involve novel mechanisms and materials that differ from those of mature memory technologies. The switching mechanisms extend beyond classical electronic processes to quantum mechanical phenomena, ionic reactions, phase transition, and molecular reconfiguration, among others. The materials include ferroelectric oxides, ferromagnetic metals, chalcogenides, metal oxides, and carbon materials. Ferroelectric random-access memory (FeRAM) has a similar construction to a DRAM but uses a ferroelectric layer instead of a dielectric layer in the capacitor. When applying an electric field, the dipoles align with the field direction. After the charge is removed, the dipoles retain their polarisation state. Phase-change resistive access memory (PCRAM), on the contrary, relies on switching between the low resistance state (LRS, crystalline phase) and

the high resistance state (HRS, amorphous phase) of chalcogenide materials. A significant difficulty is expected due to temperature cross-talk between adjacent memory cells as the technology scales down. Magnetic random-access memory (MRAM) relies on two ferromagnetic plates holding a magnetic field, separated by an insulator. While one plate holds a permanent magnetic field, the direction of another plate can be switched (parallel or anti-parallel to the permanent plate). Finally, redox-based random-access memory (redox-based resistive random-access memory (ReRAM)) relies on the formation (LRS) and the rupture (HRS) of conductive filament(s) in the oxide layer.

Table 1 summarizes the characteristics of emerging NVMs. FeRAMs offer excellent endurance, good write/read speed, and very low power consumption. However, a destructive read process and a scalability limit make it less attractive. Relatively high currents for a long time are required for PCRAMs during programming. Moreover, due to the thermal process involved, crosstalk between neighboring cells becomes an issue in large arrays for PCRAMs (Gaba, 2014). The large programming current and scalability issues (crosstalk issues when cell size scales) prevent MRAM from being cost-effective to challenge the well-established flash memory market. Resistive switching memories such as PCRAM and ReRAM are inherently freer from scaling problems than charge-based FeRAM. In particular, ReRAM has more stable resistance states and a larger on/off resistance ratio (therefore, larger noise margin for better reliability) compared to other types (Jeong et al., 2012). As such, resistive memory has recently emerged as a contender in the NVM race.

## 4.2 Resistive random-access memory

The first resistive switching effect was reported in the early 1960s (Gibbons and Beadle, 1964). In the early 2000s, renewed interest brought to the ReRAM concept and the resistive switching effect has been observed in a broad range of materials, including perovskites, solid electrolytes, and binary metal oxides. Mechanism-based classification broadly divides ReRAMs into three categories: electrochemical metallization (ECM) devices, valence change mechanism (VCM) devices, and thermochemical mechanism (TCM) devices.

The redox-based nano-ionic memory operates based on the resistance change of insulators caused by ion (cation or anion) migration combined with the redox process involving the electrode and insulator materials. An ECM-based device switching is typically due to cation motion, whereas metal oxide ReRAMs such as VCM and TCM switching are due to anion reconfiguration. In a particular example of oxide-based resistive switching devices, the switching between a low-resistance state (LRS) and high-resistance state (HRS) is known to involve the formation and rupture of conductive filament(s) during the state transitions.

### 4.2.1 Cell array configuration

A high-density ReRAM is obtained by a simple crossbar structure called CBA. The structure can have multiple memory cells arranged in a matrix (Figure 6). In the simplest case, every cross-point of CBA has one ReRAM cell (Figure 6A). The minimum unit cell size of $4F^2$ can be achieved in this configuration, where $F$ is the feature size. However, this configuration leads to a sneak path problem when the HRS cell, which is surrounded by LRS cells, is in the readout state. For an accurate cell reading or low-power writing, an extra selection device (selector) is required to be connected to every cell in the series. Using a varistor or diode as a selector element (Figure 6B) works well for the unipolar ReRAM but not for the bipolar devices. Figure 6C shows one transistor-one resistor that is called 1T1R (Sheu et al., 2009). The structure is often undesirable for high-density applications as additional space is required. Also, it is more complicated, and the high-temperature fabrication process of the transistor may be unsuitable for back-end-of-line (BEOL) processes. Although complementary mode can maintain a size of $4F^2$ (Figure 6D), it inherently serves as a penalty to induce a destructive READ operation (Linn et al., 2010).

### 4.2.2 ReRAM variability

ReRAM shows programming variability in its resistance, including device-to-device (D2D) variability, cycle-to-cycle (C2C) variability, and stochastic switching. Parameters such as LRS and HRS are random variables with a log-normal distribution. ReRAM also has inherent randomness at the device level due to the device's C2C programming variation and the manufacturing level, such as thickness and cross-sectional area variations (Chen and Lin, 2011). These resistors are random variables with a normal distribution. These resistances are random variables with a log-normal distribution.

### 4.2.3 ReRAM reliability

The reliability of ReRAM has two critical aspects: cycling endurance and data retention (Yu, 2016). The cycling endurance means how many programming cycles the ReRAM device can endure before it fails to hold the switching variability. The endurance highly depends on the programming conditions, such as current compliance and the programming voltage. Data retention refers to how long the memory device can maintain the current state; therefore, it is highly related to the stability of the memory technologies. Typically, data retention is expected to be longer than 10 years for NVM devices maintained at a high temperature up to 85°C because the operating temperature on the chip is expected to be high. Many studies report that ReRAMs can serve compatible endurance and retention with elevated temperature.

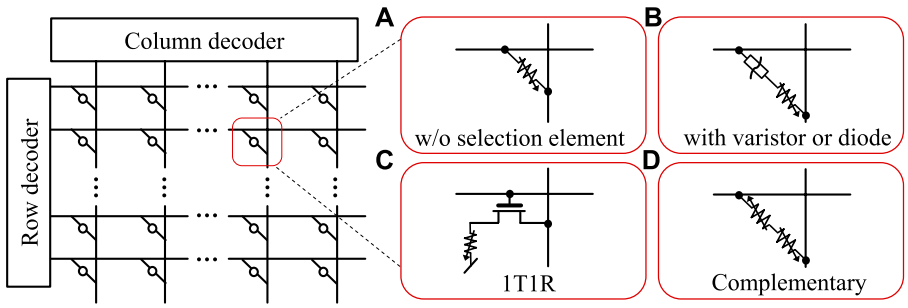


FIGURE 6
The crossbar-array architecture **(A)** without any selection elements. **(B)** Cells with a varistor or diode type of selector, **(C)** 1-transistor 1-resistor (1T1R) cell, and **(D)** a complementary state cell (adapted from Waser et al. (2016)).

Unintended current fluctuation in ReRAM is one of the main reliability concerns. Noise in ReRAM is believed to be caused by its filaments switching and conduction mechanism. Noise generally appears as a $1/f$ fluctuation of the current, resulting from a superposition of several components of random telegraph noise (RTN) (Ambrogio et al., 2014). The noise is a low-frequency random fluctuation of conductance that appears in two or more levels, and the switching time between different levels is a stochastic phenomenon.

## 4.3 ReRAM PUF

ReRAM has been widely investigated for the randomness source of PUF due to various advantageous features; ReRAM has the advantage of being well compatible with CMOS manufacturing standards, and its structure has high density (Rose et al., 2013b). It also operates at low power compared to other types of memory such as MRAM and flash memory. This memory's fast access times and programming speed have also contributed to active research in ReRAM-based applications. In addition, the reconfigurability of ReRAM also makes the ReRAM-based PUF implementation favorable. In addition to manufacturing uncertainties, the emerging memory devices, including ReRAM, have shown programming variability, which introduces stochastic switching and C2C variability. Therefore, these sufficiently (desirable) variabilities in the ultra-dense structures of ReRAM CBA are more favorable for PUF construction.

Wendt and Potkonjak (2011) introduced the idea of integrating emerging NVM into PPUF construction. Shortly after, Rajendran et al. (2012b) proposed NVM array-based PPUF. Its construction uses unique geometric structures called polyominoes, formed by connecting a certain number of adjacent blocks in horizontal or vertical directions. Resistive switching devices such as ReRAM in a CBA are used to form the polyominos. Simulation results showed the uniqueness of 49%–50% and diffuseness of 49% over a 1%–5% controlled oxide thickness variation (Rajendran et al., 2012b). Bit-aliasing and uniformity were also close to ideal (50%) (Rajendran et al., 2012a). Wendt and Potkonjak (2013) demonstrated the attack scenarios. The correlation between the input and output vectors of the PUF is non-trivial by the large input set space. Although the possibility of finding a predictive mapping was mentioned, the task for every possible input set also increases exponentially with the number of pins in the PUF. Other attack scenarios also claim that the difficulty increases with the increasing size of the PUF. Finally, side-channel attacks are infeasible because PPUF are already public, and no attack reveals new information.

Kavehei et al. (2013) proposed the concept of integrating resistive switching memory into RO-PUF structure. The resistance variability of HRS and LRS are used to determine the delay of the ring oscillator in addition to the CMOS process variation (Figure 7). Gao et al. (2015) comprehensively evaluated the performance of this PUF. The number of CRPs is estimated to be $\frac{n}{2}\binom{n}{i}\binom{n-1}{i}$, where $n$ is the number of ring oscillators, a significantly increased number compared to the conventional silicon RO-PUF. ReRAM RO-PUF has advantages such as a large number of CRPs and relatively low area overhead, but using the raw response of the PUF directly as a cryptographic key is unrealistic in terms of reliability. In order to address the issue, an error correction process needs to be included, potentially increasing the area and cost of the PUF.

Mathew et al. (2015) proposed PUF that integrates ReRAM into the Arb-PUF structure. The architecture of this PUF consists of an equal number of delay components in two different paths (Figure 8). Each delay element consists of one ReRAM cell and one transistor whose drain terminal is connected to the memory cell. At the end of the path, one D flip-flop is shared, and each input is individually connected to

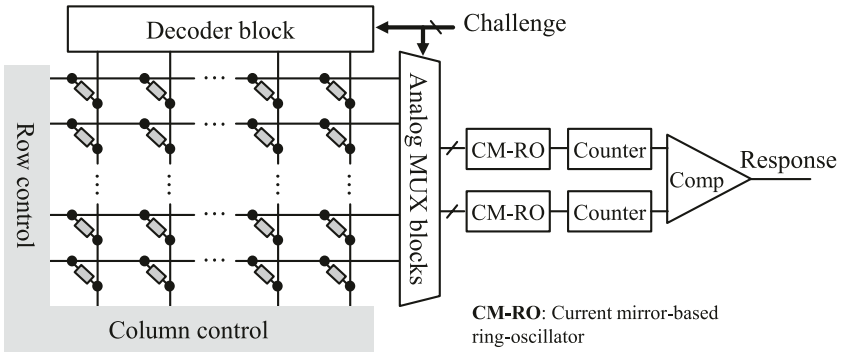


FIGURE 7
ReRAM-based RO-PUF structure (adapted from Gao et al. (2015)).

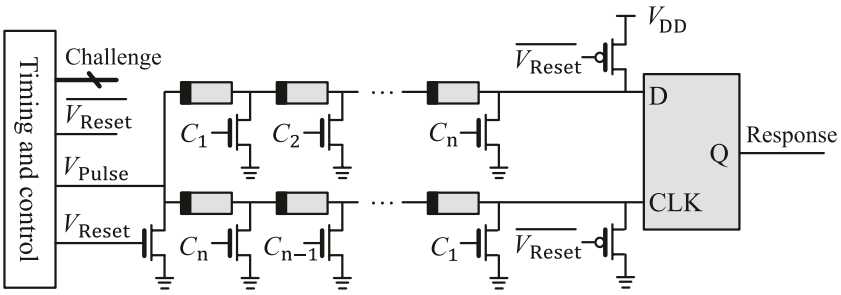


FIGURE 8
ReRAM-based Arb-PUF structure (adapted from Mathew et al. (2015)).

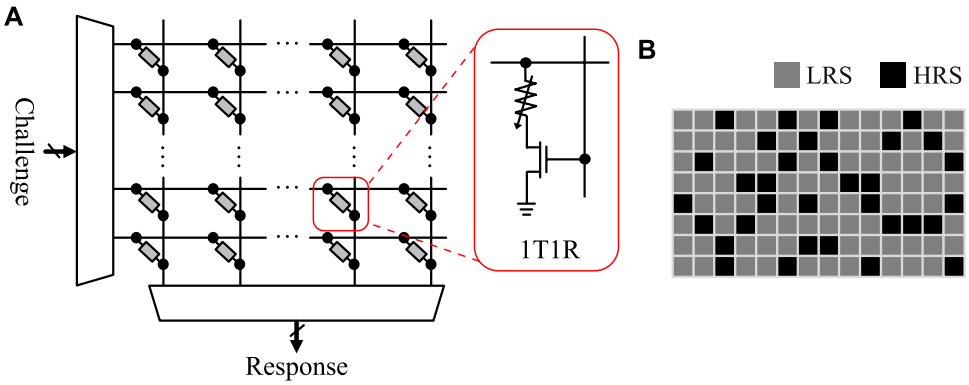


FIGURE 9
T1R ReRAM-based PUF (adapted from Chen (2015a)) using **(A)** 1T1R ReRAM array. **(B)** Expected LRS/HRS distribution.

each path. For each path, the gate terminals of the transistors are controlled with the same challenge in an asymmetrical manner. Depending on its challenge, the resistance level of each memory cell is adjusted, then a race between the pulse signal propagates through each path, resulting in a response to the challenge.

Chatterjee et al. (2016) evaluated ReRAM Arb-PUF against attacks. This includes the robustness to model-building attacks (50.37–60.67%) and the high vulnerability to the chosen challenge-based cryptanalysis attacks. To address the potential security issue, a modified ReRAM-based Arb-PUF was suggested. Drain and source terminals of a transistor connect each memory cell in this modification, which makes modulating the resistance of cells depend on the applied challenge bits. As a result, the modified PUF achieved improved immunity against the attack discussed.

Arb-PUF using 1T1R ReRAM CBA was introduced by Govindaraj and Ghosh (2016). The use of CBA increases the limited number of CRPs of the previously suggested ReRAM Arb-PUFs. Simulation results show high reliability of 99.87% under varying voltage and temperature conditions. Later, another ReRAM-based Arb-PUF was proposed by Beckmann et al. (2017).

Rose et al. (2013a) and Rose et al. (2013b) introduced PUF, focusing on the memory write-time parameter. ReRAM cells' write-time, the minimum time required to switch the memory from HRS to LRS, varies, and this variability can be the randomness source for building PUF. Data are written using the write-time, and the stored data are read out using the XOR gate, whose another input terminal is connected to the challenge bit, and the read-out corresponds to the response bit. Mazady et al. (2015) experimentally demonstrated the 1-bit write-time-based PUF. The minimum write-time requires careful calibration for solid statistical behavior. Rose and Meade (2015) proposed a modified write-time-based PUF that focuses on the structural feature of CBA to minimize the need for the extra calibration process. The modification results from using a complementary writing scheme (for two lines) that resorts to the relative write-times of pairs of the memory circuits. In addition, the modified PUF can generate multi-bit responses within one execution; however, this feature increases the vulnerability to model-building attacks similar to Arb-PUF.

Uddin et al. (2016) added the XORing technique to pairs of responses, and the improved reliability was shown from the simulation. Later, Uddin et al. (2017a) and Rose et al. (2017) added circuit blocks inside the crossbar to build non-linearities. In other words, some columns of memory CBA are routed to other arbiter inputs. Then, two arbiter outputs are combined with an XOR gate to generate a response bit. Due to the structural complexity, it is expected to be more robust against ML-based modeling attacks. Uddin et al. (2017b) evaluated the attack vulnerability of this PUF and found improved robustness to well-known machine learning algorithms.

Koeberl et al. (2013) proposed write-time- and voltage-based PUF, which has a similar concept to the previously introduced write-time-based PUF. First, all the memory cells are set to their LRS, and then, low write-voltage is applied to all cells again to reset, ideally precisely, half of the cells back to HRS. Although this modification brings some advantages, it also has disadvantages. The burden of the pre-calibration procedure increases, and the CBA size limits the total number of total CRPs.

Chen (2015a) proposed ReRAM switching probability-based PUF built on a 1T1R CBA structure (9). The operating procedure is similar to the write time/voltage-based PUF. A specific pre-calibrated voltage that resets the cells with a 50% probability is applied to all cells, and a random LRS/HRS pattern is used as a randomness source. The address (location) of the memory cell array is the challenge, and the data read is the response. More importantly, due to the random behavior of fractures and the formation of filaments, reversing reconstruction is nearly impossible, which may help lower the susceptibility to attack.

Many studies have investigated random LRS/HRS patterns across memory CBA for a randomness source for PUFs. Che et al. (2014) proposed voltage-to-digital converter- (VDC-) based PUF. Using VDC aims to achieve bimodal resistance distribution in the memory array. The LRS resistance of all memory cells is digitized to values ranging from 0 to 127 using VDC, and it is stored in an SRAM array by cell-to-cell mapping. Cells are divided into two groups according to the median of the resistance distribution. Then, all memory cells belonging to the group with high resistance distribution are reset to their HRS, producing the random LRS/HRS pattern across the memory array. This creates a unique PUF signature that is different from other PUF instances.

Liu et al. (2015) investigated the split-reference current method to build a PUF with improved reliability. First, all ReRAM cells in the array are programmed with HRS and then read to find a reference current that ideally divides them into two groups with the same number of cells. Similar to previous works, memory cells with sensing current above the reference current are set into LRS. The address is given as the challenge, and digital readout through the sense amplifier is the response of PUF. For improved PUF reliability, it utilizes eight parallel cell readout methods for response generation; the method is likely to increase area and power overheads.

Pang et al. (2019) suggested a split-resistance technique for higher reliability of PUF. The sensing window can be widened by borrowing the approach of reading the two selected memories in the challenge and programming them into opposite states, LRS and HRS, respectively, based on the result. Twenty test chips, each with an 8 kb ReRAM array, were fabricated, and PUF evaluation metrics were measured experimentally.

Liu et al. (2016) considered the tamper evidence property of PUF. ReRAM conduction in oxide is unlikely to emit photons under the laser of X-ray scanning. However, if the adversary uses a micro-probe to extract secret information, the digital response of the memory cell can be read through a sense amplifier. The layout obfuscation method was suggested to overcome the issue. In addition, a multi-cell-per-bit method was adopted for improved retention of the memory. Shrivastava et al. (2016) evaluated the reliability of the multi-cell read-out method. PUFs

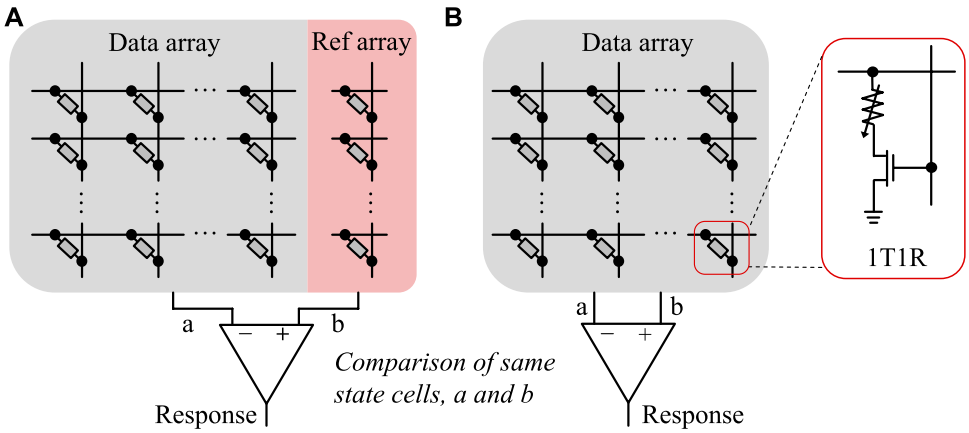


FIGURE 10
Dual mode comparison-based PUFs of **(A)** single-ended mode and **(B)** differential mode (adapted from Zhang et al. (2014)).

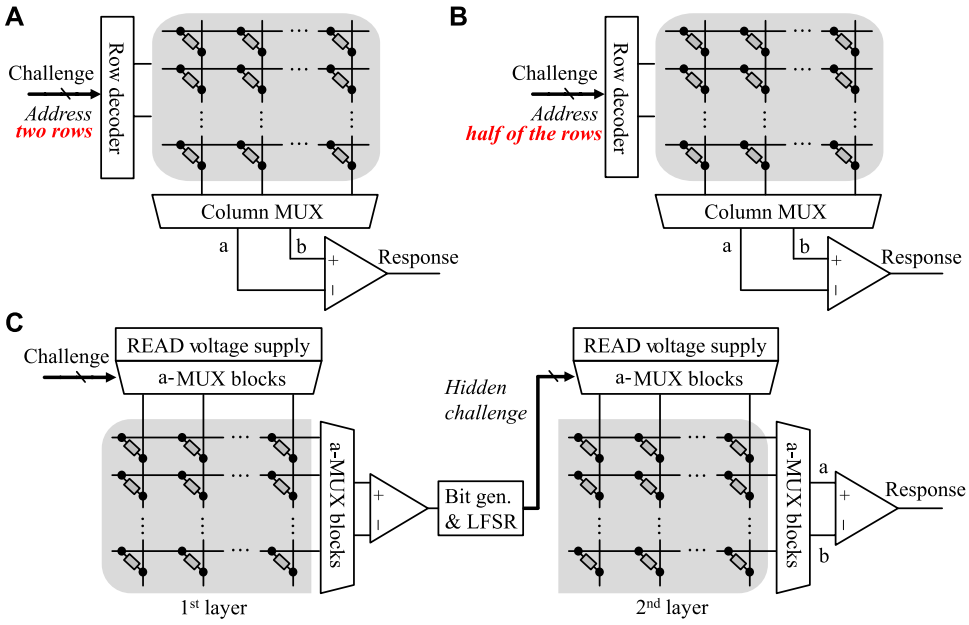


FIGURE 11
Structures of different types of ReRAM PUFs. **(A)** Cross-point-based ReRAM PUF, adapted from Chen et al. (2015), and **(B)** sneak path-based ReRAM-PUF, adapted from Gao et al. (2016). **(C)** Non-linear ReRAM-PUF adapted from Kim et al. (2018a).

without this method showed a failure rate of 1.78%. The rate was reduced to 0.13% with the two-cell-per-bit method and zero with the eight-cells-per-bit method. The zero-failure rate ensures no requirement for an error correction code (ECC) that will likely increase circuit overhead.

Pang et al. (2017a) proposed another PUF focusing on enhanced reliability. First, all the memory in a 1T1R CBA is reset to HRS. The addresses of two adjacent columns are used as a challenge, and the response is a row-by-row comparison of the resistances of the two selected columns of cells. Upon completing each row comparison, the cell with lower resistance is programmed to LRS. The method effectively enhances the reliability of the PUF to ~100%, which was ~95% of that without the method.

Cambou and Orlowski (2016) investigated the ternary state of ReRAM for building PUF. Instead of the binary

TABLE 2 Uniqueness, diffuseness, uniformity, and bit-aliasing comparison of ReRAM-based PUF constructions.

| References | Source of randomness | Type | $N_{PUF}$ | Environmental Factor | Uniqueness | Diffuseness | Uniformity | Bit-aliasing |
|---|---|---|---|---|---|---|---|---|
| Rajendran et al. (2012a) | Device R | SIM | 100 | NA | 49.0 ~ 50.0† | – | 46.0 ~ 53.0† | 46.0 ~ 53.0† |
| Rajendran et al. (2012b) | Device R | SIM | 100 | NA | 49.0 ~ 50.0 | 49.0 | – | – |
| Kavehei et al. (2013) | Group device R | SIM | 10 | Temp.: 70°C | 50.0 | – | – | – |
| Gao et al. (2015) | Group device R | SIM | 100 | NA | 50.1 | 50.0 | 50.8 | – |
| Mathew et al. (2015) | Stage delay | SIM | NA | NA | 49.9 ~ 50.4 | – | 50.6 ~ 53.8 | 49.2 ~ 52.4 |
| Chatterjee et al. (2016) | Stage delay | SIM | NA | NA | 49.4 ~ 52.0 | – | 50.3 ~ 54.8 | 48.5 ~ 53.4 |
| Govindaraj and Ghosh (2016) | Stage delay | SIM | NA | Threshold V: ± 10% | 51.3 | – | 50.0 ~ 53.0‡ | – |
| Beckmann et al. (2017) | Stage delay | S&E | 250 | Temp.: 0 ~ 125°C | 50.0† | – | – | – |
| Rose et al. (2013a), Rose et al. (2013b) | Write-time | SIM | 100 | NA | 49.9 | – | 50.0 | 50.0 |
| (Rose and Meade, 2015) | Write-time | SIM | NA | Volt: 0.7 ~ 0.9 V | 48.2 ~ 50.0 | – | 50.1 ~ 52.6 | – |
| Uddin et al. (2016) | Write-time | S&E | NA | NA | 50.0 | – | 50.2 | – |
| Uddin et al. (2017a) | Write-time | S&E | NA | Temp.: 10 ~ 100°C | 50.2 | – | 56.5 | 51.5 |
| Chen (2015a) | Write-time and volt | S&E | 100 | Line *R*: 0 ~ 2 Ω | 47.0 ~ 50.0 | – | 50.0 ~ 51.0 | – |
| Koeberl et al. (2013) | Write-time and volt | SIM | 2 | NA | 46.0 ~ 53.0† | – | – | – |
| Pang et al. (2019) | Device R | EXP | 20 | Temp.: 25°C | ~ 50.0 | – | 50.0 | – |
| Liu et al. (2015), Liu et al. (2016); Shrivastava et al. (2016) | HRS R | EXP | 40 | NA | 49.0 ~ 49.8 | – | – | – |
| Pang et al. (2017a) | HRS R | EXP | 3 | Temp.: 25 ~ 125°C | 49.8 | – | – | – |
| Zhang et al. (2014) | LRS/HRS R | SIM | 1,000 | NA | 49.0 ~ 50.0 | – | – | – |
| Chen (2015b), Chen (2015c) | HRS R | SIM | 100 | Temp.: 300 ~ 450 K | 50.0 | – | 50.0 | – |
| Chen et al. (2015) | Device R | S&E | 100 | Temp.: 0 ~ 85°C | 49.9† | – | – | – |
| Gao et al. (2016) | Device R | EXP | 28 | NA | 46.2 | ~50.0§ | ~50.0§ | – |
| Liu et al. (2017) | Device R | SIM | 100 | References I: 29 $\mu$A | 50.4 | 49.5 | 50.4 | – |
| Pang et al. (2017b) | Device R | EXP | NA | NA | ~50.0 | – | – | – |
| Liu et al. (2018) | Device R | SIM | NA | References I: 14.5 $\mu$A | 49.8 ~ 50.4 | 50.4 | 43.1 ~ 48.1 | 43.1 ~ 48.1 |
| Kim et al. (2018a) | HRS R | S&E | 1,000 | Temp. and volt: ±10% | 49.9 | 49.9 | 47.3 | 49.5 |
| Nili et al. (2018) | HRS R | EXP | NA | NA | 50.1 | 49.9 ~ 50.0 | 49.5 ~ 50.0 | – |
| Lee et al. (2019) | Quantized R | S&E | NA | Temp.: 25 ~ 90 °C | ~ 50.0 | ~ 51.0 | – | – |
| Lin et al. (2021) | Device R | EXP | NA | Temp.: 25 °C | ~ 50.0 | – | ~ 49.5 50.0 | – |

SIM: simulation; S&E: simulation based on measured device data; EXP: experiment.
† This value is estimated from a given graph. ‡ This is evaluated by NIST, test suite. § This is widely distributed.

states of memory, LRS and HRS, memory cells are divided into three groups with two thresholds, which increase the entropy to $3^n$. Additional advantageous features were claimed, including reduced vulnerability against side-channel attacks and no (or reduced) requirement for ECC.

Zhang et al. (2014) proposed emerging memory PUFs that leverage the resistance comparison. For this PUF, the intrinsic resistance variability across the memory cells of three types of emerging NVMs, spin-transfer-torque magnetic random-access memory (STT-MRAM), PCRAM, and ReRAM, was the primary source of randomness. For response generation, single-ended and differential sensing modes were suggested; the first mode compares the resistance of the selected cell to the reference cell, whereas the second mode compares the resistance of two selected cells (Figure 10). Shortly after, the resistance comparison-based emerging NVM PUF was proposed by Zhang et al. (2015). Chen (2015b) similarly proposed PUF that generates a response by bit-wise comparison of ReRAM cells. Instead of comparing a pair cell resistance, Chen et al. (2015) proposed an optimized ReRAM-based PUF that utilizes a four-cell comparison scheme (Figure 11A). Using the scheme offers a significantly larger number of CRPs, achieving a high-security level compared to a pair cell resistance comparison.

Sneak-path is an unavoidable feature of passive ReRAM CBA. Gao et al. (2016) investigated the sneak-path as its

TABLE 3 Reliability of ReRAM-based PUF constructions in the literature.

| References | Randomness source | Type | $N_{PUF}$ | Environmental factors | | Reliability (%) |
|---|---|---|---|---|---|---|
| Rajendran et al. (2012a) | Device R | SIM | 100 | Voltage: ±20% | | 90.0 ~ 98.0† |
| Gao et al. (2015) | Group device R | SIM | 20 | Temp.: 20 ~ 85°C | Voltage: ±10% | 92.5 ~ 100 |
| Mathew et al. (2015) | Stage delay | SIM | NA | Temp.: 0 ~ 80°C | Voltage: ±15% | 92.7 ~ 99.4 |
| Chatterjee et al. (2016) | Stage delay | SIM | NA | Temp.: 0 ~ 80°C | Voltage: ±10% | 97.2 ~ 99.7 |
| Govindaraj and Ghosh (2016) | Stage delay | SIM | NA | Temp.: 10 ~ 90°C | Voltage: ±10% | 99.9 |
| Beckmann et al. (2017) | Stage delay | S&E | 25 | Temp.: 0 ~ 125°C | | 97.3 |
| Uddin et al. (2016) | Write-time | S&E | NA | Temp.: 17 ~ 67°C | | 94.0 |
| Uddin et al. (2017a) | Write-time | S&E | 10 | Temp.: 10 ~ 100°C | | 80.0 ~ 90.0 |
| Cambou and Orlowski (2016) | Write-voltage | S&E | NA | Voltage: 1.8 ~ 2.1 V | | 92.0 ~ 100 |
| Zhang et al. (2014) | LRS or HRS R | SIM | NA | Temp.: 45 ~ 85°C | Voltage: ±10% | 99.0 |
| Chen et al. (2015) | Device R | S&E | 200 | Temp.: 0 ~ 85°C | | 98.0† |
| Gao et al. (2016) | Device R | EXP | 1 | Temp.: 100 ~ 140°C | | 92.0 |
| Liu et al. (2017) | Device R | SIM | 1 | References I: 70 ~ 79 $\mu$A | | 98.0† |
| Pang et al. (2017b) | Device R | S&E | 2 | Temp.: 150°C for 60 h | | 99.0 |
| Pang et al. (2019) | Device R | EXP | 20 | Temp.: 25 ~ 150 °C | Voltage: ±20% | BER: $<6.1 \times 10^{-6}$ |
| Kim et al. (2018a) | HRS R | S&E | 100 | Temp.: ±10% | Voltage: ±10% | 98.7 |
| Nili et al. (2018); Adam et al. (2017) | HRS R | EXP | NA | Temp.: 25 ~ 90°C | Voltage: ±20% | 98.4 |
| Lee et al. (2019) | Quantized R | S&E | NA | Temp.: 25 ~ 90°C | | 98.0 ~ 71 |
| Lin et al. (2021) | Device R | EXP | NA | Temp.: 25°C | | ~ 100 |

SIM: simulation; S&E: simulation based on measured device data; EXP: experiment.
†: estimated from the given graph.

randomness source for PUFs that can increase the number of CRPs compared to conventional resistance comparison-based PUFs. Half of the array rows are addressed for generating each response according to challenge bits (Figure 11B). Then, the current values of each column are read out by applying a read voltage to the selected row, whereas not selected cells remain floating.

Due to the large number of CRPs, the PUF can be immune to the man-in-the-middle attack because the CRPs are never reused. Another possible attack model is to measure every memory cell physically. Even if it is assumed that this is possible, it is a time-consuming and practically not an easy task to simulate a large-sized network of large-sized random resistor values. Public authentication protocol was adopted to negate the possible attacks in such a scenario. The main shortcoming of sneak-path-based PUF is the massive power consumption for every response bit generation since multiple memory cells need to be read out concurrently. (Liu et al., 2017) evaluated the diffuseness of PUF. A pre-calibration method was introduced to address the relatively poor diffuseness of sneak-path PUF. A split reference method that is similar to the one proposed by Liu et al. (2015) was also adopted.

ReRAM PUF focusing on the non-linearity feature was proposed by Kim et al. (2018a). A concatenated CBA layer was adopted to create a hidden challenge addressing the memory cells in the second layer (Figure 11C). In addition, an increased CRP number was obtained using a multi-cell selection scheme. For PUF evaluated by simulation, close to ideal values were obtained in all PUF evaluation metric items defined above. Later, multi-layer and multi-cell selection-based PUFs were proposed (Nili et al., 2018) and experimentally demonstrated (Adam et al., 2017; Kim et al., 2018b). Adopting multiple cell selection can enlarge CRP to $\binom{p}{n} \times \binom{q}{n}$, where $p$ is the number of row and $q$ is the number of column used for the response generation.

Lee et al. (2019) investigated multi-state of ReRAM to build reconfigurable PUF. The selected memory cell is reprogrammed at every challenge, generating different responses. It introduces superior randomness by utilizing both D2D and C2C variations. The PUF reliability, which can be significantly degraded by temperature change, was increased to 98% using temperature compensation.

## 4.4 Comparison and discussion

Section 4.3 summarizes the key characteristics of experimentally validated ReRAM-based PUFs. Performance related to the estimated area and power budget, reliability, and uniqueness of PUFs based on CMOS and emerging technologies are summarized and compared in Table 2. In

TABLE 4 ReRAM-based PUFs performance comparison.

| References | NIST test | $N_{CRP}$ | CBA structure | Energy | Area |
|---|---|---|---|---|---|
| Wendt and Potkonjak (2011); Rajendran et al. (2012a), Rajendran et al. (2012b); Wendt and Potkonjak (2013) | – | $c\lambda^m m^{-1} \times n^{\dagger}$ | $n \times n$ | – | – |
| Kavehei et al. (2013); Gao et al. (2015) | – | $\frac{1}{2}\binom{n}{i}\binom{n-1}{i} \times n^{\ddagger}$ | $n \times n$ | – | – |
| Mathew et al. (2015) | – | $2^n$ | $2n$×1T1R | – | – |
| Chatterjee et al. (2016) | – | $2^n$ | $2n$×1T1R | – | – |
| Govindaraj and Ghosh (2016) | Partially | $2^{GC+LC+N\ddagger}$ | $2n$×1T1R | – | – |
| Rose et al. (2013a); Rose et al. (2013b) | – | $2^n$ | $n$ | – | – |
| Rose and Meade (2015) | – | $2^n$ | $2n \times 2n$ | 0.56 ~ 1.63 mW | – |
| Uddin et al. (2017a); Rose et al. (2017) | – | $2^n$ | $2n \times 2n$ | 0.02 ~ 0.10 mW | – |
| Uddin et al. (2017b) | – | $2^n$ | $2n \times 2n$ | 0.25 ~ 16 mW | – |
| Chen (2015a) | – | $n^2$ | $n \times n \times$ 1T1R | – | |
| Liu et al. (2016) | – | $n^2$ | $n \times n \times$ 1T1R | 9.59 ~ 17.69 pJ | 0.01 ~ 0.20 $mm^2$ |
| Shrivastava et al. (2016) | – | $n^2$ | $n \times n$ | – | 241 ~ 272 $\mu m^2$ |
| Cambou and Orlowski (2016); Cambou and Afghah (2016) | – | $3^n$ | $n \times n$ | – | – |
| Zhang et al. (2014); Zhang et al. (2015) | – | $n \times n \log_2 n$ | $n \times n \times$ 1T1R | – | – |
| Chen (2015b) | – | $n \times n \log_2 n$ | $n \times n \times$ 1T1R | – | – |
| Chen et al. (2015) | – | $\binom{2}{n} \times n \log_2 n$ | $n \times n \times$ 1T1R | – | 0.01 ~ 0.17 $mm^2$ |
| Gao et al. (2016); Liu et al. (2017) | – | $\binom{2/n}{n}$ | $n \times n$ | 5.3 ~ 6.2 mW | – |
| Liu et al. (2018) | – | $\binom{2/n}{n}$ | $n \times n$ | 13.17 ~ 94.79 pJ | 4,504 ~ 891 $\mu m^2$ |
| Kim et al. (2018a) | – | $\binom{5}{n} \times \binom{2}{n} \times \log_2\binom{2}{n}$ | $2 \times n \times n$ | – | – |
| Nili et al. (2018); Adam et al. (2017) | Partially | $\binom{p}{n} \times \binom{q}{n}^{\varepsilon}$ | $2 \times n \times n$ | 20 fJ | – |
| Pang et al. (2019) | Pass | 64 × 128 b | 8 kb | 3.0 pJ/bit | 2.86 $\mu m^2$ per bit |
| Lin et al. (2021) | Pass | Reconfigurable | 2×8 kb | 2.4 3.0 pJ/bit | 0.15 $mm^2$ |

[†] $c = 0.3169$, $\lambda = 4.0626$, and $m$ is the number of polyominoes.
[‡] $n$ is the number of ring oscillators; $i$ is the number of inverters in each oscillator.
[‡] $GC$ is the number of global columns; $LC$ is the number of local columns; $N$ is the number of the MUX stages.
[ε] $p$ is the number of row selections and $q$ is the number of column selections.

most cases, uniqueness close to 50% occurs. However, diffuseness measurements are not often reported despite their importance. One quality that should be achieved, but is not often emphasized in the literature, is the correlation between responses when a similar set of problems is applied. The uniformity results show values close to above 50% except for the PUF proposed by Liu et al. (2018). However, the similarity between challenge sets is not clear in most literature. The multi-layer ReRAM PUF reported by Kim et al. (2018a) is still close to the ideal uniformity of 50% when applying a very similar set of challenges.

Table 3 summarizes the reliability values of ReRAM PUF, and environmental factors significantly affect the reliability. In general, excellent reliability is required to remove the need for helper data or ECC. Some early ReRAM-PUF studies are solely based on simple device behavioral models without carefully considering other inherent characteristics of ReRAM. For example, C2C, which can potentially cause reliability degradation, is not thoroughly investigated. Even for studies with compact models, the results were obtained through simulations, which may be speculative without experimental implementation and validation. However, a majority of the PUFs are not fully experimentally validated. For example, resistance variation is based on experiments, whereas peripheral circuitry is only proposed but not experimentally implemented. Notably, the sensing circuits suffer from a small

sensing margin and long access time for the resistance comparison method due to the high and minor differences in cell resistance. Therefore, a sense amplifier (SA) becomes a critical part of these PUFs.

Table 4 summarizes the opportunities for PUF design. A statistical test suit developed by the National Institute of Standards and Technology (NIST) (Bassham et al., 2010) is used to evaluate the randomness of generated responses. Only a few ReRAM-PUFs provided successful results, and some only partially performed the test. This can be because the NIST test suite recommends the use of very long bit-stream (e.g., 10 Mbit). The number of CRP for each PUF is also estimated. LRS/HRS pattern-based ReRAM PUFs show a limited number, and they often require a precise pre-calibration process. By utilizing comparison and multiple-cell selection methods, the number of CRP can be significantly increased (Gao et al., 2016; Pang et al., 2017b; Liu et al., 2017; Kim et al., 2018a; Liu et al., 2018; Nili et al., 2018).

## 5 Challenges and future outlook

Research in emerging NVM technologies has grown significantly over the past few years, and several prototype emerging NVM-based applications have been developed. These products, including PUF and random number generator (RNG), show the potential for high-speed, low-power, and cost-effective embedded memory applications. ReRAM, in particular, is one of the most promising memory technologies due to its advantages of simple structure, compatibility with existing CMOS technologies, excellent switching speed, and ability to scale to the smallest size. Despite these advantages and possibilities, one of the most critical aspects to thoroughly investigate when using ReRAM is the reliability of the memory. This is especially important when used in devices that cannot be used without reliability guarantees, such as PUFs. PUF reliability, not memory reliability, can be improved using additional read or/and programming steps or ECC algorithms. These methods increase operation time and chip manufacturing cost but are essential when the reliability of the ReRAM device is low.

ReRAM read current is directly related to the power aspect. In short, using a high-resistance ReRAM cell is more advantageous in terms of power than using a low-resistance cell; however, problems such as longer read time, the need for a sophisticated sense amplifier, and an increase in sensing error may occur. This power aspect also relates to how many memory cells are used for one challenge-response generation. Therefore, feasible PUFs can be designed and implemented by considering everything from the material aspect of the memory device itself to an appropriate sensing circuit design and response generation scheme.

One of the characteristics of ReRAM memory that has not yet been fully investigated is the multistate feature of ReRAM cells. Several previous works have shown that multi-states can be used for randomness sources of PUF. Unlike conventional memory, if multiple states of the memory cells are properly handled, they will be utilized for efficient system development in various fields. The reconfigurable feature of ReRAM PUF is an efficient way to increase the security level without additional hardware. Therefore, such a feature needs to be reflected as an important factor when judging the performance of the future work of ReRAM-based PUF.

## 6 Conclusion

Security in a general context is a topic of a long history. In the modern world, the importance has become more critical; however, despite the importance, hardware security is difficult to uphold in practice. This is likely because it must be guaranteed at the lowest possible cost and simultaneously provide the highest possible level of security. PUF is considered to address these security concerns. PUFs typically utilize variations that are typically non-ideal in CMOS as their primary source. From a component point of view, strong PUFs that take advantage of the inevitable variation in CMOS circuits and weak PUFs using mainstream memory technologies have been actively studied. As one of the emerging NVMs, ReRAM shows excellent potential to be used as a randomness source of PUFs. There are several key points where ReRAM with the memory array structure is considered for building PUF with increased CRPs. Structural advantages of ReRAM include ultra-high density and easy CMOS compatibility. In addition to these structural advantages, variability, which can be the most important in PUF, can be found not only in the existing device-to-device but also in one device (cycle-to-cycle, multistate, etc.). In short, ReRAM shows full variability in a very compact structure. The manuscript reviews various ReRAM-based PUF implementations; the main review points include the source of the randomness and how to provide CRP of each implementation. For a detailed discussion on the feasibility, each implementation's performance metric measurement results are considered. More efforts in research should aim to build methods to achieve reliable, lower power consumption, cost- and area-efficient hardware security system. In particular, memory stability and ReRAM's multistate could serve as critical points to elevate ReRAM-based PUFs to a higher level.

## Author contributions

JK reviewed and analyzed other works and wrote the manuscript.

## Conflict of interest

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

## Publisher's note



## References

Adam, G., Nili, H., Kim, J., Hoskins, B., Kavehei, O., and Strukov, D. (2017). "Utilizing IV non-linearity and analog state variations in ReRAM-based security primitives," in Proceeding of the 47th European Solid-State Device Research Conference (ESSDERC), Leuven, Belgium, September 2017 (IEEE), 74–77.

Ambrogio, S., Balatti, S., Cubeta, A., Calderoni, A., Ramaswamy, N., and Ielmini, D. (2014). Statistical fluctuations in $HfO_x$ resistive-switching memory: Part I–Set/Reset variability. *IEEE Trans. Electron Devices* 61, 2912–2919. doi:10.1109/ted.2014.2330200

Anderson, R. (2001). *Security engineering: A guide to building dependable distributed systems*. John Wiley & Sons.

Auguste, K. (1883). La cryptographie militaire. *J. des Sci. Militaires* IX, 5–38.

Bassham, L. E., Rukhin, A. L., Soto, J., Nechvatal, J. R., Smid, M. E., Barker, E. B., et al. (2010). *SP 800-22 rev. 1a. A statistical test suite for random and pseudorandom number generators for cryptographic applications*. Tech. rep. National Institute of Standards & Technology.

Beckmann, K., Manem, H., and Cady, N. C. (2017). Performance enhancement of a time-delay PUF design by utilizing integrated nanoscale ReRAM devices. *IEEE Trans. Emerg. Top. Comput.* 5, 304–316. doi:10.1109/tetc.2016.2575448

Beckmann, N., and Potkonjak, M. (2009). "Hardware-based public-key cryptography with public physically unclonable functions," in *Information hiding*, 206–220.

Beyerer, J., Jasperneite, J., and Sauer, O. (2015). Industrie 4.0. *A. T. - Autom.* 63, 751–752. doi:10.1515/auto-2015-0068

Cambou, B., and Afghah, F. (2016). "Physically unclonable functions with multi-states and machine learning," in Proceedings of the 14th International Workshop on Cryptographic Architectures Embedded in Logic Devices (CryptArchi), France, June 2016, 1.

Cambou, B., and Orlowski, M. (2016). "PUF designed with resistive RAM and ternary states," in Proceedings of the 11th Annual Cyber and Information Security Research Conference, April 2016, 1–8.

Chatterjee, U., Chakraborty, R. S., Mathew, J., and Pradhan, D. K. (2016). "Memristor based arbiter PUF: Cryptanalysis threat and its mitigation," in Proceedings of the 29th International Conference on VLSI Design and 15th International Conference on Embedded Systems (VLSID), Kolkata, India, January 2016 (IEEE), 535–540.

Che, W., Plusquellic, J., and Bhunia, S. (2014). "A non-volatile memory based physically unclonable function without helper data," in Proceedings of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, CA, USA, November 2014 (IEEE), 148–153.

Chen, A., and Lin, M. R. (2011). "Variability of resistive switching memories and its impact on crossbar array performance," in Proceedings of the IEEE International Reliability Physics Symposium (IRPS), Monterey, CA, USA, April 2011 (IEEE)–4. MY.7.1.

Chen, A. (2015a). Reconfigurable physical unclonable function based on probabilistic switching of RRAM. *Electron. Lett.* 51, 615–617. doi:10.1049/el.2014.4375

Chen, A. (2015b). Utilizing the variability of resistive random access memory to implement reconfigurable physical unclonable functions. *IEEE Electron Device Lett.* 36, 138–140. doi:10.1109/led.2014.2385870

Chen, A. (2015c). "Comprehensive assessment of RRAM-based PUF for hardware security applications," in Proceedings of the IEEE International Electron Devices Meeting (IEDM), Washington, DC, USA, December 2015 (IEEE), 10.7.1–4.

Chen, P.-Y., Fang, R., Liu, R., Chakrabarti, C., Cao, Y., and Yu, S. (2015). "Exploiting resistive cross-point array for compact design of physical unclonable function," in Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust–HOST, Washington, DC, USA, May 2015 (IEEE), 26–31.

Chen, T. M., and Abu-Nimeh, S. (2011). Lessons from Stuxnet. *Computer* 44, 91–93. doi:10.1109/mc.2011.115

Gaba, S. (2014). *Resistive-RAM for data storage applications*. Phd dissertation. University of Michigan.

Gao, Y., Ranasinghe, D. C., Al-Sarawi, S. F., Kavehei, O., and Abbott, D. (2015). Memristive crypto primitive for building highly secure physical unclonable functions. *Sci. Rep.* 5, 12785. doi:10.1038/srep12785

Gao, L., Chen, P.-Y., Liu, R., and Yu, S. (2016). Physical unclonable function exploiting sneak paths in resistive cross-point array. *IEEE Trans. Electron Devices* 63, 3109–3115. doi:10.1109/ted.2016.2578720

Gassend, B., Clarke, D., Van Dijk, M., and Devadas, S. (2002a). "Controlled physical random functions," in Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC'02), Las Vegas, NV, USA, December 2002 (IEEE), 149–160.

Gassend, B., Clarke, D., Van Dijk, M., and Devadas, S. (2002b). "Silicon physical random functions," in Proceedings of the 9th ACM Conference on Computer and Communications Security, November 2002 (IEEE), 148–160.

Gassend, B., Lim, D., Clarke, D., Van Dijk, M., and Devadas, S. (2004). Identification and authentication of integrated circuits. *Concurr. Comput. Pract. Exper.* 16, 1077–1098. doi:10.1002/cpe.805

Gibbons, J., and Beadle, W. (1964). Switching properties of thin NiO films. *Solid-State Electron.* 7, 785–790. doi:10.1016/0038-1101(64)90131-5

Govindaraj, R., and Ghosh, S. (2016). "A strong arbiter PUF using resistive RAM within 1T-1R memory architecture," in Proceedings of the IEEE 34th International Conference on Computer Design (ICCD), Scottsdale, AZ, USA, October 2016 (IEEE), 141–148.

Guajardo, J., Kumar, S. S., Schrijen, G.-J., and Tuyls, P. (2007). "FPGA intrinsic PUFs and their use for IP protection," in *International workshop on cryptographic hardware and embedded systems–CHES*, 63–80.

Hori, Y., Yoshida, T., Katashita, T., and Satoh, A. (2010). "Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs," in Proceedings of the IEEE International Conference on Reconfigurable Computing and FPGAs (ReConFig), Cancun, Mexico, December 2010 (IEEE), 298–303.

Jeong, D. S., Thomas, R., Katiyar, R., Scott, J., Kohlstedt, H., Petraru, A., et al. (2012). Emerging memories: Resistive switching mechanisms and current status. *Rep. Prog. Phys.* 75, 076502. doi:10.1088/0034-4885/75/7/076502

Jiang, D., and Chong, C. N. (2008). "Anti-counterfeiting using phosphor PUF," in Proceedings of the 2nd International Conference on Anti-counterfeiting, Security and Identification (ASID), Guiyang, China, August 2008 (IEEE), 59–62.

Junker, H. (2015). IT-Sicherheit für Industrie 4.0 und IoT. *Datenschutz Datensich.* 39, 647–651. doi:10.1007/s11623-015-0491-8

Kavehei, O., Hosung, C., Ranasinghe, D., and Skafidas, S. (2013). mrPUF: A memristive device based physical unclonable function. *arXiv preprints 1302.2191*

Kim, J. (2019). Nano-intrinsic security primitives for Internet of Everything. *Phd dissertation*. RMIT University.

Kim, J., Ahmed, T., Nili, H., Yang, J., Jeong, D. S., Beckett, P., et al. (2018a). A physical unclonable function with redox-based nanoionic resistive memory. *IEEE Trans. Inf. Forensic. Secur.* 13, 437–448. doi:10.1109/tifs.2017.2756562

Kim, J., Nili, H., Adam, G., Truong, N., Strukov, D., and Kavehei, O. (2018b). "Predictive analysis of 3D ReRAM-based PUF for securing the Internet of Things," in Proceedings of the IEEE Region Ten Symposium (Tensymp), Sydney, NSW, Australia, July 2018 (IEEE), 91–94.

Koeberl, P., Kocabaş, Ü., and Sadeghi, A.-R. (2013). "Memristor PUFs: A new generation of memory-based physically unclonable functions," in Proceedings of the Conference on Design, Automation and Test in Europe, Grenoble, France, March 2013 (IEEE), 428–431.

Kumar, S. S., Guajardo, J., Maes, R., Schrijen, G.-J., and Tuyls, P. (2008). "The butterfly PUF protecting IP on every FPGA," in Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust–HOST, Anaheim, CA, USA, June 2008 (IEEE), 67–70.

Kursawe, K., Sadeghi, A.-R., Schellekens, D., Skoric, B., and Tuyls, P. (2009). "Reconfigurable physical unclonable functions-enabling technology for tamper-resistant storage," in Proceedings of the IEEE International Workshop on Hardware-Oriented Security and Trust, San Francisco, CA, USA, July 2009 (IEEE), 22–29.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Secur. Priv. Mag.* 9, 49–51. doi:10.1109/msp.2011.67

Lee, J. W., Lim, D., Gassend, B., Suh, G. E., Van Dijk, M., and Devadas, S. (2004). "A technique to build a secret key in integrated circuits for identification and authentication applications," in Proceedings of the IEEE Symposium on VLSI Circuits. Digest of Technical Papers, Honolulu, HI, USA, June 2004 (IEEE), 176–179.

Lee, G. S., Kim, G.-H., Kwak, K., Jeong, D. S., and Ju, H. (2019). Enhanced reconfigurable physical unclonable function based on stochastic nature of multilevel cell RRAM. *IEEE Trans. Electron Devices* 66, 1717–1721. doi:10.1109/ted.2019.2898455

Lim, D. (2004). Extracting secret Keys from integrated circuits. *Phd dissertation*. Massachusetts Institute of Technology.

Lim, D., Lee, J. W., Gassend, B., Suh, G. E., Van Dijk, M., and Devadas, S. (2005). Extracting secret keys from integrated circuits. *IEEE Trans. VLSI. Syst.* 13, 1200–1205. doi:10.1109/tvlsi.2005.859470

Lin, B., Pang, Y., Gao, B., Tang, J., Wu, D., Chang, T.-W., et al. (2021). A highly reliable rram physically unclonable function utilizing post-process randomness source. *IEEE J. Solid-State Circuits* 56, 1641–1650. doi:10.1109/jssc.2021.3050295

Linn, E., Rosezin, R., Kügeler, C., and Waser, R. (2010). Complementary resistive switches for passive nanocrossbar memories. *Nat. Mat.* 9, 403–406. doi:10.1038/nmat2748

Liu, R., Wu, H., Pang, Y., Qian, H., and Yu, S. (2015). Experimental characterization of physical unclonable function based on 1 kb resistive random access memory arrays. *IEEE Electron Device Lett.* 36, 1380–1383. doi:10.1109/led.2015.2496257

Liu, R., Wu, H., Pang, Y., Qian, H., and Yu, S. (2016). "A highly reliable and tamper-resistant RRAM PUF: Design and experimental validation," in Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust–HOST, McLean, VA, USA, May 2016 (IEEE), 13–18.

Liu, R., Chen, P.-Y., and Yu, S. (2017). "Design and optimization of a strong PUF exploiting sneak paths in resistive cross-point array," in Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, MD, USA, May 2017 (IEEE), 1–4.

Liu, R., Chen, P.-Y., Peng, X., and Yu, S. (2018). X-point PUF: Exploiting sneak paths for a strong physical unclonable function design. *IEEE Trans. Circuits Syst. I.* 65, 3459–3468. doi:10.1109/tcsi.2018.2811643

Maes, R. (2012). *Physically unclonable functions: Constructions, properties and applications*. Phd dissertation. University of KU Leuven.

Maes, R., and Verbauwhede, I. (2010a). "A discussion on the properties of physically unclonable functions," in *TRUST 2010 workshop* (Berlin, 1–11.

Maes, R., and Verbauwhede, I. (2010b). "Physically unclonable functions: A study on the state of the art and future research directions," in *Information security and cryptography*, 3–37. doi:10.1007/978-3-642-14452-3_1

Maiti, A., Casarona, J., McHale, L., and Schaumont, P. (2010). Gene network analysis of oxidative stress-mediated drug sensitivity in resistant ovarian carcinoma cells. *Pharmacogenomics J.* 10, 94–104. doi:10.1038/tpj.2009.49

Maiti, A., and Schaumont, P. (2009). "Improving the quality of a physical unclonable function using configurable ring oscillators," in Proceeding of the International Conference on Field Programmable Logic and Applications, Prague, Czech Republic, September 2009 (IEEE), 703–707.

Maiti, A., and Schaumont, P. (2011). Improved ring oscillator PUF: An FPGA-friendly secure primitive. *J. Cryptol.* 24, 375–397. doi:10.1007/s00145-010-9088-4

Majzoobi, M., Koushanfar, F., and Potkonjak, M. (2008). "Testing techniques for hardware security," in Proceeding of the IEEE International Test Conference (ITC), Santa Clara, CA, USA, October 2008 (IEEE), 1–10.

Majzoobi, M., Koushanfar, F., and Potkonjak, M. (2009). Techniques for design and implementation of secure reconfigurable PUFs. *ACM Trans. Reconfigurable Technol. Syst.* 2 (5), 1–33. doi:10.1145/1502781.1502786

Mathew, J., Chakraborty, R. S., Sahoo, D. P., Yang, Y., and Pradhan, D. K. (2015). A novel memristor based physically unclonable function. *Integration, VLSI J.* 51, 37–45. doi:10.1016/j.vlsi.2015.05.005

Mazady, A., Rahman, M. T., Forte, D., and Anwar, M. (2015). Memristor PUF—A security primitive: Theory and experiment. *IEEE J. Emerg. Sel. Top. Circuits Syst.* 5, 222–229. doi:10.1109/jetcas.2015.2435532

Nili, H., Adam, G. C., Hoskins, B., Prezioso, M., Kim, J., Mahmoodi, M. R., et al. (2018). Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors. *Nat. Electron.* 1, 197–202. doi:10.1038/s41928-018-0039-7

Paar, C., and Pelzl, J. (2009). *Understanding cryptography: A textbook for students and practitioners*. Springer Science & Business Media. chap. 1. 1–28.

Pang, Y., Wu, H., Gao, B., Deng, N., Wu, D., Liu, R., et al. (2017a). Optimization of RRAM-based physical unclonable function with a novel differential read-out method. *IEEE Electron Device Lett.* 38, 168–171. doi:10.1109/led.2016.2647230

Pang, Y., Wu, H., Gao, B., Liu, R., Wang, S., Yu, S., et al. (2017b). "Design and optimization of strong physical unclonable function (PUF) based on RRAM array," in Proceeding of the International Symposium on VLSI Technology, Systems and Application (VLSI-TSA), Hsinchu, Taiwan, April 2017 (IEEE), 1–2.

Pang, Y., Gao, B., Wu, D., Yi, S., Liu, Q., Chen, W.-H., et al. (2019). "A reconfigurable rram physically unclonable function utilizing post-process randomness source with$< 6 \times 10^{-6}$ native bit error rate," in Proceeding of the IEEE International Solid-State Circuits Conference (ISSCC), San Francisco, CA, USA, February 2019 (IEEE), 402–404.

Pappu, R., Recht, B., Taylor, J., and Gershenfeld, N. (2002). Physical one-way functions. *Science* 297, 2026–2030. doi:10.1126/science.1074376

Pappu, R. S. (2001). *Physical one-way functions*. Phd dissertation. Massachusetts Institute of Technology.

Posch, R. (1998). Protecting devices by active coating. *J. Univers. Comput. Sci.* 4, 652–668.

Rajendran, J., Karri, R., Wendt, J. B., Potkonjak, M., McDonald, N. R., Rose, G. S., et al. (2012a). Nanoelectronic solutions for hardware security. *IACR Cryptol. ePrint Arch.* 575, 1–12.

Rajendran, J., Rose, G. S., Karri, R., and Potkonjak, M. (2012b). "Nano-PPUF: A memristor-based security primitive," in Proceeding of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Amherst, MA, USA, August 2012 (IEEE), 84–87.

Ravi, S., Raghunathan, A., Kocher, P., and Hattangady, S. (2004). Security in embedded systems: Design challenges. *ACM Trans. Embed. Comput. Syst.* 3, 461–491. doi:10.1145/1015047.1015049

Rose, G. S., McDonald, N., Yan, L.-K., and Wysocki, B. (2013a). "A write-time based memristive PUF for hardware security applications," in Proceeding of the IEEE/ACM International Conference on Computer-Aided Design (ICCAD), San Jose, CA, USA, November 2013 (IEEE), 830–833.

Rose, G. S., McDonald, N., Yan, L.-K., Wysocki, B., and Xu, K. (2013b). "Foundations of memristor based PUF architectures," in Proceeding of the IEEE/ACM International Symposium on Nanoscale Architectures (NANOARCH), July 2013 (IEEE), 52–57.

Rose, G. S., Majumder, M. B., and Uddin, M. (2017). "Exploiting memristive crossbar memories as dual-use security primitives in IoT devices," in Proceeding of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Bochum, Germany, July 2017 (IEEE), 615–620.

Rose, G. S., and Meade, C. A. (2015). Performance analysis of a memristive crossbar PUF design. *Proc. Annu. Des. Automation Conf. (DAC)* 75, 1–6.

Rührmair, U. (2009). SIMPL systems: On a public key variant of physical unclonable functions. *IACR Cryptol. ePrint Arch.* 255, 1–16.

Rührmair, U. (2010). "Oblivious transfer based on physical unclonable functions," in *International conference on trust and trustworthy computing*, 430–440.

Rührmair, U., Sehnke, F., Sölter, J., Dror, G., Devadas, S., and Schmidhuber, J. (2010). "Modeling attacks on physical unclonable functions," in Proceedings of the 17th ACM Conference on Computer and Communications Security, October 2010, 237–249.

Rührmair, U., Jaeger, C., Bator, M., Stutzmann, M., Lugli, P., and Csaba, G. (2011). Applications of high-capacity crossbar memories in cryptography. *IEEE Trans. Nanotechnol.* 10, 489–498. doi:10.1109/tnano.2010.2049367

Sheu, S.-S., Chiang, P.-C., Lin, W.-P., Lee, H.-Y., Chen, P.-S., Chen, Y.-S., et al. (2009). "A 5ns fast write multi-level non-volatile 1 K bits RRAM memory with advance write scheme," in Proceedings of the Symposium on VLSI Circuits, Kyoto, Japan, June 2009 (IEEE), 82–83.

Shrivastava, A., Chen, P.-Y., Cao, Y., Yu, S., and Chakrabarti, C. (2016). "Design of a reliable RRAM-based PUF for compact hardware security primitives," in Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS), Montreal, QC, Canada, May 2016 (IEEE), 2326–2329.

Su, Y., Holleman, J., and Otis, B. (2007). "A 1.6 pJ/bit 96% stable chip-ID generating circuit using process variations," in Proceedings of the IEEE International Solid-State Circuits Conference (ISSCC), San Francisco, CA, USA, February 2007 (IEEE), 406–611.

Suh, G. E., and Devadas, S. (2007). "Physical unclonable functions for device authentication and secret key generation," in Proceedings of the 44th Annual Design Automation Conference, San Diego, CA, USA, June 2007 (IEEE), 9–14.

Tuyls, P., and Škorić, B. (2006). "Secret key generation from classical physics: Physical uncloneable functions," in *AmIware hardware technology drivers of ambient intelligence*, 421–447.

Tuyls, P., Škorić, B., Stallinga, S., Akkermans, A. H., and Ophey, W. (2005). "Information-theoretic security analysis of physical uncloneable functions," in *International conference on financial cryptography and data security*, 141–155.

Uddin, M., Majumder, M. B., Rose, G. S., Beckmann, K., Manem, H., Alamgir, Z., et al. (2016). "Techniques for improved reliability in memristive crossbar PUF circuits," in Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI), Pittsburgh, PA, USA, July 2016 (IEEE), 212–217.

Uddin, M., Majumder, M., Beckmann, K., Manem, H., Alamgir, Z., Cady, N. C., et al. (2017a). Design considerations for memristive crossbar physical unclonable functions. *ACM J. Emerg. Technol. Comput. Syst.* 14 (2), 1–23. doi:10.1145/3094414

Uddin, M., Majumder, M., and Rose, G. S. (2017b). Robustness analysis of a memristive crossbar PUF against modeling attacks. *IEEE Trans. Nanotechnol.* 16, 396–405. doi:10.1109/tnano.2017.2677882

Uryasev, S. (2000). "Introduction to the theory of probabilistic functions and percentiles (value-at-risk)," in *Probabilistic constrained optimization*, 1–25.

van der Leest, V., Schrijen, G.-J., Handschuh, H., and Tuyls, P. (2010). "Hardware intrinsic security from D flip-flops," in Proceedings of the 5th ACM Workshop on Scalable Trusted Computing, Chicago, Illinois, USA, October 2010, 53–62.

van Dijk, M., and Rührmair, U. (2012). Physical unclonable functions in cryptographic protocols: Security proofs and impossibility results. *IACR Cryptol. ePrint Arch.* 228, 1–36.

Waser, R., Ielmini, D., Akinaga, H., Shima, H., Wong, H.-S. P., Yang, J. J., et al. (2016). "Introduction to nanoionic elements for information technology," in *Resistive switching: From fundamentals of nanoionic redox processes to memristive device applications* (Wiley Online Library), 1–30.

Wendt, J. B., and Potkonjak, M. (2011). "Nanotechnology-based trusted remote sensing," in Proceedings of the IEEE Sensors, Limerick, Ireland, October 2011 (IEEE), 1213–1216.

Wendt, J. B., and Potkonjak, M. (2013). "The bidirectional polyomino partitioned PPUF as a hardware security primitive," in Proceedings of the IEEE Global Conference on Signal and Information Processing (GlobalSIP), Austin, TX, USA, December 2013 (IEEE), 257–260.

Yin, C.-E. D., and Qu, G. (2010). "Lisa: Maximizing RO PUF's secret extraction," in Proceedings of the IEEE International Symposium on Hardware-Oriented Security and Trust–HOST, Anaheim, CA, USA, June 2010 (IEEE), 100–105.

Yin, C.-E., Qu, G., and Zhou, Q. (2013). "Design and implementation of a group-based RO PUF," in Proceedings of the Conference on Design, Automation and Test in Europe, Grenoble, France, March 2013 (IEEE), 416–421.

Yu, S. (2016). Resistive random access memory (RRAM). *Synthesis Lect. Emerg. Eng. Technol.* 2, 1–79. doi:10.2200/s00681ed1v01y201510eet006

Zhang, L., Fong, X., Chang, C.-H., Kong, Z. H., and Roy, K. (2014). "Feasibility study of emerging non-volatile memory based physical unclonable functions," in Proceedings of the IEEE 6th International Memory Workshop (IMW), Taipei, Taiwan, May 2014 (IEEE), 1–4.

Zhang, L., Fong, X., Chang, C.-H., Kong, Z. H., and Roy, K. (2015). Optimizating emerging nonvolatile memories for dual-mode applications: Data storage and key generator. *IEEE Trans. Comput. -Aided. Des. Integr. Circuits Syst.* 34, 1176–1187. doi:10.1109/tcad.2015.2427251