IEEE Open Journal of Nanotechnology

Received 18 November 2020; revised 8 January 2021; accepted 3 February 2021. Date of publication 9 February 2021; date of current version 8 March 2021. The review of this article was arranged by Editor K. Endo.

Digital Object Identifier 10.1109/OJNANO.2021.3058169

A Physical Unclonable Function Using a Configurable Tristate Hybrid Scheme With Non-Volatile Memory

JIANG LI [1], YIJUN CUI [1], CHONGYAN GU [2] (Member, IEEE), CHENGHUA WANG [1], WEIQIANG LIU [1] (Senior Member, IEEE), AND FABRIZIO LOMBARDI [3] (Fellow, IEEE)

[1]College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China
[2]Centre for Secure Information Technologies, Queen's University Belfast, Belfast BT3 9DT, U.K.
[3]Department of Electrical and Computer Engineering, Northeastern University, Boston, MA 40125 USA

CORRESPONDING AUTHOR: WEIQIANG LIU (e-mail: liuweiqiang@nuaa.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grants 62022041 and 61771239, and in part by the Engineering and Physical Sciences Research Council (EPSRC) under Grant EP/N508664/-CSIT2. *(Jiang Li and Yijun Cui contributed equally to this work.)*

ABSTRACT The physical unclonable function (PUF) is a promising low-cost hardware security primitive. Recent advances in nanotechnology have provided new opportunities for nanoscale PUF circuits. The resistive random access memory (RRAM) is extensively used in nanoscale circuits due to its low cost, non-volatility and easy integration with CMOS. This paper proposes a novel tristate hybrid PUF (TH-PUF) design based on a one-transistor-one-RRAM (1T1R) cell; this cell can be configured into two weak PUFs and a strong PUF using few control signals. To assess the proposed PUF design, a compact RRAM model at UMC 65 nm technology is employed. Simulation results show that the proposed TH-PUF achieves good uniqueness, reliability as well as a higher gate usability compared with an entire CMOS PUFs. The number of challenge response pairs (CRPs) of the proposed TH-PUF is larger than other RRAM-based PUFs. Moreover, the TH-PUF is more resistant to a modeling machine learning attack than traditional PUF designs.

INDEX TERMS Physical unclonable function, hardware security, resistive random access memory, modeling attack.

I. INTRODUCTION

The IoT and cloud are becoming ubiquitous in our daily life, in which millions of mobile devices are digitally connected and exchanging electronically large volume of information. Therefore, adversaries have many opportunities to access the user system and intercept private information due to the unsecure and identity information leakages. Traditional software encryption technologies are usually complex and must be capable to store secret keys in non-volatile memories (NVMs); hence, they are not suitable for resource-constrained IoT devices. Moreover, they have been shown to be vulnerable to side channel attacks (SCAs) [1]. As a lightweight hardware security primitive, the physical unclonable function (PUF) has been used for authentication and identification [2]. A PUF can extract the random manufacturing process variations of an integrated circuit (IC) as identifier [3]. In principle, any two chips cannot generate the same response with the same input.

Previous PUF designs have been proposed based on CMOS circuits, such as the tristate inverter based PUF and the flip-flop based PUF [4], [5]. However, they cannot meet the needs of IoT devices due to the limited density and scaling trend of CMOS technology; therefore, CMOS-based PUF designs encounter the same constraints, such as high power dissipation and large area. It is well known that most PUF designs are vulnerable to machine learning (ML) attacks [6]; therefore, new anti-attack PUF designs are needed. When the feature size is reduced to nanoscales, the design and manufacturing of ICs face even greater challenges. The unpredictability of the thickness and the cross-sectional area likely leads to process errors; however, more process errors and noise sources can improve the uniqueness and randomness of PUF responses.

In the last decade, new types of nanodevices have emerged, such as phase change material (PCM) [7], spin transfer torque magnetic tunnel junction (STTMTJ) [8] and resistive random access memory (RRAM) [9]. RRAM is a nonlinear non-volatile resistive memory, that changes its resistance by the charge flowing through it. RRAM has a lower power dissipation, higher density, and is compatible with CMOS. Hence, RRAMs have been used in many PUF designs [10]–[12] Most RRAM-based PUFs utilize simple RRAM cells and generate a single response bit using one or more cells [13], [14]. Due to the limited capacity of RRAM cells, emerging NVMs cannot provide a sufficient number of CRPs and therefore they cannot be used as strong PUFs. Using a small number of CRPs, these PUF designs have a lower utilization rate of the RRAMs. To address this problem, our contributions in this paper are given as follows.

- A reconfigurable TH-PUF with a so-called transformed tristate hybrid schame is proposed in this paper. The proposed TH-PUF is based on a one-transistor-one-RRAM (1T1R) cell; it can be configured to three operational modes, including two weak PUFs and a strong PUF. Depending on the requirements, the different modes can be selected.
- The proposed TH-PUF is evaluated using a compact RRAM model at the UMC 65 nm technology. Simulation results show that all three modes of the proposed TH-PUF have a good uniqueness, reliability as well as a higher density compared with schemes utilizing only CMOS PUFs. The number of CRPs of the TH-PUF is larger than the most RRAM-based PUFs.
- The results for modeling attacks of the TH-PUF are also provided and it is shown that the proposed TH-PUF is more resistant to machine learning attacks than other conventional PUFs.

The proposed PUF can be used in the PUF-based authentication protocol, allowing for extremely lightweight implementations [15]. The authentication server stores and manages CRPs for each device in the database. A random challenge is returned to the device from the server, when the request of the device is received. The server matches the PUF response generated by the device with the CRP stored in the database to authenticate the device. To prevent a reuse attack, the CRP is deleted once it is used; therefore, the number of CRPs is an important parameter in this process. The proposed PUF can provide a large number of CRPs to the authentication system.

This paper is organized as follows. In Section II, the 1T1R cell is introduced. Section III presents the design and configuration strategies of the proposed TH-PUF design. In Section IV, the simulation results are given to shown that the proposed PUF design has good performance and security. Then, conclusion is provided in Section V.

II. BACKGROUND

The RRAM is a device that operates based on the relationship between charge and magnetic flux. Strukov *et al.* [16] fabricated the first RRAM device at HP Lab showing that it can be physically realized. An RRAM has unique circuit characteristics, the relationship between charge and magnetic flux, which can change the resistance via the voltage applied to the device. The other three basic circuit components, resistor, capacitor and inductor, cannot realize it. The relationship between RRAM and other basic components is shown in Fig. 1. The resistance of the RRAM can be changed by a write pulse voltage; this change can be kept when the power is turned off. Based on this unique characteristic, RRAM can be utilized as a non-volatile memory [17].

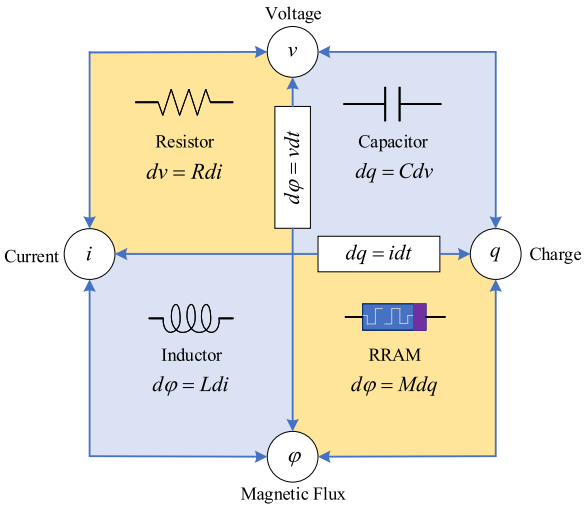


FIGURE 1. Relationship of RRAM with other basic circuit components.

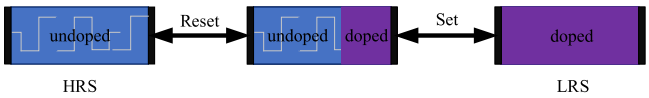


FIGURE 2. The operational principle of the RRAM (The purple area is the doped region while the blue area is the undoped region).

The RRAM can change its resistance between a high resistance state (HRS) and a low resistance state (LRS) by controlling the direction of the current flow, as shown in Fig. 2. The right terminal of the RRAM is the doped region while the left terminal is the undoped region; the conductivity of the undoped region is weaker than the doped region. The resistance of the RRAM increases when a positive pulse flows in RRAM from the undoped region to the doped region (denoted as the RESET operation), due to the diffusion of the undoped region. It is reduced when a negative pulse flows in the RRAM from the doped region to the undoped region, denoted as the SET operation. The RRAM is widely used for in-memory computing [18], neural networks [19], logic design [20] and PUF [21].

The 1T1R cell reduces the hardware overhead and is compatible with a RRAM-based memory array for most mainstream memory applications; many designs have used 1T1R as a basic cell of a PUF, in which the transistor acts as a switch. A 1T1R cell is shown in Fig. 3(a). The word line (WL)

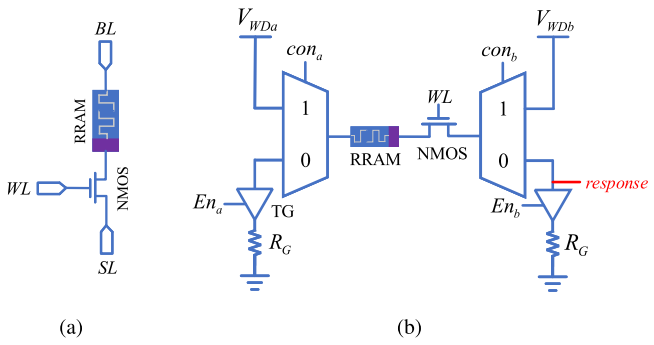


FIGURE 3. 1T1R cell: (a) basic schematic, and (b) one recommended R/W circuit.

is used to control the ON/OFF state. The bit line (*BL*) and the source line (*SL*) are used to provide the selecting pulse. The read/write (R/W) circuit is shown in Fig. 3(b), using two MUXs for control; a NMOS is controlled by the challenge signal, WL. The control signals, con_a and con_b, select the terminal of the RRAM for the pulse to be provided; then, the write pulse V_{WD} is used to change the resistance of the RRAM and configure its state. When the 1T1R cell is deactivated in the PUF, the enable signal (En) can disable it by the transmission gate (TG). If the challenge signal is '0', the resistance of the NMOS is very large, so equivalent to OFF state. In this case, even if a write pulse is applied to the 1T1R cell, the resistance of the RRAM remains unchanged. If the challenge signal is '1', the cell remains in the ON state. In this case, the control signals of the MUXs have multiple configurations to read or write the RRAM.

The Verilog-A compact model of ASU [22] has been used for the RRAM; the I-V curve of the HfO_x-based RRAM and the resistance variation of the 1T1R cell are given in Fig. 4 as simulated by Hspice. A typical DC switching plot without variation under an applied voltage range of -2 V to 2 V is shown in Fig. 4(a). The switching behaviors of the RRAM can then be established; the RRAM can be configured to LRS by a set pulse and written to HRS by a reset pulse. In Fig. 4(b), $V_{SET,on}$ denotes that a +1.5 V set pulse is applied, and $V_{RESET,on}$ denotes that a -1.5 V reset pulse is applied. The resistance of the RRAM changes differently at various temperatures, and therefore, it may lead to poor reliability. However, the LRS of the RRAM is stable, so only varying by a very small amount with a change in temperature; hence, it can be utilized for the PUF design to enhance performance. The RRAM can be RESET to a stable HRS in a short time by applying a reset voltage of 2.5 V with a pulse width of less than 1 ns; so regardless of the pulse width on the resistance of RRAM, a pulse of 2.5 V is used in the performed simulation.

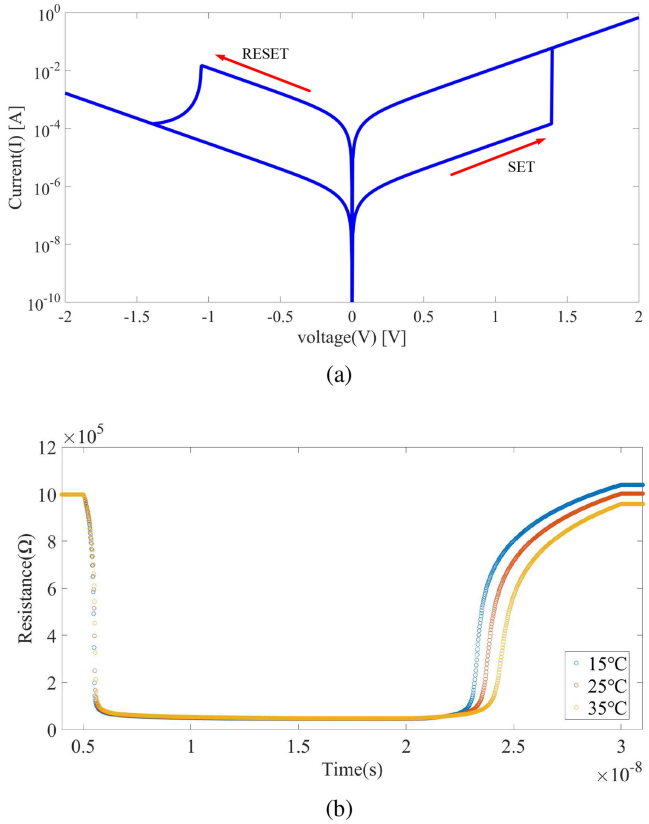


FIGURE 4. (a) The I-V curve of the used HfO_x-based RRAM and (b) the resistance variation of the RRAM during the Set and Reset with a supply voltage of 1.5 V.

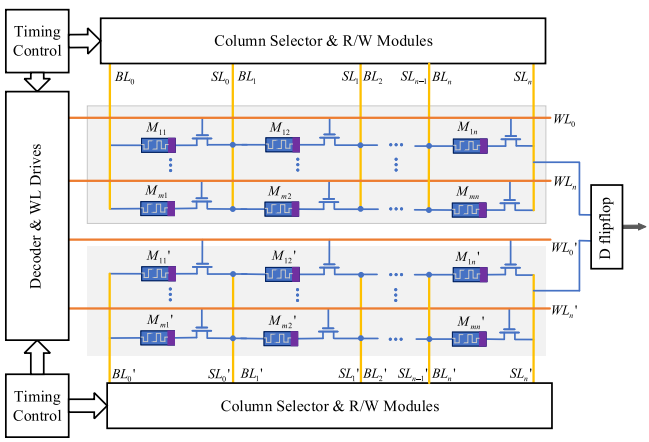


FIGURE 5. Schematic diagram of the proposed TH-PUF design with R/W modules.

III. PROPOSED PUF DESIGN

A tristate hybrid PUF design (TH-PUF) based on a 1T1R cell is proposed; the proposed design can be configured into three different PUFs. A schematic diagram of the TH-PUF design with a peripheral decoder and R/W modules is illustrated in Fig. 5. It consists of two symmetric 1T1R arrays connecting multiple 1T1R cells in series/parallel. The *BL*s are connected to the data ports of the 1T1R cell; for a 3-terminal transistor, WL is connected to all the gate terminals of the transistors along the same row, while *SL* is connected to all

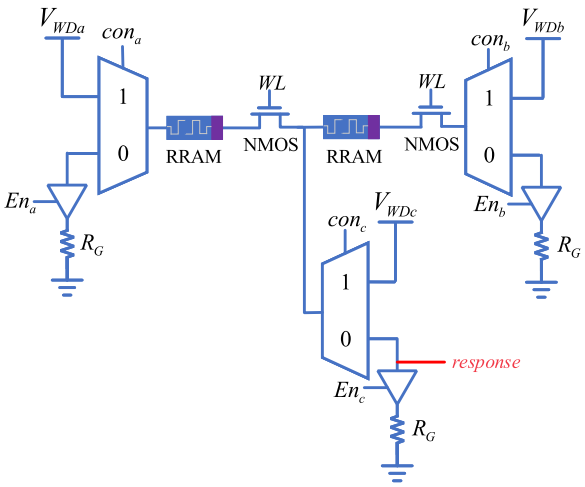


FIGURE 6. 1-bit filament growth-based PUF with a R/W circuit.

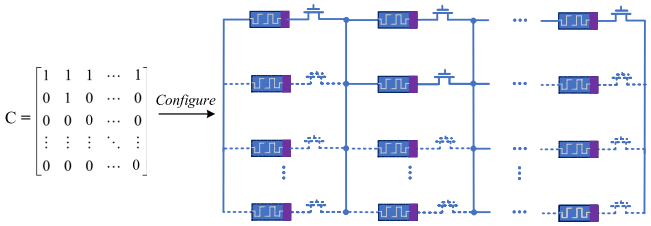


FIGURE 7. Proposed configurable PUF scheme, which needs to turn on at least a 1T1R cell every column.

source terminals of the transistors along the same column. The configuration strategies are analyzed as follows:

A. A 1-BIT MEMRISTIVE MEMORY-BASED PUF CELL

When only one 1T1R cell is enabled, the proposed TH-PUF is similar to a 1-bit memristive memory-based PUF cell [23]. However, the proposed design requires less hardware, as shown in Fig. 3(b). Due to manufacturing, the different width and range (maximum and minimum) of the doped region of the RRAM cause a different write time of the RRAM. Therefore, the width of a pulse required for setting the RRAM from HRS to LRS or resetting the RRAM from LRS to HRS is different. Assume T_w is the transition time for an ideal RRAM from HRS to LRS; the actual transition time $T_{w,actual}$ may be greater or smaller than T_w. This difference is used to generate a random response '1' or '0' and the probability of '1' or '0' should be in theory close to 50%. The operation of the PUF circuit consists of the following two steps:

1) **Reset:** the RRAM is configured to HRS by a reset pulse V_{WDa} using the control signals (con_a = '1', con_b = '0', En_b = '1').

2) **Response Generation:** Differently from Reset, when a set pulse V_{WDb} of width T_w is applied through the control signals (con_a = '0', con_b = '1', En_a = '1'), the resistance of the RRAM can be either LRS or HRS; this process is random and unpredictable. Hence, using the control signals (con_a = '1', con_b = '0', En_b = '1'), we can then utilize the series of the RRAM and a grounding resistor to generate a response by voltage division. If the RRAM is in the HRS, the response is '0', while, if the RRAM is in the LRS, the response is '1'.

B. A 1-BIT FILAMENT GROWTH BASED PUF CELL

When two 1T1R cells are enabled together, the proposed TH-PUF is equivalent to the 1-bit filament growth-based PUF cell [23], as shown in Fig. 6. Due to manufacturing variations, when two RRAMs are connected in series, the ability of a state transition is different. If two RRAMs in series are initialized to LRS, when a reset pulse is applied to the two RRAMs, there is only one RRAM to be in HRS first. If the reset voltage is disabled at this point, the PUF cell has one RRAM in LRS and the other in HRS; the RRAM completing the state transition is random and unpredictable. Moreover, when configured again, there is still the RRAM from the previous time to ensure the transition of the resistance state, so the output of the PUF is stable.

The configuration and working principle of the filament growth-based PUF are like a memristive memory-based PUF. The middle R/W circuit is floated and it configures the two RRAMs to LRS through the two side R/W circuits. One of the two RRAMs is Reset to HRS by applying a reset pulse. The middle R/W circuit and the RRAM are used to generate the response, like the memristive memory-based PUF.

C. RRAM-BASED STRONG PUF CELL

The proposed TH-PUF can be configured as a strong PUF. As for implementing a strong PUF, it is needed to configure at least one RRAM to LRS in each column of the 1T1R array of Fig. 5. The resistance of the LRS of the RRAM hardly changes under temperature variation (as shown in Fig. 4(b)); this enhances the reliability of the TH-PUF. The TH-PUF can be configures as the strong PUF structure [24], as well as, having more CRPs through different configurable methods. The main principle of the proposed PUF design is to select two symmetric 1T1R channels and compare the delay to obtain the final response through an arbiter.

For the TH-PUF structure with $m \times n$ stages, the corresponding challenge signal matrix C and its specific circuit can be simplified as shown in Fig. 7. The '1' represents that the 1T1R cell keeps the LRS mode, while a '0' represents the HRS mode. The middle R/W circuit is only enabled in the configuration phase, as used to configure the resistance state of each RRAM. The RRAM of the channel is configured to a stable LRS or HRS to keep the upper and lower channels identical. In the response generation phase, except for the left and right R/W circuits, all other circuits must be floated by the TGs. When the R/W circuit on the left applies a pulse signal, it is propagated to the D flip-flop arbiter, that consists of four NAND gates and is at a logic output by default, through the 1T1R channel turned on by the NMOSs. As the upper and lower channels are symmetric, the delay difference only

TABLE 1 Parameters of the RRAM

Parameter	Description	Value	Variation
Gap_{on}	Gap distance of LRS	0.12nm	± 15%
Gap_{off}	Gap distance of HRS	1.5nm	± 15%
Gap_d	Variation of gap distance	0.1nm ~ 1.7nm	
R_{on}*	LRS	1.073kΩ	
R_{off}*	HRS	1.621MΩ	
D	Width of RRAM	3nm	

*The resistance of R_{on} and R_{off} vary according to the Gap.

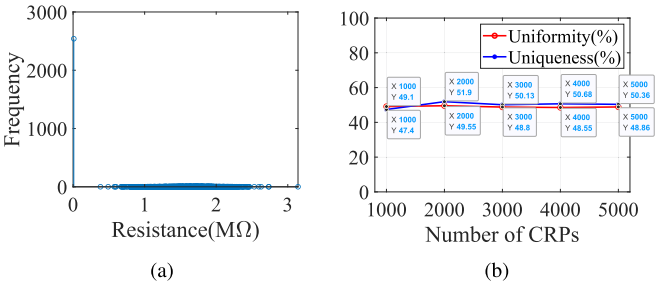


FIGURE 8. 1-bit memristive memory-based PUF: (a) resistance distribution of the RRAM after applying a pulse in over 5000 Monte Carlo simulations; (b) uniformity and uniqueness results by increasing the number of CRPs.

arises from a manufacturing error of the RRAMs. Due to the different LRS or HRS resistances of each RRAM, the delay is also different. Finally, the arbiter generates a random response by assessing the signal that arrives first.

IV. SIMULATIONS AND RESULTS OF WEAK PUFS

To evaluate and compare the proposed TH-PUF, the simulated circuits are built based on the ASU compact RRAM model at UMC 65 nm technology [22]. The parameters of the model are then re-fitted to the experimental data of the IMEC HfOx-based RRAM devices [25]. The primary internal variable used in this model is the gap distance (g), which is defined as the distance between the top electrode and the tip of the conductive filament. Increasing of the gap distance leads to an increase of the resistance of the RRAM. This paper uses Hspice to simulate the three modes of the proposed TH-PUF. The parameters of the RRAM used for simulation are listed in Table 1.

A. 1-BIT MEMRISTIVE MEMORY-BASED PUF

The RRAM is configured to HRS first, then a set pulse is applied. The results of 5000 Monte Carlo simulations for the RRAM resistance are plotted in Fig. 8(a); nearly half RRAMs are moved from HRS to LRS; the lowest HRS is significantly higher than LRS, indicating that the response is stable. The uniformity and uniqueness of this weak PUF are illustrated in Fig. 8(b); they are close to the ideal value of 50%.

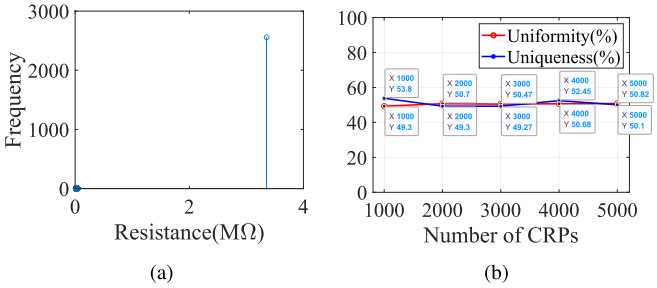


FIGURE 9. 1-bit filament growth-based PUF: (a) resistance distribution of the RRAM after applying a pulse in over 5000 Monte Carlo simulations; (b) uniformity and uniqueness results by increasing the number of CRPs.

TABLE 2 Performance of the Proposed TH-PUF At Different Number of Stages

PUF Size	Uniformity	Uniqueness	Reliability (temperature)	Reliability (voltage)
16-stages	50.62%	50.42%	99.20%	99.66%
32-stages	50.54%	50.30%	98.60%	98.52%
48-stages	50.26%	50.16%	97.62%	97.96%
64-stages	50.12%	50.00%	97.60%	97.42%

B. 1-BIT FILAMENT GROWTH BASED PUF

When the two RRAMs are in series and LRS, a reset pulse is applied to the filament growth-based PUF. 5000 Monte Carlo simulations of the resistance transition of this PUF are executed; the results are plotted in Fig. 9. The filament growth-based PUF is stable and has good uniformity and uniqueness.

V. THE CHARACTERISTIC OF STRONG PUF

After configuring the strong PUF, a pulse is applied. The delay and delay difference distribution of a 16-stage TH-PUF are shown in Fig. 10. The upper delay, the lower delay and the delay difference follow a gaussian distribution. The delay of the 16-stage path is 0.38 ns, and the delay of the 32-stage TH-PUF path is 1 ns. The input and output waveforms of the 16-stage TH-PUF are given in Fig. 11 by taking process variations for the RRAM and CMOS into account. The entire timing takes 20 ns. A 3 V pulse voltage of 10 ns width is provided as input at 5 ns and the complete pulse signal is received at the output after a short delay. There are delay differences between the outputs of the upper and lower paths.

As for the strengths of the TH-PUF, metrics such as performance, hardware efficiency and security analysis are given as follows.

A. PERFORMANCE

Fig. 12 shows the inter-chip and intra-chip HD of a 32-stage TH-PUF with 64 kb array of RRAM. The mean of the inter-chip HD (uniqueness) is 50.26% with $\sigma = 8$. The mean of the intra-chip HD is 1.4% with $\sigma = 6$, so the reliability is 98.6%. The results of uniformity, uniqueness and reliability under variations of temperature and voltage for different number of stages of the TH-PUF are given in Table 2. Uniformity

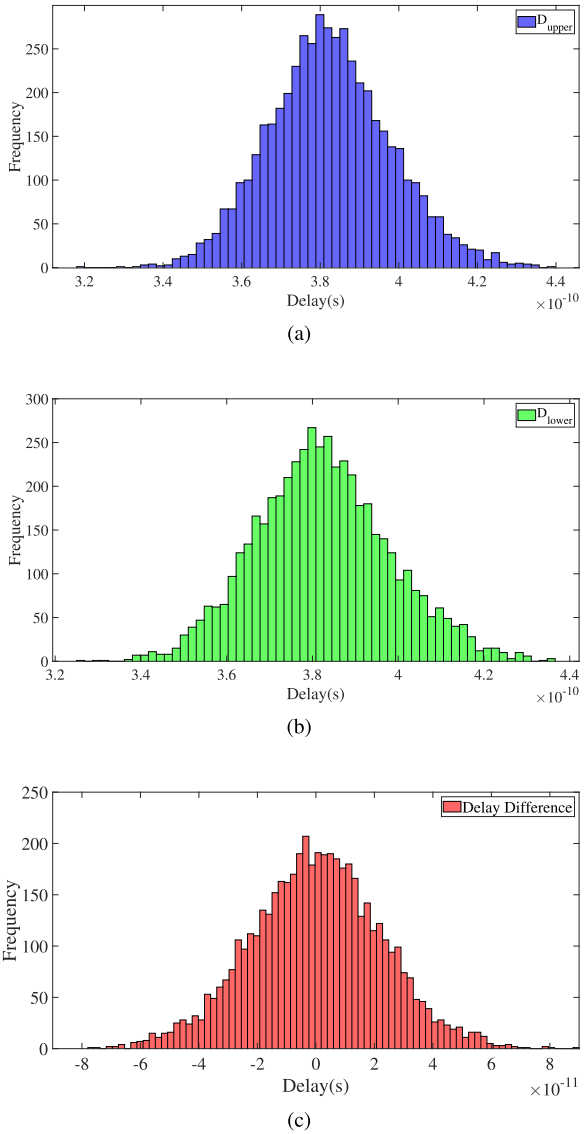


FIGURE 10. Delay and delay difference distributions obtained by 5000 Monte Carlo simulations for a 16-bit TH-PUF: (a) Distribution of the upper path delay; (b) Distribution of the lower path delay; (c) Distribution of the delay difference.

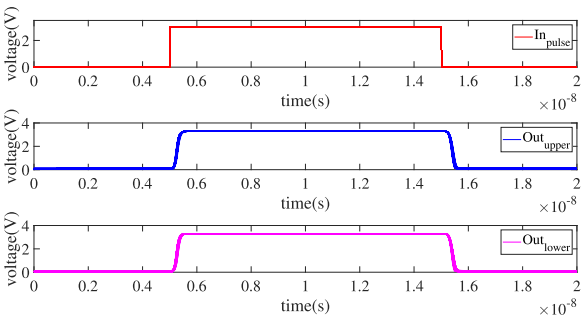


FIGURE 11. 5000 Monte Carlo simulation of the input and output wave of upper and lower 16-stage TH-PUF paths.

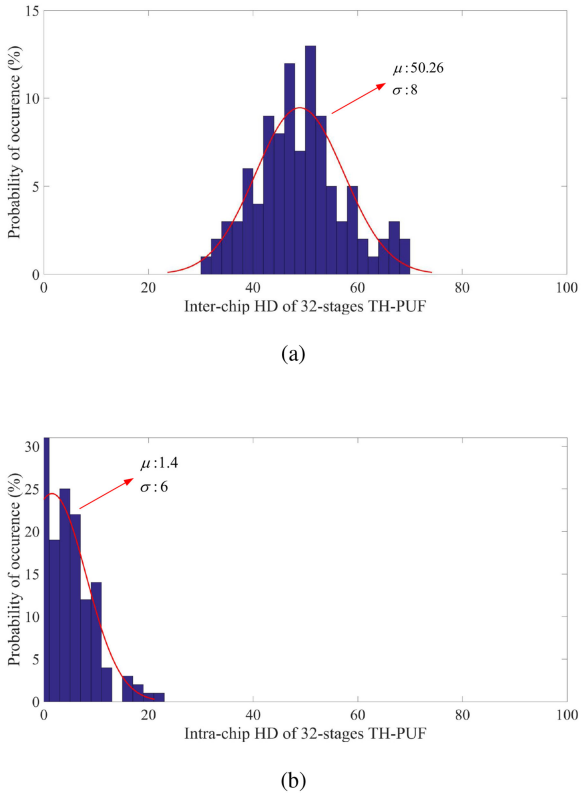


FIGURE 12. 32-stage TH-PUF: (a) inter-chip HD with a mean value of 50.26% (uniqueness); (b) intra-chip HD with a mean value of 1.4% (reliability).

and uniqueness are improved with an increase of number of PUF stages, while the reliability decreases, due to multiple variations. In general, performance of the TH-PUF is close to the ideal value.

Table 3 provides a comparative analysis of the proposed TH-PUF with other RRAM-based PUFs found in the technical literatures. There are three operational modes for the TH-PUF as a flexibility scheme. The uniformity and uniqueness of the TH-PUF are greater than most designs. The reliability of the proposed TH-PUF is 97%; this is a good value compared with other PUF designs because the result is derived with no post-processing or error correction codes. It can be applied to a lightweight authentication protocol using reverse fuzzy extractors that correct the noise in the PUF responses so allowing for implementations on devices [15].

B. HARDWARE EFFICIENCY

As adjacent 1T1R cells share the R/W circuit, then there is 1 MUX and 1 TG for each pair of 1T1R cells. The overhead of the proposed PUF includes $m + 2$ MUXs and 2 DeMuxs, $m + 2$ TGs and 1 D flip-flop arbiter for two symmetrical $n \times m$ RRAM arrays, so requiring less area than [14] and no need for the inverter and current mirror (no detail is provided on the overhead of other designs in Table 3).

TABLE 3 Comparison of 32-Stage TH-PUF With Other PUF Designs

Reference	[13]	[26]	[14]	[27]	[28]	TH-PUF
PUF type	strong	strong	strong	strong	weak	strong
Basic cell	1T1R	1T1R	RRAM	RRAM	2T2R	1T1R
Based state	LRS&HRS	LRS&HRS	HRS	LRS	Set Time	LRS
Modes	two	one	two	one	two	**three**
Uniformity	~ 50%	50-53 %	51.70%	51.00%	NA	50.54%
Uniqueness	~ 50%	51.3 %	52.01%	50.00%	50.4%	50.30%
Reliability(T)	unreliable	99.87 %	NA	98.00%	~ 100%	98.60%
Anti-attack	No	NA	No	NA	NA	**Yes**

The hardware efficiency (HE) is evaluated by the number of elements required to generate a 1-bit response. As currently it is not reported in the technical literature the relevant details on the decoder block or the R/W module in the Table 3, then only the utilization rate of the RRAM is taken into consideration in this paper. The largest number of CRPs that can be generated by the same scale RRAM-based PUFs are as follows:

for a $n \times m$ RRAM array in [13]:

$$N_{CRP} = \frac{m!}{2! \times (m-2)!} \times n^2 \tag{1}$$

for a $n \times m$ RRAM array in [26]:

$$N_{CRP} = 2^n \times 2^m \tag{2}$$

for a $n \times m$ RRAM array in [14]:

$$N_{CRP} = \frac{n!}{2! \times (n-2)!} \times m \tag{3}$$

for a $n \times m$ RRAM array in [27]:

$$N_{CRP} = 16 \times n \times m \tag{4}$$

for a $n \times m$ RRAM array in [28]:

$$N_{CRP} = \frac{n \times m}{2} \tag{5}$$

The proposed TH-PUF can be fully configured with every RRAM in the column, and any number of RRAMs can be selected to generate the response bit. Therefore, the number of CRPs of the proposed TH-PUF may increase exponentially when increasing the number of stages. As for a $n \times m$ stage in a TH-PUF, the number of CRPs is given by:

$$N_{CRP} = \left(n + \frac{n!}{2! \times (n-2)!} + \frac{n!}{3! \times (n-3)!} + \cdots + 1\right)^m \tag{6}$$

The comparison of the number of CRPs for the TH-PUF and other RRAM-based PUFs found in the literature under the same RRAM square array is shown in Fig. 13. The number of CRPs for the proposed TH-PUF is significantly larger than other PUFs under the same scale, showing a more than tenfold increase for the 16-stage PUF.

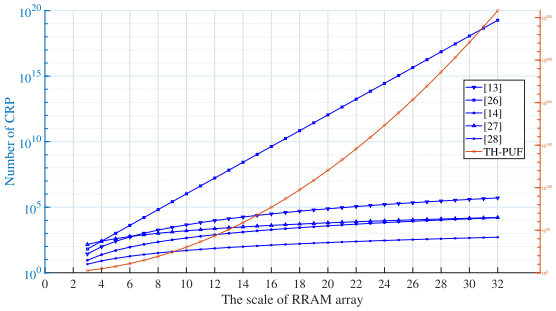


FIGURE 13. Comparison of the number of CRPs of the proposed TH-PUF and other RRAM-based PUFs under the same scale RRAM square array (The number of CRPs of the TH-PUF is on the right axis; for other PUFs it is on the left axis).

C. SECURITY ANALYSIS

To evaluate the security of the proposed TH-PUF, two common machine learning attacks to PUFs are employed, i.e. logistic regression (LR) [29] and the covariance matrix adaptation evolution strategy (CMA-ES) [30]. LR is a classification model often used for dichotomy. LR assumes that the data follows a specific distribution and then it uses maximum likelihood as parameter estimate. The loss function of LR is given as $J(w)$. w is the parameter vector, and x_i and y_i are the data samples.

$$J(w) = -\frac{1}{n}\left(\sum_{i=1}^{n}(y_i log p(x_i) + (1-y_i) log(1-p(x_i))\right) \tag{7}$$

CMA-ES is used to solve the continuous optimization problem. It is a combination of an evolutionary algorithm and probability statistics. It imitates the principle of biological evolution, on the assumption that the results always follow a gaussian distribution with a mean of zero when changes occur in a gene. CMA-ES is the most effective ML attack to non-linear PUF designs.

A prediction rate of 70% represents a successful attack to the PUF. In the simulation, an open source implementation of LR with RProp programmed in Python [31] and the reliable CMA-ES [32] are used. A gaussian noise with $\mu = 0, \sigma = 0.5$ is applied to simulate the variation of the supply voltage and the temperature. The delay equivalent circuit of the TH-PUF is shown in Fig. 14. The RRAM is simplified as a resistor, and the NMOS is modeled by a resistance and capacitance. The delay of the upper path D_{upper} is expressed as :

$$D_{upper} = R_{K_1 1} \times C_{K_1 1} K_1 + (R_{K_1 1} + R_{K_2 2}) \times C_{K_2 2} K_2 + \cdots$$

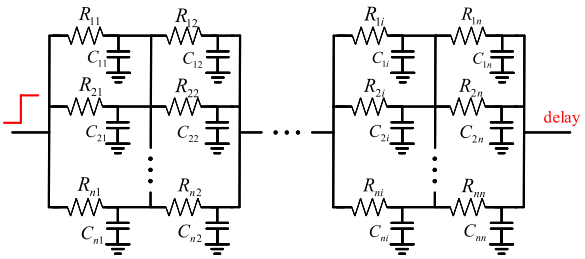


FIGURE 14. Delay model of the proposed TH-PUF (R_{11} denotes the total resistance of the RRAM and the NMOS, and C_{11} denotes the capacitance of the NMOS).

$$+ (R_{K_1 1} + R_{K_2 2} + \cdots + R_{K_i i}) \times C_{K_i i} K_i$$
$$+ (R_{K_1 1} + R_{K_2 2} + \cdots + R_{K_i i} + R_{K_n n}) \times C_{K_n n} K_n \quad (8)$$

where K_i is the challenge of the i-th column; $R_{K_i i}$ and $C_{K_i i}$ represent the resistance and the capacitor of the K_i-th row and i-th column, and D_{lower} can be found in a similar manner. So the delay difference is calculated as:

$$\begin{aligned} \Delta D &= D_{upper} - D_{lower} \\ &= D_{K_1 1} K_1 + D_{K_2 2} K_2 + \cdots + D_{K_i i} K_i + D_{K_n n} K_n \\ &= \vec{w}^T \cdot \vec{K} \end{aligned} \quad (9)$$

where $D_{K_i i} = (R_{K_1 1} + \cdots + R_{K_i i}) \times C_{K_i i} - (R'_{K_1 1} + \cdots + R'_{K_i i}) \times C'_{K_i i}$; $R_{K_i i}$ represents the resistance of the upper path, while $R'_{K_i i}$ represents the resistance of the lower path, with:

$$\vec{w} = \begin{pmatrix} D_{K_1 1} \\ D_{K_2 2} \\ \vdots \\ D_{K_n n} \end{pmatrix} \quad \text{and} \quad \vec{K} = \begin{pmatrix} K_1 \\ K_2 \\ \vdots \\ K_n \end{pmatrix} \quad (10)$$

The response is 1, if the delay difference is greater than 0; otherwise, the response is 0.

Most previous RRAM-based PUF designs of Table 3 did not evaluate performance under ML attacks. Hence, A comparison of the proposed TH-PUF design with other conventional PUF designs are presented. The prediction results of the proposed TH-PUF and the traditional arbiter PUF (APUF) [33], CRO PUF [34], XCRO PUF [35] are given in Fig. 15. Traditional PUF designs and 2 × 16 stage TH-PUF are vulnerable to LR, and the prediction rate reaches to nearly 90% with a training sample of 1000. While, the 4 × 32 stage TH-PUF is more resistant to LR; the prediction rate remains at approximately 55% independently of the number of CRP samples in training. CMA-ES is applicable to an attack to non-liner PUF designs. Although the results are weaker than LR for attacking a PUF when a small number of samples is trained, the prediction rates increase by increasing the training CRPs. The prediction rate of the 4 × 32 stage TH-PUF reaches 70% with 10 000 training CRPs compared with 1000

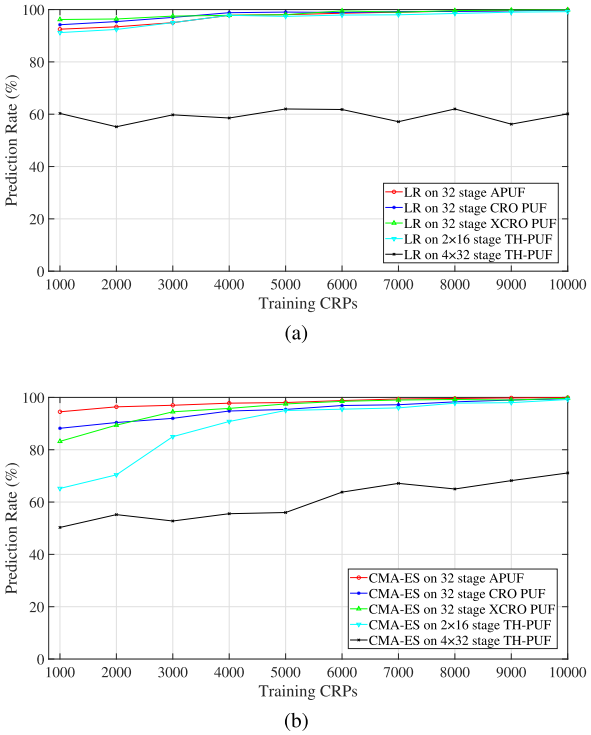


FIGURE 15. Prediction rate of (a) LR; (b) CMA-ES to TH-PUF and other PUF designs.

TABLE 4 Prediction Rate of LR and CMA-ES for Different Bit Stages of TH-PUF

	Number of CRPs	16-bit	32-bit	48-bit	64-bit
LR Accuracy	5000	63.24%	62.96%	60.60%	55.16%
	10000	64.36%	63.06%	62.24%	58.60%
CMA-ES Accuracy	5000	68.52%	65.32%	60.74%	59.64%
	10000	74.52%	68.36%	65.55%	63.34%

CRPs for other PUFs. The proposed TH-PUF mitigates the attack of LR and CMA-ES attacks compared with traditional PUF designs, because the adversary needs more time and resources to collect enough CRPs to achieve higher prediction rates for the proposed PUF. To completely thwart machine learning attacks, there are many other protocol-based approaches, such as deception protocol [36], that can be applied to the proposed TH-PUF.

The prediction rates of different stages of the proposed TH-PUF to LR and CMA-ES are reported in Table 4; an increased complexity of the proposed TH-PUF is beneficial to security, as the 64-bit TH-PUF shows robustness to the attacks. Unfortunately, an improved LR or CMA-ES attack may still be able to learn the TH-PUF with a lower number of CRPs.

VI. CONCLUSION

In the paper, an enhanced reconfigurable PUF design with transformed tristate based on the so-called 1T1R cell has been proposed. The TH-PUF can be configured to three types

of PUF, including two weak PUFs and a strong PUF. The configuration strategies have been analyzed in detail to show that they can significantly improve performance when compared with conventional PUF designs. The Monte Carlo simulation results of the three modes of the proposed TH-PUF have been provided. Simulation results show that all the three modes of the TH-PUF have excellent performance, achieving good uniformity (50.12%), uniqueness (50.00%) and reliability (97.60%). The number of CRPs of the TH-PUF is significantly larger than other RRAM-based PUF designs. Moreover, the simulation results have demonstrated that the proposed TH-PUF mitigates the common machine learning attacks, including LR and CMA-ES attacks.

REFERENCES

[1] A. Moradi, D. Oswald, C. Paar, and P. Swierczynski, "Side-channel attacks on the bitstream encryption mechanism of altera stratix II: Facilitating black-box analysis using software reverse-engineering," in *Proc. ACM/SIGDA Int. Symp. Field Programmable Gate Arrays*, 2013, pp. 91–100.

[2] M. Akgun and M. U. Caglayan, "PUF based scalable private RFID authentication," in *Proc. IEEE Int. Conf. Availability, Rel. Secur.*, 2011, pp. 473–478.

[3] J. Li, H. Gao, Y. Cui, C. Wang, and W. Liu, "Theoretical analysis of configurable RO PUFs and strategies to enhance security," in *Proc. IEEE Int. Workshop Signal Process. Syst.*, 2019, pp. 91–96.

[4] Y. Cui, C. Gu, C. Wang, M. O'Neill, and W. Liu, "Ultra-lightweight and reconfigurable tristate inverter based physical unclonable function design," *IEEE Access*, vol. 6, pp. 28478–28487, 2018.

[5] C. Gu, W. Liu, Y. Cui, N. Hanley, M. O'Neill, and F. Lombardi, "A flip-flop based arbiter physical unclonable function (APUF) design with high entropy and uniqueness for FPGA implementation," *IEEE Trans. Emerg. Top. Comput.*, doi: 10.1109/TETC.2019.2935465.

[6] Q. Guo, J. Ye, Y. Gong, Y. Hu, and X. Li, "Efficient attack on non-linear current mirror puf with genetic algorithm," in *Proc. 25th IEEE Asian Test Symp.*, 2016, pp. 49–54.

[7] A. Waqas and Z. U. Din, "Phase change material (PCM) storage for free cooling of buildings-a review," *Renewable Sustain. Energy Rev.*, vol. 18, pp. 607–625, 2013.

[8] W. Zhao, J. Duval, J. Klein, and C. Chappert, "A compact model for magnetic tunnel junction (MTJ) switched by thermally assisted spin transfer torque (TAS + STT)," *Nanoscale Res. Lett.*, vol. 6, no. 1, pp. 368–368, 2011.

[9] H. S. P. Wong *et al.*, "Metal-oxide RRAM," *Proc. IEEE*, vol. 100, no. 6, pp. 1951–1970, 2012.

[10] G. S. Rose and C. A. Meade, "Performance analysis of a memristive crossbar PUF design," in *Proc. ACM/EDAC/IEEE Des. Automat. Conf.*, 2015, pp. 1–6.

[11] R. Liu, H. Wu, Y. Pang, H. Qian, and S. Yu, "Extending 1 kb RRAM array from weak PUF to strong PUF by employment of SHA module," in *Proc. IEEE Asian Hardware Oriented Secur. Trust Symp.*, 2017, pp. 67–72.

[12] R. Zhang *et al.*, "Nanoscale diffusive memristor crossbars as physical unclonable functions," *Nanoscale*, vol. 10, no. 6, pp. 2721–2726, 2018.

[13] A. Chen, "Utilizing the variability of resistive random access memory to implement reconfigurable physical unclonable functions," *IEEE Electron Device Lett.*, vol. 36, no. 2, pp. 138–140, Feb. 2015.

[14] Y. Zhou, X. Cui, T. Yue, M. Luo, and Q. Lin, "A time-delay based RRAM PUF circuit," in *Proc. IEEE Int. Conf. Electron Devices Solid-State Circuits*, 2017, pp. 1–2.

[15] A. Van Herrewege *et al.*, "Reverse fuzzy extractors: Enabling lightweight mutual authentication for PUF-enabled RFIDs," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2012, pp. 374–389.

[16] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams, "The missing memristor found," *Nature*, vol. 453, no. 7191, pp. 80–83, 2008.

[17] H. Nili *et al.*, "Hardware-intrinsic security primitives enabled by analogue state and nonlinear conductance variations in integrated memristors," *Nat. Electron.*, vol. 1, no. 3, pp. 197–202, 2018.

[18] H. Yu, L. Ni, and H. Huang, "Distributed in-memory computing on binary RRAM crossbar," *ACM J. Emerg. Technol. Comput. Syst.*, vol. 13, no. 3, pp. 1–18, 2017.

[19] M. Cheng *et al.*, "TIME: A. training-in-memory architecture for RRAM-Based deep neural networks," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 38, no. 5, pp. 834–847, May 2019.

[20] S. Shirinzadeh, K. Datta, and R. Drechsler, "Logic design using memristors: An emerging technology," in *Proc. IEEE Int. Symp. Multiple-Valued Logic*, 2018, pp. 121–126.

[21] L. Rui, H. Wu, Y. Pang, Q. He, and S. Yu, "A highly reliable and tamper-resistant RRAM PUF: Design and experimental validation," in *Proc. IEEE Int. Symp. Hardware Oriented Secur. Trust*, 2016, pp. 13–18.

[22] P. Chen and S. Yu, "Compact modeling of RRAM devices and its applications in 1T1R and 1S1R array design," *IEEE Trans. Electron Devices*, vol. 62, no. 12, pp. 4022–4028, Dec. 2015.

[23] G. S. Rose, N. Mcdonald, L. K. Yan, B. Wysocki, and K. Xu, "Foundations of memristor based PUF architectures," in *Proc. IEEE/ACM Int. Symp. Nanoscale Architectures*, 2013, pp. 52–57.

[24] J. Mathew, R. S. Chakraborty, D. P. Sahoo, Y. Yang, and D. K. Pradhan, "A novel memristor-based hardware security primitive," *ACM Trans. Embedded Comput. Syst.*, vol. 14, no. 3, pp. 1–20, 2015.

[25] Y. Y. Chen *et al.*, "Balancing SET/RESET pulse for $> 10^{10}$ endurance in HfO_2/Hf 1T1R bipolar RRAM," *IEEE Trans. Electron Devices*, vol. 59, no. 12, pp. 3243–3249, Dec. 2012.

[26] R. Govindaraj and S. Ghosh, "A strong arbiter PUF using resistive RAM within 1T-1R memory architecture," in *Proc. IEEE Int. Conf. Comput. Des.*, 2016, pp. 141–148.

[27] G. S. Lee, G. Kim, K. Kwak, D. S. Jeong, and H. Ju, "Enhanced reconfigurable physical unclonable function based on stochastic nature of multilevel cell RRAM," *IEEE Trans. Electron Devices*, vol. 66, no. 4, pp. 1717–1721, Apr. 2019.

[28] X. Xue *et al.*, "A 28 nm 512 kb adjacent 2T2R RRAM PUF with interleaved cell mirroring and self-adaptive splitting for extremely low bit error rate of cryptographic key," in *Proc. IEEE Asian Solid-State Circuits Conf.*, 2019, pp. 29–32.

[29] F. Kianifard and D. G. Kleinbaum, "Logistic regression: A. self-learning text," *Technometrics*, vol. 37, no. 1, pp. 116–117, 2010.

[30] N. Hansen, S. D. Müller, and P. Koumoutsakos, "Reducing the time complexity of the derandomized evolution strategy with covariance matrix adaptation (CMA-ES)," *Evol. Comput.*, vol. 11, no. 1, pp. 1–18, 2003.

[31] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2010, pp. 237–249.

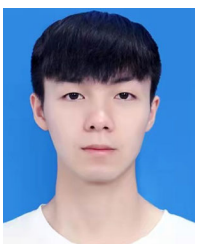
[32] G. T. Becker, "The gap between promise and reality: On the insecurity of XOR arbiter PUFs," in *Proc. Cryptogr. Hardware Embedded Syst.*, 2015, pp. 535–555.

[33] G. Hospodar, R. Maes, and I. Verbauwhede, "Machine learning attacks on 65 nm arbiter PUFs: Accurate modeling poses strict bounds on usability," in *Proc. IEEE Int. Workshop Inf. Forensics Secur.*, 2012, pp. 37–42.

[34] A. Maiti and P. Schaumont, "Improving the quality of a physical unclonable function using configurable ring oscillators," in *Proc. IEEE Int. Conf. Field Programmable Logic Appl.*, 2009, pp. 703–707.

[35] L. Zhang, C. Wang, W. Liu, M. O'Neill, and F. Lombardi, "XOR gate based low-cost configurable RO PUF," in *Proc. IEEE Int. Symp. Circuits Syst.*, 2017, pp. 1–4.

[36] C. Gu, C. H. Chang, W. Liu, S. Yu, Y. Wang, and M. O'Neill, "A modeling attack resistant deception technique for securing lightweight-PUF based authentication," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, doi: 10.1109/TCAD.2020.3036807.



JIANG LI received the B.E. degree in 2016 in information engineering from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, where he is currently working toward the Ph.D. degree. His current research interests include physical unclonable functions based on nanodevice and resistive random access memory.

YIJUN CUI received the B.Sc. degree in information engineering and the Ph.D. degree in information and communication system from the Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China, in 2010 and 2020, respectively. From 2014 to 2015, he was a Visiting Ph.D. Student with the Data Security System Group, Centre of Secure Information Technologies, Queen's University Belfast, Belfast, U.K. He is currently a Lecturer with the College of Electronics and Information Engineering of NUAA. His current research focuses on hardware security.

CHONGYAN GU (Member, IEEE) received the Ph.D. degree from Queen's University Belfast, Belfast, U.K., in 2016. She is currently a Lecturer, Assistant Professor, with the School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, Belfast, U.K. and a Member of the Center for Secure Information Technologies, Institute of Electronics Communications and Information Technologies. She is an expert in hardware security. Her research in physical unclonable function (PUF) has been utilized as part of a security architecture for electronic vehicle charging systems, licensed by LG-CNS, Seoul, South Korea, and was also licensed for evaluation by Thales, U.K. She has coauthored two research book chapters on the topics of *Lightweight Cryptographic Identity Solutions for the Internet of Things* published by IET in 2016 and *Approximate Computing and Its Application to Hardware Security* published by IET in 2016 and Springer in 2018. Her current research interests include PUFs, security in/for approximate computing, true random number generator, hardware Trojan detection, and machine learning attacks. She has successfully organized two conference special sessions, which include the IEEE APCCAS in 2018 and the ACM GLSVLSI in 2020. She was invited to give tutorial or talks in international conferences, such as, the IEEE ASP-DAC 2020 on the topic of practical PUF design on FPGA. Her team was the overall winner of INVENT 2015, a competition to accelerate the commercialization of innovative ideas.

CHENGHUA WANG received the B.Sc. and M.Sc. degrees from Southeast University, Nanjing, China, in 1984 and 1987, respectively. In 1987, he joined the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China, where he became a Full Professor in 2001. He has authored or coauthored six books and more than 100 technical papers in journals and conference proceedings. His current research interests include testing of integrated circuits and systems for communications. He was the recipient of more than ten teaching and research awards at the provincial and ministerial level.

WEIQIANG LIU (Senior Member, IEEE) received the B.Sc. degree in information engineering from the Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China, in 2006 and the Ph.D. degree in electronic engineering from Queen's University Belfast, Belfast, U.K., in 2012. In December 2013, he joined the College of Electronic and Information Engineering, NUAA, where he is currently a Professor and the Vice Dean. He has authored or coauthored one research book by Artech House and more than 100 leading journal and conference papers. His paper was selected as the Highlight Paper of the EEE TCAS-I in the 2021 January Issue and the Feature Paper of IEEE TC in the 2017 December issue. He was the recipient of the prestigious Excellent Young Scholar Award by the National Natural Science Foundation of China in 2020. He was an Associate Editor for the IEEE TRANSACTIONS ON COMPUTERS from May 2015 to April 2019, and is currently an Associate Editor for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEM I: REGULAR PAPERS from January 2020 to December 2021 and the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING from May 2019 to April 2021. He is currently a Steering Committee Member of the IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION SYSTEMS from January 2021 to December 2022, the Program Co-Chair of the IEEE ARITH 2020, and the Technical Program Committee Member for ARITH, DATE, ASAP, ISCAS, ASP-DAC, ISVLSI, GLSVLSI, SiPS, NANOARCH, AICAS, and ICONIP. He is a Member of CASCOM and VSA Technical Committee of the IEEE Circuits and Systems Society.

FABRIZIO LOMBARDI (Fellow, IEEE) received the B.Sc. degree (Hons.) in electronic engineering from the University of Essex, Colchester, U.K., in 1977, the M.Sc. degree in microwaves and modern optics and the Diploma degree in microwave engineering from the Microwave Research Unit, University College London, London, U.K., in 1978, and the Ph.D. degree from the University of London, London, U.K., in 1982. He is currently the International Test Conference Endowed Chair Professorship with Northeastern University, Boston, MA, USA. He has coauthored or edited seven books and has extensively authored and coauthored papers in his research fields, which include bio-inspired and nano manufacturing computing, and VLSI design, testing, and fault defect tolerance of digital systems.