IEEE Open Journal of Nanotechnology

Received 10 September 2020; revised 3 November 2020; accepted 22 November 2020. Date of publication 26 November 2020; date of current version 9 December 2020. The review of this article was arranged by Associate Editor Chang-Ki Baek.

Digital Object Identifier 10.1109/OJNANO.2020.3040787

Lightweight Configurable Ring Oscillator PUF Based on RRAM/CMOS Hybrid Circuits

YIJUN CUI [1], CHENGHUA WANG[1], WEIQIANG LIU [1] (Senior Member, IEEE), CHONGYAN GU [2] (Member, IEEE), MÁIRE O'NEILL[2] (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, BT7 1NN Belfast, U.K.
[3]Department of Electrical and Computer Engineering, Northeastern University, Boston, MA 02115 40125, U.S

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

This work was supported in part by the National Natural Science Foundation China under Grants 62022041 and 61771239, and in part by the Engineering and Physical Sciences Research Council (EPSRC) (EP/N508664/-CSIT2).

ABSTRACT Physical unclonable function (PUF) is a lightweight security primitive for energy constrained digital systems. As an enhanced design of conventional ring oscillator (RO) PUFs, configurable ring oscillator (CRO) PUFs improve the uniqueness and reliability compared with the conventional RO PUF designs. In typical CRO PUF designs, multiplexers (MUXs) are utilized as configurable components. In this paper, a hybrid nano-scale CRO (*hn*-CRO) PUF is proposed. The configurable components of the proposed *hn*-CRO PUF are implemented by RRAMs. The delay elements are based on CMOS inverters. Compared with traditional CRO PUF designs, the proposed *hn*-CRO PUF is cost-efficient in terms of circuit density and gate per challenge response pair (CRP) bit. To validate the proposed *hn*-CRO PUF, the Monte Carlo simulation results of a compact RRAM model under UMC 65 nm technology are presented. The results show that the proposed *hn*-CRO PUF has a good uniqueness and low hardware consumption compared with the previous works.

INDEX TERMS Configurable PUF, physical unclonable function, RRAM, ring oscillator.

I. INTRODUCTION

PUF is one of the most promising security primitives for resource constrained scenarios, e.g. the Internet of Things (IoT) applications. A PUF utilizes process variations to generate unique CRPs for each single chip. Even when manufactured under the same condition, the CRPs of a specific chip will be different and these unique CRPs can be used to prevent the adversary from an unauthorized copy of the chip. To date, various PUF structures have been proposed and they can be classified to delay based PUFs and memory based PUFs. The most cited designs include RO PUFs, Arbiter PUFs and SRAM PUFs [1].

CRO PUF, as an improved design of the conventional RO PUF, aims to acquire a high uniqueness, reliability and lower cost. A typical CRO PUF is composed of switching components and delay components, where the switching components provide the reconfigurability to the PUF structure when the design is completed and deployed. The MUXs in [2]–[4] and the tristate gates in [5] act as the switching components and selects which delay unit is involved in the construction of the CRO PUF.

As CMOS integrated circuits (ICs) are reaching its limitation, nano-device based PUFs provide new possibilities for reliable security circuits. It is a great challenge for IC designers and foundries to scale down the devices to the nanoscale size since the unpredictable thickness and the cross-sectional area introduce large process variations. However, this is a great opportunity for the PUF designers since the multiple variations and noise sources can improve the uniqueness and randomness of the PUF responses. Moreover, the entropy of a PUF design can be increased significantly due to the unpredictable variations and noises. Among the emerging PUFs based on nanotechnology, the resistive random access memory (RRAM, also referred as memristor or ReRAM [6])

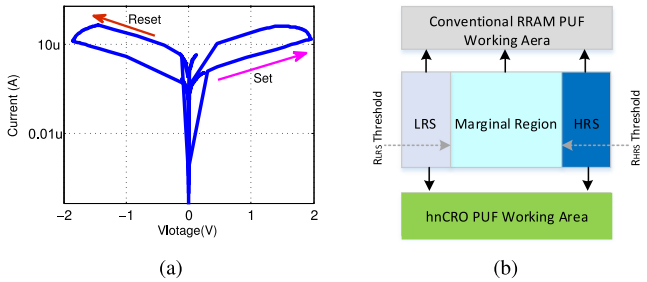


FIGURE 1. RRAM circuits: (a) I-V curve of the RRAM, and (b) working area of the RRAM PUF.

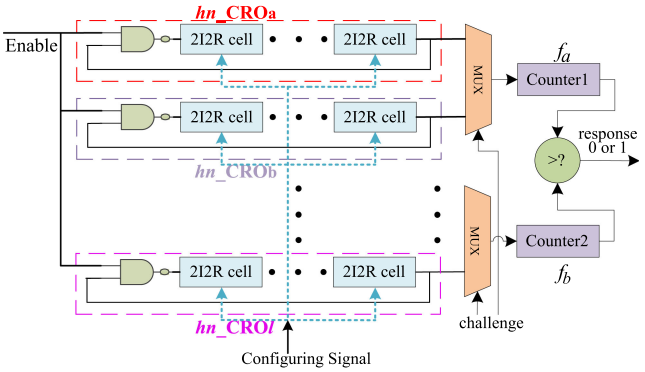


FIGURE 2. The Proposed *hn*-CRO PUF design.

based PUF designs are one of the most promising approaches. Conventional RRAM based PUF designs mainly utilize the resistance variations and mismatch of the RRAM at a fixed programming voltage or programming time.

A lightweight CRO PUF based on memristor/CMOS hybrid circuits is proposed in this paper. The RRAMs of the proposed PUF can be considered as resistive switches by configuring to a definite state ON or OFF. Both RRAMs and traditional CMOS inverters are involved to construct a basic RO, where the programmable RRAMs act as the configurable components of the CRO PUF. The new structure has a good uniqueness as well as a lightweight property compared with the conventional RO PUF and CRO PUF. When compared with the previous RRAM based structures, the proposed PUF is more reliable and efficient in terms of hardware cost.

The rest of this paper is organized as follows: Section II reviews the RRAM and RRAM based PUFs. Section III presents the detailed design of the proposed *hn*-CRO PUF and the configuring strategy. Simulation results are given in Section IV and Section V concludes the paper.

II. RELATED WORK

A. RRAM BASED PUFS

RRAMs can be classified as bipolar or unipolar according to the switching behaviors. The bipolar RRAM based on metal-oxide(shown in Fig. 1(a)) is one of the most promising candidates for applications in memory computing or configurable logic [7]. By applying a proper positive or negative pulse to the selected RRAM cell, the resistance of the RRAM will be switched between High-Resistance State (HRS) and Low-Resistance State (LRS), corresponding to ON and OFF of the circuit. When the RRAM is configured in the low-resistive ON state, it works like a diode. On the contrary, if the RRAM is in the high-resistive OFF state, the current that can flown through the RRAM is very small.

RRAM is a popular primitive for PUF designs, especially for memory based PUF designs. A survey of recent studies investigating emerging nano-electronic devices to build PUFs is given in [8]. Most of these designs rely on the resistance of the RRAMs and one major issue of the RRAM based PUF design is that the structures need extra analog reading circuits e.g. analog-to-digital converter (ADC) to generate the corresponding response. Furthermore, the resistance of the RRAM is strongly related to the operating temperature and the programming voltages or time. These make them unreliable and conventional RRAM based circuits suffers serious variability [9]. Besides, for crossbar based RRAM PUFs, the accumulated sneak current will also make them unstable and unreliable [10].

B. RRAM CMOS HYBRID DESIGNS

RRAM CMOS hybrid design offers an opportunity to accomplish high-density circuit [11], since the RRAM have been proved CMOS-compatible and it can be integrated in the metal layers over the CMOS layer [12]. Previous research have shown that RRAM based switch box (SB) can be applied to the design of high performance and high density FPGAs [12], [13]. Furthermore, the RRAM CMOS hybrid circuits can accelerate neural network computations [14].

Inspired by the idea of the RRAM CMOS hybrid designs in the FPGA, *hn*-CRO PUF is proposed in the paper. Different from the previous RRAM based PUF designs [15]–[17], in this paper, the RRAMs in this work are configured at the fixed state and works like a programmable nano-switch while the CMOS inverters act as the delay components, as shown in Fig. 1(b), which makes the proposed *hn*-CRO PUF more reliable.

III. PROPOSED HYBRID NANODEVICE CRO PUF DESIGN

The schematic of a 1-bit *hn*-CRO PUF response generation is shown in Fig. 2. The *hn*-CRO PUF is composed of l *hn*-CRO array, two MUXs, two counters and one comparator. One *hn*-CRO array includes m stages two-inverters-two-resistors (2I2R) cells and one NAND gate. Configuring signal are applied to the *hn*-CRO array to active inverters inside the 2I2R cells. In order to obtain the CRPs, two identical PUF cells will be selected and the odd numbers of the inverters will be chosen. When the same challenge bits are applied to the PUF structure, the output frequencies f_a and f_b of the selected *hn*-CRO arrary are different due to the process variations. The response bit will be '1' or '0' depending on which frequency is higher.

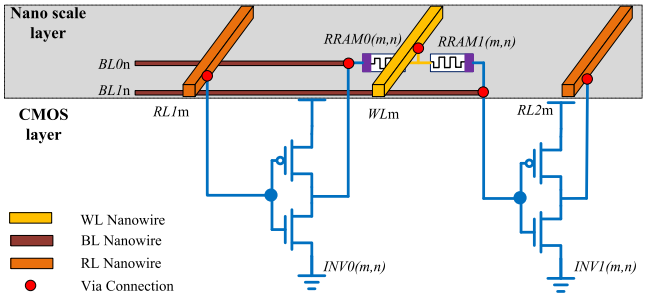


FIGURE 3. The Basic 2I2R structure of a *hn*-CRO array.

A. 2I2R STRUCTURE OF THE PROPOSED hn-CRO PUF DESIGN

The basic 2I2R structure, which consists two inverters ($INV0(m, n)$ and $INV1(m, n)$), two RRAMs ($RRAM0(m, n)$ and $RRAM1(m, n)$), three programming nanowires (WL_m, $BL0(m, n)$ and $BL1(m, n)$) and two routing nanowires ($RL0_m$ and $RL1_m$), is illustrated in Fig. 3. The basic cell is distributed into two layers: the nano scale layer and the CMOS layer. The two RRAMs, $RRAM_0$ and $RRAM_1$ of the 2I2R structure, share a common programming terminal nanowire WL. The other terminal of the RRAM is connected to ($BL0$, the output of $INV0$) and ($BL1$, the input of $INV1$), respectively.

During the configuring process, the common nanoline WL is programmed to '0' by using a tristate gate. If a positive pulse is applied to the bit line, the RRAM is at a LRS mode and the inverter is selected to contribute to the composition of the CRO PUF. On the contrary, when a negative pulse is applied to the bit line, the RRAM is turned OFF and set to HRS mode. After the configuration, the tristate gate, connected to the common nanoline WL, is programmed to a high-resistant state and the WL is left floated and acts as the routing wire.

In an ideal model, the RRAM should work like a switch and the LRS value is zero while the HRS value is infinitely large. However, in the practical implementation of the RRAM, the ON resistance is $\sim 10^3\Omega$ and its OFF resistance is $\sim 10^9\Omega$ [12]. This means even the RRAM is at the HRS mode, there will be a small leakage current, through the RRAM, affects the delay time of each stage. The inverters that connected to HRS RRAMs are defined as weak selected inverters and those connected to LRS RRAMs are defined as strong selected inverters. These two types of inverters contribute to the final oscillation frequency of the proposed *hn*-CRO PUF design. Due to the RC delay variations of the strong selected inverters and the leak current of the weak selected inverters, the randomness and uniqueness of the proposed *hn*-CRO PUF design achieve a good result compared with previous RRAM based PUF designs.

B. CONFIGURATION STRATEGY FOR THE hn-CRO PUF DESIGN

The overview of the proposed *hn*-CRO PUF cell circuit is shown in Fig. 4. For a single *hn*-CRO matrix, n 2I2R structures are connected in parallel in each stage and there are m

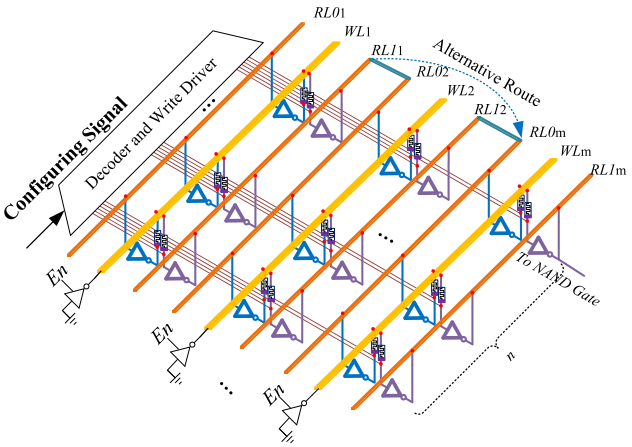


FIGURE 4. An Overview of the proposed *hn*-CRO PUF cell circuit (NAND gate, MUX and counters are not included).

stages in total. In the conventional RO PUF or CRO PUF, the stages should be always designed to odd number to make the system oscillate. While in the *hn*-CRO PUF, each 2I2R contains two inverters and the number of the inverters will be always odd when counting the NAND gate in. Due to the delay introduced by the RRAM, the full delay of a single *hn*-CRO matrix will significantly decreased when compared with the CMOS based RO PUF or CRO PUF. This will simplify the circuit designs at the CMOS level, e.g. less stages and counters.

As mentioned in Section 2, the state of a RRAM is related to the last resistive state. The next state of a RRAM can be programmed or configured by applying a proper voltage to the selected RRAM. In order to switch certain RRAMs from state OFF to state ON, the two wires leading to the RRAM are fed by a positive pulse. Before the collections of the CRPs, a proper programming voltage must be chosen and applied to the RRAM to configure the CRO PUFs. To initiate the configuring mode, the value of the En signal in Fig. 4 is set to '1' and all WLs are connected to GND. Then, a configuring signal will be applied to the *hn*-CRO PUF and both the decoding and writing circuits will transfer the signal to negative or positive pulse to program the corresponding RRAMs. If the value is '1,' the corresponding RRAM will be programmed to the LRS mode and the connected inverter is activated to joint the signal propagate. The configuring process is a procedure to decide which inverter is selected to form the basic RO and which route is activated to transmit the electronic signal. A previous work [18] has demonstrated that adjacent components have a similar aging tendency. Therefore, the configurable strategy, that always selects adjacent components, will further countermeasure the aging issue of the *hn*-CRO PUF design(compared with conventional RRAM based PUFs).

The *hn*-CRO PUF can be configured flexibly according to the requirements of applications. Furthermore, the proposed PUF structure can dynamically change the topology by reprogramming routing lines. As shown in Fig. 4, the routing line $RL1_1$ can be routed to $RL0_2$ or other routing lines, e.g. $RL0_m$.

TABLE 1. Parameters of the RRAM

Parameter	Description	Value	Variation
Gap_d	Gap distance	0.1nm ~ 1.7nm	
R_{on}	Resistance of LRS	1.073kΩ	$\pm 3\sigma$
R_{off}	Resistance of HRS	1.621MΩ	$\pm 3\sigma$
D	Width of RRAM	3nm	

In this way, the PUF *hn*-CRO can be configured to be a regular CRO PUF by routing horizontally or vertically. It can also be configured as a cross or in a zigzag manner, and uneven number of inverters can be chosen in different stages. When used in a resource constrained devices, the *hn*-CRO PUF can be configured to a lightweight mode and only several arrays can be deployed. In this case, the configuring signals can be considered as the challenge bits. In the lightweight mode, the PUF can be configured and compared by using a randomness loop or a chain like the strategy.

After the configuring procedure, the challenges will be applied to the multiplex and according to the value of the challenges, the corresponding RO array will be chosen to generate a 1-bit response by comparing the output frequencies. Compared with the previous configurable RO PUFs, the proposed *hn*-CRO PUF can choose any inverter in each column and be able to reconfigure all stages of the ROs.

IV. EXPERIMENTS AND RESULTS

A. SIMULATION SETUP

To evaluate the performance, an *hn*-CRO PUF circuit with 100 stages are constructed. The basic circuit is designed using Synopsys Hspice 2013, where one inverter and one RRAM are included to simulate the selected delay unit. In the simulation, the compact spice model introduced in [19] is utilized to simulate the behavior of a RRAM; the CMOS part is implemented using a UMC 65 nm technology with a supply voltage of 1.1 V. The simulation parameters of the RRAM are reported in Table 1. There are two main variation sources in the proposed *hn*-CRO PUF: the variations from the RRAMs and the variations from the CMOS RO. In this paper, the gap growth variation δg, temperature and supply voltage are considered as the main variations for the RRAM. The variations of the CMOS part is performed based on the statistical library provided by UMC.

As shown in Fig. 5, the RRAM performance (from LRS to HRS) will be affected by the operating temperature. The rising time from LRS to HRS will decrease with the increase of temperature. However, the final resistance is kept at the same level. The results show that the proposed hybrid circuit is more reliable than pure RRAM based circuits. The output frequency of pure CMOS based CRO, *hn*-CRO in LRS mode and *hn*-CRO in HRS mode is illustrated in Fig. 6. The results shows that the RC delay introduce by the RRAM in LRS mode helps to decrease the final frequency and this will simplify the design of counters. As shown in Fig. 6, the maximum output frequency of the pure CMOS RO circuits is approximately 870 MHz, while the maximum output frequency of

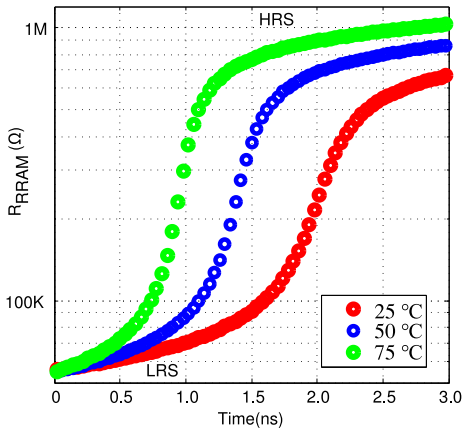


FIGURE 5. The RRAM performance under thermal variations.

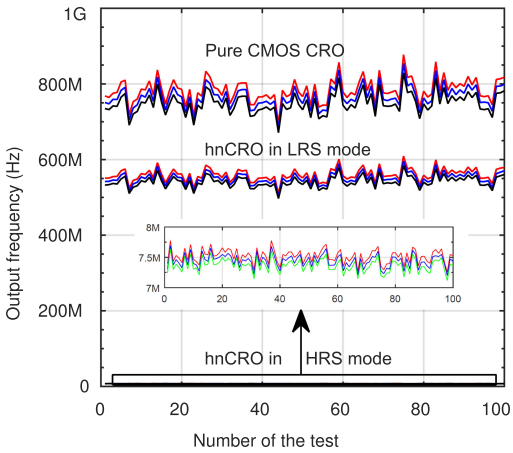


FIGURE 6. The Output frequencies at different configurations.

the combined *hn*-CRO PUF cell is approximately 580 MHz. Therefore, the *hn*-CRO structure saves 33.33% of the hardware consumption of the counters when compared with conventional CMOS based CRO PUFs. Meanwhile, when the RRAM are configured as HRS, the leak current will still contribute to the oscillation, however, this frequency is relatively small (7.5 MHz vs 580 MHz) when compared with LRS state. Though the output frequencies at a configured state vary with the temperature variation (red, blue and green lines in different mode), they share the same trend and this will not affect the final PUF responses.

B. PUF PERFORMANCE

Uniqueness and uniformity are adopted to measure the performance of the proposed *hn*-CRO PUF. Reliability is not included in this evaluation since there is no ideal statistical data for the simulation of the RRAM. Uniqueness represents the ability to distinguish different PUF instances and uniformity evaluates the proportion of the total numbers of '1' and '0' in each response of the PUF cell and can measured by

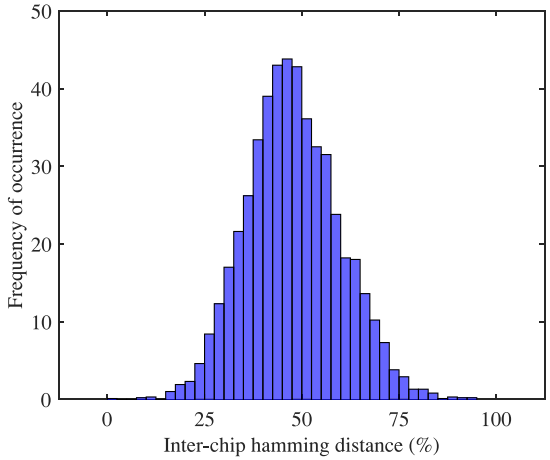


FIGURE 7. Uniqueness of the proposed PUF.

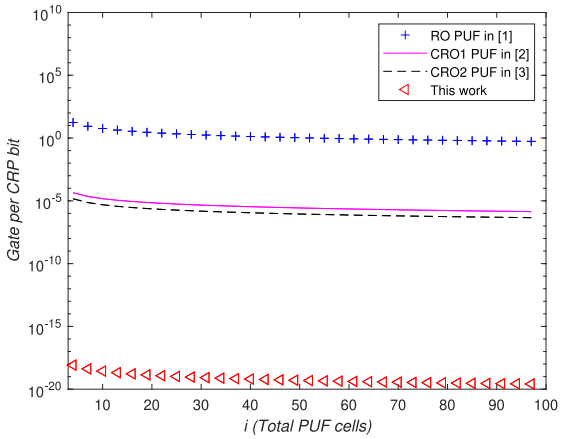


FIGURE 8. Comparison of the cost efficiency for RO and CRO PUFs.

TABLE 2 Performance Comparison With Previous Works

Design	Uniformity	Uniqueness	Strong PUF
Memristor PUF [15]	46.2%	49.97%	Yes
ReRAM PUF [16]	47.28%	49.85%	No
XBAR PUF [17]	49.5-50%	50%	No
TCRO PUF [5]	52.45%	49.69%	Yes
This work	49.76%	49.23%	Yes

calculating the average inter-chip Hamming distance (HD) of the PUF responses over different devices. The intra-chip hamming distances of the responses under different temperature and supply voltage are also calculated to evaluate the Bit Error Rate. 5000 Monte Carlo runs are carried out and the PUF responses are then calculated based on the frequency adopted from the Monte Carlo simulations.

The uniqueness of the *hn*-CRO PUF is 49.23%, as shown in Fig. 7 and the uniformity is 49.76%, which is very close to the ideal result 50%. The intra-chip hamming of the *hn*-CRO PUF is 1.95% (the reliability is given by 100%-1.95% = 98.05%); this shows that the *hn*-CRO PUF is reliable under different operating conditions. The simulation results and a comparison with previous works are presented in Table 2. When compared with previous pure RRAM based PUF designs [15]–[17], *hn*-CRO PUF has a good uniqueness and uniformity. Moreover, the *hn*-CRO PUF is a configurable strong PUF since it can generate sufficient CRPs.

C. HARDWARE COST

The proposed *hn*-CRO PUF is lightweight compared with conventional RRAM based designs, since it doesn't need any read circuits. Moreover, the proposed structure is a strong configurable RO PUF while most of the previous work are weak PUFs [8]. To comprehensively analyse the hardware efficiency, the *hn*-CRO PUF is also compared with typical CMOS based CRO PUFs. According to the evaluation metrics proposed in [5], the cost efficiency (only consider the core circuits and the decoder for the writing operation) of the proposed *hn*-CRO PUF can be expressed as:

$$\mathrm{CE}_{\mathrm{hnCRO}} = \frac{(8n+4)\cdot i}{\binom{i}{2}\cdot m^n \cdot m^n} \tag{1}$$

The CEs of conventional RO [1], CRO PUF in [2] and [3] are can be calculated as followed:

$$\mathrm{CE}_{\mathrm{RO}} = \frac{4n+8}{i-1} \tag{2}$$

$$\mathrm{CE}_{\mathrm{CRO1}} = \frac{6n+4}{(i-1)\cdot 2^{2n-3}} \tag{3}$$

$$\mathrm{CE}_{\mathrm{CRO2}} = \frac{8n+4}{(i-1)\cdot 2^{2n-1}} \tag{4}$$

where m represents the rows of the proposed PUF, n represents the stages of the ring oscillator and i represents the total numbers of the ring oscillator.

A comparison of hardware efficency with typical CMOS based CRO PUFs is shown in Fig. 8. It is assumed that $m = 11$ and $n = 16$, which means there are 11 stages of the RO and the rows of the proposed PUF is 16. It can be seen that the *hn*-CRO PUF has the highest cost efficiency (increased up to 10 orders of magnitudes) when compared with the other previous works.

V. CONCLUSION

In this paper, a configurable RO PUF based on RRAM/CMOS hybrid circuits is proposed. The proposed PUF design utilizes the switching character of the RRAM and stack them on the top of the CMOS inverters. By introducing the RRAMs circuits, the *hn*-CRO PUF can determine the total stages and select the inverters to compose the RO. Monte Carlo simulations with a compact RRAM model and UMC 65 nm library are conducted to validate the design. The experimental results show that the proposed *hn*-CRO PUF has a good uniqueness and high randomness. Furthermore, the *hn*-CRO PUF is up to 10 orders of magnitudes more cost efficient than the other works.

REFERENCES

[1] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proc. 44th ACM/IEEE Des. Automat. Conf.*, 2007, pp. 9–14.

[2] A. Maiti and P. Schaumont, "Improved ring oscillator PUF: An FPGA-friendly secure primitive," *J. Cryptol.*, vol. 24, no. 2, pp. 375–397, Apr. 2011.

[3] M. Gao, K. Lai, and G. Qu, "A highly flexible ring oscillator PUF," in *Proc. 51st Des. Automat. Conf.*, 2014, pp. 1–6.

[4] Y. Cui, C. Wang, W. Liu, Y. Yu, M. O'Neill, and F. Lombardi, "Low-cost configurable ring oscillator PUF with improved uniqueness," in *Proc. IEEE Int. Symp. Circuits Syst.*, 2016, pp. 558–561.

[5] 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.

[6] K. Beckmann, H. Manem, and N. C. Cady, "Performance enhancement of a time-delay PUF design by utilizing integrated nanoscale ReRAM devices," *IEEE Trans. Emerg. Top. Comput.*, vol. 5, no. 3, pp. 304–316, Jul.–Sep. 2017.

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

[8] Y. Gao, D. C. Ranasinghe, S. F. Al-Sarawi, O. Kavehei, and D. Abbott, "Emerging physical unclonable functions with nanotechnology," *IEEE Access*, vol. 4, pp. 61–80, 2016.

[9] Y. Pang *et al.*, "A reconfigurable RRAM physically unclonable function utilizing post-process randomness source with< 6× 10- 6 native bit error rate," in *Proc. IEEE Int. Solid-State Circuits Conf.*, 2019, pp. 402–404.

[10] Y. Zhang *et al.*, "CACF: A novel circuit architecture co-optimization framework for improving performance, reliability and energy of ReRAM-based main memory system," *ACM Trans. Architecture Code Optim.*, vol. 15, no. 2, pp. 1–26, May 2018.

[11] F. Garcia-Redondo and M. Lopez-Vallejo, "On the design and analysis of reliable RRAM-CMOS hybrid circuits," *IEEE Trans. Nanotechnol.*, vol. 16, no. 3, pp. 514–522, May 2017.

[12] J. Cong and B. Xiao, "FPGA-RPI: A novel FPGA architecture with RRAM-based programmable interconnects," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 22, no. 4, pp. 864–877, Apr. 2014.

[13] B. Khaleghi and H. Asadi, "A resistive RAM-based FPGA architecture equipped with efficient programming circuitry," *IEEE Trans. Circuits Syst. I: Regular Papers*, vol. 65, no. 7, pp. 2196–2209, Jul. 2018.

[14] H. Huang, L. Ni, K. Wang, Y. Wang, and H. Yu, "A highly parallel and energy efficient three-dimensional multilayer CMOS-RRAM accelerator for tensorized neural network," *IEEE Trans. Nanotechnol.*, vol. 17, no. 4, pp. 645–656, Jul. 2018.

[15] 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, Apr. 2015, Art. no. 60.

[16] J. Kim, *et al.*, "A physical unclonable function with redox-based nanoionic resistive memory," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 2, pp. 437–448, Feb. 2018.

[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, 2018, Art. no. 197.

[18] A. Maiti and P. Schaumont, "The impact of aging on a physical unclonable function," *IEEE Trans. Very Large Scale Integr. Syst.*, vol. 22, no. 9, pp. 1854–1864, Sep. 2014.

[19] Z. Jiang *et al.*, "A compact model for metal–oxide resistive random access memory with experiment verification," *IEEE Trans. Electron Devices*, vol. 63, no. 5, pp. 1884–1892, May 2016.

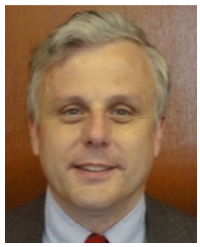
YIJUN CUI received the B.Sc. degree in information engineering and the Ph.D. degree in information and communication system from the Nanjing University of Aeronautics and Astronautics, Nanjing, China, in 2010 and 2020, respectively. He was a Visiting Ph.D. Student with the Data Security System Group, the Centre of Secure Information Technologies, Queen's University Belfast, U.K. from 2014 to 2015. He is currently a Lecturer with the College of Electronics and Information Engineering, NUAA. His current research interests include mainly in the 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 EEECS, Queen's University Belfast, and a Member of Center for Secure Information Technologies (CSIT) with in the Institute of Electronics Communications and Information Technologies (ECIT). Dr. Gu is an expert in hardware security. Her research into physical unclonable function (PUF) has been utilised as part of a security architecture for electronic vehicle (EV) charging systems, licensed by LG-CNS, South Korea, and was also licensed for evaluation by Thales, U.K. Her team was the overall winner of INVENT 2015, a competition to accelerate the commercialisation of innovative ideas. She has co-authored 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, respectively. She has successfully organised two conference special sessions (IEEE APCCAS in 2018 and ACM GLSVLSI in 2020). She was invited to give tutorial/talks to international conferences, such as, IEEE ASP-DAC 2020 on the topic of practical PUF Des. on FPGA. Her current research interests include physical unclonable functions (PUFs), security in/for approximate computing, true random number generator (TRNGs), hardware Trojan detection and machine learning attacks.

CHENGHUA WANG received the B.Sc. and M.Sc. degrees from Southeast University, Nanjing, China, in 1984 and 1987, respectively. In 1987, he was with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, where he became a Full Professor in 2001. He has authored or coauthored six books and over 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 B.Sc. degree in information engineering from NUAA and the Ph.D. degree in electronic engineering from Queen's University Belfast (QUB), Belfast, U.K., in 2006 and 2012, respectively. He is currently a Professor and Vice Dean with the College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics (NUAA), Nanjing, China. He is a Member of IEEE Circuits and Systems Society. He has served as an Associate Editor for the several IEEE journals such as TCAS-I (2020.1-2022.12), TETC (2019.5-2021.4), TC (2015.5-2019.4), a Guest Editor for PIEEE (2019-2020). He is the program Co-Chair of ARITH and Program Members of international conferences; ARITH, DATE, ASP-DAC, ISCAS, ASAP, ISVLSI, GLSVLSI, AsiaHOST, NANORACH, AICAS, SiPS & ICONIP. He has published one research book by Artech House and over 110 leading journal and conference papers. He received the prestigious Excellent Young Scholar Award from NSFC in 2020. His research interests include computer arithmetic, hardware security and VLSI Design for digital signal processing and cryptography.

MÁIRE O'NEILL (Senior Member, IEEE) is currently the Director of the U.K. Research Institute in Secure Hardware and Embedded Systems (RISE). She is the Chair of Information Security and the Research Director of Data Security Systems with the Centre for Secure Information Technologies (CSIT), Queen's University Belfast. She also leads the EU H2020 SAFEcrypto (Secure architectures for Future Emerging Cryptography) project. She previously held an EPSRC Leadership Fellowship (2008-2014) and was a former holder of a Royal Academy of Engineering Research Fellowship from 2003 to 2008. She was the recipient of numerous awards for her research work which include a 2014 Royal Academy of Engineering Silver Medal and British Female Inventor of the Year 2007. She has authored two research books and has over 130 peer-reviewed conference and journal publications. Her research interests include hardware cryptographic architectures, lightweight cryptography, side channel analysis, physical unclonable functions, post-quantum cryptography and quantum-dot cellular automata circuit design. She is an Associate Editor for the IEEE TRANSACTIONS ON COMPUTERS and IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTING and is an IEEE Circuits and Systems for Communications Technical Committee Member. She is a Member of the Royal Irish Academy and a Fellow of the Irish Academy of Engineering. She is also a member of the IET and IACR.



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