

# A highly reliable FPGA-based RO PUF with enhanced challenge response pairs resilient to modeling attacks

Zhangqing He<sup>1</sup>, Chen Wang<sup>1</sup>, Tao Ke<sup>1</sup>, Yuejiao Zhang<sup>1</sup>, Wenjun Cao<sup>1</sup>, and Jiuchun Jiang<sup>1, a)</sup>

**Abstract** Ring oscillators based physical unclonable functions (RO PUF) is a classical FPGA-friendly Weak PUF structure with better performance, but it can only produce limited challenge-response pairs (CRPs) with lack reliability. This paper proposes a new Strong RO PUF structure with highly reliability and enhanced challenge response pairs resilient to modeling attacks. It divides  $2N$  RO rings into two groups and compares their cumulative frequency under the control of the  $N$ -bit challenge to generate  $2^N$  CRPs. The reliability of each bit PUF responses is tested and marked in real time, and a highly reliable anti-fuse PUF structure is introduced to fuzzify the CRPs. FPGA verification results show that this bit self-test RO PUF (BST-RPUF) has a uniformity of 46.78% and a uniqueness of 48.64%, and the bit error rate of the marked reliable responses can be less than  $10^{-9}$ .

**Keywords:** RO PUF, bit self-test, reliability flag, resistant to modeling attacks

**Classification:** Integrated circuits

## 1. Introduction

Physical unclonable functions [1] (PUFs) is a promising hardware security primitive that can provide a low-cost, high-secure solution for key generation and authentication of IoT devices. PUF can be divided into Weak PUF and Strong PUF [2]. Weak PUFs generate a limited number of CRPs, whose responses must keep confidential, and are typically used for key generation and storage [3, 4]. Strong PUFs generate a large number of CRPs. Since they have better resistance to physical detection and side-channel attacks, a small amount of responses leakage will not affect the overall security of them, which also makes their application scope wider [5, 6]. However, Strong PUFs have also been proved to be vulnerable to modeling attacks [7, 8]. Due to the constraints of placement and routing when implemented on FPGA, the proposed Strong PUF is generally not suitable for execution on FPGA [9], such as Arbiter PUFs [10, 11], switched-capacitor PUFs [12], etc. In addition, the output of PUF circuit is inevitably affected by environmental factors (temperature, voltage, etc.). Postprocessing using helper data algorithms (HDAs) is required to extract the reliable keys from noise responses. However, most HDAs require complex error correction codes [13, 14, 15] (ECCs) such as BCH requires additional high hardware overhead and large

entropy loss, and is vulnerable to helper data manipulation attacks [16].

Compared with Arbiter PUF, RO PUF [17, 18, 19] is a classical Weak PUF structure with better performance which does not require a symmetric structure and is easy to implement on FPGAs and ASICs. Therefore, this paper proposes a new Strong RO PUF structure based on the RO PUF, which divides the RO oscillation frequencies in two RO blocks into two groups for superposition and comparison using challenge signal control to achieve an exponential level of challenge response space. Based on this, a flexible reliability self-testing method is proposed to detect the reliability of each bit response in real time so as to avoid the use of complex ECC error correction mechanism. Effective protection against modeling attacks is achieved by introducing a highly reliable anti-fuse PUF to fuzzify the CRPs. FPGA verification results show that the uniformity of BST-RPUF is 46.78%, and the uniqueness is 48.64%, the bit error rate of the reliable responses after self-test can reach less than  $10^{-9}$ .

## 2. Strong RO PUF circuit design

### 2.1 Strong RO PUF circuit principle

Conventional RO PUF generates a digital response of 0/1 by comparing the frequencies of two identical ring oscillators, and the challenge signal  $C_i$  is used to control the multiplexer. After selecting a pair of ROs, the RO frequencies are measured by two counters, and finally compare the frequency to generate a response  $R$ . The result can be expressed by Equation (1).

$$R = \begin{cases} 1, & \text{if } f_1 > f_2 \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

In order to extend the challenge response space of RO PUF, a new RO PUF structure is proposed in this paper, which is shown in Fig. 1. This Strong PUF generates  $2^N$  challenge response pairs by dividing the frequencies of  $2N$  RO rings into two groups and then compare the accumulated count values. The circuit mainly consists of two RO blocks, two RO selectors, a selection controller, a path selector, two accumulators and a comparator. The two RO blocks  $A$  and  $B$  each contain  $N$  ROs, and the selection controller sequentially generates  $N$  selection signals to select two RO rings in turn from the two blocks  $A$  and  $B$ . Under the control of the  $N$ -bit challenge signal  $C$ , the two RO rings are sent to two accumulators in turn via the path selector. The accumulator measures and accumulates the frequency of the input RO

<sup>1</sup> Hubei Engineering Research Center for Safety Monitoring of New Energy and Power Grid Equipment, Hubei University of Technology, Wuhan, 430068, China

<sup>a)</sup> [jiangjc2021@163.com](mailto:jiangjc2021@163.com)

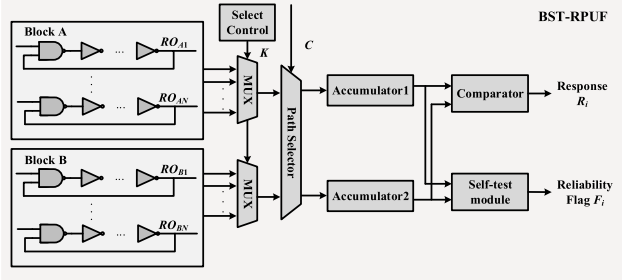


Fig. 1 Strong RO PUF circuit structure.

oscillation signal by counting the number of high levels in  $t$  time of the oscillation signal. Finally, the cumulative count values are compared to obtain the response  $R$ .

Assume that the count value in accumulator 1 is  $F_A$ , the count value in accumulator 2 is  $F_B$ , and the challenge signal of  $N$  bits is  $C_{[0]}$  to  $C_{[N-1]}$  in order from low to high. If  $C_{[i]}$  is 0, the path selector sends the  $i$ -th RO ring  $RO_{Ai}$  in the A block to the accumulator 1 and  $RO_{Bi}$  to the accumulator 2 for counting, and vice versa. Suppose the count values of  $RO_{Ai}$  and  $RO_{Bi}$  are  $F_{Ai}$  and  $F_{Bi}$ , respectively, after  $N$  rounds of operation, the total frequency difference  $T_{AB}$  of the two comparators can be expressed as follows.

$$\begin{aligned} T_{AB} &= (-1)^{C_{[0]}}(F_{A0} - F_{B0}) + (-1)^{C_{[1]}}(F_{A1} - F_{B1}) \\ &\quad + \dots + (-1)^{C_{[N-1]}}(F_{A(N-1)} - F_{B(N-1)}) \\ &= \sum_{i=0}^{N-1} (-1)^{C_{[i]}}(F_{Ai} - F_{Bi}) \end{aligned} \quad (2)$$

If  $T_{AB} > 0$ , then  $F_A > F_B$  and the output response is 1, otherwise the output response is 0. Since the  $N$ -bit challenge signal  $C$  has  $2^N$  control input cases, in each case a different frequency difference  $T_{AB}$  will be generated, resulting in a response  $R$ , thus this PUF can generate  $2^N$  challenge-response pairs.

Here we give an established case of 4-stage Strong RO PUF to further illustrate the working principle of the circuit. For a 4-stage Strong RO PUF, there are 4 ROs in each of the A and B blocks, and the  $K$  and  $C$  is 2 bits and 4 bits at length respectively. First the value of the control selection signal  $K$  is set to 00, the  $RO_{A1}$  in block A and  $RO_{B1}$  in block B are selected, the lowest bit  $C_{[0]}$  of the challenge signal  $C$  is used to control the path selector. When  $C_{[0]}$  is 0,  $RO_{A1}$  in block A is input to accumulator 1 and  $RO_{B1}$  in block B is input to accumulator 2; when  $C_{[0]}$  is 1,  $RO_{A1}$  is input to accumulator 2 and  $RO_{B1}$  is input to accumulator 1. And then the  $K$  is set to 01,  $RO_{A2}$  and  $RO_{B2}$  are selected. The next lowest challenge signal  $C_{[1]}$  is used as the control signal of the path selector to determine whether  $RO_{A2}$  and  $RO_{B2}$  are input to accumulator 1 or 2 respectively. Suppose that the input challenge  $C$  is 1001, after 4 rounds of cumulative counting, the accumulated count values in accumulators 1 and 2 are  $F_{B1} + F_{A2} + F_{A3} + F_{B4}$  and  $F_{A1} + F_{B2} + F_{B3} + F_{A4}$  respectively, and they are finally compared by the comparator to generate 1-bit response  $R$ . Since the 4-bit path selection signal  $C$  has a total of  $2^4 = 16$  cases, each of which can produce a 1-bit response, thus a 4-stage BST-RPUF consisting of 8 ROs can produce 16-bit responses.

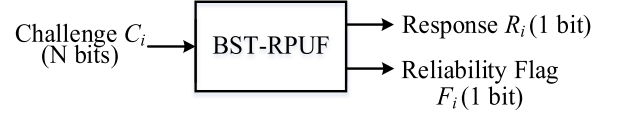


Fig. 2 Reliability self-test model.

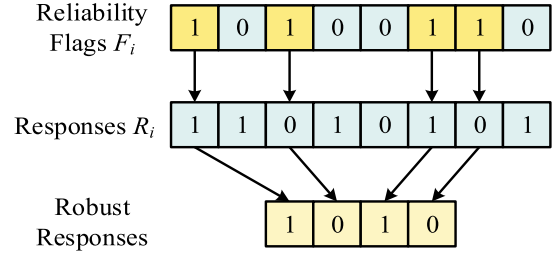


Fig. 3 Robust responses extraction process.

## 2.2 Reliability self-test

RO PUF generates a unique response mainly by detecting the difference in frequencies created by the two RO rings during the manufacturing process. When the difference is large, the PUF output is more stable and reliable, which can resist the change of outside condition [20, 21]. For our Strong RO PUF, the total difference  $|\Delta V|$  between the frequencies detected by accumulator 1 and accumulator 2 indicates the reliability of the response  $R$ . Thus we added a self-test module to the Strong RO PUF circuit to automatically test the reliability of the responses generated by the PUF in real time and to generate a reliability flag  $F_i$  for each response, as shown in Fig. 2. That is, when a challenge is input, the BST-RPUF can generate 1-bit response and 1-bit reliability flag. The subsequent circuit constructs the key by detecting the reliability flag and selecting reliable PUF responses.

The generation of the reliability flag  $F_i$  is very simple: the frequencies in the two accumulators are input to the self-test module. The module determines whether the absolute value of the frequency difference is greater than a predefined threshold [22]  $V_T$ , and outputs the reliability flag  $F_i = 1$  when  $|\Delta V|$  is greater than  $V_T$ , otherwise sets the flag  $F_i = 0$ . The subsequent circuit can select the reliable responses in the original PUF responses according to  $F_i$  to significantly reduce the error correction overhead. The robust responses extraction process is shown in Fig. 3.

## 2.3 Anti-modeling attack strategy

Since Strong PUF has a linearized structure, if an attacker can collect a certain number of CRPs, it can model the PUF and accurately predict its responses. Existing anti-modeling attack strategies can be roughly classified into two types: structural nonlinearization and CRPs fuzzification [23]. Combining Strong PUF with Weak PUF can increase the PUF structural complexity [24, 25] and fuzzify the CRPs correspondence to increase the difficulty of modeling attacks, but it requires a highly reliable Weak PUF. An unreliable Weak PUF will lead to poor reliability and uniqueness of the Strong PUF output. In this paper, an extremely reliable anti-fuse PUF [26] is introduced to dissociate the original challenge  $C_i$  with the responses  $x_i$  of the anti-fuse Weak PUF to obtain the new challenge  $C'_i$ ,  $C'_i = C_i \oplus x_i$ . The anti-fuse PUF is a new PUF, after the chip

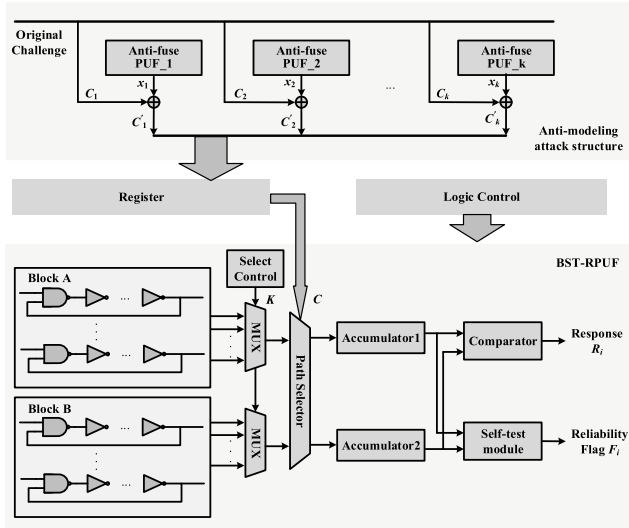


Fig. 4 BST-RPUF circuit resistant to modeling attacks.

is manufactured, it applies an external high voltage to the symmetrical transistors, and uses the inconsistencies in the high voltage tolerance formed by different transistors during the manufacturing process, thereby randomly generating a fixed circuit structure, so that the BER of its output responses is close to 0, which avoids the performance deterioration of the Strong RO PUF due to the unreliability of the Weak PUF problem.

## 2.4 Overall circuit design

The overall circuit design of the Bit Self-Test Strong RO PUF with anti-modeling attack result is shown in Fig. 4. It mainly consists of the anti-modeling attack module, the challenge register module, the BST-RPUF module and the control module. The anti-modeling attack structure and BST-RPUF have been described in the earlier part of the article. The overall workflow of the circuit is as follows: when the original  $N$ -bit challenge signal  $C_i$  is input, it is exclusive or-ed with the Weak PUF to produce the challenge  $C'_i$  and the challenge  $C'_i$  input to the challenge register. The logic control module uses each bit of  $C'_i$  to control the path selector of the BST-RPUF in turn. Then the selector sends  $2N$  RO rings in A block and B block to accumulator 1 and 2 respectively for accumulation counting. This gives the final count values  $F_A$  and  $F_B$  after  $N$  rounds of operations. Finally, the comparator and the self-test module generate a 1-bit response  $R_i$  and a 1-bit reliability flag  $F_i$ , respectively.

## 3. Results

Since the anti-fuse PUF cannot be implemented on FPGA platforms, we have tested the performance and reliability enhancement of the newly proposed BST-RPUF. PUFs require a certain number of samples to accurately evaluate their true characteristics. We designed and implemented 100 16-stage BST-RPUF circuits on 10 Xilinx Artix-7s to obtain enough PUF responses to evaluate BST-RPUFs in terms of uniqueness, uniformity and reliability, and analyzed the resource overhead.

A 16-stage BST-RPUF circuit contains 32 internal ROs

and can generating 65536-bit responses. It should be noted that the RO circuits will have different systematic mismatches when distributed in different areas of the FPGA. In order to avoid the influence of systematic errors, the ROs in the same BST-RPUF circuit are placed together by using scripts to fix the design path and location in Vivado. An RO unit is composed of an odd number of inverters. In this paper, we use 4 Not gates and 1 NAND gate design, where the NAND gate can control whether the RO oscillates or not. The design and implementation of a Not gate or NAND gate on the FPGA consumes 1 LUT, so a total of 5 LUTs are required to implement an RO unit. The selector selects an RO and delivers its oscillation signal to a 32-bit accumulator, which detects the number of high levels within 0.1 ms with an accuracy of 0.01 MHz. The test found that the overall frequency of ROs was in the range of 165.46~228.25 MHz at room temperature (25°C), and the average oscillation frequency is 207.36 MHz. The number of high levels detected in 0.1 ms for 1 RO is between 16546~22825, and 20-bit accumulator can complete the 16 times of accumulation. We use 32-bit accumulator to meet the actual demand, which can prevent data overflow. The uniqueness and uniformity characteristics are tested at room temperature, while the reliability is tested at different temperatures (−20~80°C).

In the BST-RPUF, the threshold  $V_T$  is the minimum frequency difference between the two ROs to produce a reliable response. In other words, if the frequency difference between the two ROs is less than  $V_T$ , the generated response is marked as unreliable because it may be flipped by the environment. Obviously, as the  $V_T$  value increases, the number of responses marked as reliable decreases, but the reliability of the marked robust responses will become higher and higher, so a balance between PUF utilization and reliability needs to be achieved, and the setting of a reasonable threshold is very important.

In our experiments, we tested the frequency difference between accumulators 1 and 2 for all the 65536 cases, which approximately tends to the normal distribution of (0, 21.14 MHz), and the standard deviation  $\delta$  is about 4.6 MHz. According to properties of normal distribution, the test threshold is best set within  $2\delta$ , so we choose the range of the test threshold between 0 and 6 MHz. According to the test results under different thresholds, the most appropriate threshold can be selected.

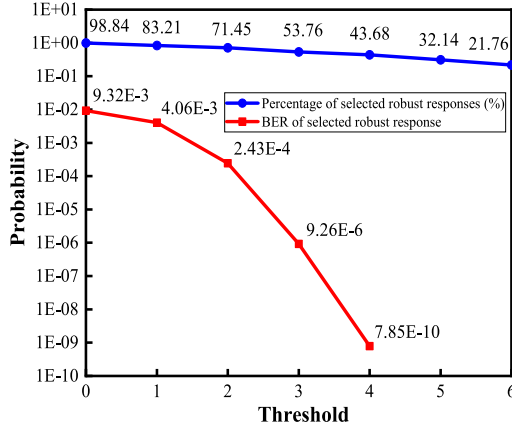
### 1. Reliability

Reliability can be measured by the Bit Error Rate (BER), the probability of error in the output responses of the same PUF circuit for different environments under the same challenge. The calculation method is as Formula (3) [27].

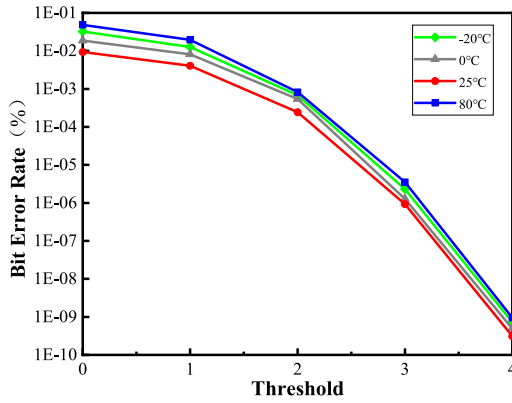
$$BER = 1 - reliability = \frac{1}{k} \sum_{j=1}^k \frac{HD(R_i, R_{i,j})}{n} \times 100\% \quad (3)$$

$R_i$  is the  $n$ -bit response generated by the  $i$ -th PUF inputting a set of challenge  $C$  under normal working conditions (25°C);  $R_{i,j}$  represents the  $j$ -th time of the  $k$  tests performed by varying the temperature.

Fig. 5 shows the ratios of the robust responses and their bit error rates at room temperature with different test thresholds of  $V_T$ . The blue line shows the percentage of reliable flag



**Fig. 5** Robust responses percentage and its bit error rate under different test thresholds.



**Fig. 6** Variation of bit error rate with test threshold for robust responses at different temperatures.

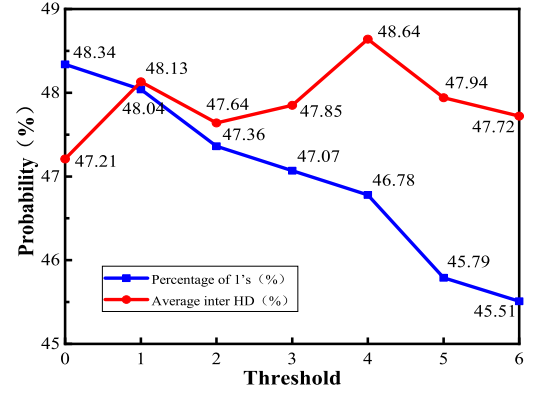
bits of “1” at different test thresholds. It can be seen that as the test threshold increases, the percentage of responses marked as reliable decreases rapidly. That is to say, the number of robust responses decreases rapidly. The red line indicates the reliability of the selected robust responses. As the threshold increases, the BER decreases rapidly, and when the threshold is set above 4, the error rate drops to below  $10^{-9}$ . We also tested the reliability of the picked robust responses at different temperatures, and the results are shown in Fig. 6.

## 2. Uniformity

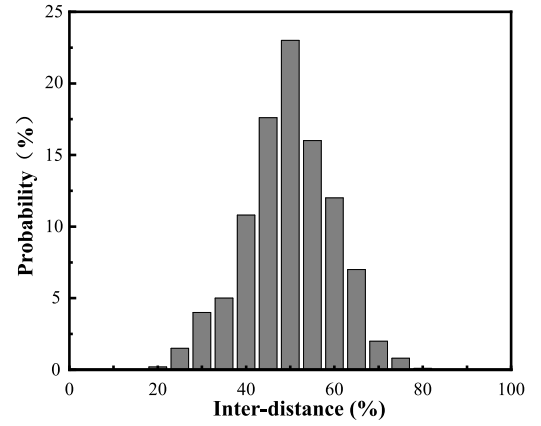
The uniformity describes the distribution of zeros and ones in the PUF output responses. Ideally, the uniformity should be 50%. The BST-RPUF circuit was tested for uniformity at normal temperature (25°C) with different thresholds, and the percentage of “1” in the PUF output responses were analyzed and calculated. It can be seen that as the test threshold increases, the percentage of “1” in the robust responses decreases, and when the threshold is set to 4, the uniformity is about 46.78%. Thus the randomness of the PUF output responses decrease as the threshold increases.

## 3. Uniqueness

Uniqueness indicates the ability of PUFs to distinguish between different devices and implies not only physical unclonability but also mathematical unclonability, and the ideal uniqueness is 50%. It can be estimated by calculating the average Hamming distance [27] with the formula as shown



**Fig. 7** Uniformity and uniqueness of BST-RPUF.



**Fig. 8** Uniqueness of the BST-RPUF circuit.

in (4), where  $m$  is the number of PUF instances, and  $R_j$  and  $R_k$  are the  $n$ -bit responses generated by two different PUF instances  $i$  and  $j$  to the same challenge, respectively.

$$HD = \frac{2}{m \times (m-1)} \sum_{j=1}^{m-1} \sum_{k=j+1}^m \frac{HD(R_j, R_k)}{n} \times 100\% \quad (4)$$

The red line in Fig. 7 shows the average Hamming distance of the selected robust responses with different test thresholds. When the threshold is set to 0, the average inter-chip Hamming distance of the output responses are 47.21%. When the test threshold is gradually increased, the uniqueness of the selected robust responses improves to some extent. When the test threshold is 4, the total inter-chip Hamming distance distribution of the samples obtained by BST-RPUF is shown in Fig. 8, which is very close to the normal distribution. The average Hamming distance is 48.64%, showing that BST-RPUF has a good uniqueness.

## 4. Resource consumption and overall performance

In this experiment, the 16-stage BST-RPUF consumes a total of 362 LUTs and 217 Registers, which can generate 65536 bits of responses. Conventional RO PUF constructed by 32 RO rings consumes about 226 LUTs and 174 Registers, which can generate at most 465 bit responses. According to the reference of conventional RO PUF [28], although our bit self-test Strong RO PUF proposed in this paper increases the resource consumption by about 60%, the number of challenge response pairs is increased from the previous  $(N-1)(N-2)/2$  to  $2^N$ , where  $N$  is the number of steps of PUF, and the larger  $N$  is, the more significant the challenge



**Table I** Comparison with related PUF.

PUF	Type	CRPs ( $N=stages$ )	Reliability	Uniqueness	Uniformity
RO PUF [28]	Weak	$(N-1)(N-2)/2$	0.86%	47.24%	50.56%
TERO [29]	Weak	$N^2$	2.60%	48.50%	50.01%
Arbiter PUF [30]	Strong	$2^N$	3.00%	48.00%	48.00%
BST-RPUF	Strong	$2^N$	10E-9	48.64%	46.78%

response space improvement is. Meanwhile, the BST-RPUF design reduces the bit error rate of the conventional RO PUF from 0.86% to less than  $10^{-9}$ , which is close to 100% reliable. Table I [29, 30] shows the results of comparing BST-RPUF with the latest proposed PUF. Compared with the mainstream PUF schemes, the reliability of the selected robust responses of the BST-RPUF designed in this paper reaches less than  $10^{-9}$  at a reliable responses selection rate of 43.68%, which is much higher than other design schemes. The uniformity and uniqueness are 46.78% and 48.64%, respectively. It can be found that the uniformity of the BST-RPUF has slightly deteriorated compared with other PUFs, this is because the selection of the reliable responses will enlarge the bias of the original responses. However, this slight deterioration will not affect the application of PUF. In addition, a debiasing algorithm can be used to improve the uniformity if necessary.

#### 4. Conclusion

For the problem of limited challenge response pairs and unreliable output responses of traditional RO PUF, this paper designs a Strong RO PUF circuit that is easy to implement in FPGA, which can use dynamic self-test technique to detect the reliability of the responses in real time, and introduces an anti-fuse PUF to construct anti-modeling attack structure.

The FPGA test shows that the reliable output of BST-RPUF can reach a bit error rate of less than  $10^{-9}$ , a uniformity of 46.78%, and a uniqueness of 48.64% with good performance at a test threshold of 4 MHz.

#### Acknowledgments

This work was supported by the National Natural Science Foundation of China (No.62174050) and Hubei Provincial Natural Science Foundation of China (No. 2020CFB814).

#### References

- [1] R. Pappu, *et al.*: “Physical one-way functions,” *Science* **297** (2002) 2026 (DOI: 10.1126/science.1074376).
- [2] K. Turgay: “A true random number generator based on a Chua and RO-PUF: design, implementation and statistical analysis,” *Analog Integr. Circuits Sign. Process.* **102** (2020) 415 (DOI: 10.1007/s10470-019-01474-2).
- [3] N.A. Anagnostopoulos, *et al.*: “Low-cost security for next-generation IoT networks,” *ACM Trans. Internet Technol.* **20** (2020) 1 (DOI: 10.1145/3406280).
- [4] M. Barbareschi, *et al.*: “On the adoption of physically unclonable functions to secure IoT devices,” *IEEE Trans. Ind. Informat.* **17** (2021) 7781 (DOI: 10.1109/TII.2021.3059656).
- [5] Y. Wang, *et al.*: “Lattice PUF: a strong physical unclonable function provably secure against machine learning attacks,” 2020 IEEE Int. Symp. Hardware Oriented Security and Trust (HOST) (2020) 273 (DOI: 10.1109/HOST45689.2020.9300270).
- [6] S. Sutar, *et al.*: “D-PUF: an intrinsically reconfigurable DRAM PUF for device authentication and random number generation,” *ACM Trans. Embed. Comput. Syst.* **17** (2017) 1 (DOI: 10.1145/3105915).
- [7] S.V.S. Avvaru, *et al.*: “Homogeneous and heterogeneous feed-forward XOR physical unclonable functions,” *IEEE Trans. Inf. Forensics Security* **15** (2020) 2485 (DOI: 10.1109/TIFS.2020.2968113).
- [8] S.S. Zalivaka, *et al.*: “Reliable and modeling attack resistant authentication of arbiter PUF in FPGA implementation with trinary quadruple response,” *IEEE Trans. Inform. Forensics Security* **14** (2019) 1109 (DOI: 10.1109/TIFS.2018.2870835).
- [9] C. Gu, *et al.*: “A modeling attack resistant deception technique for securing lightweight-PUF-based authentication,” *IEEE Trans. Computw.-Aided Design* **40** (2020) 1183 (DOI: 10.1109/TCAD.2020.3036807).
- [10] S. Morozov, *et al.*: “An analysis of delay based PUF implementations on FPGA,” *Reconfigurable Computing: Architectures, Tools and Applications* (2010) 382. (DOI: 10.1007/978-3-642-12133-3\_37)
- [11] L. Tebelmann, *et al.*: “EM side-channel analysis of BCH-based error correction for PUF-based key generation,” *ASHES-Proc. Workshop Attacks Solutions Hardw. Secur.* (2017) 43 (DOI: 10.1145/3139324.3139328).
- [12] Z. He, *et al.*: “A reliable strong PUF based on switched-capacitor circuit,” *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.* **26** (2018) 1073 (DOI: 10.1109/tvlsi.2018.2806041).
- [13] M. Hiller, *et al.*: “Review of error correction for PUFs and evaluation on state-of-the-art FPGAs,” *J. Crypt. Eng.* **10** (2020) 229 (DOI: 10.1007/s13389-020-00223-w).
- [14] A. Miller, *et al.*: “A highly reliable SRAM PUF with a capacitive pre-selection mechanism and pre-ECC BER of  $7.4 \times 10^{-10}$ ,” *Proc. Custom Integr. Circuits Conf.* (2019) 1 (DOI: 10.1109/CICC.2019.8780246).
- [15] S. Taneja and M. Alioto: “PUF architecture with run-time adaptation for resilient and energy-efficient key generation via sensor fusion,” *IEEE J. Solid-State Circuits* **56** (2021) 2182 (DOI: 10.1109/JSSC.2021.3050959).
- [16] J. Li, *et al.*: “An efficient and stable composed entropy extraction method for FPGA-based RO PUF,” *IEICE Electron. Express* **17** (2020) 20200350 (DOI: 10.1587/elex.17.20200350).
- [17] T. Ni, *et al.*: “Research on physical unclonable functions circuit based on three dimensional integrated circuit,” *IEICE Electron. Express* **15** (2018) 20180782 (DOI: 10.1587/elex.15.20180782).
- [18] A.S. Chauhan, *et al.*: “Novel randomized placement for FPGA based robust RO PUF with improved uniqueness,” *J. Electron. Testing* **35** (2019) 581 (DOI: 10.1007/s10836-019-05829-5).
- [19] S. Pei, *et al.*: “A low-overhead RO PUF design for Xilinx FPGAs,” *IEICE Electron. Express* **15** (2018) 20180093 (DOI: 10.1587/elex.17.20200350).
- [20] S. Lopez-Buedo, *et al.*: “Dynamically inserting, operating, and eliminating thermal sensors of FPGA-based systems,” *IEEE Trans. Compon. Packag. Technol.* **25** (2002) 561 (DOI: 10.1109/TCAPT.2002.808011).
- [21] G.E. Suh and S. Devadas: “Physical unclonable functions for device authentication and secret key generation,” 44th Proc. Des. Autom. Conf. (2007) 9 (DOI: 10.1109/DAC.2007.375043).
- [22] Z. Chen, *et al.*: “An efficient framework for configurable RO PUF,” *Proc. IEEE Int. Symp. Circuits Syst.* (2016) 742 (DOI: 10.1109/ISCAS.2016.7527347).
- [23] H. Yamada, *et al.*: “Modeling attacks against device authentication using CMOS image sensor PUF,” *IEICE Electron. Express* **18** (2021) 20210058 (DOI: 10.1587/elex.18.20210058).
- [24] S.T.C. Konigsmark, *et al.*: “System-of-pufs: multilevel security for embedded systems,” *Proc. IEEE/ACM/IFIP Int. Conf. Hardw./Softw. Codeign Syst. Synth.* (2014) 1 (DOI: 10.1145/2656075.2656099).
- [25] D.P. Sahoo, *et al.*: “Composite PUF: a new design paradigm for physically unclonable functions on FPGA,” *Proc. IEEE Int. Symp. Hardw. Oriented Secur. Trust, HOST* (2014) 50 (DOI: 10.1109/HST.2014.6855567).
- [26] M. Wu: U.S. Patent 726470 (2017).
- [27] M. Roel: *Physically Unclonable Functions: Constructions, Properties and Applications* (Springer, 2012) 49.
- [28] A. Maiti, *et al.*: *Embedded Systems Design with FPGAs* (Springer, 2011) 245 (DOI: 10.1007/978-1-4614-1362-2\_11).
- [29] A. Cherkaoui, *et al.*: “Design, evaluation and optimization of phys-

ical unclonable functions based on transient effect ring oscillators,”  
IEEE Trans. Inf. Forensics Security **11** (2016) 1291 (DOI: [10.1109/TIFS.2016.2524666](https://doi.org/10.1109/TIFS.2016.2524666)).

- [30] K. Hatti and C. Paramasivam: “Design and implementation of enhanced PUF architecture on FPGA,” J. Lett. Electron. (2020) 1 (DOI: [10.1080/21681724.2020.1859141](https://doi.org/10.1080/21681724.2020.1859141)).