SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

January 2016, Vol. 59 012108:1–012108:12
doi: 10.1007/s11432-015-5287-9

A dynamic PUF anti-aging authentication system based on restrict race code

Bing LI & Shuai CHEN*

Southeast University, School of Integrated Circuit, Nanjing 210000*, China*

Received October 10, 2014; accepted December 9, 2014; published online April 30, 2015

Abstract This paper presents a PUF (physical unclonable functions) authentication mechanism which can combat aging based on restrict race code (RRC). PUF provide a mechanism for identifying an integrated circuit based on the intrinsic variations of physical components uniquely and provide a cheap and secure alternative to random message storage on devices. However, due to its own characteristics, the chip-level PUF circuit reliability is easily affected by environment. The effect of reversible temporal noise on PUF is well studied and has obtained good effect (e.g. temperature, voltage), but sufficient attention has not been given so far to analyze the effect of the irreversible temporal variabilities (e.g. aging on PUF). This paper proposes a dynamic PUF authentication method, which is based on the RRC with two-ring strong characteristics structure. A combination of hardware and software system is used to improve the efficiency of authentication, and in an FPGA (field-programmable gate array)-based SRAM (static random access memory) PUF are used as an experimental object to verify the feasibility of this design. And this system can enhance the authentication system safety from the CVC (characteristic value challenge) randomness test.

Keywords aging, PUF, dynamically maintain, RRC, characteristic value

Citation Li B, Chen S. A dynamic PUF anti-aging authentication system based on restrict race code. Sci China Inf Sci, 2016, 59(1): 012108, doi: 10.1007/s11432-015-5287-9

1 Introduction

During the past 10 years, PUF have become a fixed part of security hardware. All PUF circuits are manufactured by the mismatches between different components and also those global mismatches come from inaccuracies of the production process, so it is inartificial and uncontrollable. For instance, even if two semiconductors are manufactured from the same silicon wafer and mask, wires designed to be the same will probably differ in width by a few nanometers; microscopic differences in the surface of the silicon will introduce almost trivial variations in the curvature of lines. These small differences are undesigneable and unclonable. This feature makes every circuit has an unique fingerprint, so it has extensive application in the field of security.

Based on the characteristics above, a variety of PUF have been implemented now. Figure 1 summarizes some mainstream PUF implementation: Arbiter PUF are based on the mismatches between a pair of identical delay paths [1,2]. Ring oscillators PUF are the result of an array of identically laid-out ring oscillators that produce different output after judgment because of the manufacturing differences [3]. The

* Corresponding author (email: Chenshuai_ic@seu.edu.cn)

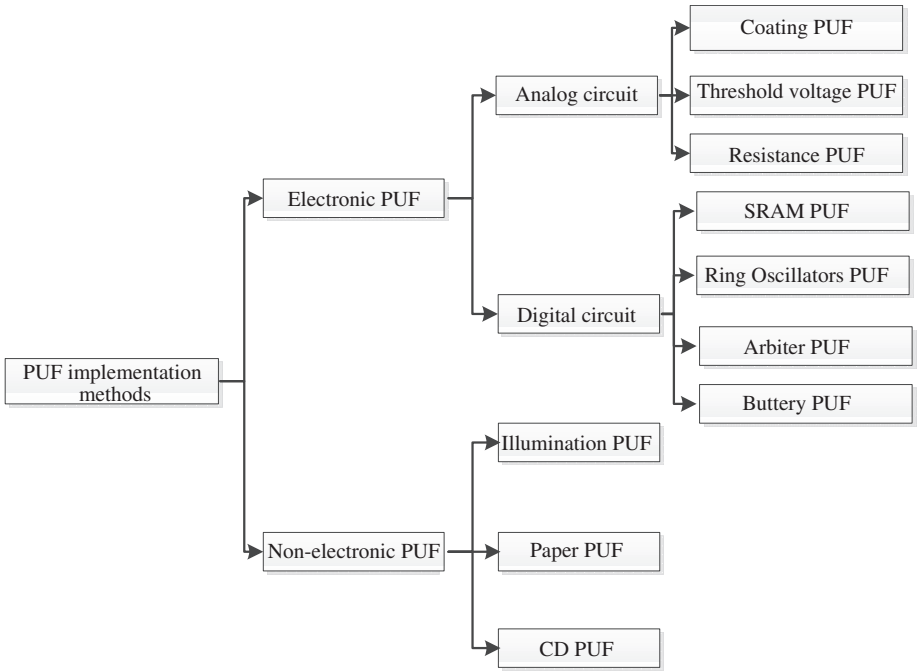


Figure 1 Variety of PUF implementation.

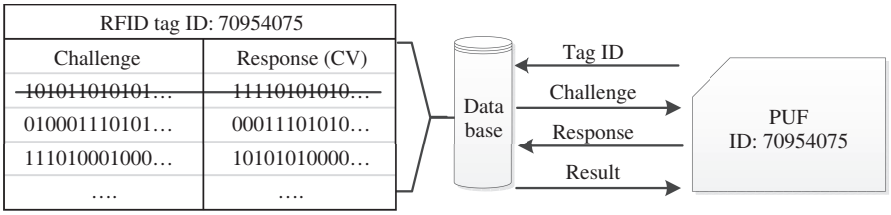


Figure 2 PUF authentication procedure.

features of random startup values of SRAM have been employed to design SRAM PUF [4]. In addition, there are a lot of excellent PUF circuit designs: Latch PUF [5], Trigger PUF [6] and Buffer PUF [7]. Moreover, there are many non-electronic PUF implementation method: Illumination PUF [8], Paper PUF [9] and CD PUF [10].

PUFs have many applications in the field of information security. For instance, it can be used in device authentication, secrete key generation and storage [1]. And RFID (ratio frequency identification) can use the PUF to prevent counterfeiting. Figure 2 is a PUF diagram authentication process. It is a hardware CRP (challenge response pair) mechanism [2].

(1) Establish the database. Based on the CRP mechanism, the PUF circuit can produce chip-unique responses when challenges are applied to it and stored in the database by the way of CRPs.

(2) Authentication. Challenges are randomly selected from the database and incentive to PUF circuit. The sender verifies the PUF response by comparing it to the expected one in the database and delete it after used. Through this comparison results to authenticate its identity.

Although PUF have some unique security advantages and broad application prospect, their application in industry is restricted due to low reliability. All PUF circuits are manufactured by the mismatches between different components and also those global mismatches come from inaccuracies in the production process. But those mismatches produced by very subtle differences are vulnerable to the effects of noise, e.g. circuit aging, temperature, voltage changes, and magnet field. Existing mainstream programs to deal with the problems are as follows: (1) ECC (error correcting code) on chip or external NVM (non-volatile memory) is needed to store the helper data [3]. (2) Parallelization of PUF cells—the control circuit and NVM store is needed [3]. (3) Using software-controlled preselection method to select the stronger characteristic PUF cells [2,3].

All these works mentioned above are emphasis on the errors in PUF responses affected by the reversible temporal variability and do not talk about the effect of deal with irreversible temporal variability. The cause of circuit aging includes mechanisms like NBTI (negative-bias temperature instability), TDDB (temperature-dependent dielectric breakdown), HCI (hot-carrier injection), and electromigration. Abhranil et al. [11]. By fully analyzing the causes as well as the impact of the PUF circuit aging, we can observe that aging makes PUF responses unreliable. With the continuous development of silicon devices (smaller and faster), aging is becoming more prominent. Therefore, it is necessary to put forward a kind of anti-aging method that is applicable to the existing PUF authentication system.

Saro et al. [12] proposed a hardware dynamic PUF whose physical properties are subject to unpredictable changes between uses. But this method increases the circuit complexity and inflexibility. Kirkpatrik et al. [13] performed a software-based techniques method to prevent drift due to aging in PUF authentication process with the assumption that aging alters the PUF response; they did not have an aging testing mechanism, so there will be a lot of useless operation and more complex system. Abhranil et al. [11] proposed an anti-aging method, but it is just for RO (ring oscillators) PUF, not universal. This paper proposed a Software-Hardware system, which is based on the RRC with the two-ring strong characteristics structure, that can do error correction dynamically in the area of PUF authentication database. It has the advantage of a simple structure, overcome the limitations of existing reliability methods, improve the reliability of PUF circuits. The experimental data are based on an SRAM PUF implemented on FPGA.

In this paper, the original performances are in the following respects.

(1) We present the concept of RRC (China invention patent), performed the way as generated by CV (characteristic value) and the two-ring structure and use it as the error detection and correction mechanism to complete the PUF anti-aging function in the authentication process.

(2) We propose the concept of CV of PUF based on RRC. Select the RRC CV as PUF CV for dynamic maintenance, in order to achieve the maintenance of the whole PUF pots in the effect of aging.

(3) The anti-aging complex operations in the authentication are in the area of database through the combination of hardware and software and does not increase the burden of PUF circuit and can be applied to the existing PUF authentication system easily. Take full advantage of the hardware characteristics of parallel computing to improve the certification efficiency.

(4) Due to the circuit aging constantly, here we performed a CV dynamic maintenance authentication system. A dynamic database also increased the resistance to aggressive.

The rest of this paper is organized as follows. Section 2 describes RRC and proposes several important parameters of the PUF test. Section 3 performs the implementation mechanism of authentication. The results of the FPGA experiments and the simulations are presented in Section 4. We conclude the paper in Section 5.

2 Background

In this section, we propose the conception of RRC, analyze the two-ring structure and error detection mechanism and perform several important parameters of the PUF circuit.

2.1 RRC

RRC was designed as a kind of Gray code that can be used to the specific application in digital integrated circuit and has the following features at the beginning: the Hamming distance between two successive code is one (two successive values differ in one bit only) and can be generated by a characteristic value in the way of shift register. However, we found that code combination under the premise of giving up some characteristics of Gray code may lead to some surprising effects and can form series of features. As shown in Figure 3(a), the binary-reflected Gray code list for n bits can be generated recursively from the list for $n-1$ bits by reflecting the list (i.e. listing the entries in reverse order), concatenating the original list with the reversed list, prefixing the entries in the original list with a binary 0, and then prefixing the

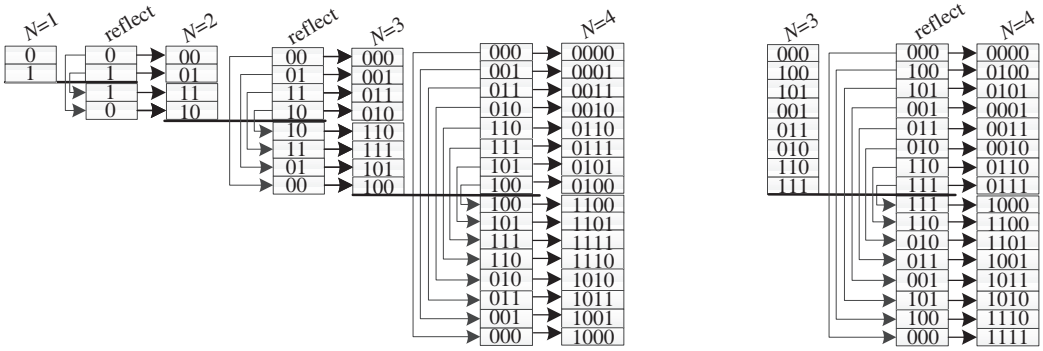


Figure 3 Binary reflection. (a) Gray code; (b) RRC code.

Table 1 RRC and CV

RRC (HEX)	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
BIT0	0	0	1	1	1	0	0	1	1	1	0	0	0	1	1	0
BIT1	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0
BIT2	0	1	1	0	0	0	1	1	1	0	0	1	1	1	0	0
BIT3	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1

entries in the reflected list with a binary 1. Compared with Gray code, the reflect extension mechanism is only applicable to the RRC $n > 3$ bits. So, the characteristic of RRC is different from Grey code, here with a 4bits RRC as an example to illustrate. From the horizontal arrangement of RRC in Table 1, we can find that BIT3–BIT0 arranged from high to low form a hexadecimal cycle and the hamming distance between two successive RRC is one. The BIT0 sequence moving right by 4bits is equal to BIT2, BIT1 moving 4bits to the right is equal to BIT3, and the first eight bits of BIT0–BIT3 is reverse symmetry of the last half. Therefore, the hexadecimal 4bits RRC can be generated by two shift cycle, the first half of BIT0 and the last half of BIT1. Here we define the left sequence of Figure 4 as the characteristic value (CV) and define this generation mechanism as CV generation. This CV is not the only, there are several CVs that can be used, such as the last 8bits of BIT0 and BIT1, the first 8bits of BIT2 and last 8bits of BIT3, etc. The CV generated mechanism is shown in Figure 5: the first half of CV input into SHTR (shift register) CV0, the second half input into SHTR CV1. the CV shift register SHTR CV0 and SHTR CV1 are cycled through inverter D and G, driven in synchronous clock. The seventh bit of SHTR CV0 generate BIT0 of RRC, the seventh bit of SHTR CV1 generate BIT1 of RRC, the third bit of SHTR CV0 generate BIT2 of RRC through inverter D and the third bit of SHTR CV1 generate BIT3 of RRC through inverter G. The gate level forming mechanism circuit is shown in Figure 5(b). SHTR CV0 make up of eight D Flip-Flop,9,10,11,12,13,14,15,16. SHTR CV0 make up of eight D Flip-Flop, 25,26,27,28,29,30,31,32. The eight "and" gate and eight "or" gate consist of the CV setting circuit. If the "Reset" is 0, "and" gate corresponding D flip-flop is been set to 1, "or" gate is been set to "0".

Because of the CV generation mechanism, it forms the double ring structure. As shown in Figure 5, RRC on the right side is a kind of cyclic code, and the CV list on the left side have the cyclic shift relationship between the successive sequence. Thus formed a kind of code has the following features. (1) Two successive values differ in only one bit (the Hamming distance is 1). (2) RRC has the ring structure, which is a kind of cyclic code. (3) The binary-reflected Gray code list for n ($n > 3$) bits can be generated recursively from the list for $n - 1$ bits by reflecting the list (i.e. listing the entries in reverse order), concatenating the original list with the reversed list, prefixing the entries in the original list with a binary 0, and then prefixing the entries in the reflected list with a binary 1. (4) RRC is embodied with the nature of CV generation mechanism. (5) RRC has the two-ring structure.

Among these features, the Hamming distance between adjacent codes and the CV generation mechanism are the basic features, this feature determines its special application. As shown in Figures 4 and

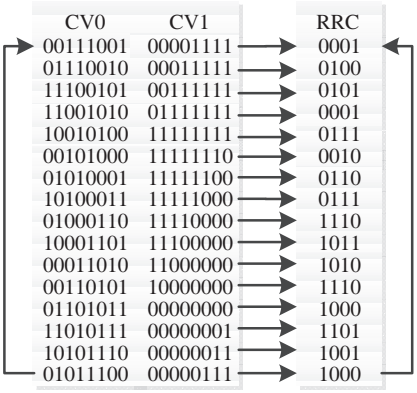
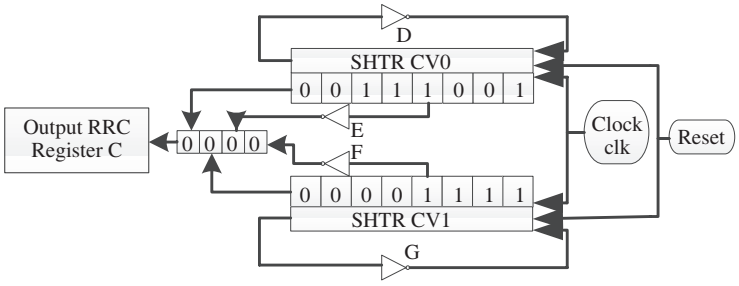
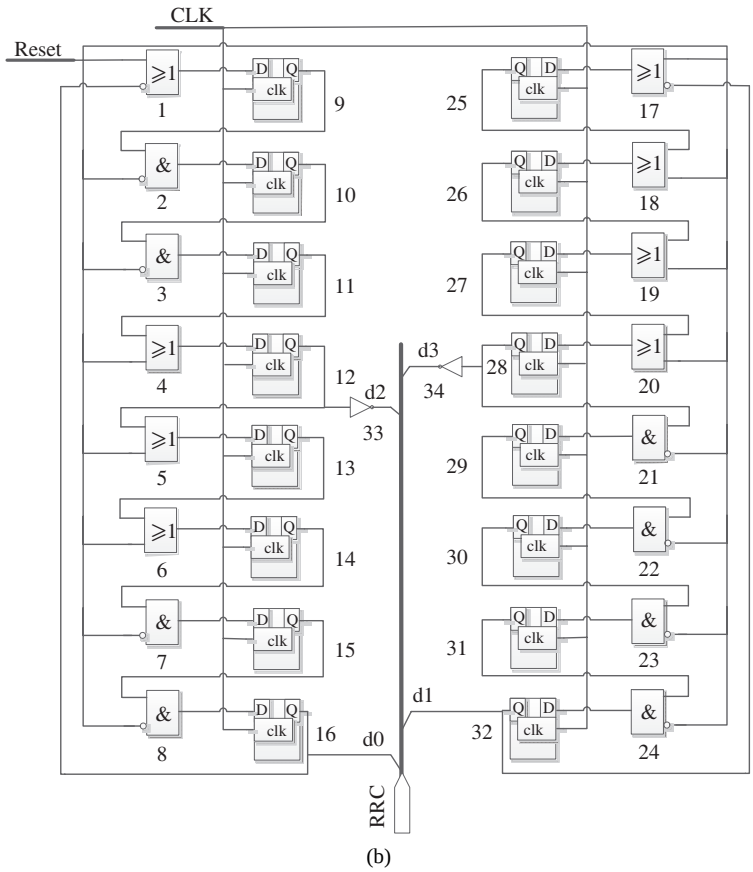


Figure 4 The two ring strcture of RRC.



(a)



(b)

Figure 5 RRC circuit. (a) Schematic; (b) gate level circuit.

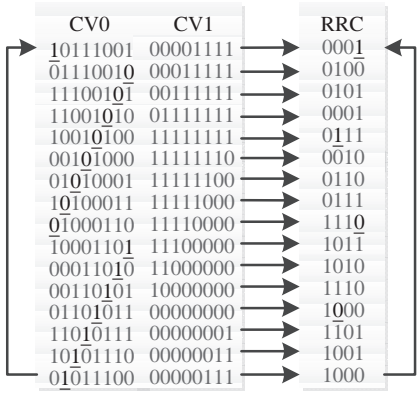


Figure 6 The error node detection.

5, a right CV can generate a correct RRC by the RRC ring circuit, which is in conformity with the intrinsic properties of RRC. Therefore, all the CV can be detected by a fixed detection mechanism or a detection circuit. Choose a sequence of CV in Figure 4 for example. Figure 6 is the error detect process, if the CV = 0011100100001111 errors into CV′ = 1011100100001111, the error is underlined and gradually move due to the cyclic shift of CV sequence. Therefore, the error node detection mechanism has the following features. (1) Due to its special formation mechanism, each node of CV will appear in RRC once after three clock. The error node will appear in the first four RRC sequence and it will occur once after every three RRC sequence, so through detection the first four RRC sequence generated by CV can complete the whole CV detection. (2) The error judgement of RRC sequence according to the hamming distance between adjacent RRC is one. If the first line of RRC sequence is error, the corresponding error node is one of CV0[7], CV0[3], CV1[7], CV1[3]. As shown in Figure 6, the odds of RRC[0] error, the corresponding CV error node is CV0[7], if the RRC[1] error, the corresponding CV error node is CV1[7], if the RRC[2] error, the corresponding error node is CV0[3], if the RRC[3] error, the corresponding error node is CV1[3]. Similarly, if the second line of RRC error, the CV error node corresponding to the error nodes RRC[0], RRC[1], RRC[2], RRC[3] is CV0[6], CV1[6], CV0[6], CV1[6]. If the third row of RRC error, the error nodes RRC[0], RRC[1], RRC[2], RRC[3] corresponding to the CV nods CV0[5], CV1[5], CV0[1], CV1[1]. If the fourth row of RRC error, the error nodes RRC[0], RRC[1], RRC[2], RRC[3] corresponding to the CV nods CV0[4], CV1[4], CV0[0], CV1[0]. This complete the whole CV sequence error detection and rapid positioning.

2.2 Specification parameters

Not all of the FPGA-based SRAM PUF can be used as PUF circuit. To characterize the hardware properties of a PUF, the following parameters are suggested [5]: Mean value, $\mathrm{HD}_{\mathrm{inter}}$ (inter-chip Hamming distance), and $\mathrm{HD}_{\mathrm{intra}}$ (intra-chip Hamming distance).

(1) Mean value. In order to ensure the safety of PUF circuit, the output of it must be predictable. So, the output values "1" and "0" should be distributed equally. Thus the ideal data of mean value should be close to 0.5. Its computation formula is:

$$\text{Mean value} = \frac{1}{n}\sum_{i=1}^{n} X_i. \tag{1}$$

The X_i is the internal node value (0 or 1) of PUF and on the stack and averaging can get its Mean value.

(2) $\mathrm{HD}_{\mathrm{intra}}$. The response of PUF should stay constant within a predefined region of operation. The error rate or bit rate can be measured using the Hamming distance. At an ideal PUF this value is 0.

(3) $\mathrm{HD}_{\mathrm{inter}}$. In order to maintain the security of PUF, it must be independent between cells; else the forecast can not be achieved. So, test this property by the parameter of $\mathrm{HD}_{\mathrm{inter}}$. The theoretical value is 50%.

3 The dynamic maintains of CV

In this section, we present the ideas for implementation and solutions of the dynamic anti-aging system based on RRC.

3.1 The implementation ideas

In the process of PUF authentication, the CRPs send some challenges to the PUF circuit and the PUF circuit returns the response to this challenge. The sender verifies this response by comparing it to the expected one in the database. The expected data in the database are called CRPs in paper. Those CRPs are established and stored in the database in a secured environment and are deleted after being used and are no longer updated before deleting completely (shown in Figure 2). But the accumulation of circuit aging dynamically changes the circuit characteristics. Abhranil et al. [11] pointed out that the effects of aging in PUF circuits are carried out gradually. So, the dynamic maintenance of the database is an effective way to solve this problem. Because the PUF circuit is through its own characteristics for the identity authentication, under the premise of authentication correction, searching PUF aging node in the circuit, recording and updating the database, making the aging process also as a characteristic of PUF circuit, can be an effective way to avoid the effects of aging.

Although each PUF circuit has a large number of CRPs, maintaining them dynamically is unrealistic, e.g. there are over 10^{10} CRPs (16 bits) in a 128 bits SRAM PUF. The solution proposed in this paper is to only maintain the strong characteristic values. The CV of RRC with a strong digital loop feature is simple in structure and has a fast and accurate maintenance advantage, meets the requirement of PUF and has strong CV dynamic maintenance. The CV in the paper is RRC CV. Every nodes of PUF have a unique address, through the monitoring mechanism to find the aging nodes and in accordance with the unique address to global change can obtain a good anti-aging effect. Shown in Table 1 is a CV of RRC.

In this paper, the experimental model is established on an FPGA-based SRAM PUF to observe the implementability. In a safe environment, large amounts of CRPs are stored in the database. Then, retrieval CV sequence in the database by RRC circuit names the corresponding challenge "characteristic value challenge (CVC)". Due to the two ring structure of RRC, as shown in Figure 4, the CV of RRC is not the only sequence but an arbitrary sequence in the shift process that can be used as characteristic values. That are 16 16bits characteristic values. For PUF circuit, each CV can be made by multiple of PUF cells combination, so a CV can be generated by multiple CVCs (one column in Figure 7). Giving each PUF node a unique address, according to the principle of address not to repeat, in accordance to the order of Figure 5 to choose CVC can generate a CVC ring (the starting point is arbitrary). Using the CVC ring as motivation, sent to the PUF circuit in turn, the response can generate a RRC CV ring, giving input as the former eight bits and last eight bits to the two shift register of RRC circuit can generate the correct RRC ring. Repeating the above process can generate a CVC database like Figure 4, the CVC database containing multiple CVC ring (because of the circular structure, the starting point of the CVC ring can be arbitrary, as long as in accordance with the order of ring). The response of CVC can complete the error node detection through the hamming distance of forming RRC by a RRC circuit. So the CVC database only needs to record the challenges and need not record the response sequence. The order of CVC ring actually contains the correct response values. As the CV database, the CVC ring can be deleted after being used to keep the randomicity and security.

As shown in Figure 7, the first line of 16 CVs (as shown in Figure 4) can form a complete CV ring. The underside part is its CVC. Suppose the number of CV1–CV16 is n_1–n_{16}, then the PUF can generate the number of CVC ring for:

$$N = C_{16}^{1} \prod_{i=1}^{16} n_i, \tag{2}$$

C_{16}^{1} is the starting sequence of CVC ring in choosing and it can be any between CV1–CV16, and the second part of the formula is the multiplicative of n_1–n_{16}.

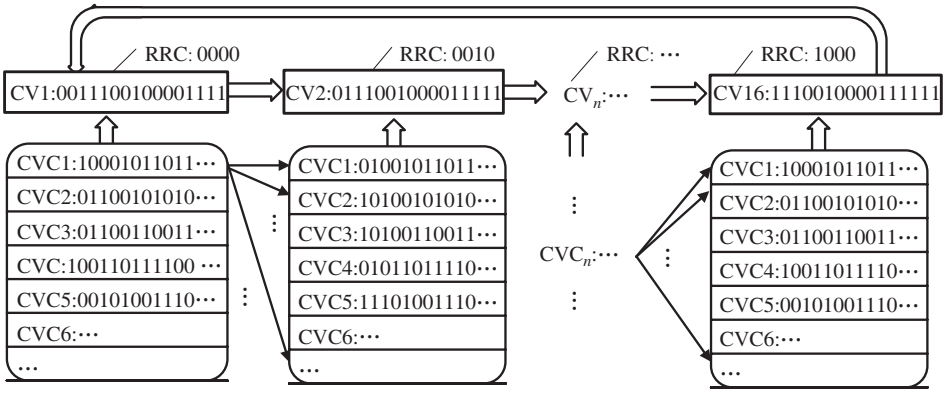


Figure 7 CVC ring.

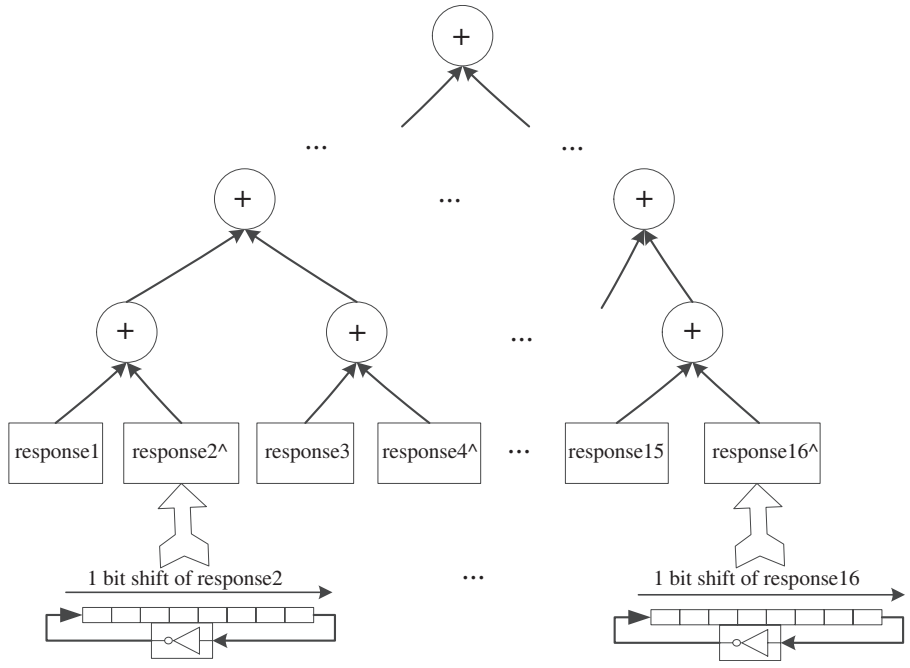


Figure 8 XOR tree.

3.2 XOR tree

As shown in Figure 5, by RRC generate order, the adjacent CV has the relationship of reverse shift. For example, CV1 = 00111001, CV2 = 01110011, if CV2 is reverse shifted by an inverter, as shown in Figure 8, CV2′ = 00111001, which is same as CV1. The study proposed in this paper joins an aging detection mechanism by XOR tree. The XOR tree is a full binary tree in which all leaves have the same depth or same level, and in which every parent has two children. As shown in Figure 8, input the sequence under detected into leaves. Through detect the root node can find the wrong leaves by the "1" path up to done. Input the wrong leaf content into RRC circuit and after four clock shifts, the generated RRC can position the error nodes rapidly.

3.3 The dynamic authentication process

In the authentication process, a claimed ID is verified by the system in Figure 2 and a new CRP is necessary for each authentication procedure. If authentication is correct, then begin the anti-aging process (as shown in Figure 9):

(1) Randomly select a CVC ring from CVC database, send it to PUF according to the fixed order and put the response in the XOR tree as shown in Figure 8. Here it should be noted that the even number

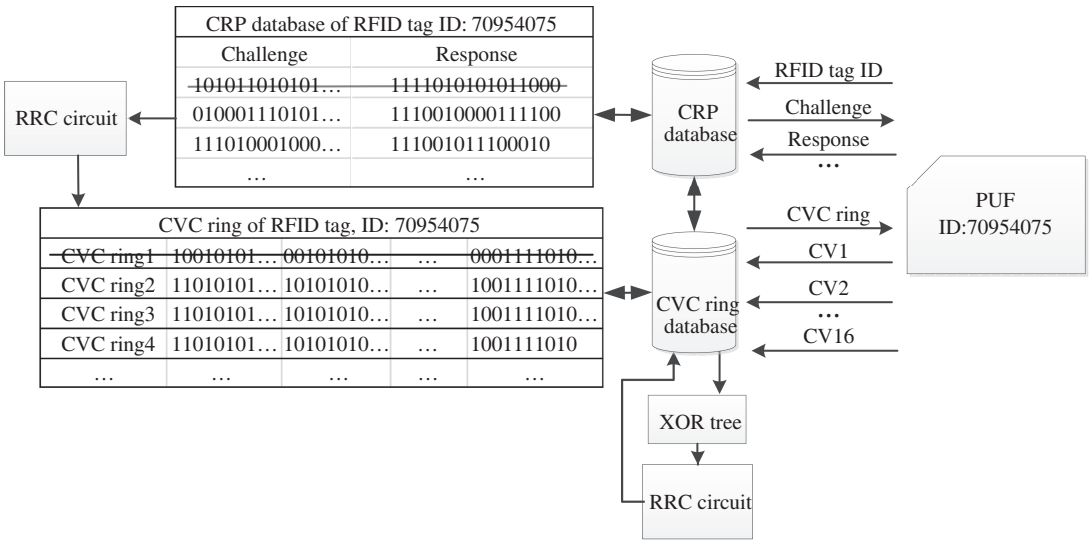


Figure 9 The dynamic maintain process.

of response should be in counter clock shift one bit into response. Since the relationship of the correct response (CV) is shifted in order, as long as the odd response and even response is the same, a XOR binary tree calculation can show the accuracy of all the CVC rings' response.

(2) If the operation results of XOR tree is "1", the binary tree can quickly retrieve the wrong leaves. Send the wrong leaves to RRC circuit and detect the closure of the generated RRC ring and record the error nodes' address. The whole testing process is implemented in the hardware so several groups can be computed in parallel.

(3) According to the results above, modify the CRP and CVC database. Since all the PUF nodes have a separate address and correspond to a unique PUF cell, the modification is complete for all the CRPs.

In the project, the digits number of RRC can be selected flexible according to the actual needs. In the same way, you can choose the number of detected CVC rings in one authentication anti-aging process. The more the number of CVC rings, the coverage for the PUF cells is higher and the aging resistance is stronger, but follows a longer authentication time.From a security perspective, compared with the static database, a dynamic one is more difficult to break. CVC ring is actually a PUF address coding, therefore, having an exponential number of CVC rings to random selection guarantees its safety. Moreover, with the increase of digits number of RRC, the CV rings increase exponentially.

4 Results

In this section, we present the results of tests based on the theory above, with eight FPGA-based 128 bits SRAM PUF as experimental objects and numbered 1–8 respectively. The tests are divided into three parts: (1) key PUF parameters tests, judging the reliability of the test results; (2) the number of CVC in PUF circuit, calculating the number of CVC ring; (3) the cover rate of CVC for PUF cells.

4.1 Key PUF parameters tests

Through a series of experiments, the probability to be used as a PUF circuit was studied. According to the evaluation criteria, the test results are as follows.

(1) Mean value. As shown in Figure 10(a), the test results are close to the theoretical value of 0.5.

(2) HD_{inter}. The measured HD_{inter} of the eight test chips are shown in Figure 10(b) (order NO. 1 FPGA as the test basis). Results are close to the theoretical value of 50%.

(3) HD_{intra}. The maximum HD_{intra} at room temperature is 1.81%. When the temperature increased to 80, the HD_{intra} is 15.7%.

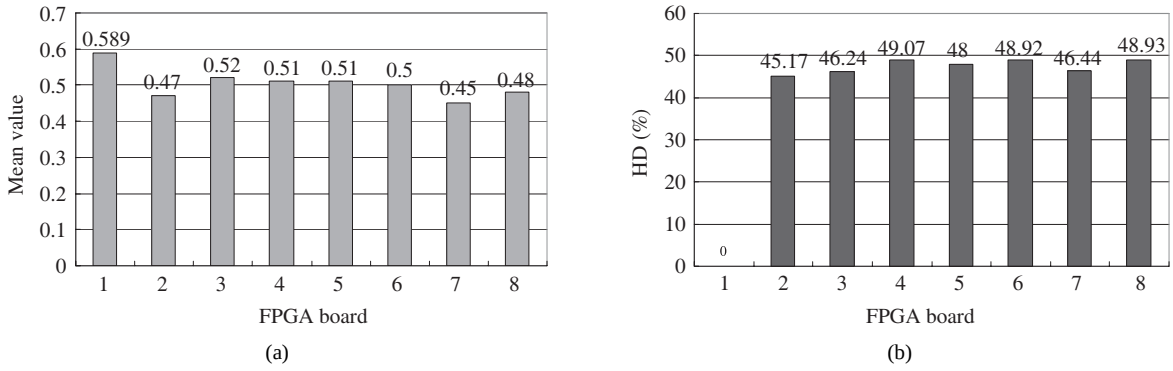


Figure 10 (a) Mean value and (b) Hamming distance of different FPGA board.

Table 2 The number of CVC in PUF

CV/FPGA	1	2	3	4	5	6	7	8
CV1: 0011100100001111	49	57	57	58	65	60	59	61
CV2: 0111001100011111	50	56	58	59	62	58	60	61
CV3: 1110011100111111	49	44	40	38	35	36	41	36
CV4: 1100111001111111	50	45	41	39	36	37	38	37
CV5: 1001110011111110	51	45	42	40	37	38	39	30
CV6: 0011100011111110	49	59	57	59	61	60	59	61
CV7: 0111000111111100	50	56	57	60	62	61	60	62
CV8: 1110001111111000	51	43	43	40	33	40	41	37
CV9: 1100011011110000	43	43	44	39	34	37	41	38
CV10: 1000110011100000	42	40	45	40	32	38	39	38
CV11: 0001100011000000	48	56	56	57	60	59	58	63
CV12: 0011000110000000	49	57	57	58	61	60	57	64
CV13: 0110001100000000	49	55	58	59	60	61	57	62
CV14: 1100011100000001	41	43	37	36	34	41	38	37
CV15: 1000111000000011	42	44	38	37	35	42	37	29
CV16: 0001110000000111	48	56	58	58	63	63	55	60

The above experimental results show that the key parameters fluctuate in a reliable range, so the SRAM PUF tests at room temperature are reliable.

4.2 CVC ring tests

Select the CV in Table 1 as the experimental object and number the CV in Table 2 from CV1 to CV16. Read all the PUF cell values out and detect the number of CV according to the address sequence by a "C program". The test results are shown in Table 2. Due to the PUF unique cells address, every CV found in the tests correspond to many CVC. Each column in Table 2 is the CV number of SRAM PUF numbered from 1 to 16, corresponding to n_1–n_{16} in formula (2). Calculated using formula (2), it can be found that the CV ring number in each PUF (1–8) is more than 10^{27}. Thus, there are enough CVC rings to be selected in PUF circuit to ensure its randomness and keep a strong anti-replay attack resistance.

4.3 Coverage tests

The anti-aging system mentioned above is not for all the PUF cells, but only for some strong characteristic cells. Therefore, the coverage tests are a necessary part in the experiment. As shown in Figure 4, because of the ring structure of RRC and CV, the starting point of CVC ring is random. No matter from which CV (one sequence of CVC ring) it is begun, it forms a correct RRC (has the same features). All the 16 CVs coverage of PUF circuits are tested here. A high coverage here means the CV has good dispersion

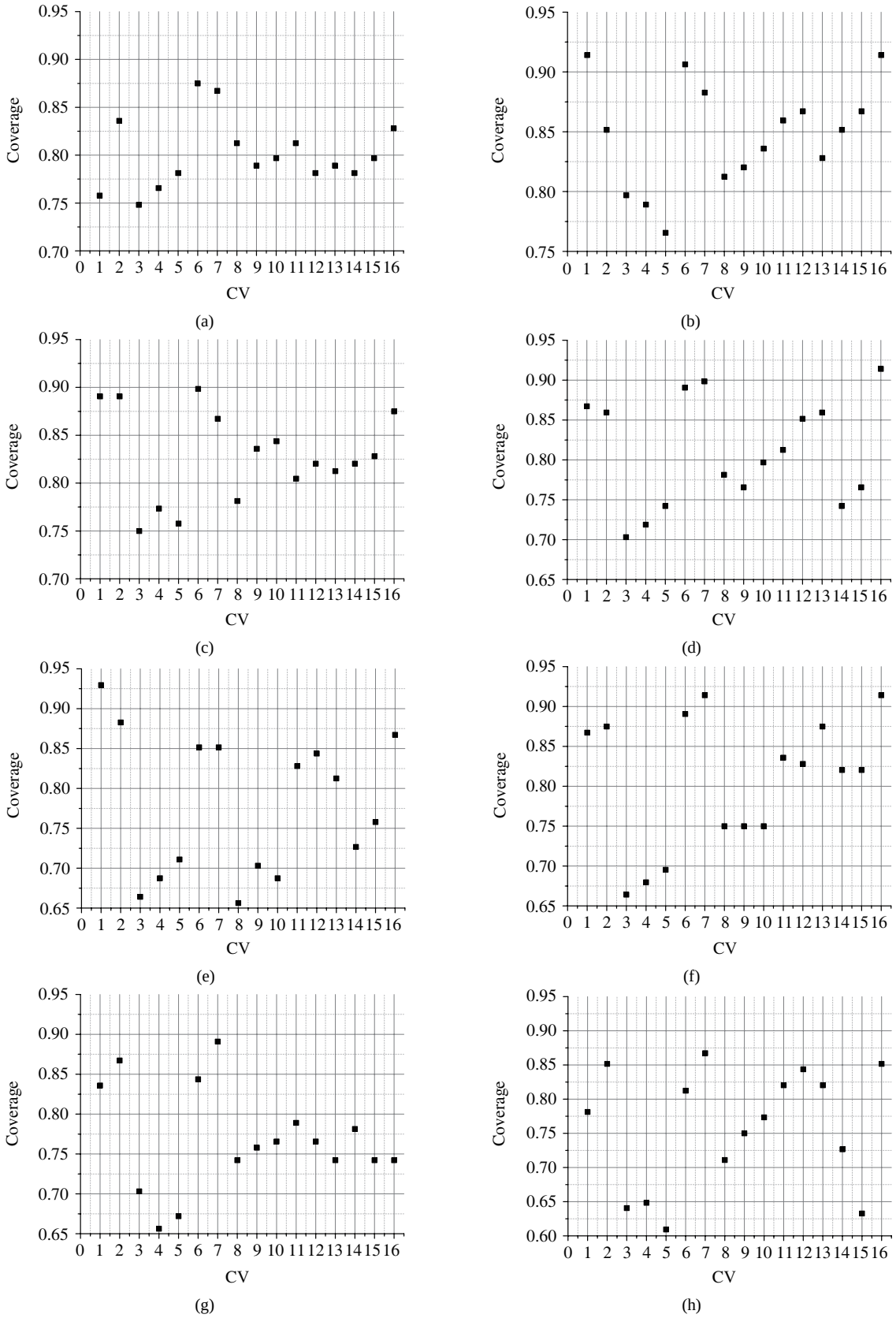


Figure 11 The 8 SRAM-PUF coverage tests of CVC in PUF. (a) FPGA1; (b) FPGA2; (c) FPGA3; (d) FPGA4; (e) FPGA5; (f) FPGA6; (g) FPGA7; (h) FPGA8.

in PUF circuit, and with the principles of address not being repeated, the formation of CVC can have a higher coverage.

The SRAM PUF test results are shown in Figure 11. It can be seen in Figure 4 that the coverage of 16 CVs in PUF are spread over 70%–90% (80.2% on average). So in PUF circuit, CV has better average distribution. To ensure that the CVC has a good dispersion,using less CVC ring can realize a large coverage. Relative to the method of all nodes dynamic maintenance, this system is simpler and plays better to the advantage of hardware circuit for digital signal processing.

5 Conclusion

The reliability of PUF goes down with circuit aging. This paper analyses the existing PUF circuit reliability improving methods. It briefly introduces the concept and mechanism of RRC. Based on this research, the paper proposes a dynamic anti-aging system based on RRC two-ring structure. The system is based on the existing PUF authentication system, searching CV in database. According to the circular order of RRC form CVC ring, the sequence in CVC ring as far as possible to meet the principle of address not repeat to have a better coverage of PUF cell. In anti-aging process, a certain number of CVC ring is selected and input into PUF. To complete the aging test, the response is returned after XOR tree and RRC circuit to detect the error nodes. The hardware circuit is used to realize the algorithm of higher duplication and is implemented in the area of database. Experimental results based on a group of FPGA-based SRAM PUF show that over 10^{27} CVC ring in PUF and these CVC in PUF circuit have very high coverage (80.2% on average). The author has achieved not less than 4 bits RRC error detection mechanism and a part of hardware circuit design. Different bits of RRC will cause different effects on its performance and due to space limitations it will be extended in a future article.

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Lim D, Lee J W, Gassend B, et al. Extracting secret keys from integrated circuits. IEEE Trans VLSI Syst, 2005, 13: 1200–1205

2 Lee J W, Lim D, Gassend B, et al. A technique to build a secret key in integrated circuits for identification and authentication application. In: Proceedings of the Symposium on VLSI Circuits, Honolulu, 2004. 176–159

3 Yin C E D, Gang Q. Maximizing RO PUF's secret extraction. In: Proceedings of IEEE Symposium on Hardware-Oriented Security and Trust, Anaheim, 2010. 100–105

4 Holcomb D E, Burleson W P, Fu K, et al. Initial SRAM state as a fingerprint and source of true random numbers for RFID tags. IEEE Trans Comput, 2007, 58: 11–13

5 Su Y, Holleman J, Otis B. A 1.6pj/bit 96% stable chip-ID generating circuit using process variations. In: Proceedings of IEEE International Solid-State Circuits Conference, San Francisco, 2007. 406–611

6 van der Leest V, Schrijen G J, Handschuh H, et al. Hardware intrinsic security from D flip-flops. In: Proceedings of the 5th ACM Workshop on Scalable Trusted Computing, New York, 2010. 53–62

7 Suzuki D, Shimizu K. The glitch puf: a new delay-puf architecture exploiting glitch shapes. In: Proceedings of Crypt-Ographic Hardware and Embedded Systems, Berlin, 2010. 366–382

8 Ravikanth P. Physical One-way Functions. Dissertation for the Doctoral Degree. Boston: Massachusetts Institute of Technology, 2001

9 Bulens P, Standaert F, Quisquater J J. How to strongly link data and its medium: the paper case. IET Inform Secur, 2010, 4: 125–136

10 Ghaith H, Aykutlu, Berk S. CDs have fingerprints too. In: Proceedings of the 11th International Workshop on Cryptographic Hardware and Embedded Systems, Berlin, 2009. 348–362

11 Maiti A, Schaumont P. The impact of aging on a physical unclonable function. IEEE Trans VLSI Syst, 2013, 99: 1854–1864

12 Meguerdichian S, Potkonjak M. Device aging-based physical unclonable functions. In: Proceedings of the 48th ACM/EDAC/IEEE Design Automation Conference, New York, 2011. 288–289

13 Kirkpatrick M S, Bertino E. Software techniques to combat drift in PUF-based authentication systems. In: Proceedings of Workshop on Secure Component and System Identification, Cologne, 2010