Journal of Electronics and Information Science (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2023.080605
ISSN 2371-9524 Vol. 8 Num. 6

A Uniformity Optimization Method for Physically Unclonable Functions of Arbiters

Austin Zuo

Beijing OCAHS International Academy, No. 88, Nanzhuang Ying, Cuicun Town, Changping District, Beijing, 100005, China
Austin2006@126.com

Keywords: Arbiter Physical Unclonable Function (PUF); Reliability; Uniformity; Delay asymmetry

Abstract: In this paper, the design principle of the Arbiter Physical Unclonable Function (APUF) based on the arbiter is studied, the existing problems are analyzed, and the problem of its delay asymmetry is studied. This paper proposes two methods that can change the uniformity of PUF, by changing the delay on each path to make the uniformity of PUF closer to 50%. The improvement of PUF uniformity can greatly increase the security of PUF, making information storage more vulnerable to external attacks.

1. Introduction uniformity

With the continuous development of human society and the emergence of various high technologies, the Internet of Things (IOT) technology has seen unprecedented development. Globally, the number of IOT terminals is growing rapidly, and tens of thousands of sensors are embedded in all corners of society. Its applications have touched every aspect of our daily lives, such as transportation infrastructure, logistics tracking, unmanned aerial vehicles, smart homes, and so on.

However, IoT devices have weak digital processing and storage capabilities, and chips and firmware are limited to provide secure data and identity authentication. Globally, IoT terminal security incidents have occurred frequently, and some miscreants have taken advantage of the flaws or vulnerabilities of IoT terminals to attack, maliciously control, steal data, and tamper with data, which has had a serious impact on communication networks and application services. According to SAMSeamless Network's "2021 Forms of IoT Security" report, after analyzing anonymized data from 132 million active IoT devices and 730,000 secure networks, it is estimated that a billion IoT devices have been attacked.

Traditional cryptographic algorithms store keys in non-volatile memory (OTP, EEPROM or Flash) and consume excessive computational resources, which are not applicable to lightweight IoT devices. To solve this problem, Physical unclonable Function (PUF) provides a low-cost lightweight encryption method for storing keys securely.

A PUF is a "digital fingerprint" used as a unique identifier for semiconductor devices (e.g. microprocessors). Based on various unpredictable random differences in the IC manufacturing process (e.g., threshold voltage, channel length), PUF can generate a unique ID for each chip. semiconductor device manufacturing differences are at the nanometer level. The endogenous

characteristics of the PUF are difficult to predict and impossible to control. The PUF is able to resist physical attacks, including reverse engineering, and is characterized by being difficult to clone. At the same time, PUFs do not need to be stored in media such as EEPROM, which also reduces the cost.

Section 2 introduces the concept, characteristics and classification of PUF, Section 3 analyzes the advantages and problems of arbiter-based PUF, and Section 4 proposes a method and implementation process to improve the uniformity of PUF.

2. Background

2.1 PUF

A PUF[1] is a physical entity with independent input (challenge) and output (response) properties. A PUF generates a unique response r = f(c) for any challenge vector c. PUFs use Chanllenge Response Pairs (CRPs) to extract manufacturing differences and thus use the endogenous properties for scenarios such as secret key storage and secure authentication. An ideal PUF should have the following properties:

(1) Easy to compute: for any challenge c, the PUF is able to generate the corresponding r = f(c) in finite time;

(2) Repeatability: the ability to repeatedly obtain r = f(c) for a given challenge c;

(3) Unclonable: there does not exist another PUF function g such that g = f ;

(4) Unpredictable: for a known set of CRPs $U = \{(c_i, r_i) \mid r_i = f(c_i)\}$, it is difficult to predict the corresponding response for a new challenge c_{i+1} , it is difficult to predict the corresponding response $r_{i+1} = f(c_{i+1}), (c_{i+1}, r_{i+1}) \notin U$

(5) Unidirectionality: there are n-bit challenges c for which, for the corresponding r = f(c), there exists no polynomial p that satisfies the formula p(f (c)) = c. The significance of this property for PUFs is that it is difficult for an attacker to reverse-compute the challenge c for the corresponding response r known.

2.2 PUF Taxonomy

With the concept of optical PUF being proposed, PUF technology has undergone more than two decades of development, during which researchers have proposed many different types of PUFs. according to the different methods of realization, PUFs are classified into two main categories, namely, electrical PUFs and non-electrical PUFs[2] as Fig. 1.

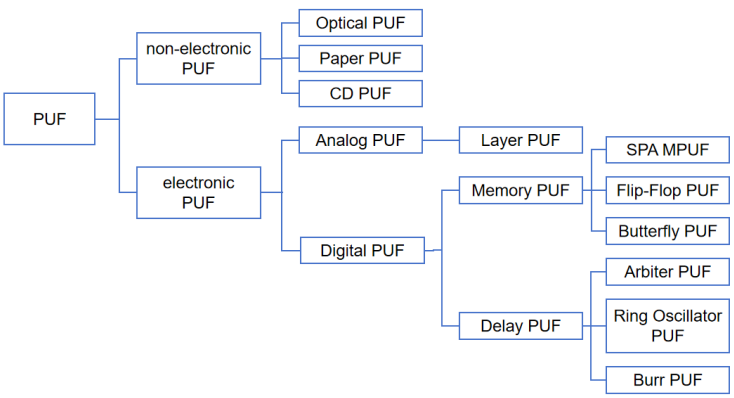

Figure 1: PUF Classificaiton

The PUF is embedded in each device during manufacturing and a subset of its CRPs are registered after the device is manufactured. These CRPs are then used to authenticate the device during operation. By avoiding storing signatures in device memory, PUFs enhance the security of the integrated circuits in which they are embedded. Based on the number of challeng response pairs, PUFs are categorized into two types, i.e., weak PUFs and strong PUFs [3]. The former consists of PUFs containing a finite set of CRPs (e.g., ring oscillator PUFs), which are mainly used for random key generation for cryptographic modules or for IC metrology to counter piracy, overproduction attacks, etc. On the other hand, strong PUFs realize a large number of CRPs and are suitable for device authentication and integrity checking.

2.3 Evaluation Matrics for PUF

Uniformity[4] refers to how evenly the proportion of "0s" and "1s" in a PUF response is distributed. For PUF responses that are unpredictable and random, ideally the probability of a "1" should be equal to the probability of a "0". We define uniformity of an m-bit PUF identifieras the percentage Hamming Weight(HW) of the m-bit identifier:

$$Uniformity(i) = \frac{1}{m} \times HW(R_i \times 100\%)$$

where Ri is the m-bit response on chip i and HW(Ri) is the number of '1's in the response. This value should be close to 50%.

Uniqueness[4] indicates how easy it is to distinguish one PUF instance from another. Uniqueness is a measure of inter-chip differences and therefore should be considered for each pair of chips. It can be averaged to compute the Hamming Distance (HD) fraction between responses generated by the same challenge from different chips as Fig. 2.

$$Uniqueness = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=k+1}^{k} \frac{HD(R_i, R_j)}{m} \times 100\%$$

where k is the number of chips and R_i and R_j denote the m-bit responses generated on different chips i and j ($i \neq j$), respectively. This value should be close to 50% in order to ensure the uniqueness of the PUF across devices.

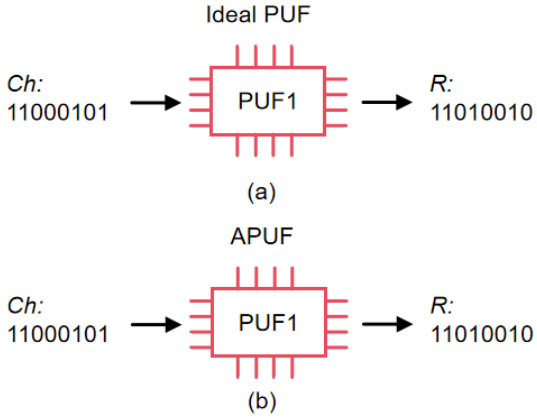

Figure 2: Uniformity

2.4 Related Works

The first arbiter PUF was proposed by Lim et al. in 2004 [5], which extracts the key information by comparing the speed of delay between two identical transmission paths with symmetric structure. To solve the problem of inefficient output response of arbiter PUF, Yoshikawa [9] designed four identical delay circuits on an integrated circuit chip, so that the same signal is transmitted over four delay circuits, which greatly improves the efficiency of arbiter PUF.

In order to improve the unpredictability and reliability of the arbiter PUF and to enhance the safety of the PUF, Takanori [6] proposed a new dual arbiter PUF to enhance the unpredictability of the PUF.

The rapid development of PUF technology has also aroused the scientific research interest of researchers and related scholars in the field of cryptography and hardware security area in China.In 2010, Zhang Junqin et al. from Shanghai Jiaotong University [7] proposed an improved scheme for signal acquisition and delay arbitration through triggers on the basis of the traditional arbiter PUF, which has a certain degree of improvement for the uniformity of the PUF output.

In 2018, Wang Zheng's team at CAS [8] proposed a current mirror array combining PUF and machine learning algorithms by implementing seven different challenge activation and response readout schemes in order to realize different weak and strong PUF functions within the same current mirror array.

3. Design of the Proposed Arbiter PUF

3.1 Circuit Analysis

The specific circuit structure of APUF[10] is shown in Fig. 3, which consists of two units containing n signal communication paths. They have the same input (Transition) and the outputs are connected to the signal input of the arbiter D flip-flop and the input of the clock.

According to the APUF circuit structure, the APUF design consists of several alternate logic gates, with the input of each alternate logic gate coming from the output of the previous logic gate. Each two alternate logic gates share a challenge signal. The specific input-output relationship is as follows: when a rising edge signal is generated at the input, the response bit is 1, if this signal arrives first at the input D. If such a signal arrives first at the clock signal terminal (clock), the response bit is 0. The path length of the upper and lower paths depends on the input of the challenge signal.

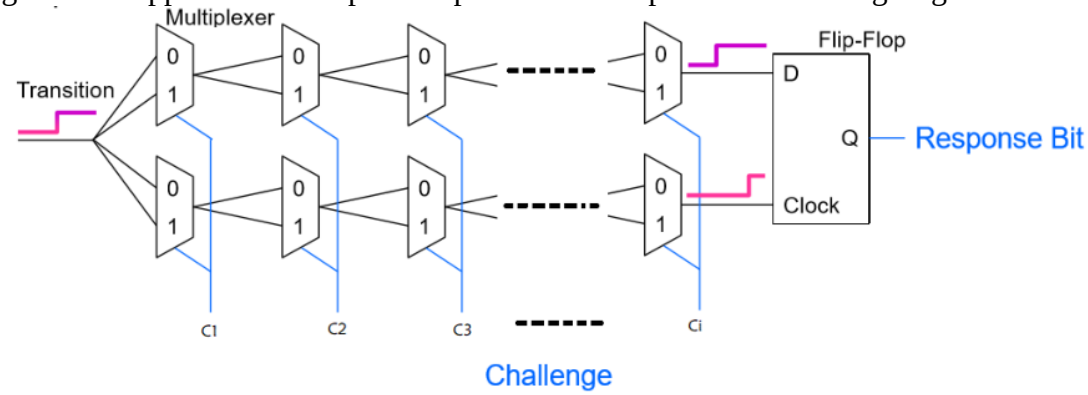

Figure 3: APUF Circuit Structure

Fig. 4 is based on Fig. 3 with the delay time data for the circuits added. Assuming a given four-bit challenge (0101), the delay data for the upper and lower circuits are marked on the circuit, and the red line segments are the circuits through which the signal actually passes, by calculating the delay of the upper circuit to be 3.96, and the delay of the lower circuit to be 3.92, the signal arrives at the

clock signal end first, and the final response bit is 0. By looking at the individual delay data, the delay of the upper path is greater than that of the lower path as a whole, and the response is skewed to 0, which severely affects the uniformity. At the same time, if the delay difference between the two paths is large, environmental influences (e.g., temperature and voltage) also make it difficult to change the corresponding output, and reliability is also affected.

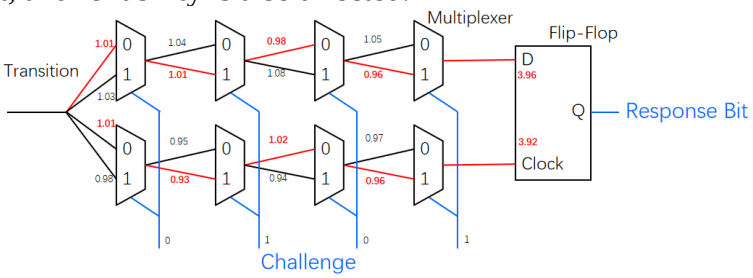

Figure 4: An example of APUF with latency data

3.2 Improved Circuitry

In order to solve the problem of APUF uniformity and reliability, this paper designs an improved circuit diagram as shown in Fig. 5, which is divided into two parts.

(1) Path segments controlled by chanllege

The first half of the circuit diagram is a traditional APUF circuit, with the values of the chanllege controlling the direction of the signal.

(2) Path segments for adjusting response distributions

Our model adds an adjustable time delay circuit buffer after the conventional APUF circuit. In adjustable module, all the upper and lower logic gates are controlled by different challenge signals, so when the challenge signal is 1, its time delay inevitably increases due to the extra buffer on that path.

Based on the output result, determine whether the signal reaches the D port or the CLOCK port first and invert it. If the signal reaches the D port first, it means that the path delay of the D port is less than the path delay of the clock. In this case, the adjustment can be made in two ways.

(1) Increasing the challenge signal input to the adjustable buffer on the D-port path increases the delay on the D-port path, thus stabilizing the delay on the upper and lower paths.Reduce the challenge signal input to the adjustable buffer on the Clock path in order to decrease the delay on the Clock path and achieve stability in the delays of both the D-path and the Clock path. Make the same adjustment when the signal reaches the clock first.

When the delay of one path is larger than that of the other due to system deviation (e.g., process deviation), the appropriate number of buffers can be inserted into the path whose time delay is often smaller so as to balance the time delay size of these two paths, ensuring that the probability of response to both 0 and 1 is similar, namely improving the randomness in chip.

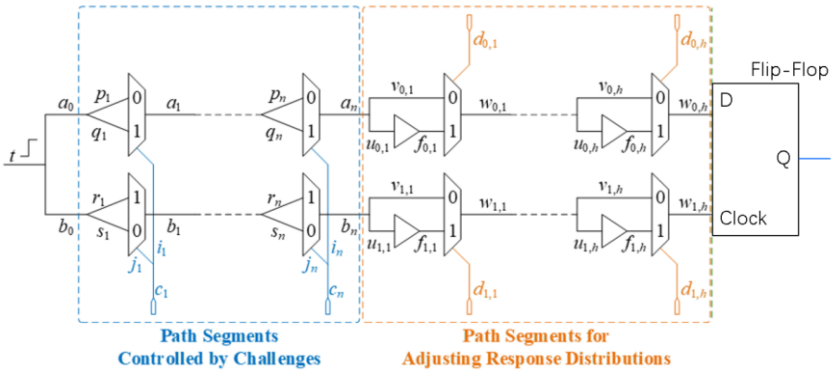

Figure 5: Adjusting APUF Circuit

3.3 Algorithm Adjustment

The self-tuning module analyzes the intra-slice uniformity of the PUF for a specific tuning signal value and further generates a more appropriate challenge signal value to achieve a higher uniformity of the PUF. To evaluate the intra-slice uniformity of the PUF for a particular challenge signal, the tuning module collects n_c single-bit responses generated by the tunable arbiter PUF module to n_c random challenges. The number of responses with a value of 1 is noted as n_1, the n_1/n_c can be used as an evaluation parameter for the on-chip uniformity. The closer this value is to 50%, the better the intra-chip uniformity is.

First, set a preset value pt as the desired uniformity. Measure the original delay of the circuit. Calculate the proportion of 1, subtract 50% from the result, and take the absolute value to compare it with the preset value. Finally, compare the calculated value with the preset value. If it is less than the preset value, the circuit passes the uniformity test; if the calculated percentage is greater than the preset value, the circuit passes the uniformity test. If the calculated ratio is greater than the preset value, the circuit needs to be adjusted. (Figure 6)

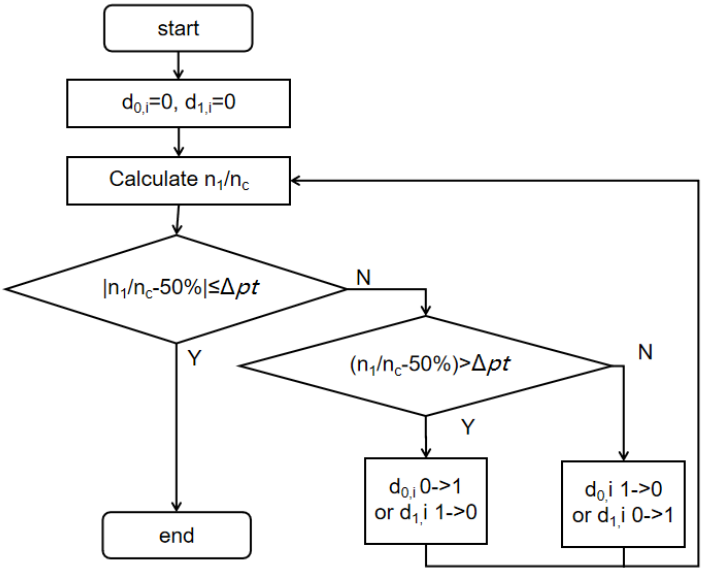

Figure 6: Work flow of adjusting APUF

4. Experimental Results and Validation

To evaluate the characteristics of the proposed design, we used Vivado provided by Xilinx to simulate the modified APUF circuit with 32-bit challenge and tested 4 PUFs for 1000 times each.

The experimental results of the uniformity of the improved APUF are shown in Table 1.

Table 1: Experimental results on uniformity of improved APUF %

PUF serial number	uniformity
1	48.94
2	51.95
3	47.40
4	50.10
average value	49.60
variance (statistics)	3.68

The experimental results of the uniqueness of the improved APUF are shown in Table 2.

Table 2: Experimental results on uniformity of improved APUF %

PUF serial number	uniqueness
1	46.57
2	48.62
3	44.87
4	49.34
average value	47.35
variance (statistics)	4.11

From the above data analysis it can be concluded that the improved APUF has good uniformity and uniqueness and achieves the desired tuning effect.

5. Conclusion

In just 20 years of development, PUF has been widely used in many fields, and has a broad development prospect and application space. Aiming at the problem that the uniformity and uniqueness of traditional APUF are not satisfactory, this paper investigates how to improve the uniformity of arbiter PUF to make the information stored in the chip more secure. The arbiter PUF has two symmetric paths, and the uniformity of the arbiter PUF is improved by increasing or decreasing the delay on the paths to make the delay of the two paths approximately equal. The uniqueness and uniformity of the proposed APUF is close to 50%, which is very close to the ideal APUF.

References

[1] Pappu R, Recht B, Taylor J, et al. Physical one-way functions [J]. Science, 297(5589), 2002: 2026-2030.

[2] Gassend B, Clarke D, Van Dijk M, et al. Silicon physical random functions [C], Proc. Of the 9th ACM conference on Computer and communications security, 2002: 148-160.

[3] Ganji Fatemeh. [T-Labs Series in Telecommunication Services] On the Learnability of Physically Unclonable Functions [J]. 10.1007/978-3-319-76717-8(2018).

[4] Maiti, Abhranil & Gunreddy, Vikash & Schaumont, Patrick,"A Systematic Method to Evaluate and Compare the Performance of Physical Unclonable Functions," IACR Cryptology ePrint Archive, 2011,pp.657, doi: 10.1007/978-1-4614-1362-2_11.

[5] Lim D,Lee JW,Gassend B,et al. 2005. Extracting secret keys from integrated secret keys from integrated circuits[J]. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 13(10): 1200-1205.

[6] Takanori M, Dai Y, Mitsugu I, et al. 2015. A New Arbiter PUF for Enhancing Unpredictability on FPGA[J]. The Scientific World Journal,2015(2015):1-13.
[7] Zhang Junqin, Gu Dawu, Hou Fangyong. Design and Analysis of Improved Arbiter PUF [J]. Computer Engineering, 2010(3): 3
[8] Wang Z., Chen Y., Patil A., et al. Current Mirror Array: A Novel Circuit Topology for Combining Physical Unclonable Function and Machine Learning [J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2018, 65(4): 1314-1326.
[9] Yoshikawa M, Naruse A. 2012. Multiplexing aware arbiter physical unclonable function[C]//IEEE International Conference on Information Reuse & Integration. Las Vegas, NV, USA, IEEE, 1-4.
[10] B. Gassend, D. Clarke, M. V. Dijk, and S. Devadas. Silicon Physical Random Functions. In: Proceedings of the 9th ACM conference on Computer and communications security, ACM pp. 148–160, 2002. Available at: https://dl.acm.org/citation.cfm?id=586132.