Theoretical Analysis of Delay-based PUFs and Design Strategies for Improvement

Yale Wang[1], Chenghua Wang[1], Chongyan Gu[2], Yijun Cui[1], Maire O'Neill[2], Weiqiang Liu[1]
[1]*College of Electronic and Information Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing, China*
[2]*Centre for Secure Information Technologies, Queen's University Belfast, Belfast, UK*
E-mails: {yalewang, chwang, yijun.cui, liuweiqiang}@nuaa.edu.cn, {c.gu, m.oneill}@ecit.qub.ac.uk

***Abstract*—Delay-based physical unclonable function (PUF) designs use the random delay differences in circuit transmission to extract response. In the existing PUF designs, there are few studies on investigating the link between process variation and PUF performance. The experimental data can reflect the performance of the new design to a certain extent, but lack of theoretical analysis to provide thorough information. In this paper, a theoretical model for delay-based PUF designs is proposed. An analysis of the delay-based PUF improvements by existing design strategies is also investigated. Moreover, a guidance to develop and improve future delay-based PUF designs using the proposed theoretical model is also given in this paper.**

***Index Terms*—Delay-based PUF, theoretical analysis, improvement strategies, performances**

I. Introduction

Physical Unclonable Function (PUF) [1], which can extract uncontrollable manufacturing differences and generate signals from circuits, is a promising security primitive for key generation and authentication for IoT devices. According to the different implementation principles [2], PUF designs include delay-based PUFs and memory-based PUFs. Delay-based PUFs [3] extract the response signal by utilizing the random delay differences in circuit transmission. Arbiter PUF (APUF, also called MUX-based PUF) and RO PUF are two typical delay-based PUFs. The delay elements in the PUF circuit can be modeled by Gaussian distribution.

The performance of a PUF design can be evaluated by PUF metrics [4], *e.g.*, uniqueness and reliability. Uniqueness reflects the independence of the response generated by the same type of chips. Reliability represents the stability of the response of a PUF design over different environmental conditions. The effect of the selection of arbitrator elements and gate sizes on APUF delay variations has been analyzed in [5]. However, the underlying parameters were regarded as fixed values, and adjustments were needed at higher levels. For example, the introduction of feed-forward structure [6] in the original APUF structure can increase uniqueness. However, it is difficult to improve both uniqueness and reliability for the PUF architecture due to constraints involved in the adjustment strategies. Therefore, the design of strong PUF often entails tradeoffs between reliability and unpredictability (including uniqueness and randomness) [7]. Post-processing techniques can be utilized to alleviate or eliminate the constraints for PUF designs. For example, using error correction code [8] can improve reliability/stability without affecting uniqueness. Specific challenge choosing mechanism [9] can improve uniqueness and reliability simultaneously. Since the unstable outputs are concentrated in the case of two comparison paths with similar delay, this mechanism can filter out the challenges for this situation and control the ratio of outputs 0 or 1 to improve both uniqueness and reliability [7], [10].

In order to perform theoretical analysis, mathematical models for APUF [13] and RO PUF [11], [12] have been studied. In [13], mathematical models for the relationship between uniqueness and reliability for an APUF was proposed. The influence of the number of stages on the performance of an APUF was analyzed. However, these theoretical analyses are rarely applied to guide the design of PUF. Most PUF designs are implemented directly in hardware, and the performance of the design cannot be known until it is tested by experiments, which is inefficient and time consuming.

In this paper, the impact of new structures on PUF performances are analyzed before implementation. The differences of this paper with the existing works are as follows. Firstly, the outputs of APUF and RO PUF are modeled in the same form. Secondly, the impact of some design strategies on the performance of PUFs is analyzed. Hence, the performance of new PUF designs can be estimated before experimental implementations. An explanations of the constraints in structure design is provided and the reason that post-processing strategies can break through these constraints is also revealed.

II. Related Works

For an APUF, one bit output is determined by N switch components [13]:

$$R_A = sign(r_N) = \begin{cases} 1, r_N \geq \Delta_{Arb} \\ 0, r_N < \Delta_{Arb} \end{cases} \quad (1)$$

where Δ_{Arb} is a constant caused by skew effect of arbiter, and r_N is the delay difference of two comparison paths under a fixed challenge:

$$r_N = \sum_{i=1}^{N} (-1)^{C'_i} \Delta_i \quad (2)$$

This work has been supported by NSFC (No. 61771239 and 61871216), and the Six Talent Peaks Project in Jiangsu Province (2018-XYDXX-009).

978-1-7281-0397-6/19/$31.00 ©2019 IEEE

where $C'_i = \oplus_{j=i+1}^{N} C_j$ and $C'_N = 0$. Assume that in one component, the delay difference Δ_i between top and bottom follow a Gaussian distribution:

$$\Delta_i = D_i^t - D_i^b \sim N(0, 2\sigma_s^2) \tag{3}$$

and we can get $r_N \sim N(0, \sigma_A^2)$, where $\sigma_A^2 = 2N\sigma_s^2$.

According to [11], in an original RO PUF, the delay of an inverter is:

$$D_i = D_{avg} + D_{pv} + D_{noise} \tag{4}$$

where D_{avg} is the average delay of the RO and is a constant, D_{pv} is the delay component due to the process variation, and $D_{pv} \sim N(0, \sigma_{pv}^2)$. D_{noise} is the delay component due to the noise factor, and $D_{noise} \sim N(0, \sigma_{noise}^2)$. The delay of RO composed of N inverters is:

$$D_{RO} = \sum_{i=1}^{N} (D_{avg} + D_{pv} + D_{noise}) \tag{5}$$

Then we can get $D_{RO} \sim N(\mu_{RO}, \sigma_{RO}^2)$, where $\mu_{RO} = ND_{avg}$, and $\sigma_{RO}^2 = N(\sigma_{pv}^2 + \sigma_{noise}^2)$.

According to the assumption on the components, the delay difference of APUF and the delay of single RO in RO PUF also obey Gaussian distribution. To verify this, the simulation results of 100-stage original APUFs were statistically calculated in [13], and Gaussian fitting curve was performed on the distribution. [11] measured and counted the frequencies of ROs of different types implemented in hardware. [12] also performed a Gauss fitting curve for the RO frequency distribution under fixed measurement time. The statistical results and Gaussian fitting curves verify the correctness of delay-based PUF output model and reflect the characteristics of its output distribution.

Let $P\left(R = 0/1\right)$ represent the output probability of 0/1. Based on the establishment of the output model, Lao *et al.* [13] derived the main two performance metrics of APUF:

$$Uniqueness = 1 - |4P(R=1)(1-P(R=1)) - 1| \tag{6}$$

$$Reliability = 1 - P_{intra} \tag{7}$$

where the ideal values of uniqueness and reliability are 1, and P_{intra} is the flipping probability of intra-chip responses, and in an original APUF,

$$\begin{aligned} P_{intra} &= P\left[sign(\sum_{i=1}^{N}(s_i+n_i)-\Delta_{Arb}) \neq sign(\sum_{i=1}^{N}(s_i+n'_i)-\Delta_{Arb})\right] \\ &= \frac{1}{2} - \frac{1}{\pi} arctan(\sqrt{\frac{\sigma_s^4}{2\sigma_s^2\sigma_n^2 + \sigma_n^4}}) \\ &\quad - \frac{\Delta_{Arb}}{\sqrt{2\pi N\sigma_s^2}}\left(1 - \frac{2}{\pi}\sqrt{\frac{\sigma_s^2}{\sigma_s^2+\sigma_n^2}} arctan(\sqrt{\frac{\sigma_s^2}{\sigma_s^2+\sigma_n^2}})\right) \end{aligned} \tag{8}$$

The analysis of this paper is mainly about uniqueness and reliability.

III. Theoretical Performance Analysis

As mentioned above, the delay of a single RO in original RO PUF obeys Gaussian distribution, but the oscillation frequency F_{RO} is inversely proportional to its delay:

$$F_{RO} = \frac{\Delta T}{D_{RO}} \tag{9}$$

where ΔT is the measurement time of the counter in RO PUF. Strictly speaking, F_{RO} does not obey the Gaussian distribution as D_{RO} does. However, ΔT is much larger than D_{RO}, and $D_{RO} > 0$. This makes the distribution of F_{RO} close to a Gaussian distribution. This is also the reason why the Gaussian fitting curve of the RO frequency distribution in [12] does not completely coincide.

Considering that the output of RO PUF is also a comparison of two ROs, and

$$R_{RO} = \begin{cases} 1, \Delta F \geq 0 \\ 0, \Delta F < 0 \end{cases} \tag{10}$$

where ΔF is the frequency difference of the two ROs:

$$\Delta F = \frac{\Delta T}{D_{RO1}} - \frac{\Delta T}{D_{RO2}} = \Delta T\left(\frac{1}{D_{RO1}} - \frac{1}{D_{RO2}}\right) \tag{11}$$

Then we can get

$$\begin{aligned} P\left(R_{RO} = 1\right) &= P\left(\Delta F \geq 0\right) \\ &= P\left(D_{RO1} \leq D_{RO2}\right) \end{aligned} \tag{12}$$

and

$$R_{RO} = \begin{cases} 1, \Delta D \leq 0 \\ 0, \Delta D > 0 \end{cases} \tag{13}$$

where ΔD is the delay difference of two ROs, $\Delta D = D_{RO1} - D_{RO2}$. According to the assumed delay distribution of RO, $D_{RO} \sim N(\mu_{RO}, \sigma_{RO}^2)$ we can get $\Delta D \sim N(\mu_{\Delta D}, \sigma_{\Delta D}^2)$, where $\sigma_{\Delta D}^2 = 2N(\sigma_{pv}^2 + \sigma_{noise}^2)$. Ideally, $\mu_{\Delta D} = \Delta D_{avg} = 0$. However, the different locations of the RO in the hardware will cause the difference in the mean value of the frequency distribution [14]. This means that the mean values of their delay distributions is different, so here we set ΔD_{avg} to be a constant.

This output model of RO PUF is similar to APUF, meaning that their outputs are identical to their delay differences of the respective internal paths. This allows the performance analysis on both PUFs. PUF structures that are difficult to model are often considered to have better security [15], but they are only supported by experimental data. In this paper we only discuss the PUF that can be modeled.

A. Uniqueness

By observing the output model of the delay-based PUF, we can find that the existence of Δ_{Arb} in APUF and ΔD_{avg} in RO PUF is the main cause of $P\left(R = 1\right) \neq P\left(R = 0\right)$. This leads to a certain difference between the uniqueness and its ideal value of 1. At the same time, the variation of σ^2 ($2N\sigma_s^2$ of APUF, $2N(\sigma_{pv}^2 + \sigma_{noise}^2)$ of RO PUF output distribution can also change the output probability. Therefore, in order to improve the uniqueness of delay-based PUF, it is necessary to make some adjustments on the basis of the original PUF structure to reduce the influence of Δ_{Arb} / ΔD_{avg}, or increase the variance of its output distribution, so that $P\left(R=1\right)$ is closer to 0.5.

B. Reliability

Reliability in PUF can be seen as its ability to resist noise. If noise does not easily change the output of PUF, then it has a good reliability. The area near the decision threshold ($x = \Delta_{Arb}$ of APUF, $x = \Delta D_{avg}$ of RO PUF) is unstable. In this area, the output of PUF is easily affected by noise and jumps to the other side of the decision threshold, and metastable state may occur, resulting in an unpredictable output. From the above reliability function of APUF in Section II, it can be found that the larger the ratio of the delay distribution variance to the noise distribution variance ($\frac{\sigma_s^4}{2\sigma_s^2\sigma_n^2+\sigma_n^4}$, specifically) of the single stage in the APUF, the closer its reliability is to the ideal value of 1. The existence of Δ_{Arb} has an impact on the reliability of APUF. From the last item of the P_{intra} function, Δ_{Arb} provides a good contribution to the reliability of the APUF. However as $\left(1-\frac{2}{\pi}\sqrt{\frac{\sigma_s^2}{\sigma_s^2+\sigma_n^2}}arctan(\sqrt{\frac{\sigma_s^2}{\sigma_s^2+\sigma_n^2}})\right)$ is close to zero, this effect is tiny [13].

From the above analysis, it is necessary to increase the impact of Δ_{Arb} on APUF output in order to increase reliability. Similarly, the impact of ΔD_{avg} needs to be increased in RO PUF to improve reliability. This is exactly the opposite of the measure to improve uniqueness. That is to say, the improvement strategy of the PUF structure will inevitably lead to a slight decrease in reliability while improving the uniqueness.

C. Constraints on Structure Design

The structure design of delay-based PUF can only affect its performance by changing the two parameters of the output Gaussian distribution. This gives it two constraints:

- Since the methods of increasing uniqueness and reliability are completely opposite, this makes it hard to simultaneously improve the two metrics.
- Since the unstable area is usually near the mean value of output distribution, this makes it difficult to eliminate the unstable area completely, and leads to a certain gap between the reliability and its ideal value.

The analysis in the next section will verify and explain the existence of these constraints.

IV. Design Strategies

A. Structure Design Strategies

As mentioned above, since reliability is not that easy to improve, the existing work on PUF structure design focuses on how to improve uniqueness. In the original APUF structure, reducing or eliminating the skew effect of arbiter (changing the value of Δ_{Arb}) is undoubtedly the most direct and effective way to improve the uniqueness, but this is limited by the inherent performance of the arbiter and does not seem to be easy to implement. Therefore, many researchers have made some adjustments to reduce the negative impact of Δ_{Arb} on uniqueness. As shown in Fig. 1, assume that $x = \Delta_{Arb}$ is on the right side of y-axis. If the new adjustment design can increase the σ^2, it means that the distribution curve is flatter. The area S_Δ of the shadow part represents the increment of $P\left(R=1\right)$, and

$$S_\Delta = \int_0^{\Delta_{Arb}} \left(\frac{exp(\frac{-x^2}{2\sigma_A^2})}{\sqrt{2\pi\sigma_A^2}} - \frac{exp(\frac{-x^2}{2\sigma_A'^2})}{\sqrt{2\pi\sigma_A'^2}}\right)dx \tag{14}$$

in the new output,

$$P'\left(R=1\right) = P\left(R=1\right) + S_\Delta \tag{15}$$

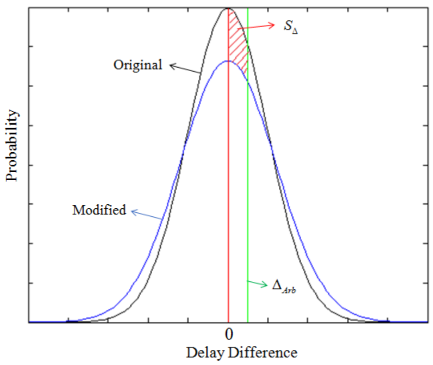

Fig. 1. Probability density function of the delay difference in APUF.

The uniqueness of the new output is:

$$\begin{aligned} Uniqueness' &= 1 - \left|4P'(R=1)(1-P'(R=1)) - 1\right| \\ &= 4P'\left(R=1\right)\left(1-P'\left(R=1\right)\right) \end{aligned} \tag{16}$$

For convenience, let $P_1{}' = P'\left(R=1\right), P_1 = P\left(R=1\right)$, then we can get

$$\begin{aligned} &Uniqueness' - Uniqueness \\ &= 4P'{}_1\left(1-P'{}_1\right) - 4P_1\left(1-P_1\right) \\ &= 4S_\Delta\left(1-2P'{}_1+S_\Delta\right) \end{aligned} \tag{17}$$

As $S_\Delta > 0$ and $0 < P\left(R=1\right) < P'\left(R=1\right) < 0.5$, $Uniqueness' - Uniqueness > 0$ is obtained. This proves that the uniqueness can be improved if the variance of output delay can be increased by adjusting the structure of delay-based PUF. In the existing structure designs, the introduction of feed-forward and its variants [13] in APUF improves the uniqueness in this way.

Unlike the Δ_{Arb} in APUF, in RO PUF, ΔD_{avg} can be changed by structural adjustments. According to the RO PUF model, the closer the mean value of the RO delay (frequency), the smaller the ΔD_{avg} will be. So the improvement of RO PUF is mainly to find a way to reduce ΔD_{avg}.

As shown in Fig. 2, assume that $x = \Delta D_{avg}$ is on the right side of y-axis, and

$$P(R=0) = \frac{1}{2} - S_D \tag{18}$$

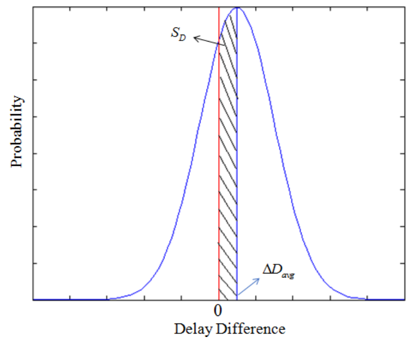

Fig. 2. Probability density function of the delay difference in RO PUF.

where

$$S_D = \int_0^{\Delta D_{avg}} \frac{exp(\frac{-x^2}{2\sigma_{RO}^2})}{\sqrt{2\pi\sigma_{RO}^2}} dx \tag{19}$$

represents the area of the shadow part. If the new adjustment design can decrease ΔD_{avg}, it means that the shadow area S_D will be smaller. According to the function of uniqueness:

$$\begin{aligned} Uniqueness &= 1 - |4P(R=1)(1-P(R=1)) - 1| \\ &= 4P(R=0)(1-P(R=0)) \\ &= 1 - 4S_D^2 \end{aligned} \tag{20}$$

This means that the uniqueness of RO PUF will increase as S_D decreases, and proves that the uniqueness can be improved by decreasing ΔD_{avg}. In [14], the authors conducted a large number of comparative tests on different types of RO (with different mean value of frequency distribution). Their experiments also showed that the closer the frequency distribution was, the better the output uniqueness would be. According to the correlation between the frequency of RO and position on the chip, in [16], the researchers chose the ROs which are closer to the relative position (with smaller ΔD_{avg}) to combine, and achieved a higher uniqueness of RO PUF. We can get these experimental results in [14], [16] by theoretical analysis.

In RO PUF, its main drawback is low hardware utilization. The original RO PUF can only get one output by comparing two ROs. Therefore, some researchers have proposed the design of CRO PUF [16] based on the idea of different paths allocated by challenges in APUF. It greatly increaces the number of response bits. This approach is also used to improve performance, similar to [16], by configuring ROs with close frequencies to enhance uniqueness. In addition, in [17], the authors also select ROs with large frequency differences for comparison to achieve higher reliability. This method of improving reliability is contrary to the method of improving uniqueness, further confirming our proposed constraints on structure design.

Based on the original APUF and RO PUF, we can build an output model for the new structure design. Then by analyzing the changes of the output distribution, we can understand the performance changes of the new design, before hardware implementation and experimental testing.

B. Post-processing Strategies

Due to the characteristics of structure design, there exist above mentioned two constraints. However, the post-processing strategies can alleviate or eliminate these constraints. Error correction mechanism [8] can improve the reliability of PUF output without changing the uniqueness. According to the output distribution of delay-based PUF, the output instability occurs when the delay difference between two comparison paths approaches 0. In CRPs selection mechanisms [7], [9], challenges of this situation are removed, the reliability of the PUF can be significantly improved. And with the control of ratio of 0/1 in the output bits, the uniqueness of the PUF output improved simultaneously.

The fundamental reason that the post-processing strategy can break through these two constraints is that it can directly delete bad outputs (unstable CRPs) without affecting other outputs (stable CRPs), which is not possible with structure design. However, the extra cost is also needed.

V. Conclusions

Delay-based PUF generates random responses based on the delay of components and wires in the circuits, and the variation of this delay obeys Gaussian distribution. This makes delay-based PUF easy to be modeled, and is conducive to theoretical analysis of its performances before implementation. Through our work, we obtained the following conclusions:

- PUF internal comparison circuit adjustment (such as the feed-forward structure, XOR operation, etc.), compared to the original structure, cannot enhance the uniqueness and reliability at the same time. The fundamental reason for this is that they can only affect the parameters of the Gaussian distribution, but cannot change the fact that its output is still obeys Gaussian distribution.
- The post-processing strategies of PUF can break through the above constraints, enables the uniqueness and reliability of PUF performance to be improved simultaneously. Because they can break the integrity of the output Gaussian distribution, just like cutting off the bad part (unstable area) with a pair of scissors.
- Using the established theoretical model, there will always be some differences between the analytic data and the experimental data. As the results calculated by probability theory are equivalent to the results of infinite sample space, while the actual measured data are collected from limited hardware implementations and experimental times. But it can correctly reflect the trend of performance under different strategies.
- The values of these performance metrics cannot fully measure the advantages and disadvantages of a PUF. In the designing, factors such as attack resistance, hardware efficiency, implementation requirements, and costs should also be considered.

Research on the theoretical analysis of PUF is very useful. It can provide guidance for PUF designers, helping to save time and costs. It can also provide a rigorous theoretical support for the improvement of new designs.

References

[1] R. Pappu, B. Recht, J. Taylor, and G. Neil, “Physical one-way functions,” Science, vol. 297, no. 5589, 2002, pp. 2030–2029.

[2] S. Joshi, S. P. Mohanty, and E. Kougianos, “Everything you wanted to know about PUFs,” IEEE Potentials, vol. 36, no.6, 2017, pp. 38–46.

[3] J. Zhang, Q. Wu, Y. Lyu, Q. Zhou, Y. Cai, and Y. Lin, “Design and implementation of a delay-based PUF for FPGA IP protection,” in Proc. International Conference on Computer-Aided Design and Computer Graphics, pp. 107–114, 2013.

[4] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, “Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs,” in Proc. International Conference on Reconfigurable Computing and FPGAs, pp. 298–303.

[5] J. Capovilla, M. Cortes, and G. Araujo, “Improving the statistical variability of delay-based physical unclonable functions,” in Proc. Symposium on Integrated Circuits and Systems Design (SBCCI), pp. 1–7, 2015.

[6] J. W. Lee, D. Lim, B. Gassend, and G. E. Suh, “A technique to build a secret key in integrated circuits for identification and authentication applications,” in Proc. Symposium on VLSI Circuits, Digest of Technical Papers, vol.42, pp. 176–179, 2004.

[7] S. S. Zalivaka, A. A. Ivaniuk, and C. H. Chang, “FPGA implementation of modeling attack resistant arbiter PUF with enhanced reliability,” in Proc. International Symposium on Quality Electronic Design, pp. 313–318, 2017.

[8] M. D. Yu, and S. Devadas. “Secure and robust error correction for physical unclonable functions,” IEEE Design and Test of Computers, vol. 27, no.1, 2010, pp. 48–65.

[9] T. Xu, and M. Potkonjak. “Robust and flexible FPGA-based digital PUF,” in Proc. International Conference on Field Programmable Logic and Applications, pp. 1–6, 2014.

[10] Y. Wen, and Y. Lao. “Enhancing PUF reliability by machine learning,” in Proc. IEEE International Symposium on Circuits and Systems, pp. 1–4, 2017.

[11] A. Maiti, J. Casarona, L. Mchale, and P. Schaumont, “A large scale characterization of RO-PUF,” in Proc. IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), pp. 94–99, 2010.

[12] R. Maes, P. Tuyls, and I. Verbauwhede, “Statistical analysis of silicon PUF responses for device identification,” 2008.

[13] Y. Lao, and K. K. Parhi, “Statistical analysis of MUX-based physical unclonable functions,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 33, no. 5, 2014, pp. 649–662.

[14] R. Hesselbarth, F. Wilde, C. Gu, and N. Hanley, “Large scale RO PUF analysis over slice type, evaluation time and temperature on 28nm Xilinx FPGAs,” in Proc. IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 126–133, 2018.

[15] Q. Ma, C. Gu, N. Hanley, C. Wang, W. Liu and M. O’Neill, ”A machine learning attack resistant multi-PUF design on FPGA,” 2018 23rd Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 97-104, 2018.

[16] W. Liu, Y. Yu, C. Wang, Y. Cui, and M. O’Neill, “RO PUF design in FPGAs with new comparison strategies,” in Proc. IEEE International Symposium on Circuits and Systems, pp. 77–80, 2015.

[17] A. Maiti, and P. Schaumont, “Improved ring oscillator PUF: an FPGA-friendly secure primitive,” Journal of Cryptology, vol. 24, no. 2, 2011, pp. 375–397.