TELKOMNIKA, Vol.17, No.1, February 2019, pp.377~383
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v17i1.10436

High secure buffer based physical unclonable functions (PUF's) for device authentication

Sadulla Shaik*[1], Anil Kumar Kurra[2], A. Surendar[3]
Department of Electronics and Communication Engineering, Vignan's Foundation For Science, Technology & Research (Deemed to be University), Guntur, India
*Corresponding author, e-mail: sadulla09@gmail.com[1], kakumar94@gmail.com[2], surendararavindhan@gmail.com[3]

Abstract

Physical Unclonable Function (PUF) is fast growing technology which utilizes the statistical variability of the manufacture variations acts as a finger print to the each device. It can be widely used in security applications such as device authentication, key generation and Intellectual Property (IP) protection. Due to the simplicity and low cost arbiter delay based PUFs have been mostly used as a cryptographic key in Internet of Things (IoT) devices. As conventional arbiter PUFs are suffers from less uniqueness and reliability. This paper provides designing of new buffer based arbiter PUF. It has been demonstrated that experimental results of new buffer based arbiter PUF shows the considerable improvement in the uniqueness and reliability of the proposed design and the Monte-Carlo analysis applied for delay variability of the PUFs.

Keywords*: cryptographic secure keys, internet of things, key extraction, masking, physical unclonable functions*

1. Introduction

As the technology has growing many aspects of our day to day life there is a demand for privacy, security and trust worthyness for the hardware devices. Recent year's authentication and device identification plays a critical issue for the electronics components. To ensure the security to hardware devices silicon Physical Unclonable Functions (PUFs) are emerged as one of the promising solution [1-4]. PUFs are the electronic circuit which utilizes the mismatch variations during the fabrication process generates the unpredictable responses. These variations without being designed explicitly or being programmed by a manufacturer. PUFs maps a digital input called a challenges and corresponding output called the response. This mapping process called the challenge-response(CRP) mechanism. various authors proposed a different PUF architectures such as arbiter PUFs ,ring oscillator PUFs [5-6], memory based PUFs [7-9] and light weight PUFs [8-9].Though many PUF architectures has been proposed cost, uniqueness plays a major challenge in any PUF architecture.In this paper we proposed a simple, low cost, more unique buffer based arbiter PUF architecture.

The rest of the paper is organised as follows: sections 2 reviews the background of the PUF metrics , classifications of PUFs,and Section 3 involves the mathematical model for arbiter PUF. Section 4 explains the buffer based arbiter PUF and arbiter design techniques and final conclusion at section 5.

2. Metrics of Physical Unclonable Function

2.1. Reliability

It is a measure of how many number of bits to be flipped during one particular PUF instance under different supply and environmental conditions. This can be mathematically expressed in expression (1) [10].

$$HD\,\text{int}\,ra = \frac{1}{m}\sum_{t=1}^{m}\frac{HD(Ri,Ri,t)}{n}\times 100\,\% \quad (1)$$

HD = Hamming distance between group of samples.
HD intra = Average distance between the number of noisy PUF response bits.

Received June 27, 2018; Revised September 5, 2018; Accepted October 7, 2018

2.2. Uniqueness

It is the estimation of how uniquely a PUF can generate the PUF responses and it will give the information about the number of output bits are different between two PUFs. It can be measured with expression (2) . Where Ri, Rj are the ith and jth response of the same device of the PUF response.

$$Uniqueness = \frac{2}{k(K-1)} \sum_{i=1}^{k-1} \sum_{j=j+1}^{k} \frac{HD(Ri, Rj)}{n} \times 100\% \quad (2)$$

2.3. Uniformity

It implies that response of the system is either 0's or 1's and it should be equally distributed. An ideal PUF shows the 50% of the uniformity. For 'n' bit PUF it can be represented by in expression (3).

$$Uniformity = \frac{1}{k} \sum_{i=1}^{k} ri \times 100\% \quad (3)$$

2.4. Classifications of PUFs

A PUF is works on based challenge response mechanism. Typically an input (challenge) is to the PUF resulting it generates the corresponding response i.e. called as challenge-response pairs (CRP).

$$\text{Re}sponse = f(Challenge)$$

Depending upon the size of the CRP, PUFs can be classified as two types such as weak and strong PUFs [4-6]. Weak PUFs (Anderson PUF) have limited number of CRPs, stable responses from noise and environment variations for multiple readings, output response should be preserve private, and response is strong enough and depends on intrinsic process variations [8-11]. Strong PUFs (Memory and delay based PUFs) have large number of CRPs, response generated from an each challenge could be strong enough to environmental variations (better reliability), no restriction to preserve the output response, not susceptible any attacks and not feasible to manufacture two PUFs with the same responses.

3. Arbiter based Physical Unclonable Function

An arbiter PUF is a class of delay based PUFs, it can be designed by using two components (i) Delay network which exhibits the difference in delay paths that lead to racing among the paths. (ii) An arbiter which acts as a storage element and produces the response depending upon the input arrival from delay network. A conventional arbiter PUF architecture shown in Figure 1 is composite a set of multiplexers (MUX) are connected in an upper and lower stages, thus can be controlled by the selection lines (challenges) [12-14]. Each selection line acts as a challenge to a MUX and at final stage of the MUX is feed to the arbiter which decides the PUF response by comparing the delay differences occurred in MUX stages. (i.e., due to manufacturing process variations lead to significant delays in MUX).

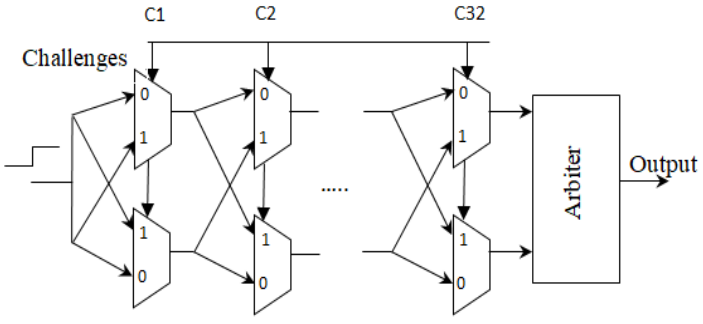

Figure 1. Silicon multiplexers based PUF

3.1. Mathematical Model for Arbiter PUF

The delay differences caused due to manufacture process variations can be modeled by additive linear delay model, it approximates the variations of delays by statistical timing analysis (SSTA) by Gaussian distribution. Therefore the process variations can be classified as a two types 1.interdie variation (die to die) and 2.intradie variation (with in the single chip). In the arbiter PUF each MUX can be treated as a independent identical distribution (IID) random variable i.e. modeled as a Gaussian random variable N (μ, σ2).μ represents the mean and σ represents the standard deviation [15]. The delay network consists of 'n' number of stages then the delay difference of n stages can be represented as N (Nμ, Nσ2). Expression (4) measures the delay difference between top stage and bottom stage of MUX's.

$$\Delta_i = D_i^t - D_i^b \sim N(0,2\sigma^2) \tag{4}$$

The response is dependent on the delay differences of the two paths and sign of the delay differences can be determined by external bits. The delay difference of the last stage can be represent by expression (5) and (6).

$$r_N = \sum_{i=1}^{N} (-1)^{C_i^{'}} \Delta_i \tag{5}$$

Where $C_i^{'} = \oplus_{j=i+1}^{N} C_j$ and $C_N^{'} = 0$ the out bit generated by

$$R = sign(r_N) = \begin{cases} 1, r_N \geq 0 \\ 0, r_N < 0 \end{cases} \tag{6}$$

The above additive linear model is used to represent the final response of the MUX PUF. The skew effect of the arbiter also affects the performance of the MUX based PUFs by reducing the uniqueness, producing the biased response that degrades the security of the PUF. Hence to improve the uniqueness of the arbiter PUF we proposed a new PUF architecture as shown in Figure 2.

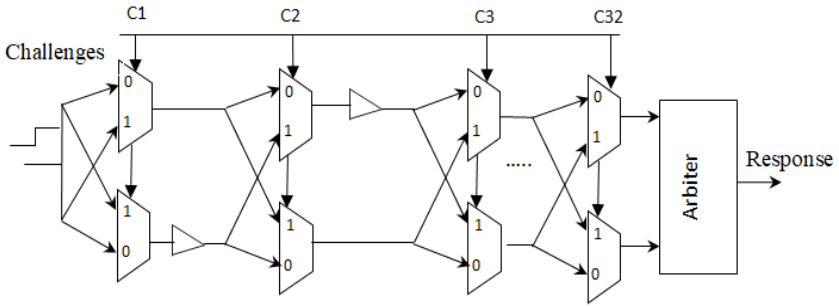

Figure 2. Buffer based arbiter multiplexers PUF

4. Buffer based Arbiter PUF

Original arbiter PUFs as shown in Figure 1 are linear PUFs which are easily attacked by side channel effects and has the less uniqueness. Hence to improve the uniqueness proposed a 32 stage buffer based arbiter structure. Here by incorporating the buffers at the intermediate stage of the mux based arbiter PUF, this leads to non-linearity of the arbiter PUFs, thereby it uses the racing which results increases the complexity of the numerical modeling attacks [16-17]. However this structure degrades the reliability of the PUF. Figure 2 depicts the buffer based arbiter PUFs and its corresponding layout shown by Figure 3.

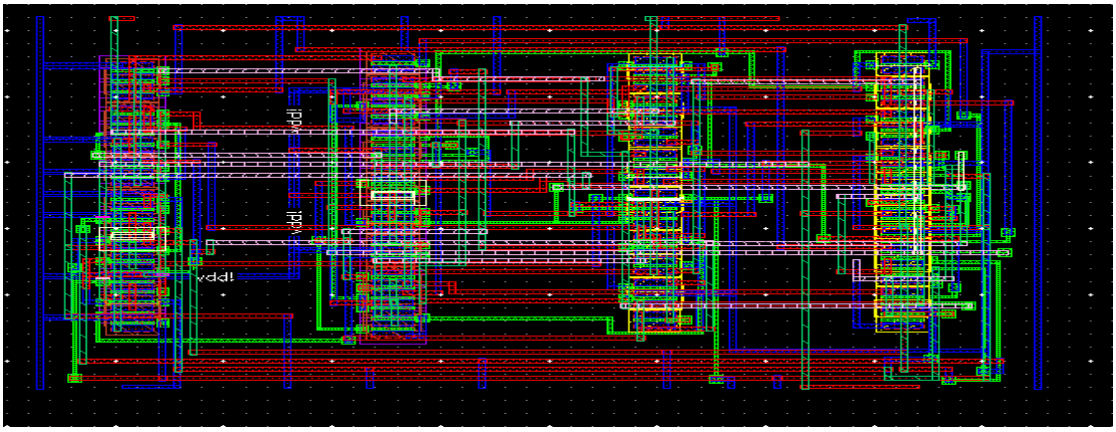

Figure 3. Buffer based arbiter multiplexers PUF Layout

4.1. Arbiter Design Techniques

An arbiter is a digital circuit which commonly used as a decision element in the arbiter PUFs and it can capture the delay differences occur during the fabrication process variability and determines the which input arrives first. Typically The most commonly used arbiter elements are D-latch and SR-latch. This can be used to detect the path differences by comparing the delays from the PUF network .The final response of the MUX network are fed to the R and S inputs of a SR-latch. Depending upon the relative delay differences, different values at output of Q. Figure 4 illustrstes the SR-latch [17].

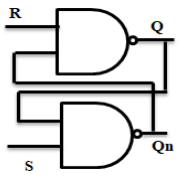

Figure 4. SR-Latch

5. Experimental Simulation

The manufacturing process variations cannot be controlled during thefabrication. These variations are considered to be statistical variations of the physical materials. The sources of variations are distinguished by two types such as variations in process parameters (i.e. due to oxide thickness, impurity concentration, diffusion depths) and the second category covers the variations in dimensions of the devices (i.e. during the photo-lithography process).these variations can be captured by using commercial simulators such as cadence spectre by applying the Monte-Carlo simulation to determine the best logic design for a PUF. Here the main aim of the design a delay based PUF is to generate the unique response and generated response should be stable for the wide range of the temperatures.

In order to achieve this we applied the same set of sequence challenge to the conventional arbiter PUF and proposed buffer based arbiter PUF and applied the Monte-Carlo simulation using spectra cadence on Virtuoso 6.1.7, platform with 180nm CMOS technology. Experimental results found that due to the non-liner delay of proposed logic circuit generated the unique response. Hence to figure out the unique response we applied the 32 bit challenge to the both the PUFs and we have estimated the standard deviation and compared the responses of two logics designs using Hamming Weight Distance (HWD) by changing the channel length (L) and widths (W) of the transistors. Figures 5 and 6 shows the estimation of HWD for delay and buffer based arbiter PUFs respectively. Buffer based PUF shows the 1.1 times better mean value than delay based PUF with 150 samples at VDD range from 0 V to 1.8 V. Delay based PUF has 99.1% lesser standard deviation when compared to buffer based PUF for 150 samples at V_{DD} range from 0 V to 1.8 V.

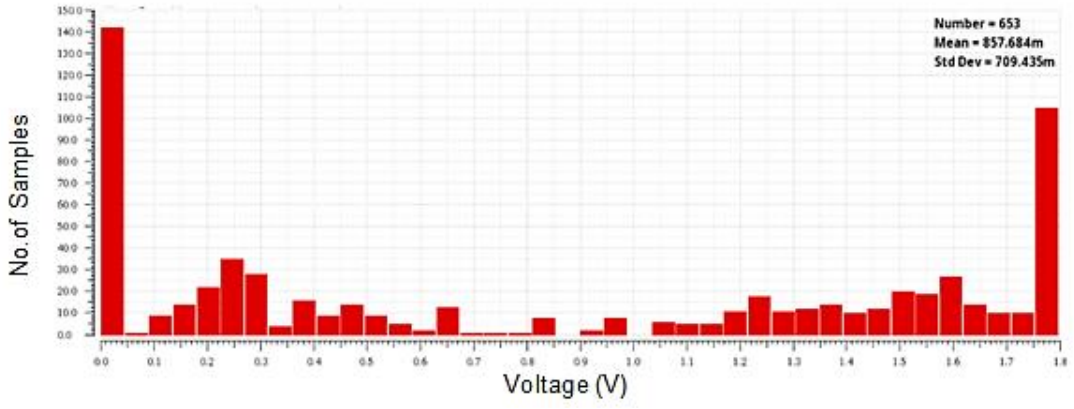

Figure 5. Estimation of Hamming weight Distance (HD) for delay based arbiter PUF for V_{DD}

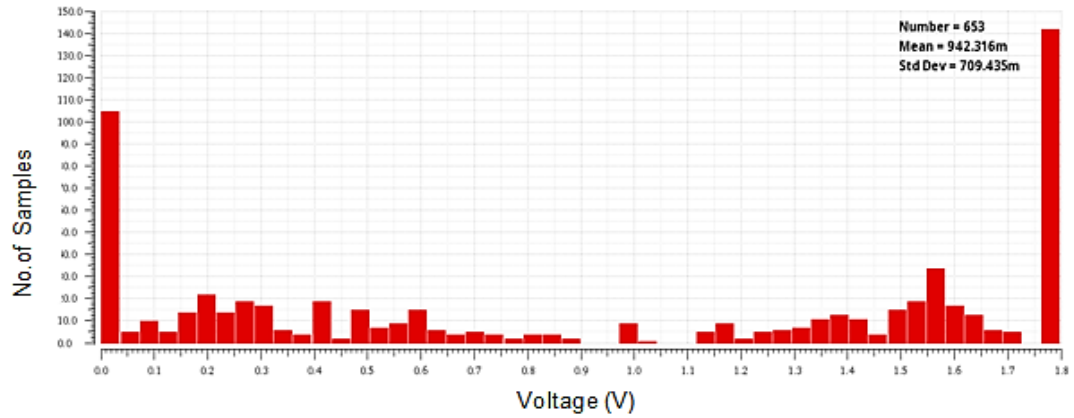

Figure 6. Estimation of Hamming weight Distance (HWD) of buffer based arbiter PUF for V_{DD}

Figures 7 and 8 depicts the estimation of uniqueness of delay and buffer based arbiter PUF with respect to delay variability (linear & Non-linear) respectively. Table 1 and Table 2 describes the performance analysis (Uniqueness, Mean HD and Reliability) of delay and buffer based arbiter PUFs with temperature variation impact at V_{DD}=1.8V.

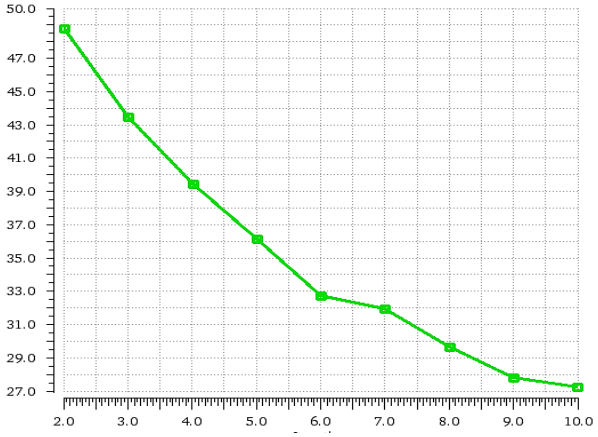

Figure 7. Estimation of uniqueness of delay based arbiter PUF with respect to delay variability (linear)

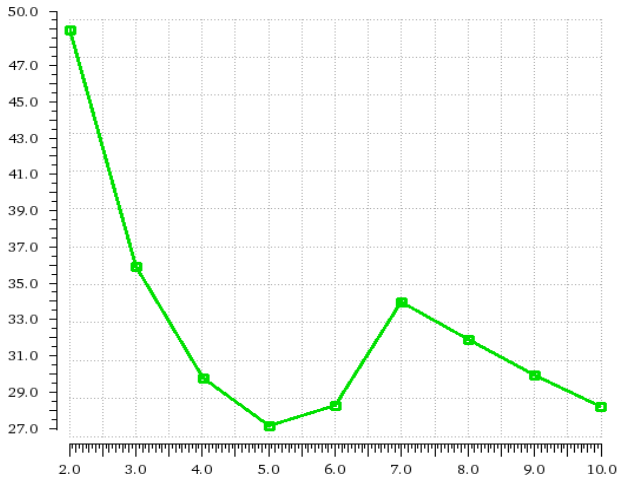

Figure 8. Estimation of uniqueness of buffer based arbiter PUF with respect to delay variability (non-linear)

Table 1. Temperature Variation Impact in Delay based Arbiter PUF at V_{DD}=1.8V

Temperature	0^0c	20^0c	40^0c	60^0c	80^0c	100^0c
Uniqueness	48.36%	48.86%	48.36%	48.47%	48.96%	48.56%
Mean HD	50.12%	50.72%	50.88%	50.01%	50.99%	50.77%
Reliability	89.63%	89.45%	88.65%	87.65%	86.54%	85.56%

Table 2. Temperature Variation Impact in Buffer based Arbiter PUF at V_{DD}=1.8V

Temperature	0^0c	20^0c	40^0c	60^0c	80^0c	100^0c
Uniqueness	49.78%	49.12%	49.77%	49.88%	49.56%	49.75%
Mean HD	52.88%	52.14%	52.47%	52.78%	52.54%	52.58%
Reliability	86.53%	85.78%	85.69%	84.78%	83.99%	83.83%

6. Conclusion

This paper helps to understand the statistical properties of delay based PUFs by Monte Carlo analysis. To choose the appropriate arbiter configuration based on the comparison of HWD of PUF responses. More considerably it improves delay variability of the proposed architecture there by significant improve in the responses of the PUF, hence it can be chosen as a wide range of the security applications such as device authentication, cryptographic key generation etc. Buffer based PUF shows the 1.1 times better mean value than delay based PUF with 150 samples at V_{DD} range from 0V to 1.8V. As a future work, it can be intended to fabricate the proposed buffer based arbiter PUF and analyze the effects due to environmental changes and work out the findings of the other delay based PUFs.

References

[1] Mugali KC, Patil MM. *Device Authentication by Physical Unclonable Functions*. International Conference on Computing Communication Control and Automation. Pune. 2015: 327-329.
[2] Rührmair U, Sehnke F, Sölter J, Dror G, Devadas S, Schmidhuber J. *Modeling attacks on physical unclonable functions*. Proceedings of the 17th ACM Conference on Computer and communications security. Chicago. 2010: 237-249.
[3] Anderson R, Kuhn M. *Low cost attacks on tamper resistant devices*. Proceedings of the 5th Springer International Workshop. Paris. 1997: 1-12.
[4] Majzoobi M, Koushanfar F, Potkonjak M. Techniques for design and implementation of secure reconfigurable PUFs*. ACM Transactions on Reconfigurable Technology and Systems*. 2009; 2(1): 5.1-5.33.
[5] Suh GE, Devadas S. *Physical unclonable functions for device authentication and secret key generation*. Proceedings of the 44th annual Design Automation Conference. San Diego. 2007: 9-14.
[6] Halak B, Hu Y, Mispan MS. *Area efficient configurable physical unclonable functions for FPGAs identification*. IEEE International Symposium on Circuits and Systems. Lisbon. 2015: 946-949.

[7] Zhang J, Wu Q, Lyu Y, Zhou Q, Cai Y, Lin Y, Qu G. *Design and implementation of a delay-based PUF for FPGA IP protection*. International Conference on Computer-Aided Design and Computer Graphics. Guangzhou. 2013: 107-114.
[8] Archana P, Kumar SV, Venkatalakshmi B. *Physical Unclonable Function for low cost authentication*. International Conference on Wireless Communications, Signal Processing and Networking. Sydney. 2016: 1098-1101.
[9] Shaik S, Jonnala P. *Performance evaluation of different SRAM topologies using 180, 90 and 45 nm technology*. International Conference on Renewable Energy and Sustainable Energy. Coimbatore. 2013: 15-20.
[10] Kodýtek F, Lórencz R, Bucek J, Buchovecká S. *Temperature Dependence of ROPUF on FPGA*. Euromicro Conference on Digital System Design. 2016: 698-702.
[11] Cui Y, Wang C, Liu W, O'Neill M. *A Reconfigurable Memory PUF Based on Tristate Inverter Arrays*. International Workshop on Signal Processing Systems. Dallas. 2016: 171-176.
[12] Gao Y, Li G, Ma H, Al-Sarawi SF, Kavehei O, Abbott D, Ranasinghe DC. *Obfuscated challenge-response: A secure lightweight authentication mechanism for PUF-based pervasive devices*. International Conference on Pervasive Computing and Communication Workshops. Sydney. 2016: 1-6.
[13] Gao Y, Ranasinghe DC, Al-Sarawi SF, Kavehei O, Abbott D. Emerging physical unclonable functions with nanotechnology. *IEEE access*. 2016; 4: 61-80.
[14] Murthy GS, Singh D, Shaik S. An Area Efficient Built-In Redundancy Analysis for Embedded Memory with Selectable 1-D Redundancy. *Advances in Intelligent Systems and Computing, Springer International Publishing AG*. 2016: 721-728.
[15] Shaik S, Kurra AK, Surendar A.. Statistical analysis of reliable and secure transmission gate based arbiter physical unclonable functions (PUFs). *International Journal of Simulation: Systems, Science and Technology*. 2018; 19(4): 6.1-6.6.
[16] Zalivaka SS, Zhang L, Klybik VP, Ivaniuk AA, Chang CH. Design and implementation of high-quality physical unclonable functions for hardware-oriented cryptography. *Secure System Design and Trustable Computing*. 2016: 39-81.
[17] Karpinskyy B, Lee Y, Choi Y, Kim Y, Noh M, Lee S. *8.7 physically unclonable function for secure key generation with a key error rate of 2E-38 in 45 nm smart-card chips*. IEEE International Solid-State Circuits Conference. San Francisco. 2016: 158-160.