A secure arbiter physical unclonable functions (PUFs) for device authentication and identification

Anil Kumar Kurra, Usha Rani Nelakuditi
Department of Electronics and Communication Engineering,
Vignan's Foundation for Science Technology & Research, India

Article Info

Article history:

Received Aug 7, 2018
Revised Oct 20, 2018
Accepted Nov 11, 2018

Keyword:

Challenge-Response pairs (CRPs)
Hardware security
Machine-Learning (ML) attacks
Monte-Carlo analysis
Physical Unclonable Functions (PUFs)

ABSTRACT

Recent fourth industrial revolution, industry4.0 results in lot of automation of industrial processes and brings intelligence in many home appliances in the form of IoT, enhances M2M / D2D communication where electronic devices play a prominent role. It is very much necessary to ensure security of those devices. To provide reliable authentication and identification of each device and to abort the counterfeiting from the unauthorized foundries Physical Unclonable Functions (PUFs) emerged as a one of the promising cryptographic hardware security solution. PUF is function, mathematically modeled by using uncontrollable/ unavoidable random variances of the fabrication process of the ICs. These variances can generate unpredictable, random responses can be used to overcome the difficulties such as storing the keys in non-volatile memories (NVMs) in the classical cryptography. A wide variety of PUF architectures such as Arbiter PUFs, Ring oscillator PUFs, SRAM PUFs proposed by authors. But due to its design complexity and low cost, Delay based Arbiter PUFs (D-PUFs) are considering to be a one of the security primitives in authentication applications such as low-cost IoT devices for secure key generation. This paper presents a review on the different types of Delay based PUF architectures proposed by the various authors, sources to exhibit the physical disorders in ICs, methods to estimate the Performance metrics and applications of PUF in different domains.

Corresponding Author:

Anil Kumar Kurra,
Department of Electronics and Communication Engineering,
Vignan's Foundation for Science Technology & Research,
University, Vadlamudi-522 213, Guntur, A.P, India.
Email: kakumar94@gmail.com

1. INTRODUCTION

Advances in technology from IT to IoT enhance the usage of electronic devices. Hence electronic hardware security emerged as one of the serious challenge due to the penetration of electronic devices in to all spheres of people life. At present classical software security mechanisms have certain limitations such as storing the secret keys in non-volatile memories such as EEPROM or flash memory. This not only incurs cost overhead and also suffers from wide variety of invasive, semi-invasive and non-invasive attacks which makes difficult to extract the secret keys [1]-[3]. The remedy to this is storing the secret key or an ID in internal memory instead of external memory, the chip can protect from external attacks. To generate the unique keys/IDs without involvement of external interaction by using only its inherent characteristics of ICs, Physical Unclonable Functions (PUFs) emerged as one of the promising solution, by creating an on chip secret keys.

Fabrication process has certain uncontrollable and unavoidable physical limitations due to which no two ICs are identical even they were produced by the same wafer. A PUF is physical system whose behaviour is mainly depends upon the intrinsic variations of the manufacturing process of ICs. PUFs are easy to evaluate and very hard to duplicate due to its manufacturing resistant. An input to the PUF is known as challenge and corresponding output is treated as a response. The typical characteristics of PUFs (reproducible, unique, unclonable.one-way, unpredictable and tamper evident) can be illustrated by Figure 1.

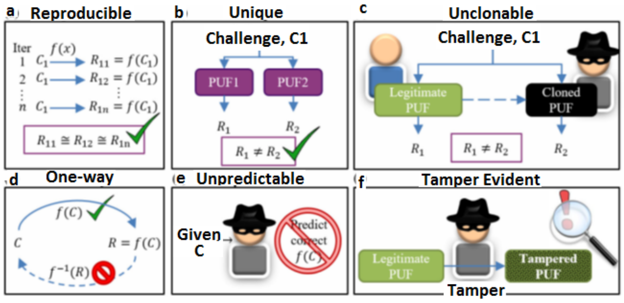


Figure 1. Properties of an ideal PUF [2]

1.1. Sources of Variability in CMOS PUF technology

A systematic spatial process variation leads to an imperfections in fabrication process which makes every IC is distinctive in its electrical characteristics. And these can be alters from die-to-die, wafer to wafer and IC to IC. The typical CMOS process variations during fabrication of an IC as shown in below Figure 2.

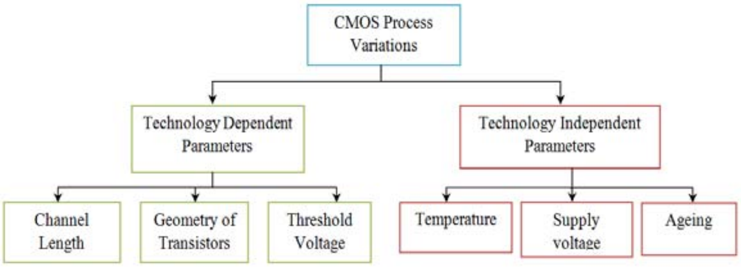


Figure 2. CMOS Process Variations in ICs

In Integrated Circuits (ICs) CMOS process parameters are varied during the fabrication process, these variations are mainly influence the performance of the whole circuit and type of mismatches (variations) are typically divided in two kinds such as global mismatches (MGlobal) which are technology dependent and on the other hand, local mismatches (Mlocal) which is technology independent and it can be expressed in (1).

$$M_{Total=}\ M_{Global}+M_{local} \qquad (1)$$

Global mismatches occur due to random process Manufacturing Variations (PMVs) this mainly because of channel length, geometry of transistors (width(w), length(L), Oxide thickness), impurity concentration, oxide thickness, threshold voltage (Vt), diffusion depth and electron mobility which are inherently present and sensitive to process variations [4]-[6]. On the other side local parameters such as environmental variations, Supply voltage and ageing which are drastically effects the performance metrics of the PUF. The impact of the variations cannot be controlled completely but these can be minimized. Whenever the temperature is increment and supply voltage is reducing, it may affect on diverse parts of the circuit which leads to degrade the reliability of PUF [7]-[9]. Ageing also one of the important concerns for PUF circuits. As the continuous utilization of the CMOS devices which leads to a progressive degradability of the system performance and the mechanisms which alters the performance of CMOS devices are Negative bias temperature instability (NBTI), Hot Carrier Injection (HCI), temperature dependent die electric break down (TDDB), positive bias temperature instability (PBTI), electro migration and soft errors are consider as a major causes to alter the properties of a ICs [10]-[12].

2. RESEARCH METHOD

A strong PUF is the one whose response is alters continuously with respect to corresponding challenges and The quality factor of any PUF architecture can be addressed by a set of PUF metrics such as uniquness, reliability, uniformity, ssand tamper resistance.

2.1. Uniqueness

It quantifies the dissimilarity of the response bits across different dies, when same challenge is applied. Inter chip Hamming Distance (HDinter) is a metric measure of the uniquness. Ideally HD should be the 50%.That implies even though the same challenge has been used for 'd'different dies half of the responses are differ with each other. The uniqueness can be computed in (2).

Let Ri and Rj be the n-bit responses generated from two different chips under same challenge.

$$\text{uniqueness}=\frac{2}{d(d-1)}\ \sum_{i=1}^{d-1}\ \sum_{j=j+1}^{d}\frac{HD(RI,RJ)}{n}\times 100\% \qquad (2)$$

2.2. Reliability

It is a measure of stability of PUF responses under various environmental variations, aging and noise. An ideal PUF should recreate the exact responses irrespective of the external factors. HDintra is a metric that measures the response of a PUF under the same challenge at different fluctuating environmental conditions and supply voltage variations. Usually it could be done in two phases: Enrolment phase and Regeneration phase. Enrolment phase is process of generating the bit stream, typically at 250c and normal supply voltage. While reconstruction phase is done at different temperatures like 0^0c, 25^0c, 85^0c and voltage ranging from -5% to +5%., reliability of the PUF is expressed by (3).

$$\text{HD intra}=\frac{1}{s}\sum_{t=1}^{s}\frac{HD(Ri,Ri',t)}{n}\ \times 100\% \qquad (3)$$

For a device i, its consistency can be assessed by calculating the typical Inter chip Hamming Distance (HDintra) of n bit PUF responses. These m responses Rj are collected under m distinct environmental conditions. Ri which is collected at nominal operating conditions.

2.3. Uniformity

It is an estimation of the randomness of a PUF, and defined as the as a ratio of the ‘0’ to ‘1’ in the response bits of a PUF. For an ideal PUF the randomness is should be 50%.mathematicallt it can be expressed by (4).

$$\text{uniformity}=\frac{1}{k}\sum_{i=1}^{k} ri\times 100\% \qquad (4)$$

k represents the total number of responses and ri is the hamming weight of the ith response.

2.4. Tamper Resistance

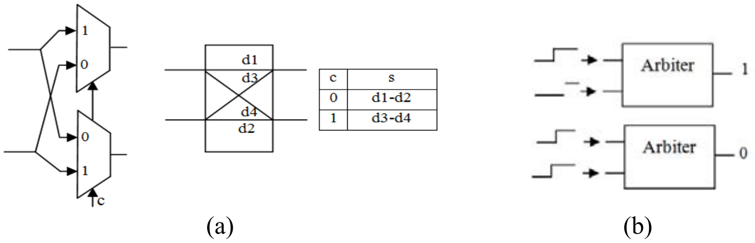
It is the degree of measure how safe a design to tampering attempts. In a real time the behavior of a PUF should alter completely when an adversary changes the structure of a design. it could be expressed using the Hamming Distance (HD) between the responses from an authenticate chip (i) and tampered chip (j), which is evaluated by (5).

$$\text{HDavg}=\frac{1}{CRP}\sum_{i=1}^{CRP}\frac{HD(Ri(l),Rj(l))}{n}\times 100\% \qquad (5)$$

CRP is the total number of challenge response pairs (CRPs). Ri (l) and Rj (l) are outputs of the authenticate and tamper chips respectively. And the modified PUF should distinctly different in terms of architecture and behavior.

3. DELAY BASED ARBITER BASED PUFs

An arbiter PUFs were first introduced by Gassend et al. in 2004 [13] by utilizing the intrinsic manufacturing variability's of a gate delays. It is a strong PUF, generates the more number of a CRPs illustrated by Figure 3. The basic architecture consists of a series of N identical switching (multiplexer) elements arranged in top and bottom stages and an arbiter i.e.SR flip-flop/D-latch is connected at its final stage to decide the final response. A rising edge of the signal is applied to enable PUF architecture and every switching element is activated by an input challenge vector (C1, C1, C2, C3, ..., Cn) signal can propagate either straight or cross according to input stimulus. The final response is evaluated based on the timing signal reaches at the input of the arbiter and an arbiter converts the analog timing difference in to the corresponding digital value based on the threshold limit. The delay of the multiplexer can be labeled as d1, d2, d3 and d4 as shown as Figure 3 (a) and (b).The estimation of the delays of the PUF can be modeled by using the linear additive delay model [14].



c	s
0	d1-d2
1	d3-d4

(a) (b)

Figure 3. (a) MUX switch (b) Effective contribution of a MUX switch to signal delay

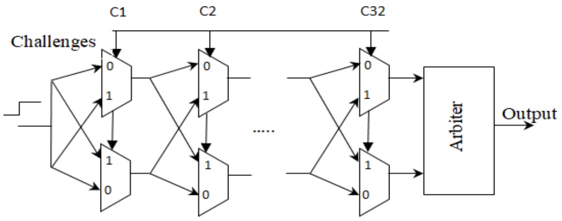


Figure 4. Arbiter PUF architecture

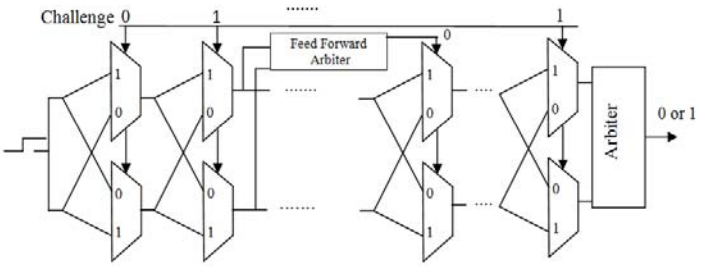


Figure 5. Feed Forward-Arbiter PUF architecture

By considering the PUF security metrics in to account To ensure the large delay variations Gassend [13] proposed a Feed-Forward (FF) arbiter PUF, by introducing an arbiter at intermediate stage of the original MUX architecture. The arbiter acts as a switch selector for the further stages to enhancing the circuit complexity, thereby improving the uniqueness and randomness[15]. However the reliability of the PUF has been degraded at wide range of the temperatures and suffers the reverse engineering attacks such as linear programming and combinatorial techniques [16]. Figure 4 illustres the Feed-forward forward arbiter architecture. Therefore Instead of the reconfiguring the CRPs directly, by reconfiguring the PUF circuit to enhancing performance metrics from the security perspective and also resists the information. leaked from each configuration, Yingjie Lao and Keshab K. Parhi [17] proposed a reconfigurable Feed-Forward PUF architectures, such as Feed-Forward Overlap (FFO), Feed-Forward Cascade (FFC), Feed-Forward Separate (FFS), MUX/DeMUX, Modified FF, Modified FFO, Modified FFC, Modified FFS architectures, (Figure 5,6,7,8,9,10,11 and 12) whose manufacturing process variations of the transistors can be modeled using the Statistical Static Timing Analysis(SSTA)[18] and experiments were done in SPICE 65nm technology by applying Monte-Carlo simulation to estimate the Inter-Chip variations(uniqueness), Intra-Chip variations (Reliability) and Randomness(as shown in table-1).

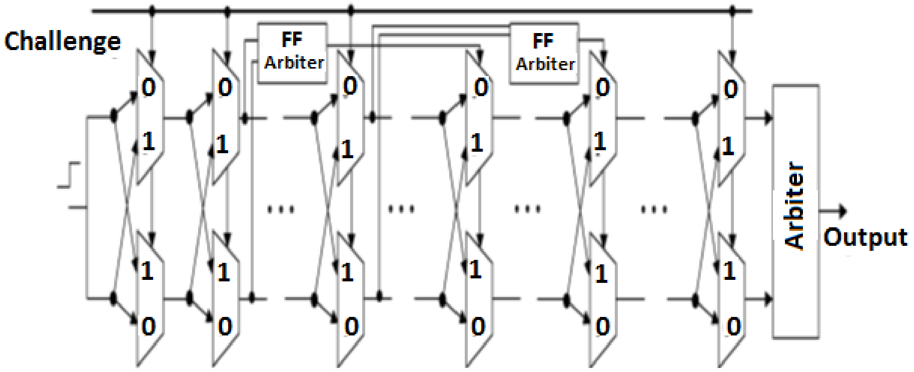


Figure 6. Feed-Forward MUX PUF overlap structure [17]

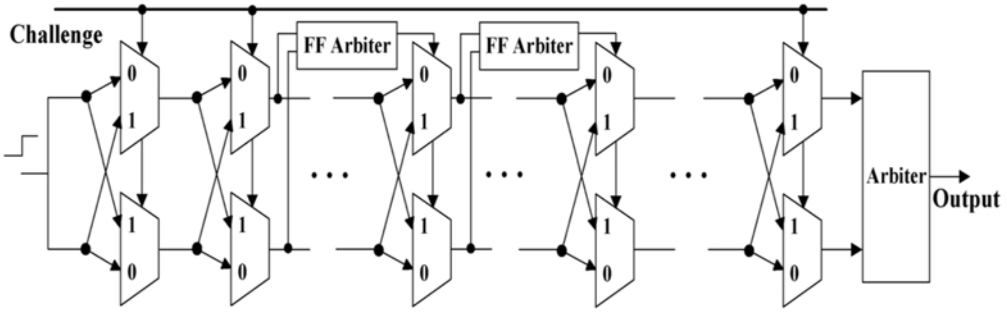


Figure 7. Feed-Forward MUX PUF cascade structure [17].

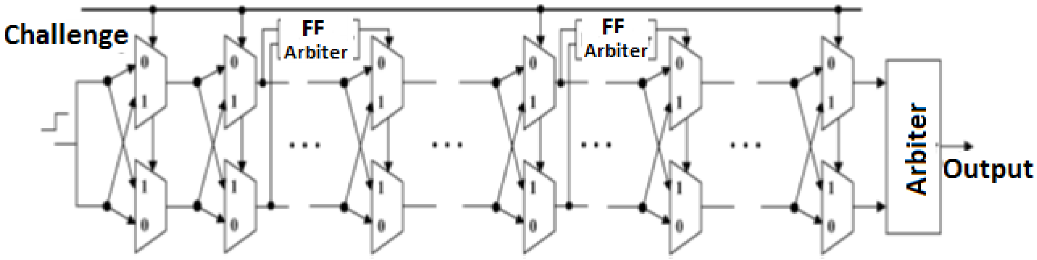


Figure 8. Feed-Forward MUX PUF separate structure [17].

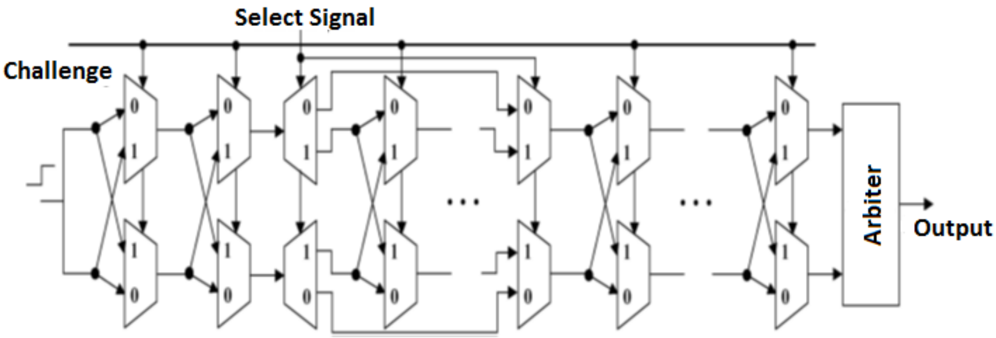


Figure 9. MUX/DeMUX PUF [17].

Table 1. The Performance indicators of the proposed architectures [17]

Architecture	Uniqueness (%)	Reliability (%)	Randomness (%)
Original MUX	88.2	94.2	65.6
FFO	95.0	91.3	77.6
FFC	97.5	89.3	84.2
FFS	96.2	90.1	80.6
MFFO	93.5	93.4	74.6
MFFC	95.9	93.0	79.6
MFFS	94.6	93.1	76.8
MUX/DeMUX	83.8	92.9	59.8

On the other hand, several authors proposed a various architecture and applied different techniques to improve the security metrics of the arbiter PUFs. According to Jefferson Capovilla, Mario Cortes, Guido Arauj [19] proposed a 32 stage tri-state buffer based arbiter circuit simulated using SPICE AMS 350nm technology, described different types of delay design network (Gate drive strength, Gate sizing) techniques as well as arbiter design techniques to improve the delay variability of the PUF,From the statistical results authors found that use of weak gates can improve the delay variability by a factor of four and instead of SR latch based arbiter D-FF arbiter should improve the Hamming Weight Distribution of a PUF.

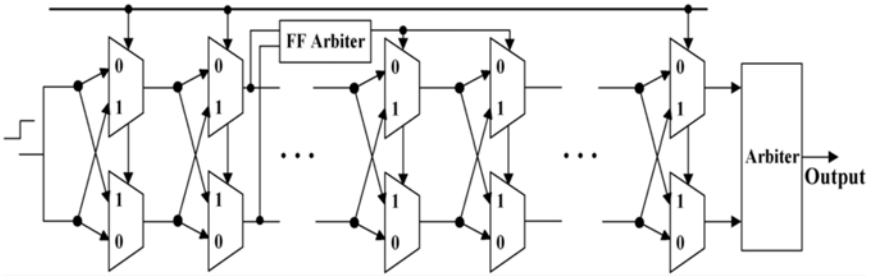


Figure 10. Modified Feed-Forward MUX PUF separate structure [17].

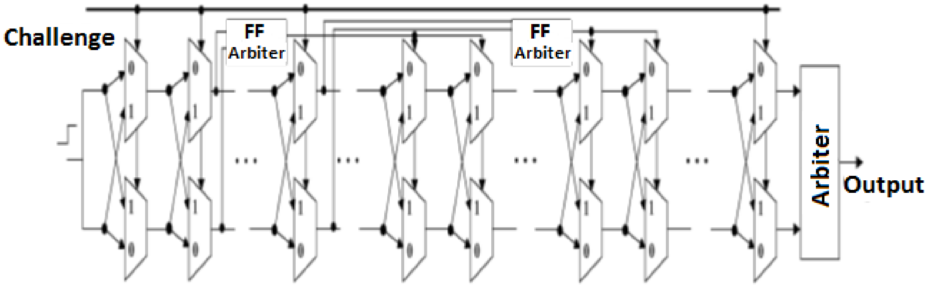


Figure 11. Modified Feed-Forward MUX PUF overlap structure [17].

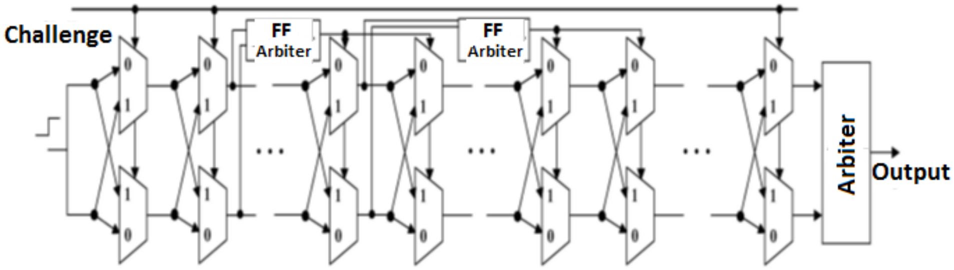


Figure 12. Modified Feed-Forward MUX PUF cascade structure [17].

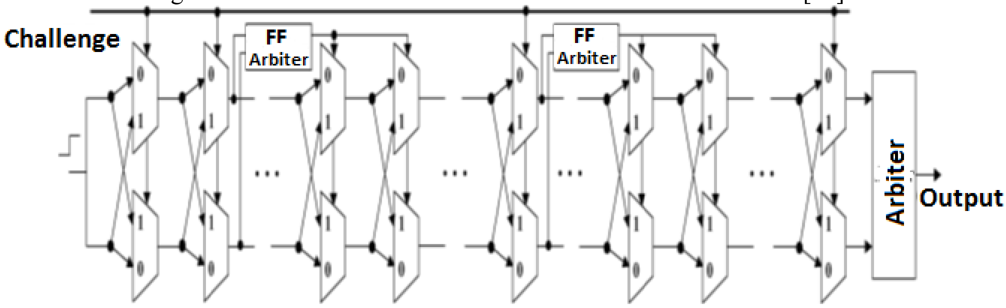


Figure 13. Modified Feed-Forward MUX PUF separate structure [17].

Anoop Koyily, Chen Zhou [20] proposed a technique in order to measure the PUF metrics accurately using Shannon entropy to determine whether PUF is linear or non linear, applied to linear, Feed-Forward, Modified-Feed Forward 32 bit PUF architectures (experiments done on IBM32nm HKMG technology) and observed almost 100% sensitivity and specificity [20].the delay of the any arbiter PUF architecture were mainly depends on the device geometry and number of stages. Hence as scaling down the technology that leads to a rapid variations in device geometry and which helps to enhance the security features of PUF architectures. Songde Hu, Huansheng Ning [21] proposed a 32-stage arbiter PUF architecture in 40nm and 65nm technology in cadence virtuoso, simulated by using Monte Carlo analysis estimated the uniqueness-42.25% and reliability -78% respectively. As the impact of the process technology and scaling down the voltage can significantly improve the uniqueness and sensitivity Lang Lin, Sudheendra Srivathsa [22] proposed a 64-bit arbiter PUF on 45nm SOICMOS technology and applied additive linear delay model to estimate the delay performance. Uniqueness should be 36.7% and its reliability is (82%) at 75˚c respectively and also resist the attack such as support vector machine (SVM).To combat the attacks over PUFs to enhance authenticity Takanori Machida, Dai Yamamoto [23] proposed a Multi input-Multi output (8 by 8) PUF design in 90 nm CMOS technology by applying Monte-Carlo analysis to estimate the statistical metrics of the switching element and improved the arbiter accuracy. Found the Inter chip Hamming Distance (HD) is almost an ideal value (~50%).

Along with the statistical analysis authors has also implemented the PUF architectures bu using FPGAs, Dinesh Ganta and Leyla Nazhandali [24] proposed an architecture called S-ArbRO PUF by integrating the arbiter and ring oscillator PUF architecture to analysis the variability and reliability. The proposed architecture consisting of a pair of the ring oscillators in each stage instead of the delay paths as a results it easy to build in both FPGAs and ASICs. For variability analysis the authors' implemented architecture in Xilinx 90nm Spartan (XC3S500E) FPGAs applied 1.2v supply voltage at 27℃ collected the different set of frequencies. For reliability chosen a four different FPGAs subjected to the temperature range from 45℃- 65℃ at 1.2 voltage. Found the variability 46% and reliability of 86%, and this architectures can also resistant to the modelling attack such as Logistic regression (LR). And Yohei Hori, Takahiro Yoshida [25] Implemented the 64-bit arbiter PUF architecture on Xilinx virtex-5 (xc5vlx30-ffg324) FPGAs at core voltage of 1.050v and performed the experiment on 1024 times. Found the uniquness-36.75, diffuness-98.36, Correctness-98.25, Stediness-98.48 and randomness-84.69. Further to improve the security metrics un hardware Takanori Machida, Dai Yamamoto [26] proposed a 3-1 double Arbiter based 64:1 PUF architecture in Xilinx vertex5 FPGA. During this design delay element can be used as 3 input XOR gates. From the experimental analysis found the uniqueness (~47%), randomness (79%) and steadiness (82%).to enhance the reliability P. Klybik and A. A. Ivaniuk [27] designed a 128-stage arbiter PUF architecture in Spartan 3E - XC3s500e and estimated the reliability (91%) and uniqueness (48%).

The proposed architecture have significant improve in their performance but suffers from Machine learning (ML) attacks. Shuai Chen, Bing Li, Fukui Dan [28] proposed a novel polynomial reconstruction-based RAPUFs (randomized Arbiter PUFs) scheme to resistant the ML attacks. It was done on four FPGAs (vertex-5) and results indicating the 60% accuracy and 100% authenticity. The overall summary of the proposed architecture by different authors has described by below table2.

Table 2. Summary of different architectures of arbiter PUFs

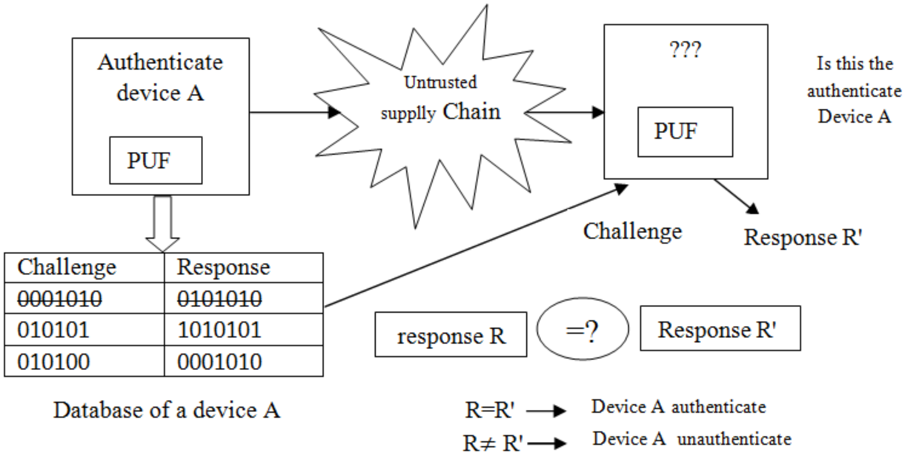
Authors	Type of a PUF	Proposed Mechanism	Strengths	Weakness
Gassend et al.in[13]	Silicon arbiter PUF	Linear additive model	1. Circuit has less complexity	1. Less reliability Suffers the modelling attacks
Yingjie Lao and Keshab K. Parhi [17]	Feed-Forward Overlap(FFO), Feed-Forward Cascade(FFC), Feed-Forward Separate(FFS), MUX/DeMUX	Gaussian distributions(Statistical static Timing Analysis(SSTA))	1. Resist through modelling attacks 2. Provides the better uniqueness	1. Area over head 2. Unstable CRPS
Jefferson Capovilla, Mario Cortes, Guido Arauj [19]	Tri-state buffer based arbiter PUF	Addition of a non linearity element	1. Enhances the reliability and variability	1.Sucesptable to noise
Takanori Machida, Dai Yamamoto[20]	Multi input multi output PUF architecture	Applied statistical static Timing Analysis(Monte-Carlo analysis)	1. Improved the better unpredictability	1.Incurs area over head
Anoop Koyily, Chen Zhou [21]	Arbiter PUF	Shannon entropy	1. Improved the sensitivity 2. Identified the better Non-linearity	1.Theoritically determined
SongdeHu, Huansheng Ning[22]	Arbiter PUF	Applied statistical Static Timing analysis(Monte-Carlo analysis)	1. Estimated Better uniqueness and reliability	1. Not directly secured from ML attacks
Implementation of PUFs in FPGAS				
Dinesh Ganta and Leyla Nazhandali [23]	S-ArbRO PUF	Implemented using Xilinx 90nm Spartan (XC3S500E) FPGAs	1. Reduction of number of gates 2. Incresed delay variability	1. More resist to the Machine learning attacks
Yohei Hori, Takahiro Yoshida [24]	Arbiter PUF	Xilinx virtex-5 (xc5vlx30-ffg324) FPGAs	1. Incresed the channel length bit	1. Difficult to measure
Takanori Machida, Dai Yamamoto [25]	Double arbiter based PUF	Xilinx virtex-5 (xc5vlx30-ffg324) FPGAs	1. Incresed the no of non linear elements	1. Reliabilty is decreases
V. P. Klybik and A. A. Ivaniuk [26]	Non lineararbiterPUF architecture	Xilinx Spartan 3E XC3s500e	1. Incresed the channel length bit	1. Sensitivity decreases
Shuai Chen, Bing Li, Fukui Dan [27]	polynomial reconstruction-based RAPUFs(randomized Arbiter PUFs)	Xilinx vertex-5 FPGAs	1. Improves CRPs inters of uniqueness and reliability	1. unstable CRPs
Lang Lin, SudheendraSrivathsa [28]	Arbiter PUF architecture	1. linear additive delay model (SOI CMOS Technology)	1. Improved reliability	1. less uniqueness

4. APPLICATIONS OF PUF

4.1. Low-cost device authentication

Due to its simple structure PUFs are used as an attractive choice for low cost authentication instead of applying the cryptographic algorithms such as data encryption and decryption [29]. As the generated output from PUF is unique and hard to predict for each IC. Hence it is can be identified by simply storing the PUF output in database and compared with the regenerated response. However a single PUF response cannot be used for device authentication.

Figure 13 depicts the overview of the PUF based authentication process. A PUF can acts as a "black box" due to its intrinsic properties generates unpredictable set of responses and has N number of CRPs whose response is unique for every challenge. Therefore, the authentication process is carried out, during the manufacturing of IC the trusted party stores its CRPs table in a secret server/data base, And PUF is given to the client. In order to verify the authenticity of an IC later, a client requests the server, server picks the set of random challenges and sent to the client. The client runs challenges on the PUF and submits the response to the server for authentication purpose. Server checks the responses ,compares with the CRPs in the server. If the observed response is near sufficient to the response in data base then verification is fruitful, otherwise it fails. To avoid the attacks from adversary CRPs can be utilized only once in each PUF and must be erased from database after verification.



Challenge	Response
~~0001010~~	~~0101010~~
010101	1010101
010100	0001010

Figure 14. PUF based Authentication [29]

4.2. Secret key generation:

Intrinsic PUFs can utilizes the inevitable manufacturing process variations which can be used as secret key generations. The fact that generated key (PUF response) should be stable over the number of read outs, but due to is noisy, error prone and limited amount of entropy, PUF responses cannot be used straightforwardly as a cryptographic key. This problem can be overcome by using the two-phase algorithm (key generation phase and key extraction phase) as shown in Figure 15(a) and (b). While initial key generation phase PUF output is combined with an additional information it is often called helper data. Both are stored in secure server/data base by the verifier. In extraction phase the verifier presents the helper data to an algorithm which extract the same key from the PUF as in the key generation phase. In this way PUF and verifier have shares a secret key, even if the helper data is publicly communicated from the verifier, the key has perfectly secret. In this scenario it is often called physically obscured keys.

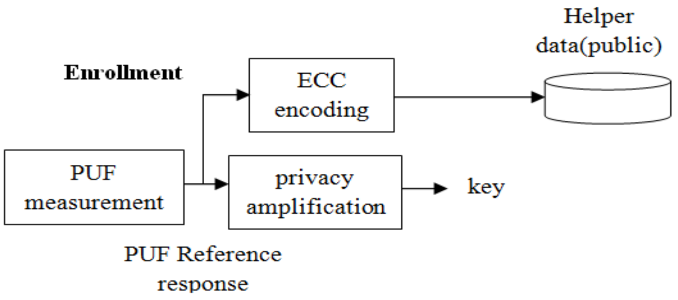


Figure 15. (a) Cryptographic key Generation in Enrolment phase

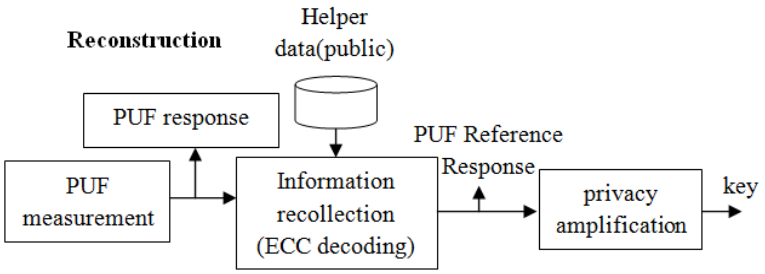
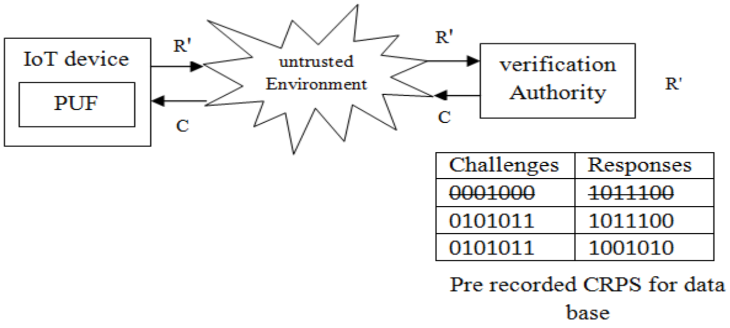


Figure 15. (b) Cryptographic key Generation in reconstruction phase

4.3. PUF in IoT Security:

Over the last decade IoT (Internet of Things) systems are emerged as one of the most spectacular phenomenon, it encompass billions of devices, each device is able to authenticate each other before sending or receiving the data. Traditional encryption techniques cannot be suitable for the IoT devices due to memory and power processing constrains. If conventional encryption techniques were applied to the IoT devices, it requires the huge memory space to store the secret keys and also it suffers different kinds of attacks such as invasive and semi invasive attacks, and also it requires huge power to process the data. Moreover providing the high level of security to the IoT devices using tamper sensitive circuitry it consumes more energy and expensive. Hence it clearly describes the current security primitives are not suitable for providing security to the IoT devices. PUFs on other hand provides an efficient and low-cost solution to the IoT security systems, without need of the storing the keys in devices, due to their random nature of the behaviour. Figure 16 illustrates the PUF based authentication in IoT devices.



Challenges	Responses
~~0001000~~	~~1011100~~
0101011	1011100
0101011	1001010

Figure 16. PUF based security authentication in IoT

5. CONCLUSION

In this paper we focused on different configurations of a delay based arbiter PUF architectures, by utilizing its random variations can be used as security metrics to identify and authenticate the recycled, overproduced, remarked ICs with low cost. The architectures were evaluated by different types of a mechanisms such as additive linear delay model, Gaussian distribution (SSTA), Shannon entropy etc. By reviewing the litreture review it was indicated that simulated using the CAD tools, at different technologies (350, 90, 65, 45) nm and, FPGAs (Spartan 3E, vitex-5) were used to validate these architectures. From the above literature survey found that delay is mainly influence the number of stages and technology parameters (W/L). In contrast to the delay based PUF architectures, mentioned different types of attacks PUFs and their impact on reliability, uniqunessand and randomness. Based on the reviewing the previous configurations, Tri-state buffer based arbiter PUF in the acoustic enviroments is the most effective architecthures, but in the noisy conditions multi input multi output PUF architectures are suggested. Future work mainly directed towards the improvement of the security metrics and tarnish modeling attacks respectively.

REFERENCES

[1] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, “Physical one-way Functions,” *Science*, vol. 297(5589), pp. 2026–2030, 2002.

[2] Grubel, Brian C., Bryan T. Bosworth, Michael R. Kossey, A. Brinton Cooper, Mark A. Foster, and Amy C. Foster, "Secure communications using nonlinear silicon photonic keys," *Optics express,* vol. 26(4), pp. 4710-4722, 2018.

[3] B. Gassend, D. Clarke, M. van Dijk, and S. Dessvadas, “Controlled physical Unclonable functions,” in Proc. *18th Annu. Comput. Security Appl. Conf.*, pp. 149–160, 2002.

[4] S. R. Nassif, “Modeling and analysis of manufacturing variations,” in *IEEE Conference on Custom Integrated Circuits*, pp. 223–228, 2001.

[5] A. Chandrakasan, W.J. Bowhill, “Design of High-Performance Microprocessor Circuits,” *Wiley-IEEE Press*, 2000.

[6] L. Daihyun, J.W. Lee, B. Gassend, G.E. Suh, Mv Dijk, S. Devadas, “*Extracting secret keys from Integrated circuits*,” *IEEE Trans. Very Large Scale Integr.* VLSI Syst. vol. 13, pp. 1200–1205, 2005.

[7] D. Rossi, M. Omaña, C. Metra, A. Paccagnella, "Impact of bias temperature instability on soft error susceptibility," in *IEEE Transaction on Very Large-Scale Integration (VLSI) Systems*, vol. 23, pp. 743–751, 2015

[8] A. Antonopoulos, M. Bucher, K. Papathanasiou, N. Mavredakis, N. Makris, R. K. Sharmaet al., "CMOS small-signal and thermal noise modeling at high frequencies," *IEEE Trans. Electron Devices,* vol.60, pp.3726–3733, 2013

[9] D. C. Matthews, M.J. Dion, "NSEU impact on commercial avionics," in *2009 IEEEInternational Reliability Physics Symposium*, pp. 181–193, 2009.

[10] S. Nassif, K. Bernstein, D.J. Frank, A. Gattiker, W. Haensch, B.L. Ji et al., "High performance CMOS variability in the 65 nm regime and beyond," in *IEEE International Electron DevicesMeeting*, pp. 569–571, 2007.

[11] X. Li, J. Qin, J.B. Bernstein, "Compact modeling of MOSFET wearout mechanisms forcircuit-reliability simulation," *IEEE Trans. Devices Mater. Reliab.*, vol. 8, pp. 98–121, 2008.

[12] F. Jianxin, S.S. Sapatnekar, "Scalable methods for the analysis and optimization of gate oxidebreakdown," in *2010 11th International Symposium on Quality Electronic Design (ISQED)*, pp. 638–645, 2010.

[13] J.-W. Lee, D. Lim, B. Gassend, G. E. Suh, M. vanDijk, and S. Devadas, "A technique to build a secretkey in integrated circuits with identification andauthentication applications," *In Proceedings of theIEEE VLSI Circuits Symposium*, Jun 2004.

[14] Z. C. Jouini, J. Danger, and L. Bossuet, “Performance evaluation of Physically Unclonable Function (PUFs) by delay statistics,” in Proc. *IEEE 9th Int. NEWCAS*, pp. 482–485, Jun 2011.

[15] B. ˇSkori´c, “On the entropy of keys derived from laser speckle; statisticalproperties of Gabor-transformed speckle,” *J. Opt. A: Pure Appl. Opt*, vol. 10(5), pp. 055304, 2008.

[16] Z. Tariguliyev and B. Ors, “Reliability and security of arbiter-based Physical Unclonable Function (PUFs) circuits,” *Int. J. Commun. Syst*., 2012.

[17] Lao, Yingjie, and Keshab K.Parhi. "Statistical analysis of MUX-based physical unclonable functions," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems 33.5*, pp. 649-662, 2014.

[18] H. Chang and S. Sapatnekar, “Statistical timing analysis consideringspatial correlation in a pert-like traversal,” in *Proc. IEEE Int. Conf. Comput. -Aided Design Integr. Circuits Syst*., pp. 621–625, 2003.

[19] Cortes, Mario, Guido Araujo, and Jefferson Capovilla. "Improving the statistical variability of delay-based physical unclonable functions," *Integrated Circuits and Systems Design (SBCCI), 28th Symposium on IEEE*, 2015.

[20] Koyily, Anoop, Chen Zhou, Chris H. Kim, and Keshab K. Parhi. "An entropy test fordetermining whether a MUX PUF is linear or nonlinear," *In Circuits and Systems (ISCAS)*, *International Symposium on IEEE*, pp. 1-4, 2017.

[21] Hu, S., Ning, H., Xu, Y., Mao, L., Li, Y., & Zhang, L., "Statistical Analysis of process variations on the delay-based PUF," *Identification, Information and Knowledge in the Internet of Things (IIKI)*, *International Conference on IEEE*, pp. 491-496, Oct 2016.

[22] Lin, L., Srivathsa, S., Krishnappa, D. K., Shabadi, P., & Burleson, W, "Design and validation of arbiter-based PUFs for sub-45-nm low-power security applications," *IEEE Transactions on Information Forensics and Security*, vol. 7(4), pp. 1394-1403, 2012.

[23] Machida, T., Yamamoto, D., Iwamoto, M., &Sakiyama, K., "A new mode of operation for arbiter PUF to improve uniqueness on FPGA," *In Computer Science and Information Systems (FedCSIS)*, *Federated Conference on IEEE*, pp. 871-878, Sep 2014.

[24] Ganta, D., &Nazhandali, L., "Easy-to-build arbiter physical unclonable function with enhanced challenge/response set. in Quality Electronic Design (ISQED)," *14th International Symposium on IEEE*, pp. 733-738, Mar 2013.

[25] Hori, Y., Yoshida, T., Katashita, T., & Satoh, A., "Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs," in *Reconfigurable Computing and FPGAs (ReConFig)*, *International Conference on IEEE*, pp. 298-303, Dec 2010.

[26] Machida, T., Yamamoto, D., Iwamoto, M., &Sakiyama, K., "A new mode of operation for arbiter PUF to improve uniqueness on FPGA," in *Computer Science and Information Systems (FedCSIS)*, *Federated Conference on IEEE*, pp. 871-878, Sep 2014.

[27] Klybik, Vladimir P., and Alexander A. Ivaniuk, "Use of arbiter Physical Unclonable Function (PUFs) to solve identification problem of digital devices," *Automatic Control and Computer Sciences*, vol. 49(3), pp.139-147, 2015.

[28] Chen, S., Li, B., Dan, F., Chen, J, "A machine learning resistant Arbiter PUFs scheme based on polynomial reconstruction," in *Signal and Image Processing (ICSIP)*, *2nd International Conference on IEEE*, pp.465-469, 2017.

[29] B. Halak, M. Zwolinski and M. S. Mispan, "Overview of PUF-based hardware security solutions for the internet of things," *IEEE 59th International Midwest Symposium on Circuits and Systems (MWSCAS)*, Abu Dhabi, pp. 1-4, 2016. doi: 10.1109/MWSCAS.2016.7870046.