Periodicals of Engineering and Natural Scinces ISSN 2303-4521
Vol.6, No.2, October 2018, pp. 58~63
Available online at: *http://pen.ius.edu.ba*

METAPUF A Challenge Response Pair Generator

Abhishek Kumar[1], Suman Lata Tripathi[2], RaviShankar Mishra[3]
[1,2]School of Electronics Engineering, Lovely Professional University
[3]Symbiosis University of Applied Sciences

Article Info

Article history:

Received Jul 23, 2018
Revised Sept 2, 2018
Accepted Oct 16, 2018

Keyword:

Physically unclonable function
Metastable
CMOS latch
Unpredictable
Challenge-Response

ABSTRACT

Physically unclonable function (PUF) is a hardware security module preferred for hardware feature based random number and secret key generation. Security of a cryptographic system relies on the quality of the challenge-response pair, it is necessary that the key generation mechanism must unpredictable and its response should constant under different operating condition. Metastable state in CMOS latch is undesirable since it response becomes unpredictable, this feature used in this work to generate a unique response. A feedback mechanism is developed which forces the latch into the metastable region; after metastable state, latch settle to high or state depends on circuit internal condition and noise which cannot be predicted. Obtained inter hamming variation for 8 PUF is 51.43% and average intra hamming distance is 99.76% with supply voltage variation and 96.22% with temperature variation.

Corresponding Author:

Abhishek Kumar,
School of Electronics Engineering,
Lovely Professional University
Punjab, India.
Email: abhishek.15393@lpu.co.in

1. Introduction

Security in a cryptographic system represented as how much secured the Response is! Kerckchoff's principle of cryptographic says "A cryptosystem should be secure even if everything about the system, except the key is public knowledge" [5] it is necessary that key must originate in a secured environment. The response is derived from random number processes by error correcting code to remove biasing error. The randomness of the random number is the strength of the key, classical algorithm based random number was deterministic in nature; it starts with an initial seed and starts repeating after sequence length. It is already proven that based on history upcoming random number can be predicted statically, which ultimately weakens the Response. Another method is physical variable based on a random number generator like thermal noise. In 2007 GE suh and S devadas [1] presented architecture of physically unclonable function (PUF) is an emerging technology for authentication and Response generation. PUF is a computational unit which output (response) is a function of input (challenge) as a well-selected hardware feature. A unique feature of hardware added into the computation [2, 20]. Two silicon ICs cannot have a similar feature; the silicon-based integrated circuit is the preferred choice for implementation of PUF circuit.

PUF circuit is unclonable and its output cannot be predicted. In 2013 NXP semiconductor has quoted that "any physical device characteristic that fluctuates can be turned into PUF". S.Devdas[1] have introduced delay-based PUF, delay unit implemented with a multiplexer, input signal raced between two parallel paths; at the destination, arbiter decides which decide which path is faster accordingly generate response bit [3]. A ring oscillator PUF introduced in 2009;s election of operating frequency depaend on a large size multiplexer, two

counters operate parallel on selected different ring oscillator. Response bit is high if value of counter1>counter2. [8-11]. In 2015 PUF found application to securing the internet of things (IOT) device. Quality of PUF response is judged by 3 parameters [1, 7, 13, 17, 18].

A) Uniformity- Probability of occurrence of bit '1' and a bit '0' in the key should equal, half of the key length. Ideal value is 50%.
B) Reliability- PUF should same response for a challenge in a different operating condition like variable supply voltage, high temperature, and noisy environment. Ideal value is 100%.
C) Uniqueness- For same challenge different PUF must produce a different response. Ideal value is 50%.

The remaining section of the paper as follows. Section 2 reviews metastability state of CMOS latch. Section 3 describes the schematic details of metastable PUF and their performance and Section 4 concludes with future directions

1.1. Metastable CMOS latch

Metastable in the system is undesirable because system behavior uncontrollable and its response are unpredictable [14] where as this unpredictable behavior enable to orginate randomness of PUF. A cross-coupled CMOS inverter based latch shown in fig 1(a) node Q and QB form bistable remain at high or low state. If we able to apply equal voltage at each node i.e threshold voltage of inverter latch enters onto metastability center of graph shown in fig 1(b), practically not possible to apply equal potential on both node slight variation exist due to circuit non linearity which pull the node settle with high or low state its completely unpredictable. Metastable PUF utilizes this feature to generate a response bit.

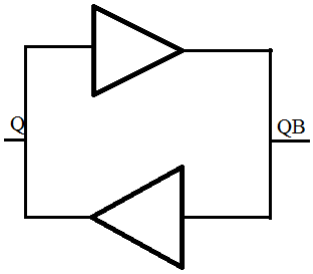

Fig1(a) CMOS latch

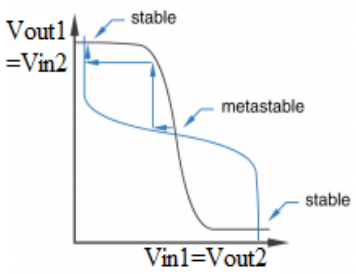

Fig1(b**)** Metastable Point

2. METASTABLE PUF

Physically unclonable function (PUF) is hardware-based security module uses inherited properties of the integrated circuit to generate an unpredictable response. In the proposed MetaPuf a CMOS based latch circuit is the basic element of PUF, which frequently enters into metastability region by maintaining equal potential at Q and QB node, depending upon circuit internal nose latch will come out from metastable state and settle to logic '1' or logic '0' which is completely unpredictable. MetaPuf uses metastability associated with CMOS latch to generate 1-bit response shown in fig2. Q and QB node of the latch is controlled by 2:1 multiplexer applies the same potential on each node and forces the latch to enter in a metastable state. A high EQ and high SEL input enable transmission gate (TG) to apply charge pump output on each node of the latch. Latch enters in metastable state there is a race to Q and QB terminal, minute potential difference on nodes senses by the sense amplifier and produces response bit. When EQ=0 and SEL=0 transmission gate disables it cut off the latch from the charge pump and creates a loop.

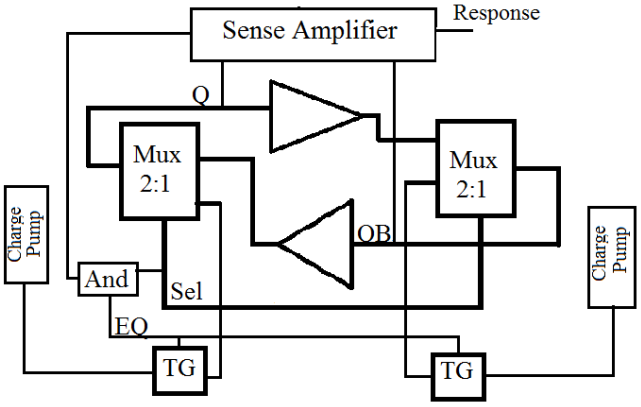

Fig2 Metastable PUF

The proposed circuit is verified for 8 different PUF fig3, each latch unit is operated by the charge pump. Challenge input is applied to decoder input; the output of decoder increase or decrease the charge pump output for logic '1' and '0' respectively. A high input applies increasing potential and low input applies to decrease potential to latch node. Charge pump potential assures that latch operates near metastable region. During metastable state potential difference between Q and QB cannot be guessed, they form a race and try to reverse. Sense amplifier generates high response bit if the potential at Q > QB else low. Response bit can store in parallel in parallel out shift register. To have more response number of PUF units are parallelized and require the large size of the decoder.

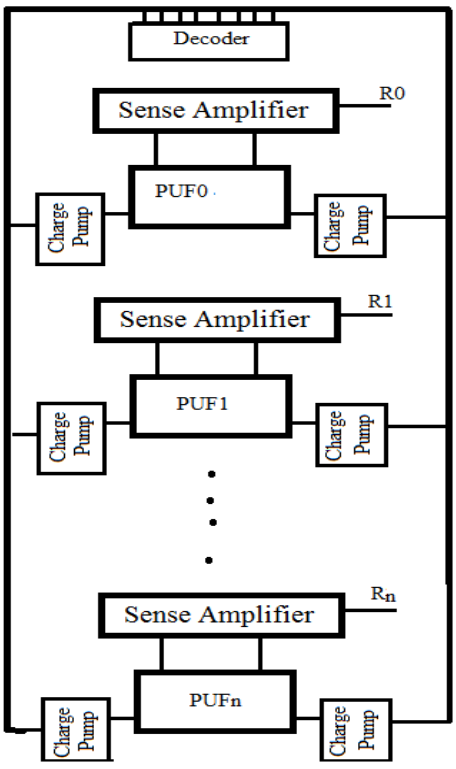

Fig3 Challenge Response Pair generator

3. RESULTS AND DISCUSSION

Performance of METAPUF is determined by 3 quality measure [4, 6, 12, 15, 16, 19]

3.1 Uniformity: - Uniformity determines by the presence of binary '1' and '0' in the response, it must have equal value and half of the response. Obtain result shows that PUF2 and PUF7 the probability of occurrence of binary '1' and '0' slightly lower than ideal value while 6 PUF achieved an ideal value of uniformity as

shown in fig4. Achieved uniformity value is 50% in 6 PUF while for 2 cases its value falls to 49.6% and 49.2%.

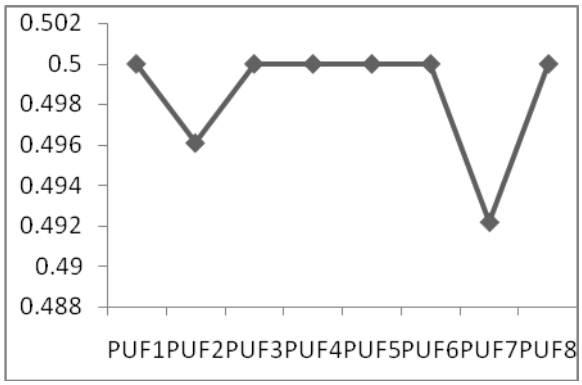

Fig4 Uniformity of PUF

3.2 Reliability: - Response must unaffected by the different operating condition. Reliability measures how much error generated in Response due to temperature variation and supply voltage variation. Reliability is calculated by intra hamming distance of PUF response at different temperature and different supply voltage. Fig 5 shows the error introduced due to supply variation form 0 to1v, the reliability value of supply variation for the MetaPuf is 99.76%.

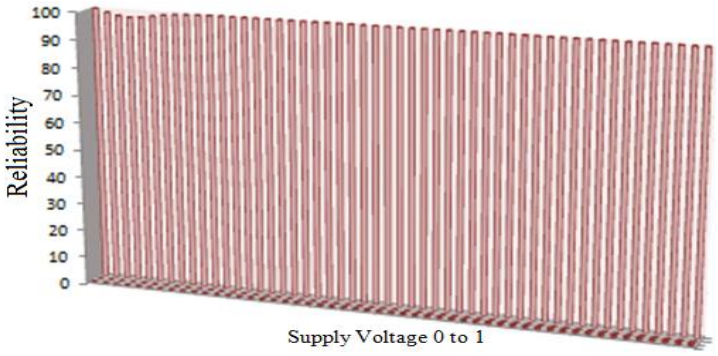

Fig5 Reliability vs Supply Voltage

Fig6 presents the effect of temperature variation over PUF responses. Intra hamming variation of PUF response is simulated in temperature range 0°C to 120°C, high temperature from 60°C PUF start increasing error and reliability falls, the reliability value with temperature variation for the MetaPuf is 96.22%.

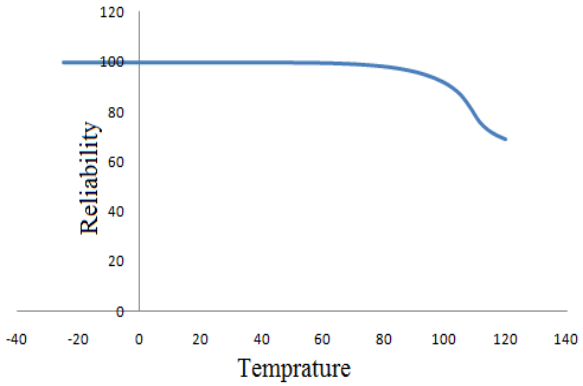

Fig6 Reliability vs temperature (°C)

3.3 Uniqueness: - It measures how much different PUF generate a different response to the same challenge. Uniqueness is measured by inter hamming distance between the response of different PUF. Ideally, its value should be 50 % of response length. Table1 represents the comparative study of METAPUF with existing ROPUF and MUXPUF with 3 quality metrics. Fig7 presents the inter hamming distance when 16-bit of

response produced from PUF, x-axis presents the average number of bit changes for same challenge applied to 32 different PUF i.e. uniqueness and y-axis presents probability of occurrence. Normal distribution function [21,22] with mean 8.23 and standard deviation 0.884; rhe average inter hamming distance between PUF is 51.43%.

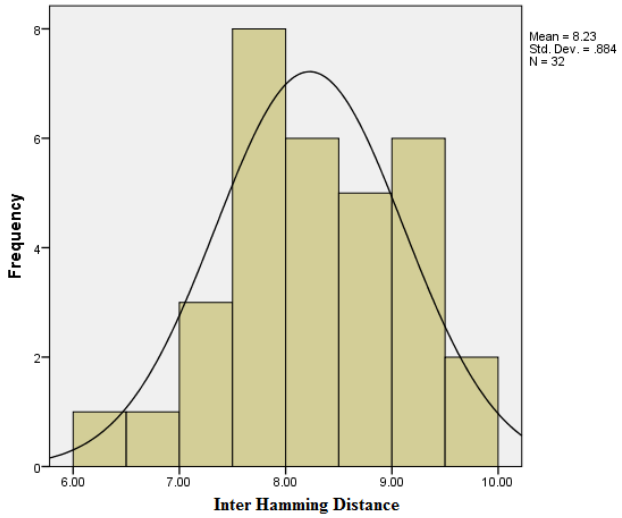

Fig7 Inter hamming distance

Table1Comparision Table of PUF Parameter

Ref →	[1]	[12]	[15]	[16]	[17]	[18]	**Proposed MetaPuf**
Uniqueness	46.14	45.24	50.42	40	95	79.85	51.43
Reliability	99.52	91.14	97.22	95.2	98.7	88.73	99.76* 96.22#
Uniformity		41.15				43	49.85

* Variation in supply (Average value)
# Variation with Temperature (Average Value)

4. Conclusion

In this paper, a unique property of CMOS latch i.e. metastability is selected to generate response bit which qualifies for acts as response bit. MetaPuf contains two parallel feedback path contains up-down charge pump control movement of Q and QB terminal towards metastable point afterward latch settle to unpredictable high or low state. Inter and intra hamming distance measure that response value is comparable with existing PUF and ideal value. It is open research question to identify new CMOS properties to have the new architecture of PUF.

5. References

1. R. G. suh and S devadas,"Physically unclonable functions for device authentication and Response generation" *Proceeding of ACM/IEEE series automation conference* pp. 9–14, (2007)
2. S Kumar, J guajardo, R maes, GJ schrijen and P tuyls,"The Butterfly PUF: Protecting IP on Every FPGA" *Proceedings of the IEEE international workshop on hardware-oriented security and trust,* pp. 67–70, (2008)
3. Erdinc Ozturk, Ghaith Hammouri, and Berk Sunar, "Physically Unclonable Function with Tristate Buffers" *IEEE International Symposium on Circuits and Systems*, pp 3194 – 3197, (2008)
4. Srinivas Devadas, Edward Suh, Sid Paral, Richard Sowell, Tom Ziola and Vivek Khandelwal, "Design and Implementation of PUF-Based Unclonable RFID ICs for Anti-Counterfeiting and Security Applications" *IEEE International Conference on RFID* pp 58-64, (2008)

5. Abhranail Maita, Raghunandan, Anand Reddy and Patric Schamont, "Physical Unclonable Function and True Number Generator: A Compact and Scalable Implementation" *Proceeding of the 19th ACM Great Lakes Symposium on VLSI*, PP 425-428, (2009)
6. Eiroa, S.; Baturone, I. ; Acosta, Antonio José ; Dávila, JorgeJacobs and C.P. Bean, "Using physically unclonable functions for hardware authentication: A survey," *Proceedings XXV Conference on Design of Circuits and Integrated Systems,* pp 1-6, (2010)
7. A maiti, I kim and P schaumont , "A robust physical unclonable function with enhanced challenge-response set*" IEEE Transaction on information forensics security* vol. 7, no. 1 pp. 333–345, (2012)
8. Masoud Rostami, Farinaz Koushanfar, and Ramesh Karr, "A Primer on Hardware Security: Models, Methods, and Metrics" *Proceedings of the IEEE* Vol 102 No 8, pp 1283-1295, (2014)
9. Miodrag Potkonjak and Vishwa Goudar, "Public Physical Unclonable Functions" *Proceedings of the IEEE*, Vol.102,No.8 pp 1142-1156, (2014)
10. Lilian Bossuet, Xuan Thuy Ngo, Zouha Cherif and Viktor Fischer,"A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon*" IEEE Transactions on Emerging Topics in Computing*, Vol 2, Issue: 1, pp 30-36, (2014)
11. Ji-Liang Zhang, Gang Qu, Yong-Qiang Lv and Qiang Zhou, "A Survey on Silicon PUFs and Recent Advances in Ring Oscillator PUFs*" Journal of Computer Science and Technology,* Vol29(4) pp 664–678, (2014)
12. Sauvagya Ranjan Sahoo, Sudeendra Kumar and Kamalakanta Mahapatra,"A Novel ROPUF for Hardware Security*" IEEE International Symposium on Nan electronic and Information Systems,* pp 320-324, (2015)
13. Yier Jin, "Introduction to Hardware Security" *Electronics letter* Vol4 pp 763-784, (2015)
14. Abdelkarim Cherkaoui, Lilian Bossuetyand C´edric Marchand,"Design, Evaluation and Optimization of Physical Unclonable Functions based on Transient Effect Ring Oscillators" *IEEE Transaction on Information, Forensic and Security* ,pp 1291-1305, (2015)
15. Abhranil Maiti and Patrick Schaumont,"Improved Ring Oscillator PUF: An FPGA-friendly secure primitive" *Journal of cryptography*, vol24 pp 375-397, (2011)
16. Yuan Cao, Le Zhang, Chip-Hong Chang and Shoushun Chen,"A Low-Powers Hybrid RO PUF With Improved Thermal Stability for Lightweight Applications" *IEEE Transaction on Computer-Aided Design of Integrated Circuits and System*, Vol 34 No 7, pp 1143-1147,(2015)
17. J. W. Lee, Daihyun Lim, B. Gassend, G.E. Suh, M. van Dijk and S. Devadas,"A technique to build a Response in integrated circuits for identification and authentication application," in *Proc. Symp. VLSI circuits*, Honolulu, HI, USA, pp. 176–179, (2004)
18. Zouha Cherif Jouini, Jean-Luc Danger and Lilian Bossuet,"Characterization of Physically Unclonable Functions at Design Stage" Colloque du GDR SoC-SiP, Paris, France <hal -00753222>, (2012)
19. Paolo Maffezzoni; Luca Daniel,"Exploiting Oscillator Arrays as Randomness Sources for Cryptographic Applications" *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, Volume: PP, Issue: 99, pp 1-1, (2017)
20. Bertrand Cambou, "An XOR Data compiler: combine with a physical unclonable function for true random number generator" *Computing Conference*. DOI 10.1109/SAI.2017.8252190, (2018)
21. Benjamin Durakovic, "Design of Experiments Application, Concepts, Examples: State of the Art", Periodical of engineering and Natural Sciences, Vol. 5, No. 3, pp. 421-439 (2017).
22. Halil İbrahim Çelik, "Determination of Air Permeability Property of Air-Laid Nonwoven Fabrics Using Regression Analyses" Periodical of engineering and Natural Sciences, Vol. 6, No. 1, pp. 210-216 (2018)