A Reliable Current Starved Inverter based Arbiter Puf Architecture for Iot Applications

Anil Kumar. Kurra, Usha Rani.Nelakuditi

Abstract— In the recent years, Physical Unclonable Functions(PUFs) are emerged to be one of the lightweight hardware security primitives for device authentication, identification, such as Internet of things (IoT). IoT comprises connection of multiple number of nodes (devices) for exchanging the information across different networks. PUFs can sense the minute and unavoidable process variations during the fabrication process and generates the unique number of challenge-response pairs(CRPs), which can be stored and extensively used for secure associations between smart devices in IoT. Arbiter PUFs and ring oscillator PUFs are most commonly used strong PUFs in current day scenario. The conventional Linear arbiter PUFs are suffers from low reliability and vulnerable to Machine Learning attacks. In this paper, we proposed a Current starved Inverter (CSI) based arbiter PUF which enhances the non- linearity and randomness. The Proposed architecture was simulated using cadence spectre CMOS 45nm technology and estimated its metrics such as uniqueness reliability and uniformity.

Keywords— Current starved Inverter (CSI) ,Physical Unclonable Functions(PUFs),Arbiter PUF, Hardware security, Machine Learning attacks.

I. INTRODUCTION

Over last one decade Internet-of-things (IoT) consequently emerged to be as one of the landmark in rapid development of smart homes, smart cities. IoT provides a wonderful platform to exchange the information between different objects without intervention of human beings or computer supervision. And it can acts a bridge between several technologies like wireless communication, micro-electro mechanical systems(MEMS), sensor technologies and internet. IoT devices are extensively used in wide number of applications such as infrastructure management, energy management, medical, environmental monitoring, economic process home automation and transportation. The IoT nodes such as bio-chip transponders, smart thermostats, RFID tags, Wi-Fi connected electronic home appliances quantitatively generates the huge amount of sensitive data and information between the node to node. Hence, a set of methods to be employed to authenticate the secure data information against the device tampering, privacy breach, denial-of service, spoofing, information disclosures etc.

Since the IoT nodes are inherently resource constrained and also rises the power dissipation issues, therefore the traditional cryptographic algorithms and protocols are sufficiently not possible to incorporate in to the IoT devices, hence a novel measures must be adopted to provide the lightweight authentication to the IoT devices.

Hence to counter attack the above mentioned constrains In IoT ,In recent years Physical Unclonable Functions (PUFs) are introduced as one of the hardware cryptographic primitive in IoT applications. PUF is a simple physical entity and it could be embodied in a physical structure it is to fabricate and practically not possible to clone. By utilizing the unavoidable process variations makes each and every IC is unique and random its properties. When an electrical stimulus being applied to the input of the PUF circuit and it produces the unpredictable random output. Eventually the applied input treated to be "challenge" and corresponding output considered as a "response". In particular specific challenge and its response together called to be challenge- response pair(CRP). Figure 1&2 illustrates the basic CRP function for PUF circuit and PUF behavior in different ICs . The assessment of the PUF circuit can be done by characterizing the physical properties of the PUF circuit. These PUF circuits can also be used for device authentication and identification[1],IC-counterfeiting [2],cryptographic key storage[3],smartcard authentication, keyless secure communication etc.

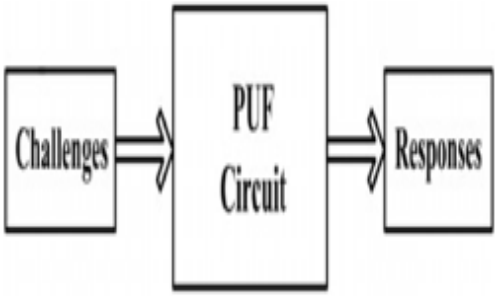

Figure 1.Challence Response protocol in ICs.

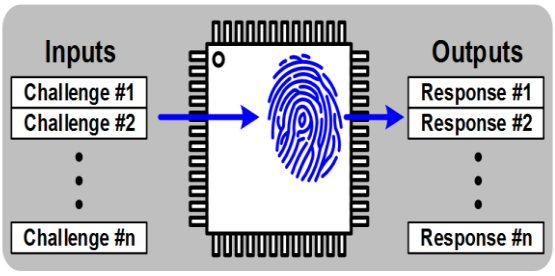

Figure 2.PUF mechanism in ICs.

Depending upon the nature of the CRPS pair PUFs can be categorized in to two types such as strong PUFs and weak PUFs. Strong PUFs can be used for the authentication and weak PUFs as for cryptographic key generation. The properties of strong and weak PUFs are represented by table1.

Revised Manuscript Received on December 15, 2019.
Anil Kumar. Kurra,Ph.D Scholar, ECE VFSTR(Deemed to be university) Vadlamudi,India-522213. kakumar94@gmail.com
Usha Rani.Nelakuditi, Professor, ECE VFSTR(Deemed to be university) Vadlamudi,India-522213. usharani.nsai@gmail.com

Table1.comparision of weak PUFs and strong PUFs

Weak PUFs	Strong PUFs
Limited number of CRPs	Large number of CRPs
Responses are stable from noise and environment variations for multiple readings.	Response generated from an each challenge could be strong enough to environmental variations (better reliability).
Output response should be preserve private	No restriction to preserve the output response
Susceptible to invasive attacks	Not susceptible any attacks
Response is strong enough and depends on intrinsic process variations.	Not feasible to manufacture two PUFs with the same responses
Example: Anderson PUF	Example: Memory based PUFs, delay based PUFs.

The rest of the paper is organized as follows section 2 describes the introduction to arbiter PUFs. Section 3 provides the various types of security metrics to measure the performance of the PUFs. Section 4 describes the overview of CSIs and proposed methodology of CSI based arbiter PUF and finally section 5 describes the conclusion.

II. ARBITERS PUFs

An arbiter PUF and ring oscillator PUFs are two different kinds of the delay based PUFs. An arbiter PUF was first developed by the researchers at MIT, by utilizing the intrinsic timing delay difference of two symmetrical designed paths. The main advantage of the arbiter PUF has exponential number of the challenge response pairs(CRPs),enables lightweight and cost-effective authentication of ICs. This architecture consists a chain of switches (multiplexers) are connected at top and bottom of the each stage and arbiter (D-flip flop/SR-flip flop) at the end of the chain .Figure 3 depicts the basic architecture of the N-bit arbiter PUF. An N-bit arbiter PUF requires the n-bit challenge and generates the single bit response. A pair of the multiplexer as denoted by the switching element. when n-bit challenge is applied to the chain of the multiplexers, each bit of a challenge should controls the pair of the paths either cross or straight and an impulse signal is feed at the input of arbiter PUF to excite the paths simultaneously. Due to uncontrollable process variations in the each multiplexer the output is transferred symmetrically, The final response being decided by the arbiter by comparing the analogy timing delay difference and converts in to digital value. If suppose the rising edge of the signal arrives at the input of the arbiter earlier than signal reaches at bottom input, then the output will be one, Otherwise the output will be zero. The conventional arbiter PUFs are suffers the poor security metrics such as reliability, uniformity ,uniqueness and also suffers invasive attacks etc. Hence By considering the security metrics to enhance the performances of the PUF ,Gassend [4][5] introduced a non linear arbiter PUFs such as feed-forward arbiter PUF,XOR arbiter PUF, lightweight security PUF, mux/demux reconfigurable PUF etc. In feed- forward arbiter PUFs architecture the non-linearity can be achieved by arbiters at the intermediate stages of the original MUX structure, the output of the intermediate arbiter acts as the challenge for the subsequent stages And also it avoids the linear delays, there by attackers cannot model the delay of the PUF. Figure 4 illustrates the feed-forward arbiter PUF. The feed- forward arbiter PUF significantly improves the performance of the PUF behavior, but primarily it suffers from reliability issue mainly due to environmental variations and ageing[6].

Figure 5 depicts the architecture of the XOR arbiter PUF. Instead of using the multiple number of arbiters at the intermediate stage, the output of the multiple arbiters are XORed to produce non-linear delay. In the above figure the output of the two conventional arbiter PUFs are XORed, which leads to generates the non-linear response without effecting the reliability and resilient to modeling attacks certain level. Hence to mitigate the above problems proposed a CSI based arbiter PUF architecture, which significantly enhances the security metrics and resists the attacks over the PUFs[10].

III.PUF Metrics

As the scaling down of the VLSI technology beyond its ability, which leads to imperfections in fabrication process, hence this causes the randomness in electrical and physical parameters of ICs. This property can be explicitly observed in CMOS technologies and by enabling this property PUF circuits can generate the unique CRPs. The efficiency of the PUF design can be evaluated by using a set of metrics, here we are going to address the most commonly used design metrics, as follows

3.1 Uniqueness:

It the measure of dissimilarity of PUF responses by applying the same challenge across different dies. It can be estimated by Inter-Chip hamming distance (HDinter). The ideal value of HD should be 50%, it indicates that, The obtained response should consist of equal amount of '0's and '1's. It can be computed by equation (1).Figure 6 illustrates the comparison of uniqueness.

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

Ri, Rj indicates the responses generated from two different chips under same challenge. N indicates the size of bit length and d represents the number of devices respectively.

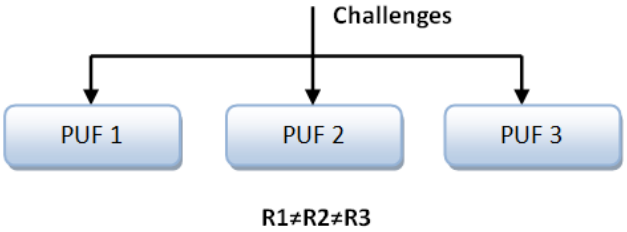

Figure 6.Interchip- variations of different devices.

3.2 Reliability:

Reliability of a PUF refers to the ability to reproduce the same kind of a response repeatedly for a given set of a challenge irrespective of the external factors. It is one of the most important metric, that the designer taken in to the account while designing the PUF architecture. Ideally the reliability of PUF should be 100%. Reliability can be estimated by using equation 2.

$$\text{Reliability}= \frac{1}{s}\sum_{i=1}^{s}\frac{HD(Ri,Ri')}{n}\times 100\% \qquad (2)$$

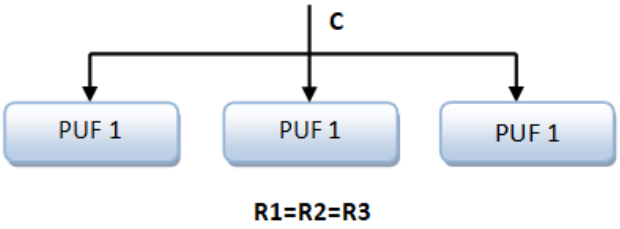

Figure 7.Intra- variations among same device.

3.3 Uniformity:

Figure 8 shows the basic diagram for measurement of uniformity. It assess the randomness of a PUF response and indicates the ratio of '0' and '1' in a given response from PUF architecture. For an ideal PUF the randomness is should be 50%.it can be mathematically expressed using the hamming weight of the response as follows.

$$\text{uniformity}= \frac{1}{K}\sum_{i=1}^{K} Ri \times 100\% \quad (3)$$

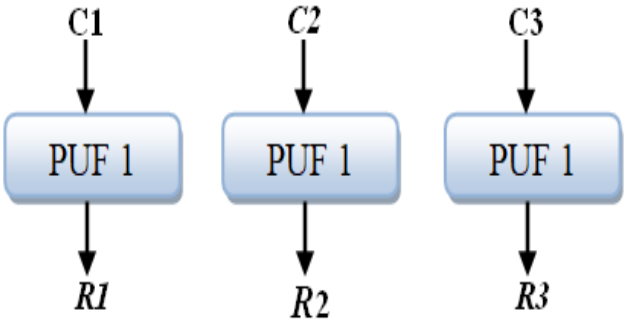

Figure 8 .Estimation of uniformity

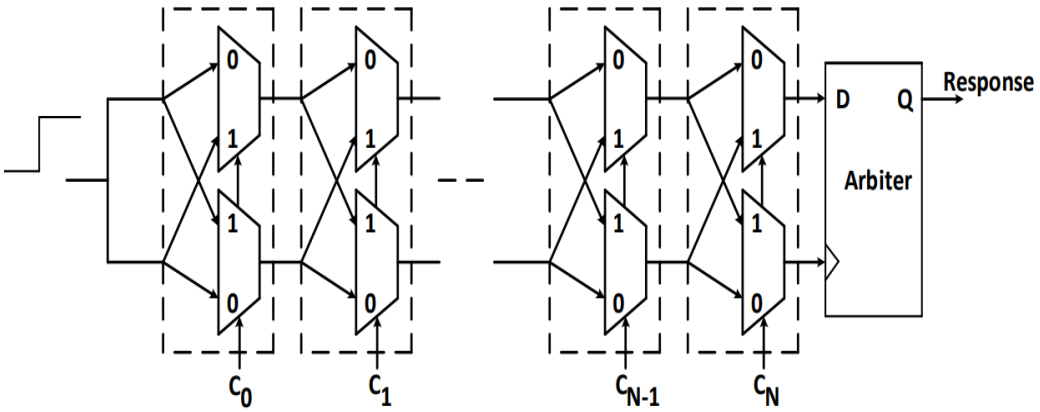

Figure 3. Schematic of the linear N-stage arbiter PUF.

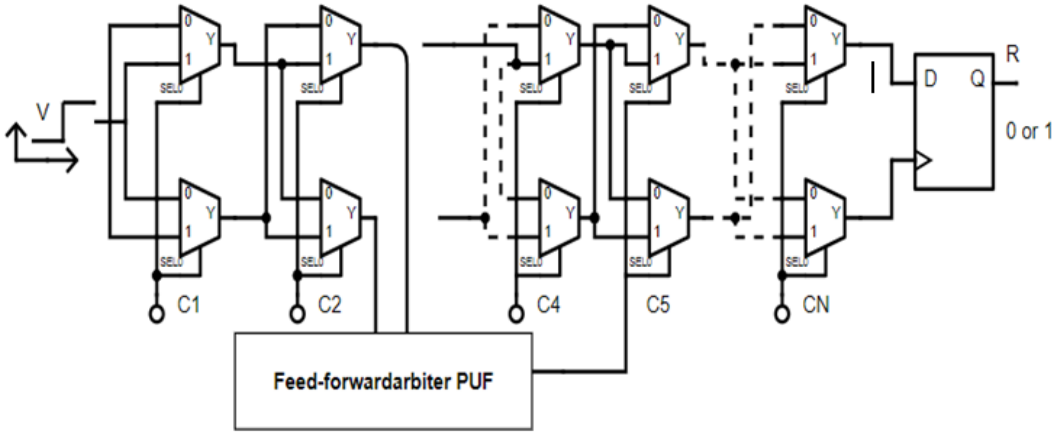

Figure 4. Feed-forward arbiter PUF architecture.

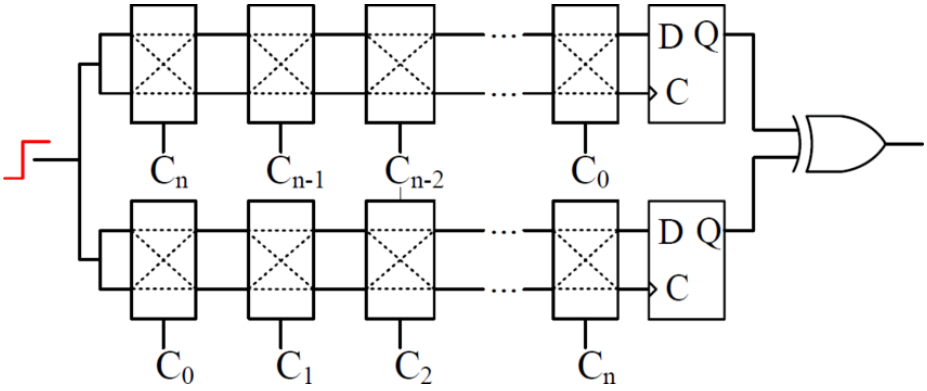

Figure 5. XOR arbiter PUF architecture.

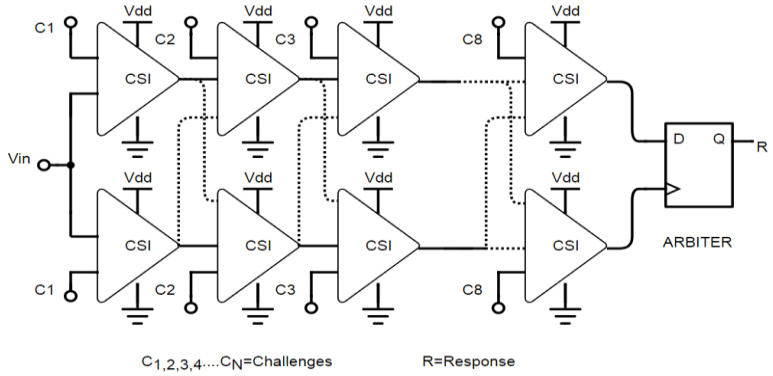

Figure 9: 8 stage CSI based arbiter PUF.

IV. CURRENT STARVED INVERTER

The proposed 8 stage CSI arbiter PUF as shown in figure 9,Each stage introduces an amount of time delay and its Delay can be altered non-linearly without introducing any external arbiters at the middle of the architecture and this can be varied mainly due to variations of the voltage at each and every individual stage. The architecture consist of two CSI elements at top and bottom stage and an input pulse signal is given to the two parallel connected CSI inverters and applied control voltage can acts as the challenge for the each and every stage. Due to applied input and control voltage results variations in the final delay difference and it can be detected by using the arbiter(D-latch) respectively. The switching element of CSI shown in figure 10 respectively. The performance of the proposed 8-stage CSI arbiter PUF is implemented in 45nm CMOS technology and estimated its metrics such as uniqueness, reliability and uniformity by applying the monte-carlo analysis.

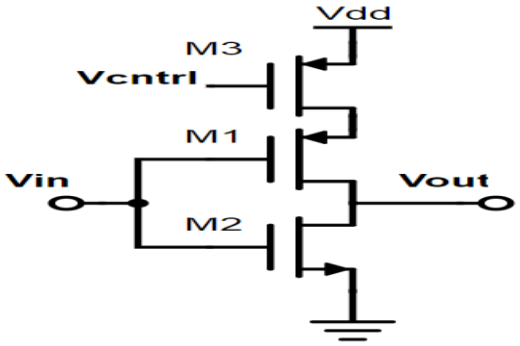

Figure 10: switching element (Current Starved Inverter (CSI)).

V. RESULT DESCRIPTION

To characterize the behavior of the PUF applied a set of 200 iterations and 100 number of samples at the each corners(SS,SF,FS,FF,TT). Its final response were being measured with respect to the 3 sigma plot. Figure 11 depicts the variations of delay due to the process variations. We applied a set of 50 random challenges and its output being constantly measured by applying the 200 number of iterations and 100 number of samples at each and every stage. From the obtained statistical data we observed the maximum amount of yield such as uniqueness should be 47.25%,reliability-82% and randomness 47% respectively. Figure 12 illustrates the maximum amount of mean at 25^0C.

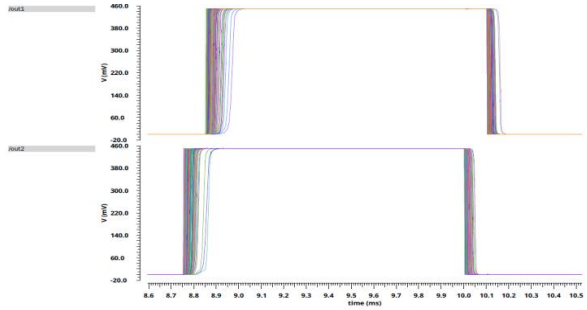

Figure 11:Variation of responses applying Monte- Carlo analysis.

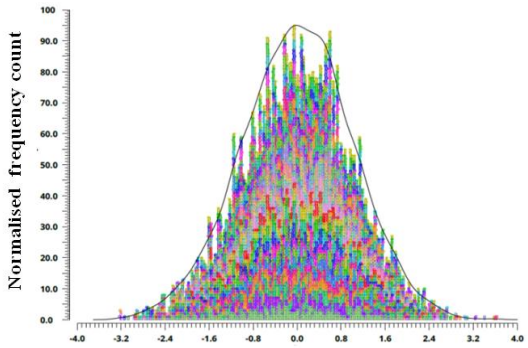

Figure 12:Frequnecy distribution of CSI PUF.

VI. CONCLUSION

At present scenario PUFs plays an effective role in device authentication. The proposed architecture significantly enhanced its performance in all security aspects and also switching elements requires only three transistors at each stage. Hence these type of the circuits can be suitable for the resource constrained devices such as IoT based applications. And our future work is directs toward the fabrication of the proposed PUF and to deployed in to the IoT security protocol respectively.

REFERENCES

1. M. Rostami, F. Koushanfar, and R. Karri. A primer on hardware security: Models, methods, and metrics. Proceedings of the IEEE, 2014.
2. Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld. Physical one-way functions. Science, 297(5589):2026–2030, 2002.
3. J. W. Lee, Daihyun Lim, B. Gassend, G. E. Suh, M. van Dijk and S. Devadas. A technique to build a secret key in integrated circuits for identification and authentication applications. In 2004 Symposium on VLSI Circuits, pages 176–179, June 2004.
4. F. Tehranipoor, W. Yan, and J. A. Chandy. Robust hardware true random number generators using DRAM remanence effects. In 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pages 79–84, May 2016.
5. J. W. Lee et al. A technique to build a secret key in integrated circuits for identification and authentication applications. In Symposium on VLSI Circuits. Digest of Technical Papers, pages 176–179, June 2004.
6. R. Yashiro, T. Machida, M. Iwamoto, and K. Sakiyama, “Deep-learning based security evaluation on authentication systems using arbiter PUF and its variants,” in Advances in Information and Computer Security, and its variants,” in Advances in Information and Computer Security. Ogawa and K. Yoshioka, Eds. Cham: Springer International Publishing, 2016, pp. 267–285.
7. U. R¨uhrmair, F. Sehnke, J. S ¨olter, G. Dror, S. Devadas, and J. ¨u. Schmidhuber, “Modeling attacks on physical unclonable functions,” Proceedings of the 17th ACM conference on Computer and communications security - CCS ’10, p. 237, 2010.
8. U. Ruhrmair, J. Solter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, “PUF modeling attacks on simulated and silicon data,” Trans. Info. For. Sec., vol. 8, no. 11, pp. 1876–1891, Nov. 2013. [Online].
9. G. Hospodar, R. Maes, and I. Verbauwhede, “Machine learning attacks on 65nm arbiter PUFs: Accurate modeling poses strict bounds on usability,” in 2012 IEEE International Workshop on Information Forensics and Security (WIFS), Dec 2012, pp. 37–42.
10. Anil Kumar Kurra *and* Usha Rani nelakuditi, “A secure arbiter physical Unclonable functions (PUFs) for device authentication and identification” Indonesian Journal of Electrical Engineering and Informatics (IJEEI), Vol. 7, No. 1, pp. 118-128, 2019.