IJCTA, 9(41), 2016, pp. 115-121 ISSN: 0974-5572

PUF Based challenge Response Pair For Secured Authentication

Abhishek Kumar*, Ravi Shankar Mishra and K. R. Kashwan*****

ABSTRACT

PUF are recent developed circuit in hardware security area. It takes advantage of uncontrollable feature of silicon IC which can have measureable output to generate a random, unpredictable secret key. PUF circuits are able to generate key at run time while in classical method key was stored in random access memory. Storing in RAM enhance cost of system, it suffers from leakage information leaks from memory. Leakage current of RAM provides a fingerprint/pattern of secret key; adversely stores it and statically guess the secret key. CMOS based PUF do have their own leakage but each bit of response for every challenge is generated from unique design. Mux based PUF utilizes delay of individual stage, RO based PUF utilizes frequency variation between stages, SRAM based PUF utilizes startup value of each cell; input signal have to go through a large number of stages. Static CMOS designs have maximum leakage, while differential dynamic CMOS have minimum leakage, a non specific pattern found between challenge and response pair. Inter and intra chip variation measure that PUF based secrete generation is reliable and uniqueness.

Keywords: PUF; MUX-PUF; RO-PUF;Weak PUF; Strong PUF; PUF Quality measure;

1. INTRODUCTION

Physical Unclonable Function is an emerging technology in cryptographic protocol and security architecture. Classic Cryptographic protocol relies on secret key for data which is stored on non volatile memory. However storing secret key on chip memory prone to attack. An encryption engine converts plain text to cipher text using secret key through rigorous computation. During computation there is leakage of valuable information in terms of power, electromagnetic radiation. The leakage power are highly correlated with input switching pattern, if a large number of sample is stored statically secrete key can be guessed making security null and void[6]. Post fabrication one time password authentication enhances security level at additional cost. PUF are promising initiative for authentication and cryptographic application. PUF derive secret key from physical characteristics of silicon integrated circuit, it eliminate the requirement of storing key on expansive memory[16]. Fig1 presents block diagram of PUF circuit, it select a unique physical characteristics which is superimposed over challenge input and generate a response for each challenge. Security is decided by selection of physical properties [4]; a well-known fact that two silicon device with dame feature is almost impossible to fabricate. Response for each challenge is function of device properties same response cannot be generated from any other silicon device. PUF usesmanufacturing variability to generate challenge response pair[27]

Classically user stores the secret key in security module of system to be authenticated. In order to authenticate user applies challenge (secret key) which is a pseudo random number generated from linear feedback shift register, if applied challenge matches with stored key system will be authenticated shown in fig 1. Limitation of classical technique is secrecy of stored key in non volatile memory which consistently leaks current. Adversely adds a small resistor of 1 ohm in series with supply voltage and record power

* Assistant Professor Lovely Professional University Phagwara, Punjab, India, *Email: abhishek.15393@lpu.co.in*

** Associate Professor Lovely Professional University Phagwara, Punjab, India, *Email: ravi.19053@lpu.co.in*

*** Professor & HOD / Dean-PG Sona College of Technology Salem, TN, India, *Email: drkrkashwan@gmail.com*

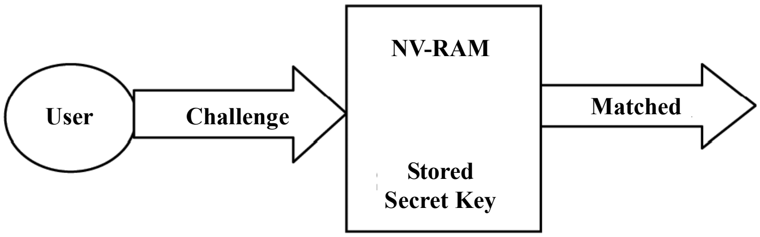

Figure 1: Classical Authentication Scheme

consumption for each challenge, if adversely compare the leakage power with re-generated one later statically it is possible to guess the correct key.

Fig 2 present PUF based authentic system; where initially user creates a challenge response pair in trusted environment and stored in the security module of the system [5]. Whenever user want to authenticate applies a challenge even in entrusted environment; if current generated response and stored response both approximately matched authentication succeed. To prevent man in middle attack the challenge-response pair cleared from database after each authentication. Requirement of PUF based authentication challenge-response pair must be large. Basically PUF is black box whose generated response is a function of internal parameter; these internal parameters are hidden in hidden because they represent variability associated with circuit.

PUF is broadly classified as strong PUF and Weak PUF, Strong PUFs are preferred for authentication, while weak PUF are preferred for key storage. Weak PUF have a small number of CRP while strong PUF can have large number of CRP [2, 3, 10]. Table 1 present a comparative study of weak PUF and strong PUF.

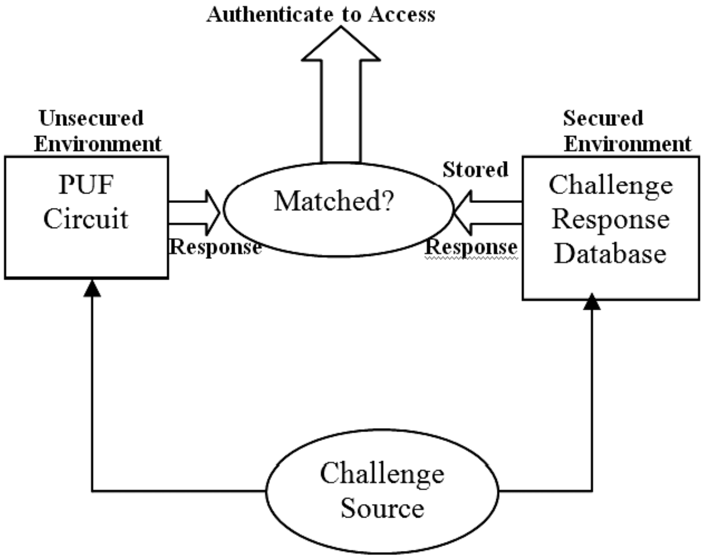

Figure 2: PUF Based Authentication Scheme

In section II, we describe the existing mux-arbiter, ring oscillator and SRAM PUF based response generation. In section III, we present the quality metric evaluation in terms of inter hamming and intra hamming distance. In section IV, we summarize this paper.

2. RELATED WORK

2.1. Arbiter PUF

Fig 3 represents mux-arbiter based delay PUF; wheredelay between two parallel identical path decide one bit response. It contains two identical path with different delay and an arbiter as decision device [19]. Basic idea of arbiter based PUF is race between identical paths and determine which path is faster. Delay stage is

Table 1
Weak PUF Vs Strong PUF

Weak PUF	*Strong PUF*
Small number of challenge response pair	Large number of challenge response pair
Response are unaffected from noise and environmental condition	Responses stable to environment
Response are unpredictable and strongly depends on intrinsic variability	CRP not maintain a correlation, new response cannot guessed based on previous CRPs
Two device cannot have similar finger print	Not possible to design two PUF have same response for same challenge
Response must processed though error correcting circuit to generate secret key for cryptographic purpose	Response can authenticate directly without using any cryptographic hardware.
Output response of PUF must preserve private	No restriction of preserving output response
Susceptible to attack	Not susceptible to attack
Example-SRAM PUF	Example-OpticalPUF, ArbiterPUF, Ring oscillatorPUF

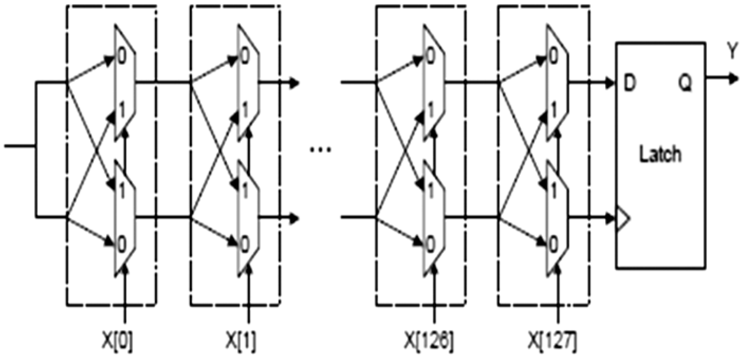

Figure 3: Mux Based 1-Bit Response [7, 18, 29]

implemented using 2:1 multiplexer, input challenge X[i] allows the mux to works as transfer or switch devices if X[i] is 0 input signal (generally rising wave) passes through top and bottom path otherwise intermediate path. In delay associated with each path have been influenced the rising input signal. The signal races through identical path and arbiter (decision device) at the end decide which of the path is faster; if D signal to D latch is faster output is 1 otherwise 0.

A mux is implemented as delay stage, depending on weather challenge bit is 0 or 1 signal is delayed by upper and lower path. Consider delay of two upper path in each mux is a_i and b_i. Let $H_i = (a_i + b_i)/2$ and $y_i – (a_i-b_i)/2$ signal going through upper path is delayed by Hi + $(–1)^{ci}y_i$ assuming there are total n/2 stage than total delay in upper path equals

$$D_H = \Sigma_{i=1}^{n/2} H_i + (-1)^{Ci} y_i \tag{1}$$

Similarly delay of lower path in each mux is d_i and f_i Let $L_i = (d_i+f_i)/2$ and $u_i = (d_i-f_i)/2$ signal going through lower stage is delayed by $L_i + (–1)^{ci}u_i$ Therefore, the total delay in the lower path given as

$$D_L = \Sigma_{i=1}^{n/2} L_i + (-1)^{Ci} u_i \tag{2}$$

Signal travelling through upper and lower path will interact decision device at the end. Condition to determine output bit response is

$$\begin{aligned} D_H < D_L \quad R = 1 \\ D_H > D_L \quad R = 0 \end{aligned} \tag{3}$$

Where setup time of arbiter and wire delay has been ignored. As the input challenges size is larger for AES128, AES192 and AES256; 128, 192 and 256 bit respectively circuit will becomes longer to determine one bit response. Same circuit copied 128 time with shuffling the delay stage randomly to determine 128 bit of response.

2.2. Ring Oscillator-PUF

Ring oscillator is a simple CMOS circuitry to generate different frequency stage where odd number of delay stage in cascaded chain determine a unique oscillating frequency f. Random variation in cmos manufacturing put deviation into in frequency f ± Δf. Basic idea of ROPUF is the frequency with variation shown in fig4. A group of N ring oscillator generate N different frequency where rising and falling edge are different of each oscillator and it depends on inverter in the ring oscillator loop [14, 15, 21]. User apply the challenge to control line of analog multiplexer, it select a particular frequency generated by ring oscillator. Two parallel mux routes tow independent frequency (f1 and f2) to counter circuit. Size of counter must be large enough to have sufficient entropy. For an applied challenge counter is compared if Q1>Q2 i.e. f1>f2 response bit set to 1 else 0. Each comparison of a pair of ring oscillator generated 1bit response, from*N* ring oscillators N (N-1)/2 distinct pairs are possible.

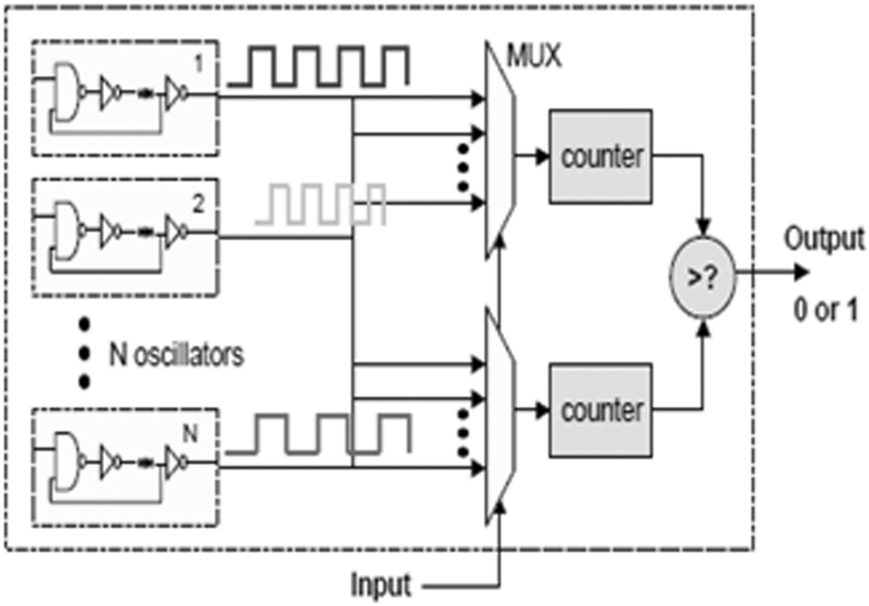

Figure 4: Ring Oscillator Based 1-Bit Response [6, 20]

2.3. SRAM-PUF

Static random access memory is based on bi-stable latch which retains its value as long power is ON. Fig 5 represents CMOS implementation SRAM requires 6-transistor for each bit arranged as 4 transistor as two crossed couple inverter and two access transistor they control access of cell during read and write by turning on WL line [12, 24, 30].

When SRAM is off input to each inverter is 0 bi-stability feature turn the output node Q as 10 or 01. Q will be 0 or 1 depends on width, length and threshold voltage of transistor in cell. If M_4 transistor dominant M_5 Q will pull up similarly M_5 dominant over M_4 Q will pull down. A complex interaction between physical variables determines (BL and BL) at the end (sense amplifier) the logical preference states of the memory cells[13,23]. To determine N response bit, N number of SRAM cell in N different variable are used. After each cycle SRAM must be power off to erase the stored content startup value of each cycle are random and unpredictable yields 1-bit responses[22].

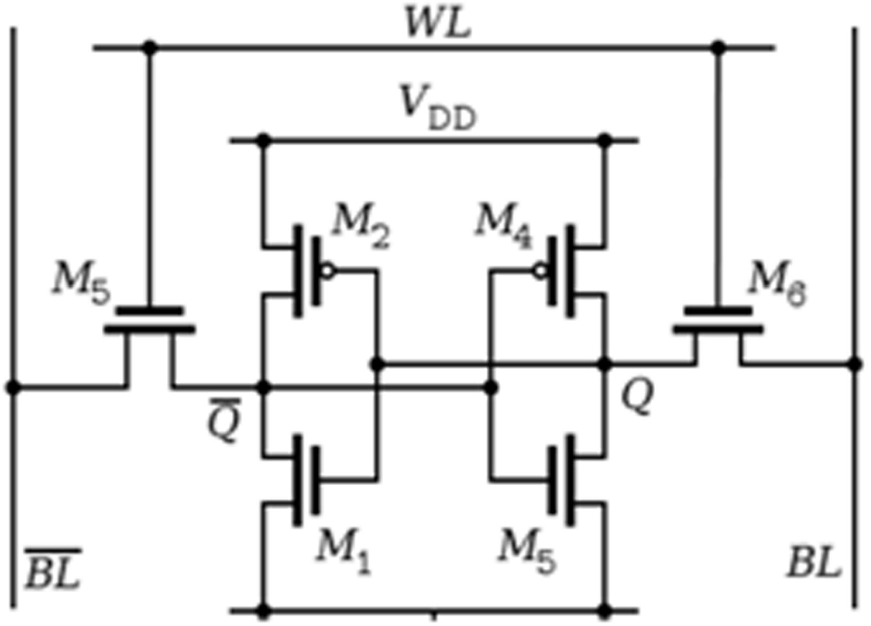

Figure 5: 1-BIT SRAM Cell 1 bit Response [8, 17]

3. PUF PERFORMANCE EVAULATION

According Hori et al [31]PUF qualities measured in term of randomness, correctness, steadiness, diffuseness, uniqueness. Maiti et al [27] says PUF qualitied as uniformity, bit aliasing, uniqueness, and reliability. Majzoobi [5, 6] et al described quality by single bit probability and conditional probability of response. In previous work Reliability and uniqueness is common which id measured in term of inter and inter hamming distance, in this work a comparative study of reliability and uniqueness is discuss for arbiter, RO and SRAM PUF. [1, 25]

(i) *Reliability:* Ability of PUF to reproduce over varying operating condition such as temperature, noise, supply voltage fluctuation. Response to each challenge should be stable. Intra hamming distance measure the probability that response will flip when a random selected challenge applied multiple time. Reliability os measured is term of intra hamming distance. Ideally intra hamming distance of PUF should be 0 represents 100% reliable [1, 26]

$$d_{\text{int}ra}(C) = \frac{1}{s}\Sigma_{J=1}^{s}\frac{HD(R_i, R_{i,j})}{m}\times 100\% \tag{4}$$

Where Ri id PUF response at normal condition Ri,j jth sample of Ri for challenge C.

(ii) *Uniqueness:* Ability to PUF to generate random response for same challenge from separate device. Difference in response of two PUF should be large. Uniqueness is measure in term of inter hamming distance, for ideal PUF hamming distance would be 50%.

$$d_{\text{int}er}(C) = \frac{2}{K(K-1)}\Sigma_{i}^{K-1}\Sigma_{J=i+1}^{K}\frac{HD(R_i, R_j)}{m}\times 100\% \tag{5}$$

Where HD(Ri, Rj) presenthamming distance between two response Ri and Rj for same challenge C from two PUF. K is the number of device and m number of bit per response,

(iii) *Security*: Ability of PUF to resistant from physical attack, generated response must be secret and should not guess through reverse engineering or side channel attack. If all information related to circuit and challenge are still PUF should immune to active and passive attack.

4. CONCLUSION

In this work challenge response paid based authentication reviewed based on manufacturing variability of silicon cmos circuit. PUF uses intrinsic featureof silicon device which is inherent are combined or coded through error correcting circuit to generate secret key. Mux and ring oscillator PUF both is kind of delay based PUF but mux puf is faster having simple circuit consume less power. Mux puf preferred for resource constrained platform like RFID and RO-PUF preferred for secured processor design. Mux-Arbiter based puf is reliable while RO and SRAM PUF generate more unique response. A variable feature of analog circuit can turn to puf circuitexample bit line of SRAM through applied into sense amplifier are design dependent, recovery of a flip flop from indefinite state to definite state are unpredictable, leakage current from starved chain, current mirror output are design dependent.

REFERENCES

[1] Y Lao and KK Parhi, “Stastical analysis of mux based physically unclonable function” IEEE transaction on computer aided design of integrated circuit and system, vol35 no5 pp 649-662, 2014.

[2] Helena handschuh, Geert jan schrijen and Pim tuyls, “Hardware intrinsic security from physically unclonable function”Towards hardware-intrinsic security part of the series information security and cryptography pp 39-53, 2010

[3] Charles herder et al, “Physically unclonable function and applicatin:A tutorial” Proceeidng of IEEE vol102 no8, 2014

[4] S Devadas et. al, “Design and implementation of PUF-based unclonable RFID IC for anti-ounterfeiting and security applications” in Proc. IEEE Int. conf. RFID, pp. 58–64, 2008

[5] M majzoobi, F koushanfar and Mpotkonjak, “Lightweight secure PUF” ACM/IEEE Int. Conf. Comput.-Aided Design, pp. 670–673, 2008.

[6] M majzoobi, M rostami, F koushanfar, DSwallach and S devadas, “Slender PUF protocol: A lightweight, robust, secure authentication by substring matching,’’ IEEE CS security and privacy workshop pp. 33–44, 2012

[7] GE suh and S devadas, “Physical unclonable functions for device authentication and secret key generation” in Proc. ACM/IEEE sesign autom. conf pp. 9–14, 2007

[8] R.S pappu, PS.ravikanth, B recht, J taylor and N gershenfeld, “Physical one-way functions” science, vol. 297 pp. 2026–2030, 2002

[9] Bhargava, Mudit, “Reliable, Secure, Efficient Physical Unclonable Functions” PhD thesis carnegie Mellon University, 2013

[10] R maes, Anthony van herrewege and Ingrid verbauwhede, “PUFKY: A fully functional PUF-Based cryptographic key generator” lecture notes in computer science, chapter cryptographic hardware and embedded systems, vlo7428 pp302–319,2012.

[11] Daihyun Lim et.al, “Extracting secret keys from integrated circuits” IEEE Trans. VLSI Syst. vol13 no10 pp 1200–1205, 2005

[12] M bhargava, C kakir and K mai. “Attack resistant sense amplifier based PUFs (SA-PUF) With deterministic and controllable reliability of PUF responses” IEEE International symposium on int hardware oriented security and trust (HOST)pp106-111, 2010

[13] M bhargava, C kakir and K. Mai, “Comparison of bi-stable and delay-based physical unclonable functions from measurements in 65nm bulk CMOS” Proceedings of the IEEE 2012 custom integrated circuits conference, pp1-4 2012

[14] Blaise gassend, Dwaine clarke, Marten van dijk and S devadas, “Silicon physical random functions” Proceedings of the 9th ACM conference on computer and communications security, pp 148–160 2002

[15] S Katzenbeisser, U¨kocaba, V Roi, AR sadeghi, I verbauwhede and C wachsmann, “PUFs: Myth, fact busted? a security evaluation of physically unclonable functions(PUFs) cast in silicon” lecture notes in computer science, vol. 7428, pp. 283–301, 2012.

[16] SS kumar, J guajardo, Rmaes, 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

[17] R maes, P tuyls and I verbauwhede, “Intrinsic PUFs from flip-flops on reconfigurable devices” In. benelux workshop on information and system security, 2008.

[18] CWO’Donnell, GE suh, S devadas, “PUF-Based Random Number Generation”MIT CSAIL CSG technical Memo 481 pp. 1-4, 2001.

[19] RS pappu, “Physical One-Way Functions” Ph.D. thesis, massachusetts institute of technology, 2001.

[20] Dinesh Ganta, “An effort toward building more secure and effcientphysical unclonable functions” PhD. thesis, virginia polytechnic Institute and state university, 2014

[21] Sudheendra K Srivastava, : Secure ans energy efficient physical unclonable function” PhD Thesis university of massachusetts, 2012

[22] Domenic Forte and Ankur Srivastava, “Manipulating manufacturing variation for better silicon physically unclonable function” IEEE computer society annual symposium on vlsi, pp. 171-176, 2010

[23] Elena I vatajelu,Giorgio di natale and Paolo prinetto, “Towards a highly reliable SRAM-based PUFs” Design, automation & test in europe conference & exhibition (DATE) pp. 273-276, 2016.

[24] Bai Chuang, Zou Xuecheng and Dai Kui, “A new physical unclonable function architecture” journal of semiconductors vol 36 no 3 pp 035005-1-035005-6, 2015.

[25] Yansong gao et al, “Memristive Crypto primitive for building highly secure phusical uniclonable fucntion” scientific reports nature, pp 1-14, 2015.

[26] Jeyavijayam Rajendran et al, “Nano meets seciruty:exploring nanoelectronics device for security application” Proceedings of the IEEE vol. 103, no. 5, pp 829-849, 2015.

[27] A maiti, I kim and P schaumont, “A robust physical unclonable function with enhanced challenge-response set” IEEE Transaction on information forenics security vol. 7, no. 1 pp. 333–345, 2012.

[28] U ruhrmair, S devadas and F koushanfar, “Security based on physical unclonability and disorder” Book chapter introduction to hardware security and trust pp. 65–102, 2012.

[29] S chellappa and Lawrence T clark, “SRAM-based unique chip identifier techniques” IEEE transaction on very large scale integration system, vol 24 no. 4 pp 1212-1222, 2016.

[30] Y Hori, T Yoshida, T Katashita and Akashi Satoh, “Quantitative and satistical performance evaluation of arbiter physical unclonable functions on FPGAs” 6th International Conference on Reconfigurable computing and FPGA, pp. 298-303, 2010.

[31] R pegu and R mudoi, “Design and analysis of mux based physical unlconable function” IEEE transactions on computer aided design of integrated circuits and systems, vol33 issue5 pp. 649-662, 2015.