A Review—Hardware Security Using PUF (Physical Unclonable Function)

Shruti Sakhare and Dipti Sakhare

Abstract With the increasing growth in electronic devices, there is equal importance for the circuit to be secured. Thus, hardware security is of great concern. In addition, many attacks have been developed every day. Hence, we need to design a PUF based system which helps us to reduce counterfeiting and avoids cloning of the circuit. A PUF (Physical Unclonable Function) is basically an external device placed in a circuit to avoid cloning. PUF's are easy to evaluate but rather hard to predict. PUF system is designed in such a way that even the manufacturer himself cannot create two copies or clones with same functionality. A PUF circuit promises easy authentication, is robust and has a unique feature that cloning cannot be done. A PUF circuit is considered very important in ongoing market as it has many applications like a circuit identifier, secret key generation and even to generate TRNG (true random number generator). This review discusses about attacks on the chip and concludes with what preventive measures that can be taken to stop cloning of circuits.

Keywords Counterfeiting · Physical unclonable function · True random number generator

1 Introduction

There is much demand for electronic devices, security of these electronic devices is also an issue behind this. So to make the particular circuit a secured one PUF (Physical Unclonable Functions) have been designed. PUF circuits are basically used to avoid cloning of devices and can solve the problem of attacks and counterfeiting. Recent study related to PUF circuit has many advance applications such as secret key generation, TRNG (True random number generator) and used as a circuit identifier,

S. Sakhare (✉)
VLSI Design and Embedded System, MIT Academy of Engineering, Pune, India
e-mail: svsakhare@mitaoe.ac.in

D. Sakhare
School of Electrical Engineering, MIT Academy of Engineering, Pune 412105, India
e-mail: dysakhare@etx.maepune.ac.in

A. Kumar and S. Mozar (eds.), *ICCCE 2019*, Lecture Notes in Electrical Engineering 570, https://doi.org/10.1007/978-981-13-8715-9_45

even our government accepts this product for security purpose. PUF have a unique feature that they cannot form clones of the circuit. PUF systems are easy to evaluate, hard to predict and are manufacturer resistant. In general sense when an input (challenge) is given to the PUF circuit and we get the output (response). This is commonly known as a CRP that is the challenge response pair. A set of these PUF's can be treated as the finger prints of the PUF circuit. This review discusses about the current state-of-the-art of silicon PUF's, attacks on different circuits, countermeasures, and applications.

2 Physical Unclonable Function

Ravikanth et al. [1] Physical Unclonable Functions (PUFs) are one way fucntions and have gained a lot of attention for hardware security. PUFs use the uncontrollable variations during the fabrication process. PUFs system have variety of applications such as secret key generation, enabling and disabling of integrated circuit, used for generation and cloning of True Random Number Generator (TRNG). PUF system have following specification reliable, unique, random and easy authentication. PUF system has its unique feature that is, delay converter. Due to its uniqueness it saves the circuit from different attacks and counterfeiting issues. Sudhanya et al. [2] every time if we give input (challenge) the PUF based circuit we get different output (response), which is very difficult to predict and analyze. This is known as challenge response pair (CRPs) and the response to a circuit is always digital values. Ayat et al. [3] have discussed about how drastically the PUF changes when damaged by an attacker. With this unclonability property of PUF, makes it interesting for secret key storage. Maiti et al. [4] PUF has the ability that the data which is stored in the non-volatile chip makes this unique signature. Hence, PUF can be used to protect private data and even can secure the Intellectual Property (IP).

2.1 Types of PUF

Zhang et al. [5] in this paper various PUF's have been classified among two categories they are strong PUF and weak PUF. Strong PUF basically has a huge pair of challenge response pair (CRP's) and they are used as authentication protocols. On the other hand there is a weak PUF which has very few number of challenge response pair (CRP's) and they are applicable to authentication Protocols. Table 1 [5] describes about the difference between the strong and weak PUF's, based on the challenge response pairs they have been differentiated.

Table 1 Difference between strong and weak PUF's

S. No.	Strong PUF	Weak PUF
1	These attacks are impossible to duplicate	Impossible to duplicate
2	Supports large CRP's (challenge response pairs) [6]	Supports less number of CRP's (challenge response pairs) [6]
3	Cryptographic key generation but for light weight authentication	Used for cryptographic key generation
4	CRP's are made public	Very good intra and inter differences
5	CRP's exponentially related to number of components	CRP's related linearly to number of components
6	For e.g. Arbiter PUF	For e.g. RO PUF

2.2 Application of PUF

PUF systems have many different applications. Based on hardware cryptography and there applications they have been listed below. Ravi Shankar [7], in their thesis they have discussed about many applications related to PUF such as Key generation and storage, Random number generator, IP protection, secure microcontrollers and processors, Radio frequency identification device (RFID), Hardware Obfuscation of Logic, vehicular security, and wireless sensor network security.

2.3 PUF Taxonomy

There has been a vast study on Physical Unclonable function since past few years. Based on these the PUF's have been classified, Table 2 describes different PUF Taxonomy, that is silicon and Non silicon PUF's. Among these two silicon PUF's are of great interest in terms of cost and fabrication. These are again classified as analog electronic PUF, delay based PUF and memory based PUF. Non silicon PUF's are non-electronic PUF such as optical PUF, paper PUF, magnetic PUF, RF-DNA PUF.

3 Ring Oscillator Physical Unclonable Function

Silicon PUF generates a unique signature for each IC. Based on the variations PUF's are categorized. Thus RO (Ring oscillator) and arbiter PUF comes under delay PUF.

Table 2 PUF taxonomy [5]

Memory based PUF	SRAM PUF, Butterfly PUF, Latch PUF, Flip Flop PUF
Non electric PUF	Optical PUF, paper PUF, RF-DNA PUF, CD PUF, Magnetic PUF
Analog electronic PUF	VT PUF, power distribution PUF, coating PUF [8]
Delay based PUF	Arbiter PUF, RO-PUF

It was built on the delay difference to generate random bit strings. It is the simplest form of PUF and its output is generated in the form of logic "0" and logic "1" and by comparing the frequencies of the pair of ring oscillators. More bits can be generated by multiple RO's. As symmetry is not needed it is easy to implement on FPGA. RO are much preferred than arbiter PUF's as arbiter requires much placement and routing on FPGA platform. Thus ring oscillators are much preferred than arbiter PUF as they are easy to implement.

Silicon based RO-PUF is shown in Fig. 1. This silicon RO-PUF are called as "weak PUF" due to the number of challenge response pairs are minimum that is it depends on the number of components. It generates a response by comparing the two ring oscillators, frequencies of each RO is slightly different due to the process variation of each oscillator. Ravi Shankar [7], in the survey on PUF they have mentioned about silicon RO-PUF which was built on FPGA platform. FPGA (Field programmable gate array) are the reprogrammable devices which can be used according to our requirements. Zhang et al. [5] the RO-PUF is a delay based function. The simplest form of PUF generates the output logic-0 or logic-1 by comparing the frequencies of a pair of oscillator circuits. More bits can be generated in the same way with multiple pairs of RO.

4 Future Scope

Recently PUF's receives attention in the chip market and is becoming a promising way which provides security to many devices and avoiding issues related to counterfeiting. In future performance evaluation of the PUF based system will be done. Rahman et al. [10] have disscued about security primitives like PUF's and TRNG. With the increasing security these systems can be used as creating opportunities and fulfilling the gap or the challenges. The main criteria on which the hardware security rely is randomness, uniqueness and enhanced Security. Large amount of work is recently going on to improve the above criteria. As PUF circuits have not be fully developed so, the cost required for any circuit to be cloned is very expensive. Further if PUF based system becomes mainstream the cost of these systems will lower down with promising results.

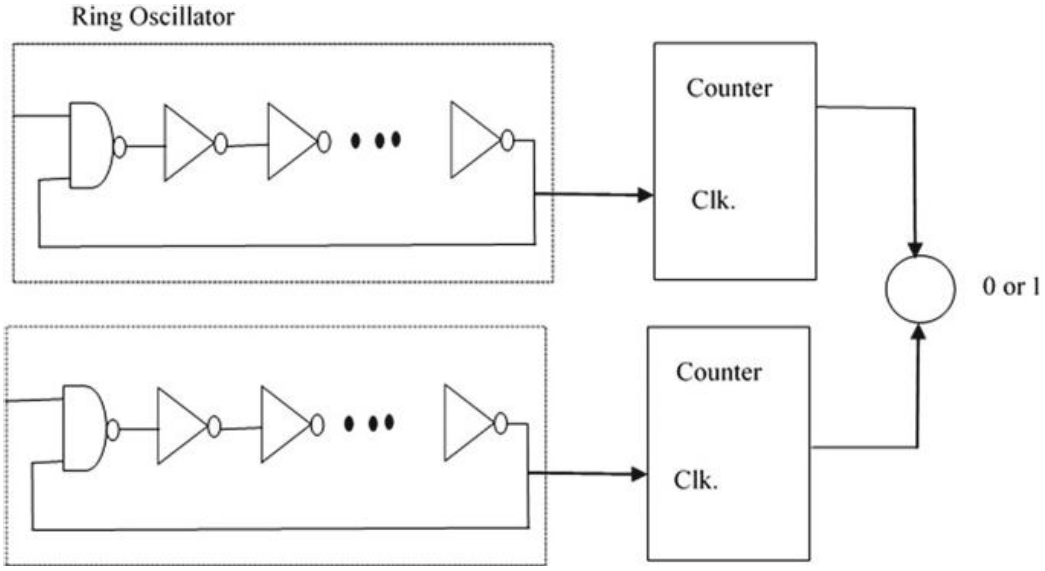

Fig. 1 Basic structure of RO PUF [9]

Zhang et al. [5] discussed about opportunities for generating PUF information from scan chain similar to VLSI-IP protection. Thus by reusing this scan chain as PUF circuit, it is easy to eliminate overhead caused by PUF. But these scan chain will impose new challenges to the PUF information.

References

1. Ravikant Pappu R, Recht B, Taylor J, Gershenfeld N (2002) Physical one-way functions. Science 297(5589): 2026–2030
2. Sudhanya P, Krishnammal PM (2016) Study of different silicon physical unclonable functions. In: International conference on wireless communications, signal processing and networking (WiSPNET), pp 81–85, September 2016
3. Ayat M, Atani RE, Mirzakuchaki S (2011) On design of PUF-based random number generators. Int J Netw Secur Appl (IJNSA) 3(3):30–40
4. Maiti A, Schaumont P (2010) Improving the quality of a physical unclonable function using configurable ring oscillator. In: International conference on FPGA, pp 703–707, April 2010
5. Zhang J-L, Qu G, Lv Y-Q, Zhou Q (2018) A survey on silicon PUFs and recent advances in ring oscillator PUFs. J Comput Sci Technol 29(4):664–678
6. Devadas S. Practical applications of physical unclonable functions. https://cap.csail.mit.edu/sites/default/files/csailiappufs.pdf
7. Ravi Shankar Y (2017) PUFs—an extensive survey. Master thesis, George Manson University, Fairfax
8. Lofstrom K, Daasch WR, Taylor D (2000) IC identification circuit using device mismatch. In: Proceedings of IEEE international solid state circuits conference, pp 372–373, February 2000
9. Anderson JH (2010) A PUF design for secure FPGA-based embedded systems. In: Proceedings of the 15th Asia and South Pacific design automation conference, pp 1–6, January 2010
10. Rahman F, Shakya B, Xu X (2017) Security beyond CMOS: fundamentals, applications, and roadmap. IEEE Trans Very Large Scale Integr VLSI Syst 25(12):3420–3433