Secret Key Generation: Single Edge-Triggered Flip-Flop PUF for IoT Environment

S. Hemavathy, C. Renju Raju, Akshara Kairali, B. G. Hari Lavanya, and V. S. Kanchana Bhaaskaran

1 Introduction

Physical Unclonable Function (PUF) is a physical device that generates a response based on the challenges or the input. The responses or the output of PUF are obtained based on the intrinsic variations that are inherently available in an integrated circuit. The output from every individual integrated circuit can act as a digital fingerprint to reproduce unique identity and non-resilient keys for highly secure crypto applications. In early periods, PUF gained attention in smartcard applications to create unique cryptographic keys for individual smartcards. Even they are used in many FPGAs to secure the secret keys for commercial applications.

The combination of input and output in a PUF is called as Challenge-Response pairs (CRPs). A PUF is a physical device integrated into an integrated chip. The semiconductor industry's continuous design of the digital circuit leads to some diverse changes in the oxide thickness, threshold voltage, and many other parameters. PUF utilizes these inherent manufacturing variations to generate a random response. Designing a PUF with the same Challenge-Response behavior is impracticable as it depends purely on the manufacturing process variations. These factors make the PUF unpredictable and uncontrollable structure.

Mathematically unclonable means it should be tough to compute CRPs for any PUF device with a given CRP. A complex challenge interaction with many or all of the unexpected properties of CMOS determines a response. In other words, PUF proves to be an unclonable device as it is physically and mathematically unclonable. These PUF features can be utilized as an inimitable and untampered device identifier.

S. Hemavathy · C. Renju Raju · A. Kairali · B. G. Hari Lavanya · V. S. Kanchana Bhaaskaran (✉)
Vellore Institute of Technology, Chennai Campus, Chennai, India
e-mail: kanchana.vs@vit.ac.in

T. Sengodan et al. (eds.), *Advances in Electrical and Computer Technologies*,
Lecture Notes in Electrical Engineering 881,
https://doi.org/10.1007/978-981-19-1111-8_17

2 Literature Survey

D flip-flop PUF architecture with symmetric cross-coupled inverters is proposed with two additional pass transistors to make the architecture symmetrical and give a high value of uniqueness [1]. The uniqueness is enhanced in the conventional D flip-flop by adding tristate logic instead of inverters [2]. The PUF metrics of flip-flop-based arbiter PUF is improved with a novel design of Feedback Oriented XORed Flip-Flop Arbiter PUF (FOXFFAPUF) [3]. The author of Coin-Flipping Physically Unclonable Function (CF-PUF) [4] has proposed a robust PUF design against the machine-learning attack. It uses the threshold voltage changes due to the nonlinearity of the convergence time of bistable rings. The author exemplifies the security of the PUF, along with less area overhead [5].

A new scheme [6] to protect the secret key against scan-based side-channel attacks is proposed to improve the uniqueness of PUF from every chip by using a lock and key scheme. Many flip-flop (FF) designs have been compared and evaluated for suitability as PUF generators by comparing their reliability, uniqueness, uniformity, and bit aliasing characteristics for PUF applications [7]. The Arbiter Physically Unclonable Function (APUF) is presented to give a low-cost and unique security solution over the expensive, standard cryptography system [8].

3 Design Methodology

3.1 Physical Unclonable Function

The PUFs can be broadly classified as Silicon and Non-Silicon based on the fabrication type as shown in Fig. 1. The various silicon PUFs can be broadly categorized based on logic as digital, analog, and adiabatic logic-based PUF. Adiabatic PUF [9] and quasi-adiabatic Tristate PUF [10, 11] are based on adiabatic logic, which can be used for low-energy applications.

The delay-based PUF generates a response based on the comparison of the delay between two paths (Arbiter PUF) or based on frequency as in Ring oscillator PUF. The memory-based PUF utilizes the cross-coupled latches to obtain the responses. Some of them are SRAM PUF, Latch PUF, and D flip-flop-based PUF.

Clock pulses are used in almost every digital circuit PUF to control the flow of responses utilizing the Finite state machine. Since the D flip-flops are spread in a wide range in an FPGA board, it is much easier to generate more CRPS. This feature also increases the robustness of the D flip-flop against side-channel attacks. The D flip-flop was earlier introduced as intrinsic PUF on the reconfigurable device to generate digital fingerprints. During power-up, the metastability in the D flip-flop generates randomness. This feature is exploited in PUF to generate a secret key. Similar to SRAM, upon power-up, all the D flip-flops are initialized to the specified

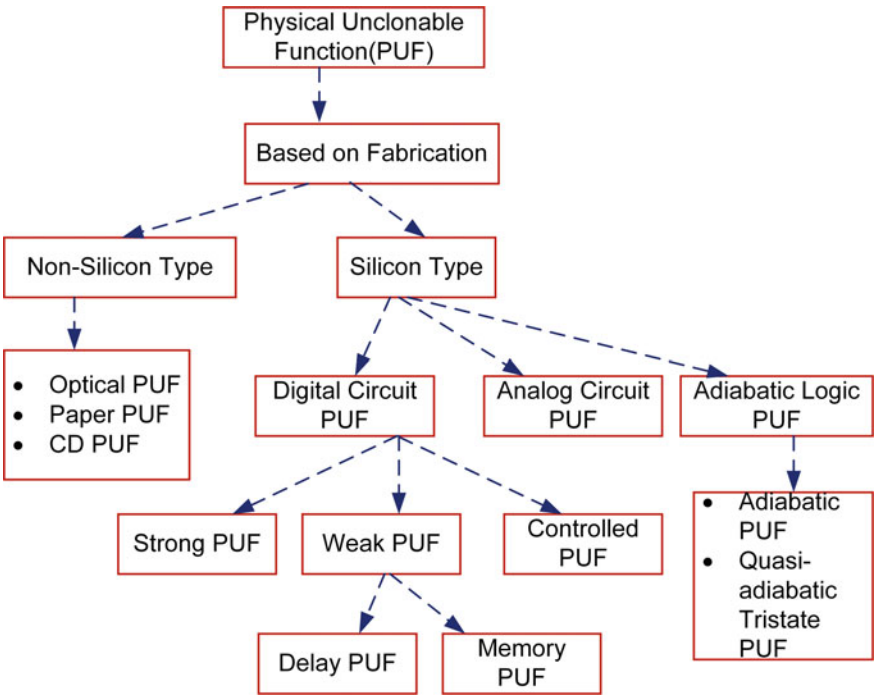

Fig. 1 Classification of PUFs [11]

initial value or '0' if the user does not specify an initial value. In FPGA, the author has used the global restore line command to remove the initialization from the bit file.

3.2 PUF Metrics

The essential security metrics for the various forms of PUFs used to characterize their resilience are Uniqueness, Uniformity, and Reliability.

Uniqueness is the most important key feature of PUF. It elucidates distinctly the number of Challenge-response pairs (CRPs) obtained from any integrated chip. It characterizes how distinct is the CRP of a PUF instance from those of other PUF devices. The fact is, it should be nearly hard to clone two PUFs. Each chip should have a different input-output mapping. Environmental conditions like the voltage, temperature, and aging can affect the CRPs obtained from each PUF design. Hence, error-correcting codes are added to replicate the responses. Inter-chip hamming distance (HD_{inter}) is employed to measure uniqueness. For the same set of challenges under nominal voltage and temperature, HD_{inter} is calculated for different PUF instances. With $R_i(n)$ and $R_j(n)$ be the n-bit responses obtained from chips i and j $(i \neq j)$ with

the same set of challenges, the uniqueness is evaluated by

$$\mathrm{HD}_{\mathrm{INTER}} = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{\mathrm{HD}\big(R_i(n), R_j(n)\big)}{n} \tag{1}$$

Uniformity is another metric of PUF where the percentage of 1's and 0's is calculated. Even distribution of bit 1 and 0 ensures a vital secret key that is hard to duplicate. The ideal value is 50%.

Reliability is a metric with which we evaluate a PUF circuit. It is an important attribute determining how repeatable or dependable a PUF's CRPs are under various environmental situations. Even at different voltages and temperatures, the reliability of the PUF needs to be ideally equal to 100%. Intra-chip hamming distance is used to evaluate Bit-Error Rate (BER). It is as given by

$$\mathrm{HD}_{\mathrm{INTRA}} = \frac{1}{k} \sum_{i=1}^{k} \frac{\mathrm{HD}\Big(R_i(n), R'_j(n)\Big)}{n} * 100\% \tag{2}$$

Here, k denotes the number of samples with the same set of challenges. $R_{i,}$ is the reference response obtained at normal working conditions, and R'_j is the response obtained by changing temperature and supply voltage.

3.3 Single Edge-Triggered Flip-Flop PUF (SETFF PUF)

Single edge-triggered flip-flops (Fig. 2) are the most commonly used flip-flops used in the semiconductor industry. Only one clock edge, either rising or falling, can be used to load data in this flip-flop. To maintain a desired logic 1 or a logic 0, all sequential components in a design must meet specific minimum data arrival timing requirements. For the data to latch at the exact clock edge (setup time), the data must arrive before the active edge of the clock (and be stable), and the data must also remain stable for a minimum specified duration after the active edge of the clock (hold time). Any breach of these time criteria may result in the latching of inaccurate results. This

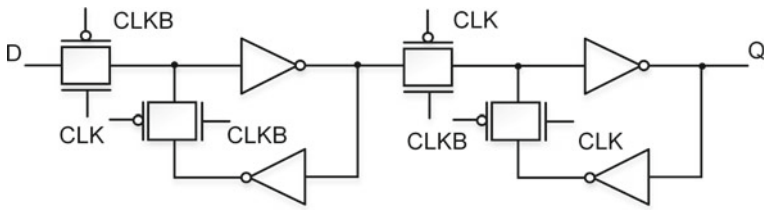

Fig. 2 Single edge-triggered flip-flop PUF (SETFF PUF)

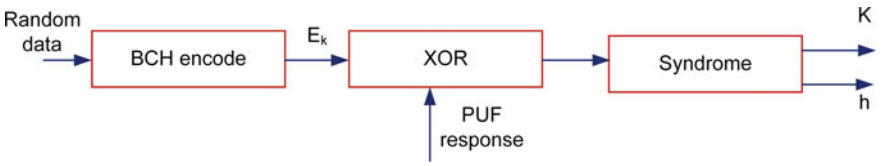

Fig. 3 Generation phase

Fig. 4 Reproduction phase

metastability condition is used to generate the random numbers. During the power-up state of the SETFF PUF, the cross-coupled inverters provide randomness in the output response of the circuit. This feature is utilized for the generation of secret keys from PUF.

3.4 Secret Key Storage and Generation

SETFF PUF can be used for key storage applications. The responses generated from the SETFF PUF cannot be used directly for any applications. A post-processing stage is usually required to verify that the device is working efficiently once it is deployed in the field. There are several methods for generating secure bit responses that are based on standard fault tolerance algorithms. In this paper, the noisy responses from the SETFF PUF can be recovered as a cryptographic key using error-correction codes. The BCH codes are generally used compared to other error-correcting code methods since they occupy less area overhead and are suitable for RFID and IoT applications.

Generation phase the noisy responses from the SETFF PUF is XORed along with the encoded key (E_k) obtained from the BCH encoder. The BCH encoder generates the encoded key from the random data. The secret key (K) is obtained from the syndrome along with helper data (h) as depicted in Fig. 3.

Reproduction phase In the reproduction phase, the noisy response along with helper data (h) is given to a BCH decoder to obtain the secret key as shown in Fig. 4.

4 Simulation Results

The SETFF PUF is simulated using the Cadence tool. UMC 90 nm technology is used to design the PUF to generate a 128-bit response. 200 such instances are designed

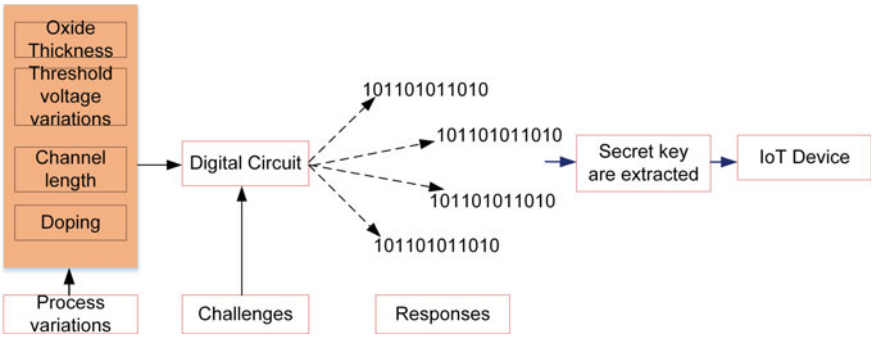

Fig. 5 SETFF PUF for IoT application

Table 1 Uniformity and Uniqueness of SETFF PUF

Voltage (V)	Uniqueness (%)	Uniformity (%)
0.9 V	49.76	57.50
0.92 V	49.81	57
0.94	49.87	55
0.96	49.95	55
0.98	50.01	53.50
1	50.07	52.50

using Monte-Carlo. The responses are post-processed using MATLAB to obtain the PUF metrics. The analysis is carried out at a nominal voltage of 1 V and 27 °C. Table 1 shows the uniformity and uniqueness obtained at different voltage conditions. It is evident that they are very near to the ideal value (50%) and almost close to nominal voltage (1 V). At 0.9 V and 0.92 V, the uniformity value has slightly deviated from the nominal voltage. The reason can be the noise incurred in the design due to the bias from nominal voltage. The BCH error-correcting codes support reproducing the same responses.

Similarly, the uniformity and uniqueness were calculated at nominal voltage and different temperatures, as shown in Fig. 6. Figure 7 shows the reliability obtained for different voltages and temperatures. The voltage and the temperature were varied from 0.9 to 1 V and −40–100 °C. The average reliability was found to be 98.35% (ideal 100%). The worst-case reliability is at −40 °C with 96.48%. The worst-case BER is to the maximum of 3.52 which can be corrected by using the BCH error-correcting codes. Table 2 illustrates the reliability for different voltages and temperatures.

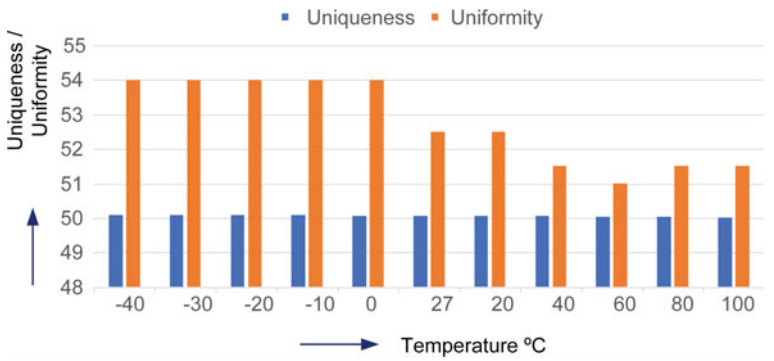

Fig. 6 Uniqueness and Uniformity of SETFF PUF at nominal voltage

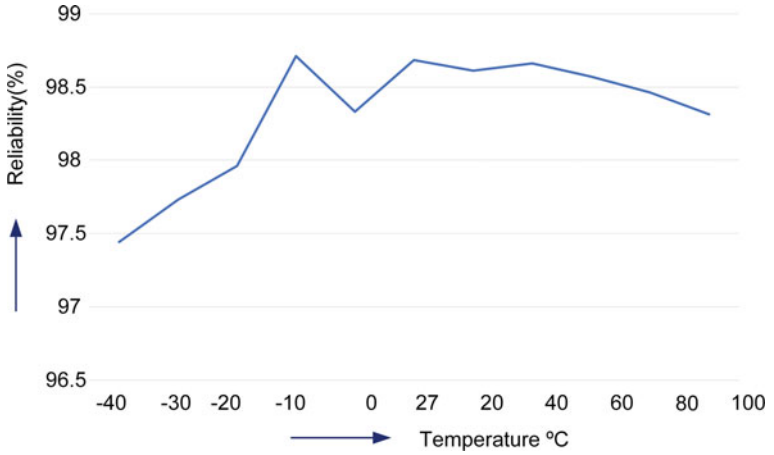

Fig. 7 Reliability of SETFF PUF

Table 2 Reliability of SETFF PUF

Temp °C /Volt (V)	0.9	0.92	0.94	0.96	0.98	1
−40	96.48	96.82	97.28	97.62	98.04	98.38
−30	96.71	97.07	97.54	97.93	98.38	98.74
−20	96.98	97.28	97.76	98.15	98.66	98.98
10	97.17	97.51	97.91	98.37	98.85	99.18
0	97.29	97.64	98.04	98.52	99.07	99.43
27	97.55	97.93	98.35	98.86	99.36	100
20	97.52	97.89	98.27	98.81	99.33	99.83
40	97.66	98	98.38	98.86	99.37	99.68
60	97.73	98.02	98.43	98.81	99.22	99.22
85	97.78	98.09	98.43	98.81	98.93	98.71
100	97.79	98.02	98.42	98.42	98.70	98.50

5 Conclusion

The SETFF PUF circuit was implemented, and the metrics like uniqueness, reliability, and uniformity were evaluated for different voltages and temperatures. From the above discussions, it is clear that the uniqueness for the SETFF PUF is about 50.07%, reliability is about 98.35%, and uniformity is about 52.50%. As the PUF metrics are close to the ideal value, the PUF responses of the PUF can be used to generate a secret key by using BCH error-correcting codes. SETFF PUF is best suited for resource-constrained IoT eco-system due to limited number of devices used and robust PUF metrics.

References

1. Khan S, Shah AP, Chouhan SS, Gupta N, Pandey JG, Vishvakarma SK (2020) A symmetric D flip-flop based PUF with improved uniqueness. Microelectron Reliab, Elsevier
2. Khan S, Shah AP, Chouhan SS, Rani S, Gupta N, Pandey JG, Vishvakarma SK (2020) Utilizing manufacturing variations to design a tri-state flip-flop PUF for IoT security applications. Analog Integr Circ Sig Process, Springer Science
3. Sushma R, Murty NS (2018) Feedback oriented XORed flip-flop based Arbiter PUF. In: 2018 Third international conference on electrical, electronics, communication, computer technologies and optimization techniques (ICEECCOT), Dec 2018
4. Tanaka Y, Bian S, Hiromoto M, Sato T (1995) Coin flipping PUF: a novel PUF with improved resistance against machine learning attacks. In: IEEE transactions on circuits and systems II: express briefs, vol 65, issue no 5, pp 602–606, Mar 20183. van Leeuwen J (ed) Computer science today. Recent trends and developments. Lecture Notes in Computer Science, vol 1000. Springer-Verlag, Berlin Heidelberg New York
5. Wang D, Liu L, Wang B, Wei S (2018) Area-efficient delay-based PUF based on logic gates. In: 2018 10th International conference on communication software and networks, Oct 2018
6. Wang Q, Cui A, Qu G, Li H (2020) A new secure scan design with PUF-based key for authentication. In: 2020 IEEE 38th VLSI test symposium (VTS), June 2020
7. Zhang H, Jiang H, Eaker MR, Lezon KJ, Narasimham B, Mahatme NN, Massengill LW, Bhuva BL (2018) Evaluation on flip-flop physical unclonable functions in a 14/16-nm Bulk FinFET technology. In: 2018 IEEE international reliability physics symposium (IRPS), May 2018
8. Mahalat MH, Mandal S, Mondal A, Sen B (2020) An efficient implementation of arbiter PUF on FPGA for IoT application. In: 2019 32nd IEEE international system-on-chip conference (SOCC), May 2020
9. Dinesh Kumar S, Thapliyal H (2020) Design of adiabatic logic-based energy-efficient and reliable PUF for IoT devices. J Emerg Technol Comput Syst 16(3), Article 34:18. https://doi.org/10.1145/3390771
10. Hemavathy S, Kanchana Bhaaskaran VS (2020) Design and analysis of secure quasi-adiabatic Tristate physical unclonable function. In: 2020 IEEE International symposium on smart electronic systems (iSES) (Formerly iNiS), pp 109–114. https://doi.org/10.1109/iSES50453.2020.00034
11. Hemavathy S, Bhaaskaran VK (2020) Design and analysis of secure quasi-adiabatic tristate physical unclonable function. In: 2020 IEEE Consumer electronics magazine. https://doi.org/10.1109/MCE.2021.3117541