ReOPUF: Relaxation Oscillator Physical Unclonable Function for Reliable Key Generation in IoT Security

Raveendra Podeti, Srihari Rao Patri, Srinivas Katkoori, Muralidhar Pullakandam

ReOPUF: Relaxation Oscillator Physical Unclonable Function for Reliable Key Generation in IoT Security

Raveendra Podeti[1], Sreehari Rao Patri[1],
Srinivas Katkoori[2], and P. Muralidhar[1]

[1] ECE Department, National Institute of Technology Warangal,
Warangal, Telangana, India, 506004
raveendra466@student.nitw.ac.in, {patri, pmurali}@nitw.ac.in
[2] CSE Department, University of South Florida,
Tampa, FL, USA, 33620
katkoori@usf.edu

Abstract. Physical Unclonable Function (PUF) has emerged as a hardware security block designed with low-cost and key generation for IC identification and authentication. The process variations being uncontrollable, they can be exploited as PUF that could generate unique identifiers representing robust keys. Arbiter-based PUFs work on the principle of the conventional delay-based approach realized between two symmetrical engaged paths. On the other hand, oscillator-based PUFs work on frequency differences among a group of identical oscillators arranged in a specific pattern. In this paper, a novel PUF is proposed based on Relaxation Oscillator PUF (ReOPUF) topology for device identification and authentication that can produce unique, unpredictable, and reliable keys to improve the robustness against the supply voltage and temperature variations. The ReOPUF is designed to generate a 4.4 MHz frequency that is suitable for powering IoT sub-systems including sensors while protecting them from malicious attacks. Based on Monte Carlo simulations, the reliability of PUF responses has been improved from 95.33% for the regular Ring Oscillator (RO) PUF to 99.19% for the proposed ReOPUF over a temperature range of -40°C to +120°C with ±10% fluctuations in supply voltage. Moreover, it achieves a good uniqueness result of 49.22%, diffuseness of 49.52%, and worst-case reliability of 97.41% over a range of 10°C to 85°C, and 10% fluctuations in supply voltage. Thus, we report significant improvement over previous works.

Keywords: Hardware Security, Internet-of-Things (IoT), PUF, Process Variations, Reliability, Arbiter PUF, RO PUF

1 Introduction

The design of secure electronic systems is very important so that they can store sensitive information as well as communicate securely with the authorized

devices. The rapid down scaling in feature sizes of Integrated Circuits (ICs) has exponentially improved computing power of processors which require robust security mechanisms [1]. Currently, the secure device authentication and data integration is provided by incorporating cryptographic functions implemented as hardware blocks [4]. The secret key is stored in non-volatile memory such as erasable programmable read-only memories which is vulnerable to invasive or non-invasive attacks. Physical Unclonable Function (PUFs) [2, 3, 5] emerged as robust security primitives to generate volatile security keys based on the inherent random manufacturing Process Variations (PVs) [6]. It offers a strong volatile key generation and storage to make the system tamper-resistant. When a PUF is fed with a challenge, it generates unique responses based on the physical characteristics of the silicon and is an alternative to the conventional digital signature mechanism.

A group of identical PUF cells with the same manufacturing process leverage the physical properties of each cell and generate a device-specific fingerprint or key [7]. PUF can be used in several applications such as device authentication or identification, key generation for encryption, and pseudo-noise random number generation [8, 9]. The uniqueness and randomness are the unpredictable features of a PUF that makes it resistant to security attacks. PUFs are only uncertain in power-up conditions when side-channel or power analysis attacks are performed. To make a strong PUF the key generation must stable and reliable which means the key should not change over time. Several PUF topologies have been proposed to improve reliability in the past decade, such as Arbiter PUF, Ring Oscillator (RO) PUF, SRAM PUF, etc. Among them, Arbiter PUFs [10] are very complex and generate strong challenge and response pairs [11, 12], whereas, RO PUFs are less complex and easy to design.

As mobile electronic gadgets become more widespread, day-to-day business (financial transactions, document exchange, health data, etc.) is done through integrated circuits. Thus, it is essential to incorporate strong security to ensure data privacy and trust [1]. PUFs serve as key generators for cryptographic devices to provide secure communication in an untrusted environment [7]. Security in data is generally raised through data sharing or distribution of the keys generated through key generators. The main characteristics of the key generated by a PUF are its randomness and uniqueness due to PVs. The key should be unaffected due to temperature and supply voltage variations and must be resistant to side-channel attacks.

RO PUFs [12, 13] are most popular due to their security, simplicity, ease of implementation, and evaluation. However, the main disadvantage of RO PUFs is poor response generation with temperature and supply voltage variations [14, 15]. Therefore, the reliability is enhanced by selecting a strong RO pair from 1-out of n-RO pairs, which has the maximum frequency distance from n-pairs. Multi-level supply voltage powered RO PUF are proposed to select the highest reliable voltage configuration [16]. The feedback-based supply voltage control can improve the reliability better than the conventional RO PUFs [17]. A temperature-aware RO PUF with different RO pairs can generate reliable bits against tempera-

ture variations [18, 19]. The temperature sensitivity is the major drawback in RO PUFs and can be reduced by applying a negative temperature coefficient of resistance to the inverters with two source feedback resistors. However, to achieve high reliability, a lightweight hybrid RO PUF was proposed with high thermal stability against supply voltage variation [15]. The security can be further strengthened when the system is designed with machine learning [21] based schemes for IoT edge node security.

To this end, we make the following contributions:

- We propose a new Relaxation Oscillator PUF design which we refer to as ReOPUF. The ReOs in ReOPUF is designed to explicitly produce the low frequency i.e., 4.4 MHz suitable for IoT sensor node security.
- The respective PUF quality metrics are evaluated and analyzed for the proposed PUF to demonstrate the high reliability in key generation.
- We perform extensive simulations (in 65 nm CMOS technology) to compare the proposed PUF with conventional RO PUFs in terms of PUF quality metrics with respect to supply voltage and temperature variations. We evaluate two more quality metrics, namely, Diffuseness (D) and Uniformity (u). We compare the strong CRP generation of the proposed ReOPUF with that of arbiter PUF. Further, we perform the entropy and correlation analysis.

The rest of the paper is organized as follows. Section 2 motivates the IoT authentication with PUFs. Section 3 surveys related research regarding existing PUFs and their reliability measurement with PUF quality metrics in response key generation. Section 4 proposes the methodology to achieve high uniqueness and reliability to enhance the security of IoT devices. Section 5 reports the simulation results, evaluates PUF quality metrics and, compares the proposed design with other PUFs. Section 6 presents a detailed security evaluation. Finally, Section 7 concludes the paper.

2 IoT Node Authentication with PUFs - Motivation

With the increasing demands on strong security, key generation and device authentication became the most challenging design concerns, particularly for IoT-enabled devices. Traditional security mechanisms that store keys in erasable programmable memories and use thenm with standard cryptographic algorithms suffer from power limitations. To implement information encryption and authentication, the tamper-resistant devices are equipped with countermeasures to defeat different types of physical attacks. Severe limitations on resources such as memory, CPU and battery power make classical cryptographic solutions unaffordable. Therefore, PUF has become a relatively simple and fast alternative for security.

PUFs are promising hardware security primitives to produce device-dependent challenge-response pairs based on unclonable properties and thus are suitable for reliable key generation [1]. The keys generated by PUFs are more resilient to malicious attacks from physical tampering. Figure 1 shows the security concept of

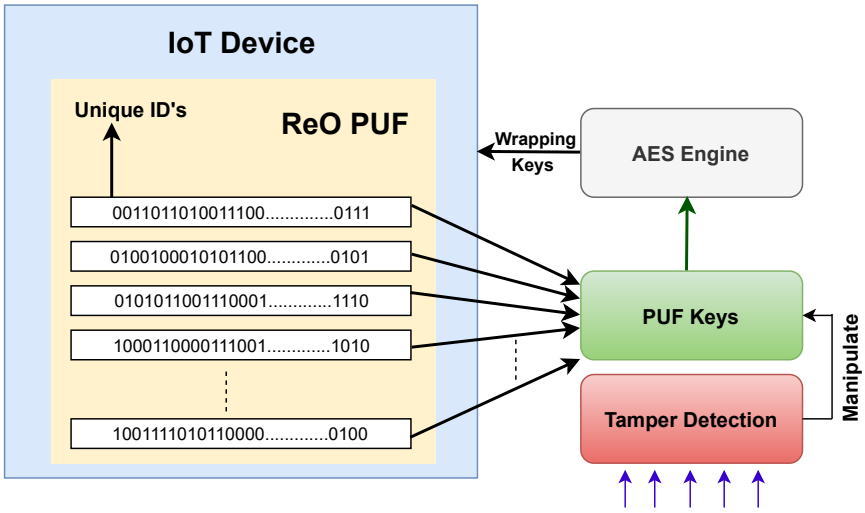

Fig. 1. PUF for IoT enabled devices

IoT-enabled devices. An IoT device equipped with ReOPUF generates PUF key as a unique ID and is shared through a gateway with the Cloud server. PUF keys are acquired by the Advanced Encryption Standard (AES) engine in the Cloud that can be employed to identify and authorize an IoT device. For example, consider an IoT-enabled sensor node in the field that senses the temperature or moisture data continuously upload the data to the Cloud at regular intervals. This data can be protected in the Cloud by encrypting it with PUF keys generated by ReOPUF. Therefore, due to the uniqueness and reliability of the ReOPUF, the sensor node can be authenticated.

3 Related Research

In this section, we briefly summarize the existing PUF topologies and their quality metrics to generate CRPs for device identification or authentication.

3.1 Ring Oscillator PUF

Figure 2 shows a conventional Ring Oscillator (RO) PUF for key generation [11]. It consists of N identically designed ROs (RO1, RO2, . . . , RON), two multiplexers, two counters, and one comparator. Each RO oscillates at different frequency due to manufacturing process variations, even though ROs are designed with an equal number of inverter stages [12]. An N-bit multiplexer can select a pair of frequencies generated from the RO stage based on the challenge input (through selection lines). The counters are used to get the count of the pulses obtained from the MUX stage. The difference in the pulses between the

two counters is verified by the comparator and a response is generated. For example, if Counter 1 output is greater than that of Counter 2 then a '1' is generated, otherwise, a '0'. In this manner, an N-bit key can be obtained from an N copies of RO PUF.

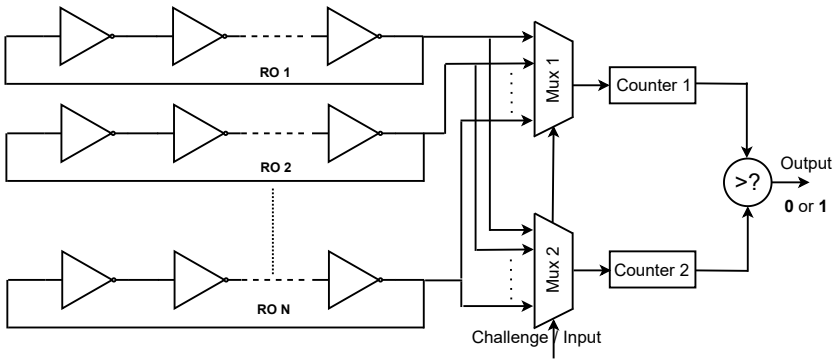

Fig. 2. Ring Oscillator PUF

3.2 Arbiter PUF

Figure 3 shows a basic arbiter PUF. It consists of switch components (SCs) and arbiter block to route the input signal and to perform the arbitration process for earlier response detection respectively [9]. Input and a random challenge are simultaneously fed to the switching components (multiplexers). Based on the delay of the paths the arbiter will detect early rising edge as the response. The mechanism of delay-based PUF is to introduce a race condition between two equally designed delay paths and the faster path will determine the output.

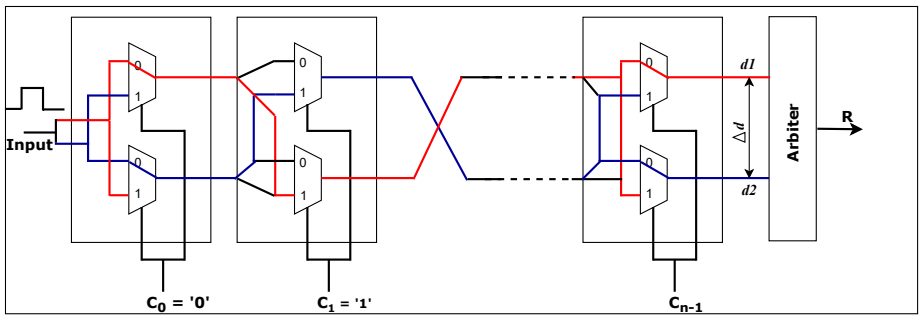

Fig. 3. Arbiter PUF

The circuit accepts of n-bit input challenge 'C' and computes 1-bit response 'R' based on the contention between two symmetrical paths based on relative delay difference (Δd = d1 - d2). The delay of the input is determined by the two-path processing of multiplexers (MUXs). Formally, the SCs are designed with 2 x 1 MUXs and properly tuned to get the precise delay (d) as a response. The delays are generally considered as PVs in APUFs, such as produced by the placement of a different combination of transistor arrangements in MUXs to produce certain delays at SCs. The MUXs will active the straight path if the selection (challenge) C_i is '0' and crossed when C_i is '1'. Likewise, MUX stages acting as SCs can create a pair of delay paths that can be selected with challenge input. The output is evaluated for a particular input while a rising signal is fed to both paths at the same time. The two signals race through the delay paths and the arbiter circuit (generally use D Flip-flop) catches the signal which comes earlier. The arbiter determines which rising edge arrives first and sets its output to '0' or '1' depending on the winner. For example, if a 16-bit input is given with a pre-defined challenge, an output '1' is produced if path1 is arrived early otherwise '0' is produced for path2.

3.3 PUF Quality Metrics

The quality of a PUF is measured using three major metrics, namely, *Uniqueness*, *Randomness*, and *Reliability* [20]. Uniqueness measures how different PUF instances can generate different responses when the same challenge is applied. The average inter-chip Hamming Distance (HD) calculated between the obtained responses should ideally be 50%. Randomness is the measure of unpredictability of responses from a PUF. For a good PUF design, the generation of response bits '1's and '0's should be distributed equally i.e., 50%. Reliability of a PUF determines how efficiently a PUF can generate the same response at different operating conditions for a given challenge. It is considered as intra-HD and should ideally be 0%.

4 Proposed Relaxation Oscillator PUF (ReOPUF)

An oscillator is a circuit that generates a repetitive waveform of fixed amplitude and frequency without any external input signal. Oscillators are used in radio, television, computer, and communications. Relaxation Oscillator (ReO) shown in Figure 4 is specifically preferred for low-frequency applications such as waveform generators, triggering circuits, etc. ReO is considered as a non-linear oscillator that can generate a periodic non-sinusoidal waveform (either voltage or current) at its output such as a square wave, triangular wave, etc. It is also called a non-sinusoidal waveform generator. ReOs do not require external components and are easily implemented in CMOS technology. In addition, ReOs are capable of producing sustained square wave oscillations determined by the time constant RC even though the frequency accuracy is restricted by the tolerances of on-chip

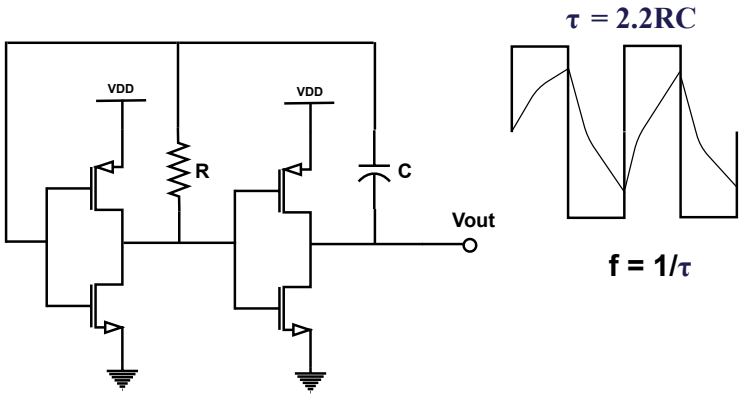

Fig. 4. Basic Relaxation Oscillator

capacitors and resistors. ReOs consume less current and power to generate jitter less clock generation.

A major drawback of ReO is its susceptibility to process and temperature variations. By the use of polysilicon resistors and the utilization of electron mobility in a MOS transistor offers an accurate frequency reference subjected to achieve fewer process variations and frequency stability over temperature. Most of the reported oscillators suffer from external components, reliability, and excessive power consumption and are not suitable for low-frequency applications requiring long battery lifetime.

The circuit can be designed with an energy storing device such as a capacitor or inductor which charges and discharges continuously to produce a cycle regarding a pre-determined threshold voltage. The frequency (f) or period (t) of oscillation with ReO is determined by the time constant ($\tau = 2.2RC$) of the capacitive or inductive circuit. Likewise, the frequency is calculated for the basic ReO is f=$1/\tau$ i.e., 4.4 MHz. ReOs are widely used to produce internal clock signals in several low frequency digital circuits. ReOs are also found in applications of thyristor triggering circuits, oscilloscopes, etc.

ReOPUF is a hardware PUF that exploits PVs occurring in the silicon manufacturing process to produce reliable keys. The random number extracted via ReOPUF is unique and unclonable that can be used as a silicon "fingerprint" for a wide range of security purposes, including encryption, identification, authentication, and security key generation.

Figure 5 shows a Relaxation Oscillator (ReO) PUF consists of 'N' identical ReOs (ReO1, ReO2,.....ReON), two n-bit multiplexers (MUXs), two counters, and a comparator. Each ReO generates a unique frequency when fed with different challenges or inputs. The frequency of 4.4 MHz is specially designed and generated for IoT sensor node applications. The MUXs can produce non-identical frequencies due to the process variations of the device, even though they are designed with the same device characteristics. The challenge or input

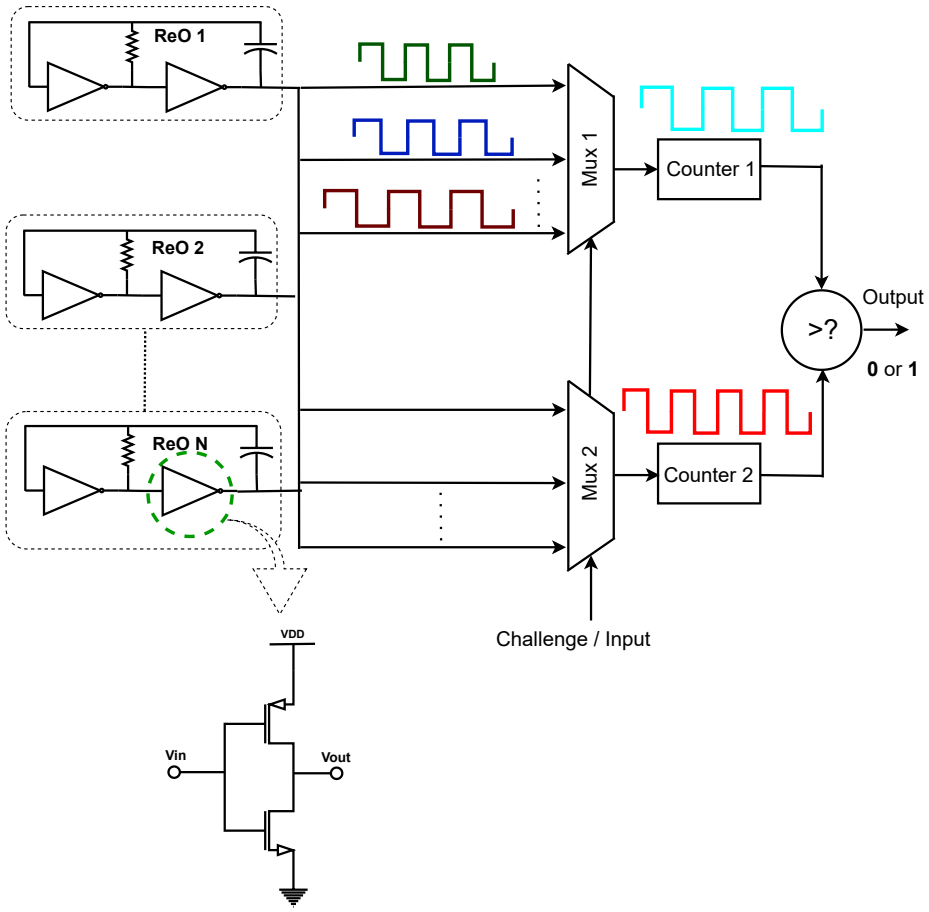

Fig. 5. Proposed Relaxation Oscillator (ReO) PUF

applied to both MUXs selects one pair of ReO the frequency difference of which will determine the output. The obtained frequency difference in terms of 1-bit response (either 0s or 1s) is considered for key generation. The counter can help to count the number of oscillations of selected ReO pairs processed from MUXs in a fixed time interval. The pulse counts from the counters are compared with the comparator, which gives the response '0' or '1'.

5 Experimental Results

The proposed ReOPUF circuit is implemented in UMC 65nm technology and simulated with Cadence Spectre. To perform characterization of 50 different PUFs, 100 runs of Monte-Carlo simulations are performed. During simulation, intra-die and inter-die PVs are generated to evaluate the responses. Each 32-

stage ReOPUF becomes active with the 5-bit challenge or input (C_0 to C_4) and is evaluated under the nominal operating conditions of 27°C and 1.2V supply voltage.

5.1 Evaluation of PUF Quality Metrics

The performance of the ReOPUF is measured and evaluated with the following metrics [20] as defined by National Institute of Standards and Technology (NIST).

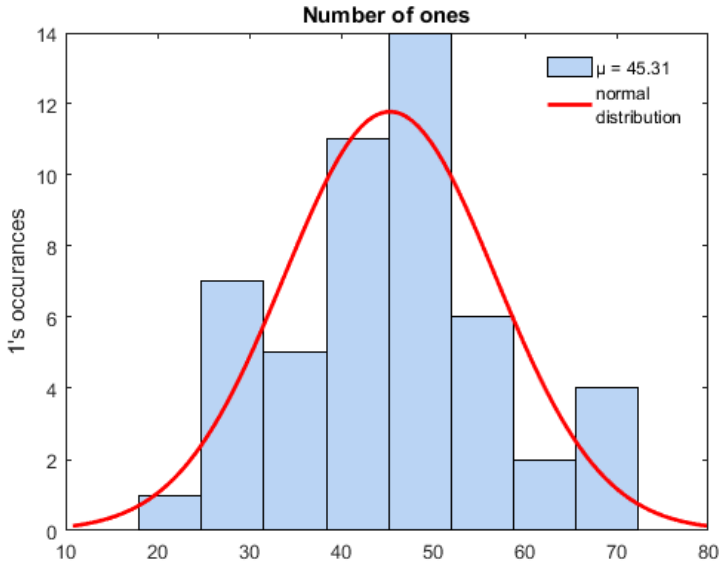

Fig. 6. Uniformity of ReOPUF - Distribution of 1s

5.1.1 Uniformity (u) Uniformity is the measure of distribution of '1s' and '0s' in the response vector $R_{i,j}$ and is defined as

$$Uniformity = \frac{1}{n}\sum_{j=1}^{n} R_{i,j} \times 100\% \tag{1}$$

where, $R_{i,j}$ is the j^{th} binary bit of an n-bit response for an i^{th} input. An ideal PUF should have equal probabilities for '1' and '0' in response, i.e., 50%. We evaluate the 32-bit responses from 50 ReOPUF instances at nominal operating condition i.e., 27°C, 1.2V is shown in Figure 6. The distribution of 1's and 0's generated by the ReOPUF is shown in Figure 7 as a pixel distribution with a

Fig. 7. Uniformity of ReOPUF - Pixel Representation

white pixel interpreted as a '1' and a black pixel as a '0'. The probability of generating 1s is 45.31%, which indicates that ReOPUF output is not predictable and it is hard to attack.

5.1.2 Diffuseness (D) Diffuseness (shown in Figure 8) is the degree of variation observed in same ReOPUF with different challenges applied nominally. It can be measured by calculating the mean of Hamming Distance (HD) from the response vectors obtained as 49.53%. It is defined as

$$Diffuseness = \frac{2}{l(l-1)} \times \sum_{i=1}^{l-1} \sum_{j=j+1}^{l} \frac{\mathrm{HD}(R_i, R_j)}{n} \times 100\% \tag{2}$$

where 'l' represents randomly selected response vector from CRP space. R_i and R_j are two different n-bit response vectors obtained from two different challenges.

5.1.3 Uniqueness (U) The randomness in different PUF responses reflects the performance in terms of uniqueness. Ideally, the probability of each response (i.e., '0' or '1') generated by identical PUFs with the same challenge should be 50%. Uniqueness (shown in Figure 9) measures inter-chip variation among different ReOPUF instances implemented with same challenge. It can be calculated with inter-chip hamming distance (inter-HD) 49.22% as shown below

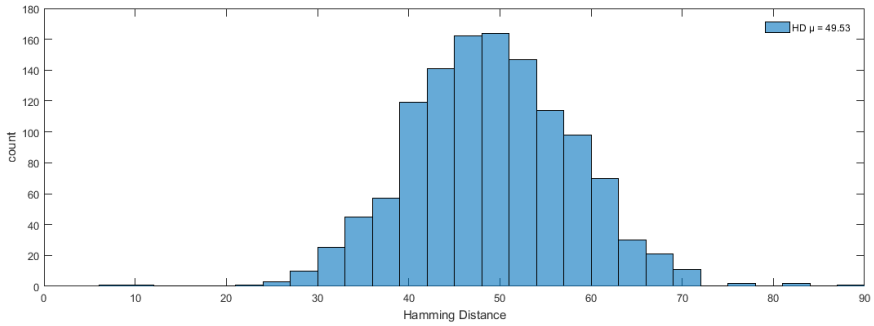

Fig. 8. Diffuseness of ReOPUF

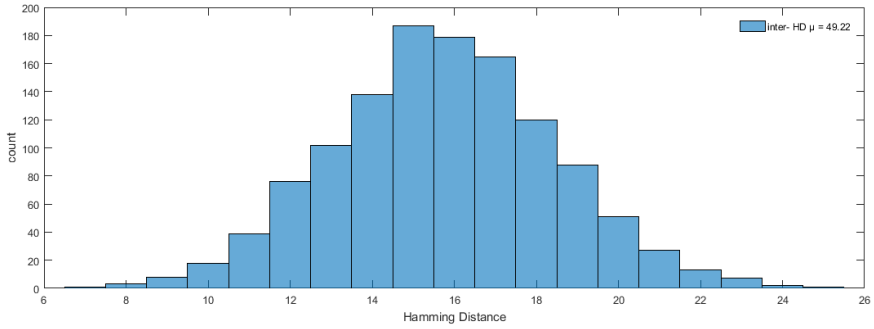

Fig. 9. Uniqueness of ReOPUF

$$Uniqueness = \frac{2}{m(m-1)} \times \sum_{i=1}^{m-1} \sum_{j=j+1}^{m} \frac{\mathrm{HD}(R_i, R_j)}{n} \times 100\% \tag{3}$$

where R_i and R_j are two different n-bit response vectors obtained from same challenge and 'm' represents different ReOPUF instances with same challenge.

5.1.4 Reliability (R) A PUF should generate the same response in any state for the same challenge applied. Unfortunately, the variations in the supply voltage or temperature can change the behavior of the IC in the form of circuit delay and lead to unpredicted responses. Therefore, the same response bits should be produced at different operating conditions.

Reliability is measured by *intra-HD*, which is performed between two n-bit response vectors generated from the same PUF instances with the same challenges. Ideally, it should be close to 0% for an environment-friendly PUF and can be calculated as follows.

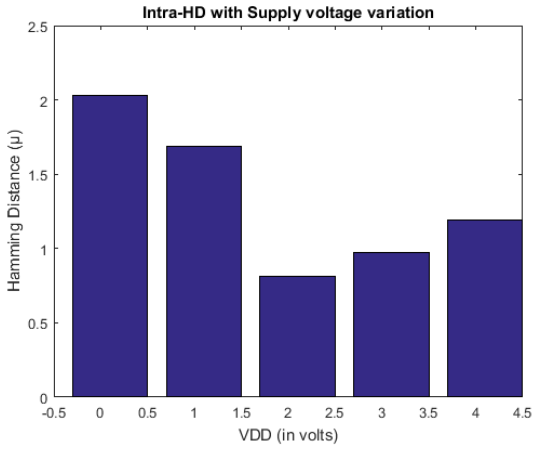

Fig. 10. Reliability of ReOPUF with VDD variation

$$\textit{intra-HD} = \frac{1}{m} \times \sum_{t=1}^{m} \frac{\mathrm{HD}(R_{i,ref}, R_{i,t})}{n} \times 100\% \tag{4}$$

$$\textit{Reliability} = 100 - (\textit{intra-HD}) \tag{5}$$

where 'm' represents some measured trials applied on ReOPUF instances with the same challenge. $R_{i,ref}$ is the reference response measured at normal operating conditions (27°C and 1.2V), $\mathrm{R}_{i,t}$ is the t^{th} measured response at a different operating conditions. We measure the reliability of the 32-bit responses from 50 ReOPUF instances in different operating conditions.

The average reliability calculated from 50 ReOPUF responses over commercial range (0°C to 85°C) is 99.31% at 27°C as shown in Figure 11, and the worst-case reliability is 97.19% at 0°C. A supply voltage variation up to ±10% VDD is applied to the ReOPUF as shown in Figure 10. The corresponding reliability is 99.19% at 1.2V, and the worst-case reliability is 97.97%. In addition, over the industrial range (-40°C to 100°C) the reliability is 97.41%. Table 1 presents the comparison of different PUF designs with ReOPUF. Table 2 shows the ReOPUF analysis with different temperatures.

6 Security Evaluation of the Proposed PUF

PUFs are specifically proposed for security applications that can withstand attacks under various threat models [21]. A PUF uses a CRP mechanism derived from inbuilt process variations performed by the ICs. Invasive attacks (such as reverse engineering attacks) may alter the physical properties of the device resulted in breaching of CRPs. However, PUF-based systems may be susceptible to two threat models such as PUF for authentication and PUF for secret

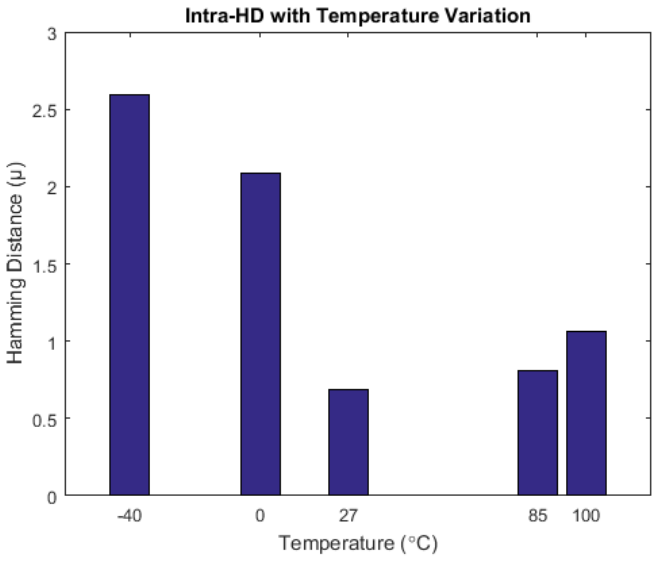

Fig. 11. Reliability of ReOPUF temperature variation

Table 1. Comparison of metrics of different PUF designs (t=temperature variation and v=supply voltage variation)

References	Technology	U (ideal 50%)	R (ideal 100%)
Liu *et al.*[18]	40nm	49.97%	95.88%
Yuan*et al.*[15]	65nm	50.42%	97.28%^{t}, 96.30%^{v}
Sauvagya*et al.*[19]	90nm	46.22%	95.89%
G Edward*et al.*[10]	90nm	46.14%	99.52%
Tauhidur*et al.*[17]	90nm	47%	96.91%
This work	**65nm**	**49.22%**	**97.41%**^{t}, **97.97%**^{v}

key generation. If a PUF is used for authentication, the attacker can perform different trials to extract valid CRPs which can be used to crack the PUF function. If it is a secret key generation the attacker can concentrate on the PUF response pairs by exploiting the PUF weakness. In this section, we evaluate the security of PUF by performing the entropy analysis on the responses.

6.1 Entropy Analysis

Entropy can be used as a measure of unpredictability of a response key from PUFs, though the uncertainty from process variations is unmeasurable [22]. For example, a 32-bit key that is uniformly and randomly generated has 32 bits of entropy. It also takes (ignoring actual computing) 2^{32}-1 guesses to break by brute force. Entropy fails to capture the number of guesses required if the possible keys are not chosen uniformly. Entropy is measured for ReOPUF generated 32-bit

Table 2. ReOPUF quality metrics at different temperatures

	-40°C	**0°C**	**85°C**	**100°C**
Intra-HD Temp (%)	97.41	97.91	99.19	98.94
Intra-HD Vdd (%)	97.97	98.31	99.03	98.81
Inter-HD (%)	85.74	94.25	81.89	78.36
Diffuseness (%)	46.27	49.32	48.79	48.03
Uniformity (%)	40.26	45.21	44.35	43.36

response when varying with different temperature and supply voltage variations as shown in Figures 12 and 13. From the analysis, we assure that the ReOPUF responses offer high uncertainty and high average information carried out for communication. It is observed that at different temperatures the entropy varies from 2.39 to 2.48, while at different supply voltages it varies from 2.41 to 2.44.

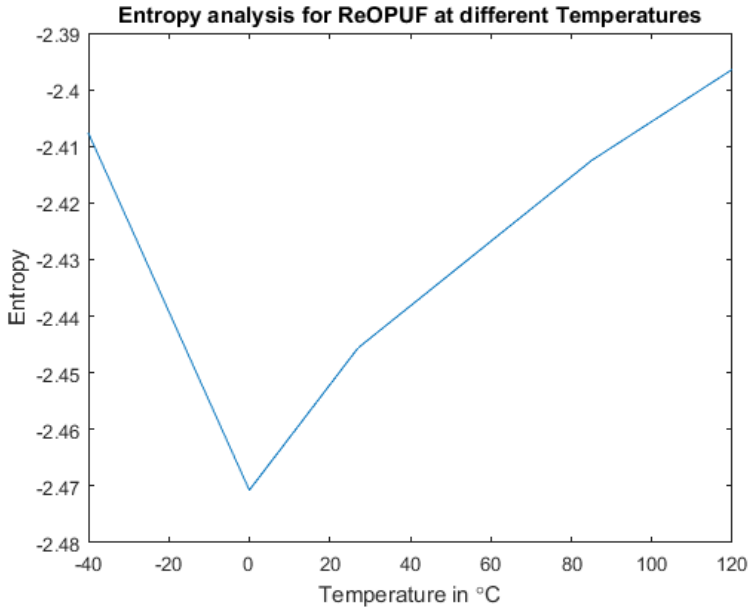

Fig. 12. Entropy of ReOPUF with temperature variation

6.2 Correlation Coefficient Analysis

The correlation coefficient is calculated for every PUF instance to determine if there is any correlation among the PUF cells [23]. If zero correlation is attained, then there is no such dependency exists among PUF cells. In the

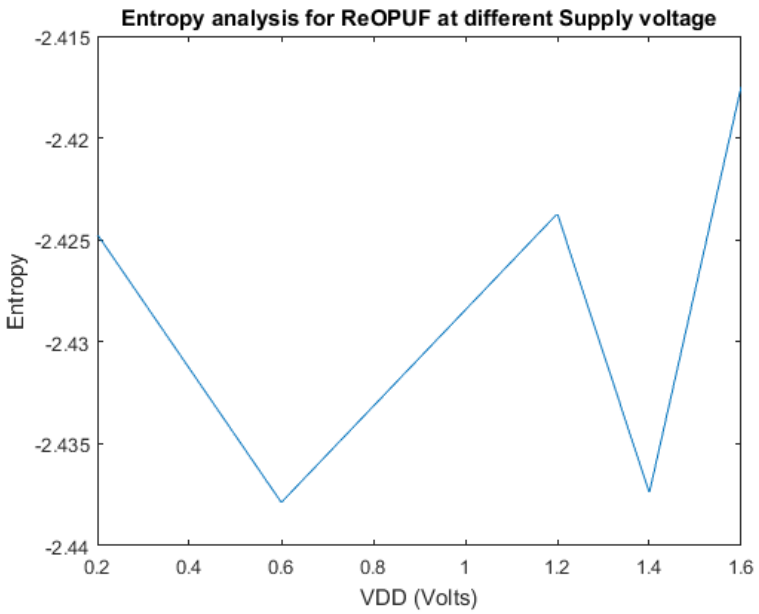

Fig. 13. Entropy of ReOPUF with supply voltage variation

occurrence of -1 or +1 attainment there exists a linear dependency among the PUF cells i.e., weakly dependent (-1) or strongly dependent (+1) based on the CRPs generated by PUFs. For this test, 32 PUF cells are used. Pairwise, the covariance of two cells is divided by the product of their standard deviations as shown:

$$\rho(X,Y) = \frac{E[(X-\mu X)(Y-\mu Y)]}{\sigma_x \sigma_y} \tag{6}$$

where ρ is defined as the correlation coefficient of two independent variables X and Y, μ and σ represent mean and standard deviation of the independent responses obtained from the PUFs respectively. A positive (negative) value of ρ indicates a positive (negative) correlation between the two variables. The higher (lower) the value of ρ stronger the positive (negative) correlation. The closer this value lies to zero the weaker the relationship between the two PUF cells. The obtained ρ for ReOPUF falls between 1.57 to 2.59 states that the responses are strongly correlated to the respective challenges and the uncertainty becomes the matter of reliability in security evaluation.

6.3 Power Analysis of ReOPUF

We measure the power consumption of the single-stage implementation of ReOPUF and RO-PUF as shown in Table 3. For 32-bit key implementations, the estimated average powers of ReOPUF and RO-PUF are 3.79mW and 15mW respectively.

Table 3. Power comparison for different PUFs

	RO-PUF	**ReOPUF**
Power (single PUF instance) (in μW)	497.53	118.42
Power (32 PUF instances) (in mW)	15	3.79

7 Conclusion

In this paper, we have introduced a relaxation oscillator-based PUF mechanism with the advantage that challenges fed through simple oscillation can achieve more reliability than any other oscillator PUFs. The experimental evaluation of ReOPUF shows the uniqueness and reliability of 49.22% and 97.97% respectively, which is better than that of the previous works. ReOPUF significantly improves upon the previous ROPUF designs, and has the potential to be the basis for CRPs based identification and authentication applications designed for IoT.

Bibliography

[1] Babaei, A. and Schiele, G., 2019. Physical unclonable functions in the internet of things: State of the art and open challenges. Sensors, 19(14), p.3208.

[2] Challa, R. P. and Islam, S. A. and Katkoori, S., 2019. An SR Flip-Flop based Physical Unclonable Functions for Hardware Security. In Proceedings of 2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS), Dallas, TX, USA, pp. 574-577.

[3] Govindaraj, R. and Ghosh, S. and Katkoori, S., Dec. 2020. Design, Analysis and Application of Embedded Resistive RAM Based Strong Arbiter PUF. In IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 6, pp. 1232-1242.

[4] Potkonjak, M. and Goudar, V., 2014. Public physical unclonable functions. Proceedings of the IEEE, 102(8), pp.1142-1156.

[5] Liang, W., Liao, B., Long, J., Jiang, Y. and Peng, L., 2016. Study on PUF based secure protection for IC design. Microprocessors and Microsystems, 45, pp.56-66.

[6] Abu-Rahma, M.H. and Anis, M., 2007, May. Variability in VLSI circuits: Sources and design considerations. In 2007 IEEE International Symposium on Circuits and Systems (pp. 3215-3218). IEEE.

[7] Lee, J.W., Lim, D., Gassend, B., Suh, G.E., Van Dijk, M. and Devadas, S., 2004, June. A technique to build a secret key in integrated circuits for identification and authentication applications. In 2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No. 04CH37525) (pp. 176-179). IEEE.

[8] Lim, D., Lee, J.W., Gassend, B., Suh, G.E., Van Dijk, M. and Devadas, S., 2005. Extracting secret keys from integrated circuits. IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 13(10), pp.1200-1205.

[9] O'donnell, C.W., Suh, G.E. and Devadas, S., 2004. PUF-based random number generation. In MIT CSAIL CSG Technical Memo, 481.

[10] Suh, G.E. and Devadas, S., 2007, June. Physical unclonable functions for device authentication and secret key generation. In 2007 44th ACM/IEEE Design Automation Conference (pp. 9-14). IEEE.

[11] Bernard, F., Fischer, V., Costea, C. and Fouquet, R., 2012. Implementation of ring-oscillators-based physical unclonable functions with independent bits in the response. International Journal of Reconfigurable Computing, 2012.

[12] Gao, M., Lai, K. and Qu, G., 2014, June. A highly flexible ring oscillator PUF. In Proceedings of the 51st Annual Design Automation Conference (pp. 1-6).

[13] Avaroğlu, E., 2020. The implementation of ring oscillator based PUF designs in Field Programmable Gate Arrays using of different challenge. Physica A: Statistical Mechanics and its Applications, 546, p.124291.

[14] Tao, S. and Dubrova, E., 2017. MVL-PUFs: multiple-valued logic physical unclonable functions. International Journal of Circuit Theory and Applications, 45(2), pp.292-304.

[15] Cao, Y., Zhang, L., Chang, C.H. and Chen, S., 2015. A low-power hybrid RO PUF with improved thermal stability for lightweight applications. IEEE Transactions on computer-aided design of integrated circuits and systems, 34(7), pp.1143-1147.

[16] Mansouri, S.S. and Dubrova, E., 2012, September. Ring oscillator physical unclonable function with multi level supply voltages. In 2012 IEEE 30th International Conference on Computer Design (ICCD) (pp. 520-521). IEEE.

[17] Rahman, M.T., Forte, D., Fahrny, J. and Tehranipoor, M., 2014, March. ARO-PUF: An aging-resistant ring oscillator PUF design. In 2014 Design, Automation & Test in Europe Conference Exhibition (DATE) (pp. 1-6). IEEE.

[18] Liu, C.Q., Cao, Y. and Chang, C.H., 2017. ACRO-PUF: A low-power, reliable and aging-resilient current starved inverter-based ring oscillator physical unclonable function. IEEE Transactions on Circuits and Systems I: Regular Papers, 64(12), pp.3138-3149.

[19] Sahoo, S.R., Kumar, S., Mahapatra, K. and Swain, A., 2016, December. A novel aging tolerant RO-PUF for low power application. In 2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS) (pp. 187-192). IEEE.

[20] Maiti, A., Gunreddy, V. and Schaumont, P., 2013. A systematic method to evaluate and compare the performance of physical unclonable functions. In Embedded systems design with FPGAs (pp. 245-267). Springer, New York, NY.

[21] Laguduva, V., Islam, S.A., Aakur, S., Katkoori, S. and Karam, R., 2019, July. Machine learning based iot edge node security attack and countermeasures. In 2019 IEEE Computer Society Annual Symposium on VLSI (ISVLSI) (pp. 670-675). IEEE.

[22] Van Den Berg, R., 2012. Entropy analysis of physical unclonable functions. MSc. thesis, Dept. Math. Comput. Sci., Eindhoven Univ. Technol., Eindhoven.

[23] Lin, L., Holcomb, D., Krishnappa, D.K., Shabadi, P. and Burleson, W., 2010, August. Low-power sub-threshold design of secure physical unclonable functions. In Proceedings of the 16th ACM/IEEE international symposium on Low power electronics and design (pp. 43-48).