Microelectronics Reliability 106 (2020) 113595

Contents lists available at ScienceDirect

Microelectronics Reliability

journal homepage: www.elsevier.com/locate/microrel

A symmetric D flip-flop based PUF with improved uniqueness

Sajid Khan[a], Ambika Prasad Shah[b], Shailesh Singh Chouhan[c], Neha Gupta[a], Jai Gopal Pandey[d], Santosh Kumar Vishvakarma[a,*]

[a] Nanoscale Devices, VLSI Circuit & System Design Lab, Discipline of Electrical Engineering, Indian Institute of Technology Indore, M.P. 453552, India
[b] Institute for Microelectronics, Technische Universität Wien, Vienna 1040, Austria
[c] EIS Lab, Department of Computer Science, Electrical and Space Engineering, Lulea University of Technology, 97187, Sweden
[d] Integrated System Group, CSIR-CEERI, Pilani, Rajasthan 333031, India

ARTICLE INFO

Keywords:
Physically unclonable function
Flip-flop
Lightweight
IoT
Challenge-response pair
Security

ABSTRACT

Physically unclonable functions (PUF) emerged as security primitives that generate high entropy, temper resilient bits for security applications. However, the implementation area budget limits their use in lightweight applications such as IoT, RFID, and biomedical applications. In the form of SRAM or D flip-flop, intrinsic PUFs are abundantly available in almost all of the designs. Being an integral part of the design, they can be used with compromised performance. In this work, to address the usage of intrinsic PUF, a D flip-flop based lightweight PUF is proposed. The proposed architecture is implemented on 40 nm CMOS technology. The simulation results show that it offers a uniqueness of 0.502 and the worst-case reliability of 95.89% at high temperature 125 °C and 97.89% at a supply voltage of 1.2 V. To evaluate the performance of various PUF architectures, A novel term, the uniqueness-to-reliability ratio, is proposed. When compared to the conventional D flip-flop, it offers 4.491 times more uniqueness and 127.74 times more uniqueness-to-reliability ratio with the same layout area. Since it uses the symmetrical structure, unlike other architectures, the proposed architecture does not require any post-processing schemes for bias removal, which further saves the silicon area. To verify the functional correctness of the simulation results, an FPGA implementation of the conventional and proposed D Flip-flop is also presented.

1. Introduction

The Internet of Things (IoT) is predicted to become a primary driver for the next phase growth of the electronics industry. IoT is being used in various emerging areas, such as smart homes, intelligent vehicles, remote healthcare, environment monitoring system, etc. [1]. The expanding usage of IoT for monitoring and control requires high security for the recorded data as security failure of these IoT devices can cause huge financial loss and invasion of privacy [2, 3]. Usually, off-chip approaches are quite common in practice at the cost of large implementation area, which is in contrast to the demand for miniaturization in the consumer market. Lightweight security techniques are in practice in most of this connectivity of devices and systems. However, the area and power budget have extremely restricted the strength of the on-chip cryptography algorithm that can be implemented in radio frequency identification (RFID). As the key required by cryptographic algorithms can be easily reverse-engineered and copied; hence, the widespread adoption of IoT will make cyberattack a destructive threat [4]. To address this issue, physically unclonable functions (PUF) have emerged as a new easy to implement, low-cost, and secure primitives for chip identification. It is well known from the literature that each fabricated transistor is unique due to the random process variation during manufacturing. These inherent properties, due to the process variations, are random, unpredictable, and uncontrollable in nature; therefore, it is nearly impossible to clone or re-create a device with selected electronics fingerprints. A PUF consists of an electronic circuit that harvest these manufacturing and process-induced properties, to generate innate secrets. These innate secrets are easy to challenge but extremely hard to reproduce or predict (even for the manufacturer) [5, 6]. These secrets act as the foundation for key generation, device identification/authentication/anti-counterfeiting, and IP protection. Thus, the volatile nature of PUFs provides high-level security and tamper resistance.

The existing silicon PUFs can be broadly classified as either delay-based or memory-based [7-9]. In the delay-based PUFs, bits are generated by comparing the delay of two nominally identical paths. The random delay difference between the two paths determines the output bit. While in the memory-based PUFs, a bi-stable structure of two cross-coupled inverters is used to generate the output bit. The asymmetry due to the random process variations causes the cross-coupled inverters to

* Corresponding author.
E-mail address: skvishvakarma@iiti.ac.in (S.K. Vishvakarma).

https://doi.org/10.1016/j.microrel.2020.113595
Received 30 July 2019; Received in revised form 24 January 2020; Accepted 29 January 2020
Available online 09 February 2020

resolve to a proffered state at power-up. All the delay-based PUFs are extrinsic, while all the memory-based PUFs are intrinsic except butterfly PUF [10]. In the memory-based PUF, PUF circuits are embedded in the design itself; hence, the effective hardware cost is zero. This makes memory-based PUF the best candidate for application where the silicon area is one of the prime concerns.

Various memory-based PUF variants are in use, such as SRAM based PUF [7], butterfly PUF [10], D flip-flop PUF [11]. The SRAM PUF is based on the startup values of SRAM memory, which are unpredictable in nature. The use of SRAM PUF is limited in FPGA based implementation as the SRAM memories are initialized to a known state upon power-up. This limits the use of SRAM PUF in FGPA. Also, in FPGA and ASIC both, after power-up, SRAM PUF can be used only once, until a write operation has not occurred. Once a write operation has been performed, the PUF output is overwritten. Thus, to regenerate the previous response, the SRAM needs to be re-powered on. Hence, if PUF responses are required very often, the part of SRAM used in PUF, can not be shared. Due to the power-on initialization of SRAM in FGPA, butterfly PUF replaces the SRAM cross-coupled inverters by cross-coupled latches on FPGA. By resetting one of the latches and presetting the other one, latches can be forcibly brought to an unstable condition. After removing the preset and reset signals, the butterfly cell settles back to one of the two stable states. It should be noted that the settling state depends upon the manufacturing mismatch between the two latches. However, the butterfly cell needs extra attention in placement and routing, because the preferred stable state is also a function of mismatch present in signal routing. In addition to this, butterfly PUF requires dedicated latches that can not be shared or reused by the system; therefore, it cost hardware overhead.

Almost all the synchronous digital VLSI systems rely on clock pulses to control the movement of data in the Finite-State-Machines (FSM). One of the major components in FSM are D flip-flops [12]. As mentioned earlier, the D flip-flop based PUFs are also a preferred choice since they have a higher level of security advantage against invasive attacks than SRAM PUF. Additionally, it is also possible that D flip-flops can be spread randomly across a design to make it much harder for an attacker to locate them and their signal lines. Based on the above discussion, in this paper, we have proposed a D flip-flop design, which can also be used as a PUF. The main contributions of the paper are as follows:

- A D flip-flop with integrated PUF is proposed with improved PUF uniqueness.
- An FGPA implementation, along with the simulation, is carried out to validate the functional correctness of the proposed design.
- The PUF output can be reproduced without re-powering the device.
- A mathematical model is presented for mismatch analysis.
- A novel term, the uniqueness-to-reliability ratio, is proposed to evaluate the performance of PUF architectures.

The rest of the paper is organized as follows: Section 2 discusses an overview of the existing D flip-flop based PUF. Section 3 explains our proposed D flip-flop and its implementation as a PUF. Functional verification via FPGA implementation is provided in Section 4. The compilation of the flip-flop characteristics followed by the PUF performance of the proposed D flip-flop is discussed in Section 5, followed by the conclusion in Section 6.

2. Related work

D flip-flop based PUF was first introduced in [11]. The authors have used the power-up state of D flip-flop as a PUF on FPGA. Similar to the SRAM, upon power-up, all the D flip flops on FPGA are initialized to the specified initial value or '0' if the user does not specify an initial value. In [11], this initialization is prevented by removing the *global restore line* command from the bit file. However, this alteration in bit file affects the behavior of other modules mentioned in bit file, as no flip flop in any module is initialized, and this cause a fault finite-state-machine based designs like a counter or any design where initialization is essential. Similar to the SRAM PUF, D flip-flop based PUF can also be used only once until a (p)reset or a data has not been stored.

An ASIC implementation of the D flip flop based PUF is presented

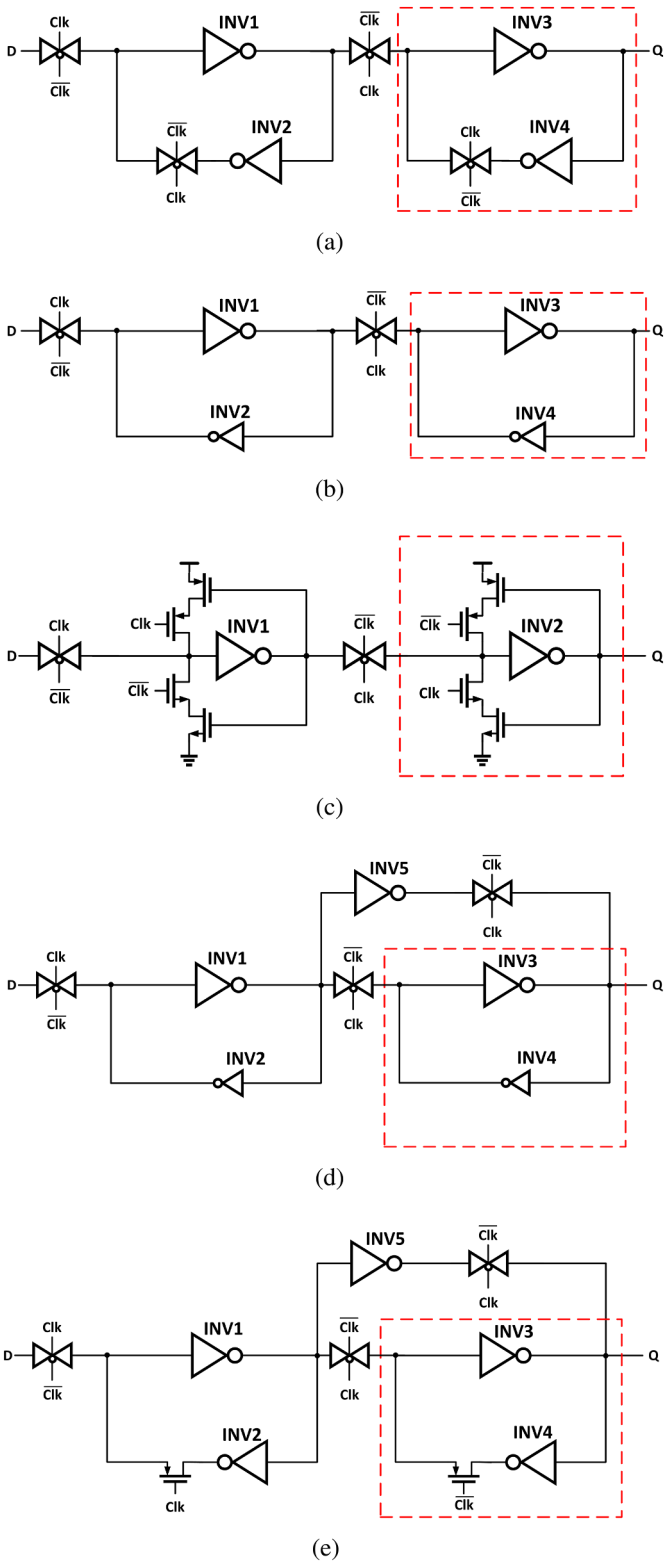


Fig. 1. D flip-flop architectures: (a) conventional [13], (b) low area [12], (c) cow power [14], (d) push-pull [12], (e) push-pull isolation [12].

in [15], where the PUF responses are extracted from 40 devices. However, a strong bias towards '0' and '1' is found. A similar effect has also been reported in FPGA [11]. Hence, a post-processing scheme is required to reduce the effect, which costs hardware and power overhead. The reason for the strong biased is described in the following subsection.

2.1. Bias in D flip-flop

State-of-the-art D flip-flop architectures including the conventional D flip-flop is shown in Fig. 1. It can be seen from Fig. 1 (a), (c)–(e), that the cross coupled inverters are not symmetrical due to presence of transistor(s) in the output path of *INV* 4. Because of the asymmetrical cross-coupled architecture, the top inverter dominates the other one. When used as a PUF, this asymmetry results in a bias towards '1' or '0', hence upon power-on, most of the flip-flops prefer to resolve to either '1' or '0'. The architectures of Fig. 1 (a), (d), and (e) requires additional pass transistor(s) in the output of second inverter that makes the second transistor slower than the other one. In Fig. 1 (c) one inverter with a tri-state inverter is used to reduce the power consumption. However, A tri-state inverter is slower than the conventional CMOS inverter. Although in Fig. 1 (b) and (d), both inverters look like similar but to minimize the short circuit power dissipation due to the voltage contention, the width of transistors in the feedback inverter are kept smaller than the other one. Thus, the smaller transistor width makes the feedback inverter slower. Hence in all the implementation, the top inverter dominates over the other one that becomes the main cause for the affinity of a bias towards '1' or '0' in PUF responses.

3. Proposed D flip flop with integrated PUF

It is in the literature that the PUF architecture with symmetric cross-coupled inverters shows a high value of uniqueness [7, 16, 17]. Thus based on this the proposed D flip-flop architecture in Fig. 2 has two additional pass transistors (*M*12, *M*13) to make it symmetrical. To re-generate the PUF responses even after a (p)reset or write operation, *M9* are added to bring *INV* 3 and *INV* 4 in an unstable state. The truth table of the proposed D flip-flop for flip-flop and PUF operation is shown in Table 1.

Table 1
Truth table of the proposed D flip-flop.

Input Clk	D	PUF	Output Q_{N+1}	$\overline{Q_{N+1}}$	Operation
1	X	0	Q_N	$\overline{Q_N}$	Flip-flop
0	X	0	Q_N	$\overline{Q_N}$	Flip-flop
↑	1	0	1	0	Flip-flop
↑	0	0	0	1	Flip-flop
↓	X	0	Q_N	$\overline{Q_N}$	Flip-flop
1	1	1	1	1	PUF
1	0	1	0	0	PUF
0	X	0	*PUF_OUT*	$\overline{PUF\_OUT}$	PUF

From Table 1 it is clear that, when $PUF = '0'$ the proposed circuit acts as a normal positive-edge-triggered D flip-flop. When $Clk = '1'$ and $PUF = '1'$ then both the outputs Q_{N+1} and $\overline{Q_{N+1}}$ are set to either '0' or '1' depending upon the output of the previous latch. In this state Q_N is not a complement of Q_N, since both are either '0' or '1' at the same time. In this condition the equivalent circuit of the proposed D flip-flop is shown in Fig. 3. Now when both *Clk* and *PUF* become '0', Q_N and Q_{N+1}, quickly settle back to one of the two stable states which depend upon the mismatch. Now $\overline{Q_N}$ becomes the complement of Q_N.

3.1. Mathematical model for mismatch analysis

As discussed, the circuit is used as a PUF when both *Clk* and *PUF* signals are at logic high. Setting $Clk = PUF = '1'$ forces the outputs Q_N and $\overline{Q_N}$ to either '0' or '1' and when we force $Clk = PUF = '0'$, because of the cross-coupling, the input and output of both the inverters become the same for a moment. Consider after setting $Clk = PUF = '0'$, the voltage at the input of both inverters (*INV* 3 and *INV* 4) is *x*, Hence $V_Q = V_{\bar{Q}} = x$.

Since $Clk = PUF = '0'$, for simplification purpose, replacing the transmission gates with short circuit as shown in Fig. 3

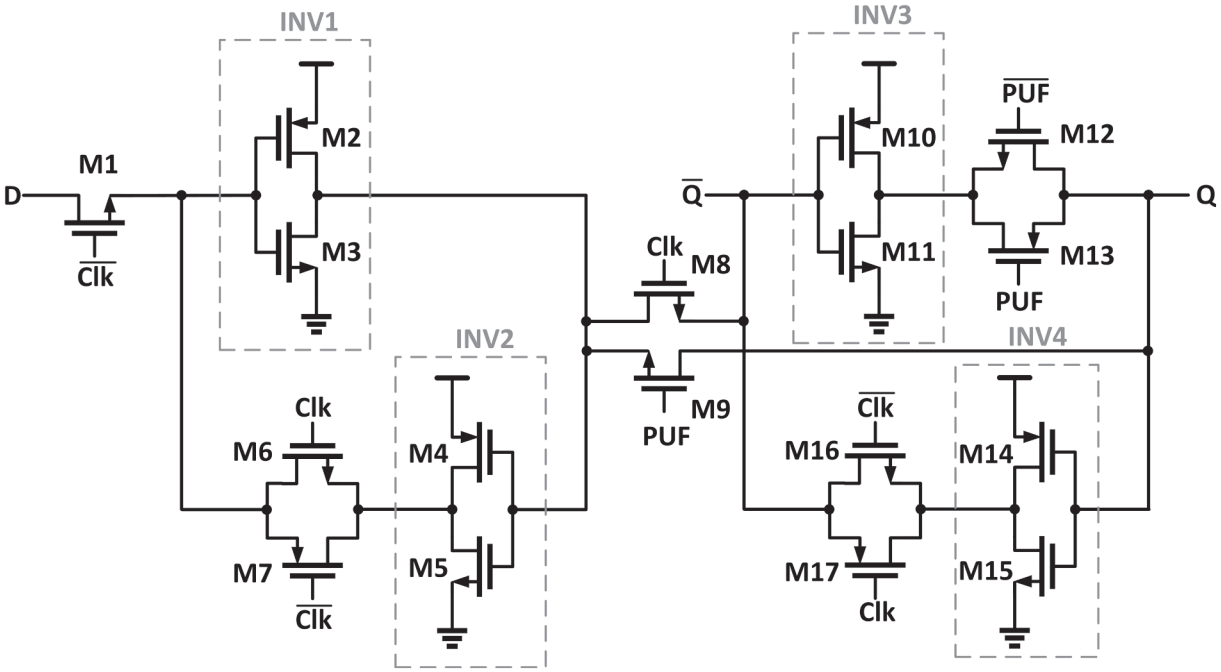


Fig. 2. Schematic of the proposed D flip-flop. Additional pass transistors (*M*12 and *M*13) are added to make the circuit symmetric.

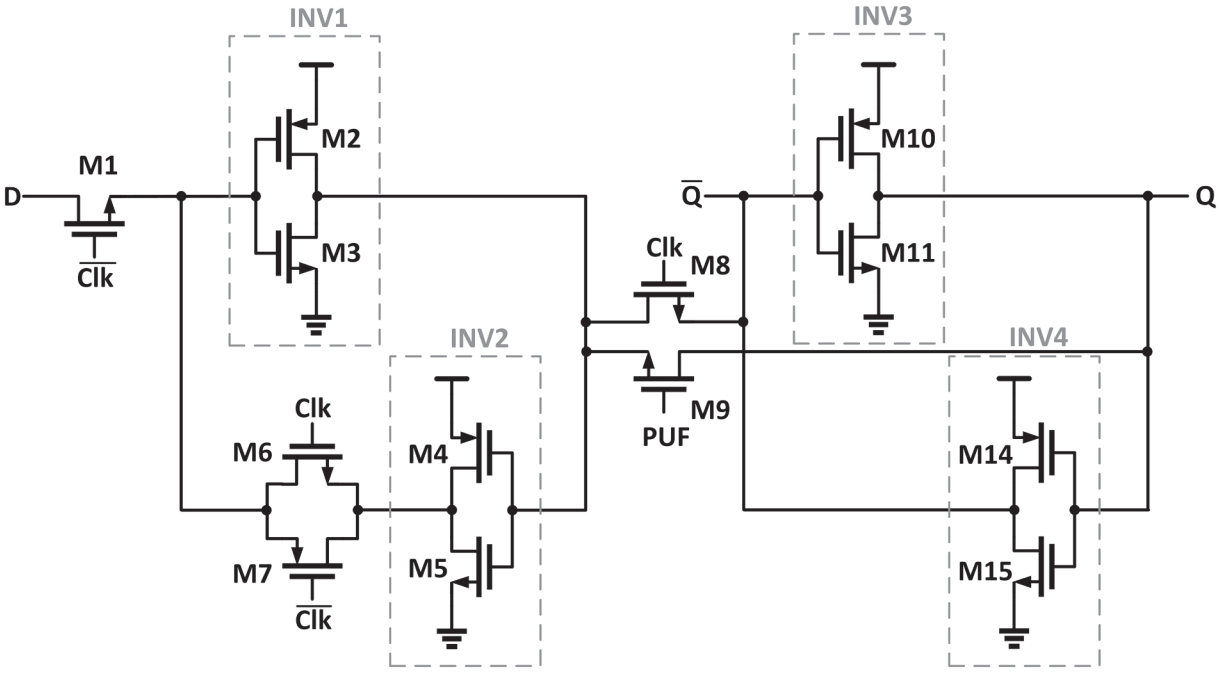


Fig. 3. Equivalent circuit of proposed architecture when *PUF* and *Clk* = '0', in this condition, two pass transistors act as a short circuit.

$$V_{SD_{M10}} = V_{SG_{M14}} = V_{DD} - x = V_{DD} - V_Q \tag{1}$$

$$V_{SG_{M10}} = V_{SD_{M14}} = V_{DD} - x = V_{DD} - V_{\bar{Q}} \tag{2}$$

Similarly,

$$V_{DS_{M11}} = V_{GS_{M15}} = x = V_Q \tag{3}$$

$$V_{GS_{M11}} = V_{DS_{M15}} = x = V_{\bar{Q}} \tag{4}$$

The condition for NMOS to be in saturation is

$$V_{DS_N} \geq V_{GS_N} - V_{T_N}$$

Similarly, for PMOS

$$V_{SD_P} \geq V_{SG_P} - |V_{T_P}|$$

Here, $M10$, $M11$, $M14$, and $M15$ are in the saturation. Hence,

$$I_{D_{M11}} = I_{D_{M10}}$$

$$\frac{1}{2}\mu_N C_{ox}\frac{W_N}{L}(V_{\bar{Q}} - V_{T_{M11}})^2 = \frac{1}{2}\mu_P C_{ox}\frac{W_P}{L}(V_{DD} - V_{\bar{Q}} - |V_{M10}|)^2 \tag{5}$$

or,

$$(V_{\bar{Q}} - V_{T_{M11}}) = (V_{DD} - V_{\bar{Q}} - |V_{T_{M10}}|)\alpha$$

or,

$$V_{\bar{Q}} = \frac{(V_{DD} - |V_{T_{M10}}|)\alpha + V_{T_{M11}}}{(1+\alpha)} \tag{6}$$

where

$$\alpha = \sqrt{\frac{\mu_{M10} W_{M10}}{\mu_{M11} W_{M11}}}$$

Similarly,

$$V_Q = \frac{(V_{DD} - |V_{T_{M14}}|)\beta + V_{T_{M15}}}{(1+\beta)} \tag{7}$$

where

$$\beta = \sqrt{\frac{\mu_{M14} W_{M14}}{\mu_{M15} W_{M15}}}$$

Now assume that $\alpha = \beta$ (Assuming both *INV* 3 and *INV* 4 are identical), then

$$V_Q = V_{\bar{Q}} = \frac{(V_{DD} - |V_{T_{M14}}|)\beta + V_{T_{M15}}}{(1+\beta)} = \frac{(V_{DD} - |V_{T_{M10}}|)\alpha + V_{T_{M11}}}{(1+\alpha)} \tag{8}$$

From Eq. (8) it is clear that when both the inverters are perfectly matched, i.e $W_{M10} = W_{M14}$, $\mu_{M10} = \mu_{M14}$, $W_{M11} = W_{M15}$ and $\mu_{M11} = \mu_{M15}$ then the output of both the inverters is same.

Now if there is a slight mismatch between NMOS and/or PMOS of both the inverters, then the following conditions can occur:

- If $\mu_{M14} > \mu_{M10}$ and/or $W_{M14} > W_{M10}$ this will make $\beta > \alpha$ and hence $V_Q < V_{\bar{Q}}$. From Eqs. (1)–(4) it can be seen that in this condition $M11$ and $M14$ goes into linear region while $M10$ and $M15$ are in saturation region. From the voltage-transfer-curve of CMOS inverter it can be observed that, in this situation the output of the top inverter is near to '0' while the output of bottom inverter is near to V_{DD}. Hence in this case Q and $\bar{Q}$ settle to '0' and V_{DD}, respectively.
- If $\mu_{M15} > \mu_{M11}$ and/or $W_{M15} > W_{M11}$ this will make $\beta < \alpha$ and hence $V_Q > V_{\bar{Q}}$. In this condition $M10$ and $M15$ goes into linear region while $M11$ and $M14$ are in saturation region. Hence in this case, Q and $\bar{Q}$ settle to V_{DD} and '0', respectively.
- If $V_{T_{M14}} > V_{T_{M10}}$ this will make $V_Q < V_{\bar{Q}}$. In this condition $M11$ and $M14$ goes into linear region while $M10$ and $M15$ are in saturation region. Hence in this case, Q and $\bar{Q}$ settle to '0' and V_{DD}, respectively.
- If $V_{T_{M11}} < V_{T_{M15}}$ this will make $V_Q > V_{\bar{Q}}$. In this condition $M10$ and $M15$ goes into linear region while $M11$ and $M14$ are in saturation region. Hence in this case, Q and $\bar{Q}$ settle to V_{DD} and '0', respectively.

From the above discussion, it is clear that whenever there is a mismatch between both of the inverters, Q and $\bar{Q}$ settle to any stable and opposite state. So far, in our analysis, we have neglected the transmission gate for the sake of simplification. However, the transmission gate transistors are also subjected to process variations, and

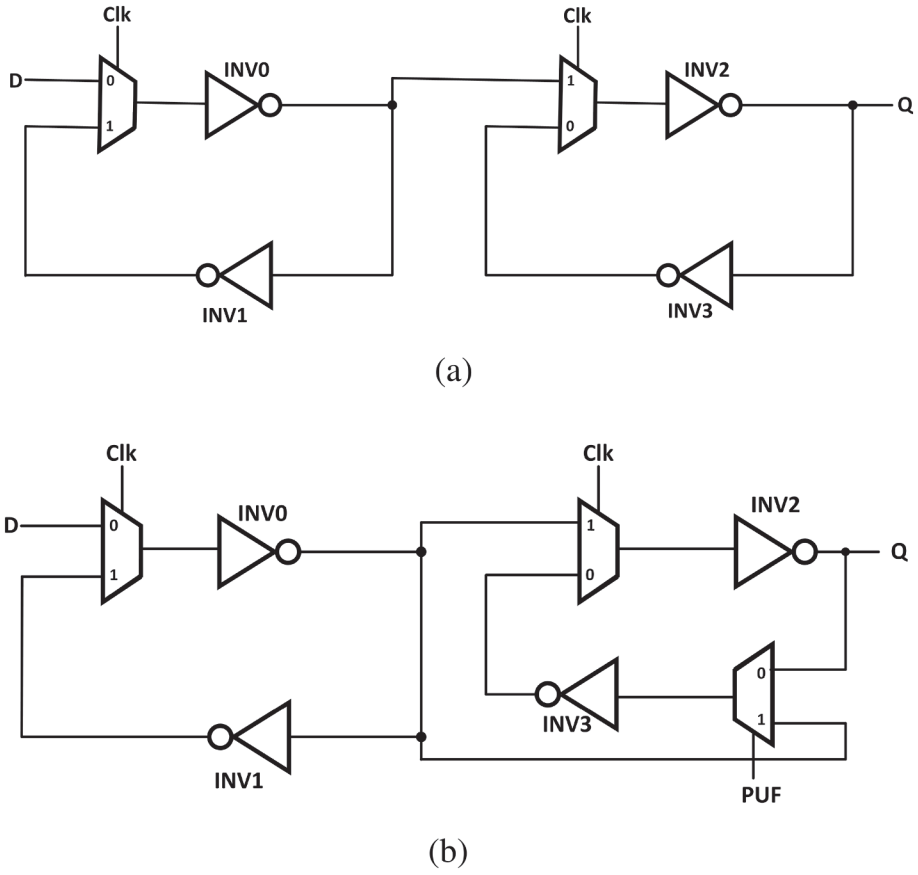


Fig. 4. FPGA implemented architecture of (a) conventional and (b) proposed D flip-flop.

due to process variation, they also get some unique characteristics. Together with inverters, the pass transistor also contributes to the increase of the uniqueness. Therefore when used as a PUF, the proposed D flip-flop shows higher uniqueness when compared with the other state-of-the-art D flip-flop architectures.

4. FPGA implementation: the functional testing

To verify the functional correctness of the proposed D flip-flop, we have implemented the logically equivalent circuit of the proposed and conventional D flip-flop on ten Basys3 FPGA boards using *Xilinx Vivado*. The FPGA implemented circuit is shown in Fig. 4, where the two transmission gates are replaced by a multiplexer. We have implemented 1024 instances of proposed and conventional D flip-flop in three different locations on each FPGA, in total, we have 240 128-bit PUF responses for the proposed as well as a conventional D flip-flop. All the instances are placed manually to avoid any routing effect.

Fig. 5 shows a comparison for the distribution of one and zero between proposed and conventional D flip-flop PUF. In FPGA implementation, we have taken 240 samples of both the architectures, and in correspond to each sample, we have analyzed the number of ones and zeros presented in each 128-bit response. From Fig. 5, we can observe that although the distribution is scattered, the number of ones and zeros are distributed randomly and centered around the mean value for the proposed D flip-flop, while the conventional D flip-flop has more number of ones than zeros. It is also observed that the mean value of one's population for proposed and conventional D flip-flops are 62.961 and 121.179, respectively.

4.1. Uniqueness

The uniqueness differentiates the responses obtained from two PUF instances and calculated using the inter-die Hamming distance (HD). It has an ideal value of 50%, which means when the same challenge is applied to any two PUF instances, then half of the PUF response should be different.

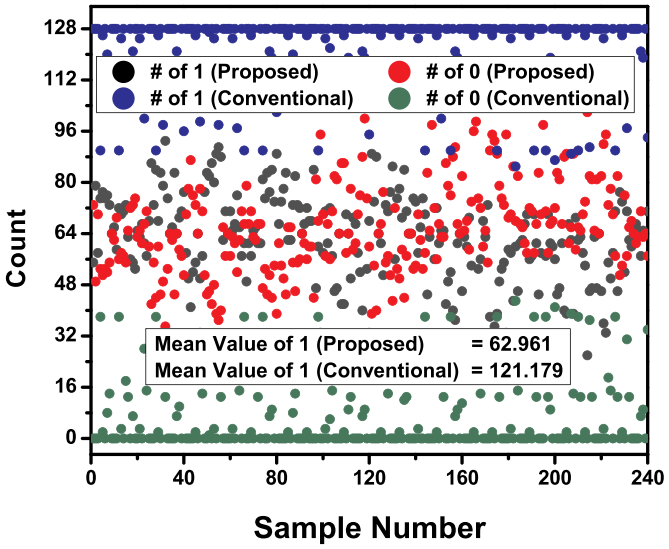


Fig. 5. FPGA implemented distribution of one and zero for the proposed and conventional D flip-flop.

Let us consider that corresponds to a challenge *C*, *Rp* and *Rq* are respectively two *n*-bit responses from randomly selected chip *p* and *q* out of *m* number of available chips. The uniqueness(U) from *m* chips can be expressed as:

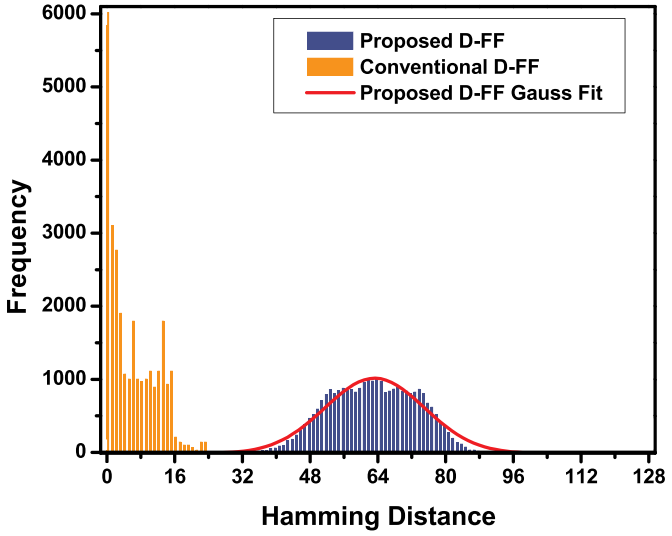


Fig. 6. FPGA implemented distribution of inter-chip hamming distance for the proposed and conventional D flip-flop.

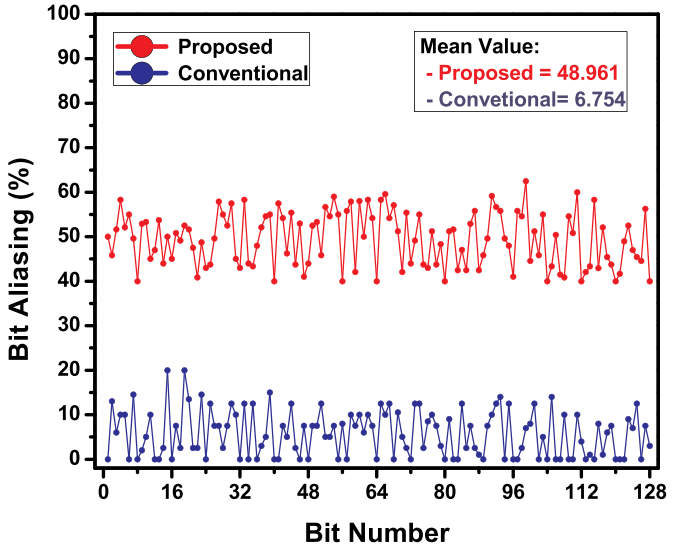


Fig. 7. Bit-aliasing effect in proposed and conventional D flip-flop in FPGA implementation.

$$U = \frac{2}{m(m-1)} \sum_{p=1}^{m-1} \sum_{q=p+1}^{m} \frac{HD(R_p, R_q)}{n} \times 100\% \tag{9}$$

where, $HD(R_p,R_q)$ is the hamming distance between R_p and R_q

The distribution of fractional Hamming distance for the proposed and conventional architecture is shown in Fig. 6. From the histogram, it is observed that the histogram is symmetrical to its center value 64 for the proposed PUF, which means, out of 128-bit most of the time, 64-bits are different in two PUF responses. For the conventional architecture, the hamming distance has values between 0 to 26-bit, which means most of the time, two 128-bit PUF responses have differed to each other by 0 to 26-bits. In the conventional architecture, most of the time, the two 128-bit PUF responses have either no difference at all or maximum have a 26-bit difference only. Also, the calculated uniqueness value for the conventional PUF and proposed PUF are 0.103 and 0.492, respectively. The uniqueness of the proposed PUF is very close to the ideal value and also much better than the conventional D flip-flop PUF architecture.

4.2. Bit-aliasing

Systematic variations causes multiple chips to produce significantly same response for same challenge and results in bit-aliasing [18]. For a challenge C, bit-aliasing for the *i*th bit of a PUF across *n* number of different chips can be defined as:

$$\text{Bit-aliasing} = \frac{1}{n} \sum_{j=1}^{n} R_{i,j} \times 100\% \tag{10}$$

where *n* is the number of chips and $R_{i,j}$ is the value of *i*th bit in the *j*th chip response. Bit-aliasing has an ideal value of 50%.

To consider the effect of systematic variation, we have calculated the bit-aliasing in all 128-bit of proposed as well as conventional D flip-flop architectures, as shown in Fig. 7. From results, it can be seen that, with a maximum value of 60 and a minimum value of 40, the proposed architecture has a mean value of 48.961 for the bit-aliasing, which is also close to the ideal value 50. The conventional architecture has a mean value of 6.754 with a minimum and maximum value of 0 and 20, respectively.

5. ASIC implementation and simulation results

In order to explain the usefulness of the proposed D flip-flop along with it, the conventional [13], low area based [12], low power based [14], push-pull based [12], push-pull isolation based [12] D flip-flop architectures have been implemented on 40 nm industry-standard foundry. We have also drawn the layout of the conventional and proposed flip-flop for better area comparison. Fig. 8 shows the layout of the conventional and proposed D flip-flop. From Fig. 8 it can be seen that, the proposed flop-flop has 1.056 times larger width and 0.948 times smaller length as compared to the conventional flip-flop. The conventional and proposed architectures have an area of 4.330 μm^2 and 4.336 μm^2, respectively. Although the proposed D flip-flop has more number of transistors than conventional architecture, due to the use of drain sharing technique, the overall area of the proposed architecture is almost the same as the conventional D flip-flop architecture.

All the simulations were performed using *Cadence V irtuoso* at V_{DD} = 1.1 *V* and considering operation temperature of 27 °C, unless specified. Since the primary function of the proposed circuit is to be used as a flip-flop, hence, apart from PUF, all the flip-flop parameters are also extracted.

5.1. Performance as a flip-flop

Power and delay are the two important parameters for the analysis of a flip-flop. The flip-flop performance of the proposed architecture, along with existing architectures, is analyzed by varying supply voltages and observing the Clock-to-Q delay, dynamic power, and leakage power. The Clock-to-Q delay of various D flip-flop architectures at different supply voltages are shown in Fig. 9. From results, it can be seen that among all of the implemented architectures, the push-pull isolation flip-flop has the lowest Clock-to-Q delay because it uses the push-pull architecture. However, the proposed architecture has delay comparable to the conventional D flip-flop. The negligible delay difference is due to the use of an additional transmission gate in the second latch. The proposed D flip-flop has 2.04% and 0.43% more delay as compared to the conventional flip-flop, at the supply voltage of 0.6 V and 1.1 V, respectively. Results also demonstrate that the delay difference among considerable architectures reduces as the supply voltage increase.

The dynamic power consumption of all the considered D flip-flop at the room temperature with various supply voltages is shown in Fig. 10 (a). The proposed architecture consumes less dynamic power compared to push-pull, low area, and push-pull isolation, because the proposed architecture has less number of transistor compared to push-pull

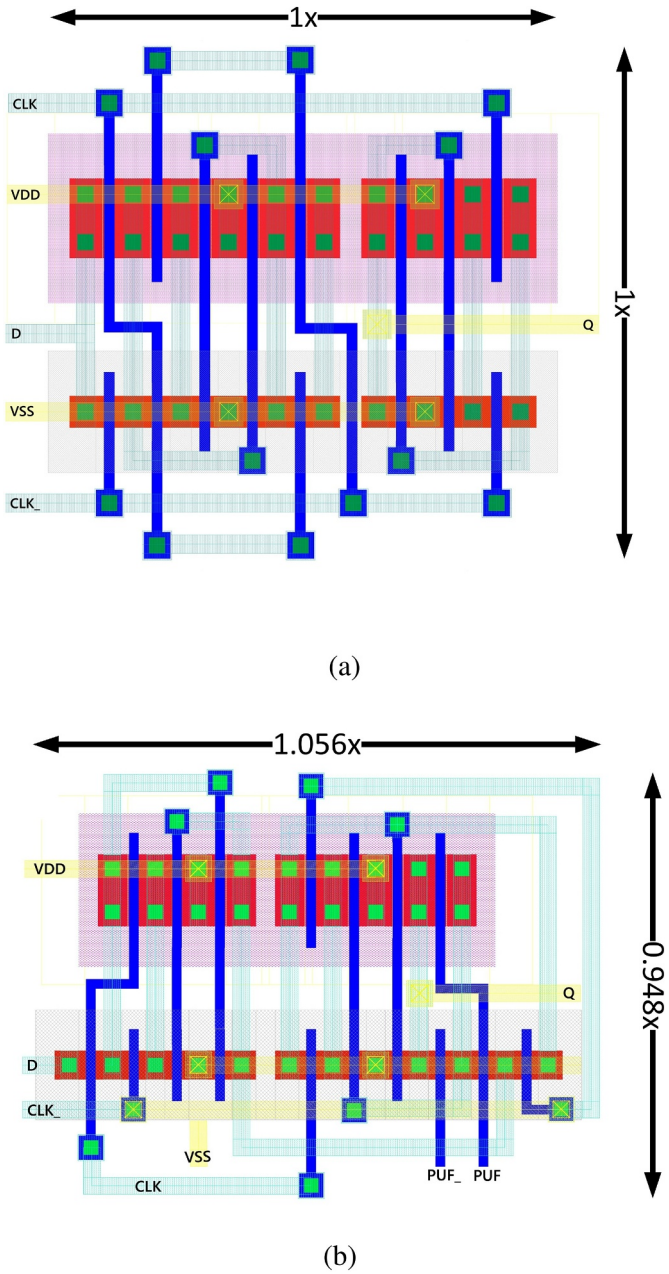


Fig. 8. Layout of: (a) conventional D flip-flop (b) proposed D flip-flop.

isolation and no short circuit power dissipation as in case of low area and push-pull architectures. However, power consumption is higher when compared to the conventional and low power D flip-flop, because the proposed architecture has more number of transistors. The proposed D flip-flop has 0.72% and 8.61% more dynamic power consumption as compared to the conventional flip-flop, at the supply voltage of 0.6 V and 1.1 V, respectively.

To analyze the power consumption during static conditions, when the architecture is used as a flip-flop, we have evaluated the leakage power of all the considered circuits with the supply voltage variations. The leakage power consumption at various supply voltage considering 27 ˚C operating temperature is shown in Fig. 10 (b). The proposed architecture consumes less leakage power compared to push-pull isolation because the proposed architecture has less number of transistors compared to push-pull isolation. However, leakage power consumption is nominally higher when compared to the low area, low power, push-pull, and conventional D flip-flop, because the proposed architecture

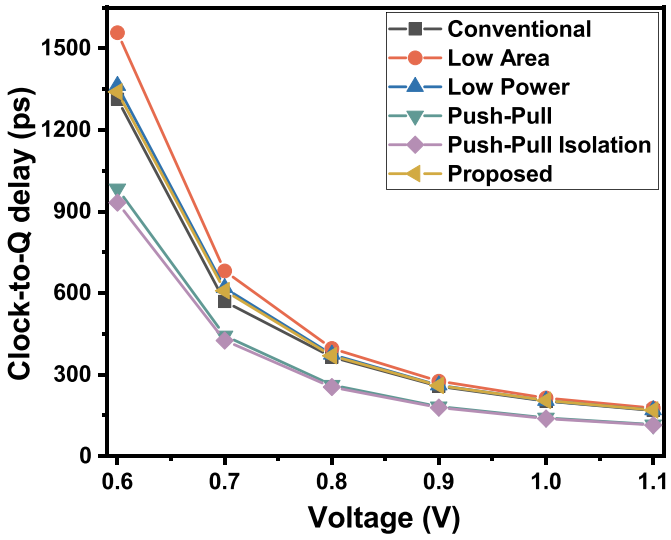


Fig. 9. Clock-to-Q delay of various D flip-flop architectures at different supply voltages.

has more number of transistors. Results show that the proposed D flip-flop has 0.72% and 2.50% more leakage power as compared to the conventional flip-flop, at the supply voltage of 0.6 V and 1.1 V, respectively.

5.2. Performance as a PUF

We have performed 350-thousand sets of Monte Carlo simulation with ± 3σ deviation on proposed PUF along with the conventional [13], low area [12], low power [14], push-pull [12], push-pull isolation [12] architectures. This gives us 2734 128-bit challenge-response-pairs (CRPs). Fig. 11 shows a comparison between proposed and conventional D flip-flop PUF for the distribution of one and zero. We have taken 1054 samples of both the architectures and in correspond to each sample, we have analyzed the number of ones and zeros. It can be seen from Fig. 11 that the number of ones and zeros are approximately equal for the proposed D flip-flop and is centered around the mean value 64, while the conventional flip-flop has more number of ones than zeros. It is also observed that the mean value of one's population for proposed and conventional D flip-flop are 63.876 and 126.872, respectively. The above discussions indicate that the proposed D flip-flop has symmetric distribution for both one's and zero's as compared to conventional D flip-flop.

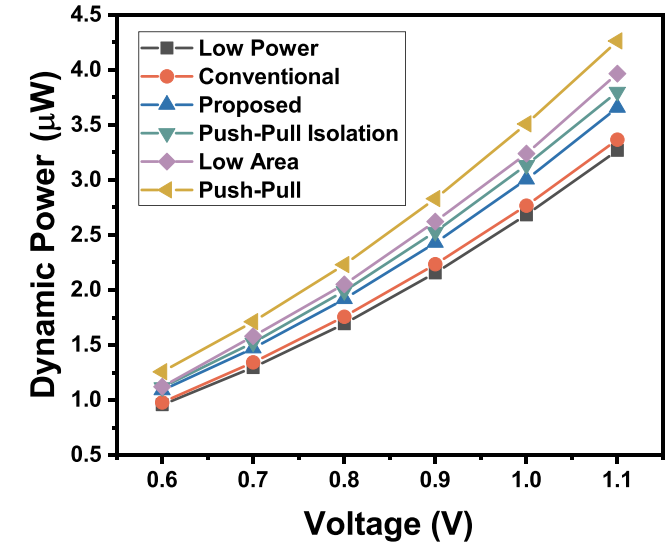
The performance as a PUF has been analyzed on the basis of Bit-aliasing, Uniqueness, Reliability, and Randomness. A detailed description of each of the above parameters is presented in the following subsections.

5.2.1. Bit-aliasing

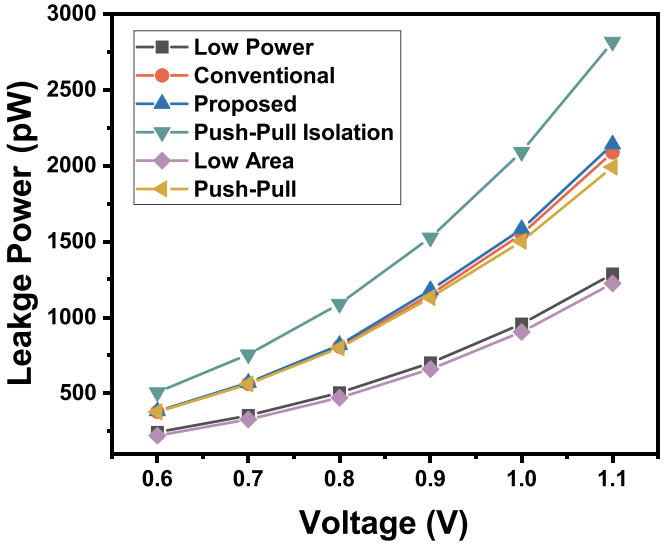
Bit-aliasing effect in the ASIC implementation of proposed and conventional architecture is shown in Fig. 12. From results, it can be seen that with a maximum value of 52 and a minimum value of 47, the proposed architecture has a mean value of 49.613 for the bit-aliasing, which is also very close to the ideal value 50. The conventional architecture has a mean value of 5.676 with a minimum and maximum value of 1 and 97, respectively.

5.2.2. Uniqueness

Fig. 13 shows the uniqueness value for the various considered PUF architectures. The result shows that the proposed architecture has the highest uniqueness, which is also very closed to the ideal value of 0.5. The higher uniqueness value for the proposed PUF is because of the symmetric feedback and main path. Apart from proposed architecture,



(a)



(b)

Fig. 10. Power consumption of different D flip-flop architectures with various supply voltages: (a) dynamic power (b) leakage power.

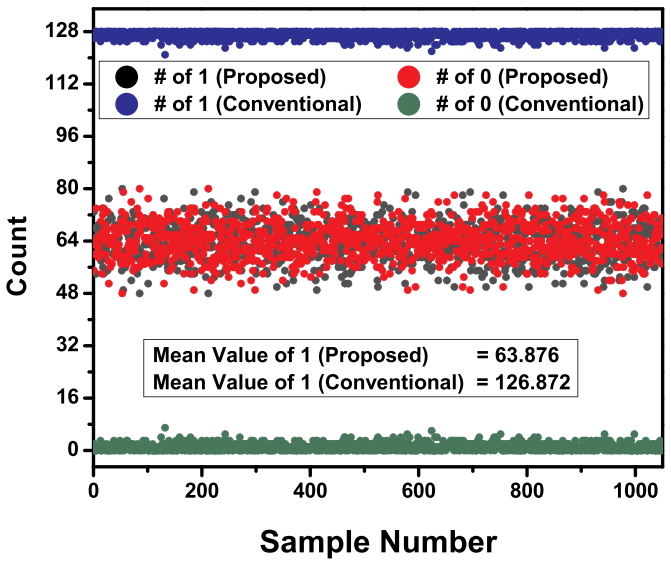


Fig. 11. Distribution of one and zero in proposed and conventional D flip-flop in ASIC implementation.

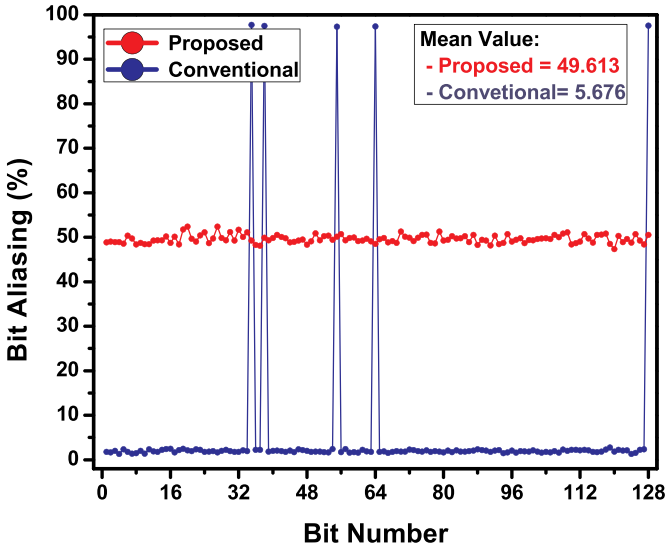


Fig. 12. Bit-aliasing effect in proposed and conventional D flip-flop in ASIC implementation.

the low area and push-pull architectures have almost the same and second-highest value, and this is because in both of the architectures, there is no transmission gate or pass transistor in the path of the cross-coupled inverters. But still, the uniqueness value of the low area and push-pull architecture is not good, due to the mismatch in width of both the inverters in main and feedback paths.

The distribution of fractional Hamming distance for the proposed and conventional architecture is shown in Fig. 14. From the histogram, it can be seen that for the proposed PUF, the histogram is symmetrical to its center value 64, which means out of 128-bit most of the time, 64-bits are different in two PUF responses. It has a minimum value of 48 and 80, which means at the worst case it has a minimum 48-bit and a maximum 80-bit difference out of 128-bit PUF responses. For the conventional architecture, the hamming distance has values between 0 to 8-bit, which means most of the time, two 128-bit PUF responses have differed to each other by 0 to 8-bit. Hence in the conventional architecture, the two 128-bit PUF responses have either no difference at all or have the only 8-bit difference. Also, the calculated uniqueness value for the conventional PUF is 0.112, and for the proposed PUF, it is 0.503, which is very close to the ideal value and much better than the other implemented architectures. The uniqueness near to the ideal value shows that the proposed architecture is an excellent candidate for IoT security applications.

5.2.3. *Reliability*

Reliability is a measure of the PUF stability under various environmental conditions. Ideally, the PUF response under varying environmental conditions should be the same, however, temperature variation and supply voltage fluctuations are the two major factors which affect the performance of a circuit in practice. Reliability can be measured by comparing the two responses of the same chip taken at different temperatures and/or supply voltages. The reliability R of a chip can be measured by:

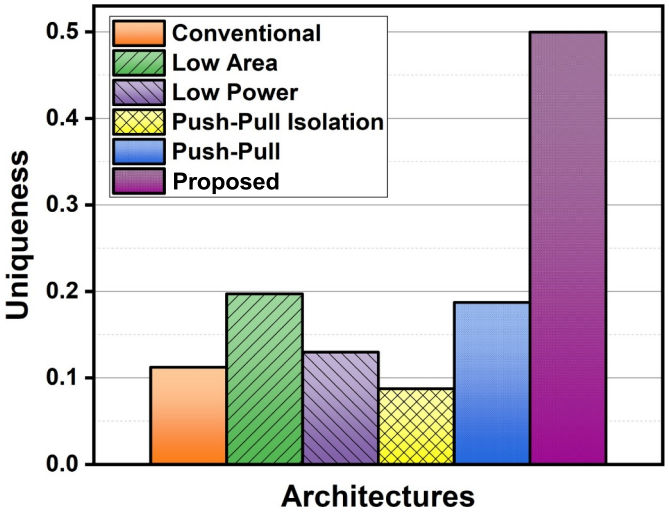


Fig. 13. Simulated uniqueness of various architectures.

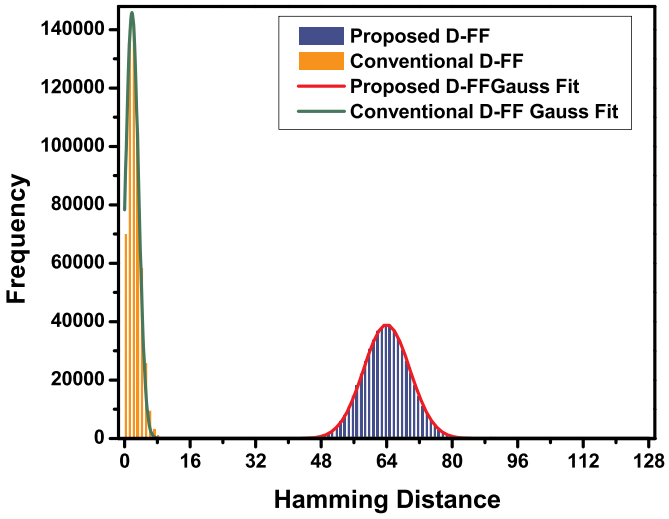


Fig. 14. Distribution of hamming distance for the proposed and conventional D flip-flop based PUF.

$$R = 1 - \frac{1}{k}\sum_{m=1}^{k}\frac{HD(R_a, R_a')}{n} \times 100\% \tag{11}$$

where k is the number of samples, n is the number of generated bits, R_a and R_a' are the responses taken at nominal and varying operating conditions, respectively. and $HD(R_a, R_a')$ is the Hamming distance between R_a and R_a'.

Since the temperature and supply voltage variations are two primary concern for PUF reliability, we have measured the reliability of all the implemented architectures after varying the supply voltage and the operating temperature. The nominal operating voltage for the PDK is 1.1 V, we have changed the supply voltage with ± 10%.

Fig. 15 (a), (b) shows the supply voltage reliability at 1 V and 1.2 V, respectively, considering 27 °C operating temperature. It can be seen that among all of the architectures, the proposed one has the lowest value for the supply voltage reliability. When compared to the conventional D flip-flop PUF, the proposed PUF has 1.56% and 1.05% less reliability at 1 V and 1.2 V, respectively.

Similarly, Fig. 16 (a) and (b) show the thermal reliability at 100 °C, and 125 °C, respectively considering 1.1 V supply voltage. It can be seen that among all of the architectures of the proposed one has the lowest value for the thermal reliability. When compared to the conventional D flip-flop PUF, the proposed PUF has 1.16% and 1.93% less thermal reliability at 100 °C and 125 °C, respectively.

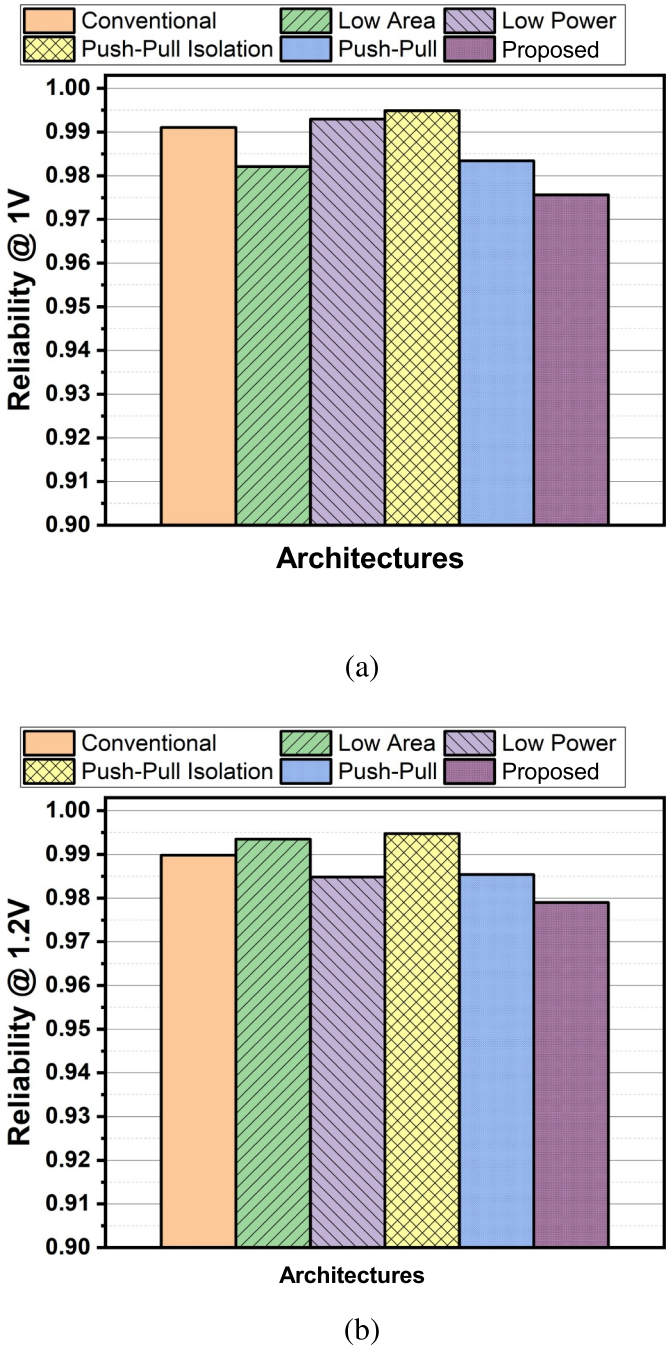
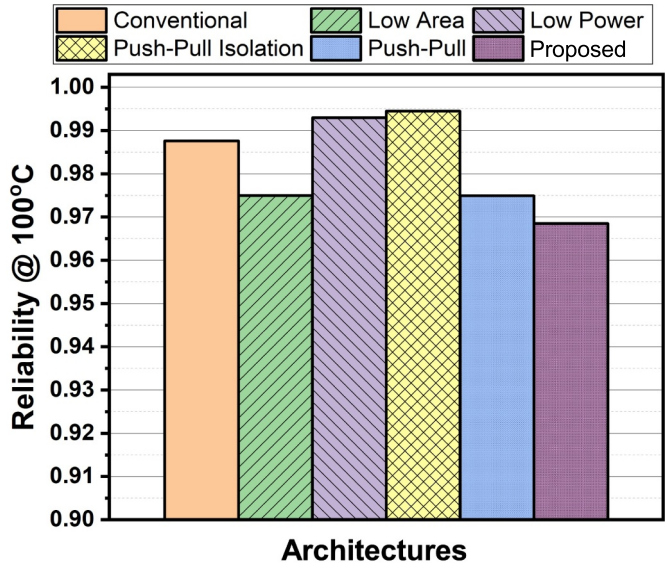


Fig. 15. Simulated reliability of various architectures at 27 °C operating temperature with supply voltage variations: (a) 1 V and (b) 1.2 V.

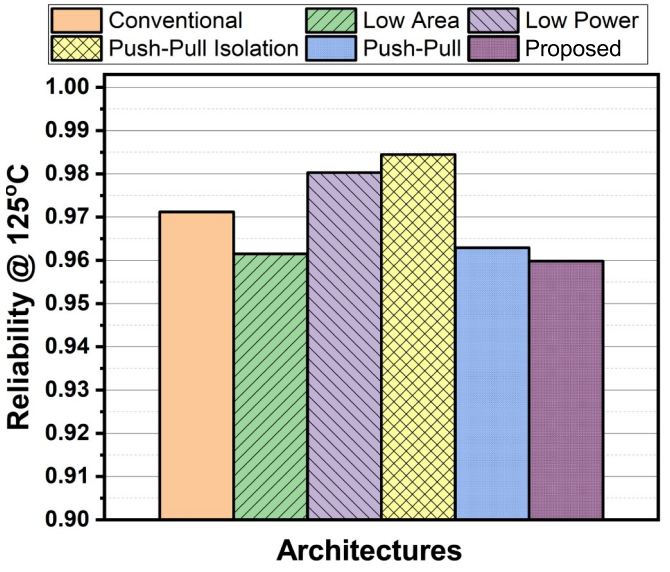
It can be seen that among all of the considered architectures, the proposed one has the lowest value for the thermal and supply voltage reliability. Since the primary function of a PUF is to provide uniqueness to every integrated circuit. Without uniqueness, reliability is not useful. Although, rest of the architectures has a higher value of reliability, but they failed to provide a good uniqueness, which is an essential PUF performance parameter, while the proposed architecture shows better uniqueness with an acceptable value of reliability.

5.2.4. *Reliability-to-uniqueness ratio (RUR)*

In any PUF implementation, reliability and uniqueness are the two desired PUF parameters. Uniqueness has an ideal value of 0.5, while the



(a)



(b)

Fig. 16. Simulated reliability of various architectures at 1.1 V supply voltage with temperature variations: (a) 100 °C and (b) 125 °C.

ideal value for reliability is 1. To evaluate the PUF performance of all the considered architectures, we have proposed a term reliability-to-uniqueness ratio (RUR) which can be defined as:

$$RUR = \frac{R_{WT} + R_{WS}}{2 \times |(0.5 - U)|} \tag{12}$$

where U is the uniqueness, and R_{WT} and R_{WS} are the worst-case thermal and supply voltage reliability, respectively. The reliability-to-uniqueness ratio for various architectures are shown in Fig. 17. The result shows that among all the considered architectures, the proposed architecture has the highest value for the reliability-to-uniqueness ratio, which means the performance of the proposed architecture as a PUF is much better than the other considered architectures.

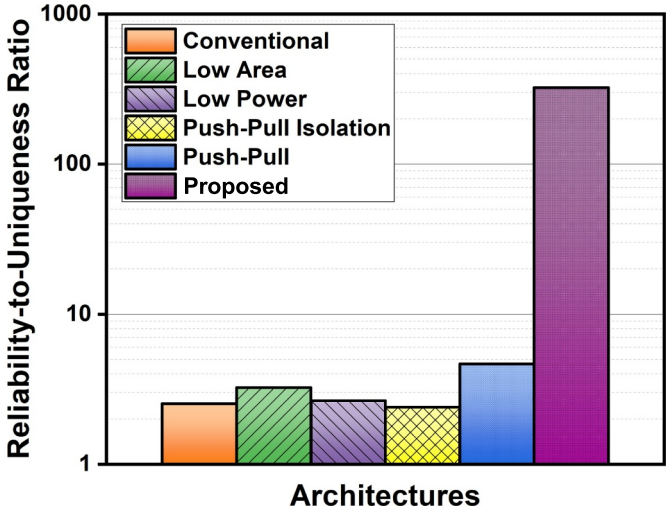


Fig. 17. Reliability-to-uniqueness ratio for various architectures.

5.2.5. Randomness

Apart from uniqueness and reliability, the randomness is another PUF property, which states that the PUF output must be random. This means that in a PUF set, the responses of any PUF should be unpredictable in nature. To evaluate the randomness, we have used the PUF responses as input to the NIST randomness test suite [19]. Table 2 shows that the proposed PUF passes all the NIST randomness tests that we are able to perform. Due to the limited number of the dataset, the NIST randomness test that requires a large dataset has been omitted.

6. Conclusion

In this paper, we have presented a symmetric D flip-flop with improved uniqueness. The proposed design shows a better uniqueness as compared to the other existing architectures without using any post-processing schemes. The FPGA implementation verifies the functional correctness of the proposed architecture. The proposed PUF passes all the NIST randomness tests, which we were able to perform. The power and delay of the proposed flip-flop are almost the same as the conventional flip-flop. The proposed architecture requires the same area when compared with the conventional flip-flop. However, on the other hand, a large amount of area can be saved since the proposed architecture does not require and post-processing schemes. From the above discussion, we can conclude that the proposed architecture has better PUF performance compared to the other existing architectures, which makes it suitable for PUF implementation in miniaturized IoT ASIC.

CRediT authorship contribution statement

Sajid Khan: Conceptualization, Methodology, Investigation. **Ambika Prasad Shah:** Data curation, Writing - original draft. **Shailesh Singh Chouhan:** Visualization, Writing - review & editing. **Neha Gupta:** Software. **Jai Gopal Pandey:** Formal analysis. **Santosh Kumar Vishvakarma:** Project administration, Supervision.

Table 2
NIST randomness test suite result.

NIST test	P-value	Proportion	Status
Frequency	0.0974	328/330	Pass
Block frequency	0.4917	326/330	Pass
Cumulative sums (forward)	0.0494	328/330	Pass
Cumulative sums (reverse)	0.1345	329/330	Pass
Runs	0.0187	329/330	Pass
Serial	0.0193	326/330	Pass

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The authors would like to thank the UGC, Government of India, under the JRF Scheme for providing financial support (Ref. No. 3548/NET-DEC. 2015). We also extend our sincere gratitude to the SMDP-C2SD program Government of India.

References

[1] A. Zanella, N. Bui, A. Castellani, L. Vangelista, M. Zorzi, Internet of things for smart cities, IEEE Internet Things J. 1 (1) (2014) 22–32.
[2] A.-R. Sadeghi, C. Wachsmann, M. Waidner, Security and privacy challenges in industrial internet of things, Proceedings of the 52nd Annual Design Automation Conference, ACM, 2015, p. 54.
[3] B. Halak, J. Murphy, A. Yakovlev, Power balanced circuits for leakage-power-attacks resilient design, Science and Information Conference (SAI), IEEE, 2015, pp. 1178–1183.
[4] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, V. Khandelwal, Design and implementation of PUF-based "unclonable" RFID ICs for anti-counterfeiting and security applications, 2008 IEEE International Conference on RFID, IEEE, 2008, pp. 58–64.
[5] K. Yang, Q. Dong, D. Blaauw, D. Sylvester, 14.2 A physically unclonable function with BER < 10-8 for robust chip authentication using oscillator collapse in 40 nm CMOS, 2015 IEEE International Solid-State Circuits Conference-(ISSCC) Digest of Technical Papers, IEEE, 2015, pp. 1–3.
[6] B. Karpinskyy, Y. Lee, Y. Choi, Y. Kim, M. Noh, S. Lee, 8.7 Physically unclonable function for secure key generation with a key error rate of 2E − 38 in 45 nm smartcard chips, 2016 IEEE International Solid-State Circuits Conference (ISSCC), IEEE, 2016, pp. 158–160.
[7] J. Guajardo, S.S. Kumar, G.-J. Schrijen, P. Tuyls, FPGA intrinsic PUFs and their use for IP protection, International Workshop on Cryptographic Hardware and Embedded Systems, Springer, 2007, pp. 63–80.
[8] B. Gassend, D. Clarke, M. Van Dijk, S. Devadas, Silicon physical random functions, Proceedings of the 9th ACM Conference on Computer and Communications Security, ACM, 2002, pp. 148–160.
[9] S. Khan, A.P. Shah, N. Gupta, S.S. Chouhan, J.G. Pandey, S.K. Vishvakarma, An ultra-low power, reconfigurable, aging resilient RO PUF for IoT applications, Microelectron. J. 92 (2019) 104605.
[10] S.S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, P. Tuyls, The butterfly PUF protecting IP on every FPGA, 2008 IEEE International Workshop on Hardware-Oriented Security and Trust, IEEE, 2008, pp. 67–70.
[11] R. Maes, P. Tuyls, I. Verbauwhede, Intrinsic PUFs from flip-flops on reconfigurable devices, 3rd Benelux Workshop on Information and System Security (WISSec 2008), vol. 17, 2008, p. 2008.
[12] U. Ko, P.T. Balsara, High-performance energy-efficient D-flip-flop circuits, IEEE Trans. Very Large Scale Integr. VLSI Syst. 8 (1) (2000) 94–98.
[13] L.P. Ching, O.G. Ling, Low-power and low-voltage Dlatch, Electron. Lett. 34 (7) (1998) 641–642.
[14] G. Gerosa, S. Gary, C. Dietz, D. Pham, K. Hoover, J. Alvarez, H. Sanchez, P. Ippolito, T. Ngo, S. Litch, et al., A 2.2 W, 80 MHz superscalar RISC microprocessor, IEEE J. Solid State Circuits 29 (12) (1994) 1440–1454.
[15] V. Van der Leest, G.-J. Schrijen, H. Handschuh, P. Tuyls, Hardware intrinsic security from D flip-flops, Proceedings of the Fifth ACM Workshop on Scalable Trusted Computing, ACM, 2010, pp. 53–62.
[16] D.E. Holcomb, W.P. Burleson, K. Fu, Power-up SRAM state as an identifying fingerprint and source of true random numbers, IEEE Trans. Comput. 58 (9) (2009) 1198–1210.
[17] F. Tehranipoor, N. Karimian, W. Yan, J.A. Chandy, DRAM-based intrinsic physically unclonable functions for system-level security and authentication, IEEE Trans. Very Large Scale Integr. VLSI Syst. 25 (3) (2017) 1085–1097.
[18] A. Maiti, P. Schaumont, Improved ring oscillator PUF: an FPGA-friendly secure primitive, J. Cryptol. 24 (2) (2011) 375–397.
[19] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, A statistical test suite for random and pseudorandom number generators for cryptographic applications, Tech. Rep. Booz-Allen and Hamilton Inc, Mclean, Va, 2001.