# An Innovative Architecture of DRAM PUF

Abhishek Kumar, Manoj Sindhwani, and Shippu Sachdeva

School of Electronics and Electrical Engineering, Lovely Professional University, India
e-mail: abkvjti@gmail.com

*Abstract*— **Cryptographic solutions based on traditional authentication methods are susceptible to several attacks on secret keys. Dynamic random access memory (DRAM)-based physical unclonable functions (PUF) are described as promising security building blocks to enable cryptography and authentication services. PUFs frequently suffer reliability concerns since they are sensitive to both internal and exterior noises. The need for enhanced resistance and dependability results in significant additional overheads. In this work, we proposed a DRAM-PUF based on the inclusion of selective hardware features in the computation. The proposed solution offers a higher number of challenge-response pairs (CRP) without additional circuitry. An innovative structure of PUF is presented in the paper which offers a reliable challenge-response pair module for authentication and authorization based on the ubiquitous nature of memory without the need for an additional circuit. DRAM PUF utilized the random startup value initialized by a capacitor followed by a random number generator. Our proposed PUF shows a reliability of 99.46% with temperature variation, a reliability of 99.5% with supply voltage variation, a uniqueness of 49.46%, a bit aliasing of 46.875%, and a uniformity of 47.65%.**

*Index Terms*— **PUF; Hardware Security; Threats; Sense Amplifier; DRAM.**

## I. Introduction

A hardware security module (HSM) is one of the best solutions for authentication and authorization purposes of cryptographic applications. A large number of HSM have been implemented based on PUF architecture [1]. Semiconductor-based PUF utilizes unique intrinsic features or circuit variation, which occurs naturally during manufacturing variation proposed by G.Suh and S. Devdas in [2][3]. The device's characteristics, which can be utilized to create inherent identifiers, are impacted by these fluctuations that cannot be prevented [4][5]. PUF serves as a mandatory component in the security protocol's authentication mechanism, generating challenge-response pairs (CRP)[6] [7]. The CRP is a critical element of device authentication, and the response is a non-linear function of the challenge and the specific features of the device or circuit [8][9]. Since responses of the PUF are derived from hardware intrinsic attributes it is almost impossible to construct a model. Post-processing of the PUF's response requires ad-ditional circuitry to be used for authentication or secret key generation. Two popular architectures of PUF are delay-based MuxPUF and frequency variation-based ROPUF presented by Gassendi and Blaise et al.[10] Implementation of MuxPUF is simple but the response generation rate is low whereas ROPUF architecture is complex. lectronic properties that are variable and remain stable can be used to create a PUF circuit [11]. Before creating a computational PUF circuit, a unique feature needs to be identified. The output of the circuit depends on the applied challenge input and the individual behavior of the circuit, which makes the PUF response unpredictable. The variable nature of the electronic signal attracts VLSI designers to present new architectures for PUFs. Identifying new intrinsic properties is another challenge for designers. Eiroa et al. [12] described different PUF structures such as Arbiter PUF, Ring oscillator PUF, Butterfly PUF, NOR-based PUF, and SRAM memory-based PUFs based on SRAM, latch, and flip-flop designs with the unique feature of remanence decay. Memory-based PUFs have got popularity compared to existing PUFs due to the minimum requirement of additional circuity for the computation[13][14][15][16]. Existing PUF architecture utilizes helper data algorithms and complex error correction codes (ECCs) for the responses, which requires significant hardware recourses. DRAM-based PUF offers large address spaces and multiple features to generate unique identifiers [17] exploiting the timing parameter of the DRAM to generate the device's signatures. Uniqueness and reliability are two important parame-ters to measure PUF quality, which proves CRP pairs are independent of noise and environmental conditions. Post-processing circuits like ECC are recommended for reliable responses however at the cost of circuit area overhead and extra storage. Random startup value of the DRAM cell features exploited in this work to present DRAM-PUF architecture. DRAM-based PUFs rely on the remanence property of non-volatile memory to store binary values for extended periods. Remanence measures how long the information can be retained despite the effects of decay, leakage, or environmental factors. The time for which the charge remains stored in the capacitor is used as a unique identifier for DRAM-based PUFs, which are composed of a capacitor and an access transistor in each cell. Capacitive memory (DRAM) needs to re-fresh the content after a definite period so that sufficient charge remains to maintain the binary value. Charging and discharging paths accessed by a capacitor by an NMOS transistor (1T-1C) cell act as a DRAM cell. Capacitance acts as a storage element and can store the potential half of the charging voltage accessed by the NMOS transistor[18]. The discharging nature of the capacitor is device-specific and depends on the resistance offers into the discharging path and time constant (RC). It stores charge constantly for retention time afterward starts leakages and looking the potential can measure by discharging current presented in equation (1).

$$t = \frac{C_s(V_{max} - V_{min})}{I_L} = \frac{C_s(V_{DD} - V_{th} - V_{new})}{I_L} \quad (1)$$

Where $V_{max}$ is the maximum voltage at which capacitor

Digital Object Identifier 10.29292/jics.v18i2.675

$C_s$ is charged and $V_{new}$ is the voltage after discharging of time t with discharging current $I_L$. Potential in the discharging path has been exploited as an intrinsic characteristic of the PUF and incorporated into the computation to generate the PUF's response. The startup value of the DRAM cell is unpredictable due to interfaced component precharge, and decoder while powered on. One side of the capacitor is charged to $V_{DD}/2$ thus at the startup $V_c = V_{DD}/2$. The process variation allows to have a permissible variation of Vc; when $V_c < V_{DD}/2$ sense amplifier produces logic 0 at the output. Similarly when $V_c > V_{DD}/2$ the sense amplifier de-tects and produces logic 1 at the output. The startup value of the DRAM cell is random and enables the DRAM cell as a promising candidate for PUF technology. DRAM is available on every computer system on board, and is cheaper than SRAM. Other investigations of the DRAM as PUF fo-cused on variable write cycles or variable refresh cycles. DRAM PUF based on the refresh cycle requires a variety of decay of bit, and the observation time of variation if decay makes impractical. Variation of the write cycle is one of the effective features but significant modification requires in the memory bus scheduler. The primary contribution of this work is the identification of the startup value of the DRAM cell. Additionally, explore the variation of a process that influences the DRAM PUF behavior. The structure of the paper has been organized as follows; section II briefs the transistor-capacitor cell and their retention time. Section III presented the structure of the PUF and their analysis of the generated response and their evaluation at a different corner given in section IV followed by the performance evaluation in section V and the conclusion in section VI.

## II. DRAM CELL

The existing PUF architecture suffers from the limita-tion of low CRP generation rate and complex architecture. Mux-PUF possesses simple architecture but has a limitation of a slow CRP generation rate while ROPUF can generate at a high rate but require complex architecture. The current research trend of PUF of identification of new electronic circuit properties to have new architecture and enhance the response generation rate with simple architecture. In this work, a novel architecture of PUF based on the discharging property of the capacitor is presented.

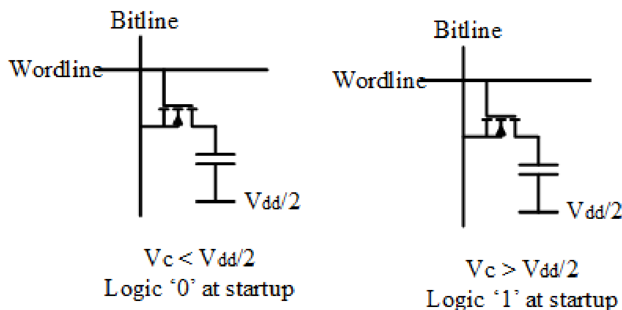


Fig. 1 Startup nature of DRAM cell [19]

A capacitor is an energy storage device that stores energy with the effect of an electrical field, capacitor access by NMOS (1T-1C cell) gets charged to a maximum of half of the applied potential and discharged to a lower value, the charging and discharging activity is controlled by the NMOS transistor. The discharging path offers the discharging resistance; the time constant (RC) measures 36.8% of stored charge leaked, and after 5-times constant the charge in the capacitor approximated to [20].

Capacitor discharging time has been used as an intrinsic feature of PUF. The discharging nature of the capacitor is unique the available charge in the capacitor is different and cannot be observed externally. A capacitor is a device that stores energy between two conductors separated by small distances. The charge stored is proportional to the applied voltage i.e Q=CV. The capacitor acts as the primary storage element in DRAM and requires less area to store a binary value compare to SRAM. A popular structure of DRAM (1T-1C) needs one transistor and one capacitor to store one bit of value. When a high bit '1' is stored, the capacitor should charge, and vice versa low bit '0' is presented as a discharged capacitor. The word line and bitline are arranged for turning NMOS ON and to store data onto the capacitor respectively, the word line must charge to $V_{DD}$ before a word line is activated bit line must recharge, and the capacitor in connection with the bit line; causes the flow of charge. If $V_C = V_{DD}$ charges with bit line voltage and vice versa discharges of $V_C \approxeq V_{DD}/2$. The time for which a capacitor can stores the charge is known as the retention time. Fig.1 presents the charging and discharging of a capacitor controlled by an NMOS transistor, voltage source $V_{PWL}$ generates logic-1 for 10 ns, enables the capacitor to get charged by $V_{DD}/2$, while the transistor is ON and the bit line is not charged the capacitor stored charge begins to discharge. The discharging time is not abrupt, charges leaked through the capacitor with each time constant step by step as a function of capacitance and discharging path resistance. After the retention time after which charges start to degrade, the capacitor does not leak charge abruptly. The discharging time is proportional to the available voltage and inversely proportional to the current value presented in equation (1).

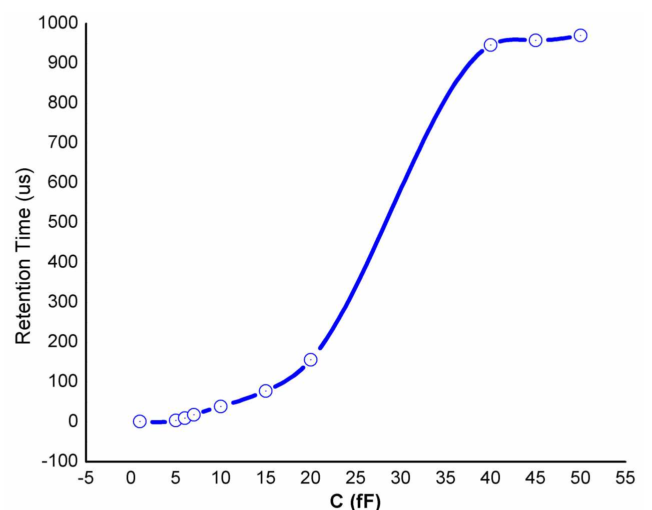


Fig. 2 Retention time vs capacitance

Retention time is the time for which capacitance-voltage remains stable, and increases with increasing value of capacitance. As shown in Fig.2; the 1 fF capacitor holds the

constant value until $1.24\mu s$ after it starts discharging, exponentially decaying. A higher capacitance value of 50 fF has a low decaying factor and presents the retention time $970\mu s$ following an almost linear decaying curve. A pulse width input ON the NMOS for 10 ns to charge the capacitor to DC voltage 1V. Parametric analysis of the cell with capacitance-voltage 1 fF to 50 fF presents, the rate of leakage decreases with the capacitance value present in Fig.3. Capacitance does not completely discharge, a fraction of the charge remains present as a residue charge, with a capacitance value. Residue voltage remains 0.4705 V at 1 fF and grows up to 0.7823V for 50 fF after 10 ns of discharging time interval. Thus higher residue voltage presents a longer retention time and holds the voltage for a longer duration.

## III. NOVEL ARCHITECTURE OF DRAM PUF

DRAM cells are grouped into memory arrays, each row in memory arrays made up of DRAM cells is coupled to a word line, allowing access to that row. A bitline, which is used to retrieve the value stored on a specific DRAM cell to which access has been enabled by the word line, is con-nected to all the cells in a single column. The bitlines are linked to sense amplifiers, which increase each bitline's voltage to a point where it may be understood as logically either zero or one. Capacitor PUF presented in Fig.4 consists of banks of transistor-capacitive cell, an array of 8 sense amplifiers controlled by a variable time delay generator. DRAM arrays are arranged as 2 dimensional where the row is connected to the word line and the column is connected to the bitline. Particular rows of array enable by the decoder allow charging the capacitor to the maximum value of $V_{DD}/2$. All the cells of this row can be read simultaneously however, the sense amplifiers function differently. To access the row's transistors to make contact and, as a result, allow access to the appropriate capacitors, the bit lines must first be charged to half of $V_{DD}$, followed by the charging of required word line. The charge travels from the bitline to capacitor. When a cell's capacitor is charged, making the bitline slightly more charged. In contrast, when the capacitor is not charged, charge flows from bitline to the capacitor, making the bitline slightly less charged. The difference between the charge on this bitline and the reference $V_{DD}/2$ charge stored on a different bitline is then amplified by a sensing amplifier. When reading the cells in a row, this results in the cell's value being recognized as a logical-1 or logical-0. DRAM cells are typically divided into two groups to simplify the differential amplification process: true cells, whose charged capacitor signifies a logical one value, and anticells, which store a logical-1 value when their capacitor is drained. The opposite condition of their capacitors for both types of cells denotes a logical-0 value. The startup charge of the capacitor of each cell may be slightly above or below the $V_{DD}/2$ threshold values, a situation that leads to the cell's value being interpreted as logical-1 or logical-0, respectively.

In this work an 8-row and 8 columns of the DRAM cell have been placed as an array; the 3:8 decoder selects a particular row and the 3:8 column decoder enables a particular sense amplifier. Address input requires a row and column decoder to act as challenge input to the PUF. The challenge input allows the charge capacitive array in a particular row and column bit line of each cell holds the charge in each cell. The column of the bit line selected from an individual capacitive bank acts as input to the sense amplifier, the difference between them is amplified when SE=1 and settles to response high or low. The capacitor holds the charge till retention time afterward it starts to leak discussed in section 2. Challenge input as the address of row and column decoder selects a particular DRAM cell for 4 ns, and the control unit activates the sense amplifiers at the interval of 0.5 ns after 2 ms. The initial time of 2 ns to acquire the startup value of DRAM cell capacitance. The current value of the capacitive voltage at the DRAM cell acts as a startup, which tends to decrease with time. The available charge of the capacitor is different at each moment. Sense amplifiers signal SE activated at a unique delay interval of 0.5 ns and responses are compared. Due to discharging nature of the capacitor the startup value of each cell BL and BLB compared to read the sensed response as an 8-bit random response. Sense amplifier senses the cell with a charge greater than the threshold stable otherwise flipped the value. The generated response is the function of startup value and discharging behavior of the capacitor provides the span to entropy. The 8-bit response generated by parallel sense amplifiers listed in table1 presents the startup value of the capacitance value of the cell selected by row and column decoder which act as BL and BLB input to the sense amplifier, compares the value, and generates a response of either high or low as a function of startup value of cell capacitor. The internal component of the presented PUF is the sense amplifier and variable delay generator presented in Fig.4.

### A. *Sense Amplifier*

Sense amplifier presented in Fig.5[21] acts as a read circuitry of memory read operation implement differential current mirror amplifier. It sensed the difference between voltage levels at two parallel bit lines and generates a recognizable logic level of 'High' or 'Low'. Consists of two NMOS (M1 & M2) to accept the external input and a long $3^{rd}$ NMOS (M3) acts as a current source controlled by a square pulse (sense enable). Initially SE=0 OFF the M3, bitline makes M1 & M2 conducts and pull up through PMOS (P1 & P2). When SE=1 drives the M3, if input coming from the bitline forces the bitline C to decrease slightly, transistor M1 gets off, and the output voltage drops immediately. The inverter produces a high output. If input coming from the bit line forces the bit line $\neg C$ to drop slightly, M2 gets off, produces a high terminal, and the inverter yields a logic-low output level. The minimum voltage difference that can be sensed is 0.6 mV.

Table I. Generated Response at Sense amplifier's output

| Cell | BL(V) | BLB(V) | SE Trigger | Output |
|---|---|---|---|---|
| 0 | 0.399 | 0.408 | 2 | High |
| 1 | 0.044 | 0.238 | 2.5 | High |
| 2 | 0.421 | 0.264 | 1.5 | Low |
| 3 | 0.49091 | 0.49151 | 0.5 | High |
| 4 | 0.45 | 0.405 | 1 | Low |
| 5 | 0.309 | 0.267 | 4 | Low |
| 6 | 0.322 | 0.297 | 3 | Low |
| 7 | 0.288 | 0.331 | 305 | High |

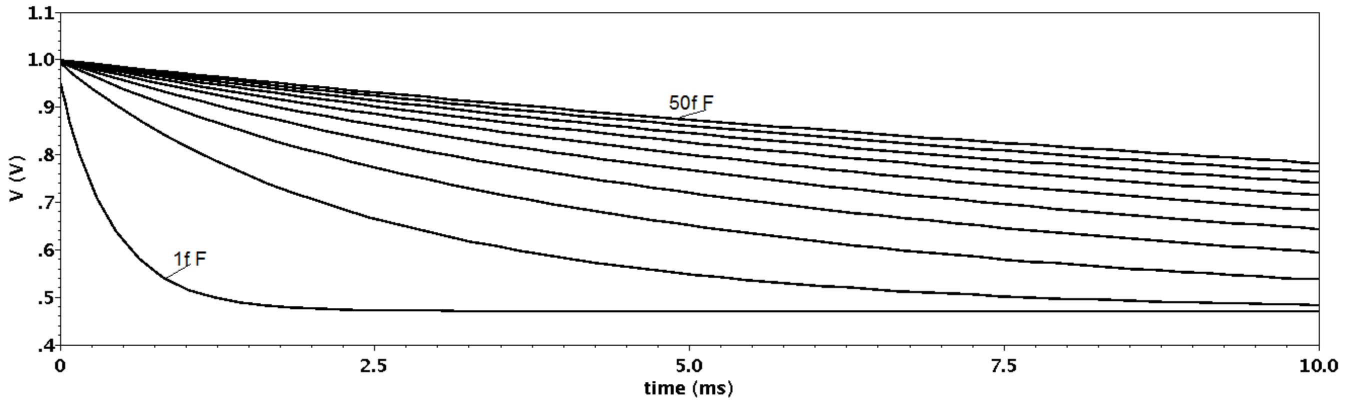


Fig. 3 Parametric analysis of the discharging path

Fig. 4 DRAM PUF Architecture

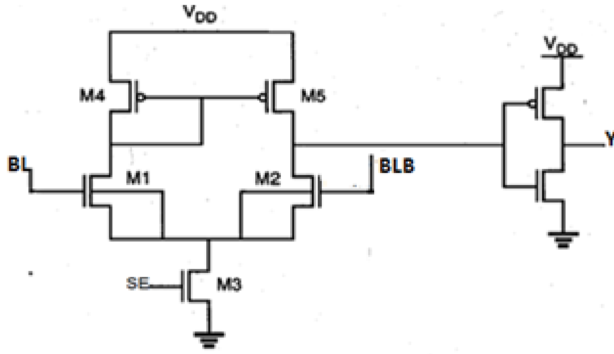


Fig. 5 Schematic of the Sense amplifier

### B. Control Unit

The flowchart in Fig.6 presents the function of control module of the PUF that generates the necessary control signal namely PE, SE, and clock. PE=0 enables the precharge operation within the first 2 ns and then goes to 1 (since the precharge block comprises PMOS). Afterward, enable the sense amplifier with variable delay in the range of (2 ns to 4 ns in the interval of 0.5 ns), triggers one of the sense amplifiers in active mode. Lastly clock signal enables the linear feedback shift register to generate the random response with seed value provided by the sense amplifier. The simulation waveform in present Fig.7 presents the startup value of the cell at the sense amplifier output when 8 columns have been read in a row.

### C. Random Response Generator

A random number represents a set of numbers with absolutely no relationship to one another anywhere in the sequence. All integers have an equal chance of happening at any given time and are unpredictable. A random number generator is a digital circuit that generates a sequence of random numbers. A pseudorandom number generator (PRNG) is based on a deterministic algorithm able to generate random sequences. PRNG has an internal state to be kept secret known as seed. produces deterministic output that, to individuals who don't know and can't guess the internal state, is identical to random numbers. The algorithm and its seeds are what determine the PRNG's overall security, hence the seed should be confidential and random. The startup value of the DRAM cell is unpredictable and acts as a seed for the RNG. LFSR is the most popular type of PRNG, which is made up of cyclic binary states, is calculated from its prior state, and requires D type flip flop and XOR gate. A different state of "n" bits is produced by the LFSR with each iteration, which starts with a seed value. The rightmost bit is the output, and the inner state is shifted to the right. Taps are the bit positions that determine the following state.

$$P(x) = x^7 + x^5 + x^3 + x^1 + x^0 \quad (2)$$

Linear feedback is the process of successively XORing the taps with the output bit to replace the leftmost bit presented as a polynomial equation(2). A sequence of random bits can be produced by an LFSR with carefully chosen taps.

## IV. DRAM STARTUP VALUE AT DIFFERENT CORNER

Inherent properties of hardware are taken advantage of by hardware-based security primitives to extract entropy in the form of random and distinct outputs that can be used to create cryptographic solutions. Due to manufacturing variation and temperature discharging a capacitor of DRAM cell varies, in some cells charge leaks faster, and in other cells slower. The irregularities in design are the cause of process variation. Due to PVT variation, a random shift in characteristics of VLSI parameters was seen. The impact of PVT variation on the startup value of the dram cell is examined at ITRS standardization supply voltage variation of $1V \pm 10\%$ and temperature up to 80°C. With changes in process, voltage, and temperature, transistor production can become either fast or slow, which has an impact on the entire circuit. We cannot specify to select a transistor to locate on a specific corner during fabrication. The designer's job is to thoroughly check every aspect of the design to ensure its dependability. The design at most end of parameter variation is validated using corner analysis and describes the design's best and worst corners as TT, FF, FS, SF, and SS corners, where the first characterizes NMOS and the second characterizes PMOS. Since the delay of the MOS transistor varies at different corners the arrival time of input to the sense amplifier varies leading to different responses. The waveform in Fig.8 presents the generated response at a different corner.

The response is almost the same at TT, FF, and FS corners while the difference arises at SF and SS corners. The fast NMOS into the design is dominant and leads the response to high. Practically, the delay and leakage power of the fast NMOS circuit decreases with temperature, but they increase with supply voltage. Similarly, leakage power tends to rise while slow PMOS delay tends to decrease [22][23][24]. The waveform in Fig.8 presents the different startup values of DRAM cells at different corners. The faster cell pulls the BL value faster and produces sensed value high. Fast NMOS and slower PMOS at TT, FF, and FS corners produce upper nibble high, and lower nibble settles too low response. Similarly slow NMOS and fast PMOS at SF and SS corners produce upper nibble '0111' and lower nibble '1110' or '1111' respectively. The response generation rate for TT, FF, and FS corners is much higher than for SF and SS corners.

## V. RESULT AND DISCUSSION

PUF circuits are expected to produce unique response bits for the same input challenge, with a constant response despite changes in operating conditions, and a uniform distribution of bits. The performance of PUF circuits is evaluated based on the inter and intra variation of response bits. The author has proposed several parameters in [11] to measure the quality of PUF circuits in terms of randomness, correctness, steadiness, diffusionism, and uniqueness[25][26][27] measure qualities such as uniformity, uniqueness, bit aliasing, and reliability. The evaluation of PUF functions is typically based on standard parameters, as outlined in[8], which include uniformity, uniqueness, and reliability. It is important to determine whether the PUF outputs are both unique (for security purposes) and reproducible (for ensuring reliability).

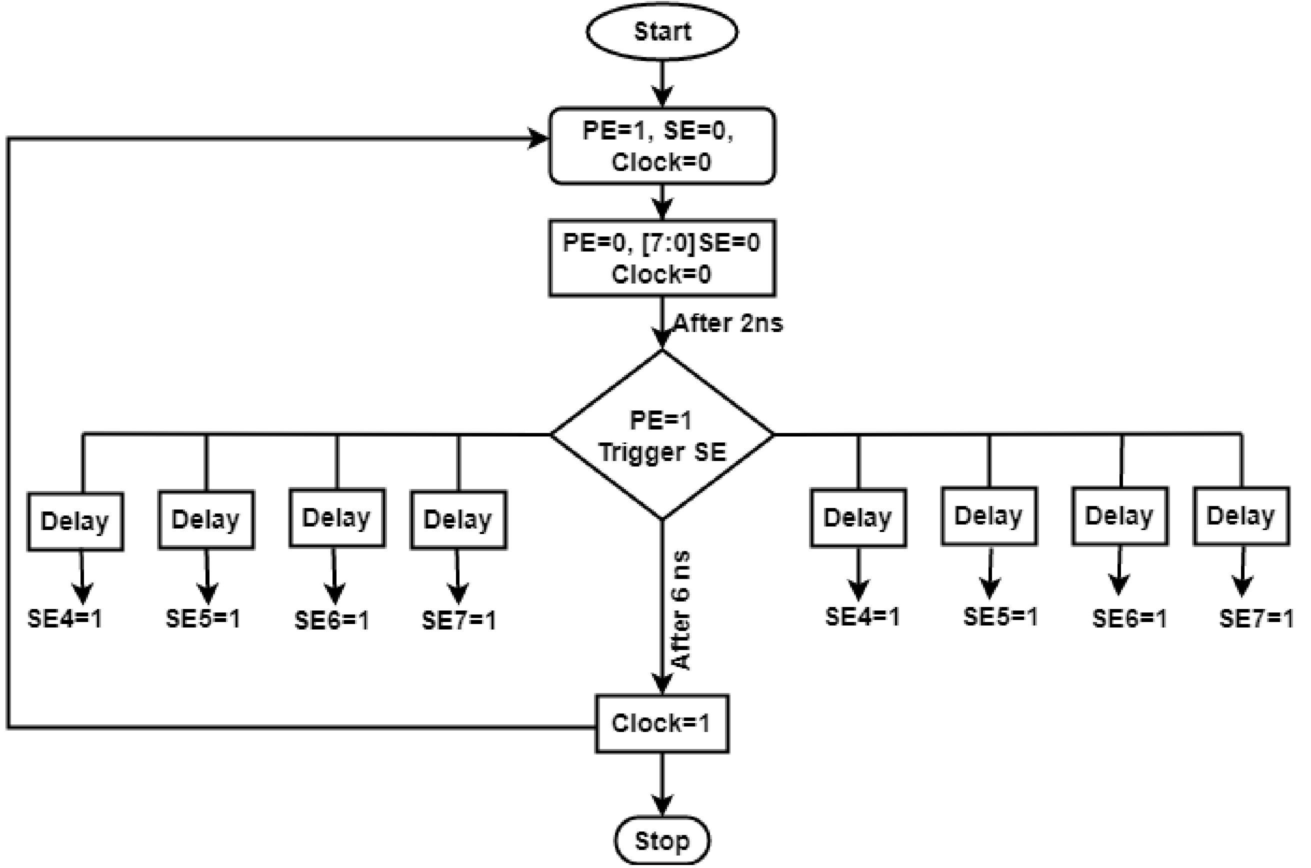


Fig. 6 Flowchart of the control module

Fig. 7 Startup value of DRAM cell sense by the sense amplifier

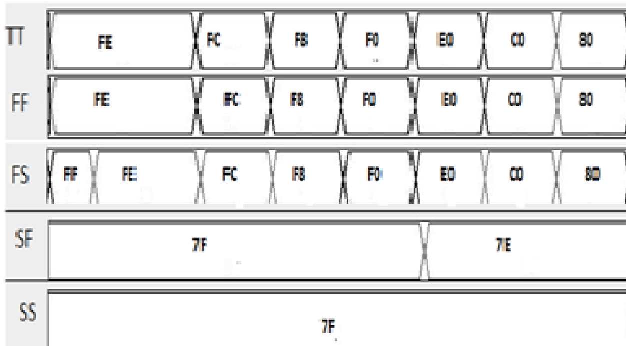


Fig. 8 Startup value at different corner

These metrics are important for assessing the security and reliability of PUF outputs. A high inter-chip variation indicates that PUF outputs are unique and cannot be easily predicted or duplicated, which is desirable for security applications. A low intra-chip variation indicates that PUF outputs are reproducible and consistent, which is important for reliable authentication and key generation.

### A. Inter Variation

In DRAM PUF, it is expected that different DRAM cells will produce different responses for the same input challenge. Inter variation is used to estimate the number of bit differences between the responses of two DRAM cells for the same input challenge. The Hamming distance is a measure of the number of bit changes in the response, ideally around 50% [21]. To calculate the typical inter PUF variation for n-number of bits per response from k number of devices, equation(3) is used.

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

Where $HD(R_i, R_j)$ is the Hamming distance(HD) between any two responses of $R_i$ and $R_j$ obtained from the different cells for the same challenge input.

### B. Intra Variation

Intra variation is used to measure the separation of response bits within responses originating from the same DRAM cell when a one-bit change occurs at the input. Ideally, 50% of the bits should change whenever a one-bit flip occurs at the input terminal, calculated using Hamming distance. Intra variation provides an estimate of the stability of the response bits, which must remain stable. To measure intra Hamming distance for n number of bits per response obtained from k number of devices, equation(4) is used.

$$InttaHD = \frac{1}{k} \sum_{i=1}^{k} \frac{HD(R_i, R_j)}{n} \times 100\% \tag{4}$$

Where $HD(R_i, R_j)$ is the hamming distance between $1^{st}$ and $2^{nd}$ samples of response at a different time obtain from the same cell.

### C. Uniformity

Uniformity of a DRAM PUF refers to how uniformly the proportion of '1's and '0's are distributed in the response bits of the PUF. A PUF with a bias towards '1' or '0' in its responses can be easily guessed by an attacker. Therefore, a PUF should have a uniform distribution of '1's and '0's in its responses to enhance security. The expected number of '1's and '0's bit is 50% of the total response bit. Uniformity is computed using equation(5) producing an n-bit response for a challenge input.

$$Uniformity = \frac{1}{n}\sum_{j=1}^{n} R_{i,j} \times 100\% \quad (5)$$

where $R_{i,j} = 1$, if the $j^{th}$ bit from the chip 'i' else '0' and n is the number of bits in response. The percentage of '1' and '0' at startup measures uniformity. Without any write operation, the DRAM cell has a startup value from a cell that is not perfectly uniform

### D. Uniqueness

Uniqueness measures the ability of DRAM PUF to generate new or unique responses for a challenge that applies to different DRAM cells. Different cells must produce different responses for the same input. Uniqueness is calculated as inter-Hamming distance [26], which is evaluated by comparing the Hamming distance of unique responses generated by different cells, as presented in equation(6). Ideally, 50% of the response bits between two PUFs should differ. Lower uniqueness indicates biasness towards '0', while higher biasness indicates biasness towards '1'.

$$InterHD = \frac{2}{k(k-1)}\sum_{i=1}^{k-1}\sum_{j=i+1}^{k}\frac{HD(R_i, R_j)}{n} \times 100\% \quad (6)$$

Where $R_i$ and $R_j$ are the n-bit responses of two chips i and j to the same input challenge and the k number of the chip. Since the startup value of the DRAM cell is different seed unique value of the LFSR circuit result in a higher unique CRP generator.

### E. Reliability

Reliability is a metric that measures how many DRAM PUF output bits change when re-generated with or without environmental changes[28]. It indicates the reproducibility of the DRAM PUF outputs. Ideally, the intra-chip variation should be 0%. If a challenge is repeated, the response generated by a DRAM PUF should remain consistent. For instance, if chip 'i' produces the response $R_{T1}$ and $R_{T2}$ for the same challenge at two different instants of time both responses should be identical. Equation(7) quantified the reliability of DRAM PUF.

$$Reliability = 100 - \frac{1}{m}\sum_{t=T_2}^{T_m}\frac{R_{T1}}{n} \times 100\% \quad (7)$$

Reliability of PUF evaluated with temperature variation ranges 20°C to 80°C and supply variation $1V \pm 10\%$. The response of PUF depends on the retention time and latency of the DRAM cell. At higher temperature retention exceed the latency and produces more stable responses. Reliability increases with higher supply voltage and reduces as supply voltage lowers.

### F. Bit Aliasing

Bit aliasing is an estimate of the biasness of response bits due to static hazards. Some of the bits in response are stuck to '0' if biased to zero or ground or stuck to '1' if biased to one or power supply. When the DRAM PUF response is repeated for the same challenge among different cells, it gives a piece of exclusive side information to the attacker to predict the response. When bit aliasing occurs, distinct chips generate comparable responses, making it easier for an attacker to predict the response. Bit aliasing can be determined as the proportion of similarity for the $i^{th}$ bit of a DRAM PUF among K different chips, given in equation(8).

$$BitAliasing = \frac{1}{k}\sum_{j=1}^{k} R_{i,j} \times 100\% \quad (8)$$

Where $R_{i,j} = 1$, if the $i^{th}$ bit from the chip 'j' for the challenge C else 0.

Table II. Comparison of PUF's Parameter

| Parameter | DRAM PUF | [29] | [15] | [18] | [30] |
|---|---|---|---|---|---|
| Uniformity(%) | 47.65 | 48 | 43.5 | 48 | 47.28 |
| Bit Aliasing(%) | 46.875 | - | - | - | 47.48 |
| Uniqueness(%) | 49.46 | 45.8 | 41.4 | 49.37 | 49.85 |
| *Reliability(%) | 99.46 | 99.23 | 78.8 | 81.4 | 98.67 |
| **Reliability(%) | 99.5 | 96.85 | 55.4 | - | - |

*Temperature variation (20 – 80°C)
**Supply voltage variation ($1V \pm 10\%$)

Table II presents the comparison of performance metrics for the presented DRAM PUF with other DRAM PUF architecture. The proposed DRAM PUF is very reliable and robust against temperature and supply voltage variation effects. Uniformity achieves 47.65% because the startup value generated with inherent features without writing is not much stable. Bit aliasing value 46.875% signifies response bits are biased towards bit '1' due to the retention time of the capacitor. As a result, DRAM PUF can be used for system authentication and anti-counterfeiting applications with high confidence that PUF reliability will be maintained over time.

## VI. CONCLUSION

In this work, the innovative architecture of PUF has been presented based on the startup value of the DRAM cell. PUF as CRP pairs generates unique responses using circuit inherent characteristics. Existing DRAM-PUF with startup value added feature of discharging nature of the capacitor has been induced to compute responses. Corner analysis validates CRP rate at TT, FF, and FS corners are higher than SS and SF corners. The obtained challenge-response pair is 49.46% unique and reliable 99.46% with temperature variation and 99.5% with supply voltage variation. The presented PUF response bit is a function of the challenge input and discharging feature of the capacitor stand for application for authentication and random number generation.

## VII. Author Contribution

In this work, the authors have presented an innovative architecture based on the startup value. Retention time of the capacitive cell holds the charge for a unique time producing a unique startup value of the DRAM cell. Process corner analysis shows the response generation rate is higher for fast NMOS in FF and FS corners. It is the first time in the literature the startup value of the DRAM cell is presented. An LFSR at the output terminal result in an efficient unique and reliable CRP generator.

## VIII. Acknowledgment

The authors would like to acknowledge VLSI Design lab of Lovely Professional University for providing necessary simulation tool.

## References

[1] A. Babaei and G. Schiele, "Physical unclonable functions in the internet of things: State of the art and open challenges," *Sensors*, vol. 19, no. 14, p. 3208, 2019.

[2] S. Katzenbeisser, Ü. Kocabaş, V. Rožić, A.-R. Sadeghi, I. Verbauwhede, and C. Wachsmann, "Pufs: Myth, fact or busted? a security evaluation of physically unclonable functions (pufs) cast in silicon," in *Cryptographic Hardware and Embedded Systems–CHES 2012: 14th International Workshop, Leuven, Belgium, September 9-12, 2012. Proceedings 14*. Springer, 2012, pp. 283–301.

[3] G. E. Suh and S. Devadas, "Physical unclonable functions for device authentication and secret key generation," in *Proceedings of the 44th annual design automation conference*, 2007, pp. 9–14.

[4] S. S. Avvaru, Z. Zeng, and K. K. Parhi, "Homogeneous and heterogeneous feed-forward xor physical unclonable functions," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2485–2498, 2020.

[5] Z. Zhou, P. Wang, and Z. Li, "A quadratic residue-based rfid authentication protocol with enhanced security for tmis," *Journal of ambient intelligence and humanized computing*, vol. 10, pp. 3603–3615, 2019.

[6] A. Kumar, R. S. Mishra, and K. Kashwan, "Challenge-response generation using ro-puf with reduced hardware," in *2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*. IEEE, 2016, pp. 1305–1308.

[7] I. Kim, A. Maiti, L. Nazhandali, P. Schaumont, V. Vivekraja, and H. Zhang, "From statistics to circuits: Foundations for future physical unclonable functions," *Towards Hardware-Intrinsic Security: Foundations and Practice*, pp. 55–78, 2010.

[8] A. Kumar, S. L. Tripathi, and R. S. Mishra, "Metapuf: A challenge response pair generator," *Periodicals of Engineering and Natural Sciences*, vol. 6, no. 2, pp. 58–63, 2018.

[9] Y. Cao, W. Liu, L. Qin, B. Liu, S. Chen, J. Ye, X. Xia, and C. Wang, "Entropy sources based on silicon chips: True random number generator and physical unclonable function," *Entropy*, vol. 24, no. 11, p. 1566, 2022.

[10] B. Gassend, D. Clarke, M. Van Dijk, and S. Devadas, "Silicon physical random functions," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 148–160.

[11] Y. Cao, L. Zhang, C.-H. Chang, and S. Chen, "A low-power hybrid ro puf with improved thermal stability for lightweight applications," *IEEE Transactions on computer-aided design of integrated circuits and systems*, vol. 34, no. 7, pp. 1143–1147, 2015.

[12] S. Eiroa, M. I. Baturone Castillo, A. J. Acosta Jiménez, and J. Dávila, "Using physical unclonable functions for hardware authentication: A survey," in *Proceedings XXV Conference on Design of Circuits and Integrated Systems*, 2010.

[13] R. P. Challa, S. A. Islam, and S. Katkoori, "An sr flip-flop based physical unclonable functions for hardware security," in *2019 IEEE 62nd International Midwest Symposium on Circuits and Systems (MWSCAS)*. IEEE, 2019, pp. 574–577.

[14] J. S. Kim, M. Patel, H. Hassan, and O. Mutlu, "The dram latency puf: Quickly evaluating physical unclonable functions by exploiting the latency-reliability tradeoff in modern commodity dram devices," in *2018 IEEE International Symposium on High Performance Computer Architecture (HPCA)*. IEEE, 2018, pp. 194–207.

[15] F. Tehranipoor, N. Karimian, K. Xiao, and J. Chandy, "Dram based intrinsic physical unclonable functions for system level security," in *Proceedings of the 25th edition on Great Lakes Symposium on VLSI*, 2015, pp. 15–20.

[16] M. Tehranipoor, N. Pundir, N. Vashistha, and F. Farahmandi, "Intrinsic racetrack puf," in *Hardware Security Primitives*. Springer, 2022, pp. 1–16.

[17] B. B. Talukder, B. Ray, D. Forte, and M. T. Rahman, "Prelatpuf: Exploiting dram latency variations for generating robust device signatures," *IEEE Access*, vol. 7, pp. 81 106–81 120, 2019.

[18] F. Tehranipoor, N. Karimian, W. Yan, and J. A. Chandy, "Dram-based intrinsic physically unclonable functions for system-level security and authentication," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 3, pp. 1085–1097, 2016.

[19] S. Chen, B. Li, and Y. Cao, "Intrinsic physical unclonable function (puf) sensors in commodity devices," *Sensors*, vol. 19, no. 11, p. 2428, 2019.

[20] S. M. Kang and Y. Leblebici, *CMOS digital integrated circuits*. MacGraw-Hill, 2003.

[21] M. Bhargava and K. Mai, "An efficient reliable puf-based cryptographic key generator in 65nm cmos," in *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2014, pp. 1–6.

[22] A. Kumar, S. L. Tripathi, and U. Subramaniam, "Variability analysis of sbox with cmos 45 nm technology," *Wireless Personal Communications*, pp. 1–12, 2022.

[23] A. Kumar and S. L. Tripathi, "Sbox under pvt variation," *Analog Integrated Circuits and Signal Processing*, vol. 105, no. 1, pp. 73–82, 2020.

[24] K. A. Kumar and R. Nelakuditi, "An impact of aging on arbiter physical unclonable functions," in *VLSI Architecture for Signal, Speech, and Image Processing*. Apple Academic Press, 2022, pp. 101–122.

[25] A. Maiti, R. Nagesh, A. Reddy, and P. Schaumont, "Physical unclonable function and true random number generator: a compact and scalable implementation," in *Proceedings of the 19th ACM Great Lakes symposium on VLSI*, 2009, pp. 425–428.

[26] K. Yelamarthi, "Timing-driven variation-aware partitioning and optimization of mixed static-dynamic cmos circuits," vol. 4, no. 2, pp. 73–82, 2013.

[27] S. Sutar, A. Raha, and V. Raghunathan, "D-puf: An intrinsically reconfigurable dram puf for device authentication in embedded systems," in *Proceedings of the International Conference on Compilers, Architectures and Synthesis for Embedded Systems*, 2016, pp. 1–10.

[28] M. S. Hashemian, B. Singh, F. Wolff, D. Weyer, S. Clay, and C. Papachristou, "A robust authentication methodology using physically unclonable functions in dram arrays," in *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*. IEEE, 2015, pp. 647–652.

[29] Z. Huang, L. Li, Y. Chen, Z. Li, Q. Wang, and X. Jiang, "Rppuf: An ultra-lightweight reconfigurable pico-physically unclonable function for resource-constrained iot devices," *Electronics*, vol. 10, no. 23, p. 3039, 2021.

[30] J. Kim, T. Ahmed, H. Nili, J. Yang, D. S. Jeong, P. Beckett, S. Sriram, D. C. Ranasinghe, and O. Kavehei, "A physical unclonable function with redox-based nanoionic resistive memory," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 2, pp. 437–448, 2017.