Design of Adiabatic Logic Based Energy-Efficient and Reliable PUF for IoT devices

S DINESH KUMAR AND HIMANSHU THAPLIYAL, University of Kentucky, USA

Internet of Things (IoT) devices have stringent constraints on power and energy consumption. Adiabatic logic has been proposed as a novel computing platform to design energy-efficient IoT devices. Physically Unclonable Functions (PUFs) is a promising paradigm to solve security concerns such as IC piracy, IC counterfeiting, etc. PUFs have shown great promise for generating the secret bits that can be used in the secure systems in an inexpensive way. However, designing a reliable PUF along with energy-efficiency is a big challenge. Therefore, for energy-efficient and reliable PUF, we are proposing a novel energy-efficient adiabatic logic based PUF structure. The proposed adiabatic PUF uses energy recovery concept to achieve high energy efficiency and uses the time ramp voltage to exhibit the reliable start-up behavior. The channel length of the transistors play a major role in controlling manufacturing variations. So, in this paper, the circuit simulations are performed with 180nm and 45nm CMOS technology in Cadence Spectre simulator to analyze the impact of channel length variations. The proposed adiabatic PUF has worst-case reliability of 96.84% and 99.6% with temperature variations at 180nm and 45nm CMOS technology respectively. Further, the proposed adiabatic PUF consumes 1.071fJ/bit-per cycle at 180nm CMOS technology and 0.08fJ/bit-per cycle at 45nm CMOS technology.

CCS Concepts: • **Security and privacy → Embedded systems security**; • **Hardware → Emerging architectures**.

Additional Key Words and Phrases: Hardware Security, IoT Devices, Physically Unclonable Functions (PUFs), Adiabatic Computing

1 INTRODUCTION

The Internet of Things (IoT) is the network of physical objects including devices, vehicles, home appliances and other items which are embedded with electronics, software, sensors, and actuators that are connected through the Internet to exchange data for intelligent applications [2], [17]. IoT-based consumer electronics are playing a key role in boosting the global economy by improving the quality of life, creating new markets, creating new products, and creating new research paradigms. Further, smart environments such as smart cities, smart homes, smart transport systems, and smart grids are deeply impacted by the research progress on IoT devices and systems. Though IoT based smart environment have several advantages, they also equally present challenges related to security and privacy.

Author's address: S Dinesh Kumar and Himanshu Thapliyal, University of Kentucky, Department of Electrical and Computer Engineering, Lexington, KY, 40506, USA, hthapliyal@uky.edu.

1550-4832/2010/3-ART39 $15.00

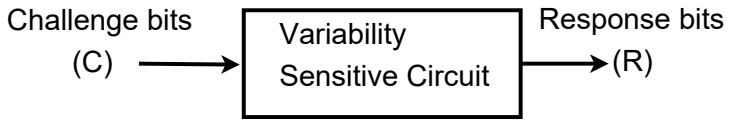

Fig. 1. PUF production using inherent variations

Physically Unclonable Functions (PUFs) are a class of circuits that use the inherent variations in an Integrated Circuit (IC) manufacturing process to create unique and unclonable Identity bits (IDs). PUFs have emerged as a powerful solution to a variety of security concerns such as IC piracy, IC counterfeiting, etc.[27]. PUFs play a major role in secure authentication and key management in cyber-physical security and IoT devices [20]. A PUF is provided with challenge bits (C) and due to the intrinsic variations in the IC manufacturing process, it results in unpredictable outputs called response bits (R). The uncontrollable IC manufacturing errors make the PUF response to be unique and unclonable. Fig. 1 shows the block diagram for PUF production using inherent variations. Hence, a PUF can be considered as a fingerprint for Integrated Circuits.

One of the main application of PUF is to generate the secret key for cryptographic applications and to reliably store them without the need of non-volatile memory [25],[9]. However, the PUF circuit characteristics vary with the environmental variations such as supply voltage variations, temperature etc. The environmental variations affect the repeatability of the responses which is referred as reliability in PUF context. Reliability of PUFs is one of the key concern in the design of PUFs, as the responses of PUFs are used for key generation in cryptographic applications.

Along with the security, another important aspect of IoT devices are the energy consumption. IoT devices are usually small and have limited power density. In the recent years, energy harvesting based techniques has been used to power up the IoT devices. Wireless/RF based power harvesting techniques have received attention in recent years due to the enormous amount of RF energy around the world. Adiabatic logic based circuits has found excellent application in the design of wireless energy harvesting circuits [34], [23]. Crypto circuits can be implemented in using existing adiabatic logic circuits [13]. However, there is no key generation method utilizing adiabatic principles has been investigated so far. This paper investigates the design of PUF which can be implemented in adiabatic logic processors, wireless energy harvesting systems employing adiabatic circuits, IoT devices, etc.

1.1 Motivation of the paper

PUFs are a class of circuits which can be used to generate secret keys for cryptographic applications. However, PUF circuit characteristics vary with environmental variations which affects the reliability of the PUF circuit. Fuzzy extractor based Error Correcting Code (ECC) have been used to correct the noisy PUF responses. Unfortunately, ECC are computationally intensive and consume high power and area which makes them not suitable to implement in IoT devices [8]. The main motivation of this work is to design an energy-efficient and reliable PUF using the principle of adiabatic computing which can generate reliable key for the cryptographic application in IoT devices. Implementation of the proposed adiabatic PUF in small battery operated IoT device can prolong the battery life of the device along with the secure key generation.

In the recent years, Further, the proposed design of PUF can also be applicable wireless power harvesting systems which is built based on adiabatic logic circuits.

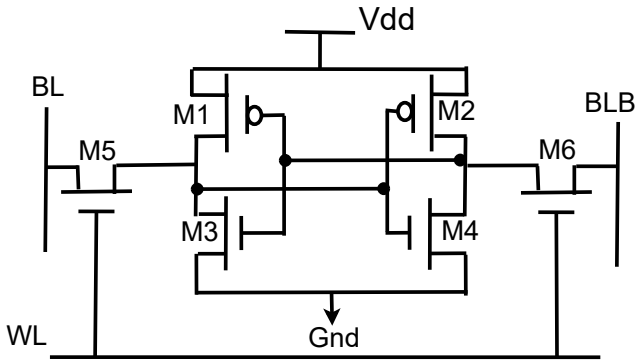

Fig. 2. SRAM PUF cell

1.2 Contribution of the paper

Adiabatic logic is one of the circuit design technique to design energy-efficient hardware. Time ramp voltages are used in adiabatic logic technique to recover the energy from each node of the circuit. In this work, we propose a novel adiabatic logic based PUF that utilizes the unique property of adiabatic computing of having time ramp voltages to improve the energy efficiency as well as the reliability. The preliminary version of the paper can be found in [12]. Reliability test is performed by varying the following parameters:

- By varying the temperature from $-40°C$ to $80°C$.
- By varying the supply voltages by $\pm 20\% V_{dd}$.

Further, we have investigated the security properties of the proposed adiabatic logic based PUF in metrics of uniqueness and uniformity. The body of the PMOS transistors in the proposed adiabatic PUF can be connected to either Vdd (constant voltage) or Vpc (power clock). Therefore, we have also analyzed the impact of body bias effect on the reliability, uniqueness, uniformity and energy-efficiency of the proposed adiabatic PUF cell. The results of the proposed adiabatic PUF are compared with the state-of-art PUFs. All the simulations are performed in Cadence Spectre simulator in 180nm and 45nm CMOS technology nodes evaluate the impact of change in technology nodes in the proposed adiabatic PUF characteristics.

1.3 Organization of the paper

Section II describes the background of the existing SRAM PUF, adiabatic logic principles and existing adiabatic SRAM memory that would form the foundation of the proposed adiabatic PUF. Section III describes the operation of the proposed adiabatic logic based PUF. Section IV presents PUF evaluation metrics. Section V presents the simulation results of the proposed adiabatic PUF. Section VI presents the simulation and the analysis of the proposed adiabatic PUF. Further, Section VI also presents the comparison of the security metrics of the proposed adiabatic PUF along with state-of-art PUFs. Section VII concludes the paper.

2 BACKGROUND

The background on SRAM PUF and the adiabatic logic technique are described in this section.

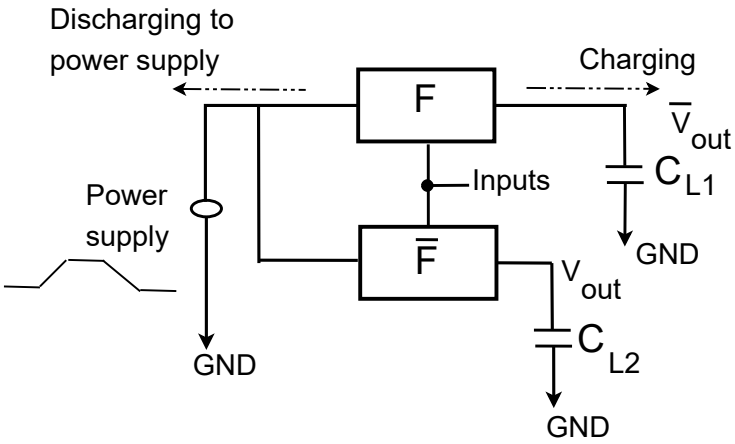

Fig. 3. Adiabatic charging/discharging

2.1 SRAM PUF

Fig. 2 shows the schematic of the 6T SRAM PUF cell [10]. The 6T SRAM cell consists of a bistable circuit which has two cross coupled inverters (M1, M2, M3 and M4). When the SRAM cell is powered, current will be start flowing through M1 and M2. Due to the intrinsic variation in the transistors, the threshold voltage of one PMOS will be higher than the other. So, more current will start flowing through the PMOS with lower resistance and hence one output will be biased towards logic "1" while the other output will be at logic "0". Since both the inverters are designed to be identical in strength, the output response will be determined by the intrinsic process variations.

Though SRAM PUF has several advantages such as low-power, high density etc., the reliability is one of the major concerns in the design of SRAM PUF in particular for key generation application. Cortez et. al [6] has reported that intelligent choosing of time ramp up at a particular temperature can improve the reliability of SRAM PUF cells. However, this technique requires additional circuitry to perform the intelligent time ramp up operation to improve the reliability of SRAM PUF cell. Similarly, Vijayakumar et. al [33] has proposed a majority voting technique to improve the reliability of the SRAM PUF. However, this technique requires multiple turning on and turning off of the SRAM cell.

2.2 Adiabatic Logic technique

Adiabatic logic uses time ramp voltages (power clocks) to efficiently recycle the charge stored in the load capacitor of the output nodes [31]. Adiabatic logic has reduced dynamic switching energy loss due to the recycling of charge to the power clock. Fig. 3 shows the adiabatic charging/discharging of the load capacitors. The energy dissipated in an adiabatic circuit when considering the charge is supplied through a constant current source is shown by [31],

$$E_{diss} = \frac{RC}{T} C V_{dd}^2 \tag{1}$$

where T is the charging/discharging time of the capacitor, C is the load capacitor, V_{dd} is the full swing of the power clock. If T $\gg$ 2RC (time constant), then the energy dissipated by the adiabatic circuit is less than the conventional CMOS circuit. The details of power clock generators for adiabatic circuits can be found in [1].

One of the main limitation of the adiabatic logic is that these circuits can operate energy-efficiently at frequency less than 1GHz. Further, the usage of the multi-phase clocking increases the overhead of adiabatic logic based circuits. However, adiabatic logic based circuits finds its application in wireless energy harvesting based circuits which has reduced area and improved energy efficiency as compared to the conventional CMOS circuits.

2.3 Adiabatic SRAM memory

Various research has been performed on developing low-power SRAM memories using the adiabatic logic circuits. This section will briefly discusses the existing adiabatic SRAM memories. For example, Nakata et al. has proposed a adiabatic SRAM which enables gradual charging during the writing mode which reduces the problem of electro migration [21] . In this design, authors have not used any multi-phase clock for the energy savings. Rather, the charges are moved gradually to attain the energy savings. Takahashi et. al has proposed adiabatic 9T SRAM cell [28]. This adiabatic 9T SRAM cell uses two trapezoidal waveforms for adiabatic operation and reduces the short circuit current. From the spice simulation, authors have showed that the adiabatic 9T SRAM cell has lower energy consumption than the conventional 6T SRAM cell. Kumar et. al has proposed adiabatic SRAM based on split level charge recover logic [11]. However, this adiabatic SRAM cell requires 8 phase power clock in order to recover the charge which increases the overall area of the implementation.

3 PROPOSED ADIABATIC LOGIC BASED PUF

Time ramp voltages are used in adiabatic logic technique to recover the energy from each node of the circuit. In this work, we propose a novel adiabatic logic based PUF that utilizes the unique property of adiabatic computing of having time ramp voltages to improve the energy efficiency as well as the reliability. Fig. 4 shows the schematic of the proposed adiabatic logic based PUF cell. The proposed adiabatic PUF cells consists of the cross coupled inverter (M1, M2, M3 and M4) as similar to the memory based PUF. Further, the proposed adiabatic PUF cell also consists of a sleep transistor to enable or disable the PUF cell. When $\overline{enable}/disable$ is "1", then the adiabatic PUF cell will be at the idle state (no operation will be performed). Fig. 5 shows the time ramp voltage or the power clock (Vpc) voltage which is used to charge and discharge the output nodes in the proposed adiabatic PUF cell.

3.1 Operation of the proposed adiabatic logic based PUF cell

Let us try to understand the operation of the proposed adiabatic logic based PUF cell through different phases of the clock (wait, evaluate, hold and recover). Let us assume that disable is "0", so the MN0 transistor will be turned ON for the whole operation.

3.1.1 ***Wait Phase.*** During the wait phase, power clock (Vpc) will be at gnd. So, the PUF cell will be at idle state at this phase.

3.1.2 ***Evaluate phase.*** During the evaluate phase of Vpc, the Vpc will slowly rise from gnd to Vdd. When Vpc starts rising from gnd, both M1 and M2 transistors starts conducting. Due to the imperfections in the manufacturing process, both the transistors will have different threshold voltages. The transistor which has the lower threshold voltage conducts the current quickly as compared to the other and the corresponding load capacitor will quickly get charged. This leads to the flip in the outputs where one of the outputs leads to logic "1" and other to logic "0". For example, let us assume that the threshold voltage of M2 is greater than the threshold voltage of M1.

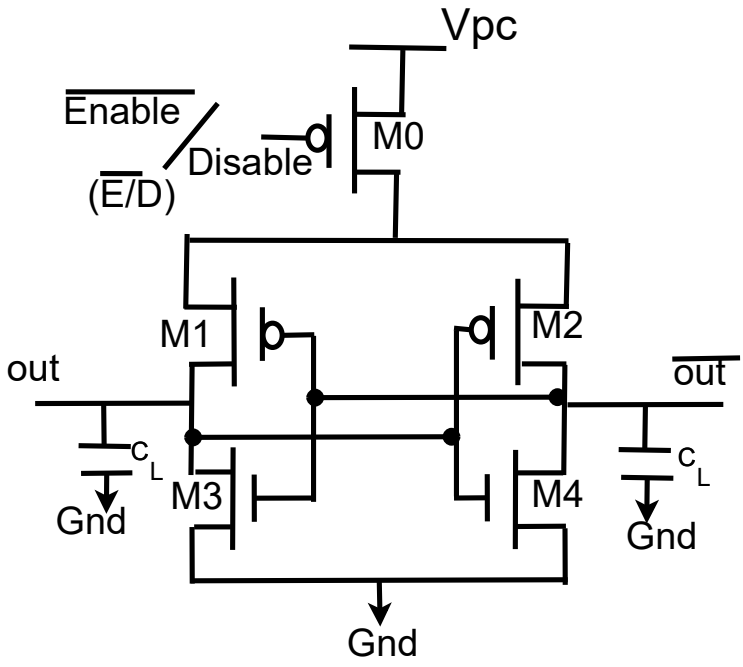

Fig. 4. Schematic of the proposed adiabatic logic based PUF cell

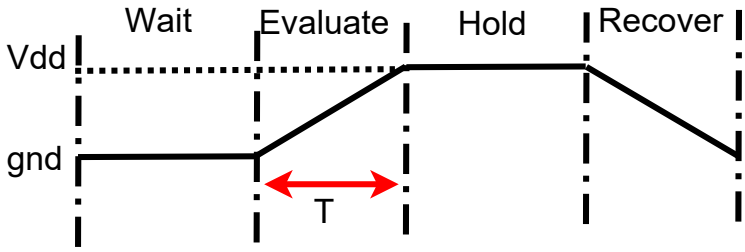

Fig. 5. Time ramp voltage or power clock (Vpc) which is used in the proposed adiabatic PUF cell

Since the threshold voltage of M2 is greater than M1, the resistance of M2 will be greater than M1. When Vpc is greater than Vtp, both M1 and M2 are turned ON. Since $R_{M2} > R_{M1}$, the output load capacitor will be charged quicker through M1 as compared to $\overline{out}$ load capacitor. The operation of the proposed adiabatic logic PUF cell during the evaluate phase is shown in Fig. 6 (a).

3.1.3 ***Hold Phase***. During the hold phase of the Vpc, the proposed adiabatic PUF will have stable PUF response.

3.1.4 ***Recover phase***. During the recover phase of the clock, the time ramp voltage is slowly reduced from Vdd to gnd. During this phase, the charge stored in the load capacitor is slowly recovered back to the power clock generator circuit through the M1 transistor. Fig. 6 (b) shows the

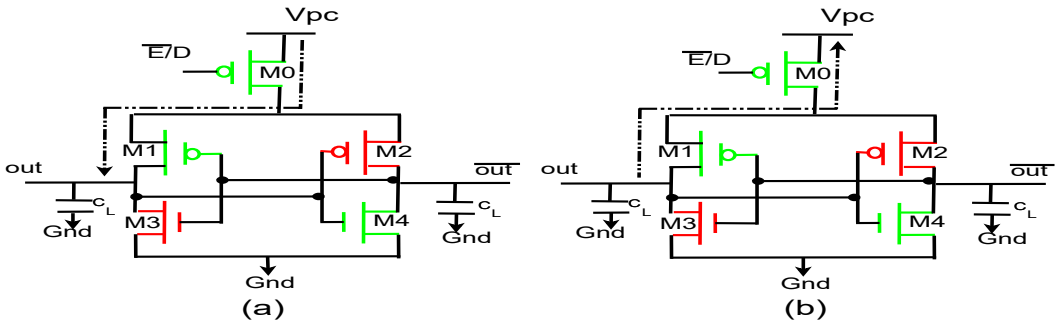

Fig. 6. Operation of the proposed adiabatic PUF during a) Evaluate phase b) Recover phase

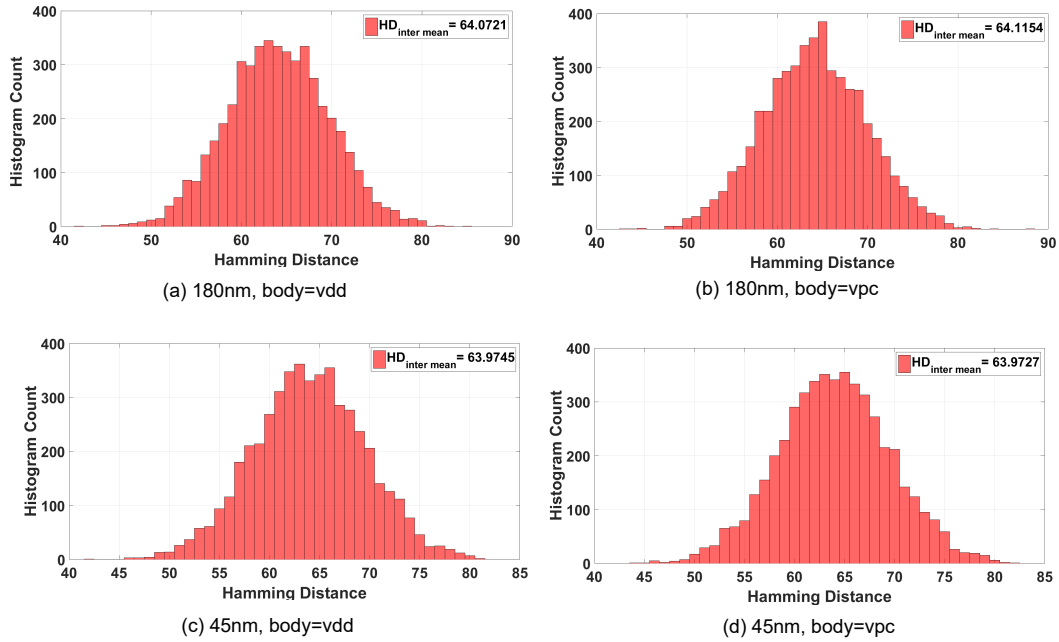

Fig. 7. Inter-chip Hamming distance (HD) variations of the proposed 128 × 100 PUF at different CMOS technology and with body of PMOS connected to Vdd and Vpc

operation of the proposed adiabatic PUF cell during the recover phase of the clock. Further, it has to be noted that the redundant voltage will be stored at the out node since M1 will be turned OFF when Vpc reaches $Vdd - V_{th}$. However, the redundant voltage (V_{tp}) will be useful to bias the PUF cell towards a constant logic“1" or logic “0" in the consecutive cycle of Vpc.

4 PUF EVALUATION METRICS

The metrics which are used to evaluate the performance of the proposed adiabatic PUF are presented in this section [4].

4.0.1 Uniqueness. Uniqueness is used to determine the ability of a PUF to uniquely distinguish a chip among the group of other chips. The ideal value of the uniqueness metric is 50 %. If two different PUF instances (i and j), have responses R_i and R_j which is of n-bit length, then uniqueness is given by,

$$Uniqueness = \frac{2}{k(k-1)} \Sigma_{i=1}^{k-1} \Sigma_{j=i+1}^{K} \frac{HD(R_i, R_j)}{n} \times 100 \tag{2}$$

where HD(R_i, R_j) represents the hamming distance between R_i and R_j. k represents the total number of IC chips. In our case, k=100 and n=128. Obtained from the 100 instances of 128-bit PUF, totally $100 \times 99/2 = 4950$ comparisons are made to obtain the uniqueness value.

4.0.2 Uniformity. Uniformity is used to measure whether the number of zeros and number of ones in the response bits are balanced or not. Uniformity is given by measuring number of 1's in the proposed 128-bit PUF. The ideal value of uniformity is 50%. Uniformity is given by,

$$Uniformity = \frac{1}{n \times k} \Sigma_{i=1}^{k-1} r_{i,l} \times 100 \tag{3}$$

where $r_{i,l}$ represents the l-th bit from PUF instance i.

4.0.3 Reliability. The reproducibility of the response bits from the same PUF instance with the varying environmental conditions such as temperature and supply voltage is given by reliability metrics. For i^{th} PUF instance, let R_i be the reference response or the golden response recorded under nominal operating conditions. Then, applying the same challenges to the same PUF but under different environmental conditions, n responses are observed. Reliability metric is given by,

$$Reliability = 100 - \frac{1}{k} \Sigma_{i=1}^{k} \frac{HD(R_i, R_{i,t}^{'})}{n} \tag{4}$$

where $HD(R_i, R_{i,t}^{'})$ is the hamming distance between the golden response and the response generated by the same PUF instance at different environmental conditions. k represents the total number of IC chips. In other words, reliability is the measure of total number of bits flipped between the golden response and the response recorded from the same PUF instance with different environmental conditions. Reliability is one important PUF metric to be considered while designing PUFs for key generation. The ideal value of the reliability metric is 100 %.

In this paper, temperature is varied from -40°C to 80°C with 27°C as the reference temperature. Further, the reliability of the proposed adiabatic PUF is also evaluated by varying the peak power clock voltages by $\pm 20\% V_{dd}$.

5 SIMULATION RESULTS

To analyze the reproducibility of the proposed adiabatic logic PUF, we have designed and implemented a 128 bit PUF in a standard 180nm CMOS technology and simulated using Cadence Spectre simulator. Further, the evaluation of the proposed adiabatic PUF is also presented in 45nm CMOS technology. In this section, the PUF fingerprint generation is presented. Secondly, the metric which is used to evaluate the performance of the proposed adiabatic PUF is presented. Third, simulation environments and the experiments are described. Finally, the simulation results are presented.

5.1 Proposed PUF response

Each bit of the proposed adiabatic logic based PUF response is generated from the individual adiabatic logic based PUF cell. The major application of the proposed adiabatic PUF cell is to generate the key for the cryptographic operations, so we have implemented a 128 bit PUF array. In order to emulate the characterization of 100 IC PUF chips, 100 runs of Monte-Carlo simulation were performed.

5.2 Simulation environment and experiments

All simulations reported in this paper are performed using Cadence Spectre simulator. The transient noise is added through the simulation tool. The following parameters are considered for the proposed adiabatic PUF.

5.2.1 Body effect. In order to consider the body effect, we have simulated all the designs by connecting the body of the PMOS to Vdd (constant voltage) and to Vpc (power clock).

5.2.2 Temperature variation. In order to consider the temperature variations, we have varied the temperature from -40°C to 80°C. Simulations were performed at -40°C,-20°C,0°C,20°C,27°C,40°C,60°C, and 80°C .

5.2.3 Supply variation. We have varied the supply voltage variation by ±20% of the peak voltage of Vpc.

5.2.4 Technology parameters. In this work, we have considered the variation of PUF metrics by simulating the circuits at two different technology nodes. The channel lengths of the transistors play a major role in controlling manufacturing variations. So, in this paper, we consider 180nm CMOS technology (long-channel) and 45nm CMOS technology (short-channel) analyze the impact of channel length variations. In first case, we presented all the values at 180nm CMOS technology and in the second case, we presented the PUF metrics when the circuit is simulated with 45nm CMOS technology.

Table 1. Simulated and calculated results of uniqueness(%) for the proposed 128 × 100 adiabatic PUF

Technology	Body	$HD_{inter-mean}$	uniqueness(%)
180nm	Vdd	64.0721	49.5607
180nm	Vpc	64.1154	49.5706
45nm	Vdd	63.9743	49.4796
45nm	Vpc	63.9727	49.4839

5.3 Simulation results and analysis

The simulation results and the analysis are presented in this section.

5.3.1 Uniqueness. Fig. 7 shows the inter-chip Hamming Distance (HD) comparison of each pair of the proposed 128 × 100 adiabatic PUF at 180nm CMOS technology and 45nm CMOS technology. Fig. 7 (a) and (b) shows the inter chip HD comparison of each pair of the proposed adiabatic PUF at

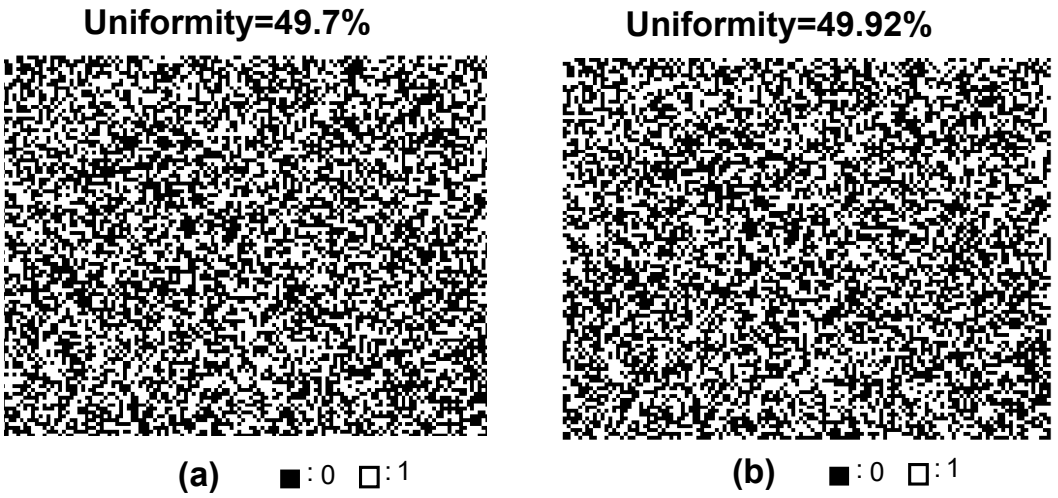

Fig. 8. Gray scale bitmap showing the response of the proposed 128 × 100 adiabatic PUF at 180nm CMOS technology when the body of the PMOS devices connected to a) Vdd and b) Vpc. Black pixel represents bit 0 and white pixel represents bit 1.

180nm CMOS technology with the body of PMOS connected to Vdd and Vpc respectively. Similarly, Fig. 7 (c) and (d) shows the inter chip HD comparison of each pair of the proposed adiabatic PUF at 45nm CMOS technology with the body of PMOS connected to Vdd and Vpc respectively. For the calculation purposes, we use the read response values of the proposed adiabatic PUF at the end of recovery phase. Based on the responses collected from 100 PUF instances, with each providing 128 bits, the mean inter chip HD value ($HD_{inter-mean}$)of the proposed 128 × 100 adiabatic PUF at 180nm CMOS technology when the body is connected to Vdd is 64.0721 while when the body is connected to Vpc, $HD_{inter-mean}$ value is 64.1154. Similarly, $HD_{inter-mean}$ value of the proposed adiabatic PUF with the body connected to Vdd and Vpc is 63.9745 and 63.9727 respectively.

From the simulation results and calculations, we found that the uniqueness value of the proposed 128 × 100 adiabatic PUF at 180nm CMOS technology with body of PMOS connected to Vdd is 49.5607% and to Vpc is 49.5706%. Similarly, the uniqueness value of the proposed 128 × 100 adiabatic PUF at 45nm CMOS technology with body of PMOS connected to Vdd is 49.4796% to Vpc is 49.4839%. The ideal value of uniqueness is 50%. Table I summarizes the uniqueness result of the proposed adiabatic PUF at different CMOS technology.

5.3.2 Uniformity. Fig. 8 (a) and (b) shows the gray scale bit map image of the proposed 128 × 100 adiabatic PUF simulated at 180nm with body of the PMOS connected to Vdd and Vpc respectively. Similarly, Fig. 9 (a) and (b) shows the gray scale bit map image of the proposed 128 bit adiabatic PUF with 100 instances simulated at 45nm CMOS technology with body of the PMOS connected to Vdd and Vpc respectively. From the simulation results and calculations, the uniformity of the proposed adiabatic PUF at 180nm CMOS technology with the body of PMOS connected to Vdd is 49.7%. The uniformity of the proposed adiabatic PUF at 180nm CMOS technology with the body of PMOS connected to Vpc is 49.92%. Similarly, the uniformity of the proposed adiabatic PUF at 45nm CMOS technology with the body of the PMOS connected to Vdd is 49.45% and the uniformity of the PUF at 45nm with the body of the PMOS connected to Vpc is 49.41%. As the probability of

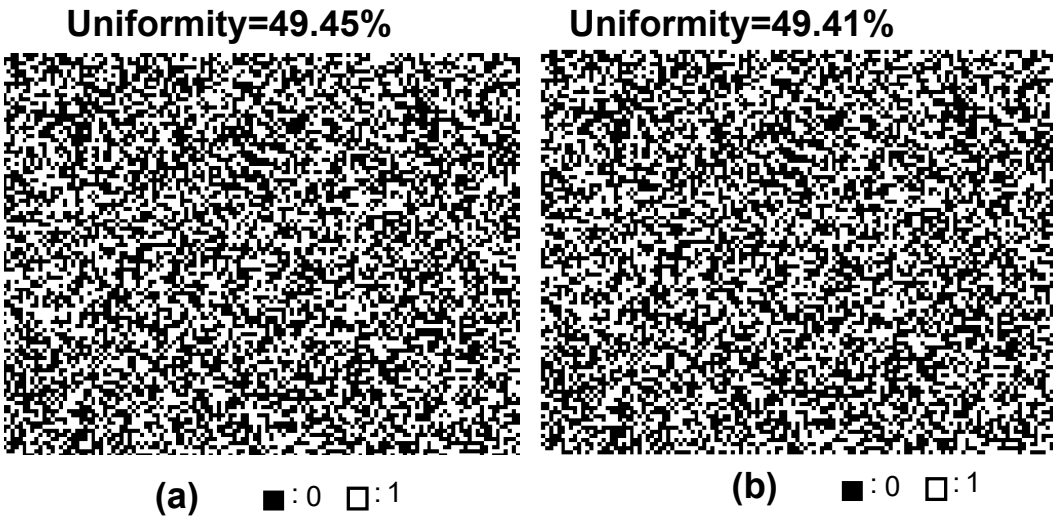

Fig. 9. Gray scale bitmap showing the response of the proposed 128 × 100 adiabatic PUF at 45nm technology when the body of the PMOS devices connected to a) Vdd and b) Vpc. Black pixel represents bit 0 and white pixel represents bit 1.

generating ones is close to ideal value of 50%, it indicates that the proposed adiabatic PUF output is not predictable and makes it hard to attack. Table II shows the uniformity results of the proposed adiabatic PUF with different configurations.

Table 2. Simulated and calculated results of uniformity(%) for the proposed 128 × 100 adiabatic PUF

Technology	Body	uniformity(%)
180nm	Vdd	49.7
180nm	Vpc	49.92
45nm	Vdd	49.45
45nm	Vpc	49.41

5.3.3 Reliability. In this paper, we have evaluated the reliability of the proposed adiabatic PUF by varying the temperature from -40°C to 80°C with 27°C as the reference temperature. Further we have also evaluated the variation of supply voltage by varying the peak power clock voltage by Vdd±20%Vdd. Fig. 10 shows reliability of the proposed adiabatic PUF against temperature variations for all the configurations of the proposed adiabatic PUF simulated at 180nm and 45nm CMOS technology.

Reliability of proposed PUF at 180nm CMOS technology: The average reliability of the proposed 128 bit adiabatic PUF with 100 instances at 180nm CMOS technology with body of PMOS connected to Vdd is 97.7511% while with body of PMOS connected to Vpc is 98.2109%. The worst case reliability of the proposed adiabatic PUF at 180nm CMOS technology when the body is connected to Vdd and Vpc is 96.3750% at 80°C and 96.8438 at 80°C respectively. Table III summarizes the average reliability of the proposed adiabatic PUF at different CMOS technologies and at different configurations.

Reliability of proposed PUF at 45nm CMOS technology: The average reliability of the proposed 128 bit adiabatic PUF with 100 instances at 45nm CMOS technology with body of PMOS connected to Vdd is 99.5368%, while with body of PMOS connected to Vpc is 99.7588%. The worst case reliability for the proposed adiabatic PUF at 45nm CMOS technology when the body is connected to Vdd and Vpc is 99.3281% at 60°C and 99.6016% at -40°C respectively. From our simulations and calculations, it is concluded that the proposed adiabatic PUF at 45nm CMOS technology has high reliability as compared to the 180nm CMOS technology.

Table 3. Simulated and calculated results of average and worst case reliability(%) of the proposed 128×100 adiabatic PUF against temperature variations

Technology	Body	Average (%)	worst case (%)
180nm	Vdd	97.7511	96.3750
180nm	Vpc	98.2109	96.8438
45nm	Vdd	99.5368	99.3281
45nm	Vpc	99.7588	99.6016

Reliability of proposed PUF against supply voltage variations: Further, we have also evaluated the reliability of the proposed adiabatic PUF against supply voltage variations. The 100 PUF instances were simulated under different supply voltages from 0.8 to 1.2 V for 45nm CMOS technology and 1.6 to 2 V for 180nm CMOS technology and at three different temperatures, -40°C, 27°C, and 80°C. Reading the responses at the supply voltage of 1.8 V for 180nm technology and 1 V for 45nm technology as reference, Bit Error Rate (BER) is calculated. Reliability can also calculated as be expressed in terms of Bit Error Rate (BER).

BER is expressed as,

$$BER\% = 100 - Reliability\% \tag{5}$$

Fig. 11 (a) and (b) shows the BER of the proposed 128 bit adiabatic PUF when simulated at 180nm CMOS technology with body connected to Vdd and Vpc respectively. From the simulation results, we found that the worst case BER for 180nm CMOS technology is less than 6.2% and 6% when the body of PMOS connected to Vdd and Vpc respectively. Similarly, Fig. 12 (a) and (b) shows the BER of the proposed 128 bit adiabatic PUF when simulated at 45nm CMOS technology with body connected to Vdd and Vpc. From our simulation results, we found that the worst case BER is less than 0.36% when the body is connected to Vdd while the BER is less than 0.42% when the body is connected to Vdd and Vpc respectively.

5.3.4 Aging effect. In this paper, along with the reliability of PUF with respect to environmental variations, aging effect of proposed PUF is also investigated. The continuous degradation in the functionality of IC is referred as aging effect. Among the various aging mechanisms, the mechanisms which impact the threshold voltage of the transistors plays a major role in the determining stability of proposed PUF. Negative Bias Temperature Instability (NBTI) and Hot Carrier Injection (HCI) stress plays a major role in changing the threshold variations in transistors with respect to time [35]. NBTI effect is caused due to constant DC stress on the PMOS transistors while HCI is mainly due to the AC stress i.e logic switching in the NMOS devices. Aging based reliability simulations for our proposed PUF is performed using Cadence Virtuoso Reliability Simulator. Table IV and V shows the average number of bits flipped over years with the HCI and NBTI stress applied at 180nm and 45nm CMOS technology respectively.

As discussed in [14], NBTI will have minimum effect if the cells are not exposed to continuous DC stress. Proposed adiabatic logic based PUF uses the trapezoidal based power clocks to recover

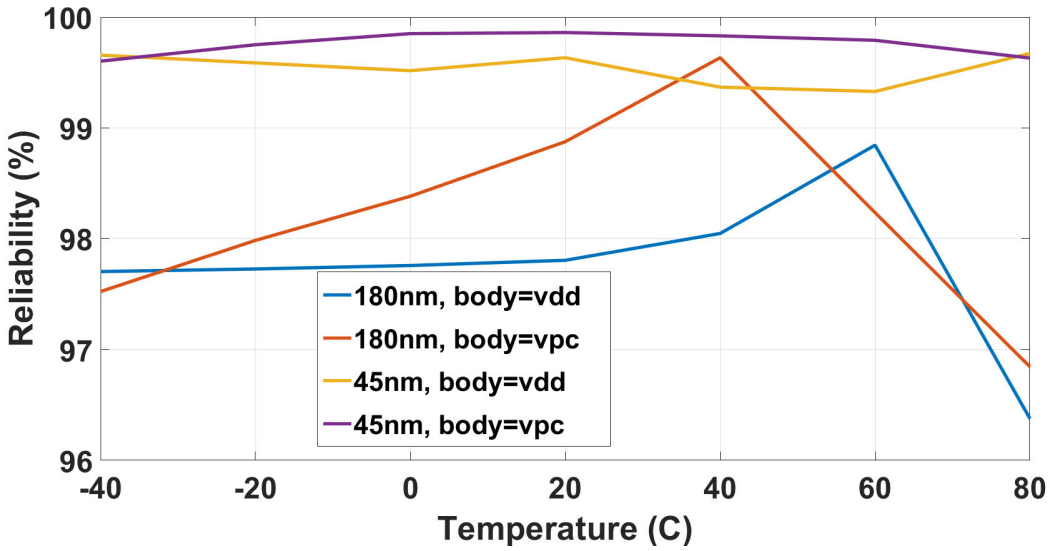

Fig. 10. Reliability of the proposed adiabatic PUF with the change in temperature at different technology nodes and with body effect

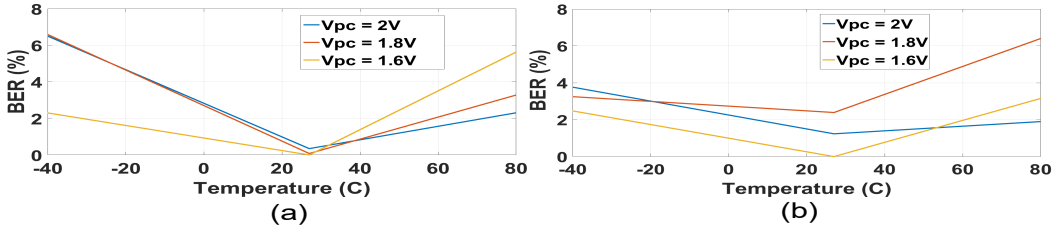

Fig. 11. Bit Error Rate (BER) of the proposed adiabatic PUF with the supply voltage variation at 180nm CMOS technology with PMOS connected to a) Vdd b) Vpc

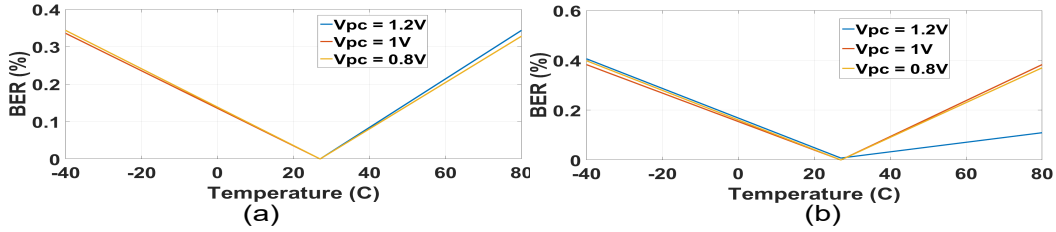

Fig. 12. Bit Error Rate (BER) of the proposed adiabatic PUF with the supply voltage variation at 45nm CMOS technology with PMOS connected to a) Vdd b) Vpc

energy from the load capacitances. Usage of trapezoidal power clock not only used to recover energy from the load capacitances, also helps in minimizing the NBTI effect on proposed adiabatic logic based PUF along with HCI stress as the transistors are switching slower.

Table 4. Average number of bits flipped with respect to years due to aging effect with 180nm CMOS technology

Years	Body= Vdd	Body= Vpc
2	0.78%	0.78%
4	0.78%	0.78%
6	1.56%	1.56%
8	2.34%	1.56%

Table 5. Average number of bits flipped with respect to years due to aging effect with 45nm CMOS technology

Years	Body= Vdd	Body= Vpc
2	1.56%	1.56%
4	2.34%	2.34%
6	3.125%	2.34%
8	3.9%	3.9%

5.3.5 Energy consumption. Energy consumption is a very important parameter in the design of resource constrained devices. Table VI provides the energy consumption comparison of the proposed adiabatic PUF along with the state-of-art PUFs. From Table VI, we can see that the proposed adiabatic PUF is energy efficient as compared to the PUFs listed in the table IV. However, it has to be noted that the proposed adiabatic PUF has more energy consumption than [22] because the PUF proposed in [22] is operated at lower technology node and lower voltage than the proposed adiabatic PUF.

Table 6. Energy consumption comparison of the proposed adiabatic PUF with the state-of-art PUFs

PUF	Tech.	Vdd	Energy/bit
Lim et. al (2005) [15]	180nm	1.8 V	1.37 pJ
Stanzione et. al (2011) [26]	90nm	1.2 V	3.8 pJ
Majzoobi et. al (2011) [18]	90nm	1.2 V	15 fJ
Cao et. al (2015) [3]	180nm	3.3 V	23.9 pJ
Yang et. al (2015) [36]	40nm	0.9 V	17.75 pJ
Neale et. al (2015) [22]	28nm	0.6 V	0.045 fJ
Tao et. al (2016) [29]	65nm	0.6 V	10.3 fJ
Proposed (This work)	180nm	1.8 V	1.071 fJ
Proposed (This work)	45nm	1 V	0.08 fJ

6 DISCUSSION

In this paper, we have employed adiabatic logic for several reasons to design the PUF circuit. Adiabatic logic technique is used to achieve low power and low energy consumption as compared to the conventional CMOS circuits. Further, the adiabatic logic uses time ramp trapezoidal voltages to slowly charge and discharge the load capacitors. The general idea behind adiabatic switching is to use a constant current source to charge the output load capacitor [31]. However, it is more practical to use a time ramp voltage source than a current source as shown in Fig. 13.

The trapezoidal voltage ramp (Vpc) (refer Fig. 5) is expressed as,

Table 7. Security metric comparison of the proposed adiabatic PUF with the state-of-art PUFs

PUF	Tech.	Vdd	Key (bits)	Uniqueness	Uniformity	Reliability	Energy/bit
[15]	180nm	1.8 V	64	NA	NA	95.18%	1.37 pJ
[26]	90nm	1.2 V	256	NA	NA	99.9%	3.8 pJ
[18]	90nm	1.2 V	64	NA	NA	97%	15 fJ
[3]	180nm	3.3 V	64	49.37 %	NA	99.1 %	23.9 pJ
[36]	40nm	0.9 V	256	47.22 %	NA	≥ 99.99 %	17.75 pJ
[22]	28nm	0.6 V	128	49.11 %	49.96 %	88.39	0.045 fJ
[29]	65nm	0.6 V	128	50.04 %	49.5 %	98.56 %	10.3 fJ
[29]	65nm	1.1 V	128	49.70 %	51.6 %	94.66 %	NA
[5]	40nm	0.9 V	NA	50.1%	49.8 %	NA	NA
[30]	NA	4.5 V	263	53.9 %	53.35 %	81%	NA
[32]	45nm	1V	256	49.53 %	51 %	97.86%	NA
[7]	65nm	1.1 V	128	49.69 %	52.45 %	95.27 %	NA
[16]	NA	NA	128	48.76 %	NA	97.72%	NA
Proposed	180nm	1.8 V	128	49.97 %	49.92 %	96.84 %	1.071 fJ
Proposed	45nm	1 V	128	49.48 %	49.41 %	99.60 %	0.08 fJ

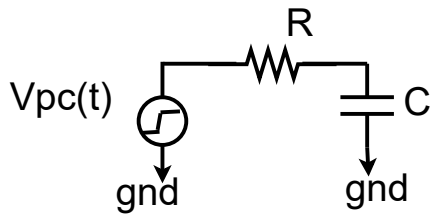

Fig. 13. RC network charging using a trapezoidal voltage ramp

$$\text{Vpc(t)} = \begin{cases} 0 & : \text{t} \leq 0 \\ \text{Vdd.t/T} & : 0 \leq \text{t} \leq \text{T} \\ \text{Vdd} & : \text{T} \leq \text{t} \end{cases}$$

The voltage in the load capacitor is given by,

$$V_c(t) = \begin{cases} 0 & : \text{t} \leq 0 \\ \text{C}.\frac{Vdd}{T}.(1 - e^{\frac{-t}{RC}}) & : 0 \leq \text{t} \leq \text{T} \\ \text{C}.\frac{Vdd}{T}.(1 - e^{\frac{-t}{RC}}).e^{\frac{-(t-T)}{RC}}) & : \text{T} \leq \text{t} \end{cases}$$

By choosing T >> 2RC, it is possible to reduce the energy consumption. Further, it is also important to point out that some of the IoT devices will operate from KHz to 10's of MHZ. For example, RFID devices will operate at 13.56 MHz. Similarly, adiabatic logic has also found huge applications in the design of wireless medical devices such as implantable devices [24].

The initial idea of adiabatic logic based PUF was proposed in [12]. However, the design in [12] will always generate a response '0' for the challenge '0'. This reduces the complexity of generating keys which makes the PUF vulnerable to hardware attacks. Further, the PUF presented in [12] has cascaded PUF cells in to generate multiple response bits. This cascading structure increases the

complexity of the designs. However, in adiabatic logic based PUF proposed in this work, there is no cascade connection of cells. Trapezoidal clocks are applied to all cells and response bits are generated at one time.

In this paper, we have modified the design proposed in [12] to generate the secure key for the cryptographic systems in IoT devices. Further, the reliability of the PUF is an important parameter to consider while designing the PUF to generate the reliable keys. Cortez et. al [6] has reported that intelligent choosing of time ramp up at a particular temperature can improve the reliability of SRAM PUF cells. However, this technique requires additional circuitry to perform the intelligent time ramp up operation to improve the reliability of SRAM PUF cell. Similarly, A. Vijayakumar et. al [33] has proposed a majority voting technique to improve the reliability of the SRAM PUF. However, this technique requires multiple turning on and turning off of the SRAM cell which results in additional power consumption. In our adiabatic logic based PUF, time ramp

In our adiabatic logic based PUF, time ramp voltages are used to recover the charge thereby reducing the energy consumption. Moreover, the usage of time ramp voltages is also used to improve the reliability of the proposed adiabatic PUF as discussed in [6]. The adiabatic clock can be generated as discussed in [1]. Further, it is also need to be noted that the adiabatic clock generator circuit will also be used to drive the cryptographic processor in the circuit to improve the energy-efficiency.

In order to derive a 100% stable key, error correcting codes and fuzzy extractors are used in practice. However, the error correcting code and fuzzy extractors can be complicated with the decrease in the reliability of the PUF [33]. Complicated fuzzy extractors can lead to increase in area and power consumption of overall key generation process [19]. In this paper, we have evaluated the energy consumption of a full fledged PRESENT-80 cryptographic algorithm implemented with the recently proposed EE-SPFAL based adiabatic logic gates [13] along with proposed PUF for key generation. From our simulation, we have seen that the proposed adiabatic PUF consumes about 26% of energy of the entire cryptographic protocol per cycle along with peripheral circuits. It has to be noted that the proposed adiabatic PUF has the worst case reliability of more than 96% for 180nm technology while more than 99% for 45nm technology. Hence, the high reliability of proposed PUF helps in deploying reduced complex fuzzy extractors and ECC codes for the generation of the stable keys for the cryptographic operation.

6.1 Security metric comparison of proposed adiabatic PUF with state-of-art PUFs

Table VII provides the security metric comparison with the proposed adiabatic PUF. All the data reported here are obtained from the corresponding paper. NA in the table represents data not available. From Table VII, we can see that the PUF proposed in [15] using 180nm technology with 1.8 V has the worst case reliability of 95.18% with 1.37 pJ of energy consumption per bit. Our proposed adiabatic PUF which is simulated in 180nm technology has the worst case reliability of 96.84% with the 1.071 fJ of energy consumption per bit per cycle. However, PUF proposed in [4] using 180nm CMOS technology has better worst case reliability than the proposed adiabatic PUF, while consuming 23.9 pJ of energy/bit. The PUF proposed in [26] using 90nm CMOS technology has 99.99% of worst case reliability consuming 3.8pJ/bit of energy. The PUF proposed in [18] using 90nm CMOS technology has lower reliability than PUF proposed in [26] consuming lower energy.

Similarly, the PUF proposed in [36] has very high reliability of 99.99% but suffers from high energy consumption which makes it not suitable to implement in IoT devices. Our proposed adiabatic PUF at 45nm CMOS technology has a worst case reliability of 99.68 % with very low energy consumption. The high reliability, very low energy consumption and low implementation cost make the proposed adiabatic PUF a suitable candidate to implement in battery operated IoT devices and medical devices. The proposed adiabatic PUF in 45nm CMOS technology has more

energy consumption than [22] because the PUF proposed in [22] is operated at lower technology node and lower voltage than the proposed adiabatic PUF. However, the reliability of the PUF in [22] is 88.39% which makes them not suitable to generate reliable key for IoT devices. PUF design proposed in [5] utilizes the CMOS breakdown operation for generating the PUF response bits. Further, a DRAM based PUF was proposed in [30]. However, the reliability of the DRAM PUF still needs to be improved.

7 CONCLUSION

A low cost adiabatic logic based CMOS PUF that generates unique and reliable response bits have been proposed and evaluated in this paper. The proposed adiabatic logic based PUF uses the time ramp voltages to recover the charge from the load capacitor to achieve energy efficiency as well as to improve the reliability. From our simulation results, we have observed that the proposed adiabatic PUF at 180nm CMOS technology and 45nm CMOS technology has the uniqueness and uniformity values close to the ideal value of 50%. The reliability of the PUF is also verified by varying the temperature from -40°C to 80°C and also by varying the supply voltage by ±20% Vdd. Moreover, the proposed adiabatic PUF has significant energy savings as compared to the existing PUFs. Low energy consumption per bit, high reliability, close to ideal uniqueness and uniformity values make our proposed adiabatic PUF a suitable candidate to implement in battery operated IoT devices. Some of the applications of our proposed PUF include secure key generation, device authentication, memoryless key storage, Intellectual Property (IP) protection etc.

ACKNOWLEDGMENT

This work is partially supported by National Science Foundation CAREER Award No. 1845448.

REFERENCES

[1] Muhammad Arsalan and Maitham Shams. 2005. Charge-recovery power clock generators for adiabatic logic circuits. In *VLSI Design, 2005. 18th International Conference on.* IEEE, 171–174.

[2] Debasis Bandyopadhyay and Jaydip Sen. 2011. Internet of things: Applications and challenges in technology and standardization. *Wireless Personal Communications* 58, 1 (2011), 49–69.

[3] Yuan Cao, Le Zhang, Chip-Hong Chang, and Shoushun Chen. 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 (2015), 1143–1147.

[4] Yuan Cao, Le Zhang, Siarhei S Zalivaka, Chip-Hong Chang, and Shoushun Chen. 2015. CMOS image sensor based physical unclonable function for coherent sensor-level authentication. *IEEE Transactions on Circuits and Systems I: Regular Papers* 62, 11 (2015), 2629–2640.

[5] K-H Chuang, Erik Bury, Robin Degraeve, Ben Kaczer, Guido Groeseneken, Ingrid Verbauwhede, and Dimitri Linten. 2017. Physically unclonable function using CMOS breakdown position. In *2017 IEEE International Reliability Physics Symposium (IRPS).* IEEE, 4C–1.

[6] Mafalda Cortez, Said Hamdioui, Ali Kaichouhi, Vincent van der Leest, Roel Maes, and Geert-Jan Schrijen. 2015. Intelligent voltage ramp-up time adaptation for temperature noise reduction on memory-based PUF systems. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 34, 7 (2015), 1162–1175.

[7] Yijun Cui, Chongyan Gu, Chenghua Wang, Máire O'Neill, and Weiqiang Liu. 2018. Ultra-lightweight and reconfigurable tristate inverter based physical unclonable function design. *IEEE Access* 6 (2018), 28478–28487.

[8] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. 2004. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In *International conference on the theory and applications of cryptographic techniques.* Springer, 523–540.

[9] Jorge Guajardo, Sandeep S Kumar, Geert Jan Schrijen, and Pim Tuyls. 2007. FPGA intrinsic PUFs and their use for IP protection. In *CHES*, Vol. 4727. Springer, 63–80.

[10] Daniel E Holcomb, Wayne P Burleson, and Kevin Fu. 2009. Power-up SRAM state as an identifying fingerprint and source of true random numbers. *Computers, IEEE Transactions on* 58, 9 (2009), 1198–1210.

[11] S Dinesh Kumar and SK Noor Mahammad. 2015. A novel adiabatic SRAM cell implementation using split level charge recovery logic. In *2015 19th International Symposium on VLSI Design and Test.* IEEE, 1–2.

[12] S Dinesh Kumar and Himanshu Thapliyal. 2016. Qualpuf: A novel quasi-adiabatic logic based physical unclonable function. In *Proceedings of the 11th Annual Cyber and Information Security Research Conference*. ACM, 24.

[13] S. D. Kumar, H. Thapliyal, and A. Mohammad. 2019. EE-SPFAL: A Novel Energy-Efficient Secure Positive Feedback Adiabatic Logic for DPA Resistant RFID and Smart Card. *IEEE Transactions on Emerging Topics in Computing* 7, 2 (April 2019), 281–293. https://doi.org/10.1109/TETC.2016.2645128

[14] Sanjay V Kumar, KH Kim, and Sachin S Sapatnekar. 2006. Impact of NBTI on SRAM read stability and design for reliability. In *Quality Electronic Design, 2006. ISQED'06. 7th International Symposium on*. IEEE, 6–pp.

[15] Daihyun Lim, Jae W Lee, Blaise Gassend, G Edward Suh, Marten Van Dijk, and Srinivas Devadas. 2005. Extracting secret keys from integrated circuits. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 13, 10 (2005), 1200–1205.

[16] Weiqiang Liu, Lei Zhang, Zhengran Zhang, Chongyan Gu, Chenghua Wang, Maire O'neill, and Fabrizio Lombardi. 2019. XOR-based low-cost Reconfigurable PUFs for IoT Security. *ACM Transactions on Embedded Computing Systems (TECS)* 18, 3 (2019), 25.

[17] Denise Lund, Carrie MacGillivray, Vernon Turner, and Mario Morales. 2014. Worldwide and regional internet of things (iot) 2014–2020 forecast: A virtuous circle of proven value and demand. *International Data Corporation (IDC), Tech. Rep* (2014).

[18] Mehrdad Majzoobi, Golsa Ghiaasi, Farinaz Koushanfar, and Sani R Nassif. 2011. Ultra-low power current-based PUF. In *Circuits and Systems (ISCAS), 2011 IEEE International Symposium on*. IEEE, 2071–2074.

[19] Sanu K Mathew, Sudhir K Satpathy, Mark A Anders, Himanshu Kaul, Steven K Hsu, Amit Agarwal, Gregory K Chen, Rachael J Parker, Ram K Krishnamurthy, and Vivek De. 2014. 16.2 A 0.19 pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS. In *2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)*. IEEE, 278–279.

[20] Debdeep Mukhopadhyay. 2016. PUFs as promising tools for security in Internet of things. *IEEE Design & Test* 33, 3 (2016), 103–115.

[21] Shunji Nakata. 2006. Adiabatic SRAM with the large margin of Vth variation by the gradual change of the voltage. *IEICE Electronics Express* 3, 13 (2006), 304–309.

[22] Adam Neale and Manoj Sachdev. 2015. A low energy SRAM-based physically unclonable function primitive in 28 nm CMOS. In *Custom Integrated Circuits Conference (CICC), 2015 IEEE*. IEEE, 1–4.

[23] Yu Pu and Giby Samson. 2018. Electronic devices employing adiabatic logic circuits with wireless charging. US Patent App. 15/230,885.

[24] Carl A Schu, Daniel R Greeninger, and David L Thompson. 2002. Power dissipation reduction in medical devices using adiabatic logic. US Patent 6,438,422.

[25] Boris Škoric, Pim Tuyls, and Wil Ophey. 2005. Robust key extraction from physical uncloneable functions. In *Applied Cryptography and Network Security*, Vol. 3531. Springer, 407–422.

[26] Stefano Stanzione, Daniele Puntin, and Giuseppe Iannaccone. 2011. CMOS silicon physical unclonable functions based on intrinsic process variability. *IEEE Journal of Solid-State Circuits* 46, 6 (2011), 1456–1463.

[27] G Edward Suh and Srinivas Devadas. 2007. Physical unclonable functions for device authentication and secret key generation. In *Proceedings of the 44th annual design automation conference*. ACM, 9–14.

[28] Yasuhiro Takahashi, Nazrul Anuar Nayan, Toshikazu Sekine, and Michio Yokoyama. 2014. Low-power adiabatic 9T static random access memory. *The Journal of Engineering* 2014, 6 (2014), 259–264.

[29] Sha Tao and Elena Dubrova. 2016. Ultra-energy-efficient temperature-stable physical unclonable function in 65 nm CMOS. *Electronics Letters* 52, 10 (2016), 805–806.

[30] Fatemeh Tehranipoor, Nima Karimian, Wei Yan, and John A Chandy. 2017. DRAM-based intrinsic physically unclonable functions for system-level security and authentication. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 25, 3 (2017), 1085–1097.

[31] Philip Teichmann. 2011. *Adiabatic logic: future trend and system level perspective*. Vol. 34. Springer Science & Business Media.

[32] Elena Ioana Vatajelu, Giorgio Di Natale, Mario Barbareschi, Lionel Torres, Marco Indaco, and Paolo Prinetto. 2016. STT-MRAM-based PUF architecture exploiting magnetic tunnel junction fabrication-induced variability. *ACM Journal on Emerging Technologies in Computing Systems (JETC)* 13, 1 (2016), 5.

[33] Arunkumar Vijayakumar, Vinay C Patil, and Sandip Kundu. 2017. On Improving Reliability of SRAM-Based Physically Unclonable Functions. *Journal of Low Power Electronics and Applications* 7, 1 (2017), 2.

[34] Tutu Wan, Yasha Karimi, Milutin Stanaćević, and Emre Salman. 2017. Perspective paper—Can AC computing be an alternative for wirelessly powered IoT devices? *IEEE Embedded Systems Letters* 9, 1 (2017), 13–16.

[35] Xiaoxiao Wang, LeRoy Winemberg, Donglin Su, Dat Tran, Saji George, Nisar Ahmed, Steve Palosh, Allan Dobin, and Mohammad Tehranipoor. 2015. Aging adaption in integrated circuits using a novel built-in sensor. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 34, 1 (2015), 109–121.

[36] Kaiyuan Yang, Qing Dong, David Blaauw, and Dennis Sylvester. 2015. 14.2 A physically unclonable function with BER< 10- 8 for robust chip authentication using oscillator collapse in 40nm CMOS. In *Solid-State Circuits Conference-(ISSCC), 2015 IEEE International*. IEEE, 1–3.