Eternal-Thing: A Secure Aging-Aware Solar-Energy Harvester Thing for Sustainable IoT

Saswat Kumar Ram, *Student Member, IEEE*, Sauvagya Ranjan Sahoo, *Student Member, IEEE*, Banee Bandana Das, *Student Member, IEEE*, Kamalakanta Mahapatra, *Member, IEEE*, and Saraju P. Mohanty, *Senior Member, IEEE*

***Abstract*—Security and energy-consumption are two conflicting challenges in the design and operation of the smart cities that use Internet-of-Things (IoT). Providing power to IoT things (i.e., sensors and their communications) is a challenge as battery have a limited lifetime, and their maintenance and disposal are costly and hazardous. System on chip (SoC) power requirements for IoT ultra-low-power realm is different and is a challenge for the design engineers to provide uninterrupted power. In this paper, a paradigm shift research that addresses a secure self-sustainable solar-energy harvesting system (EHS) with a security mechanism is proposed. This design incorporates Physically Unclonable Functions (PUFs) for the security of EHS along with an aging sensor for recycled IC detection. The control unit monitors the computational load, recharging of the battery, and security mechanism. Capacitor value modulation (CVM) is used for impedance matching between solar cell and converter during maximum power point tracking (MPPT) to avoid quiescent power consumption. The existing resources of EHS used for designing the PUFs and aging sensor. The secure EHS is designed and fabricated in CMOS 90nm technology. The resulting output is in the range of 3-3.55 V with an input 1-1.5 V. The proposed EHS is consuming 22 μW of power, that satisfies the ultra-low-power requirements of IoT smart nodes.**

***Index Terms*—Internet-of-Things (IoT), Sustainable IoT, Energy Harvesting System (EHS), Physically Unclonable Functions (PUFs), Maximum Power Point Tracking (MPPT), Capacitor Value Modulation (CVM)**

I. Introduction

A City that engages the technology to improve the well-being of its citizens, enhancing the performances of its resources and more prominently connected to humanity, can be termed as a smart city [1]. By 2030, 60% of the population is expected to live in cities. Intelligent control will be needed to coordinate their daily lives and make society safe. The regular monitoring of data, and taking an appropriate decision by using the collected data at the proper time, enhances the performance in a smart city [2]. It is possible by installing a large number of autonomous sensors capable of monitoring parameters related to various applications for the well-being of the society. The main challenge in this deployment is the need for continuous energy supply to these sensors and other devices for a extended period of time. Is there any way to power these smart sensors? The answer lies in one solution called energy harvesting. Energy harvesting has broad market coverage in recent days and in various applications includes wearables in health care [3], sensors used in smart cities, monitoring civil infrastructures like bridges, dams, etc. Many segments in our cities can be infused with scavenging energy from the environment and can be used to power various communication and sensors technologies [4]. The concept behind sustainable IoT [5] is well depicted in Fig. 1, where the solar energy is used as a supply for the IoT end node devices in a smart node thereby transmitting the required data to cloud via gateways.

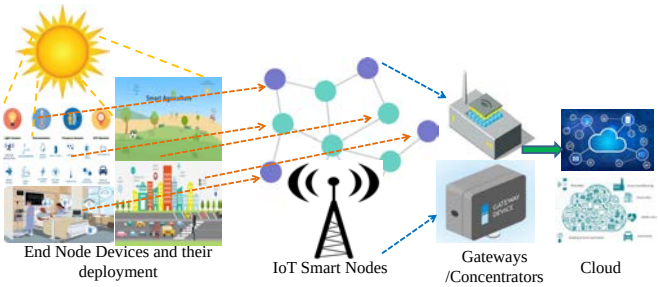


Fig. 1: Sustainable IoT for Sustainable Smart Cities.

System designs that include sensing, processing, and communication properties are gaining more attention in the current realm. These operations in a node connected to the internet constitute IoT [6]. The number of interconnected systems may exceed 24 billion in 2020 [7]. The challenges in security are hard to address, as it is not easy to fit a unique security model for all layers in IoT. The "Security Shield for the Internet of Things" is essential with a broader vision of the internet itself [7]. The edge node devices have to be active for a more extended period, maybe a year or tens of years, and used to gather information correctly [8], [9]. Investigation on harnessing of available natural resources for designing an uninterrupted power supply should be carried out.

Several energy sources like Solar [8], Microbial, RF, Thermoelectric generators [9], [10], [21], [22] can be used for energy harvesting. By adopting a state of art harvesting

S. K. Ram is with the Dept. of Electronics and Communication Engineering, National Institute of Technology, Rourkela,India, E-mail: saswatram01@gmail.com.

S. R. Sahoo is with the Dept. of Electronics and Communication Engineering, National Institute of Technology, Rourkela,India, E-mail: sauvagya.nitrkl@gmail.com.

B. B. Das is with the Dept. of Computer Science Engineering, National Institute of Technology, Rourkela,India, E-mail: banee.bandana@gmail.com.

K. K. Mahapatra is with the Dept. of Electronics and Communication Engineering, National Institute of Technology, Rourkela,India, E-mail: kkm@nitrkl.ac.in.

S. P. Mohanty is with the Dept. of Computer Science and Engineering, University of North Texas, Denton, TX, E-mail: saraju.mohanty@unt.edu.

TABLE I: Summary of Related Research Works

Works	Methodology Used	Salient Features
Ramadass, et al. [9]	Digital Capacitance Modulation	⇒ Switched Capacitor DC-DC converter design. ⇒ Extracting different voltage levels from a fixed supply with constant frequency using capacitor value modulation technique.
Carreon, et al. [10]	Dynamic Impedance Matching with Thermoelectric generators (TEG) as source	⇒ TEG as an alternative energy source. ⇒ Impedance matching of boost converter. ⇒ Additional condition circuit needed for DC conversion of TEG output.
Shao, et al. [11]	DC-DC Converter (Charge Pump) with Variable Switching Frequency for maximum output Power control	⇒ Inductor Less converter design. ⇒ The MPPT is implemented with variable Switching Frequency. ⇒ Variable frequency needs additional circuitry.
Kim, et al. [12]	Regulated Charge Pump with Optimum Power Point Algorithm (OPPT)	⇒ Inductor less design with regulated charge pump. ⇒ Optimum power point algorithm (OPPT) for MPPT for Indoor light conditions. ⇒ Application limited to indoor lightning.
Lauterbach, et al. [13]	Adiabatic Charge Sharing	⇒ Techniques to reduce power consumption during boosting of voltage. ⇒ Reduction in EMI issues.
Mondal, et al. [14]	Adaptive MPPT for harvesting System	⇒ Current starved VCO for frequency adjustment during MPPT. ⇒ It uses negative feedback control for MPPT. ⇒ The circuit used is complex.
Kim, et al. [15]	Successive Approximation Register (SAR) MPPT with Active and Power down Mode	⇒ SAR MPPT for low power consumption in Indoor light conditions. ⇒ Limited to indoor lightning.
Rahman, et al. [16]	Aging tolerant RO-PUF	⇒ Low power RO-PUF for security of ICs. ⇒ Aging tolerant mechanisms.
Zhang, et al. [17]	Recycled IC detection	⇒ On-chip RO sensor for recycled IC detection. ⇒ PUFs as a security alternative in low power circuits.
Shih, et al. [18]	DC-DC converter (Charge Pump) with Band gap Reference output Controller	⇒ Four-phased charge pump design. ⇒ Bandgap reference circuit in the feedback path for regulation through comparators. ⇒ Clock generation scheme is complex.
Mohsen, et al. [19]	Comprehensive study of security in IoT	⇒ Defining scope of security in IoT. ⇒ Emerging security challenges addressed. ⇒ Several counter measures discussed for securing things.
Perera, et al. [20]	IoT smart solutions for market place	⇒ Discussion on smat city, smart environment, smart industry etc. ⇒ Examining the efficiency and effectiveness of solutions for consumers life style. ⇒ Fruitful discussions on supply chain management.
Current Paper (Eternal Thing)	**Ultra low power secure solar harvesting system design using existing circuitry with aging detection mechanism**	⇒ Secure self-sustainable harvesting system design. ⇒ Converter with adiabatic charging scheme for reduction in power. ⇒ Physically unclonable functionality (PUF) used for securing the harvesting chip. ⇒ Aging sensor incorporated within chip to detect counterfeiting of ICs.

mechanisms, IoT nodes can supplied with uninterrupted power supply [11], [23]. To extract maximum power from input source, a well-suited maximum power point tracking (MPPT) scheme is used [12], [24], [25]. A small size panel that is used for a IoT node is not capable to drive the computational load and to charge the rechargeable battery/Supercapacitor [13], [14], [26]; therefore DC-DC converters [15], [27]–[29] are used.

With an increase in demand for IoT in almost all applications and its deployment, the security is also a critical concern similar to power, performance, and area [30]. Security starting from the fabrication till deployment is crucial. In the foundry, the chip may be cloned, so counter mechanism should be adopted to avoid this forge [16]. As discussed in [17], [31], security aspects include identification and authentication of IC, preventing from invasive or semi-invasive attacks, detection of refurbished (counterfeited) IC from the obsolete information etc. [7].

The rest of this article is organized in the following manner: Section II is related research work. Section III describes novel contributions of the current paper to the state of art. Section IV is about our vision for sustainable IoT for smart cities. The proposed secure thing with energy harvesting capabilities is well described in Section V. Section VI describes the hardware design and characteristics of the proposed thing. Section VII validates the experimental results. Finally, Section VIII concludes the paper with discussions on future research.

II. Related Prior Works

Table I presents the summary of the related work with methodologies used along with a brief discussion.

There are various types of natural energy sources available including, solar [11], [23], wind, piezoelectric [9], [21], and microbial, which can be used with proper conditioning towards energy storage. Shao, et al. in [11] presented a solar power management system towards inductor-less design. A detailed study of energy management was presented in [32].

In [15], [18] researchers presented energy harvesting and output regulation through the bandgap referenced output controller. The DC-DC converters (charge pumps) are used for boosting the low input energy and are well presented in [33]–[35]. Maximum power can be extracted from the input by adopting maximum power point tracking (MPPT) techniques towards high power efficiency and are discussed by Liu, et al. in [8] and Hunyh, et al. in [28]. A successive approximation register MPPT algorithm with low power-down mode and an adaptive MPPT technique was presented in [12] and [14], respectively, for harvesting system design. A thermoelectric generator as an energy source with MPPT methodologies for impedance matching was described in [10] and [36]. The ambient backscatter transmission methods with energy harvesting capabilities was discussed in detail based on Wi-Fi architecture in [4] for energy-efficient transmission. Lauterbach, et al. [13] presented new charge sharing schemes, applied an adiabatic process for charging the charge pump capacitors for saving the power.

A secure EHS is a state of art technology outcome for securing the hardware that leads to sustainable IoT. In hardware security, PUF is used as an alternative, as the key generated from PUF is unique and forge-proof. The functionality and reliability of PUF can be improved by using additional technologies to make it more secure, and is discussed in [30]. The key generation process in PUFs is presented in [16]. The use of PUF to make the chip more secure is presented in [31]. Additional techniques using PUF towards the mitigation of counterfeiting of hardware have been presented in [7], [17].

III. Novel Contributions of the current Paper to the State of Art

The current paper addresses a unified design to combine energy-awareness and security-awareness for building IoT, which can lead to sustainability in smart cities. To best of authors' knowledge, this is a paradigm shift work as existing literature deals with either energy-awareness or security-awareness, but not both. In the rest of the section, we discuss these two categories of the existing literature.

A. Research Question and Challenges Addressed in the Current Paper

The choice of an energy source and its proper conditioning for societal use is a challenge. Extracting maximum power from a natural energy source with a suitable algorithm that uses less hardware needs lots of effort. As per the deployment of the smart node, its security is a major concern. The harvesting system ICs may face counterfeiting issues at various levels, including foundry. The security in IoT is an essential parameter starting from the end nodes to the cloud and cannot be compromised. The energy requirement of the sensors in IoT is continuous that needs harvesting energy from natural resources to fulfill the required demand. The attack in the energy harvesting circuitry by an adversary can destroy the sensors that would lead to denial of supply (DoS) type attack (The adversary may be few malicious Trojans). The continuous supply requirement, starting from the edge node to the cloud is a must. It must be ensured that the collection of data at the edge node must not be affected primarily due to DoS attack. These discussions raised many research questions in mind, and the authors tried their level best to address these challenges in this paper.

B. Proposed Solution of the Current Paper

Researcher's review on harvesting natural energy, undoubtedly advocate solar energy as a suitable alternative for ultra-low-power harvesting system design for IoT targeting the smart cities. In this work, solar power is taken as an input energy source. DC-DC converters (charge pumps) and hill-climbing algorithm for MPPT is used for the power conditioning and extraction of maximum power from the input. Impedance matching between solar cells and converter is addressed using capacitor value modulation (CVM). The finite state machine (FSM) generates the control signals for various operations in the system [37], [38].

Towards the security of the harvesting system, PUF is incorporated into the design by reusing the existing hardware. The usage of existing circuitry as an aging sensor for the recycled IC detection is an advantage. It may be noted that, the ring oscillator is reused as aging sensor, such that no additional circuit is used for the purpose and is reliable against aging. The solar energy harvesting system presented in this paper is self-sustainable, secure, and with other mechanisms inherent towards counterfeiting IC and recycled IC detection.

C. Novelty of the Proposed Solution

To address the energy and security requirement of the numerous autonomous sensors used in smart cities, the proposed secure self-sustainable solar energy harvesting system (SEHS) is a state of art key. We summarize the novel contributions of the paper as follows:

1) A novel approach to combine security, solar-energy harvesting, and aging-detection, in a unified system for self-sustainable SEHS.
2) A novel approach for DC-DC conversion for SEHS.
3) Novel PUFs for securing self-sustainable SEHS.
4) A novel approach for counterfeiting and recycled IC detection with an inbuilt aging sensor in SEHS.

IV. The Eternal-Thing: Our Vision for Sustainable IoT for Smart Cities

The primary objective of this work is to design an ultra-low-power solar energy harvesting system (SEHS) with a security mechanism, to secure during fabrication at the foundry and further stages. The security of EHS points to the usage of two PUFs. The reuse of the ring oscillator (RO) available in EHS as an aging sensor would provide information about the EHS IC, that is fresh or otherwise. These PUFs uses less hardware and is cost-effective. The detail design process and validation of the proposed concept are discussed in subsequent Sections. Fig. 2 explains a secure self-sustainable IoT smart node.

Due to the development of silicon technology, the chip size is shrinking with time. System-on-a-chip (SoC) implementation of smart nodes in IoT is a reality and consumes

a small area. The IoT intelligent nodes are SoCs capable of sensing, processing and transmitting useful information [18], [33], [4]. The information sensed by the tiny sensors may be temperature, pressure, humidity, irradiance level, etc. The IoT is two-way communication in WSNs, where appropriate decisions are taken and implemented in real-time. The sensors used in IoT need to be functional for a prolonged period (maybe tens of years) regardless of the area of deployment. A continuous power supply requirement for these end node devices is mandatory. Usually small batteries are used that drain out after an interval. Hence, it demands design of an uninterrupted power supply. Therefore EHS is gaining more attention from researcher's prospective. Proper methodology for choosing natural energy sources with a rechargeable battery or supercapacitor plays a revolutionary achievement in this realm. The security of these smart nodes, as per the area of deployment, is a challenge. The safety of the EHS chip is an unexplored domain starting from fab lab till deployment. To secure the EHS chip from adverse scenarios, and during its functioning, PUFs are used as security primitives.

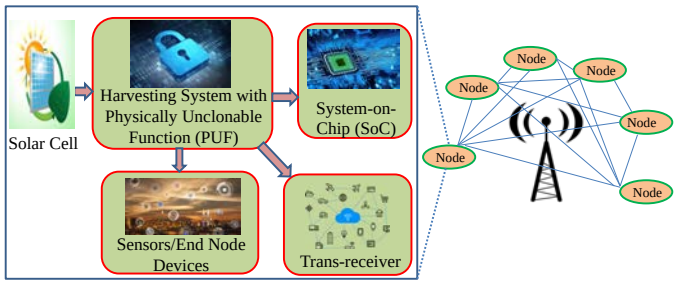


Fig. 2: A secure self-sustainable IoT smart node.

V. The Proposed Secure Thing with Energy-Harvesting Capability

Towards an uninterrupted power supply design for IoT smart nodes, solar energy harvesting plays an important role. The DC-DC converter boosts the solar voltage, and extraction of maximum power is achieved using hill-climbing algorithm. The energy harvesting system is made secure by using PUFs and an aging sensor. Fig. 3a shows energy harvesting concept and basic principle behind energy harvesting for IoT end node devices, that uses energy sources, DC-DC Converters, MPPT tracking, supercapacitor as energy storage and finally the computational load. Fig. 3b presents the proposed secure energy harvesting system.

A. Proposed Solar-Energy Harvesting System

The energy harvesting system is for charging supercapacitor and handling the computational load. The EHS depicted in Fig. 3b consists of various modules as: (1) Ring Oscillator (RO), (2) A Non-overlapping Clock Generator (NOCG), (3) The Auxiliary Charge Pump (ACP), (4) DC-DC Converter, (5) A Current Sensor (CS), (6) MPPT Decision Circuit (MDC), (7) Digital Controller (FSM), (8) PUFs as security premitives, and (9) Aging Sensor.

1) RO, NOCG, ACP : The RO used is to generate the required switching pulses of 150 kHz for the smooth operation of the SEHS. The output of the RO is fed to the NOCG to generate non-overlapping clocks, as shown in Fig. 4a.

These non-overlapping clocks (V_{clk1} and V_{clk2}) are then given to the ACP, as depicted in Fig. 4b. The ACP is used to generate the essential body bias (V_{PB}) for the DC-DC converter for boosting the solar voltage, such that no additional external bias is required off-chip.

2) Charge Pump as Voltage Booster: In conventional charge pumps, power loss is a significant concern for maintaining high efficiency. The reasons for power losses in switched converters can be categorized as conduction loss, switching loss, and charge redistribution loss. As depicted in Fig. 5a, a two-stage adiabatic charging process is adopted in this work to minimize power consumption. In one step charging process, the capacitor charges from 0 to V_{DD}, and the energy delivered by the voltage source is the following:

$$E_{source} = Q * V_{DD} \tag{1}$$

During two-stage charging of the capacitor, the energy delivered by the source is reduced to the following expression:

$$E_{source} = \frac{1}{2}Q * \frac{1}{2}V_{DD} + \frac{1}{2}Q * V_{DD} = \frac{3}{4}Q * V_{DD} \tag{2}$$

The two-stage charging with charge sharing reduces the energy delivered by the voltage source to 50% as compared to one-step charging, as shown in equation 3.

$$E_{source} = \frac{1}{2}Q * V_{DD} = \frac{1}{2}C * {V_{DD}}^2 \tag{3}$$

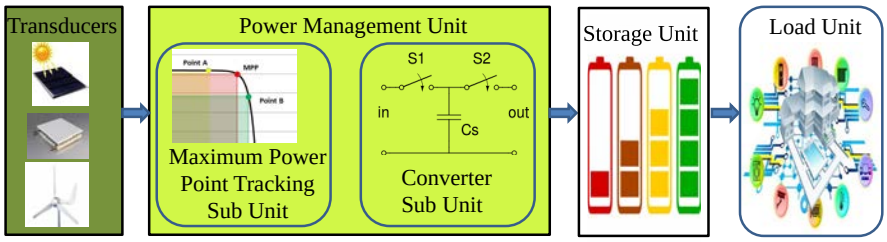
To achieve a better boosting of output voltage, the body of the MOS devices is connected to separate higher bias voltage (V_{PB}) to resolve the issues related to threshold voltages (V_{th}). During the charge transfer, there is an increase in threshold voltage and is taken care of by applying higher voltages to the body of the MOS device. This gives better voltage efficiency as compared to the other architectures. Fig. 5b depicts the pumping capacitors connected to the capacitor banks for impedance matching between the solar cell and the DC-DC converter. The impedance matching is achieved through capacitor value modulation (CVM).

The power conversion efficiency (PCE) [8] is a measure of boosting of input as per conversion ratio (CR), and is expressed by the following expression:

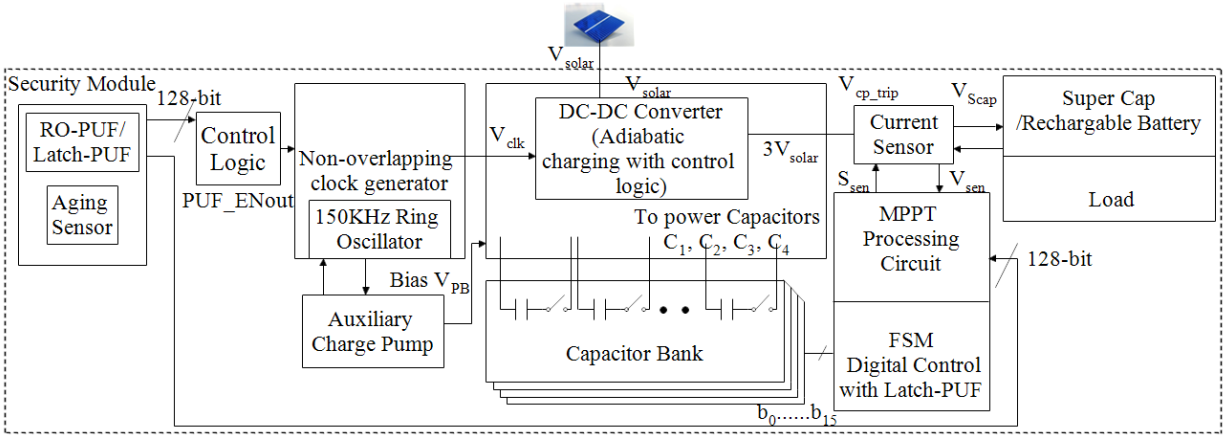
$$PCE = \left(\frac{V_{out}}{V_{solar} \times CR}\right) \times 100\% \tag{4}$$

Fig. 5c depicts the clock generation for the converter using the tristate drivers, and NOR gate. The two-step charging and charge sharing further reduce the power. The circuit comprises two tristate drivers and signals n_1 and n_2, which are responsible for charging and discharging the capacitors C_{a1} and C_{a2} as depicted in Fig. 5c.

The transistor T_s used for charge sharing. T_s equalize C_{a1} and C_{a2} to V_{DD}/2 before discharging to zero, which leads to energy gain in the first part in equation 2. The voltage source does the charging of V_{DD}/2 to V_{DD}. The CP_1 and CP_2 are the pumping clocks used by the converter for voltage boosting.



(a) Energy harvesting concept



(b) Design of the proposed system

Fig. 3: The proposed PUF-secured solar-energy harvesting system.

The output of the converter is sensed at intervals by a current sensor for MPPT.

3) Current Sensor (CS): The current sensor depicted in Fig. 6 is used for sensing power information from the converter output during the MPPT procedure. Once the MPPT achieved, the control section releases proper switching signals such that the converter charges the supercapacitor and handles the computational load. The discrete use of the current sensor leads to less power consumption as compared to always ON devices [33]. The SW_{C_1} and SW_{C_2} are controlled by the signal S_{sen} and S_{senbar} generated by the finite state machine (FSM) controller. The V_{sen} is a part of the power information sensed at R_{SEN}. The following expression governs the closed-loop transfer function from the charge pump output to the current sensor output:

$$\left(\frac{Vsen}{Icp}\right) = \frac{R_{SEN}}{\left(1 + \frac{1}{g_{MCP3}}.T_{FB}\right)}, \tag{5}$$

where T_{FB} is the open loop trans-conductance [8]. The sensing voltage V_{sen} is obtained across R_{SEN} resistor. When the MPPT decision achieved, the S_{sen} becomes Low, and the converter output charges the supercapacitor (S_{cap}). So the transfer function can be rewritten as the following:

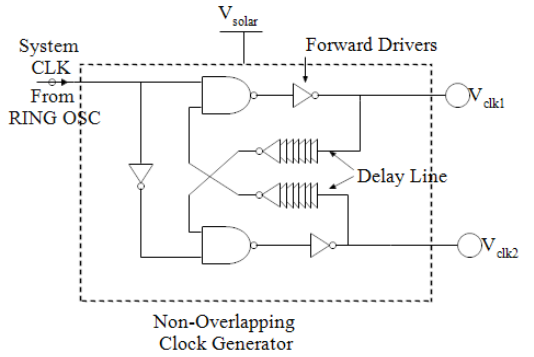
$$\left(\frac{Vsen}{Icp}\right) = \frac{R_{SEN}}{\left(1 - \frac{g_{MCN2}}{g_{MCP3}}\right)}, \tag{6}$$

where $Z_{n1} = 1/g_{MCN1}$ and $Z_{CP2} = 1/g_{MCP2}$ at low frequencies [8]. The trans-conductance of $MCP3$ is made larger than $MCN2$ for stability and I_{cp} is converted to V_{sen}.

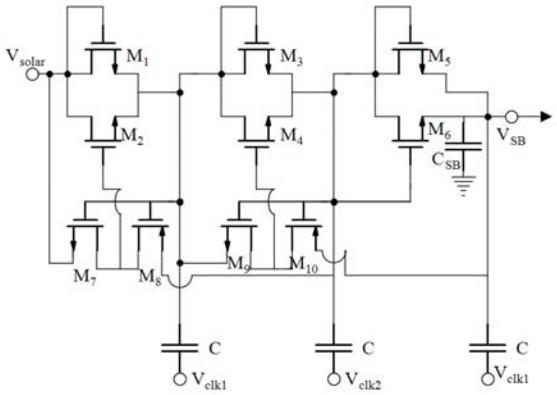
4) MPPT Decision Circuit (MDC): The solar cell output is influenced by various environmental parameters. Fig. 7 depicts the solar cell characteristics (power v/s voltage), which shows that at a particular point, the power is maximum, called a maximum power point (MPP). Hill-climbing approach is suitable to track the MPP. Furthermore, hardware implementation of this method is simpler compared to other MPPT approaches. The process for achieving the MPP is as follows.

- The two power information is sensed at different time intervals as P_n (old power) and P_{n+1} (new power), and are compared to check whether $P_n > P_{n+1}$ or $P_n < P_{n+1}$. If $P_n < P_{n+1}$, then the algorithm will continue to find the maximum power point in subsequent cycles. If the $P_n > P_{n+1}$, then the MPPT is achieved.
- The MPPT algorithm is implemented with the help of sample and hold (S/H) circuits, comparator, D-latch and XNOR gate as depicted in Fig. 8a.
- An FSM is used to generate the necessary control signals for the entire operation along with binary to thermometer code for CVM.
- The use of the thermometer codes is for a smooth transition of binary bits during CVM. Fig. 8a depicts the thermometer code b_0 to b_{15} (output of the FSM) that controls the capacitor value modulation, and Fig. 8b depicts the connection of the capacitor bank with C_u along with the thermometer code.

5) Digital Controller (FSM): Fig. 9a shows the FSM for MPPT. The FSM uses 32-clock cycles for one MPPT cycle, as depicted in Fig. 9b. As per the MPPT procedure, the



(a) Circuit diagram of non-overlapping clock generator

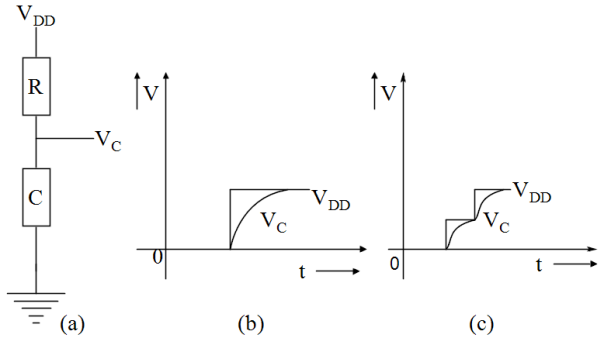


(b) Circuit Diagram of Auxiliary Charge Pump for Bias generation

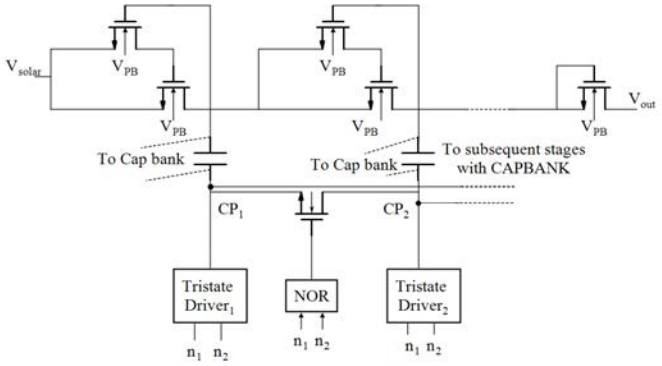
Fig. 4: Clock and higher bias generation for converter.

number of MPPT cycles required is taken care of by the FSM. The sensing and decision making procedure during MPPT is presented in Fig. 8a and its associated timing diagram depicted in Fig. 9b, that are self explanatory.

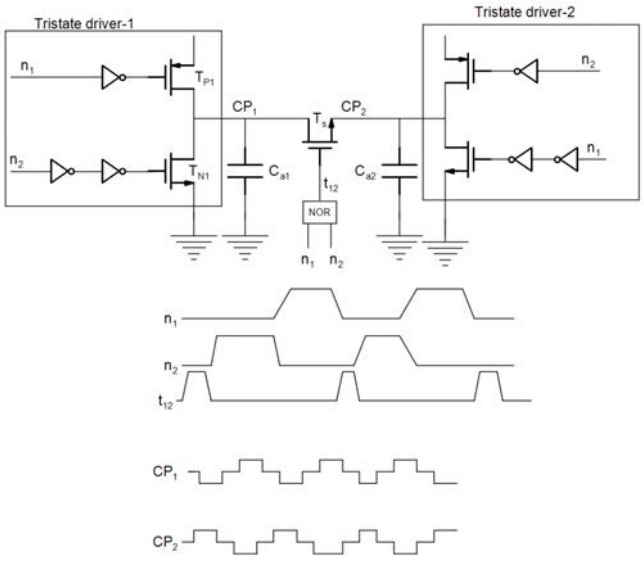
- The first 14-cycles used to sense the old power information P_n and is stored in the sample and hold circuit S/H_1. During this period, the S_{sen} is active to sense the converter output current through the current sensor.
- The control signal S_1 is high during these 14-clock cycles. The thermometer code b_0 to b_{15} are initially High and are Low one by one at each MPPT cycle (in the 15^{th} clock cycle) for CVM by the FSM.
- The new power information P_{n+1} is sensed in the next 14-clock cycles and is stored in the sample and hold circuit S/H_2. During this period, the S_{sen} is active for sensing. The control signal S_2 is High during these 14-cycles.
- The two power information is now stored in the S/H_1 and S/H_2 and is ready for comparison using the comparator.
- The FSM releases the control signal S_3 (High for two clock cycles) for comparison. The output of the comparator is fed to the D-latch and the XNOR gate for the final decision of MPPT achievement.
- The XNOR output is initially High during comparison and is High till $P_n < P_{n+1}$. When $P_n > P_{n+1}$, that indicates the MPPT is achieved and changes the signal X_{nor_out} to Low.



(a) Adiabatic charging



(b) Two phase clocking with two step charging Charge Pump with separate body bias



(c) Circuit diagram of generating pumping clocks for DC-DC converter

Fig. 5: Charge pump as voltage booster with associated signals.

- This decision bit makes the FSM release the necessary control signals for the current sensor, thereby making all MPPT related control signals to become reset.
- The FSM releases S_5 at the end of MPPT to initiate any I/O Communication.

The various control signals used during MPPT procedure with proper explanations are well described in Table II.

TABLE II: FSM control signals and specifications

FSM Control Signals	Specifications
S	Environmental sensor triggers MPPT operation (1 MPPT Cycle=32 Clock Periods)
S_1	High for first 14 clock periods and enables $C_{(S/H)1}$ and ϕ_n is stored
S_2	High for another 14 clock periods and enables $C_{(S/H)2}$ and ϕ_{n+1} is stored
S_{sen}	High during S_1 and S_2 High values for sensing and low for 14^{th} ,30^{th} and 31^{th} clock period for decisions
S_3	High for 30^{th} and 31^{st} clock periods for comparison of values in $C_{(S/H)1}$ and $C_{(S/H)2}$
S_4	High for 31^{st} clock cycle for decision
S_5	High after 31^{st} clock cycle for some I/O initialization
$b_0 - b_{15}$	Binary to Thermometer output bits. Each bit-becomes low once at every 14^{th} clock cycle for CVM (Initially all are High)

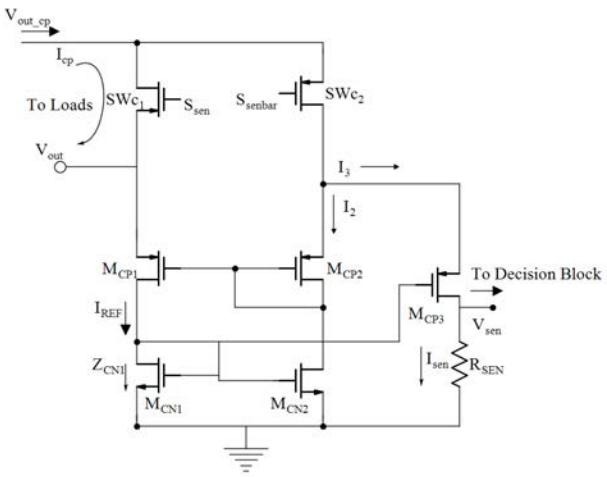


Fig. 6: Current Sensor

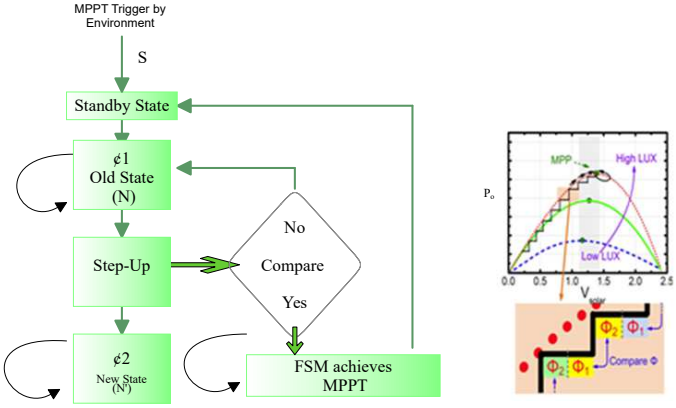
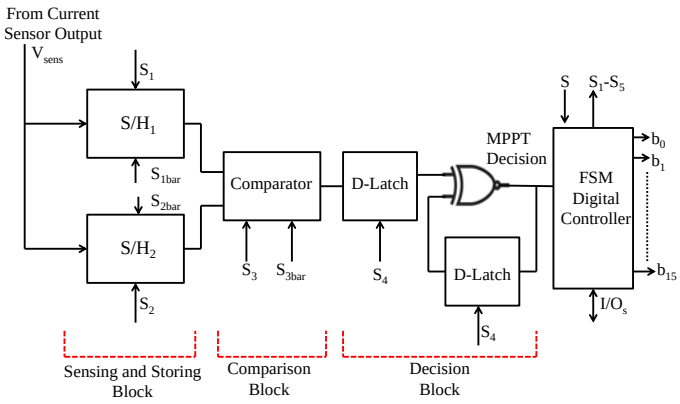
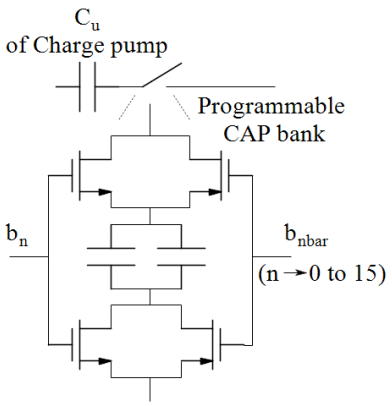


Fig. 7: Flow chart of Hill-Climbing algorithm with procedure



(a) MPPT procedure with FSM Control Signals



(b) Digitally programmable capacitor bank

Fig. 8: HCA with Capacitor value modulation for impedance matching.

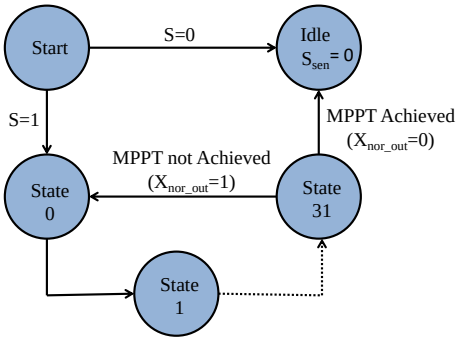
B. The Proposed Novel PUF Authentication Method

As discussed in [17], [31], security aspects include identification and authentication of IC, preventing from invasive or semi-invasive attacks, detection of refurbished IC from the obsolete information, etc. [7].

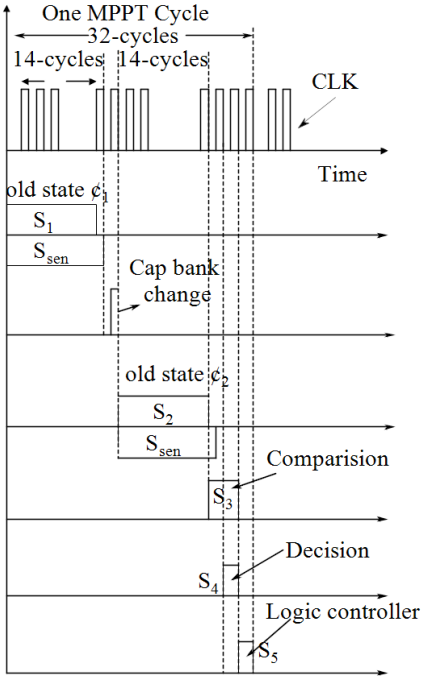
The reason for using PUF is twofold i.e., along with unclonable secure key extracted from PUF; these are also used for authentication [16], [17], [30], [31]. The extracted 128-bit key from both RO-PUF and Latch-PUF is used to trigger the RO and MPPT module simultaneously. The same keys i.e., CRPs (challenge response pairs), are stored in a database, as shown in Fig. 10. In our analysis, we have collected 1000 CRPs from both these PUFs and stored them in the database. It is well known that the stored CRPs are PV dependent; it is tough to create a replica of these CRPs by an adversary. The extracted key is compared with the stored CRPs for authentication purpose after the chip gets fabricated.

RO-PUF is one of the widely used delay-based PUF along with Latch-PUF, which is one of the highly reliable PUFs. Both these possess better quality metrics.

A counterfeiting IC affects the performance, along with a significant loss of revenue for semiconductor companies. The different counterfeited ICs includes the ones from an untrusted foundry, defective, off-specification, tampered, cloned, recycled IC, etc. Recycled ICs are generally extracted from the used PCB or old system and contribute to 80% of the total reported counterfeited product [7]. Although a used/recycled



(a) Finite State Machine (FSM) for MPPT



(b) Timing diagram of MPPT Controller

Fig. 9: FSM with associated signals for MPPT.

IC initially functions correctly and adequately reduces the lifespan of IC as compared to a fresh IC. So it is highly essential for the detection of recycled IC in a system. This paper parallelly addresses the recycling issue of IC. A recycled IC undergoes continuous aging, and its performance deteriorates. Researchers in the literature [30], accelerate this aging mechanism for efficient detection of recycled IC. Out of several techniques proposed in the literature [17], RO based aging sensor is least expensive and pragmatic method for the detection of recycled ICs and is well-suited for lightweight applications. This technique accelerates the NBTI (negative bias temperature instability) effect [17], which is one of the significant aging mechanisms out of NBTI, hot carrier injection (HCI), temperature-dependent dielectric breakdown (TDDB), etc.

NBTI occurs in PMOS when a constant DC stress is applied. The continuous negative bias across the gate and source of PMOS i.e., negative V_{GS}, causes degradation in the V_{th} [31].

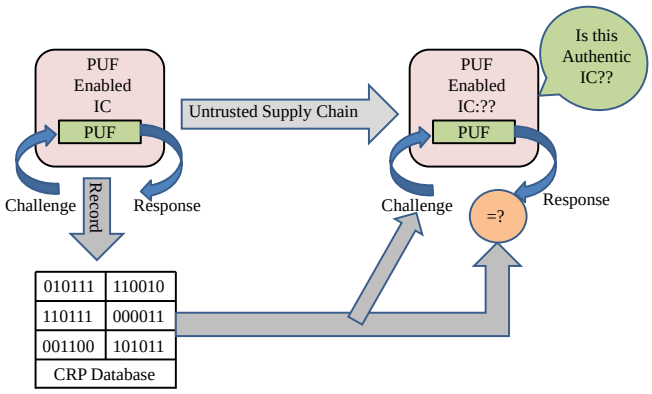


Fig. 10: PUF based authentication.

The change in V_{th} is modeled as follows:

$$\Delta Vth_{,NBTI} = A_{NBTI} * t_{ox}\sqrt{c_{ox}(V_{DD}-Vth)}e^{\left(\frac{V_{DD}-Vth}{tox*E0}-\frac{E\alpha}{Kt}\right)} * t_{stress}^{0.25}, \quad (7)$$

where A_{NBTI}= Constant, and is proportional to aging, t_{ox}=Oxide thickness, C_{ox}= Gate capacitance per unit area, E0, E_{α}= Device dependent parameters, K=Boltzmann constant, t_{stress}= stress time duration. Equation 7 indicates that an increase in stress duration or higher negative bias results in higher degradation in the threshold voltage of PMOS. This degradation in V_{th} affects the oscillation frequency of RO [30]. RO sensor [17] picks up this oscillation frequency variation to predict whether the IC under test is a fresh or recycled one. In this paper, the available RO of the EHS module is reused for designing an aging sensor to make the EHS area efficient.

To determine the impact of NBTI stress on both the RO, the Relxpert simulator is used, and we observe the frequency of F_{DIF}. NBTI stress applied for a period of $5D$, $10D$, $15D$, and $20D$, and the corresponding F_{DIF} shown in Table III, Lower value of F_{DIF} observed when NBTI stress is applied continuously for 5-days ($5D$). Due to this lower value, if an IC is being used, then there is a probability that it may be treated as a fresh IC. Higher value of F_{DIF} is observed after a stress period of $10D$, which shows the IC under test is a recycled IC. This discussion confirms efficient detection of recycled IC is possible, if it is used for a period of more than $10D$.

TABLE III: Average Frequency F_{DIF} with f_{OSC} change.

Oscillating Frequency f_{OSC}	Average Frequency F_{DIF}
T=0D	150 kHz
T=5D	148.17 kHz
T=10D	132.88 kHz
T=15D	112.68 kHz
T=20D	110.68 kHz

C. Proposed Novel Method to Determine Aging of the Thing

To track the duration for which the IC is being used after fabrication, the aging sensor is incorporated. The on-chip aging sensor module used in our proposed EHS is shown in

Fig. 15. When the aging sensor module is enabled, it predicts the duration for which SEHS is used, for our analysis, we have used the aging sensor module proposed in [17]. As shown in Fig. 15, it mainly consists of a reference RO i.e., $(RO)_{REF}$ and stressed RO i.e., $(RO)_{STR}$. The RO module of the EHS is used to design the aging sensor along with the circuit level modification proposed in [17], where one RO becomes heavily stressed and the other one is less stressed. The frequency difference i.e. F_{DIF}= F_{REF}-F_{STR}, is used for both registration and authentication purposes [17], [30]. The authentication process in this EHS is discussed as follows:

- For a fresh IC, F_{DIF} is approximately zero because both the ROs designed to oscillate at the same frequency. However, due to PV, there exists a very less frequency difference, which leads to a finite value.
- When the IC is idle (powered ON), $(RO)_{STR}$ undergoes NBTI stress by the control module, and at the same time, the $(RO)_{REF}$ is isolated from the supply to make it stress-free [30].
- As a result, NBTI causes the degradation in the oscillation frequency of $(RO)_{STR}$ and increases with an increase in stress duration i.e., if that particular IC used continuously.
- However, at the same time, the absence of NBTI stress does not affect the oscillation frequency of $(RO)_{REF}$.
- This variation in NBTI stress leads to an increase in the magnitude of F_{DIF}. The magnitude of F_{DIF} is used to predict the duration for which the IC under test is used. The flow to determine aging of an IC is depicted in Fig. 11, and is self explanatory.

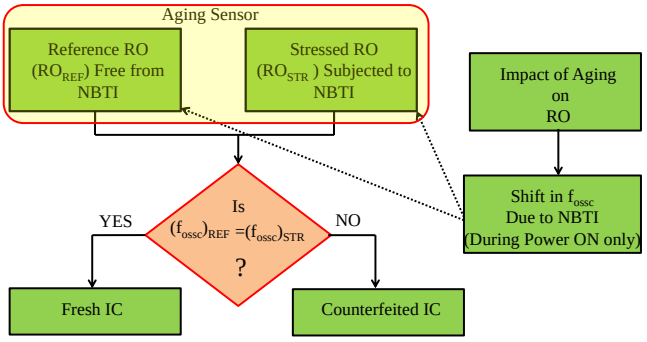


Fig. 11: Flow of Aging Determination.

D. EHS with On-chip Security

The security of the IC is an important criterion, as the EHS chip after fabrication has to deploy in different places. The IC may be forged and can be sold illegally in the market. To make our EHS secure, we have used an added security feature for RO and MPPT. PUF triggers the security feature. As discussed in [30], [31], PUF is one of the most promising security features and generate the unclonable key from the inherent manufacturing PV. In our system, an RO-PUF is used to enable the ring oscillator of EHS and Latch-PUF is used to trigger the MPPT module. The reason to use the RO-PUF, and Latch-PUF is evident, because these PUFs can be designed from the existing modules of EHS, which indicates that the area overhead due to additional PUF module can be lowered. Both the PUFs are designed to generate a 128-bit secret key, which is used to trigger the different modules of EHS. Further, due to the unclonability property of PUF, it is impossible to generate the secret key by the adversary. The reason to use PUF is to have higher security in the EHS. The basic circuit diagram of RO-PUF [16], [31] is shown in Fig. 12.

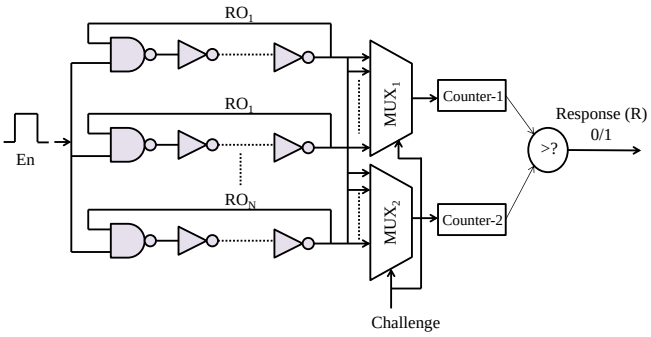


Fig. 12: RO−PUF

The first stage security is for the EHS to ON through appropriate cryptographic key generated by the RO-PUF with suitable control logic. The second stage of protection of the EHS is in the MPPT procedure, where the Latch-PUF makes a key which will decide whether the MPPT circuit is accessed or not. The Latch-PUF reuses the resources like D-latches used in the MPPT decision circuit, to save area in our design. The key from Latch-PUF, if incorrect, then the MPPT procedure is bypassed, and EHS runs without MPPT, thereby degrading the EHS performance. The chip, if forged, then the EHS chip is not ON in the first stage of the security level. If due to some adverse and extreme conditions, the first stage security fails, the second stage security will not make the MPPT circuitry ON.

The RO-PUF generates the 128-bit key and passed to the control logic for the generation of PUF_EN_{out}. When the environmental sensor S=1, indicating the requirement of MPPT, then the second PUF output $Latch\_PUF_{out}$ is evaluated. The algorithm for the first stage and second stage security is presented in Fig. 13, that indicates the authentication process.

The FSM is shown in Fig. 14 depicts the second stage of security for MPPT circuitry along with associated control signals.

VI. Hardware Design and Characterization of the Proposed Thing

The proposed Eternal-Thing has been designed and fabricated using CMOS 90nm technology library. Virtuoso analog design environment (ADE) used for the simulation. The input solar cell voltage is between 1-1.5 V concerning a solar panel of $2.5mm^2$. The load for the EHS is designated with a 200 kΩ resistor and a 33mf supercapacitor. The MIM (Metal-Insulator-Metal) type capacitors used for the DC-DC converter and digital capacitor banks. The die photograph of the chip sent for fabrication is depicted in Fig. 16.

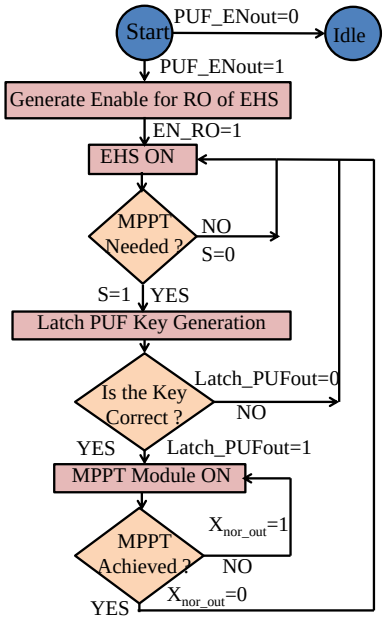


Fig. 13: Flow chart indicating the security level using PUFs.

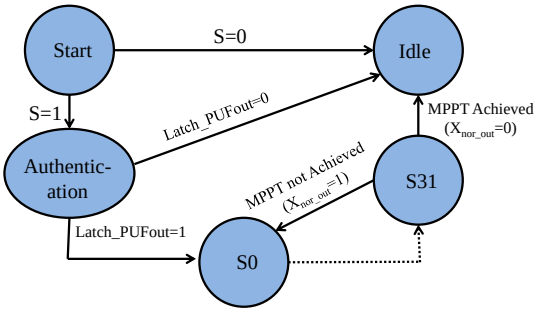
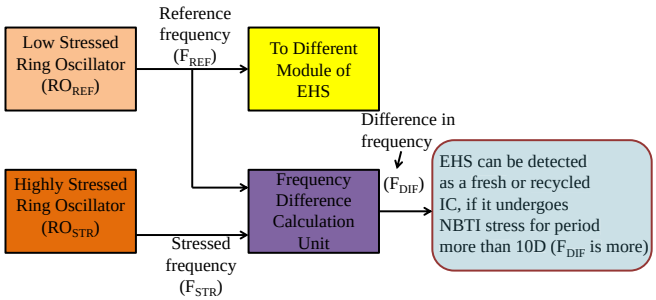


Fig. 14: FSM for MPPT with Latch-PUF control

A. Analysis of Metrics of the Proposed PUF

The CRPs are collected from both RO-PUF and Latch-PUF using Monte Carlo simulations in CMOS 90nm technology and proceed for further investigation to analyze various PUF metrics. Monte Carlo simulation uses a statistical transistor model provided by the foundry with a 3σ variation. The key



* Increase in Stress for Aging is Through Negative Bias Temperature Instability (NBTI).

Fig. 15: Proposed aging sensor

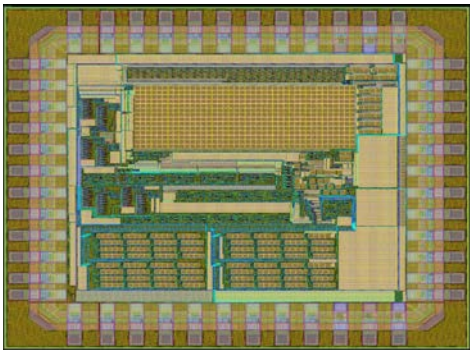


Fig. 16: Die photograph of the secure EHS chip.

PUF metrics measured from CRPs are discussed as follows:

1) Uniqueness: This is a measure for inter-chip [30] variation. It is a criterion to check PUFs ability to distinguish a specific chip among multiple chips. An ideal PUF possess a uniqueness of 50%. Higher the value of the uniqueness of PUF, better is its ability for authentication. The uniqueness is measured using the following expression [31]:

$$Uniqueness = \frac{2}{C(C-1)} \sum_{i=1}^{C-1} \sum_{j=i+1}^{C} \frac{HD(S_i, S_j)}{m} \times 100\%, \quad (8)$$

where S_i and S_j are the responses obtained from PUF (i and j), m= Number of bit in the response, HD=Hamming distance between any two responses and is given by the following expression:

$$HD(S_i, S_j) = \sum_{t=1}^{m} (S_{i,t} \oplus S_{j,t}). \quad (9)$$

In the above expression, $S_{i,t}$ is the t^{th} response bit of the m-bit response strings of PUF_i.

2) Reliability: It is a measure of inter-chip variation. PUF can reproduce response bit against environmental variables like temperature, supply voltage, noise, etc. An ideal PUF must possess the reliability of 100%. Due to environmental variations, some response bits in the collected CRPs gets flipped, which leads to degradation in the reliability of PUF. The reliability [30] is measured using the following expression:

$$Reliability = 100\% - \frac{1}{x} \sum_{y=1}^{x} \frac{HD(S_i, S_{i,y}')}{m} \times 100\%. \quad (10)$$

In the above expression, $S_{i,y}$ is the y^{th} sample of S_i.

To measure the above PUF metrics, PV dependent CRPs are extracted from both RO-PUF and Latch-PUF and are reported in Table IV. For analysis, we have used the recently proposed area-efficient configurable ring oscillator PUF [30] and the conventional Latch-PUF [31] is designed using D-latch. The extracted CRPs possess better uniqueness and higher reliability. Both the PUFs designed using the available RO and D-Latch in the EHS module facilitates area efficient chip design. The methodology proposed in [31] used to measure uniqueness and reliability. 100 different instantiation of the PUF is created through Monte Carlo simulation. To measure the uniqueness, HD (hamming distance) between the response

collected from the different instantiations of the same chip, to a particular challenge, and the corresponding value is shown in Table IV. The reliability degradation due to flip in response bit collected from the same instances at different room temperature (measured by varying the temperature from 0 to 100 °C). The extracted CRPs possess better uniqueness and higher reliability. Both the PUFs possess better quality metrics as mentioned in Table IV. As a result, the extracted 128-bit key from the PUF becomes more secure and reliable for IC authentication.

TABLE IV: Analysis of PUF metrics

PUF metrics	C-CRO PUF	Latch-PUF	Ideal Value
Uniqueness	46.25%	46.08%	50%
Reliability	95.33%	95.855%	100%

B. Power Consumption Characterization

Fig. 17 depicts the power consumption by the individual module. Among all modules, the primary power-consuming modules are RO and current sensor, which consume 80% of total power. The continuous oscillating mode of RO is responsible for its higher power consumption. The periodic ON/OFF of the current sensor by FSM saves power as compared to the techniques, where it is always ON. The total power consumed by the EHS is 22μW (which is $<$ 1 mW), which satisfies that the harvesting system is designed for ultra-low-power IoT requirements. The security using PUFs and aging sensor features included in the harvesting system consuming a small amount of power. This power consumption is reasonable for secure EHS and is under the ultra-low-power range.

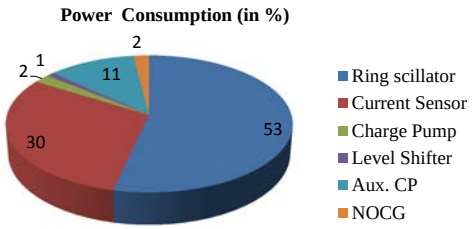


Fig. 17: Power consumption (in %) by each unit in the EHS.

VII. Experimental Results

A. Experimental Setup

The PV dependent 128-bit secure key from the security module (RO-PUF and Latch-PUF) are extracted using Monte Carlo simulation. This technique uses a statistical transistor model provided by the foundry with a 3σ variation. Further, the Relxpert simulator in ADE used to measure the reliability degradation of RO due to aging.

B. Results and Discussion

The key from the RO-PUF used to trigger the RO of EHS once it is powered ON. The subsequent operation, once the RO-PUF enables the EHS, is shown in Fig. 18a, Fig. 18b, and Fig. 18c.

The simulation results in Fig. 18a depicts,

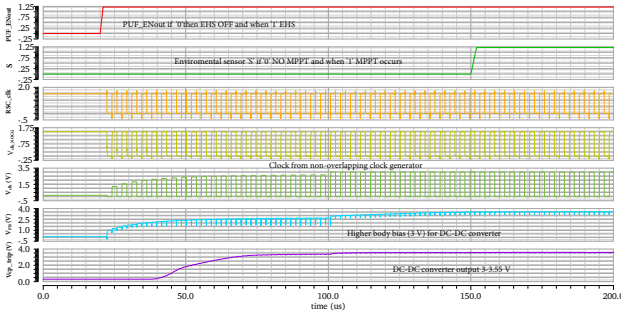
- The PUF_EN_{out}=0 makes the SEHS OFF, as the ring oscillator (RO) is disabled, so clock signals are not generated (as shown by green lines) and the converter output is zero (as shown by violet line in V_{cp_trip}).
- The PUF_EN_{out}=1, RO is enabled thereby generating clocks and makes the SEHS to be ON and the converter output (V_{cp_trip}) starts rising and reaches to 3-3.55V due to boosting of input solar voltage.
- The auxiliary charge pump uses two non-overlapping clocks ($V_{clk-NOCG}$) to generate the required body bias V_{PB} of 3V (as depicted by light blue line) for the converter.
- The environmental sensor S initiates the MPPT operation. Simulation result shows that when S is Low for 150μS; SEHS runs without MPPT. When S is High, MPPT process starts in SEHS.

The simulation results in Fig. 18b depicts,

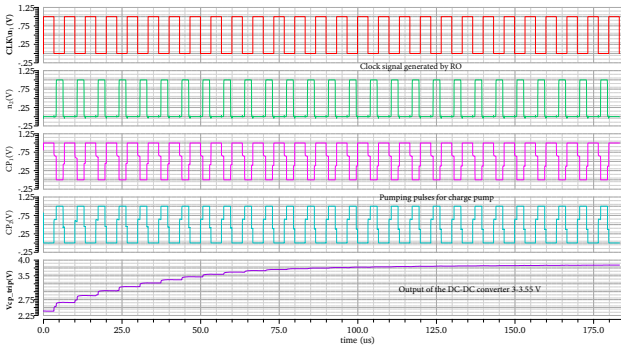
- The required clock signal $(CLK/n_1/RSC\_clk)$ is generated from RO for self-sustainable operation of EHS.
- The clock signal n_2 is generated from n_1 by adding appropriate delays to achieve a non-overlapping signal with n_1.
- The generation of the pumping clocks CP_1 and CP_2 for the converter is achieved by processing n_1 and n_2 through tri-state drivers and NOR gate.
- The converter generates output voltage of V_{cp_trip}=3-3.55 V with CP_1 and CP_2 as pumping clocks.

The detail operation of the MPPT procedure, once enabled by an environmental sensor/timer (S) and Latch-PUF after 150μS, is discussed in Fig. 18c. The Latch-PUF will generate a 128-bit secret key. The secret key, if correct, then the control circuit activates the MPPT procedure if S=1. The secret key, if not matched, then the MPPT circuitry is not accessed, and no MPPT occurs. The sequence of operations, once the MPPT is triggered, is depicted in Fig. 18c.

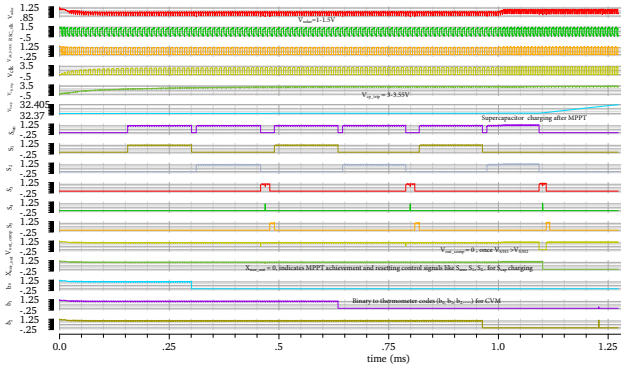
- The simulation results in Fig. 18c shows the control signals needed for the MPPT procedure are generated by the FSM controller after 150μS i.e. current sensing signal (S_{sen}), enable signal for S/H_1 and S/H_2 circuits (S_1 and S_2), comparator signal (S_3), decision signal (S_4) and finally S_5 for external WSNs.
- The period when S_{sen} is Low (specifically, for first 150μS and after MPPT achievement) is marked by violet line in Fig. 18c, the output of the converter supplied to supercapacitor and computational load, and the output of the current sensor V_{sen} is zero (as no sensing occurs in that period).
- The period when S_{sen} is High (after 150μS in Fig. 18c), the output of the converter is sensed by current sensor as V_{sen}. The V_{sen} represents the power at the output of the converter.
- The output of current sensor (V_{sen}) is sensed during MPPT procedure, and power information P_n and P_{n+1} are stored as V_{out1} and V_{out2} in S/H_1 and S/H_2.



(a) Simulation result for generation of V_{SB}



(b) RO and Pumping clocks with converter output



(c) Simulation result of EHS with different control signals with MPPT achievement

Fig. 18: Simulation results of secure SEHS with MPPT achievment.

- The simulation results in Fig. 18c shows the control signals S_1 and S_2 are High for 14-clock cycle each to enable S/H_1 and S/H_2 to store the V_{out1} and V_{out2}.
- The thermometer bits (b_0-b_{15}) generated by the FSM controller are initially High and become Low at 15^{th} clock cycle (between S_1 and S_2) one by one at every MPPT cycle for CVM.
- During CVM, the S_{sen} is again Low (where no sensing occurs), such that V_{out2} is sensed with a different voltage and is stored in S/H_2 after 15^{th} clock cycle.
- The two power information stored in S/H_1 and S/H_2 are compared in a comparator, when S_3 is High (as depicted in simulation result by red line in Fig. 18c). The S_{sen}, S_1, and S_2 are driven to Low till end of MPPT cycle for comparing the stored information. The output of the comparator V_{out_comp} is initially High.
- The number of MPPT cycles needed can be tracked by each transition of S_1 (S_2) from Low to High (one transition indicates one MPPT cycle) in the simulation result.
- In the simulation result shown in Fig. 18c, at the initial two MPPT cycles (32-clocks each) it is found that $P_n < P_{n+1}$ during comparison (S_3 High) of S/H_1 and S/H_2, the output of the comparator (V_{out_comp}) is maintained High (MPP not achieved).
- In the third MPPT cycle, it is observed that the $P_n > P_{n+1}$, as a result the output of the comparator (V_{out_comp}) becomes Low as depicted in Fig. 18c.
- The XNOR output (X_{nor_out} become High upon reset) switches from High to Low indicates the achievement of MPPT else MPPT is not achieved.
- In the simulation result shown in Fig. 18c, as the X_{nor_out} switches to zero (presented in green line), it resets all the control signals (S_{sen}, S_1, S_2, S_3, etc.,) and makes the S_{sen} to be Low, such that the harvesting system again continues to charge the supercapacitor (V_{scap}) and supply the computational load. The charging of the supercapacitor is shown in Fig. 18c by V_{scap} once the MPP is achieved.
- The same process gets repeated during further MPPT requirements.

The simulation results reveal that, once MPP is achieved, the MPPT process ceases and continues to regular operation until the next MPPT requirement. In the simulation result shown in Fig. 18c, after three consecutive MPPT cycles, the MPP is achieved. The EHS now charges the supercapacitor and supply to the computational load till further MPPT requirement as per the environmental sensor S.

The secure PV-EHS designed, is compared with the other state of art solar EHS in Table V. The EHS designed for temperature sensors and wireless trans-receivers that are consuming maximum power within the ultra-low-power range.

VIII. Conclusions and Future Directions

The failure of sensor nodes in the IoT is a catastrophic situation. The denial of supply attack may cause information loss in IoT. To identify the recycled IC and secure the EHS (energy harvesting system) IC is a challenge. Keeping these facts into consideration, the proposed secure self-sustainable solar EHS is a state of art technology outcome towards clean energy and handling IoT edge node devices in smart cities and other related applications. The secure solar EHS has inbuilt PUFs (two-stage security mechanism) for securing the IC. The aging sensor in the chip will help in identifying the recycled EHS chips. The higher bias voltages required are generated on-chip, such that no external bias is needed. The secure self-sustainable solar energy harvesting system (solar-EHS) designed is well suited for a minimum voltage of 1.22 V as MPP in the range of 1-1.5 V. The resulting output is in the range of 3-3.55 V, which is the requirement of many IoT edge node devices. The proposed secure EHS is consuming $22\mu W$ of power and is within the ultra-low-power range. The future directions of this research are (a) the converters used for power conditioning has some ripples within tolerable range

TABLE V: Comparison of different low energy solar harvesting systems

Works	**Feature/ Characteristics**							
	Technology	Fully Integrated	Self-Sustaining	Input Range (V)	Output Range (V)	Power Throughput (μW)	Aging Tolerant Mechanism	Security Features Incorporated
Shao, et al. [11]	350nm	Yes	No	2.1-3.5	3.6-4.4	100-775	No	No
Kim, et al. [12]	350nm	Yes	No	1-2.7	2	0-80	No	No
Qian, et al. [36]	250nm	No	Yes	0.5-2	0-5	5-1000	No	No
Shih, et al. [18]	130nm	Yes	Yes	1.8	1.4	< 10	No	No
Kim, et al. [15]	350nm	No	Yes	1.5-5	0-4	800	No	No
Liu, et al. [33]	180nm	Yes	Yes	1-1.5	3-3.5	0-29	No	No
Current Paper	90nm	Yes	Yes	1-1.5	3-3.55	0-22	**Yes**	**Yes**

at the output due to the switching mechanism involved for boosting. The smart node has to act for years or tens of years, so aging can increase the ripples content at the output, which may affect the rechargeable battery/supercapacitor operation. A proper aging analysis of the secure EHS can be addressed. (b) The sensors used in IoT has different supply requirement, and by using adequate power management techniques, various power supplies can be generated further.

ACKNOWLEDGMENTS

This research work is supported by Special Manpower Development Program for Chips to System Design (SMDP-C2SD) of Government of India.

REFERENCES

[1] S. P. Mohanty, U. Choppali, and E. Kougianos, "Everything You wanted to Know about Smart Cities: The Internet of Things is the backbone," *IEEE Consumer Electronics Magazine*, vol. 5, no. 3, pp. 60–70, July 2016.

[2] G. Rostirolla, R. da Rosa Righi, J. L. V. Barbosa, and C. A. da Costa, "ElCity: An elastic multilevel energy saving model for smart cities," *IEEE Transactions on Sustainable Computing*, vol. 3, no. 1, pp. 30–43, 2017.

[3] P. Sundaravadivel, E. Kougianos, S. P. Mohanty, and M. K. Ganapathiraju, "Everything you wanted to know about smart health care: Evaluating the different technologies and components of the Internet of Things for better health," *IEEE Consumer Electronics Magazine*, vol. 7, no. 1, pp. 18–28, 2017.

[4] B. Ji, B. Xing, K. Song, C. Li, H. Wen, and L. Yang, "The efficient BackFi transmission design in ambient backscatter communication systems for IoT," *IEEE Access*, vol. 7, pp. 31 397–31 408, 2019.

[5] T. Wang, Y. Li, G. Wang, J. Cao, M. Z. A. Bhuiyan, and W. Jia, "Sustainable and efficient data collection from WSNs to cloud," *IEEE Transactions on Sustainable Computing*, vol. 4, no. 2, pp. 252–262, April 2017.

[6] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, September 2013.

[7] U. Guin, K. Huang, D. DiMase, J. M. Carulli, M. Tehranipoor, and Y. Makris, "Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1207–1228, 2014.

[8] X. Liu and E. Sánchez-Sinencio, "A highly efficient ultralow photovoltaic power harvesting system with MPPT for internet of things smart nodes," *IEEE Transactions on Very Large Scale Integration (VLSI) systems*, vol. 23, no. 12, pp. 3065–3075, 2015.

[9] Y. K. Ramadass and A. P. Chandrakasan, "A battery-less thermoelectric energy harvesting interface circuit with 35 mV startup voltage," *IEEE Journal of Solid-State Circuits*, vol. 46, no. 1, pp. 333–341, 2011.

[10] S. Carreon-Bautista, A. Eladawy, A. N. Mohieldin, and E. Sánchez-Sinencio, "Boost converter with dynamic input impedance matching for energy harvesting with multi-array thermoelectric generators," *IEEE Transactions on Industrial Electronics*, vol. 61, no. 10, pp. 5345–5353, 2014.

[11] H. Shao, C.-Y. Tsui, and W.-H. Ki, "The design of a micro power management system for applications using photovoltaic cells with the maximum output power control," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 17, no. 8, pp. 1138–1142, 2009.

[12] J. Kim, J. Kim, and C. Kim, "A regulated charge pump with a low-power integrated optimum power point tracking algorithm for indoor solar energy harvesting," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 58, no. 12, pp. 802–806, 2011.

[13] C. Lauterbach, W. Weber, and D. Romer, "Charge sharing concept and new clocking scheme for power efficiency and electromagnetic emission improvement of boosted charge pumps," *IEEE Journal of solid-state circuits*, vol. 35, no. 5, pp. 719–723, 2000.

[14] S. Mondal and R. Paily, "On-chip photovoltaic power harvesting system with low-overhead adaptive MPPT for IoT nodes," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1624–1633, 2017.

[15] H. Kim, S. Kim, C.-K. Kwon, Y.-J. Min, C. Kim, and S.-W. Kim, "An energy-efficient fast maximum power point tracking circuit in an 800-μW photovoltaic energy harvester," *IEEE Transactions on Power Electronics*, vol. 28, no. 6, pp. 2927–2935, 2013.

[16] M. T. Rahman, F. Rahman, D. Forte, and M. Tehranipoor, "An aging-resistant RO-PUF for reliable key generation," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 3, pp. 335–348, 2016.

[17] X. Zhang and M. Tehranipoor, "Design of on-chip lightweight sensors for effective detection of recycled ICs," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 22, no. 5, pp. 1016–1029, 2014.

[18] Y.-C. Shih and B. P. Otis, "An Inductorless DC–DC Converter for Energy Harvesting With a 1.2 μW Bandgap-Referenced Output Controller," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 58, no. 12, pp. 832–836, 2011.

[19] A. Mosenia and N. K. Jha, "A comprehensive study of security of internet-of-things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586–602, 2016.

[20] C. Perera, C. H. Liu, and S. Jayawardena, "The emerging internet of things marketplace from an industrial perspective: A survey," *IEEE Transactions on Emerging Topics in Computing*, vol. 3, no. 4, pp. 585–598, 2015.

[21] M. Bond and J.-D. Park, "Current-sensorless power estimation and MPPT implementation for thermoelectric generators," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 9, pp. 5539–5548, 2015.

[22] Y. Qiu, C. Van Liempd, B. O. het Veld, P. G. Blanken, and C. Van Hoof, "5μW-to-10mW Input Power Range Inductive Boost Converter for Indoor Photovoltaic Energy Harvesting with Integrated Maximum Power Point Tracking Algorithm," in *Proceedings of the IEEE International Solid-State Circuits Conference*, 2011, pp. 118–120.

[23] A. Omairi, Z. H. Ismail, K. A. Danapalasingam, and M. Ibrahim, "Power harvesting in wireless sensor networks and its adaptation with maximum power point tracking: Current technology and future directions," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2104–2115, 2017.

[24] Y. Sun, Z. Yuan, Y. Liu, X. Li, Y. Wang, Q. Wei, Y. Wang, V. Narayanan, and H. Yang, "Maximum energy efficiency tracking circuits for converter-less energy harvesting sensor nodes," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 64, no. 6, pp. 670–674, 2017.

[25] H. A. Sher, A. A. Rizvi, K. E. Addoweesh, and K. Al-Haddad, "A single-stage stand-alone photovoltaic energy system with high tracking efficiency," *IEEE Transactions on Sustainable Energy*, vol. 8, no. 2, pp. 755–762, 2017.

[26] M. J. D. Huab, L. P. Alarcón, C. V. J. Densing, R. J. M. Maestro, M. D. Rosales, and M. T. G. de Leon, "Implementation of a maximum power point tracking system and an LDO regulator for interface circuits of

solar energy harvesters for wireless sensor nodes," in *Proceedings of the IEEE Region 10 Conference (TENCON)*, 2017, pp. 203–202.
[27] T. Ozaki, T. Hirose, H. Asano, N. Kuroki, and M. Numa, "Fully-integrated high-conversion-ratio dual-output voltage boost converter with MPPT for low-voltage energy harvesting," *IEEE Journal of Solid-State Circuits*, vol. 51, no. 10, pp. 2398–2407, 2016.
[28] D. C. Huynh and M. W. Dunnigan, "Development and comparison of an improved incremental conductance algorithm for tracking the MPP of a solar PV panel," *IEEE Transactions on Sustainable Energy*, vol. 7, no. 4, pp. 1421–1429, 2016.
[29] X. Liu, K. Ravichandran, and E. Sánchez-Sinencio, "A switched capacitor energy harvester based on a single-cycle criterion for MPPT to eliminate storage capacitor," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 65, no. 2, pp. 793–803, 2018.
[30] S. R. Sahoo, S. Kumar, and K. Mahapatra, "A novel configurable ring oscillator PUF with improved reliability using reduced supply voltage," *Microprocessors and Microsystems*, vol. 60, pp. 40–52, 2018.
[31] V. P. Yanambaka, S. P. Mohanty, and E. Kougianos, "Making use of manufacturing process variations: A dopingless transistor based-PUF for hardware-assisted security," *IEEE Transactions on Semiconductor Manufacturing*, vol. 31, no. 2, pp. 285–294, 2018.
[32] A. Taherin, M. Salehi, and A. Ejlali, "Reliability-aware energy management in mixed-criticality systems," *IEEE Transactions on Sustainable Computing*, vol. 3, no. 3, pp. 195–208, 2018.
[33] X. Liu and E. Sánchez-Sinencio, "An 86% efficiency 12 μW self-sustaining PV energy harvesting system with hysteresis regulation and time-domain MPPT for IOT smart nodes," *IEEE Journal of Solid-State Circuits*, vol. 50, no. 6, pp. 1424–1437, 2015.
[34] B. P. Baddipadiga and M. Ferdowsi, "A high-voltage-gain DC-DC converter based on modified dickson charge pump voltage multiplier," *IEEE Transactions on Power Electronics*, vol. 32, no. 10, pp. 7707–7715, 2017.
[35] A. Khorami and M. Sharifkhani, "Low-power technique for dynamic comparators," *Electronics Letters*, vol. 52, no. 7, pp. 509–511, 2016.
[36] Y. Qian, H. Zhang, Y. Chen, Y. Qin, D. Lu, and Z. Hong, "A SIDIDO DC–DC converter with dual-mode and programmable-capacitor-array MPPT control for thermoelectric energy harvesting," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 64, no. 8, pp. 952–956, 2017.
[37] S. K. Ram, S. R. Prusty, P. K. Barik, K. Mahapatra, and B. Subudhi, "FPGA implementation of digital controller for active power line conditioner using SRF theory," in *Proceedings of the 10th International Conference on Environment and Electrical Engineering*, 2011, pp. 1–5.
[38] S. K. Ram and B. B. Das, "Comparison of different control strategy of conventional and digital controller for active power line conditioner (APLC) for harmonic compensation," in *Proc. 12th International Conference on Environment and Electrical Engineering*, 2013, pp. 209–214.

Saswat Kumar Ram (S'14) received the professional degree in Electronics and Telecommunication Engineering from Biju Patanaik University of Technology, India in 2005, the M.Tech degree in VLSI Design and Embedded systems from NIT, Rourkela, India in 2011. He is currently Pursuing the Ph.D. degree in Electronics and communication engineering at NIT, Rourkela, India. His current research interest includes energy harvesting for IoT, low power VLSI design, embedded systems, Hardware security, signal processing, machine learning.

Sauvagya Ranjan Sahoo (S'18) received the engineering degree (EN&TC) from DRIEMS, Odisha in 2006. In 2012, he obtained his M.Tech in VLSI Design & Embedded Systems from National Institute of Technology, Rourkela, Odisha. In 2019, he obtained his Ph.D. in Electronics and Communication Engineering from National Institute of Technology, Rourkela. His main research interests include low power CMOS VLSI circuit design, Hardware security.

Banee Bandana Das (S'19) received the professional degree in Computer Science Engineering from Biju Patanaik University of Technology, India in 2010, the M.Tech degree from from Biju Patanaik University of Technology, India in 2012. She is currently Pursuing the Ph.D. degree in computer science engineering in NIT, Rourkela, India. Her current research interest includes machine learning, computer vision, neural network and computational intelligence, Internet-of-Things.

Kamalakanta Mahapatra (M'12) obtained his B. Tech degree with Honours from Regional Engineering College, Calicut in 1985, M. Tech from Regional Engineering College, Rourkela in 1989 and Ph. D. from IIT Kanpur in 2000. He is currently a Professor in Electronics and Communication Engineering Department of National Institute of Technology (NIT), Rourkela. He assumed this position since February 2004. He is a fellow of the institution of Engineers (India) in ECE Division. He has published several research papers in National and International Journals. His research interests include Embedded Computing Systems, VLSI Design, Hardware Security and Industrial Electronics.

Saraju P. Mohanty (SM'08) received the bachelor's degree (Honors) in electrical engineering from the Orissa University of Agriculture and Technology, Bhubaneswar, in 1995, the masters degree in Systems Science and Automation from the Indian Institute of Science, Bengaluru, in 1999, and the Ph.D. degree in Computer Science and Engineering from the University of South Florida, Tampa, in 2003. He is a Professor with the University of North Texas. His research is in "Smart Electronic Systems" which has been funded by National Science Foundations (NSF), Semiconductor Research Corporation (SRC), U.S. Air Force, IUSSTF, and Mission Innovation. He has authored 300 research articles, 4 books, and invented 4 U.S. patents. His Google Scholar h-index is 35 and i10-index is 129 with 5400+ citations. He has over 20 years of research experience on security and protection of media, hardware, and system. He introduced the Secure Digital Camera (SDC) in 2004 with built-in security features designed using Hardware-Assisted Security (HAS) or Security by Design (SbD) principle. He is widely credited as the designer for the first digital watermarking chip in 2004 and first the low-power digital watermarking chip in 2006. He was a recipient of 12 best paper awards, IEEE Consumer Electronics Society Outstanding Service Award in 2020, the IEEE-CS-TCVLSI Distinguished Leadership Award in 2018, and the PROSE Award for Best Textbook in Physical Sciences and Mathematics category from the Association of American Publishers in 2016 for his Mixed-Signal System Design book published by McGraw-Hill. He has delivered 9 keynotes and served on 5 panels at various International Conferences. He has been serving on the editorial board of several peer-reviewed international journals, including IEEE Transactions on Consumer Electronics (TCE), and IEEE Transactions on Big Data (TBD). He is the Editor-in-Chief (EiC) of the IEEE Consumer Electronics Magazine (MCE). He has mentored 2 post-doctoral researchers, and supervised 11 Ph.D. dissertations and 26 M.S. theses.