Solar Cell Based Physically Unclonable Function for Cybersecurity in IoT Devices

S. Dinesh Kumar, Carson Labrado, Riasad Badhan, Himanshu Thapliyal, and Vijay Singh
Department of Electrical and Computer Engineering
University of Kentucky, Lexington, KY, USA

***Abstract*—Internet of Things (IoT) devices are mostly small and operate wirelessly on limited battery supply, and therefore have stringent constraints on power consumption and hardware resources. Therefore, energy-efficient (low energy) design is paramount for the successful deployment of resource constrained IoT devices. Further, Physical Unclonable Functions (PUFs) have evolved as a popular hardware security primitive for low cost, mass produced IoT devices with very constrained resources. Energy harvesting technologies utilizing solar cells are being used in ultra-low power IoT devices to satisfy the energy requirement. In this paper, we utilize the intrinsic variations in solar cells to design a novel solar cell based PUF. As a proof of concept, we have used the Tiva TM4C123GH6PM microcontroller to build our solar cell based PUF. From our experiments, we found that the proposed solar cell based PUF has the uniformity value of 49.21% which is close to the ideal value of 50%. Further, the proposed solar cell based PUF has worst case reliabilities of 92.97% and 90.62% with variations in temperature and light intensity, respectively.**

I. Introduction

The Internet of Things (IoT) is a network of machines, physical objects, and other devices that are connected through the Internet to exchange data for intelligent applications [1]. One of the main advantages of the IoT environment is that IoT allows the direct integration between physical objects and the digital world which helps to improve the quality of human life. Within the past decade, there have been numerous IoT devices introduced in the market. It is expected that more than 50 billion IoT devices will connect with each other by 2021 [2]. Generally, IoT devices are small and operate wireless on limited battery supply. Therefore, they have stringent constraints on power consumption and hardware resources.

Although there are numerous methods to achieve energy efficiency, the recent technology trend of energy harvesting provides a fundamental method to prolong battery life. Thus, energy harvesting is a promising approach to improve energy efficiency in IoT devices [3]. Though there are several energy harvesting modalities, solar energy harvesting through photovoltaic conversion provides the highest power density, which makes it an ideal choice to power a low power IoT device as illustrated in Fig. 1 [4]. Solar energy could allow IoT devices to be powered indefinitely without battery replacement. For example, Alta Devices has developed an extremely light weight, flexible and thin Gallium Arsenide (GaAs) solar cell with and efficiency of 28.8% [5].This type of solar cells can be integrated into the IoT devices as the energy source thereby increasing the time between battery replacements or possibly never depending on the life and the efficiency of the solar cells.

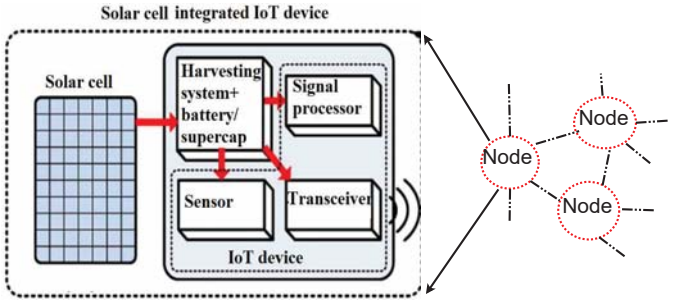

Fig. 1. IoT system with solar cell based IoT devices at each nodes

Along with the energy-efficiency, IoT devices also provide challenges in privacy and security. Among the various security needs for IoT devices, authentication and access control are one of the most important features of the IoT that needs to be implemented [6]. Currently, the secret keys which are used for authentication are stored in non-volatile memories. But these keys are vulnerable to active attacks [7], [8]. Moreover, implementing tamper resistant circuitry in IoT devices to provide high level physical security may be very expensive in terms of cost and energy. In recent years, Physically Unclonable Functions (PUFs) have evolved as one of the popular hardware security primitives for low cost, mass produced IoT devices with very constrained resources (battery driven, very small volatile and persistent memory, and low processor power).

Lately, silicon PUF have emerged as a powerful solution to a variety of security concerns such as IC piracy, IC counterfeiting, etc. [9]. PUFs also play a major role in secure authentication and key management in cyber-physical security and IoT devices [10]. PUFs can also be considered as a promising solution for authentication in IoT devices [11]. 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. 2 shows the block diagram for PUF production using inherent variations. In this manner, a PUF can be considered as a fingerprint for CMOS ICs.

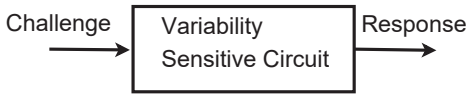

Fig. 2. PUF production using inherent variations

A. Motivation

PUFs are a class of circuits that use the inherent variations in the device manufacturing process to create unique and unclonable IDs. The existing CMOS IC based PUF requires dedicated hardware which results in additional hardware cost and power consumption. In recent years, solar cells have been integrated with IoT devices for various purposes such as power generation and sensing applications. The main motivation of this paper is to design a solar cell based PUF with minimum hardware cost suitable for implementation in IoT devices. In the proposed PUF, solar cell array acts not only as a power generator, but also as an entropy source for generating the secret bits. To the best of our knowledge, this is the first kind of work to integrate the solar cells along with IoT devices for designing a PUF to generate the unique IDs. Our proposed solar cell based PUF fall under the category of energy harvesting based PUFs.

B. Contribution of the paper

A novel architecture to build a solar cell based PUF is proposed in this paper. The proposed solar cell based PUF is built using a Tiva TM4C123GH6PM micro-controller. The challenge for our proposed PUF will be the selection of solar cells through the microcontroller and the response bits will be the V_{oc} comparison bits of the micro-controller. We also develop an algorithm to effectively choose the V_{oc} of the solar cells to generate a 128 bit response. This algorithm can also be used to generate a higher number of response bits. Further, the security metrics of the proposed PUF such as uniformity, reliability against temperature variations and reliability against light intensity variations are also presented in this paper.

C. Organization of the paper

Section II discusses the background on PUF and solar cells. Section III describes the design parameter chosen to design the solar cell based PUF. Section IV presents the architecture of the proposed solar cell based PUF. Section V presents the implementation details of the solar cell based PUF. Section VI discusses the security metric results of the solar cell based PUF. Section VII provides discussion and conclusion of the paper.

II. BACKGROUND

A. Physical Unclonable Function

PUFs are a class of circuits that use the inherent variations in the Integrated Circuit (IC) manufacturing process to create unique and unclonable IDs (Fig. 2). PUFs hold the potential to simplify or solve many important security problems such as IC piracy, IC counterfeiting, secure authentication and key management in IoT security. Further, object authentication is of utmost importance in businesses that are threatened by counterfeited devices. PUFs can't be cloned or copied and could be used to identify products unambiguously to avoid counterfeiting. PUFs have the potential to seal multiple types of vulnerabilities in IoT devices specifically in the security classes of authentication, non-repudiation, and privacy. Silicon PUFs utilizes the uncontrollable manufacturing variations in IC to generate the unique bits. Some of the examples of silicon PUFs include arbiter PUF [12], Ring Oscillator (RO) [13], SRAM PUF [14], etc.

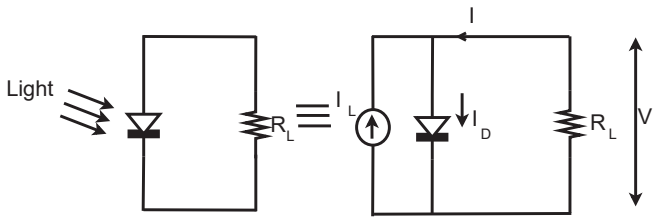

Fig. 3. Equivalent circuit of a photovoltaic solar cell

B. Solar cell

Solar cells are considered a major candidate for obtaining energy from the light source, since they can convert light directly to electricity with high conversion efficiency. They can provide nearly permanent power at low operating cost, and are virtually free of pollution. A solar cell is a device which converts light into electricity. Light shining on the solar cell produces both a current and a voltage. This process requires a material to absorb light and raise electrons to a higher energy state, and transport this higher energy electron from the solar cell into an external circuit. Then, electrons dissipate their energy in the external circuit and return to the solar cell. Photovoltaic energy conversion often uses semiconductor materials and inorganic-organic materials in the form of a p-n junctions (Refer Fig. 3). Recently, solar cells have been used in IoT devices to improve the energy-efficiency [15]. [16], [17] have explored their usefulness for designing PUFs. However, [16], [17] have used the light source as the challenge which makes the PUF relatively unreliable and make them unsuitable to implement in real world IoT devices.

III. PARAMETERS TO DESIGN SOLAR CELL PUF

There are several electrical parameters which can be used to design the solar cell based PUF. However, for reliability, the chosen parameters must have a predictable relationship with the variation in environmental parameters to design a reliable PUF. In this section, we discuss the parameter with which we have chosen to design a reliable solar cell based PUF.

There are two important and easily measurable electrical parameters which define the characteristics of solar cells. These are the short circuit current (I_{sc}) and the open circuit

voltage (V_{oc}). The fundamental current-voltage (I-V) equation of a solar cell is,

$$I = I_0[exp(\frac{qV}{\eta KT} - 1)] - I_L \quad (1)$$

where I_0 is the reverse saturation current, η is diode ideality factor, I_L is light generated current, K is plank's constant and T is temperature. The short circuit current (I_{sc}) is the current that flows through the p-n junction under illumination at zero applied bias. In the ideal case, I_{sc} equals the photo-generated current (I_L). Therefore, the short-circuit current is the largest current which may be drawn from the solar cell. The short-circuit current mainly depends on quantum efficiency and spectrum of the incident light (the number of photons).

The open-circuit voltage V_{oc} is the maximum voltage available from a solar cell when the current through the junction is zero, and can be expressed as,

$$V_{oc} = \frac{\eta KT}{q} ln(\frac{I_L}{I_0} + 1) \quad (2)$$

The above equation shows that V_{oc} depends on the saturation current of the solar cell and the light-generated current. Because I_L typically has a small variation and the reverse saturation current may vary by orders of magnitude, the reverse saturation current plays a key role in determining V_{oc}. The saturation I_0 depends on many materials and device characteristics of the individual solar cells like the electron-hole recombination lifetimes, trap levels, defects and impurities, potential barrier at the p-n junction, interface state density and capture cross section. It can vary by orders of magnitude in nominally "identically produced" solar cell devices. Thus it is a good choice as an entropy source for generating the secret bits in a PUF. But an even better choice is the open circuit voltage, V_{oc}. We can see from equation (2) that the entropy of I_0 is contained also in the entropy of V_{oc}. However, V_{oc} is far more easily measured than I_0 in a solar cell PUF during operation in remote field.

We have selected silicon solar cells to design our PUF circuit. Silicon solar cells are of different kinds, such as, amorphous silicon, single- or mono-crystalline silicon and poly-crystalline silicon. We have chosen monocrystalline or single-crystalline solar cell because it contains far less impurities than poly-crystalline or amorphous solar cells, and as such the power conversion efficiency does not degrade over operating time. Due to wide spectral range, they can be used in both indoor and outdoor applications. For a simple and elegant design, we selected open-circuit voltage (V_{oc}) as the parameter that would be used in the design of the PUF circuit. Solar cells from the same batch (supposedly identical solar cells) display variation in V_{oc} due to random process variations, which happen during manufacturing. V_{oc} is linearly proportional to a change in temperature and is considered a more stable parameter to use in the PUF circuit so that changing light intensity and temperature would generate more reliable data. Fig. 4 depicts how the V_{oc} of our solar cells varies with light intensity. V_{oc} also depends on the temperature

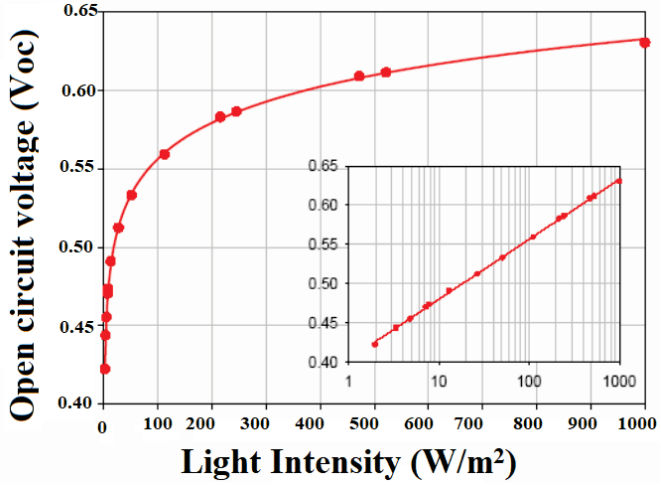

Fig. 4. Relationship between open circuit voltage (V_{oc}) and light intensity of silicon solar cells [18]

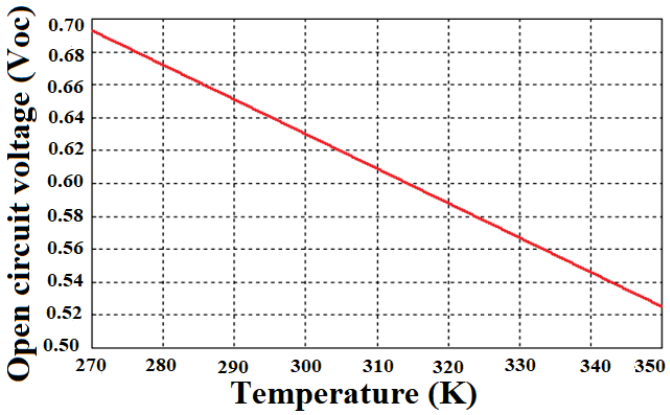

Fig. 5. Relationship between open circuit voltage (V_{oc}) and temperature [18]

of the operating condition. By changing the temperature of the environment of the PUF circuit, the V_{oc} of a solar cell can be controlled to our advantages (Fig. 5).

IV. Architecture of Proposed Solar Cell Based PUF

Fig. 6 shows the architecture of the proposed solar cell based PUF. In the proposed solar cell based PUF, the manufacturing variations in the solar cells are used to generate the response bits.

As shown in Fig. 6, each solar cell (SC) is connected to a Analog-to-Digital Converter (ADC) input pin in the microcontroller. The ADC input pins are connected to one of the two available ADC channels in the microcontroller. The ADC channels are chosen by configuring the corresponding registers in the microcontroller. The converted digital bits are read through a personal computer (PC) connected through Universal Asynchronous Receiver and Transmitter (UART).

When photons hit the solar cells, due to photovoltaic effect, voltage (V_{oc}) will be created across the solar cells. However, due to the intrinsic variations in the material characteristics,

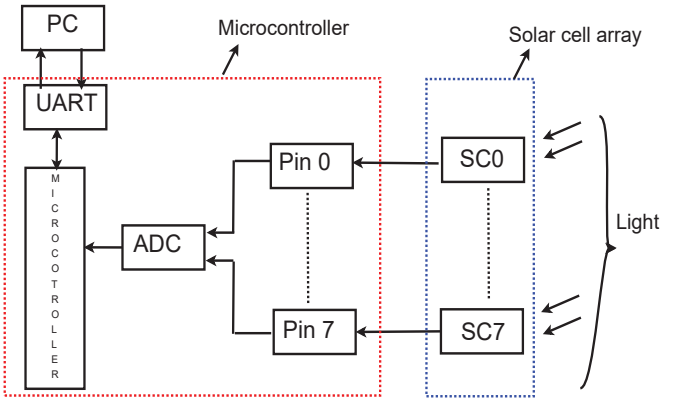

Fig. 6. Architecture of the proposed solar cell based PUF. SC represent solar cell, ADC represent Analog-to-Digital Converter, PC represent computer

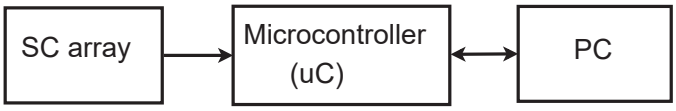

Fig. 7. Experimental setup for the proposed solar cell based PUF

there will be variations in the output voltage of the solar cells. These output voltage from the solar cells are measured using the ADC available in the microcontroller. ADC will convert the analog voltage values into 12 bit digital values. After converting the analog values to digital bits, the 12 bit digital values are compared with each other in a pre-determined pattern to generate a 128 bit response. Each generated bit of the response is the result of a comparison between two groupings of solar cells. The hardware portion and software portion of the proposed solar cell based PUF are further explained in Section V.

V. Implementation of Proposed Solar Cell Based PUF

This section describes the prototyping effort of the proposed solar cell based PUF. The prototype includes 8 solar cells along with a Tiva TM4C123GH6PM microcontroller and a personal computer (PC). As discussed in Section III, the V_{oc} of the solar cells are measured using the ADC of the microcontroller. In this experiment, we have chosen a TM4C123GH6PM microcontroller as these microcontrollers have several IoT based applications. Some of the applications of TM4C123GH6PM microcontrollers include remote monitoring, electronic point-of-sale machines, network appliances and switches, factory automation, HVAC and building control etc. [19]. The complete experimental set up for the proposed solar cell based PUF is shown in Fig. 7.

A. Hardware portion of the proposed solar cell based PUF

The hardware portion of the proposed solar cell based PUF consists of 8 solar cells along with a microcontroller. The entire system is connected via UART to a PC with a BAUD rate of 9600. The PC is used to send challenges to the system and output the generated responses. The solar

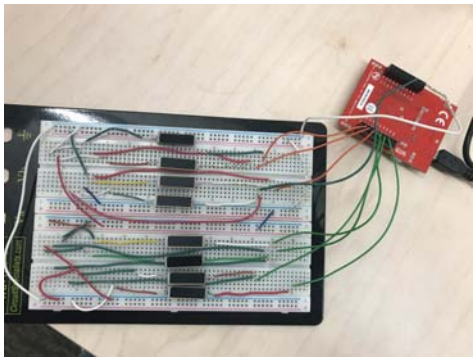

Fig. 8. Prototype of the proposed solar cell based PUF

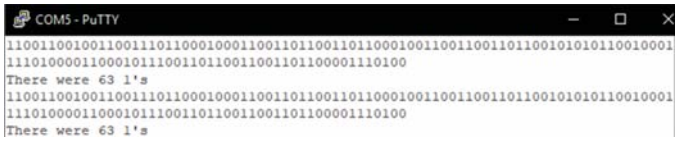

Fig. 9. Output response from the proposed solar cell based PUF

cells are connected to one of the ADCs in microcontroller. The microcontroller is configured to read the analog open circuit voltage from the solar cells. The clock frequency of the microcontroller used in this experiment is 20MHz. The sampling rate for the ADC is 125,000 samples per second.

B. Software portion of the proposed solar cell based PUF

The software portion of the proposed solar cell based PUF consists of the software running on the microcontroller to read from the cells and generate a response. The software running on the PC has no real bearing on the functionality of PUF. The PC is simply used to send challenges and display the generated response to the user. The ADC on the microcontroller can only read from a single pin at a time. Additionally, there is some noise inherent to the ADC that can manifest when taking readings. As a result, the following steps have been used to get reliable readings from a given solar cell:

- Select ADC input pin to read the V_{oc} value from the solar cell on the microcontroller
- Configure ADC to read from the selected pin in previous step
- Take 16,000 readings from ADC
- Average together to try to offset the noise from ADC to get reliable readings
- Repeat the above steps 'n-1' times for 'n' solar cells connected to the microcontroller

VI. Results

The prototype of the proposed solar cell based PUF is shown in Fig. 8. All of the experiments are performed with a uniform light intensity of 50 $Watts/m^2$. The output response bits from the proposed solar cell based PUF is recorded in the PC using the communications through UART. Recorded responses are used to evaluate the PUF against various PUF performance metrics.

Fig. 10. Experimental setup to measure the reliability of the proposed solar cell based PUF against temperature variations

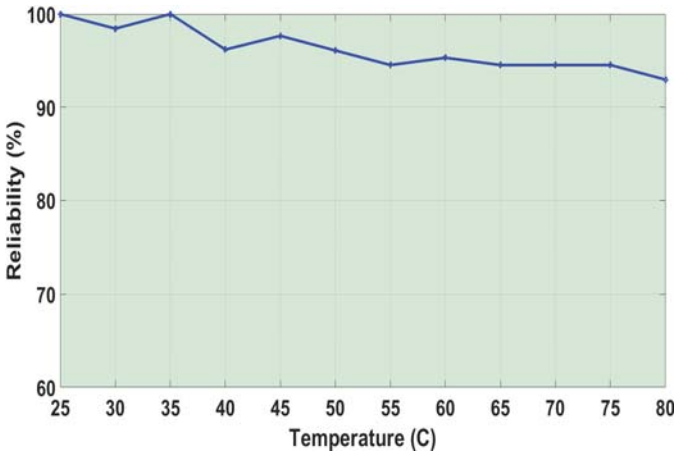

Fig. 11. Reliability of the proposed solar cell based PUF against temperature variations

A. Evaluation metrics for proposed solar cell based PUF

In this paper, we are evaluating the performance of the proposed solar cell based PUF against two important metrics. These metrics are uniformity and reliability.

1) 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,

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

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

2) 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. Variable 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 %.

B. Testing results for proposed solar cell based PUF

The testing results of the proposed solar cell based PUF are presented in this section. There are two important environmental variations that need to be considered while designing the solar cell based PUF. They are (i) variation in temperature and (ii) variation in light intensity.

1) Uniformity results of the proposed solar cell based PUF: As shown in Fig. 9, the 128 bit responses generated from the proposed solar cell based PUF consists of 63 ones and 65 zeros. The calculated value of uniformity (equation 3) for the proposed solar cell based PUF is 49.21%. The proposed solar cell based PUF has the uniformity value close to the ideal value of 50%. As the probability of generating number of ones is close to the ideal value 50%, it indicates that the proposed solar cell based PUF output is not predictable and makes it hard to attack.

2) Reliability results of the proposed solar cell based PUF against temperature variations: Fig. 10 shows the experimental setup to perform the reliability analysis of the proposed PUF against temperature variations. In this experiment, we have varied the temperature from 25°C to 80°C. As a future work, we plan to test the reliability of the proposed solar cell based PUF from -10°C to 80°C.

Fig. 11 shows the reliability of the proposed solar cell based PUF with the temperature variations with 25°C as the reference temperature. The response bits generated from the proposed PUF at 25°C is the golden response and the response bits generated at different temperature are compared with the golden response to get the reliability values. The proposed PUF has worst case reliability of 92.97% at 80°C and average reliability of 95.88%.

3) Reliability results of the proposed solar cell based PUF against light intensity variations: Unlike CMOS IC's, light intensity plays a major role in controlling the electrical parameters of the solar cells. So, in this paper, we have also performed the reliability analysis of the proposed solar cell based PUF against light intensity variations. In this experi-

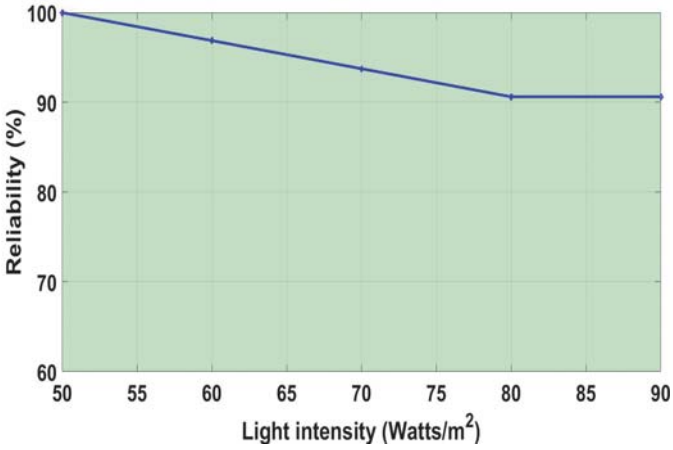

Fig. 12. Reliability of the proposed solar cell based PUF against light intensity variations

ment, we have used LED bulb to emulate the real time day light behavior with 300 lumens. A variable transformer is used to vary the light intensity of the LED bulb.

Fig. 12 shows the reliability of the proposed solar cell based PUF with the light intensity variations. In our experiment, we have chosen 50 $Watts/m^2$ as the reference light intensity value. One of the reasons to choose this low level of light intensity is to emulate a normal room environment where the light intensity is around 10-50 $Watts/m^2$. We have varied the light intensity from 50 $Watts/m^2$ to 90 $Watts/m^2$ using a variable transformer. The proposed PUF has worst case reliability of 90.62% at 80 and 90 $Watts/m^2$. The average reliability of the proposed solar cell based PUF against light intensity variations is 92.96%.

VII. Discussion and Conclusion

A low hardware cost solar cell based PUF that generates reliable bits has been developed and evaluated in this paper. This PUF uses the open circuit voltage in solar cells as an entropy source to generate the response bits. From our experimental results, we have observed that this solar cell based PUF has the uniformity value of 49.21% which is close to the ideal value of 50%. The worst case reliabilities of the proposed solar cell based PUF are 92.97% and 90.62% with variations in temperature and light intensity, respectively.

Low implementation cost along with the novel solar cell based entropy source make our PUF an ideal choice to implement in IoT devices. Further, vehicular security is a critical consideration today due to manifold use of IoT devices in a vehicular network [20], [21]. The embedded IoT devices in vehicles are susceptible to malicious cyber-attacks [22]. Therefore, we are also exploring the application of the proposed solar cell based PUF to create a security infrastructure at the hardware and software level to improve vehicular security.

Acknowledgment

This research was partially supported by grants from Kentucky Science and Engineering Foundation per Grant Agreement KSEF-3998-RDE-020 and National Science Foundation under Grant No:1738662.

References

[1] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," *Wireless Personal Communications*, vol. 58, no. 1, pp. 49–69, 2011.

[2] D. Lund, C. MacGillivray, V. Turner, and M. Morales, "Worldwide and regional internet of things (iot) 2014–2020 forecast: A virtuous circle of proven value and demand," *International Data Corporation (IDC), Tech. Rep*, vol. 1, 2014.

[3] A. Klinefelter, N. E. Roberts, Y. Shakhsheer, P. Gonzalez, A. Shrivastava, A. Roy, K. Craig, M. Faisal, J. Boley, S. Oh *et al.*, "21.3 a 6.45 μw self-powered iot soc with integrated energy-harvesting power management and ulp asymmetric radios," in *Solid-State Circuits Conference-(ISSCC), 2015 IEEE International*. IEEE, 2015, pp. 1–3.

[4] 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.

[5] E. Yablonovitch, O. D. Miller, and S. Kurtz, "The opto-electronic physics that broke the efficiency limit in solar cells," in *Photovoltaic Specialists Conference (PVSC), 2012 38th IEEE*. IEEE, 2012, pp. 001 556–001 559.

[6] C. Marchand, L. Bossuet, U. Mureddu, N. Bochard, A. Cherkaoui, and V. Fischer, "Implementation and characterization of a physical unclonable function for iot: a case study with the tero-puf," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 1, pp. 97–109, 2018.

[7] R. Anderson and M. Kuhn, "Low cost attacks on tamper resistant devices," in *International Workshop on Security Protocols*. Springer, 1997, pp. 125–136.

[8] K. Kursawe, D. Schellekens, and B. Preneel, "Analyzing trusted platform communication," in *ECRYPT Workshop, CRASH-CRyptographic Advances in Secure Hardware*, 2005.

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

[10] M. N. Aman, K. C. Chua, and B. Sikdar, "Position paper: Physical unclonable functions for iot security," in *Proceedings of the 2nd ACM international workshop on IoT privacy, trust, and security*. ACM, 2016, pp. 10–13.

[11] D. Mukhopadhyay, "Pufs as promising tools for security in internet of things," *IEEE Design & Test*, vol. 33, no. 3, pp. 103–115, 2016.

[12] Y. Hori, T. Yoshida, T. Katashita, and A. Satoh, "Quantitative and statistical performance evaluation of arbiter physical unclonable functions on fpgas," in *Reconfigurable Computing and FPGAs (ReConFig), 2010 International Conference on*. IEEE, 2010, pp. 298–303.

[13] D. Merli, F. Stumpf, and C. Eckert, "Improving the quality of ring oscillator pufs on fpgas," in *Proceedings of the 5th workshop on embedded systems security*. ACM, 2010, p. 9.

[14] D. E. Holcomb, W. P. Burleson, and K. Fu, "Power-up sram state as an identifying fingerprint and source of true random numbers," *IEEE Transactions on Computers*, vol. 58, no. 9, pp. 1198–1210, 2009.

[15] P. Würfel, *Physics of solar cells*. Wiley-vch Weinheim, 2005, vol. 1.

[16] K. Rosenfeld, E. Gavas, and R. Karri, "Sensor physical unclonable functions," in *Hardware-Oriented Security and Trust (HOST), 2010 IEEE International Symposium on*. IEEE, 2010, pp. 112–117.

[17] E. Aponte, "A study on energy harvesters for physical unclonable functions and random number generation," Ph.D. dissertation, Virginia Tech, 2017.

[18] IXYS, "Ixolar high efficiency solarbit," Nov. 2016.

[19] T. Instruments, "Tiva tm4c123gh6pm microcontroller-data sheet," 2013.

[20] D. K. Oka, T. Furue, L. Langenhop, and T. Nishimura, "Survey of vehicle iot bluetooth devices," in *Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on*. IEEE, 2014, pp. 260–264.

[21] A. Parodi, M. Maresca, M. Provera, and P. Baglietto, "An iot approach for the connected vehicle," in *International Internet of Things Summit*. Springer, 2015, pp. 158–161.

[22] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015.