International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

Embedded System Security: Prevention Against Physical Access Threats Using PUFs

AP Deepak[1], A Krishna Murthy[2], Ansari Mohammad Abdul Umair[3], Krathi Todalbagi[4], Dr.Supriya VG[5]

B.E. Students, Department of Electronics and Communication Engineering, Sir M. Visvesvaraya Institute of Technology, Bengaluru, India[1,2,3,4]

Professor, Department of Electronics and Communication Engineering, Sir M. Visvesvaraya Institute of Technology, Bengaluru, India[5]

ABSTRACT: Embedded systems are the driving force in the development of technology and innovation. It is used in plethora of fields ranging from healthcare to industrial sectors. As more and more devices come into picture, security becomes an important issue for critical application with sensitive data being used. In this paper we discuss about various vulnerabilities and threats identified in embedded system. Major part of this paper pertains to physical attacks carried out where the attacker has physical access to the device. A Physical Unclonable Function (PUF) is an integrated circuit that is elementary to any hardware security due to its complexity and unpredictability. This paper presents a new low-cost CMOS image sensor and nano PUF based on PUF targeting security and privacy. PUFs holds the future to safer and reliable method of deploying embedded systems in the coming years.

KEYWORDS:Physically Unclonable Function (PUF), Challenge Response Pair (CRP), Linear Feedback Shift Register (LFSR), CMOS Image Sensor, Polyomino Partition Strategy, Memristor.

I. INTRODUCTION

The need for security is universal and has become a major concern in about 1976, when the first initial public key primitives and protocols were established. Mathematical and algorithmic mechanisms were deployed to create a secure environment for software and communication. The search for more secure techniques is always hunted and one such technique used is the PUF. Physically Unclonable Function (PUF) is physical object that, for a given input (challenge) results in an output (response) that is unique only to that physical object produced during manufacturing. The set of Challenge Response Pair (CRP) is unique to each individual PUF. The basic idea is take advantage of uncontrollable variations of physical properties of an object during manufacturing process. These variations can be classified as spatial and temporal variations [4]. Spatial variations include variations such as minuscule dimensions, random dopant fluctuations, output state of a flip-flop and so on. These variations are fixed once they are manufactured and can be manipulated to obtain unique 'fingerprints' of each device such threshold voltage, CMOS offset voltage etc. Temporal variation includes noise, supply power, temperature fluctuations, transient effects and so on.

A function in mathematics is a relation which associates elements of a set A, typically referred to as the domain, with elements of a set B, known as the range or image. The relation between the elements in A with that of B is defined via a mathematical formula, graph, table etc. Here we take the challenges C_i and map it with the response pair R_i[23].Thus we can write,

$$R_i \leftarrow PUF(C_i)$$

Physical Unclonable Function basically has two parts: (i) a physical part and (ii) an operational part. The physical part is a physical object that's almost impossible to replicate. This ensures every piece is as unique as possible. It generates this trait due to uncontrollable manufacturing process variations. These variations occur at microscopic level such as doping variations in a transistor. The operation part is with respect to its function it performs. In order for the function to perform it requires a set of challenges C_i (stimuli) to which the PUF responds with a set of sufficiently different responses R_i.

There are several PUFs developed to thwart attackers from taking access to the embedded system. In this paper we will be discussing two such PUFs along with their reliability and applications.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

II. REQUISITES FOR AN ATTACK

For an attacker to be able to exploit vulnerabilities in an embedded system, there are few preconditions that must be met in order to carry out the attack. Common Vulnerabilities and Exposures (CVE) [1] is a sophisticated database of security vulnerabilities, listing a comprehensive set of security breaches not necessarily related to embedded systems. CVE database can be shared to identify the security breaches occurred in the past and prevent such occurrences from happening in the future. We use CVE to identity few conditions that were present during the attack; there are many such conditions but we list the most common ones [2].

A. Internet connection

Many of the security vulnerabilities stem from the device's ability to connect to the internet where the attacker is able to connect to it remotely. The attacker may be able to send the system messages, intercept messages and in some cases, compromise the system entirely if the device is discoverable on the internet.

B. *Local or remote access*

Here the attacker has to have some level of privilege to be able to get into the system. It may be remote access or just a user level privilege, not necessarily administrator level access. This gives the attacker some level of access to the services or functions provided by the device.

C. Physical access

Attacker needs to have physical access to the device. However, the attacker does not need any access privilege. Contact may be through USB stick, memory cards, LAN connection and so on.

D. Physical proximity

Sometimes an attacker can access a device simply by being within its wireless proximity say, within the radio wave range of a RADAR. Attacker may communicate wirelessly with the device instead of having physical access and manage to corrupt it.

E. Unknown

Lack of sufficient information in some cases has made it difficult to determine the conditions around some security breaches. The CVE has yet to fill in this information once the preconditions have been identified.

III. TYPES OF ATTACKS

Attackers use a wide variety of methods to gain access to a device. The CVE has an extensive record of types of attacks that have been successful, some of which are listed below [2].

A. Control hijacking attacks

In a normal flow of program execution, the attacker diverts the flow of control running in the embedded system by injecting his/her own program to perform malicious acts. The attacker can then disrupt the original program and own the device.

B. Reverse Engineering

Sometimes it is possible to analyse the program flow by knowing the device's functionality thereby knowing how the program works. Thus, the attacker can identify vulnerabilities (e.g., memory overflow) in the code and exploit it to obtain sensitive information like access credentials.

C. Malware

A common attack is using malicious software i.e., malware to infect the system and try to gain access. Several types of malwares have been identified but they all have a common purpose of creation: to potentially harm the targeted devices. A malware may try to extract sensitive data, gain root access, or modify system behaviour.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

D. *Injecting crafted packets or inputs*

Systems that work on protocol are vulnerable to these kinds of attacks. An attacker provides a manipulated input or packet to the system that cannot handle such an input. The systems throws a parsing error and may cause the software to crash or the protocols to fail leaving the system wide open. The attack tests the systems by providing various packets to cause the system failure.

E. Eavesdropping

Here the attacker only intercepts and observes the messages sent and received by the embedded systems. Such types of attacks are usually called as passive attacks. The messages intercepted may contain sensitive information which are weakly or not at all protected by cryptography. Information gathered by the attacker through this means could further be used to create crafted packets or inputs to disrupt the device.

F. Brute force search

An attacker may perform exhaustive key search attacks against cryptographic algorithms to crack the key used to decrypt authentication. This works against devices with weak cryptography and weak authentication methods. Such attacks are possible only when the search sample is small enough, for example, dictionary search against a password with only lowercase letters or 4-digit passcode.

G. Normal use

Some devices have absolutely no protection mechanism against unauthorized users and an attacker can access the device simply as if he/she were a normal legitimate user. The attacker can access all files and services on the embedded systems if there is no access control mechanism implemented.

H. Unknown

Some of the attacks listed in CVE did not identify any particular methods used to exploit the vulnerabilities found in an embedded system.

In this paper we will be dealing with security measures against control hijacking attacks by authenticating the software before the device can boot up. [3] presents an attack against a smart home automation device, the Nest Thermostat. Pressing and holding the power reset button for 10 minutes initiates a global reset. Immediately, there is small time frame within which the systems accepts USB sticks and boots up through the provided USB without verifying if it is indeed factory firmware. Now the attacker can also gain access to other devices through this device and collect information, set up surveillance, or perform any other malicious acts. Therefore, there is a need to validate the software before the device is able to function or boot up.

IV. CMOS IMAGE SENSOR BASED PUF

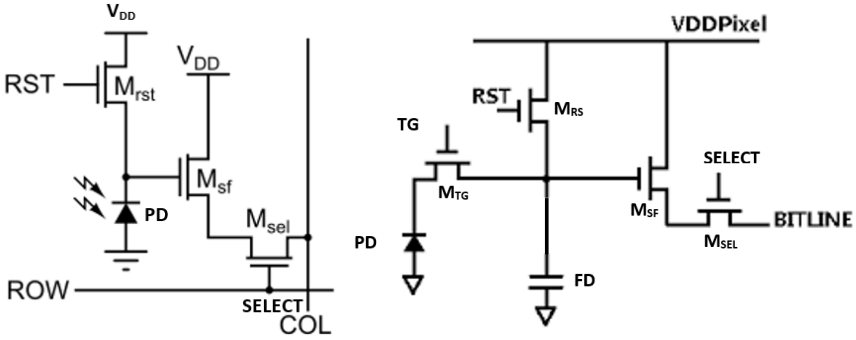
Physically unclonable functions (PUFs) have proved to be an effective measure for secure device authentication and key generation. The proposed PUF is resilient against the sensor decoupling attack as its input challenges are the digital addresses of the pixels, which are not taken from the measurement of any incident illumination intensity. The image sensor can be fabricated by standard CMOS process without additional processing steps. The inherent process mismatch between pixel sensors and readout circuits in an image sensor manifests as unique fixed pattern noise (FPN) in the image. We exploit FPN caused by dark signal non-uniformity (DSNU) as the basis for implementing the PUF. Also, FPN does not change appreciably with series of captures, vary with exposure time, temperature, imager gain and incident illumination, it is not expressed in a random (changing) spatial distribution, occur only at certain, fixed pixel locations. DSNU can be extracted only from dark images that are not shared with others, and only the legitimate user can obtain it with full control of the image sensor. Compared to other FPN components that can be extracted from shared images, DSNU facilitates more secure and usable device authentication. We present an efficient and reliable key generation procedure for use in wireless low-power devices. The only modification required from the commercial CMOS image sensor core is a switch transistor for bypassing the correlated double sampling (CDS) circuit. This makes it feasible to be implemented on existing cameras that use CMOS active pixel sensor, and easily integrated with other CMOS functional blocks for digital image processing.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

A. *Fundamentals*

A typical architecture of a CMOS image sensor consists of a pixel array, vertical and horizontal scanners, and readout circuits. The pixel array is the key region of an image sensor and the imaging quality is mostly determined by the performance of this array. There are two popular types of pixel structure: 3T-APS and 4T-APS.



(a) (b)

Fig. 1. The schematic of (a) 3T-APS pixel, (b) 4T-APS pixel.

Fig. 1 shows the transistor-level implementations of 3T-APS and 4T-APS [5] (T here stands for transistors). In the 3T-APS, each pixel cell consists of a photodiode (PD), a reset transistor M_{rst}, a select transistor M_{SEL} and a source follower readout transistor M_{SF}. When M_{rst} is turned on, the voltage on the PD is reset to the value:

$$V_{PD} = V_{DD} - V_{th,RS} \qquad -(1)$$

where $V_{th,RS}$ is the threshold voltage of M_{rst}. When M_{rst} is turned off, the PD is electrically floated. The photocurrent I_{ph} due to the incident illumination discharges the PD (omitting the small dark current). After an exposure time t, M_{SEL} is turned on. The output voltage of this pixel is read out.

This voltage can be expressed as:

$$V_{out} = V_{DD} - V_{th,RS} - V_{th,SF} - \frac{I_{ph} \times t}{C_{PD}} \qquad -(2)$$

where, $\{V = \frac{Q}{C}\}$ and $\{Q = I_{ph} \times t\}$

where $V_{th,SF}$ and C_{PD} are the threshold voltage of M_{SF} and the PD junction capacitance, respectively. The output voltage V_{out} is linearly proportional to I_{ph}. From (2), the variations in pixel output values are mainly caused by the variations in the size and capacitance of the photodiode, as well as the threshold voltages of M_{rst} and M_{SF}.

The 4T-APS is shown in Fig. 1(b). It consists of the same components as 3T-APS except for the transfer gate M_{TG} and the pinned PD (When you design the depletion of the PD to deplete at a certain voltage you are pinning that PD to that voltage). The operation of 4T-APS is explained as follows. Assume that there is no accumulated charge in the PD initially. The floating diffusion (FD) is reset by turning on M_{RS}. The voltage on the FD is the same as that expressed in (1). It can be read out by turning on M_{SEL}. The photocurrent I_{ph} is accumulated in the PD for an exposure time t. The accumulated charge is transferred to the FD by turning on M_{TG}, followed by turning on M_{SEL} to readout the signal. This output voltage can also be expressed by (2), if the charge in the FD is completely depleted. This process is repeated to read the reset voltage and signal voltage successively.

Due to the more effective cancellation of reset noise, 4T-APS provides better image quality, but 3T-APS has lower processing cost and more compact pixel layout [5].

B. *Working*

Irrespective of 3T- or 4T-APS, the pixel voltage of the CMOS image sensor is preserved during the readout, which makes it possible to read the pixel voltage value multiple times. As FPN can badly degrade the image qualities, noise cancelation circuits, such as correlated double sampling (CDS), are employed in the readout circuits [7] to suppress them. Or a suppression method called Flat-field correction (FFC) is employed which uses DSNU and Photo Response Non-Uniformity (PRNU) to linearly interpolate and reduce the local photo response to the array average, which basically improves the quality of the digital imaging. The response of the proposed PUF is a binary string extracted from the pixel array [6]. Each response bit is obtained by comparing the reset voltages of two pixels. The output of the pixel is measured twice to obtain the reference voltage (i.e., the pixel voltage after reset) and the signal voltage (i.e., the pixel voltage after exposure). The reset noise is reduced by taking the difference between these two voltages. The output bit is '0' or '1' depending on which reset voltage is larger. The address of the selected pixel pair is determined

by a digital input challenge. As the CMOS image sensor has non-destructive readout, the original function will not be affected by operating the image sensor in the PUF mode.

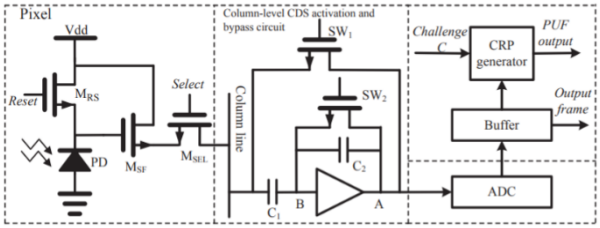


Fig. 2. Architecture of the proposed CMOS image sensor based PUF

Fig. 2 shows the architecture of the proposed CMOS image sensor based PUF with CDS enabling and disabling switches for regular sensing and PUF modes. Although 3T-APS is illustrated, another pixel structure is equally applicable as long as the random reset voltage of the pixel can be accessed before it is suppressed by the CDS. The CDS can be bypassed in PUF mode by inserting a bypass transistor (i.e., SW_1) in parallel with the CDS circuit.

During normal sensing mode, SW_1 is turned off and the reference signal (i.e., reset signal) on the capacitor C_1 is subtracted from the column level CDS [5] to reduce the fixed pattern noise (FPN). The operation of the column level CDS can be explained as follows. In the first phase, the pixel signal value on the capacitor C_1 is sampled. The switch SW_2 is closed to reset the capacitor C_2 and the operational amplifier input offset is sampled. In the second phase, SW_2 is open to reset the pixel. The reset pixel voltage on C_1 is sampled. The output of the amplifier is the difference between the reset and signal values. During the PUF mode, the reset pixel output voltage is directly read out by turning on SW_1. Otherwise, the CDS may bias the FPN and impact the randomness of PUF response. The digitized sensor outputs are buffered and fed into the CRP generator to produce the stable response bits to the applied challenges. Based on (1), the pixel output voltage during the reset phase can be written as:

$$V_{rst} = V_{DD} - V_{th,RS} - V_{th,SF} \qquad -(3)$$

V_{rst} can be varied due to the variations of $V_{th,RS}$and $V_{th,SF}$. The variation of V_{rst} generates a unique pattern for each pixel array. However, as V_{rst} is sensitive to the random reset noise and the variations of supply voltage and temperature, the IC signature produced directly from V_{rst} is unstable. To obtain a more reliable signature from the image sensor, a differential readout scheme is proposed.

The architecture of the proposed CRP generator is shown in Fig. 3, and the process of its CRP generation is shown in Fig. 4. First, the bypass transistor (SW_1) is turned on to skip the column level CDS. V_{rst} of each pixel is then scanned out and stored in the frame memory after it is digitized. For ease of interpretation, the entire image of V_{rst} is called the "reset image". The address decoder decodes an n-bit address C to read out a pixel voltage value P_C of the "reset image". The bit length n of the challenge can be determined by:

$$n = \log_2 (H \times V) \qquad -(4)$$

where H and V are the numbers of rows and columns of the image sensor, respectively.

Another challenge (address) C ′ can be generated from C through an n-bit Linear Feedback Shift Register (LFSR) counter. The LFSR is initialized by an arbitrary user selectable n-bit seed N ($0 < N < 2^n$), i.e.,

$$C' = C \oplus N \qquad -(5)$$

where $\oplus$ denotes a bitwise XOR operation.

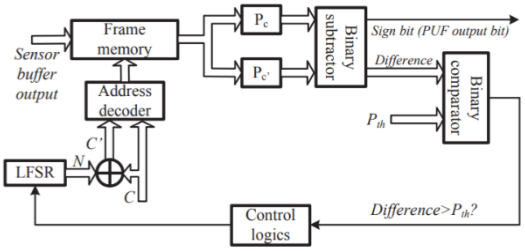


Fig. 3. Architecture of CRP generator circuit.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

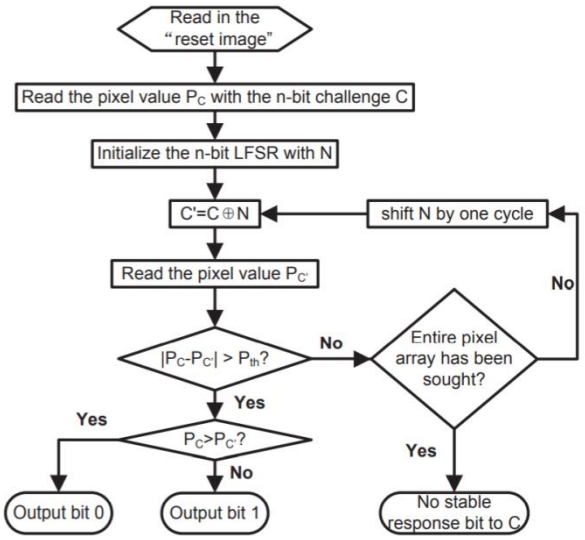


Fig. 4. Procedure for CRP generation.

Since N ≠ 0, C ≠ C′. A different pixel voltage value $P_{C'}$ is read out by the challenge C′ and compared with P_C by a binary subtractor and a binary comparator. The PUF output bit is either 0 or 1 depending on which pixel voltage value is larger. When the difference between P_C and $P_{C'}$ is sufficiently large, i.e., the absolute value of $P_C - P_{C'}$ is larger than a predefined threshold P_{th}, the generated bit is considered stable and will be retained as the response bit to the input challenge C. Otherwise, another pair of pixels will be sought by shifting the content N of the LFSR by one more clock cycle to generate a new C′. This procedure is repeated until a stable CRP is found or the entire pixel array has been exhausted. The threshold of difference P_{th} (empirically determined) is process technology dependent, which provides a knob to tune the noise margin of the pixel pairs to stabilize the response bit against temperature and voltage variations. With a different seed value N (also initializes the LFSR counter), the mapping of the CRPs can be changed. This is particularly useful when the original CRP mapping is suspected to be compromised or the CRP can be periodically refreshed to prevent modelling attacks [8]. If logical reconfigurability is not required, N of the LFSR can be fixed to produce C′ from C as if two different but fixed challenges generated externally are fed successively into the PUF.

C. Reliability enhancement

It can be shown that the proposed differential readout scheme can improve the PUF's reliability against temperature and supply voltage variations. Let V_{sig} denote the signal voltage $P_C - P_{C'}$, where P_C and $P_{C'}$ are the two reset voltages of the pixels selected by the addresses, C and C′, respectively. From (3), V_{sig} can be expressed as:

$$V_{sig} = V_{rst} - V'_{rst}$$
$$V_{sig} = V_{DD} - V_{th,RS} - V_{th,SF} - V_{DD} + V'_{th,RS} + V'_{th,SF}$$
$$V_{sig} = V'_{th,RS} + V'_{th,SF} - V_{th,RS} - V_{th,SF} \quad \text{-(6)}$$

Equation (6) indicates that V_{sig} is insensitive to the supply voltage variations V_{DD}.
The threshold voltage is temperature dependent and can be expressed as [9]:

$$V_{th}(T) = V_{th}(T_0) + \sigma_{th}(T - T_0) \quad \text{-(7)}$$

where T_0 is the reference temperature and σ_{th} is the threshold voltage temperature coefficient (TVTC) in the range of 0.5~ 3 mV/K.Taking the partial derivative of V_{sig} with respect to T,

$$\frac{\partial V_{sig}}{\partial T} = \sigma'_{th,RS} + \sigma'_{th,SF} - \sigma_{th,RS} - \sigma_{th,SF} \text{ -(8)}$$

{Where TVTC ,is $\sigma_{th} = \frac{\partial V_{th}}{\partial T}$}
The differential readout voltage V_{sig} is less sensitive to temperature variation than any single pixel reset voltage V_{rst}as

$$\left|\frac{\partial V_{sig}}{\partial T}\right| < \left|\frac{\partial V_{rst}}{\partial T}\right| = \left|\sigma_{th,RS} + \sigma_{th,SF}\right| \quad \text{-(9)}$$

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

To show the robustness of the differential readout scheme against supply voltage and temperature variations, 50 runs of Monte Carlo simulation of a 3T-APS are performed at the transistor-level using 180 nm CMOS process design kit (PDK).

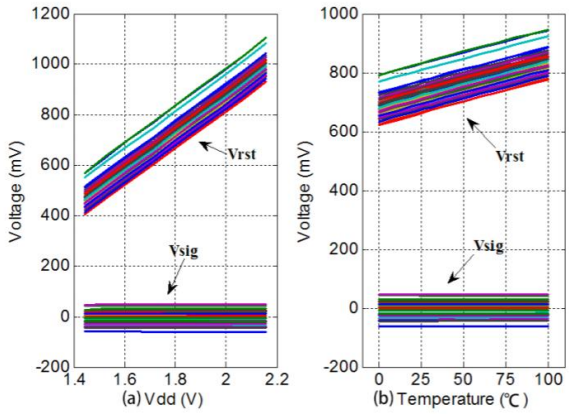


Fig. 5. Monte Carlo simulation results of V_{rst} and V_{sig} against the variations of (a) supply voltage, and (b) temperature.

The Monte Carlo simulation method [10] is used to introduce randomly sampled device parameter variations from a normal distribution. The results are shown in Fig. 5 for the pixel reset output voltage V_{rst} and the differential output signal voltage V_{sig} with the supply voltage varies by ±20% and the temperature varies from 0 to 100ºC. It is evident that the noises induced by the variations of the supply voltage and the temperature are well suppressed by the differential readout method.

The differential readout scheme is inadequate to mitigate other random effects due to KTC noise (thermal noise), shot noise (noise due to the dark current and photocurrent), 1/f noise, column switch noise, etc... Since the response of our PUF is generated during reset, the KTC noise dominates [11].

Also, in the CRP generator, if the difference exceeds P_{th}, the response bit generated by this pair of pixels is discarded for use as CRP. The reliability is increased at the cost of a reduction in the total number of CRPs.

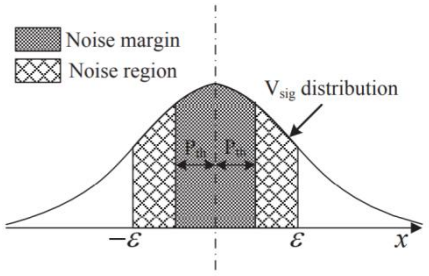


Fig. 6. Effects of P_{th} on PUF reliability and the number of CRPs.

Fig. 6 depicts the effect of changing P_{th} on the PUF reliability. Assuming that the threshold voltage V_{th} of the transistors in each pixel are Gaussian distributed, then V_{sig} is also Gaussian distributed. With ε representing the overall noise voltage, the CRPs located in the noisy region are considered to be unstable. The CRPs with V_{sig} lying in the range between $-P_{th}$ and $+P_{th}$ are discarded.

Based on the above analysis, the noise margin P_{th} provides a trade-off between the reliability of PUF as a whole and the number of CRP pairs. Decreasing P_{th} will enable more CRP pairs to be extracted but with lower overall reliability. On the other hand, increasing P_{th} will result in higher reliability but less number of extractable CRPs.

V. APPLICATIONS OF CMOS PUF

A. *Smart phone Authentication and Anti-counterfeiting*

The proposed image sensor based PUF has given a new approach with low-cost, secure and robust solution for on chip CMOS image sensor device authentication and key generation. Presently, device-specific IDs such as

IMEI (device ID), IMSI (subscriber ID) and ICC-ID (SIM card serial number) are used for the identification and authentication of mobile phones. As these digital IDs are kept in the Non-Volatile Memory (NVM) in sim cards, these can easily be copied by hackers to knockoff cell phones [12] and these cell phones are virtually indistinguishable to the authentic ones. Some of the advantages of this application are:

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

- Nowadays most of the smart phones are integrated with more than one CMOS image sensor (back and front). As modern integrated CMOS image sensors have high resolution, it can provide large CRP space. A large CRP helps in enhancement of security of the PUF.
- The proposed PUF can generate highly reliable response by tuning P_{th}. Unlike the ID stored in NVMs, it cannot be easily copied, compromised or removed. The secrets in these are integral parts of the structure inherited from its manufacturing process and can only be generated when the chip is powered on. Any invasive attack to steal the secret will destroy the original secrets and render the chip.
- The proposed PUF can be seamlessly integrated into the image sensor. No extra expensive secure EEPROM/RAM, dedicated encryption module or other auxiliary PUF module is required for the purpose of device authentication, which can further reduce the total cost of the system.

B. *Fortification against virtual camera attack*

Virtual camera is a software tool that could not only modify the face look, hair and backgrounds, but also stream a pre-recorded video to spoof the operating system into believing that the image is captured by the physical webcam in real time. Virtual cameras are bigger threat to surveillance camera system, image sensor based biometric authentication etc. A secured encryption is possible between user and device communication using proved secure algorithms AES and DES but in this case the attacker can easily copy the message authentication code (MAC) stored in EEPROM or fuses [13]. The virtual cameras can then use the cloned MAC to masquerade as the device to deliver the fake image or video to gain access to a restricted area or the confidential information. The proposed PUF uses a unique and trusted signature which is extremely hard to be copied and compromised by videos or images taken from any other image sensors.

VI. RELIABILITY

A. *Uniqueness in the assessment*

The difference in the CRPs generated by one PUF to another determines the uniqueness. Uniqueness can be estimated by the average inter-die Hamming Distance (HD) of the responses produced by different PUFs. Let R_u and R_v be the n-bit responses from two different chips, u and v, with the same input challenge C, the uniqueness U for m chips is formulated as [14]:

$$U = \frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^{m} \frac{HD(R_u, R_v)}{n} \times 100\%$$

Ideally, the uniqueness of a PUF is 50% for the highest distinguishability of the CRPs generated by the PUF. The uniqueness of the proposed PUF can be efficiently estimated by simulating the CRPs generated from a reasonably large number of PUF instances by Monte Carlo simulation. Based on the CRPs collected from 10,000 PUF instances, with 120 CRPs generated for each instance, the frequency distribution of the inter-die HDs is obtained in Fig 7(a). The uniqueness of these 10,000 instances is calculated to be 50.01%. The best fit Gaussian curve to the histogram has mean $\mu = 50.09\%$ and standard deviation $\sigma = 4.44\ \%$. Physical measurements obtained from the five PUFs were also used for this evaluation. A total of 8000 CRPs were generated by the five PUFs Fig 7(b) shows the measured frequency distribution of the inter-die HDs. The uniqueness calculated from the inter-die HDs of the proposed PUF is 49.37%, which is very close to the ideal value of 50%.

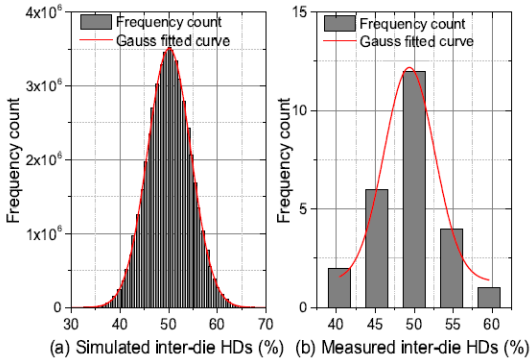


Fig. 7. Frequency distribution of (a) the simulated inter-die HDs for 10,000 PUF instances and (b) the measured inter-die HDs from the five image sensor based PUF chips.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

B. *Reliability assessment*

Reliability measures how reproducible or stable are the CRPs of a PUF under different operating conditions. The reliability of a PUF can be measured by its Bit Error Rate (BER), which can be characterized by comparing the responses taken at different time with a reference response to the same challenge. The bit error rate (BER) is the number of bit errors per unit time. The bit error ratio (also BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval. Bit error ratio is a unitless performance measure, often expressed as a percentage.Let R_i be the reference n-bit response to an input challenge C produced by the PUF of a chip *i*under the nominal operating condition. The same set of challenges are then applied k times to the same PUF under varying environmental conditions to obtain the responses R_{ij} for j = 1,2...k. BER is given as

$$\frac{1}{k}\sum_{j=1}^{k}\frac{HD(R_i, R_{i,j})}{n}\times 100\%$$

The reliability S for chip *i* can be expressed as [14]

$$S = 1 - BER = 1 - \frac{1}{k}\sum_{j=1}^{k}\frac{HD(R_i, R_{i,j})}{n}\times 100\%$$

Fig. 8(a) shows the reliability measured using 1000 CRPs generated by each image sensor based PUF under varying supply voltages with different P_{th}. The nominal power supply for this CMOS technology is 3.3V and the CRP collected under this supply voltage is used as a reference. The supply voltage is varied from 3 to 3.6 V. The average reliability of the CRPs obtained from the five test chips is 97.66% with P_{th} = 0. With P_{th} = 30, the average reliability and the worst reliability can still be maintained at 99.77% and 99.10%, respectively when V_{dd} = 3.6 V. The reliability of the proposed PUF operating at different temperature is also measured. The operating temperature was increased by generating heated air around the die and the ambient temperature was measured by the TK-610B thermometer. The working temperature was varied from 15ºC to 115ºC. The CRP collected under 27ºC is used as a reference. Fig. 8(b) shows the average reliability of the five PUF chips under different operating temperatures. The average reliability measured from the PUF chips is 95.97% with P_{th} = 0. The reliability can be increased to 100% when P_{th} = 30. The results corroborate that the proposed image sensor based PUF can be made much less susceptible to power supply and temperature fluctuations by increasing P_{th}.

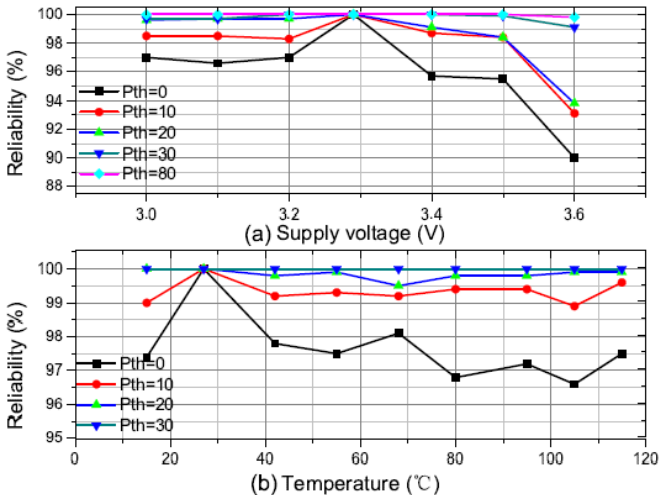


Fig. 8. The measured average reliability of hybrid RO PUF against (a) voltage variations, (b) temperature variations.

C. *Unpredictability assessment*

Unpredictability measures how difficult an attacker can predict the CRPs of a PUF. For the proposed PUF, the number of independent bits that can be generated is a function of N_{pixel}. N_{pixel} is the total number of pixels of the image sensor. There are $N_{pixel}!$ different orderings of pixels based on their reset voltages. If the orderings are equally likely, the entropy corresponding to the number of independent bits will be $\log_2(N_{pixel}!)$ bits. The maximum number of independent CRPs is intended as the primary assurance of unpredictability; these generated random output bits are also

tested by the NIST suite. The Statistical Test Suite developed by NIST is an excellent and exhaustivedocument looking at various aspects of randomness in a long sequence of bits. The Test Suitewas developed after DES was cracked in order to choose today's AES. It is a very importanttool to understand randomness for crypto ciphers.If they fail to pass the NIST test, the responses are considered as not random enough and may be vulnerable to cryptanalysis. As the proposed PUF is a property of the image sensor, its area/bit is dominated primarily by the pixel area required for the imaging function. Our proposed PUF has great advantage of high reliability by virtue of the differential readout method. By increasing the adaptive threshold P_{th} to 80, the worst reliability for our proposed image sensor PUF can still be maintained at 99.80% with ±10% supply voltage variations from 3.0∼3.6 V and a temperature variation of 15∼115ºC. This is highly competitive for the hostile operating condition variations that can be achieved among all PUFs in comparison.

VII.NANO PPUFs

Nano-PPUFs provide a faster, low-energy and more secure alternative to device aging, to overcome the burden of simulating the entire Public PUF (PPUF) at one of the communicating parties. Nanotechnology components are inherently faster and use lower power than current complementary metal–oxide– semiconductor (CMOS) technologies. They exhibit nonlinear characteristics. Nanotechnology components also express the unique characteristic of bidirectional signal propagation: since input signals can be applied at any end of the circuit, this exponentially increases the input and output spaces with respect to a comparable CMOS PPUF.
While conventional VLSI design tries to eliminate sneak paths, reduce effects of process variations, and build compact simulation models, we leveraged these factors to build a security primitive. Even with just a few hundreds of memristors, we were able to build a PPUF which will take several years for an attacker to simulate. Furthermore, the developed nano-PPUF is more robust [16] to changes in temperature then CMOS devices.
Overall, these characteristics makes nano PPUF better than any regular physical unclonable function in terms of security, speed and power efficiency.

A. Structure

It is composed of a grid of nano-PPUF cells, with adjacent cells connected over matching pins. Each cell is modelled as a geometric random network generated during the synthesis of III–V nanowires. Nodes within the network are uniformly distributed and connected based on threshold distances. Each node exhibits nonlinear current–voltage characteristics, which gives rise to the nonlinear circuit characteristics of nano-PPUF cells and grids. The bidirectional signal propagation property of these circuits allows for inputs to be applied at any of the pins at the boundary of each cell Therefore, nano-PPUF inputs are defined as a combination of input values which is the voltages applied at the inputs and input sets which is the set of pins at which the voltages are applied. The rest of the boundary pins define nano-PPUF outputs, and are similarly composed of output values and output sets. To enable runtime, each pin at the boundary of a cell is multiplexed to facilitate input or output. Specifically, Wendt and Potkonjak [17] define a polyomino partitioning strategy where the set of cells accepting inputs are adjacent and connected, and formed by joining one or more equally sized squares edge to edge.

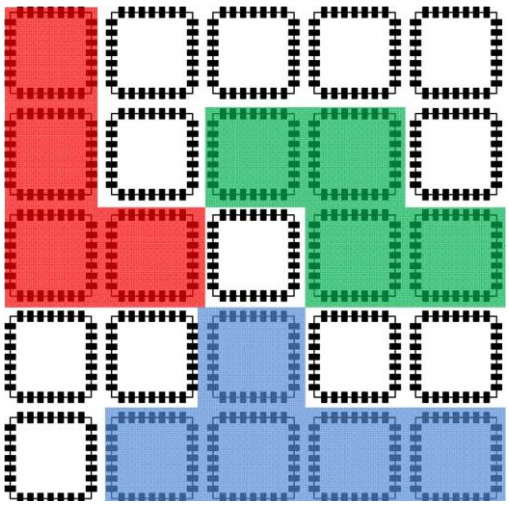


Fig.9. Example of a 5×5 nano-PPUF grid. Adjacent nano-PPUF cells are connected via adjacent pins. Example polyomino partitions of size 4, 4, and 5 are shaded [19].

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

B. *Memristor-based crossbars*

The grids in nano-PUF consist of N×N crossbars with N wires running perpendicular to each other. At the junction of each wire,a resistive device such as memristor is grown [20].

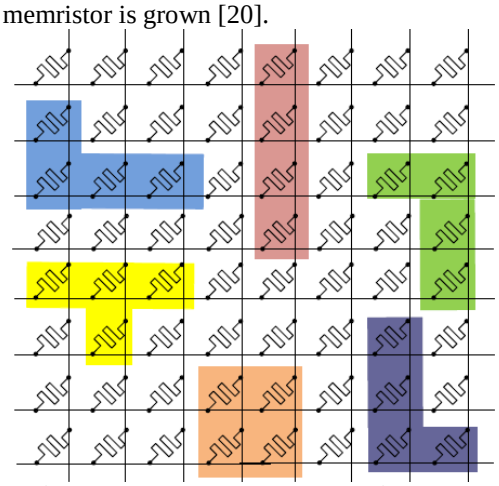


Fig.10. Example of 8×8 memristor. Polyomino partition of size (4,4,4,4,4,4) are shaded.

Memristors are resistive devices fabricated by placing a metal oxide (such as TiO_2-X) layer with oxygen vacancies, on a perfect metal oxide (TiO_2) layer, and sandwiching them between metal electrodes [21]. When a sufficiently large positive voltage is applied to it for a long period of time, the memristor state changes to M_{on} (ON state). When a sufficiently large negative voltage is applied to it over a long period of time, the memristor state changes to M_{off} (OFF state). In between these two states, memristors can display several characteristics all dependent on voltage and time; memristors changes states based on these two parameters.

When $M_{off} >> M_{on}$, the relation between the memristance of the device M(φ(t)) and flux φ(t) at time *t* is given as [22]:

$$M(\emptyset(t)) = \left(\frac{\rho_{off}}{L \times W}\right) \sqrt{D_2 - 2\eta \frac{\rho_{on}}{\rho_{off}} \emptyset(t)\mu}$$

where ρ_{on} and ρ_{off} are the resistivities of the TiO_2 layers with and without oxygen vacancies, respectively. L, W, and D are the length, width, and thickness parameters of the memristor, respectively. The parameter η (±1) is the polarity of the applied voltage signal and μ is the mobility of the ions.

The memristive behaviour is primarily affected by (i)the thickness of the oxide layers or device thickness, *D*, (ii) the lateral dimensions of the device, *L* and *W* and (iii) the doping concentration of the oxygen vacancies in the TiO_2-X layer, μ. From the above equation, variations in the lateral dimensions (L and W) are inversely proportional to the memristance values. The effect of process variation in D on memristance is highly non-linear; memristors are more sensitive to variability near M_{on} than near M_{off}. The memristance values differ by several orders of magnitude (10^3) due to variation. This feature is exploited to produce unique hardware signatures.

C. *Size of the Crossbar-N*

The complexity of performing computation simulation of a nano-PUF depends on: 1) the complexity of the memristor model and 2) the complexity in simulating a crossbar. Memristor simulation models tend to be complex because they include computationally intensive operations such as the integration and square root for each device as shown in the above equation. The simulation of a crossbar is hard as there is an exponential number of paths from an input to an output if the devices at the crosspoints are bidirectional[2].

There are two kinds of paths in a crossbar. In a direct path, current flowing from an input (row) to an output (column) is the function of the resistance of the device at the crosspoint of that input and output. In sneak path, the current flowing from an input to an output is a function of resistance of devices at other crosspoints in the crossbar.

Suppose an attacker wants to simulate the nano-PUF, the attacker has to evaluate the current flowing through all the sneak paths. Increasing the size of the crossbar exponentially increases the number of paths and thereby the attacker's simulation time is exponentially increased. As there is an exponential number of sneak paths and *N* outputs in a crossbar, the simulation time for the attacker is given by $N \times 2^N \times t_{memristor,\ sim}$.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

The size of the crossbar also affects the user's delay in obtaining an output. On applying an input, the current flows in parallel through the sneak paths and reaches the output. As there are N^2 devices in the crossbar, the execution time, t_{exe}, is $N^2 \times Delay_{memristor}$. Notice that increasing the crossbar size exponentially increases the attacker's effort but increases the user's execution time quadratically.

As shown in fig.11 below, even for a 20×20 crossbar, the simulation time is several tens of years (10^9) seconds. However, the user, who has the nano-PPUF, can obtain the response within several microseconds. The difference between the simulation and execution time is 10^{15} seconds andis the basis for a secure time-bounded authentication protocol.

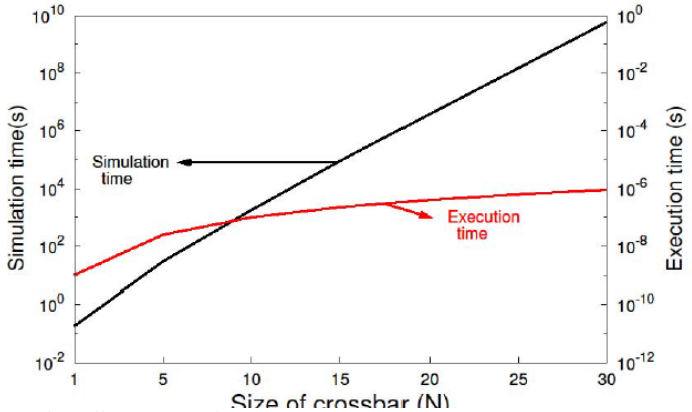


Fig.11. Simulation and execution times for different sizes of memristor basedcrossbar.

D. Polyominoes

A polyomino is a plane geometric figure formed by joining one or more equal squares edge to edge. It is a polyform whose cells are squares. It may be regarded as a finite subset of the regular square tiling. The verifier has to select a section of the nano-PPUF to perform the simulation to authenticate the user.

Polyomino	n
Monomino	1
Domino	2
Tromino	3
Tetramino	4
Pentamino	5
Hexamino	6
Heptamino	7
Octomino	8
Nonomino	9
Decomino	10

Table 1: Polyomino nomenclature according to size.

The constraints on this selection are:

1. The possible number of sections should be exponential. If the number of possible sections is small, the hacker can simulate all possible combinations a priori.
2. The size of the section should be small enough for the verifier to simulate in real time.
3. At least one of the outputs should be a part of this section as the verifier has to verify the user's output with their simulated output. To satisfy these constraints, we use polyomino shapes. The total number of possible polyomino shapes with M cells is exponential as given by the equation [18]:

$$\text{Number of M-ominoes} = \frac{c\lambda^m}{M}$$

where λ and c are 4.0626 and 0.3169, respectively. The verifier will choose any of the polyominoes with at least one of N outputs of the crossbar is in the polyomino. The number of possible polyominoes of size M in an N×N crossbar is

$$\frac{c\lambda^m}{M} \times \text{N}$$

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

Two protocols are described as applications for nano PPUFs: AUTHENTICATION and PUBLIC KEY COMMUNICATION.

E. Authentication

Authentication is as follows, the verifier issues a challenge to the user as an input to the user's nano-PPUF (input set and values). The user executes the challenge on his PPUF and presents the response to the verifier. The verifier simulates one or a few partitions of the user's nano-PPUF to verify that the input and outputs along their boundaries converge to the response provided. Consider the situation where the user requests the verifier to authenticate him. The user has the nano-PPUF.

1. The verifier obtains the simulation model of the user's nano-PPUF from the public registry.
2. The verifier randomly picks a challenge (V_{in1}, V_{in2}, etc.) and sends it to the user.
3. The user applies this challenge to the nano-PPUF that is in his possession. He sends the response (V_{out1}, V_{out2}, etc.) to the verifier. This takes an order of several nanoseconds (ignoring the network delay for now).
4. The verifier picks a subsection of the user's nano-PPUF, say the 2×2 section at the left-bottom verifier of the crossbar in Figure 1. She then requests from the user the voltages at the boundary of the selected section (e.g., V_C, V_D, V_E, V_F) shown as red points.
5. The user measures these voltages and sends them to the verifier.
6. The verifier simulates the selected section for the given challenge and the boundary conditions (V_C, V_D, V_E, V_F), and obtains V_{out1} and V_{out2}. The time to simulate this smaller crossbar is much less than the time taken to simulate the entire nano PPUF.
7. If the user's response matches the verifier's response (obtained by simulation), then she authenticates him.

An attacker cannot know which partitions the verifier may simulate and must simulate the response over the entire nano-PPUF circuit, which is an infeasible task if the circuit is large enough.
Increasing the polyomino size exponentially increases the number of possible polyominoes but also linearly increases the simulation time for the verifier. Fig.12 shown below represents the number of possible polyominoes and the simulation times for different sizes of polyominoes in a 20×20 memristor-based crossbar.

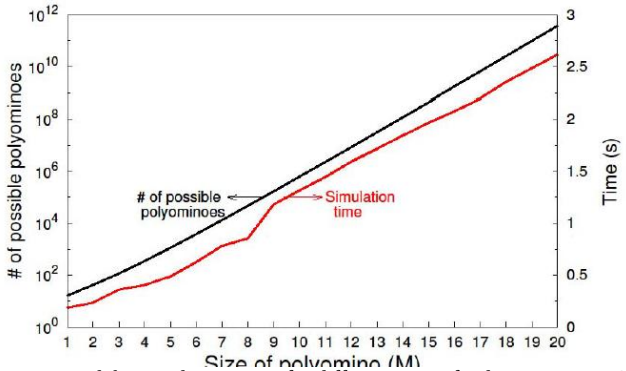


Fig.12. Number of possible polyominoes and the simulation times for different sizes of polyominoes in a 20×20 memristor-based crossbar.

One can infer from Fig.12 that even for a small size of the polyomino such as 20, the number of possible polyominoes is more than a billion. The hacker does not know which of these billion polyominoes that verifier will select for her simulation. With a polyomino size of 20, the simulation time for the verifier is around 2 seconds which is feasible to perform the authentication protocol.

VIII. APPLICATIONS OF NANO PUF

A. Authentication Communication

The verifier issues a challenge to the user as an input to the user's nano-PPUF (input set and values). The user executes the challenge on his PPUF and presents the response to the verifier. The verifier simulates one or a few partitions of the user's nano-PPUF to verify that the input and outputs along their boundaries converge to the response provided. An attacker cannot know which partitions the verifier may simulate and must simulate the response over the entire nano-PPUF circuit, which is an infeasible task if the circuit is large enough.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

B. Public key communication

Public-key communication is achieved as follows, the sender simulates a challenge and response on a partition of the receiver's nano-PPUF, and encrypts his message with the challenge. He transmits the encrypted message along with the response and the input set of the challenge to the receiver. The receiver searches for the input values corresponding to the challenge until the response values are matched. Once the entire challenge is recovered, the message is decrypted. On average, an attacker must simulate a search over half the set of all input values for the given input set, which is exponential in the size of the input set, making the attack infeasible.

VIII. RELIABILITY

I. Polyomino Size-M

Increasing the polyomino size exponentially increases the number of possible polyominoes but also linearly increases the simulation time. The small size of the polyomino such as 20, has a number of possible polyominoes that is more than a biilion.

II. Cross Bar Size

Increasing the crossbar size exponentially increases the simulation time but also quadratically increases the execution time.

III. Unique Responses

Unique responses to analyse the proposed nano-PPUF for producing unique IDs, we used two different metrics: i) the intra-crossbar Hamming distance (Hamming distance between the responses from a crossbar upon application of two different challenges which differ by 1-bit) and ii) the inter-crossbar Hamming distance (Hamming distance between the responses from two different crossbars upon application of the same challenge). Ideally, both of these metrics should be 50%. The output for both of these metrices came out to be 49%.

REFERENCES

[1] MITRE Corporation, "Common Vulnerabilities and Exposures," https://cve.mitre.org/, 1999-2015.
[2] D. Papp, Z. Ma and L. Buttyan, "Embedded systems security: Threats, vulnerabilities, and attack taxonomy," 2015 13th Annual Conference on Privacy, Security and Trust (PST), Izmir, 2015, pp. 145-152, doi: 10.1109/PST.2015.7232966.
[3] G. Hernandez, O. Arias, D. Buentello, and Y. Jin, "Smart nest thermostat: A smart syp in your home," ser. Black Hat, 2014.
[4] J. Kim et al., "A Physical Unclonable Function With Redox-Based Nanoionic Resistive Memory," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 2, pp. 437-448, Feb. 2018, doi: 10.1109/TIFS.2017.2756562.
[5] J. Ohta, Smart CMOS Image Sensors and Applications. London, New York: CRC Press, 2007.
[6] Y. Cao, L. Zhang, S. S. Zalivaka, C. Chang and S. Chen, "CMOS Image Sensor Based Physical Unclonable Function for Coherent Sensor-Level Authentication," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 62, no. 11, pp. 2629-2640, Nov. 2015, doi: 10.1109/TCSI.2015.2476318.
[7] A. E. Gamal et al., "Modeling and estimation of FPN components in CMOS image sensors," in Proc. Int. society for optics and photonics (SPIE), San Jose, USA, Jan. 1998, pp. 168–177.
[8] L. Zhang, Z. H. Kong, C. H. Chang, A. Cabrini, and G. Torelli, "Exploiting process variations and programming sensitivity of phase change memory for reconfigurable physical unclonable functions," IEEE 12 Trans. Inform. Forensics and Security, vol. 9, no. 6, pp. 921–932, June 2014.
[9] E. Socher, S. Beer, and Y. Nemirovsky, "Temperature sensitivity of SOICMOS transistors for use in uncooled thermal sensing," IEEE Trans. Electron Devices, vol. 52, no. 12, pp. 2784–2790, 2005.
[10] L. Lang et al., "Design and validation of arbiter-based PUFs for sub45-nm low-power security applications," IEEE Trans. Inform. Forensics and Security, vol. 7, no. 4, pp. 1394–1403, Aug. 2012.
[11] H. Tian et al., "Analysis of temporal noise in CMOS photodiode active pixel sensor," IEEE Journal of Solid-State Circuits, vol. 36, no. 1, pp. 92–101, 2001.
[12] "Free tool can change SN and IMEI to unlock iphone," 2013. [Online]. Available: http://yjjhen.sinaapp.com/

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 8, August 2020 ||

[13] Y. S. Lee, H. J. Lee, and E. Alasaarela, "Mutual authentication in wireless body sensor networks (WBSN) based on Physical Unclonable Function (PUF)," in *Proc. 9th Int. Wireless Communications and Mobile Computing Conf. (IWCMC)*, Sardinia, Italy, July 2013, pp. 1314–1318.
[14] A. Maiti, I. Kim, and P. Schaumont, "A robust physical unclonable function with enhanced challenge-response set," *IEEE Trans. Inform. Forensics and Security*, vol. 7, no. 1, pp. 333–345, Feb. 2012.
[15] A. Rukhin*et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *NIST Special Publication 800-22 (revised May 15, 2002)*, 2010.
[16] [J. P. Strachan, et al., "The switching location of a bipolar memristor: chemical, thermal and structural mapping," IOP Nanotechnology, vol. 22, no. 25, 2011.
[17] J. Wendt and M. Potkonjak, ''The bidirectional polyomino partitioned PPUF as a hardware security primitive,'' in Proc. Global Conf. Signal Inf. Process., 2013, pp. 257–260.
[18] I. Jensen and A. J. Guttmann, "Statistics of lattice animals (polyominoes) and polygons," Journal of Physics A: Mathematical and General, vol. 33, pp. L257–L263, 2000.
[19]MiodragPotkonjak, VishwaGoudar, "Public Physical Unclonable Functions", Vol. 102, No. 8, August 2014, pp 1149.
[20] JeyavijayanRajendran, Garrett S. Rose, Ramesh Karri, and MiodragPotkonjak, "Nano-PPUF: A Memristor-based Security Primitive", 19-21 Aug. 2012, pp 85-86.
[21] D. B. Strukov, et al., "How we found the Missing Memristor," Nature, vol. 453, pp. 80–83, 2008.
[22] J. Rajendran, et al., "Approach to Tolerate Process Related Variations inMemristor-Based Applications," Intl Conf. on VLSI Design, pp. 18–23, 2011.
[23] Guajardo, Jorge &Skoric, Boris &Tuyls, Pim& Kumar, Sandeep & Bel, Thijs &Blom, Antoon&Schrijen, Geert. (2009). Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions. Information Systems Frontiers. 11. 19-41. 10.1007/s10796-008-9142-z.