CMOS Image Sensor Based Physical Unclonable Function for Coherent Sensor-Level Authentication

Cao, Yuan; Zhang, Le; Zalivaka, Siarhei S.; Chang, Chip-Hong; Chen, Shoushun

2015

Cao, Y., Zhang, L., Zalivaka, S. S., Chang, C. H., & Chen, S. (2015). CMOS Image Sensor Based Physical Unclonable Function for Coherent Sensor-Level Authentication. IEEE Transactions on Circuits and Systems I: Regular Papers, 62(11), 2629-2640.

https://hdl.handle.net/10356/82927

https://doi.org/10.1109/TCSI.2015.2476318

CMOS Image Sensor based Physical Unclonable Function for Coherent Sensor-level Authentication

Yuan Cao, *Student Member, IEEE,* Le Zhang, *Student Member, IEEE,* Siarhei S. Zalivaka, *Student Member, IEEE,* Chip-Hong Chang, *Senior Member, IEEE,* and Shoushun Chen, *Senior Member, IEEE*

Abstract—**In the applications of biometric authentication and video surveillance, the image sensor is expected to provide certain degree of trust and resiliency. This paper presents a new low-cost CMOS image sensor based physical unclonable function (PUF) targeting a variety of security, privacy and trusted protocols that involves image sensor as a trusted entity. The proposed PUF exploits the intrinsic imperfection during the image sensor manufacturing process to generate unique and reliable digital signatures. The proposed differential readout stabilizes the response bits extracted from the random fixed pattern noises of selected pixel pairs determined by the applied challenge against supply voltage and temperature variations. The threshold of difference can be tightened to winnow out more unstable response bits from the challenge-response space offered by modern image sensors to enhance the reliability under harsher operating conditions and loosened to improve its resiliency against masquerade attacks in routine operating environment. The proposed design can be classified as a weak PUF which is resilient to modeling attacks, with direct access to its challenge-response pair restricted by the linear feedback shift register. Our experiments on the reset voltages extracted from a 64×64 image sensor fabricated in 180 nm 3.3 V CMOS technology demonstrated that robust and reliable challenge-response pairs can be generated with a uniqueness of 49.37% and a reliability of 99.80% under temperature variations of 15∼115 °C and supply voltage variations of 3∼3.6 V.**

Index Terms—**Physical Unclonable Function, CMOS image sensor, Device authentication, Trusted integrated circuits, Random number generator, Process variation.**

I. Introduction

DRiven by the Internet of Things (IoT) and smartphone industry, the CMOS image sensor market is expected to hit a total value of $10,172 million by 2020 [1]. A noteworthy growth is envisaged from the proliferation of CMOS image sensors into emerging security applications in biometric authentication, reconnaissance and surveillance [2], [3]. To prevent attackers from exploiting the image sensing system by inserting the unauthorized nodes, the image sensor itself should be trusted [2]. Recently, phishers have also begun to use images to evade detection by text-based anti-phishing filters. While certified cryptographic protocols and infrastructures have been developed for securing the communication channels [4], they cannot prevent false pretenses from masquerading as trustworthy imaging devices in the electronic communications. This security hole can be closed up by integrating dedicated security functions into the image sensor [5]. If the authentication is assured at the sensor level, the camera and its relatively large software stack would no longer need to be implicitly trusted [5]. Researchers have proposed a few sensor-level authentication schemes to provide the integrity and authenticity of image sensors [6]–[8]. The encryption techniques are performed on-chip to guarantee a real end point security, i.e., security that actually starts at the data source and ends at the data receiver. However, this is very demanding and costly. Another drawback about this method is that the private key used for the encryption is generally stored in a non-volatile memory (NVM), such as EEPROM or polysilicon fuses [6]. Unfortunately, these NVM technologies are often vulnerable to invasive attacks as the secrets have to be preserved instead of generated upon demand, and often reside persistently in a digital form [9].

A Physical Unclonable Function (PUF) is a circuit module that generates chip signatures relying on the uncontrollable and unpredictable process variations. The mapping of challenge and response pairs (CRPs) is unique to each PUF instance. The response of the silicon PUF is usually a binary string generated by applying its corresponding challenge. PUF provides a secure and low-cost solution for key generation, device authentication, counterfeit detection and prevention [9]. The small footprint makes it promising for the cost-sensitive sensor market and remote trusted sensing system. In contrast to the IDs stored in NVM, the signatures produced by the PUF cannot be easily removed, copied or compromised, as the secrets are inherent in the physical structure of the PUF. Any invasive or semi-invasive attack on the chip can easily destroy the original secrets. Many silicon PUFs have been proposed and successfully implemented in secure applications owing to the simplicity of their design and fabrication, as well as their compatibility with modern integrated systems [9]–[16].

In this paper, we proposed a new CMOS image sensor based PUF for on-chip authentication and identification. It exploits the dark signal non-uniformity (DSNU) of fixed pattern noise (FPN) in a CMOS image sensor to generate a unique and reliable signature. FPN as a whole refers to the variations in the output pixel voltage values, under uniform illumination, due to the device and interconnect mismatches across an image sensor [17]. It consists of two parameters, DSNU and photo response non-uniformity (PRNU) [18]. The former refers to the offset from the average pixel intensity across the array at a specified setting of temperature and integration time in the absence of external illumination, whereas the latter relates the optical power on a pixel to the electrical signal output. Unfortunately, these patterns are susceptible to the

The authors are with the School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798. Emails: ycao3, lzhang15, zali0001@e.ntu.edu.sg; echchang, eechenss@ntu.edu.sg.

changes in the operating environments such as power supply voltage, temperature and ambient noise. A differential readout is proposed to desensitize the impact of environment variations on the PUF response. This readout scheme enables the PUF reliability and demand on security protocol efficiency to be optimized by a thresholding parameter, making it adaptable for use in different applications. With one response bit per addressable pixel, the proposed PUF can be classified as a weak PUF, which is resilient against modeling attacks [19]. To prevent the adversary from directly accessing the CRPs, a linear feedback shift register (LFSR) is used to generate a fixed internal challenge from an external input and the internal challenge can be reconfigured if necessary. It can be easily implemented on existing image sensors without affecting their original functionality and performance. It eliminates the potential security flaws and vulnerability caused by the separation of image sensing and authentication module without the need for additional encryption module or ancillary PUF circuitry.

The rest of the paper is organized as follows. Related works on sensor-level authentication is reviewed in Section II. In Section III, the design and operations of the proposed PUF are elaborated. The figures of merit and experimental results of the proposed image sensor based PUF are analyzed in Section IV. Promising emerging trusted sensing system applications are identified and discussed in Section V. Finally, the conclusion is given in Section VI.

II. Related Works

The method to identify a camera by the image sensor's imperfection during manufacturing is not new. Related works can be found in the area of image forensics. Previously, the defective pixels (including hot pixels and dead pixels) are used for camera identification [20]. Advanced methods [21], [22] utilize the pixel non-uniformity noise caused by different sensitivity of pixels to light to characterize the individual cameras. These methods can extract unique property of an image sensor, but they do not fulfill the definition and criteria of a PUF. The lack of a native challenge-response mapping makes them incompatible with modern PUF based security protocols such as [23].

Recently, a sensor PUF was proposed in [24]. It is different from the conventional PUFs in that it includes two inputs: a traditional binary challenge and a physical quantity being sensed. An example of a light level sensor PUF based on the optical system similar to the optical PUFs [25] was illustrated. In [26], the notion of virtual proofs (VP) of reality is introduced. Its basic idea is to convert certain external physical property into digital data for authentication. The conversion is accomplished by the so called "witnessed objects" without any secret keys or tamper-proof hardware. The generic concept of VP is extended to a camera of p pixels. As each pixel can have s states, there are p^s possible images. The VP of reality is constructed from the response bits generated from an input image sensed with the help of a light sensor PUF similar to that of [24]. A SIMPL camera was patented in [27]. SIMPL, stands for "SIMulation Possible, but Laborious" [28], is a PUF that comes with a digital simulation and prediction model. The response to a challenge can be simulated by the public simulation model with a significantly lower speed than the real-time response of its physical device. Other than exploiting the execution and simulation time gap to achieve the public-key equivalent cryptography, the SIMPL camera is similar to the PUF based cameras of [24] and [26] in other aspects. It also measures the analog signal of incoming light intensity from the image to generate the digital bits.

Instead of introducing a new and more robust PUF, these methods actually exploit the new features (the sensing functions) of existing PUFs [26] for sensor-level authentication. For example, the light sensor PUF [24] and VPs of destruction and distance in [26] are built upon an optical system likes the optical PUF [25], and the VP of temperature [26] is designed based on a temperature dependent system similar to the Bistable Ring PUF [15]. A conventional PUF was used in [24] to transform the public challenge into a volatile secret initialization vector for the stream cipher and in [27] to realize the SIMPL based public-key authentication. These ancillary PUFs add extra hardware area, power and operational complexity to the sensor chip of the camera. More importantly, the sensed physical quantity for authentication can be easily decoupled from the sensor, which makes them vulnerable to sensor decoupling attack [24]. The light sensor PUF [24] makes use of non-homogeneous coatings to achieve uniqueness and unclonability, which incur additional processing steps, and are not standard CMOS compatible. The non-uniform optical transmittance of the coating applied on the sensor area can reduce its sensitivity and degrade the image quality. Unfortunately, there is no physical implementation reported for all these camera-based PUFs except [26] to assess their costs and performances.

Our proposed sensor PUF is different from the above in that it extracts the digital signature intrinsically from the DSNU of FPN resulting from the manufacturing process variations of CMOS image sensor. As the PUF itself is a monolithic CMOS imager, its device signature can be spontaneously imbedded into the images it took. This offers greater flexibility to use the imaging device for versatile security applications as the camera can be identified reliably independent of lighting conditions. The images taken by the camera can also be directly encrypted or watermarked by the unique signature of the CMOS imager within the camera system. 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 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.

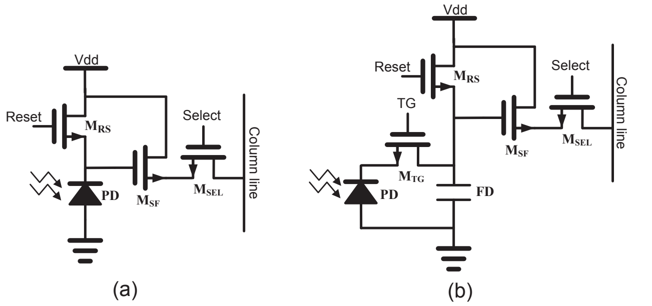


Fig. 1. The schematic of (a) 3T-APS pixel, (b) 4T-APS pixel.

III. Circuits and Operations

A. CMOS Image Sensor 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.

Fig. 1 shows the transistor-level implementations of 3T-APS and 4T-APS [29]. In the 3T-APS, each pixel cell consists of a photodiode (PD), a reset transistor M_{RS}, a select transistor M_{SEL} and a source follower readout transistor M_{SF}. When M_{RS} is turned on, the voltage on the PD is reset to the value:

$$V_{PD} = V_{dd} - V_{th,RS} \tag{1}$$

where $V_{th,RS}$ is the threshold voltage of M_{RS}. When M_{RS} 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:

$$V_{out} = V_{dd} - V_{th,RS} - V_{th,SF} - \frac{I_{ph} \times t}{C_{PD}} \tag{2}$$

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_{RS} and M_{FS}.

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. 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.

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 CDS, are employed in the readout circuits [30]. 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. It is noted that the signal voltage can be read out just after the reset voltage is read out from the 4T-APS. This is essential for the CDS operation and it is achieved by separating the charge accumulation region (PD) from the charge readout region (FD). 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 [29].

B. Proposed Image Sensor based PUF

The response of the proposed PUF is a binary string extracted from the pixel array. Each response bit is obtained by comparing the reset voltages of two pixels. 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 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, other 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 [29] to reduce the 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:

$$V_{rst} = V_{dd} - V_{th,RS} - V_{th,SF} \tag{3}$$

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

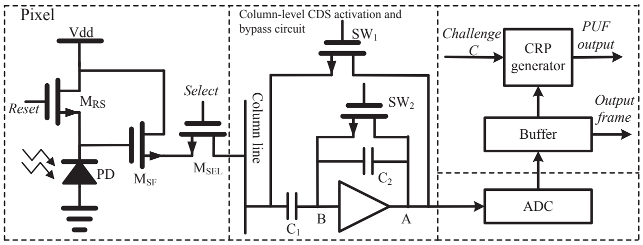


Fig. 2. Architecture of the proposed CMOS image sensor based PUF.

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 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 exposition, 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:

$$n = \log_2 (H \times V) \tag{4}$$

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 LFSR counter. The LFSR is initialized by an arbitrary user selectable n-bit seed N $(0 < N < 2^n)$, i.e.,

$$C' = C \oplus N \tag{5}$$

where $\oplus$ denotes a bitwise XOR operation.

Since $N \neq 0$, $C \neq C'$. 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} is process technology dependent and is determined empirically. P_{th} provides a knob to tune the noise margin of the pixel pairs to stabilize the response bit against temperature and voltage variations. Besides, the entire CRP mappings of the PUF can be reconfigured by selecting a different value of N to initialize the LFSR counter. With a different seed value N, 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 thwart modeling attacks [31]. 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.

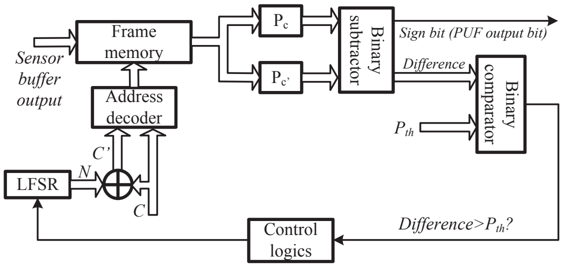


Fig. 3. Architecture of CRP generator circuit.

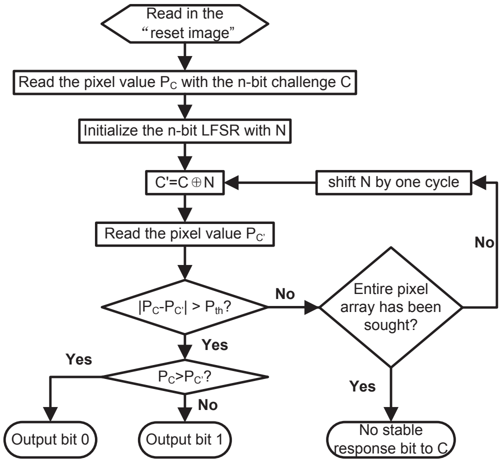

Read in the “reset image”
Read the pixel value P_C with the n-bit challenge C
Initialize the n-bit LFSR with N
C'=C⊕N
shift N by one cycle
Read the pixel value P_C'
|P_C-P_C'| > P_th?
No
Yes
Entire pixel array has been sought?
No
Yes
P_C>P_C'?
Yes
No
Output bit 0
Output bit 1
No stable response bit to C

Fig. 4. Procedure for CRP generation.

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:

$$\begin{aligned} V_{sig} &= V_{rst} - V'_{rst} \\ &= V'_{th,RS} + V'_{th,SF} - V_{th,RS} - V_{th,SF} \end{aligned} \tag{6}$$

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 [32]:

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

where T_0 is the reference temperature and σ_{th} is the threshold voltage temperature coefficient in the range of 0.5∼ 3 mV/K.

Taking the partial derivative of V_{sig} with respect to T,

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

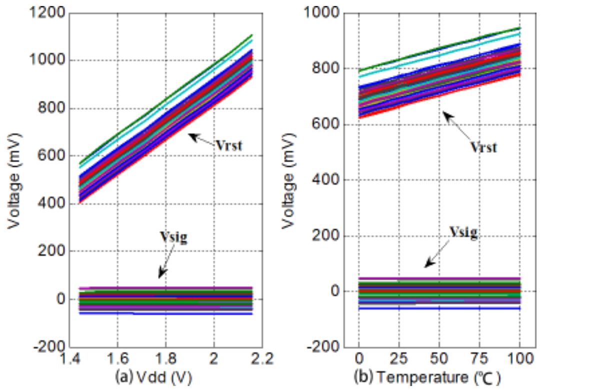


Fig. 5. Monte Carlo simulation results of V_{rst} and V_{sig} against the variations of (a) supply voltage, and (b) temperature.

The differential readout voltage V_{sig} is less sensitive to temperature variation than any single pixel reset voltage V_{rst} as

$$\left|\frac{\partial V_{sig}}{\partial T}\right| < \left|\frac{\partial V_{rst}}{\partial T}\right| = |\sigma_{th,RS} + \sigma_{th,SF}| \tag{9}$$

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). The PDK provided by the foundry contains the variation profile of key parameters in 180 nm CMOS technology. It can well represent the ranges of parameter values of the physical design due to the manufacturing process variations. The Monte Carlo simulation method [13] 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 $100°C$. Each line in the figure represents an instance of the Monte Carlo simulation. 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 [17]. The root mean square (RMS) voltage of the KTC noise is given by [29]:

$$\overline{V_n^2} = \frac{KT}{C} \tag{10}$$

where K is the Boltzmann constant, T is the temperature in Kelvin and C is the photodiode junction capacitance for a 3T-APS or the floating diffusion capacitance for a 4T-APS. For C = 22 fF, the input referred RMS KTC noise voltage is 414 μV at room temperature. Owing to the fact that the reset time is not long enough for the circuit to be in steady state, the actual reset noise is closer to half the commonly quoted KTC value [17]. The RMS voltage induced by the process variations is much larger. Based on the extracted parameters from the PDK of 180nm CMOS process, a Monte Carlo simulation of 1000 runs shows that V_{sig} is Gaussian distributed with mean μ = 250 μV and standard deviation σ = 22.55mV. According to [33],

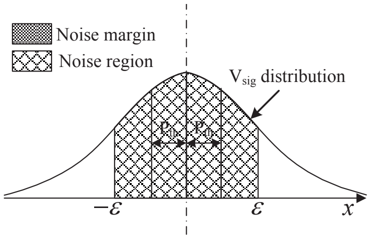


Fig. 6. Effects of P_{th} on PUF reliability and the number of CRPs.

$$\overline{V^2} = \mu^2 + \delta^2 \tag{11}$$

The RMS voltage contributed by the process variation is calculated to be 22.55 mV. This is two orders of magnitude larger than the KTC noise. The margin is more than sufficient for them to be segregated by comparing V_{sig} with a predefined threshold P_{th}, which can be empirically determined and adjusted based on the characterization model of target fabrication process. 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 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. If the CRPs with V_{sig} lying in the range between $-P_{th}$ and $+P_{th}$ are discarded, the statistic mean of the bit error rate (BER) can be calculated by:

$$\overline{BER} = \frac{1}{n}\sum_{i=1}^{n} \Pr(|V_{sig} - P_{th}| < \varepsilon_i) \tag{12}$$

Fig. 7 plots the BER against the parameters P_{th} and $\overline{\varepsilon}$, where $\overline{\varepsilon}$ is the mean of ε. The BER is calculated from one thousand V_{sig} voltages generated by the Monte Carlo simulation using the PDK. Fig. 7 shows the BER decreases with increasing P_{th}. In principle, a BER of 0% can be obtained when $P_{th} > \overline{\varepsilon}$.

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. This trade-off will be further evaluated in our experimental results.

IV. Experimental Results and Discussions

The raw reset voltages required for CRP generation cannot be read out directly from commercially available CMOS image sensors due to the built-in CDS. To evaluate the quality of the proposed PUF, a switch transistor was added into the column-level CDS circuit (see Fig. 2) to bypass the CDS of a 180

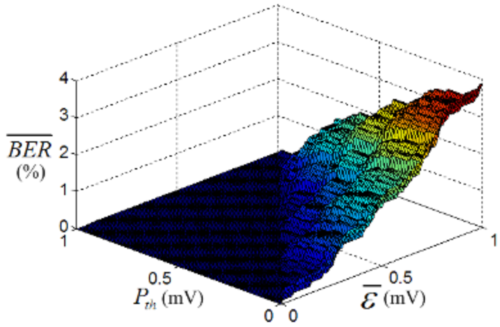


Fig. 7. Simulation results of BER for different parametric combinations of P_{th} and ε.

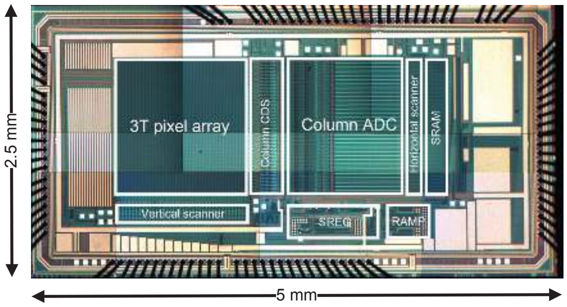


Fig. 8. The microphotograph of the image sensor used for the validation of the proposed PUF.

nm CMOS image sensor chip, which was originally designed for another high-speed imaging project. The CRP generator shown in Fig. 3 was implemented on an off-chip Xilinx Virtex-6 ML605 FPGA board to simplify its communication with the personal computer. Since FPGA can introduce a lot more overheads that are not pertinent to the proposed CRP generator, the implementation overheads in Section IV.D are reported based on the 180nm standard cell synthesis results. The raw data from the CMOS image sensor during the reset phase are read out and processed by the MATLAB scripts. The image sensor ASIC mainly consists of a 64×64 3T-APS array, a column level CDS, an on-chip column level 10-bit ADC, and a readout buffer. The chip microphotograph is shown in Fig. 8. The die area including IO pads is 2.5 mm × 5 mm. Five chips have been packaged and tested. The measured FPN without CDS is 9.82%. To show the higher non-uniformity of the image taken before the FPN is suppressed by the on-chip CDS, the reset image and the pixel voltages of a plain image taken under office lighting after the CDS are measured and compared in the histograms of Fig. 9. The standard deviation of the pixel voltages has been reduced by 68.5% by the CDS from 99.09 in Fig. 9(a) to 31.24 in Fig. 9(b).

Uniqueness, reliability and unpredictability are the three most important figures of merit (FOMs) of a PUF. These FOMs are analyzed in the following experiments. The seed N of the LFSR is fixed at 100 to emulate the direct feeding of arbitrary challenges without logical reconfigurability.

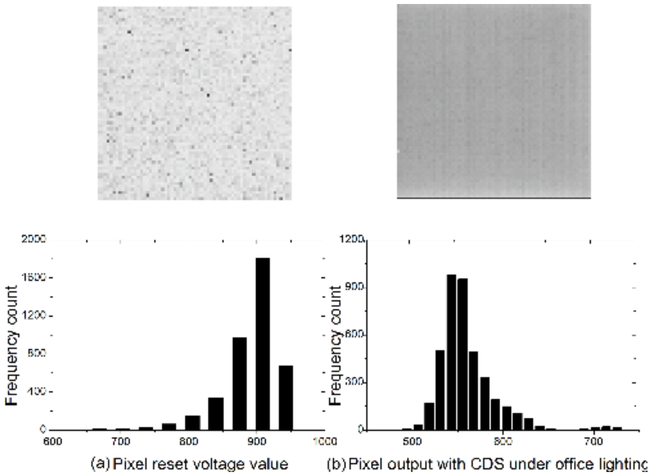


Fig. 9. The distribution of pixel voltage values of the image (a) without CDS and (b) with CDS under office lighting.

A. Uniqueness Assessment

Uniqueness measures how much the CRPs generated by one PUF differ from the other. 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 [34]:

$$U = \frac{2}{m(m-1)} \sum_{u=1}^{m-1} \sum_{v=u+1}^{m} \frac{HD(R_u, R_v)}{n} \times 100\% \qquad (13)$$

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. The simulation is carried out at the transistor-level by Cadence Virtuoso Spectre using the PDK of 180 nm CMOS process technology. Each iteration of Monte Carlo simulation applies a unique set of random variations to the proposed 64×64 image sensor PUF to create a PUF instance, and a number of CRPs are collected from each PUF instance and processed by the MATLAB scripts. 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. 10(a). The uniqueness of these 10,000 instances is calculated to be 50.01%. The best fit Gaussian curve to the histogram has mean μ = 50.09% and standard deviation σ = 4.44%. The 3σ variation of 13.32% accounts for 99.90% of its statistical population.

Physical measurements obtained from the five dice were also used for this evaluation. A total of 8000 CRPs were generated by the five PUFs. Fig. 10(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%. The histogram is well fitted by a Gaussian curve with $\mu = 49.37\%$

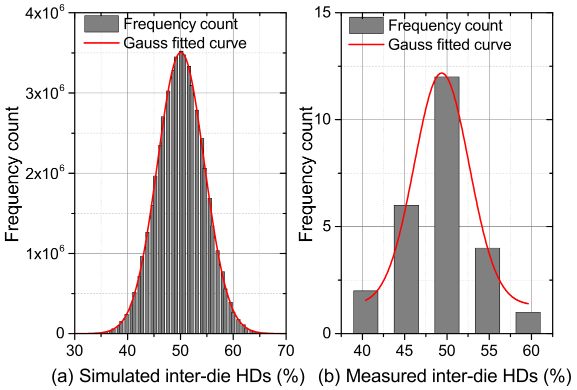


Fig. 10. Frequency distribution of (a) the simulated inter-die HDs for 10,000 PUF instances and (b) the measured inter-die HDs from the five image sensor based PUF chips.

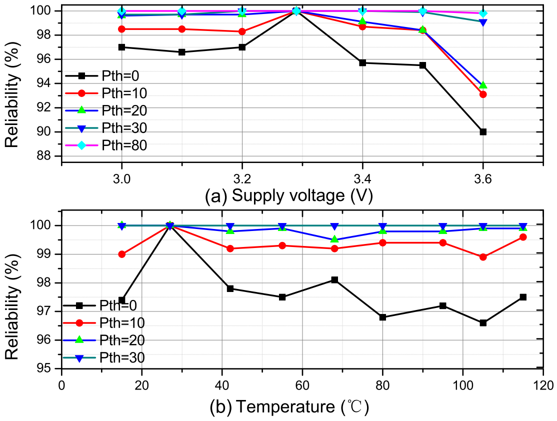


Fig. 11. The measured average reliability of hybrid RO PUF against (a) voltage variations, (b) temperature variations.

and $\sigma = 6.48\%$. The measured results show a good uniqueness and are consistent with the Monte Carlo simulation.

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 BER, which can be characterized by comparing the responses taken at different time with a reference response to the same challenge. 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 $R_{i,j}$ for $j = 1, 2, \cdots, k$. The reliability S for chip i can be expressed as [34]:

$$S = 1 - BER = 1 - \frac{1}{k}\sum_{j=1}^{k}\frac{HD(R_i, R_{i,j})}{n} \times 100\% \quad (14)$$

Fig. 11(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 15°C to 115°C. The CRP collected under 27°C is used as a reference. Fig. 11(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. 12 shows the measured relationship of the threshold voltage P_{th} versus the number of valid pixels and the reliability of the fabricated 64×64 image sensor. As discussed in Section III-C, the number of valid bits decreases with P_{th}, while the reliability increases with P_{th}. Due to the demand for high resolution imaging, modern CMOS image sensors usually have a large number of pixels, which provide enough headroom to have a high P_{th} for enhanced reliability while still preserving a reasonably large CRP space.

C. Unpredictability Assessment

Unpredictability measures how difficult an attacker can predict the CRPs of a PUF. The CRPs of a good PUF are assumed to be unpredictable by any adversary from a subset of CRPs in his possession. This requires the correlation between any two CRPs generated from the PUF to be acceptably small. For instance, if the reset voltage P_A is larger than P_B (which produces a response bit of 1) and P_B is larger than P_C, then the output bit obtained by the comparison of P_A and P_C can be predicted to be 1 with certainty. The unpredictability of a PUF can be estimated by the entropy of its CRPs. The entropy of a discrete random variable X with probabilities $Pr[X = x] = p_x$ is defined as:

$$H(X) = -\sum_{x\in X} p_x \log p_x \quad (15)$$

However, it is very difficult to directly measure the entropy of a PUF exactly. This is because it requires the actual distribution of its CRPs, which is generally unknown. Fortunately, the maximum entropy can be determined by the number of independent output bits of a PUF and used as an estimate of the PUF's unpredictability [9]. 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

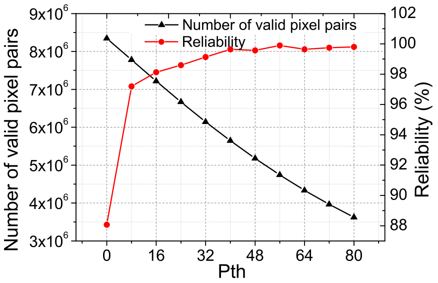


Fig. 12. The measured relationship between P_{th} versus the number of valid pixels and the reliability.

TABLE I
NIST TEST RESULTS ON THE RANDOM SEQUENCES GENERATED BY THE PROPOSED IMAGE SENSOR BASED PUF.

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P VAL	PROP	TEST
11	5	13	8	14	7	15	10	9	8	0.401199	100/100	Frequency
11	13	11	12	11	2	6	7	11	16	0.115387	97/100	BlockFrequency
11	9	3	15	12	11	12	11	12	4	0.181557	100/100	CumulativeSums
10	7	7	15	10	14	7	13	6	11	0.401199	100/100	CumulativeSums
19	9	18	8	8	8	6	9	9	6	0.023545	99/100	Runs
12	11	11	12	9	10	13	6	11	5	0.719747	100/100	LongestRun
5	9	14	6	8	9	18	11	12	8	0.137282	100/100	FFT
12	20	9	8	12	11	11	6	6	5	0.045675	96/100	ApproximateEntropy
11	9	14	7	11	12	13	12	7	4	0.437274	100/100	Serial(forward)
11	11	11	7	15	8	11	12	7	7	0.699313	99/100	Serial(backward)
18	6	4	7	8	12	7	8	13	17	0.015598	97/100	LinearComplexity

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. For example, in the 64×64 sensor, $\log_2(4096!) = 43,250$ independent bits can be found. This is equivalent to 10.56 bits/pixel, which is more than 10 times that of cell based PUF (e.g., SRAM PUF, latch PUF).

While 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 [35]. If they fail to pass the NIST test, the responses are considered as not random enough and may be vulnerable to cryptanalysis. 500,000 response bits generated from the five dies are collected and divided into 100 blocks of 5,000 bits each. Table I shows the results of NIST tests. The uniform distribution across columns C1 through C10 indicates a uniform distribution of the frequency of various P-values. The 11th column indicates the P-value obtained via a chi-square test. The 12th column indicates the proportion of binary sequences that passed testing. The results show that the random numbers generated by the proposed image sensor based PUF have passed all tests, and support the extraction of statistically random numbers from the proposed PUF.

A comparison of the FOMs for the silicon PUFs reported in the literature is summarized in Table II. Except the results of RO PUF [9], Bistable ring PUF [15] and Butterfly PUF [36] , which are reported based on FPGA implementation, the results of the remaining PUFs are obtained from custom chip implementation. Due to the large CRP space of strong PUFs, their area/bit values are negligibly small. 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 variations of 15∼115 °C. This is highly competitive for the hostile operating condition variations that can be achieved among all PUFs in comparison.

TABLE III
RESOURCE USAGE OF CRP GENERATOR IN FPGA.

Component	Number of slice LUTs	Number of slice registers
Subtractor	19	0
Comparator	9	0
Control logics	31	11
LFSR	1	12
Address decoder	134	0
Total	194	23

D. Implementation Overheads

1) Area overhead: The area overhead of our proposed CMOS image sensor based PUF is mainly contributed by the switch transistors and the CRP generator. One switch transistor per column is added to bypass the column level CDS circuitry. This area is negligible as it can be minimized by sizing the transistors with the minimum feature size of the target process technology. In our design, the size of a switch transistor is $W = 460nm$ and $L = 350nm$, which occupies a total area of 0.21 μm^2. The total area incurred by these switches is only 0.00026% of the core area of the image sensor PUF. The CRP generator contributes a fixed overhead irrespective of the pixel array size. Table III shows the resources consumed (estimated by the Xilinx ISE 14.4) for its implementation on FPGA. The total number of LUTs and registers required are 196 and 27, respectively. The CRP generator is also synthesized by Synopsys Design Compiler using the standard cell library of 180nm process PDK. The total area for the CRP generator including the cell area and interconnect area is 63540 μm^2. The CRP generator synthesized using the standard cells (1.8 V power supply) can be integrated with the CMOS image sensor core (3.3 V power supply) in a single die by adding twelve level shifters (ten for the pixel data output, one for the clock input and one for the enable input). Each cross coupled level shifter [42] occupies only 210 μm^2. The area overhead of level shifters does not increase when more independent cells are added.

2) Power overhead: The baseline CMOS image sensor was designed for a high-speed imaging application, which operates at 780 frames per second (fps) at 3.3 V with a power consumption of 300.5mW. The energy consumption per CRP can be calculated as follows. Each frame of 64 × 64 pixel resolution produces 43,250 independent bits, which gives a bit rate of 43,250 b/frame × 780 fps = 33.735 Mb/s. The energy per CRP is 300.5 mW ÷ 33.735 Mb/s = 8.9077 nJ/b. This can be reduced substantially if the PUF is piggybacked on an image sensor targeting for low-power instead of high-speed

TABLE II
COMPARISON OF QUALITIES OF OUR PROPOSED PUF WITH OTHER PUFS.

PUF	Type	Technology (nm)	Area/bit (μm^2)	CRP length (bits)	Uniqueness (%)	Worst case reliability (%)	Reliability conditions	Number of dies for reliability measurement
ISSCC'00 [11]	Weak	350	209	112	NA	95.00	$1.5 \sim 5V, -25 \sim 125°C$	5
DAC'07 [9]	Weak	90	NA	128	46.14	99.52	$1.2 \sim 1.08V, 20 \sim 120°C$	15
VLSI'04 [12]	Strong	180	1.05×10^{-14}	8	23.00	95.20	$\pm2\%V_{DD}, 20 \sim 70°C$	NA
Subthreshold arbiter [13]	Strong	45	NA	64	42.70	82.00	$\pm10\%V_{DD}, 75°C$	4
ISSCC'07 [14]	Weak	130	119	128	50.55	96.96	$0.9 \sim 1.2V$	19
HOST'08 [36]	Weak	65	NA	NA	45.00	94.00	$-20 \sim 80°C$	36
HOST'11 [15]	Strong	NA	NA	NA	50.90	98.70	$-55 \sim 125°C$	1
VLSI'10 [37]	Weak	65	10	128	49.95	100.00	$\pm10\%V_{DD}, 0 \sim 85°C$	14
JSSC'11 [38]	Strong	90	3.50×10^{-21}	NA	NA	99.90	$\pm10\%V_{DD}, 25 \sim 115°C$	50
ISSCC'14 [39]	Weak	22	4.66	256	49.00	99.03*	$0.7 \sim 0.9V, 25 \sim 55°C$	6
ISSCC'15A [40]	Weak	65	25	256	50.14	91.76	$0.6 \sim 1V, 25 \sim 85°C$	6
ISSCC'15B [41]	Strong	40	1.54×10^{-26}	100	50.07	100.00	$0.7 \sim 1.2V, -25 \sim 125°C$	NA
This work	Weak	180	123	120	49.37	88.00 ($P_{th} = 0$) 99.10 ($P_{th} = 30$) **99.80** ($P_{th} = 80$)	$3.0 \sim 3.6V, 15 \sim 115°C$	5

* Reliability is 100% after ECC.

application. For example, if our proposed PUF is applied on a low-voltage 176 × 144 3T-APS CMOS image sensor [43], which operates at 20 fps and dissipates only 48 μW at 1.2 V, the energy per CRP will be reduced to 23.9 pJ/b. The power consumed by our proposed PUF is only a fraction of the total power consumed by the baseline CMOS image sensor. With additional capacitance added onto the column bus, the extra power contributed by the bypass transistor simulated using the 180nm process PDK is 0.33 μW per column. The power consumption due to the bypass transistors in the sensor chip is 0.33 μW × 64 = 21.12 μW. The total power consumption as well as the leakage power of the CRP generator are simulated by Synopsys PrimeTime PX using the same 180nm CMOS process. The random input patterns are fed at a frequency of 100 MHz. The power simulation is performed based on the Monte Carlo method [44] with more than 95% confidence that the error is bounded below 1.5%. The simulated total power consumption and leakage power are 562.40 μW and 15.48 nW, respectively. Hence, the total power overhead due to the proposed PUF is estimated to be 583.54 μW.

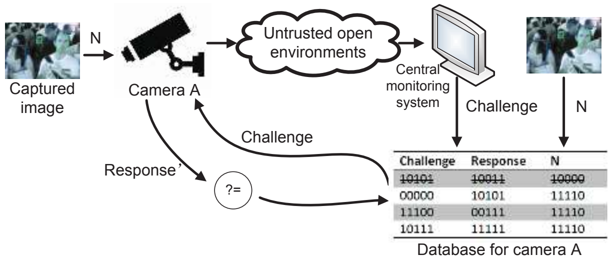
E. Attack Analyses

1) Modeling attack: Modeling attack assumes that the adversary can create a model of the target PUF with a given number of CRPs. With the derived model, other CRPs can be predicted with a high accuracy. Modeling attacks are found to be successfully mounted on some strong PUFs but poses no real threat to weak PUFs [19]. Strong PUFs are PUFs that have exponentially many CRPs per area [45]. Arbiter PUF is an example of a strong PUF. In contrast, weak PUFs have a much smaller number of CRPs per area. In the extreme case, there is only one CRP such as the chip ID of a SRAM PUF. Weak PUFs are usually structured in an array-like architecture, in which many independent devices are abutted and used in parallel to produce the response to a challenge. They do not possess enough CRPs for an attacker to build a prediction model. For example, an additive linear delay model can be constructed by assuming a linear sum of each segment delay along the path of an arbiter PUF [19], but it is not possible to derive an additive linear model from our proposed PUF because the reset voltages of the pixels in the pixel array are independent of each other. The modeling resilience of a weak PUF is attained with the assumption that its challenge-response interface is protected. In our proposed PUF, a LFSR is integrated with the image sensor core to cipher the input challenge and restrict the direct access to its CRP. The address to select the second pixel in the pair is obtained by encrypting (XORing) the input challenge by a LFSR-based stream cipher (see Section III-B). Different seed value of LFSR produces different random number, which causes the original CRPs collected by the attacker to be invalid after the seed value has been changed. Furthermore, the characteristic polynomial can be changed by reconfiguring the properties of LFSR [46]. Such capability makes it extremely difficult for an adversary to predict the proposed PUF output with the currently available modeling attack methodologies [31], [46].

2) Sensor decoupling attack [24]: Sensor decoupling refers to the separation of the sensor from its measured physical quantity. This attack can be easily mounted on the sensor PUFs proposed in [24], [27]. For example, the light sensor PUF can be deployed in a black box to cause an authentication failure or make it reporting the wrong light level. In contrast, our proposed PUF does not mix the measured light level of an image with an input challenge to produce its response. Since the response generated based on the DSNU of FPN is independent of the external illumination, sensor decoupling attack is infeasible for our proposed PUF.

F. Authentication Scheme

Fig. 13 illustrates a possible authentication scheme using the proposed CMOS image sensor based PUF. A trusted party, e.g., an authorized user or a central monitoring system first records the CRPs obtained with different seeds N of the LFSR from the authentic camera in an enrollment phase. The collected data are stored in a secure database. The camera is then deployed in an untrusted or distributed environment. When the identification or the authentication is queried (before the commencement of the transmission of sensitive video stream or triggered by a dubious image or an exceptional activity), the sensor and its image can be mutually authenticated by



Challenge	Response	N
~~10101~~	~~10011~~	~~10000~~
00000	10101	11110
11100	00111	11110
10111	11111	11110

Fig. 13. An authentication scheme using the proposed CMOS image sensor based PUF.

either making the device signature a property of the image or vice versa. The former can be achieved by using the PUF response as a secret key to encrypt the image or as a watermark embedded into the image by the embedded processor of the camera to provide an undeniable proof that the image is taken by the camera. The latter can be achieved by loading the hashed image features (which can be extracted by methods such as abstracted edges, digitized histogram or the Eigen values of the face images) as a seed N of the LFSR before a randomly selected challenge transmitted to the camera is applied to its intrinsic PUF. The generated response of the PUF and the captured image are then sent back to the central monitor for authentication. The same method is applied to the received image to recover the seed N by the central monitor. The authentication is successful only if the response matches exactly or close enough to that recorded in the database for the same challenge and N. This is because except the trusted party, only the authentic image sensor can produce the correct CRP with the seed N extracted from the same image. Here the image feature can be deemed as a means to indirectly reconfigure the CRP space of the PUF to avoid replay (eavesdropping) attacks.

V. Emerging Applications

A. Smart phone Authentication and Anti-counterfeiting

The proposed image sensor based PUF has opened new avenues for low-cost, secure and robust solution for on-chip CMOS image sensor device authentication and key generation. Besides surveillance cameras, one attractive application for this new form of PUF is the smart phone authentication and counterfeit prevention. 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 device IDs are normally kept in the NVM in SIM cards, the hackers can easily copy them to another low-cost refurnished or knockoff cell phones [47]. These cloned phones are virtually indistinguishable from the authentic ones. The proposed PUF is advantageous over the standard secure digital storage for the following reasons:

- Most 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 an enormously large CRP space. For example, the back camera in iPhone 5s has 8×10^6 pixels, which is capable of providing $\log_2(8 \times 10^6!) = 1.72 \times 10^8$ independent CRPs. A larger CRP space is advantageous in enhancing the security of the PUF [45].
- 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 as the secrets 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 inoperable.
- The proposed PUF can be easily implemented with a negligible hardware cost and does not affect or compromise the original functionality and performance of CMOS image sensor.
- 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. Against Virtual Camera Attack

Another promising application for the proposed PUF is the fortification against virtual camera attack [3]. 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. Examples of such cameras are Virtual Webcam, ManyCam, Magic Camera, etc [3]. Virtual cameras pose a severe threat to the surveillance camera system, image sensor based biometric authentication, etc.. Even though the communication between devices and users can be encrypted with provable secure algorithms like AES and DES, the attacker can easily copy the message authentication code (MAC) stored in EEPROM or fuses [48]. 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 can be used to tag the images and video streams produced by its image sensor with a unique and trusted signature which is extremely hard to be copied and compromised by videos or images taken from any other image sensors. Being an intrinsic function of a CMOS image sensor, it avoids the risks of man-in-the-middle, replay and masquerade attacks as the sensor and the authentication module are inseparable [8].

C. Optimize P_{th} for Different Applications

Modern PUF based secure protocols [9] can be used with our proposed image sensor based PUF for authentication. A secure database is required to store a set of CRPs from each image sensor PUF before the use of the sensor. When the authenticity of the sensor is queried, a set of CRPs are chosen randomly from this database and applied to the PUF circuit. The obtained response is compared with the responses stored in the database to authenticate the IC. The authentication is successful when the HD between the CRP stored in the database and the CRP generated by the PUF in use is lower than a predefined value. For strong resilience against masquerade attacks, it is highly desirable that the challenges are never reused [9]. This case mandates a lower P_{th} to support a large number of CRPs as a lower reliability is tolerable by the augmented authentication protocol. On the other hand, when the proposed PUF is used as encryption primitives for secret key generation, a high reproducibility of responses is required under all circumstances including operating in noisy and harsh environments. In this case, a larger P_{th} is required to achieve a high reliability. In summary, the trade-off between the reliability and number of CRPs of our proposed PUF provides an adaptable solution for different security applications.

VI. Conclusion

This paper presents a new CMOS image sensor based PUF. The proposed PUF has been validated on a CMOS image sensor fabricated in 180 nm CMOS technology. The intrinsic IDs measured from the imager core have a uniqueness of 49.37%. A high reliability of 99.80% with ±10% supply voltage variations and temperature range of 15∼115 °C can be attained by tuning the differential threshold P_{th}. As a standard and indispensable component of the surveillance camera and smart phones, the introduction of this integrated security primitive for device identification and authentication has not only enhanced the security of existing sensor level applications but also created exciting new opportunities for the development of security, privacy and trust protocols in distributed and mobile sensing applications.

Acknowledgement

This work is supported by the Singapore Ministry of Education Academic Research Fund Tier I (MOE 2014-T1-002-141). The first author would like to thank J. Guo and G. Xin for their help in collecting the image sensor data, and X. Qian for the helpful comments.

References

[1] "CMOS image sensors market analysis and segment forecasts to 2020," Grand View Research, Inc., San Francciscо, USA, Tech. Rep., May 2014.

[2] D. Serpanos and A. Papalambrou, "Security and privacy in distributed smart cameras," *Proceedings of the IEEE*, vol. 96, no. 10, pp. 1678–1687, Oct. 2008.

[3] S. Chen *et al.*, "Sensor-assisted facial recognition: an enhanced biometric authentication system for smartphones," in *Proc. 12th annual Int. Conf. on Mobile systems, Applications, and Services*, Bretton woods, USA, June 2014, pp. 109–122.

[4] F. Bagci, T. Ungerer, and N. Bagherzadeh, "SecSens - security architecture for wireless sensor networks," in *Proc. 3rd Int. Conf. on Sensor Technologies and Applications, SENSORCOMM '09*, Athens, Glyfada, June 2009, pp. 18–23.

[5] T. Winkler and B. Rinner, "Security and privacy protection in visual sensor networks: A survey," *ACM Computing Surveys (CSUR)*, vol. 47, no. 1, p. 2, July 2014.

[6] P. Stifter, K. Eberhardt, A. Erni, and K. Hoffmann, "Image sensor for security applications with on-chip data authentication," *Proc. the Society of Photo-Optical Instrumentation Engineers*, vol. 6241, p. 8, April 2006.

[7] S. P. Mohanty, "Secure digital camera architecture for integrated real-time digital rights management," *Journal of Systems Architecture*, vol. 55, no. 10-12, pp. 468–480, Oct. 2009.

[8] T. Winkler and B. Rinner, "Sensor-level security and privacy protection by embedding video content analysis," in *Proc. Int. Conf. on Digital Signal Processing (DSP)*, Fira, July 2013, pp. 1–6.

[9] G. Suh and S. Devadas, "Physical unclonable function for device authentication and secret key generation," in *Proc. Design Automation Conf. (DAC'07)*, San Diego, USA, June 2007, pp. 9–14.

[10] T. Addabbo, A. Fort, M. Di Marco, L. Pancioni, and V. Vignoli, "Physically unclonable functions derived from cellular neural networks," *IEEE Trans. Circuits and Systems I: Regular Papers*, vol. 60, no. 12, pp. 3205–3214, Dec. 2013.

[11] K. Lofstrom, W. Daasch, and D. Taylor, "IC identification circuit using device mismatch," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, San Francisco, USA, Feb. 2000, pp. 372–373.

[12] J. Lee *et al.*, "A technique to build a secret key in integrated circuits for identification and authentication application," in *Proc. Symp. VLSI Circuits*, Hawaii, USA, June 2004, pp. 176–179.

[13] L. Lang *et al.*, "Design and validation of arbiter-based PUFs for sub-45-nm low-power security applications," *IEEE Trans. Inform. Forensics and Security*, vol. 7, no. 4, pp. 1394–1403, Aug. 2012.

[14] Y. Su, J. Holleman, and B. Otis, "A 1.6 pJ/bit 96% stable chip-ID generating circuit using process variations," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, San Francisco, USA, Feb. 2007, pp. 406–407.

[15] Q. Chen *et al.*, "The bistable ring PUF: A new architecture for strong physical unclonable functions," in *Proc. IEEE Int. Symp. on Hardware-Oriented Security and Trust (HOST)*, San Diego, CA, USA,, June 2011, pp. 134–141.

[16] R. Maes and I. Verbauwhede, "Physically unclonable functions: a study on the state of the art and future research directions," in *Proc. Towards Hardware-Intrinsic Security*. Heidelberg, Berlin: Springer-Verlag, 2010.

[17] 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.

[18] H. Gou, A. Swaminathan, and M. Wu, "Intrinsic sensor noise features for forensic analysis on scanners and scanned images," *IEEE Transactions on Inf*, vol. 4, no. 3, pp. 476–491, July 2009.

[19] U. Ruhrmair *et al.*, "PUF modeling attacks on simulated and silicon data," *IEEE Trans. Inform. Forensics and Security*, vol. 8, no. 11, pp. 1876–1891, August 2013.

[20] K. Kurosawa, K. Kuroki, and N. Saitoh, "CCD fingerprint method c identification of a video camera from videotaped images," in *Proc ICIP 99*, Kobe, Japan, Oct. 1999, pp. 537–540.

[21] J. Lukas and J. Fridrich, "Digital camera identification from sensor pattern noise," *IEEE Trans. Inform. Forensics and Security*, vol. 1, no. 2, pp. 205–214, June 2006.

[22] X. Kang, Y. Li, Z. Qu, and J. Huang, "Enhancing source camera identification performance with a camera reference phase sensor pattern noise," *IEEE Trans. Inform. Forensics and Security*, vol. 7, no. 2, pp. 393–402, April 2012.

[23] M. van Dijk and U. Ruhrmair, "Protocol attacks on advanced PUF protocols and countermeasures," in *Proc. Design, Automation and Test in Europe Conference and Exhibition (DATE), 2014*, Dresden, German, March 2014, pp. 1–6.

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

[25] R. S. Pappu, "Physical one-way functions," Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, 2001.

[26] U. Ruhrmaier *et al.*, "Virtual proofs of reality and their physical implementation," in *Proc. IEEE Symp. on Security and Privacy*, San Jose, CA, May 2015, pp. 70–85.

[27] M. Stutzmann *et al.*, "Method for security purposes," Europe Patent, 2013, eP Patent 2,237,183. [Online]. Available: http://www.google.com/patents/EP2237183B1?cl=en

[28] U. Ruhrmair, "SIMPL systems: On a public key variant of physical unclonable functions," IACR Cryptology ePrint Archive, 2009. [Online]. Available: https://eprint.iacr.org/2009/255.pdf

[29] J. Ohta, *Smart CMOS Image Sensors and Applications*. London, New York: CRC Press, 2007.

[30] 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.

[31] 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*

Trans. Inform. Forensics and Security, vol. 9, no. 6, pp. 921–932, June 2014.

[32] E. Socher, S. Beer, and Y. Nemirovsky, "Temperature sensitivity of SOI-CMOS transistors for use in uncooled thermal sensing," *IEEE Trans. Electron Devices*, vol. 52, no. 12, pp. 2784–2790, 2005.

[33] C. C. Bissell and D. A. Chapman, *Digital Signal Transmission*. Cambridge University Press, 1992.

[34] 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.

[35] 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.

[36] S. Kumar, J. Guajardo, R. Maes, G.-J. Schrijen, and P. Tuyls, "Extended abstract: The butterfly PUF protecting IP on every FPGA," in *Proc. IEEE Int. Symp. on Hardware-Oriented Security and Trust (HOST)*, Anaheim, CA, June 2008, pp. 67–70.

[37] N. Liu, S. Hanson, D. Sylvester, and D. Blaauw, "OxID: On-chip one-time random ID generation using oxide breakdown," in *Proc. 2010 IEEE Symp. on VLSI Circuits*, Honolulu, HI, June 2010, pp. 231–232.

[38] S. Stanzione, D. Puntin, and G. Iannaccone, "CMOS silicon physical unclonable functions based on intrinsic process variability," *IEEE Journal of Solid-State Circuits*, vol. 46, no. 6, p. 14561463, April 2011.

[39] S. Mathew *et al.*, "A 0.19pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS," in *Proc. 2014 IEEE Int. Solid-State Circuits Conf. (ISSCC)*, San Francisco, CA, Feb. 2014, pp. 278–279.

[40] A. Alvarez, W. Zhao, and M. Alioto, "15fJ/b static physically unclonable functions for secure chip identification with $<2\%$ native bit instability and 140x inter/intra puf hamming distance separation in 65nm," in *Proc. 2015 IEEE Int. Solid-State Circuits Conf. (ISSCC)*, San Francisco, CA, Feb. 2015, pp. 1–3.

[41] K. Yang, Q. Dong, D. Blaauw, and D. Sylvester, "A physically unclonable function with BER $< 10^{-8}$ for robust chip authentication using oscillator collapse in 40nm CMOS," in *Proc. 2015 IEEE International Solid State Circuits Conference*, San Francisco, CA, Feb. 2015, pp. 1–3.

[42] S.-C. Luo, C.-J. Huang, and Y.-H. Chu, "A wide-range level shifter using a modified wilson current mirror hybrid buffer," *IEEE Trans. Circuits Sys. II Regular Papers*, vol. 61, no. 6, pp. 1656–1665, May 2014.

[43] K.-B. Cho, A. Krymski, and E. Fossum, "A 1.2 V micropower CMOS active pixel image sensor for portable applications," in *Proc. IEEE Int. Solid-State Circuits Conf. (ISSCC)*, San Francisco, CA, Feb. 2000, pp. 114–115.

[44] R. Burch, F. N. Najm, P. Yang, and T. N. Trick, "A Monte Carlo approach for power estimation," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 1, no. 1, pp. 63–71, Mar. 1993.

[45] C. Herder, M. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[46] L. Alaus, D. Noguet, and J. Palicot, "A reconfigurable linear feedback shift register operator for software defined radio terminal," in *Proc. 3rd Int. Symp. on Wireless Pervasive Computing*, Santorini, May 2008, pp. 319–323.

[47] "Free tool can change SN and IMEI to unlock iphone," 2013. [Online]. Available: http://yjjhen.sinaapp.com/

[48] 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.

Yuan Cao (S'09) received his B.S. degree from Nanjing University, M.E. degree from Hong Kong University of Science and Technology in 2008 and 2010, respectively. Currently he is working towards the Ph.D. degree in Electrical and Electronic Engineering at Nanyang Technological University. His research interests include hardware security, ASIC physical unclonable function, and analog/mixed-signal VLSI circuits and systems.

Le Zhang (S'11) received the B.Eng. degree from Harbin Institute of Technology, China in 2010. He is now working towards Ph.D at School of Electrical and Electronic Engineering in Nanyang Technological University. He was a visiting scholar to Purdue University in 2013. His current research interests are low-power and process variation tolerant circuits and systems, non-volatile memory, hardware security and physical unclonable function.

Siarhei S. Zalivaka received the B. Eng (Hons.) degree and M.Eng. degree in Belarussian State University of Informatics and Radioelectronics (BSUIR) in 2012 and 2013, respectively. He is currently working towards the Ph.D. degree in the School of Electrical and Electronic Engineering of Nanyang Technological University (NTU). His area of research is Active Metering Schemes for Digital Rights Management, Physical Unclonable Functions.

Chip-Hong Chang (S'92-M'98-SM'03) received the B.Eng. (Hons.) degree from the National University of Singapore in 1989, and the M. Eng. and Ph.D. degrees from Nanyang Technological University (N-TU) in 1993 and 1998, respectively. He served as a Technical Consultant in industry prior to joining the School of Electrical and Electronic Engineering (EEE) of NTU in 1999, where he is currently an Associate Professor. He holds joint appointments with the university as Assistant Chair of Alumni of the School of EEE from 2008 to 2014, Deputy Director of the Center for High Performance Embedded Systems from 2000 to 2011, and the Program Director of the Center for Integrated Circuits and Systems from 2003 to 2009. He has coedited two books, published eight book chapters and more than 200 research papers in refereed international journals and conferences. His current research interests include hardware security and trust, low power and fault-tolerant arithmetic circuits and digital filter design.

Dr. Chang has served as Associate Editor of IEEE Access since 2013, IEEE Transactions on Circuits and Systems-I from 2010-2013, IEEE Transactions on Very Large Scale Integration (VLSI) Systems since 2011, Integration, the VLSI Journal since 2013 and Microelectronics Journal since 2014, and was Editorial Advisory Board Member of Open Electrical and Electronic Engineering Journal and Journal of Electrical and Computer Engineering. He also guest edited several journal special issues and served in many international conference advisory and technical program committees. He is a Fellow of the IET.

Shoushun Chen (M'05-SM'13) received his B.S. degree from Peking University, M.E. degree from Chinese Academy of Sciences and PhD degree from Hong Kong University of Science and Technology in 2000, 2003 and 2007, respectively.

He held a post-doctoral research fellowship in the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology for one year after graduation. From February 2008 to May 2009 he was a post-doctoral research associate within the Department of Electrical Engineering, Yale University. In July 2009, he joined Nanyang Technological University as an assistant professor.

He serves as a technical committee member of Sensory Systems, IEEE Circuits and Systems Society (CASS); Associate Editor of IEEE Sensors Journal; Program Director (Smart Sensors) of VIRTUS, IC Design Centre of Excellence, NTU. His research interests include smart vision sensors, motion detection sensors, energy-efficient algorithms for bio-inspired vision, and analog/mixed-signal VLSI circuits and systems.