A Proposal of PUF Utilizing Pixel Variations in the CMOS Image Sensor

Shunsuke Okura*, Yuki Nakura†, Masayoshi Shirahata‡,
Mitsuru Shiozaki‡, Takaya Kubota‡, Kenichiro Ishikawa*, Isao Takayanagi*, and Takashi Fujino§
*Brillnics Japan Inc., 6-21-12 Minami-Oi, Shinagawa-ku, Tokyo, 140-0013 Japan,
Email: okura.shunsuke@brillnics.com, Phone: +81-3-6404-8728
†Graduate School of Science and Technology Ritsumeikan University,
1-1-1 Noji-Higashi, Kusatsu, Shiga, 525-8577, Japan
‡Department of Science and Engineering Ritsumeikan University
§Research Organization of Science and Engineering Ritsumeikan University

I. Introduction

In order to make the IoT (Internet of Things) a success, the information security will have to be assured and the privacy of the collected data protected [1]. While the security of the communication channel is well developed, the identity theft can be a security hole unless security functions are integrated in the sensor device [2]. In order to define whether images and video sequences were recorded using a specific camera, a camera identification technique which utilizes photo response non-uniformity (PRNU) [3] was proposed. While the technique is effective as long as the illumination level on the focal plane is uniform, the identification pattern generated with PRNU varies depending on various imaging conditions since it depends on the input optical power. A chip ID generation utilizing random telegraph signal (RTS) [4] is also expected to be applied to the CMOS image sensors. The repeatability of the chip ID with RTS is good because of the ID is independent of the illumination. However, each pixel has to be sampled many times to define the ”hot” pixel, during which the normal image capture is disturbed.

For the image information security, we propose a CMOS image sensor with a physically unclonable function (CIS-PUF), which utilizes the pixel-to-pixel fixed pattern noise (PPFPN) as a fingerprint of each device. Though many silicon PUFs, which utilize the device matching of Latch [5], SRAM [6], ReRAM [7], and so on, have been presented, the PPFPN is expected as the most compatible with the CMOS image sensor because (1) a conventional circuit is used to read out the enhanced PPFPN and (2) the uniqueness of the fingerprint pattern is ensured with the large number of pixels. In Sec. II, the concept and diagram of the CIS-PUF are described. Evaluation results of the device ID of 2 Mpixel CIS are reported in Sec. III, followed by a conclusion in Sec. IV.

II. Concept and Operation Diagrams

Figure 1 shows a concept diagram of the CIS-PUF. The imager outputs PPFPN data and a captured image according to the control register setting for a PUF mode and an image readout mode, respectively. The PPFPN data is processed in order to improve repeatability and uniqueness and then to generate a device ID of 128 bit length. In addition to the normal image data, the device ID is embedded in a normal image data and is then read out from the CIS chip for the device authorization. The device ID is not easily copied, since it is not stored in a non-volatile memory which are often

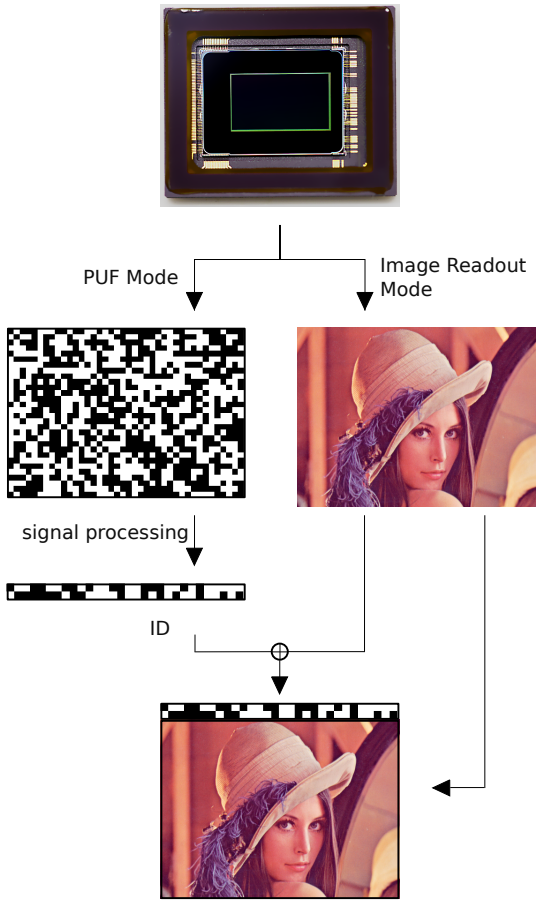


Fig. 1. Concept of the CIS-PUF

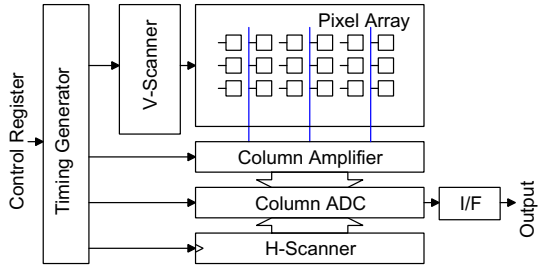


Fig. 2. Block diagram of the CMOS image sensor

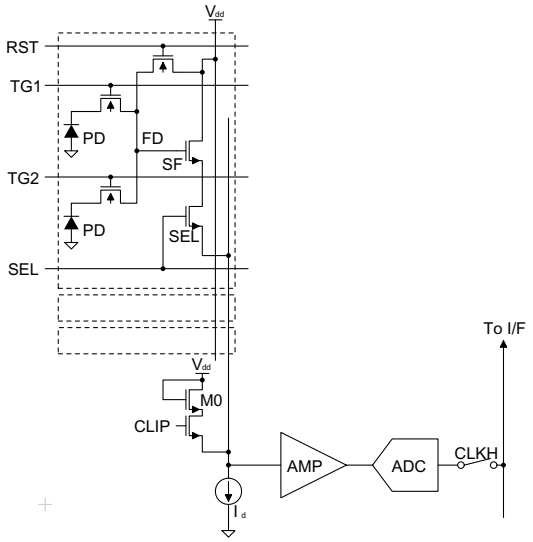
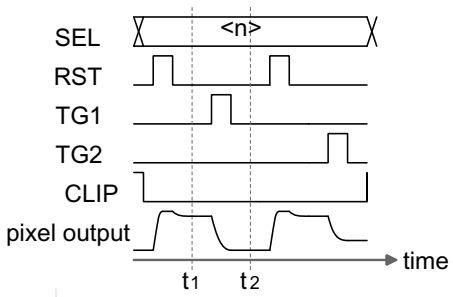


Fig. 3. Block diagram of the column readout circuit

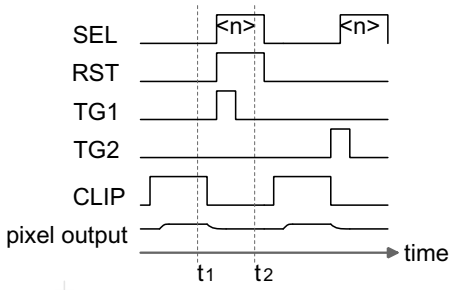
vulnerable to side-channel attacks.

Figures 2 and 3 respectively show a block diagram of a CMOS image sensor and a column readout circuit. The pixel array is composed of 2M pixels, using a 2-shared pixel structure. The vertical scanner controlled by a timing generator drives the pixels, where the control register switches the image readout mode and the PUF mode. The column readout circuit which employs an amplifier, an A/D converter (ADC), and a horizontal scanner processes the pixel output voltage, and then generate the digital output that is fed to the I/F circuit. The clip transistor (M0) is utilized in order to reduce the Vdd/ground bounce during the image readout mode, and also to derive the threshold voltage (Vth) of the pixel SF transistor during the PUF mode.

The timing diagrams of the CMOS image sensor are shown in Fig. 4. During the image readout mode shown in Fig. 4(a), the reset level and the signal level of a selected *n*-th row pixel are respectively read out at t_1 and t_2. The Vth of the SF transistor is then canceled by the subtraction of the reset and signal levels by the correlated double sampling (CDS). On the other hand, during the PUF mode shown in Fig. 4(b), the difference of output levels of a diode connected clip-transistor M0 and SF transistor in a selected pixel on the *n*-th row is



(a) image readout mode



(b) PUF mode

Fig. 4. Timing diagram of PUF mode

read out by respectively turning CLIP and SEL high at t_1 and t_2. Even though the CDS is disabled, this differential double sampling (DDS) derives only the Vth variation and thus the gain of the column amplifier can be set to high in order to reduce the input referred noise. The PPFPN data is read out by the DDS readout of the pixel array, but it is noted that column-FPN is also included in the output data. Variations of threshold voltage of the clip-transistor M0 and bias current I_d result in column-FPN and degrade the uniqueness of the fingerprint pattern. The control sequence of the peripheral circuit is identical for the normal image readout mode and the PUF mode.

Figure 5 shows a diagram of the signal processing to derive the device ID with the PPFPN data. First, the vertically adjacent data of 2-shared pixels are averaged in order to reduce random noise, thereby improving the repeatability of the device ID. Then, the array data is binarized by comparing the vertically adjacent averaged data to each others. Since the variations of a clip-transistor M0 and a bias current I_d are canceled through the comparison, the column-FPN is removed and uniqueness of the device ID is also improved.

Figure 6 shows a result of a Monte-Carlo simulation for the image readout mode and the PUF mode. While the output variation in the image readout mode is only 0.5 LSB at 1σ because of the CDS operation, the variation in the PUF mode is 50.9 LSB at 1σ. In the meanwhile, the random noise of the readout circuit is 1.2 LSB at 1σ. The signal, which is the PPFPN in the PUF mode, to noise ratio is therefore 32.6 dB, resulting in good repeatability of the generated IDs.

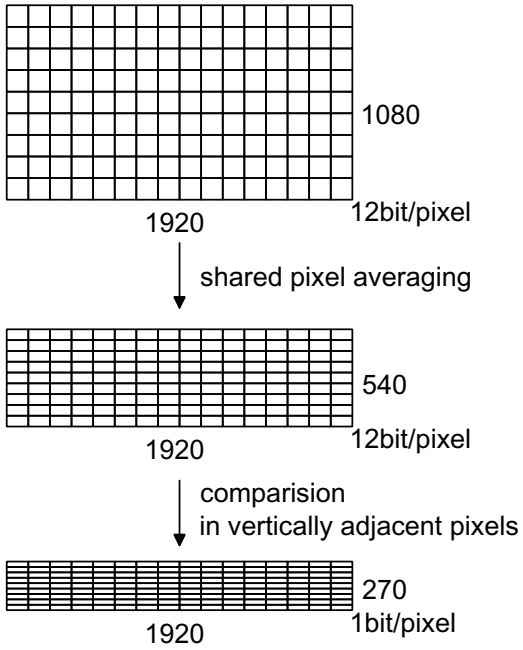


Fig. 5. Key Signal Processing

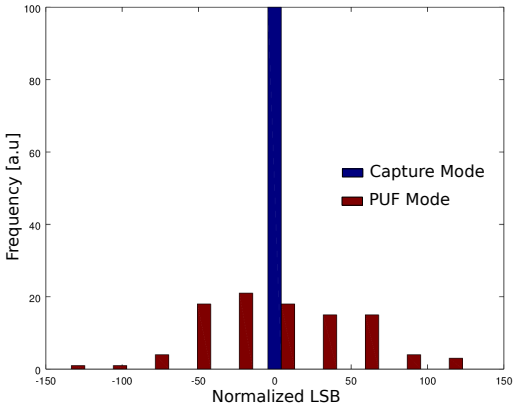
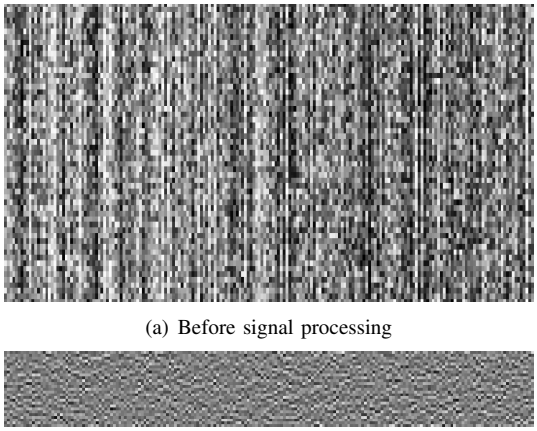


Fig. 6. Monte-Carlo simulation results

III. Evaluation Results

The device ID is evaluated with a 2M pixel CMOS image sensor which operates at 60 fps with 12 bit digital output. The raw data is saved, processed, and analyzed in a PC. The register setting is also transferred from PC to the CIS in order to switch the operation mode between the image readout mode and the PUF mode.

Figure 7 shows an example of a PPFPN data captured with the PUF mode. The data without signal processing shown in Fig. 7(a) includes considerable column FPN, where the column FPN and pixel-pixel variation are respectively 35.9 LSB and 62.1 LSB. The signal processing removes the column FPN by 96.7% as shown in Fig. 7(b), where the column FPN and pixel-pixel variation are respectively 1.2 LSB and 34.0 LSB. The column FPN is negligible small after the signal processing.



(a) Before signal processing

(b) After signal processing

Fig. 7. An example of ID data

In order to quantify the repeatability and the uniqueness of the generated ID, an intra-hamming distance and an inter-hamming distance are utilized. The hamming distance is the number of bits in which the corresponding bit data are different.

intra-hamming distance

The hamming distance evaluated with multiple outputs of a given device represents the repeatability. For instance, 100 frames of PPFPN data are captured with a given CIS, and then averaged to be a reference data. Each of 100 frames of PPFPN data is then compared to the reference data. The bit difference among the compared frame data is caused by the random noise. As long as the noise is zero, the intra hamming distance is 0.0 bits and the same device ID is always repeated.

inter-hamming distance

The hamming distance evaluated with outputs of multiple devices represents the uniqueness. For instance, 100 frames of PPFPN data are captured with 15 CISs, and then averaged in order to neglect the random noise effect. The bit difference in the compared 2 of 15 devices is caused by the device-to-device mismatches. As long as the mismatch is non-correlated, the inter-hamming distance shows the normal distribution where the mean is 50% of bits and the device ID is different to each others among the devices.

Figure 8 shows repeatability and uniqueness of the device ID with hamming distance, in which each frame data is cutout into 128 bits strings for simplicity of the analysis. An intra-distance derived from a given device is only 1.10 bits (=0.86%), which means that the repeatability is very high because PPFPN is larger than the random noise. An inter-distance among the devices is 63.99 bits (=49.99%), which is almost close to the ideal of 50% and means the ID of each device is unique. Since the distribution of the inter hamming distance and the intra hamming distance does not overlap to

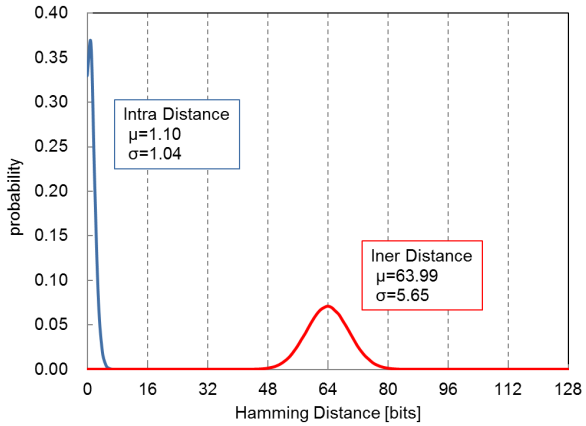


Fig. 8. Repeatability and Uniqueness

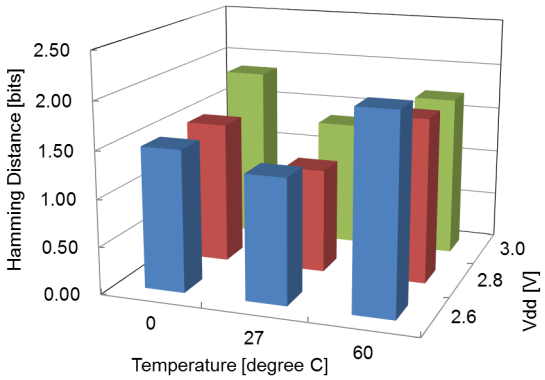


Fig. 9. Repeatability and Uniqueness

each others, the device ID of a given CIS device will not be mis-identified with other devices.

The repeatability is also evaluated under voltage and temperature (VT) variations, over 2.6 V to 3.0 V supply voltage range and 0 °C to 60 °C ambient temperature range. Figure 9 shows the measurement result. The hamming distance is measured, where a single frame PPFPN data at each VT conditions is compared to the reference data that is the average of the 100 frame data at 2.8 V and 27 °C. The repeatability gets the worst at 2.6 V and 60 °C, where the hamming distance is 2.07 bits (=1.62%). The random noise, which increases as temperature increases, is suspected to degrade the repeatability. At lower supply voltages, the back bias effect is small, and thus the transistor mismatch is suspected to be smaller and the S/N ratio decreases.

Table I summarizes the performance of recent silicon PUF devices. Since repeatability and the uniqueness are comparable to other PUFs, CIS-PUF is expected to be available as a fingerprint for the chip authorization.

IV. Conclusion

We have proposed and evaluated CIS-PUF for applications with high security requirements which will be necessary for the upcoming IoT age. With a 2M-pixel CMOS image sensor, PPFPN is derived as a device ID. The uniqueness has been confirmed very high, since the obtained inter-distance of device IDs is 49.99%. The repeatability is robust to the voltage and temperature variations since the intra-distance is 1.62% at the worst corner condition.

The evaluation results suggest that only a few row readout is necessary to generate a reliable 128 bit device ID and the readout operation of the device ID can be finished even in a V-blank period of the image readout. This means that there is no timing overhead for the image readout. Future work is needed to implement a CMOS image sensor in which the reliable device ID is embedded in an image data.

TABLE I
PUF benchmark

	this work	[6]	[5]	[7]
Device	CIS	SRAM	Latch	ReRAM
Temperature [°C]	0 to 60	25 to 85	0 to 80	-40 to 125
Voltage [V]	2.6 to 3.0	0.7 to 0.9	0.6 to 1.2	1.0 to 1.2
Repeatability [%]	1.62	0.97	3.5	0.49
Uniqueness [%]	49.99	48.05	50.01	49.39

References

[1] O. Willers, *et al.*, "MEMS-based gyroscopes as physical unclonable functions," IEICE Technical Committee on CCS, 2016
[2] Y. Nakazawa, *et. al.*, "Security evaluation of on-vehicle distance sensor," Symposium on Cryptography and Information Security, 2016
[3] K. Kurosawa, *et. al.*, "Individual camera identification using correlation of fixed pattern noise in image sensors," Journal of Forensic Sciences, 2009, pp. 639-641
[4] J. Chen, *et al.*, "Further investigations on traps stabilities in random telegraph signal noise and the application to a novel concept physical unclonable function (PUF) with robust reliabilities," Symposium on VLSI Technology, 2015, pp. T40-T41
[5] J. Li, *et. al.*, "A 3.07um2/bitcell physically unclonable function with 3.5% and 1% bit-instability across 0 to 80°C and 0.6 to 1.2V in a 65nm CMOS," Symposium on VLSI Circuit Digest of Technical Papers, 2015
[6] S. K. Mathew, *et. al.*, "16.2 A 0.19pJ/b PVT-variation-tolerant hybrid physically unclonable function circuit for 100% stable secure key generation in 22nm CMOS," IEEE International Solid-State Circuits Conference, 2014, pp. 278-279
[7] Y. Yoshimoto, *et. al.*, "A ReRAM-based physically unclonable function with Bit Error Rate < 0.5% after 10 years at 125°C for 40nm embedded application," IEICE Technical Report, 2016, pp.89-94