A 2-Mpixel CMOS Image Sensor with Device Authentication and Encryption Key Generation based on Physically Unclonable Function

Shunsuke Okura*, Ryota Ishiki†, Syohei Takano†, Masayoshi Shirahata†, Takaya Kubota†, Mitsuru Shiozaki†, Kenichiro Ishikawa*, Isao Takayanagi*, and Takeshi Fujino†
*Brillnics Japan Inc., 6-21-12 Minami-Oi, Shinagawa-ku, Tokyo, 140-0013 Japan,
†Research Organization of Science and Engineering Ritsumeikan University,
1-1-1 Noji-Higashi, Kusatsu, Shiga, 525-8577, Japan

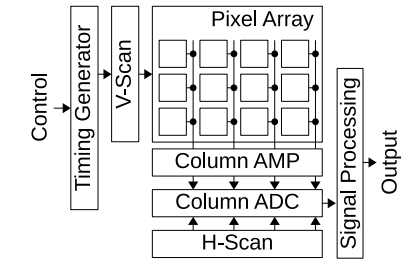
I. Introduction

To make the Internet of Things (IoT) a success, information security will have to be guaranteed. To achieve high enough information security, data confidentiality, data integrity, and device authentication are required. For such functions, the Physically Unclonable Function (PUF) [1]–[5] serves as a unique identifier (ID) and key for a device, based on physical variations caused during the manufacturing process. The strong dependence on the internal parameters makes a PUF a highly tamper-evident ID and key storage without non-volatile memory (NVM). Therefore the PUF can provide security that starts at the data source to prevent attackers from exploiting sensor networks.

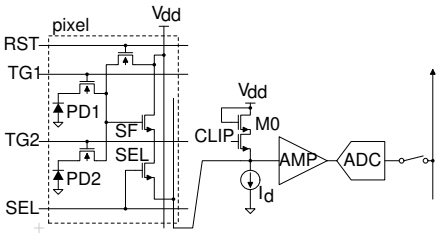
For the image information security, a 2 Mpixel 12 bit CMOS image sensor with a PUF (CIS-PUF) is proposed [6], in which the pixel-to-pixel fixed pattern noise (PPFPN) is utilized as a PUF ID of each device. The CIS-PUF based device authentication is realized by a challenge-response (CR) authentication, whose scheme consists of two phases, *enrollment* and *verification*. During the enrollment phase, the whole PUF ID bits derived from the pixel array are recorded by the verifier. During the verification phase, the verifier issues a challenge that is a randomly selected pixel address. The CIS must respond with the one string of PUF ID which fits the challenge the verifier issued. The verifier issues a different challenge each time, and thus knowing a previous correct response is of no use.

The PUF can moreover be used to generate keys for cryptographic purposes such as data confidentiality and integrity, effectively binding the key to the hardware. The secret key initially generated is recorded by a host device. The CIS-PUF regenerates the key on demand to encrypt the image data, in which the key must be 100% recovered for the decryption by the host. In order to generate a cryptographic key removing noise present in the PUF response measurement, post-processing is required. For CIS-PUF, a dynamic soft-decision error correction is proposed which realizes high error correction capability with small circuit overhead [7].

In this paper, evaluation results of the CR authentication are described. For the cryptographic purpose, a novel topology to generate a true random number required for the error correction is proposed.



(a) Chip overview



(b) Column readout circuit

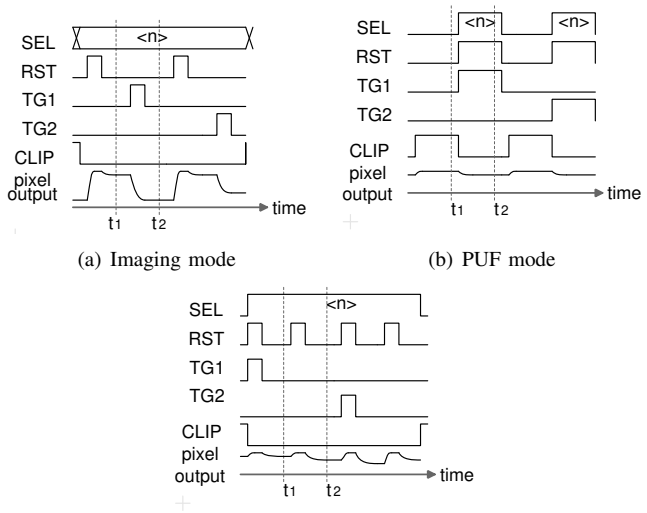
Fig. 1. Block Diagram

II. Overview of CIS-PUF

A. Chip Overview

Figure 1 shows a chip overview of the CIS and a column readout circuit. The pixel array is composed of 2 Mpixels, using a 2-shared pixel structure. The vertical scanner controlled by a timing generator drives the pixels, where control registers switch the pixel operation mode among an imaging mode, a PUF mode, and a true random number generator (TRNG) mode. The column readout circuit processes the pixel output voltage and generates a digital output to a signal processing circuit.

The timing diagrams are shown in Fig. 2. During the imaging mode shown in Fig. 2(a), the reset and signal levels



(a) Imaging mode (b) PUF mode

(c) TRNG mode

Fig. 2. Timing diagram of CIS operation modes

TABLE I
READOUT SIGNAL ON EACH OPERATION MODE

Mode	Imaging	PUF	TRNG
Optical Signal	**readout**	removed	canceled
Vth variation	canceled	**readout** (100 mV_{pp})	canceled
kTC noise	canceled	**readout** (10 mV_{pp})	**readout**

of a selected *n*-th row pixel are respectively read out at t_1 and t_2. The threshold voltage (Vth) of the SF transistor and the kTC noise frozen on the FD is canceled after CDS.

During the PUF mode shown in Fig. 2(b), the difference in output levels of clip-transistor M0 and SF in the *n*-th row is obtained from the readout signals at t_1 and t_2. This differential double sampling (DDS) derives the Vth variation and random noise. The Vth variation is around 100 mV_{pp}, since the SF transistor size is very small to maximize PD fill factor. The DDS output is therefore dominated by the fixed Vth variation rather than the random noise that will be around 10 mV_{pp}. A PUF response bit is 1 or 0 given by the comparison of vertically adjacent shared pixels. While the pixel-to-pixel FPN data of the pixel array is read out, a column FPN caused by variations of M0 and bias current I_d is also read out. The comparison between the vertically adjacent pixels removes the column FPN and improves the uniqueness of the PUF response. The whole PUF response bit length of a 2 Mpixel CIS is 518.4 kbit ($= 1920 \times 1080/2/2$), because of the shared pixel structure and the vertical comparison.

During the TRNG mode shown in Fig. 2(c), the FD is reset before both t_1 and t_2. The uncorrelated kTC noise frozen on FD are read out after the DDS, removing both the optical signal integrated in PD and the threshold voltage of the SF transistor. The FD capacitance is around 1 fF and the DDS output will be around 10 mV_{pp}. The readout signals are summarized in Table I.

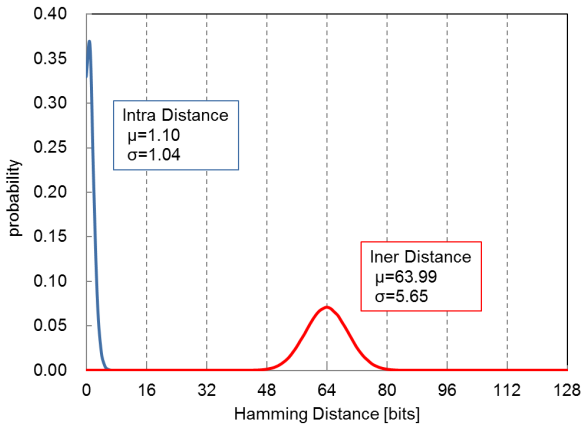


Fig. 3. Repeatability and Uniqueness

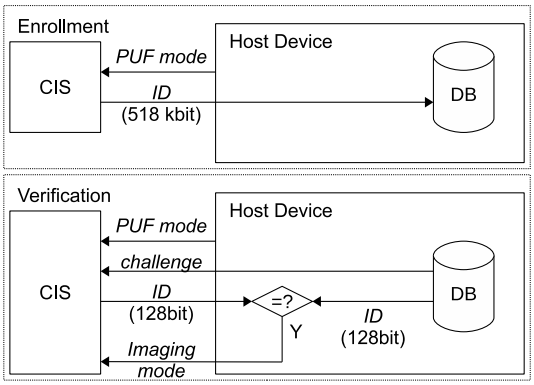
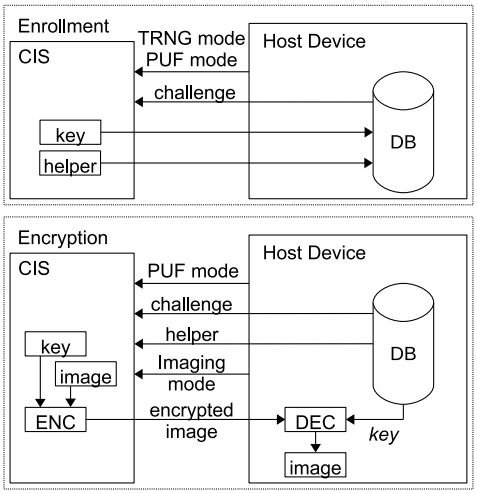


Fig. 4. Operation diagram of CR authentication

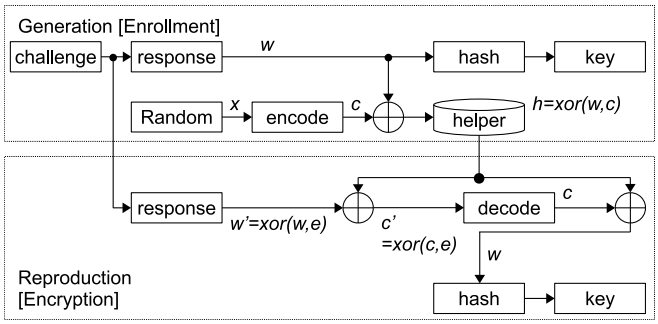
The PUF response is evaluated with hamming distance (HD) as an example shown in Fig. 3 [6]. An intra-distance derived from a given device is affected by the random noise, and means the repeatability of the response. An inter-distance among the different devices means the uniqueness of the response, whose value is ideally 50%. As long as the distribution of the intra-distance and the inter-hamming distance does not overlap to each others, the PUF response of a given device will be identified with other devices.

B. Device Authentication

The PUF response is utilized as a device ID for the device authentication. Figure 4 shows the scheme of the CR device authentication given by an enrollment and a verification phases. In the enrollment phase, the CIS is set to the PUF mode and transfers the whole PUF ID bits to be stored in secure database DB in a host device. In the verification phase, the CIS receives a pixel address as the challenge and then transfers 128 bit length of PUF ID, that start from the received address, to the host. The host device can identify the CIS device if the HD between the response transferred from the CIS and that stored in the DB is lower than a given threshold value considering the random noise, and then set the CIS to



(a) A scheme of image encryption



(b) Fuzzy extractor circuit

Fig. 5. Image encryption scheme using PUF key

the imaging mode. The authentication can be carried out 3840 times, since challenge-response pairs cannot be reused in order to avoid replay attacks.

C. Key Generation and Fuzzy Extractor

Figure 5(a) shows a scheme of image encryption which is also given by two phases. In an initial enrollment phase, the CIS generates a PUF key and helper data according to a given challenge. The key and the helper data are stored in a host device. In an image encryption phase, the CIS receives the same challenge and the helper data to reproduce a key that is coincident with the key stored in the secure host DB. The reproduced key is utilized to encrypt images captured at the imaging mode. The encrypted images are decrypted by the host with the key stored in the DB. As shown in Fig. 5(b), a fuzzy extractor in the CIS-PUF generates the key and the helper data in the enrollment phase and reproduces the key correcting error caused by random noise in the image encryption phase. During the generation, the CIS is set to the TRNG mode, and a random x is measured. Then, the CIS is set to the PUF mode, and a PUF response w is measured for the given challenge. The fuzzy extractor derives the initial key from the response w and computes the helper data h with c and w, where the random number x is encoded to c with error-correcting code. During the reproduction, a PUF response w' is measured for the same challenge. The response w' will not be exactly the same as the initial w due to the random noise e. However, the reproduction procedure is able to recover the secret key by using the previously produced helper data h. The error correcting code can recover the code c by decoding the xor of w' and h. The secret w is then recovered by the xor-ing of the recovered c and the helper data h so that the secret key is reproduced. The random x should be unpredictable in order to hide the secret key because the response w can be revealed with the random x and the public helper data h.

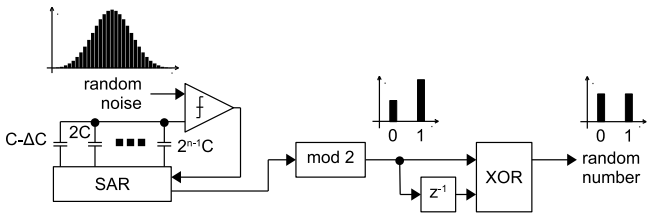


Fig. 6. Block diagram of random number generator

In order to provide the unpredictable random x, the true random number is generated from the pixel array in the TRNG mode. The block diagram of the random number generator is shown in Fig. 6. The random noise readout from the pixel array, which shows normal distribution, is applied to the column SAR ADC. The random noise is readout twice and then xor-ed following to a mod 2 function. Now, let's suppose that the LSB capacitor in the column SAR ADC is smaller than the ideal value, even though the DNL of the ADC is less than 0.5 LSB. The probability of LSB 1 will be higher than that of LSB 0. In this case, the probability of 1 at the mod 2 output is higher than that of 0, which means that number could be predictable. Therefore, in order to improve the randomness, the xor is utilized. A string of random number is generated from the random noise of the multiple number of pixels in the array.

III. Evaluation and Simulation Results

A. Device Authentication

Figure 7 shows a evaluation environment, in which a 2 Mpixel CIS is mounted on a camera board. The device authentication is demonstrated, in which the FPGA process the pixel variation to generate the PUF ID.

Figure 8 shows false negative rate (FNR) and false positive rate (FPR) calculated from the measurement data. When the threshold HD is 0 bit, a true device will be always misidentified as a false device. When the threshold HD is 128 bit, a false device will be always misidentified as a true device. From this measurement results, it is confirmed that the authentication error rate will be less than 1×10^{-9} as long as the threshold is set among 12 bit and 29 bit. This device authentication capacity will be enough in the *trillion* sensors universe in the IoT world.

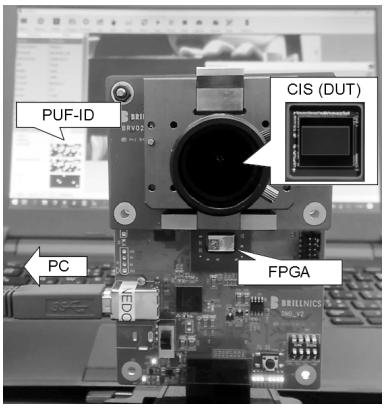


Fig. 7. Evaluation environment

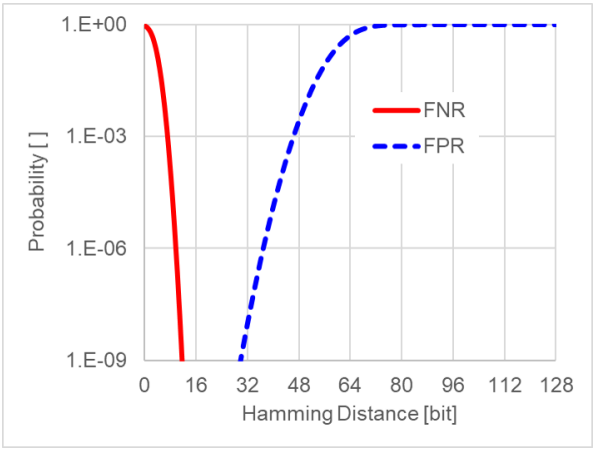


Fig. 8. evaluated FNR and FPR

B. Key Generation

For the cryptographic purpose, the key extraction and recovery are simulated 620×10^3 times with the measured PUF response. The Reed-Muller (RM) code, which is often used in wireless communications applications, is utilized as the error correction code in the fuzzy extractor. The RM(16,5,8) is more redundant than RM(8,4,4), but has better error correction capability. With RM(8,4,4), the key recovery fails 476 times and the error rate is only 0.077%. With more redundant RM(16,5,8), all key recovery are successful and the error rate is less than 0.00017% taking into account the finite number of key recovery operations.

The random number derived from the pixel random noise is also evaluated. Figure 9 shows a histogram of a taken random noise, which shows normal distribution. As shown in Table II, the probability of 0 and 1 before xor is $50\% \pm 0.18\%$. The probability of 0 is lower than 1, which results in "not" true random number. After the xor, the frequency of 0 and 1 is improved to $50\% \pm 6.2 \times 10^{-4}\%$, which passes the validity criteria of the NIST random number test [8]. It is also confirmed that the unpredictable true random number is generated from the pixel array.

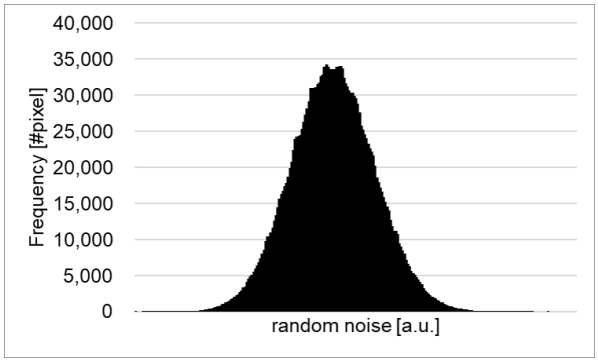


Fig. 9. Histogram of random noise

TABLE II
BIT PROBABILITY OF RANDOM NUMBER

	before XOR	after XOR
0	49.82%	49.99938%
1	50.18%	50.00062%

IV. SUMMARY

The device authentication based on PUF is demonstrated with CIS and FPGA. The misidentificaiton rate is less than 1×10^{-9}, that will be required for the *trillion* sensors universe. For the cryptographic purpose, a novel TRNG based on pixel random noise is proposed. It is confirmed that the random number is not predictable according to the NIST random number test, where the frequency of 0 and 1 is almost constant as $50\% \pm 6.2 \times 10^{-4}\%$.

ACKNOWLEDGMENT

This work is based on results obtained from a project commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

REFERENCES

[1] J. Li and M. Seok, in *Symp. on VLSI Circuits*, June 2015, pp. C250–C251.
[2] Y. Yoshimoto, Y. Katoh, S. Ogasahara, Z. Wei, and K. Kouno, in *Symp. on VLSI Technology*, June 2016, pp. 1–2.
[3] O. Willers, C. Huth, J. Guajardo, and H. Seidel, *IEICE Technical Committee on CCS*, 2016.
[4] J.Chen, T. Tanamoto, H. Noguchi, and Y. Mitani, in *Symp. on VLSI Technology*, June 2015, pp. T40–T41.
[5] Y. Cao, L. Zhang, S. S. Zalivaka, C. H. Chang, and S. Chen, *IEEE TCAS-I*, vol. 62, no. 11, pp. 2629–2640, Nov 2015.
[6] S. Okura, Y. Nakura, M. Shirahata, M. Shiozaki, T. Kubota, K. Ishikawa, I. Takayanagi, and T. Fujino, in *International Image Sensor Workshop*, 2017, pp. 66–69.
[7] S. Okura, R. Ishiki, M. Shirahata, T. Kubota, M. Shiozaki, K. Ishikawa, I. Takayanagi, and T. Fujino, in *2018 ISPACS*, Nov 2018.
[8] L. E. Bassham, III, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, E. B. Barker, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, "Sp 800-22 rev. 1a," Tech. Rep., 2010.