A Proposal of Efficient Error Recovery Method Utilizing Output Characteristics of CMOS Image Sensor PUF

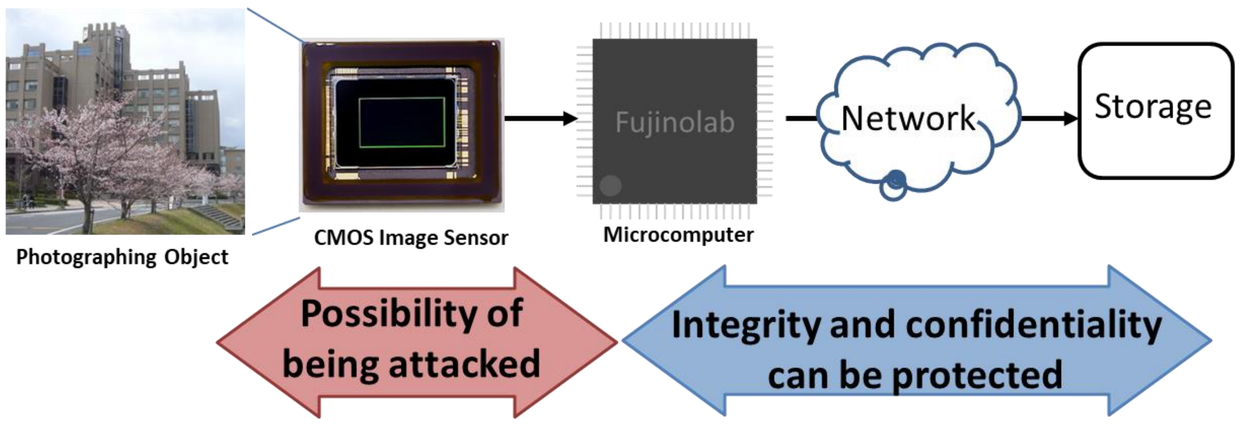
Masayoshi Shirahata*, Shunsuke Okura**, Takaya Kubota*, Mitsuru Shiozaki*,
Kenichiro Ishikawa**, Isao Takayangi**, and Takeshi Fujino*
*Ritsumeikan University, **Brillnics Japan Inc.

Background

Information security on sensor devices implemented on IoT nodes is essential. If the signal from the sensor to the microcomputer is not protected, the data can be falsified before being transferred to the next microcomputer.

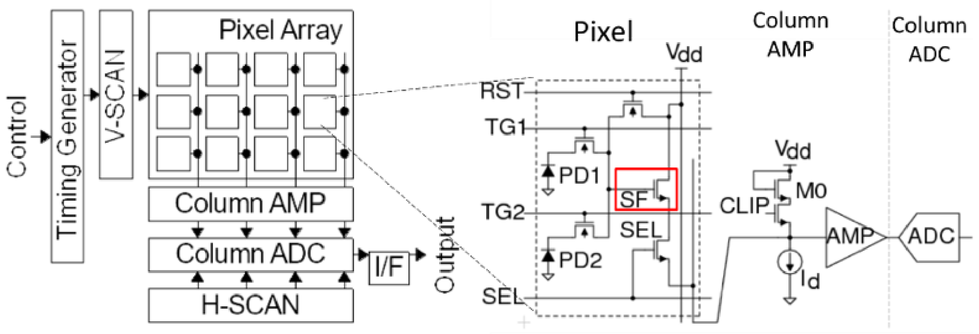
CMOS image sensor PUF (**CIS-PUF**) had been proposed[1,2], however, the output of PUF ID is not stable. Therefore, the error recovery of PUF ID is required when PUF ID is used as a cryptographic key.

In this work, we propose two methods for stabilization of CIS-PUF ID. One is an improved method of soft decision error correction based on reference [3,4]. Another is a method by masking the unstable bits in advance.



CIS-PUF Circuits and Operations

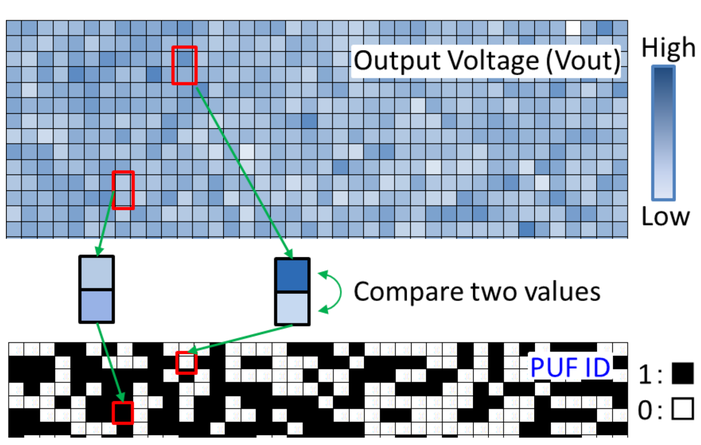
Normal CDS※ operation is not performed in order to obtain variations in output [1,2]. (※CDS : Correlated Double Sampling)
The variations in the output are mainly characteristic variations of SF Tr.



(a) Chip overview (b) Column readout circuit

Block Diagram of CMOS image sensor

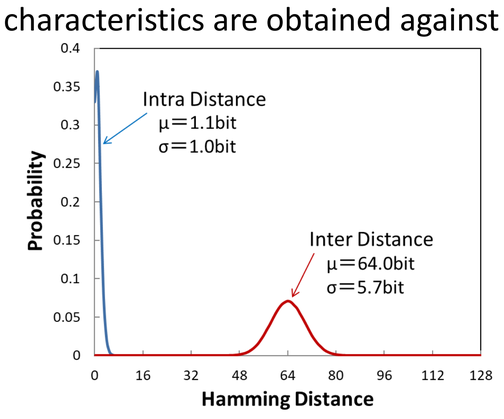
Generating 1/0 is done by comparing magnitudes of 2 adjacent output[1].
By this method, it is possible to eliminate global variations in output and to obtain good random 1/0 data.

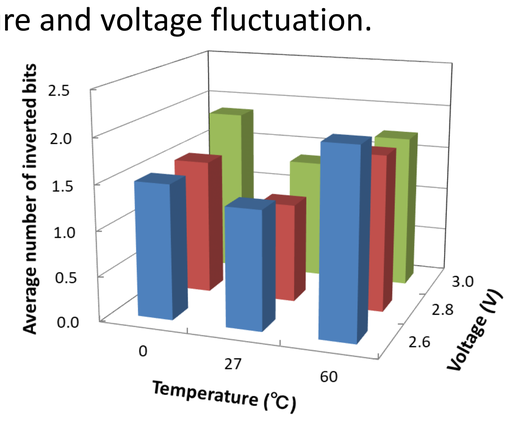


Typical output and ID

Data and Discussion

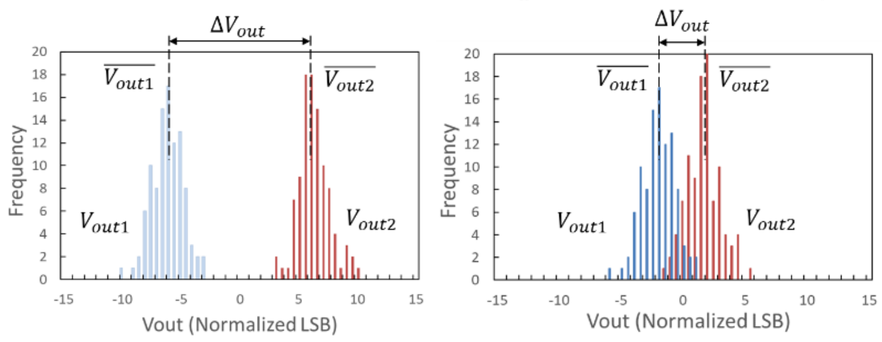
Data was acquired from the actual CMOS Image Sensor CHIP of Full HD (2M pixels).
In the evaluation in units of 128bits, the intra distance is 64bits(Uniqueness 50%)、Intra Distance is 1.1bit(bit inversion ratio 1.6%). Good characteristics are obtained as PUF.
Good characteristics are obtained against temperature and voltage fluctuation.





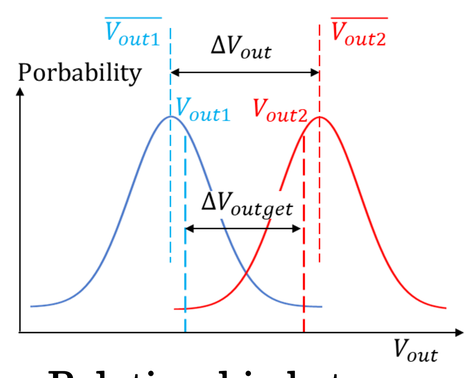
Performance of CIS-PUF

It is possible to estimate the bit stability from the difference of the average output.
There is a difference between the output of the single measurement and the average output due to the influence of noise.
By assuming the variation distribution, it is possible to estimate the average output difference from the difference of the single measurement output.



(a)Stable PUF ID (b) Unstable PUF ID

Typical Vout data measured 100 times

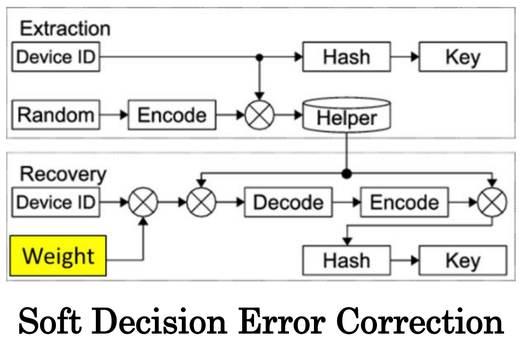


Relationship between ΔVoutget and ΔVout

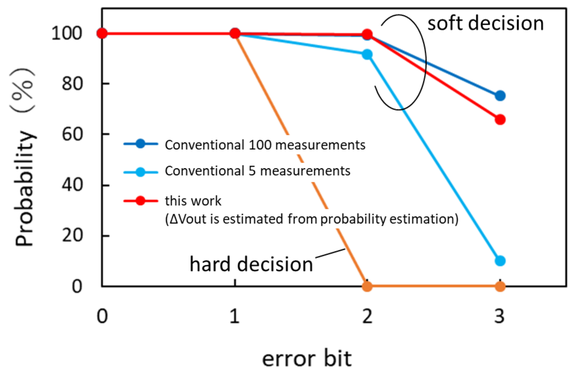
Two proposals for stabilization of CIS-PUF ID

1. Improved soft decision error correction

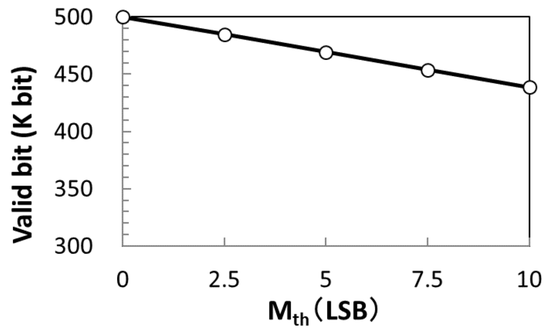
The weight is taken into consideration at key regeneration as with other soft decision algorithms[1,2].There is no need to record the weight to helper data and a repetition code is not required.
Accuracy is equivalent to 85 iterations of the conventional method[3] and helper data size is 1/8 in the case of using RM(8,4,4)



Soft Decision Error Correction for CIS-PUF



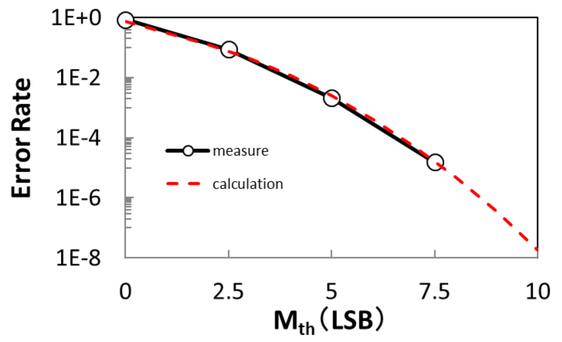
Comparison of Error Correction against Error Bit



Valid bit vs Mask Threshold

2. A method by masking the unstable bits in advance

The pair output is masked If the difference between the two outputs is less than Mth.
The error rate can be lowered to 1E-8 if the masked and not used bits are 10%.
Since CIS-PUF has low computing ability (it is not the minimum line process), the next task is a proposal of a system that reduces the calculation load at CIS-PUF.



Error Rate vs Mask Threshold

Conclusion

- The PUF output using the characteristic variation of the CMOS image sensor is shown. It was the first time our group got data from Full HD CIS (2M Pixels).
- We proposed two countermeasures against bit flip which can not be eradicated from PUF. Both proposal methods make use of the characteristics of CISPUF.
- One is an estimation method of weight for soft decision.
  The weight can be estimated by one PUF measurement at key regeneration. The helper data size is the same as hard decision and no need for repetition code.
- Another is a method by masking the unstable bits in advance.
  The error rate can be controlled by adjusting Mth.
- We will consider how to use each proposal depending on the application of CIS-PUF for the next research.

References

[1] Y. Cao *et al.*, *IEEE TCAS-I*, vol. 62, pp. 2629–2640, Nov 2015.
[2] S. Okura *et al.*, *International Image Sensor Workshop*, 2017, pp. 66–69.
[3] R. Maes *et al.*, *International Workshop on Cryptographic Hardware and Embedded Systems*, 2009, pp. 332–347.
[4] L. Vincent *et al.*, *International Workshop on Cryptographic Hardware and Embedded Systems*, 2012, pp. 268–282.

Acknowledgements

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