A Physical Unclonable Function Chip Exploiting Load Transistors' Variation in SRAM Bitcells

S. Okumura[1], S. Yoshimoto[1], H. Kawaguchi[1] and M. Yoshimoto[1, 2]
[1]Graduate School of System Informatics, Kobe University, [2]JST CREST
E-mail: s-oku@cs28.cs.kobe-u.ac.jp

Abstract - We propose a chip identification (ID) generating scheme with random variation of transistor characteristics in SRAM bitcells. In the proposed scheme, a unique fingerprint is generated by grounding both bitlines. It has high speed, and it can be implemented in a very small area overhead. We fabricated test chips in a 65-nm process and obtained 12,288 sets of unique 128-bit fingerprints, which are evaluated in this paper. The failure rate of the IDs is found to be 2.1×10^{-12}.

I. Introduction

For many applications, a unique identification (ID) on each chip is necessary to prevent illegal copying of secret information [1]. For instance, a radio frequency identification (RFID) tag and chip validation must have unique IDs. In conventional methods, chip IDs are provided by laser fuses or writing data to ROM. These methods, however, necessitate additional costs or fabrication processing. Recently, to address this issue, physical unclonable functions (PUFs) using inherent transistor variation have been proposed [2]. The fingerprint generated by a PUF is unpredictable. Therefore, the PUFs cannot be reproduced using a manufacturing process. In this paper, we introduce a PUF chip which is applied SRAM for generating fingerprint.

II. Proposed Fingerprint Generating Scheme Using SRAM

In a conventional SRAM PUF [3], an initial value stored to bitcells at power-on is applied as a fingerprint. However, in the conventional scheme, it is difficult to initialize data of the bitcells after the device is once powered on; the device can no longer generate fingerprint repeatedly because the power-on takes a long time to discharge their internal node voltages completely.

We therefore propose a chip ID generation scheme that realizes repeatable generations of fingerprints using SRAM. Fig. 1 presents the proposed circuit for generating chip IDs. In the figure, a bitcell represents a commonly used 6T. In the proposed scheme, the fingerprint is generated by the control of the bitlines and VBC in a bitcell. Adding nMOSes on a bitline pair (BL and BL_N) is the modification made to the write driver. They are controlled using a BLCTRL signal. The additional driver is so simple that the area overhead is 3.52 μm^2 in each column of the bitcell array, which is attributable to the additional write drivers. In the proposed fingerprint generating scheme, we ground both bitlines simultaneously by asserting the BLCTRL signal when making an ID.

Fig. 2 portrays simulated waveforms focusing on the "low-and-low" writing scheme. The internal nodes (N0 and N1) in a bitcell are discharged by control of the BCSW, BLCTRL, and WL signals; the internal nodes are fully discharged, although VBC remains at the V_{th} of the load pMOSes in bitcell. Next, negating WL cuts off the access transistors. Finally, either internal node charges up to the supply voltage by negating the BCSW and BLCTRL. Each bitcell stores a unique value depending on the variation.

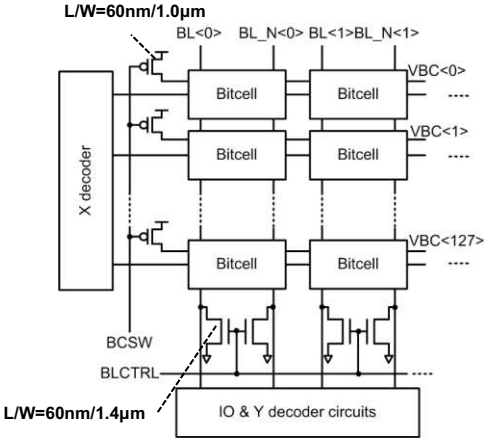

Fig. 1. SRAM architecture with additional nMOS write drivers and pMOS switches for VBC.

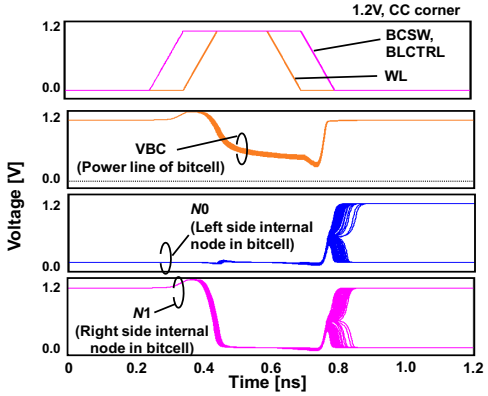

Fig. 2. Simulation waveforms in the proposed scheme.

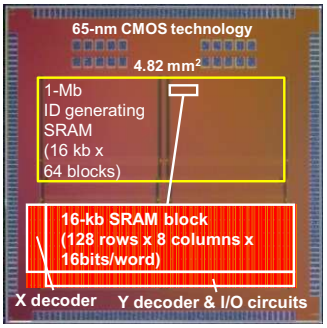

Fig. 3. Photograph of a 1-Mb SRAM test chip and the layout of a 16-kb block.

978-1-4673-3030-5/13/$31.00 ©2013 IEEE

III. Measurement Results and Conclusion

We designed a test chip in a 65-nm CMOS technology and obtained generated random data patterns by measurement. Fig. 3 presents a die photograph of a 1-Mb SRAM and the 16-kb block layout. The 16-kb block consists of 128 rows × 8 columns × 16 bit/word. This SRAM can function as a normal SRAM.

Next, we present discussion of the repeatability of the generated fingerprint. To investigate the repeatability, a fingerprint generation test is used 100 times on 12,288 rows: The fingerprint data length is 128 bit, which is placed in a single row in an SRAM block. Fig. 4 depicts the measured Hamming distance distribution. To calculate the Hamming distance, we obtained the most-likely response (MLR). The MLRs are expected values that are stored in each bitcell at fingerprint generating operation. The fingerprint generated in the same bitcell row is compared to the MLR. Then we calculate a Hamming distance. In the proposed scheme, the average value (μ) is 3.90. The standard deviation (σ) is 1.70 in the Hamming distance metric. The repeatability of the proposed scheme is improved compared with the conventional scheme.

As a uniqueness test, 12,288 samples were measured. Fig. 5 depicts the measured Hamming distance distribution and the approximate curve. "Known device" denotes that the fingerprint is generated by a registered device, and compared to MLR data that are recorded beforehand from the same device. "Latent device" means that the fingerprint generated by the other devices is compared to MLRs. For latent devices, the average and standard deviation of the Hamming distance are 63.64 and 5.74, respectively, and the mode value of the Hamming distance is 64. If the 128-bit fingerprint is generated randomly, then the average and standard deviation values are 64 and 5.65, respectively; probably the proposed scheme generates random series data.

Next, we discuss the failure rate of identification. Presuming that a generated fingerprint is identifiable where the Hamming distance is zero or less than a threshold, t, then the identification failure rate is changed by t. For chip identification, there are error probabilities of two kinds: The false alarm rate (FAR) corresponds to the authentication failure of registered devices. The false detection rate (FDR) corresponds to authentication of a latent device as a registered device. A worse rate of FAR and FDR is recognized as an identification failure rate.

To calculate the identification failure rate, the hamming distance distributions of the known and latent devices are utilized. The histograms in Fig. 5 shall have binominal distribution, B(n, p), where n is 128 (= the number of bitcells in a fingerprint) and p is a mismatch probability in a single bitcell. The fitted curves with binominal distribution and their parameters are also shown in Fig. 5; p in the fitted curve can be obtained as μ / 128 from the measurement.

Fig. 6 shows the identification failure rate when t is varied. The minimum identification failure rate at the 1.2 V and at room temperature (25°C) is 3.5×10^{-13} when t is 24. The worst identification failure rate at 1.1 V is 2.1×10^{-12} when t is 25. The identification failure rate can be increased easily because, in the proposed scheme, numerous SRAM bitcells are embedded on a chip and the bit length can be extended easily.

Acknowledgment

The VLSI chips in this study were fabricated in the chip fabrication program of VLSI Design and Education Center (VDEC). The authors would like to thank H. Fujiwara, M. Yabuuchi, H. Nakano, H. Kawai, K. Nii and K. Arimoto of Renesas Electronics Corporation.

References

[1] M. Y. Wang, et. al., IEEE Trans. on VLSI Systems, vol. 18, no. 4, pp. 541-552, 2010.

[2] W. Choi, et. al., IEEE Conference on CIT, pp. 2323-2328, 2010.

[3] D. E. Holcomb, et. al., IEEE Trans. on Computers, vol. 58, no. 9, pp. 1198-120, Sep. 2009.

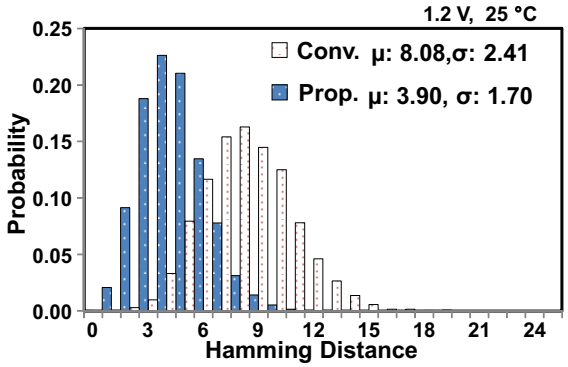

Fig. 4. Histograms of the measured Hamming distance.

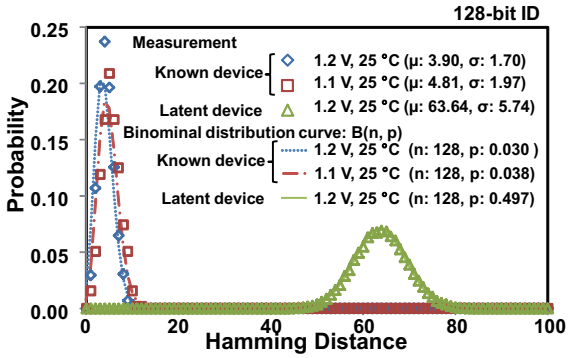

Fig. 5. Histograms of the measured Hamming distance.

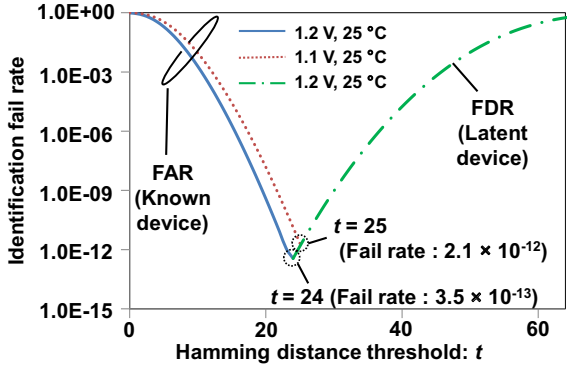

Fig. 6. Identification failure rates.