A 128-bit Chip Identification Generating Scheme Exploiting SRAM Bitcells with Failure Rate of 4.45×10^{-19}

Shunsuke Okumura[1], Shusuke Yoshimoto[1], Hiroshi Kawaguchi[1], and Masahiko Yoshimoto[1,2]
[1]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 in write operation. The generated fingerprint mainly reflects threshold voltages of load transistors in the bitcells. We fabricated test chips in a 65-nm process and obtained 384 sets of unique 128-bit fingerprints from 12 chips, which were evaluated in this paper. The fail rate of the ID was found to be 4.45×10^{-19} at a nominal supply voltage of 1.2 V and at room temperature. This scheme can be implemented for existing SRAMs through minor modifications. It has high speed, and is implemented in a very small area overhead.**

I. INTRODUCTION

For many applications, a unique identification (ID) on each chip is necessary to prevent illegal copying of secret information [1–2]. 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 [3]. 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 [4]. The fingerprint generated by PUF is unpredictable. Therefore, the PUFs can not be reproduced using a manufacturing process. To identify a registered chip, a challenge-response pair (CRP) recorded in a database is referred. The proposed scheme for a chip ID is a kind of PUF.

Lostrom presented extraction of a fingerprint with variation in a transistor current [5]. Statistical delay variation and threshold voltage (V_{th}) mismatch of cross-coupled NOR circuits were exploited to generate a chip fingerprint [6–7]. These approaches necessitate implementation of special circuits on the chip. A fingerprint generating scheme using SRAM is also proposed [8–9]. In a conventional SRAM PUF, an initial value stored to bitcells at power-on is applied as a fingerprint. The data are determined by the V_{th} mismatches of the transistors composed the bitcells. 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 a new fingerprint because the power-on takes a long time to discharge their internal node voltages completely. This disadvantage is unsuitable for use of a fuzzy extractor [10], which improves the PUF's reliability; it must measure responses many times to extract the most likely response. We therefore propose a chip ID generation scheme that realizes repeatable generations of fingerprints using SRAM. The proposed scheme achieves low-power and high-reliability fingerprint generation by modifying a write driver and power switches in the SRAM. This scheme is suitable for application to devices such as RFIDs, which require low-power operation.

II. CONVENTIONAL FINGERPRINT GENERATING SCHEME

We introduce the conventional fingerprint generation scheme using SRAM. Figure 1(a) shows a bitcell representing a commonly used six-transistor (6T) cell that has an inverter couple (load transistors, L0 and L1; drive transistors, D0 and D1) and access transistors (A0 and A1). When a device is powered on, VBC is charged to VDD from the ground. A unique datum is stored in each bitcell. We portray simulation waveforms in the conventional scheme [8–9] in Fig. 1(b). The results are derived from Monte Carlo simulation using HSPICE. The conventional scheme is executed at (i) in Fig. 1(b), and random data are stored in the internal nodes, N0 and N1. To refresh the unique data, "0" is written to the bitcell at (ii). Then VBC is turned off by shutting down to initialize the internal nodes in the bitcell. However, the internal voltage of N0 is not completely grounded in a short time. Moreover, it takes a long time to be discharged completely. Consequently, the written data affect the conventional fingerprint-generating scheme; the newly generated fingerprint has some relation to the past state. Even if the VBC is powered on again after 20 ns, the voltage of internal nodes reverts to the past "0" state at (iii); this is not random. A unique datum cannot be generated by the conventional scheme after the device is powered on.

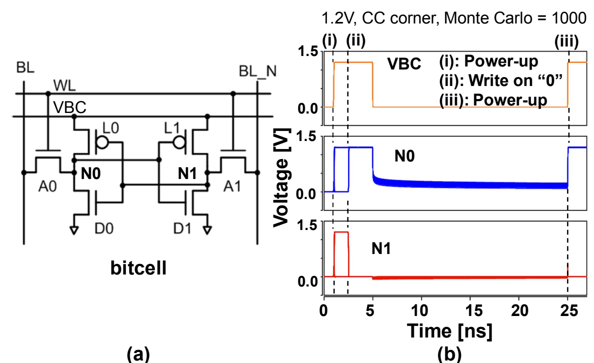


Figure 1. (a) 6T bitcell and (b) simulation waveforms in the conventional scheme.

III. PROPOSED FINGERPRINT GENERATING SCHEME

Figure 2 presents the proposed circuit for generating chip IDs. In the figure, a bitcell represents a commonly used 6T. However, other topologies such as an 8T bitcell [11] are applicable to the proposed scheme. 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. In the general write operation, a datum is written to a bitcell by charging a bitline to a supply voltage and discharging the other bitline to ground. In contrast, we ground both bitlines simultaneously by asserting the BLCTRL signal when making an ID.

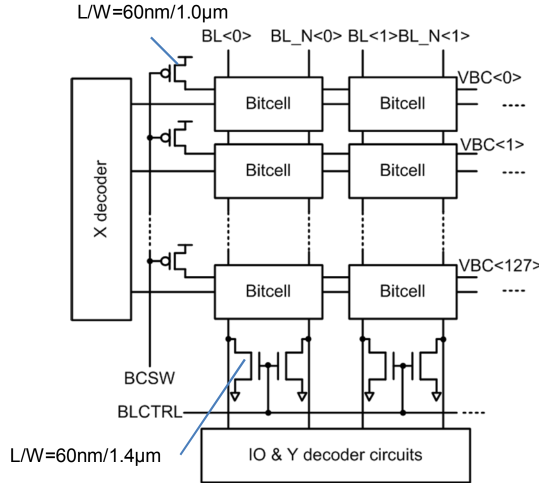


Figure 2. SRAM architecture with additional nMOS write drivers and pMOS switches for VBC.

In the proposed scheme with grounding of both bitlines, continuous current flows from a “high” node in a bitcell to the additional bitline driver. The internal nodes can not be fully discharged to the ground because of the effect of the respective V_{th} of the pMOSes (L0 and L1). Therefore, we add a pMOS switch to the VBC line to ground the internal nodes and to improve the reliability of the fingerprint generation operation. The VBC is divided horizontally and controlled by the BCSW signal; VBC is in a floating state on a row-by-row basis when BCSW is “high”. Because of the VBC switches, continuous current does not flow. The internal nodes are fully grounded. The additional driver and switch are so simple that the area overhead is 1.63%.

The fingerprint-generating procedure takes three steps: First, a data row must be initialized. All bitcells are written to “low” (or “high”) because old uneven data affect a newly generated fingerprint. Next, in the target data row, “low-and-low” writing is conducted. Then random data are generated. Finally, they are read out and processed to produce a unique ID.

Figure 3 portrays simulated waveforms in the “low-and-low” writing scheme. First, the internal nodes (N0 and N1) in a bitcell are discharged by control of the BCSW, BLCTRL, and WL signals. The internal nodes (N0 and N1) are fully discharged, although VBC remained at the V_{th} of the pMOSes (L0 and L1). Next, negating WL cuts off the access transistors. Finally, either internal node in the load transistors (L0 and L1) charges up to the supply voltage by negating the BCSW and BLCTRL. Each bitcell stores a unique value depending on the variation.

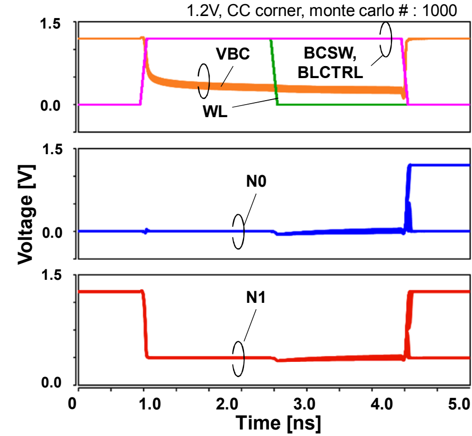


Figure 3. Simulation waveforms in the proposed scheme.

In the proposed scheme, although the internal nodes are fully discharged, the node voltages must not have absolutely equal value. The leakage currents from VBC to the internal nodes differ because they flow through the load transistors; their V_{th} mismatch produces the voltage difference between N0 and N1, and affects the generation of data. Compared with the conventional scheme, the proposed scheme has better repeatability because the generated data are strongly affected by the unique V_{th} of the load transistors. Figure 4 shows the distribution of the drive and load transistor’s V_{th}. Although N0 tends to be “high” in the opposite case if L0 has a higher V_{th} and L1 has a lower V_{th}, then N0 tends to be “low”. The variation in the drive transistors gives less influence than that in the load transistors, meaning the V_{th}s of the load transistors are the most sensitive to randomness.

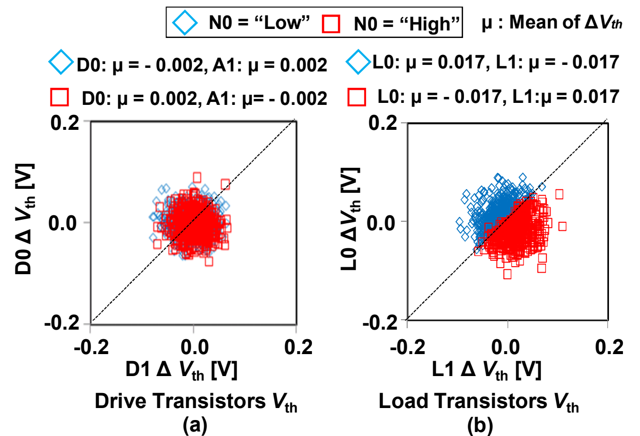


Figure 4. Distribution of V_{th}s in a) drive transistors and b) load transistors.

Next, we compare the power consumption with conventional scheme. Figure 5 depicts the simulation results of power consumption per bit. The conventional scheme must fully charge all nodes in the bitcells at the power-on phase.

However, the power consumption can be reduced in the proposed scheme because VBC is not fully discharged. Compared with the conventional scheme, the proposed fingerprint generating scheme uses 42.6% less power.

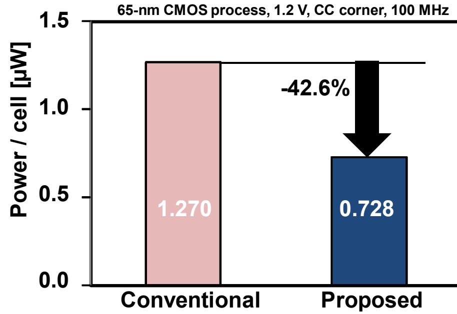
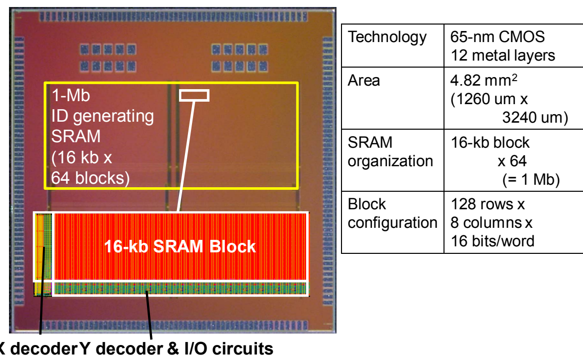


Figure 5. Power comparison.

IV. Measurement Results

We designed a test chip in a 65-nm CMOS technology and obtained generated random data patterns by measurement. Figure 6 presents a die photograph of a 1-Mb SRAM and the 16-kb block layout. The 64-kb block consists of 128 rows × 8 columns × 16 b/word. This SRAM can function as a normal SRAM. Figure 7 presents an example of a generated random data pattern.



Technology	65-nm CMOS 12 metal layers
Area	4.82 mm^2 (1260 um x 3240 um)
SRAM organization	16-kb block x 64 (= 1 Mb)
Block configuration	128 rows x 8 columns x 16 bits/word

Figure 6. Photograph of a 1-Mb SRAM test chip and the layout of a 32-kb block.

A. Repeatability

In this section, we present discussion of the repeatability of the generated fingerprint. To investigate the repeatability, the fingerprint generation test is examined 160 times on 128-bit-wide rows: The fingerprint data length is 128 bit, which is placed in a single row in an SRAM block. Figure 8 depicts the measured Hamming distance distribution. The fingerprint generated in the first test is recorded as the original response. The other fingerprint generated in the same bitcell row is compared to the original response; then we calculate a Hamming distance. In the proposed scheme, the average value (μ) is 1.38, and the standard deviation (σ) is 1.19 in the Hamming distance metric. In contrast, the average value and standard deviation are, respectively, 3.68 and 1.78 in the conventional scheme. The proposed scheme has better repeatability than the conventional scheme, indicating that the identification population is also larger in the proposed scheme.

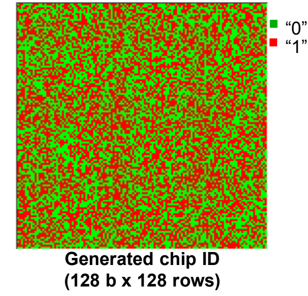


Figure 7. Example of a generated random data pattern.

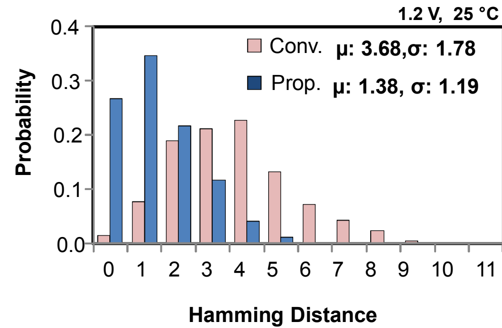


Figure 8. Histograms of the measured Hamming distance.

B. Impact of supply voltage and temperature fluctuation

We show the experimentally obtained results for the impact of supply voltage and temperature fluctuation on repeatability. It is important that a PUF has resistance to supply voltage and temperature fluctuation. As an expected "response", the fingerprint has been generated and registered at a nominal voltage of 1.2 V and at room temperature (25°C). At a lower voltage of 1.1 V, the average and standard deviation values are degraded, respectively, to 3.44 and 1.74. At 100°C operation, the average and standard deviation values are degraded, respectively, to 2.87 and 1.80.

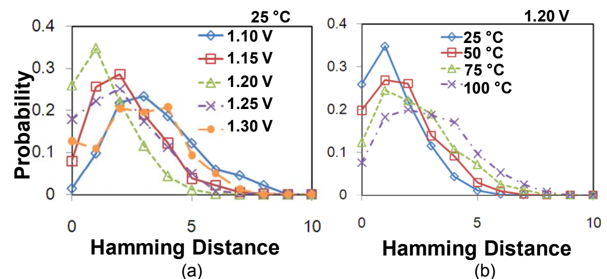


Figure 9. Histogram variations when changing (a) supply voltage and (b) temperature.

C. Uniqueness of the generated fingerprint

As a uniqueness test, 384 samples on 12 chips were measured. Figure 10 depicts the measured Hamming distance distribution. "Known device" denotes that the fingerprint is generated by a registered device, and compared to "response" data that are recorded beforehand from the same device. "Latent device" means that the fingerprint generated by the

other devices is compared to a "response". For latent devices, the average and standard deviation of the Hamming distance are 64.88 and 5.29, respectively, and the mode value of the Hamming distance is 65. 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.

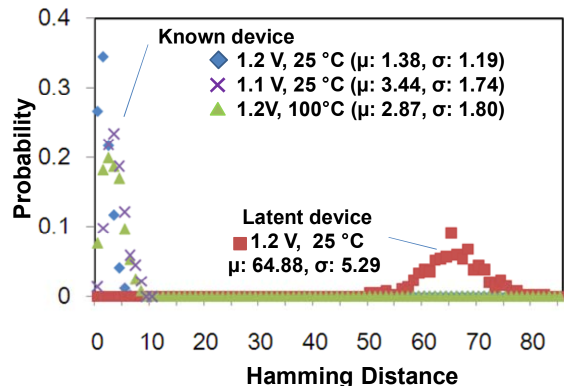


Figure 10. Histograms of the measured Hamming distance.

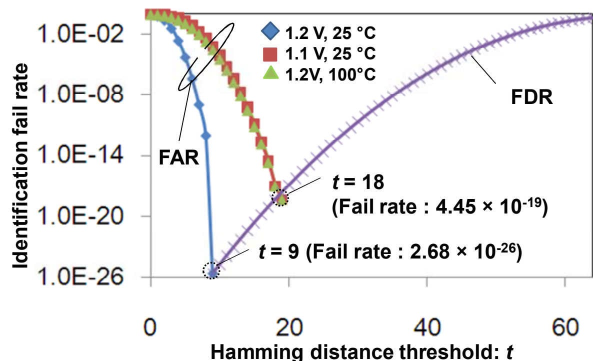


Figure 11. Identification fail rate.

Next, we discuss the fail 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 fail 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 [12]. We assume that the distribution of hamming distance is normal distribution, FDR and FAR are calculated on the basis of the probability distribution functions. A worse rate of FAR and FDR is recognized as an identification fail rate. Figure 11 shows the identification fail rate when *t* is varied. The minimum identification fail rate at the 1.2 V and at room temperature (25°C) is 2.68×10^{-26} when *t* is 9. The worst identification fail rate at 1.1 V or 100°C is 4.45×10^{-19} when *t* is 18 The identification failure rate can be decreased easily because, in the proposed scheme, numerous SRAM bitcells are embedded on a chip and the bit length can be extended easily.

V. SUMMARY

We presented a chip ID generating scheme with transistor variation in SRAM bitcells. By writing "low" on both bitlines, a unique fingerprint is obtainable. The proposed scheme achieved low-power and high-reliability fingerprint generation by modifying a write driver and power switches in SRAM. We confirmed that the V_{th} variation in load transistors is the basis of the randomness by simulation. The proposed scheme reduces power consumption by 39.5% compared with the conventional power-up scheme. We fabricated test chips in a 65-nm process and obtained a unique 128-bit fingerprint from 12 chips. The repeatability of the proposed scheme is better than that of the conventional scheme, and high identification probability is realized. The identification failure rate is 4.45×10^{-19}.

ACKNOWLEDGMENTS

The VLSI chips in this study were fabricated in the chip fabrication program of VLSI Design and Education Center (VDEC) at The University of Tokyo in collaboration with STARC, e-Shuttle, Inc., and Fujitsu Ltd. 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., "Single- and Multi-core Configurable AES Architectures for Flexible Security," IEEE transaction on VLSI Systems, vol. 18, issue 4, pp. 541-552, 2010.

[2] T. Phillips et al., "Security Standards for the RFID Market," IEEE, Security & Privacy, vol. 3, Issue 6, pp. 85-89, 2005.

[3] J. J. Lee et al., "CMOS ROM Arrays Programmable by Laser Beam Scanning," IEEE Journal of Solid-State Circuits, vol. 22, Issue 4, pp. 622-624, 1987

[4] W. Choi et al., "PUF-based Encryption Processor for the RFID Systems," IEEE International Conference on CIT, pp. 2323-2328, 2010.

[5] K. Lofstrom et al., "ID Identification Circuit using Device Mismatch," IEEE ISSCC, pp. 372-373, Feb. 2000.

[6] D. Lim et al., "Extracting Secret Keys from Integrated Circuits," IEEE Trans. VLSI Systems, vol. 13, no. 10, pp. 1200-1205, Oct. 2005.

[7] Y. Su et al., "A Digital 1.6pj/bit Chip Identification Circuit Using Process Variation," IEEE J. Solid-State Circuits, vol. 43, no. 1, Jan. 2008.

[8] J. Guajardo, S. S. Kumar, G. J. Schrijen, and P. Tuyls, "FPGA Intrinsic PUFs and Their Use for IP Protection," CHES 2007 LNCS, vol. 4727/2007, pp. 63-80, Springer, Heidelberg, 2007.

[9] D. E. Holcomb, W. P. Burleson, and K. Fu. "Power-up SRAM State as an Identifying Fingerprint and Source of True Random Numbers," IEEE Transactions on Computers, vol. 58, no. 9, pp. 1198-120, Sep. 2009.

[10] R. Maes, P. Tuyls, and I. Verbauwhede, "A soft Decision Helper data Algorithm for SRAM PUFs," IEEE International Symp. Information Theory, pp. 2101-2105, July, 2009.

[11] Y. Morita et al., "An Area-Conscious Low-Voltage-Oriented 8T-SRAM Design under DVS Environment," IEEE Symp. VLSI Circuits, pp. 256-257, 2007.

[12] D. Lim, J. W. Lee, B. Gassed, G. E. Suh, M. van Dijk, and S. Devadas, "Extracting Secret Keys From Integrated Circuits," IEEE Transactions on Very Large Scale Integration Systems, vol. 13, no. 10 Oct., 2005.