Kobe University Repository : Kernel

PDF issue: 2025-12-05

A 128-bit Chip Identification Generating Scheme Exploiting Load Transistors' Variation in SRAM Bitcells

Okumura, Shunsuke
Yoshimoto, Shusuke
Kawaguchi, Hiroshi
Yoshimoto, Masahiko

(Citation)
IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences,95(12):2226-2233

(Issue Date)
2012-12-01

(Resource Type)
journal article

(Version)
Version of Record

(Rights)
copyright©2012 IEICE

(URL)
https://hdl.handle.net/20.500.14094/90002976

IEICE TRANS. FUNDAMENTALS, VOL.E95–A, NO.12 DECEMBER 2012

PAPER Special Section on VLSI Design and CAD Algorithms

A 128-bit Chip Identification Generating Scheme Exploiting Load Transistors' Variation in SRAM Bitcells*

Shunsuke OKUMURA[†a)], **Shusuke YOSHIMOTO**[†], ***Student Members***, **Hiroshi KAWAGUCHI**[†], ***and*** **Masahiko YOSHIMOTO**[†,††], ***Members***

SUMMARY 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 operations. Through minor modifications, this scheme can be implemented for existing SRAMs. It has high speed, and it can be implemented in a very small area overhead. The generated fingerprint mainly reflects threshold voltages of load transistors in the bitcells. 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}.

key words: *SRAM, chip ID, physical unclonable function (PUF)*

1. 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 a PUF is unpredictable. Therefore, the PUFs cannot be reproduced using a manufacturing process. To identify a registered chip, a challenge-response pair (CRP) recorded in a database is referred.

Lostrom presented extraction of a fingerprint with variation in a transistor current [5]. Statistical delay variation with a threshold voltage ($V_{\rm th}$) mismatch of cross-coupled NOR circuits was 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 $V_{\rm th}$ 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. Fujiwara presented a fingerprint generating scheme using SRAM fail bit addresses [11]. To find less margin bitcells and enhance their fingerprint repeatability, this method requires several hundred trials using a built-in self test (BIST) circuit, which results in complicated and long-time operation. Chellappa proposed a "high-and-high" fingerprint generating scheme, which makes both internal nodes in an SRAM bitcell metastable [12]. The power consumption, however, becomes a problem in this scheme because short current flows through bitcells.

In this paper, 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.

In the next section, we mention a conventional fingerprint generating scheme and its problem. In Sect. 3, we explain our proposed fingerprint generating scheme that achieves higher repeatability and low-power operation. In Sect. 4, we show measurement results. The proposed scheme is evaluated by a Hamming distance metric considering voltage fluctuation, temperature fluctuation, and aging effect. The final section summarizes this paper.

2. Conventional Fingerprint Generating Scheme Using SRAM

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 $V_{\rm DD}$ from the ground. A unique datum is stored in each bitcell at that time in the conventional scheme. The simulation waveforms in the conventional scheme [8], [9] are illustrated in Figs. 1(b) and (c). The results are derived from Monte Carlo simulation using HSPICE. Figure 1(b) shows that a random datum is gener-

Manuscript received March 19, 2012.
Manuscript revised June 18, 2012.
[†]The authors are with Kobe University, Kobe-shi, 657-8501 Japan.
[††]The author is with JST CREST, Tokyo, 102-0076 Japan.
*This paper is the extended version of IEEE European Solid-State Circuits Research Conference [16].
a) E-mail: s-oku@cs28.cs.kobe-u.ac.jp
DOI: 10.1587/transfun.E95.A.2226

Copyright © 2012 The Institute of Electronics, Information and Communication Engineers

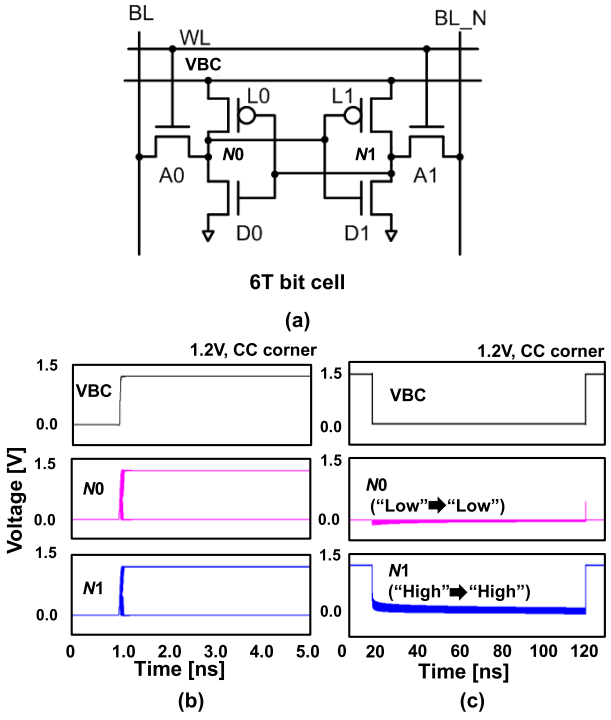


Fig. 1 (a) 6T bitcell, (b) simulation waveforms in the conventional scheme, and (c) effect of past data.

ated in the internal node, $N0$ (and $N1$ for the complement datum). Ideally, the internal nodes must be discharged completely before VBC is charged up. Past data, however, affect to the inherent data.

Figure 1(c) shows the effect of the past data. Assume that the bitcells hold data "0" ($N0$ = "0", and $N1$ = "1"). Then VBC is turned off by shutting down to initialize the internal nodes in the bitcells. In reality, the both internal voltages are not completely grounded in a short time; it takes a long time to be discharged completely. Consequently, the past written datum, "0", affects 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 100 ns (actually even after 4,000 ns), the voltage of internal nodes tend to revert to the past "0" state; this does not mean to be random. A unique datum cannot be generated by the conventional scheme after the device is once powered on. This disadvantage is unsuitable for use of fuzzy extractor.

3. Proposed Fingerprint Generating Scheme Using SRAM

Figure 2 presents the proposed circuit for generating chip IDs. In the figure, a bitcell represents a commonly used 6T. The other topologies such as an 8T bitcell [13] 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

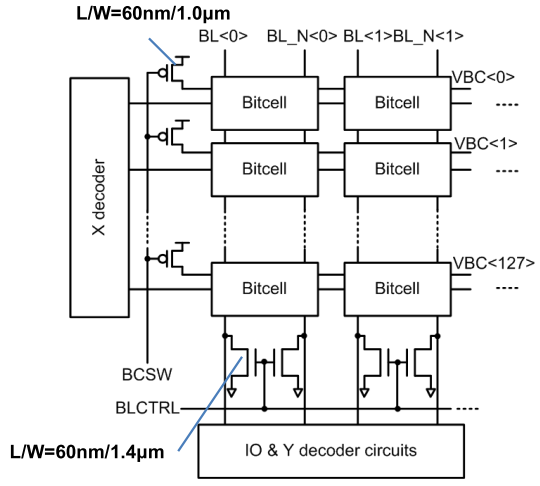


Fig. 2 SRAM architecture with additional nMOS write drivers and pMOS switches for VBC.

controlled using a BLCTRL signal. The additional driver is so simple that the area overhead is $3.52\,\mu m^2$ in each column of the bitcell array, which is attributable to the additional write drivers. 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.

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 cannot be fully discharged to the ground because of the current of the respective pMOSes (L0 and L1). Therefore, we add a pMOS switch to the VBC line to ground the internal nodes and to decrease the power consumption 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 eventually grounded full.

The proposed fingerprint-generating procedure takes four 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 VBC is cut off. Then, in the target data row, "low-and-low" writing is conducted and VBC is resumed; random data are generated. Finally, they are read out and processed to produce a unique ID.

Figure 3 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 (L0 and L1). 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.

Figure 4 shows the distribution of the drive and load

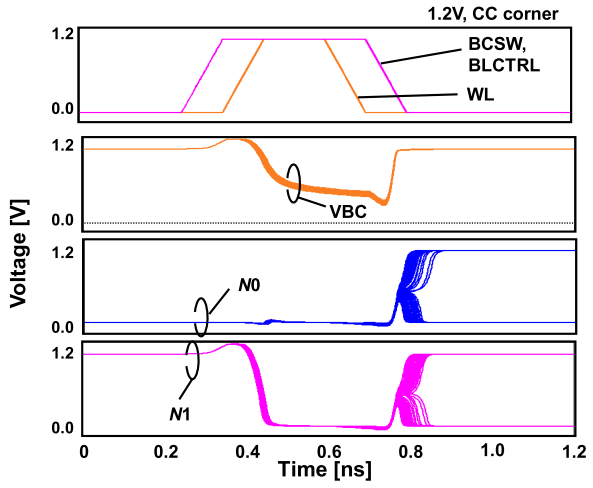


Fig. 3 Simulation waveforms in the proposed scheme.

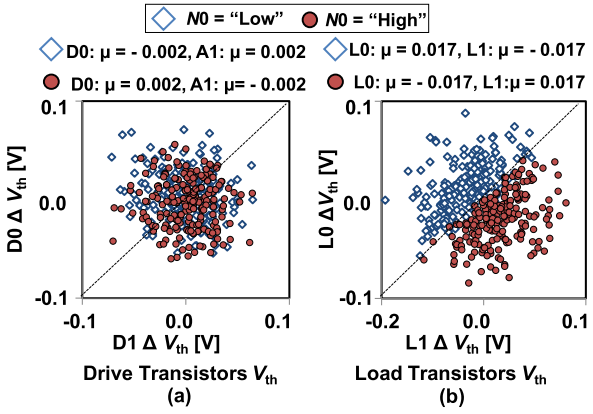


Fig. 4 Distribution of V_{th}s in (a) drive transistors and (b) load transistors.

transistors' V_{th}s. 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 much more sensitive to randomness.

Next, we discuss the stability of fingerprint generation schemes. Noises affecting each transistor such as thermal noise and random telegraph noise can invert the inherent data.

In the conventional scheme, the voltages of the internal nodes and VBC are discharged to generate a fingerprint. V_{ds}s of the load transistors are equal to almost zero at the initial state of the fingerprint generation (see Fig. 1(b)). Under this condition, the inherent data are easily inverted by noise because V_{ds}s of the load transistors are small.

In the proposed scheme, although the internal nodes are fully discharged, the VBC have some residue voltages that are V_{th}s of the load transistors (see Fig. 3). This means that the proposed scheme has higher immunity to noise. 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 it affects data generation. Table 1 shows voltages and currents at the initial state of fingerprint generation. Table 1 is derived from 10,000 iterations of a Monte Carlo simulation at nominal supply voltage and at room temperature. The V_{diff} and I_{diff} respectively represent the V_{ds} and I_{ds} differences between the load transistors (L0 and L1). The proposed scheme has large difference of V_{diff} and I_{diff} compared with the conventional scheme. In other words, the proposed scheme has better repeatability because the generated data are affected strongly by the unique V_{th}s of the load transistors.

Table 1 Voltage and current differences at initial state.

	V_{diff} [V]		I_{diff} [A]		VBC [V]	
	Conv.	Prop.	Conv.	Prop.	Conv.	Prop.
μ	0.00	4.73×10^{-5}	1.87×10^{-20}	1.08×10^{-8}	0.00	3.12×10^{-1}
σ	0.00	3.09×10^{-5}	1.43×10^{-20}	7.04×10^{-9}	0.00	2.15×10^{-2}

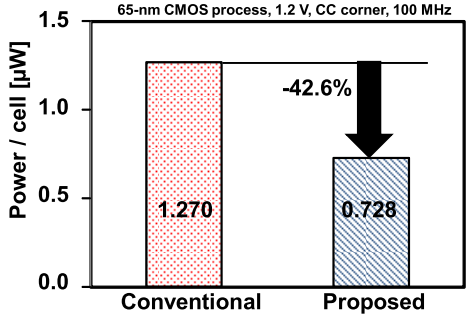


Fig. 5 Power comparison.

Table 2 128-bit fingerprint output speed comparison (1.2 V, CC corner, 100 MHz = 10-ns period).

	Conv. [ns]	Prop. [ns]
Fingerprint generating time	4723.34	0.56
Fingerprint readout time	80.00	80.00
Total time	4803.34	80.56

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

Table 2 shows the comparison of the output speeds in 128-bit fingerprinting. In the proposed scheme, the time until the fingerprint data is generated in bitcells ("fingerprint generating time" in the table) is drastically reduced (see Fig. 3). Then, the 128-bit fingerprint readout takes 80 ns in a case of 16 bits/word at a 100-MHz operation. Consequently, the total time is reduced by 98.3% in the proposed scheme

over the conventional one.

4. Measurement Results

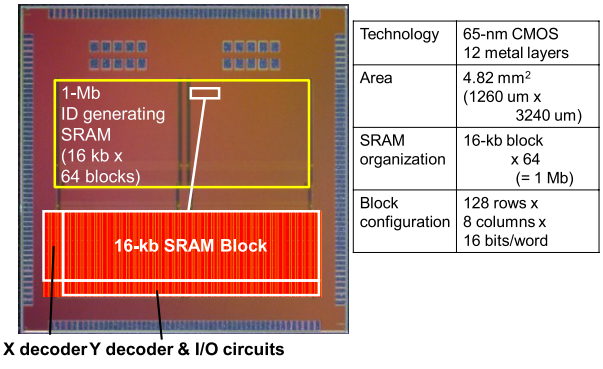
We designed a test chip in a 65-nm CMOS technology and obtained generated random data patterns by measurement. Figure 6 presents a die photograph of a 1-Mb SRAM and the 16-kb block layout. The 16-kb block consists of 128 rows × 8 columns × 16 b/word. This SRAM can function as a normal SRAM. Figure 7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

4.1 Repeatability

In this subsection, 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 (see Fig. 7). Figure 8 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 expected values are calculated from 100 time measurements at each bitcell row. 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. In contrast, the average value and standard deviation in the conventional scheme are 8.08 and 2.41, respectively.

Regarding the bit error probability (BEP), the stability differs among bitcells in the fingerprint generation scheme. A bitcell's inherent data are flipped easily by each trial, and other bitcell's inherent data are always the same. BEP denotes the probability that the generated data differ from the MLR in each bitcell. When BEP equals 0.5, the bitcell generate random data in the fingerprint generation scheme. However, when BEP is 0, the bitcells generate the same data in every trial. We calculated the BEP from 100 time measurements at 12,288 rows × 128-bits fingerprint. The results are shown in Fig. 9.

In the conventional scheme and the proposed scheme, the stable bitcell (BEP = 0) rates are 87.1% and 93.7%, respectively. This result means that the proposed scheme can reduce the unstable bitcell (BEP > 0) rates to less than half. The distribution tendencies of the BEP are the same between the conventional and proposed scheme. However, the proposed scheme, which has fewer unstable bits, has lower probability than the conventional scheme in the BEP > 0 region. The larger stable bits improve the efficiency of fingerprint generation scheme. The proposed scheme has better



Technology	65-nm CMOS 12 metal layers
Area	4.82 mm² (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

Fig. 6 Photograph of a 1-Mb SRAM test chip and the layout of a 16-kb block.

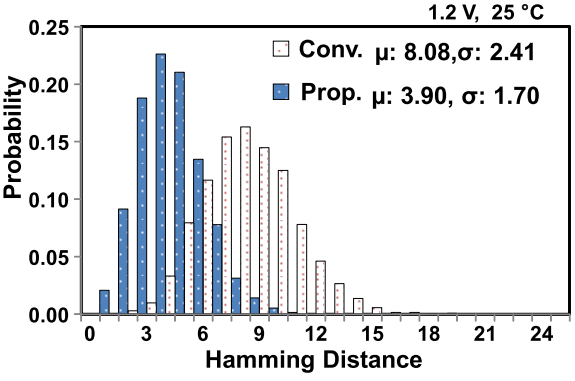


Fig. 8 Histograms of the measured Hamming distance.

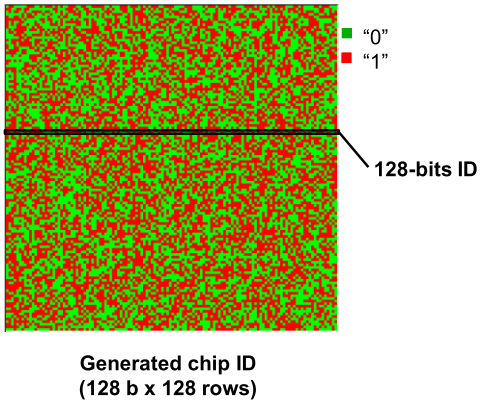


Fig. 7 Example of a generated random data pattern.

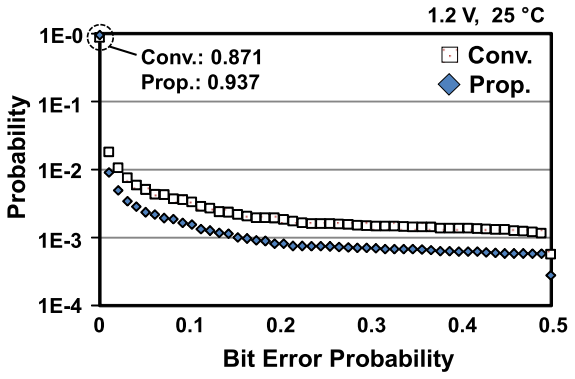


Fig. 9 Bit error probability (BEP) comparison (the figure shows probability density functions).

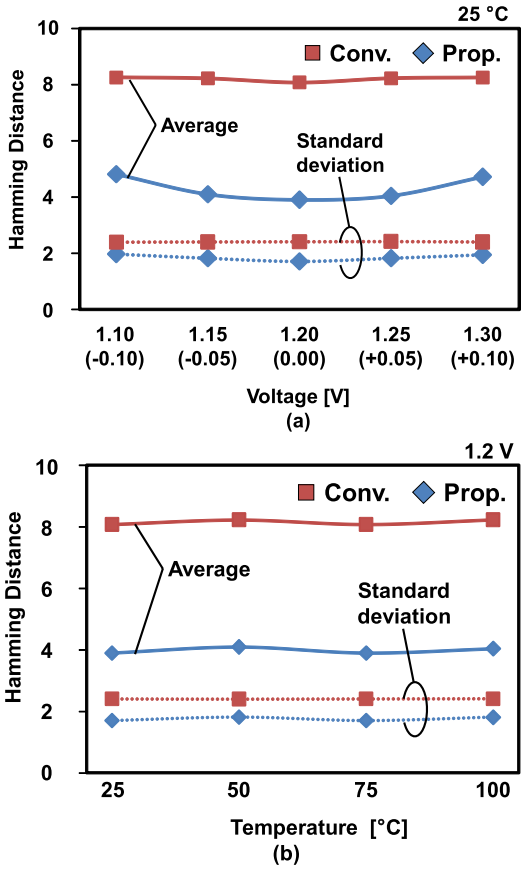


Fig. 10 Average and standard deviation values when changing (a) supply voltage and (b) temperature.

repeatability than the conventional scheme, indicating that the identification population is also larger in the proposed scheme.

4.2 Impact of Supply Voltage and Temperature Fluctuation

We show 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 MLR, the fingerprint has been generated and registered at a nominal voltage of 1.2 V and at room temperature (25°C). Then we measured 512 samples as a 128-bit fingerprint. Figure 10(a) shows the impact of supply voltage on repeatability.

In the conventional scheme, the supply voltage does not affect the repeatability because the inherent data are fixed at a very lower voltage than the supply voltage.

In the proposed scheme, however, the repeatability is dependent on VBC voltage, which is changed by the supply voltage. At a lower voltage of 1.1 V, the average and standard deviation values are degraded, respectively, to 4.81 and 1.97. The repeatability becomes worse by the supply voltage decrease. At a high voltage, it is seen that the Hamming distance is increased. Nevertheless the proposed scheme exhibits higher repeatability than the conventional scheme does.

Figure 10(b) depicts the impact of the temperature fluctuation. The repeatability of the conventional or proposed scheme is not either affected very much by temperature. The effect of the temperature change is less than that of the supply voltage change.

4.3 Impact of Aging

In this subsection, we discuss the aging impact on the fingerprint generation scheme. The repeatability degradation by the aging effect must be considered. Negative bias temperature instability (NBTI) is the main reason underlying repeatability degradation in the fingerprint generation scheme.

In the conventional scheme, aging needs not to be considered because voltage is hardly biased across a transistor in generating the fingerprints.

In the proposed scheme, we measured 512 samples as 128-bit fingerprints to verify the aging effect. The aging measurement takes four steps:

1) A fingerprint is iteratively generated 100 times at the nominal voltage (1.2 V) and a high temperature (100°C), from which we calculate an MLR of each fingerprint. The obtained MLR signifies the worst case for the aging test because a pMOS with a lower $|V_{\mathrm{th}}|$ is stressed by aging in every bitcell; increasing the lower $|V_{\mathrm{th}}|$ worsens the repeatability. The obtained MLR is set in the bitcells at the beginning of the aging test.
2) The SRAM chip is kept at the high temperature and a high voltage (1.8 V).
3) The supply voltage is lowered to the nominal one, and the fingerprint is generated once again in manner of the proposed scheme.
4) The regenerated fingerprint is compared with the original MLR that was generated at the first step.

Note that the high temperature is applied through the steps to merely consider the aging effect. If the temperature at the first step was low and that at the following steps was high, the impact of the temperature fluctuation mentioned in the previous subsection would be given in the aging measurement.

The waiting times are 10^{-6} to 10^{3} s in this aging test. In this condition, the total acceleration factor is a product of the thermal acceleration factor (TAF) and voltage acceleration factor (VAF) [14]. The respective formulae are shown below:

$$\mathrm{TAF} = \exp[(E_{\mathrm{a}}/k) \times (1/T_{\mathrm{operation}} - 1/T_{\mathrm{stress}})],$$
$$\mathrm{VAF} = \exp[\gamma \times (V_{\mathrm{stress}} - V_{\mathrm{operation}})],$$

where E_{a} is the activation energy, k represents Boltzmann's constant, $T_{\mathrm{operation}}$ is 298 K (= 25°C), T_{stress} is 373 K (= 100°C), γ is the voltage exponent factor, V_{stress} is 1.8 V, and $V_{\mathrm{operation}}$ is 1.2 V. The total acceleration factor is TAF × VAF

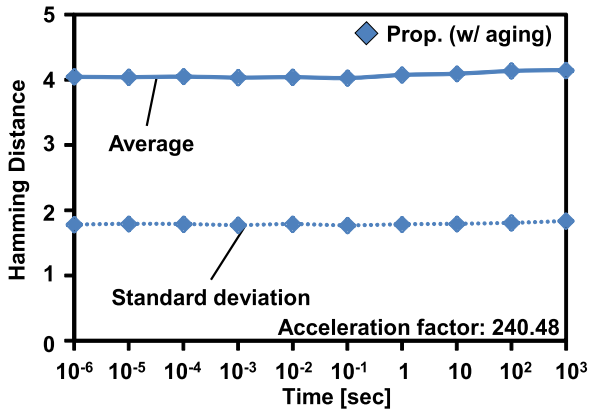


Fig. 11 Average and standard deviation values in aging.

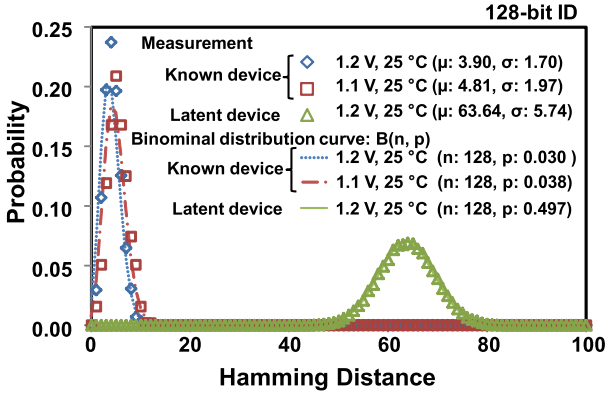


Fig. 12 Histograms of the measured Hamming distance.

$= 50.1 \times 4.8 = 240.48$.

Figure 11 shows the measured results of the aging tests. The repeatability is slightly degraded with increasing stress time because the BEP is increased by the effect of NBTI. As described above, if the L0 transistor has higher V_{th} than the L1 transistor, then the internal node "*N*0" tends to be "Low". In this case, the L1 transistor is stressed and its V_{th} is increased. The effect of NBTI reduces the V_{th} difference between load transistors by the stored inherent data. However, as shown in Fig. 11, if the aging time is short, then the proposed method has higher repeatability than that of the conventional method, even considering the aging degradation.

4.4 Uniqueness of the Generated Fingerprint

As a uniqueness test, 12,288 samples were measured (4,096 samples/chip × 3 chips; although one chip has 8,192 rows of 128 bits, a half of them were merely measured due to a side issue on chip implementation). Figure 12 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

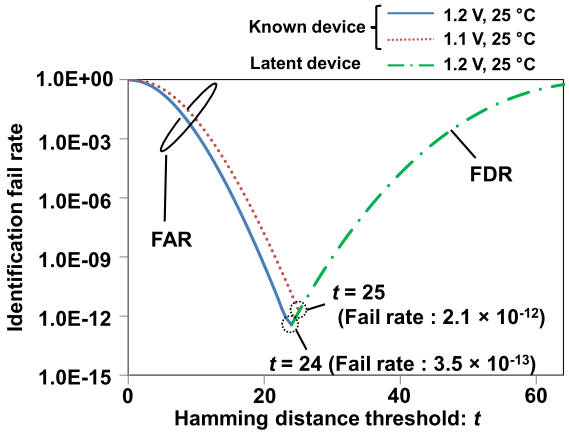


Fig. 13 Identification failure rates.

devices is compared to MLRs; in this paper, "latent device" data are obtained from different SRAM blocks in the same chip and different SRAM blocks in different chips. In other words, one third of the samples are compared to the "known device" on the same chip; however, this is reasonable because the randomness is derived from the local variation as described in Sect. 3. 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 [15]. 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. 12 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. 12; p in the fitted curve can be obtained as $\mu/128$ from the measurement.

Figure 13 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.

5. Conclusion

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 $V_{\rm th}$ variation in load transistors is the basis of the randomness by simulation. The proposed scheme reduces power consumption by 42.6% compared with the conventional power-up scheme. We fabricated test chips in a 65-nm process and obtained a unique 128-bit fingerprint. 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 2.1×10^{-12} at the worst condition, which indicates that the proposed scheme can identify more than 10^{11} devices. The identification failure rate can be improved easily by extending the fingerprint bit length.

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, C.P. Su, C.L. Horng, C.W. Wu, and C.T. Huang, "Single- and multi-core configurable AES architectures for flexible security," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol.18, no.4, pp.541–552, 2010.

[2] T. Phillips, T. Karygiannis, and R. Kuhn, "Security standards for the RFID market," IEEE Security and Privacy, vol.3, no.6, pp.85–89, 2005.

[3] J.J. Lee and N.R. Strader, "CMOS ROM arrays programmable by laser beam scanning," IEEE J. Solid-State Circuits, vol.22, no.4, pp.622–624, 1987.

[4] W. Choi, S. Kim, Y. Kim, Y. Park, and K. Ahn, "PUF-based encryption processor for the RFID systems," IEEE International Conference on Computer and Information Technology (CIT), pp.2323–2328, 2010.

[5] K. Lofstrom, W.R. Daasch, and D. Taylor, "ID identification circuit using device mismatch," IEEE International Solid-State Circuits Conference, pp.372–373, Feb. 2000.

[6] D. Lim, J.W. Lee, B. Gassend, G.E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol.13, no.10, pp.1200–1205, Oct. 2005.

[7] Y. Su, J. Holleman, and B.P. Otis, "A digital 1.6 pJ/bit chip identification circuit using process variation," IEEE J. Solid-State Circuits, vol.43, no.1, pp.69–77, Jan. 2008.

[8] J. Guajardo, S.S. Kumar, G.J. Schrijen, and P. Tuyls, "FPGA intrinsic PUFs and their use for IP protection," Cryptographic Hardware and Embedded Systems, Lect. Notes Comput. Sci., Springer, vol.4727, pp.63–80, 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 Trans. Comput., vol.58, no.9, pp.1198–1210, Sept. 2009.

[10] R. Maes, P. Tuyls, and I. Verbauwhede, "A soft decision helper data algorithm for SRAM PUFs," IEEE International Symposium on Information Theory, pp.2101–2105, July 2009.

[11] H. Fujiwara, M. Yabuuchi, H. Nakano, H. Kawai, K. Nii, and K. Arimoto, "A chip-ID generating circuit for dependable LSI using random address errors on embedded SRAM and on-chip memory BIST," IEEE Symposium on VLSI Circuits, pp.76–77, June 2011.

[12] S. Chellappa, A. Dey, and L.T. Clark, "Improved circuits for microchip identification using SRAM mismatch," IEEE Custom Integration Circuits Conference, pp.1–4, Sept. 2011.

[13] Y. Morita, H. Fujiwara, H. Noguchi, Y. Iguchi, K. Nii, H. Kawaguchi, and M. Yoshimoto, "An area-conscious low-voltage-oriented 8T-SRAM design under DVS environment," IEEE Symposium on VLSI Circuits, pp.256–257, 2007.

[14] "Altera Reliability Report 49 Q1 2010," www.altera.com/literature/rr/rr.pdf

[15] D. Lim, J.W. Lee, B. Gassed, G.E. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol.13, no.10, pp.1200–1205, Oct. 2005.

[16] S. Okumura, S. Yoshimoto, H. Kawaguchi, and M. Yoshimoto, "A 128-bit chip identification generating scheme exploiting SRAM bitcells with failure rate of 4.45×10^{-19}," IEEE European Solid-State Circuits Research Conference, pp.527–530, Sept. 2011.

Shunsuke Okumura received B.E. and M.E. degrees in Computer and Systems Engineering in 2008 and 2010, respectively from Kobe University, Hyogo, Japan, where he is currently working in the doctoral course. His current research is high-performance, low-power SRAM designs, dependable SRAM designs, and error correcting code implementation. He is a student member of IPSJ and IEEE.

Shusuke Yoshimoto received B.E. and M.E. degrees in Computer and Systems Engineering from Kobe University, Hyogo, Japan, in 2009 and 2011, respectively. He is currently working in the doctoral course at that university. His current research is low-power and soft-error tolerant SRAM designs. He was a recipient of IEEE SSCS 2011 and 2012 Japan Chapter Academic Research Award. He is a student member of IPSJ and IEEE.

Hiroshi Kawaguchi received B.Eng. and M.Eng. degrees in electronic engineering from Chiba University, Chiba, Japan, in 1991 and 1993, respectively, and earned a Ph.D. degree in electronic engineering from The University of Tokyo, Tokyo, Japan, in 2006. He joined Konami Corporation, Kobe, Japan, in 1993, where he developed arcade entertainment systems. He moved to The Institute of Industrial Science, The University of Tokyo, as a Technical Associate in 1996, and was appointed as a Research Associate in 2003. In 2005, he moved to Kobe University, Kobe, Japan. Since 2007, he has been an Associate Professor with The Department of Information Science at that university. He is also a Collaborative Researcher with The Institute of Industrial Science, The University of Tokyo. His current research interests include low-voltage SRAM, RF circuits, and ubiquitous sensor networks. Dr. Kawaguchi was a recipient of the IEEE ISSCC 2004 Takuo Sugano Outstanding Paper Award and the IEEE Kansai Section 2006 Gold Award. He has served as a Design and Implementation of Signal Processing Systems (DISPS) Technical Committee Member for IEEE Signal Processing Society, as a Program Committee Member for IEEE Custom Integrated Circuits Conference (CICC) and IEEE Symposium on Low-Power and High-Speed Chips (COOL Chips), and as an Associate Editor of IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences and IPSJ Transactions on System LSI Design Methodology (TSLDM). He is a member of the IEEE, ACM, and IPSJ.

Masahiko Yoshimoto joined the LSI Laboratory, Mitsubishi Electric Corporation, Itami, Japan, in 1977. From 1978 to1983 he had been engaged in the design of NMOS and CMOS static RAM. Since 1984 he had been involved in the research and development of multimedia ULSI systems. He earned a Ph.D. degree in Electrical Engineering from Nagoya University, Nagoya, Japan in 1998. Since 2000, he had been a professor of Dept. of Electrical & Electronic System Engineering in Kanazawa University, Japan. Since 2004, he has been a professor of Dept. of Computer and Systems Engineering in Kobe University, Japan. His current activity is focused on the research and development of an ultra low power multimedia and ubiquitous media VLSI systems and a dependable SRAM circuit. He holds on 70 registered patents. He has served on the program committee of the IEEE International Solid State Circuit Conference from 1991 to 1993. Also he served as Guest Editor for special issues on Low-Power System LSI, IP and Related Technologies of IEICE Transactions in 2004. He was a chair of IEEE SSCS (Solid State Circuits Society) Kansai Chapter from 2009 to 2010. He is also a chair of The IEICE Electronics Society Technical Committee on Integrated Circuits and Devices from 2011–2012. He received the R&D100 awards from the R&D magazine for the development of the DISP and the development of the realtime MPEG2 video encoder chipset in 1990 and 1996, respectively. He also received 21th TELECOM System Technology Award in 2006.