Extended Abstracts of the 2014 International Conference on Solid State Devices and Materials, Tsukuba, 2014, pp962-963

Evaluation of Uniqueness of Output from Current Mismatch ID Generation Circuit for Sensor Network Services

Kenichi Matsunaga[1], Shoichi Oshima, Tadashi Minotani, Toshihiko Kondo, and Hiroki Morimura

[1] NTT Microsystem Integration Laboratories
3-1 Morinosato Wakamiya, Atsugi-shi, Kanagawa 243-0198, Japan
Phone: +81-46-240-2489 E-mail: matsunaga.kenichi@lab.ntt.co.jp

Abstract

This paper presents a low-power and uniquely-distributed ID-generation circuit based on process variation. The Developed circuit utilizes current mismatch in an NMOS pair for unique ID output. To evaluate the output 1/0 probability-uniformity and process dependence, we fabricated a prototype in two different 0.18-μm standard CMOS technologies. We tested 382 chips and calculated the hamming distances between each chip. The result shows the circuit architecture generates a unique and process-independent ID. Furthermore, the bit-generation efficiency was found to be 0.96 pJ/bit.

1. Introduction

Unique hardware ID generation is a key technology for reducing ID-generation and ID-management costs in sensor networks. A common way to add an ID to each device is to record the ID using non-volatile memory, an electric fuse, or mask-ROM. However, these methods need additional processes and increase cause service costs. In attempts to solve the above problems, various types of management-free ID-generation methods based on process variation are being developed. The output ID uniqueness is important because output 1/0 bias degrades the effective bit width.

The most popular circuit is based on a SRAM architecture that uses SRAM initial-state 1/0 randomness after the power-on period as an ID [1]. Another method uses intrinsic delay variation [2]. However, it is, in principle, not random because it is influenced by global process variation. A third method uses gate-oxide breakdown, caused by the application of an overvoltage [3]. Although this method is energy-efficient and intrinsic immunity to noise immunity, the overvoltage may cause degradation of chip reliability.

In this paper, we describe an energy-efficient and unique ID generation circuit that uses NMOS current mismatch to achieve uniquely distributed ID output.

2. Circuit architecture

Fig. 1 shows the whole ID generator configuration. The current generation units (CGUs) draw current from input nodes of the dynamic latches, which compare the current difference between the positive and negative node of the input and outputs 1 or 0. To avoid power-line noise caused by current dissipation in the CGUs and latches, the clock timing is shifted using a delay line. In this work, the latch architecture described in [4] was used because of its low-power and low-noise operation.

Fig. 2 shows the CGU and dynamic-latch circuit structures. The CGUs consist of a pair of NMOS transistors and a ground switch controlled by a trigger. This pair structure cancels global process variation and the relationship between NMOS and PMOS out, and the outputs depend on local random variation only. In addition, the ground switch rejects static current and achieves low-power operation. The width and length of the pair of NMOS transistors were designed as small as possible under the process rule, because, from [5], the current mismatch is inversely proportional to the square root of the effective transistor gate area. In contrast, transistors in dynamic-latches were designed to be about five times larger than the transistors in the CGUs to avoid the influence of process variation in the dynamic latches. The parasitic capacitance of the dynamic-latch transistors also reduces noise generated in the CGU, and it increases noise immunity.

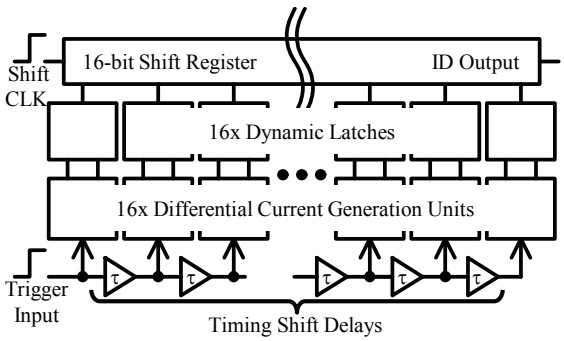

Fig. 1. ID generator configuration.

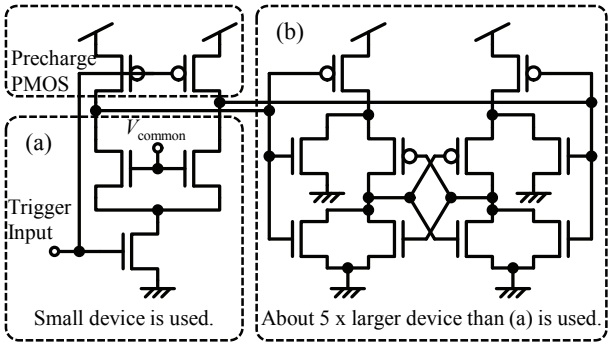

Fig. 2. Circuit schematics of (a) CGU and (b) dynamic-latch.

Table. 1 Performance comparison

	[1]	[2]	[3]	**This work**
Technology, ID length	65 nm, 128 bit	0.18 μm, 256 bit	0.18 μm, 64 bit	0.18 μm, 16 bit
Tr. breakdown	**Not Used**	**Not Used**	Used	**Not Used**
Cell structure	**Differential**	Single	**Pseudo Differential**	**Differential**
Efficiency	1.6 pJ/bit	4.2 pJ/bit	1.2 pJ/bit	**0.96 pJ/bit**
Size of core	135 μm x 70 μm	134.3 μm x 36.2 μm	96 μm x 30 μm	250 μm x 50 μm
Tested number of chips	20 chips	N/A	20 chips	**382 chips (200 + 182 chips)**

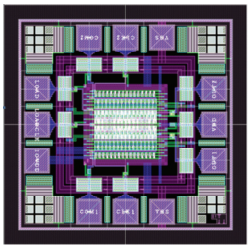

Fig. 3. Chip layout

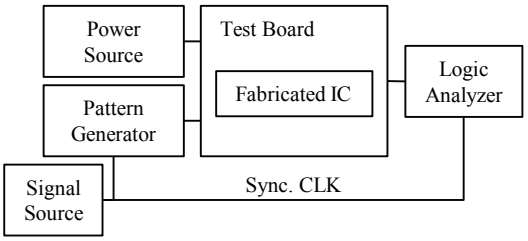

Fig. 4. Measurement setup

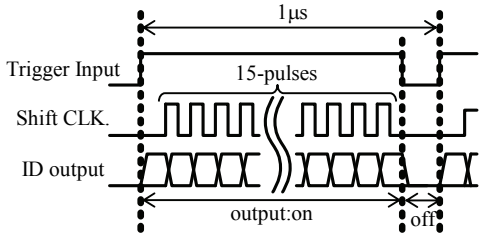

Fig. 5. Timing chart of ID output operation

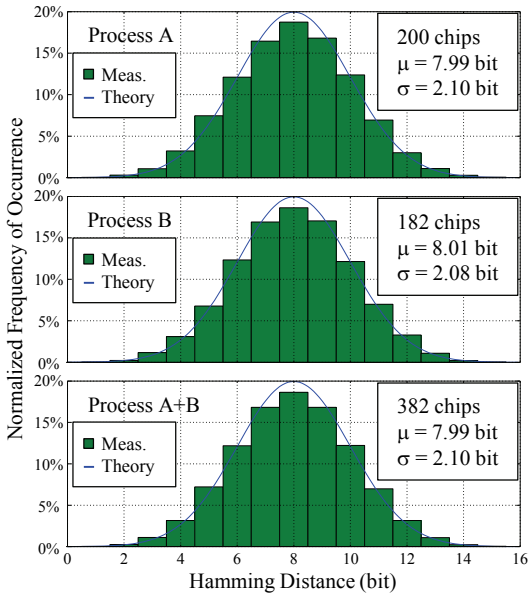

Fig. 6. Measured hamming distance between chips.

3. Measurement results

Fig. 3 shows the chip layout of the developed circuit. To evaluate process dependency, we fabricated a total of 382 chips in two different 0.18-μm CMOS processes. The power consumption and ID uniqueness were measured using the setup in Fig. 4. Fig. 5 shows the timing diagram. The trigger input and shift CLK were fed to the IC and the outputs were captured with a logic analyzer.

The ID uniqueness was examined by calculating the hamming distance between each pair of chips. Fig. 6 shows the relationship between hamming distance and normalized frequency of occurrence. Theoretically, the distribution approximately obeys a normal distribution with a mean of 8 and a standard deviation of 2. All measurement results show the mean of 8, and the standard deviation of 2.09 without distortion. Hamming distance degradation due to 1/0 bias did not appear. This agrees with the theoretically predicted result, and it clarifies that the output has no systematic pattern. Furthermore, the proposed architecture is process-independent, because cross-process measurement (A+B) has nearly the same distribution form.

The power consumption at the operating frequency of 1 MHz with 16-bit output was found to be 15.3 μW, and the calculated bit-generation efficiency is 0.96 pJ/bit.

Table 1 compares our results with the results for previous ID-generation circuits. The developed chip generates 382 chip-test-passed unique IDs without using any gate-oxide breakdown or post-fabrication process with high bit-generation efficiency.

4. Conclusions

The proposed circuit architecture was tested through inter-chip hamming distance measurement and uniqueness was proved in two different 0.18-μm CMOS technologies. This result shows that the proposed circuit can use bit-width efficiently and that it will be useful for ID-generation IP.

In addition, the current mismatch could become larger because the available transistor-size will become smaller with process advancement. Thus, the developed circuit can be easily scaled down for future technology nodes.

References

[1] Y. Su *et al.*, *IEEE J. Solid-State Circuits*, Vol. 43, No. 1, pp. 69-77, Jan. 2008.

[2] K. Fruhashi *et al.*, *IEEE International Symposium on Circuits and Systems*, pp. 2325 - 2328, July. 2011.

[3] F. Tang *et al.*, *IEEE Electron Device Lett.*, Vol. 35, No. 1, pp. 54-56, Jan. 2014.

[4] M. Miyahara *et al.*, *IEEE Asian Solid-State Circuits Conference*, pp. 269-272, Nov. 2008.

[5] M. Pelgrom *et al.*, *IEEE J. Solid-State Circuits*, Vol. 24, No. 5, pp. 1433–1439, Oct. 1989.