Extended Abstracts of the 2002 International Conference on Solid State Devices and Materials, Nagoya, 2002, pp. 250-251

D-4-4

Novel Random Number Generator Using MOS Gate After Soft-Breakdown

Shin-ichi Yasuda, Tetsufumi Tanamoto, Hideki Satake and Shinobu Fujita
Advanced LSI Technology Laboratory, Toshiba Corporation
1, Komukai Toshiba-cho, Saiwai-ku, Kawasaki 212-8582, Japan
Phone: +81-44-549-2313, Fax: +81-44-520-1257, E-mail: shinichi3.yasuda@toshiba.co.jp

1. Introduction

The importance of random numbers has increased for network security systems which are based on the difficulty of predicting secret numbers such as identification numbers, keys to ciphers, and so on. For use in mobile network services, random number generators (RNGs) must be small digital circuits, ideally composed of only CMOS. To date, pseudo-random numbers have been used because they are easily produced using small digital circuits such as feedback shift registers. In the future, RNGs that can generate the random numbers close to "true" random numbers will be required. RNGs using white noise such as thermal noise or shot noise of Si transistors are commercially available [1]. Although they can generate high-quality random numbers close to true random numbers, those RNGs are large in area because thermal noise is essentially a very weak signal that must be highly amplified by analog circuits, which are rather large in area.

One effective way to realize both downsizing and acceptable performance of RNGs is to use the signal fluctuation in CMOS. The candidates for such fluctuation are the strongly fluctuating signals arising from defects in metals, semiconductors, or insulators in MOSFETs. Although some trials to generate random numbers using these fluctuating signals have been reported [2], high-quality random numbers have not been obtained. This is because such fluctuating signals show 1/f -like properties, which adversely affects the statistical balance of random numbers compared with the above thermal noise, although such fluctuating signals are much larger than thermal noise. Hence, it is important to add specific digital circuits to eliminate the influence of 1/f -like properties.

In this report, we demonstrate a new RNG that can generate high-quality random numbers close to true random numbers. The results for this RNG have been achieved both by using the large fluctuating currents of MOS gates after soft-breakdown (SBD) and by using specific digital circuit, with a digital multivibrator and one-bit counter to eliminate 1/f -like properties. This RNG is very small, composed of about 20 CMOS gates.

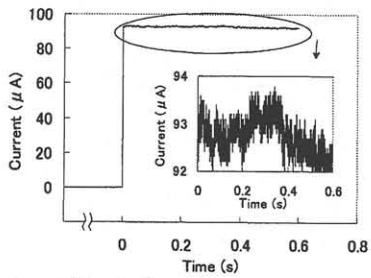

Fig. 1: Current fluctuation under constant gate voltage (V_G = – 4.5 V) on MOS gate with the area of 25 μm^2. (T_{ox} = 4.8nm) The Current changed by about one percent randomly after SBD.

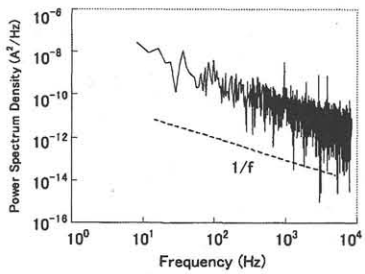

Fig. 2: Power spectrum density of current fluctuation after SBD. Power spectrum shows 1/f -like properties.

2. MOS gate after soft-breakdown as a random number source

The device used in this work is a MOS gate fabricated by the conventional LOCOS process on a p-type substrate. The area of the MOS gate is 25 μm^2, and the oxide thickness is 4.6 nm. The gate electrode is n^+-poly silicon. The SBD was induced by applying a constant negative voltage to the gate electrode. Figure 1 shows the current fluctuation when a –4.5 V constant gate voltage was applied. The current changed by about one percent. This fluctuating signal is very large. This result also means that the resistance of the MOS gate fluctuates after SBD. These current fluctuations have been explained by changing conduction of the leak path [3,4]. Figure 2 shows the power spectrum density from Fourier transformation of the current fluctuation. It is confined that the power spectrum shows 1/f -like properties.

3. Experimental results

An astable multivibrator is an oscillating circuit that outputs a rectangle wave. The period of the rectangle wave is determined by the resistance (R_A and R_B) and capacitance (C_A and C_B) associated with the NAND gates. Hence, when resistor (R_B) is replaced with MOS gate after SBD (SBD-MOS), the period of the rectangle wave (t_l) fluctuates due to the fluctuation in resistance. By measuring time t_l with a one-bit counter, the fluctuating resistance of the

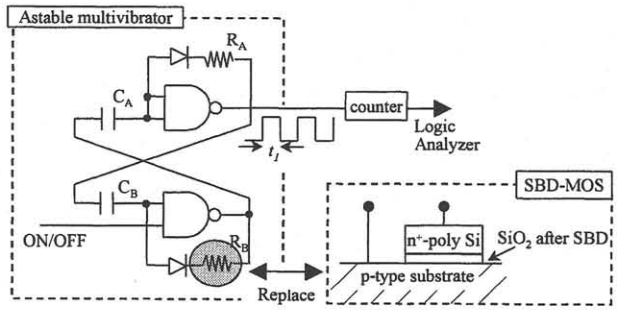

Fig. 3: Schematic diagram of the overall circuit. The period of the rectangle wave (t_l) fluctuates by replacing resister R_B with an SBD-MOS. One-bit counter measures each t_l and converts fluctuating resistance of SBD-MOS to one-bit random numbers.

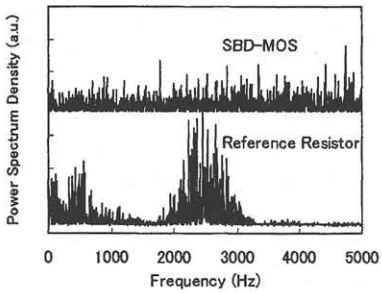

Fig. 4: Power spectrum density obtained by Fourier transformation of random number sequence from an SBD-MOS and a resistor. There are some peaks for the reference resistor, whereas no peaks for the SBD-MOS. It indicates random numbers from the SBD-MOS have no periodicity.

SBD-MOS can be converted to one-bit random numbers. Figure 3 shows the overall circuit diagram. This circuit can be constructed using about 20 CMOS gates.

The supply voltage for the astable multivibrators was 4.5 V, the clock for the one-bit counter was 4 MHz, and the frequency for the output signals was 10 kHz.

Fourier transformations of the output signals were performed to compare the power spectrum density for the SBD-MOS (Fig. 2) with that for the output signals. The results are shown in Fig. 4. Those using a resistor are also shown for reference, where sequences of 0's and 1's were generated for the resistor due to external noise. Figure 4 shows that there are some peaks in the case of the reference resistor. On the other hand, in the case of the SBD-MOS, no peaks can be seen. This means that 1/f -like properties could be effectively eliminated.

In order to check the quality of the generated random numbers, standard statistical tests were performed in accordance with FIPS140-2 (Federal Information Processing Standard, DoC., U.S., 140-2) [5]. The random numbers generated using the SBD-MOS passed all of the tests.

Figure 5 shows self-correlation plots for sequential eight-bit random numbers (decimal:0~255) to compare the quality of the generated random numbers with that of an RNG using thermal noise. Random and well-balanced plots indicate high-quality of random numbers. This method can be used to clarify the periodicity and regularity of random numbers that cannot be sufficiently qualified only by the test of FIPS140-2 [6]. Figure 5 (a) shows the results for random numbers generated using the SBD-MOS, (b) shows the results for random numbers generated from thermal noise, and (c) shows the results for the reference resistor. Our

Test	Requirement	Our Results	Pass?
Monobit	9725~10275	9925	Yes
Poker	2.16~46.17	25.1712	Yes
Long Run	1~26	zero: 11 one: 12	Yes
Length of Run 1	2315~2685	zero: 2631 one: 2670	Yes
Length of Run 2	1114~1386	zero: 1284 one: 1277	Yes
Length of Run 3	527~723	zero: 636 one: 613	Yes
Length of Run 4	240~384	zero: 286 one: 308	Yes
Length of Run 5	103~209	zero: 161 one: 149	Yes
Length of Run 6+	103~209	zero: 148 one: 129	Yes

Table 1: Statistical test of 20,000 random numbers in accordance with FIPS140-2 [5] that is standard test to check the quality. Our results using SBD-MOS passed all tests.

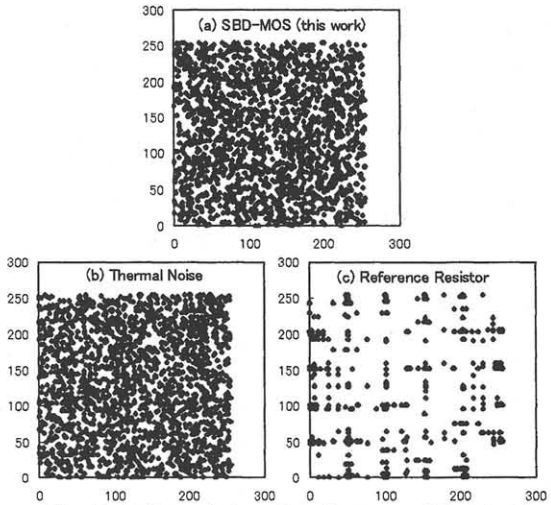

Fig. 5: Self-correlation plots for sequential eight-bit random numbers (decimal:0~255). Our results are superior to the results for the reference resistor, and equivalent to those for thermal noise.

results are superior to the results for the reference resistor, and equivalent to those for thermal noise. These results show that our circuit holds promise as a high-quality random number generator.

4. Conclusion

We demonstrate a new RNG for generating high-quality random numbers close to true random numbers using the large fluctuating resistance of MOS gates after soft-breakdown. This RNG is a small circuit composed of an astable multivibrator and a one-bit counter that can convert the fluctuating currents to random signals without periodicity.

Acknowledgments

We would like to thank K. Uchida for valuable advice to measure fluctuating signals. This work was supported in part by TAO (the Telecommunications Advancement Organization of Japan).

References

[1]Toshiba:http://www.toshiba.co.jp/product/abwr/random/index.htm,
Intel:http://www.intel.com/design/security/rng/rng.htm

[2] T. Asano, Y. Maeda, G. Nakagawa and Y. Arima: Ext. Abs. Solid State Devices and Materials (2001) 96.

[3] F. Crupi, R. Degraeve, G. Groeseneken, T. Nigam and H. E. Maes, IEEE Trans. Electron Devices **45** (1998) 2329.

[4] K. Okada and K. Taniguchi, Appl. Phys. Lett. **70** (1997) 351.

[5] Federal information processing standards publication: FIPS PUB 140-2 (2001) May 25. *The monobit test: count the number of ones in the sequence. The poker test: divide the sequence into consecutive four-bit segments, and examine chi-square tests about the number of each four-bit value (0~15). The long runs test: A long run is defined to be a run of length 26 or more. The runs test: A run is defined as a maximal sequence of consecutive bits of either all ones or all zeros (1~5, over 6).*

[6] D. E. Knuth, The Art of Computer Programming, 3rd ed., Vol. 2 (Addison-Wesley, Boston, 1998).