Extended Abstracts of the 2003 International Conference on Solid State Devices and Materials, Tokyo, 2003, pp. 374-375

G-3-4

Ultra Small Random Number Generating Circuits With A Novel Noise Source Device

Shinichi Yasuda, Hideki Satake, Hanae Nozaki †, Tetsufumi Tanamoto, Ryuji Ohba, Ken Uchida, Atsuhiro Kinoshita and Shinobu Fujita

Advanced LSI Technology Laboratory, Corporate Research & Development Center, Toshiba Corporation
† Computer & Network Systems Laboratory, Corporate Research & Development Center, Toshiba Corporation
1, Komukai Toshiba-cho, Saiwai-ku, Kawasaki, Kanagawa 212-8582, Japan
Phone: +81-44-549-2313, Fax: +81-44-520-1257, E-mail: shinichi3.yasuda@toshiba.co.jp

1. Small Random Number Generators for Security of Mobile Information Systems

Random numbers are used for various purposes in network security systems, for example, as identification numbers, as encryption keys, for blinding secret internal signals from hackers, and so on. With increasing demand for strong security systems, random numbers must be of high quality. In the case of mobile information systems such as smart cards and cellular phone, random number generators (RNGs) must be reduced to chip size. Because conventional high-quality RNGs based on physical phenomena are too large to be used in smart cards, pseudo RNGs are generally used in smart cards, though RNGs show periodicity and regularity. Therefore, it is essential in future security systems to realize a small circuit that can generate high-quality random numbers.

2. Desirable Noise Source Device for the RNG

We proposed various types of small RNGs [1-3]. One of promising RNGs is a novel RNG composed of about twenty CMOS logic gates and several passive devices [1]. This RNG uses a MOS capacitor after soft-breakdown (SBD) as a noise source device whose electrical properties fluctuate randomly, and an astable multivibrator is used for A/D conversion. Figure 1 shows the overall circuit diagram. Even though the noise power spectrum of the MOS capacitor after SBD (MOS-SBD) shows 1/f-like properties that adversely affect the generated random numbers, we demonstrated that the combination of an astable multivibrator and a one-bit counter could eliminate these properties, and that the RNG could produce high-quality random numbers.

However, it is necessary to apply a certain voltage for SBD after the fabrication of RNG. Considering the implementation of this RNG into system LSI, it is not easy to cause SBD of a certain MOS capacitor in an integrated circuit. Therefore, a new noise source device without the post voltage application is more desirable to our RNG.

In this report, we propose a novel noise source device composed of stacked structure of Si and SiO_2, for use in our RNG. Unlike MOS-SBD, the electrical properties of this device fluctuate without post voltage application. We demonstrate high-quality random number generation using our RNG with the noise source device equivalent to that using the SBD-based RNG.

3. Fabrication of Noise Source Device

The noise source device was fabricated on a (100) oriented p-type silicon surface. Thermal oxide film was grown under dry conditions. Undoped silicon was deposited by LPCVD. Next, surface of the deposited silicon layer was oxidized by plasma oxidation. As a result, stacked structure of $SiO_2/Si/SiO_2$ was formed. Finally, the top electrode of phosphorous-doped poly-silicon was deposited. Device patterning was done with photolithography and dry etching. The area of this device is 0.01 mm^2. Figure 2 shows a cross-sectional structure of the device. The thickness of the upper and lower oxide layers is about 1 nm, and the thickness of intermediate silicon layer is also about 1 nm.

In the case of MOS-SBD, multi-tunneling currents flow through trap sites in the oxide film, and the tunneling conductance may fluctuate due to coulomb repulsion. The origin of noise is tunneling conductance fluctuation. In the case of the stacked structure of $SiO_2/Si/SiO_2$, electrons flow from the top electrode to the substrate by double tunneling conduction as shown in Fig. 2. It is expected that the tunneling conductance is strongly affected by quantity of charge trapped in the intermediate silicon layer. Since the quantity of charge changes frequently, the tunneling conductance is expected to fluctuate largely.

4. Device Characteristics

Figure 3 shows the current-voltage characteristics of the noise source device. The dashed line shows the results for silicon dioxide film with a thickness of 2.9 nm, which was almost the same as the total thickness of $SiO_2/Si/SiO_2$ layer for the noise source device. The current was extremely higher than that in silicon dioxide film. This result suggests that the current is subject not to direct tunneling from n^+-poly silicon to substrate but to the double tunneling. Figure 4 shows the current fluctuation at a constant voltage of –1 V. It was confirmed that the current fluctuated. Figure 5 shows the normalized power spectrum density of the current fluctuation determined by Fourier transform. The MOS-SBD signals, where the oxide thickness was 4.9 nm, and drain current noise in pMOSFET with the gate dielectric of oxynitride, channel length of 0.25 μm, and channel width of 10 μm, are also shown for comparison. We could obtain the noise source device with the noise power comparable to the MOS-SBD signal. It is also noted that the noise power is much larger than that for the pMOSFET with relatively large noise.

5. Circuit Performance

The frequency of the astable multivibrator was about 100 kHz, the clock frequency of one-bit counter was 16 MHz, and the bit rate of our RNG is 10 kbit/s. Table 1 shows the results of standard statistical tests of FIPS140-2 [4]. The random numbers for the noise source device passed all of these tests, as well as those for SBD. This shows that this noise source device is suitable for use in our RNG for cryptographic applications.

6. Conclusion

We have demonstrated random number generation using a new noise source device without post voltage application unlike MOS-SBD. Such a device is easy to be fabricated using conventional silicon MOSFET processes. The noise power is large enough to be used for the RNG based on an astable multivibrator. The random numbers generated from the noise signals in this device are of sufficient quality for cryptographic applications.

Acknowledgments

We would like to thank T. Shimizu and K. Miyano for their kind cooperation in fabricating the devices, T. Ohguro for offering data of the MOSFET noise spectrum, and T. Onodera for valuable discussions concerning random number generators. This work was supported in part by the Telecommunications Advancement Organization of Japan (TAO).

References

[1] S. Yasuda, H. Satake, T. Tanamoto and S. Fujita: Ext. Abs. Solid State Devices and Materials (2002) p.250.

[2] K. Uchida, T. Tanamoto, R. Ohba, S. Yasuda, and S. Fujita: Tech. Dig. IEDM (2002) p.47.

[3] S. Fujita, K. Uchida, and S. Yasuda: TOSHIBA REVIEW **58**, No.8, (2003) August.

[4] Federal Information Processing Standards Publication: FIPS PUB 140-2 (2001).

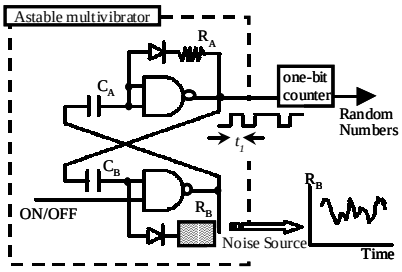

Fig. 1: Schematic diagram of the overall circuit. The period of the rectangular wave (t_1) fluctuates by replacing resister R_B with a noise source device. One-bit counter measures each t_1 and converts fluctuating resistance to one-bit random numbers.

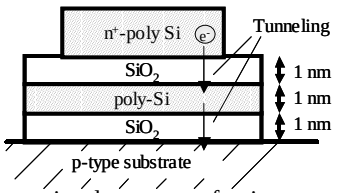

Fig. 2: Cross-sectional structure of noise source device. The thickness of upper and lower oxide is about 1 nm. The thickness of intermediate silicon layer is also about 1 nm.

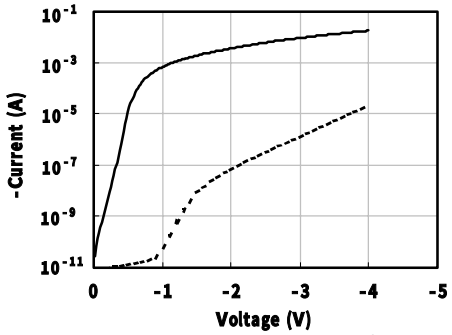

Fig. 3: Current voltage characteristics of noise source device. Dashed line is results for silicon dioxide film with a thickness of 2.9 nm for reference. Electrons flow from the top electrode to the substrate.

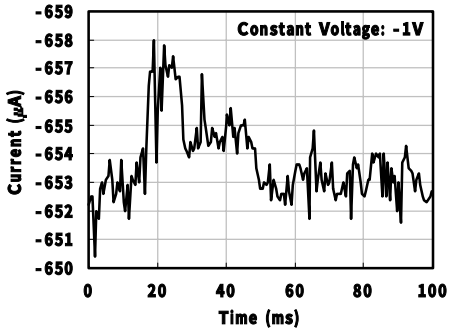

Fig. 4: Current fluctuation under constant voltage of –1 V. The current changed randomly.

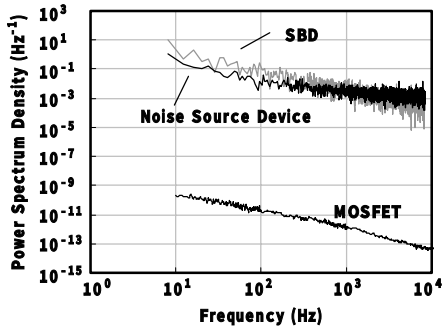

Fig. 5: Normalized power spectrum density of the current fluctuation determined by Fourier transform. The SBD signals and drain current in pMOSFET are also shown for comparison. The noise power for our device is comparable to the SBD signal, and is much larger than that for the pMOSFET.

	Test	Requirement	This Work		SBD	
	Monobit	9725 - 10275	10000	○	10002	○
	Poker	2.16 - 46.17	9.792	○	16.95	○
"0"	Run 1	2315 - 2685	2470	○	2515	○
	Run 2	1114 - 1386	1234	○	1253	○
	Run 3	527 - 723	621	○	662	○
	Run 4	240 - 384	319	○	312	○
	Run 5	103 - 209	157	○	157	○
	Run 6+	103 - 209	168	○	134	○
	Long Run	1 - 26	12	○	16	○
"1"	Run 1	2315 - 2685	2445	○	2551	○
	Run 2	1114 - 1386	1295	○	1232	○
	Run 3	527 - 723	607	○	642	○
	Run 4	240 - 384	294	○	284	○
	Run 5	103 - 209	160	○	162	○
	Run 6+	103 - 209	168	○	162	○
	Long Run	1 - 26	22	○	15	○

Table 1: Results of the statistical tests in FIPS140-2 [2]. Random numbers for the noise source device passed all of these tests, as well as those for SBD.