Extended Abstracts of the 2001 International Conference on Solid State Devices and Materials, Tokyo, 2001, pp. 96–97

D-1-5

Physical Random-Number Generator Using Schottky MOSFET

Tanemasa ASANO, Yasuhiro MAEDA, Gou NAKAGAWA and Yutaka ARIMA
Center for Microelectronic Systems, Kyushu Institute of Technology
680-4 Kawazu, Iizuka, Fukuoka 820-8502, Japan
Phone: +81-948-29-7582, Fax: +81-948-29-7586, E-mail: asano@cms.kyutech.ac.jp

1. Introduction

With the increase in demand of information security and scientific computer simulation, high-quality random-number generators become of great importance. Although arithmetic random-number generation has been widely used, physical random-number generators are highly required to create a high-quality random-number array. Moreover, a generator that is simple in circuit and compact in size are required for embedding in a chip.

Physical random-number generators proposed to date utilize noise from a resistor[1] or a Zener diode[2]. These circuits, however, require a high-gain analog amplifier to pickup noise signal. The high-gain amplification causes an undesired circuit operation such as self-oscillation when, in particular, it is embedded in a chip together with digital logics.

In this report, we propose a physical random-number generator using reversely-operated Schottky MOSFET. The use of Schottky MOSFET[3,4] can eliminate the analog amplifier from generator circuit. Moreover, a control signal can be directly input into the device of noise source, which can make the circuit very simple. This is the first report on the use of a three terminal device as the noise source for a random number generator.

2. Schottky MOSFET as the Noise Source

We have used an SOI MOSFET whose source and drain are composed of PtSi Schottky contacts. The Schottky SOI MOSFETs were fabricated using a self-aligned silicide (salicide) process on SIMOX wafers. Figure 1 shows a cross-sectional view of the fabricated device. Figure 2 shows a subthreshold characteristic of the PtSi Schottky SOI-MOSFET. When the gate is negatively biased, it turns on similarly to the conventional p-channel MOSFET. Extensive characterization has shown that the thermal injection of holes from the source contact to the channel takes place under this bias. On the other hand, when the gate is positively biased, drain current increases with the gate bias. We can clearly see that this current contains noise. Under this gate bias, n-channel is formed and, therefore, electrons are supplied from the PtSi contact to the channel by the field emission through a relatively high potential-barrier (about 0.9 V). This tunneling phenomenon generates noise in drain current. The random-number generator being proposed in this work utilizes this noise.

In Fig. 3, noise levels of the PtSi-Schottky SOI MOSFET when it is operated in field emission mode and of a conventional SOI MOSFET whose source/drain are made of pn-junctions are compared. These results clearly show that the PtSi-Schottky SOI MOSFET operated in the field emission mode contains noise which are much higher in signal level than the conventional SOI MOSFET. It has been confirmed that noise level of the Schottky SOI MOSFETs depends on the workfunction of the contact material. It is noteworthy that the noise characteristic is not peculiar to Schottky MOSFETs on SOI but was observed also for devices fabricated on bulk Si wafers.

3. Circuit and Operation

Figure 4 shows the circuit of the physical random-number generator using the Schottky SOI MOSFET. An inverter is constructed using the Schottky MOSFET. In this study, this inverter was constructed using PtSi-Schottky SOI MOSFETs. A periodic signal is applied to the input of the inverter. The output of the inverter drives a Schmidt triggered inverter. The output of the Schmidt triggered inverter is connected to subsequent JK Flip-Flop circuits. One is to J and K inputs of the first JK Flip-Flop. This JK Flip-Flop counts the number of clock pulses supplied from an external source while the output of the Schmidt triggered inverter is High. The duration of the High signal from the Schmidt inverter fluctuates since the drain current of the Schottky MOSFET of the primary inverter contains noise due to tunneling field emission. Therefore the number of clock pulses counted by the first JK Flip-Flop varies according to the noise of the primary inverter. The output of the Schmidt triggered inverter is also feeded to the clock terminal (CK) of the second JK Flip-Flop. Thus the output Q of the second JK Flip-Flop determines the number of clocks counted during the High state of the output of the Schmidt triggered inverter is even or odd.

In the experimental, a triangular wave of 1 kHz was input to the primary inverter composed of the PtSi SOI MOSFETs. The frequency of the clock pulse supplied to CK of the first JK Flip-Flop was 1 MHz. The circuit blocks other than the primary inverter were constructed using standard CMOS logics. The supply voltage V_{DD} of the circuit was 5 V. For comparison, a primary CMOS inverter composed of conventional pn-junction SOI-MOSFET was also fabricated and tested. Figures 5(a) and 5(b) show output signals of the circuits constructed using Schottky MOSFET and conventional C-MOS inverter, respectively. We can clearly see that the circuit constructed using Schottky SOI MOSFET produces a signal whose duration irregularly varies, while

the circuit constructed using the conventional MOSFET produces a regulated signal in terms of pulse duration. It has been shown that the appearance probabilities of the High and Low states at a constant time interval is equal within statistical error, which indicates the randomness of the generated numbers. Further investigation on the quality of the random number is in progress.

4. Conclusion

A new physical-random-number generator has been proposed and its operation was demonstrated using PtSi-Schottky MOSFETs on SOI. The physics is on the bases of the field emission of electrons in the Schottky source MOSFET. The use of a transistor as the noise source can eliminate a high-gain analog amplifier from the circuit and make the circuit very simple. The circuit can be implemented using bulk Si wafers.

Acknowledgment

This work was supported in part by the Grant-in-Aid for Scientific Research (No. 13025239) from the Ministry of Education, Culture, Sports, Science and Technology.

References

1. E. J. Hoffman: US Patent, No. 5,506,218, 1998.
2. D. P. Brown et al: US Patent, No. 4,853,884, 1989.
3. M. Nishisaka and T. Asano: Jpn. J. Appl. Phys. **37** (1998) 1295.
4. M. Nishisaka, Y. Ochiai and T. Asano: 56th Ann. Device Research Conf. Dig., 1998, p. 74.

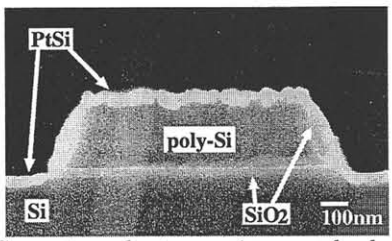

Fig. 1: Scanning electron micrograph showing the cross-section of a Schottky SOI MOSFET whose source/drain are made of PtSi. The device was fabricated using a salicide process on a SIMOX wafer.

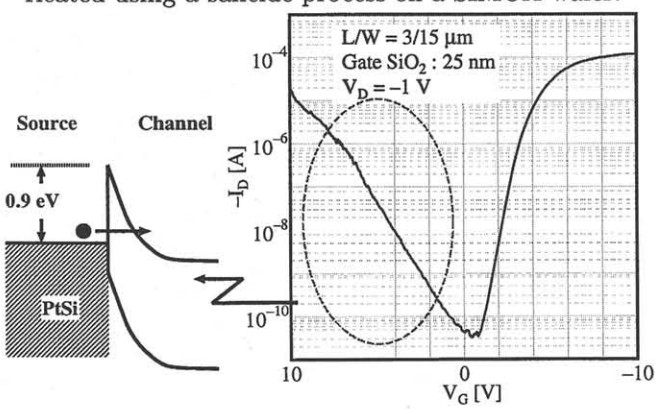

Fig. 2: Subthreshold characteristic of the PtSi-Schottky SOI MOSFET. When the gate is positively biased, i.e. in n-channel operation, noise appears due to the field emission of electrons from the PtSi source to the channel. This characteristic is used as the noise source of the proposed random-generator.

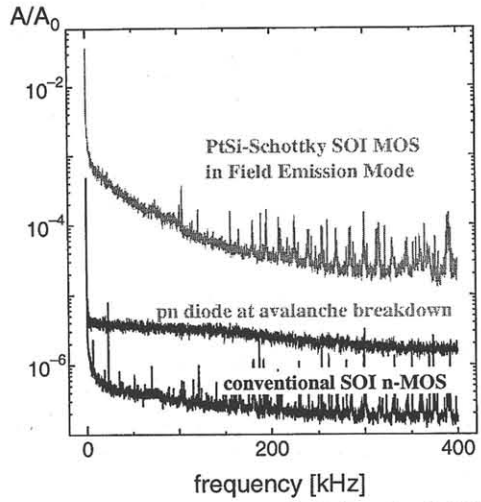

Fig. 3: Noise level of the PtSi-Schottky SOI MOSFET as it is compared with the conventional (pn-junction) SOI MOSFET and avalanche breakdown of a pn-junction diode.

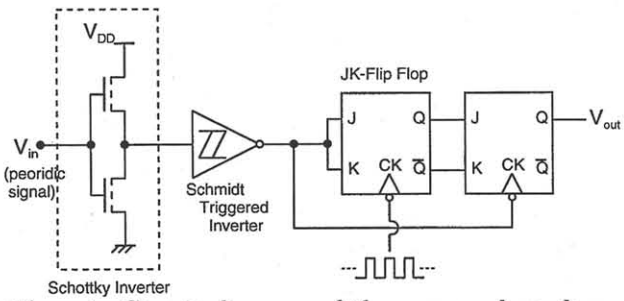

Fig. 4: Circuit diagram of the proposed random-number generator. The Schottky MOSFET constructs a primary inverter to produce a randomly fluctuated pulse widths in conjunction with the subsequent Schmidt triggered inverter.

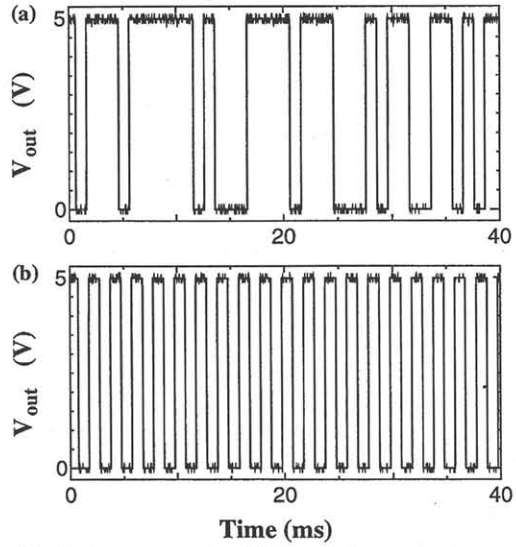

Fig. 5: Output signals of the random-number generators in which the primary inverter was constructed using PtSi-Schottky SOI MOSFET (a) and conventional CMOS (b), showing that the randomly varying pulse duration is produced by using the Schottky MOSFET.