Extended Abstracts of the 2006 International Conference on Solid State Devices and Materials, Yokohama, 2006, pp. 280-281

C-3-2

Random Number Generator with 0.3MHz Generation Rate using Non-Stoichiometric Si_xN MOSFET

Mari Matsumoto, Ryuji Ohba, Shinichi Yasuda, Ken, Uchida, Tetsufumi Tanamoto and Shinobu Fujita

Advanced LSI Technology Laboratory, Toshiba Corporation
Komukai-Toshiba-cho, Saiwai-ku, Kawasaki 212-8582, Japan
Phone: +81-44-549-2313 E-mail: mari.matsumoto@toshiba.co.jp

1. Introduction

Recently, network ubiquitous security for mobile applications has become more important. For network security, a random number generator (RNG) capable of generating unpredictable "true" random numbers is required. In mobile uses, the RNG circuit must be small. However, the present RNGs using white noises are very large circuits [1], because very weak random noise must be amplified using a very large circuit. For small RNG, we examined Si-dot MOSFET noise source device [2], and a simple RNG circuit without amplification circuit was attained. However, the random number generation rate of 25kbits/s was too slow for many mobile applications. A generation rate of 1MHz order is desirable because it is applicable to almost all mobile security uses.

In this work, we propose a new noise source device non-stoichiometric Si_xN (x=1) MOSFET (SiN MOSFET) as shown in Fig.1. Using this device, a much higher generation rate of 0.3MHz is achieved, which is very close to the desirable rate of 1MHz order. In addition, generated random numbers show an excellent randomness, which guarantees unpredictability. SiN MOSFET is a promising noise source for future mobile security.

2. Experiments

SiN nMOSFET with 0.15μm channel width was fabricated based on 40 nm CMOS process. To get large I_D random noise, we use non-stoichiometric Si_xN (x=1) with many dangling bond traps on 0.7nm tunnel oxide (Fig.1). For comparison, we also fabricated a highest density Si-dot MOSFET which has almost the highest density Si dots (10nm size and $1\times10^{12}cm^{-2}$ density) on 0.7 nm thick tunnel insulator, and reference MOSFET with only a gate oxide.

3. Results and Discussion

3-1. Random noise characteristics

Figure 2 shows I_D fluctuation in SiN, highest density Si-dot and ref. MOSFETs for the same L and W at constant voltages. In the highest density Si-dot MOSFET, we can hardly increase Si dot density further. Nevertheless, it is to be noted that I_D fluctuation of SiN MOSFET is much larger than that of the highest density Si-dot device. It is also confirmed that SiN has the strongest noise for all frequency by Fourier characteristics (Fig.3). Therefore, SiN MOSFET is more promising noise source than Si-dot MOSFET.

3-2. Device parameter dependence

Next, we give a device design guideline for enhancement of random fluctuation. Fourier coefficients increase for shorter L (Fig.4 (a)). This is because screening effects due to carrier electrons are more remarkable in longer channel, since carrier density in long channel is more than that in short channel at the same I_D. Fourier coefficients increase for narrower W (Fig.4(b)). This is because the influence of Coulomb force due to a trapped electron is larger for narrower W. It is found that Fourier coefficients depend on Tox exponentially due to tunnel resistance change (Fig.4(c)). We also find that Fourier coefficients increase with Si/N ratio due to trap number increase (Fig.4 (d)).

These results show that even stronger noise can be obtained by suitable device design.

4. Random Number Generation

A simple random number generation circuit composed of astable multi-vibrator and one-bit counter is shown in Fig.5 [3]. The period of output pulse t_j is R_BC_B product in Fig.5, and it fluctuates due to the I_D fluctuation (Fig.6). One-bit counter converts each period t_j to 1-bit random number, '0' or '1'.The generation rate, 0.3Mbits/s, is the inverse of 3.3μs period in Fig.6.

The quality of the random numbers is checked by a statistical test FIPS140-2 (table1) and spectral test (Fig.7)[4,5]. Only SiN satisfies all requirements in the statistical test, and, in the spectral test, no periodicity in SiN MOSFET. Note that complete randomness is achieved in SiN only.

We could obtain near 1MHz (0.3MHz) generation rate. For 1MHz-order generation rate, we can increase I_D random noise by further device design (Fig.4). Moreover, we can also improve converting circuit design, for example, smaller C_B leads to shorter t_j, that is, faster generation rate.

5. Conclusion

We have shown that non-stoichiometric SiN MOSFET shows the strongest random noise, and enables a simple RNG with 0.3Mbits/s generation rate, keeping an excellent randomness. Further device and circuit designs will make 1MHz order generation rate possible SiN MOSFET is an excellent noise source device for future mobile security.

Acknowledgements

This work was supported in part by the National Institute of Information and Communications Technology (NICT) of Japan.

References

[1]http://www.t-rs.co.jp/trs_new/trs_english/products/rmh.htm(Toshiba); http//www.intel.co..design.security rng/rng.htm

[2] R. Ohba et al., IEDM Tech. Dig. P745 (2003)

[3] S. Fujita, et al., ISSCC, pp.294-295, 2004

[4] Federal information processing standard publication FIPS PUB 140-2 (2001) May 25.

[5] D. Knuth, The art of Computer programming 3rd. ed. Vol.2 (Addi-son-Wesley.1998)

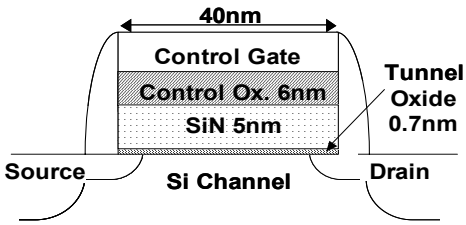


Fig.1 Schematic diagram of device structure

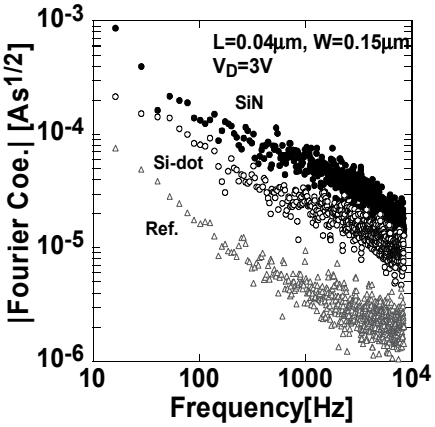


Fig.3 Fourier characteristics corresponding to Fig.2

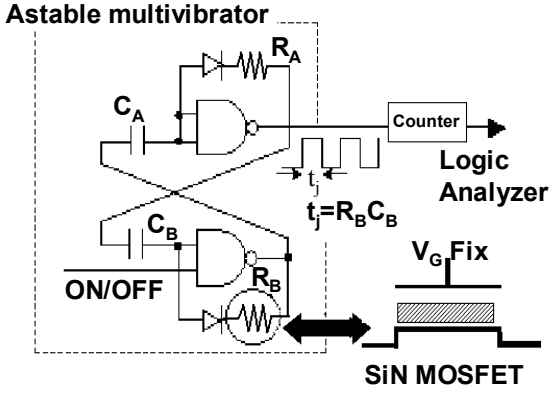
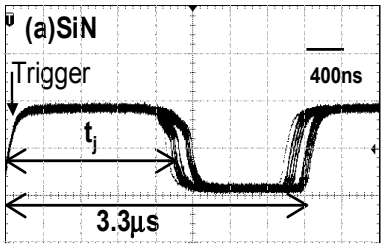


Fig.5 Schematic diagram of the circuit for generating random numbers



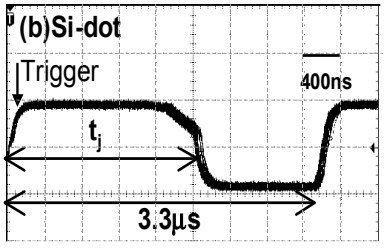


Fig.6 0.3MHz output pulse (a) SiN MOSFET, (b) highest density Si-dot MOSFET

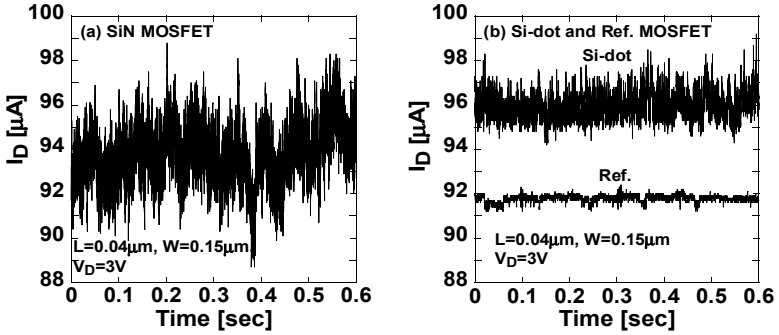


Fig.2 I_D fluctuation for (a) SiN MOSFET and (b) highest density Si-dot and Ref. MOSFET. Time resolution was 60 μs.

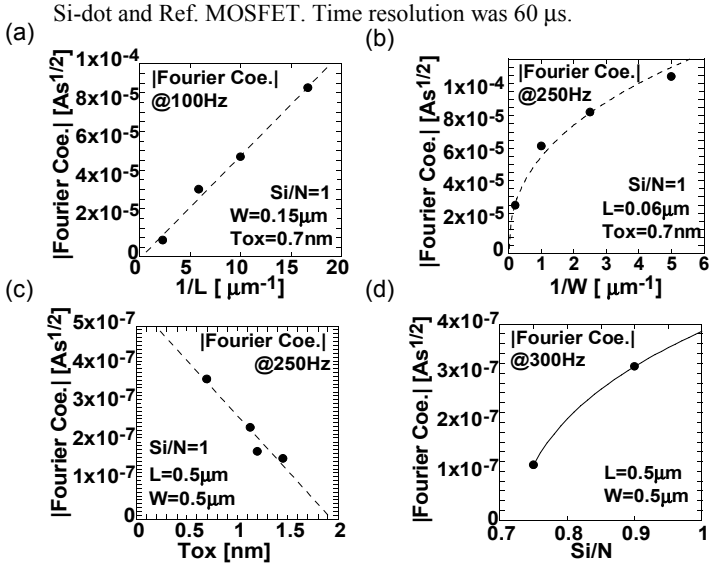


Fig.4. (a) gate length L, (b) channel width W, (c) tunnel oxide thickness Tox, (d) Si/N atomic number ratio dependence of Fourier coefficient magnitude

Test	Requirement	SiN		Si-dot		Ref.	
Monobit	9725-10275	9795	○	10175	○	10030	○
Poker test	2.16-46.17	30.9184	○	531.494	×	12978.3	×
Long run test "0"	1.0-26	12	○	13	○	6	○
"1"		15	○	10	○	6	○
Length of run 1 "0"	2315-2685	2319	○	2250	×	7537	×
"1"		2416	○	2097	×	7495	×
Length of run 2 "0"	1114-1386	1218	○	1946	×	1055	×
"1"		1231	○	1993	×	1085	×
Length of run 3 "0"	527-723	629	○	645	○	62	×
"1"		597	○	695	○	72	×
Length of run 4 "0"	240-384	350	○	217	×	19	×
"1"		306	○	266	○	22	×
Length of run 5 "0"	103-209	156	○	98	×	7	×
"1"		171	○	93	×	5	×
Length of run 6 "0"	103-209	198	○	57	×	4	×
"1"		149	○	69	×	6	×

Table1 Standard statistical test for 20000 random numbers generated at 0.3Mbits/s rate. All requirements are satisfied for SiN MOSFET only.

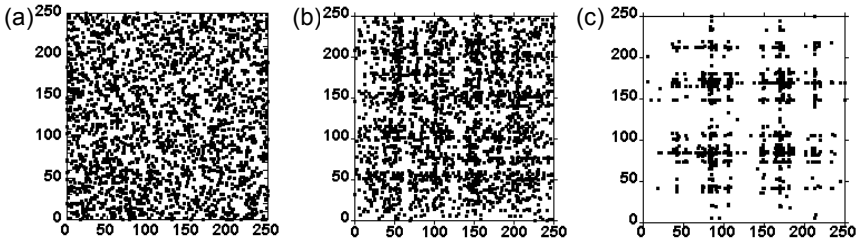


Fig.7 Self-correlation plots for parallel 8-bit random numbers to check periodicity of 20000 random numbers with 0.3Mbits/s rate. (a)SiN, (b)highest density Si-dot, (c) reference MOSFETs