A Hybrid Random Number Generator Using Single Electron Tunneling Junctions and MOS Transistors*

Zhang Wancheng and Wu Nanjian†

(*State Key Laboratory for Superlattices and Microstructures, Institute of Semiconductors, Chinese Academy of Sciences, Beijing* 100083, *China*)

Abstract: This paper proposes a novel single electron random number generator (RNG). The generator consists of multiple tunneling junctions (MTJ) and a hybrid single electron transistor (SET)/MOS output circuit. It is an oscillator-based RNG. MTJ is used to implement a high-frequency oscillator, which uses the inherent physical randomness in tunneling events of the MTJ to achieve large frequency drift. The hybrid SET and MOS output circuit is used to amplify and buffer the output signal of the MTJ oscillator. The RNG circuit generates high-quality random digital sequences with a simple structure. The operation speed of this circuit is as high as 1GHz. The circuit also has good driven capability and low power dissipation. This novel random number generator is a promising device for future cryptographic systems and communication applications.

Key words: random number generator; single electron transistor; multiple tunneling junction; oscillator
PACC: 7335C
CLC number: TN389 **Document code**: A **Article ID**: 0253-4177(2008)04-0693-08

1 Introduction

Random number generators (RNGs) are a critical component in modern cryptographic systems, modern communication systems, and statistical simulation systems. Some RNGs have already been proposed in the literature. Traditional linear feedback shift register circuits only generate pseudo random numbers, which is unsafe in cryptographic applications. The electrical-noise-based RNG consists of a thermal noise source and a noise amplifier, which are difficult to implement in VLSI circuits because the device size and power dissipation of the circuit are large. The oscillator-based RNG uses timing jitter in ring oscillators as a source of randomness[1]. However, sufficient randomness is hard to achieve by relying on the drift of the CMOS ring oscillator alone. Moreover, the power dissipation of the circuit is quite large. Therefore, the development of the RNG with good randomness, compact structure, and low power dissipation is an important issue.

A single electron (SE) shows stochastic tunneling behaviors in SE tunneling devices. Two kinds of SE RNGs have been proposed that rely on the physical randomness of SE tunneling. One RNG employs electron potential pockets as electron traps to stochastically capture or emit an SE[2]. The circuit can work at room temperature (RT) and generates true random bit sequences. The operation speed of the circuit is relatively low, and high-speed random number generation requires additional shift-register-based circuits[3]. Moreover, since both the single-electron transistor (SET) and the electron trap are formed by undulating ultrathin silicon-on-insulator (SOI) film, it is not easy to control the potential barrier between the trap and the channel. The second RNG consists of two complementary SET inverters[4]. The operation speed of the circuit is as high as 1GHz. But, there are serious problems in this RNG: low operation temperature, small output voltage swing, and poor driving capability.

In this paper, we propose a novel hybrid oscillator-based RNG circuit using SE tunneling junctions and metal-oxide-semiconductor (MOS) transistors. A multiple tunneling junction (MTJ) oscillator generates a high-frequency signal whose oscillation period is highly random. A SET and MOS transistor hybrid circuit is used to amplify and buffer the output signal of the MTJ oscillator, and the output of the hybrid circuit is sampled by a conventional D-flip-flop at a lower frequency. The novel RNG has several advantages: (1) the randomness is sufficient to pass standard statistical randomness tests and the score is comparable to commercial RNGs; (2) the power dissipation of

* Project supported by the National Natural Science Foundation of China (No. 90607007) and the Special Funds for Major State Basic Research Project of China (No. 2006CB921201)
† Corresponding author. Email: nanjian@red.semi.ac.cn
Received 5 September 2007, revised manuscript received 23 November 2007

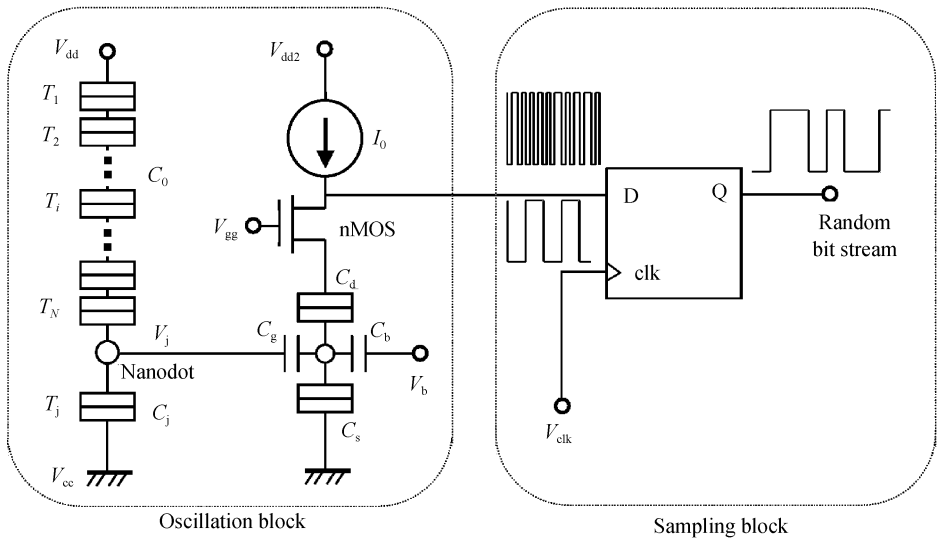

Fig. 1 Schematic of the proposed RNG circuit It consists of an oscillation block and a sampling block.

the circuit is low; (3) the structure of the circuit is simple; (4) the operation speed of the circuit is high and the randomness of the output sequence does not depend on the sampling frequency; (5) the driving capability is large; (6) the circuit tolerates parameter dispersions to some extent. We study the characteristics of the circuit by computer simulation, and we discuss some practical considerations and the integration issue.

2 Novel hybrid random number generator

Figure 1 shows the basic block of the novel hybrid RNG circuit. It consists of two main blocks: the oscillation block and the signal sampling block. The oscillation block generates a high frequency signal with random oscillation periods and outputs it with load capability. The signal sampling block samples the high frequency output signal of the oscillation block at a lower sampling frequency and generates a random bit stream.

The oscillation block consists of an MTJ oscillator and a hybrid SET/MOS circuit. First, we present the operating principle of the MTJ oscillator. There is a nanodot, a main tunneling junction T_j, and an MTJ in the MTJ oscillator. The MTJ consists of N tunneling junctions T_i ($i = 1, 2, 3, \cdots, N$) connected in series. Single electrons tunnel continuously from the ground to V_{dd} one by one through the nanodot and the MTJ. The capacitance of the main tunneling junction C_j is designed to be small enough to sustain a Coulomb blockade at operating temperature, so $C_j \ll e^2/2k_B T$, where e is the electron charge, k_B is the Boltzmann constant, and T is temperature. The tunneling events through T_j are governed by a Coulomb blockade. The voltage V_j across T_j oscillates periodically with the SE tunneling if the main tunneling junction T_j is biased by a constant current source. On the other hand, the capacitance C_0 of each tunneling junction in the MTJ is designed to be much larger than C_j. The probability of each tunneling event in the MTJ oscillator depends on the total free energy of the oscillator circuit. Each tunneling event in the MTJ changes V_j. The time for an SE to transfer from the nanodot to V_{dd} through the MTJ is the summation of the time of many tunneling events, thus the oscillation period of V_j becomes highly random.

Because the MTJ oscillator only possesses a small driving capability, a hybrid SET/MOS circuit is used to buffer the oscillating voltage signal V_j and to output the signal into the signal sampling block. The SET/MOS hybrid circuit possesses a large driving capability. The circuit consists of a pMOS transistor as a constant current source, a dual gate SET, and a nMOS transistor as a cascade device. This is the SET/MOS hybrid circuit proposed and experimentally demonstrated by Inokawa[5]. The SET has two gates: the input gate and the phase control gate. The input gate is connected to the output of the MTJ oscillator. The input signal at the input gate induces Coulomb oscillation of the drain-source current of SET. Combined with the nMOS transistor, the current change of the SET is converted and amplified. The phase control gate is connected to a fixed voltage V_b to adjust the phase of the periodic oscillating output voltage. The hybrid circuit serves as an inverter[6]. When the input voltage is low, the drain-source current of the SET is very low and the output voltage of the inverter is nearly V_{dd2} because the SET nearly operates in a cut

off region. When the input voltage gradually increases, the output voltage sharply switches to low value. Thus, the operation of the hybrid circuit can be divided into three regions: the ON region of SET when the output voltage is low, the OFF region of SET when the output voltage is high, and the linear region when the input voltage is linearly amplified. We can adjust V_b to an appropriate value so that when the input voltage is 0V, the output of the hybrid circuit is the logic threshold of the inverter, which is $V_{dd2}/2$. In this case, if the input signal oscillates from negative value to positive value, the input signal will be nearly linearly amplified. Thus, we can regard the hybrid SET/MOS circuit as a sensitive amplifier.

The sampling block consists of an edge-triggered D-flip-flop and an external sampling clock signal. The high frequency output signal from the SET/MOS circuit is inputted into the sampling block and is sampled at a lower frequency. The output of the D-flip-flop is a binary bit stream. Since the oscillation periods of the oscillator are highly random, the output bit streams are also random.

The characteristic of the oscillation block can be theoretically estimated as follows. The output terminal of the MTJ oscillator is connected to the input gate of the SET, so the output swing of the MTJ oscillator could be approximately given by

$$V_{swing} \approx e/C_{tot}, C_{tot} = C_j + C_g(C_s + C_d + C_b)/(C_g + C_s + C_d + C_b) + C_0/N \quad (1)$$

where C_s, C_d, C_g, C_b is the SET source capacitance, SET drain capacitance, SET gate capacitance, and SET phase gate capacitance, respectively, and N is the number of tunneling junctions in the MTJ. A large V_{swing} is preferable to drive the output buffer. To attain a large voltage swing, C_{tot} should be as low as possible. We use the orthodox theory to calculate the average oscillation frequency of the MTJ oscillator. We assume all tunneling junctions in the MTJ have the same resistance R_0, and we assume the resistance R_j of T_j is much smaller than R_0, so that the average tunneling time through T_j is neglectable. When N is large and temperature is low, the average oscillation frequency f at $T = 0$K is approximately given by

$$f \approx \frac{P + K + N + 1}{2(K + N)C_0R_0} \Big/ \left[\ln\left(\frac{P + K + N + 1}{P + K + 1}\right) + \ln\left(\frac{N + 1}{\alpha}\right)\right] \quad (2)$$

where $K = C_0/(C_j + C_g)$, $P = 4V_{dd}C_0/e - 2N$ and $\alpha \approx 3$. The calculation procedure is shown in the appendix. From Eq. (2), we see that f increases with V_{dd}. Figure 2 shows the typical relationship between f and V_{dd} at various operating temperatures, simulated by the MONTE CARLO simulator SIMON[7]. Calculated

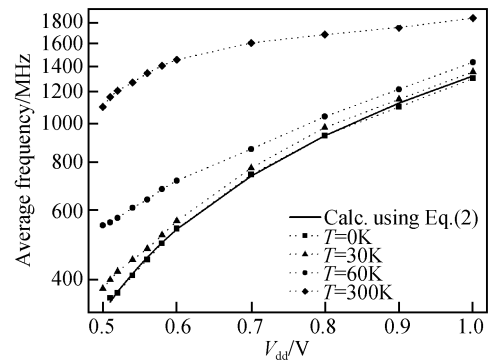

Fig. 2　The average oscillation frequency of the MTJ oscillator as a function of V_{dd} at $T = 0$, 30, 60, and 300K using SIMON2.0 Simulation parameters are: $C_j = 0.6$aF, $C_g = 0.2$aF, $C_m = 4$aF, $R_m = 100$MΩ, $R_j = 10$MΩ, $N = 25$. The solid line denotes the calculated frequency using Eq. (2).

results using Eq. (2) are also shown. Simulation parameters are: $C_j = 0.6$aF, $C_0 = 4$aF, $C_g = 0.2$aF, $R_0 = 100$MΩ, $R_j = 10$MΩ, and $N = 25$. At $T = 0$K, the calculated results fit well with simulation results. At $T > 0$K f is larger, and when $e^2/2C_0$ is comparable with thermal energy, thermal-induced tunneling events dominate and the dependence of f on V_{dd} is weakened. From Eq. (2), we see that both R_0 and N in the MTJ should be large to ensure that the oscillation frequency of the MTJ oscillator is low enough that an external circuit can sense the single tunneling events through T_j.

3　Simulation method and results

The proposed RNG circuit is an SET/MOS hybrid circuit and is hard to simulate with only the MOS circuit simulation method or the SET circuit simulation method. The probability of each tunneling event in the MTJ depends on the total free energy of the MTJ oscillator and the SET. Therefore, we first simulated the oscillation block including the MTJ and the SET by the Monte-Carlo simulator SIMON[7]. The nMOS transistor is treated as a load resistor. We could then obtain the output waveform of the MTJ oscillator from SIMON. This output waveform is an oscillating voltage signal with a random period. The effect of the coupling between the SET and the MTJ has been considered by this Monte-Carlo simulation. Next, we verify the amplifying operation of the SET/MOS hybrid circuit by SPICE. The output waveforms of the MTJ oscillator are transformed into input stimuli of SPICE. Several SPICE-compatible models have been proposed to describe the behavior of SET[8,9]. We choose the compact analytical SPICE model proposed by Inokawa[8]. The model is implemented in SPICE as a subcircuit and its accuracy has been ve-

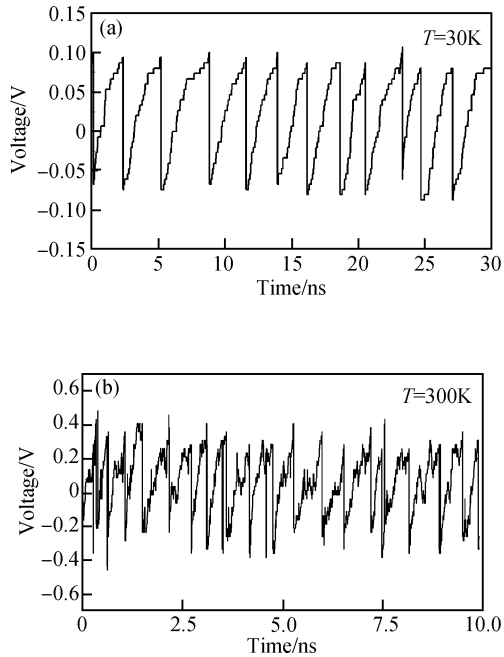

Fig. 3 (a) Typical output characteristic of the MTJ oscillator at T = 30K Simulation parameters are: C_j = 0.6aF, C_g = 0.2aF, C_m = 4aF, R_m = 100MΩ, R_j = 10MΩ, N = 25 and V_{dd} = 0.5V. (b) Typical output characteristics of the MTJ oscillator at T = 300K. Simulation parameters are: C_j = 0.1aF, C_g = 0.1aF, C_m = 2aF, R_m = 30MΩ, R_j = 10MΩ, N = 25 and V_{dd} = 0.5V.

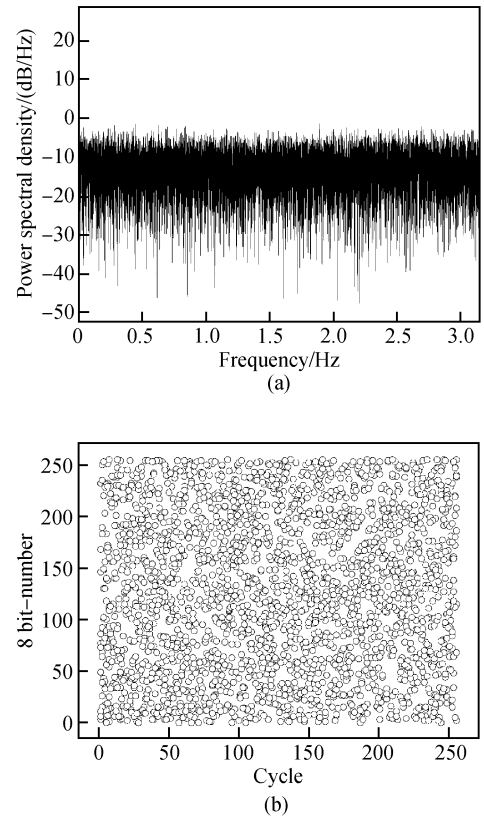

Fig. 4 (a) Power spectral density of the output bit sequence (The result shows a good white noise spectral density); (b) Self-correlation plots for sequential 8-bit random numbers (The distribution of the dots represents the randomness of the sequence)

rified by both SIMON and experiments[10]. We use the Predictive Technology SPICE models of MOS transistor[11] for the MOS transistors.

We simulated the circuit with SIMON and HSPICE. First, we consider the case of low temperature operation. Fig. 3(a) represents a typical characteristic of the output oscillating signal of the MTJ oscillator at T = 30K. Simulation results clearly demonstrate that the oscillation periods are random. For the MTJ oscillator, we choose C_j = 0.6aF, C_m = 4aF, N = 25, R_m = 100MΩ. These parameters are feasible using state-of-the-art fabrication processes. With a 0.5V supply voltage, the corresponding average oscillation frequency is 380MHz. For the SET, we choose C_s = C_d = 0.8aF, R_s = R_d = 90kΩ, and C_g = 0.2aF. For the MOS transistors, we used a commercially available 90nm technology node. The SET/MOS hybrid circuit buffers and amplifies the input oscillating signals well. Next, we consider the case of room temperature operation. In this case, the tunneling junction capacitances of T_j and SET should be small enough to sustain a Coulomb blockade. Thus, both C_j and C_g are set to 0.1aF to attain a large oscillation amplitude. We set C_0 = 2aF so that $e^2/2C_0$ is comparable to the room-temperature thermal energy, and we set R_m = 30MΩ, N = 25. Figure 3(b) represents a typical characteristic of the output oscillating signal of the MTJ oscillator at T = 300K. The magnitude of the oscillation periods ranges from 0.2 to 0.6ns, which is much larger than the CMOS oscillator-based RNGs. The oscillating signal is more irregular due to thermal-induced tunneling events. The average oscillation frequency is 2.3GHz, which indicates that the bandwidth of the SET/MOS hybrid circuit should be much higher. To achieve this, we set C_s = C_d = 0.1aF and we used the 45nm technology node MOS transistors to reduce the inner capacitance of the hybrid SET/MOS circuit.

Simulation results show that the circuit could generate highly random bit sequences with a sampling frequency up to 1GHz. Figure 4(a) shows the spectral density of the output bit sequence when T = 300K and the sampling frequency is 1GHz. Figure 4(b) shows the self-correlation plots for sequential 8-bit random numbers. The randomness of the output bit stream is clearly demonstrated. To examine whether the output sequence is composed of truly random digital numbers, we use the statistical tests of random numbers for cryptographic applications, given in Refs. [12, 13]. We test the randomness of the sequences generated by 100 various operating frequencies between 10 and 100MHz at T = 30K and the randomness of the sequences generated 45 various operating frequencies

Table 1　Results of statistical tests of random numbers generated by the proposed RNG　A comparison with previous work[2] is also listed. √ indicates that the value passes the test.

	Test	Pass Condition	Ref.[2]	T = 30K, 100MHz	T = 300K, 300MHz	T = 300K, 1GHz
FIPS PUB 104-2	Monobit	9725～10275	10043	9840 √	9991 √	9964 √
	Poker test	2.16～46.17	15.88	37.24 √	10.13 √	7.61 √
	Longest Run	1～26	14	16 √	18 √	13 √
	Runs of length 1	2315～2685	[0] 2462 [1] 2409	[0] 2526 √ [1] 2421 √	[0] 2485 √ [1] 2432 √	[0] 2493 √ [1] 2493 √
	Runs of length 2	1114～1386	[0] 1243 [1] 1296	[0] 1373 √ [1] 1431 √	[0] 1248 √ [1] 1217 √	[0] 1236 √ [1] 1220 √
	Runs of length 3	527～723	[0] 647 [1] 586	[0] 582 √ [1] 549 √	[0] 639 √ [1] 640 √	[0] 611 √ [1] 610 √
	Runs of length 4	240～384	[0] 290 [1] 329	[0] 297 √ [1] 254 √	[0] 314 √ [1] 326 √	[0] 300 √ [1] 316 √
	Runs of length 5	103～209	[0] 147 [1] 177	[0] 192 √ [1] 161 √	[0] 149 √ [1] 165 √	[0] 178 √ [1] 138 √
	Runs of length 6 +	103～209	[0] 166 [1] 158	[0] 165 √ [1] 118 √	[0] 160 √ [1] 180 √	[0] 112 √ [1] 179 √
NIST SP 800-22	Freq.	>0.05	0.085	0.308 √	0.898 √	0.611 √
	Freq. within Block	>0.05	0.508	0.295 √	0.158 √	0.247 √
	Runs	>0.05	0.556	0.739 √	0.724 √	0.240 √
	Cumulative-sums	>0.01	N/A	[0] 0.246 √ [1] 0.491 √	[0] 0.730 √ [1] 0.612 √	[0] 0.858 √ [1] 0.922 √
	Spectral DFT	>0.01	N/A	0.896 √	0.516 √	0.06 √
	Serial	>0.01	N/A	[0] 0.143 √ [1] 0.305 √	[0] 0.258 √ [1] 0.377 √	[0] 0.143 √ [1] 0.305 √
	Linear-complexity	>0.01	N/A	0.589 √	0.783 √	0.858 √

between 100MHz and 1GHz at T = 300K. All sequences pass these standard tests. Table 1 shows the typical results of the tests, with an operating frequency of 100MHz at T = 30K and an operating frequency of 300MHz and 1GHz at T = 300K, respectively. A comparison with previous SE RNG[2] is also listed. The performance of the sequence is as good as or even better than commercial ones.

What is striking here is that the frequency separation between the high frequency of the MTJ oscillator and the sampling clock frequency is very small. Unlike previous oscillator-based RNG designs[1], sufficient randomness is achieved by relying on oscillator drift alone. The key point is that the frequency drift of the MTJ oscillator is very large. Moreover, this frequency separation between the high frequency and the clock frequency is arbitrary, which means the clock frequency does not affect the performance of the circuit. To illustrate this, we use a standard quantitative check of the randomness of the bit sequence, which is also referred as "the poker test". The equation is given by Ref.[14]

$$\Phi = \left[\frac{64}{N_m}\sum_{i=0}^{15} f^2(i)\right] - \frac{1}{4}N_m \qquad (3)$$

where N_m is the number of bits in the sequence and $f(i)$ is the number of non-overlapping 4-bit nibbles with decimal equivalent i. This variable determines how uniformly the bit stream is distributed when grouped in nibbles. Figure 5 shows the effect of sampling frequency on randomness. Unlike conventional oscillator-based RNGs[14], there is no clear relationship between frequency and Φ, which indicates that the sampling frequency has a wide range.

If we set the supply voltage of the hybrid SET/MOS circuit to 1V and the constant current I_0 to less than 400nA, the power dissipation of the oscillator block is less than 500nW, which is much lower than conventional RNGs. The structure of the circuit is also simple. We believe the proposed circuit may serve as a promising component in future on-chip VLSI appli-

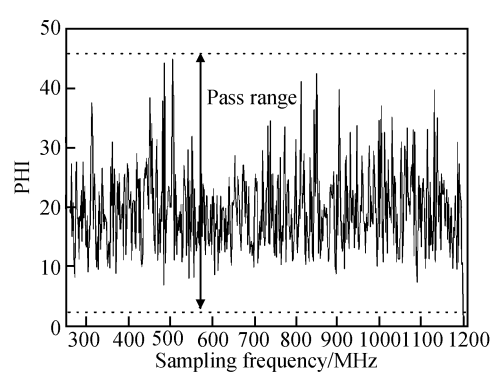

Fig. 5　The relationship between working frequency and Φ at T = 300K　Here Φ is a good quantitative check of the randomness of a 20000 bit sequence[15]. No clear relationship could be obtained.

cations.

4 Discussion

In the previous sections, we showed the operation principle of the novel RNG. For practical implementation of the circuit, the integration issue and the effect of parameter dispersions must be taken into account. In this section, we will discuss these points in detail.

4.1 Integration issue

Recent developments in semiconductor-based MTJ open up the possibility of practical high temperature applications[15~19]. An 11-island Si-based MTJ with average tunneling capacitance of 3.4aF was reported in Ref. [15], and a reproducible Si-based MTJ was reported in Ref. [16]. Two dimensional Si-based MTJ with an average tunneling capacitance of 0.56aF was reported in Ref. [17]. Moreover, epitaxially grown nanowire MTJ with small tunneling capacitance was reported in Ref. [18], and tunneling of SEs through the MTJ was detected[18]. Moreover, the recent development of self-assembled molecular devices opens up the possibility of highly reproducible SE devices with RT operation[19].

Fabricating an MTJ with N tunneling junctions with large capacitances and one tunneling junction with a much smaller capacitance is difficult with the current fabrication process. However, since semiconductor-based tunneling junctions can be fabricated by thermal oxidizing the etched pattern, it is possible to fabricate an MTJ with N-M tunneling junctions having relatively large capacitance C_0 and M tunneling junctions with decreasing capacitance ($C_{ji} < C_{jk}$, $i < k$). For instance, $C_{jM} = C_0$, $C_{jM-1} = 0.8C_0$, ..., $C_{j1} = 0.15C_0$. In this case, the operation principle of the MTJ oscillator remains the same. Actually, the key points of the successful operation of the MTJ oscillator are the oscillation of the output signal and the randomness of the oscillation period. We have verified that, whenever $N \gg M$, with various parasitic capacitances and tunneling capacitances C_{ji} ($i = 1, \ldots, M$), the MTJ oscillator functions well and the circuit generates random bits. Compared with the ideal case, we only have to adjust the supply voltage and the operating point of the SET/MOS hybrid circuit.

4.2 Effect of parameter dispersions

Fluctuations of device parameters in nanodevices are unavoidable. When parameter dispersions in the MTJ are small, the average oscillation frequency drifts, but the operating principle of the MTJ oscillator remains same. When the parameter dispersions in the MTJ are too large, the tunneling events are not dominated by T_j, and the output signal may be irregular. We simulated various circuits in which the capacitance and resistance of each tunneling junction are randomized to be $(1 \pm p_1\alpha)\ C_0$ and $(1 \pm p_2\alpha)\ R_0$, where p_1 and p_2 are uniform random numbers between 0 and 1, and α denotes the maximum percentage of parameter dispersions, $\alpha < 1$. For each α, we randomize the parameters more than 150 times. We tested whether the output sequences can pass all the FIPS tests. Fig. 6 shows the relationship between the pass rate and α, with a 100MHz operating frequency. When $\alpha < 0.5$, the pass rate is higher than 98%. When $\alpha > 0.5$, the pass rate decreases rapidly as α increases. So the MTJ oscillator tolerates a large extent of parameter dispersion.

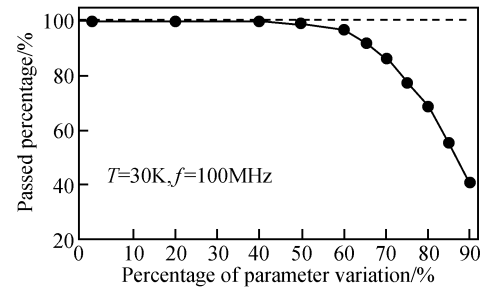

Fig. 6 Relationship between the pass rate of the statistical tests of the output bit sequences and maximum percentage of parameter dispersions

Background charge is an infamous problem in the field of SE devices. Simulation results show that the performance of the MTJ oscillator is nearly not affected by background charge of nanodots. However, the Coulomb oscillation characteristic of the SET is strongly affected by background charge. This effect can be compensated by adjusting the bias voltage V_b on the phase control gate of SET. We can also use an automatically phase controlled circuit containing a Memory-Node[20] to compensate the effect of the background charge.

4.3 Appropriate number of junctions in the MTJ

As discussed above, a large N is essential for the MTJ oscillator. An interesting question is what N is appropriate, since the area of the circuit increases with N. We simulated various circuits with different N in the MTJ while keeping the equivalent overall resistance and capacitance of the MTJ unchanged. For each circuit, we generate more than 100 random bits sequences to determine whether they pass all the FIPS tests. Figure 7 shows the relationship between N and the pass rate of bit sequences. The pass rate increases

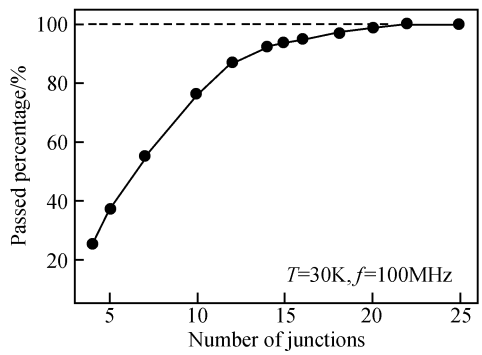

Fig. 7　Relationship between the pass rate of the statistical tests of the output bit sequences and number of junctions in the MTJ (The equivalent total resistance and capacitance of the MTJ is held constant).

as N increases, and when $N > 20$, it is larger than 99%. Since the area of the circuit increases with N and an MTJ with too many tunneling junctions is difficult to fabricate, $20 < N < 40$ seems appropriate.

5　Conclusion

A single electron RNG using MTJ and MOS transistors has been proposed. The circuit uses an MTJ oscillator to generate high-frequency oscillation signals. Due to its inherently stochastic characteristic, the MTJ oscillator outputs oscillating voltage with a random cycle. A hybrid SET/MOS circuit was used to amplify and buffer the oscillation signal. A D-flip-flop with a low-frequency sampling signal samples the high-frequency signal to generate random bit signals. Compared to conventional CMOS RNG circuits, the structure of the circuit is simple, while the power dissipation is much lower. Moreover, the randomness of the circuit does not depend on the operating frequency. The output bit streams of the circuit are sufficient to pass all standard statistical tests. If the RNG proposed in Ref. [4] is regarded as an SE counterpart of the conventional electrical-noise-based RNGs, the circuit proposed in this paper could be viewed as an SE counterpart of the conventional oscillator-based RNGs.

Appendix

We consider the case when $T = 0$ and $N \gg 1$. To transfer an SE through the MTJ, at least N tunneling events occurs, so the average oscillation period is the summation of the averaging tunneling time through the N tunneling junctions in the MTJ, and the average oscillation frequency is $1/f = \sum_{i=1}^{N} t_i$, where t_i is the average tunneling time of the ith tunneling event. Since tunneling is a stochastic process, using the MONTE CARLO approach, the probability that a tunnel event happens at t and not earlier is $P_0(t) = e^{-\Gamma t}$. In the tunnel junctions of the MTJ, the event with the smallest tunneling time will happen first, so that t_i is given by

$$t_i = \min_{j=1}^{N+1-i}(t_i(j)), t_i(j) = -\ln(\gamma)/\Gamma_i \quad (1)$$

where γ is a uniform random number between 0 and 1, and Γ_i is the tunneling rate of the ith tunneling event. When $i \ll N$, $t_i \approx 1/(N+1-i)\Gamma_i$. Γ_i is given by

$$\Gamma_i = \frac{\Delta W(i)}{e^2 R_0} \times \frac{1}{1 - \exp(-\Delta W(i)/k_B T)} \quad (2)$$

Here $\Delta W(i)$ is the change of electrostatic energy of the system after the ith tunneling event, which is given by

$$\Delta W(i) = \frac{(i + P + K)e^2}{2(K + N)C_m} \quad (3)$$

where $K = C_0/(C_j + C_g)$, $P = 4V_{dd}C_0/e - 2N$. When $N \gg 1$, we can replace summation with integration. So that the average oscillation frequency is approximately

$$f \approx \frac{N + K + P + 1}{2(K + N)C_0 R_0} \Big/ \left[\ln\left(\frac{P + K + N + 1}{P + K + 1}\right) + \ln\left(\frac{N + 1}{3}\right)\right] \quad (4)$$

References

[1] Fairfield R C, Mortenson R L, Coulthart K B. An LSI random number generator. Proc Advances in Cryptology Conf (CRYPTO '84), 1984: 203

[2] Uchida K, Tanamoto T, Ohba R, et al. Single-electron random-number generator (RNG) for highly secure ubiquitous computing applications. International Electron Devices Meeting (IEDM), 2002: 177

[3] Fujita S, Uchida K, Yasuda S, et al. Si nanodevices for random number generating circuits for cryptographic security. 2004 IEEE International Solid-State Circuits Conference (ISSCC), 2004: 294

[4] Akima H, Sato S, Nakajima K. Single electron random number generator. IEICE Trans Electron, 2004, E87-C(5): 832

[5] Inokawa H, Fujiwara A, Takahashi Y. A merged single-electron transistor and metal-oxide-semiconductor transistor logic for interface and multiple-valued functions. Jpn J Appl Phys, 2002, 41 (1-4B): 2566

[6] Zhang W C, Wu N J. Novel hybrid voltage controlled ring oscillators using single electron and MOS transistors. IEEE Trans Nanotechnol, 2007, 6: 146

[7] Wasshuber C, Kosina H, Selberherr S. SIMON-a simulator for single-electron tunnel devices and circuits. IEEE Trans Comput Aided Des, 1997, 16: 937

[8] Inokawa H, Takahashi Y. A compact analytical model for asymmetric single-electron tunneling transistors. IEEE Trans Electron Devices, 2003, 50: 455

[9] Mahapatra S, Vaish V, Wasshuber C, et al. Analytical modeling of single electron transistor for hybrid CMOS-SET analog IC design. IEEE Trans Electron Devices, 2004, 51(11): 1772

[10] Inokawa H, Takahashi Y. Experimental and simulation studies of single-electron-transistor-based multiple-valued logic. Proc 33rd IEEE Int Symp Multiple -Valued-logic, 2003: 259

[11] Cao Y, Sato T, Sylvester D, et al. New paradigm of predictive

MOSFET and interconnect modeling for early circuit design. Proc CICC,2000:201
[12] NIST (National Institute of Standards and Technology). Security Requirements for Cryptographic Modules (FIPS PUB 104-2, 2001)
[13] NIST(National Institute of Standards and Technology). A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications (NIST SP 800-22)
[14] Petrie C S, Connelly J A. Modeling and simulation of oscillator-based random number generators. IEEE International Symposium on Circuits and Systems(ISCAS '96),1996,4:324
[15] Nakajima A, Ito Y, Yokoyama S. Conduction mechanism of Si single-electron transistor having a one-dimensional regular array of multiple tunnel junctions. Appl Phy Lett,2002,81:733
[16] Single C, Prins F E, Kern D P. Simultaneous operation of two adjacent double dots in silicon. Appl Phy Lett,2001,78:1421
[17] Nuryadi R, Ishikawa Y, Tabe M. Single-photon-induced random telegraph signal in a two-dimensional multiple-tunnel-junction array. Phy Rev B,2006,73:049903
[18] Thelander C, Nilsson H A, Jensen L E, et al. Nanowire single-electron memory. Nano Lett,2005,5:635
[19] Likharev K K. SET: coulomb blockade devices. Nano et Micro Technologies,2003,3(1/2):71
[20] Nishiguchi K, Inokawa H, Ono Y, et al. Automatic control of oscillation phase of a single-electron transistor. IEEE Electron Device Lett,2004,25(1):31

一种基于单电子隧穿结和 MOS 晶体管的混合随机数发生器*

张万成 吴南健†

(中国科学院半导体研究所 超晶格国家重点实验室, 北京 100083)

摘要: 提出了一种新颖的单电子随机数发生器(RNG). 该随机数发生器由多个单电子隧穿结(MTJ)以及单电子晶体管(SET)/MOS管混合输出电路组成. MTJ 被用于实现一个高频率的振荡器. 它利用了电子隧穿的物理随机性得到了很大的振荡频率漂移. SET/MOS 管输出电路放大并输出 MTJ 振荡器的输出信号. 该信号经过一个低频信号采样后,产生随机数序列. 所提出的随机数发生器使用简单的电路结构产生了高质量的随机数序列. 它具有简单的结构,输出随机数的速度可以高达 1GHz. 同时,该电路还具有带负载能力以及很低的功耗. 这种新颖的随机数发生器对未来的密码和通讯系统具有一定的应用前景.

关键词: 随机数发生器; 单电子电路; 多隧穿结; 振荡器
PACC: 7335C
中图分类号: TN389 **文献标识码**: A **文章编号**: 0253-4177(2008)04-0693-08

* 国家自然科学基金(批准号: 90607007)和国家重点基础研究发展规划(批准号:2006CB921201)资助项目
† 通信作者. Email:nanjian@red.semi.ac.cn
2007-09-05 收到,2007-11-23 定稿