A low power true random number generator in 0.18μm CMOS

Zhi-Wen Huang, Ming Li and Pei-Yuan Wan
Beijing Embedded System Key Lab, College of Electronic Information & Control, Engineering, Beijing University of Technology, Beijing 100124, China
E-mail: wanpy@bjut.edu.cn

This paper presents the design and implementation of a true random number generator (TRNG) for smart card application. Based on the effect of the oscillator phase noise and meta-stable state of the trigger, the random number is generated. An efficient calibration method can correct the uniformity of random number sequences and improve the distribution of the random number. The prototype of the TRNG is fabricated in a 0.18μm CMOS technology. Under the standard diehard test, the results show that bit rate is 1Mb/s and the TRNG has a good pass rate under a bad condition. The power consumption of the TRNG is 0.066mW with a 1.8V power supply.

Keywords: True Random Number Generator; Smart Card; Oscillator.

1. Introduction

With the development of the information society, cryptography is widely used in the information system. The unpredictability and non-repeatability of random number plays key roles in cryptography. Random number generator is divided into true random number generator (TRNG) and pseudo random number generator (PRNG). PRNG cannot meet the requirements of unpredictability and non-repeatability. TRNG is based on the stochastic characteristics of the physical phenomena that can meet the requirements. In the circuit level, general methods for the implementation include amplifier noise [1], oscillator phase noise [2] and so on. In this paper, a low power TRNG is designed and realized for smart card applications.

This paper is organized as below. Firstly the principle of TRNG, including oscillator sampling and trigger meta-stable state, is described. Secondly a calibration module for the true random number generator is analyzed. At last, the testing results of the prototype TRNG is presented. In addition, the low power design is described.

2. Design of True Random Number Generator

Traditional oscillation sampling method [3] uses a low frequency clock to sample a high frequency clock. The output of the sampling value is random number sequence. This method has two disadvantages. The first one is that the jitter of the oscillator is difficult to meet the design random requirements. Another is that the random number rate is restricted. In order to solve these problems, a TRNG based on the phase noise of the oscillator [4] and the metastability of the trigger with effective calibration circuit is presented in this paper.

In the following, the time jitter of the circular oscillator and the metastability of the trigger are explained to generate true random sequence, which is to obtain the true random number seed. And then, the digital calibration and lower frequency sampling method are used to effectively improve the statistical characteristics of true random number sequence.

2.1. *The true random number sequence generation module*

As shown in Figure 1, ring_osc1 and ring_osc2 are two symmetrical circular oscillators. Ideally, ring_osc1 and ring_osc2 have the same rising and falling edge. However in practice, the thermal noise, flicker noise and substrate noise can lead to the random jitter of the output of the oscillator, and this random jitter is satisfied the Gauss statistical distribution. In order to simplify the analysis, it is assumed that ring_osc1 is an ideal clock without phase noise and the total phase noise is equivalent to ring_osc2. Because of the random jitter of noise, the first rising edge of ring_osc2 is ahead of the first rising edge of ring_osc1 as shown in Figure 2. So the sampling value of the trigger is 0. The second rising edge of ring_osc2 is behind of that of ring_osc1, the sampling value is 1. Accordingly, the random number sequence generator based on phase noise can be obtained.

If metastability of the trigger is considered, the hold time of the trigger cannot be satisfied when the rising edge of the ring_osc2 comes first. Conversely, the setup time of the trigger cannot be satisfied when the rising edge of the ring_osc1 comes first. The two above cases have some certain probability of the occurrence of metastability[5].

In the metastable condition, the output of the D trigger over a period of time will be in a state of uncertainty, oscillating between 0 and 1, rather than a samples value. After a period of recovery time, the output will be stable. When metastable occurs, the result of the trigger is uncertain with randomness. In order to use this randomness, three stage D trigger is used as the synchronizer shown in Figure 3.

Based on the metastability model, when the metastable state occurs in the first stage, the probability of stable state of the second and third stage is 90% and 99%, respectively. The third stage output level of the trigger is almost stable and the result of the output is random.

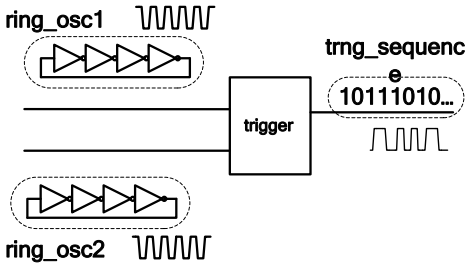


Fig. 1 Generation module of true random number

According to the above analysis, whether or not the first stage D trigger metastable is, the output of the third stage D trigger will not be metastable and the output will be random.

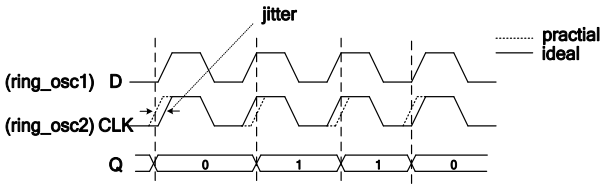


Fig. 2 Oscillator sampling timing diagram

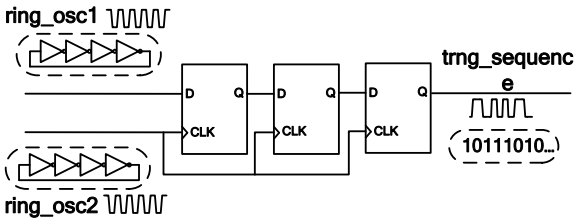


Fig. 3 Three stage synchronous trigger

Figure 4 shows the circuit structure of the oscillator. This oscillator is based on 3-invertor rings. A current is injected into the ring oscillator, which makes the oscillator with only a little current consumption. The traditional ring oscillator use rail to rail power supply. It is obviously that the proposed oscillator can achieve low power design.

The relationship between power, frequency and voltage is explained as below:

$$P \propto f \bullet V^2 \quad (1)$$

Also by the formula (1), the higher the output voltage swing of the oscillator is, the higher the power consumption is. The traditional structure of the oscillator voltage swing is 0 to 1.8V, while the structure of the figure 4 is improved with 0.6V swing. So the power consumption associated with the voltage swing is reduced by about 75%.

In the layout design of the oscillator, two oscillators need to ensure symmetry and matching with similar process deviations. Sampling of trigger in this design adopts full custom design without digital standard cell.

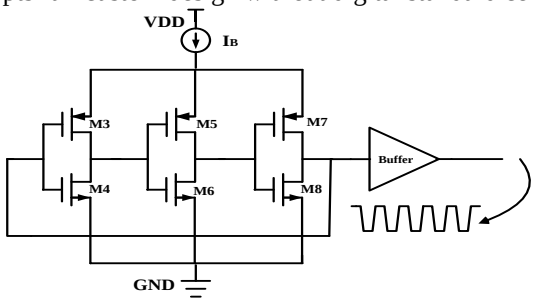


Fig. 4 Low power circular oscillator

2.2. *Random number uniformity calibration module*

Ideally the true random number sequence generated by the physical method has the advantage of unpredictability and non-repeatability. But sampling process is vulnerable, such as variations of voltages, temperature and etc, which results in poor uniformity of a true random number sequence [6]. At the same time, a long string of 0 or a long string of 1 sequence also belongs to true random. But the statistical nature of above sequence is poor. Therefore, a calibration circuit is needed to resolve the above problems.

The common calibration method uses a Von-Neumann corrector, XOR chain or linear feedback shift register. Among them, Von Neumann has a very good effect on the uniformity and correlation of the correction sequence. But it can cause uncertain declination of internal random number sequence.

Figure 5 shows the structure of the calibration module proposed in this design. It contains four stages XOR chain, linear feedback shift register and the feedback calculation module.

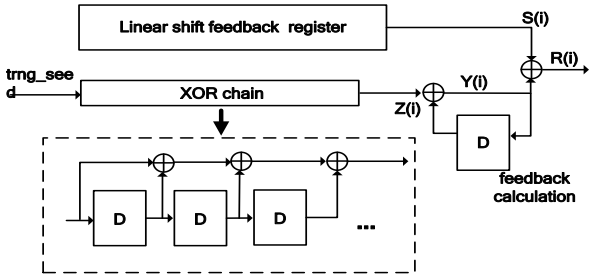


Fig. 5 True random number calibration module

Based on the previous analysis, the probability of the trigger output 1 is p before the calibration. Then the probability of the trigger output 0 is (1-p). And the probability of each level output 1 or 0 is independent. So after the first stage XOR chain, the probability of the trigger output 1 is 2p (1-p). By mathematical induction, the probability of the trigger output 1 is $0.5\text{-}2^{N-1}(p\text{-}0.5)^N$ with N XOR chain. So, if N tends to infinity, the probability of the trigger output 0 or 1 is equal in the ideal state, which is desired for the true random number sequence with excellent uniformity. However, the more XOR chain is, the greater compression ratio of the data is. This is a tradeoff in realization. In this design four stages XOR chain is used. In order to improve the statistical characteristics of true random number, the calibration module contains a feedback module and a generation module with uniform distributed and non-related periodic sequence [7].

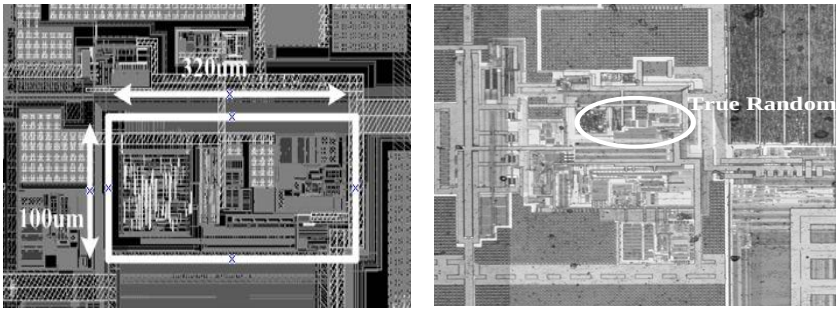
There are many ways to realize the uniform distribution and non-related periodic sequence. This design uses the linear shift feedback register. From Figure 5, it can be obtained:

$$E[Y(i+1)] = E[Y(i)] + E[Z(i)] - 2E[Y(i)]E[Z(i)] \tag{2}$$

Because E[Y(i+1)]=E[Y(i)], if E[Z(i)] ≠0, then E[Y(i)]=0.5. After the XOR operation, the Y(i) is uniformly distributed. Ultimately, the generated random number sequence is non-related and uniform.

3. Experimental Results

The TRNG proposed in this paper is designed on smart card applications. The prototype TRNG is implemented with a 0.18-μm CMOS technology. Figure 6 shows the layout of the TRNG circuit. The active area is about 320μm*100μm. With a power supply of 1.8V, the power consumption of TRNG is 0.066mW.



(A)Layout of the TRNG circuit (B) Microscope photo of the TRNG circuit

Fig. 6 Layout and Microscope photo of the TRNG circuit

With Asynchronous sampling by a logic analyzer, the random number sequences can be captured and analyzed. A total of 50 samples were tested for standard diehard under different temperatures and voltages. With variation of voltages from 1.70V to 1.98V, and temperatures from -40℃ to 40℃, the test results is shown in the Figure7.

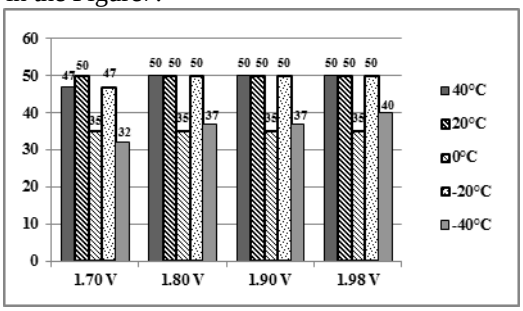


Fig. 7 Result of test

4. Conclusion

In this paper, a low power TRNG for smart card applications is designed and implemented. The TRNG combined the utilization oscillator phase noise and metastable state of the trigger. A calibration circuit is proposed to improve the statistical characteristics performance of the TRNG. The prototype of the TRNG is measured with standard diehard test under various voltage and temperatures. Under standard diehard test, the test results of TRNG shows that bit rate is 1Mbit/s and the true random number generator pass diehard testing standards.

References

1. Petrie C S and Connelly J A, IEEE Trans circ and Syst, 2000, 47(5):615-616.

2. M.Bucci L, Germani, R.Luzzi and etc, IEEE Trans Computers, 2003,52(4):403-409.
3. Y.Ogasahara, M.Hashimoto and T.Oneye, IEEE J Solid-State Circuits, 2009, 44(6):1745-1755.
4. M.Azarmehr, R.Rashidzadeh and M.Ahmadi, IEEE IET Circuits Devices Syst, 2012:79-80.
5. Carlos Tokunaga, David Blaauw, Trevor Mudge, True Random Number Generator With a Metastability-Based Quality Control[J], IEEE Journal of Solid-State Circuits, 2008,43(1):78-85.
6. Behzad Razavi, Design of Analog CMOS Integerated Circuits[M], New York:McGraw,2011.
7. Eberhard Bohl, Simple true random number generator for any semi-conductor technology[J], IET Journals & Magazines, 2014,8(6):239-245.