A true random number generator based on meta-stable state

Lingyan Fan¹, Yongping Long¹, Jianjun Luo¹a, Liangliang Zhu¹, and Hailuan Liu²

¹ Micro-Electronics Research Institute, Hangzhou Dianzi University, Hangzhou Zhejiang 310018, China
² Sage Microelectronics Corporation, 910 Campisi Way, Campbell, CA 95008, USA
a) jianjun.luo@hdu.edu.cn

Abstract: This paper presents a ring oscillator structure which combines meta-stable states with Fibonacci ring oscillators (FIRO) and Galois ring oscillators (GAROs). Based on the new structure, a true random number generator (TRNG) of 64-bit was created. This new TRNG was verified by FPGA platform with Altera Cyclone IV series chips, and its output has attained NIST SP800-22 certification. The testing demonstrates that the proposed meta-stable random number generators improve randomness over traditional methodologies.

Keywords: meta-stability, Fibonacci ring oscillator, Galois ring oscillator, TRNG

Classification: Electron devices, circuits and modules

References

[1] V. Bahadur, et al.: “Reconfigurable side channel attack resistant true random number generator,” 2016 International Conference on VLSI Systems, Architectures, Technology and Applications (VLSI-SATA) (2016) 1 (DOI: 10.1109/VLSI-SATA.2016.7593048).
[2] S. Li and F. Cao: “Random numbers from an integrated CMOS double-scroll,” IEICE Electron. Express 7 (2010) 1382 (DOI: 10.1587/elex.7.1382).
[3] D. Yoshioka, et al.: “On transformation between discretized Bernoulli and Tent maps,” IEICE Trans. Fundamentals E88-A (2005) 2678 (DOI: 10.1093/ietfec/e88-a.10.2678).
[4] J. D. Golic: “New methods for digital generation and postprocessing of random data,” IEEE Trans. Comput. 55 (2006) 1217 (DOI: 10.1109/TC.2006.164).
[5] Ü. Güler, et al.: “A digital IC random number generator with logic gates only,” IEEE International Conference on Electronics, Circuits, and Systems (2010) 239 (DOI: 10.1109/ICECS.2010.5724498).
[6] M. Epstein, et al.: “Design and implementation of a true random number generator based on digital circuit artifacts,” Proc. International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2003 (2003) 152.
[7] M. Majzoobi, et al.: “FPGA-based true random number generation using circuit metastability with adaptive feedback control,” Proc. International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2011 - (2011) 17 (DOI: 10.1007/978-3-642-23951-9_2).
[8] I. Vasyltsov, et al.: “Fast digital TRNG based on metastable ring oscillator,”
1 Introduction

True Random Number Generator (TRNG) is an important part of encryption systems. The output of the TRNG is unpredictable numbers or strings, which are essential keys for encrypting the information. In a way, the performance of encryption algorithms is affected by the randomness of random numbers [1, 2, 3]. In 2006, Jovan Dj.Golic [4] proposed a digital TRNG based on asynchronous feedback logic. In their method, the entropy source is designed by the Fibonacci Ring Oscillator (FIRO) and the Galois Ring Oscillator (GARO), which combines pseudo-randomness of the Linear Feedback Shift Register (LFSR) with the true randomness of the clock jitter. In 2010, based on Golic’s method, Ülkühan et al. [5] used seven entropy sources composed of 31 GAROs and 15 FIROs to achieve the highest random number output of 31.25 Mbit/s. The randomness of the random number generated by the above methods is mainly from true randomness of clock jitter and the pseudo-randomness introduced by LFSR method. In this paper, the randomness of meta-stable states is introduced for the TRNG at the same time.

2 Metastable state

Meta-stable random source is a commonly used as random source. Epstein et al. [6] proposed a TRNG structure by a meta-stable circuit as early as 2003, in which two inverters and two multiplexers were the basic meta-stable unit [6]. It is shown in Fig. 1. According to the control signal, the meta-stable unit changes between steady state and meta-stable state. When the control signal changes from a logic low to a logic high, the whole unit will be a stable structure. But now the output signal may be 0 or 1, which generates randomness. A random sequence has been generated by using 15 such basic meta-stable unit, 14 XOR gates and the von Neumann rectifying method for post-processing, which has passed DIEHARD statistical test [6].

In 2011, M. Majzoobi et al. [7] used the Programmable Delay Lines (PDL) to control precisely trigger propagation delay of the flip-flop, which makes the
flip-flop to produce meta-stable events. A TRNG has been designed by this the structure.

These above methods can be achieved by using an all-digital circuit, and can be easily transplanted into programmable logic devices. However, a large number of the above basic circuits are required to obtain sufficient randomness, which increases the resource of the device and the consumption of power. In this paper, a meta-stable circuit based on CMOS inverter is proposed. The structure is shown in Fig. 2.

In Fig. 2(a), after the switch is turned on, the output of the inverter will gradually converge to the meta-stable state. Due to the thermal noise of the circuit, the output fluctuates slightly in the meta-stable region. When the switch is turned off, the output of the inverter will quickly change from the meta-stable state into a steady state [7]. At that time it is uncertain that the output of the inverter become high or low for the semiconductor thermal noise.

The meta-stable unit in Fig. 2 can be introduced into traditional FIRO and GARO, which are shown in Fig. 3 and Fig. 4. A selector is used as the switch, and its control signal determines the meta-stable state or stable state of the inverter. In this paper, the improved ring is called a meta-stable Fibonacci feedback ring (Met_.FIRO) and a meta-stable Galois feedback loop (Met_.GARO).

According to the different control signal, there are two conditions: When the control signal is low, the input of each inverter is connected to its respective output, and the output of the inverter will converge to the meta-stable state. When the control signal goes high, each inverter is disconnected from the sub-
loop. The output of each inverter changes from the meta-stable state to steady state. Each inverter will be connected in the big loop. The above structure is converted into the traditional FIRO and GARO structure, which are shown in Fig. 5 and Fig. 6.

For the Met_FIRO and the Met_GARO, when the circuit is changed from the previous meta-stable state to a steady state, the output of each inverter is determined by its random noise, which introduces very high entropy. The higher the entropy greater the level of randomness possible. The output can be sampled as long as the circuit is stable. In traditional FIRO and GARO, every sample needs noise accumulation to achieve the necessary level of randomness, which is shown in Fig. 7. This figure is based on the Fig. 2 of Vasyltsov [8]. The process of the noise accumulation may be several ring oscillator cycles. So with Met_FIRO and the Met_GARO structure, the output rate of TRNG is improved. At the same time, the proposed structure can significantly reduce the output sequence dependency caused by the internal factors of FIRO and GARO ring, which makes the output bits independent of each other.

3 Design of true random number generator

Based on the Met_FIRO and the Met_GARO structure, this paper presents a high-speed TRNG. The block diagram is shown in Fig. 8. As shown in Fig. 9, the entropy source consists of 9 Met_GAROs and 9 Met_FIROs.

A FIRO’s or GARO’s output is:

\[ f(x) = (1 + x)h(x) \quad & \quad h(1) = 1 \]  

(1)
In other words, $f(x)$ can be divisible by $1 + x$, but $h(x)$ can’t be divisible by $1 + x$, and the number of series (n) must be odd. If the feedback polynomial is a primitive polynomial, the above conditions will be met if the control signal $= 1$, and the generated sequence is a $2^n - 2$ pseudo-random number. As shown in Table I, here are the different 7th order primitive polynomials as a feedback loop oscillator. The output of Met.FIRO and the Met.GARO is subjected to sequence offset cancellation after a 4-stage XOR chain circuit. Then it is used as the data and key input of the DES module respectively. The DES algorithm further eliminates the common mode components in the sequence and increases the randomness of the final output sequence.
4 Verification and result

Under the Altera’s Cyclone IV series EP4CE15F17C8 type FPGA platform, the TRNG designed in this paper has been verified, and 1,063 logical units and 396 registers are occupied after the synthesis. The output of Met_FIRO and Met_GARO is shown Fig. 10 by the oscilloscope, which is under 50 MHz system clock.

![Output of Met_FIRO and Met_GARO](image)

| Feedback Ring Oscillator | The Primitive Polynomial be used by Fibonacci Feedback Ring Oscillator | The Primitive Polynomial be used by Galois Feedback Ring Oscillator |
|--------------------------|--------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| 1                        | $x^7 + x + 1$                                                                 | $x^7 + x^3 + 1$                                                                                   |
| 2                        | $x^7 + x^3 + x^2 + x + 1$                                                        | $x^7 + x^4 + 1$                                                                                   |
| 3                        | $x^7 + x^4 + x^3 + x^2 + 1$                                                        | $x^7 + x^3 + x^2 + x + 1$                                                                        |
| 4                        | $x^7 + x^5 + x^3 + x + 1$                                                        | $x^7 + x^5 + x^3 + 1$                                                                            |
| 5                        | $x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$                                            | $x^7 + x^6 + 1$                                                                                   |
| 6                        | $x^7 + x^6 + x^5 + x^2 + x + 1$                                                   | $x^7 + x^6 + x^3 + x + 1$                                                                         |
| 7                        | $x^7 + x^6 + x^5 + x^3 + x + 1$                                                   | $x^7 + x^5 + x^2 + x + 1$                                                                         |
| 8                        | $x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$                                            | $x^7 + x^6 + x^5 + x^4 + x + 1$                                                                  |
| 9                        | $x^7 + x^6 + x^5 + x^3 + x^2 + 1$                                                | $x^7 + x^6 + x^3 + x^2 + 1$                                                                       |

Under the NIST’s SP800-22 standard released by National Institute of Standards and Technology (NIST) [9], the randomness test has been performed for 1000 sets of random numbers (a total 126M bits) generated by the proposed method. The output of traditional FIRO and GARO, not meta-stable and the proposed Met_FIRO and Met_GARO have been compared. The results of experiment are shown in Table II.

From the data in Table II, we can see that the true random number generator by Met_FIRO and Met_GARO can work steadily in a certain clock range. Compared with the traditional FIRO and GARO, the randomness of its TRNG output has improved. Under 150 Mhz, the output of Met_FIRO and Met_GARO can be passed by the NIST standard test, but the output of the traditional FIRO and GARO cannot
be passed under all the test cases. When the clock increases to 200 Mhz, the random numbers generated by the two random number generators are significantly degraded. However, the random number generated by the meta-stable state is still better than the random number generated by the traditional method. The comparison result is shown in Fig. 11. In fact, the true random number generator designed in this paper has a maximum output rate of 88 Mb/s.
5 Conclusion

Information security issues have become more and more critical in today's IT world. The quality of a random number has direct influence on the whole system's security. Based on the traditional FIRO and GARO feedback torques, the metastable state was applied in the circuit by adding a mode selector (or switch). A true random number generator was designed and implemented with this improved structure. Compared to the traditional structure of the true random number generator, the randomness of the generated random numbers, as well as the throughput, was improved. This design was fully compatible with pure digital/logical semiconductor process, which has the features such as low power consumption and high density. The whole circuit module finally passed NIST certification and can be reused as an IP core for future system-on-chip designs.

Acknowledgments

This work was supported by National Natural Science Foundation of China (Grant No. 61702149 and No. U1709220), Zhejiang provincial Science & Technology Innovation Team focused fund (Grant No. 2013TD03) and Zhejiang Key Laboratory of Solid State Drive and Data security (Grant No. 2015E10003).