electronics

MDPI

Article

A 200 kb/s 36 µw True Random Number Generator Based on Dual Oscillators for IOT Security Application

Chengying Chen, Shuhui Li and Changkun Song *

School of Opto-Electronic and Communication Engineering, Xiamen University of Technology, Xiamen 361024, China; chenchengying363@163.com (C.C.)
* Correspondence: sck15710630059@163.com

Abstract: As a module of the internet of things (IOT) information security system, the true random number generator (TRNG) plays an important role in overall performance. In this paper, a low-power TRNG based on dual oscillators is proposed. Two high-frequency cross-coupled oscillators are used to generate high-jitter clock signals, and then the SR latch with power supply below standard power supply voltage is adopted to process the oscillator output to maintain its metastability and increase jitter. The circuit is realized by an SMIC 180 nm 1P6M mixed-signal process. The experimental results show that when power supply voltage is 1.8 V, the circuit outputs a random number bit rate of 200 kb/s, the core area is 0.0039 mm^2, and the power consumption is only 36 µw. The output random sequences can pass the NIST SP 800-22 test.

Keywords: true random number generator (TRNG); oscillator; low power; jitter

Citation: Chen, C.; Li, S.; Song, C. A 200 kb/s 36 µw True Random Number Generator Based on Dual Oscillators for IOT Security Application. *Electronics* **2023**, *12*, 2332. https://doi.org/10.3390/electronics12102332

Academic Editor: Luca Bertulessi

Received: 2 May 2023
Revised: 17 May 2023
Accepted: 19 May 2023
Published: 22 May 2023

1. Introduction

With the arrival of the information age, information security has been paid more and more attention in IOT systems. Therefore, encryption methods with high quality have become a research hotspot in recent years. In most encryption algorithms, random numbers are an important factor. Random numbers are divided into two categories: the true random number generator (TRNG) and the pseudo random number generator (PRNG). Pseudo random numbers are generated by certain algorithms and have inevitable periodicity, while true random numbers can be generated by extracting randomness from complementary metal oxide semiconductor (CMOS) circuits or new devices (resistive variable memory). Compared with PRNG, TRNG can generate an infinite and theoretically unpredictable random number sequence, which has higher security and better randomness, so it is more secure and reliable. On the other hand, true random numbers are also widely used in Monte Carlo simulation, stochastic process modeling and other simulation methods [1–4]. In this context, the TRNG has been widely analyzed and studied.

In smart cards, vending machines and other terminal applications, the output bit rate of TRNG chips is usually hundreds of kb/s, which can meet the application requirements. However, they have extremely strict requirements for power consumption and area. Kim et al. proposed a low-power TRNG for RFID tags [5]. When the power supply voltage is 0.8 V, the power consumption is only 1 µW. However, the pass rate in the poker test was slightly low, reaching only 86%. A TRNG architecture based on the tetrahedral oscillator is presented in [6]. Two ring oscillators with different frequencies are used to generate high-frequency clock signals, which increases clock jitter. At an output rate of 100 kb/s, the power consumption is 40 µW. The small area of 0.005 mm^2 was achieved. The power consumption performance and area are compromised. Wieczorek et al. deeply analyzed the theory of high-frequency clock signal jitter and period, and implemented it with a slow-clock circuit of charge pump and Schmitt trigger [7]. At an output bit rate of 400 kb/s, the power consumption is 600 µW and the area is 0.0396 mm^2. Its overall performance is average. In recent years, with the rapid development of new nanoscale devices, RRAM-based true

random number generators have also become a research hotspot. Compared with the noise used in CMOS circuits, RRAM has a more natural randomness and more abundant random characteristics that can be directly utilized. A TRNG based on a high-speed reconfigurable current-starving ring oscillator uses the random noise of resistive random-access memory (RRAM) [8]. The output sequences bit rate reaches 6 MHz, which has certain power consumption advantages, and has obtained an NIST randomness certification. However, the instability of RRAM technology restricts its application in large-scale industry. Jeremy et al. designed a 1T1R RRAM array based on the HfO_2 structure [9]. This scheme breaks the limitations of using a single RRAM unit and successfully introduces the array structure into the TRNG implementation. Since the transition of RRAM from high-resistance to low-resistance status is a normal distribution with a probability of 50%, it has extremely high randomness. Jeeson et al. utilized a differential readout circuit to amplify the transient effects of metastable RRAM, which can effectively suppress the impact of temperature on the output [4]. This scheme will increase the chip area, but it can obtain high-quality random signals. The test results have been verified by NIST and machine learning. Hassen et al. proposed an ICL (input current limit) method to implement TRNG [10]. Its basic idea is to use the 1T1R RRAM structure to control the threshold resistance value from logic 0 to 1 and input a fixed current to the array. Due to the limited current being unable to fully set the entire RRAM array, the resistance of RRAM in array exhibits a random distribution with each programmed current input. This method requires XOR circuits to increase the stability issues caused by circuit parameter degradation, and the implemented circuit has passed 12 NIST tests.

To optimize the power consumption and area performance, a low-power TRNG based on dual oscillators is proposed in this paper. Two cross-coupled oscillators of the same period generate high-frequency clock signals with high jitter. Different from the traditional way of using XOR to increase jitter, our design adopts a two-stage SR latch of low-power supply voltage to form a metastable loop with the high-frequency oscillator, which further increases the jitter of the high-frequency clock signal. The circuit is realized by SMIC 180 nm 1P6M mixed-signal process. The test results show that when the power supply voltage is 1.8 V, the circuit outputs a random number bit rate of 200 kb/s, the core chip area is 0.0039 mm^2, the power consumption is only 36 μw, and the overall performance is excellent.

2. Circuit Design

The principle of a traditional ring oscillator-based TRNG is shown in Figure 1 [5,11,12]. High frequency clock is the input of D flip-flop. The clock of the D flip-flop is a low-frequency clock signal with jitter, and the jitter of the slow clock follows a normal distribution approximately. When the frequency ratio of the high-frequency clock to low-frequency clock exceeds a certain ratio (usually greater than 20), and the cycle jitter of the low-frequency clock covers the high-frequency clock signal in a certain period of time. Thus, the sampling of input signal by the clock terminal of D flip-flop is random. That is, the output will be completely determined by the jitter of the slow clock. After that, the final true random number output can be obtained by further randomizing the output sequence through a post-processing circuit.

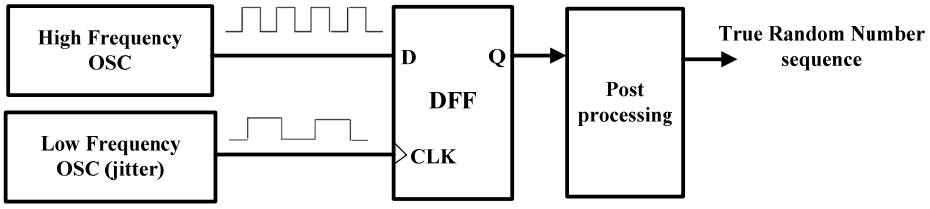

Figure 1. Ring oscillator-based TRNG.

This structure requires that the frequency of high-frequency clock signal is much higher than that of the low-frequency clock signal, so that the low-frequency clock signal jitter can cover the high-frequency clock signal for a long time as much as possible to obtain better randomness. The following problem is the significant increase in power consumption, which needs to be improved for its further application in low-power portable devices [13–15]. Therefore, in applications such as smart cards, high-frequency signals are usually subject to high jitter, and a standard low-frequency clock is used for sampling to effectively reduce the frequency of high-frequency clock signals and achieve low-power design. The dual-oscillators-based low-power TRNG using high-frequency jitter is shown in Figure 2, which includes current mirror, high-frequency oscillator (OSC1. OSC2), two-stage SR latch, level shift, duty-cycle adjustment circuit and D flip-flop.

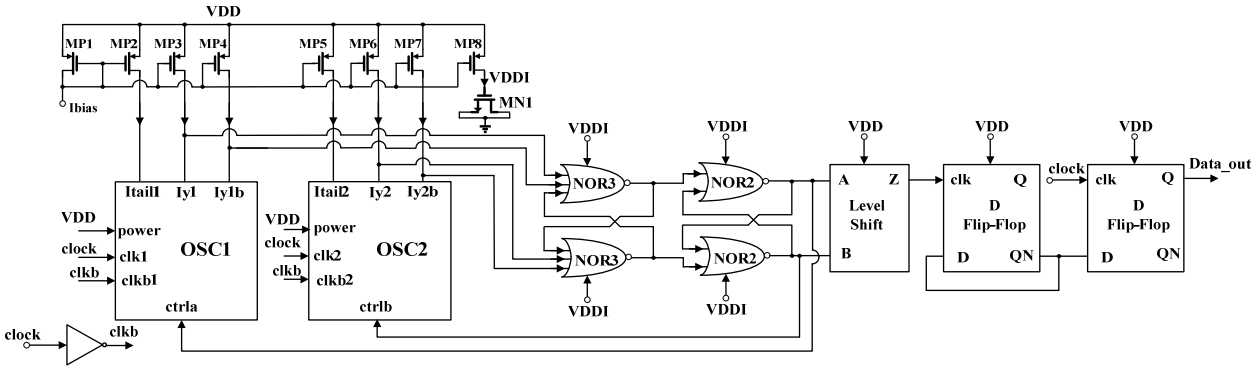

Figure 2. Block diagram of proposed TRNG.

The current mirror consists of PMOS transistors MP1-MP8. MP2 (MP5) is the tail-current transistor of two high-frequency oscillators (OSC1, OSC2). MP3/MP4 (MP6/MP7) provide initial bias voltage for the two high-frequency oscillator outputs. As the tail-current transistor of two-stage SR latch, MP8 is used to generate a certain voltage drop, and a supply voltage VDDI lower than the standard supply voltage VDD makes the two-stage SR latch operate in a low-voltage environment. This scheme ensures that the output of the high-frequency oscillator meets the metastable working state of the two-stage SR latch and increases jitter. NMOS transistor NM1 is used as an MOS capacitor to stabilize the output voltage VDDI. Since the power supply voltage of the two-stage SR latch is lower than the standard power supply voltage, the output of the high-frequency oscillator is designed to be near VDDI/2, which makes the SR latch and high-frequency oscillator loop work in a metastable state and improves the high-frequency jitter. At the same time, the output of the second stage SR latch is also used as the feedback control signals (ctrla, ctrlb) of the two high-frequency oscillators. When the high-frequency oscillator completes a cycle of switching from low to high, the output is pulled down for the next charging process to form a periodic oscillation signal. The level shift works under the standard power supply voltage VDD, and restores the SR latch output to VDD to represent logic 1. The duty-cycle adjustment circuit is a D flip-flop connected as a divider, which aims to recover the sharp rising edge of the clock and is conducive to sampling the jitter of the high-frequency clock. The input low-frequency clock signal of the last D flip-flop is the main clock of the circuit. This design uses the same clock source to generate high-frequency jitter. The clock is also used as the low-frequency sampling clock, which simplifies the circuit terminal design. The circuits of two high-frequency oscillators (OSC1 and OSC2) are shown in Figure 3 (the terminals in the figure are marked with OSC1).

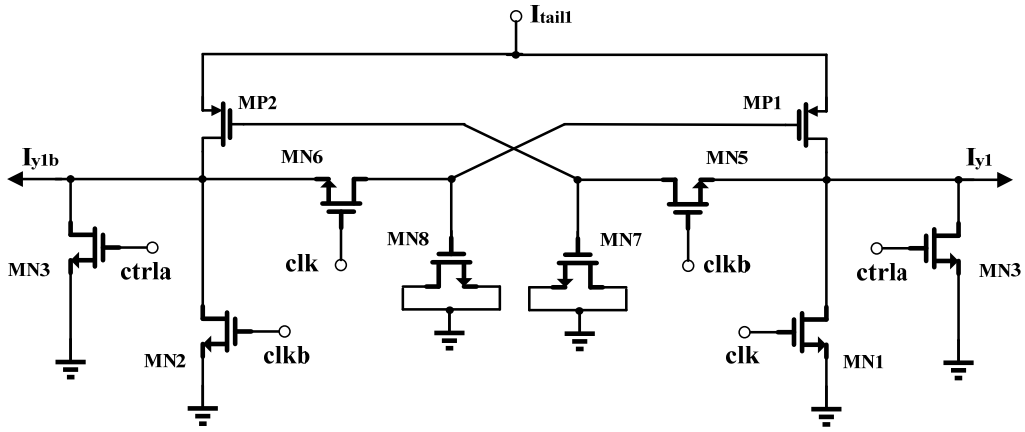

Figure 3. High-frequency oscillators.

The working principle of the high-frequency oscillator is thus: First, when the power is on, the two outputs Iy1 and Iy1b are biased at an initial voltage by the current mirror. when the main clock signal (low-frequency clock) is high (clkb is the output of the clock after passing through the inverter, and clkb is low), that is, the clk is high, so the NMOS transistor MN1 is turned on, and the output Iy1 is pulled down. The gate voltage of the PMOS transistor MP2 is low at the initial time, making the MP2 turn on. Meanwhile the gate voltage of MN6 is high, and is also in turn-on state. The tail current Itail1 charges MOS capacitor MN8, and the output Iy1b starts to rise. The inputs of the first SR latch are logic 1 and 0. The second SR latch outputs a high voltage signal (ctrla) and pulls the output Iy1b to low. After both Iy1 and Iy1b output a low voltage, the second SR latch outputs a low voltage signal (ctrla). Therefore, it turns off transistor MN3, and Iy1b restarts a new round of charging and voltage rise process. When the main clock signal is low, the operating state of Iy1 and Iy1b is the same as the above process, except that Iy1b is always maintained at low level, while Iy1 repeats the process of voltage rise and then being pulled down by ctrla. Due to deviation in charging time, high-frequency clock jitter occurs. Because the two SR latch works at a lower power supply voltage, the loop between the high-frequency oscillator and the SR latch can easily work in a metastable state, further increasing the jitter of the high-frequency clock.

The level shift is shown in Figure 4. A.B is the input signal of the second SR latch. When A is high and B is low, MN1 is turned on, and node N1 is pulled down to low, so MP3 is turned on. MP4/MN3 forms an inverter, and Z outputs high. Since the SR latch's power supply is lower than the standard power supply, and the high-level value of A at the initial time is lower than the power supply voltage, that means NM1 may be in linear region, which makes the voltage of node N1 not completely equal to ground potential. MP3 is also in linear region, so Z is high, but its high voltage is slightly lower than the power supply voltage VDD, but after Z forms a high output, NM2 turns on. It further pulls N1 down to ground potential, and finally makes Z equal to the power supply voltage VDD. While A is low and B is high, the working principle is similar. The output Z further ensures that node N1 is high by controlling MP1. So that MP1 is completely cut off, and the output Z is equal to ground potential.

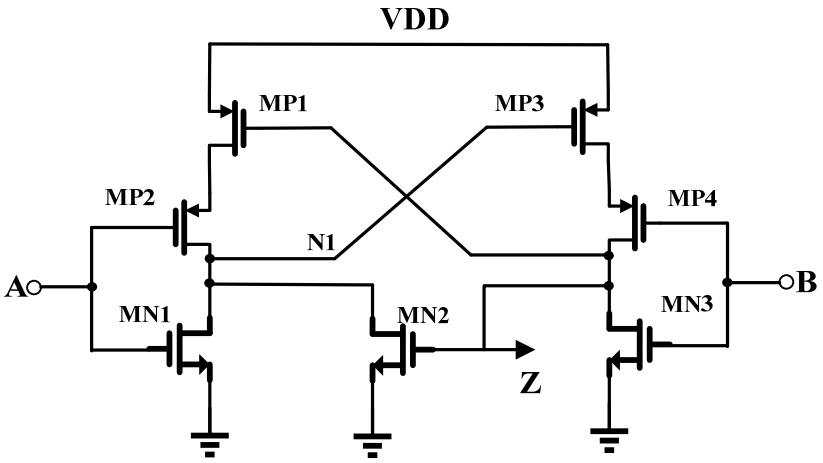

Figure 4. Level shift.

3. Measurement Results

The proposed design is implemented by SMIC 180 nm 1P6M mixed-signal process. A bandgap is integrated on the chip. The chip microphoto and test board is shown in Figure 5 with an overall area of 0.37 mm^2. The core area of TRNG is 0.0039 mm^2.

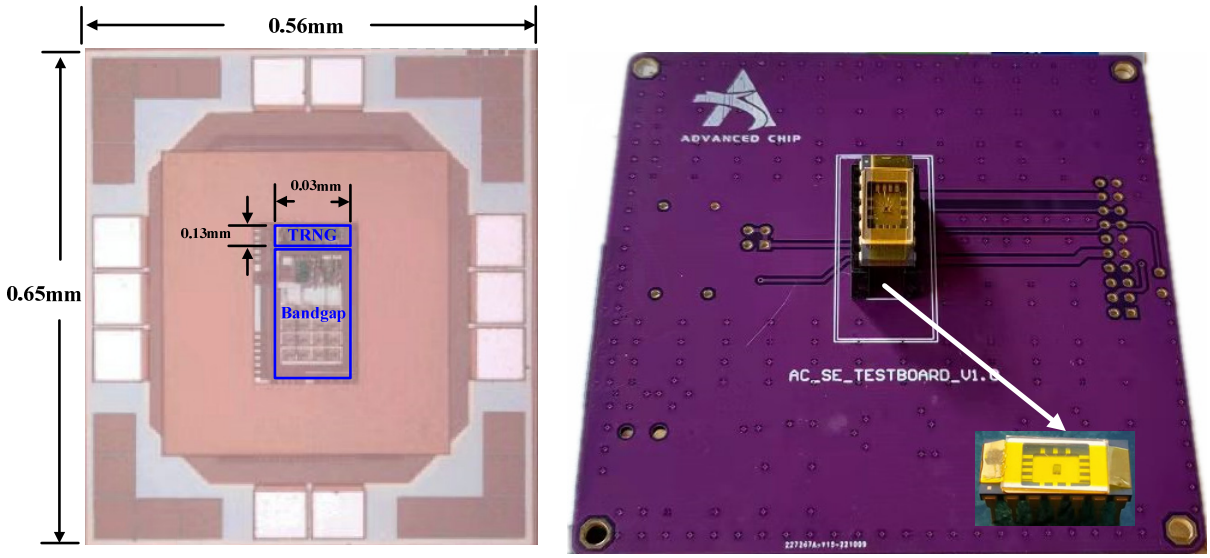

Figure 5. Chip microphoto and test board.

The test is carried out after tapeout. Firstly, collect the output sequence data with an oscilloscope and observe the transient output waveform. Afterwards, the collected data will be saved and converted into ASCII format using Python. Finally, the data will be input into the NIST SP800-22 suite for randomness verification. Simultaneously, SPSSPRO tool is adopted to perform autocorrelation function (ACF) testing on the exported data. The transient output waveform is shown in Figure 6, which shows no significant bias in the output sequence, and the 1/0 output is relatively uniform, indicating that the output sequence has good randomness. Powered with a single 1.8 V supply, the TRNG has a power consumption of 36 µW. The minimum time interval is 5 µs. The bit rate of the TRNG is 203 kb/s.

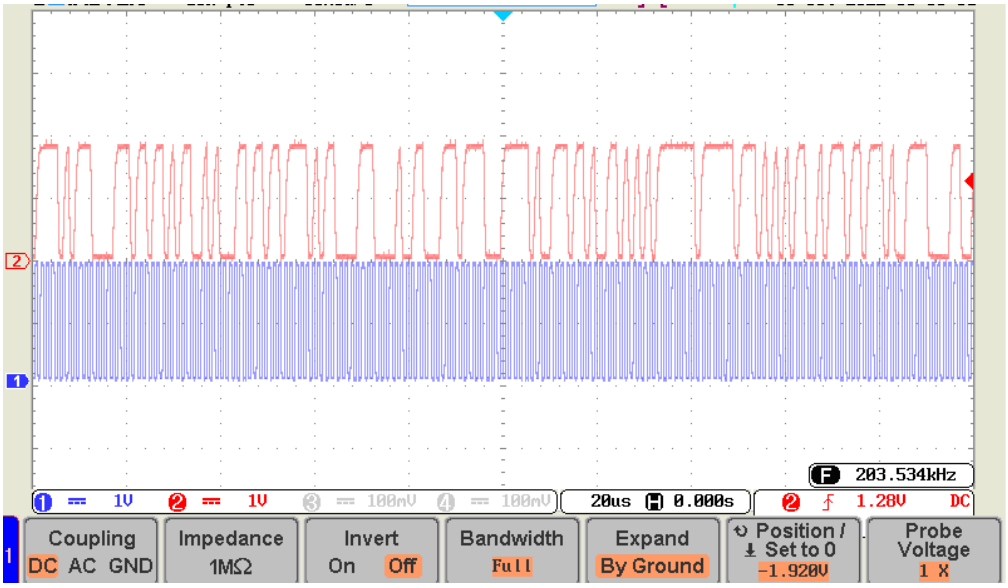

Figure 6. Output sequences.

Then 1000 groups of 1M-bit streams were acquired and processed. Figure 7 shows the output sequences in pixel mode, where white represents 1 and black represents 0. It can be seen from the figure that 1/0 is evenly distributed as a whole. It is proved that the output sequence has good randomness.

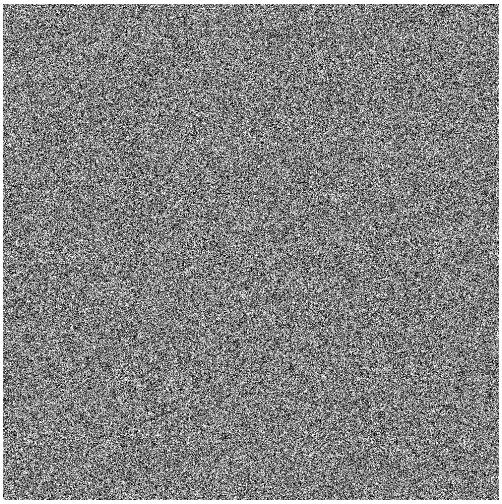

Figure 7. Output sequences in pixel mode.

The autocorrelation characteristic of output sequences is tested, and the results obtained by SPSSPRO analysis are shown in Figure 8. ACF is a way to determine independence in data streams, and ACF testing has demonstrated its ability to resist autocorrelation attacks. The lower the ACF value, the more independent the data in the sequence are. It is observed from Figure 8 that within the 95% confidence interval of the Gaussian distribution, the ACF value only fluctuates between -0.003 and 0.003. The results show that the sequence is independent and can be regarded as white noise.

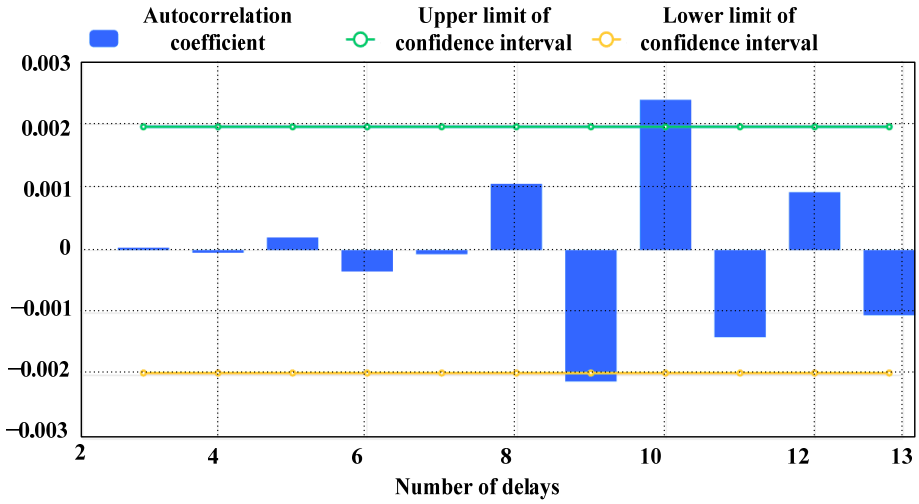

Figure 8. Autocorrelation characteristics of output sequences.

NIST SP800-22 (National Institute of Standards and Technology) is a statistical tool released by the National Institute of Standards and Technology (NIST) for testing randomness and pseudorandomness, aimed at evaluating the quality and safety of random number generators. NIST SP800-22 covers 15 tests, including frequency, block frequency, cumulative sums, runs, longest run, rank, FFT, non-overlapping template, overlapping template, universal, approximate entropy, random excursions, random excursions variant, serial and linear complexity test. The NIST test steps are as follows: (1) By collecting the data output from the oscilloscope, convert the data into ASCII code in Python and save it in txt format. (2) Run the NIST test suite on your computer. Divide the output sequences into 128 groups and input them into the NIST SP800-22 test suite. If the *p*_value is greater than 0.01, it passes the random test. The *p*_value of each test result is shown in Table 1. The output sequences have good randomness.

Table 1. NIST test result.

NIST Test	*p*_Value	Result
Frequency	0.9850	pass
Block Frequency	0.9496	pass
Cumulative Sums	0.9114	pass
Runs	0.5341	pass
Longest Run	0.3504	pass
Rank	0.2133	pass
FFT	0.3504	pass
Non-Overlapping Template	0.7399	pass
Overlapping Template	0.3504	pass
Universal	0.5341	pass
Approximate Entropy	0.7399	pass
Random Excursions	0.1223	pass
Random Excursions Variant	0.3504	pass
Serial	0.7391	pass
Linear Complexity	0.7399	pass

The output jitter acquired from level shift output is shown in Figure 9. It is sampled 21,867 times in 1 mS. The bit rate of output jitter is 8.023 kb/s in average and the standard deviation is about 6.4 MHz. The normal quantile plot of the sampled quantiles versus theoretical quantiles from a normal distribution is in shown in Figure 10, which demonstrates that the distribution is normal. The wide range deviation proves that enough entropy source is acquired from the metastable state of both dual oscillators and SR latches.

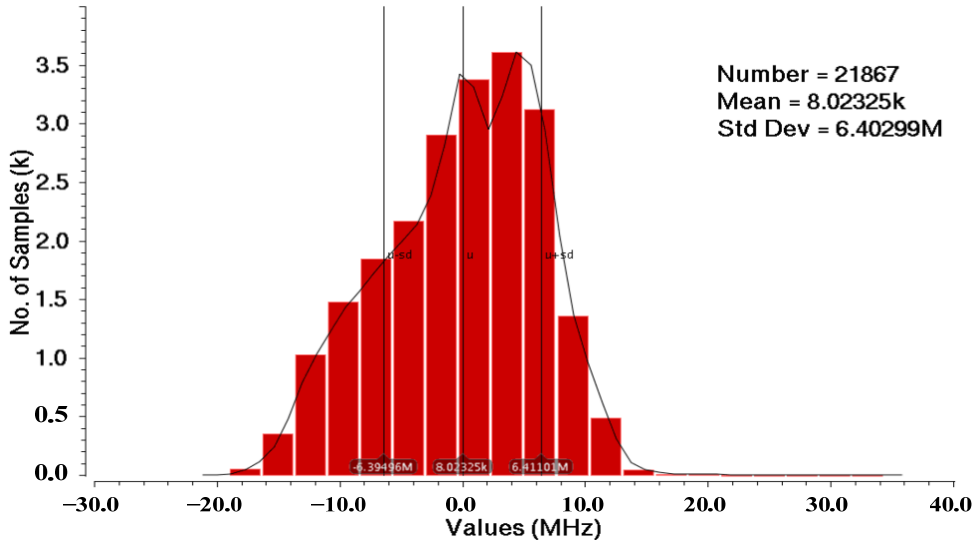

Figure 9. Output clock jitter histogram.

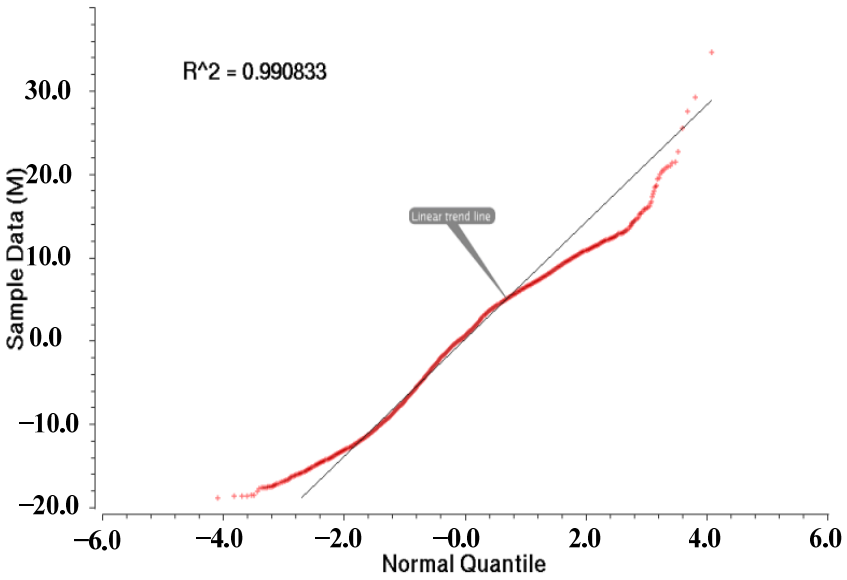

Figure 10. Normal quantile plot of output jitter.

Figure 11 shows the relationship between the throughput and temperature of different clock frequencies. The throughput of the proposed TRNG increases with clock frequency. It can be seen that output frequency is easily controlled by the clock and has great stability of temperature. Figure 12 shows the relationship between throughput and temperature of different clock frequencies. The throughput of the proposed TRNG increases with clock frequency. It can be seen that the output frequency is easily controlled by the clock and has great stability of temperature. The relationship between the output bit rate and power supply is demonstrated in Figure 12, which shows that the output bit rate increases with supply voltage. Within a 10% variation range of power supply voltage, the maximum output bit rate can reach 230 kHz.

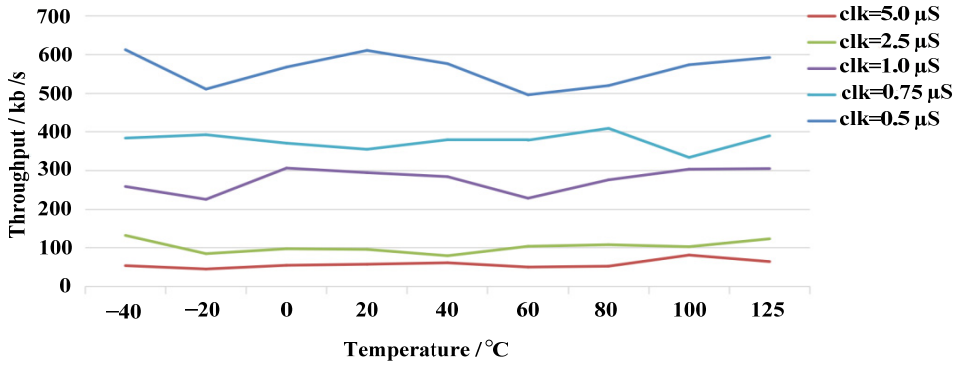

Figure 11. Throughput vs. temperature.

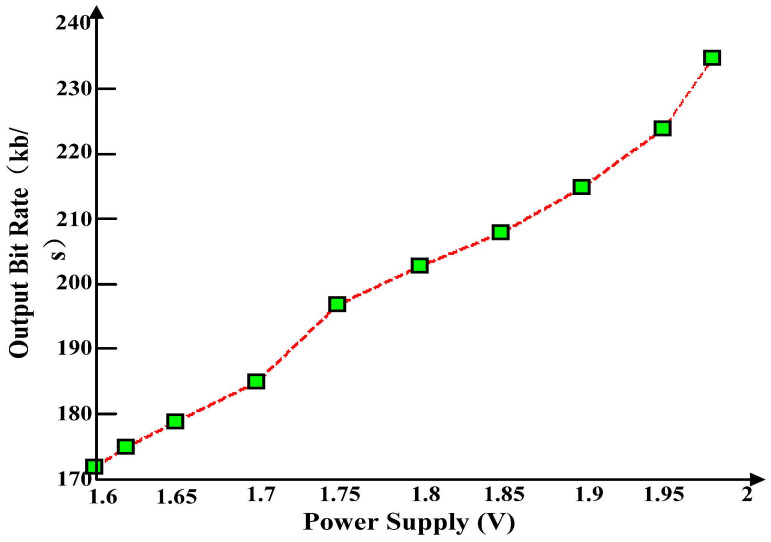

Figure 12. Output bit rate vs. power supply.

Table 2 shows the comparison between our design and those of others. The design in this paper realizes the optimization design of output bit rate, area and power consumption. Compared with advanced technology, the output bit rate and power consumption still have certain advantages. Under similar process conditions, our design adopts a novel dual oscillators structure to effectively improve the randomness of the output data, and only one clock input is used, which greatly simplifies overall design. Minimum power consumption and area achieved at the same output rate.

Table 2. Performance comparison.

Parameter	[6]	[15]	[16]	[17]	[18]	This Work
Technology (nm)	130	65	350	180	180	180
Power supply (V)	1.8	1.2	3.3	0.6	1.8	1.8
Bit rate (kb/s)	100	2800	400	270	180	200
Power consumption (μW)	40	159	600	0.082	109	36
Area (μm^2)	5000	960	39600	4500	72500	3900
Randomness	High	High	High	High	High	High

4. Conclusions

A low-power TRNG structure based on dual oscillators is proposed for IOT applications for smart cards, vending machines and other terminals. Two co-frequency cross-coupled oscillators use the charging and discharging process of MOS capacitors to periodically generate two high-frequency clock signals with high jitter. The SR latch is placed in a working state lower than the standard power supply voltage, and forms a metastable loop with two high-frequency oscillators to control the charge/discharge cycle. It further increases the high-frequency jitter. The TRNG chip is tapeout by SMIC 180 nm 1P6M mixed-signal process. The test results show that when the power supply voltage is 1.8 V, the circuit the output bit rate is 200 kb/s, the core chip area is 0.0039 mm^2 and the power consumption is only 36 μw. The output sequences are input into the NIST test suite and the *p*_value shows that the output sequences have passed the test requirements and have good randomness.

Author Contributions: Conceptualization, C.C. and S.L.; software simulation and parameter optimization, C.C. and C.S.; data processing, C.S.; writing—original draft preparation, S.L. and C.S.; writing—review and editing, C.C. and C.S.; supervision, C.C. and C.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Xiamen Youth Innovation Fund Project (3502Z20206074) and major science and technology projects of Xiamen (3502Z20221022).

Data Availability Statement: All the data are reported/cited in the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Huang, C.-Y.; Shen, W.C.; Tseng, Y.-H.; King, Y.-C.; Lin, C.-J. A Contact-Resistive Random-Access-Memory-Based True Random Number Generator. *IEEE Electron Device Lett.* **2012**, *33*, 1108–1110. [CrossRef]
2. Balatti, S.; Ambrogio, S.; Wang, Z.; Ielmini, D. True Random Number Generation by Variability of Resistive Switching in Oxide-Based Devices. *IEEE J. Emerg. Sel. Top. Circuits Syst.* **2015**, *5*, 214–221. [CrossRef]
3. Yang, J.; Lin, Y.; Fu, Y.; Xue, X.; Chen, B.-A. A small area and low power true random number generator using write speed variation of oxidebased RRAM for IoT security application. In Proceedings of the 2017 IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, MD, USA, 28–31 May 2017; pp. 1–4.
4. Kim, J.; Nili, H.; Truong, N.D.; Ahmed, T.; Yang, J.; Jeong, D.; Sriram, S.; Ranasinghe, D.; Ippolito, S.; Chun, H. Nano-Intrinsic True Random Number Generation: A Device to Data Study. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2019**, *66*, 2615–2626. [CrossRef]
5. Chen, W.; Che, W.; Bi, Z.; Wang, J.; Yan, N.; Tan, X.; Wang, J.; Min, H.; Tan, J. A 1.04 μW truly random number generator for Gen2 RFID tag. In Proceedings of the 2009 IEEE Asian Solid-State Circuits Conference, Taipei, Taiwan, 16–18 November 2009.
6. Liu, D.-S.; Liu, Z.; Li, L.; Zou, X.-C. A Low-Cost Low-Power Ring Oscillator-based Truly Random Number Generator for Encryption on Smart Cards. *IEEE Trans. Circuits Syst. II Express Briefs* **2016**, *63*, 608–612. [CrossRef]
7. Wieczorek, P.-Z. Lightweight TRNG based on multiphase timing of bistables. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2016**, *63*, 1043–1054. [CrossRef]
8. Govindaraj, R.; Ghosh, S.; Katkoori, S. CSRO-Based Reconfigurable True Random Number Generator Using RRAM. *IEEE Trans. Very Large Scale Integr. VLSI Syst.* **2018**, *26*, 2661–2670. [CrossRef]
9. Postel, P.-J.; Bazzi, H.; Aziza, H.; Canet, P.; Harb, Z. True random number generation exploiting SET voltage variability in resistive RAM memory arrays. In Proceedings of the 2019 19th Non-Volatile Memory Technology Symposium (NVMTS), Durham, NC, USA, 28–30 October 2019; pp. 1–5.
10. Aziza, H.; Postel-Pellerin, J.; Bazzi, H.; Canet, P.; Moreau, M.; Della Marca, V.; Harb, A. True Random Number Generator Integration in a Resistive RAM Memory Array Using Input Current Limitation. *IEEE Trans. Nanotechnol.* **2020**, *19*, 214–222. [CrossRef]
11. Nakura, T.; Ikeda, M.; Asada, K. Ring Oscillator Based Random Number Generator Utilizing Wake-up Time Uncertainty. In Proceedings of the Solid-State Circuits Conference, San Francisco, CA, USA, 8–12 February 2009; pp. 1–4.
12. Amaki, T.; Hashimoto, M.; Onoye, T. An oscillator based true random number generator with jitter amplifier. In Proceedings of the International Symposium on Circuits and Systems (ISCAS), Rio de Janeiro, Brazil, 15–18 May 2011; pp. 1–4.
13. Dai, L.; Harjani, R. Design of low phase noise CMOS ring oscillators. *IEEE Trans. Circuits Syst. II Analog Digit. Signal Process.* **2002**, *49*, 328–338.
14. Stewart, R.; Leung, B.; Gong, G. Truly Random Number Generator Based on Ring oscillator Utilizing Last Passage Time. *IEEE Trans. Circuits Syst. II Express Briefs* **2014**, *61*, 937–941.

15. Yang, K.; Fick, D.; Henry, M.-B.; Lee, Y.; Sylvester, D. A 23 Mb/s 23 pJ/b fully synthesized true-random-number generator in 28 nm and 65 nm CMOS. *IEEE Int. Solid-State Circuits Conf.* **2014**, *16*, 280–283.
16. Bejar, E.; Saldana, J.; Raygada, E.; Silva, C. On the Jitter-to-Fast-Clock-Period Ratio in Oscillator-Based True Random Number Generators. In Proceedings of the 24th IEEE International Conference on Electronics, Circuits and Systems (ICECS), Batumi, Georgia, 5–8 December 2017; pp. 1–4.
17. Kim, M.; Ha, U.; Lee, Y.; Lee, K.; Yoo, H.-J. A 82-nW chaotic map true random number generator based on a subranging SAR ADC. *IEEE J. Solid State Circuits* **2017**, *52*, 1953–1965. [CrossRef]
18. Yang, K.; Blaauw, D.; Sylvester, D. An all-digital edge racing true random number generator robust against PVT variations. *IEEE J. Solid State Circuits* **2016**, *51*, 1022–1031.