10-Gbps True Random Number Generator Accomplished in ASIC

Xinzhe Wang, Futian Liang, Peng Miao, Yi Qian, Ge Jin

***Abstract*–Random number generators are wildly used in many applications in a diverse set of areas ranging from statistics to cryptography. Pseudo random number generators (PRNGs) are quite satisfactory for most applications. However, for cryptography and security applications, true random number generators (TRNGs) are required for the unpredictability. High density and high data output rate are as important as the quality of the TRNG in the nowadays true random number required devices and instruments.**

We present the design and the primary test results of our 10-Gbps TRNG, which is named TRNG2015, in the paper. The entropy source of the TRNG2015 is the jitter of ring oscillators. The TRNG2015 is fabricated in a 130nm CMOS process and assembled in a 6mm x 6 mm QFN48 package. It has one LVDS clock input and ten LVDS random data outputs. The output data rate depends on the input clock which is up to 1 GHz, and the output data rate is up to 1 Gbps per channel and up to 10 Gbps in total.

I. Introduction

Random number has been wildly applied in a diverse set of areas, such as statistics, simulation, computer science and cryptography. Pseudo random number generators (PRNGs) are quite satisfactory for most applications. PRNGs provide number sequence generated by calculation. The number sequence is random in a certain period, which means the sequence is not truly random. For some special applications, such as cryptography, random in period is not enough. The rapid development of computing power has resulted in the demand of true random number generators (TRNGs) to guarantee the security of cryptography. TRNGs provide random number acquired from physical process. True random number is unpredictable, and is random in the whole time domain. Theoretically, true random number is unprovable because the examination range for the periodicity is always limited. We can only use some standards to prove a number sequence to be pseudo. And we call number sequences which can pass the standard tests TRUE random numbers.

The quality is usually the most valued for true random number generators. As the development of communication technology and the appearance of new methods, high density and high data output rate are as important as the quality of the TRNGs in the nowadays true random number required devices and instruments. Mature commercial TRNGs provide data rate from hundreds of Kbps to dozens of Mbps, while most high speed TRNGs in laboratory are composed of huge and complex systems and are not convenient for practical applications. To meet the requirement of high density and high data rate, we designed the TRNG2015, a high speed TRNG chip accomplished in ASIC.

II. Entropy source

A true random number generator is usually composed of entropy source, sampling module and post processing module. Random number is generated from entropy source, which is made up of physical random phenomenon in reality. The sampling module determines the value and data rate of the generator's output. And the posting module uses math method to improve the 0/1 ratio of number sequence got from entropy source.

Determining the scheme of a TRNG, entropy source is the core of a TRNG. And there are different types of entropy source based on different physical phenomenons. In most published TRNGs which are based on electronics, thermal noise amplification, voltage controlled oscillator, discrete-time chaos and clock jitter in digital circuit are the common entropy source. We choose clock jitter as our entropy source for its simple structure and easy implementation.

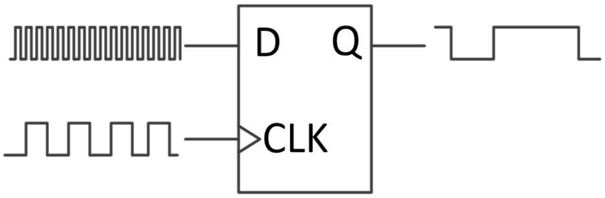


Fig.1 Scheme of TRNG Based on Clock Jitters in Digital Circuit

Traditional scheme of TRNG sampling from clock jitters, shown in Fig. 1, uses a slow clock to sample a fast clock produced by a free-running oscillator. The randomness are produced from clock jitters of the oscillator and the output is determined by the rising edge of the slow clock using a D flip-flop. Under the ideal condition, shown in Fig. 2(a), there is no clock jitter and each bit sampled by the slow clock is a certain one or zero. The output is certain and determined by

Manuscript received May 3, 2016. This work is supported by the National Natural Science Foundation of China under grant number 61401422, 11375179.

Xinzhe Wang, Futian Liang, Peng Miao, and Ge Jin are with State Key Laboratory of Particle Detection and Electronics, University of Science and Technology of China, Hefei, Anhui, 230026, P.R. of China (e-mail: wxzyf@mail.ustd.edu.cn, ftliang@ustd.edu.cn, mpmp@mail.ustc.edu.cn, goldjin@ustc.edu.cn).

Yi Qian is with State Key Laboratory of Particle Detection and Electronics, University of Science and Technology of China, Hefei, Anhui 230026, and with Hefei Electronic Engineering Institute, Hefei, Anhui 230037, P.R. of China (e-mail: yiqian@mail.ustd.edu.cn).

978-1-5090-2014-0/16/$31.00 ©2016 IEEE

the frequency of the oscillator and sampling clock and phase difference between the two clocks. In practice, as shown in Fig. 2(b), there are some clock jitters in the edge of oscillator clock, and the bits sampled at the uncertainty jitter domain are random. However, published RNG designs using ring oscillators report that typical levels of oscillator jitter is not sufficient to produce statistical randomness. Consequently, pseudo-random techniques are added to further randomize the output, potentially compromising the unpredictability of the system [1]. To get a consecutive random consequence without pseudo-random techniques, which may cause unpredictable influence to our TRNG, we improve the traditional scheme by increasing the number of oscillators. We join multiple free-running oscillators together and each oscillator is independent. As shown in Fig. 2(c), the XOR results of enough independent free-running oscillators will provide enough clock jitters to cover the whole time domain uniformly and ensure a consecutive random consequence which is exactly what we want.

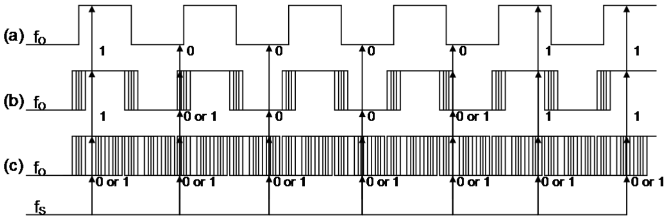


Fig. 2 Clock Jitters Sampled by Slow Clock

III. Design scheme

Based on the clock jitter of digital circuit method, we designed TRNG2015, a true random number generator ASIC chip, which aims to provide 10-channel paralleled true random number outputs and each channel can achieve a data rate as high as 1Gbps. We use the 130nm CMOS process as our TRNG's process to achieve the high performance and high integrated density. The TRNG2015 is set by a 4-line SPI bus.

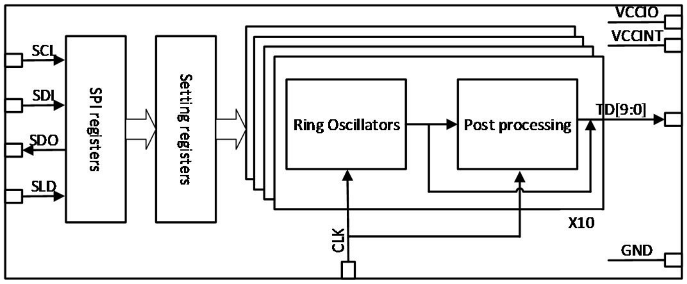


Fig. 3 Structure of the TRNG2015

A. Ring Oscillators

Concerning about the demand of data rate and volume, we use three-inverter ring oscillator, which can provide an output at about 4.7GHz when simulated by cadence virtuoso ADE tools. We replace one inverter with a NAND gate to make it possible to control the working condition of the ring oscillator. This improvement can reduce the power dissipation in idle time.

Each channel consists of 256 ring oscillators and all the outputs are merged together by xor gate. If we use a 256-input xor gate, we'll have a difficulty to place all the ring oscillators properly in layout. And more importantly, the 256 inputs are asynchronous, and the overturn speed of xor gate isn't fast enough to response to every overturn of inputs. So we use a multistage 2-input xor gate net instead of a 256-input xor gate, and put a D flip-flop after every ring oscillator output and xor gate output to synchronize the inputs by sampling clock. The randomness is determined right at the D flip-flop after the ring oscillator output, and won't be influenced by the rest part of the circuit.

B. Sampling Clock

Output data rate of a TRNG is determined by the sampling clock. Sampling clock of the TRNG2015 is provided from an off-chip clock source. And all ten channels use the same clock to make the simultaneous use of paralleled channels convenient. Users can adjust the data rate of TRNG2015 by changing the frequency of sampling clock properly. The highest sampling clock frequency allowed can be as high as 1GHz.

C. Post Processing

As previously mentioned, the post processing module uses pseudo-random techniques to add further randomize to original output, potentially compromising the unpredictability of the system. Theoretically, the post processing module won't add entropy of the system, so it won't change the randomize of the output, either. In practice, there are still many argument about post processing. So we use enough ring oscillators to make sure our original output data is random. And we add FIR11, a classic post processing, after the output of the original data just in case. Users can use a bypass setting to select to output the original data or the data processed by the post processing module.

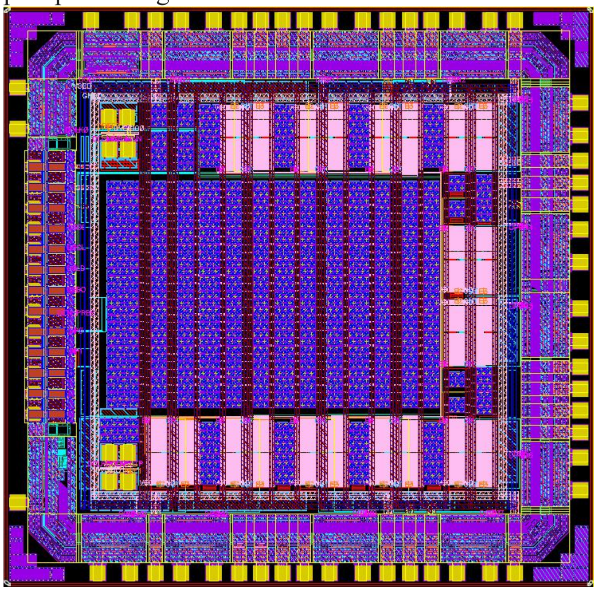


Fig. 4 Layout of the TRNG2015

The TRNG2015 is fabricated in a 130 nm CMOS process. Each die occupies an area of 2.5mm x 2.5mm and is assembled in a 6mm x 6 mm QFN48 package. The layout and wire bonding of the chip are shown in Fig. 4 and Fig. 5.

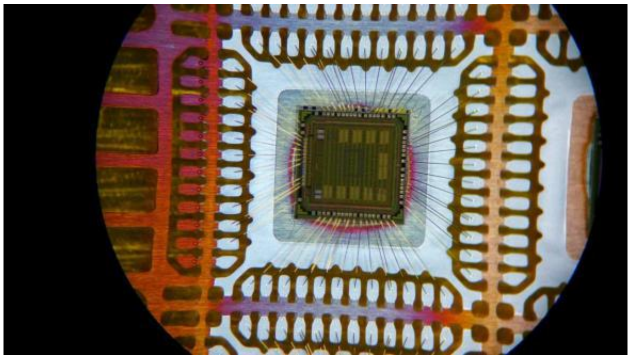


Fig. 5 Picture of the TRNG2015 Chip

IV. TRNG TESTING

The TRNG2015 is still under testing. In this paper, we provide the electrical performance and NIST test results at 1Gbps data rate of the TRNG2015.

The TRNG2015 can output normally with a 1GHz sampling clock. The power dissipation when all the ten channels are fully functional is about 700mW in total. In Fig. 6, the waveform of input clock, a pair of single-ended outputs of channel 1, and the differential output of channel 1 are shown in order. There is an overshoot with about 1-ns width and 150-mV amplitude at the rising edge in single-ended waveform, and a undershoot which is symmetrical with the overshoot at the falling edge. The differential waveform won’t have this appearance so the overshoots and the undershoots won’t lead to sampling mistakes.

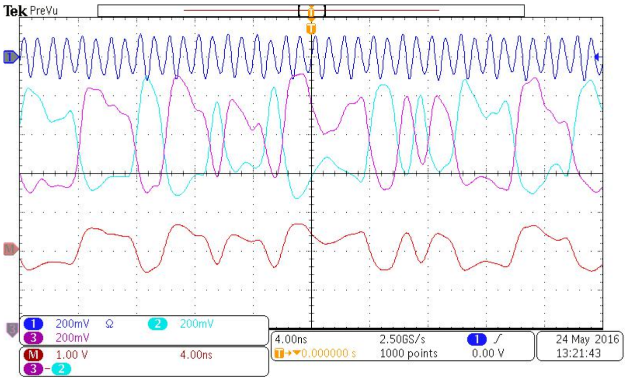
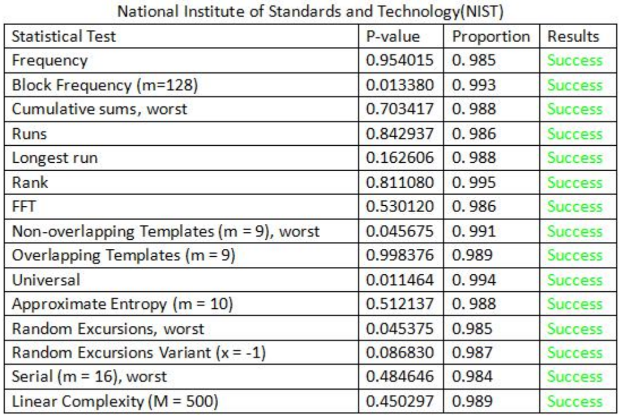


Fig. 6 Waveform of Channel 1 of TRNG2015

We use National Institute of Standards and Technology Special Publication 800-22 statistical tests to test the quality of the random sequences generated by TRNG2015. At 1Gbps data rate each channel, the original output of TRNG2015 without post processing can pass the NIST test. The testing results are shown in Fig. 7.



National Institute of Standards and Technology(NIST)

Statistical Test	P-value	Proportion	Results
Frequency	0.954015	0. 985	Success
Block Frequency (m=128)	0.013380	0. 993	Success
Cumulative sums, worst	0.703417	0. 988	Success
Runs	0.842937	0. 986	Success
Longest run	0.162606	0. 988	Success
Rank	0.811080	0. 995	Success
FFT	0.530120	0. 986	Success
Non-overlapping Templates (m = 9), worst	0.045675	0. 991	Success
Overlapping Templates (m = 9)	0.998376	0.989	Success
Universal	0.011464	0. 994	Success
Approximate Entropy (m = 10)	0.512137	0. 988	Success
Random Excursions, worst	0.045375	0.985	Success
Random Excursions Variant (x = -1)	0.086830	0.987	Success
Serial (m = 16), worst	0.484646	0.984	Success
Linear Complexity (M = 500)	0.450297	0.989	Success

Fig. 7 NIST testing results of the TRNG2015. Data size is 1000 Mbits (1000 sequences with each sequence around 1 Mbits). For ’success’ using 1000 samples of 1 Mbits data and significance level = 0.01, the P-value (uniformity of p-values) should be larger than 0.0001 and the proportion should be in the range of 0.99 ± 0.0094392

V. CONCLUSION

In the primary testing, the TRNG2015 is fully functional. All the ten output channels have 1 Gbps output with a 1 Gbps clock input. The output random number can pass the NIST statistical tests. With ten channels working at 1 Gbps, the power dissipation is only about 700 mW in total.

The TRNG2015 with a very small size and a low power dissipation can generate true random number at an ultra-high data rate. It can satisfy most of the random number demands from the cryptography and security applications in real-time. With the ultra-high data rate, the applications can use the random number as needed. The TRNG2015 even could upper the performance of the application which is limited by the random before.

REFERENCES

[1] Petrie C S, Connelly A. A noise-based IC random number generator for applications in cryptography[J]. Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on, 2000, 47(5): 615-621.

[2] Petrie, Craig S., and J. Alvin Connelly. "Modeling and simulation of oscillator-based random number generators." Circuits and Systems, 1996. ISCAS'96, Connecting the World, 1996 IEEE International Symposium on. Vol. 4. IEEE, 1996.

[3] Sunar B, Martin W J, Stinson D R. A provably secure true random number generator with built-in tolerance to active attacks[J]. Computers, IEEE Transactions on, 2007, 56(1): 109-119.

[4] Wold K, Tan C H. Analysis and enhancement of random number generator in FPGA based on oscillator rings[J]. International Journal of Reconfigurable Computing, 2009, 2009: 4.