



10-Gbps True Random Number Generator Accomplished in ASIC

Xinzhe Wang^{1,2}, Futian Liang^{1,2}, Peng Miao^{1,2}, Yi Qian^{1,2}, Ge Jin^{1,2}

1. Modern Physics Department, University of Science and Technology of China
2. State Key Laboratory of Particle Detection and Electronics, USTC, Hefei, 230026

Poster ID: 016

Design of a 10-Gbps Random Number Recorder

Yi Qian^{1,2}, Futian Liang^{1,2}, Xinzhe Wang^{1,2}, Houbing Lu^{1,2}, and Ge Jin^{1,2}

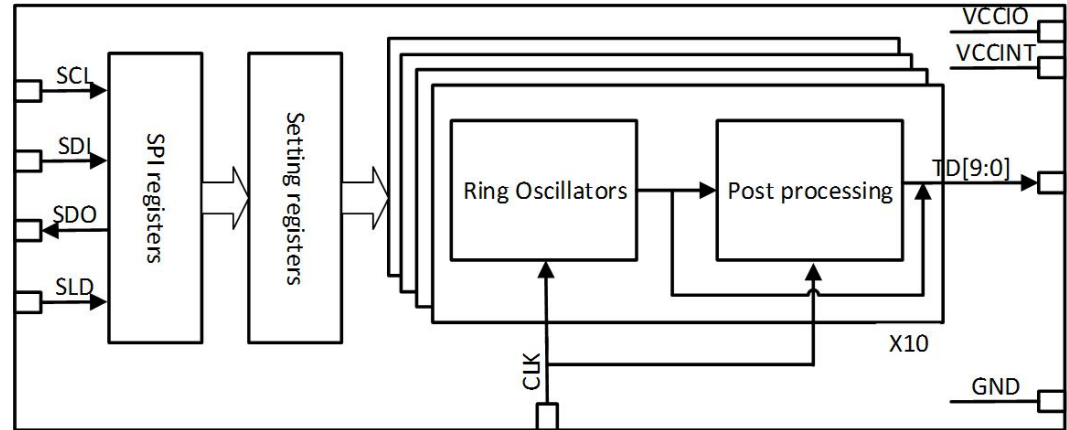
1. Modern Physics Department, University of Science and Technology of China
2. State Key Laboratory of Particle Detection and Electronics, USTC, Hefei, 230026

Poster ID: 051



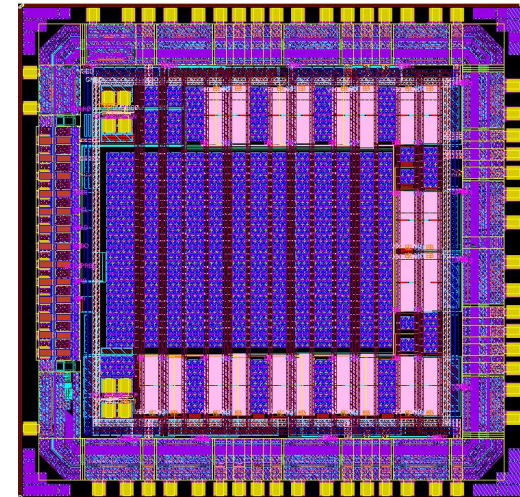


The TRNG2015 is a 10-channel paralleled high speed true random number generator accomplished in ASIC



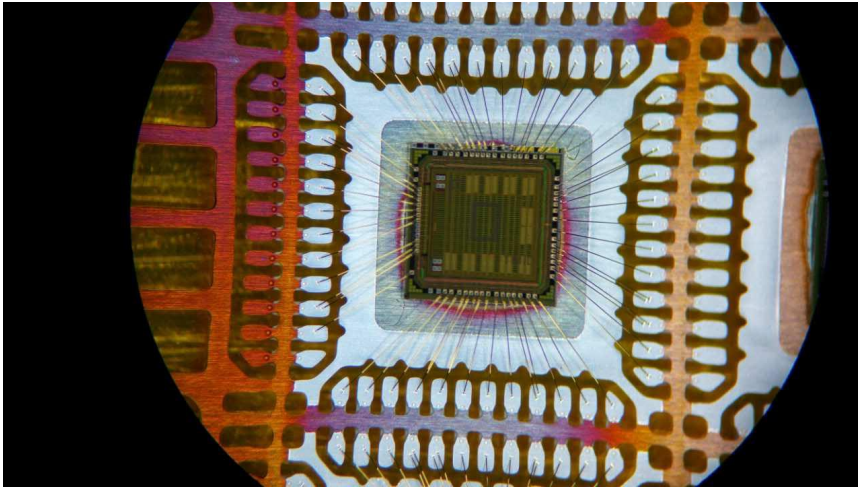
Structure of the TRNG2015

The TRNG2015 uses clock jitters of digital circuit as its entropy source.
The data rate is determined by the off-chip sampling clock.
The whole circuit can be set by SPI bus.

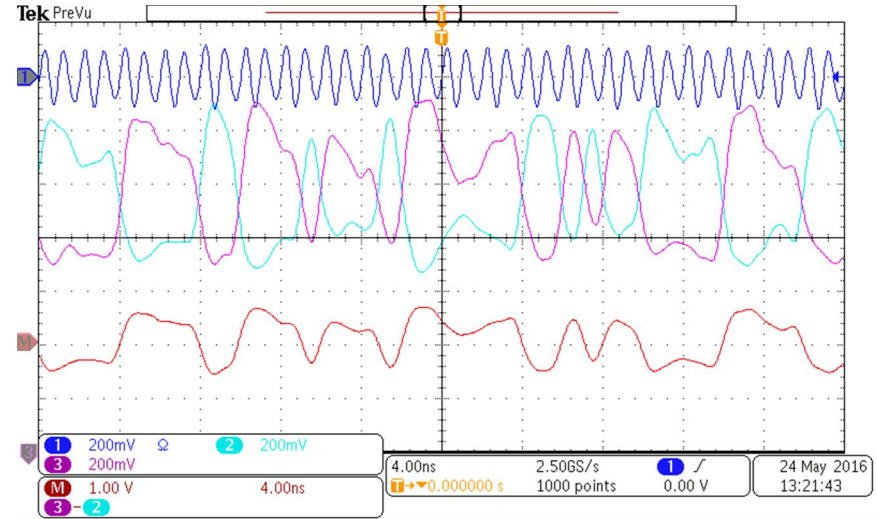


Layout of the TRNG2015





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.

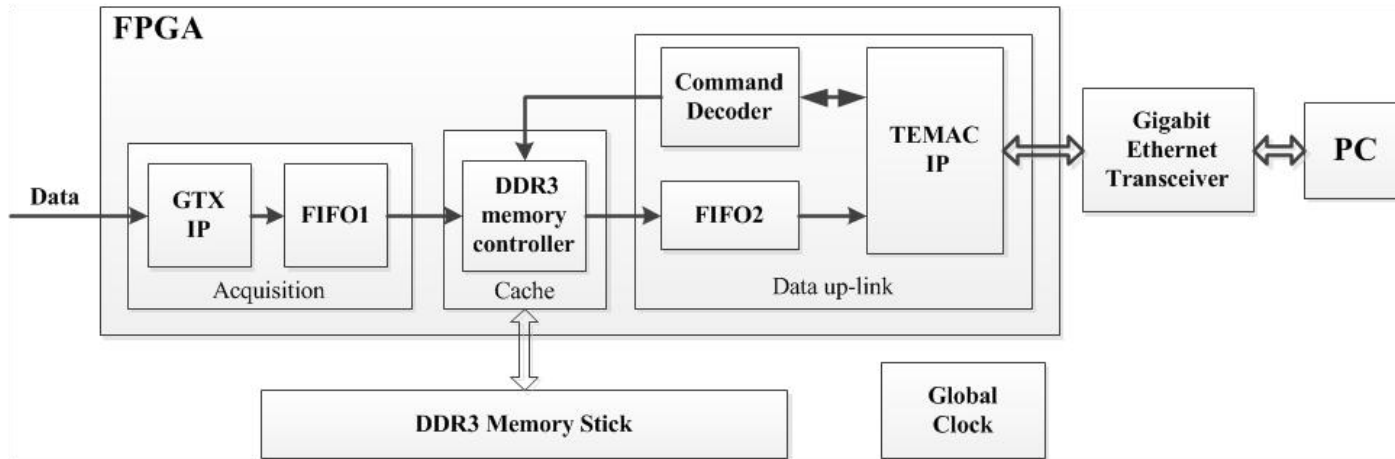


The data rate of each channel can be as high as 1Gbps. The power dissipation when all the ten channels are fully functional is about 700mW in total.





Design of a 10-Gbps Random Number Recorder



The high speed data acquisition is designed to receive and cache the random number generated by TRNG2015. The prototype is based on a Xilinx Vertex-6 FPGA ML605 evaluation board.





PRBS	Total Bits	Errors	Error Ratio
PRBS7	1.6×10^9	0	$< 6.25 \times 10^{-10}$
PRBS15	1.6×10^9	0	$< 6.25 \times 10^{-10}$
PRBS23	1.6×10^9	0	$< 6.25 \times 10^{-10}$
PRBS31	1.6×10^9	0	$< 6.25 \times 10^{-10}$

Results of bit error ratio test

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

The data recorded from TRNG2015 can pass the NIST tests.

In the NIST tests, 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





Poster Session 2

10-Gbps True Random Number Generator Accomplished in ASIC

Xinzhe Wang^{1,2}, Futian Liang^{1,2}, Peng Miao^{1,2}, Yi Qian^{1,2}, Ge Jin^{1,2}

1. Modern Physics Department, University of Science and Technology of China
2. State Key Laboratory of Particle Detection and Electronics, USTC, Hefei, 230026

Poster ID: 016

10-Gbps True Random Number Generator Accomplished in ASIC

Xinzhe Wang¹, Futian Liang^{1,2}, Peng Miao^{1,2}, Yi Qian^{1,2}, Ge Jin^{1,2}
 1. Anhui Key Laboratory of Physical Electronics, Modern Physics Department, University of Science and Technology of China
 2. State Key Laboratory of Technology of Particle Detection and Electronics, Hefei, Anhui, 230026

The difficulty is mainly the requirement for true random number generator. As the development of communication technology and the requirement of the network, high-speed and high-quality output rate are as important as the quality of the TRNG in the network true random number generator devices and components. Based on the TRNG structure design from the viewpoint of the structure of the TRNG, we designed the TRNG2023, a high-speed TRNG accomplished in ASIC.

Entropy source
 TRNG can be accomplished by many methods such as the noise and chaotic change inherent in nature. However, the circuit is difficult for the high-speed requirements, we use the clock jitter in digital circuit as the entropy source.

TRNG Testing
 The TRNG2023 is a high-speed TRNG. The power dissipation when the TRNG2023 is working is about 200mW in the 2.5um ASIC. The TRNG2023 is tested by the TRNG2023 test program. The test results show that the TRNG2023 is a high-speed TRNG. The TRNG2023 is tested by the TRNG2023 test program. The test results show that the TRNG2023 is a high-speed TRNG.

Design Scheme
 Based on the clock jitter in digital circuit, we designed the TRNG2023, a true random number generator ASIC chip, which can generate 10 Gbps true random number generator output data. The TRNG2023 is tested by the TRNG2023 test program. The test results show that the TRNG2023 is a high-speed TRNG.

Conclusion
 In the primary testing, the TRNG2023 is a high-speed TRNG. The TRNG2023 is tested by the TRNG2023 test program. The test results show that the TRNG2023 is a high-speed TRNG.

Design of a 10-Gbps Random Number Recorder

Yi Qian^{1,2}, Futian Liang^{1,2}, Xinzhe Wang^{1,2}, Houbing Lu^{1,2}, and Ge Jin^{1,2}
 1. Modern Physics Department, University of Science and Technology of China
 2. State Key Laboratory of Particle Detection and Electronics, USTC, Hefei, 230026

1. Introduction
 In order to meet the requirements of high-speed random number generation, a 10-Gbps random number recorder is designed. The recorder is designed to record the random number data generated by the TRNG2023. The recorder is designed to record the random number data generated by the TRNG2023.

2. System Design
 The design of the 10-Gbps random number recorder is based on the TRNG2023. The recorder is designed to record the random number data generated by the TRNG2023. The recorder is designed to record the random number data generated by the TRNG2023.

3. BERT & NIST TEST
 The BERT & NIST test results show that the TRNG2023 is a high-speed TRNG. The BERT & NIST test results show that the TRNG2023 is a high-speed TRNG.

4. Conclusions
 In this paper, a design of a 10-Gbps random number recorder is presented. The recorder is designed to record the random number data generated by the TRNG2023. The recorder is designed to record the random number data generated by the TRNG2023.

References
 [1] X. Wang, F. Liang, P. Miao, Y. Qian, and G. Jin, "10-Gbps True Random Number Generator Accomplished in ASIC," *IEEE Transactions on Nuclear Science*, vol. 69, no. 1, pp. 1-8, 2023.

Design of a 10-Gbps Random Number Recorder

Yi Qian^{1,2}, Futian Liang^{1,2}, Xinzhe Wang^{1,2}, Houbing Lu^{1,2}, and Ge Jin^{1,2}

1. Modern Physics Department, University of Science and Technology of China
2. State Key Laboratory of Particle Detection and Electronics, USTC, Hefei, 230026

Poster ID: 051

