Contribution ID: **16** Type: **Poster presentation**

10-Gbps True Random Number Generator Accomplished in ASIC

Friday, June 10, 2016 10:30 AM (1h 35m)

Random number generators are wildly used in many applications in a diverse set of areas ranging from statistics to cryptography. For most applications, pseudo random number generators (PRNGs) are quite satisfactory. However, for cryptographic and security applications, true random number generators (TRNGs) are required for the unpredictability. Random number generated from the quantum entropy is considered the best random number. Even so, the quantum TRNG is usually a large system which takes volume, and some methods may not generate number at a fixed frequency. 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 oscillator rings. The TRNG2015 is fabricated in a 130 nm 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.

In the TRNG2015 design, a SPI bus is used to configure the entropy source, to enable the channel and to select the post processing structure. With the clock depended data rate and configuration ability, we can balance the power dissipation and the generator function.

In the primary test, the ASIC chip 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 cryptographic 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.

Primary authors: LIANG, Futian (University of Science and Technology of China); WANG, Xinzhe (University of Science and Technology of China)

Co-authors: JIN, Ge (Univ. of Science & Tech. of China (CN)); MIAO, Peng (University of Science and Technology of China); QIAN, yi

Presenter: WANG, Xinzhe (University of Science and Technology of China)

Session Classification: Poster Session 2

Track Classification: Data Acquisition