Contribution ID: **39** Type: **Poster presentation**

FPGA Implementation of Toeplitz Hashing Extractor for Real Time Post-processing of Raw Random Numbers

Tuesday, June 7, 2016 3:00 PM (1h 30m)

Random numbers are widely used in many fields such as statistical analysis, numerical simulation and cryptography. However, most existing random number generators cannot directly output ideal random bits without post-processing, where complicated mathematical operation is usually needed and the speed is severely limited. With the development of random number generation, the speed of raw random data generation has reached to Gbps magnitude and existing post-processing cannot satisfy the growth of demand. To close the gap between experimental demonstration and practical application, we propose a concurrent, pipeline-like algorithm based on Toeplitz hashing function and implement it in a resource-limited FPGA. By taking advantage of the concurrent computation features of FPGA instead of common computer serial computation, the post-processing speed is greatly improved by three or four orders of magnitudes to above 3.36 Gbps, which is suited for Gbps real-time post-processing of raw random numbers. In our scheme, a matrix building seed unit is employed to store the elements to construct the Toeplitz matrix by signal fan-out. The entire Toeplitz matrix multiplication is evenly decomposed into several sub-matrix multiplications, which are sequentially calculated in a shared time division multiplexing unit. The sub-intermediate results are then accumulated to obtain the final random bits. All the calculation units work in a concurrent pipeline mode. By employing this kind of time division multiplexing calculation structure, FPGA resources are substantially saved and the extractor can be successfully realized. To implement the Toeplitz hashing function, a data acquisition and post-processing board is developed. In the board, the random signal is sampled and digitalized as raw random data by an 8-bit analog-to-digital converter and then the raw data are transferred to a high-performance FPGA for real-time post-processing. At the same time, small form-factor pluggable (SFP) is employed to output the final random bits at a real-time speed of 3.2 Gbps, USB 2.0 and Gigabit Ethernet are also provided for different scenarios.

Primary author: Mr ZHANG, Xiaoguang (State Key Laboratory of Particle Detection and Electronics and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, P.R.China)

Co-authors: Prof. LIANG, Hao (State Key Laboratory of Particle Detection and Electronics and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, P.R.China); Prof. ZHANG, Jun (Hefei National Laboratory for Physical Sciences at the Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, P.R.China); Mr NIE, Youqi (Hefei National Laboratory for Physical Sciences at the Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, P.R.China)

Presenter: Mr ZHANG, Xiaoguang (State Key Laboratory of Particle Detection and Electronics and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, P.R.China)

Session Classification: Poster session 1

Track Classification: Emerging Technologies / Feedback on Experience