Authors:
Miloš Drutarovský (milos.drutarovsky@tuke.sk)
Michal Varchola (michal@varchola.com)

Affiliation:
Technical University of Košice, Faculty of Electrical Engineering and Informatics, Department of Electronics and Multimedia Communication
Park Komenského 13, 04120, Košice, Slovakia

Analysis of Randomness Sources in Transition Effect Ring Oscillator based TRNG

The paper presents an analysis of the True Random Number Generator (TRNG) based on a new high entropy digital element for FPGA which was introduced at the CryptArchi 2009. Experimental results from Actel FPGA are attached as well in order to show its suitability for practical use. An original idea behind the principle lies in the randomness gathering on an oscillatory trajectory when bistable circuit is resolving previous (not necessarily metastable) event. Although oscillatory behavior is a well know issue in the field of synchronization flip-flops, this feature was neglected when designing TRNGs for FPGAs up to now. A bistable circuit used in this design is Transition Effect Ring Oscillator (TERO) where oscillatory phase can be excited on the demand and reliably synthesized in FPGA. The analyzed TERO loop consists of two NAND gates and four inverters used in practical Actel TERO TRNG implementation. Inputs of NAND gates that are outside the loop are connected together to excitation signal. Randomness is represented by the various number of oscillations counted after each excitation by binary asynchronous counter and extracted as LSB bit of this counter. Number of generated oscillations is directly related to the actual TERO working conditions during random bit generation. There are three potential random processes that can affect resulting number of oscillations: 1) The actual noise and circuit parameters when excitation pulse forces entering of the oscillatory phase; 2) The random shortening of excited pulse due to noise at threshold level; and 3) Very small discrete levels of the last pulse of lowest energy that will cause high sensitivity of last counter incrementation to actual noise in logic gate. All of those three factors are evaluated by the LT Spice simulation in order to evaluate their portion on the random result. Moreover, according simplified mathematical model evaluated by VHDL simulation the second potential random process is simulated in two boundary situations: 1) constant level of noise meanwhile a single bit generation; 2) highest possible noise frequency in order to show randomness extracting capabilities for both cases. Comparison with traditional ring oscillator based TRNG confirms superior features of new TERO based TRNG topology.