How (not) to end up with dependent random bits (Abstract)

Markus Dichtl

April 29, 2019

Sampling a jittering ring oscillator with a D-flip-flop in order to generate random bits seems to be a completely trivial operation. However, this talk provides experimental evidence from an Artix-7 FPGA that the bits sampled strongly depend on the bit stored in the flip-flop prior to the sampling. In a ring oscillator based true random number generator, the bit stored in the flip-flop usually is the previous random bit. As a consequence, subsequent random bits can be dependent.

This phenomenon was studied on ring oscillators of different lengths and in different phase situations. Additionally, the sampling of the xor of signals from multiple ring oscillators was evaluated.

The talk discusses possible reasons for this problem and why it has not been observed previously. Furthermore, several approaches to overcome the problem are suggested.