A Critical Look at Measurements of the Statistically Independent Components of Ring Oscillator Noise (Abstract)

Markus Dichtl, Pascale Böffgen

Siemens Corporate Technology

At Cryptarchi 2011, Richard Newell showed in his talk "Measurement of FPGA ring oscillator noise, and analysis using the Allan Variance method" that jitter contributions of ring oscillators are not at all independent, whereas previous analyses of random number generation with ring oscillators had been based on independence assumptions.

Hence, ring oscillator based true random number generators were without a valid theoretical basis until in 2014 the paper "On the assumption of mutual independence of jitter realizations in P-TRNG stochastic models" by Patrick Haddad, Yannick Teglia, Florent Bernard, and Viktor Fischer at the DATE conference suggested a solution. The authors proposed a method how to distinguish the independent noise contributions from the dependent ones. Secure ring oscillator based random number generators should rely on the independent contributions only.

Our talk will give a closer look at this method of distinguishing dependent and independent noise contributions. Our analysis will be based both on the measurement results given in the paper by Haddad et al., and on our own measurements of ring oscillators implemented on FPGAs. We will discuss the inclusion of quantization noise into the noise model. Quantization noise should be considered, as the jitter measurement method suggested in the paper of Haddad et al. can determine accumulated jitter only in units of whole ring oscillator periods. In our talk, also methods allowing to measure jitter in much smaller temporal units, will be discussed.

Keywords: random, true random number generator, statistical dependence, ring oscillator, jitter