# Techniques to Improve the Extraction of Entropy from Circuits with Random Behaviour (Abstract)

Markus Dichtl[1] and Bernd Meyer[2]⋆

[1] Siemens AG, Corporate Technology
[2] Infineon AG

Most current true random number generators (TRNG) produce single random bits in temporal sequence and assume that the bits are statistically independent.

This talk introduces greedier techniques which allow producing several random bits simultaneously. As these bits may be statistically dependent, suitable deterministic post processing algorithms, which are adequate for dependent data, are required. The choice of suitable post processing algorithms will be discussed in the talk.

We suggest three different methods to achieve improved entropy extraction from circuits with random behaviour: usage of several flip-flops to sample the same signal, usage of multiple toggle flip-flops for the same signal, and sampling several signals in the circuit with random behaviour simultaneously.

Both sampling the same signal simultaneously with multiple flip-flops and using multiple toggle flip-flops for the same signal may sound absurd, but the talk will provide experimental evidence that both are well suited for the enhanced production of random bits. The paradox is resolved by the explanation that the flip-flops are operating far away from their specified operating conditions.

All techniques will be illustrated by experimental examples with numerical results on the entropy achieved. The main circuit with random behaviour used in the experiments covered by the talk is the Fibonacci ring oscillator, but other TRNG circuits will be considered as well. Even the randomness extracted from classical ring oscillators can be enhanced considerably.

**Keywords: random, true random number generator, entropy, entropy extraction, post processing, ring oscillator, Fibonacci ring oscillator**

⋆ The results described in this talk were achieved when the author was employed at Siemens.