# Using Higher Harmonics of Ring Oscillators for Physical Random Number Generation on FPGAs

# (Abstract)

Markus Dichtl and Bernd Meyer

Siemens AG, Corporate Research and Technologies, Munich, Germany

Most physical oscillators may not only oscillate at their fundamental frequency, but also at multiples of it. So it is a natural question to ask whether ring oscillators can also oscillate on higher harmonics of their fundamental frequency. In normal ring oscillator operation, at any instant of time there is one inverter of the ring which changes its output voltage. When the switching level is reached, the next inverter changes its output voltage, and so on. However, it is also possible to have simultaneously several, preferably equidistant, positions in the ring where the state of the inverter output changes. We show how to bring a ring oscillator in such a state by starting it from suitable initial conditions.

We were not the ones to discover this phenomenon, we only rediscovered it. It was first described in the paper "Higher Harmonic Generation in CMOS/SOS Ring Oscillators" by Nobuo Sasaki (IEEE Transactions on Electron Devices, vol. ED-29, no. 2, February 1982). He showed that ring oscillators with an odd number of inverters oscillate only on odd harmonics, whereas only even harmonics are possible with an even number of inverters.

However, we are the first ones to suggest a useful application of this phenomenon, namely to use it for random number generation. Our proposal is based on the observation that for rings with a small number of inverters the oscillations on the harmonics only exist for a relatively short duration. Then the rings fall back to lower harmonics or the fundamental frequency. The duration of the oscillation on the harmonics varies randomly. We verified this by repeatedly restarting the ring oscillators from identical starting conditions. The easiest way to generate random bits from this is to toggle a flip-flop at each positive edge of some fixed inverter output of the ring oscillator. The ring is started from a suitable initial condition and the state of the flip-flop is sampled after a fixed time. As the length of time running on the higher frequency is random, so is the number of positive edges registered by the flip-flop. Ring oscillators of even length stop oscillating when falling back from the second harmonic.

In this talk, we will show oscillogramms of Spartan 3 FPGA experiments, both of the harmonic ring oscillator phenomenon, and the physical random number generators derived from it. FPGAs are the best way to implement these generators, as they use table lookup to determine the values of logical functions. This leads to equal delays for all kinds of logical gates. In contrast, implementing the generators with standard cells from ASIC libraries lead to significantly different delay times for the simple inverters and the NAND or NOR gates needed to enforce the required startup conditions. The different delay times do not make ASIC implementations impossible, but tend to shorten the times the oscillators run on higher harmonics.

Physical random number generators based on ring oscillator harmonics turn out to be one of the most compact and fastest designs for FPGA implementation.