Fibonacci Ring Oscillators as True Random Number Generators - A Security Risk

Abstract

Markus Dichtl

Siemens Corporate Technology

Fibonacci ring oscillators are easily implemented on FPGAs and ASICs and seem to be good source of true randomness. The randomness is assumed to be caused by chaotic oscillations. However, in this paper Fibonacci ring oscillators are shown to have a risk to oscillate periodically instead of chaotically. The security implications of this are discussed. The probability of the occurrence of the periodic oscillations is determined experimentally on an FPGA for Fibonacci ring oscillators of lengths 16 and 32. Means to overcome the problem of the periodic oscillations are also discussed.

Keywords: Fibonacci ring oscillator, randomness, true random number generator, security, FPGA, ASIC