Cryptology ePrint Archive: Report 2011/637

Random Number Generation Based on Oscillatory Metastability in Ring Circuits

Laszlo Hars

Abstract: Random number generator designs are discussed, which utilize oscillatory metastability, induced by switching between two stable states of ring-connected digital gates. For a short time after the switch-over the circuits behave quite randomly, influenced by the circuit noise. We provide simple programs, which simulate the fundamental behavior of our circuits. We also present a mathematical model and theoretical explanations of the underlying physical phenomena, the random phase drift and pulse decay. These also illuminate the principles of other recently published random number generators. The feasibility of the designs was confirmed by FPGA prototypes. These random number generators are small, fast and built of standard logic gates. The simplest example contains just one XOR gate as the source of randomness.

Category / Keywords: applications / Electronic random number generators, Ring oscillators, Metastability, Random walk

Date: received 25 Nov 2011

Contact author: Laszlo at Hars US