A fully-digital Chaos-based Random Bit Generator

Marco Bucci, Raimondo Luzzi
Infineon Technologies AG
{marco.bucci, raimondo.luzzi}@infineon.com

June 6, 2016

Abstract

In this paper, the design of a fully-digital chaos-based random bit generator (RBG) is reported. The proposed generator exploits a chaotic system whose map is implemented in the time domain where the state variables of the system are represented by the phase of digital ring oscillators. This results in an extremely robust and efficient entropy source which can be implemented as a digital standard-cell thus overcoming the main drawbacks of chaotic RBGs. An implementation in a $40nm$ CMOS technology shows a final throughput after post-processing of 12.5Mbit/s at 50MHz with a worst case current consumption below $40\mu A$.

The entropy rate of the source can be determined a priori and, in our implementation, it results to be >1.43 bits over 4 bits generated by the source in one clock cycle. After a 16 times compression in a 32-bit linear feedback shift register (LFSR), the final data have full-entropy. A descrambling method for a direct evaluation of the entropy after post-processing is provided which can cancel the pseudo-randomness introduced the the LFSR.

The proposed generator has been integrated in a test chip in order to test it in a realistic operating environment. Extensive measurements over about 100 devices extracted from different process corners, in the temperature range $-40$to 110°C, show that the measured entropy rate of the source fits with high accuracy the calculated entropy rate from the chaotic system model. Compressed data after descrambling show full-entropy and AIS31 statistical tests (procedure A and B) are passed.