A Multimode Ring Oscillator based TRNG for FPGAs

Miloš Grujić, Vladimir Rožić and Ingrid Verbauwhede
imec-COSIC, KU Leuven, Belgium

Abstract

True random number generators (TRNGs) are essential cryptographic components. Due to ever increasing ubiquity of FPGAs in modern embedded security systems, there exists a growing demand for fully-digital TRNGs that are suitable for FPGAs. As one possible solution to this problem, the TRNGs based on time-to-digital conversion are proposed. TDC based TRNGs rely on the concept of sampling the unstable signal of the ring oscillator with very high precision by using fast delay-chains.

In this work, we present a novel delay-chain based TRNG design with conservative security evaluation. Our design aims to minimize the effects of the unwanted noise sources and pseudo-randomness. Unlike previous DC-TRNG designs, our TRNG extracts significant entropy from the jittery pulse of the multimode ring oscillator. Additionally, we improved the design of digitization part to further boost the TRNG entropy rate. Our design is accompanied with a stochastic model which takes into account disparities and non-linearities in the structure of FPGAs. Further, we discuss influence of the correlated noises and the switched-mode power supply (SMPS) on the performance and security of the proposed TRNG.