On True Random Number Generators Based on Chaotic Oscillations in General and Their Implementation on FPGAs in Particular

Markus Dichtl

Abstract

True random number generators based on chaotic oscillations have been around for some time, but they have always been playing a minor role. Known examples of chaos based TRNGs are described in J. Golic's paper "New Methods for Digital Generation and Postprocessing of Random Data" (IEEE Transactions on Computers, October 2006, pp. 1217-1229, vol. 55), which introduced Fibonacci and Galois ring oscillator, and "A fully-digital Chaos-based Random Bit Generator" by Bucci and Luzzi(e. g. Cryptarchi 2016). The talk considers these and various other TRNGs based on chaos from various perspectives, among them the implementability on FPGAs.

The talk will also consider the fundamental question to what extent it makes sense to base TRNGs on a mathematical theory which is only defined for deterministic systems, and how these seemingly contradictory concepts can be conciliated. SPICE simulation, being completely deterministic, helps to identify chaotic behaviour were very small changes of parameters lead very quickly to very different behaviour.

In the past, various chaos based TRNGs have turned out to fail by oscillating with short periods (e. g. IACR ePrint 2015/270) which is demonstrated in the talk by SPICE simulations. The progress achieved for this problem by the recent paper "A Closer Look at the Chaotic Ring Oscillators based TRNG Design" by Su et al. (IACR ePrint 2023/040) is also discussed.

As well, the talk looks at chaos based TRNGs with respect to the generally accepted requirement for stochastic models in the style of AIS31.