High-throughput TRNGs on FPGAs

Vladimir Rožić, Bohan Yang and Ingrid Verbauwhede

April 7, 2015

Abstract

True random number generators (TRNGs) are essential components in security systems because they are used for generating session keys, mask values and challenges in various authentication protocols. One of the most important requirements of TRNG designs is entropy assessment using a stochastic model of the entropy source. Unfortunately, very few TRNGs are provided with a formal evaluation of security. Moreover, this requirement is very difficult to meet together with demands for a high-throughput and compact implementation.

In this work, we present a novel design method for high-throughput randomness generation on FPGAs. In addition to look-up tables and flip-flops, slices on Xiling Spartan-6 FPGA also contain carry-chain primitives which are normally used to generate high-speed adders and multipliers. Similar primitives exist in most commercial FPGAs. These primitives can also be used to efficiently extract entropy from jitter-based entropy sources.

Our novel TRNG based on carry-chain primitives achieves a throughput of 14.3 Mb/s while consuming only 67 slices. It is provided with a stochastic model and it is amenable to on-the-fly testing.