True Random Number Generators
Project Proposal/Abstract

Astri M. Ravnaas  Nicolai Eeg-Larsen
astrimra@umail.ucsb.edu  nicolai@umail.ucsb.edu

April 28, 2015

True Random Number Generators

Random numbers and randomization techniques are critical for modern cryptography. Most random numbers used in computer programs are pseudo-random, which means they are generated in a predictable fashion using a mathematical formula. The importance of TRNGs is increasing, and the demand is especially high in cryptography, but also other areas as gambling and lotteries, statistics etc.

A true random number generator (TRNG) utilizes a physical processes to generate a random number. TRNG are commonly built from the following three components: Entropy Source, Harvesting Technique and Postprocessing. A large number of TRNG designs have been proposed. Each design has its strengths and weaknesses. In common for them all is that they have some desirable features. In our paper we will discuss what building blocks that are needed for a TRNG and which features that are desirable.