A general framework to model $1/f^2$ noise of TRNG

David Lubicz, DGA-MI, France

Abstract

In this talk, we present a general framework for stochastic models of TRNG. This framework is based on very general assumptions :
- the state of the TRNG is given by a point in a continuous space of phases ;
- a random variable in this space of phase describe the knowledge of the attacker ;
- each time a random bit is produced by the TRNG, the attacker learns some information about the random variable X;
- the $1/f^2$ noise produce some uncertainty.

We will show that the Kullback-Leibler divergence gives a precise meaning to the uncertainty of the random variable X and so of the entropy accumulated inside the TRNG. In the case, that the TRNG is a oscillator based elementary TRNG, we use this framework to study the following questions: What is a entropy rate per second that we can reach ? For a given entropy rate per second what is the entropy rate per bit ? We will show that in order to obtain the highest entropy rate per second, the sampling oscillator must have the highest possible frequency and then the entropy rate per bit will be small. We give an equation, based on some heuristically assumptions, linking all these quantities.