An illustration of a new certification approach for TRNGs

Elie Noumon Allini, Florent Bernard, Viktor Fischer

Hubert Curien Laboratory, UMR CNRS 5516, University of Lyon

St-Etienne, France

Abstract

Random number generators represent important cryptographic primitives. They generate random numbers or random bit streams that are used at many security levels in various cryptographic schemes, and have to be unpredictable and flawless. Unpredictability is guaranteed the best by using a random physical process in a physical True Random Number Generator (TRNG). However, the design of physical TRNGs is a very challenging one because many aspects related to this kind of generators are not mastered as they should be. A work in progress is aiming to propose an approach to evaluate TRNGs and check if they are safe enough to be used in cryptographic schemes. This apporach will be illustrated with the evaluation of a PLL-based TRNG secured by dedicated statistical tests.