Random number generators for cryptography – design, evaluation and tests

Viktor Fischer
Hubert Curien Laboratory, Jean Monnet University Saint-Etienne, France

Random numbers are crucial in cryptography: they are used as confidential keys, initialization vectors, nonces in challenge-response protocols, padding values, and even as masks in side channel attack countermeasures. Random number generators (RNGs) must generate random numbers that have good statistical properties and the generated sequences must be impossible to predict and manipulate.

Stringent security evaluation of RNGs is not straightforward. This is because it necessitates expertise in several scientific fields such as: microelectronics and physics to understand random physical processes in electronic circuits; mathematics and statistics for constructing simple, but sufficiently precise stochastic models; information processing and information theory to estimate and manage entropy; and cryptography for dealing with security and cryptographic post-processing.

Goal: The objective of this tutorial is to introduce the participant to random number generation for cryptography in logic devices as well as to generator design and security evaluation criteria. Strong and weak ways of generating random numbers in hardware will be illustrated on state-of-the-art designs. Finally, a comprehensive example of a complete TRNG design including embedded randomness testing will be given and practically demonstrated on a dedicated evaluation board.

Of interest to: Engineers and young researchers in cryptography engineering and embedded security.

Preliminary skills: Basics in cryptography, electronics, mathematics and probability (Bachelors Degree).

Outline: **Part 1 – Basics on random number generation for cryptography**
Introduction to random number generation
Sources of randomness
Entropy extraction
Statistical models and entropy estimators
Post-processing
RNG testing

Part2 – State of the art and pitfalls in TRNG designs
“Maximum entropy” TRNGs
Non-testable TRNGs
Internally testable TRNGs

Part3 – Practical example: design and evaluation of a secure TRNG
Example of an internally testable TRNG
Statistical modeling and entropy estimation of the proposed TRNG
Proposition of a model-based online test
RNG calibration and testing