

Seminar

# RNG on FPGA

Random number generation (RNG) is an essential part of many applications, be it for encryption, testing, or other purposes. However, randomness is difficult to accomplish in digital circuits which are supposedly deterministic.

The goal of this seminar topic is to understand and explain the challenges of RNG in hardware, and to compare different true random number generation (TRNG) and pseudo random number generation (PRNG) methods that are suitable for implementation on FPGA.

## Advisors

Max Koenen