Remotely Testable eDiViDe FPGA Setup of Soft CPU with Cryptographic TRNG Coprocessor Extension

Milos Drutarovsky, Michal Varchola

Dept. of Electronics and Multimedia Communications
Technical University of Kosice
Park Komenskeho 13, 04120 Kosice, Slovakia

Abstract

eDiViDe (European Digital Virtual Lab) is an online learning platform for digital electronics and focuses on providing a real FPGA based lab environment to students and researches. It is developed by several universities from Belgium, Germany, Norway and Slovakia and it is currently in development phase. The goal of eDiViDe is to motivate students to practice digital design by providing them with both simple and advanced setups and making the setups available remotely. Selected advanced setups can link also ongoing research and provide tools for cooperation among research groups.

As one of advanced setups we provide complete design for remote testing of custom configurable TRNG coprocessor. The coprocessor is connected to the standard Altera Nios II soft CPU embedded into Altera Cyclone III FPGA in Nios II embedded evaluation Cyclone III kit. Parameterized TRNG design is provided in VHDL and its main design parameters can be modified by end user. Nios II CPU software evaluates on-line quality of generated random bit stream by using standard FIPS140 statistical tests. Complete design uses Nios II Cyclone III embedded evaluation kit board and additional configuration, debug and monitoring interfaces prepared for remotely accessible infrastructure of eDiViDe project infrastructure. Proposed setup and eDiViDe infrastructure enable remote evaluation and testing of proposed complete demonstration of TRNG design. Moreover, the end user can use provided infrastructure and remotely test even its own TRNG design submitted in VHDL code.