

A novel ring oscillator based PUF on FPGA.

Robert Lorencz and Filip Kodytek

Abstract

Our contribution deals with design of Physical unclonable functions (PUFs) based on FPGA. Our approach promises a cheap, efficient, and secure device identification, and also generation of cryptographic keys. A proposal of a ring oscillator (RO) based PUF producing more than one output bit from one RO pair is presented. 24 Digilent Basys 2 FPGA boards were tested and statistically evaluated indicating suitability of our design for device identification. Ultimately the design is combined with error correction codes in order to generate cryptographic keys.