Abstract: Physically unclonable functions (PUFs) are an innovative way to generate device unique keys using uncontrollable production tolerances. In this work, we present a method to use PUFs on modern FPGA-based system-on-chips (SoCs). The processor system part of the SoC is used to configure the FPGA part. We propose a reconﬁgurable PUF design that can be changed by using the partial reconﬁguration (PR) feature of modern FPGAs. Multiple ring oscillator PUF (RO PUF) designs are loaded on the same logic blocks of the FPGA in order to make use of different resources, i.e., sources of entropy, on the FPGA. Their frequencies are read out individually and the differences between neighbored oscillators are used to generate a bit response. The responses of each design can be concatenated to a larger response vector that can be used to generate a cryptographic key. We present an implementation that is able to decrease the needed resources by 87.5% on a Xilinx Zynq.

Stichworte: Physically unclonable functions; FPGA; SoC; RO-based PUF; partial reconfiguration.