Implementing Physically Unclonable Functions (PUFs) on FPGAs is quite inefficient in terms of resource usage. Many logic and routing resources that could serve as entropy sources remain unused. We introduce a method that uses the partial reconfiguration ability of modern FPGAs as a way to maximize the entropy that can be extracted out of a logic block. Different implementations and types of PUFs can be reprogrammed on the same logic blocks and each of their outputs used as an individual partial key. We show with a first implementation that up to six PUFs can be used on the same logic block on a Xilinx Zynq. The correlation between the PUF outputs remains very small, so that the area needed for the same length of PUF response can be shrunk up to 83%.
2014

Quartal:
  4. Quartal

Jahr / Monat:
  2014-12

Monat:
  Dec

Revied:
  ja

Sprache:
  en

WWW:
  http://www.isic2014.org/

Occurences:
  · Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2014

entries: