Dokumenttyp: Konferenzbeitrag
Art des Konferenzbeitrags: Vortrag / Präsentation
Autor(en) des Beitrags: Nisha Jacob and Jakob Wittmann and Johann Heyszl and Robert Hesselbarth and Florian Wilde and Michael Pehl and Georg Sigl and Kai Fisher
Titel des Beitrags: Securing FPGA SoC Configurations Independent of Their Manufacturers
Abstract: System-on-Chips which include FPGAs are important platforms for critical applications since they provide significant software performance through multi-core CPUs as well as high versatility through integrated FPGAs. Those integrated FPGAs allow to update the programmable hardware functionality, e.g. to include new communication interfaces or to update cryptographic accelerators during the life-time of devices. Updating software as well as hardware configuration is required for critical applications such as e.g. industrial control devices or vehicles with long life-times. Such updates must be authenticated and possibly encrypted. One way to achieve this is to rely on static FPGA manufacturer-provided cryptography and respective master keys. However, in this contribution, we show how to retrofit Xilinx Zynq FPGAs with an alternative cryptographic accelerator and how to establish device-individual keys using Physical Unclonable Function (PUF) technology. These two key aspects reduce the required trust in manufacturer-provided security features while increasing
the security by binding configurations to a specific device.

Stichworte:
SoC, FPGA, Zynq, PUF, cryptographic engine, partial reconfiguration, secure boot

Dewey Dezimalklassifikation (Liste):
620 Ingenieurwissenschaften

Kongress- / Buchtitel:
30th IEEE International System-on-Chip Conference SOCC

Kongress / Zusatzinformationen:
Munich, Germany

Jahr:
2017

Quartal:
3. Quartal

Jahr / Monat:
2017-09

Monat:
Sep

Revied:
ja

Sprache:
en

WWW:
https://www.ieee-socc.org/

Occurences:
- Hochschulbibliographie > 2017 > Fakultäten > Elektrotechnik und Informationstechnik > Sicherheit in der Informationstechnik (Prof. Sigl)
- Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2017

Entries: