Lehrstühle und Professuren

Dokumenttyp: Konferenzbeitrag

Autor(en) des Beitrags: Reinbrecht, Cezar and Forlin, Bruno and Sepulveda, Johanna

Titel des Beitrags: On the Aspects of MPSoCs Security: Avoiding Logical Attacks with Network-on-Chip

Abstract: Logical Side Channel Attacks (SCAs) became a relevant threat for Multi-Processors System-on-Chips (MPSoCs). They are able to extract remotely, sensitive information from the timing behaviour of the MPSoC. Previous works have proposed MPSoCs architectures capable of mitigating some of the SCAs which arise from sharing memory and processor resources. In this work, we discuss the actual logical attacks and countermeasures, and we sustain that the NoC can play the main role in MPSoC security through the proposal of AEGIS NoC. AEGIS NoC was able to harden the protection against several known SCAs through the integration of two main strategies: i) Blinding; and ii) Masking. AEGIS security and performance was evaluated under state-of-the-art attacks on real hardware at FPGA. Results demonstrate the potential to explore the NoC as the central defense mechanism of complex systems.


Dewey Dezimalklassifikation (Liste): 620 Ingenieurwissenschaften

Kongress- / Buchtitel: The IEEE International Symposium on Circuits and
Systems (ISCAS) 2019

Kongress / Zusatzinformationen:
Sapporo, Japan

Datum der Konferenz:
26.05.-29.05.2019

Jahr:
2019

Quartal:
2. Quartal

Jahr / Monat:
2019-05

Monat:
May

Revied:
ja

Sprache:
en

WWW:
https://www.iscas2019.org/

Occurences:
- Einrichtungen > Fakultäten > Fakultät für Elektrotechnik und Informationstechnik > Lehrstühle und Professuren > Sicherheit in der Informationstechnik (Prof. Sigl) > 2019

Entries: