Track 4

System Security & Cryptography

Moderator: Daniel Gruss, Maria Eichlseder,
Bettina Könighofer

ISW @ IAIK 2023/24

- **N.N.**: Exotic cache designs L. Giner
- **N.N.**: VIVT L1 Implementation in Gem5 L. Giner
- **N.N.**: Implementing Advanced Cache Attacks in a Simulator L. Giner
- **N.N.**: Power PAC Man A. Kogler
- **N.N.**: Power PAC Man A. Kogler

Session 4A: **Caches & Attacks**

14:00–14:50, IAIK Seminarraum
28 Feb 2024
www.iaik.tugraz.at/isw

IAIK

- **N.N.**: ReloCATor: A Rowhammer Mitigation using Cache Allocation Technology
  J. Juffinger
- **N.N.**: Video fingerprinting attacks via CPU side-channels S. Gast
- **N.N.**: Mobile Power Side-Channel Attacks M. Oberhuber
- **N.N.**: Masking Hybrid Homomorphic Encryption Schemes Aikata

Session 4B: **Side-Channel Attacks & Mitigations**

15:00–15:40, IAIK Seminarraum
28 Feb 2024
www.iaik.tugraz.at/isw

IAIK

- **N.N.**: Ascon & ISAP M. Eichlseder
- **N.N.**: CPU vs GPU: A comparison of architectures M. Nageler
- **N.N.**: Sharing Knowledge Without Sharing Data – Privacy Preserving Computations
  F. Schmid
- **N.N.**: MPC-use case of the Boston Women Workforce Council F. Schmid
- **N.N.**: Error correcting codes: Correct single-bit errors with the Hamming code
  L. Heimberger

Session 4C: **Cryptography**

15:50–16:40, IAIK Seminarraum
28 Feb 2024
www.iaik.tugraz.at/isw

IAIK

- **N.N.**: Foundations of Solving Satisfiability Modulo Theory S. Pranger
- **N.N.**: Easy-to-Use Shield Integration for Reinforcement Learning S. Pranger

Session 4D: **Formal Methods**

16:40–17:00, IAIK Seminarraum
28 Feb 2024
www.iaik.tugraz.at/isw

IAIK