preliminary announcement of a special issue on

Fault-Aware Security Design of Current and Post-Quantum Computing Systems

Journal of Systems Architecture (JSA)

The call for contributions to this special issue will be open to all researchers and practitioners.

The authors of selected high-quality papers accepted for presentation at FDTC 2025 (22nd Workshop on Fault Diagnosis and Tolerance in Cryptography, Kuala Lumpur, Malaysia, Sun 14 September 2025) will be invited to extend their work and submit it for consideration of publication in this special issue.

All papers accepted at FDTC 2025 will be published by Conference Publishing Services.

Guest editors:

- **Alessandro Barenghi** Politecnico di Milano
- **Juliane Krämer** University of Regensburg
- **Gerardo Pelosi** Politecnico di Milano

Tentative schedule of call, submission and review:

- Call for papers published: October 2025
- Submission deadline: February 2026
- Completion of review and revision: April 2026

Topics include (but are not limited to):

FAULT INJECTION SETUP AND PRAXIS:
- novel and improved mechanisms for fault injection
- practical issues in fault injection setup and validation of results
- practical limitations of attacks and their implications for security

HIGHLY-INVASIVE ATTACKS ON DEVICE SECURITY:
- setups for invasive attacks and their practical results, such as photonic emission analysis, laser thermal imaging, laser-voltage imaging and focused-ion beam technology
- practical issues, potential and limitations

ATTACKS ON MACHINE LEARNING (ML) ARCHITECTURES:
- validation of earlier results
- resilience of ML models to faults

CASE STUDIES:
- attacks on cryptographic implementations, classical and post-quantum
- attacks on embedded devices, e.g., mobile phones, industrial control devices, hardware wallets, security tokens and smartcards

COUNTERMEASURES (DETECTION, RESISTANCE AND TOLERANCE):
- countermeasures for cryptographic implementations, classical and post-quantum
- countermeasures for firmware of embedded systems
- detection countermeasures, e.g., control flow integrity
- HW/SW co-design countermeasures for CPU architectures

DESIGN TOOLS FOR THE ANALYSIS OF FAULT ATTACKS AND COUNTERMEASURES:
- early estimation of fault attack robustness
- automated insertion of fault countermeasures