FDTC 2024
Fault Diagnosis and Tolerance in Cryptography

Twentyfirst Workshop on Fault Diagnosis and Tolerance in Cryptography

September 4, 2024 • on-site: Halifax, Nova Scotia, Canada

(affiliated to CHES 2024)

FDTC 2024 is held in cooperation with IACR

Important dates (2024)

Submission:	May 26
Notification final acceptance:	July 12
Final version (camera-ready):	July 26
Workshop:	Sept. 4

Fault injection is one of the most exploited means for extracting confidential information from embedded devices and for compromising their intended operation. Therefore, research on established as well as upcoming methodologies, and techniques for fault injection, architectures and design tools for the design of robust and protected cryptographic systems and embedded devices (both hardware and software), are essential. Fault injection case studies on popular categories of embedded devices like mobile phones, industrial control devices, hardware wallets for cryptocurrencies, security tokens, etc., are of high interest to improve the understanding of the implications on realistic applications. FDTC is the reference event in the field of fault injection appliances, fault attacks and countermeasures.

Topics of interest include but are not limited to:

- Fault injection setups and praxis:
  - novel and improved mechanisms for fault injection, e.g., using lasers, electromagnetic induction, or clock / power supply manipulation
  - practical issues in fault injection setups and validation results
  - practical limitations of attacks and implications for security
  - fault injection in emerging technologies, e.g., memristor, carbon nanotubes, etc.
- Case studies:
  - attacks on cryptographic implementations including post-quantum cryptography and lightweight cryptography
  - attacks on embedded devices like mobile phones, industrial control devices, hardware wallets for cryptocurrencies, security tokens, smartcards, TEEs, secure enclaves, etc.
  - attacks on machine learning architectures and validation of results
  - attacks on privacy-preserving technologies, e.g., homomorphic encryption, zero-knowledge proofs and multi-party computation
  - attacks on remote targets, e.g., fpgas in the cloud
- Related highly-invasive attacks on device security:
  - setups and practical results from invasive attacks, such as photonic emission analysis, laser thermal imaging, laser-voltage imaging, etc.
  - practical issues, limitations and potential
- Countermeasures (detection, resistance and tolerance):
  - countermeasures for cryptographic implementations
  - countermeasures for firmware of embedded devices, e.g., for bootloaders
  - detection countermeasures, e.g., control flow integrity
  - HW/SW co-design countermeasures for CPU architectures
- Design tools for analysis of fault attacks and countermeasures:
  - early estimation of fault attack robustness
  - automatic applications of fault countermeasures
  - formal methods and techniques for the verification of fault resiliency

Instructions for authors

Submissions must not substantially duplicate work that any of the authors published elsewhere or that was submitted in parallel to any other conference or workshop. Submissions should be anonymous, with no author names, affiliations, acknowledgments or obvious references. Papers should be up to 12 pages (including bibliography and appendices), and formatted according to the provided template.

FDTC encourages the submission of short papers, which will also be subject to peer review. Authors are encouraged to introduce work in progress, novel applications and corporate/industrial experiences. Short papers will be evaluated with a focus on novelty and potential for sparking the interest of the participants and future research avenues. Short paper submissions are limited to 6 pages, formatted as the regular ones, and their title must include the text "Short Paper:".

All accepted papers (regular and short) will be published in an archival proceedings volume by CPS and will be distributed at the time of the workshop. The submission of final papers is managed by Conference Publishing Services (CPS), which directly contacts the authors with instructions for finalizing and uploading the manuscripts.

At least one author of each accepted paper must register for the workshop and present the paper in order to be included in the proceedings. Additional submission instructions and further information can be found at: `fdtc-workshop.eu`