Ronan Lashermes

Engineer, PhD, HDR (2025) in Embedded Systems Security | 36 years old
ronan.lashermes@0nline.fr | 06 79 81 67 82 | ronan.lashermes.0nline.fr
1 rue Alexis Garnier, 35410 Châteaugiron, France

RESPONSIBILITIES

LHS INRIA
Scientific manager of the platform
I develop experiments (hardware and software) for physical attacks.

RISC-V FOUNDATION
Chair of Working Groups
Microarchitectural Side Channels SIG and *Timing Fences TG* on microarchitecture security.

PEPR CYBERSECURITY PROJECT - ARSENE
Core Committee Member
Inria coordinator for the project.

JAIF (THEMATIC DAY)
Member of the organizing committee
Local organizer for the 2024 edition.

SUPERVISION
Advisor of 4 PhD theses, including 1 as supervisor: 2 completed, 2 ongoing (end in 2025).

EDUCATION

CEA / UVSQ
PhD in Computer Science/Cryptography
2011-2014 / Gardanne, FR
Jury: Antoine Joux, Jean-Pierre Seifert (reviewers), Pierre-Alain Fouque, Jacques Fournier, Louis Goubin, Daniel Page

GRENOBLE-INP PHELMA / POLITO / EPFL
Engineering Degree
International Master in Nanotech Physics and Microelectronics
2008-2011 / Grenoble (FR), Turin (IT), Lausanne (CH)

LANGUAGES

French and English

HOBBIES

Rink hockey, basketball, and saxophone.

PROFESSIONAL EXPERIENCE

INRIA-RBA | Postdoc then Research Engineer
2016-... / Rennes, FR
Research work in two main areas:
1) Physical attacks at the LHS in Rennes. Both observation attacks and fault injection attacks, targeting both microcontrollers and application processors.
2) Microarchitecture security. Countermeasures against emerging attacks: control flow integrity, mitigation of covert and side channels, countermeasures against speculative attacks, ...

SECURE-IC | Research Engineer
2014-2016 / Rennes, FR
Development and use of physical security evaluation platforms. Design of electronic circuits, VHDL IPs, and software platform development.

CEA/UVSQ | PhD in Computer Science/Cryptography: "Security Analysis of Pairing-Based Implementations"
2011-2014 / Gardanne, FR
Supervisors: Jacques Fournier (CEA-Tech/SAS), Louis Goubin (UVSQ)
Pairing-based algorithms enable certificate-free cryptographic schemes. This work demonstrated theoretical and practical vulnerability (via electromagnetic fault injection) of such algorithms to fault attacks.

CEA | Research Engineer (internship)
March – August 2011 / Gardanne, FR
Supervisor: Jacques Fournier
Development and evaluation of AES symmetric encryption IPs. Implementation of fault attacks and design of countermeasures.

UNIVERSITY OF PENNSYLVANIA | Research at Mechanical Engineering and Applied Mechanics (internship)
June – August 2010 / Philadelphia, US
Characterization work on the nano-aquarium: a device for observing solutes by TEM. Characterization and nanoscale simulations (experiments and COMSOL simulations).

SKILLS

SOFTWARE DEVELOPMENT
Experience in industrial, team-based software development. Software engineering techniques, Git workflow. Currently used languages: C, Rust, SpinalHDL, VHDL, Python; but I have used lots of other languages in the past.

COMPUTER SCIENCE AND MATHEMATICS
Microelectronics and security, microarchitecture design, computer architecture, embedded systems, information systems security, algorithms, 3D rendering, statistical data analysis, theoretical and applied cryptology, physical attacks.

ELECTRONICS, PHYSICS AND MATERIALS
Semiconductor physics, fabrication processes for micro and nano technologies, electronic circuit design.

Portfolio

SELECTED SCIENTIFIC PUBLICATIONS, ONLINE LIST

COSADE 2024 | Characterizing and Modeling Synchronous Clock-Glitch Fault Injection
Marotta A., Lashermes R., Bouffard G., Sentieys O., Dafali R.
Where we explain a new physical mechanism leading to faults.

JCEN 2024 | Generic SCARE: reverse engineering without knowing the algorithm nor the machine
Lashermes R., Le Bouder H.
Where we show that knowing the inputs and outputs of a symmetric encryption algorithm, combined with an execution trace such as a power consumption measurement, is enough for an attacker to clone the algorithm.

CARDIS 2021 | Under the dome: preventing hardware timing information leakage
Escouteloup M., Lashermes R., Fournier J., Lanet J.L.
Where we design a microarchitecture preventing information leakage through covert channels.

JCEN 2021 | Electromagnetic fault injection against a complex CPU, new microarchitectural fault models
Trouchkine T., Bukasa K., Escouteloup M., Lashermes R., Bouffard G.
Where we explore how electromagnetic fault injection interacts with a complex System-on-Chip.

NORDSEC 2018 | Hardware-Assisted Program Execution Integrity: HAPEI
Lashermes R., Le Bouder H., Thomas G.
Where we propose a new Instruction Set Randomization scheme to ensure execution integrity on microcontrollers.

CHES 2013 | Inverting the Final Exponentiation of Tate Pairings on Ordinary Elliptic Curves Using Faults
Lashermes R., Fournier J., Goubin L.
Where we demonstrate that it is possible to recover the preimage of the final exponentiation, a surjective algorithm, using fault injection attacks.

SIDE PROJECTS

These are side projects that showcase skills beyond my main professional role.

BIBLIOGRAPHIC MONITORING APPLICATION

Personal productivity app for continuous monitoring of new academic publications. Uses Electron + Svelte.

LOCAL AI ASSISTANT FOR AUTOMATIC EMAIL REPLIES

Personal Thunderbird extension to write automatic replies to incoming emails, as a demonstrator to evaluate the technology. Uses llama.cpp as a server + prompt engineering + JavaScript.

HARDWARE SECURITY COURSE

Responsible for the advanced hardware security course unit at the University of Rennes, with minor contributions at CentraleSupélec and IMT-Atlantique. Created a course handbook (French), labs, etc.

PHYSICAL ATTACKS MOOC

Created a MOOC on physical attacks available on FUN (French).

DACTYL KEYBOARD

Personal project building an ergonomic keyboard. 3D printing of an existing model, assembling the electronic circuit, and developing a custom Rust firmware.

ACCOUNTING APPLICATION FOR CO-OWNERSHIP

Personal productivity application as a volunteer syndic for managing the finances of a small co-ownership. Uses Tauri (Rust) + TypeScript + Svelte + Bulma.

WEBSITES

Occasional design of small static websites.
Examples: personal website, LHS Rennes website, ARSENE project website.