07.50.64.15.22
florian.duzes@cea.fr
www.linkedin.com/in/florian-duzes/
github.com/FloDarPie

Duzés Florian

Interests — I am interested in many topics I discovered during my studies: *Secure and safe implementation, Homomorphic encryption, Cryptanalysis, Side-channel security, Embedded software security and Post-Quantum Cryptography*

Skills

Algorithmic : Quantum Computing, algebra, complexity
Cryptology : McEliece, LWE, Kyber, Dilithium, AES, RSA, DES
Systems : Windows, Linux
Architectures : INTEL, ARM, RISC-V, shellcodes

Programming : Python, SageMath, C, Rust, LaTeX, OCaml, F*, Nix
Languages : English & Spanish - C1
Working : Team work, organized, curious, taking the initiative, autonomous

Working experiences

Engineer - assistant research **2025**
CEA list
– Enhancing symbolic binary analysis tool BINSEC. Design of pedagogical content, designing services and optimization for productivity.

Researcher in Security **2025**
INRIA Paris - Prosecco / CEA *5 months*
– Security against time side-channels attacks. Work with BINSEC over HACL*. Developed automation for analysis of security against compilers and architectures. Build of proof of concept CI for HACL*.

Students Presidencies **2022 - 2023**
Association Alea - Institute Champollion *12 months*
CFVU Institute Champollion *12 months*
Student Council Institute Champollion *12 months*

Youth Animation - Center Director **2017 - 2024**
Éclaireuses et éclaireurs de France (EEDF, secular scoutism) - benevolent *7 years*
Wakanga - director in 2024 *3 years*

Early labor eperiences **2015 - 2024**

Education

Master's degree - Cryptology and Computer Security **2025**
Focus : Post-Quantum Cryptography, Arithmetic algorithms, Cryptanalysis, Side channels attacks, System Security
University of Bordeaux

Bachelor's degree - Computer Science **2022**
Focus : Artificial intelligence
National University Institute Jean-François Champollion

Various projects

Research works, projects and internships **2019 - 2025**
– Generalized timing side-channel detection on HACL* using BINSEC - *Project* . *Presentation*
– Side-channel attack on ECDSA by lattice simplification, programmed in SageMath - *Presentation*
– Complete introduction (state of the art) to PRNG - Article
– Study of Paillier cryptosystem and application on message application, implemented in C - *Archive*
– Study of humans habits and reaction to disturb AI, programed in Python - *Restricted*
– Simplified C Compiler in OCaml - *Usable artefact*

Global Game Jam - 2020/2021/2022/2023/2024 **2020 - 2024**
– Creativity and experiences in differents gaming developpements aspects, roles and technologies.

Nuit de l'info - Passage Python **2019 - 2021**
– Some awards for the team's solutions

Hobbies

Gastronomie **Cinema** **Sports** *Tennis, Taekwondo, VTT* **Reading** *Hyperion, The Belgariad, Knights of Emerald*