XABIER LEGASPI, PHD

Embedded Software Engineer

@ mailto:xlegaspij@protonmail.ch   EU Citizen

SKILLS

Programming

C | C++ | Python | Fortran (familiar) | Rust (familiar)

Embedded

ARM Cortex-M | STM32 | RTOS | Embedded Linux | VHDL/Verilog (familiar)

Security

Cryptography | Threat Models | Docker/Ansible (familiar)

DSP/SDR

DSP Algorithms | GNU Radio | HackRF

LANGUAGES

Spanish	●●●●●
Galician	●●●●●
English (C1)	●●●●○
French (B2)	●●●○○
German (A2)	●○○○○

AWARDS

Postdoctoral Fellowship
CREACH LABS / DGA Maîtrise de l'information (2023)

Predoctoral Fellowship
Spanish State Research Agency (2019)

SUMMARY

Embedded Software Engineer (PhD, MSc Cybersecurity) with expertise in secure firmware, cryptography, DSP, and embedded systems (ARM Cortex-M, RTOS, Embedded Linux). Experienced in aerospace/defense R&D bridging software, hardware, and applied cryptography.

EXPERIENCE

Postdoctoral Researcher – Embedded Systems Security

Université de Rennes - DGA Maîtrise de l'information

Oct 2024 – Present   Rennes, France

- **SCI3D project:** securing the additive manufacturing chain (design, slicing, printing).
- Conducted **white-box analysis of Klipper firmware**, identifying vulnerabilities in 3D printing.
- Developed a **C++ tool** to reconstruct 3D geometry from CAN/UART/USB data, proving feasibility of sniffing attacks.
- Proposed defenses: **AES-GCM-AEAD** for CAN communication, **ARM TrustZone** secure boot.
- Collaborated across disciplines: firmware, RF systems, applied cryptography.

Predoctoral Researcher – Mathematics (Algebra & Geometry)

Universidad Complutense de Madrid - CSIC

2019 – 2023 Madrid, Spain

- Specialized in **geometric group theory**, publishing results in hyperbolic groups and small cancellation theory.
- Invited speaker at international institutions (Bilbao, Bristol, Paris, Warwick, etc.).
- Research stays in Montréal, Oxford, Paris, and Vienna.
- Teaching Assistant for undergraduate mathematics.

Research Internships – Data Science & HPC

CiTIUS & CESGA

2016 – 2017 Santiago de Compostela, Spain

- Data-to-Text generation for social networks (CiTIUS), applying NLG and graph analysis.
- HPC-based sensitivity analysis of marine ecosystem models (CESGA) using R, Monte Carlo, Dakota, Open-TURNS on FinisTerrae2.

PROJECTS

[1] **Automotive Key Fob Security Analysis.** Reverse-engineered LPD433 RF signals with HackRF One; demodulated with *Inspectrum*/*GNU Radio*; decoded Manchester in Python; emulated transmissions with GNU Radio for controlled testing.

[2] **Shor's Algorithm (MSc Thesis).** Studied quantum algorithms, focusing on integer factorization. Highlighted impact on RSA cryptography and computational complexity.

EDUCATION

MSc in Cybersecurity (Software & Hardware Security)

Université de Rennes

2023–2024 France

PhD in Mathematics (Algebra & Geometry, Cotutelle)

Univ. Santiago de Compostela / Univ. de Rennes

2019–2023 Spain/France

MSc in Mathematics, Cryptography minor

Univ. de Santiago de Compostela

2017–2019 Spain

BSc in Mathematics

Univ. de Santiago de Compostela

2013–2017 Spain

RESEARCH PUBLICATIONS (SELECTED)

[1] Growth of quasi-convex subgroups in groups with a constricting element, *Groups Geom. Dyn.* 18 (2024).

[2] Uniform growth in small cancellation groups, submitted (2024), arXiv:2405.14387.