Alin-Petru Rosu

rosualinpetru@gmail.com | linkedin.com/in/rosualinpetru | github.com/rosualinpetru | +34 699 486 098 | Madrid, Spain

Summary

Cybersecurity engineer with a strong software development background, specialising in cryptography and PKI. Bridging hands-on engineering and research. Delivered satellite ground-segment cryptographic services and open-source privacy-preserving libraries, while contributing to applied cryptography research. Author of three double-blind peer-reviewed papers and two awards, with work spanning space PKI and privacy-preserving data sharing on blockchain. Motivated to explore cryptography and privacy, especially in critical infrastructure, with a drive for continuous learning, and operating autonomously while thriving in collaborative team environments.

Experience

Cryptography Research Software Engineer – Verifiable FHE 06/2026 – Present
IMDEA Software Institute *Madrid, Spain*

- **Stack**: *C, Python, CKKS, SNARKs, CPU Intrinsics*
- Designed and implemented an open-source library for verifiable **CKKS** homomorphic encryption with **SNARKs**.
- Optimised performance-critical polynomial arithmetic using **CPU intrinsics** and profiling-guided tuning.
- Developed a **machine learning PoC** for end-to-end verifiable inference over encrypted data.
- Versioned and deployed library releases to GitHub and PyPI in close collaboration with the research team.

Cybersecurity Software Engineer – Satellite Ground Segment Cryptography 08/2025 – 03/2026
European Space Agency *(via Telespazio Belgium)* *Noordwijk, The Netherlands*

- **Stack**: *Java, Scala, C++, JCE, Bouncy Castle, OpenSSL, PKCS#11, XMSS, EJBCA, Docker*
- Owned the design and implementation of a **ground segment service exposing** 27 **cryptographic functions** over UDP, including encryption, signatures, hashing, key derivation, PKI, and a hybrid key negotiation protocol.
- Implemented **key management for stateful hash-based signatures** using BKS keystores and HSM.
- Proposed and integrated a **self-hosted *EJBCA* PKI** via REST API, halving custom PKI development time.

Cybersecurity Intern – Public Key Infrastructure 10/2024 – 07/2025
European Space Agency *Noordwijk, The Netherlands*

- **Stack**: *C++, OpenSSL, ML-KEM, ML-DSA, X.509, DER, C509, CBOR*
- Researched **post-quantum certificate formats** for constrained and interoperable space PKI deployments.
- Designed the **first open-source tool for composite *C509***, supporting lattice-based cryptography with *ECC*.
- Demonstrated that *CBOR CRLs* reduce size by 55% at 1k entries, quantifying DER encoding overhead at scale.
- Proposed *SCVP* for federated space PKI validation, leading to an **invitation for in-orbit experimentation**.

Cybersecurity Research Assistant – Privacy-Preserving Blockchain 05/2024 – 09/2024
Delft University of Technology *Delft, The Netherlands*

- **Stack**: *Hyperledger Fabric, Java, Spring Boot, Protobuf, Docker, Privacy-Enhancing Technologies*
- Coordinated a team of four and **took full technical ownership** of a platform for medical device data research.
- Designed a permissioned *Hyperledger Fabric* network with end-to-end TLS, delivering a **prototype in 4 weeks**.
- Implemented privacy-preserving smart-contract queries using *threshold Paillier homomorphic encryption*, *ε-differential privacy*, and *integer linear programming*, enabling grouped counting without per-record decryption.
- Received **Best Demo Award** and integrated into the EU-funded *SEPTON* initiative as a candidate architecture.

Backend Software Engineer – Payments Processing 08/2022 – 07/2023
ING Bank *Bucharest, Romania*

- **Stack**: *Scala*, *Typelevel*, *Cats-Effect*, *Akka Streams*
- Developed ISO 20022 instant payment systems, **sustaining 90+ transactions per second**.
- Delivered features and resolved bugs in a 10+ developer agile team, onboarding three engineers to full autonomy.
- Developed REST/HTTP integrations with external anti-money laundering and automated clearing house services.

Cloud DevOps Engineer 11/2021 – 07/2022
The Lindau Nobel Laureate Meetings *(via BusyMachines)* *Germany (Remote)*

- **Stack**: *AWS (VPC, EC2, RDS, ECS, ELB, S3, EFS, IAM), GitLab, Jitsi*
- **Owned cloud infrastructure and CI/CD** for a production mentoring hub and videoconferencing platform.
- Designed and operated cloud networking, compute, storage, and databases, and configured self-hosted *Jitsi Meet*.
- Proposed and configured self-hosted *GitLab Runners* to eliminate compute-minute limits and reduce CI/CD costs.

DevOps Engineer 09/2020 – 10/2021
BioCopy AG *(via BusyMachines)* *Germany (Remote)*

- **Stack**: *Bash, Nix, Docker Swarm, Prometheus, PostgreSQL, MinIO, ELK*

- **Owned the on-premises software platform** for a large-scale bioinformatics experiment-processing system.
- Operated a 15+ node *Docker Swarm* cluster across Windows and Linux for core, storage, and monitoring services.
- Developed deployment scripts, and configured packaging and container registries for cluster updates and releases.
- Retained as consultant after project completion to ensure production stability and maintenance until 01/2024.

Backend Software Engineer 06/2020 – 07/2022
BusyMachines *Timisoara, Romania*

- **Stack**: *Java*, *Spring Boot*, *Scala*, *Typelevel*, *Cats-Effect*
- Developed and maintained internal development tools and backend services across multiple client projects.

Education

Delft University of Technology Delft, The Netherlands
MSc Computer Science, Cybersecurity (GPA: 8.7/10, Cum Laude) *08/2023 – 07/2025*

- **Teaching Assistant**: Compiler Construction, Computer Security
- **Coursework**: Security and Cryptography, Privacy-Enhancing Technologies, Blockchain Engineering

Politehnica University of Timisoara Timisoara, Romania
MEng Software Engineering (GPA: 9.5/10) *08/2022 – 07/2023*

- **Teaching Assistant**: Object-Oriented Programming, Functional Programming

Politehnica University of Timisoara Timisoara, Romania
BEng Computer and Information Technology (GPA: 9.66/10) *08/2018 – 07/2022*

Projects

ers *(Encrypted Range Search)* | **Stack**: *Python* 10/2024 – 01/2025

- Implemented encrypted range search schemes using Hilbert curves for multi-dimensional query processing.
- Evaluated algorithmic trade-offs via synthetic benchmarks, building practical intuition for applied cryptography.

jFamilyCounselor | **Stack**: *Java, Eclipse JDT* 08/2022 – 08/2023

- Designed and implemented static analysis metrics and tooling to detect hidden familial type correlations in Java.
- Published work awarded **Best Paper at an academic conference**.

Additional Information

Publications: *https://orcid.org/0009-0005-8537-7265*
Selected Presentations & Talks:

- Panellist, *Romanian Space Initiative International*, 11/2025
- Presenter, *Security for Space Systems Conference*, 11/2025
- Presenter, *CCSDS Spring Meeting*, 05/2025

Volunteering & Mentorship:

- Managed a C coding club of 30 primary school students between 10/2019 - 10/2020.

Languages: English (C1), Spanish (B1), German (B1)