Matteo **Steinbach**

Cryptography Researcher · Cybersecurity Engineer · Bsc in Computer Science

Luxembourg

matteo.steinbach.pro@gmail.com | mattc-try | matteo-steinbach

Summary

I hold a Bachelor's degree in Computer Science from the University of Luxembourg, where I specialized in cybersecurity and cryptography with distinction very good and conducted research leading to **2 peer reviewed cryptography papers during my studies**. My background spans both classical and post-quantum cryptography, including public- and private-key systems as well as the optimization of cryptographic algorithms on constrained devices such as microcontrollers.

I am currently employed as a Cryptography R&D Engineer. In this role, I contribute in european research projects to the design of quantum-resistant secure communication systems. In parallel I am still collaborating on academic research.

Skills

Cryptography	Classic and Post Quantum, Kyber, Dilithium, Falcon, Hawk, RSA, AES, DSA, ECC, Curve25519, openssl
Cybersecurity	Vulnerabilities, Scripting, Kali Linux, Nmap, Wireshark, Burp Suite, Hydra
Software Engineering	Agile Methodologies, Git, Continuous Integration/Continuous Deployment (CI/CD)
Programming	C/C++, Python, Java, Bash, Assembly, Rust, JavaScript, Go, Haskell, LaTeX, Web Dev
Languages	French(Nat), Italian(Nat), English(C2), Spanish (B1), German(A2)

Experience

Integrasys Group
Kirchberg, Luxembourg

R&D Cryptography — *Sep. 2025 - today*

- Conducting research work and participating on multiple european funded projects
- Public Key Infrastructure
- Post Quantum Cryptography
- Key Combinations
- Lightweight cryptography on custom embedded devices, custom ISA instructions

Integrasys Group, partnering with the university of luxembourg APSIA research group of prof. Peter Ryan
Kirchberg, Luxembourg

Cryptography Researcher/Engineer — *Feb. 2025 - Aug. 2025*

- Lightweight cryptography
- Post Quantum Cryptography
- Hybrid Scheme

SnT Security and Trust, (Prof.Johann Grozchadl/Peter Roenne)
Belval, Luxembourg

Security Researcher — *Aug. 2024 - Feb. 2025*

- Researched and Learned cryptographic software testing paradigms
- This research conducted during student researcher position and bachelor led to 2 peer reviewed academic papers at international crypto conferences SPACE2025, SECITC
- Compiled a database of Hard-To-Find bugs, very subtle cryptography bugs and studied them
- Implemented whycheproof(google) crypto testing library in C, for openssl testing
- Introduced new Cryptographic very subtle bugs

SnT Security and Trust, University of Luxembourg
Belval, Luxembourg

Part Time Student Researcher — *Oct. 2023 - Jan. 2024*

- Worked with a microcontroller STM23F40 for cryptography testing purposes
- Optimized the ntt of crystals-kyber the post quantum cryptography algorithm using assembly components, and parallelization
- Implemented a fast NTT Number Theoretical Transform

Summer Job, Royal Agency, BGL BNP Paribas
Kirchberg, Luxembourg

Account Manager — *Aug. 2022 - Sept. 2022*

- Worked on my communication skills with all sorts of customers in all my known languages.
- Performed support and banking actions for clients, Web Banking.

Summer Job, IT, BGL BNP Paribas
Kirchberg, Luxembourg

Software Engineer Intern — *July. 2021 - Aug. 2021*

- Checked the format of administration tables for internal software.
- Implemented a script allowing seamless key formatting for virtual machines access

Education

University of Luxembourg
Belval, Luxembourg

B.S. in Computer Science — *Sept. 2022 - Aug. 2025*

- Focus on cryptography, cybersecurity, computer architechtures, and low level algorithm optimization
- Key courses: Cryptography Testing Paradigms, Post Quantum Fast NTT, CyberSecurity, Maths, Data Structures
- Led to 2 peer reviewed academic papers in cyber/crypto conferences SPACE2025, SECITC

Politecnico di Milano, Echange
Milano, Italy

B.S/(M.S) in Computer Science — *Feb. 2024 - Sept. 2024*

- Advanced Computer Architechtures and Cryptography and Architechtures for Computer Security, Master Courses
- Deepened my knowledge in cryptography and built stronger mathematical/engineering basis

Schola Europea Luxembourg 1
Kirchberg, Luxembourg

European Baccalaureate — *Sept. 2015 - July. 2022*

- Advanced Mathematics, Chemistry, Physics, ICT

Extracurricular Activity

Scientific Research Readings

Security Research — *2021 - Present*

- Cryptography.
- Pen Testing techniques.
- CyberSecurity Vulnerabilities.

Implementation of a complete depense in depth crypto testing library

Cryptography Tester/Researcher — *2024 – Present*

- Full Know Answers Tests KATs suite targetting low occurence bugs in cryptographic implementation
- Verifying cryptographic libraries and implementations of cryptographic algorithms for bugs

Capture The Flag (PicoCTF and Hack The Box)

Penetration Tester — *2022 – Present*

- Regularly participated in solving challenges focused on cryptography, web exploitation, reverse engineering, and forensics.
- Enhanced practical skills in penetration testing and vulnerability analysis using tools like Burp Suite, Wireshark, and Nmap.
- Solved advanced cryptographic challenges, including real-world attack scenarios.

Full Rust Oauth implementation

Cybersecurity Engineer — *2025*

- Implemented a full oauth2 implementation in rust compatible with google and more
- https://github.com/mattc-try/rust-google-oauth2

PyNetPwn (Penetration Testing Software)

Software/Security Engineer — *2024*

- Designed and implemented PyNetPwn, a Python-based tool for automating network penetration testing tasks.
- Integrated modules for scanning, exploiting, and reporting vulnerabilities in target networks.
- Developed a user-friendly command-line interface to streamline penetration testing workflows.

Lys/portfolio Website

Web Developer — *2022*

- Built a shop/portfolio website (not currently online)
- Pen tested my own website

Progression Mobile App

Software Engineer — *2023*

- Built a SwiftUI app using MVVM.
- Google Firebase Database management.