Reinhard **Lüftenegger**

CRYPTOGRAPHY RESEARCHER AND ENGINEER

Graz, Austria

rluft@pm.me | remalue.github.io

Academic Education

Nov 2019 - Nov 2023 **PhD, Applied Cryptography & Privacy** - with highest honors — Graz, Austria

GRAZ UNIVERSITY OF TECHNOLOGY

Thesis: Algebraic Analysis of Arithmetization-Friendly Cryptographic Primitives; supervised by Prof. Christian Rechberger, assessed by Prof. Anne Canteaut.
I researched symmetric cryptography, in particular the design and analysis of cryptographic primitives for MPC, FHE, and ZKP.

Oct 2013 - Aug 2017 **MSc, Mathematics** - with highest honors — Salzburg, Austria

PARIS LODRON UNIVERSITY OF SALZBURG

Thesis: Quaternions and Rotations.
I specialized in algebra and physics, and implemented selected cryptographical applications of quaternions in Python. During my Master's studies I worked as freelance Java software developer for a payment service provider.

Oct 2010 - Oct 2013 **BSc, Mathematics** - with highest honors — Salzburg, Austria

PARIS LODRON UNIVERSITY OF SALZBURG

Thesis: Hilbert Spaces and the Lebesgue Measure.

Professional Experience

May 2024 - Sep 2024 **Bikepacker** — South America

INDEPENDENT

I ventured to traverse the Andes mountains by bike and crossed Chile, Argentina, Bolivia, Peru and Colombia on my way from south to north.

Jan 2024 - May 2024 **Post-Doctoral Researcher** — Graz, Austria

GRAZ UNIVERSITY OF TECHNOLOGY

Besides continuing to work on my doctoral research topics, I co-organized a 3-day scientific workshop, and worked on a joint research grant proposal.

Nov 2019 - Nov 2023 **Doctoral Researcher** — Graz, Austria

GRAZ UNIVERSITY OF TECHNOLOGY

I co-designed the arithmetization-friendly hash functions Reinforced Conrete and Monolith, and the cryptographic permutation Hades which underlies the Poseidon hash function.
Every winter term, I taught algebra, elliptic curves, and symmetric cryptography at Master's level.

Nov 2017 - Nov 2019 **University Project Assistant** — Graz, Austria

GRAZ UNIVERSITY OF TECHNOLOGY

I implemented cryptographic algorithms in Java during my participation in an EU Horizon 2020 research project; with a focus on the verification of digital signatures.

Jul 2013 - Jul 2014 **Java Software Developer** — Salzburg, Austria

HOBEX AG

I implemented a serial communication protocol to connect point-of-sale and electronic-cash payment terminals in Java, with minor work in C#. Furthermore, I worked on a simulator for virtualizing electronic-cash payment terminals.

Skills

Languages	German (native), English (fluent), Spanish (advanced), French (beginner)
Programming	Rust (PoC), Python (advanced), HTML/CSS/JS (basic), Java (basic)
CAS	SageMath, Magma, Mathematica
Cryptography	Research knowledge about the analysis and design of cryptographic permutations, block ciphers, and hash functions
Mathematics	Deep knowledge of the mathematical foundations of cryptography, in particular higher algebra (groups, rings, fields, homomorphisms), elliptic curves, boolean functions, polynomials and solving systems of polynomial equations
Leadership	Teaching university courses at Bachelor's and Master's level, supervising Master's students, taking the lead in writing jointly-authored scientific articles
Soft Skills	Passionate, enthusiastic, creative, driven by excellence, self-motivated, reflective, open-minded, team-oriented

Honours, Awards & Activities

2024 **Promotio sub auspiciis praesidentis rei publicae**
Highest possible distinction for outstanding academic achievements by the Republic of Austria

2024 **Finalist, Award for dissertations with extraordinary societal relevance**
University-wide 6 finalists per year, Panel for Technology and Society, Austria

2024 **Nominee, Heinz-Zemanek award for outstanding dissertations in computer science**
University-wide 2 nominees per year, Graz University of Technology, Austria

2024 **Participant, Klartext award for scientific communication**
Klaus Tschira Foundation, Germany

2017 **Academic excellence grant, MSc**
Paris Lodron University of Salzburg, Austria

2013 **Academic excellence grant, BSc**
Paris Lodron University of Salzburg, Austria

Research

I published my research at several top-tier (A, A*) peer-reviewed conferences. For a list of my publications please see `https://dblp.org/pid/240/8228.html`.