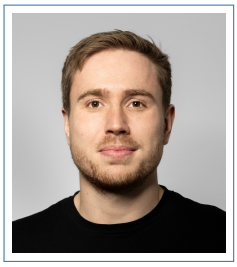

Roman Walch

Curriculum Vitae

Experience

2023– **Co-Founder, Lead Cryptographer**, *TACEO*, Graz, Austria
Conducting research in privacy enhancing technologies (HE/MPC/ZK). Design and implementation of cryptographic software solutions.

2022–2023 **Co-Founder, Cryptographer**, *TACEO*, Graz, Austria
Part Time

2022–2023 **Researcher**, *Know-Center GmbH*, Graz, Austria
Part Time

2019–2022 **Researcher**, *Know-Center GmbH*, Graz, Austria
Researching privacy enhancing cryptographic protocols and primitives, such as Secure Multiparty Computation (MPC) and Fully Homomorphic Encryption (FHE), and their applications.

Miscellaneous

2014 **Community Service**, *Austrian Red Cross*, Telfs, Austria
Paramedic

2013–2014 **IT Support**, *Physiotherm GmbH*, Thaur, Austria
Part Time

Teaching

2019–2023 **Lecturer**, *University of Technology*, Graz, Austria
Courses: IT Security, Privacy Enhancing Technologies, Modern Public Key Cryptography

2016–2019 **Teaching Assistant**, *University of Technology*, Graz, Austria
Courses: Calculus I, Introduction to Programming (C), Software Developement (C++), Real Time Operating Systems, Information Security

Education

2019–2024 **Doctoral Programme (PhD) in Computer Science**, *University of Technology*, Graz, Austria
Passed with distinction
Supervisor: Univ.-Prof. Christian Rechberger

2017–2019 **MSc in Information and Computer Engineering**, *University of Technology*, Graz, Austria
Passed with distinction
Major: Secure and Correct Systems
Minor: Embedded and Automotive Systems

2014–2017 **BSc in Information and Computer Engineering**, *University of Technology*, Graz, Austria
Passed with distintion

2008–2013 **Matura**, *HTBLVA Anichstraße*, Innsbruck, Austria
Passed with distintion
Electrical Engineering

Languages

German **Mother-tongue**
English **Advanced** *Conversationally fluent, able to understand and create scientific documents*

Technological skills

Coding C, C++, Rust, Python, Sage, LaTeX, VHDL, Assembly
OS Linux, Microsoft Windows

Interests

- Member of TU Graz CTF team LosFuzzys (https://hack.more.systems)
- Running, Hiking

Doctoral Thesis

Title *Improving Efficient Computation on Private Data*
Supervisors Univ.-Prof. Christian Rechberger
Description In this thesis we continue research on efficient privacy enhancing technology (PET) use cases and building blocks. Concretely, we propose protocols which have the potential to contribute to solving real world problems, such as combining health and location data efficiently to help the containment of the spread of infectious diseases while ensuring the privacy of all involved datasets. Furthermore, we propose new symmetric ciphers, dubbed Pasta and Hydra, optimized for fast encryption when used in combination with homomorphic encryption (HE) and secure multi-party computation (MPC). Then we propose the new hash function Monolith which is especially suited for fast hashing in common zero knowledge (ZK) use cases. Finally, we also investigate alternative solutions to replace Merkle trees, a common building block in ZK applications, with novel MPC-based public key accumulators to gain more efficiency.

Master Thesis

Title *Design and Implementation of a Picnic Coprocessor*
Supervisors Univ.-Prof. Christian Rechberger, Dipl.-Ing. Daniel Kales, Dipl.-Ing Mario Werner
Description In this thesis I developed efficient VHDL-based FPGA implementations of the block cipher LowMC and the post-quantum signature scheme Picnic.

Conference/Journal Publications

Note: The standard convention in this discipline is to list the authors in alphabetical order.

[1] Alexandros Bampoulidis, Alessandro Bruni, Lukas Helminger, Daniel Kales, Christian Rechberger, and Roman Walch. "Privately Connecting Mobility to Infectious Diseases via Applied Cryptography". In: *Proc. Priv. Enhancing Technol.* 2022.4 (2022), pp. 768–788.

[2] Remco Bloemen, Bryan Gillespie, Daniel Kales, Philipp Sippl, and Roman Walch. "Large-Scale MPC: Scaling Private Iris Code Uniqueness Checks to Millions of Users". In: *IACR Cryptol. ePrint Arch.* (2024), p. 705.

[3] Christoph Dobraunig, Lorenzo Grassi, Lukas Helminger, Christian Rechberger, Markus Schofnegger, and Roman Walch. "Pasta: A Case for Hybrid Homomorphic Encryption". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2023.3 (2023), pp. 30–73.

[4] Lorenzo Grassi, Yonglin Hao, Christian Rechberger, Markus Schofnegger, Roman Walch, and Qingju Wang. "Horst Meets Fluid-SPN: Griffin for Zero-Knowledge Applications". In: *CRYPTO (3)*. Vol. 14083. Lecture Notes in Computer Science. Springer, 2023, pp. 573–606.

[5] Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, Markus Schofnegger, and Roman Walch. "Monolith: Circuit-Friendly Hash Functions with New Nonlinear Layers for Fast and Constant-Time Implementations". In: *IACR Trans. Symmetric Cryptol.* 2024.3 (2024), pp. 44–83.

[6] Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, Markus Schofnegger, and Roman Walch. "Reinforced Concrete: A Fast Hash Function for Verifiable Computation". In: *CCS*. ACM, 2022, pp. 1323–1335.

[7] Lorenzo Grassi, Fukang Liu, Christian Rechberger, Fabian Schmid, and Roman Walch. "Minimize the Randomness in Rasta-Like Designs: How Far Can We Go? — Application to Pasta." In: *Selected Areas in Cryptography*. IACR. Montreal, Quebec, Canada, Aug. 2024.

[8] Lorenzo Grassi, Morten Øygarden, Markus Schofnegger, and Roman Walch. "From Farfalle to Megafono via Ciminion: The PRF Hydra for MPC Applications". In: *EUROCRYPT (4)*. Vol. 14007. Lecture Notes in Computer Science. Springer, 2023, pp. 255–286.

[9] Lukas Helminger, Daniel Kales, Sebastian Ramacher, and Roman Walch. "Multi-party Revocation in Sovrin: Performance through Distributed Trust". In: *CT-RSA*. Vol. 12704. Lecture Notes in Computer Science. Springer, 2021, pp. 527–551.

[10] Daniel Kales, Sebastian Ramacher, Christian Rechberger, Roman Walch, and Mario Werner. "Efficient FPGA Implementations of LowMC and Picnic". In: *CT-RSA*. Vol. 12006. Lecture Notes in Computer Science. Springer, 2020, pp. 417–441.

[11] Shibam Mukherjee, Roman Walch, Fredrik Meisingseth, Elisabeth Lex, and Christian Rechberger. "Hiding Your Awful Online Choices Made More Efficient and Secure: A New Privacy-Aware Recommender System". In: *SEC*. Vol. 710. IFIP Advances in Information and Communication Technology. Springer, 2024, pp. 353–366.

[12] Christian Rechberger and Roman Walch. "Privacy-Preserving Machine Learning Using Cryptography". In: *Security and Artificial Intelligence*. 2022, pp. 109–129.

[13] Roman Walch, Samuel Sousa, Lukas Helminger, Stefanie N. Lindstaedt, Christian Rechberger, and Andreas Trügler. "CryptoTL: Private, efficient and secure transfer learning". In: *CoRR* abs/2205.11935 (2022).