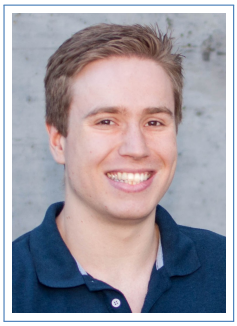

Roman Walch

Curriculum Vitae

Education

2019– **Doctoral Programme in Computer Science**, *University of Technology*, Graz.
Supervisor: Univ.-Prof. Christian Rechberger

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

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

2008–2013 **Secondary Technical College**, *HTBLVA Anichstraße*, Innsbruck, Passed with distintion.
Electrical Engineering

Experience

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

2016–2019 **Teaching Assistant**, *TU Graz*, Graz.
Courses include: Mathematics, Programming (C/C++), Real Time Operating Systems, Information Security

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

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

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

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.

Conferences / Journal Publications

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

[1] Alessandro Bruni, Lukas Helminger, Daniel Kales, Christian Rechberger, and Roman Walch. Privately connecting mobility to infectious diseases via applied cryptography. *IACR Cryptol. ePrint Arch.*, 2020:522, 2020.

[2] Lukas Helminger, Daniel Kales, Sebastian Ramacher, and Roman Walch. Multi-party revocation in sovrin: Performance through distributed trust. *IACR Cryptol. ePrint Arch.*, 2020:724, 2020.

[3] Daniel Kales, Sebastian Ramacher, Christian Rechberger, Roman Walch, and Mario Werner. Efficient FPGA implementations of lowmc and picnic. In *CT-RSA*, volume 12006 of *Lecture Notes in Computer Science*, pages 417–441. Springer, 2020.