Markus Schofnegger

Curriculum Vitae

Education

2018–2022 **Doctoral Program in Computer Science**, *University of Technology*, Graz.
Supervisor: Prof. Christian Rechberger

2015–2018 **Master of Computer Science**, *University of Technology*, Graz.
Major: Information Security
Minor: Software Technology

2012–2015 **Bachelor of Computer Science**, *University of Technology*, Graz.

2003–2011 **Secondary School**, *BRG Klagenfurt-Viktring*, Klagenfurt, Emphasis on Musical Education.

1999–2011 **Piano Education**, *Musikschule Klagenfurt*, Klagenfurt.

Experience

since 2022 **Cryptographer**, *Horizen Labs*, Milan.
Zero-Knowledge Protocols

2018–2022 **Researcher**, *IAIK, Graz University of Technology*, Graz.
Symmetric Cryptography

Lecturer, *IAIK, Graz University of Technology*, Graz.
Courses include: Cryptography, Cryptanalysis, IT Security, Privacy-Enhancing Technologies

2014–2018 **Teaching Assistant**, *Graz University of Technology*, Graz.
Courses include: Design and Analysis of Algorithms, Enumerative Combinatoric Algorithms, Human-Computer Interaction

2011-2012 **Community Service**, *Lebenshilfe Österreich*, Klagenfurt.

Languages

German **Mother tongue**

Italian **Mother tongue**

English **Advanced** *Conversationally fluent, able to understand and create scientific documents*

French **Elementary**

Technological Skills

Coding C, C++, Python, Sage, Rust, Lua, Java, LaTeX

OS Linux, Microsoft Windows, Mac OS

Interests

Music I am a passionate listener of music of many genres, and I am playing the piano myself.

Photography Photography has started to become one of my leisure activities recently.

Master Thesis

Title *Implementing and Optimizing Lightweight Block Ciphers in the Context of a Signature Scheme*

Supervisors Prof. Christian Rechberger, Dipl.-Ing. Dr.techn. Sebastian Ramacher

Description In this thesis I implemented various cryptographic primitives in the context of a post-quantum signature scheme. The main focus was to increase the efficiency of these implementations.

Doctoral Thesis

Title *Design and Analysis of Arithmetization-Oriented Cryptographic Primitives*

Assessors Prof. Christian Rechberger, Prof. Tyge Tiessen

Description This thesis explores the area of symmetric cryptographic primitives optimized for zero-knowledge and multi-party computation use cases.

Conference / Journal Publications

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

[1] Martin R. Albrecht, Carlos Cid, Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, and Markus Schofnegger. Algebraic Cryptanalysis of STARK-Friendly Designs: Application to MARVELlous and MiMC. In *ASIACRYPT (3)*, volume 11923 of *LNCS*, pages 371–397. Springer, 2019.

[2] Martin R. Albrecht, Lorenzo Grassi, Léo Perrin, Sebastian Ramacher, Christian Rechberger, Dragos Rotaru, Arnab Roy, and Markus Schofnegger. Feistel Structures for MPC, and More. In *ESORICS (2)*, volume 11736 of *LNCS*, pages 151–171. Springer, 2019.

[3] Carlos Cid, Lorenzo Grassi, Aldo Gunsing, Reinhard Lüftenegger, Christian Rechberger, and Markus Schofnegger. Influence of the Linear Layer on the Algebraic Degree in SP-Networks. *IACR Trans. Symmetric Cryptol.*, 2022(1), 2022.

[4] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Markus Schofnegger. Algebraic Cryptanalysis of Variants of Frit. In *SAC*, volume 11959 of *LNCS*, pages 149–170. Springer, 2019.

[5] Christoph Dobraunig, Daniel Kales, Christian Rechberger, Markus Schofnegger, and Greg Zaverucha. Shorter Signatures Based on Tailor-Made Minimalist Symmetric-Key Crypto. *IACR Cryptol. ePrint Arch.*, page 692, 2021. To appear at ACM CCS 2022.

[6] Orr Dunkelman, Maria Eichlseder, Daniel Kales, Nathan Keller, Gaëtan Leurent, and Markus Schofnegger. Practical key recovery attacks on FlexAEAD. *Des. Codes Cryptogr.*, 90(4):983–1007, 2022.

[7] Maria Eichlseder, Daniel Kales, and Markus Schofnegger. Forgery Attacks on FlexAE and FlexAEAD. In *IMACC*, volume 11929 of *LNCS*, pages 200–214. Springer, 2019.

[8] 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)*, volume 14083 of *Lecture Notes in Computer Science*, pages 573–606. Springer, 2023.

[9] Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, Markus Schofnegger, and Roman Walch. Reinforced Concrete: A Fast Hash Function for Verifiable Computation. *IACR Cryptol. ePrint Arch.*, page 1038, 2021. To appear at ACM CCS 2022.

[10] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. Poseidon: A New Hash Function for Zero-Knowledge Proof Systems. In *USENIX Security Symposium*. USENIX Association, 2021.

[11] Lorenzo Grassi, Dmitry Khovratovich, Sondre Rønjom, and Markus Schofnegger. The Legendre Symbol and the Modulo-2 Operator in Symmetric Schemes over GF$(p)^n$. *IACR Trans. Symmetric Cryptol.*, 2022(1), 2022.

[12] Lorenzo Grassi, Dmitry Khovratovich, and Markus Schofnegger. Poseidon2: A Faster Version of the Poseidon Hash Function. In *AFRICACRYPT*, Lecture Notes in Computer Science. Springer Nature Switzerland, 2023.

[13] Lorenzo Grassi, Reinhard Lüftenegger, Christian Rechberger, Dragos Rotaru, and Markus Schofnegger. On a Generalization of Substitution-Permutation Networks: The HADES Design Strategy. In *EUROCRYPT (2)*, volume 12106 of *LNCS*, pages 674–704. Springer, 2020.

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

[15] Lorenzo Grassi, Christian Rechberger, and Markus Schofnegger. Proving Resistance Against Infinitely Long Subspace Trails: How to Choose the Linear Layer. *IACR Trans. Symmetric Cryptol.*, 2021(2), 2021.

[16] Lorenzo Grassi and Markus Schofnegger. Mixture Integral Attacks on Reduced-Round AES with a Known/Secret S-Box. In *INDOCRYPT*, LNCS. Springer, 2020.

[17] Maria Eichlseder Lorenzo Grassi, Reinhard Lüftenegger, Morten Øygarden, Christian Rechberger, Markus Schofnegger, and Qingju Wang. An Algebraic Attack on Ciphers with Low-Degree Round Functions: Application to Full MiMC. In *ASIACRYPT (3)*, LNCS. Springer, 2020.