Simon-Philipp Merz

Applied Cryptography Group
ETH Zürich, Switzerland

research@simon-philipp.com
https://simon-philipp.com

Current position

Postdoctoral researcher in Applied Cryptography Group, ETH Zürich
Focus on cryptanalysis of post-quantum hardness assumptions and solving the challenges of deploying post-quantum protocols in practice.

Education

Royal Holloway, University of London, Oct 2018 - Jun 2023
PhD in Cryptography, Cryptanalysis and design of post-quantum cryptography with a special focus on isogeny-based cryptography

University of Oxford, Oct 2017 – Sept 2018 (Distinction)
MSc in "Mathematics and Foundations of Computer Science"
Thesis: *Cryptanalysis of WalnutDSA*

Imperial College London, Oct 2016 – Sept 2017 (Distinction)
MSc in "Pure Mathematics"
Thesis: *Fermat's Last Theorem for Regular Primes*

Free University of Berlin, Apr 2014 – Sept 2016 (grade average 1.0)
BSc in Mathematics, graduated top of year
Thesis: *Reproducing Kernel Hilbert Spaces*

Work Experience

Teaching assistant at Free University of Berlin (2015-2016)
Computational Mathematics and Scientific Computing

Research intern at IBM Research, Zurich (2022)
Foundations of Cryptography group under the guidance of Luca De Feo

Publications

Improved algorithms for finding fixed-degree isogenies between elliptic curves
Submitted, eprint 2023/1618
B. Benčina, P. Kutas, S.-P. Merz, C. Petit, M. Stopar, C. Weitkämper

Weak instances of class group action based cryptography via self-pairings
CRYPTO 2023, eprint 2023/549
W. Castryck, M. Houben, S.-P. Merz, M. Mula, S. van Buuren, F. Vercauteren

SCALLOP: Scaling the CSI-FiSh
PKC 2023, eprint 2023/058
L. De Feo, T.B. Fouotsa, P. Kutas, A. Leroux, S.-P. Merz, L. Panny, B. Wesolowski

On the Isogeny Problem with Torsion Point Information
PKC 2022, eprint 2021/153
T.B. Fouotsa, P. Kutas, S.-P. Merz, Y.B. Ti

Cryptanalysis of an oblivious PRF from supersingular isogenies
ASIACRYPT 2021, eprint 2021/706
A. Basso, P. Kutas, S.-P. Merz, C. Petit, A. Sanso

**One-way functions and malleability oracles:
Hidden shift attacks on isogeny-based protocols**
EUROCRYPT 2021, eprint 2021/282
P. Kutas, S.-P. Merz, C. Petit, C. Weitkämper

On Index Calculus Algorithms for Subfield Curves
SAC 2020, eprint 2020/1315
S.D. Galbraith, R. Granger, S.-P. Merz, C. Petit

On Adaptive Attacks against Jao-Urbanik's Isogeny-Based Protocol
AFRICACRYPT 2020, eprint 2020/244
A. Basso, P. Kutas, S.-P. Merz, C. Petit, C. Weitkämper

Another look at some isogeny hardness assumptions
CT-RSA 2020, eprint 2019/950
S.-P. Merz, R. Minko, C. Petit

Factoring Products of Braids via Garside Normal Form
PKC 2019, eprint 2018/1142
S.-P. Merz, C. Petit

Academic Responsibilities

Reviewing or Subreviewing
Conferences: Crypto 2019, Mathcrypt 2019, Africacrypt 2019, SAC 2019, IMACC 2019, ANTS 2020, Africacrypt 2020, PKC 2020, PKC 2021, PQCrypto 2021, Asiacrypt 2021, SAC 2021, IMACC 2021, ANCS 2022, Africacrypt 2022, ANTS 2022, Asiacrypt 2022, Eurocrypt 2023

Journals: Advances of Mathematics in Communications;
Applicable Algebra in Engineering, Communication and Computing;
Designs, Codes and Cryptography; IET Information Security

Grants and Awards

Exposé scholarship (2019)
by the German National Academic Foundation

EPSRC PhD scholarship (2018-2023)
by the Engineering and Physical Sciences Research Council (EPSRC) of the UK

Studienstiftung scholarship (2015-2018)
full scholarship by the German National Academic Foundation

BMG Graduation award (2016)
by the Berlin Mathematical Society for a remarkable Bachelor's thesis

MLP MINT Excellence award (2015)
by the MLP MINT Excellence network for student achievements

Languages and Skills

German (native), English (fluent), French (basic), Latin (basic)
LaTeX, Python, MAGMA