Simon-Philpp Merz

Royal Holloway, University of London
Information Security Group
Egham

simon-philipp.merz.2018@rhul.ac.uk

Education

Royal Holloway, University of London
PhD student in Information Security Group, Oct 2018 - now
Interests: Cryptology, Algorithmic number theory

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

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

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

Weinberg-Gymnasium Kleinmachnow
Abitur, Jun 2013 (final grade average 1.0 | graduated top of year)
Major field of study: Mathematics and Physics

Publications

On the Isogeny Problem with Torsion Point Information
B. Fouotsa Tako, P. Kutas, S.-P. Merz

One-way functions and malleability oracles:
Hidden shift attacks on isogeny-based protocols
To appear at Eurocrypt 2021
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

Teaching
Teaching assistant, Free University of Berling
Computational Mathematics and Scientific Computing, 2015-2016

Reviewing or Subreviewing
Conferences: Crypto 2019, Mathcrypt 2019, Africacrypt 2019, SAC 2019, IMACC 2019, ANTS 2020, Africacrypt 2020, PKC 2020, PKC 2021

Journals: Advances of Mathematics in Communications; Designs, Codes and Cryptography; IET Information Security

Grants and Awards

Exposé scholarship (2019)
by the German National Academic Foundation

EPSRC Ph.D. scholarship (2018-now)

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

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

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

DPG Graduation award (2013)
by German Physics Society for student achievements

Languages and Skills

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