Prof. Dr. Violetta Weger

Curriculum Vitae

Technical University of Munich
Departement of Mathematics
Theresienstrasse 90, 80333 Munich
Germany
violetta.weger@tum.de

Updated: August 14, 2025

Personal Information

Current Position: **Rudolf Mößbauer Tenure Track Assistant Professor for Applied Algebra**
in the Mathematics Department at the Technical University of Munich

Research Interests: Algebraic Coding Theory, Cryptography, Code-based Cryptography

Education

March, 2017- January, 2021 **Ph.D. in Mathematics**
at the University of Zurich
under the supervision of Prof. J. Rosenthal
Thesis: *Information Set Decoding in the Lee Metric and the Local to Global Principle for Densities*

2016- 2017 **Master in Mathematics**
University of Zurich
Thesis: *A Code-Based Cryptosystem using GRS codes*

2011 - 2016 **Bachelor in Mathematics**
University of Zurich

Previous Positions

September, 2022 - July 2024 **Marie-Curie Fellow** at the Technical University of Munich in the group of Prof. A. Wachter-Zeh and at the Eindhoven University of Technology in the group of Prof. A. Ravagnani

March, 2021 - September, 2022 **SNF Fellow** at the Technical University of Munich in the group of Prof. A. Wachter-Zeh and at the University College Dublin in the group of Prof. E. Byrne

Fundings and Fellowships

January, 2023 - December, 2025 Participant of DFG and ANR joint project: CROWD
PI: A. Wachter-Zeh, P. Loidreau

September, 2022 - September 2024 Marie Skłodowska-Curie fellowship: EuroTechPostdoc2 Programme

March, 2021 - September, 2022 Swiss National Science Foundation Early Postdoc.Mobility, Grant number 195290

Committees, Boards and Memberships

Steering Committee of Conferences CBCrypto since 2025

Program Committee of Conferences Public-Key Cryptography (PKC) since 2026
Workshop on Coding theory and Cryptography (WCC) since 2026
CBCrypto since 2023
AAC24 (Advances in Asymmetric Cryptanalysis)

Membership Swiss Mathematical Society
IEEE
Associate Fellow of ICA

Editorial Board Collectanea Ciphrarum

Guest Editor Special issue on Code-Based Cryptography
in *Designs, Codes and Cryptography*

Organization of Conferences

Post-quantum cryptography	Co-organizer of the workshop on the mathematics of post-quantum cryptography with M. Baldi, L. De Feo, E. Gorla, J. Rosenthal
CBCrypto 2024	Main chair of the 5th International Workshop on Code-based Cryptography (CBCrypto 2024) with A.-L. Horlemann, J.-C. Deneuville
SIAM AG23	Co-organizer of the symposium: Advances in Code-based Signatures, with J. Bariffi
MTNS 2022	Co-organizer of invited session: Applications of coding theory in security, with A. Wachter-Zeh
ACT22	Co-organizer of summer school on algebraic coding theory, with G. Alfarano, K. Khathuria, A. Neri and J. Rosenthal
Coding theory and cryptography	Co-organizer of conference in honor of Joachim Rosenthal's 60th birthday, with G. Alfarano, E. Gorla, A.-L. Horlemann, K. Khathuria and R. Smarandache
SIAM AG21	Co-organizer of the symposium: Algebraic Methods in Cryptography, with G. Micheli
ACT21	Co-organizer of summer school on algebraic coding theory, with G. Alfarano, K. Khathuria, A. Neri and J. Rosenthal
SIAM AG19	Co-organizer of the symposium: Applications of Finite Fields Theory, with G. Micheli and A. Joux

Teaching

Coding Theory	Technical University of Munich, Lecturer Summer semester 2025
Elementary Number Theory	Technical University of Munich, Lecturer, Winter Semester 2024
Coding Theory for Storage and Networks	Technical University of Munich, Co-Lecturer, Spring Semester 2024
Security in Communications and Storage	Technical University of Munich, Co-Lecturer, Fall Semester 2023
Geometry	University of Zurich, Teaching Assistant and Tutor, Fall Semester 2020, 2019, 2018
Number Theory	University of Zurich, Teaching Assistant and Tutor, Spring Semester 2020, 2019, 2018
Linear Algebra and Geometry	University of Zurich, Teaching Assistant and Tutor, Fall Semester 2017
Foundations of Mathematics	University of Zurich, Teaching Assistant and Tutor, Spring Semester 2017

Supervision of Junior Researchers

Ph.D. Students

- Angelica Piccirillo
- Luana Kurmann

Mentoring of Ph.D. Students

- Jessica Bariffi, Ph.D. supervisor: Dr. H. Bartz, Prof. J. Rosenthal
- Sebastian Bitzer, Ph.D. supervisor: Prof. A. Wachter-Zeh
- Anmoal Porwal, Ph.D. supervisor: Prof. A. Wachter-Zeh
- Hugo Sauerbier Couvée, Ph.D. supervisor: Prof. A. Wachter-Zeh

Co-supervision of Master Students

- Irena Syla, University of Zurich, Spring 2024,
  Project title: *Code-based Signature Schemes.*
- Niklas Gassner, University of Zurich, Spring 2020,
  Project title: *Weight-induced distance functions on $\mathbb{Z}/p^s\mathbb{Z}$-codes.*

Selected Publications

- J. Bariffi, G. Cavicchioni, V. Weger. *The Existence of MacWilliams-Type Identities for the Lee, Homogeneous and Subfield Metric.* 2024.
- M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, V. Weger. *Zero Knowledge Protocols and Signatures from the Restricted Syndrome Decoding Problem.* PKC 2024.
- M. Grassl, A.-L. Horlemann, V. Weger. *The subfield metric and its applications to quantum error correction.* Journal of Algebra and its Applications, 2023.
- M. Baldi, S. Bitzer, A. Pavoni, P. Santini, A. Wachter-Zeh, V. Weger. *Generic Decoding of Restricted Errors.* ISIT 2023.
- J. Bariffi, V. Weger. *Better bounds on the minimal Lee distance*, 2023.
- G. Micheli, S. Schraven, S. Tinani, V. Weger. *Geometric sieve over number fields for higher moments.* Research in Number Theory, Volume 9, Number 62, 2023.
- E. Byrne, V. Weger *Bounds in the Lee metric and optimal codes.* Finite Fields and their Applications, Volume 87, 102151, 2023.
- S. Ritterhoff, G. Maringer, S. Bitzer, V. Weger, P. Karl, T. Schamberger, J. Schupp, G. Sigl, A. Wachter-Zeh. *FuLeeca: Lee-metric signature scheme.* CBCrypto 2023. Lecture Notes in Computer Science, Springer, 2023.
- V. Weger, K. Khathuria, A.-L. Horlemann, M. Battaglioni, P. Santini, E. Persichetti. *On the Hardness of the Lee Syndrome Decoding Problem.* Advances in Mathematics of Communications, 2022.
- A. Porwal, L. Holzbaur, H. Liu, J. Renner, A. Wachter-Zeh, V. Weger. *A New Generic Decoder for Interleaved Codes.* PQCrypto 2022. Lecture Notes in Computer Science, Volume 13512. Springer, Cham.
- E. Byrne, A.-L. Horlemann, K. Khathuria, V. Weger *Density of Free Modules over Finite Chain Rings.* Linear Algebra and its Applications, Volume 651, 2022.
- G. Micheli, S. Schraven, V. Weger. *Local to global principle for expected values.* Journal of Number Theory, Volume 238, 2022.
- K. Kathuria, J. Rosenthal, V. Weger. *Encryption Scheme Based on Expanded Reed-Solomon Code*. Advances in Mathematics of Communications, Volume 15, Issue 2, pp 207-218, 2021.
- A.-L. Horlemann-Trautmann, V. Weger. *Information Set Decoding in the Lee Metric with Applications to Cryptography.* Advances in Mathematics of Communications, Volume 15, Issue 4, pp 677-699, 2021.
- G. Micheli, V. Weger. *On rectangular unimodular matrices over the algebraic integers.* SIAM Journal on Discrete Mathematics, Volume 33, Issue 1, pp 425-437, 2019.

NIST Submissions

- M. Baldi, A. Barenghi, S. Bitzer, P. Karl, F. Manganiello, A. Pavoni, G. Pelosi, P. Santini, J. Schupp, F. Slaughter, A. Wachter-Zeh, V. Weger. *CROSS: Codes and Restricted Objects Signature Scheme.* NIST PQC Call for Additional Digital Signature Schemes, 2023. Round 2 Candidate.
- S. Ritterhoff, S. Bitzer, P. Karl, G. Maringer, T. Schamberger, J. Schupp, G. Sigl, A. Wachter-Zeh, V. Weger. *FuLeeca: A Lee-based signature scheme.* NIST PQC Call for Additional Digital Signature Schemes, 2023. Round 1 Candidate.

Workshop Lecturer

September, 2025. Brussels, BE	Finite Geometry and Friends. Title: *Code Equivalence*
July, 2025. Munich, DE	Encode. Title: *Information Set Decoding*
July, 2024. Riva San Vitale, CH	VT-Swiss Coding Theory and Cryptography Summer School. Title: *The Mysterious Case of Code Equivalence.*

Book Chapters

- V. Weger, N. Gassner, J. Rosenthal. *A survey on code-based cryptography.* 2022.

Theses

Ph.D. Thesis.	*Information Set Decoding in the Lee Metric and the Local to Global Principle for Densities.* University of Zurich, 2020.
Master Thesis.	*A Code-Based Cryptosystem using GRS codes.* University of Zurich, 2017.

Selected Talks

May 3-4, 2025. Madrid, ESP	CBCrypto 2025. Title: *CROSS: Signature scheme with restricted errors*
January 9, 2025. Seattle, USA	Joint Mathematics Meeting. Title: *A novel generalization of the MacWilliams identity*
November 28, 2024. Genova, IT	Young Cryptographers in Genova. Title: *What is going on in the on ramp call?*
August 27. 2024. Rome, IT	De Cifris. Title: *CROSS: signature scheme with restricted errors*
May 13, 2024. Munich, DE	AISEC: 3rd PQC Update. Title: *CROSS: signature scheme using restricted errors*
March 29, 2024. Rennes, FR	Effective Geometry and Algebra. Title: *Open Problems in the Lee Metric.*
March 28, 2024. Paris, FR	Séminaire Mathématiques Discrétes, Codes et Cryptographie Title: *Open Problems in the Lee Metric.*
November 29, 2023. Virtual	Sabanci University Math Seminars. Title: *Open problems in the Lee metric*
November 8, 2023. Ghent, BE	Colloquium on Coding Theory and Cryptography. Title: *Open problems in code-based cryptography*
September 25, 2023. Ilmenau, DE	Deutsche Mathematiker Vereinigung. Title: *CROSS: Signature scheme with restricted errors*
September 20, 2023. Brussels, BE	Finite Geometry and Friends. Title: *Introduction to code-based signatures*
September 7, 2023. Darmstadt, DE	CAST: Quantentechnologie und Quantencomputer-resistente Sicherheit. Title: *Jüngste Fortschritte in codebasierten Signaturen*
September 5, 2023. Oxford, GBR	2nd Oxford Post-quantum Cryptography Workshop. Title: *The rise and fall of FuLeeca*
July 13, 2023. Eindhoven, NL	SIAM AG23 Title: *The search for the right support: better bound for the Lee metric.*
July 7, 2023. Aalborg, DK	29th Nordic Congress of Mathematicians with EMS. Title: *How to sign using restricted errors.*
June 23, 2023. Aubervilliers, FR	Fq 15. Title: *The search for the right support: better bound for the Lee metric.*
April 22, 2023. Lyon, FR	CBCrypto 2023. Title: *Signature Scheme from Restricted Errors*
October 7, 2022. Passau, DE	Crossfyre Workshop 2022. Title: *Recent Advances and Challenges in Code-based Signatures.*
June 3, 2022. Mantova, IT	Combinatorics 22. Title: *On the Density of Free Codes over Finite Chain Rings.*
May 11, 2022. St. Gallen, CH	Arbeitsgemeinschaft in Codierungstheorie und Kryptographie. Title: *Bounds and optimal codes in the Lee metric.*
January 27, 2022. Virtual	PICS: Postgraduate International Coding theory Seminar. Title: *Bounds and optimal codes in the Lee metric*
October 5, 2021. Virtual	ACCESS. Title: *Behavior of random ring-linear codes*
August 17, 2021. Virtual	SIAM AG21. Title: *On the density of free codes over finite chain rings*
June 22, 2021. Virtual	CBCrypto 2021. Title: *On the hardness of the Lee syndrome decoding problem*
April 15, 2021. Virtual	UCD Algebra and Number Theory Seminar. Title: *Local-to-Global Principle for Densities*
July 9, 2019. Bern, CH	SIAM AG19. Title: *Generalization of the ball-collision algorithm**
May 19, 2019. Darmstadt, DE	CBCrypto 2019. Title: *Generalization of the ball-collision algorithm*
August 3, 2017. Atlanta, US	SIAM AG17. Title: *Weight Two Masking in the McEliece Public Key System*
June 5, 2017. Gaeta, IT	Fq13. Title: *Weight Two Masking in the McEliece System*