Jens Zumbrägel

Curriculum Vitae

Prof. Dr. Jens Zumbrägel
University of Passau
Innstr. 33, 94032 Passau, Germany
☎ +49 (851) 509 3133
✉ jens.zumbraegel@uni-passau.de
www.fim.uni-passau.de/kryptographie

Personal

Born	28 Apr 1980 in Vechta, Germany
Citizenship	German
Current position	Professor of Mathematics with Focus on Cryptography Faculty of Computer Science and Mathematics University of Passau, Germany

Positions Held

Apr 2017 –	**Associate Professor**, University of Passau.
Jul 18 – Sep 18	**Visiting Professor**, Aalto University, Helsinki.
Oct 16 – Mar 17	**Substitute Professor**, TU Dresden.
Apr 15 – Sep 16	**Scientist**, EPFL, Lausanne.
Oct 13 – Mar 15	**Marie Curie Fellow**, TU Dresden.
Jan 09 – Sep 13	**Postdoc**, University College Dublin.
Nov 04 – Dec 08	**Assistant**, University of Zurich.

Education

Nov 04 – Dec 08	**Doctoral student**, Mathematics Institute, University of Zurich.
Oct 02 – Jun 03	**M. Sc. student**, *Part III of Mathematical Tripos*, University of Cambridge.
Oct 99 – Oct 04	**Study of mathematics**, *Diploma*, University of Oldenburg.

Degrees

Jun 2016	**Habilitation**, *Postdoctoral degree*, TU Dresden. Title: "The Discrete Logarithm Problem in Finite Fields of Small Characteristic"
Dec 2008	**Ph. D. in Mathematics**, *Dissertation in cryptography*. Title: "Public-Key Cryptography Based on Simple Semirings" Advisor: Prof. Dr. J. Rosenthal, University of Zurich

Oct 2004 **Diploma in Mathematics**, *Thesis in functional analysis*.
Advisor: Prof. Dr. A. Defant, University of Oldenburg

Jun 2003 **Certificate of Advanced Study in Mathematics**, University of Cambridge.

Committee Involvement

Oct 2014 – **Associate Editor**, *Advances in Mathematics of Communications*.

Technical Program Committee

2024 IEEE International Symposium on Information Theory
2022 Workshop of Coding and Cryptography
2014 Mathematical Theory of Networks and Systems

Co-organization

2022 IEEE International Symposium on Information Theory, Publication Chair
2021 Joint Annual Meeting of the German Mathematical Society and the Austrian Mathematical Society, Webmaster

Academic Self-Governance

University of Passau

Oct 2022 – **Board Member**, *Educational Accreditation*.

Faculty of Computer Science and Mathematics

Oct 2022 – **Dean of Studies**.
Oct 2021 – **Faculty Council Member**.
Oct 2019 – **Board Member**, *Doctoral Program*.
Oct 20 – Sep 22 **Deputy Chair**, *Board of Examiners*.

Selected Teaching

University of Passau

Apr 2017 – M. Sc. lectures "Rings and Modules", "Cryptography", "Cryptanalysis", "Elliptic Curves" and "Information Theory"
B. Sc. lectures on Linear Algebra, Algebra and Number Theory
Oct 2018 – Seminars "Finite Geometry" and "Post-Quantum Cryptography"

EPFL, Lausanne

Sep 15 – Feb 16 Seminar "Advanced Topics in Cryptology"

TU Dresden

Oct 13 – Mar 17 M. Sc. lecture "Applied Algebra"
Oct 16 – Mar 17 B. Sc. lecture "Discrete Structures for Computer Science"

Supervision of Researchers

University of Passau

Oct 2023 – **Doctoral supervision**, *Maximilian Reif*.
Thesis topic: Structure Theory of Semirings

Jun 2020 – **Doctoral supervision**, *Knud Ahrens*.
Thesis topic: Isogeny-Based Cryptography

University College Dublin

Oct 10 – Sep 14 **Co-supervision of Ph. D. student**, *Oliver Gnilke*.
Thesis title: "The Semigroup Action Problem in Cryptography"
Current position: Professor, Aalborg University, Denmark

Apr 09 – Mar 12 **Co-supervision of Ph. D. student**, *Andreas Kendziorra*.
Thesis title: "Computational Aspects of Finite Simple Semirings"
Current position: Research Scientist, Lightcurve

External Reviews of Theses

Nov 2022 **Habilitation**, *Miroslav Korbelář*, Czech Technical University.
Title: "Simple and Commutative Semirings"

Nov 2020 **Dissertation**, *Violetta Weger*, University of Zurich.
Title: "Information Set Decoding in the Lee Metric and the Local to Global Principle for Densities"

May 2020 **Dissertation**, *Noha Abdelghany*, Western Michigan University.
Title: "On Codes over Rings: the MacWilliams Extension Theorem and the MacWilliams Identities"

May 2018 **Habilitation**, *Erkko Lehtonen*, TU Dresden.
Title: "Reconstruction of Functions from Minors"

Mar 2018 **Dissertation**, *Yauhen Yakimenka*, Tartu University.
Title: "Failure Structures of Message-Passing Algorithms in Erasure Decoding and Compressed Sensing"

Research Funding

As Principal Applicant

Oct 13 – Sep 16 **Irish Research Council and Marie Curie Actions**, *Research position funded by grant ELEVATEPD/2013/82*.
Project: "Finite Semirings and DLP Based Cryptosystems"

Co-Investigator or Involved in the Application

Jul 13 – Jun 15 **Irish Centre for High-End Computing**, *Class A High Impact Award for 2 million core hours*.
Title: "Setting a World Record for Discrete Logarithm Based Cryptography"

Apr 12 – Apr 16 **European Science Foundation**, *COST Action IC1104*.
Framework to support international collaborations, 26 participating countries, Theme: "Random Network Coding and Designs over GF(q)"

Jan 09 – Sep 12 **Science Foundation Ireland**, *Postdoctoral position funded under PI Grant 08/IN.1/I1950*.
Project: "Public-Key Cryptography Based on Finite Simple Semirings"

Selected Publications

2023 T. G. Nam and **J. Zumbrägel**. Congruence-simplicity of Steinberg algebras of non-Hausdorff ample groupoids over semifields. *J. Pure Appl. Algebra*, vol. 227, no. 3, 16 p. DOI: 10.1016/j.jpaa.2022.107207

2021 R. Granger, T. Kleinjung, A. K. Lenstra, B. Wesolowski, **J. Zumbrägel**. Computation of a 30750-bit binary field discrete logarithm. *Math. Comp.*, vol. 90, no. 332, pp. 2997–3022. DOI: 10.1090/mcom/3669

2019 F. M. Schneider and **J. Zumbrägel**. MacWilliams' extension theorem for infinite rings. *Proc. Amer. Math. Soc.*, vol. 147, no. 3, pp. 947–961. DOI: 10.1090/proc/14343

2018 R. Granger, T. Kleinjung, **J. Zumbrägel**. On the discrete logarithm problem in finite fields of fixed characteristic. *Trans. Amer. Math. Soc.*, vol. 370, no. 5, pp. 3129–3145. DOI: 10.1090/tran/7027

2018 Y. Katsov, T. G. Nam, **J. Zumbrägel**. On congruence-semisimple semirings and the K_0-group characterization of ultramatricial algebras over semifields. *J. Algebra*, vol. 508, pp 157–195. DOI: 10.1016/j.jalgebra.2018.04.024

2017 F. M. Schneider and **J. Zumbrägel**. Profinite algebras and affine boundedness. *Adv. Math.*, vol. 305, pp. 661–681. DOI: 10.1016/j.aim.2016.10.001

2014 M. Greferath, T. Honold, C. Mc Fadden, J. A. Wood, **J. Zumbrägel**. MacWilliams' extension theorem for bi-invariant weights over finite principal ideal rings. *J. Combin. Theory Ser. A*, vol. 125, pp. 177–193. DOI: 10.1016/j.jcta.2014.03.005

2014 R. Granger, T. Kleinjung, **J. Zumbrägel**. Breaking '128-bit Secure' Supersingular Binary Curves. In: *Advances in Cryptology – CRYPTO 2014, Part II*. Santa Barbara, USA, pp. 126–145. DOI: 10.1007/978-3-662-44381-1_8

2013 A. Kendziorra and **J. Zumbrägel**. Finite simple additively idempotent semirings. *J. Algebra*, vol. 388, pp. 43–64. DOI: 10.1016/j.jalgebra.2013.04.023

2013 F. Göloğlu, R. Granger, G. McGuire, **J. Zumbrägel**. On the Function Field Sieve and the Impact of Higher Splitting Probabilities. In: *Advances in Cryptology – CRYPTO 2013, Part II*. Santa Barbara, USA, pp. 109–128. DOI: 10.1007/978-3-642-40084-1_7

Awards

Aug 2013 **Best Paper Award**, *International Conference CRYPTO 2013.*
"On the Function Field Sieve and the Impact of Higher Splitting Probabilities"

Invited Talks

Nov 2022 *Computation of a 30750 Bit Discrete Logarithm*
Algebra Colloquium, Charles University in Prague

Jun 2021 *Aspects of Ring-Linear Coding Theory*
Algebraic Coding Theory e-Summer School, University of Zurich

Mar 2020 *MacWilliams Equivalence Theorem for Codes over Rings*
Communications Engineering Seminar, TU Munich

Nov 2018 *Splitting Polynomials and the Discrete Logarithm Problem*
Seminar on Coding Theory and Cryptography, University of Zurich

Oct 2018 *Indiscreet Logarithms?*
RICAM Workshop on Pseudo-Randomness and Finite Fields, Linz

Sep 2018 *Indiscreet Logarithms?*
Department of Mathematics and Systems Analysis, Aalto University, Helsinki

Aug 2018 *Ring-Linear Coding Theory and the Grey-Rankin Bound*
CIMPA School on Quasi-Cyclic and Related Algebraic Codes, METU, Ankara

Feb 2017 *Simple Semirings and Post-Quantum Cryptography*
Arbeitstagung Allgemeine Algebra, Bern

Dec 2016 *Discrete Logarithm Problem – from Gauß to Adleman and Beyond*
Dresden Mathematical Seminar, TU Dresden

Nov 2015 *On the Discrete Logarithm Problem in Finite Fields of Fixed Characteristic*
Seminar on Coding Theory and Cryptography, University of Zurich

Jan 2015 *The Discrete Logarithm Problem in Finite Fields of Small Characteristic*
Institute of Algebra and Geometry, University of Magdeburg

Oct 2014 *Breaking '128-bit Secure' Supersingular Binary Curves*
18th Workshop on Elliptic Curve Cryptography, Chennai, India

June 2014 *Attacks on Small Characteristic Finite Fields for Discrete Log Cryptography*
International Supercomputing Conference, Leipzig

May 2014 *New Algorithms for the Discrete Logarithm Problem in Small Characteristic*
Plenary talk, Computer Algebra Workshop 2014, Kassel

May 2013 *On the Function Field Sieve and the Impact of Higher Splitting Probabilities*
Seminar on Coding Theory and Cryptography, University of Zurich

Nov 2012 *On the Classification of Finite Simple Semirings*
Algebraic Coding Workshop, University of Electro-Communications, Tokyo

Jan 2012 *Simple Semirings – an Overview and new Results*
Algebra Institute Seminar, TU Dresden

Selected Conferences

Jul 2024	IEEE International Symposium on Information Theory 2024, Athens
Jul 2023	29th Nordic Congress of Mathematicians, Aalborg, Denmark
Jun 2022	IEEE International Symposium on Information Theory 2022, Helsinki
Sep 2021	Annual Meeting of the German Mathematical Society, Passau
Mar 2019	Oberwolfach Workshop on Contemporary Coding Theory
Dec 2018	Dagstuhl Seminar on Algebraic Coding Theory
Mar 2018	Annual Meeting of the German Mathematical Society, Paderborn
Apr 2016	Final COST Conference on Network Coding and Designs, Dubrovnik
Aug 2014	Advances in Cryptology – CRYPTO 2014, Santa Barbara
Jul 2014	Summer School crypt@b-it 2014, Bochum
Jul 2014	IEEE International Symposium on Information Theory 2014, Honolulu
May 2014	Aspects of the Discrete Log Problem, Centro Stefano Franscini, Ascona
Oct 2012	Trends in Coding Theory, Centro Stefano Franscini, Ascona
Jul 2012	IEEE International Symposium on Information Theory 2012, Boston
Nov 2011	Dagstuhl Seminar on Coding Theory

Passau, May 2024