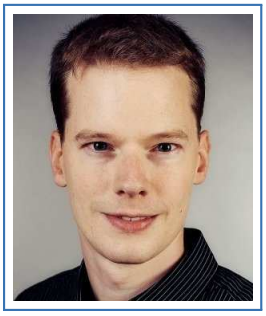
Jens Zumbrägel

Curriculum Vitae

Dr. Jens Zumbrägel
EPFL IC LACAL
CH - 1015 Lausanne
✉ *jens.zumbragel@epfl.ch*
www.math.tu-dresden.de/∼jzumbr



Personal

Born 28 April 1980 in Vechta, Germany
Citizenship German

Positions Held

since 2015 **Scientist**, *LACAL, EPFL, Lausanne.*
2013 – 2015 **Marie Curie Fellow**, *Dresden University of Technology.*
2009 – 2013 **Postdoctoral Research Fellow**, *University College Dublin.*
2004 – 2008 **Assistant**, *University of Zurich.*
2000 – 2004 **Teaching Assistant**, *University of Oldenburg.*

Education

2004 – 2008 **Doctoral student**, *at the Mathematics Institute, University of Zurich.*
2002 – 2003 **M. Sc. student**, *Part III of the Mathematical Tripos, University of Cambridge.*
1999 – 2004 **Study of mathematics (Diplom)**, *University of Oldenburg.*
1999 – 2001 **Study of computer science (Vordiplom)**, *University of Oldenburg.*

Degrees

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*, with Distinction.
Advisor: Prof. Dr. A. Defant, University of Oldenburg

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

*No grade was given for the dissertation.

Research Interests

- **Algebra:** Frobenius rings, simple semirings, computer algebra, general algebra, combinatorial designs
- **Cryptography:** discrete logarithm problem, public-key cryptography
- **Coding Theory:** codes over rings, network coding, LDPC codes

Research Funding

As Principal Applicant

2013 – 2016 **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

2013 – 2015 **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"

2012 – 2016 **European Science Foundation**, *COST Action IC1104.*
Framework to support international collaborations, 26 participating countries,
Theme: "Random Network Coding and Designs over GF(q)"

2009 – 2012 **Science Foundation Ireland**, *Postdoctoral position funded under PI Grant 08/IN.1/I1950.*
Project: "Public-Key Cryptography Based on Finite Simple Semirings"

2005 – 2008 **Swiss National Science Foundation**, Doctoral studies partially funded under grants #107887 and #121874.

Awards and Honours

Aug 2013 **Best Paper Award**, *International Conference CRYPTO 2013.*

1998 – 2004 **German National Academic Foundation (Studienstiftung)**, *Scholarship.*

2000 – 2004 **International Collegiate Programming Contest (ICPC)**.
Mar 2002: 18th place at the ICPC World Finals, Honolulu, Hawaii.
Nov 2001: 1st place at the Northwestern Europe Regional Contest (NWERC).
2000 – 2004: 3rd, 4th and 6th place resp. at the NWERC.

Skills

- **Programming:** C, C++, Java, Python; OpenMP, MPI
- **Computer Algebra:** Magma, Sage, Maple
- **Webtools:** HTML, MySQL, PHP, Typo3
- **Operating Systems:** GNU/Linux, Windows

Talks (selected)

Apr 2016 *Designs in Affine Geometry*
Network Coding and Designs, Dubrovnik, Croatia

Nov 2015 *On the Discrete Logarithm Problem in finite fields of fixed characteristic**
Seminar on Coding Theory and Cryptography, University of Zurich

Mar 2015 *On Bounds for Batch Codes*
Algebraic Combinatorics and Applications (ALCOMA 15), Banz, Germany

Jan 2015 *The Discrete Logarithm Problem in finite fields of small characteristic**
Oberseminar, Institut of Algebra and Geometry, University of Magdeburg

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

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

May 2014 *Neue Algorithmen für das diskrete Logarithmusproblem in Körpern kleiner Charakteristik** 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

July 2012 *On the Algebraic Representation of Certain Optimal Non-Linear Binary Codes*
IEEE International Symposium on Information Theory (ISIT 2012), MIT, USA

Jan 2012 *Simple Semirings - an Overview and new Results**
Institutsseminar Algebra, Dresden University of Technology

Nov 2011 *On the Pseudocodeword Redundancy of Binary Linear Codes*
Dagstuhl Seminar on Coding Theory, Dagstuhl, Germany

Apr 2011 *Algebraic Decoding of Negacyclic Codes Over $\mathbb{Z}_4$*
7th International Workshop on Coding and Cryptography (WCC 2011), Paris

July 2012 *Exploration of AWGNC and BSC Pseudoredundancy*
Mathematical Theory of Networks and Systems (MTNS 2010), Budapest

Apr 2010 *On the Minimum Pseudoweight of Codes with Large Automorphism Group*
Algebraic Combinatorics and Applications (ALCOMA 10), Thurnau, Germany

June 2009 *Finite Congruence-Simple Semirings and their Applications to Public-Key Cryptography** 2nd Mile High Conference on Nonassociative Mathematics, Denver

May 2009 *Classification and Cryptographic Applications of Finite Simple Semirings**
Oberseminar Algebra, University of Oldenburg

July 2008 *Efficient Recovering of Operation Tables of Black Box Groups and Rings*
IEEE International Symposium on Information Theory (ISIT 2008), Toronto

Oct 2006 *Public-Key Cryptography Using Semigroup Actions and Semirings**
Number Theory and Cryptography Research Seminar, Fields Institute, Toronto

*Invited Talk

Conferences and Schools (selected)

28–30 Sep 15	19th Workshop on Elliptic Curve Cryptography (ECC), Bordeaux
17–21 Aug 14	Advances in Cryptology—CRYPTO 2014, Santa Barbara, USA
4–9 May 14	Aspects of the Discrete Log Problem (DLP 2014), Ascona, Switzerland
15–19 Apr 13	Workshop on Coding and Cryptography (WCC 2013), Bergen
28 Oct-2 Nov 12	Trends in Coding Theory, Ascona, Switzerland
13–18 Nov 11	Dagstuhl Seminar on Coding Theory, Wadern, Germany
11–15 Apr 11	Workshop on Coding and Cryptography (WCC 2011), Paris
30 Aug-2 Sep 10	IEEE Information Theory Workshop (ITW 2010), Dublin
26–30 Apr 09	Advances in Cryptology—EUROCRYPT 2009, Cologne
9–12 Mar 08	Public-Key Cryptography PKC 2008, Barcelona
5–7 Sep 07	11th Workshop on Elliptic Curve Cryptography (ECC), Dublin
25 Jun-6 Jul 07	NATO School on Higher-dimensional Geometry over finite fields, Göttingen
30 Oct-3 Nov 06	Workshop on Computational Challenges Arising in Algorithmic Number Theory and Cryptography, Fields Institute, Toronto
19–21 Sep 05	9th Workshop on Elliptic Curve Cryptography (ECC), Copenhagen
7–13 Nov 04	Seminar on Arithmetic Geometry and Cryptography, Oberwolfach
8–26 Jun 04	IMA PI Summer Program for Graduate Students on Coding and Cryptography, University of Notre Dame, USA

Teaching

EPFL

fall 2015	*Seminar on Advanced Topics in Cryptology*, Organiser.

Dresden University of Technology

winter 2014/15	*Applied Algebra*, Instructor.
summer 2014	*New Algorithms for the DLP*, Graduate Lectures, Instructor.
winter 2013/14	*Applied Algebra*, Instructor.

University College Dublin

fall 2010	*Differential Equations via Computer Algebra*, Instructor.
spring 2009	*Calculus II*, Instructor.

University of Zurich

fall 2008	*Seminar on Finite Fields*, Organiser and tutor.
spring 2008	*Coding Theory*, Tutor.
fall 2007	*Algebra I*, Tutor.
year 2006/07	*Linear Algebra I, II*, Tutor.
year 2005/06	*Analysis I, II*, Tutor.
summer 2005	*Introduction to Applied Mathematics*, Tutor.

University of Oldenburg
Tutor for exercise classes on *Linear Algebra*, *Analysis*, and *Probability*.

Students Co-supervised

2010 – 2014 Ph. D. student *Oliver Gnilke*, University College Dublin
Thesis title: "The Semigroup Action Problem in Cryptography"

2009 – 2012 Ph. D. student *Andreas Kendziorra*, University College Dublin
Thesis title: "Computational Aspects of Finite Simple Semirings"

2008 – 2009 Master student *Manuel Ribic*, University of Zurich
Thesis title: "Matsumoto-Imai Tame-Transformation-Method Cryptosystem"

Service

since 2014 Editorial Board member, journal *Advances in Mathematics of Communications*.

2012 – 2016 Management Committee member of COST Action IC1104 on "Random Network Coding and Designs over GF(q)".

Feb 2015 Member of organising committee of the *89th Workshop on General Algebra, AAA89*, Dresden (100 participants).

2014, 2016 Associate Editor for the conference proceedings of *Mathematical Theory of Networks and System MTNS 2014 and MTNS 2016*.

2012, 2013 Instructor of training courses for the Irish Mathematical Olympiad.

Aug 2010 Member of organising committee of the *IEEE Information Theory Workshop, ITW 2010*, Dublin (160 participants).
Publication handling, website creation and maintenance, and local organisation.

Aug 2009 Member of organising committee of the *5th Workshop on Coding and Systems WCS 2009*, Dublin (40 participants).

Review reports, including for

- Adv. Math. Comm.
- Des. Codes Cryptogr.
- Discrete Math.
- IEEE Trans. Inform. Theory
- J. Algebra Appl.
- Linear Algebra Appl.
- Math. Comp.
- Semigroup Forum
- Mathematical Reviews (MathSciNet)
- several conference proceedings

Lausanne, May 2016