Lukas Kölsch

Curriculum Vitae

Department of Mathematics and Statistics
University of South Florida, Tampa, FL, USA
✉ lukas.koelsch.math@gmail.com
🖰 lkoelsch.github.io

Personal Information

Name	Lukas Kölsch
Nationality	German
Date of birth	05/19/1993
Place of birth	Gifhorn, Germany
Current Position	Assistant Professor, University of South Florida

Employment

08/2023-	**Tenure track assistant professor**, *University of South Florida*.
09/2021-08/2023	**Postdoctoral Scholar** , *University of South Florida*, Tampa, USA, (position was supposed to start 01/2021, but delayed due to the coronavirus pandemic).
12/2020-08/2021	**Research Associate (PostDoc position)**, *University of Rostock*, Rostock, Germany.
10/2017-11/2020	**Research Associate (PhD student)**, *University of Rostock*, Rostock, Germany.
04/2017	**Software Developer**, *Marabu GmbH*, Magdeburg, Germany.
02/2017–03/2017	**Internship as a Software Developer**, *Marabu GmbH*, Magdeburg, Germany.

Education

10/2017-11/2020	**PhD Student**, *University of Rostock*, Rostock, Germany, Title of Thesis: Mathematical aspects of the design and security of block ciphers. Defended: 11/24/20. Grade: summa cum laude. Supervisor: Gohar Kyureghyan
10/2014–03/2017	**Master of Science in Mathematics (awarded with distinction)**, *Otto-von-Guericke Universität Magdeburg*, Magdeburg, Germany, Title of thesis: Constructing irreducible polynomials over finite fields using the composed product. Supervisor: Gohar Kyureghyan
10/2011–12/2014	**Bachelor of Science in Mathematics (awarded with distinction)**, *Otto-von-Guericke Universität Magdeburg*, Magdeburg, Germany.

Research Interests

Finite fields and their application to coding theory and cryptography, Finite Geometry, Rank-metric Codes, Design and cryptanalysis of block and stream ciphers, (vectorial) Boolean functions and their connections to cryptography (e.g. APN functions, bent functions), Connections between cryptography and combinatorial structures like difference sets and designs

List of Publications and Preprints

[12] Kölsch, L., Polujan, A. Value Distributions of Perfect Nonlinear Functions. *Combinatorica* (2023). Preprint: `https://arxiv.org/abs/2302.03121`.

[11] Bartoli, D., Kölsch, L., Micheli, G.: Differential biases, c-differential uniformity, and their relation to differential attacks. Preprint: `https://arxiv.org/abs/2208.03884`.

[10] Göloğlu, F., Kölsch, L.: Counting the number of non-isotopic Taniguchi semifields. *Designs, Codes, Cryptography* (2023), Preprint: `https://arxiv.org/abs/2207.13497`.

[9] Göloğlu, F., Kölsch, L.: Equivalences of biprojective almost perfect nonlinear functions. Preprint: `https://arxiv.org/abs/2111.04197`.

[8] Göloğlu, F., Kölsch, L.: An exponential bound on the number of non-isotopic commutative semifields. *Transactions of the American Mathematical Society* 376 (2023), 1683-1716. `https://doi.org/10.1090/tran/8785`. Preprint availabe: `https://arxiv.org/abs/2109.04923`

[7] Kölsch, L., Kriepke, B., Kyureghyan, G.M.: Image sets of perfectly nonlinear maps. *Designs, Codes, Cryptography* (2022). `https://doi.org/10.1007/s10623-022-01094-4`

[6] Kölsch, L., Schüler, R.: Formal self-duality. *Cryptogr. Commun.* 13, 815–836 (2021), `https://doi.org/10.1007/s12095-021-00508-9`.

[5] Kölsch, L.: On CCZ-equivalence of the inverse function, *IEEE Transaction on Information Theory*, vol. 67, no. 7, pp. 4856-4862, July 2021, `https://doi.org/10.1109/TIT.2021.3065068`.

[4] Kölsch, L.: On the inverses of Kasami and Bracken-Leander exponents, *Designs, Codes, Cryptography* 88, 2597-2621 (2020), `https://doi.org/10.1007/s10623-020-00804-0`

[3] Göloğlu, F., Kölsch, L., Kyureghyan, G., Perrin, L.: On subspaces of Kloosterman zeros and permutations of the form $L_1(x^{-1}) + L_2(x)$, In: Bajard J.C., Topuzoglu A. (eds) *Arithmetic of Finite Fields. WAIFI 2020. Lecture Notes in Computer Science*, vol 12542. Springer, Cham. `https://doi.org/10.1007/978-3-030-68869-1_12`

[2] Canteaut, A., Kölsch, L., Li, C., Li, C., Li, K., Qu, L., Wiemer, F.: Autocorrelations of Vectorial Boolean Functions. In: Longa P., Ràfols C. (eds) *Progress in Cryptology – LATINCRYPT 2021. LATINCRYPT 2021. Lecture Notes in Computer Science*, vol 12912. `https://doi.org/10.1007/978-3-030-88238-9_12`

  ○ merged article based on: Canteaut, A., Kölsch, L., Wiemer, F.: Observations on the DLCT and Absolute Indicators, `https://eprint.iacr.org/2019/848`

[1] Kölsch, L.: XOR-Counts and Lightweight Multiplication with Fixed Elements in Binary Finite Fields In: Ishai Y., Rijmen V. (eds) *Advances in Cryptology – EUROCRYPT 2019. EUROCRYPT 2019. Lecture Notes in Computer Science*, vol 11476. `https://doi.org/10.1007/978-3-030-17653-2_10`

Selected Research Talks

07/05/2023   *Permutations of the projective plane and associated planar functions*   Seminar talk at University of Rostock, Germany. Invited by G. Kyureghyan

06/23/2023   *Value distributions of perfect nonlinear functions* Conference on Finite Fields and their Applications (Fq15), Paris, France. (Contributed Talk)

06/07/2023   *Value distributions of perfect nonlinear functions* CanaDAM 2023, Winnipeg, Canada. (Invited symposium talk)

04/18/2023   *Rank-metric codes from semifields* Talk at the online Algebraic Coding and Cryptography Seminar Series (ACCESS)

03/30/2023   *Bivariate Semifields* Seminar talk at University College Dublin, Ireland. Invited by J. Sheekey

03/02/2023   *Semifields, and their relations to cryptography* Seminar talk at University of Alabama, Huntsville.

02/24/2023   *Semifields, and their relations to coding theory and cryptography* Seminar talk at University of South Florida.

02/13/2023   *Semifields, and their relation to cryptography* Seminar talk at Florida Atlantic University.

10/26/2022   *Bivariate Semifields: Constructions, Symmetries and Equivalences.* Seminar Talk at Sabanci university, Istanbul, Turkey. Invited by M. Lavrauw.

09/27/2022   *Equivalences and symmetries in combinatorial structures: From Boolean functions to finite geometries.* Seminar Talk at University of Rostock. Invited by G. Kyureghyan.

09/16/2022   *Techniques for proving equivalences of Boolean functions*, 7th international Workshop on Boolean functions and their applications, Balestrand, Norway. (Invited Talk)

08/29/2022   *Bivariate semifields and their isotopies*, Finite Geometries 2022, Irsee, Germany. (Invitation only conference)

03/10/2022   *Counting the number of non-isotopic semifields inside some known semifield families*, Workshop for Coding and Cryptography 2022, Rostock, Germany. (Refereed Talk)

08/17/2021   *Equivalences of S-Boxes*, SIAM conference on Applied Algebraic Geometry (SIAM AG 21), Minisymposium on Algebraic Methods in Cryptography, virtual. (Invited Talk)

07/08/2020   *On subspaces of Kloosterman zeros and permutations of the form $L_1(x^{-1}) + L_2(x)$*, International Workshop on the Arithmetic of Finite Fields (WAIFI) 2020, Rennes, France (virtual). (Refereed Talk)

06/06/2019   *How do binary operations interact with the subfield structure of a finite field?*, Finite Fields and their Applications (Fq14), Vancouver, Canada. (Contributed Talk)

05/20/2019   *XOR-counts and Lightweight Multiplication with Fixed Elements in Binary Finite Fields*, EUROCRYPT 2019, Darmstadt, Germany. (Refereed Talk)

11/23/2018   *Optimal implementations of matrix multiplication in finite fields* , Colloquium on Combinatorics 2018, Paderborn, Germany. (Contributed Talk)

05/02/2018 *Efficient multiplication in binary finite fields*, Discrete Mathematics Seminary, University of Rostock, Germany.

Grants and Awards

2022 Joachim-Jungius price for my dissertation (top 3 dissertation at the University of Rostock in 2020/2021) (2000 Euros)

2021 co-wrote the proposal for the National Science Foundation grant number 2127742, *Applications of Galois Theory to the Search for Non-Linear Functions*, volume: $500,000. Principal Investigators: Giacomo Micheli, Jean-Francois Biasse (University of South Florida, Tampa, FL, USA)

08/21 Travel support *SIAM conference on Applied Algebraic Geometry* ($200)

05/19 Registration fee waived for *EUROCRYPT 2019* ($350)

2019 Free one year membership of the *IACR (International Association for Cryptologic Research)*

Outreach

07/18/2022- Instructor of *CodebreakHERS 2022*, an annual cybersecurity camp for grade 8-12 girls
07/22/2022 at the University of South Florida

09/2021– Part of the organization team for *CodebreakHERS*

05/25/2019 Co-Organization of the *Day of Mathematics* at the University of Rostock

09/07/2018 Lecture *Der RSA-Algorithmus (The RSA algorithm)* for gifted high school students, Rostock

Teaching

University of South Florida

Fal 2023 Graduate Algebra I (MAS 5311) and Calculus I (MAC 2311), lecturer.

Spring 2023 Calculus II (MAC 2312), lecturer.

Fall 2022 Lecture series on Cryptography on graduate level (4 lectures), lecturer and co-organizer.

Spring 2022 Bridge to abstract Mathematics (MGF 3301), lecturer.

Fall 2021 Calculus I (MAC 2311), lecturer, two sections.

University of Rostock

2017-2021 4 undergraduate student co-supervised, including review of Bachelor theses

Summer 2021 Linear Algebra II (Co-Organizer, Teaching Assistant)

Winter 2020 Linear Algebra I (Co-Organizer, Teaching Assistant)

Summer 2020 Linear Algebra II (Co-Organizer, Teaching Assistant)

Winter 2019 Linear Algebra I (Co-Organizer, Teaching Assistant)

Winter 2019 Abstract Algebra (Co-Organizer, Teaching Assistant)

Winter 2019 Preparatory course for new students in mathematics, University of Rostock

Winter 2018 Introduction to Mathematics for Economics (Co-Organizer, Teaching Assistant)

Winter 2018 Abstract Algebra (Co-Organizer, Teaching Assistant)

Winter 2018	Preparatory course for new students in mathematics
Summer 2018	Mathematics for Computer Science and Electrical Engineering (Co-Organizer, Teaching Assistant)
Summer 2018	Linear Algebra II (Co-Organizer, Teaching Assistant)
Winter 2017	Linear Algebra I (Co-Organizer, Teaching Assistant)

Otto-von-Guericke University Magdeburg

Winter 2015, Summer 2016	Tutorials for Undergraduates

Academic Activities and memberships

Reviewer for the journals/conferences *Finite Fields and Applications*, *Designs, Codes, Cryptography*, *Cryptography and Communications*, *Discrete Mathematics*, *Journal of Algebraic Combinatorics*, *IEEE Transactions on Information Theory*, *Journal of Mathematical Cryptography*, *EUROCRYPT* and others

Reviewer for *mathscinet* and *zbMATH* (both since 2021)

Member of the Program Committee for the Boolean functions and their applications (BFA) conference 2023

Languages

German	Native
English	Fluent
French	Intermediate

Programming Languages

Python, Sage, Magma, GAP, Java, C++

References

Gohar Kyureghyan, University of Rostock, Germany. `gohar.kyureghyan@uni-rostock.de`

Lilya Budaghyan, University of Bergen, Norway. `lilya.budaghyan@uib.no`

Alexander Pott, Otto-von-Guericke University Magdeburg, Germany. `alexander.pott@ovgu.de`

Faruk Gologlu, Charles University Prague, Czech Republic. `farukgologlu@googlemail.com`

(Teaching only) Mathias Sawall, University of Rostock, Germany. `mathias.sawall@uni-rostock.de`