Karan Khathuria — Curriculum vitae

Contact Information

Quantinuum
Partnership House
Carlisle Place
London SW1P 1BX, United Kingdom

karan.khathuria@quantinuum.com

ORCID 0000-0002-9886-2770

Personal Information

Date of Birth: August 15, 1993
Place of Birth: Udaipur, India
Citizenship: Indian

Research Interests

Post-quantum and quantum cryptography, Discrete mathematics, Coding theory, Commutative Algebra, Computational Algebra and Algorithms

Positions

Research Scientist - Theoretical Cryptography — January 2023 – (now)
Quantinuum

Postdoctoral Researcher — March 2021 – December 2022
University of Tartu

Postdoctoral Researcher — November 2020 – February 2021
University of Zurich

Education

Doctorate of Philosophy in Mathematics — November 2016 – October 2020
University of Zurich
Thesis: "Algebraic Study of Some Recent Asymmetric Cryptosystems"
Advisor: Prof. Joachim Rosenthal

Integrated Master of Science in Mathematics — August 2011 – June 2016
Centre for Excellence in Basic Sciences, Mumbai
Thesis: "Symbolic Rees Algebra"
Advisor: Prof. Jugal K. Verma, IIT Bombay
CGPA – 9.42/10.00

Publications

Journal articles:

8. H. Hollmann, K. Khathuria, A.-E. Riet, and V. Skachek. On some batch code properties of the simplex code. *Designs, Codes and Cryptography*, 10.1007/s10623-022-01173-6, 2022. Extended version: arXiv:2110.07421

7. E. Byrne, A.-L. Horlemann, K. Khathuria, and V. Weger. Density of free modules over finite chain rings. *Linear Algebra and its Applications*, 10.1016/j.laa.2022.06.013, 2022

6. V. Weger, K. Khathuria, A.-L. Horlemann, M. Battaglioni, P. Santini, and E. Persichetti. On the Hardness of the Lee Syndrome Decoding Problem. *Advances in Mathematics of Communications*, 10.3934/amc.2022029, 2022

5. N. Aragon, M. Baldi, J.-C. Deneuville, K. Khathuria, E. Persichetti, and P. Santini. Cryptanalysis of a code-based full-time signature. *Designs, Codes and Cryptography*, 89:2097–2112, 2021

4. G. N. Alfarano, K. Khathuria, and V. Weger. A survey on single server private information retrieval in a coding theory perspective. *Applicable Algebra in Engineering, Communication and Computing*, pages 1–24, 2021

3. K. Khathuria, J. Rosenthal, and V. Weger. Encryption Scheme Based on Expanded Reed-Solomon Codes. *Advances in Mathematics of Communications*, 15(2):207–218, 2021

2. K. Khathuria, G. Micheli, and V. Weger. On the Algebraic Structure of $E_p^{(m)}$ and Applications to Cryptography. *Applicable Algebra in Engineering, Communication and Computing*, 32:495–505, 2021

1. C. Interlando, K. Khathuria, N. Rohrer, J. Rosenthal, and V. Weger. Generalization of the Ball-Collision Algorithm. *Journal of Algebra, Combinatorics, Discrete Structures and Applications*, 7:195 – 207, 2020

Conference Proceedings:

4. J. Bariffi, K. Khathuria, and V. Weger. Information Set Decoding for Lee-Metric Codes using Restricted Balls. In *Code-Based Cryptography Workshop CBCrypto 2022*, pages 110–136. Springer, 2022

3. I. E. Bocharova, H. D. L. Hollmann, K. Khathuria, B. D. Kudryashov, and V. Skachek. Coding with Cyclic PAM and Vector Quantization for the RLWE/MLWE channel. In *2022 IEEE International Symposium on Information Theory (ISIT)*, pages 666–671, 2022

2. K. Khathuria, J. Rosenthal, and V. Weger. Weight Two Masking of the Reed-Solomon Structure in Conjugation with List Decoding. In *Proceedings of the 23$^{\text{rd}}$ International Symposium on Mathematical Theory of Networks and Systems – MTNS*, 2018

1. J. Baena, D. Cabarcas, D. Escudero, K. Khathuria, and J. Verbel. Rank Analysis of Cubic Multivariate Cryptosystems. In *Post-Quantum Cryptography*, Berlin, Heidelberg, 2018. Springer Berlin Heidelberg

Preprints:

3. G.N. Alfarano, K. Khathuria, and S. Tinani. On Cyclic Matroids and their Applications. Submitted to Discrete Mathematics, arXiv preprint arXiv:2107.14214, July 2021

2. M. Baldi, K. Khathuria, E. Persichetti, and P. Santini. Cryptanalysis of a Code-Based Signature Scheme Based on the Lyubashevsky Framework. Cryptology ePrint Archive, Report 2020/905, July 2020

1. K. Khathuria. Galois Ring Isomorphism Problem. arXiv preprint arXiv:2008.11927, August 2020

CONFERENCE/ SEMINAR TALKS

Invited talks:

- *On some batch code properties of the simplex code*, Neuchatel - St.Gallen - Zurich Seminar in Coding Theory and Cryptography, University of St. Gallen, Switzerland (November 16, 2022)
- *On some batch code properties of the simplex code*, Invited talks at the Technical University of Munich (October 4, 2022)
- *Recent Advances in Decoding General Lee Metric Codes*, International Symposium on Mathematical Theory of Networks and Systems (MTNS) 2022, University of Bayreuth (September 12, 2022).
- *Cryptography, coding theory and the future*, Graduate and Undergraduate Student Seminar (GAUSS), University of Iowa (April 22, 2021).
- *An overview of single-server private information retrieval in a coding theory perspective*, eSeminar Discrete Mathematics, Codes and Cryptography, University of Paris 8 (February 11, 2021).
- *WHAT IS ... Private Information Retrieval?*, Zurich Graduate Colloquium, Zurich, Switzerland (December 8, 2020).
- *Rank analysis of cubic multivariate cryptosystems*, SIAM Conference on Applied Algebraic Geometry, Bern, Switzerland (July 9, 2019).
- *McEliece cryptosystem based on weight two masking of Reed-Solomon codes*, 3rd International Conference on Applied Mathematics and Informatics, San Andrés, Colombia (December 1, 2017).

Other talks:

- *Coding with Cyclic PAM and Vector Quantization for the RLWE/MLWE Channel*, 2022 IEEE International Symposium on Information Theory (ISIT), Aalto University, Finland (June 27, 2022).
- *New McEliece cryptosystem using Reed-Solomon codes over an extension field*, 7th Code-Based Cryptography Workshop, Darmstadt, Germany (May 18, 2019).
- *The two-dimensional and three-dimensional MinRank problem*, CIMPA Research School and Workshop: Quasi-Cyclic and Related Algebraic Codes, METU, Ankara, Turkey (September 4, 2018).
- *Rank analysis of cubic multivariate cryptosystems*, Coding Theory and Cryptography Seminar, University of Neuchatel, Switzerland (May 9, 2018).

TEACHING TRAINING

- University teaching program conducted by the Human Resources Office of the University of Tartu, held during Spring 2022 semester.

TEACHING EXPERIENCE

Teaching assistant and tutor:

- Design and Analysis of Algorithms — Fall 2022
  Institute of Computer Science, University of Tartu
- Theoretical Computer Science — Spring 2022
  Institute of Computer Science, University of Tartu
- Design and Analysis of Algorithms — Fall 2021
  Institute of Computer Science, University of Tartu
- Programming — Fall 2020
  Institute of Mathematics, University of Zurich
- Stochastics for the Natural Sciences — Spring 2020
  Institute of Mathematics, University of Zurich
- Cryptography — Fall 2019
  Institute of Mathematics, University of Zurich
- Coding Theory — Spring 2019
  Institute of Mathematics, University of Zurich
- Algebra I — Fall 2018
  Institute of Mathematics, University of Zurich
- Elliptic Curves — Spring 2018
  Institute of Mathematics, University of Zurich
- Cryptography — Fall 2017
  Institute of Mathematics, University of Zurich
- Numerical Analysis I — Spring 2017
  Institute of Mathematics, University of Zurich

Student seminars:

- Research Seminars in Cryptography — Spring 2022
  Institute of Computer Science, University of Tartu

Master thesis supervised:

- N. V. Wyk — Spring 2021
  Institute of Mathematics, University of Zurich
  Thesis title: "Analysis of a Code-Based Public Key Cryptosystem having Quasi-Cyclic Structure"
  Supervised jointly with: J. Rosenthal
- A. Venzin — Fall 2020
  Institute of Mathematics, University of Zurich
  Thesis title: "Castelnuovo-Mumford Regularity and the Complexity of Gröbner Basis Algorithms"
  Supervised jointly with: J. Rosenthal
- S. Sewer — Spring 2020
  Institute of Mathematics, University of Zurich
  Thesis title: "Analysis of the Post-Quantum Cryptosystem FrodoKEM based on the Learning with Errors Problem"
  Supervised jointly with: J. Rosenthal
- R. Schüürmann — Spring 2019
  Institute of Mathematics, University of Zurich
  Thesis title: "Gröbner Basis Algorithms and Applications in Multivariate Cryptography"
  Supervised jointly with: J. Rosenthal
- P. Christinat — Spring 2018

Institute of Mathematics, University of Zurich
Thesis title: "Pseudorandom Number Generator from the Finite Field Isomorphism Problem"
Supervised jointly with: J. Rosenthal

Scholarships and Fellowships

- Forschungskredit PhD Grant 2019 November 2019 - October 2020
  University of Zurich
- Scholarship for Higher Education(SHE) August 2011 - July 2016
  INSPIRE Programme, Department of Science and Technology (DST) Govt. of India
- Summer Research Fellowship Programme Summer 2014
  Indian Academy of Sciences

Achievements

- Acquired the 32^{nd} spot all over India in Joint CSIR-UGC Test for Junior Research Fellowship in June 2016 conducted by Council of Scientific and Industrial Research, Govt. of India (This is a national level exam taken by about 30,000 students with Masters degree in mathematics)
- Acquired the 29^{th} spot all over India in JAM 2014 conducted by Indian Institute of Technology (IIT) Kanpur (This is national level exam taken by about 15,000 students with Bachelors degree in mathematics)
- Awarded Cheer Prize in Madhava Mathematics Competition 2013 (National level competition for Bachelors students in Mathematics)
- Successfully cleared Regional Mathematics Olympiad 2010 conducted by National Board of Higher Mathematics (NBHM), Department of Atomic Energy (DAE)

Volunteer Activities

Organizational:

- Co-organizer of 'Coding Theory and Cryptography: a conference in honor of Joachim Rosenthal's 60^{th} birthday', July 11–15, 2022 (link).
- Co-organizer of 'Algebraic Coding Theory (ACT) Summer School 2022', July 4–8, 2022 (link).
- Co-organizer of 'Algebraic Coding Theory (ACT) eSummer School 2021', June 7–11, 2021 (link).
- Headed the organizing team of 'Jigyasa-2013', which is an annual inter-college Science Quiz conducted by Centre for Excellence in Basic Sciences. Created prerequisites for the event like posters, brochures and a website.

Reviewing:

- Journal of Algebra and its Applications
- International Workshop on Code-Based Cryptography (CBCrypto) 2021
- Journal of Mathematical Cryptology
- Number-Theoretic Methods in Cryptology (NutMiC) 2019
- 7th Code-Based Cryptography Workshop (CBC) 2019
- MathCrypt 2018

Others

- Integral part of the creative team of Novellus – an annual magazine of Centre for Excellence in Basic Sciences, in the year 2013.

Memberships

- Society for Industrial and Applied Mathematics (SIAM)
- IEEE Information Theory Society

Skills

- Technical Skills: Sage, Macaulay2, Python, Wolfram Mathematica, Magma, Matlab, C++, FORTRAN, HTML.
- Advanced user of LaTeX and MS Office applications.
- Skilled in making digital artistic creations using Adobe Photoshop, Adobe InDesign, etc.

References

- Prof. Joachim Rosenthal rosenthal@math.uzh.ch
  Institute of Mathematics, University of Zurich, Switzerland
- Prof. Vitaly Skachek vitaly.skachek@ut.ee
  Institute of Computer Science, University of Tartu, Estonia