Curriculum Vitae

# Nicolas Resch

July 2023

---

## Contents

# 1 Brief Bio

Nicolas is an assistant professor in the Theoretical Computer Science Group of the Informatics Institute within the University of Amsterdam. He obtained his PhD in computer science at Carnegie Mellon University, where he was very fortunate to be co-advised by Venkatesan Guruswami and Bernhard Haeupler. Subsequently he was a researcher in the cryptology group at the CWI, headed by Ronald Cramer. While he has broad interests in many areas of theoretical computer science, his research has mostly focused on questions arising in coding theory, cryptography and pseudorandomness. He has a particular interest in combinatorial properties of random code ensembles, as well as algebraic constructions of codes and other combinatorial structures. Recently, he has become interested in code-based cryptography, particularly its security and uses in secure multiparty computation. Previously, he obtained his B.Sc. from McGill University in the Joint Honours Mathematics and Computer Science program.

# 2 Personal Data


- **Webpage:** `https://nicolas-resch.carrd.co`
- **Email:** n.a.resch@uva.nl
- **Citizenship:** Canadian.
- **Date of Birth:** 2 June, 1993. (Age: 29.)


# 3 Work Experience

**Assistant Professor** *September 2022–present*
*Informatics Institute, University of Amsterdam*, the Netherlands.

**Postdoctoral Researcher** *July 2020–August 2022*
*Centrum Wiskunde & Informatica*, Amsterdam, the Netherlands.

- **Host:** Ronald Cramer.

# 4 Academic Degrees

**PhD in Computer Science** *September 2015–May 2020*
*Carnegie Mellon University*, Pittsburgh, USA.

- **Thesis:** List-Decodable Codes: (Randomized) Constructions and Applications.
- **Co-advisors:** Venkatesan Guruswami and Bernhard Haeupler.

**Bachelor's of Science** *September 2011–May 2015*
*McGill University*, Montréal, Canada.

- **Thesis:** Item Pricing with Price Ranges, Budgets and Competition.
- GPA: 3.98/4.0
- B.Sc. in Joint Honors Mathematics & Computer Science.

# 5 Research

## 5.1 Journal publications

1. Thomas Debris-Alazard, Léo Ducas, Nicolas Resch, and Jean-Pierre Tillich. *Smoothing Codes and Lattices: Systematic Study and New Bounds. IEEE Transactions on Information Theory.* Accepted; to appear.

2. Jonathan Mosheiff, Nicolas Resch, Noga Ron-Zewi, Shashwat Silas, and Mary Wootters. *LDPC Codes Achieve List-Decoding Capacity. SIAM Jounal on Computing (SICOMP)* (special issue of FOCS 2020). Accepted; to appear.

3. Venkatesan Guruswami, Jonathan Mosheiff, Nicolas Resch, Shashwat Silas, and Mary Wootters. *Threshold rates for properties of random codes. IEEE Transactions on Information Theory*, Volume 68(2), pages 905-922, 2021.

4. Venkatesan Guruswami, Ray Li, Nicolas Resch, Jonathan Mosheiff, Shashwat Silas, and Mary Wootters. *Bounds for list-decoding and list-recovery of random linear codes. IEEE Transactions on Information Theory*, Volume 68(2), pages 923-939, 2021.

5. Swastik Kopparty, Nicolas Resch, Noga Ron-Zewi, Shubhangi Saraf, and Shashwat Silas. *On list-recovery of high-rate tensor codes. IEEE Transactions on Information Theory*, Volume 67(1), pages 296-316, 2021.

6. Venkatesan Guruswami, Nicolas Resch, and Chaoping Xing. Dimension Expanders via Linearized Polynomials and Subspace Designs. *Combinatorica*, pages 1-35, 2021.

## 5.2 Refereed conference publications

1. Nicolas Resch and Chen Yuan. *Two-Round Perfectly Secure Message Transmission with Optimal Rate. Proc. of the 4th Conference on Information-Theoretic Cryptography (ITC),* 2023.

2. Nicolas Resch, Chen Yuan, and Yihan Zhang. *Plotkin Points and New Capacity Bounds for List-Decoding and List-Recovery. Proc. of the 50th EATCS International Colloquium on Automatca and Language Processing (ICALP),* 2023.

3. Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, Nicolas Resch, and Peter Scholl. *Oblivious Transfer with Constant Computational Overhead. Proc. of the 42nd International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT),* 2023.

4. Klim Efremenko, Bernhard Haeupler, Yael Tauman Kalai, Gillat Kol, Nicolas Resch, and Raghuvansh R. Saxena. *Interactive Coding with Small Memory. Proc. of the 42nd Symposium on Discrete Algorithms (SODA),* 2023.

5. Elette Boyle, Geoffroy Couteau, Niv Gilboa, Yuval Ishai, Lisa Kohl, Nicolas Resch, and Peter Scholl. *Correlated Pseudorandomness from Expand-Accumulate Codes. Proc. of the 42nd Conference on Advances in Cryptology (CRYPTO),* 2022.

6. Nicolas Resch and Chen Yuan. *New Bounds for Thresholds of Code Ensembles. Proc. of the 49th EATCS International Colloquium on Automatca and Language Processing (ICALP),* 2022.

7. Klim Efremenko, Bernhard Haeupler, Yael Tauman Kalai, Pritish Kamath, Gillat Kol, Nicolas Resch, and Raghuvansh R. Saxena. *Coding for Interactive Communication with Small Memory and Applications to Robust Circuits. Proc. of the 54th ACM SIGACT Symposium on Theory of Computing (STOC),* 2022. Invited to *SIAM Journal on Computing (SICOMP)* special issue of STOC 2022.

8. Venkatesan Guruswami, Jonathan Mosheiff, Nicolas Resch, Shashwat Silas, and Mary Wootters. *Sharp threshold rates for random codes. Proc. of the 12th Innovations in Theoretical Computer Science Conference (ITCS)*, 2021.

9. Jonathan Mosheiff, Nicolas Resch, Noga Ron-Zewi, Shashwat Silas, and Mary Wootters. *LDPC Codes Achieve List-Decoding Capacity. Proc. of the 61st IEEE Symposium on Foundations of Computer Science (FOCS)*, 2020.

10. Venkatesan Guruswami, Ray Li, Nicolas Resch, Jonathan Mosheiff, Shashwat Silas, and Mary Wootters. *Bounds for list-decoding and list-recovery of random linear codes. Proc. of the 24th International Conference on Randomization and Computation (Random)*, 2020.

11. Swastik Kopparty, Nicolas Resch, Noga Ron-Zewi, Shubhangi Saraf, and Shashwat Silas. *On List Recovery of High-Rate Tensor Codes. Proc. of the 23rd International Conference on Randomization and Computation (Random)*, 2019.

12. Venkatesan Guruswami, Nicolas Resch, and Chaoping Xing. *Dimension Expanders via Linearized Polynomials and Subspace Designs. Proc. of the 33rd Computational Complexity Conference (CCC)*, pages 4:1–4:16, 2018.

13. Venkatesan Guruswami and Nicolas Resch. *On the List-Decodability of Random Linear Rank-Metric Codes. Proc. of the 47th IEEE International Symposium on Information Theory (ISIT)*, 2018.

### 5.3 Unpublished manuscripts

1. Thomas Attema, Serge Fehr, and Nicolas Resch. *A Generalized Special-Soundness Notion and its Knowledge Extractors.* In submission; pre-print available at https://eprint.iacr.org/2023/818.pdf

2. Thomas Debris-Alazard and Nicolas Resch. *Worst and Average Case Hardness of Decoding via Smoothing Bounds.* In submission; pre-print available at https://eprint.iacr.org/2022/1744.pdf.

## 6 Teaching Experience

### Assistant Professor

**Lecturer** *Period 2 of Fall 2022*

- Course titles: *Information Theory* and *Introduction to Information Theory* (a combined MSc and BSc course).
- Course numbers: 5341INTH6Y and 5122ITSL6Y.

### Postdoctoral Fellow

**Co-Lecturer and Lead Teaching Assistant** *Fall 2021*

- Course title: *Introduction to Cryptography.*

- Course number: M1 - 8EC (offered by Mastermath).

### PhD Studies

**Teaching Assistant** *Fall 2017*

- Course title: *Graduate Computational Complexity Theory.*
- Course number: 15-855.

**Teaching Assistant** *Fall 2016*

- Course title: *Artificial Intelligence: Representation and Problem Solving.*
- Course number: 15-381/781.

## 7 Supervision

### PhD Supervision

**Martijn Brehm** *September 2023–Present*

- Title: *TBD.*

### MSc Supervision

**Mark Bebawy** *Spring 2023*

- Title: *Cryptographic Compilers for Linear Probabilistically Checkable Proofs.*

### BSc Supervision

**Jelle Sipkes** *Spring 2023*

- Title: *Cryptanalysis of Weak Pseudorandom Functions.*
- Joint Honours Mathematics and Computer Science Thesis, co-supervised with Jeroen Zuiddam.

## 8 Professional Service

### Program Committees

- Innovations in Theoretical Computer Science (ITCS 2024)

## 9 Awards & Distinctions

**PhD Studies**

- 2017–2019 Awarded *Natural Sciences and Engineering Research Council (NSERC)* CGS D scholarship.
  - Most prestigious PhD fellowship offered by NSERC, Canada's preeminent federal agency responsible for funding natural sciences and engineering research.
  - Rejected in favor of PGS D (the CGS D may only be held at a Canadian institution).

**Bachelor Studies**

- 2015: William Moser Undergrad Award.
  - Awarded to top performer on McGill's Putnam competition team.
- 2013–15: Sir Edward Beatty Memorial Scholarship.
  - Awarded in recognition of high academic merit to students entering the intermediate or final year in Major or Honours Mathematics, based on the recommendation of the Department of Mathematics.
- 2011–15: Dean's Honour List.
  - Awarded to students from Faculty of Science with GPA in top 10%.
- 2011–15: Major Entrance Scholarship from McGill University.
  - Scholarship awarded upon admittance to McGill University on the basis of academic achievement and outstanding leadership in school or related activities.

# 10 Invitations

**Visiting Scholar with Noga Ron-Zewi** *Fall 2018*
*University of Haifa*

- Coding theory.

**Visiting Scholar with Eric Blais** *Summer 2016*
*University of Waterloo*

- Property testing.

**Research Assistant for Eyal Goren & Payman Kassaei** *Summer 2014*
*McGill University*

- Dynamics of algebraic correspondences (an emerging field containing elements of dynamics, algebraic geometry and $p$-adic analysis).
- Supported by an NSERC USRA grant.

**Research Assistant for F. Bruce Shepherd** *May & June 2013*
*McGill University*

- Machine Learning and Combinatorial Optimization, particularly the Envy-Free Pricing Problem.

# 11 Service to the Community

**Program Committees**

- ITCS '24.

**Refereeing**

- **External reviewer** for CCC '18, CRYPTO '18, ISIT '19, FOCS '19, SODA '20, ITCS '20 (2 papers), CRYPTO '21 (2 papers), CCC '21, ITW '21, Random '21, SODA '22, ITCS '22, STOC '22, TCC '22, SODA '23, Eurocrypt '23, STOC '23, ISIT '23, ICALP '23, CRYPTO '23, FOCS '23, RANDOM '23, TCC '23.
- **External reviewer** for SICOMP (3 times), IEEE TIT (5 times), JCSS, Random Structures & Algorithms.

**Organizational Roles**

- **Organizer** for *CWI Student Seminar*. January–May and September–December 2021.
- **Student member** of *Admissions Committee*. December 2017 and January 2018.
- **Organizer** for *CMU Theory Lunch*. January–May and September–December 2017.
- **Student Coordinator** for *CMU CSD Open House*. Spring 2016.

**Other Service Roles**

- **Computer Science Department Representative** for *Graduate Student Assembly* at Carnegie Mellon University. May 2018–May 2020.
- **Tutor** for *Math & Stats Helpdesk* at McGill University. 2013–15.
- **Vice-President, Executive** for *Society of Undergraduate Mathematics Students (SUMS) Council* at McGill University. 2013–14.
- **U1 (second-year student) Representative** for *SUMS Council* at McGill University. 2012–13.

# 12 Presentations & Invited Talks

**Presentations**

- *Oblivious Transfer with Constant Computational Overhead.* CWI Student Seminar. November 2022.
- *Zero-Rate Thresholds and New Capacity Bounds for List-Decoding and List-Recovery.* CWI Student Seminar. November 2022.
- *Zero-Rate Thresholds and New Capacity Bounds for List-Decoding and List-Recovery.* Inria. October 2022.
- *Two-Round Perfectly Secure Message Transmission with Optimal Transmission Rate.* CWI Student Seminar. February 2021.
- *Sharp threshold rates for random codes: or, how I learned to stop worrying and love the union bound.* Innovations in Theoretical Computer Science (ITCS) (short live talk). January 2021.
- *LDPC Codes Achieve List-Decoding Capacity.* Toyota Technical Insititue at Chicago (TTIC) External Speaker Series. December 2020.
- *Thresholds for Random Linear Codes.* CWI Student Seminar. September 2020.
- *Bounds for List-Decoding and List-Recovery of Random Linear Codes.* Random (long pre-recorded talk). August 2020.
- *LDPC Codes Achieve List-Decoding Capacity.* CWI RISC Seminar. November 2019.
- *Lossless Dimension Expanders via Linearized Polynomials and Subspace Designs.* Stanford Theory Lunch. March 2019.
- *Lossless Dimension Expanders via Linearized Polynomials and Subspace Designs.* Weizmann Institute Seminar. November 2018.
- *Lossless Dimension Expanders via Linearized Polynomials and Subspace Designs.* University of Tel Aviv Theory of Computation Seminar. November 2018.

- *On the List-Decodability of Random Linear Rank-Metric Codes.* Technion Coding Theory Seminar. November 2018.
- *Lossless Dimension Expanders via Linearized Polynomials and Subspace Designs.* Technion Theory Lunch. October 2018.
- *Lossless Dimension Expanders via Linearized Polynomials and Subspace Designs.* CMU Theory Lunch. September 2018.
- *On the List-Decodability of Random Linear Rank-Metric Codes.* IEEE International Symposium on Information Theory. June 2018.
- *Lossless Dimension Expanders via Linearized Polynomials and Subspace Designs.* Computational Complexity Conference. June 2018.
- *Lossless Dimension Expanders via Linearized Polynomials and Subspace Designs.* Harvard CMSA Workshop on Coding and Information Theory. April 2018.
- *On the List-Recovery of Random Linear Rank-Metric Codes.* CMU Theory Lunch. October 2017.
- *Stone Duality.* Seminars in Undergraduate Mathematics in Montreal. January 2015.
- *p-Adic Numbers: Basis Properties & Finite Field Extensions.* Canadian Undergraduate Mathematics Conference. July 2014.

**Posters**

- *Dynamics of Correspondences on the Projective Line.* McGill Undergraduate Research Conference. October 2014.

# 13 Other Information

**Hobbies**

- Running, cycling.
  - Completed 2019 Pittsburgh Marathon.
  - Survived 2019 "Dirty Dozen" cycling race.
- Playing guitar.
- Solving crosswords.

**Languages**

- English – Mother Tongue.
- French – Fluent. Successful completion of the DELF B2 examination.
- Dutch – Intermediate.