January 4, 2025

Curriculum Vitae of Joachim Rosenthal

Forchstrasse 438
CH-8702 Zollikon
Switzerland

University of Zürich
Mathematics Institute
Winterthurerstr 190
CH-8057 Zürich
Tel: +41-44-635-5884

Date of Birth: September 19, 1961
Place of Birth: Basel, Switzerland
Marital Status: Married, 4 children.

www.math.uzh.ch/rosen/
Citizenship: Switzerland.

Positions held:

7/04 – Present:	Professor of Applied Mathematics, University of Zürich.
8/16 – 7/20:	Vice-Dean, College of Science, University of Zürich.
8/09 – 7/13:	Co-Director (2009–2011), Director (2011–2013). Institute of Mathematics, University of Zürich.
8/06 – 7/14:	Adjunct Professor, University of Notre Dame.
2/03 – 8/06:	The Notre Dame Chair in Applied Mathematics.
8/01 – 8/06:	Concurrent Professor of Electrical Engineering, University of Notre Dame.
8/99 – 8/06:	Full Professor of Mathematics, University of Notre Dame.
7/99 – 6/00:	Invited guest Professor, EPFL, Switzerland.
8/95 – 8/99:	Associate Professor (with tenure), University of Notre Dame.
8/95 – 8/96:	Director of Undergraduate Studies, Mathematics, University of Notre Dame.
6/94 – 7/95:	Member of CWI, Amsterdam, The Netherlands.
8/90 – 8/95:	Assistant Professor of Mathematics, University of Notre Dame.
8/89 – 5/90:	Research Assistant and Lecturer, Washington University, St.Louis.
8/87 – 8/89:	Teaching and Research Assistant, Arizona State University, Arizona.

Education:

1990:	Ph.D. in Mathematics, Arizona State University, Arizona.
1986:	Diplom in Mathematics, University of Basel, Switzerland.

Editorial Boards:

- *Archiv der Mathematik*, Editor, 1/21–.
- *SIAM Journal on Applied Algebra and Geometry (SIAGA)*, Corresponding Editor, 1/16–12/20.
- *International Journal of Information and Coding Theory (IJOCT)*, Associate Editor, 1/14–.
- *Journal of Algebra Combinatorics Discrete Structures and Applications*, Area Editor, 1/14–.
- *Advances in Mathematics of Communications (AMC)*, Associate Editor, 1/07–.
- *Journal of Algebra and its Applications (JAA)*, Associate Editor, 5/05–.
- *Mathematics of Control Signals and Systems (MCSS)*, Associate Editor, 1/03 – 12/10.
- *SIAM Journal on Control and Optimization, (SICON)*, Associate Editor, 1/96 – 12/01. Corresponding Editor, 1/03–12/08.

- *Linear Algebra and its Applications (LAA)*, Associate Editor, 1/04–12/07.
- *Journal of Mathematical Systems, Estimation & Control*, Associate and Communicating Editor, 1/97 – 12/98.
- *Systems & Control Letters*, Associate Editor, 7/93 – 12/98.

Honors:

- Fellow IEEE.
- Fellow SIAM.
- Honorary Professor (2019), Universidad del Norte, Colombia.
- Doctor honoris causa (2025), University of Alicante, Spain.

Service:

- *Swiss Mathematical Society:*
  Treasurer (2020–2021), Vice President (2022–2023), President (2024–2025).
- *IEEE Information Theory Society:* Member of Board of Governors, 2020–2022.
- *RICAM:* The Johann Radon Institute for Computational and Applied Mathematics, Linz, Austria. Advisory Board, 2017–2027.
- *arXiv:* Moderator (together with Madhu Sudan) for the subject areas cs.IT and math.IT, 2004–2018.
- *MTNS*, International Symposium on the Mathematical Theory of Networks and Systems, Steering Committee 7/00 – Present, Chair of Steering Committee 8/02 – 7/04.
- *European COST Action IC1104 on Random Network Coding and Designs over* $GF(q)$, Management Committee 4/12 – 4/16.
- *Junior Euler Society*, an outreach program of the Mathematics Institute at the University of Zürich for gifted highschool students. Director 8/13–7/17.

Grants and Awards:

- Swiss National Science Foundation, grant on "Research in Algebraic Coding Theory", 2023–2027. (Grant# 212865, CHF765,324.00 PI)
- Armasuisse, grant on "Code based Cryptography", 2020-2024. (CHF420,000, PI).
- Swiss National Science Foundation, grant on "New Constructions of Convolutional Codes", 2020–2022. (Grant# 188430, CHF560,447.00 PI)
- Swiss National Science Foundation, grant on "Algebraic Constructions and Decoding of Rank Metric Codes with Applications to Network Coding and Code based Cryptography", 2016–2019. (Grant# 169510, CHF231,012.00 PI)
- Armasuisse, grant on "Noisy GCD", 2014-2015. (CHF311,520, PI).
- Swiss National Science Foundation, grant on "Algebraic Constructions of Subspace Codes", 2013–2016. (Grant# 149716, CHF285,780.00, PI)
- Swiss National Science Foundation, grant on "Computing Equipment", 2013–2014. (Grant# 144973, CHF120'220.00, PI)
- Swiss National Science Foundation, grant on "Algebraic Constructions and Decoding of Network Codes", 2011–2013. (Grant# 138080, CHF120,000.00, PI)
- Armasuisse, grant on "Factorization", 2011-2012. (CHF155,000, PI).
- Swiss National Science Foundation, grant on "New Public-Key Cryptosystems based on Algebra", 2010–2012. (Grant# 121874, CHF130,420.00, PI)

- Swiss National Science Foundation, grant on "Algebraic Constructions of Network Codes", 2009–2011. (Grant# 126948, CHF116,264.00, PI)
- Swiss National Science Foundation, grant on "New Public-Key Cryptosystems based on Algebra", 2008-2010. (Grant# 121874, CHF130,420, PI).
- Armasuisse, grant on "Stream Ciphers", 2008-2011. (CHF218,120, PI).
- Swiss National Science Foundation, grant on "Algebraic Constructions of Codes on Graphs", 2006–2009. (Grant# 113251, CHF206,368.00, PI)
- Swiss National Science Foundation, grant on "New Public-Key Cryptosystems", 2005-2008. (Grant# 107887, CHF184'809, PI).
- National Science Foundation, Division of Mathematical Sciences,
  Grant for IMA Summer Program for Graduate Students in Coding and Cryptography. (DMS-04-37347, $18'600, PI).
- Kaneb Teaching Award, University of Notre Dame, 2001.
- National Science Foundation, Computer & Information Sciences & Engineering.
  CCR-ITR Program, 2002-2006. (CCR-ITR-02-05310, $1'025'000, CO-PI).
- National Science Foundation, Division of Mathematical Sciences,
  Travel grant for MTNS 2002. (DMS-01-39236, $15'000, PI).
- Institute for Mathematics and its Applications, Minneapolis, Minnesota. Travel grant for MTNS 2002. ($5'000, PI).
- Faculty Research Program, 2002-2003. ($9720, Joint grant with K. Chandler)
- National Science Foundation, Division of Mathematical Sciences,
  Applied Mathematics Program, 2000-2003. (DMS-00-72383, $119'000, PI).
- National Science Foundation, Division of Mathematical Sciences,
  Applied Mathematics Program, 1997-2000. (DMS-96-10389, $105'000, PI).
- National Science Foundation, Division of Mathematical Sciences,
  Applied Mathematics Program, 1994-1997. (DMS-94-00965, $60'000, PI).
- Jesse H. Jones Faculty Research Fund, 1992-1993. (Joint grant with J. Migliore).
- National Science Foundation, Division of Mathematical Sciences,
  Applied Mathematics Program, 1992-1994. (DMS-92-01263, $30'000, PI).

Patents:

- M. Elia, J. Rosenthal, D. Schipani, *Evaluation of Polynomials*, International Patent Application, Pub. No. WO/2012/098157, International Application No. PCT/EP2012/050704, 18.01.2012.
- M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, D. Schipani, *Method and Apparatus for public-key Cryptography based on Error Correcting Codes*, International Patent Application, Pub. No. WO/2012/139919, International Application No. PCT/EP2012/056005, 02.04.2012.
- J. Rosenthal, D. Schipani, J. Lopez-Ramos, *System, Apparatus and Method for Efficient Multicast Key Distribution*, International Patent Application, Pub. No. WO/2012/160137, International Application No. PCT/EP2012/059707, 24.05.2012.
- M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, D. Schipani, *Metodo e sistema per la firma digitale*, Italian Patent Application No. MO2013A000140, May 2013.

Postdoctoral Research Associates supervised:

1. Christopher Monico, 7/2002-7/2003.
2. Jun Xu, 8/2003 – 5/2004.

3. Deepak Sridhara, 8/2003 – 1/2004 and 1/2005 – 4/2006.
4. Elisa Gorla, 8/2004 – 7/2008.
5. Gerard Maze, 10/2004 – 7/2007.
6. Mark Flanagan, 9/2008 – 12/2008.
7. Felix Fontein, 1/2011 – 2/2014.
8. Davide Schipani, 1/2014 – 12/2016.
9. Yilmaz Durgun, 8/2016 – 7/2017.
10. Javier de la Cruz, 8/2016 – 7/2017.
11. Elif Sacikara, 9/2019 – 8/2022.
12. Julia Lieb, 9/2019 – 8/2023.
13. Henry Chimal-Dzul, 9/2021 – 8/2022.

Ph.D. Students supervised:

T1. Eric York. PhD thesis: *Algebraic Description and Construction of Error Correcting Codes, a Systems Theory Point of View*, University of Notre Dame, May 1997.
Placement: National Security Agency.

T2. Paul Weiner. PhD thesis: *Multidimensional Convolutional Codes*, University of Notre Dame, May 1998.
Current: Professor (with tenure), Saint Mary's University of Minnesota.

T3. Brian Allen. PhD thesis: *Linear Systems Analysis and Decoding of Convolutional Codes*, University of Notre Dame, August 1999.
Placement: National Security Agency.

T4. Roxana Smarandache. PhD thesis: *Maximum Distance Separable Convolutional Codes, Construction and Decoding*, University of Notre Dame, August 2001.
Current: Professor (with tenure), University of Notre Dame.

T5. Christopher Monico. PhD thesis: *Semirings and Semigroup Actions in Public-Key Cryptography*, University of Notre Dame, May 2002.
Current: Associate Professor (with tenure), Texas Tech University, Lubbock, Texas.

T6. Gerard Maze. Thesis Title: *Algebraic Methods for Constructing One-Way Trapdoor Functions*, University of Notre Dame, May, 2003.
Current: Swiss Government.

T7. Guangyue Han. PhD thesis: *Space Time Coding with Multiple Antenna Systems*, University of Notre Dame, May, 2004.
Current: Professor (with tenure), Hong Kong University.

T8. Carmelo Interlando. PhD thesis: *Toward a Theory of One-Way Functions via Gate Complexity of Boolean Functions*, University of Notre Dame, December 2005.
Current: Professor (with tenure), San Diego State University, California.

T9. Christine Kelley. PhD thesis: *Pseudocodewords, Expander Graphs and the Algebraic Construction of Low-Density Parity-Check codes*, University of Notre Dame, May, 2006.
Current: Professor (with tenure), University of Nebraska.

T10. Ryan Hutchinson. PhD thesis: *Generic Properties of Convolutional Codes*, University of Notre Dame, May 2006.
Current: Associate Professor, Hillsdale College, Michigan.

T11. Jens Zumbrägel. PhD thesis: *Public Key Cryptography Based on Simple Semirings*, Universität Zürich, December 2008.
Current: Associate Professor, University of Passau, Germany.

T12. Felix Fontein. PhD thesis: *The Infrastructure of a Global Field and Baby Step – Giant Step Algorithms*, Universität Zürich, March 2009.
Current: Industry.

T13. Virtudes Tomás. (Advised with J. Climent). PhD thesis: *Complete-MDP Convolutional Codes over the Erasure Channel*, Universidad de Alicante, July 2010.
Current: Industry.

T14. Alina Ostafe. (Advised with M. Brodmann). PhD thesis: *Polynomial Dynamics and Pseudorandomness*, Universität Zürich, October 2010.
Current: Associate Professor (with tenure), University of New South Wales, Australia.

T15. Felice Manganiello. PhD thesis: *Spread Codes and more General Network Codes*, Universität Zürich, October 2011.
Current: Associate Professor (with tenure), Clemson University.

T16. Davide Schipani. PhD thesis: *Efficient Decoding of Cyclic Codes and Applications in Cryptography*, Universität Zürich, October 2012.
Current: Industry.

T17. Anna-Lena Trautmann. PhD thesis: *Constructions, Decoding and Automorphisms of Subspace Codes*, Universität Zürich, July 2013.
Current: Associate Professor (with tenure), University of St. Gallen.

T18. Urs Wagner. PhD thesis: *Considerations on Computational Lattice Problems*, Universität Zürich, July 2013.
Current: Swiss Government.

T19. Giacomo Micheli. PhD thesis: *Densitites over Global Fields, Arithmetic of Subfield Preserving Maps and Applications to Cryptography* , Universität Zürich, October 2015.
Current: Associate Professor, University of South Florida.

T20. Kyle Marshall. PhD thesis: *A Study of Cryptographic Systems based on Rank Metric Codes*, Universität Zürich, July 2016.
Current: Industry.

T21. Julia Lieb. (Advised with U. Helmke and P. Müller). PhD thesis: *Counting Polynomial Matrices over Finite Fields with Certain Coprimeness Properties and Applications to Linear Systems and Coding Theory*, Universität Würzburg, July 2017.
Current: Assistant Professor University of Ilmenau, Germany.

T22. Reto Schnyder. PhD thesis: *Shifted Eisenstein Polynomials, Irreducible Compositions of Polynomials and Group Key Exchanges*, Universität Zürich, July 2017.
Current: Industry.

T23. Tovohery Hajatiana Randrianarisoa. PhD thesis: *Rank Metric Codes, Codes Using Linear Complexity and Application to Public Key Cryptosystem*, Universität Zürich, July 2018.
Current: PostDoc, Umea University, Sweden.

T24. Alessandro Neri. PhD thesis: *Algebraic Theory of Rank-Metric Codes: Representations, Invariants and Density Results*, Universität Zürich, July 2019.
Current: Assistant Professor, University of Naples Federico II, Italy.

T25. Karan Khathuria. PhD thesis: *Algebraic Study of Some Recent Asymmetric Cryptosystems*, Universität Zürich, November 2020.
Current: Industry.

T26. Violetta Weger. PhD thesis: *Information Set Decoding in the Lee Metric and the Local to Global Principle for Densities*, Universität Zürich, November 2020.
Current: Assistant Professor, Technical University Munich, Germany.

T27. Gianira Alfarano. PhD thesis: *Algebraic, Combinatorial and Geometric Aspects of Some Error-Correcting Codes*, Universität Zürich, August 2022.
Current: Assistant Professor, University of Rennes, France.

T28. Simran Tinani. *Algebraic Methods in Asymmetric Cryptography – Algorithms, Con-*

structions, and Attacks, Universität Zürich, June 2023.
Current: Industry.

T29. Jessica Bariffi. *Analysis and Decoding of Linear Lee-Metric Codes with Application to Code-Based Cryptography*, Universität Zürich, May 2024.
Current: PostDoc, Technical University Munich, Germany.

T30. Niklas Gassner. *Codes over Rings, their Generic Decoding and their Use in Code-Based Cryptography*, Universität Zürich, December 2024.
Current: Industry.

T31. Silvia Sconza. Started February 2023.

T32. Michael Schaller. Started September 2023.

T33. Beatrice Toesca. Started September 2023.

T34. Abhinaba Mazumder. Started September 2023.

T35. Abigail Sutton. Started February 2024.

T36. Giacomo Borin. Started February 2024.

Masters Students supervised:

1. Changyan Di. MS Degree University of Notre Dame, 2000.
2. Marylee Ruehle. MS Degree University of Notre Dame, 2001.
3. Thomas Doherty. MS Degree University of Notre Dame, 2001.
4. Ali Pusane. MS Degree University of Notre Dame, 2006.
5. Ariel Amir. Diplom Universität Zürich, 2006.
6. Helen Stassen. Diplom Universität Zürich, 2006.
7. Wufei Zhang. MS Degree University of Notre Dame, 2007.
8. Andres Gentzen. MS Degree Universität Zürich, 2007.
9. Richard Koeppel. Diplom Universität Zürich, 2007.
10. Michele Casartelli. Diplom Universität Zürich, 2007.
11. Marion Wimmer, Diplom Universität Zürich, 2008.
12. Urs Wagner, MS Degree Universität Zürich, 2008.
13. Sandra Steiner, Diplom Universität Zürich, 2009.
14. Manuel Ribic, MS Degree Universität Zürich, 2009.
15. Vita Pasic, MS Degree Universität Zürich, 2009.
16. Dominik Looser, MS Degree Universität Zürich, 2010.
17. Karin Sommer, MS Degree Universität Zürich, 2011.
18. Ian Hersberger, MS Degree Universität Zürich, 2012.
19. Andrea De Giorgi, MS Degree Universität Zürich, 2012.
20. Amaro Barreal, MS Degree Universität Zürich, 2013.
21. Rahel Spiess, MS Degree Universität Zürich, 2013.
22. Kevin Brand, MS Degree Universität Zürich, 2013.
23. Helen Riedtmann, MS Degree Universität Zürich, 2013.
24. Milan Markovic, MS Degree Universität Zürich, 2014.
25. Mustafa Aylidere, MS Degree Universität Zürich, 2014.
26. Isabelle Raemy, MS Degree Universität Zürich, 2015.
27. Marko Seric, MS Degree Universität Zürich, 2015.
28. Christoph Irniger, MS Degree Universität Zürich, 2015.
29. Edoardo Dotti, MS Degree Universität Zürich, 2015.

30. Martin Holzer, MS Degree Universität Zürich, 2015.
31. Michael Hartmann, MS Degree Universität Zürich, 2015.
32. Dominique Negele, MS Degree Universität Zürich, 2015.
33. Christoph Gasche, MS Degree Universität Zürich, 2016.
34. Sophie Leuenberger, MS Degree Universität Zürich, 2016.
35. Amos Cattaneo, MS Degree Universität Zürich, 2016.
36. Chiara Agnese Salvini, MS Degree Universität Zürich, 2017.
37. Violetta Weger, MS Degree Universität Zürich, 2017.
38. Nicole Gubser, MS Degree Universität Zürich, 2017.
39. Alessandro Verzasconi, MS Degree Universität Zürich, 2018.
40. Nicole Rohrer, MS Degree Universität Zürich, 2018.
41. Pascal Christinat, MS Degree Universität Zürich, 2018.
42. Andreas Bolfing, MS Degree Universität Zürich, 2019.
43. Davide Walder, MS Degree Universität Zürich, 2019.
44. Raffael Schüürmann, MS Degree Universität Zürich, 2019.
45. Anina Gruica, MS Degree Universität Zürich, 2020.
46. Jessica Bariffi, MS Degree Universität Zürich, 2020.
47. Marc Newman, MS Degree Universität Zürich, 2020.
48. Sabrina Sewer, MS Degree Universität Zürich, 2020.
49. Andreia Venzin, MS Degree Universität Zürich, 2021.
50. Sebastian Heri, MS Degree Universität Zürich, 2021.
51. Niko Van Wyk, MS Degree Universität Zürich, 2021.
52. Kilian Fabian Werder, MS Degree Universität Zürich, 2022.
53. Martin Bergamin, MS Degree Universität Zürich, 2022.
54. Sascha Hoppler, MS Degree Universität Zürich, 2022.
55. Josua Rutishauser, MS Degree Universität Zürich, 2022.
56. Danai Hansmann, MS Degree Universität Zürich, 2023.
57. Diana Rauseo, MS Degree Universität Zürich, 2023.
58. Yves Krähenbühl, MS Degree Universität Zürich, 2023.
59. Tatjana Bossalini, MS Degree Universität Zürich, 2023.
60. Vivien Caroline Bammert, MS Degree Universität Zürich, 2024.
61. Bettina Wohlfender, MS Degree Universität Zürich, 2024.
62. Diana Patrizia Teider, MS Degree Universität Zürich, 2024.
63. Jens Kopp, MS Degree Universität Zürich, 2024.

External Examiner on Ph.D. Dissertations:

1. Pascal Vontobel, ETH, Zürich, Switzerland.
   Date of defense: December 13, 2002.
2. Henry O'Keeffe, University College Cork, Ireland.
   Date of defense: October 21, 2003.
3. Maria Victoria Herranz Cuadrado, Universidad Miguel Hernandez, Spain.
   Date of defense: March 2, 2007.
4. F.L. Tsang, University of Groningen, The Netherlands.
   Date of defense: June 23, 2008.
5. Andreas Kendziorra, University College Dublin, Ireland.

Date of defense: May 1, 2012.

6. Sara Diaz Cardell, University of Alicante, Spain.
   Date of defense: August 8, 2012.
7. Ghid Maatouk, EPFL, Switzerland.
   Date of defense: July 2, 2013.
8. Toni Ernvall, Turku University, Turku, Finland.
   Date of defense: February 13, 2015.
9. Paresh Saxena, Universitat Autonoma, Barcelona, Spain.
   Date of defense: February 23, 2015.
10. Maria Antonela Lodroman, Universidad de Almeria, Spain.
    Date of defense: May 6, 2016.
11. Alberto Ravagnani, University of Neuchatel, Switzerland.
    Date of defense: September 1, 2016.
12. Umberto Martínez-Penas, Aalborg University, Denmark.
    Date of defense: November 13, 2017.
13. Miguel Angel Navarro Perez, University of Alicante, Spain.
    Date of defense: January 11, 2022.
14. Akansha Arora, IIIT Delhi, India.
    Date of defense: March 31, 2023.
15. Rocco Mora, INRIA, Paris.
    Date of defense: April 7, 2023.
16. Maria Dolores Gomez Olvera, Universidad de Almeria, Spain.
    Date of defense: February 16, 2024.
17. Austin Dukes, University of South Florida, USA.
    Date of defense: June 12, 2024.
18. Flavio Salizzoni, University of Neuchatel, Switzerland.
    Date of defense: June 26, 2024.

External Examiner of Institutes at Universities:

1. Member of Expert Panel to evaluate Departments of Mathematics and Theoretical Computer Science at KTH, Stockholm, Sweden, June 24–27, 2008.
2. Member of Review Panel of Mathematics Institute and units for engineering Mathematics and Geometry at Innsbruck University, Austria, January 16–17, 2009.
3. Member of Review Panel of Mathematics and Physics Departments at Aalto University, Helsinki, Finland, June 7–12, 2009.
4. Member of Review Panel of several departments at Mid-Sweden University, November 10–14, 2013.
5. Member of Expert Panel at INRIA in Paris, March 14–15, 2017.
6. Member of Expert Panel to evaluate the School of Data Science at City University of Hong Kong, September 4-7, 2023.

Organization of Conferences, Workshops and Sessions:

MTNS 1993, International Symposium on the Mathematical Theory of Networks and Systems, Regensburg, Germany, August 2– 6, 1993. Organizer of invited session: "Algebro-Geometric Methods in Systems Theory".

34th IEEE Conference on Decision and Control, New Orleans, Louisiana, December 13–15, 1995. Organizer of Invited Session: "Connections between Systems Theory and Coding Theory".

University of Notre Dame Symposium on Current and Future Directions in Applied Mathematics, University of Notre Dame, Notre Dame, Indiana, April 18–21, 1996. Co-organizer of this international symposium and organizer of a special workshop in systems theory. (130 participants from 15 countries).

MTNS 1996, International Symposium on the Mathematical Theory of Networks and Systems, St. Louis, Missouri, June 24–28, 1996. Organizer of invited mini-course: "Inverse Eigenvalue Problems for Linear Multivariable Systems" and organizer of the invited session: "Inverse Eigenvalue Problems in Control Theory".

Midwest Algebraic Geometry Conference, University of Notre Dame, Notre Dame, Indiana, November 7–9, 1997. Member of Organizing Committee of this international conference. (160 participants from 10 countries).

MTNS 1998, International Symposium on the Mathematical Theory of Networks and Systems, Padova, Italy, July 6–10, 1998. Organizer (jointly with H.A. Loeliger) of a Minisymposium on *Systems, Codes, and Graphical Models*.

IMA Summer Program on Codes, Systems and Graphical Models, Minneapolis, August 2–13, 1999. Organizer with G.D. Forney, B. Marcus and A. Vardy of this event.

ISIT 2002, IEEE International Symposium on Information Theory, Lausanne, Switzerland, June 30–July 5, 2002. Technical Program Committee.

MTNS 2002, International Symposium on the Mathematical Theory of Networks and Systems, University of Notre Dame, August, 2002. Symposium Chair of this conference. (420 participants from 31 countries)

Institute of Mathematics and its Applications PI Summer Program for Graduate Students, held at the University of Notre Dame, June 7–27, 2004. Organizer of this event.

Third Workshop on Coding and Systems, University of Zürich, December 8–9, 2006. Organizer of this event.

IMA Workshop on Complexity, Coding, and Communications, Minneapolis, April 16–20, 2007. Organizer (with P. Bürgisser, K. Mulmuley, J.M. Rojas and M. Sudan) of event.

Oberwolfach Workshop on Coding Theory, Oberwolfach, Germany, December 2–8, 2007. Organizer with A. Shokrollahi of this event.

ITW, IEEE Information Theory Workshop, Dublin, Ireland, August 30– September 3, 2010. Conference Chair (with M. Greferath).

Solving Polynomial Equations, KTH Stockholm, Sweden, February 21–25, 2011. Organizer with S. Di Rocco and B. Sturmfels.

Dagstuhl Seminar on Coding Theory, Dagstuhl, Germany, November 13–18, 2011. Organizer with A. Shokrollahi and J. Walker.

Trends in Coding Theory, Centro Stefano Franscini, Ascona (Switzerland), October 28–November 2, 2012. Organizer with A. Shokrollahi and E. Gorl).

Zurich COST Meeting - Random Network Coding and Designs over GF(q), University of Zürich, June 20–21, 2013. Organizer of this event.

DLP 2014, Centro Stefano Franscini, Ascona (Switzerland), May 5–9, 2014. Organizer with Dimitar Jetchev, Emmanuel Kowalski, Arjen Lenstra, Philippe Michel.

DIMACS Workshop on The Mathematics of Post-Quantum Cryptography, DIMACS Center, Rutgers University, January 12 - 16, 2015. Organizer with Nigel Boston, Elisa Gorla and Tanja Lange.

SIAM Conference on Applied Algebraic Geometry, Daejeon, Korea, August 3–7, 2015. Together with Greg Blekherman chair of the international program committee.

Mathematical Coding Theory in Multimedia Streaming, Banff, Canada, October 11–16, 2015. Organizer with Heide Gluesing-Luerssen, Ashish Khisti and Emina Soljanin.

The First Colombian Workshop on Coding Theory (CWC 17), Barranquilla, Colombia, November 24-27, 2015. Organizer with Javier de la Cruz, Wilson Olaya and Wolfgang Willems.

Second Colombian Workshop on Coding Theory (CWC 19), Barranquilla, Colombia, January 15–18, 2019. Organizer with Javier de la Cruz, David Karpuk and Wolfgang Willems.

Oberwolfach Workshop on Contemporary Coding Theory, Oberwolfach, Germany, March 17–23, 2019. Organizer with C. Hollanti and M. Greferath of this event.

SIAM Conference on Applied Algebraic Geometry, Bern, Switzerland, July 9–13, 2019. Local organizer (with E. Delucchi, J. Draisma and E. Gorla) of this event.

Workshop on Convolutional Codes, University of Zurich, June 5–9, 2023. Organizer (with G. Alfarano and J. Lieb) of this event.

VT-Swiss Coding Theory and Cryptography Summer School, Riva San Vitale, Switzerland July 1–5, 2024. Organizer (with F. Manganiello, G. Matthews, H. Lopez, E. Gorla and A. Horlemann) of this event.

ISIT 2024, IEEE International Symposium on Information Theory, Athens, Greece, July 7-12. 2024. International Program Chair (with C. Fragouli and I. Kontoyiannis).

Publications

Books and Monographs:

[B1] J. Rosenthal. *Geometric Methods for Feedback Stabilization of Multivariable Linear Systems*. PhD thesis, Arizona State University, 1990.

[B2] M. Alber, B. Hu, and J. Rosenthal, editors. *Current and Future Directions in Applied Mathematics*, Birkhäuser Verlag, Boston-Basel-Berlin, 1997.

[B3] B. Marcus and J. Rosenthal, editors. *Codes Systems and Graphical Models*, *IMA Vol. 123 in Math. and its Appl.*, series published by Springer Verlag, 2001.

[B4] J. Rosenthal and D. Gilliam, editors. *Mathematical Systems Theory in Biology, Communication, Computation and Finance*, *IMA Vol. 134*, series published by Springer Verlag, 2003.

Journal Publications and Chapter of Books:

1989

[1] J. Rosenthal. Tuning natural frequencies by output feedback. In K. Bowers and J. Lund, editors, *Computation and Control*, pages 276–282. Birkhäuser Verlag, Boston, 1989.

1992

[2] J. Rosenthal. New results in pole assignment by real output feedback. *SIAM J. Control Optim.*, 30(1):203–211, 1992.

[3] J. Rosenthal. A compactification of the space of multivariable linear systems using geometric invariant theory. *Journal of Math. Systems, Estimation & Control*, 2(1):111–121, 1992.

1993

[4] J. Rosenthal and X. Wang. What is the distance between two autoregressive systems. In K. Bowers and J. Lund, editors, *Computation and Control III*, pages 333–340. Birkhäuser Verlag, Boston, 1993.

[5] X. Wang and J. Rosenthal, "Hasse Diagram and Dynamic Feedback of Linear Systems," *Computation and Control III* (K. Bowers and J. Lund, eds.) Birkhäuser Verlag, Boston, 1993, pp. 391–398.

1994

[6] J. Rosenthal. On dynamic feedback compensation and compactification of systems. *SIAM J. Control Optim.*, 32(1):279–296, 1994.

[7] M. S. Ravi and J. Rosenthal. A smooth compactification of the space of transfer functions with fixed McMillan degree. *Acta Appl. Math*, 34:329–352, 1994.

[8] J. A. Ball and J. Rosenthal. Pole placement, internal stabilization and interpolation conditions for rational matrix functions: a Grassmannian formulation. In P. van Dooren and B. Wyman, editors, *Linear Algebra for Control Theory*, volume 62 of *IMA Vol. in Math. and its Appl.*, pages 21–30. Springer Verlag, 1994.

[9] J. Rosenthal, M. Sain, and X. Wang. Topological considerations for autoregressive systems with fixed Kronecker indices. *Circuits Systems Signal Process*, 13(2–3):295–308, 1994.

[10] X. Wang and J. Rosenthal. A cell structure for the set of autoregressive systems. *Linear Algebra Appl.*, 205/206:1203–1226, 1994.

[11] M. S. Ravi, J. Rosenthal, and X. Wang. On generic stabilizability and pole assignability. *Systems & Control Letters*, 23(2):79–84, 1994.

1995

[12] U. Helmke and J. Rosenthal. Eigenvalue inequalities and Schubert calculus. *Mathematische Nachrichten*, 171:207–225, 1995.

[13] B. K. Ghosh and J. Rosenthal. A generalized Popov-Belevitch-Hautus test of observability. *IEEE Trans. Automat. Control*, AC-40(1):176–180, 1995.

[14] M. S. Ravi and J. Rosenthal. A general realization theory for higher order linear differential equations. *Systems & Control Letters*, 25(5):351–360, 1995.

[15] M. S. Ravi, J. Rosenthal, and X. Wang. On decentralized dynamic pole placement and feedback stabilization. *IEEE Trans. Automat. Contr.*, AC-40(9):1603–1614, 1995.

[16] J. Rosenthal, J. M. Schumacher, and J. C. Willems. Generic eigenvalue assignment by memoryless real output feedback. *Systems & Control Letters*, 26:253–260, 1995.

1996

[17] J. Rosenthal. An observability criterion for dynamical systems governed by Riccati differential equations. *IEEE Trans. Automat. Contr.*, AC-41(3):434–436, 1996.

[18] M. S. Ravi, J. Rosenthal, and X. Wang. Dynamic pole assignment and Schubert calculus. *SIAM J. Control Optim.*, 34(3):813–832, 1996.

[19] J. Rosenthal and X. Wang. Output feedback pole placement with dynamic compensators. *IEEE Trans. Automat. Contr.*, AC-41(6):830–843, 1996.

[20] J. Rosenthal, J. M. Schumacher, and E.V. York. On behaviors and convolutional codes. *IEEE Trans. Inform. Theory*, 42(6):1881–1891, 1996.

1997

[21] J. Rosenthal and E.V. York. On the generalized Hamming weights of convolutional codes. *IEEE Trans. Inform. Theory*, 43(1):330–335, 1997.

[22] U. Helmke, J. Rosenthal, and J. M. Schumacher. A controllability test for general first-order representations. *Automatica*, 33(2):193–201, 1997.

[23] J. Rosenthal and X. Wang. Inverse eigenvalue problems for multivariable linear systems. In C. I. Byrnes, B. N. Datta, D. Gilliam, and C. F. Martin, editors, *Systems and Control in the Twenty-First Century*, pages 289–311. Birkäuser, Boston-Basel-Berlin, 1997.

[24] M. S. Ravi, J. Rosenthal, and J. M. Schumacher. Homogeneous behaviors. *Math. Contr., Sign., and Syst.*, 10:61–75, 1997.

[25] J. Rosenthal and J. M. Schumacher. Realization by inspection. *IEEE Trans. Automat. Contr.*, AC-42(9):1257–1263, 1997.

[26] W. Helton, J. Rosenthal, and X. Wang. Matrix extensions and eigenvalue completions, the generic case. *Trans. Amer. Math. Soc.*, 349(8):3401–3408, 1997.

1998

[27] M. S. Ravi, J. Rosenthal, and X. Wang. Degree of the generalized Plücker embedding of a quot scheme and quantum cohomology. *Math. Ann.*, 311(1):11–26, 1998.

[28] J. Rosenthal and F. Sottile. Some remarks on real and complex output feedback. *Systems & Control Letters*, 33(2):73–80, 1998.

[29] J. Rosenthal and J. C. Willems. Open problems in the area of pole placement. In V.D. Blondel, E.D. Sontag, M. Vidyasagar, and J.C. Willems, editors, *Open Problems in Mathematical Systems and Control Theory*, chapter 37, pages 181–191. Springer-Verlag, London, Berlin, New York, 1998.

[30] J. Rosenthal. An optimal control theory for systems defined over finite rings. In V.D. Blondel, E.D. Sontag, M. Vidyasagar, and J.C. Willems, editors, *Open Problems in Mathematical Systems and Control Theory*, chapter 38, pages 193–201. Springer-Verlag, London, Berlin, New York, 1998.

[31] V. Lomadze, M. S. Ravi, J. Rosenthal, and J. M. Schumacher. A behavioral approach to singular systems. *Acta Appl. Math*, 54(3):331–344, 1998.

1999

[32] B.M. Allen and J. Rosenthal. A matrix Euclidean algorithm induced by state space realization. *Linear Algebra Appl.*, 288:105–121, 1999.

[33] J. Rosenthal. An algebraic decoding algorithm for convolutional codes. In G. Picci and D.S. Gilliam, editors, *Dynamical Systems, Control, Coding, Computer Vision: New Trends, Interfaces, and Interplay*, pages 343–360. Birkäuser, Boston-Basel-Berlin, 1999.

[34] J. Leventides, J. Rosenthal, and X. Wang. The pole placement problem via PI feedback controllers. *Internat. J. Control*, 72(12):1065–1077, 1999.

[35] J. Rosenthal and E.V. York. BCH convolutional codes. *IEEE Trans. Inform. Theory*, 45(6):1833–1844, 1999.

[36] J. Rosenthal and R. Smarandache. Maximum distance separable convolutional codes. *Appl. Algebra Engrg. Comm. Comput.*, 10(1):15–32, 1999.

2000

[37] J. Rosenthal and X. Wang. Eigenvalue completions by affine varieties. *Proc. of Amer. Math. Soc.*, 128(3):643–646, 2000.

[38] H. Gluesing-Luerssen, J. Rosenthal, and P. A. Weiner. Duality between multidimensional convolutional codes and systems. In F. Colonius, U. Helmke, F. Wirth, and D. Prätzel-Wolters, editors, *Advances in Mathematical Systems Theory, A Volume in Honor of Diederich Hinrichsen*, pages 135–150. Birkhauser, Boston, 2000.

2001

[39] J. Rosenthal. Connections between linear systems and convolutional codes. In B. Marcus and J. Rosenthal, editors, *Codes, Systems and Graphical Models*, IMA Vol. 123, pages 39–66. Springer-Verlag, 2001.

[40] J. Rosenthal and A. Zelevinsky. Multiplicities of points on Schubert varieties in Grassmannians. *Journal of Algebraic Combinatorics*, 13:213–218, 2001.

[41] R. Smarandache, H. Gluesing-Luerssen and J. Rosenthal. Constructions of MDS-convolutional codes. *IEEE Trans. Inform. Theory*, 47(5):2045–2049, 2001

[42] J. Rosenthal and X. Wang. The multiplicative inverse eigenvalue problem over an algebraically closed field. *SIAM J. Matrix Anal. Appl.*, 23(2):517–523, 2001.

2002

[43] J. Rosenthal. Minimal bases of rational vector spaces and their importance in algebraic systems theory. In R. E. Blahut and R. Koetter, editors, *Codes, Graphs, and Systems*, pages 345–357. Kluwer Academic Publishers, 2002.

[44] V. D. Blondel, D. Hinrichsen, J. Rosenthal, and P. Van Dooren. Fourth special issue on linear systems and control, preface. *Linear Algebra Appl.*, 351–352:1–9, 2002.

[45] M. S. Ravi, J. Rosenthal, and U. Helmke. Output feedback invariants. *Linear Algebra Appl.*, 351–352:623–637, 2002.

2003

[46] J. Rosenthal. A polynomial description of the Rijndael advanced encryption standard. *J. Algebra Appl.*, 2(2):223–236, 2003.

2004

[47] M. Kim, J. Rosenthal, and X. Wang. Pole placement and matrix extension problems: A common point of view. *SIAM J. Control Optim.*, 42(6):2078 - 2093, 2004.

[48] D. N. Hoover, R. Longchamp, and J. Rosenthal. Two-degree-of-freedom ℓ_2-optimal tracking with preview. *Automatica*, 40(1):155-162, 2004.

2005

[49] R. Hutchinson, J. Rosenthal and R. Smarandache. Convolutional codes with maximum distance profile. *Systems & Control Letters*, 54(1):53–63, 2005.

[50] J. Rosenthal. The Hermann-Martin curve. In *New directions and applications in control theory*, volume 321 of *Lecture Notes in Control and Inform. Sci.*, pages 353–365. Springer, Berlin, 2005.

2006

[51] H. Gluesing-Luerssen, J. Rosenthal, and R. Smarandache. Strongly MDS convolutional codes. *IEEE Trans. Inform. Theory*, 52(2):584–598, 2006.

[52] G. Han and J. Rosenthal. Geometrical and numerical design of structured unitary space time constellations. *IEEE Trans. Inform. Theory*, 52(8):3722–3735, 2006.

[53] G. Han and J. Rosenthal. Unitary space time constellation analysis: An upper bound for the diversity. *IEEE Trans. Inform. Theory*, 52(10):4713–4721, 2006.

[54] U. Helmke, J. Rosenthal, and X. A. Wang. Output feedback pole assignment for transfer functions with symmetries. *SIAM J. Control Optim.*, 45(5):1898–1914, 2006.

2007

[55] J. J. Climent, E. Gorla, and J. Rosenthal. Cryptanalysis of the CFVZ cryptosystem. *Adv. in Math. of Communications*, 1(1):1–11, 2007.

[56] C. Kelley, D. Sridhara, and J. Rosenthal. Tree-based construction of LDPC codes having good pseudocodeword weights. *IEEE Trans. Inform. Theory*, 53(4):1460–1478, 2007.

[57] G. Maze, C. Monico and J. Rosenthal. Public key cryptography based on semigroup actions. *Adv. in Math. of Communications*, 1(4):489–507, 2007

[58] J. Rosenthal and P. Weiner. Coding theory. In L. Hogben, editor, *Handbook of Linear Algebra*, Discrete Mathematics and its Applications (Boca Raton), chapter 61, pages 61.1–61.14. Chapman & Hall/CRC, Boca Raton, FL, 2007.

[59] C. A. Kelley, J. Rosenthal, and D. Sridhara. Systems theoretic questions in coding theory. *PAMM, Proc. Appl. Math. Mech.*, 7(1):1030601–1030602, 2007. Proceedings of Sixth International Congress on Industrial Applied Mathematics (ICIAM07).

2008

[60] C. A. Kelley, D. Sridhara, and J. Rosenthal. Zig-zag and replacement product graphs and LDPC codes. *Advances in Mathematics of Communications*, 2(4):347–372, November 2008.

2009

[61] J. Rosenthal. Der Mathematiker Emanuel Lasker. In R. Forster, S. Hansen, and M. Negele, editors, *Emanuel Lasker: Denker, Weltenbürger, Schachweltmeister*, pages 213–230. Exzelsior Verlag, Berlin, 2009.

2010

[62] V. Tomás and J. Rosenthal. Convolutional codes : A module theoretic approach. In *Algèbre and Télécommunications*, Journée Annuelle, pages 25–41. Société Mathématique de France, 2010.

[63] E. Gorla and J. Rosenthal. Pole placement with fields of positive characteristic. In X. Hu, U. Jonsson, B. Wahlberg, and B. Ghosh, editors, *Three Decades of Progress in Control Sciences*, pages 215—231. Springer Verlag, 2010.

2011

[64] G. Maze, J. Rosenthal, and U. Wagner. Natural density of rectangular unimodular integer matrices. *Linear Algebra Appl.*, 434(5):1319–1324, 2011.

2012

[65] M. Elia, J. Rosenthal, and D. Schipani. Polynomial evaluation over finite fields: new algorithms and complexity bounds. *Appl. Algebra Engrg. Comm. Comput.*, 23(3-4):129–141, 2012.

[66] E. Gorla, F. Manganiello, and J. Rosenthal. An algebraic approach for decoding spread codes. *Adv. in Math. of Communications*, 6(4):443–466, 2012.

[67] V. Tomás, J. Rosenthal, and R. Smarandache. Decoding of convolutional codes over the erasure channel. *IEEE Trans. Inform. Theory*, 58(1):90 –108, 2012.

2013

[68] J. Rosenthal and A.-L. Trautmann. A complete characterization of irreducible cyclic orbit codes and their Plücker embedding. *Des. Codes Cryptogr.*, 66(1–3):275–289, 2013.

[69] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani. Using LDGM codes and sparse syndromes to achieve digital signatures. In Philippe Gaborit, editor, *Post-Quantum Cryptography: 5th International Workshop, PQCrypto 2013, Limoges, France, June 4-7, 2013. Proceedings*, pages 1–15. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[70] J. Rosenthal and A.-L. Trautmann. Decoding of subspace codes, a problem of Schubert calculus over finite fields. In K. Hüper and J. Trumpf, editors, *Mathematical System Theory – Festschrift in Honor of Uwe Helmke on the Occasion of his Sixtieth Birthday*, pages 353–366. CreateSpace, 2013.

[71] A.-L. Trautmann, F. Manganiello, M. Braun, and J. Rosenthal. Cyclic orbit codes. *IEEE Trans. Inform. Theory*, 59(11):7386–7404, November 2013.

2014

[72] J. Rosenthal, N. Silberstein, and A.-L. Trautmann. On the geometry of balls in the Grassmannian and list decoding of lifted Gabidulin codes. *Des. Codes Cryptogr.*, 73(2):393–416, 2014.

2015

[73] G. Micheli, J. Rosenthal, and P. Vettori. Linear spanning sets for matrix spaces. *Linear Algebra Appl.*, 483:309–322, 2015.

2016

[74] R. Schnyder, J. A. Lopez-Ramos, J. Rosenthal, and D. Schipani. An active attack on a multiparty key exchange protocol. *Journal of Algebra Combinatorics Discrete Structures and Applications*, 3:31–36, 2016.

[75] K. Marshall, D. Schipani, A.-L. Trautmann, and J. Rosenthal. Subspace fuzzy vault. volume 358 of *Lecture Notes in Electrical Engineering*, pages 163–172. Springer Verlag, 2016.

[76] G. Micheli, J. Rosenthal, and R. Schnyder. An information rate improvement for a polynomial variant of the Naccache-Stern knapsack cryptosystem. volume 358 of *Lecture Notes in Electrical Engineering*, pages 173–180. Springer Verlag, 2016.

[77] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani. Enhanced public key security for the McEliece cryptosystem. *Journal of Cryptology*, pages 1–27, 2016.

2017

[78] J. A. Lopez-Ramos, J. Rosenthal, D. Schipani, and R. Schnyder. Group key management based on semigroup actions. *Journal of Algebra and Its Applications*, 16(08):1750148, 2017.

[79] J.A. Alvarez-Bermejo, J. A. López Ramos, J. Rosenthal, and D. Schipani. Managing key multicasting through orthogonal systems. *Journal of Discrete Mathematical Sciences and Cryptography*, 20(8):1721–1740, 2017.

[80] J. Bolkema, H. Gluesing-Luerssen, C.A. Kelley, K.E. Lauter, B. Malmskog, and J. Rosenthal. Variations of the McEliece Cryptosystem. In *Algebraic Geometry for Coding Theory and Cryptography*, pages 129–150. Springer, 2017.

[81] D. Napp, R. Pinto, J. Rosenthal, and F. Santana. Column rank distances of rank metric convolutional codes. In *Coding theory and applications*, volume 10495 of *Lecture Notes in Comput. Sci.*, pages 248–256. Springer, Cham, 2017.

2018

[82] F. Arias, J. de la Cruz, J. Rosenthal, and W. Willems. On q-Steiner systems from rank metric codes. *Discrete Math.*, 341(10):2729–2734, 2018.

[83] A.-L. Horlemann-Trautmann and J. Rosenthal. Constructions of constant dimension codes. In M. Greferath, M. Pavcevic, N. Silberstein, and M.A. Vazquez-Castro, editors, *Network Coding and Subspace Design*, Signals and Communication Technology, pages 25–42. Springer Verlag, 2018.

[84] A.-L. Horlemann-Trautmann, K. Marshall, and J. Rosenthal. Extension of Overbeck's attack for Gabidulin based cryptosystems. *Designs, Codes and Cryptography*, 86(2):319–340, 2018.

[85] J. A. Lopez-Ramos, J. Rosenthal, D. Schipani, and R. Schnyder. An application of group theory in confidential network communications. *Math. Methods Appl. Sci.*, 41(6):2294–2298, 2018.

[86] A. Neri, A.-L. Horlemann-Trautmann, T. Randrianarisoa, and J. Rosenthal. On the genericity of maximum rank distance and Gabidulin codes. *Designs, Codes and Cryptography*, 86(2):341–363, 2018.

[87] A. Neri, J. Rosenthal, and D. Schipani. Fuzzy authentication using rank distance. In M. Baldi, Quaglia E., and Tomasin S., editors, *Proceedings of the 2nd Workshop on Communication Security. WCS 2017.*, volume 447 of *Lecture Notes in Electrical Engineering*, pages 97–108. Springer Verlag, 2018.

[88] S. R. Blackburn, M. Greferath, C. Hollanti, M. O. Pavčević, J. Rosenthal, L. Storme, Á. Vázquez-Castro, and A. Wassermann. Preface to the special issue on network coding and designs. *Des. Codes Cryptogr.*, 86(2):237–238, 2018.

[89] J. Rosenthal. Lasker and mathematics. In R. Forster, M. Negele, and R. Tischbierek, editors, *Emanuel Lasker: Struggle and Victories: World Chess Champion for 27 Years*, volume 1, chapter 5, pages 187–218. Exzelsior Verlag, Berlin, 2018.

2019

[90] M. Baldi, F. Chiaraluce, J. Rosenthal, P. Santini, and D. Schipani. Security of generalized Reed-Solomon code-based cryptosystems. *IET Information Security*, 13(4):404–410, April 2019.

2020

[91] C. Interlando, K. Khathuria, N. Rohrer, J. Rosenthal, and V. Weger. Generalization of the ball-collision algorithm. *J. Algebra Comb. Discrete Struct. Appl.*, 7(2):195–207, 2020.

2021

[92] G. N. Alfarano, J. Lieb, and J Rosenthal. Construction of LDPC convolutional codes via difference triangle sets. *Des. Codes Cryptogr.*, 89(10):2235–2254, 2021.

[93] K. Khathuria, J. Rosenthal, and V. Weger. Encryption scheme based on expanded Reed-Solomon codes. *Adv. Math. Commun.*, 15(2):207–218, 2021.

[94] J. Lieb and J. Rosenthal. Erasure decoding of convolutional codes using first-order representations. *Math. Control Signals Syst.*, 33:499–513, 2021.

[95] S. Tinani and J. Rosenthal. Existence and cardinality of k-normal elements in finite fields. In *Arithmetic of finite fields*, volume 12542 of *Lecture Notes in Comput. Sci.*, pages 255–271. Springer, Cham, [2021] ©2021. arXiv:2003.09748.

[96] J. Lieb, R. Pinto, and J. Rosenthal. Convolutional codes. In J.; Sole P Huffman, C; Kim, editor, *Concise Encyclopedia of Coding Theory*. CRC Press, 2021.

2022

[97] S. Tinani and J. Rosenthal. A deterministic algorithm for the discrete logarithm problem in a semigroup. *J. Math. Cryptol.*, 16(1):141–155, 2022.

2023

[98] G. N. Alfarano, A. Gruica, J. Lieb, and J. Rosenthal. Convolutional codes over finite chain rings, MDP codes and their characterization. *Adv. Math. Commun.*, 17(1):1–22, 2023.

[99] J. Bariffi, S. Mattheus, A. Neri, and J. Rosenthal. Moderate-density parity-check codes from projective bundles. *Des. Codes Cryptogr.*, 90(12):2943–2966, 2022.

[100] N. Gassner, M. Greferath, J. Rosenthal, and V. Weger. Bounds for coding theory over rings. *Entropy*, 24(10):Paper No. 1473, 16, 2022.

2024

[101] Z. Abreu, J. Lieb, R. Pinto, and J. Rosenthal. Criteria for the construction of MDS convolutional codes with good column distances. *Adv. Math. Commun.*, 18(2):595–613, 2024.

[102] S. Heri, J. Lieb, and J. Rosenthal. Self-dual convolutional codes. *IEEE Trans. Inform. Theory*, 70(2):950–963, 2024.

[103] J. Bariffi, H. Bartz, G. Liva, and J. Rosenthal. Error-correction performance of regular ring-linear LDPC codes over Lee channels. *IEEE Trans. Inform. Theory*, 70(11):7820–7839, 2024.

Preprints:

[104] V. Weger, N. Gassner and J. Rosenthal. A survey on code-based cryptography. *arXiv:2201.07119*, 2022.

[105] S. Tinani, C. Matteotti, and J. Rosenthal. Cryptanalysis of some nonabelian group-based key exchange protocols. *arxiv:2203.03525*, 2023.

[106] G. N. Alfarano, J. Rosenthal, and B. Toesca. Schubert subspace codes. *arXiv:2405.20047*, 2024.

Publications in Conference Proceedings: (Mainly refereed, some by invitation)

[107] J. Rosenthal. On minimal order dynamical compensators of low order systems. In *Proc. of European Control Conference*, pages 374–378, Grenoble, France, 1991.

[108] J. Rosenthal and M. K. Sain. On Kronecker indices of transfer functions and autoregressive systems. In *Proc. of the Second Int. Symposium on Implicit Systems*, pages 173–176, Warsaw University of Technology, Warsaw, Poland, July 1991.

[109] M. S. Ravi, J. Rosenthal, and X. Wang. On homogeneous autoregressive systems. In *Proceedings of Symposium on Implicit and Nonlinear Systems*, pages 229–235. The University of Texas at Arlington, December 1992.

[110] J. Rosenthal and M. S. Ravi. Dynamic pole placement and the connection to geometry. In *Proc. of the 31st IEEE Conference on Decision and Control*, pages 179–180, Tucson, Arizona, 1992.

[111] X. Wang and J. Rosenthal. Pole placement with small order dynamic compensators. In *Proc. of the 31st IEEE Conference on Decision and Control*, pages 3098–3099, Tucson, Arizona, 1992.

[112] J. Rosenthal, M. S. Ravi, and X. Wang. On subsets of autoregressive systems and stabilization conditions. In *Proc. of European Control Conference*, pages 1879–1882, Groningen, The Netherlands, 1993.

[113] J. Rosenthal, M. S. Ravi, and X. Wang. On decentralized dynamic feedback compensation. In *Proc. of the 32nd IEEE Conference on Decision and Control*, pages 357–358, San Antonio, Texas, 1993.

[114] M. S. Ravi, J. Rosenthal, and X. Wang. Robustness of autoregressive systems. In *Proc. of the 32nd IEEE Conference on Decision and Control*, pages 2878–2879, San Antonio, Texas, 1993.

[115] X. Wang, M. S. Ravi, and J. Rosenthal. Algebraic and combinatorial aspects of the dynamic pole assignment problem. In U. Helmke, R. Mennicken, and J. Saurer, editors, *Systems and Networks: Mathematical Theory and Applications*, volume 79 of *Mathematical Research*, pages 547–550. Akademie Verlag, Berlin, Germany, 1994. Proc. of the International Symposium MTNS 93 held in Regensburg Germany. Vol II: Invited and contributed papers.

[116] J. Rosenthal and E. York. An ideal theoretic approach for classifying high rate convolutional codes. In *Proceedings of the 1994 IEEE International Symposium on Information Theory*, page 169, Trondheim, Norway, 1994.

[117] X. Wang, M. S. Ravi, and J. Rosenthal. Recent applications of algebraic geometry in linear system theory. In J. G. Lewis, editor, *Proc. of Fifth SIAM Conference on Applied Linear Algebra, held in Snowbird, Utah*, pages 206–210. SIAM, 1994.

[118] J. Rosenthal and E.V. York. Linear systems defined over a finite field, dynamic programming and convolutional codes. In *Proc. of the IFAC Conference on System Structure and Control*, pages 466–471, Nantes, France, 1995.

[119] U. Helmke, J. Rosenthal, and J. M. Schumacher. A controllability test for behavior systems. In *Proc. of the IFAC Conference on System Structure and Control*, pages 318–323, Nantes, France, 1995.

[120] M. S. Ravi, J. Rosenthal, and J. M. Schumacher. A realization theory for homogeneous AR-systems, an algorithmic approach. In *Proc. of the IFAC Conference on System Structure and Control*, pages 183–188, Nantes, France, 1995.

[121] J. Rosenthal and E. York. Generalized Hamming weights for convolutional codes. In *Proceedings of the 1995 IEEE International Symposium on Information Theory*, page 162, Whistler, British Columbia, 1995.

[122] J. Rosenthal and E. York. First order representations for convolutional encoders. In *Proceedings of the 1995 IEEE International Symposium on Information Theory*, page 165, Whistler, British Columbia, 1995.

[123] M. S. Ravi, J. Rosenthal, and J. M. Schumacher. System equivalences and canonical forms from a behavioral point of view. In *Proc. of the 34th IEEE Conference on Decision and Control*, pages 484–489, New Orleans, Louisiana, 1995.

[124] M. S. Ravi, J. Rosenthal, and X. Wang. Dynamic pole assignment for systems in generalized first order form: A report on results derived by algebro-geometric techniques. In *Proc. of the 34th IEEE Conference on Decision and Control*, pages 1900–1904, New Orleans, Louisiana, 1995.

[125] J. Rosenthal, J. M. Schumacher, X. Wang, and J. C. Willems. Generic eigenvalue assignment for generalized linear first order systems using memoryless real output feedback. In *Proc. of the 34th IEEE Conference on Decision and Control*, pages 492–497, New Orleans, Louisiana, 1995.

[126] J. Rosenthal and X. Wang. Eigenvalue assignment by dynamic output feedback: A new sufficiency criterion in the real case. In *Proc. of the 34th IEEE Conference on Decision and Control*, pages 2710–2715, New Orleans, Louisiana, 1995.

[127] E.V. York, J. Rosenthal, and J. M. Schumacher. On the relationship between algebraic systems theory and coding theory: Representations of codes. In *Proc. of the 34th IEEE Conference on Decision and Control*, pages 3271–3276, New Orleans, Louisiana, 1995.

[128] B. Allen and J. Rosenthal. Analysis of convolutional encoders via generalized sylvester matrices and state space realization. In *Proc. of the 34-th Allerton Conference on Communication, Control, and Computing*, pages 893–902, 1996.

[129] C. Peterson, J. Rosenthal, and P. A. Weiner. Connections between multidimensional systems theory and algebraic geometry. In *Proc. of the 34-th Allerton Conference on Communication, Control, and Computing*, pages 583–592, 1996.

[130] B. Allen and J. Rosenthal. Analyzing convolutional encoders using realization theory. In *Proceedings of the 1997 IEEE International Symposium on Information Theory*, page 287, Ulm, Germany, 1997.

[131] J. Rosenthal and E.V. York. A construction of binary BCH convolutional codes. In *Proceedings of the 1997 IEEE International Symposium on Information Theory*, page 291, Ulm, Germany, 1997.

[132] J. Rosenthal and R. Smarandache. Construction of convolutional codes using methods from linear systems theory. In *Proc. of the 35-th Annual Allerton Conference on Communication, Control, and Computing*, pages 953–960, 1997.

[133] M. S. Ravi, J. Rosenthal, and U. Helmke. On output feedback invariants and cascade equivalence of systems. In *Proc. of the 36th IEEE Conference on Decision and Control*, pages 4243–4248, San Diego, California, 1997.

[134] J. Rosenthal. Some interesting problems in systems theory which are of fundamental importance in coding theory. In *Proc. of the 36th IEEE Conference on Decision and Control*, pages 4574–4579, San Diego, California, 1997.

[135] R. Smarandache and J. Rosenthal. A state space approach for constructing MDS rate $1/n$ convolutional codes. In *Proceedings of the 1998 IEEE Information Theory Workshop on Information Theory*, pages 116–117, Killarney, Kerry, Ireland, June 1998.

[136] B. M. Allen and J. Rosenthal. Parity-check decoding of convolutional codes whose systems parameters have desirable algebraic properties. In *Proceedings of the 1998 IEEE International Symposium on Information Theory*, page 307, Boston, MA, 1998.

[137] R. Smarandache and J. Rosenthal. Convolutional code constructions resulting in maximal or near maximal free distance. In *Proceedings of the 1998 IEEE International Symposium on Information Theory*, page 308, Boston, MA, 1998.

[138] J. Rosenthal and R. Smarandache. On the dual of MDS convolutional codes. In *Proc. of the 36-th Annual Allerton Conference on Communication, Control, and Computing*, pages 576–583, 1998.

[139] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Generalized first order descriptions and canonical forms for convolutional codes. In A. Beghi, L. Finesso, and G. Picci, editors, *Mathematical Theory of Networks and Systems*, pages 1091–1094, July 1998. Proceedings of the MTNS-98 Symposium held in Padova, Italy.

[140] C. Monico, J. Rosenthal, and A. Shokrollahi. Using low density parity check codes in the McEliece cryptosystem. In *Proceedings of the 2000 IEEE International Symposium on Information Theory*, page 214, Sorrento, Italy, 2000.

[141] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Construction results for MDS-convolutional codes. In *Proceedings of the 2000 IEEE International Symposium on Information Theory*, page 294, Sorrento, Italy, 2000.

[142] J. Rosenthal and P. Vontobel. Constructions of LDPC Codes Using Ramanujan Graphs and Ideas from Margulis. In *Proc. of the 38-th Annual Allerton Conference on Communication, Control, and Computing*, pages 248–257, 2000.

[143] J. Rosenthal and P. Vontobel. Constructions of Regular and Irregular LDPC Codes using Ramanujan Graphs and Ideas from Margulis. In *Proceedings of the 2001 IEEE International Symposium on Information Theory*, page 4, Washington D.C., 2001.

[144] G. Han, K. Portman, and J. Rosenthal. Unitary matrices with maximal or near maximal diversity product. In *Proc. of the 39-th Allerton Conference on Communication, Control, and Computing*, pages 82–91, 2001.

[145] G. Maze, C. Monico, and J. Rosenthal. A public key cryptosystem based on actions by semigroups. In *Proceedings of the 2002 IEEE International Symposium on Information Theory*, page 266, Lausanne, Switzerland, 2002.

[146] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Strongly MDS convolutional codes, a new class of codes with maximal decoding capability. In *Proceedings of the 2002 IEEE International Symposium on Information Theory*, page 426, Lausanne, Switzerland, 2002.

[147] G. Han and J. Rosenthal. Unitary constellation design with application to space-time coding. In D. Gilliam and J. Rosenthal editors, *Mathematical Theory of Networks and Systems*, (12 pages), August 2002. Electronic Proceedings of MTNS-2002 Symposium held at the University of Notre Dame.

[148] G. Maze, C. Monico, J. Rosenthal and J. Climent Public key cryptography based on simple modules over simple rings In D. Gilliam and J. Rosenthal editors, *Mathematical Theory of Networks and Systems*, (8 pages), August 2002. Electronic Proceedings of MTNS-2002 Symposium held at the University of Notre Dame.

[149] R. Smarandache, H. Gluesing-Luerssen, and J. Rosenthal. Construction and decoding of strongly MDS convolutional codes In D. Gilliam and J. Rosenthal editors, *Mathematical Theory of Networks and Systems*, (6 pages), August 2002. Electronic Proceedings of MTNS-2002 Symposium held at the University of Notre Dame.

[150] G. Han and J. Rosenthal. Unitary Constellations with Large Diversity Sum and Good Diversity Product. In *Proc. of the 40-th Allerton Conference on Communication, Control, and Computing*, pages 48-57, 2002.

[151] E. Byrne, C. Kelley, C. Monico, and Rosenthal J. Non-linear codes for belief propagation. In *Proceedings of the 2003 IEEE International Symposium on Information Theory*, page 43, Yokohama, JAPAN, 2003.

[152] G. Han and Rosenthal J. A numerical approach for designing unitary space time codes with large diversity product and diversity sum. In *Proceedings of the 2003 IEEE International Symposium on Information Theory*, page 178, Yokohama, JAPAN, 2003.

[153] H. Gluesing-Luerssen, R. Hutchinson, J. Rosenthal and R. Smarandache. Convolutional codes which are maximum distance separable and which have a maximum distance profile. In *Proc. of the 41st Allerton Conference on Communication, Control, and Computing*, pages 844-852, 2003.

[154] C. Kelley, J. Rosenthal, and D. Sridhara. Some new algebraic constructions of codes from graphs which are good expanders. In *Proc. of the 41st Allerton Conference on Communication, Control, and Computing*, pages 1280-1289, 2003.

[155] C. Kelley, D. Sridhara, J. Xu and J. Rosenthal. Pseudocodeword weights and stopping sets. In *Proceedings of the 2004 IEEE International Symposium on Information Theory*, page 67, Chicago, 2004.

[156] G. Han and J. Rosenthal. Upper bound analysis of diversity for unitary space time constellations In *Proceedings of the 2004 IEEE International Symposium on Information Theory*, page 157, Chicago, 2004.

[157] J. C. Interlando, E. Byrne, and J. Rosenthal, The gate complexity of syndrome decoding of Hamming codes. In *Proceedings of the Tenth International Conference on Applications of Computer Algebra*, pages 33-37, Beaumont, Texas, 2004.

[158] C. Kelley, D. Sridhara, and J. Rosenthal. Tree-based construction of LDPC codes. In *Proceedings of the 2005 IEEE International Symposium on Information Theory*, Adelaide, Australia, Sept. 4 - 9, 2005.

[159] G. Han and J. Rosenthal. Good packings in the complex stiefel manifold using numerical methods. In *Proceedings of the 17th International Symposium on the Mathematical Theory of Networks and Systems*, pages 1710–1719, Kyoto, Japan, 2006.

[160] C. Kelley, D. Sridhara, J. Rosenthal Pseudocodeword weights for non-binary LDPC codes. In Proceedings of the 2006 IEEE international Symposium on Informaion Theory, pages 1379 - 1383, Seattle, USA, 2006. ISIT 2006

[161] U. Helmke, J. Rosenthal, and X. A. Wang. Pole placement results for complex symmetric and Hamiltonian transfer functions. In *Proc. of the 46th IEEE Conference on Decision and Control*, pages 3450–3453, 2007

[162] A. Amir, F. Müller, P. Fornaro, R. Gschwind, J. Rosenthal, and L. Rosenthaler. Towards a channel model for microfilm. In *Archiving 2008, Bern, Switzerland*, pages 207–211, Springfield, Virginia, June 2008. IS&T: The Society for Imaging Science and Technology.

[163] A. Mitchell and J. Rosenthal. Design of irregular graphs for erasure decoding. In *Proceedings of the 18th International Symposium on the Mathematical Theory of Networks and Systems*, Blacksburg, Virginia, USA, July 2008.

[164] F. Manganiello, E. Gorla, and J. Rosenthal. Spread codes and spread decoding in network coding. In *Proceedings of the 2008 IEEE International Symposium on Information Theory*, pages 851–855, Toronto, Canada, 2008.

[165] J. Zumbrägel, G. Maze, and J. Rosenthal. Efficient recovering of operation tables of black box groups and rings. In *Proceedings of the 2008 IEEE International Symposium on Information Theory*, pages 639–643, Toronto, Canada, 2008.

[166] V. Tomas, J. Rosenthal, and R. Smarandache. Decoding of MDP convolutional codes over the erasure channel. In *Proceedings of the 2009 IEEE International Symposium on Information Theory*, pages 556–560, Seoul, South Korea, 2009.

[167] A. Amir, A. Mitchell, and J. Rosenthal. LDPC codes from matrix equations. In *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems – MTNS*, pages 301–305, Budapest, Hungary, 2010.

[168] S.D. Cardell, G. Maze, J. Rosenthal, and U. Wagner. Correlations in stream ciphers: A systems theory point of view. In *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems – MTNS*, pages 419–423, Budapest, Hungary, 2010.

[169] D. Schipani and J. Rosenthal. Coding solutions for the secure biometric storage problem. In *Information Theory Workshop (ITW), 2010 IEEE*, pages 1 –4, Dublin, Ireland, August 2010.

[170] V. Tomás, J. Rosenthal, and R. Smarandache. Reverse-maximum distance profile convolutional codes over the erasure channel. In *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems – MTNS*, pages 2121–2127, Budapest, Hungary, 2010.

[171] A.-L. Trautmann, F. Manganiello, and J. Rosenthal. Orbit codes - a new concept in the area of network coding. In *Information Theory Workshop (ITW), 2010 IEEE*, pages 1 –4, Dublin, Ireland, August 2010.

[172] A.-L. Trautmann and J. Rosenthal. New improvements on the echelon-ferrers construction. In *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems – MTNS*, pages 405–408, Budapest, Hungary, 2010.

[173] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani. A variant of the McEliece cryptosystem with increased public key security. In *Proceedings of the Seventh International Workshop on Coding and Cryptography (WCC) 2011*, pages 173 – 182, 2011.

[174] F. Manganiello, A. Trautmann, and J. Rosenthal. On conjugacy classes of subgroups of the general linear group and cyclic orbit codes. In *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*, pages 1916 –1920, August 2011.

[175] D. Schipani, M. Elia, and J. Rosenthal. Efficient evaluations of polynomials over finite fields. In *Communications Theory Workshop (AusCTW), 2011 Australian*, pages 154–157, February 2011.

[176] D. Schipani, M. Elia, and J. Rosenthal. On the decoding complexity of cyclic codes up to the BCH bound. In *Information Theory Proceedings (ISIT), 2011 IEEE International Symposium on*, pages 835 –839, August 2011.

[177] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani. On fuzzy syndrome hashing with LDPC coding. In *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*, ISABEL '11, pages 24:1–24:5, New York, NY, USA, 2011. ACM.

[178] A.-L. Trautmann and J. Rosenthal. A complete characterization of irreducible cyclic orbit codes. In *Proceedings of the Seventh International Workshop on Coding and Cryptography (WCC) 2011*, pages 219 – 228, 2011.

[179] F. Fontein, K. Marshall, J. Rosenthal, D. Schipani, and A.-L. Trautmann. On burst error correction and storage security of noisy data. In *Proceedings of the 20th International Symposium on Mathematical Theory of Networks and Systems – MTNS*, pages 1–15, Melbourne, Australia, 2012.

[180] A.-L. Horlemann-Trautmann, K. Marshall, and J. Rosenthal. Considerations for rank-based cryptosystems. In *Proceedings of the IEEE International Symposium on Information Theory (ISIT) 2016*, pages 2544–2548, July 2016.

[181] D. Napp, R. Pinto, J. Rosenthal, and P. Vettori. Rank metric convolutional codes. In *Proceedings of the 22nd International Symposium on Mathematical Theory of Networks and Systems – MTNS*, pages 361–363, Minneapolis, Minnesota, 2016.

[182] D. Napp, R. Pinto, J. Rosenthal, and P. Vettori. MRD rank metric convolutional codes. In *Proceedings of the 2017 IEEE International Symposium on Information Theory, Aachen, Germany*, pages 2766–2770, June 2017.

[183] T. Randrianarisoa and J. Rosenthal. A decoding algorithm for twisted Gabidulin codes. In *Proceedings of the 2017 IEEE International Symposium on Information Theory, Aachen, Germany*, pages 2776–2779, June 2017.

[184] Karan Khathuria, Joachim Rosenthal, and Violetta Weger. Weight Two Masking of the Reed-Solomon Structure in Conjugation with List Decoding. In *Proceedings of 23rd International Symposium on Mathematical Theory of Networks and Systems*, pages 309–314, Hong Kong University of Science and Technology, Hong Kong, 2018.

[185] D. Napp, R. Pinto, J. Rosenthal, and P. Vettori. Faster decoding of rank metric convolutional codes. In *Proceedings of 23rd International Symposium on Mathematical Theory of Networks and Systems*, pages 507–510, Hong Kong University of Science and Technology, Hong Kong, 2018.

[186] G.N. Alfarano, J. Lieb, and J. Rosenthal. Construction of rate $(n-1)/n$ non-binary LDPC convolutional codes via difference triangle sets. In *2020 IEEE International Symposium on Information Theory (ISIT), Los Angeles, USA*, pages 138–143, 2020.

[187] H. Chimal-Dzul, N. Gassner, J. Rosenthal, and R. Schnyder. Efficient description of some classes of codes using group algebras. *IFAC-PapersOnLine*, 55(30):7–12, 2022. 25th International Symposium on Mathematical Theory of Networks and Systems MTNS 2022.

[188] H. Chimal-Dzul, J. Lieb, and J. Rosenthal. Generator matrices of quasi-cyclic codes over extension fields obtained from Gröbner basis. *IFAC-PapersOnLine*, 55(30):61–66, 2022. 25th International Symposium on Mathematical Theory of Networks and Systems MTNS 2022.

[189] J. Bariffi, H. Bartz, G. Liva, and J. Rosenthal. Analysis of low-density parity-check codes over finite integer rings for the lee channel. In *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, pages 1–6, 2022.

[190] Z. Abreu, J. Lieb, and J. Rosenthal. Binary convolutional codes with optimal column distances. In *2023 IEEE International Symposium on Information Theory (ISIT)*, pages 1271–1276, 2023.

[191] Z. Abreu, J. Rosenthal, and M. Schaller. Algorithms for computing the free distance of convolutional codes. In *2024 IEEE International Symposium on Information Theory (ISIT)*, pages 1764–1769, 2024.

[192] N. Gassner, A. Mazumder, J. Rosenthal, and A. Sutton. An approach to constructing convolutional codes with moderate density and quasi-cyclic structure. *IFAC-PapersOnLine*, 58(17):304–309, 2024. 26th International Symposium on Mathematical Theory of Networks and Systems MTNS 2024.

Book Reviews:

[193] J. Rosenthal. Review of: *Introduction to Mathematical Systems Theory. A Behavioral Approach*, by Jan Willem Polderman and Jan C. Willems, Springer Verlag, 1998. In *IEEE Trans. Automat. Contr.*, 47(4):706–708, 2002.

Invited Addresses:

Washington University, St.Louis, Missouri. January 10, 1991. Seminar talk: "Large Order Systems with Low Order Compensators".

Centro Nazionale di Richerche, Padova, Italy , July 10, 1991. Seminar talk: "The Geometry behind the Pole Placement Problem".

Swiss Federal Institute of Technology, Lausanne, Switzerland, July 26, 1991. Seminar talk at Institute d'Automatique: "A Geometric Formulation of the Pole Placement Problem".

Virginia Tech, Blacksburg, Virginia, January 20-22, 1993. Colloquium talk: "On Interpolation, Dynamic Pole Placement and Schubert Calculus". Seminar talk: "On rational interpolation conditions of Schubert type".

Washington University, St.Louis, Missouri, May 18, 1993. Seminar talk: "On Stabilization of Autoregressive Systems and Pole Assignability".

University of Groningen, Groningen, The Netherlands, June 23, 1993. Seminar talk: "On Feedback Stabilization of Autoregressive Systems".

Center for Math. & Comp. Science, Amsterdam, The Netherlands, July 6, 1993. Seminar talk: "Transfer Functions, Autoregressive Systems and their Feedback Interconnection".

University of Eindhoven, Eindhoven, The Netherlands, July 13, 1993. Seminar talk: "A generalized Hautus test of observability".

University of Regensburg, Regensburg, Germany, July 23, 1993. Colloquium talk: "Systemtheorie und der Schubert Kalkühl".

University of Groningen, Groningen, The Netherlands, October 6, 1994. Seminar talk: "The behavior of Convolutional Codes ".

University of Eindhoven, Department of Mathematics, Eindhoven, The Netherlands, November 2, 1994. Title of colloquium talk: "On the Algebraic Structure of a Convolutional Code".

University of Eindhoven, Department of Electrical Engineering, Eindhoven, The Netherlands, November 16, 1994. Seminar talk: "An Elementary proof of Wang's Pole Placement Result".

University of Oldenburg, Oldenburg, Germany, February 7, 1995. Colloquium talk: "Polvorgabe und allgemeine inverse Eigenwert Probleme; ein geometrischer Gesichtspunkt".

University of Bremen, Bremen, Germany, February 5–15, 1995. Colloquium talk: "Inverse Eigenwert Probleme und ihr Zusammenhang mit dem Schubert Kalkühl" Title of seminar talk: "Über die Geometrie des Raumes der linearen Systeme".

City University of London, London, England, March 2, 1995. Seminar talk: "Convolutional Codes, a Systems Theory Point of View".

Vrije Universiteit Amsterdam, Amsterdam, The Netherlands, March 16, 1995. Seminar talk: "Inverse Eigenvalue Problems and Eigenvalue Inequalities, a Geometric Approach".

University of Twente, The Netherlands, April 26-27, 1995. Seminar talks: "On Pole Placement Result and Inverse Eigenvalue Problems" and "Convolutional Codes and systems defined over finite fields".

Universität Würzburg, Würzburg, Germany, June 30, 1995. Seminar talk: "Inverse Eigenwert Probleme und die Verbindung zum Schubert-Kalkühl".

East Carolina University, March 22, 1996. Title of colloquium talk: "Convolutional Codes, a Bridge Between Coding Theory, Systems Theory and Algebraic Geometry".

University of Illinois at Urbana-Champaign, Coordinated Science Laboratory, November 7, 1996. Title of colloquium talk: "On the Duality between Convolutional Codes and Linear Systems".

Texas Tech University, January 23, 1997. Title of colloquium talk: "An Algebraic Theory for Convolutional Codes".

Universität Kaiserslautern, Kaiserslautern, Germany, June 9–13, 1997. Seminar talks: "Inverse Eigenwertprobleme, Polvorgabe und Beziehungen zum Quantum-Ring der Grassmann-Varietät" and "Faltungscodes und Systeme über endliche Körpern".

Universität Würzburg, Würzburg, Germany, June 16–21, 1997. Mini-Course of 3 lectures entitled: "Dynamische Systeme über endlichen Körpern und Kodierungstheorie". Colloquium talk on June 20, 1997: "Inverse Eigenwert-Probleme mittels Schnitttheorie".

University of Toronto, October 22, 1997. Title of colloquium talk: "Pole Placement Problems, Inverse Eigenvalue Problems and some Relations to the Quantum Ring of the Grassmannian".

Swiss Federal Institute of Technology, Lausanne, Switzerland, June 8, 1998. Seminar talk: "Algebraic Construction and Decoding of Convolutional Codes".

Centro Internacional de Matemática, Coimbra, Portugal. Summer school on Linear Algebra and Control Theory (June 15-23, 1998). Invited Lecture Series on "Linear Systems over Finite Fields and Coding Theory". One hour talk entitled "An Algebraic Geometric Framework for Pole Placement and Matrix Extension Problems" during a workshop held June 24-26, 1998.

University of Padova, July 2, 1998. Seminar talk: "Algebraic Constructions of Convolutional Codes".

MSRI in Berkeley, California, Member in October, 1998. Title of invited one hour talk on October 20, 1998: "An Algebraic Geometric Framework for Inverse Problems arising in Control Theory and Linear Algebra".

University of Groningen, Groningen, The Netherlands, April 19, 1999. Seminar talk: "Construction of Maximum Distance Separable Convolutional Codes".

Michigan State University, May 4, 1999. Title of seminar talk: "An Algebraic Geometric Framework for Inverse Problems arising in Control Theory and Linear Algebra".

University of Toronto, June 7-9, 1999. Title of seminar talks: "Construction of Convolutional Codes with Large Free Distance" and "Algebraic Geometric Intersection Problems arising in Control Theory and Linear Algebra".

Swisscom research in Bern, Switzerland, September 17, 1999. Title of talk: "Kryptographie und ihre Anwendungen".

University College Cork, Ireland, November 4, 1999. Colloquium talk: "Reflections on Shannon's Challenges".

Trinity College Dublin and University College Dublin, joint Mathematics colloquium, November 5, 1999. Title: "Reflections on Shannon's Challenges".

Swiss Federal Institute of Technology, Lausanne, Switzerland, November 12, 1999. Seminar talk at Institute d'Automatique: "Realization by Inspection".

Swiss Federal Institute of Technology, Lausanne, Switzerland, November 16, 1999. Seminar talk at the Department of Mathematics: "Reflections on Shannon's three Challenges".

University of Oldenburg, Oldenburg, Germany, November 23, 1999. Colloquium talk: "Ein Quotienten Schema und seine Bedeutung in der Systemtheorie und der Codierungstheorie".

University of Bremen, Bremen, Germany, November 24-27, 1999. Series of three lectures on the relation between systems theory and coding theory.

University of Basel, Basel, Switzerland, December 1, 1999. Title of talk: "Ein Public-Key Kryptosystem basierend auf dünnen bipartiten Graphen".

University of Frankfurt, Frankfurt, Germany, December 10, 1999. Colloquium talk: "Konstruktion von Faltungscodes mit grosser Distanz".

University of Innsbruck, Innsbruck, Austria, March 22, 2000. Colloquium talk: "Konstruktion von Faltungscodes mit grosser Distanz".

Royal Institute of Technology (KTH), Stockholm, Sweden, April 4-8, 2000. Seminar talks: "Pole Placement Problems, Inverse Eigenvalue Problems and Schubert Calculus" and "Reflections on Shannon's three Challenges".

Lund Institute of Technolog, Lund, Sweden, April 27, 2000. Seminar talk: "Connections between Linear Systems and Convolutional Codes".

Ben Gurion University of the Negev, Beer-Sheva, Israel, May 13–18, 2000. Colloquium talk: "Reflections on Shannon's three challenges". Seminar talk: "Pole placement problems, inverse eigenvalue problems and quantum Schubert calculus".

University of Geneva, Geneva, Switzerland, July 4, 2000. Colloquium talk: "Holomorphic Curves in Grassmannians and their Appearance in Systems Theory".

University of Notre Dame, Notre Dame, Indiana, September 6, 2000. Colloquium talk: "Three Challenges by Claude Shannon".

Texas Tech University, Lubbock, Texas, January 12, 2001. Colloquium talk: "Three Challenges by Claude Shannon".

University of Michigan, Ann Arbor, Michigan, January 26, 2001. Seminar talk: "Reflections on Shannon's three Challenges".

Technical University of Berlin, Berlin, Germany, March 29, 2001. Seminar talk: "Inverse Eigenwertprobleme und Schubertkalkuehl".

Free University of Berlin, Berlin, Germany, March 30, 2001. Colloquium talk: "Public-Key Verschluesselung, Quantum Computer und klassische Invariantentheorie".

Ohio State University, Columbus, Ohio, April 9-12, 2001. Seminar talks: "Three Challenges by Claude Shannon" and "Constructions of LDPC codes using Ramanujan graphs and ideas from Margulis".

University of Illinois at Chicago, October 22-23, 2001. Colloquium talk: "Claude Shannon's three Challenges". Seminar talk: "Constructions of LDPC codes using Ramanujan graphs and ideas from Margulis".

Ohio University, Athens, Ohio, March 4-9, 2002. First invited speaker of the new "Center of Ring Theory and its Applications". 5 talks on coding theory and cryptography including a University-wide public lecture entitled "The Three Challenges of Claude Shannon".

Saint Mary's University, Winona, Minnesota, March 15, 2002. Colloquium talk: "Public Key Cryptography, e-Commerce, and Number Theory".

Northern Illinois University, DeKalb, Illinois, April 5, 2002. Colloquium talk: "Three Challenges by Claude Shannon".

Texas Tech University, Lubbock, Texas, April 11, 2002. Colloquium talk: "Semi-Group Actions, Public Key Cryptography and e-Commerce".

Universität Würzburg, Würzburg, Germany, June 20, 2002. Seminar talk: "Ring Theoretic Methods in Cryptography"

University of Zurich, Zurich, Switzerland, June 25, 2002. Colloquium talk: "Algebraische Elemente kryptographischer Protokolle".

ETH, Zurich, Switzerland, June 28, 2002. Seminar talk in the Department of Computer Science: "Diffie Hellman and ElGamal protocols from semi-group actions".

University of Frankfurt, Frankfurt, Germany, July 8, 2002. Colloquium talk in Department of Computer Science: "Algebraische Elemente kryptographischer Protokolle".

University of Nebraska, Lincoln, Nebraska, November 7–9, 2002. Colloquium talk: "Three challenges of Claude Shannon". Seminar talk: "Constructions of LDPC codes using Ramanujan graphs and ideas from Margulis"

ETH, Zurich, Switzerland, December 13, 2002. Seminar talk in the Department of Electrical Engineering: "A Numerical Approach for Designing Unitary Space Time Codes with Large Diversity".

Virginia Tech, Blacksburg, Virginia, March 14, 2003. Colloquium talk: "Reflections on Shannon's three Challenges".

University of Illinois at Urbana-Champaign, April 9-11, 2003. Electrical and Computer Engineering graduate seminar: "Algebraic Techniques in Cryptography". Seminar at Coordinated Science Laboratory: "Convolutional Codes with Maximal or near-Maximal Distance".

Mittag Leffler Institute, Stockholm, Sweden, May 5 until June 4, 2003. Lecture on May 8, 2003: "Claude Shannon's three Challenges". Lecture on May 13, 2003: "Convolutional Codes with Maximal or near-Maximal Distance".

University of Wisconsin, Madison, Wisconsin, September 3-6, 2003. Seminar talk in Computer Science: "Public Key Cryptography and Semi-Group Actions". Colloquium talk in Mathematics: "Three challenges of Claude Shannon".

University College Cork, Ireland, October 20, 2003. Colloquium talk: "Algebraic Methods in Cryptography".

Texas Tech University, Lubbock, Texas, November 13, 2003. Seminar talk: "Ring Theoretic Methods in Cryptography".

University of California San Diego, La Jolla, California, February 5, 2004. Colloquium: "Algebraic Methods in Cryptography".

San Diego State University, San Diego, California, February 6, 2004. Computational Sciences Colloquium: "Three Challenges of Claude Shannon".

The College of William and Mary, Williamsburg, Virginia, April 2, 2004, *The Cissy Patterson Lecture 2004:* "Public Key Cryptography, e-Commerce and Number Theory".

University of Bern, Bern, Switzerland, January 17, 2005. Colloquium: "Public Key Crypto-Systems built from Semi-Group Actions".

University of Neuchâtel, Neuchâtel, Switzerland, January 25, 2005. Colloquium: "LDPC Codes, Codes on Graphs and Ramanujan Graphs".

Technical University Ilmenau, Ilmenau, Germany, May 20, 2005. Colloquium: "Drei Problemstellungen von Claude Shannon".

University College Dublin, Dublin, Ireland, September 29, 2005. Colloquium: "Constructing One-way Trapdoor Functions from Simple Semi-Rings and Semi-Modules".

Royal Institute of Technology (KTH), Stockholm, Sweden, November 23, 2005. Colloquium: "Building Public Key Crypto-Systems from Semi-Rings".

University of Innsbruck, Innsbruck, Austria, January 24, 2006. Colloquium: "Building Public Key Crypto-Systems from Semi-Rings".

University of Wyoming, Laramie, Wyoming, March 27, 2006. WIDMIA Lecture: "Three challenges of Claude Shannon".

University of British Columbia, Vancouver, Canada, October 10, 2006. Colloquium: "Three challenges of Claude Shannon".

University of Fribourg, Fribourg, Switzerland, November 7, 2006. Colloquium: "Three challenges of Claude Shannon".

University of Alicante, Alicante, Spain, February 28, 2007. Colloquium: "Building Public Key Crypto Systems".

University of Kentucky, Lexington, Kentucky, April 2, 2008. Yearly Hayden-Howard Lecture: "Three Challenges of Claude Shannon".

University of Groningen, Groningen, The Netherlands, June 23, 2008. Seminar talk: "Constructing Oneway Trapdoor Functions from Semirings".

University of Oldenburg, Oldenburg, Germany, November 5, 2008. Main Speaker of the "Mathematik Tag": "Kryptographie und Mathematik: Datenverschlüsselung".

INRIA, Paris–Rocquencourt, France, January 7, 2009. Seminar talk: "Algebraic Properties of Convolutional Codes".

University Pais Vasco, Bilbao, Spain, June 1, 2009. Colloquium Talk: "Building Public Key Crypto-Systems from Semi-Rings".

University of the Basque Country, Vitoria-Gasteiz, Spain, June 2-4, 2009. Seminar Talks: "Convolutional Codes and Systems over Finite Fields" and "Systems theoretic questions arising in cryptography".

University of Porto, Porto, Portugal, January 21, 2010. Colloquium talk: "Systems Theoretic Questions arising in Cryptography".

University of Aveiro, Aveiro, Portugal, January 22, 2010. Seminar talk: " Systems over Finite Fields and Convolutional Codes".

University of Melbourne, Melbourne, Australia, January 27, 2011. Colloquium talk: "Building Public Key Crypto-Systems".

Australian National University, Canberra, Australia, February 3, 2011. Seminar talk: "Construction of Network Codes, a Grassmannian Approach".

National University of Singapore, February 8, 2011. Seminar talk: "Public Key Crypto-Systems: an Overview and New Constructions".

Hong Kong University, March 21, 2011. Seminar talk: "Claude Shannon's work in Coding Theory and Cryptography".

HIT Shenzhen Graduate School, March 18, 2011. Colloquium talk: "Theree Challenges of Claude Shannon".

University of Notre Dame, Notre Dame, April 26, 2011. Seminar talk: "Linear Random Network Codes, a Grassmannian Approach".

San Diego State University, San Diego, May 5, 2011. Seminar talk: "Construction of Network Codes, a Grassmannian Approach".

Hochschultag der Zürcher Mittelschulen, ETHZ, February 2, 2012. Survey talk: "Kryptographie und Mathematik".

University of Nebraska, Lincoln, Nebraska, October 9, 2012. Seminar talk: "Public Key Crypto-Systems: an Overview and New Constructions".

University of Wisconsin, Madison, Wisconsin, October 12, 2012. Colloquium talk: "Linear Random Network Codes, a Grassmannian Approach".

Kinder-Universität, UZH, November 21, 2012. Talk for about 500 children: "Wie geheim ist eine Geheimschrift?".

Science Alumni Zurich, UZH, January 29, 2013. Title of talk: "Kryptographie und Mathematik: Von Chiffriermaschinen zu sicherer Kommunikation im Internet."

Universidad Politecnica de Valencia, Valencia Spain, April 26, 2013. Colloquium talk: "Three Challenges of Claude Shannon."

University of Alicante, Alicante, Spain, September 12, 2013. Colloquium: "Public Key Cryptography, e-Commerce and Number Theory".

University of Salamanca, Salamanca, Spain, October 11, 2013. Colloquium: "The work of Claude Shannon in Coding Theory and Cryptography".

University of Almeria, Almeria, Spain, February 11, 2014. Colloquium: "Algebraic Structure of Convolutional Codes and their use over the Erasure Channel.".

Universidad del Norte, Barranquilla, Columbia, April 26, 2014. Colloquium: "Three Challenges of Claude Shannon".

Technion, Israel Institute of Technology, Haifa, Israel, October 12-17, 2014. Research visit as guest of Prof. Tuvi Etzion.

University of Alicante, Alicante, Spain, November 6-12, 2014. Research visit as guest of Prof. Josep Climent.

Aalto University, Helsinki, Finland, February 11, 2015. Colloquium talk: "Three Research Challenges from Claude Shannon". Seminar talk: "Cryptography after the time of Shannon and in the presence of a Quantum Computer".

EPFL, Lausanne, Switzerland, February 19, 2015. Seminar talk: "Semirings, Semigroup Actions and their use for Cryptographic Protocols".

Politecnico di Torino, Torino, Italy, May 15, 2015. Seminar talk: "Semirings, Semigroup Actions and their potential use in Post-Quantum Cryptography".

University of Aveiro, Aveiro, Portugal, October 19, 2016. Colloquium talk: "Public Key Cryptographic Systems in a Post-Quantum Environment".

Pädagogische Hochschule Zürich, Zürich, Switzerland, November 19, 2016. Title of talk during Tagung für Mathematik und Mathematikdidaktik: "Die Mathematik als Grundlage der Kryptographie".

Oxford University, Oxford, England, February 1, 2017. Seminar talk: "Code based Cryptography using different Metrics".

University of Granada, Granada, Spain, February 16, 2017. Seminar talk: "Code Based Systems for Post-Quantum Cryptography".

University of Bern, Bern, Switzerland, April 28, 2017. Seminar talk: "An Overview on Post-Quantum Cryptography with an Emphasis on Code based Systems".

University of Almeria, Almeria, Spain, October 30-November 2, 2017. Series of lectures on: "From Classical Cryptography to Post-Quantum Cryptography".

University of Siegen, Siegen, Germany, January 25, 2018. Colloquium talk: "Public Key Cryptography in a Post-Quantum Computer Environment".

East China Normal University, Shanghai, China, July 23, 2018. Colloquium talk: "Candidates for Post-Quantum Cryptography with an Emphasis on Code based Systems".

Nanjing University of Aeronautics and Astronautics, July 26, 2018. Colloquium talk: "Rank Metric Codes, Subspace Codes and Orbit Codes".

University of Notre Dame, Notre Dame, October 16, 2019. Colloquium talk: "Overview of post-Quantum Cryptography with an Emphasis on Code based Systems".

Aachen University, Aachen, Germany, October 30, 2020. Online Colloquium talk: "Post-Quantum Cryptography".

York University, York, United Kingdom, December 15, 2020. Online Colloquium talk: "An Overview of Code based Cryptography".

Vienna School of Mathematics, Weissensee, Austria, September 21–24, 2021. Series of three talks on Coding Theory and Cryptography.

Sonderforschungsbereich TRR 195, Blaubeuren, Germany, September 21, 2022. Colloquium talk: "What mathematics is used in Post-Quantum Cryptography"

Armasuisse Cyberspace Jahresreporting, Thun, Switzerland, May 2, 2023. Title of talk: "Code-based Cryptography"

University of Almeria, Almeria, Spain, February 15, 2024. Colloquium talk: "Post-Quantum Cryptography and the search for new Cryptographic Standards".

University of Paris 8, Paris, France, October 17, 2024. Colloquium talk: "Optimal Packings in Finite Schubert Varieties and its Connection to Network Coding".

University of Basel, Basel, Switzerland, November 21, 2024. Colloquium talk: "Towards a Standardization in Post-Quantum Cryptography".

Online ACCESS Seminar, December 3, 2024. Title of talk: "Semigroup Action Problem (SAP) and other Generalizations of the DLP".

University of Basel, Basel, Switzerland, December 10, 2024. Colloquium talk: "The Standardization Process in Post-Quantum Cryptography".

Conferences and Workshops:

Second SIAM Conference on Linear Algebra in Signals Systems and Control, San Francisco, California , November 5–8, 1990. Title of talk: "A Compactification of the Space of Multivariable Linear Systems using Geometric Invariant Theory".

European Control Conference, Grenoble, France , July 2–5, 1991. Title of talk: "On Minimal Order Dynamical Compensators of Low Order Systems".

Second International Symposium on Implicit and Robust Systems, Warsaw, Poland, July 17–19, 1991. Title of talk: "On Kronecker Indices of Transfer Functions and Autoregressive Systems".

Workshop on Matrix Computation and Applications, Winnipeg, Manitoba, Canada, December 9–10, 1991.

IMA Workshop on Linear Algebra for Control Theory, Minneapolis, June 1–5, 1992. Title of talk: "A Smooth Compactification of the Space of Transfer Functions with Fixed McMillan Degree".

Computation and Control III, Bozeman, Montana, August 5–11, 1992. Title of talk: "What is the Distance between two Transfer Functions?"

SIAM Conference on Control and its Applications, Minneapolis, September 17–19, 1992. Title of talk: "The Mapping Degree of the Pole Placement Map".

Symposium on Implicit and Nonlinear Systems, Ft. Worth, Texas, December 14–15, 1992. Title of talk: "On Homogeneous Autoregressive Systems".

31st IEEE Conference on Decision and Control, Tucson, Arizona, December 16–18, 1992. Title of talk: "Dynamic Pole Placement and the Connection to Geometry."

AMS Sectional Meeting, Northern Illinois University, DeKalb, Illinois, May 20–23, 1993. Title of talk: "A Cell Structure for the Set of Autoregressive Systems."

European Control Conference, Groningen, The Netherlands, June 28–July 1, 1993. Title of talk: "On Subsets of Autoregressive Systems and Stabilization Conditions".

International Symposium on the Mathematical Theory of Networks and Systems, Regensburg, Germany, August 2– 6, 1993. Title of talk: "Schubert Calculus and Dynamic Pole Placement".

IT Workshop on Coding, System Theory, and Symbolic Dynamics, Mansfield, MA, October 18–20, 1993. Title of talk: "Autoregressive Systems over Finite Fields, with Applications to Coding".

32nd IEEE Conference on Decision and Control, San Antonio, Texas, December 15–17, 1993. Title of talk: "On Decentralized Dynamic Feedback Compensation".

1994 IEEE International Symposium on Information Theory, Trondheim, Norway, June 27 – July 1, 1994. Title of talk: "An Ideal Theoretic Approach for Classifying High Rate Convolutional Codes".

Fourth Conference of the International Linear Algebra Society (ILAS), Rotterdam, The Netherlands, August 15–19, 1994. Title of talk: "Grassmannians, a Link between Linear Algebra, Linear Systems Theory and Geometry".

14-th BeNeLux Meeting on Systems and Control, Houthalen, Belgium, March 29-31, 1995. Title of talk: "On a General Realization Theory".

IFAC Conference on System Structure and Control, Nantes, France, July 5–7, 1995. Title of talks: "A Realization Theory for Homogeneous AR-Systems, an Algorithmic Approach", and "Linear Systems Defined over a Finite Field, LQ Theory and Convolutional Codes".

1995 IEEE International Symposium on Information Theory, Whistler, B.C. Canada, September 17-22, 1995. Title of talk: "First Order Representations for Convolutional Encoders".

Third Symposium on Matrix Analysis and Applications, Kalamazoo, Michigan, October 13-14, 1995. Title of talk: "A General Sufficient Condition for the Matrix Completion Problem".

34th IEEE Conference on Decision and Control, New Orleans, Louisiana, December 13–15, 1995. Title of talks: "A Parameterization of Homogeneous AR-Systems" and "Generic Eigenvalue Assignment for Generalized Linear First Order Systems using Memoryless Real Output Feedback".

Second Southeastern Linear Algebra Meeting (SELAM), The College of William and Mary, Virginia, March 23 1996. Title of talk: "Inverse Eigenvalue Problems and Matrix Completion Problems Arising in Systems Theory".

International Symposium on the Mathematical Theory of Networks and Systems, St. Louis, Missouri, June 24–28, 1996. Title of talk: "The Pole Placement Problem: Past, Present and Future Directions".

34*th Annual Allerton Conference on Communication, Control, and Computing,* Illinois, October 2-4, 1996.

First Lincoln Workshop in Cryptology & Coding Theory, Lincoln, Nebraska, June 1-4, 1997. Title of talk: "A BCH Construction for Convolutional Codes".

1997 IEEE International Symposium on Information Theory, Ulm, Germany, June 29–July 4, 1997. Title of talk: "A construction of binary BCH convolutional codes".

35*th Annual Allerton Conference on Communication, Control, and Computing,* Illinois, September 29–October 1, 1997. Title of talk: "Construction of convolutional codes using methods from linear systems theory".

36th IEEE Conference on Decision and Control, San Diego, California, December 10-12, 1997. Title of talks: "On output feedback invariants and cascade equivalence of systems" and "Some interesting problems in systems theory which are of fundamental importance in coding theory".

MTNS 98, International Symposium on the Mathematical Theory of Networks and Systems, Padova, Italy, July 6–10, 1998. Title of talk: "Block and convolutional codes and relations to systems theory".

1998 IEEE International Symposium on Information Theory, MIT, August 16-21, 1998.

36*th Annual Allerton Conference on Communication, Control, and Computing,* Illinois, September 23–25, 1998. Title of talk: "Maximum Distance Separable Convolutional Codes".

37th IEEE Conference on Decision and Control, Tampa, Florida, December 16-18, 1998. Title of talks: "Open problems in the area of pole placement" and "An optimal control theory for systems defined over finite rings".

Advances in Mathematical Systems Theory, Workshop in honour of Diederich Hinrichsen, Borkum Island, Germany, April 20-23, 1999. Title of talk: "Construction and Decoding of Multidimensional Convolutional Codes".

ForneyFest, a conference in honour of G.D. Forney on the occasion of his 60th birthday, Cambridge, Massachusetts, March 3rd and 4th 2000. Title of talk: "Minimal Bases of Rational Vector Spaces and their Importance in Algebraic Systems Theory".

Mark Pinsker Jubilee Seminar, a conference in honour of Mark Pinsker on the occasion of his 75th birthday, Lund Institute of Technolog, Lund, Sweden, April 25, 2000. Title of talk: "Maximum Distance Separable Convolutional Codes".

AMS-IMS-SIAM Joint Summer Research Conference on Symbolic Computation, Mount Holyoke College, June 11 - 15, 2000. Title of invited one hour plenary talk: "On the Minimal Number of Terms to Describe a Submodule in R^n and the Importance of this Question in Coding Theory".

2000 IEEE International Symposium on Information Theory, Sorrento, Italy, June 25-30, 2000.

38*th Annual Allerton Conference on Communication, Control, and Computing,* Illinois, October 4–6, 2000. Title of talk: "Constructions of LDPC Codes Using Ramanujan Graphs and Ideas from Margulis".

2nd Midwest Arithmetical Geometry in Cryptography Workshop, University of Illinois at Urbana-Champaign, November 17 - 19, 2000. Title of talk: "Using Low Density Parity Check Codes in the McEliece Cryptosystem".

AMS Sectional Meeting, Hoboken, NJ, April 28–29, 2001. Title of talk: "Maximum Distance Separable Convolutional Codes, Constructions and Decoding."

2001 IEEE International Symposium on Information Theory, Washington DC, June 24-29, 2001.

SIAM Conference on Control and its Applications, San Diego, California, July 11–14, 2001. Title of talk: "Operator Algebras and Public Key Cryptography ."

SIAM Conference on Linear Algebra in Signals, Systems and Control, Boston, Massachusetts, August 12–14, 2001. Title of invited special topics lecture (45 Min): "Coding Theory and Systems over Finite Fields."

39*th Annual Allerton Conference on Communication, Control, and Computing,* Illinois, October 3–5, 2001. Title of talk: "Unitary matrices with maximal or near maximal diversity product".

3rd Midwest Arithmetical Geometry in Cryptography Workshop, University of Illinois at Urbana-Champaign, November 2 - 4, 2001. Title of talk: "One-way trapdoor functions from group actions".

AMS National Meeting, San Diego, January 6–9, 2002. Title of invited special topics lecture (45 Min): "Convolutional Codes, an Algebraic Geometric Point of View."

ISIT 2002, IEEE International Symposium on Information Theory, Lausanne, Switzerland, June 30–July 5, 2002. Two papers presented by coauthors.

Symbolic Computational Algebra 2002, Fields Institute special meeting on Symbolic and Numeric Computation in Geometry, Algebra and Analysis, University of Western Ontario, London, Ontario, Canada, July 15 - 19, 2002. One of the main speakers with a total of 4 one hour lectures on coding and cryptography.

40*th Annual Allerton Conference on Communication, Control, and Computing,* Illinois, October 2–4, 2002. Title of talk: "Unitary Constellations with Large Diversity Product and Small Diversity Sum".

IWOTA 2003, Fourteenth International Workshop on Operator Theory and Applications, Cagliari, Italy, June 24-27, 2003. Invited plenary talk (45 Min): "Operator Algebras and Public Key Cryptography".

41*st Annual Allerton Conference on Communication, Control, and Computing,* Illinois, October 1–3, 2003. Title of talk: "Some new Algebraic constructions of Codes from Graphs which are good Expanders".

Directions on Control Theory and Applications, Lubbock, Texas, November 14–15, 2003. Title of talk: "Output Feedback Pole Assignment for Transfer Functions with Symmetries".

Oberwolfach Meeting in Coding Theory, Oberwolfach, Germany, December 8–12, 2003. Invited one hour plenary talk: "Algebraic Constructions of Low Density Parity Check Codes".

MTNS 2004, International Symposium on the Mathematical Theory of Networks and Systems, Leuven, Belgium, July 5–9, 2004. Invited one hour plenary talk: "Convolutional Codes, Systems over Finite Fields and Fault Tolerance".

ILAS 2004, 11th Conference of the International Linear Algebra Society, Coimbra, Portugal, July 19–22, 2004. Invited plenary talk (45 Min): "Public Key Crypto-systems built from Semi-Group Actions".

Annual Meeting of the Swiss Mathematical Society, Lausanne, Switzerland, September 15-16, 2004. Invited one hour plenary talk: "Public Key Crypto-systems built from Semi-Group Actions".

Seminar on Convolutional Codes and Algebraic Geometry, Salamanca, Spain, November 4–5, 2004. One hour plenary talk: "Survey on Convolutional Codes and Relations to Algebraic Geometry".

Conference on Algebra and its Applications, Athens, Ohio, March 22–26, 2005. Invited plenary talk: "Public Key Crypto-Systems built from Finite Simple Semirings".

IWOTA 2005, 16th International Workshop on Operator Theory and Applications, Connecticut, July 24-27, 2005. Invited plenary talk (45 Min): "Building Public Key Crypto-Systems from Operators over Semi-Rings".

Workshop on Linear Systems Theory, Sde Boker, Israel, September 12-16, 2005. Invited plenary talk: "Public Key Crypto-Systems and Linear Systems over Semi-Rings".

MAGIC 2005, Midwest Algebraic Geometry and their Interactions Conference, Notre Dame, Indiana, October 7–11, 2005. Invited plenary talk (45 Min): "Constructing One-way Trapdoor Functions from Simple Semi-Rings and Semi-Modules".

Tagung der Berufsmittelschule-Fachhochschule Dozenten in Mathematik, Winterthur, Switzerland, November 12, 2005. One hour plenary talk: "Kryptographie und Mathematik: Von Chiffriermaschinen zum Internet".

Workshop on Convolutional Codes and Systems Theory, Würzburg, Germany, November 16–18, 2005. One hour plenary talk: "LDPC Codes, Codes on Graphs and Ramanujan Graphs".

MTNS 2006, International Symposium on the Mathematical Theory of Networks and Systems, Kyoto, Japan, July 24-28, 2006. Title of talk: "Good Packings in the Complex Stiefel Manifold using Numerical Methods".

International Conference on Interdisciplinary Mathematical & Statistical Techniques, Tomar, Portugal September 1-4, 2006. Invited talk: "Black box queries for finite groups".

3rd International Workshop on Mathematical Techniques and Problems in Telecommunications, Leiria, Portugal, Sept 4-8, 2006. Three hours plenary lectures on "Encryption".

10th Workshop on Elliptic Curve Cryptography (ECC 2006), Fields Institute, Canada, September 18-20, 2006.

Projective Geometry and Commutative Algebra in Applications, Genova, Italy, June, 15-16, 2007. Title of talk: "Factoring Integers".

ICIAM 07, 6th International Congress on Industrial and Applied Mathematics, Zürich, Switzerland, July 16–20, 2007. Title of talk: "Systems theoretic questions in coding theory".

4th Workshop on Coding and Systems, Alicante & Elche, Spain, March 13-15, 2008.

AMS Sectional Meeting, Bloomington, Indiana, April 5-6, 2008. Title of talk: "Spread Codes for Network Coding, a Grassmannian Approach".

ISIT 2008, IEEE International Symposium on Information Theory, Toronto, Canada, July 6–11, 2008. Two papers presented by coauthors.

MTNS 2008, Virginia Tech, July 28-August 1, 2008. Paper presented by coauthor.

A Workshop on Linear Systems Theory: Model Reduction, Sde Boker, Israel, September 15–19, 2008. Invited plenary talk: "Cryptography and Systems".

ALAMA, Vitoria-Gasteiz, Spain, September 25-26, 2008. Title of plenary talk: "Construction and Decoding of Spread Codes".

ISIT 2009, IEEE International Symposium on Information Theory, Seoul, Korea, June 28–July 3, 2009. Paper presented by coauthor.

5th Workshop on Coding and Systems, Dublin, Ireland, September 2–4, 2009. Title of Talk: "Observing a very noisy state output system and applications to stream ciphers".

A Celebration of the Field of Systems and Control, Stockholm, Sweden, September 9-11, 2009. Title of talk: Pole placement in characteristic p.

Jornadas de Matematicas en la Sociedad de la Informacion, Alicante, Spain, November 26–27, 2009. Title of talk: "Correlations in Stream Ciphers, a Systems Theory Point of View".

Algebraic Combinatorics and Applications (ALCOMA10) Thurnau, Germany, April 11–18, 2010. Title of talk: "MDP Convolutional Codes".

Journée annuelle of the French Mathematical Society, Paris, France, June 26–27, 2010. Title of plenary talk: "Convolutional Codes, Mathematical Properties and their Applications".

10th International Conference Computational and Mathematical Methods in Science and Engineering, Almeria Spain, June 26–30, 2010. Title of plenary talk: "Building Public Key Crypto-Systems".

MTNS 2010, Budapest, Hungary, July 5–9, 2012. 4 talks given by co-authors.

Rüdlingen Conference, Rüdlingen, Switzerland, September 6, 2010. Title of plenary talk: "Construction Questions in Public Key Cryptography".

Workshop in Celebration of the Life, Mathematics and Memories of Christopher I. Byrnes, Lubbock, Texas, September 10–12, 2010. Title of talk: "Pole Placement and its Connection to Geometry".

WCC 2011, the Seventh International Workshop on Coding and Cryptography, Paris, France, April 11-15, 2011. 2 Papers presented by coauthors.

ISIT 2011, IEEE International Symposium on Information Theory, St. Petersburg, Russia, July 31 – August 5, 2011. 2 Papers presented by coauthors.

WCS 2011, 6th Workshop on Coding and Systems, Aveiro, Portugal, June 13 - 15, 2011. Title of plenary talk: "Decoding of MDS and near MDS Convolutional Codes over the Erasure Channel".

Algebraic Structure in Network Information Theory, Banff, Canada, August 14–19, 2011. Title: Schubert Calculus and its Relation to Network Coding.

Workshop on Computational Security, Centre de Recerca Matematica, Bellaterra, Spain, November 28 - December 2, 2011. Title of talk: "The Difficulty of constructing Oneway Trapdoor Functions".

Conference on Codes and Topology, Castro Urdiales, Spain, May 31st-June 1st, 2012. Title of plenary talk:"Convolutional Codes, a Study via Duality".

MTNS 2012, Melbourne, Australia, July 9–13, 2012. Title of talk: "Decoding of Subspace Codes, a Problem of Schubert Calculus".

Trends in Coding Theory, Centro Stefano Franscini, Ascona (Switzerland), October 28–November 2, 2012. Organizer (with A. Shokrollahi and E. Gorla).

European Training School in Network Coding, Barcelona, Spain, February 4–8, 2013. Title of plenary talk: "Schubert Calculus over Finite Fields".

Elgersburg Workshop in Systems Theory, Elgersburg, Germany, February 11–14, 2013. Title of plenary talk: "Systems Theoretic Questions in Coding Theory".

The Art of Iterating Rational Functions over Finite Fields, Banff, Canada, May 5–10, 2013. Title of talk: "Some Dynamical Systems over Finite Fields appearing in Coding Theory and Cryptography".

Zurich COST Meeting - Random Network Coding and Designs over GF(q), June 20-21, 2013. Organizer of this Event.

ISIT 2013, IEEE International Symposium on Information Theory, Istanbul, Turkey, July 7–12, 2013.

SIAM Conference on Applied Algebraic Geometry, Fort Collins, Colorado, August 1–4, 2013. Title of talk: "List Decoding of Subspace Codes".

Dagstuhl Seminar on Coding Theory, Dagstuhl, Germany, August 25–30, 2013.

Conference on Random network codes and Designs over GF(q), Ghent, Belgium, September 18-20, 2013. Title of talk: "List Decoding of Subspace Codes".

Workshop On Coding and Information Theory (WCI 2013), The University of Hong Kong, December 11-13, 2013. Title of talk: "Subspace Codes and Orbit Codes".

Algebra, Codes and Networks, Bordeaux, France, June 16 - 20, 2014.

MTNS 2014,Groningen, The Netherlands, July 7–11, 2014. Title of talk: "Limitations of Polynomial-Size List-Decoding of Projective Space Codes".

Workshop on Communication Security, Ancona, Italy, September 11–12, 2014. Title of plenary talk: "The Semigroup Action Problem, a Cryptographic Primitive to build Asymmetric Cryptographic Protocols".

4th International Castle Meeting in Coding Theory, Palmela, Portugal, September 15–19, 2014. Title of plenary talk: "Convolutional Codes over Large Alphabets and their Decoding over the Erasure Channel".

Expanders Everywhere, University of Neuchatel, Neuchatel, Switzerland, December 1–5, 2014. Title of plenary talk: "Codes based on Expander Graphs and Ramanujan Graphs".

Algebraic Combinatorics and Applications (ALCOMA 15) Kloster Banz, Germany, March 15–20, 2015. Title of talk: "McEliece type Cryptosystem based on Gabidulin Codes".

7th Workshop on Coding and Systems, Salamanca, Spain, July 1-3, 2015 Title of talk: "Variants of McEliece type Cryptosystems based on Subspace Codes and Rank Metric Codes".

SIAM Conference on Applied Algebraic Geometry, Daejeon, Korea, August 3–7, 2015. Title of talk: "How Grassmannians are relevant in Coding Theory".

Design and Application of Random Network Codes (DARNEC 15), Istanbul, Turkey, Nov 4-6, 2015. Title of talk: "Cryptanalyis of McEliece type Public Key Systems based on Gabidulin Codes".

Algebraic Geometry for Coding Theory and Cryptography, IPAM, UC Los Angeles, February 22 - 26, 2016. Title of talk: "Code Based Crypto".

Network Coding and Designs, Dubrovnik, Croatia, April 4–8, 2016. Title of talk: "Public Key Crypto Systems based on Rank Metric Codes and Subspace Codes".

ISIT 2016, IEEE International Symposium on Information Theory, Barcelona, Spain, July 10-15, 2016. Title of talk: "Consideration for Rank-based Cryptosystems".

Dagstuhl Seminar on Coding Theory in the Time of Big Data, Dagstuhl, Germany, August 7–12, 2016.

CAM 2016, Conference on Applied Mathematics, The University of Hong Kong, August 23-26, 2016. Title of talk: "An Overview to Code based Cryptography".

Workshop on Networks on Linear Systems, Sde Boker, Israel, March 19–21, 2017. Invited plenary talk: "Algebraic Systems Theory and Coding Theory".

Fq13, 13th International Conference on Finite Fields and their Application, Gaeta, Italy, June 4–10, 2017.

IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, June 25–30, 2017. Two papers presented by coauthors.

Munich Workshop on Coding and Applications 2017 (MWCA 2017), Munich, Germany, July 3, 2017. Invited plenary talk: "Hiding Distinguishers in Code Based Cryptography".

SIAM Conference on Applied Algebraic Geometry, Georgia Tech, Atlanta, Georgia, July 30–August 4, 2017. Paper presented by co-author.

Fifth Irsee Conference on Finite Geometries, Kloster Irsee, Germany, September 10–16, 2017. Invited plenary talk: "An Overview on Post-Quantum Cryptography with an Emphasis on Code based Systems".

Munich Workshop on Coding and Cryptography (MWCC 2018), Munich, Germany, April 10-11, 2018. Invited plenary talk: "Convolutional Codes having good Distance Profile for a Particular Metric".

ALAMA 2018, Alicante, Spain, May 30–June 1, 2018. Invited plenary talk: "Convolutional Codes Old and New".

MTNS 2018, Hong Kong, July 16–20, 2018. Co-Organizer of three sessions. Title of talk: "Weight Two Masking of the Reed-Solomon Structure in Conjunction with List Decoding".

CIMPA Research School, Middle East Technical University, Ankara, Turkey, August 27 - September 7, 2018. One of the main lecturer.

Workshop on Pseudo-Randomness and Finite Fields, RICAM, Linz, Austria, October 15–19, 2018. Title of plenary talk: "Masking an algebraic structure in code based cryptography".

Dagstuhl Seminar on Algebraic Coding Theory for Networks, Storage, and Security, December 16–21, 2018.

SIAM Conference on Applied Algebraic Geometry, University of Bern, Bern, Switzerland, July 9–13, 2019. Title of talk: "Rank Metric Codes and Subspace Codes in a Convolutional Setting".

Munich Workshop on Coding and Cryptography (MWCC 2019), Munich, Germany, July 15–16, 2019. Invited plenary talk: "Code Based Crypto Involving Expanded Reed-Solomon Codes".

CIRM Conference on Arithmetic, Geometry, Cryptography and Coding Theory, AGCT 2021, Luminy, France, May 31–June 4, 2021. Invited online talk: "The Algebraic Theory of Convolutional Codes".

Crittographia e Codici, Italy, September 21, 2021. Invited online talk: "The Work of Michele Elia on Continued Fractions and Factoring".

Applications of Computer Algebra, ACA 2022, Gebze Technical University, Turkey, August 15–17, 2022. "Construction of Subspace Codes using Evaluation".

25th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2022) , Bayreuth, Germany, September 12–16, 2022. Title of talk: "Evaluation Subspace Codes and Convolutional Codes".

PQCifris 2022, School & Workshop on Post-Quantum Cryptography, Trento, Italy, October 10-14, 2022. 3 hours of lectures on post-quantum cryptography.

SIAM Conference on Applied Algebraic Geometry, Eindhoven University, Eindhoven, The Netherlands, July 10–14, 2023. Title of talk: "Optimal Subspace Codes in a Schubert Variety".

International Conference on Algebraic Geometry, Coding Theory and Combinatorics. A Conference in honour of Prof. Sudhir Ghorpade , Hyderabad, December 4–8, 2023. Title of talk: "Subspace Codes with near optimal distance in a Schubert Variety".

MatSI network meeting, University of Alicante, Spain, June 5, 2024. Title of talk: "Post-Quantum Cryptography and Code based Cryptography".

A workshop in honor of Paula Rocha, University of Porto, Portugal, July 19, 2024. Title of talk: "Using Linear Systems for building a Public Key System".

26th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2024) , Cambridge University, August 18-23, 2024. Title of talk: "An Approach to Constructing Convolutional Codes with Moderate Density and Quasi-Cyclic Structure".

Emerging Topics in Design and Cryptanalysis of Post-quantum schemes, Institute Henri Poincaré, Paris, France, November 4-8, 2024. Title of talk: "Semigroup Action Problem (SAP) and other Generalizations of the DLP".