RAINER STEINWANDT

EDUCATION

UNIVERSITY OF KARLSRUHE, GERMANY

DR. RER. NAT. (COMPUTER SCIENCE, PH.D. EQUIVALENT) 5/2000

summa cum laude

Thesis: *On the Algorithmic Decomposition of Systems of Polynomial Equations*

Supervisor: Thomas Beth (computer science)

Second Reviewer: Frank Herrlich (mathematics)

UNIVERSITY OF KARLSRUHE, GERMANY

DIPL.-INFORM. (COMPUTER SCIENCE, M.S. EQUIVALENT) 3/1998

summa cum laude

Thesis: *Algorithms for Rational Function Fields*

Supervisor: Thomas Beth (computer science)

PROFESSIONAL APPOINTMENTS

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE **1/2021–**

Dean, College of Science

Professor, Department of Mathematical Sciences

FLORIDA ATLANTIC UNIVERSITY **8/2005–12/2020**

established in 1961; member of Florida's State University System; main campus in Boca Raton, FL; five additional campuses/sites through six-county service region; Hispanic-Serving Institution; accredited by the Southern Association of Colleges and Schools; serves more than 29,000 undergraduate and graduate students through ten colleges; Carnegie classification – Doctoral Universities: High Research Activity

DEPARTMENT OF MATHEMATICAL SCIENCES

46 faculty; 4 staff; 46 GTAs; annual budget ca. 6.3M; ca. 33,000 student contact hours in academic year 2018/2019

Department Chair	7/2015–12/2020
Professor	9/2008–12/2020
Graduate Director	9/2010–6/2015
Associate Professor	8/2005–8/2008

CENTER FOR CRYPTOLOGY & INFORMATION SECURITY

Through this center, spanning across four FAU Colleges – Business, Computer Science and Engineering, Design & Social Inquiry, and Science – FAU has been recognized as a National Center of Academic Excellence in Information Assurance/Cyber Defense Research (CAE-R) for academic years 2014–2019 and 2019–2024.

Director	10/2013–12/2020

PEACE, JUSTICE AND HUMAN RIGHTS INITIATIVE

One of nine key platforms in FAU's strategic plan; a multidisciplinary effort bringing together scholars, practitioners, students and community leaders invested in human rights, peace and social justice.

Faculty Affiliate 10/2017–12/2020

UNIVERSITY OF KARLSRUHE (GERMANY) 6/2000–8/2005

public research university; established 1825; since 2009 part of Karlsruhe Institute of Technology; about 25,000 students; #135 in Times Higher Education world university rankings 2019

DEPARTMENT OF COMPUTER SCIENCE

Research Associate at Institute for Algorithms & Cognitive Systems

Research and teaching in cryptology and computer algebra.

ADMINISTRATIVE ACHIEVEMENTS

- Improved extramural funding of Department of Mathematical Sciences; proposals awarded in Fiscal Year 2015: $202,259 (7 awards) vs. Fiscal Year 2019: $1,275,072 (16 awards)
- Curriculum revisions and introduction of active learning:
  - collaborated with FAU's Math Learning Center to introduce Learning Assistants in the classroom; student success rate in Calculus 1 raised by 28% (Fall '14 vs. Fall '19)
  - College Algebra: implemented co-remediation approach; student success rate raised by 18% (Fall '14 vs. Fall '19)
  - Methods of Calculus: introduced major-specific sections and group learning; student success rate raised by 32% (Fall '14 vs. Fall '19)
- Collaborations with university administration:
  - established FAU-wide intervention for underprepared students ("Math Boot Camp"): about 70% success rate for students who before failed a math course twice
  - overhaul of placement for Mathematics courses; move to multi-factor-placement
- Reduced textbook cost for students through use of open educational resources in several courses.
- Hired 6 tenure-track and 7 non-tenure track full-time faculty.
- Established departmental bylaws.
- Implemented systematic teaching training for GTAs.
- Collaborated with institutional advancement and worked with private donor to secure funds for graduate student awards ($83,000).
- Co-developed a Master's degree in Data Science and Analytics across four Colleges.

- Established a cross-College Cybersecurity Certificate.
- Master's degree in Teaching Mathematics program moves fully online.
- Expanded student recruitment with emphasis on diversifying our graduate student cohort; established Florida's first faculty mentor alliance with *the National Alliance for Doctoral Studies in the Mathematical Sciences*, department joins *Association for Women in Mathematics*, FAU joins AAUW.
- Established three departmental student chapters of professional organizations; AWM chapter received Association for Women in Mathematics' 2018 and 2019 Fundraising and Sustainability awards.
- Expanded FAU's Center for Cryptology & Information Security from one to four FAU Colleges.
- Established FAU as designated DHS/NSA National Center of Academic Excellence in Information Assurance/ Cyber Defense Research (CAE-R).

ADMINISTRATIVE COMMITTEES

- FAU representative on State-University-System Cybersecurity Steering Group
- Member of Dean Search Committee at FAU's College of Science (twice; once as departmental representative, once as representative of the chairs)
- Member of Steering Committee of the International Conference on Post-Quantum Cryptography
- Member of FAU's College of Science Graduate Committee (2010–2015)
- Member of Expert Committee for the Election of Lead Research Fellow in Cryptography, University of Tartu, Estonia (2013)

RESEARCH AND TEACHING AWARDS

- 2018 NATO Science for Peace and Security Partnership Prize
- Research Mentoring Award as mentor, Florida Atlantic University (twice)
- Excellence in Teaching, Public Key Kryptographie, University of Karlsruhe
- Excellence in Teaching, Kryptographie und Datensicherheit, University of Karlsruhe
- German Research Foundation excellence program: Ph.D. stipend, renewable for three years

GRANTS & CONTRACTS

Secured extramural funding of more than $2.8M:

- PI*: Determining Cryptographic Security Margins in the Presence of Quantum Computing*, NSA (Sep 2020 – Aug 2022, project budget $322,179.80)
- PI: NATO Advanced Research Workshop *Toward a quantum-safe communication infrastructure* (Feb 2021, project budget ca. $51,936)
- Co-PI: *Online Modules for Emerging Topics in Cryptography*, Cyber Florida (Jul 2019 – Jun 2020, project budget $75,000)

- Co-PI: *Young CryptograpHers: a Cybersecurity Summer Camp for K-12 Girls*, Cyber Florida (Jul 2019, project budget $73,930)
- Co-PI: *Lattice Algorithms for Post-Quantum Cryptography*, NIST (Dec 2018 – Dec 2021, project budget $386,013)
- Co-PI: *A Platform for the Evaluation of Post-Quantum Primitives*, NIST (Dec 2018 – Dec 2020, project budget $194,980)
- PI of US partner: NATO multi-year Science for Peace (SfP) project *Secure Communication in the Quantum Era* (Oct 2018– Sep 2021, joint project with Slovak University of Technology, University of Malta, Universidad Rey Juan Carlos (Spain), project budget ca. $326,070)
- PI of US partner: *Quantum computers and their cryptographic impact* (study for German Federal Office for Information Security in collaboration with Saarland University, Germany, since Jan 2017, project budget ca. $420,900)
- PI: *Quantum Technology, High-Speed Encryption and Global Analysis of Networks*, Department of the Air Force (Jan 2015-Feb 2018, project budget ca. $392,400, joint project with FAU's Department of Physics)
- PI of US partner: NATO multi-year Science for Peace (SfP) project MD.SFPP 984520 – *Secure Implementation of Post-Quantum Cryptography* (Dec 2013 – Nov 2016, joint project with Slovak University of Technology, Tel Aviv University and Hubert Curien Laboratory, Jean Monnet University Saint-Etienne, project budget ca. $394,700+preceding planning grant, ca. $9,400)
- PI: NSF EAGER project 1049296, *Small-scale Quantum Circuits with Applications in Cryptanalysis* (Jan 2011 – Dec 2012, project budget ca. $110,534)
- Co-PI: *Security in GIG-like Architectures* (Pragmatics/Department of Defense project, Pervasive Computing, Oct 2008 – Sep 2009, project budget ca. US$ 132,000)
- PI: DFG project Ste-1041-1 *ANTI-BQP* within a special focus program on IT security (1 BAT IIa salary for 4 years)
- Co-PI: *Basing Security on Combinatorially Algebraic Techniques* (DAAD project with Universidad Rey Juan Carlos, several research sojourns Karlsruhe ↔ Madrid)
- Co-PI: *Feasibility study on special purpose hardware for factoring large integers* for the German Federal Office for Information Security (in collaboration with PACT XPP Technologies; 7 person months)

EDITORIAL WORK

Co-founded two journals (one published by de Gruyter, one diamond open access), member of four other editorial boards:

- Co-founding editor: *Journal of Mathematical Cryptology*

- Co-founding editor: *Mathematical Cryptology*
- Editorial board member: *Cryptography*
- Editorial board member: *Designs, Codes and Cryptography*
- Editorial Board Member: *Journal of Algebra, Combinatorics, Discrete Structures & Applications*
- Editorial board member: *Journal of Universal Computer Science*

Co-guest edited five special issues of journals:

- Co-guest editor, special issue Hardware Architectures for Algebra, Cryptology and Number Theory of *Integration, the VLSI Journal* (44(4), 2011)
- Co-guest editor, special issue of *Designs, Codes and Cryptography* on the occasion of Spyros Magliveras's 70th birthday (55(2–3), 2010)
- Co-guest editor, special section Special-Purpose Hardware for Cryptography and Cryptanalysis of *IEEE Transactions on Computers* (57(11), 2008)
- Co-guest editor, special issue Applications of Algebra to Cryptography for *Discrete Applied Mathematics* (156(16), 2008)
- Co-guest editor, special issue Mathematical Techniques in Cryptology of *Applicable Algebra in Engineering, Comm. & Computing* (16(6), 2006)

ORGANIZATION OF CONFERENCES & WORKSHOPS

- General Chair 9th International Conference on Post-Quantum Cryptography PQCrypto 2018
- Co-chair 2015 Korea-US Joint Workshop on Quantum Information
- Program Chair 10th International Conference on Post-Quantum Cryptography PQCryto 2019 (with J. Ding)
- Program Chair 9th International Conference on Post-Quantum Cryptography PQCryto 2018 (with T. Lange)
- Organizer of six Dagstuhl-Seminars and of two other meetings:
    - Dagstuhl-Seminar 19421: Quantum Cryptanalysis (with M. Mosca, M. Naya-Plasencia and K. Svore)
    - Dagstuhl-Seminar 17401: Quantum Cryptanalysis (with M. Mosca, K. Svore and N. Sendrier)
    - Dagstuhl-Seminar 15371: Quantum Cryptanalysis (with M. Mosca, M. Rötteler and N. Sendrier)
    - Dagstuhl-Seminar 13371: Quantum Cryptanalysis (with S. Fehr, M. Mosca and M. Rötteler)
    - Dagstuhl-Seminar 11381: Quantum Cryptanalysis (with S. Fehr, M. Mosca and M. Rötteler)

- Dagstuhl-Seminar 08491: Theoretical Foundations of Practical Information Security (with R. Canetti, S. Goldwasser and G. Müller)
- Special session Mathematics in Cryptology, International Conference on Computational and Mathematical Methods in Science and Engineering, CMMSE 2011
- Cryptology, Designs and Finite Groups 2009

PROGRAM COMMITTEES

Program Committee Member of 64 conferences/workshops:

- 12th International Conference on Post-Quantum Cryptography PQCrypto ’21
- R track of 2020 CAE in Cybersecurity Symposium
- 2nd International Workshop on Quantum Resource Estimation QRE 2020
- 20th Central European Conference on Cryptology CECC'20
- 23rd International Conference on Practice and Theory of Public Key Cryptography PKC 2020
- 6th International Conference on Information Systems Security and Privacy, ICISSP 2020
- 11th International Conference on Post-Quantum Cryptography PQCrypto ’20
- 13th International Conference on Provable & Practical Security ProvSec ’19
- 19th Central European Conference on Cryptology CECC'19
- 6th International Conference on Cryptology and Information Security in Latin America Latincrypt 2019
- 2nd International Workshop on Mathematical Cryptology MathCrypt 2019
- 12th International Conference on Information Technology and Communication Security SECITC ’19
- 14th ACM ASIA Conference on Computer and Communications Security ACM ASIACCS 2019
- 11th Workshop of Coding and Cryptography WCC 2019
- 5th International Conference on Information Systems Security and Privacy ICISSP 2019
- 18th Central European Conference on Cryptology CECC'18
- 12th International Conference on Provable Security ProvSec 2018
- 1st International Workshop on Mathematical Cryptology MathCrypt 2018
- 4th International Conference on Information Systems Security and Privacy, ICISSP 2018

- 11th International Conference on Information Technology and Communications Security SECITC 2018
- 23rd Annual International Conference on Theory and Application of Cryptology and Information Security ASIACRYPT 2017
- 20th Annual International Conference on Information Security and Cryptology ICISC 2017
- 8th International Conference on Post-Quantum Cryptography PQCrypto ’17
- 10th International Conference on Security for Information Technology and Communications SECITC 2017
- 3rd International Conference on Information Systems Security and Privacy ICISSP 2017
- 22nd Annual International Conference on Theory and Application of Cryptology and Information Security ASIACRYPT 2016
- 19th Annual International Conference on Information Security and Cryptology ICISC 2016
- 2nd International Conference on Information Systems Security and Privacy ICISSP 2016
- 9th International Conference on Information Theoretic Security
- 7th International Conference on Post-Quantum Cryptography PQCrypto ’16
- 9th International Conference on Security for Information Technology and Communications SECITC 2016
- 14th International Conference on Cryptology and Network Security CANS 2015
- 18th Annual International Conference on Information Security and Cryptology ICISC 2015
- International Conference on Information Science and Security 2015
- International Conference on IT Convergence and Security 2015
- 4th International Conference on Cryptology and Information Security in Latin America LATINCRYPT 2015
- IACR International Conference on Practice and Theory of Public-Key Cryptography PKC 2015
- 8th International Conference on Security for Information Technology and Communications SECITC 2015
- 9th International Workshop on Coding and Cryptography WCC 2015
- 1st International Conference on Information Systems Security and Privacy ICISSP 2015

- 17th Annual International Conference on Information Security and Cryptology ICISC 2014
- 6th International Conference on Post-Quantum Cryptography PQCrypto ’14
- 16th Annual International Conference on Information Security and Cryptology ICISC 2013
- 15th Annual International Conference on Information Security and Cryptology ICISC 2012
- 15th Information Security Conference ISC 2012
- 15th International Workshop on Practice and Theory in Public Key Cryptography PKC 2012
- Special-purpose Hardware for Attacking Cryptographic Systems SHARCS 2012
- 14th Annual International Conference on Information Security and Cryptology ICISC 2011
- 14th Information Security Conference ISC 2011
- 13th Annual International Conference on Information Security and Cryptology ICISC 2010
- 13th Information Security Conference ISC 2010
- 11th International Workshop on Cryptographic Hardware and Embedded Systems CHES 2009
- 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2009
- 12th Annual International Conference on Information Security and Cryptology ICISC 2009
- 12th Information Security Conference ISC 2009
- 11th Annual International Conference on Information Security and Cryptology ICISC 2008
- Mathematical Methods in Computer Science MMICS 2008
- 11th International Workshop on Practice and Theory in Public Key Cryptography PKC 2008
- 1st International Conference on Symbolic Computation & Cryptography SCC 2008
- The 27th Annual International Cryptology Conference CRYPTO 2007
- Information Security and Cryptology: 3rd Sklois Conference Inscrypt 2007
- Special-purpose Hardware for Attacking Cryptographic Systems SHARCS 2007

- 7th Central European Conference on Cryptology TATRACRYPT 2007
- Emerging Trends in Information & Communication Security ETRICS 2006
- Information Security and Cryptology: 2nd Sklois Conference Inscrypt 2006

ACADEMIC PROGRAM REVIEWER

- Institut national de recherche en informatique et en automatique (INRIA, France) theme *Algorithmics, Computer Algebra and Cryptology* (2019)
- Undergraduate Mathematics program at University of Texas of the Permian Basin (2018)

PROJECT REVIEWER

- Project reviewer for ten funding agencies:
    - Austrian Research Promotion Agency (FFG)
    - Austrian Science Fund (FWF)
    - British Engineering and Physical Sciences Research Council
    - FWO Research Foundation Flanders
    - German-Israeli Foundation for Scientific Research and Development
    - Israel Science Foundation
    - National Science Foundation
    - Natural Sciences and Engineering Research Council of Canada
    - Netherlands Organisation for Scientific Research
    - United States-Israel Binational Science Foundation

BOOK & JOURNAL REVIEWER

- Book reviewer:
    - Chapman & Hall/CRC
    - Cambridge University Press
- Journal reviewer for 26 journals:
    - Algorithms
    - Annals of Mathematics and Artificial Intelligence
    - Applicable Algebra in Engineering, Communication and Computing
    - Designs, Codes and Cryptography
    - Discrete Applied Mathematics
    - Entropy
    - Finite Fields and Their Applications

  - Experimental Mathematics
  - IEEE Transactions on Computers
  - IEEE Transactions on Dependable and Secure Computing
  - IEEE Transactions on Information Forensics and Security
  - IEEE Transactions on Information Theory
  - IEEE Transactions on Quantum Engineering
  - Information Processing Letters
  - Integration, the VLSI Journal
  - International Journal of Circuit Theory and Applications
  - International Journal of Communication Systems
  - International Journal of Information Security
  - Journal of Combinatorial Mathematics & Combinatorial Computing
  - Journal of Cryptology
  - Journal of Mathematical Analysis and Applications
  - Journal of Pure and Applied Algebra
  - Journal of Symbolic Computation
  - Journal of Systems and Software
  - New Journal of Physics
  - Quantum Information Processing
  - SCIENCE CHINA Information Sciences

COURSES TAUGHT

FLORIDA ATLANTIC UNIVERSITY

Undergraduate level:

- Calculus–Analytic Geometry 1 (MAC 2311): Fall 06, Spring 07, Fall 12
- Calculus–Analytic Geometry 2 (MAC 2312): Fall 07
- Calculus–Analytic Geometry 3 (MAC 2313): Spring 08, Fall 08, Spring 09
- Introduction to Computational Mathematics (MAD 2502): Spring 2010, Fall 14, Fall 15, Fall 16, Fall 17, Fall 18, Fall 19, Fall 20
- Engineering Mathematics I (MAP 3305): Spring 12
- Applying Mathematics to Information Security (MAT 4906, co-located with MAD 6209): Summer 07
- Cryptography and Information Security (CIS 4362, co-located with MAD 5474): Fall 06, Fall 08, Spring 13
- Introduction to Coding Theory (MAD 4605): Fall 13

- Modern Algebra (MAS 4301): Spring 14
- Intro Quantum Computing with Applications to Crypto (MAT 4930): Fall 19

Graduate level:

- Advanced Topics in Cryptology (MAD 6209): Spring 06
- Introduction to Cryptology and Information Security (MAD 5474, co-located with CIS 4362): Fall 06, Fall 08, Spring 13
- Cryptanalysis (MAD 6478): Fall 06, Spring 08
- Ideals, Varieties and Algorithms (MAS 6396): Spring 07
- Applying Mathematics to Information Security (MAT 4906, collocated with MAD 6209): Summer 07
- Elliptic Curves (MAS 6396): Fall 07, Fall 09
- Computational Mathematics (MAT 5932): Spring 09
- Linear Algebra (MAS 5145): Fall 10
- Coding Theory (MAD 6607): Spring 11
- Number Theory and Cryptography (MAS 6217): Fall 11

UNIVERSITY OF SOUTH FLORIDA

Graduate level – I was hired to develop a new fully online course for USF, as the university lacked the necessary faculty expertise in cryptography.

- Applied Cryptography (MAT 5932): Spring 15

UNIVERSITY OF KARLSRUHE, GERMANY

Graduate level:

- Public-Key Kryptographie: WS 00/01, WS 01/02, WS 02/03, WS 03/04
- Public-Key Kryptographie II: SS 01, SS 02
- Ausgewählte Kapitel der Kryptoanalyse: SS 03
- Grundlagen der Computersicherheit: SS 04, SS 05
- Symbolische Vereinfachung polynomialer Gleichungssysteme: WS 04/05

Regular problem solving sessions accompanying a course/recitation:

- Übungen zu Informatik IV: SS 00
- Übungen zu Public-Key Kryptographie: WS 01/02, WS 02/03

Seminars:

- Kryptographie und Mathematik: WS 00/01
- Sicherheitsanalyse von Seitenkanälen: SS 02
- Systemsicherheit: Modelle und Methoden: WS 03/04
- Formale Sicherheitsmodelle: SS 04
- Faktorisieren: WS 04/05
- Kryptoanalyse auf parallelen Architekturen: SS 05

Programming lab courses:

- Kryptoanalyse: SS 01, SS 02, SS 03, SS 04, SS 05
- Kryptographie & Datensicherheit: WS 00/01, WS 01/02, WS 02/03, WS 03/04, WS 04/05

THESES

Habilitation à diriger des recherches (external reviewer):

- Françoise Levy-dit-Vehel*: Problèmes algébriques en cryptographie asymétrique*, Université Pierre et Marie Curie (France).

Supervised 12 Ph.D. students:

- Brittanney Amento: *Quantum Circuits for Cryptanalysis*
- Parshuram Budhathoki: *Elliptic Curves: Identity-based Signing and Quantum Arithmetic* (jointly supervised with T. Eisenbarth)
- WeiZheng Gao: *Password-authenticated two-party key exchange with long-term security*
- Madeline González Muñiz: *Cryptography in the presence of key-dependent messages*
- Brandon Langenberg: *Quantum Circuits for Symmetric Cryptanalysis*
- Kenneth Matheis: *An algebraic attack on block ciphers* (jointly supervised with S. Magliveras)
- Kashi Neupane: *Design and analysis of key establishment protocols*
- Hai Pham: *Contributions to quantum-safe cryptography: hybrid encryption and reducing the T gate cost of AES*
- Angela Robinson: *Biometric Visual Authentication and Quantum Resistance*
- Adriana Suárez Corona (Universidad de Oviedo, Spain): *Compilers and protocols for key establishment* (jointly supervised with C. Martínez López)
- Shaun Miller: *Algorithms in lattice-based cryptanalysis* (jointly supervised with S. Bai)
- Viktória I. Villányi: *Signature schemes in single and multi-user settings*

Ph.D. theses (external reviewer):

- Tomáš Fabšič: *Contributions to the Analysis of the QC-LDPC McEliece Cryptosystem*, Slovenská Technická Univerzita v Bratislave (Slovakia)
- Ludovic Perret: *Etude d'outils algébriques et combinatoires pour la cryptographie à clef publique*, Université de Marne-la-Vallée (France)
- Tony Thomas: *On Public-key Cryptography Using Hard Problems in Braid Group*s, Indian Institute of Technology (India)
- Pavol Zajac: *Discrete Logarithm Problem in Degree Six Finite Fields*, Slovenská Technická Univerzita v Bratislave (Slovakia)

M.S. theses:

- Brittanney Amento: *Message Authentication in an Identity-based Encryption Scheme: 1-Key-Encrypt-then-MAC*
- Hai Pham: *Distinguishability of Public Keys and Experimental Validation: the McEliece Public-Key Cryptosystem*

Diploma Theses at University of Karlsruhe (co-supervisor):

- Michael Blume: *CAPTCHAs zur Identifikation von menschlichen Benutzern*
- Regine Endsuleit: *Bedeutung multivariater Polynome für die Kryptoanalyse von Public-Key-Systemen*
- Ivonne Heinemann: *Polynomwahl im Zahlkörpersieb*
- Dennis Hofheinz: *Ein Seitenkanalangriff auf das Signaturverfahren QUARTZ*
- Florian Probst: *Mobile vertrauenswürdige Rechnerplattformen in Unternehmensanwendungen*
- Dominik Raub: *Algebraische Spezifikation von Privacy Policies*

Student Projects at University of Karlsruhe (co-supervisor):

- Jens-Matthias Bohli: *Schwache Schlüssel des Public-Key-Systems MST*$_1$
- Regine Endsuleit: *Algebraische Analyse der Hashfunktion von Tillich und Zémor*
- Michael Güttinger: *Faktorisierungen endlicher Gruppen für das Public-Key-System BMW*
- Dennis Hofheinz: *Angriffe auf das Public-Key-System Polly Cracker*
- Fabian Januszewski: *Formale Modelle für Mehrparteienprotokolle*
- Florian Rabe: *Modelling Honest-Looking Parties in Cryptographic Protocols*
- Zhenyu Sun: *Public-Key-Kryptographie auf Basis hyperelliptischer Kurven*

PUBLICATIONS

BOOKS

(in chronological order)

1. M.I. González Vasco and R. Steinwandt: *Group Theoretic Cryptography*, Chapman and Hall/CRC Cryptography and Network Security Series, 2015.
2. T. Lange and R. Steinwandt (eds.): Post-Quantum Cryptography, 9th International Conference, PQCrypto 2018, Lectures Notes in Computer Science, vol. 10786, Springer, 2018.
3. J. Ding and R. Steinwandt (eds.): Post-Quantum Cryptography, 10th International Conference, PQCrypto 2019, Lectures Notes in Computer Science, vol. 11505, Springer, 2019.

BOOK CHAPTERS

(in chronological order)

1. T. Beth, S. González, M.I. González Vasco, C. Martínez and R. Steinwandt: *Cryptographic Shelter for the Information Society: Modeling and Fighting Novel Attacks on Cryptographic Primitives*; in: Techno-Legal Aspects of Information Society and New Economy: an Overview, A. Mendez-Vilas, J.A. Mesa González, V. Guerrero Bote, F. Zapico Alonso, eds., Formatex, 2003
2. W. Geiselmann and R. Steinwandt: *On Specialized Hardware for Supporting the Number Field Sieve*; in: Embedded Cryptographic Hardware: Methodologies & Architectures, N. Nedjah and L. de Macedo Mourelle, eds., Nova Science, 2004.
3. W. Geiselmann, H. Köpfer, A. Shamir, R. Steinwandt and E. Tromer: *Fault-Tolerance in Hardware for Sparse Systems of Linear Equations, with Applications to Integer Factorization*; in: New Trends of Embedded Cryptographic Systems, N. Nedjah and L. de Macedo Mourelle, eds., Nova Science, 2006.

JOURNAL ARTICLES

(in chronological order)

1. J. Müller-Quade and R. Steinwandt: *Basic Algorithms for Rational Function Fields*; Journal of Symbolic Computation 27(2): 143–170, 1999.
2. R. Steinwandt and J. Müller-Quade: *Freeness, Linear Disjointness, and Implicitization—a Classical Approach*; Beiträge zur Algebra and Geometrie/Contributions to Algebra and Geometry 41(1): 57–66, 2000.
3. J. Müller-Quade and R. Steinwandt: *Gröbner Bases Applied to Finitely Generated Field Extensions*; Journal of Symbolic Computation 30(4): 469–490, 2000.

4. M. Schmid, R. Steinwandt, J. Müller-Quade, M.Rötteler and T. Beth: *Decomposing a matrix into circulant and diagonal factors*; Linear Algebra and its Applications, vol. 306, pp. 131–143, 2000.
5. J. Müller-Quade and R. Steinwandt: *Recognizing Simple Subextensions of Purely Transcendental Field Extensions*; Applicable Algebra in Engineering, Communication and Computing 11(1): 35–41, 2000.
6. R. Steinwandt: *On computing a separating transcendence basis*; SIGSAM Bulletin 34(4): 3–6, 2000.
7. R. Steinwandt: *On Ideal and Subalgebra Coefficients in Semigroup Algebras*; Results in Mathematics/Resultate der Mathematik, vol.39, pp.183–187, 2001.
8. M.I. González Vasco and R. Steinwandt: *Clouds over a Public Key Cryptosystem Based on Lyndon Words*; Information Processing Letters,vol.80, pp.239–242, 2001.
9. W. Geiselmann and R. Steinwandt: *Kryptoanalyse der Ruland/Schweitzer-Signatur von Bitströmen*; DuD —Datenschutz und Datensicherheit 25(10): 616–617, 2001.
10. R. Steinwandt, D. Janzing and T. Beth: *On using quantum protocols to detect traffic analysis*; Quantum Information and Computation 1(3): 62–69, 2001.
11. T. Beth, W. Geiselmann and R. Steinwandt: Angriffe auf physikalischer Ebene; Spektrum der Wissenschaft; Dossier 4/2001, pp.60–63, 2001.
12. W. Geiselmann, J. Müller-Quade, R.Steinwandt and T. Beth: *Über Quantencomputer und Quantenkryptographie*; DuD — Datenschutz und Datensicherheit 26(8): 453–457, 2002.
13. W. Geiselmann and R. Steinwandt: *Cryptanalysis of a knapsack-like cryptosystem*; Periodica Mathematica Hungarica 45(1): 21–27, 2002.
14. M. Hausdorf, W.M. Seiler and R. Steinwandt: *Involutive Bases in the Weyl Algebra*; Journal of Symbolic Computation 34(3): 181–198, 2002.
15. R. Steinwandt and W. Geiselmann: *Cryptanalysis of Polly Cracker*; IEEE Transactions on Information Theory 48(11): 2990–2991, 2002.
16. R. Steinwandt, W. Geiselmann and R. Endsuleit: *Attacking a polynomial-based cryptosystem: Polly Cracker*; International Journal of Information Security 1(3): 143–148, 2002.
17. W. Geiselmann, J. Müller-Quade and R. Steinwandt: *On "A New Representation of Elements of Finite Fields* $GF(2^m)$ *Yielding Small Complexity Arithmetic Circuits"*; IEEE Transactions on Computers 51(12): 1460–1461, 2002.
18. M.I. González Vasco and R. Steinwandt: *Obstacles in Two Public Key Cryptosystems Based on Group Factorizations*; Tatra Mountains Mathematical Publications, vol.25, pp. 23–37, 2002.

19. J. Müller-Quade and R. Steinwandt: *On the problem of authentication in a quantum protocol to detect traffic analysis*; Quantum Information and Computation 3(1): 48–54, 2003.
20. W. Geiselmann and R. Steinwandt: *A Redundant Representation of GF(q^n) for Designing Arithmetic Circuits*; IEEE Transactions on Computers, 52(7): 848–853, 2003.
21. M.I. González Vasco, M. Rötteler and R. Steinwandt: *On Minimal Length Factorizations of Finite Groups*; Experimental Mathematics, 12(1): 1–12, 2003.
22. W. Geiselmann, W. Meier and R. Steinwandt: *An Attack on the Isomorphisms of Polynomials Problem with One Secret*; International Journal of Information Security, 2(1): 59-64, 2003.
23. M.I. González Vasco and R. Steinwandt: *A Reaction Attack on a Public Key Cryptosystem Based on the Word Problem*; Applicable Algebra in Engineering, Communication and Computing, 14(5): 335–340, 2004.
24. M.I. González Vasco, D. Hofheinz, C. Martínez and R. Steinwandt: *On the security of two public key cryptosystems using non-abelian groups*; Designs, Codes and Cryptography, 32: 207–216 (Special Issue on the 3rd Pythagorean Conference), 2004.
25. W. Geiselmann and R. Steinwandt: *Power Attacks on a Side-Channel Resistant Elliptic Curve Implementation*; Information Processing Letters, 91(1): 29–32, 2004.
26. M.I. González Vasco, C. Martínez and R. Steinwandt: *Towards a Uniform Description of Several Group Based Cryptographic Primitives*; Designs, Codes and Cryptography, 33: 215–226, 2004.
27. J.-M. Bohli, M.I. González Vasco and R. Steinwandt: *Weak Keys in MST_1*; Designs, Codes and Cryptography, 37(3): 509–524, 2005.
28. W. Geiselmann and R. Steinwandt*: A Key Substitution Attack on $SFLASH^{v3}$*; Journal of Discrete Mathematical Sciences & Cryptography, 8(2): 137–141, 2005.
29. T. Beth, J. Müller-Quade and R. Steinwandt: *Cryptanalysis of a Practical Quantum Key Distribution With Polarization-Entangled Photons*; Quantum Information and Computation, 5(3): 181–186, 2005.
30. J.-M. Bohli, B. Glas and R. Steinwandt: *Algebraic Cryptosystems and Side Channel Attacks: Braid Groups and DPA*, Congressus Numerantium, 182: 145–154, 2006.
31. T. Beth, J. Müller-Quade and R. Steinwandt: *Computing restrictions of ideals in finitely generated k-algebras by means of Buchberger's algorithm*; Journal of Symbolic Computation (Logic, Mathematics and Computer Science: Interactions in honor of Bruno Buchberger (60th birthday)), 41(3–4), 372–380, 2006.

32. D. Hofheinz, J. Müller-Quade and R. Steinwandt: *On IND-CCA security modeling in cryptographic protocols*; Tatra Mountains Mathematical Publications, 33: 83–97,2006.
33. M.I. GonzálezVasco and R. Steinwandt: *Chosen ciphertext attacks as common vulnerability of some group-and polynomial-based encryption schemes*; Tatra Mountains Mathematical Publications, 33: 149–157, 2006.
34. J.-M. Bohli, S. Röhrich and R. Steinwandt: *Key substitution attacks revisited: taking into account malicious signers*; International Journal of Information Security 5: 30–36, 2006.
35. W. Geiselmann, M. I. González Vasco and R. Steinwandt: *Entwurf asymmetrischer kryptographischer Verfahren unter Berücksichtigung von Quantenalgorithmen*;it-Information Technology, 48(6): 327–331, 2006.
36. M. I. González Vasco and R. Steinwandt: *Pitfalls in public key cryptosystems based on free partially commutative monoids and groups*; Applied Mathematics Letters, 19(10): 1037–1041, 2006.
37. W. Geiselmann and R. Steinwandt: *Special Purpose Hardware in Cryptanalysis: The Case of 1024 Bit RSA*; IEEE Security & Privacy, 5(1): 63–66, 2007.
38. R. Steinwandt and M.I. González Vasco: *On ideal and subalgebra coefficients in a class of k-algebras*; Note di Matematica, 27(1): 77–83, 2007.
39. J.-M. Bohli, M.I. González Vasco and R. Steinwandt: *Secure Group Key Establishment Revisited*; International Journal of Information Security, 6(4): 243–254, 2007.
40. R. Steinwandt and V. I. Villányi: *A one-time signature using run-length encoding*; Information Processing Letters, 108(4): 179–185, 2008.
41. M. Grassl and R. Steinwandt: *Cryptanalysis of an Authentication Scheme Using Truncated Polynomials*; Information Processing Letters, 109(15): 861–863, 2009.
42. R. Steinwandt: *A ciphertext-only attack on Polly Two*; Applicable Algebra in Engineering, Communication and Computing, 21(2): 85–92, 2009.
43. M. González Muñiz and R. Steinwandt: *Security of Signature Schemes in the Presence of Key-Dependent Messages*; Tatra Mountains Mathematical Publications 47: 15–29, 2010.
44. R. Steinwandt and A. Suárez Corona: *Attribute-based group key establishment*; Advances in Mathematics of Communications, 4(3): 381–398, 2010.
45. W. Geiselmann, K. Matheis and R. Steinwandt: *PET SNAKE: A Special Purpose Architecture to Implement an Algebraic Attack in Hardware*, Transactions on Computational Science 10: 298–328, 2010.

46. R. Steinwandt and A. Suárez Corona: *Cryptanalysis of a 2-party key establishment based on a semigroup action problem*; Advances in Mathematics of Communications 5(1): 87–92, 2011.
47. M. Grassl, I. Ilić, S. Magliveras and R. Steinwandt: *Cryptanalysis of the Tillich-Zémor hash function*; Journal of Cryptology 24(1): 148–156, 2011.
48. V. Božović, D. Socek, R. Steinwandt and V. I. Villányi: *Multi-authority attribute based encryption with honest-but-curious central authority*; International Journal of Computer Mathematics 89(3): 268-283, 2012.
49. R. Steinwandt and A. Suárez Corona: *Identity-based non-interactive key distribution with forward security*; Designs, Codes and Cryptography 64: 195–208, 2012.
50. M. González Muñiz and R. Steinwandt: *Security of Message Authentication Codes in the Presence of Key-Dependent Messages*; Designs, Codes and Cryptography 64:161–169, 2012.
51. B. Amento, M. Rötteler and R. Steinwandt: *Quantum Binary Field Inversion: Improved Circuit Depth via Choice of Basis Representation*; Quantum Information & Computation 13: 116–134, 2013.
52. B. Amento, M. Rötteler and R. Steinwandt: *Efficient quantum circuits for binary elliptic curve arithmetic: reducing T-gate complexity*; Quantum Information & Computation 13: 631–644, 2013.
53. L. Klingler, R. Steinwandt and D. Unruh: *On using probabilistic Turing machines to model participants in cryptographic protocols*; Theoretical Computer Science 501: 49–51, 2013.
54. M. Rötteler and R. Steinwandt: *A quantum circuit to find discrete logarithms on ordinary binary elliptic curves in depth* $O(log^2n)$; Quantum Information & Computation 14: 888–900, 2014.
55. R. Steinwandt and A. Suárez Corona: *Scalable Attribute-based Group Key Establishment: from Passive to Active and Deniable*; Applicable Algebra in Engineering, Communication and Computing, vol. 25, pp. 1–20, 2014.
56. W. Gao, K. Neupane and R. Steinwandt: *Tuning a 2-round group key agreement*; International Journal of Information Security, vol. 13, pp. 467–476, 2014.
57. M. Roetteler and R. Steinwandt: *A note on quantum related-key attacks*; Information Processing Letters, vol. 115, no. 1, pp. 40–44, 2015.
58. P. Budhathoki and R. Steinwandt: *Automatic synthesis of quantum circuits for point addition on ordinary binary elliptic curves*; Quantum Information Processing, vol. 14, no. 1, pp. 201–216, 2015.
59. S. Kepley and R. Steinwandt: *Quantum circuits for* $\boldsymbol{F}_{2^n}$ *-multiplication with subquadratic gate count*; Quantum Information Processing, vol. 14, no. 7, pp. 2373–2386, 2015.

60. T. Eisenbarth, A. Meyerowitz and R. Steinwandt: *On the security margin of MAC striping*; Information Processing Letters, vol. 115, no. 11, pp. 899–902, 2015.
61. S. Kepley, D. Russo, and R. Steinwandt: *Cryptanalysis of a modern rotor machine in a multicast setting*, Cryptologia, vol. 40, no. 6, pp. 515–521, 2016.
62. P. Budhathoki, T. Eisenbarth, R. Steinwandt, and A. Suárez Corona: *Pairing-friendly curves with discrete logarithm trapdoor could be useful*, Applied Mathematics & Information Sciences, vol. 10, no. 6, 2016.
63. M.I. González Vasco, F. Hess and R. Steinwandt: *Combined schemes for signature and encryption: the public-key and the identity-based setting*, Information and Computation, vol. 246, pp. 1–10, 2016.
64. C. Chen, T. Eisenbarth, I. von Maurich, and R. Steinwandt: *Horizontal and Vertical Side Channel Analysis of a McEliece Cryptosystem*, IEEE Transactions on Information Forensics and Security, vol. 11, no. 6, pp. 1093–1105, 2016.
65. P. D'Arco, M. I. González Vasco, A. L. Pérez del Pozo, C. Soriente, and R. Steinwandt: *Private Set Intersection: New Generic Constructions and Feasibility Results*, Advances in Mathematics of Communications, vol. 11, no. 3, pp. 481–502, 2017.
66. K. Morozov, P. S. Roy, R. Steinwandt, and R. Xu: *On the security of the Courtois-Finiasz-Sendrier signature*, Open Mathematics, vol. 16, pp. 161–167, 2018.
67. M.I. González Vasco, A. Robinson and R. Steinwandt: *Cryptanalysis of a proposal based on the discrete logarithm problem inside S_n*, Cryptography, vol. 2, no. 3, 2018.
68. O. Seker, A. Fernandez-Rubio, T. Eisenbarth, and R. Steinwandt: *Extending Glitch-Free Multiparty Protocols to Resist Fault Injection Attacks*, IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 3, pp. 394–430, 2018.
69. A. Robinson and R. Steinwandt: *Group key establishment with physical unclonable functions*, Journal of Information and Optimization Sciences, vol. 40, no. 1, pp. 69–80, 2019.
70. J.-M. Bohli, M.I. González Vasco, and R. Steinwandt: *Password-authenticated group key establishment from projective hash functions*, International Journal of Applied Mathematics and Computer Science, vol. 29, no. 4, 2019.
71. H. Pham, R. Steinwandt, and A. Suárez Corona: *Integrating Classical Preprocessing into an Optical Encryption Scheme*, Entropy, vol. 21, no. 9, 872, 2019.

72. K. Matheis, R. Steinwandt, and A. Suárez Corona: *Algebraic Properties of the Block Cipher DESL*, Symmetry – Special Issue Interactions between Group Theory, Symmetry and Cryptology, vol. 11, no. 11, 1411, 2019.
73. E. Persichetti, R. Steinwandt, and A. Suárez Corona: *From Key Encapsulation to Authenticated Group Key Establishment – a Compiler for Post-Quantum Primitives*, Entropy – Special Issue Blockchain: Security, Challenges, and Opportunities, vol. 21, no. 12, 1183, 2019.
74. J.-M. Bohli, M.I. González Vasco, and R. Steinwandt: *Building Group Key Establishment on Group Theory: A Modular Approach*, Symmetry – Special Issue on Interactions between Group Theory, Symmetry and Cryptology, vol. 12, no. 2, 197, 2020.
75. B. Langenberg, H. Pham, and R. Steinwandt: *Reducing the cost of implementing AES as a quantum circuit*, IEEE Transactions on Quantum Engineering, vol. 1, 2500112, 2020.
76. M.I. González Vasco, A. L. Pérez del Pozo, and R. Steinwandt: *Group Key Establishment in a Quantum-Future Scenario*, Informatica, pp. 1-18, 2020.

ARTICLES IN CONFERENCE & WORKSHOP PROCEEDINGS

(in chronological order)

1. J. Müller-Quade and R. Steinwandt: *An application of Gröbner bases to the decomposition of rational mappings*; in Gröbner Bases and Applications, Lecture Note Series, vol. 251, pp. 448–462, Cambridge University Press, 1998.
2. R. Steinwandt: *Decomposing Systems of Polynomial Equations*; in Proceedings of the Second Workshop on Computer Algebra in Scientific Computing CASC '99, pp. 387–407, Springer, 1999.
3. R. Steinwandt and J. Müller-Quade: *On restricting ideals in finitely generated k-algebras*; in Proceedings of the Seventh Rhine Workshop on Computer Algebra RWCA '00, T.Mulders, ed., pp. 119–124, 2000.
4. R. Steinwandt, M. Grassl, W. Geiselmann and T. Beth: *Weaknesses in the* $SL_2(\boldsymbol{F}_{2^n})$ *Hashing Scheme*; in Advances in Cryptology – CRYPTO 2000 Proceedings, M. Bellare, ed., vol. 1880 of Lecture Notes in Computer Science, pp. 287–299, Springer, 2000.
5. F. Bao, T. Beth, R.H. Deng, W. Geiselmann, C. Schnorr, R. Steinwandt and H. Wu: *Cryptanalysis of Two Sparse Polynomial Based Public Key Cryptosystems*; in Public Key Cryptography, 4th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2001 Proceedings, K.Kim, ed., vol. 1992 of Lecture Notes in Computer Science, pp. 153–164, Springer, 2001.
6. R. Steinwandt: *Loopholes in Two Public Key Cryptosystems Using the Modular Group*; in Public Key Cryptography, 4th International Workshop on Practice and Theory in Public Key Cryptosystems, PKC 2001

Proceedings, K.Kim, ed., vol. 1992 of Lecture Notes in Computer Science, pp. 180–189, Springer, 2001.

7. R. Steinwandt, W. Geiselmann and T. Beth: *A Theoretical DPA-Based Cryptanalysis of the NESSIE Candidates FLASH and SFLASH*; in Information Security, 4th International Conference, ISC 2001 Proceedings, G.I. Davida, Y. Frankel, eds., vol. 2200 of Lecture Notes in Computer Science, pp. 280–293, Springer, 2001.
8. W. Geiselmann, R. Steinwandt and T. Beth: *Attacking the Affine Parts of SFLASH*; in Cryptography and Coding, 8th IMA International Conference, B. Honary, ed., vol. 2260 of Lecture Notes in Computer Science, pp. 355–359, Springer, 2001.
9. W. Geiselmann and R. Steinwandt: *A Reversible Redundant Representation of Extension Fields of* $GF(2^m)$; in 3. Kolloquium des Schwerpunktprogramms der Deutschen Forschungsgemeinschaft VIVA Grundlagen und Verfahren verlustarmer Informationsverarbeitung, D. Müller, C. Kretzschmar and R. Siegmund, eds., pp. 98–104, 2002.
10. R. Steinwandt: *Implicitizing without tag variables*; in Proceedings of the 8th Rhine Workshop on Computer Algebra RWCA 2002, H.Kredel, W.K. Seiler, eds., pp. 217–224, 2002.
11. D. Hofheinz and R. Steinwandt: *A "Differential" Attack on Polly Cracker*; in Proceedings of 2002 IEEE Inernational Symposium on Information Theory ISIT 2002, extended abstract, p. 211, 2002.
12. W. Geiselmann, R. Steinwandt and T. Beth: *Revealing the Affine Parts of SFLASHv1, SFLASHv2, and FLASH*; in Actas de la VII Reunión Española de Criptología y Seguridad de la Información; Tomo I, S. González, C. Martínez, eds., pp. 305–314, 2002.
13. M.I. González Vasco, C. Martínez and R. Steinwandt: *Un Marco Común para Varios Esquemas de Clave Pública Basados en Grupos*; in Actas de la VII Reunión Española de Criptología y Seguridad de la Información; Tomo I, S. González, C. Martínez, eds., pp. 353–364, 2002.
14. T. Beth, J. Müller-Quade and R. Steinwandt: *Computing restrictions of ideals in finitely generated k-algebras by means of Buchberger's algorithm*; in Proceedings of Symposium in Honor of Bruno Buchberger's 60th Birthday; Logic, Mathematics and Computer Science: Interactions (LMCS 2002), K.Nakagawa, ed., pp. 39–47, 2002.
15. W. Geiselmann, R. Steinwandt and T. Beth: *Revealing 441 Key Bits of* $SFLASH^{v2}$; in workshop record of the 3rd NESSIE Workshop, Munich, November 6–7, 2002.
16. D. Hofheinz and R. Steinwandt: *A Practical Attack on Some Braid Group Based Cryptographic Primitives*; in Public Key Cryptography, 6th International Workshop on Practice and Theory in Public Key

Cryptography, PKC 2003 Proceedings, Y.G. Desmedt, ed., vol. 2567 of Lecture Notes in Computer Science, pp. 187–198, Springer, 2002.

17. W. Geiselmann and R. Steinwandt: *A Dedicated Sieving Hardware*; in Public Key Cryptography, 6th International Workshop on Practice and Theory in Public Key Cryptography, PKC 2003 Proceedings, Y.G. Desmedt, ed., vol. 2567 of Lecture Notes in Computer Science, pp. 254–266, Springer, 2002.
18. W. Geiselmann and R. Steinwandt: *Hardware to Solve Sparse Systems of Linear Equations over GF(2)*; in Cryptographic Hardware and Embedded Systems, 5th International Workshop, CHES 2003 Proceedings, C.D. Walter, Ç.K. Koç, C. Paar, eds., vol. 2779 of Lecture Notes in Computer Science, pp. 51–61, Springer, 2003.
19. W. Geiselmann and R. Steinwandt: *On the security of cryptographic primitives regarding technological innovations*, in Proceedings of 33. Jahrestagung der Gesellschaft für Informatik, Informatik 2003.
20. D. Hofheinz, J. Müller-Quade and R. Steinwandt: *Initiator-Resilient Universally Composable Key Exchange*, in 8th European Symposium on Research in Computer Security, ESORICS 2003 Proceedings, E. Snekkenes, D. Gollmann, eds., vol. 2808 of Lecture Notes in Computer Science, pp. 61–84, Springer, 2003.
21. W. Geiselmann and R. Steinwandt: *Yet Another Sieving Device*, in RSA Conference 2004, Cryptographers' Track (CT-RSA 04) Proceedings, T. Okamoto, ed., vol. 2964 of Lecture Notes in Computer Science, pp. 278–291, Springer, 2004.
22. W. Geiselmann and R. Steinwandt: *Attacks on a Secure Group Communication Scheme with Hierarchical Access Control*, in Proceedings of 2004 IEEE International Symposium on Information Theory ISIT 2004, extended abstract, p. 14, 2004.
23. M. Backes, M. Dürmuth and R. Steinwandt: *An Algebra for Composing Enterprise Privacy Policies*, in 9th European Symposium on Research in Computer Security, ESORICS 2004 Proceedings, P. Samarati et al., ed., vol. 3193 of Lecture Notes in Computer Science, pp. 33–52, Springer, 2004.
24. M.I. González Vasco, D. Pérez García and R. Steinwandt: *On the Security of Certain Public Key Cryptosystems Based on Rewriting Problems*, in 8th Spanish Conference on Cryptology and Information Security, RECSI '04 Proceedings, pp. 175–184, 2004.
25. M.I. González Vasco, C. Martínez, R. Steinwandt and J. Villar: *On Provably Secure Encryption Schemes Based on Non-Abelian Groups*, in 8th Spanish Conference on Cryptology and Information Security, RECSI '04 Proceedings, pp. 101–111, 2004.
26. D. Raub, R. Steinwandt and J. Müller-Quade: *On the Security and Composability of the One Time Pad*, in 31st Annual Conference on Current

Trends in Theory and Practice of Informatics, SOFSEM 2005 Proceedings, P. Vojtáš et al., eds., vol. 3381 of Lecture Notes in Computer Science, pp. 288-297, Springer, 2005.

27. M.I. González Vasco, C. Martínez, R. Steinwandt and J. Villar: *A New Cramer-Shoup Like Methodology for Group Based Provably Secure Encryption Schemes*, in 2nd Theory of Cryptography Conference, TCC 2005 Proceedings, J. Kilian, ed., vol. 3378 of Lecture Notes in Computer Science, pp. 495–509, Springer, 2005.
28. J.-M. Bohli and R. Steinwandt: *On Subliminal Channels in Deterministic Signature Schemes*, in 7th Annal International Conference on Information Security and Cryptology, ICISC 2004 Proceedings, C. Park and S. Chee, eds., vol. 3506 of Lecture Notes in Computer Science, pp. 182–194, Springer, 2005.
29. W. Geiselmann, H. Köpfer, R. Steinwandt and E. Tromer: *Improved Routing-Based Linear Algebra for the Number Field Sieve*, in Proceedings of ITCC 2005 – Track on Embedded Cryptographic Systems, IEEE Computer Society, pp. 636-641, 2005.
30. W. Geiselmann, A. Shamir, R. Steinwandt and E. Tromer: *Scalable Hardware for Sparse Systems of Linear Equations, with Applications to Integer Factorization*; in Workshop on Cryptographic Hardware and Embedded Systems 2005, CHES 2005 Proceedings, J. R. Rao and B. Sunar, eds., vol. 3659 of Lecture Notes in Computer Science, pp. 131–146, Springer, 2005.
31. D. Raub and R. Steinwandt: *An Algebra for Enterprise Privacy Policies Closed Under Composition and Conjunction*, in International Conference on Emerging Trendsin Information and Communication Security, ETRICS 2006 Proceedings, G. Müller, ed., vol. 3995 of Lecture Notes in Computer Science, pp. 130–144, Springer, 2006.
32. M. I. González Vasco, R. Steinwandt and Jorge L. Villar: *Towards Provable Security for Cryptographic Constructions Arising from Combinatorial Group Theory*, in Algebraic methods in cryptography, L. Gerritzen, D. Goldfeld, M. Kreuzer, G. Rosenberger and V. Shpilrain, eds., vol. 418 of Contemporary Mathematics, pp. 89–101, American Mathematical Society, 2006.
33. A. Groch, D. Hofheinz, and R. Steinwandt: *A Practical Attack on the Root Problem in Braid Groups*, in Algebraic Methods in Cryptography, L. Gerritzen, D. Goldfeld, M. Kreuzer, G. Rosenberger and V. Shpilrain, eds., vol. 418 of Contemporary Mathematics, pp. 121–131, American Mathematical Society, 2006.
34. J.-M. Bohli, M. I. González Vasco and R. Steinwandt: *A Subliminal-Free Variant of ECDSA*, 8th Information Hiding IH 2006 Proceedings, J.

Camenisch et al., eds., vol. 4437 of Lecture Notes in Computer Science, pp. 375–387, Springer, 2007.

35. W. Geiselmann, F. Januszewski, H. Köpfer, J. Pelzl and R. Steinwandt: *A Simpler Sieving Device: Combining ECM and TWIRL*, in 9th International Conference on Information Security and Cryptology-ICISC 2006 Proceedings, M. S. Rhee and B. Lee, eds., vol. 4296 of Lecture Notes in Computer Science, pp. 118–135, Springer, 2006.
36. J.-M. Bohli and R. Steinwandt: *Deniable Group Key Agreement*, in International Conference on Cryptology in Vietnam 2006, VietCrypt 2006 Proceedings, P. Q. Nguyen, ed., vol. 4341 of Lecture Notes in Computer Science, pp. 298–311, Springer, 2006.
37. J.-M. Bohli, B. Glas, and R. Steinwandt: *Towards Provably Secure Group Key Agreement Building on Group Theory*, in International Conference on Cryptology in Vietnam 2006, VietCrypt 2006 Proceedings, P. Q. Nguyen, ed., vol. 4341 of Lecture Notes in Computer Science, pp. 322–336, Springer, 2006.
38. M. Abdalla, J.-M. Bohli, M. I. González Vasco and R. Steinwandt: *(Password) Authenticated Key Establishment: From 2-Party to Group*, Fourth Theory of Cryptography Conference, TCC 2007 Proceedings, S. P. Vadhan, ed., vol. 4392 of Lecture Notes in Computer Science, pp. 499–514, Springer, 2007.
39. W. Geiselmann and R. Steinwandt: *Non-Wafer-Scale Sieving Hardware for the NFS: Another Attempt to Cope with 1024-bi*t, Advances in Cryptology – EUROCRYPT 2007 Proceedings, M. Naor, ed., vol. 4515 of Lecture Notes in Computer Science, pp. 466–481, Springer, 2007.
40. W. Geiselmann and R. Steinwandt: *Cryptanalysis of a Hash Function Proposed at ICISC 2006*, International Conference on Information Security ICISC 2007 Proceedings, K.-H. Nam and G. Rhee, eds., vol. 4817 of Lecture Notes in Computer Science, pp. 1–10, Springer, 2007.
41. D. Naccache, R. Steinwandt and M. Yung: *Reverse Public Key Encryption*, Proceedings of the Special Interest Group on Biometrics and Electronic Signatures – BIOSIG 2009, vol. 155 of Lecture Notes in Informatics, Gesellschaft für Informatik (GI), 2009.
42. M. González Muñiz and R. Steinwandt: *Cryptanalysis of a Message Recognition Protocol by Mashatan and Stinson*, in 12th International Conference on Information Security ICISC 2009, vol. 5984 of Lecture Notes in Computer Science, pp. 362–373, Springer, 2010.
43. C. Martínez, R. Steinwandt and A. Suárez Corona: *Attribute-based group key establishment: a non-technical introduction*, 10th International Conference on Computational and Mathematical Methods in Science and Engineering CMMSE 2010 Proceedings, 2010.

44. K. Neupane and R. Steinwandt: *Server-assisted long-term secure 3-party key establishment*, in Proceedings of 5th International Conference on Security and Cryptography SECRYPT 2010, pp. 372–378, 2010.
45. K. Neupane and R. Steinwandt: *Communication-efficient 2-round group key establishment from pairings*, in Proceedings of CT-RSA 2011, vol. 6558 of Lecture Notes in Computer Science, pp. 65–76, Springer, 2011.
46. K. Neupane, R. Steinwandt and A. Suárez Corona: *Group key establishment: adding perfect forward secrecy at the cost of one round*, Proceedings of 11th International Conference on Cryptology and Network Security CANS 2012, vol. 7712 of LectureNotes in Computer Science, pp. 158–168, Springer, 2012.
47. K. Neupane, R. Steinwandt and A. Suárez Corona: *Scalable Deniable Group Key Establishment* (short paper), Proceedings of 5th International Symposium on Foundations and Practice of Security FPS 2012, vol. 7743 of Lecture Notes in Computer Science, pp. 365–373, Springer, 2013.
48. D. Naccache, R. Steinwandt, A. Suárez Corona and M. Yung: *Narrow Bandwidth is Not Inherent in Reverse Public-Key Encryption*, Proceedings of 9th Conference on Security and Cryptography for Networks SCN 2014, vol. 8642 of Lecture Notes in Computer Science, pp. 598-607, Springer, 2014.
49. C. Chen, T. Eisenbarth, I. von Maurich and R. Steinwandt: *Differential Power Analysis of a McEliece Cryptosystem*, Proceedings of 13th International Conference on Applied Cryptography and Network Security ACNS 2015, vol. 9092 of Lecture Notes in Computer Science, pp. 538-556, Springer, 2015.
50. C. Chen, T. Eisenbarth, I. von Maurich and R. Steinwandt: *Masking Large Keys in Hardware: A Masked Implementation of McEliece*, Proceedings of 22nd Conference on Selected Areas in Cryptography SAC 2015, vol. 9566 of Lecture Notes in Computer Science, pp. 293-309, Springer, 2016.
51. M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt: *Applying Grover's Algorithm to AES: Quantum Resource Estimates,* Proceedings of Post-Quantum Cryptography 2016, vol. 9606 of Lecture Notes in Computer Science, pp. 29-43, Springer, 2016.
52. B. Langenberg, H. Pham, and R. Steinwandt: *Reducing the cost of implementing AES as a quantum circuit* (extended abstract), 1st International Workshop on Quantum Resource Estimation QRE 2019, 2019
53. C. Colombo, M. I. González Vasco, R. Steinwandt, and P. Zajac: *Secure Communication in the Quantum Era: (Group) Key Establishment*, Advanced Technologies for Security Applications, NATO Science for Peace and Security Series B: Physics and Biophysics, pp. 65-74, Springer, 2020.

INVITED PRESENTATIONS & PANELS

1. *Some remarks on side-channel attacks on algebraic cryptosystems*, Workshop “Algebraic Methods in Cryptography”, Ruhr-Universität Bochum, November 9, 2001.
2. *Neue Algorithmen zur Kryptoanalyse mit physikalischen Methoden*, Ernst & Young-Konferenz “IT-Sicherheit in Gefahr?”, Munich, November 26, 2002.
3. *On the security of some cryptosystems based on non-abelian groups*, Third Pythagorean Conference, Faliraki, Rhodes, June 5, 2003.
4. *A special purpose mesh architecture for sieving in the number field sieve*, EIDMA-CWI Workshop on Factoring Large Numbers, Utrecht, December 12, 2003.
5. *Non-abelian groups in public key cryptography* (plenary talk), Winter Meeting 2004 of the Canadian Mathematical Society, Montréal, December 13, 2004.
6. *A systolic design for supporting Wiedemann’s algorithm*, SHARCS—Special-purpose Hardware for Attacking Cryptographic Systems, Paris, February 25, 2005.
7. *Polynomial Systems of Equations as Building Block of Asymmetric Cryptographic Schemes*, Gesellschaft für Angewandte Mathematik und Mechanik e.V.; 76th Annual Scientific Conference GAMM 2005, Luxembourg, March 31, 2005.
8. *Algebraic Cryptosystems and Side Channel Attacks*, special session “Algebraic Cryptography” at 2nd Joint Meeting of AMS, DMV, ÖMG, Mainz, June 18, 2005.
9. *Non-abelian groups in cryptography: constructions and attacks*; Workshop on Mathematical Problems and Techniques in Cryptology, CRM, Barcelona, June 21, 2005.
10. *Dedicated Hardware to Solve Sparse Systems of Linear Equations: State of the Art & Application to Integer Factoring*, 9th Workshop on Elliptic Curve Cryptography, DTU, Copenhagen, September 20, 2005.
11. *A Ciphertext-Only Attack on Polly Two*, Workshop Algebraic Methods in Cryptography, Bochum, November 18, 2005.
12. *What To Expect From a Key Establishment Protocol?*, Geometric and Asymptotic Group Theory with Applications, Barcelona, September 4, 2006.
13. *Another Attempt to Sieve With Small Chips -Part II: Norm Factorization*, Workshop Special purpose hardware for cryptography: Attacks and Applications, IPAM, UCLA, Los Angeles, December 6, 2006.
14. *Some Comments on Security Goals in the Presence of Malicious Insiders*, Workshop on Cryptographic Protocols WCP 2007, Bertinoro, March 6, 2007.

15. *On Defining and Proving Security in Cryptographic Key Establishment*, Special Session on Mathematical Aspects of Cryptography at AMS Sectional Meeting Spring 2007, Hoboken, NJ, April 15, 2007.
16. *Group Key Establishment: Some Security Goals and Constructions*, TATRACRYPT ’07 (plenary talk), Smolenice, June 23, 2007.
17. *Cryptography Tutorial*, Workshop Generic Case Complexity, American Institute of Mathematics, Palo Alto, CA, August 14, 2007.
18. *Non-Abelian Constructions in Cryptography: Challenges and Hopes*, SIAM Conference on Discrete Mathematics, Minisymposium Mathematical Aspects of Cryptography, Burlington, VT, June 19, 2008.
19. *On asymmetric encryption and digital signature with the same key*, Second Workshop on Mathematical Cryptology WMC 2008, Santander, October 25, 2008.
20. *Group Theory in Authenticated Key Establishment: What Assumption(s) Do We Make?*, MAA-AMS Joint Mathematics Meeting, AMS Special Session on Algebraic Cryptography and Generic Complexity, January 7, 2009.
21. *Minicourse on Mathematical Techniques in Modern Cryptography*, Stevens Institute of Technology, Hoboken, NJ, March 4–5, 2009.
22. *On combining identity-based encryption and signature schemes*, Geometric and Asymptotic Group Theory with Applications, Hoboken, NJ, March 12, 2009.
23. *Speeding up algebraic attacks: Multiple Right Hand Sides in hardware?*, Fields Cryptography Retrospective Meeting, Toronto (Canada), May 11, 2009.
24. *PET SNAKE: Implementing an Algebraic Attack in Hardware?*, 2009 Workshop on Cryptographic Protocols & Public-Key Cryptography, Bertinoro (Italy), May 26, 2009.
25. *Violating Key Separation: On Using One Secret Key for Two Purposes*, 9th Central European Conference on Cryptography, Třebíč (Czech Republic), June 23, 2009.
26. *Message authentication in the presence of key-dependent messages*, 4th Pythagorean Conference, An Advanced Research Workshop in Geometry, Combinatorial Designs & Cryptology, Corfu (Greece), June 1, 2010.
27. *Attribute-based group key establishment*, Workshop on Complexity and Group-based Cryptography, CRM Montréal (Canada), September 1, 2010.
28. *Mathematics in cryptographic key exchange: Alice, Bob, and Carol need to talk*, 11th International Conference Computational and Mathematical Methods in Science and Engineering CMMSE 2011 (plenary talk), Alicante (Spain), June 29, 2011.

29. *Algebraic properties of a lightweight block cipher*, Special Session on Mathematical Aspects of Cryptography and Cyber Security at 2011 Fall AMS Eastern Sectional Meeting, Ithaca, NY, September 10, 2011.
30. *Quantum Circuits for Binary Finite Field Arithmetic*, TATRACRYPT '12 (plenary talk), Smolenice (Slovakia), July 2, 2012.
31. *New hardness assumptions for post-quantum cryptography?*, Workshop on Post-Quantum Cryptography and Quantum Algorithms, Lorentz Center Leiden (The Netherlands), November 9, 2012.
32. *Implementing Binary Elliptic Curve Addition as Quantum Circuit*, Special Session on "Algorithmic problems of group theory and applications to information security," AMS Spring Eastern Sectional Meeting, April 6, 2013.
33. *Low-depth quantum circuits for computing discrete logarithms on binary elliptic curves*, Geometric and Asymptotic Group Theory with Applications, New York, May 30, 2013.
34. *Tapas of Quantum Cryptanalysis*, Central European Conference on Cryptology 2013(plenary talk), Telč (Czech Republic), June 26, 2013.
35. *Applying Shor's algorithm to the discrete logarithm problem on binary elliptic curves*, Special Session on Algebraic Cryptography at 2013 Fall AMS Southeastern Sectional Meeting, Louisville, KY, October 5, 2013.
36. *Post-Quantum Cryptography: How about Non-Abelian Groups?* (keynote talk), Workshop "Recent Developments in Post-Quantum Cryptography", Institute of Mathematics for Industry, Kyushu University, March 3, 2014.
37. *Cryptanalysis as a source for elementary circuit benchmarks*, Quantum Programming and Circuits Workshop, Waterloo (Canada), June 8, 2015.
38. *Resource estimates for quantum cryptanalysis*, Jahrestagung der Deutschen Mathematiker-Vereinigung 2015, mini-symposium on Algebraic Aspects of Cryptology, Hamburg (Germany), September 23, 2015.
39. *Quantum circuits for cryptanalysis*, 2015 Korea-US Joint Workshop on Quantum Information, Seoul (Korea), November 17 2015.
40. *Bounding the post-quantum security margin of block ciphers*, 16th Central European Conference on Cryptology, Piešťany (Slovakia), June 22, 2016.
41. Panelist: *Post-Quantum Cryptography*, Florida Center for Cybersecurity's 2018 Research Symposium, April 3, 2018.
42. Panelist: *Current Issues in Cryptography*, Florida Cyber Conference 2018, October 11, 2018.
43. *On implementing the AES S-box as a quantum circuit*, Special Session on Mathematical Cryptology at 2019 Spring Eastern Sectional Meeting, Hartford, CT, April 14, 2019.

44. *Secure communication in the quantum era: (group) key establishment*, NATO SPS Cluster Workshop on Key Priority Area Advanced Technologies, Leuven, Belgium, September 17, 2019.
45. *Password-Authenticated Key Establishment in the Advent of Scalable Quantum Computing*, AMS Special Session on Mathematics in Security & Defense, Joint Mathematics Meeting, January 7, 2021.