Krzysztof Pietrzak

Professor
Institute of Science and Technology Austria
ISTA

last compiled **March 9, 2026**
pietrzak@ista.ac.at
https://ist.ac.at/en/research/pietrzak-group/
https://sites.google.com/view/istacrypto/

Personal Details

Full Name:	Krzysztof Zbigniew Pietrzak
Citizenship:	Swiss & Polish.
Languages:	German & Swiss-German, English, Polish (fluent), French, Dutch (speak/read), Norwegian (read)

Research Interests

I have a broad interest in foundational and practical aspects of cryptography.

Current Employment

- **Institute of Science and Technology Austria (ISTA)** — Vienna, Austria
  Professor (Promoted form Assistant to Full Professor in Aug 2016) — *Aug 2011-current*

Previous Employment

- **CWI (Centrum Wiskunde & Informatica)** — Amsterdam, Netherlands
  Scientific staff member in the Crypto Group (Head Ronald Cramer) — *Jan 2007-Jul 2011*
- **École Normale Supérieure** — Paris, France
  Postdoc in the Crypto Group (Head David Pointcheval) — *Jan-Dec 2006*

Selected Distinctions

- **ERC Starting Grant (1.12mio €)**
  Provable Security for Physical Cryptography (PSPC) — *2010-2015*
- **ERC Consolidator Grant (1.8mio €)**
  Teaching Old Crypto New Tricks (TOCNeT) — *2016-2021*
- **Best Paper Awards at**
  Eurocrypt 2011, 2017 and 2018

Education

- **ETH** — Zürich, Switzerland
  PhD in Cryptography — *2001 - 2005*
  - Adviser: Prof. Ueli Maurer.

– Title: Indistinguishability and Composition of Random Systems.

- **ETH** Zürich, Switzerland
  Dipl.Inf.Ing.ETH (Master Degree in Computer Science) *1996 - 2001*
  – Minor subject: Quantum Physics.
  – Diploma thesis done at McGill (see below.)

- **McGill University** Montréal, Canada
  Diploma Thesis *autumn 2001*
  – Advisers: Prof. Michael Hallett (McGill) and Prof. Gaston Gonnet (ETH).
  – Title: *On the Parameterized Complexity of the fixed Alphabet Shortest Common Supersequence and Longest Common Subsequence Problems.* Appeared as [J. Comput. Syst. Sci. 67 (4) (2003), pp. 757-771].

- **NTNU** Trondheim, Norway
  Erasmus Exchange Semester *winter 2000*

Teaching

Teaching

- **IST Austria** Austria

autumn 18 & 19	(at TU Vienna) Introduction to modern cryptography
autumn 16 & 17	CS core course
autumn 12,13 & 14	Algorithms I (core module)
spring 13	Algorithms II (core module)
spring 12,13 & 14	Complexity Theory (core module)
spring 13	Cryptography (block-course)

- **University of Amsterdam** Netherlands

spring 11	Complexity Theory (mastermath course)

Teaching Assistance

- **ETH Zürich** Switzerland

summer 03 & 04	Kryptographische Protokolle (lecturer Prof. Ueli Maurer)
winter 02 & 03	Informationssicherheit und Kryptographie (Prof. Ueli Maurer)
winter 01	Informatik 2 (Prof. Emo Welzl)
summer 99	Information und Kommunikation (Prof. Ueli Maurer)

Supervision

- **Current and former PhD Students**
  at IST Austria
  – Christoph Günther (since 2022, to graduate in 2026)
  – Miguel Cueto Noval (since 2021, to graduate in 2026)
  – Mirza Ahad Baig (since 2020, to graduate in 2026)
  – Charlotte Hoffmann (2021-2025 “Theory and Applications of Verifiable Delay Functions”, now postdoc)

- Guillermo Pascual Perez (2019-2024 "On the Efficiency and Security of Secure Group Messaging")
- Michelle Yeo (2019-2023 "Advances in Efficiency and Privacy in Payment Channel Network Analysis")
- Karen Azari (former Klein) (2016-2021 "On the Adaptive Security of Graph-based Games")
- Chethan Kamath (2015-2019 "On the Average-Case Hardness of Total Search Problems")
- Hamza Abusalah (2014-2017 "Proof systems for sustainable decentralized cryptocurrencies")
- Michal Rybar (2013-2017 "The exact security of message authentication codes")

- **Current and former Postdocs**
at IST Austria
  - Ray Neiheiser (since 9.2022)
  - Akin Ünal (since 4.2024)

  - Anshu Yavad (9.2023-1.2026)
  - Avarikioti Georgia (5.2021 to 3.2022, IST fellow, co-supervised with Tim Roughgarden)
  - Suvradip Chakraborty (1.2020 to 12.2021)
  - Benedikt Auerbach (12.2019 to 9.2024)
  - Michael Walter (1.2018-6.2021)
  - Maciej Skorski (2016-2017)
  - Joel Alwen (2014-2018)
  - Georg Fuchsbauer (2013-2016)
  - Peter Gazi (2013-2017)
  - Stephan Krenn (2012-2013)

- **Interns and Summer Students**
at IST Austria and CWI Amsterdam
  - Linus Klockner (TU Wien, Intern, 3.2026-5.2026)
  - Mahdi Ali Hamad (Harvard, Intern, 10.2025-4.2026)
  - Emiel Wiedijk (University of Amsterdam, 1.2024-5.2024)
  - Pengxiang Wang (University of Michigan, 5.2023-11.2023)
  - Matthias Pleschiner (Uni Salzburg, Intern, 7.2023)
  - Konrad Klier (TU Wien, Intern, 4.2023-5.2023)
  - Mahsa Bastankhah (Sharif, ISTernship followed by internship 9.2021-1.2022)
  - Ahmadreza Rahimi (University of Virginia, visiting PhD student, 2019)
  - Margarite Capretto (University of Rosaria/Argentina, ISTern, Summer 2019)
  - Miguel Cueto (University of Oviedo/Spain, ISTern, Summer 2019)
  - Arka Rai Choudhuri (John Hopkins, graduate summer student, 2018)
  - Samarth Tiwari (NYU, ISTernship, Summer 2018)
  - Sasha Lapiga (Taras Shevchenko National University of Kyiv, ISTernship, Summer 2018)
  - Anastasia Kucherenko (Taras Shevchenko National University of Kyiv, ISTernship, Summer 2017)
  - Mukesh Pareek (IIT Bombay, ISTernship, 2017)
  - Hana Dlouha (CTU in Prague, ISTernship, 2017)
  - Theresa Steiner (TU Wien, student intern, 2016)
  - Danylo Khilko (Taras Shevchenko National University of Kyiv, ISTernship, 2016)
  - Zahra Jafargholi (UCLA, graduate summer student, 2014)
  - Maciej Skorski (U of Warsaw, graduate summer student, 2012/13/14/15)
  - Sophie Stevens (Bristol, ISTernship, 2014)
  - Kristian Tokmakov (Oxford, ISTernship, 2014)
  - Alexander Golovnev (NYU, graduate summer student, 2014)
  - Momchil Konstantinov (Oxford, ISTernship, 2013)
  - Vanishree Rao (UCLA, graduate summer student, 2013)
  - Akshay Wadia (UCLA, graduate summer student, 2012)

– Aris Tentes (NYU, graduate summer student, 2011)

Professional Activities

- **Program co-Chair:** TCC (IACR Theory of Cryptography Conference) 2020
  Program Committees:
  Theory of Cryptography Conference (TCC) 2011, 2013, 2014, 2016, 2017, 2018, 2020 & 2024
  EUROCRYPT 2009, 2012, 2017, 2019
  CRYPTO 2009, 2014, 2026
  Financial Cryptography (FC) 2025 & 2026
  Advances in Financial Technologies (AFT) 2024, 2025 & 2026 Conference on Security and Cryptography for Networks (SCN) 2010
  MFCS 2011
  PKC 2012 & 2025
  CHES 2012
  STOC 2018

- **General chair:** Eurocrypt 2016, Vienna. `https://www.iacr.org/conferences/eurocrypt2016/`
  General chair: International Conference on Information Theoretic Security - ICITS. May 21-24 2011, Amsterdam, Netherlands. `http://event.cwi.nl/icits2011/`

- **Organizer:** Summer school on *Symmetric Proof Techniques*, July 29 to August 3, 2018, Bertinoro, Italy. `https://spotniq.school/`
  Organizer: Austrian Computer Science Day 2013. May 3, IST Austria.
  `http://ist.ac.at/austrian-computer-science-day-2013/home/`
  Organizer: Workshop *Provable Security against Physical Attacks.* Lorentz Center, Feb. 15-19 2010, Leiden, Netherlands. `http://www.lorentzcenter.nl/lc/web/2010/383/extra.php3?wsid=383`

- **Scientific advisor:** Chia network `chia.net`

- **Steering Committee:** TCC (Theory of Cryptography Conference), since 2022
  `https://www.iacr.org/workshops/tcc/sc.html`
  Steering Committee: Austrian Computer Science Day.

- **Board:** Informatik Austria `www.informatikaustria.at`

Talks/Tutorials, Talks/Panels for general public etc. (since 2007)

Selected Talks/Panels for General Public

Oct. 2018	Panel at Europa Forum Wachau, Klosterneuburg, Austria. `http://www.noel.gv.at/noe/Europa_Forum_Wachau__Erfolgreicher_Start_der_Salonreihe.html`
Sep. 2018	Netzpolitischer Abend, Metalab, Vienna: *Nachhaltige Blockchains*
Sep. 2018	Internet Summit Austria 2018: *Nachhaltige Blockchains* `computerwelt.at/news/blockchain-jenseits-von-bitcoin-co`

Tutorials/Lectures at Schools

Nov. 2025 TU Wien, Public Lecture Series: Sustainability in Computer Science 2025, *Blockchains and Sustainability*.

Nov. 2024 TU Wien, Public Lecture Series: Sustainability in Computer Science 2024, *Sustainable Blockchains.*

Nov. 2023 TU Wien, Public Lecture Series: Sustainability in Computer Science 2023, *Sustainable Blockchains.*

Apr. 2022 IACR-CROSSING School on Combinatorial Techniques in Cryptography, Malta: *Pebbling techniques in Cryptography.*

Jul. 2018 Summer school on Symmetric Proof Techniques, Bertinoro, Italy: *Lower & Upper Bounds on inverting functions.*

Jul. 2018 CryptoBG International Summer School, Oriahovitza, Bulgaria: *Beyond Proofs of Work: New Proof Systems for Sustainable Blockchains.*

Nov. 2016 COST-IACR School on Randomness in Cryptography, Barcelona: *Lectures on Pseudoentropy.*

Oct. 2012 ECRYPT II Summer School on Lattices, Porto: *Secret-Key Cryptography from LPN.*

Aug. 2009 Crypto in the clouds Workshop, MIT Boston: *Survey on Different Leakage Models.*

Dec. 2007 Short Course in Cryptology Mathematical Institute Leiden: *Basic Concepts*.

Dec. 2007 Indocrypt 2007, Post-Conference Tutorial, Chennai - India: *Robust Combiners*.

Invited Talks/Talks at Invitation only Workshops

Aug. 2025 Berkeley, The Science of Blockchain Conference 2025 (SBC'25): *Permissionless Blockchains from Physical Resources*.

Jul. 2025 Berkley, Simons Institute: *Efficiently Testable Circuits.*

Sep. 2020 VISP Workshop on Security and Privacy in Contact Tracing: *Relay, replay and inverse-sybil attacks in automated contact tracing*.

Dec. 2019 Asiacrypt 2019 Invited lecture: *New proof systems for sustainable blockchains: proofs of space and verifiable delay functions*.

Oct. 2018 FOCS 2018 Workshop (Theory of Blockchains and Cryptocurrency): *Proofs of Sequential Work and Verifiable Delay Functions*.

Aug. 2018 Stanford, Ethereum Foundation workshop on Verifiable Delay Functions: *Cryptographic Speed-bumps: Time-Lock Puzzles, PoSW and VDFs*.

Jan. 2017 Oberwolfach Workshop: *Beyond Hellman's Time-Memory Trade-Offs*.

Jul. 2015 Simons Institute, Berkeley: *Nested Hybrids*.

Apr. 2015 Workshop in Cryptography at Bochum University: *Adaptive Security via the Nested Hybrids Technique.*

Sep. 2014 10-year anniversary of the RISC crypto meetings, Amsterdam: *Nested hybrid arguments with applications to selective decryption and constrained PRFs.*

May. 2014 CECC14, Central European Conference on Cryptology, Budapest *Cryptographic Applications of (Computational) Min-Entropy.*

Dec. 2013 Visions of Cryptography: a two-day workshop on theory of cryptography, Weizmann institute: *Nested Hybrids.*

Oct. 2012 ECRYPT II Summer School on Lattices: *Secret-Key Cryptography from LPN.*

Nov. 2012 Workshop on Physical Attacks: *Challenges in Leakage-Resilient Symmetric Cryptography.*

Aug. 2012 ICITS 2012: *How to Fake Auxiliary Input.*

Jun. 2012 Austrian Computer Science Day 2012: *Leakage-Resilient Cryptography.*

Apr. 2012 Workshop in honour of Alan Turings 100th Birthday on "Formal and Computational Cryptographic Proofs", Newton Institute, Cambridge: *How to Fake Auxiliary Input*

Jan. 2012 SOFSEM 2012: *Efficient Cryptography from Hard Learning Problems.*

Sep. 2011 Dagstuhl Seminar "Public-Key Cryptography": *Commitments and Efficient ZeroKnowledge from Hard Learning Problems.*

Jul. 2011 International Math Olympiad (IMO) 2011, Amsterdam (Visit of Participants at CWI): *When Life Gives you Hard Problems, Make Crypto!*

Feb. 2011 Mathematics of Information-Theoretic Cryptography, Institute for Pure & Applied Mathematics (IPAM), UCLA: *Subspace LWE and Applications.*

Jan. 2011 Trends in Theoretical Cryptography, Tsinghua University, Beijing, China: *Efficent MACs from (subspace) LPN.*

Aug. 2010 Cloud Cryptography Workshop, Microsoft Research, Redmond: *Subspace LWE.*

Aug. 2009 Crypto in the clouds Workshop, MIT Boston: *On leakage-resilient pseudorandom functions.*

Aug. 2009 Western European Workshop on Research in Cryptology, Graz, Austria: *Provable security for physical cryptography.*

Mai. 2009 Workshop on Cryptographic Protocols and Public-Key Cryptography, Bertinoro, Italy: *Leakage-Resilient Public-Key Cryptography.*

Dec. 2008 Dagstuhl Seminar "Theoretical Foundations of Practical Information Security": *Theoretical Foundations of Side-Channel Security.*

Sep. 2008 University Wrocław: *Leakage-Resilient Cryptography, Schemes Secure against all Side-Channel Attacks.*

Jun. 2008 Lorentz Center (Leiden) Workshop "Hash functions in cryptology: theory and practice" : *Uninstantiability of Full-Domain Hash.*

Sep. 2007 Dagstuhl Seminar "Cryptography": *Black-Box Combiners for Collision Resistance Really don't Exist.*

Conference Talks

Apr. 2018 EUROCRYPT 2017, Tel-Aviv, *Simple Proofs of Sequential Work.*
Mar. 2015 TCC 2015, Warsaw, Poland: *Key-Homomorphic Constrained Pseudorandom Functions.*
Aug. 2013 CRYPTO 2013, Santa Barbara: *Digital Signatures with Minimal Overhead from Indifferentiable Random Invertible Functions.*
Apr. 2012 EUROCRYPT 2012, Cambridge, England: *Message Authentication, Revisited.*
Mar. 2012 TCC 2012, Taormina, Italy: *Subspace LWE.*
May 2011 EUROCRYPT 2011, Tallinn, Estonia: *Efficient Authentication from Hard Learning Problems (Best Paper Talk).*
Dec. 2010 ASIACRYPT 2010, Singapore: *Leakage-Resilient ElGamal Encryption*.
Aug. 2010 CRYPTO 2010, Santa-Barbara - USA/CA: *Leakage-Resilient Pseudorandom Functions and Side-Channel Attacks on Feistel Networks*.
Apr. 2009 EUROCRYPT 2009, Köln - Germany: *A leakage-resilient mode of operation*.
Aug. 2008 CRYPTO 2008, Santa-Barbara - USA/CA: *Compression from collisions, or why CRHF combiners have a long output*.
Jul. 2008 35th International Colloquium on Automata, Languages and Programming, ICALP 2008, Reykjavik - Iceland: *Weak Pseudorandom Functions in Minicrypt*.
Apr. 2008 EUROCRYPT 2008, Istanbul - Turkey: *A New Mode of Operation for Block Ciphers and Length-Preserving MACs*.
May 2007 EUROCRYPT 2007, Barcelona - Spain: *Range Extension for Weak PRFs; The Good, the Bad and the Ugly*.
May 2007 EUROCRYPT 2007, Barcelona - Spain: *Non-Trivial Black-Box Combiners for Collision-Resistant Hash-Functions Don't Exist*.
Mar. 2007 FSE 2007, Luxembourg City - Luxembourg: *Improving the Security of MACs via Randomized Message Preprocessing*.
Feb. 2007 TCC 2007, Amsterdam, Netherlands: *Parallel Repetition of Computationally Sound Protocols Revisited*.

Publications

See `https://dblp.org/pers/hd/p/Pietrzak:Krzysztof` for an automatically updated list.

Preprints

1. Christoph U. Günther, and Krzysztof Pietrzak; *Preventing Sybil Attacks in Peer-to-Peer Networks using Proofs of Space.* **under submission** *https://eprint.iacr.org/2025/804*

2. Zeta Avarikioti, Ray Neiheiser, Krzysztof Pietrzak, Michelle X. Yeo; *Wonderboom – Efficient, and Censorship-Resilient Signature Aggregation for Million Scale Consensus.* **under submission** *https://arxiv.org/abs/2602.06655*

3. Stefan Dziembowski and Sebastian Faust and Paweł Kedzior and Marcin Mielniczuk and Susil Kumar Mohanty and Krzysztof Pietrzak; *Beholder Signatures.* **under submission** *https://eprint.iacr.org/2025/1900*

4. Charlotte Hoffmann and Krzysztof Pietrzak; *Blind Verifiable Delay Functions.* **under submission**

5. Charlotte Hoffmann and Krzysztof Pietrzak; *SPoCK: Sequential Proofs of Complete Knowledge.* **under submission**

2025

6. Benedikt Auerbach, Miguel Cueto Noval, Boran Erol, and Krzysztof Pietrzak. *Continuous group-key agreement: Concurrent updates without pruning.* **CRYPTO** *2025*

7. Mirza Ahad Baig, Christoph U. Günther, and Krzysztof Pietrzak. *Nakamoto consensus from multiple resources.* **ATF** *2025*

8. Jesko Dujmovic, Christoph U. Günther, and Krzysztof Pietrzak; *Space-deniable proofs.* **TCC** *2025*

9. Charlotte Hoffmann and Krzysztof Pietrzak; *Watermarkable and zero-knowledge verifiable delay functions from any proof of exponentiation.* **PKC** *2025*

10. Krzysztof Pietrzak and Pengxiang Wang; *Time-space tradeoffs of truncation with preprocessing.* **ITC** *2025*

2024

11. Michael Anastos, Benedikt Auerbach, Mirza Ahad Baig, Miguel Cueto Noval, Matthew Kwan, Guillermo Pascual-Perez, and Krzysztof Pietrzak; *The cost of maintaining keys in dynamic groups with applications to multicast encryption and group messaging.* **TCC** *2024*

12. Benedikt Auerbach, Christoph U. Günther, and Krzysztof Pietrzak. *Trapdoor memory-hard functions.* **EUROCRYPT** *2024*

13. Zeta Avarikioti, Mahsa Bastankhah, Mohammad Ali Maddah-Ali, Krzysztof Pietrzak, Jakub Svoboda, and Michelle Yeo; *Route discovery in private payment channel networks.* **ESORCS** *2024*

14. Krishnendu Chatterjee, Amirali Ebrahim-Zadeh, Mehrdad Karrabi, Krzysztof Pietrzak, Michelle Yeo, and Dorde Zikelic; *Fully automated selfish mining analysis in efficient proof systems blockchains.* **PODC** *2024*

15. Christoph U. Günther and Krzysztof Pietrzak; *Deniability in automated contact tracing: Impossibilities and possibilities.* **Proc. Priv. Enhancing Technol.** *2024*

2023

16. Benedikt Auerbach, Miguel Cueto Noval, Guillermo Pascual-Perez, and Krzysztof Pietrzak; *On the cost of post-compromise security in concurrent continuous group-key agreement.* **TCC** *2023*

17. Mirza Ahad Baig, Suvradip Chakraborty, Stefan Dziembowski, Malgorzata Galazka, Tomasz Lizurej, and Krzysztof Pietrzak; *Efficiently testable circuits.* **ITCS** *2023*

18. Mirza Ahad Baig, Suvradip Chakraborty, Stefan Dziembowski, Malgorzata Galazka, Tomasz Lizurej, and Krzysztof Pietrzak; *Efficiently testable circuits without conductivity.* **TCC** *2023*

19. Yevgeniy Dodis, Niels Ferguson, Eli Goldin, Peter Hall, and Krzysztof Pietrzak; *Random oracle combiners: Breaking the concatenation barrier for collision-resistance.* **CRYPTO** *2023*

20. Charlotte Hoffmann, Pavel Hubácek, Chethan Kamath, and Krzysztof Pietrzak; *Certifying giant nonprimes.* **PKC** *2023*

2022

21. Samarth Tiwari, Michelle Yeo, Zeta Avarikioti, Iosif Salem, Krzysztof Pietrzak, Stefan Schmid: *Wiser: Increasing throughput in payment channel networks with transaction aggregation.* **AFT** *2022*

22. Charlotte Hoffmann, Pavel Hubáček, Chethan Kamath, Karen Klein, Krzysztof Pietrzak: *Practical Statistically-Sound Proofs of Exponentiation* **CRYPTO** *2022*

23. Joël Alwen, Benedikt Auerbach, Miguel Cueto, Karen Klein, Guillermo Pascual-Perez, Krzysztof Pietrzak, Michael Walter: *CoCoA: Concurrent Continuous Group Key Agreement.* **EUROCRYPT** *2022*

24. Zeta Avarikioti, Krzysztof Pietrzak, Iosif Salem, Stefan Schmid, Samarth Tiwari, Michelle Yeo: *Hide & Seek: Privacy-Preserving Rebalancing on Payment Channel Networks.* **Financial Cryptography** *2022*

2021

25. Joel Alwen, Margarita Capretto, Miguel Cueto, Chethan Kamath, Karen Klein, Guillermo Pascual-Perez, Krzysztof Pietrzak, Michael Walter: *Keep the Dirt: Tainted TreeKEM, an Efficient and Provably Secure Continuous Group Key Agreement Protocol.* **IEEE S&P** *2021*

26. Benedikt Auerbach, Karen Klein, Krzysztof Pietrzak, Michael Walter, Suvradip Chakraborty, Guillermo Pascual Perez, Michelle Yeo: *Inverse-Sybil Attacks in Automated Contact Tracing.* **CT-RSA** *2021*

27. Joël Alwen, Benedikt Auerbach, Mirza Ahad Baig, Miguel Cueto Noval, Karen Klein, Guillermo Pascual-Perez, Krzysztof Pietrzak, and Michael Walter. *Grafting key trees: Efficient key management for overlapping groups.* **TCC** *2021*

28. Suvradip Chakraborty, Stefan Dziembowski, Malgorzata Galazka, Tomasz Lizurej, Krzysztof Pietrzak, and Michelle Yeo. *Trojan-resilience without cryptography.* **TCC** *2021*

29. Chethan Kamath, Karen Klein, and Krzysztof Pietrzak. *On treewidth, separators and yao's garbling.* **TCC** *2021*

30. Chethan Kamath, Karen Klein, Krzysztof Pietrzak, and Michael Walter. *The cost of adaptivity in security games on graphs.* **TCC** *2021*

31. Chethan Kamath, Karen Klein, Krzysztof Pietrzak, and Daniel Wichs. *Limits on the adaptive security of yao's garbling.* **CRYPTO** *2021*

32. Krzysztof Pietrzak, Iosif Salem, Stefan Schmid, and Michelle Yeo. Lightpir: Privacy-preserving route discovery for payment channel networks. **IFIP Networking** 2021

2020

33. Krzysztof Pietrzak: *Delayed Authentication: Preventing Replay and Relay Attacks in Private Contact Tracing.* **INDOCRYPT** *2020*

2019

34. Hamza Abusalah, Chethan Kamath, Karen Klein, Krzysztof Pietrzak, Michael Walter: *Reversible Proofs of Sequential Work.* **EUROCRYPT** *2019*

35. Georg Fuchsbauer, Chethan Kamath, Karen Klein, Krzysztof Pietrzak: *Adaptively Secure Proxy Re-encryption.* **PKC** *2019*

36. Arka Rai Choudhuri, Pavel Hubacek, Chethan Kamath, Krzysztof Pietrzak, Alon Rosen, Guy N. Rothblum: *Finding a Nash equilibrium is no easier than breaking Fiat-Shamir.* **STOC** *2019*

37. Krzysztof Pietrzak: Simple Verifiable Delay Functions. *Innovations in Theoretical Computer Science (***ITCS***) 2019*

38. Krzysztof Pietrzak: Proofs of Catalytic Space. *Innovations in Theoretical Computer Science (***ITCS***) 2019*

2018

39. Stefan Dziembowski and Krzysztof Pietrzak and Daniel Wichs: Non-Malleable Codes. In **Journal of the ACM**, 5(4): 20:1-20:32, 2018 (journal version of conference paper [86]).

40. Joël Alwen, Peter Gazi, Chethan Kamath, Karen Klein, Georg Osang, Krzysztof Pietrzak, Leonid Reyzin, Michal Rolinek and Michal Rybár: On the Memory-Hardness of Data-Independent Password-Hashing Functions. In **AsiaCCS** *2018*

41. oël Alwen, Jeremiah Blocki and Krzysztof Pietrzak: Sustained Space Complexity. In **EUROCRYPT** *2017*

42. Bram Cohen and Krzysztof Pietrzak: Simple Proofs of Sequential Work. In **EUROCRYPT** *2018* **(best paper award)**

2017

43. Hamza Abusalah, Joël Alwen, Bram Cohen, Danylo Khilko, Krzysztof Pietrzak, Leonid Reyzin: Beyond Hellman's Time-Memory Trade-Offs with Applications to Proofs of Space In **ASIACRYPT** *2017*

44. Joshua Brody, Stefan Dziembowski, Sebastian Faust and Krzysztof Pietrzak: Position-Based Cryptography and Multiparty Communication Complexity In **TCC** *2017*

45. Eike Kiltz, Krzysztof Pietrzak, Daniele Venturi, David Cash and Abhishek Jain: Efficient Authentication from Hard Learning Problems **J. Cryptology**, 30(4): 1238-1275, 2017. (invited journal version of conference paper [80]).

46. Zahra Jafargholi, Chethan Kamath, Karen Klein, Ilan Komargodski, Krzysztof Pietrzak and Daniel Wichs: Be Adaptive, Avoid Overcommitting In **CRYPTO** *2017*

47. Joël Alwen, Jeremiah Blocki, Krzysztof Pietrzak: Depth-Robust Graphs and Their Cumulative Memory Complexity. In **EUROCRYPT** *2017*

48. Joël Alwen, Binyi Chen, Krzysztof Pietrzak, Leonid Reyzin, and Stefano Tessaro Scrypt Is Maximally Memory-Hard. In **EUROCRYPT** *2017* **(best paper award)**

49. Krzysztof Pietrzak, and Maciej Skorski. Non-Uniform Attacks Against Pseudoentropy. In **ICALP** *2017*

2016

50. Stephan Krenn, Krzysztof Pietrzak, Akshay Wadia, and Daniel Wichs. A counterexample to the chain rule for conditional HILL entropy. In **Computational Complexity** 25(3): 567-605 (2016)

51. Peter Gaži, Krzysztof Pietrzak, and Michal Rybár. The Exact Security of PMAC. In **IACR Trans. Symmetric Cryptol.** 2016(2): 145-161 (2016)

52. Hamza Abusalah, Georg Fuchsbauer, and Krzysztof Pietrzak. Offline witness encryption. In **ACNS** *2016*

53. Joël Alwen, Binyi Chen, Chethan Kamath, Vladimir Kolmogorov, Krzysztof Pietrzak, and Stefano Tessaro. On the complexity of Scrypt and proofs of space in the parallel random oracle model. In **EUROCRYPT** *2016*

54. Krzysztof Pietrzak, and Maciej Skorski. Pseudoentropy: Lower-Bounds for Chain Rules and Transformations. In **TCC** *2016*

55. Georg Fuchsbauer, Felix Heuer, Eike Kiltz, and Krzysztof Pietrzak. Standard security does imply security against selective opening for markov distributions. In **TCC** *2016*

56. Hamza Abusalah, Georg Fuchsbauer, and Krzysztof Pietrzak. Constrained PRFs for unbounded inputs. In **CT-RSA** *2016*

2015

57. Abhishek Banerjee, Georg Fuchsbauer, Chris Peikert, Krzysztof Pietrzak, and Sophie Stevens. Key-homomorphic constrained pseudorandom functions. In **TCC** *2015*

58. Fabrice Benhamouda, Stephan Krenn, Vadim Lyubashevsky, and Krzysztof Pietrzak. Efficient zero-knowledge proofs for commitments from learning with errors over rings. In **ESORICS** *2015*

59. Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak. Proofs of space. In **CRYPTO** *2015*

60. Georg Fuchsbauer, Zahra Jafargholi, and Krzysztof Pietrzak. A quasipolynomial reduction for generalized selective decryption on trees. In **CRYPTO** *2015*

61. Peter Gaži, Krzysztof Pietrzak, and Stefano Tessaro. The exact PRF security of truncation: Tight bounds for keyed sponges and truncated CBC. In **CRYPTO** *2015*

62. Peter Gaži, Krzysztof Pietrzak, and Stefano Tessaro. Generic security of NMAC and HMAC with input whitening. In **ASIACRYPT** *2015*

63. Tatsuaki Okamoto, Krzysztof Pietrzak, Brent Waters, and Daniel Wichs. New realizations of somewhere statistically binding hashing and positional accumulators. In **ASIACRYPT** *2015*

64. Krzysztof Pietrzak and Maciej Skorski. The chain rule for HILL pseudoentropy, revisited. In **LATINCRYPT** *2015*

65. Maciej Skorski, Alexander Golovnev, and Krzysztof Pietrzak. Condensed unpredictability. In **ICALP** *2015*

2014

66. Marc Fischlin, Anja Lehmann, and Krzysztof Pietrzak. Robust multi-property combiners for hash functions. *J. Cryptology*, 27(3):397–428, 2014. (conference version [92]).

67. Georg Fuchsbauer, Momchil Konstantinov, Krzysztof Pietrzak, and Vanishree Rao. Adaptive security of constrained PRFs. In **ASIACRYPT** *2014*

68. Peter Gaži and Krzysztof Pietrzak and Michal Rybár. The Exact PRF-Security of NMAC and HMAC. In **CRYPTO** *2014*

69. Yevgeniy Dodis and Krzysztof Pietrzak and Daniel Wichs. Key Derivation without Entropy Waste. In **EUROCRYPT** *2014*

70. Eike Kiltz and Daniel Masny and Krzysztof Pietrzak. Simple Chosen-Ciphertext Security from Low-Noise LPN. In **PKC** *2014*

71. Dimitar Jetchev and Krzysztof Pietrzak. How to Fake Auxiliary Input. In **TCC** *2014*

2013

72. Joël Alwen and Stephan Krenn and Krzysztof Pietrzak and Daniel Wichs. Learning with Rounding, Revisited - New Reduction, Properties and Applications. In **CRYPTO** *2013*

73. Eike Kiltz and Krzysztof Pietrzak and Mario Szegedy. Digital Signatures with Minimal Overhead from Indifferentiable Random Invertible Functions. In **CRYPTO** *2013*

74. Stephan Krenn and Krzysztof Pietrzak and Akshay Wadia. A Counterexample to the Chain Rule for Conditional HILL Entropy, and what Deniable Encryption has to do with it. In **TCC** *2013*

2012

75. Krzysztof Pietrzak and Douglas Wikström. Parallel repetition of computationally sound protocols revisited. *J. Cryptology*, 25(1):116–135, 2012. (conference version [100]).

76. Abhishek Jain and Stephan Krenn and Krzysztof Pietrzak and Aris Tentes. Commitments and Efficient Zero-Knowledge Proofs from Learning Parity with Noise. In **ASIACRYPT** *2012*

77. Sebastian Faust and Krzysztof Pietrzak and Joachim Schipper. Practical Leakage-Resilient Symmetric Cryptography. In **CHES** *2012*

78. Yevgeniy Dodis and Eike Kiltz and Krzysztof Pietrzak and Daniel Wichs. Message Authentication, Revisited. In **EUROCRYPT** *2012*

79. Stefan Heyse and Eike Kiltz and Vadim Lyubashevsky and Christof Paar and Krzysztof Pietrzak. Lapin: An Efficient Authentication Protocol Based on Ring-LPN. In **FSE** *2012*

80. Abhishek Jain and Krzysztof Pietrzak and Aris Tentes. Hardness Preserving Constructions of Pseudorandom Functions. In **TCC** *2012*

81. Krzysztof Pietrzak and Alon Rosen and Gil Segev. Lossy Functions Do Not Amplify Well. In **TCC** *2012*

82. Krzysztof Pietrzak. Subspace LWE. In **TCC** *2012*

2011

78. Boaz Barak and Yevgeniy Dodis and Hugo Krawczyk and Olivier Pereira and Krzysztof Pietrzak and Francois-Xavier Standaert and Yu Yu. Leftover Hash Lemma, Revisited. In **CRYPTO** *2011*

79. Sebastian Faust and Krzysztof Pietrzak and Daniele Venturi. Tamper-Proof Circuits: How to Trade Leakage for Tamper-Resilience? In **ICALP** *2011*

80. Eike Kiltz and Krzysztof Pietrzak and David Cash and Abhishek Jain and Daniele Venturi. Efficient Authentication from Hard Learning Problems. In **EUROCRYPT** *2011* **(best paper award)**

81. Abhishek Jain and Krzysztof Pietrzak. Parallel Repetition for Leakage Resilience Amplification Revisited. In **TCC** *2011*

2010

82. Yevgeniy Dodis and Krzysztof Pietrzak Leakage-Resilient Pseudorandom Functions and Side-Channel Attacks on Feistel Networks. In **CRYPTO** *2010*

83. Johan Håstad and Rafael Pass and Krzysztof Pietrzak Douglas Wikström. An efficient parallel repetition theorem. In **TCC** *2010*

84. Eike Kiltz and Krzysztof Pietrzak Leakage-Resilient ElGamal Encryption. In **ASIACRYPT** *2010*

85. Sebastian Faust and Eike Kiltz and Krzysztof Pietrzak and Guy Rothblum. Leakage-Resilient Signatures. In **TCC** *2010*

86. Stefan Dziembowski and Krzysztof Pietrzak and Daniel Wichs. Non-Malleable Codes and Algorithmic Tamper Proof Security. In **ICS** *2010: 1st Innovations in Computer Science*, 2010.

2009

87. Eike Kiltz and Krzysztof Pietrzak. On the security of padding-based encryption schemes - or - why we cannot prove OAEP secure in the standard model. In Antoine Joux, editor, **EUROCRYPT** *2009*, LNCS, pages 389–406, Cologne, Germany, April 26–30, 2009. Springer-Verlag, Berlin, Germany.

88. Eike Kiltz, Krzysztof Pietrzak, Martijn Stam, and Moti Yung. A new randomness extraction paradigm for hybrid encryption. In Antoine Joux, editor, **EUROCRYPT** *2009*, LNCS, pages 590–609, Cologne, Germany, April 26–30, 2009. Springer-Verlag, Berlin, Germany.

89. Krzysztof Pietrzak. A leakage-resilient mode of operation. In Antoine Joux, editor, **EUROCRYPT** *2009*, LNCS, pages 462–482, Cologne, Germany, April 26–30, 2009. Springer-Verlag, Berlin, Germany.

2008

90. Stefan Dziembowski and Krzysztof Pietrzak. Leakage-resilient cryptography. In *49th* **FOCS**, pages 293–302. IEEE Computer Society Press, 2008.

91. Krzysztof Pietrzak. Compression from collisions, or why CRHF combiners have a long output. In David Wagner, editor, **CRYPTO** *2008*, LNCS, pages 413–432, Santa Barbara, CA, USA, August 17–21, 2008. Springer-Verlag, Berlin, Germany.

92. Marc Fischlin, Anja Lehmann, and Krzysztof Pietrzak. Robust multi-property combiners for hash functions revisited. In **ICALP** *(2)*, pages 655–666, 2008.

93. Krzysztof Pietrzak and Johan Sjödin. Weak pseudorandom functions in minicrypt. In **ICALP** *(2)*, pages 423–436, 2008.

94. Yevgeniy Dodis, Krzysztof Pietrzak, and Prashant Puniya. A new mode of operation for block ciphers and length-preserving MACs. In Nigel P. Smart, editor, **EUROCRYPT** *2008*, LNCS, pages 198–219, Istanbul, Turkey, April 13–17, 2008. Springer-Verlag, Berlin, Germany.

2007

95. Yevgeniy Dodis and Krzysztof Pietrzak. Improving the security of MACs via randomized message preprocessing. In Alex Biryukov, editor, **FSE** *2007*, volume 4593 of *LNCS*, pages 414–433, Luxembourg, Luxembourg, March 26–28, 2007. Springer-Verlag, Berlin, Germany.

96. Stefan Dziembowski and Krzysztof Pietrzak. Intrusion-resilient secret sharing. In *48th* **FOCS**, pages 227–237, Providence, USA, October 20–23, 2007. IEEE Computer Society Press.

97. Ueli M. Maurer, Krzysztof Pietrzak, and Renato Renner. Indistinguishability amplification. In Alfred Menezes, editor, **CRYPTO** *2007*, volume 4622 of *LNCS*, pages 130–149, Santa Barbara, CA, USA, August 19–23, 2007. Springer-Verlag, Berlin, Germany.

98. Krzysztof Pietrzak. Non-trivial black-box combiners for collision-resistant hash-functions don't exist. In Moni Naor, editor, **EUROCRYPT** *2007*, volume 4515 of *LNCS*, pages 23–33, Barcelona, Spain, May 20–24, 2007. Springer-Verlag, Berlin, Germany.

99. Krzysztof Pietrzak and Johan Sjödin. Range extension for weak PRFs; the good, the bad, and the ugly. In Moni Naor, editor, **EUROCRYPT** *2007*, volume 4515 of *LNCS*, pages 517–533, Barcelona, Spain, May 20–24, 2007. Springer-Verlag, Berlin, Germany.

100. Krzysztof Pietrzak and Douglas Wikström. Parallel repetition of computationally sound protocols revisited. In Salil P. Vadhan, editor, **TCC** *2007*, volume 4392 of *LNCS*, pages 86–102, Amsterdam, The Netherlands, February 21–24, 2007. Springer-Verlag, Berlin, Germany.

pre-2007

101. Krzysztof Pietrzak. *Indistinguishability and Composition of Random Systems*. PhD thesis, ETH Zurich, 2006. Reprint as vol. 6 of *ETH Series in Information Security and Cryptography*, ISBN 3-86626-063-7, Hartung-Gorre Verlag, Konstanz, 2006.

102. Mihir Bellare, Krzysztof Pietrzak, and Phillip Rogaway. Improved security analyses for CBC MACs. In Victor Shoup, editor, **CRYPTO** *2005*, volume 3621 of *LNCS*, pages 527–545, Santa Barbara, CA, USA, August 14–18, 2005. Springer-Verlag, Berlin, Germany.

103. Yevgeniy Dodis, Roberto Oliveira, and Krzysztof Pietrzak. On the generic insecurity of the full domain hash. In Victor Shoup, editor, **CRYPTO** *2005*, volume 3621 of *LNCS*, pages 449–466, Santa Barbara, CA, USA, August 14–18, 2005. Springer-Verlag, Berlin, Germany.

104. Yevgeniy Dodis, Krzysztof Pietrzak, and Bartosz Przydatek. Separating sources for encryption and secret sharing. In Shai Halevi and Tal Rabin, editors, **TCC** *2006*, volume 3876 of *LNCS*, pages 601–616, New York, NY, USA, March 4–7, 2006. Springer-Verlag, Berlin, Germany.

105. Ueli M. Maurer, Yvonne Anne Oswald, Krzysztof Pietrzak, and Johan Sjödin. Luby-Rackoff ciphers from weak round functions? In Serge Vaudenay, editor, **EUROCRYPT** *2006*, volume 4004 of *LNCS*, pages 391–408, St. Petersburg, Russia, May 28 – June 1, 2006. Springer-Verlag, Berlin, Germany.

106. Ueli M. Maurer and Krzysztof Pietrzak. The security of many-round Luby-Rackoff pseudo-random permutations. In Eli Biham, editor, **EUROCRYPT** *2003*, volume 2656 of *LNCS*, pages 544–561, Warsaw, Poland, May 4–8, 2003. Springer-Verlag, Berlin, Germany.

107. Krzysztof Pietrzak. Composition does not imply adaptive security. In Victor Shoup, editor, **CRYPTO** *2005*, volume 3621 of *LNCS*, pages 55–65, Santa Barbara, CA, USA, August 14–18, 2005. Springer-Verlag, Berlin, Germany.

108. Krzysztof Pietrzak. Composition implies adaptive security in minicrypt. In Serge Vaudenay, editor, **EUROCRYPT** *2006*, volume 4004 of *LNCS*, pages 328–338, St. Petersburg, Russia, May 28 – June 1, 2006. Springer-Verlag, Berlin, Germany.

109. Krzysztof Pietrzak. A tight bound for EMAC. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, **ICALP** *2006, Part II*, volume 4052 of *LNCS*, pages 168–179, Venice, Italy, July 10–14, 2006. Springer-Verlag, Berlin, Germany.

110. Krzysztof Pietrzak. On the parameterized complexity of the fixed alphabet shortest common supersequence and longest common subsequence problems. *J. Comput. Syst. Sci.*, 67(4):757–771, 2003.