Krzysztof Pietrzak
Professor
IST Austria

last updated **September 29, 2022**

pietrzak@ist.ac.at
http://pub.ist.ac.at/crypto/

Personal Details

Full Name:	Krzysztof 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 (IST) Austria** — Vienna, Austria
  Professor (Assistant Professor before 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)
  - Charlotte Hoffmann (since 2021)
  - Miguel Cueto (since 2021)
  - Mirza Ahad Baig (since 2020)
  - Guillermo Pascual Perez (since 2019)
  - Michelle Yeo (since 2019)

- Karen Klein (since 2016, thesis defended 2021 "On the Adaptive Security of Graph-based Games")
- Chethan Kamath (since 2015, thesis defended 2019 "On the Average-Case Hardness of Total Search Problems")
- Hamza Abusalah (affiliated 2014, thesis defended 2017 "Proof systems for sustainable decentralized cryptocurrencies")
- Michal Rybar (affiliated 2013, thesis defended 2017 "The exact security of message authentication codes")

- **Current and former Postdocs**
  at IST Austria
  - Avarikioti Georgia (starts May 2021, IST fellow, co-supervised with Tim Roughgarden)
  - Suvradip Chakraborty (since 2020)
  - Benedikt Auerback (since 2019)
  - Michael Walter (since 2017)

  - 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
  - Mahsa Bastankhah (Sharif, ISTernship followed by internship 2021-2022)
  - 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: ICALP'07, CRYPTO'09 & 14, EUROCRYPT'09 & 12,17,19 SCN'10, TCC'11 & 13,14,16, 17, 18 MFCS'11, PKC'12, CHES'12, STOC'18

- **General chair:** Eurocrypt 2016, Vienna. http://ist.ac.at/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. **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

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

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.

2022

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

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

3. 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

4. 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*

5. 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*
6. 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*
7. Suvradip Chakraborty, Stefan Dziembowski, Malgorzata Galazka, Tomasz Lizurej, Krzysztof Pietrzak, and Michelle Yeo. *Trojan-resilience without cryptography.* **TCC** *2021*
8. Chethan Kamath, Karen Klein, and Krzysztof Pietrzak. *On treewidth, separators and yao's garbling.* **TCC** *2021*
9. Chethan Kamath, Karen Klein, Krzysztof Pietrzak, and Michael Walter. *The cost of adaptivity in security games on graphs.* **TCC** *2021*
10. Chethan Kamath, Karen Klein, Krzysztof Pietrzak, and Daniel Wichs. *Limits on the adaptive security of yao's garbling.* **CRYPTO** *2021*
11. Krzysztof Pietrzak, Iosif Salem, Stefan Schmid, and Michelle Yeo. Lightpir: Privacy-preserving route discovery for payment channel networks. **IFIP Networking** 2021

2020

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

2019

13. Hamza Abusalah, Chethan Kamath, Karen Klein, Krzysztof Pietrzak, Michael Walter: *Reversible Proofs of Sequential Work.* **EUROCRYPT** *2019*
14. Georg Fuchsbauer, Chethan Kamath, Karen Klein, Krzysztof Pietrzak: *Adaptively Secure Proxy Re-encryption.* **PKC** *2019*
15. 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*
16. Krzysztof Pietrzak: Simple Verifiable Delay Functions. *Innovations in Theoretical Computer Science (***ITCS***) 2019*
17. Krzysztof Pietrzak: Proofs of Catalytic Space. *Innovations in Theoretical Computer Science (***ITCS***) 2019*

2018

18. 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 [65]).
19. 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*
20. oël Alwen, Jeremiah Blocki and Krzysztof Pietrzak: Sustained Space Complexity. In **EUROCRYPT** *2017*
21. Bram Cohen and Krzysztof Pietrzak: Simple Proofs of Sequential Work. In **EUROCRYPT** *2018* **(best paper award)**

2017

22. 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*

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

24. 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 [59]).

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

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

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

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

2016

29. 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)

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

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

32. 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*

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

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

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

2015

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

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

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

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

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

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

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

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

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

2014

45. Marc Fischlin, Anja Lehmann, and Krzysztof Pietrzak. Robust multi-property combiners for hash functions. *J. Cryptology*, 27(3):397–428, 2014. (conference version [71]).

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

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

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

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

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

2013

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

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

53. 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

54. Krzysztof Pietrzak and Douglas Wikström. Parallel repetition of computationally sound protocols revisited. *J. Cryptology*, 25(1):116–135, 2012. (conference version [79]).

55. 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*

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

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

58. 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*

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

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

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

2011

57. 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*

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

59. 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)**

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

2010

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

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

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

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

65. 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

66. 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.

67. 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.

68. 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

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

70. 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.

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

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

73. 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

74. 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.

75. 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.

76. 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.

77. 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.

78. 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.

79. 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

80. 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.

81. 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.

82. 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.

83. 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.

84. 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.

85. 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.

86. 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.

87. 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.

88. 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.

89. 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.