

Krzysztof Pietrzak

Assistant Professor
IST Austria

last updated **August 16, 2011**

pietrzak@ist.ac.at

<http://ist.ac.at/en/research/research-groups/pietrzak-group/>

Personal Details

Full Name: Krzysztof Pietrzak
Place and date of birth: Poznan, Poland. August 23, 1977
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
Assistant Professor *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*

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**
Erasmus Exchange Semester

Trondheim, Norway
winter 2000

Teaching / Supervision

- **IST Austria** Austria
Teaching, Computer Science Module, Complexity Theory. autumn 2011
- **University of Amsterdam** Netherlands
Teaching, Mastermath Course, Complexity Theory. spring 2011
– Mathermath is a course on the master level for students from all over the Netherlands.
- **ETH** Zürich, Switzerland
Teaching Assistance
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)
- **Current PhD Students:** Joachim Schipper. Since May 2010.

Professional Activities

- **Program Committees:** ICALP'07, CRYPTO'09, EUROCRYPT'09/'12, SCN'10, TCC'11, MFCS'11, PKC'12
- **General chair:** International Conference on Information Theoretic Security - ICITS. May 21-24 2011, Amsterdam, Netherlands. <http://event.cwi.nl/icits2011/>
- **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>

Recent Talks

Tutorials

- 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*.

Recent Invited Talks

- Apr. 2012 Workshop in honour of Alan Turings 100th Birthday on “Formal and Computational Cryptographic Proofs”, Newton Institute, Cambridge: *TBA*
- Jan. 2012 SOFSEM 2012: *Efficient Cryptography from Hard Learning Problems*.
- Sep. 2011 Dagstuhl Seminar “Public-Key Cryptography”: *TBA*.
- 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: *Efficient 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*.

Recent Conference Talks

- 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*.
- TCC 2007 Theory of Cryptography Conference, Amsterdam: *Parallel Repetition of Computationally Sound Protocols Revisited*.

Publications

In theoretical computer science in general, and cryptography in particular, conferences (not journals) are the most important venues where results are published. As to maximize visibility and impact of my research, I usually submit my major results to one of our two top conferences CRYPTO or EUROCRYPT (I published in every CRYPTO and EUROCRYPT since 2007 unless I was in the program committee.)

2011

1. 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**
2. Sebastian Faust and Krzysztof Pietrzak and Daniele Venturi. Tamper-Proof Circuits: How to Trade Leakage for Tamper-Resilience? In **ICALP 2011**
3. 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)**
4. Abhishek Jain and Krzysztof Pietrzak. Parallel Repetition for Leakage Resilience Amplification Revisited. In **TCC 2011**

2010

5. Yevgeniy Dodis and Krzysztof Pietrzak Leakage-Resilient Pseudorandom Functions and Side-Channel Attacks on Feistel Networks. In **CRYPTO 2010**
6. Johan Håstad and Rafael Pass and Krzysztof Pietrzak Douglas Wikström. An efficient parallel repetition theorem. In **TCC 2010**
7. Eike Kiltz and Krzysztof Pietrzak Leakage-Resilient ElGamal Encryption. In **ASIACRYPT 2010**
8. Sebastian Faust and Eike Kiltz and Krzysztof Pietrzak and Guy Rothblum. Leakage-Resilient Signatures. In **TCC 2010**
9. 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

10. 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.
11. 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.
12. 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

13. Stefan Dziembowski and Krzysztof Pietrzak. Leakage-resilient cryptography. In *49th FOCS*, pages 293–302. IEEE Computer Society Press, 2008.
14. 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.
15. Marc Fischlin, Anja Lehmann, and Krzysztof Pietrzak. Robust multi-property combiners for hash functions revisited. In **ICALP (2)**, pages 655–666, 2008.
16. Krzysztof Pietrzak and Johan Sjödin. Weak pseudorandom functions in minicrypt. In **ICALP (2)**, pages 423–436, 2008.
17. 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

18. 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.
19. 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.
20. 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.
21. 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.
22. 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.
23. 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

24. 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.
25. 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.

26. 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.
27. 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.
28. 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.
29. 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.
30. 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.
31. 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.
32. 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.
33. 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.