

Stefan Dziembowski

Curriculum vitae

Dipartimento di Informatica
Università La Sapienza
Via Salaria 113
00198 Rome, Italy

☎ +39 32 98 25 65 75

☎ +39 06 49 91 84 25

FAX +39 06 85 41 842

✉ stefan@dziembowski.net

web-page: www.dziembowski.net

Education

- 1997–2000 **PhD studies in computer science**, Århus University, Denmark.
- 1996-1997 **PhD studies in computer science**, Warsaw University, Poland.
(interrupted)
- 1992-1996 **MSc studies in computer science**, Warsaw University, Poland, full marks and honors.

Work experience

Accademic

- 1.2008 - onwards **assistant professor (ricercatore)**, Department of Computer Science, University of Rome La Sapienza, Italy.
- 7.2006 - 12.2007 **post-doctoral fellow**, Department of Computer Science, University of Rome La Sapienza, Italy.
founded by the EU Marie Curie Intra-European Fellowships program
- 10.2005 - 6.2006 **post-doctoral fellow**, Institute Institute for Informatics and Telematics, National Research Council (CNR), Pisa, Italy.
founded by the European Research Consortium for Informatics and Mathematics, ERCIM
- 12.2004 - 9.2006 **assistant professor (adiunkt)**, Institute Institute of Mathematics of the Polish Academy of Sciences, Warsaw, Poland.
(part-time)
- 10.2002 - 3.2007 **assistant professor (adiunkt)**, Institute Institute of Informatics, Warsaw University, Poland.
(from 10.2005 on leave)
- 3.2001 - 8.2002 **post-doctoral fellow**, Information Security and Cryptography Research Group (prof. Ueli Maurer), Swiss Federal Institute of Technology (ETH) Zurich, Switzerland.
- 8.1997 - 12.2000 **PhD student, research assistant**, Institute Department of Computer Science, University of Århus, Denmark.
- 10.1996 - 7.1997 **PhD student, research assistant**, Institute Institute of Informatics, Warsaw University, Poland.
(from 8.1997 on leave)

Other

8.2002 - 2.2003 **senior analyst**, *TLS-Technologies*, Warsaw, Poland.

Theses

PhD thesis

title *Multiparty Computations Information-Theoretically Secure Against an Adaptive Adversary*
supervisor Ivan Damgård
referees Ran Canetti and Peter Landrock

Master thesis

title *On the complexity of bounded-variable fixpoint queries*
supervisor Damian Niwiński

Publications

Journals

- Stefan Dziembowski and Ueli Maurer. *The Bare Bounded-Storage Model: The Tight Bound on the Storage Requirement for Key Agreement*. IEEE Transactions on Information Theory 54(6): 2790-2792 (2008)
- Ran Canetti, Ivan Damgård, Stefan Dziembowski, Yuval Ishai, and Tal Malkin. *Adaptive versus non-adaptive security of multi-party protocols*. Journal of Cryptology, 17(3):153–207, 2004
- Stefan Dziembowski and Ueli Maurer. *Optimal randomizer efficiency in the bounded-storage model*. Journal of Cryptology, 17(1):5–26, 2004

Conferences

- Stefan Dziembowski *How to Pair with a Human*. accepted to the Seventh Conference on Security and Cryptography for Networks (SCN 2010)
- Francesco Davi and Stefan Dziembowski and Daniele Venturi *Leakage-Resilient Storage*. accepted to the Seventh Conference on Security and Cryptography for Networks (SCN 2010)
- Stefan Dziembowski, Daniel Wichs and Krzysztof Pietrzak. *Non-Malleable Codes* In Proceedings of the First Symposium on Innovations in Computer Science, ICS 2010, pages 434-452, Tsinghua University Press, 2010
- Stefan Dziembowski. *A Lower Bound on the Key Length of Information-Theoretic Forward-Secure Storage Schemes*. In Proceedings of the Fourth International Conference Information Theoretic Security, ICITS 2009, pages 19-26, Springer 2010

- Stefan Dziembowski and Alessandro Mei and Alessandro Panconesi. *On Active Attacks on Sensor Network Key Distribution Schemes*. In Algorithmic Aspects of Wireless Sensor Networks, 5th International Workshop, ALGOSENSORS 2009, pages 52-63, Springer 2009
- Stefan Dziembowski and Krzysztof Pietrzak. *Leakage-Resilient Cryptography*. In Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science (FOCS) 2008, pages 293-302, IEEE, 2008
- Stefan Dziembowski and Krzysztof Pietrzak. *Intrusion-Resilient Secret Sharing*. In Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS) 2007, pages 227-237, IEEE, 2007
- Stefan Dziembowski. *On Forward-Secure Storage*. In Advances in Cryptology CRYPTO 2006, volume 4117 of Lecture Notes in Computer Science, pages 251-270. Springer-Verlag, August 2006
- Stefan Dziembowski. *Intrusion-Resilience via the Bounded-Storage Model*. In Third Theory of Cryptography Conference, TCC 2006, volume 3876 of Lecture Notes in Computer Science, pages 207-224. Springer-Verlag, March 2006
- Stefan Dziembowski and Ueli Maurer. *On generating the initial key in the bounded-storage model*. In Advances in Cryptology — EUROCRYPT '04, volume 3027 of Lecture Notes in Computer Science, pages 126–137. Springer-Verlag, May 2004.
- Stefan Dziembowski and Ueli Maurer. *Tight security proofs for the bounded-storage model*. In Proceedings of the 34th Annual ACM Symposium on Theory of Computing (STOC) 2002, pages 341–350. ACM, May 2002.
- Ran Canetti, Ivan Damgård, Stefan Dziembowski, Yuval Ishai, and Tal Malkin. *On adaptive vs. non-adaptive security of multiparty protocols*. In Advances in Cryptology — EUROCRYPT '01, volume 2045 of Lecture Notes in Computer Science, pages 262–279. Springer-Verlag, May 2001.
- Ronald Cramer, Ivan Damgård, and Stefan Dziembowski. *On the complexity of verifiable secret sharing and multiparty computation*. In Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (STOC) 2000, pages 325–334. ACM, May 2000.
- Ronald Cramer, Ivan Damgård, Stefan Dziembowski, Martin Hirt, and Tal Rabin. *Efficient multiparty computations secure against an adaptive adversary*. In Advances in Cryptology — EUROCRYPT '99, volume 1592 of Lecture Notes in Computer Science, pages 311–326. Springer-Verlag, May 1999.
- Stefan Dziembowski, Marcin Jurdzinski, and Igor Walukiewicz. *How much memory is needed to win infinite games?* In Proceedings, 12th Annual IEEE Symposium on Logic in Computer Science (LICS), pages 99–110. IEEE, June 1997.
- Stefan Dziembowski. *Bounded-variable fixpoint queries are PSPACE-complete*. Computer Science Logic (CSL) '96, volume 1258 of LNCS, pages 89–105. Springer, September 1996.

Selected talks

- A Lower Bound on the Key Length of Information-Theoretic Forward-Secure Storage Schemes, The 4th International Conference on Information Theoretic Security, ICITS 2009, December 3 2009. Shizuoka, Japan
- Cryptography on Non-Trusted Machines, University of Lugano, October 2009

- Crittografia: dagli antichi codici di Cesare ai protocolli avanzati per l'economia digitale, Workshop of the Department of Computer Science, University of Rome La Sapienza, September 2009
- Cryptography on Non-Trusted Machines, DYNAS 2009, International Workshop on DYNAMIC Networks: Algorithms and Security, September 2009, Wroclaw, Poland, invited talk
- Leakage-Resilient Cryptography, Workshop on Cryptographic Protocols and Public-Key Cryptography, May 2009, Bertinoro, Italy
- Leakage-Resilient Cryptography, Philadelphia, USA, October 2008, FOCS'08
- Intrusion-Resilient Secret Sharing, Providence, USA, October 2007, FOCS'07
- On Forward-Secure Storage, Santa Barbara, USA, August 2006, CRYPTO'06
- Intrusion-Resilience via the Bounded-Storage Model, New York, USA, March 2006, TCC'06
- Information-theoretic security. An area only for theoreticians?, a talk on Enigma conference, June 2005, Warsaw, Poland
- Introduction to the Bounded-Storage Model, Bedlewo, Poland, July 2004, invited talk on Wartacrypt'04, the 4th Central European Conference on Cryptology.
- Introduction to the Multiparty Computations, Warsaw, Poland, May 2004, Cryptology
- On generating the initial key in the bounded-storage model, Interlaken, Switzerland, May 2004, EUROCRYPT'04.
- Multiparty computation protocols, Warsaw, Poland, May 2003, a talk on workshop Quo vadis cryptology? A look at the state of the art in cryptology and new challenges ahead.
- The Story of Alice and Bob, a talk about cryptography on a workshop of the Polish Children's Fund, May 2003.
- Mathematical Foundations of Cryptography, a talk on the Warsaw University Open Days, March 2003.
- Tight Security Proofs for the Bounded-Storage Model, Montreal, Canada, May 2002, Symposium on Theory of Computing (STOC) 2002.
- Tight Security Proofs for the Bounded-Storage Model, Rutgers University, USA, May 2002, DIMACS Workshop on Cryptographic Protocols in Complex Environments.
- Tight Security Proofs for the Bounded-Storage Model, Santa Barbara, USA, August 2001, Rump Session of CRYPTO'01.
- Adaptive vs. Non-adaptive Security of Multiparty Protocols, Monte Verita, Switzerland, March 2001, Cryptographic Protocols for Distributed Systems workshop.
- On the Complexity of Verifiable Secret Sharing and Multiparty Computation, Portland, Oregon, USA, May 2000, Symposium on Theory of Computing (STOC) 2000.
- Efficient Multiparty Computations Secure Against an Adaptive Adversary, Prague, Czech Republic, May 1999, EUROCRYPT '99.
- Bounded-Variable Fixpoint Queries are PSPACE-complete, Utrecht, The Netherlands, September 1996, Computer Science Logic '96.
- Bounded-Variable Fixpoint Queries are PSPACE-complete, University of Bordeaux I, France, July 1996.

Teaching

University of Rome *La Sapienza*

- Lecturer:

Cryptography (2007/08, 2008/09, 2009/10) (standard introductory course on cryptography)

- Teaching Assistant: *Algorithms II, Computer Programming Methods*

Warsaw University

- Lecturer:

Cryptography on Non-Trusted Machines (12.2008 - 1.2009) a mini-course for PhD students

Practical Cryptographic Protocols (2004/05) (introduction to practical cryptography, overview of authentication and key-establishment protocols, Kerberos, PKI (X.509), SSL, IPsec, password-based protocols)

Mathematical Foundations of the Digital Signature Schemes (2004/05) (introduction to cryptography, classical signature schemes, random oracle model, Cramer-Shoup signatures, various types of signature schemes: threshold, blind, fail-stop, undeniable, forward-secure)

Cryptographic Protocol Theory (2003/04) (introduction to cryptography, interactive proofs, zero-knowledge, multiparty computations, e-voting, e-cash, private information retrieval, traitor tracing)

Introduction to Applied Cryptography (2002/03) (standard introductory course on cryptography)

- Teaching Assistant: *Discrete Mathematics; Languages, Automata and Computations, Introduction to Programming, Methods of Programming.*
- Co-supervisor of a seminar for graduate students: *Logic, Theory of Computations and Cryptography.* Supervisor of graduate students (8 MSc theses have been completed)

Polish Academy of Sciences

- Introduction to Cryptology (lecturer, together with prof. A. Wittlin)

ETH Zurich

- Teaching Assistant: *Information Security and Cryptography* (prof. U. Maurer), *Theory of Computation* (prof. J. Nievergelt)

Other

- Nippon Telegraph and Telephone Corporation Laboratories, Japan: A short (15 hours) course on the Multiparty Computations and on the Bounded-Storage Model, January 2004
- Bertinoro international Spring School *Modern Cryptography* a mini-course for PhD students, March 2009
- *Methods of the Modern Theoretical Cryptography*, a mini-course, Wroclaw Information Technology Initiative, Wroclaw, Poland, September 2009

The web-pages of the lectures listed above can be found at www.dziembowski.net/Teaching.

Scholarships and Achievements

- Winner of the European Research Council (ERC) Starting Independent Research Grant competition, project: *Cryptography on Non-Trusted Machines (CNTM)* (budget: 872.550 euro, duration: 5 years)
- Marie Curie Intra European Fellowship, EU Sixth Framework Program (call for proposals: FP6-2004-Mobility-5, proposal 024300-CRYPTOSENSORS, Cryptographic Security of Wireless Sensor Networks) 7.2006 - 12.2007. Host: *La Sapienza* University, Rome.
- Post-doctoral fellowship (at IIT Pisa) from the European Research Consortium for Informatics and Mathematics, ERCIM (10.2005-6.2006).
- Scientific scholarship from the rector of Warsaw University (2004).
- The Annual Stipend for Young Scientists from the Foundation for Polish Science (FNP).
- PhD scholarship at International PhD School Basic Research in Computer Science, University of Århus, Denmark (1997-2000).
- PhD scholarship at Warsaw University (academic year 1996/97).
- A Summer Student Scholarship in 1996 in Basic Research in Computer Science Research Center, University of Århus, Denmark.
- Scholarship for a high average grade at Warsaw University.
- Finalist of the Polish Mathematical Olympiads for High-School Students in the school years 1990/91 and 1991/92.

Project Participation

- European Research Council (ERC) Starting Independent Research Grant, project: *Cryptography on Non-Trusted Machines (207908-CNTM)*, budget: 872.550 euro, duration: 11.2008-10.2013, principal investigator.
- European Union grant MEIF-CT-2006-024300-CRYPTOSENSORS (a Marie Curie Intra European Fellowship), budget: 109.780 euro, duration 7.2006-12.2007, fellow
- European Union grant IST-2002-507932: *ECRYPT - European Network of Excellence for Cryptology*, participant
- European Union grant HPRN-CT-2002-00283: *Games and Automata for Synthesis and Validation*, 2002-2006, participant

- Polish State Committee for Scientific Research (KBN) grant 4 T11C 042 25: *Mathematical foundations of the correctness, security and effectiveness of computer systems*, 2003-2006, participant.
- Polish State Committee for Scientific Research (KBN) grant 7 T11C 027 20: *Mathematical methods for verification of computer systems*, 2001-2002, participant.
- Polish State Committee for Scientific Research (KBN) grant 8 T11C 002 11: *Mathematical models and logical calculi for reasoning about properties of computer systems*, 1996-1998, participant.

PC member

- Public Key Cryptography Conference (PKC) 2011,
- International Conference on Information Theoretic Security (ICITS) 2011,
- International Workshop on DYnamic Networks: Algorithms and Security (DYNAS) 2010,
- Financial Cryptography 2010,
- ASIACRYPT 2009,
- Financial Cryptography 2009,
- International Conference on Information Theoretic Security (ICITS) 2009,
- Theory of Cryptography Conference 2009,
- INSCRYPT 2008,
- ASIACRYPT 2008,
- International Conference on Information Theoretic Security (ICITS) 2008,
- Financial Cryptography Conference 2008,
- ICALP 2008, Track C: Security and Cryptography Foundations,
- ICALP 2007, Track C: Security and Cryptography Foundations,
- EUROCRYPT 2007,
- Theory of Cryptography Conference 2006,
- ASIACRYPT 2003.

Reviewer

Journals

Journal of Cryptology; Theoretical Computer Science; Information Processing Letters; IEEE Transactions on Information Theory; Fundamenta Informaticae

Conferences

EUROCRYPT, CRYPTO; Symposium on Theoretical Aspects of Computer Science (STACS); Logic in Computer Science (LICS); Foundations of Computer Science (FOCS); International Colloquium on Automata; Languages and Programming (ICALP); Financial Cryptography; International Symposium on Information Theory (ISIT); Symposium on Principles of Database Systems (PODS), International Conference on Algorithms and Complexity (CIAC), ACM Symposium on Principles of Distributed Computing; International Symposium on Fundamentals of Computation Theory (FCT); European Symposium on Algorithms; Colloquium on Structural Information and Communication Complexity (SIROCCO); International Conference on Trust, Privacy And Security in Digital Business (Trust-Bus); European PKI Workshop (EuroPKI)

Funding institutions

European Research Council (EU FP7 program)

Languages

Polish	Native
English	Fluent
Italian	Fluent
Russian	Basic

Media appearances

- Interview about cryptography given to the First Program of Polish Radio (2003)
- Interview about cryptography given to the Polish Radio Bis (2003)
- Appeared in the article *Cervelli in fuga dagli Usa, ma per amore*, Corriere Della Sera, 17.12.2008

Last update July 21, 2010