Stefan Dziembowski

Institute of Informatics, University of Warsaw
Banacha 2, 02-097 Warsaw, Poland
☎ +48 22 55 44 154 • FAX +48 22 55 44 400
✉ S.Dziembowski@crypto.edu.pl
www.crypto.edu.pl/Dziembowski

Current position

Institute of Informatics **University of Warsaw, Poland**
associate professor
head of the Cryptology and Data Security Group (www.crypto.edu.pl)

Degrees

Habilitation in Computer Science (summa cum laude)

dissertation title: Cryptographic Applications of the Bounded-Output Functions
institution: University of Warsaw
date: March 2012

PhD in Computer Science

dissertation title: Multiparty Computations Information-Theoretically Secure Against an Adaptive Adversary
insitution: Aarhus University
date: January 2001
supervisor: prof. Ivan Damgård

MSc in Computer Science (summa cum laude)

institution: University of Warsaw
date: September 1996
supervisor: prof. Damian Niwiński

Education

Århus University **Denmark**
PhD studies in computer science *1997–2000*

University of Warsaw **Poland**
MSc studies in computer science and mathematics *1992-1996*

Professional experience

academic

Institute of Informatics **University of Warsaw, Poland**
research associate (until Oct 2013) *Dec 2010–onwards*
associate professor (from Nov 2013)

Department of Computer Science — ***Sapienza* University of Rome, Italy**
assistant professor (from Dec 2010 on leave) — *Jan 2008–May 2014*
post-doc financed by the EU Marie-Curie Program (until Dec 2007)

Institute of Informatics and Telematics, Pisa — **National Research Council (CNR), Italy**
post-doc financed by the European Research Consortium for Informatics and Mathematics (ERCIM) — *Oct 2005–Jun 2006*

Institute of Mathematics — **Polish Academy of Science**
assistant professor (part-time) — *Dec 2004–Sep 2005*

Institute of Informatics — **University of Warsaw, Poland**
assistant professor — *Oct 2002–Sep 2005*

Information Security and Cryptography Research Group — **ETH Zürich, Switzerland**
post-doc (prof. Ueli Maurer group) — *Mar 2001–Aug 2002*

Basic Research in Computer Science (BRICS) PhD School — **Århus University, Denmark**
PhD student — *Aug 1997–Dec 2000*

Institute of Informatics — **University of Warsaw, Poland**
PhD student — *Oct 1996–Jun 1996*

other

TLS-Technologies — **Poland**
senior analyst — *Aug 2002–Feb 2003*

consulting

Medicalgorithmics S.A. (medical data security), Zunit sp. z o. o. (financial cryptography)

Papers

Journals

1. Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski and Łukasz Mazurek, *Secure Multiparty Computations on Bitcoin.* Communications of the ACM, accepted for publication, a version of a conference paper [9]
2. 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), a journal version of a part of a conference paper [28]
3. Stefan Dziembowski and Ueli Maurer. *Optimal randomizer efficiency in the bounded-storage model.* Journal of Cryptology, 17(1):5–26, 2004, the journal version of a conference paper [29])
4. 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, the journal version a conference paper [30])

Refereed conference proceedings

1. Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov and Krzysztof Pietrzak, *Proofs of Space.* accepted to Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA
2. Marcin Andrychowicz and Stefan Dziembowski, *PoW-Based Distributed Cryptography with no Trusted Setup.* accepted to Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology

Conference, Santa Barbara, CA, USA

3. Stefan Dziembowski, Sebastian Faust and Maciej Skórski, *Noisy Leakage Revisited.* the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2015
4. Marcin Andrychowicz, Ivan Damgaard, Stefan Dziembowski, Sebastian Faust and Antigoni Polychroniadou, *Efficient Leakage Resilient Circuit Compilers.* the RSA Conference Cryptographers' Track (CT-RSA) 2015
5. Divesh Aggarwal, Stefan Dziembowski,Tomasz Kazana and Maciej Obremski *Leakage-resilient non-malleable codes.* The Twelfth IACR Theory of Cryptography Conference TCC 2015
6. Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski and Łukasz Mazurek *On the Malleability of Bitcoin Transactions.* The Second Workshop on Bitcoin Research 2015 (in Assocation with Financial Crypto)
7. Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski and Łukasz Mazurek *Modeling Bitcoin Contracts by Timed Automata.* The 12th International Conference on Formal Modeling and Analysis of Timed Systems FORMATS 2014
8. Stefan Dziembowski and Maciej Zdanowicz *Position-Based Cryptography from Noisy Channels.* The 7th International Conference on Cryptology AFRICACRYPT 2014, Marrakech, Morocco
9. Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski and Łukasz Mazurek *Secure Multiparty Computations on Bitcoin.* The 35th IEEE Symposium on Security and Privacy (Oakland) 2014, **(Best Paper Award)**
10. Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski and Łukasz Mazurek *Fair Two-Party Computations via the Bitcoin Deposits.* The 1st Workshop on Bitcoin Research 2014 (in assocation with Financial Crypto'14)
11. Alexandre Duc, Stefan Dziembowski, Sebastian Faust *Unifying leakage models: from probing attacks to noisy leakage.* The 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2014, **(Best Paper Award, invited to the Journal of Cryptology)**
12. Konrad Durnoga, Stefan Dziembowski, Tomasz Kazana, Michał Zając *One-time Programs with Limited Memory.* In INSCRYPT 2013 The 9th China International Conference on Information Security and Cryptology Nov. 27 - Nov. 30, 2013, Guangzhou, China
13. Stefan Dziembowski, Tomasz Kazana, Maciej Obremski *Non-Malleable Codes from Two-Source Extractors.* In Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA,
14. Michał Jastrzębski, Stefan Dziembowski *Leakage Resilience of the Blom's Key Distribution Scheme.* In the 7th International Conference on Information Theoretic Security, ICITS 2013, Singapore, November 28-30, 2013.
15. Stefan Dziembowski, Sebastian Faust *Leakage-Resilient Circuits without Computational Assumptions.* In Theory of Cryptography - 9th Theory of Cryptography Conference, TCC 2012, Taormina, Sicily, Italy, March 19-21, 2012. Proceedings.
16. Stefan Dziembowski, Sebastian Faust *Leakage-Resilient Cryptography from the Inner-Product Extractor.* In Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings.
17. Stefan Dziembowski, Tomasz Kazana, Daniel Wichs *Key-Evolution Schemes Resilient to Space-Bounded Leakage.* In Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011.

18. Stefan Dziembowski, Tomasz Kazana, Daniel Wichs *One-Time Computable Self-erasing Functions.* In Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011.
19. Stefan Dziembowski *How to Pair with a Human* In Proceedings of the Seventh Conference on Security and Cryptography for Networks (SCN 2010), pages 200-218, Springer 2010
20. Francesco Davi and Stefan Dziembowski and Daniele Venturi *Leakage-Resilient Storage* Seventh Conference on Security and Cryptography for Networks (SCN 2010), pages 121-137, Springer 2010
21. 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
22. Stefan Dziembowski. *A Lower Bound on the Key Length of Information-Theoretic Forward-Secure Storage Schemes.* In Proceedings of the Fourth International ConferenceInformation Theoretic Security, ICITS 2009, pages 19-26, Springer 2010
23. 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
24. 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
25. 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
26. 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
27. 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
28. 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.
29. 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.
30. 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.
31. 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.
32. 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.

33. 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.
34. 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

- *Noisy Leakage Revisited*, Eurocrypt 2014, Sofia, Bulgaria, April 2015
- *PoW-Based Distributed Cryptography with no Trusted Setup*, Workshop in Cryptography, Bochum University, Germany, April 2015
- *Why do the cryptographic currencies need a solid theory*, Theoretical Computer Science Forum, Warsaw, January 2015
- *How to compute securely using Bitcoin scripts*, Invited talk at the International Workshop on P2P Financial Systems, Deutsche Bundesbank, Frankfurt, Germany, January 2015
- *Mathematical aspects of cryptocurrencies*, Poland's 2nd Interdisciplinary Symposium – Inter-Mix 2014m, Wojanów (Poland), November 2014
- *Introduction to Bitcoin – a tutorial*. The First Greater Tel Aviv Area Cryptography Symposium, Israel, November 2014
- *Recent advances in non-malleable codes*, Invited talk at the Joint Estonian-Latvian Theory Days at Ratnieki, Latvia, October 2014
- *Cryptography - from art to science*, A seminar at the Warsaw University of Technology before the ceremony of awarding IEEE Milestone to the Polish mathematicians who broke the Enigma machine, August 2014
- Bitcoin contracts – digital economy without lawyers? ZISC Workshop on Information Security, ETH Zurich, September 2014
- Bitcoin contracts – digital economy without lawyers? The Summer Research Institute, EPFL Lausanne, June 2014
- Cryptographic aspects of Bitcoin, Horizons In Mathematics - MCMCS Conference for Students (Będlewo, Poland), March 2014
- MPCs on Bitcoin, Rump session at the Cryptolens 2013 workshop at the Weizmann Institute, December 2013
- Leakage resilience of Blom key distribution scheme, The 7th International Conference on Information Theoretic Security (ICITS 2013)
- Non-Malleable Codes from Two-Source Extractors, Aarhus University Theory Seminar, October 9, 2013
- One-Time Computable Self-Erasing Functions Trends in Theoretical Cryptography 2011 January 10-12, 2011 ITCS, Tsinghua University, Beijing, China
- On the only computation leaks information paradigm Provable Security against Physical Attacks Lorentz Center, the Netherlands, February 2010
- How to Pair with a Human, The Seventh Conference on Security and Cryptography for Networks, SCN 2010, September 2010, Amalfi, Italy

- 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.

Graduated PhD students

- Francesco Davì (2012,*Sapienza* University of Rome)
- Tomasz Kazana (2013, University of Warsaw)
- Maciej Obremski (2013, University of Warsaw)

Current PhD students

Marcin Andrychowicz, Łukasz Mazurek, Maciej Skórski, Michał Zając, Maciej Zdanowicz.

Other

Number of graduated MSc students : University of Warsaw (15)

Number of completed PhD reviews: University of Warsaw (1), Institute of Computer Science of the Polish Academy of Sciences (2), Århus Universitet (3)

Lecturer

University of Warsaw

- *Financial Cryptography* (2014/15)
- *Information Theory* (2014/15)
- *Cryptography II* (2012/13,2013/14)
- *Cryptography I* (2011/12, 2012/13)
- *Practical Cryptographic Protocols (2004/05)*
- *Foundations of the Digital Signatures* (2004/05)
- *Cryptologic Protocol Theory* (2003/04)
- *Introduction to Applied Cryptography* (2002/03)

Università degli Studi di Roma La Sapienza

- *Crittografia* (2007/08, 2008/09, 2009/10)

Polish Academy of Sciences

- *Introduction to Cryptography* (2004/05, together with prof. A. Wittlin)

Other

- *Cryptography on Non-Trusted Machines* (short course for the PhD students University of Warsaw, 12.2008 - 1.2009)
- *Modern Cryptography* (short course for the PhD students, Bertinoro International Spring School, Italy, 3.2009)
- *Methods of the Modern Theoretical Cryptography* (short course, Wrocław Information Technology Initiative, Wrocław, Poland, 9.2009)
- *Multiparty Computations*, and *Bounded-Storage Model* (short courses, Nippon Telegraph and Telephone Corporation Laboratories, Japan, 1.2004)

PI of the grants

- National Science Centre, *Opus* grant, project: *Foundations of Cryptocurrencies*, budget: 649 600 zł, duration: 10.2015-9.2018
- The Foundation for Polish Science. *Welcome* grant, project: *Cryptographic Protocols Provably-Secure Against Physical Attacks, WELCOME/2010-4/2*, budget: 3.238.580 PLN, period: 06.2011-5.2015
- European Research Council (ERC) Starting Independent Research Grant, project: *Cryptography on Non-Trusted Machines (207908-CNTM)*, budget: 872.550 EUR, period: 11.2008-10.2013
- Marie Curie Intra European Fellowship, project MEIF-CT-2006-024300-CRYPTOSENSORS, budget: 109.780 euro, period 7.2006-12.2007

Conference service

PC member

- Workshop on Bitcoin Research 2015,
- International Conference on Information Theoretic Security (ICITS) 2013,
- International Colloquium on Automata, Languages, and Programming (ICALP) 2015,
- BalkanCryptSec 2014,
- Conference on Security and Cryptography for Networks (SCN) 2014,
- International Conference on Information Theoretic Security (ICITS) 2013,
- CRYPTO 2013,
- Public-Key Cryptography 2012,
- LATINCRYPT 2012,
- Conference on Security and Cryptography for Networks (SCN) 2012,
- International Colloquium on Automata, Languages, and Programming (ICALP) 2012,
- International Conference on Information Theoretic Security (ICITS) 2011,
- Public-Key Cryptography (PKC) 2011,
- 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,
- International Colloquium on Automata, Languages, and Programming (ICALP) 2008,
- International Colloquium on Automata, Languages, and Programming (ICALP) 2007,
- EUROCRYPT 2007,
- Theory of Cryptography Conference (TCC) 2006,
- ASIACRYPT 2003.

Other

- General chair of the *IACR Theory of Cryptography Conference (TCC) 2015.*

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); Public-Key Cryptography (PKC); 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

- Reviewer for: the European Research Council (ERC), the Foundation for Polish Science (FNP), the Polish National Science Centre (NCN), the Israel Science Foundation (ISF), the Netherlands Organisation for Scientific Research (NWO)
- Panel member of: the KOLUMB grants (Foundation for Polish Science, Warsaw, 2009), the European Coordinated Research on Long-term Challenges in Information and Communication Sciences & Technologies ERA-Net (CHIST-ERA) grants (Paris, 2015)

Languages

Polish: native

English: fluent

Italian: fluent

Russian: basic

Latest changes: May 16, 2015