Stefan Dziembowski

Institute of Informatics, University of Warsaw
Banacha 2, 02-097 Warsaw, Poland
✉ S.Dziembowski@crypto.edu.pl • www.crypto.edu.pl/Dziembowski
Stefan-Dziembowski • 0000-0002-6914-6425
scholar.google: VgiXQ2YAAAAJ • in stefan-dziembowski
SteDziembowski

Degrees

Professor title

date: October 2019

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

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

Institute of Informatics — **University of Warsaw, Poland**
research associate (until Oct 2013)
associate professor (Nov 2013 — Sep 2019)
professor (from Oct 2019) — *Dec 2010–onwards*
head of the Cryptography and Blockchain Lab (www.crypto.edu.pl)

IDEAS NCBR — **Warsaw, Poland**
Intelligent Algorithms for Digital Economy institute (ideas-ncbr.pl) — *Jul 2021–onwards*
Systems security and data privacy group leader (part-time)

Department of Computer Science — ***Sapienza* University of Rome, Italy**
assistant professor (from Dec 2010 on leave) — *Jan 2006–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*

Longer research visits

Simons Institute — **UC Berkeley, USA**
Visiting Scientist — *Oct 2019 – Nov 2019*

Simons Institute — **UC Berkeley, USA**
Visiting Scientist — *Jul 2015 – Aug 2015*

Awards and achievements

- Elected to be a member of the *Warsaw Scientific Society* (Pol.: *Towarzystwo Naukowe Warszawskie)* 2020
- First Degree Individual Award from the Rector of the University of Warsaw 2020
- Keynote speaker at the Conference on Cryptographic Hardware and Embedded Systems (CHES) 2020
- Nicolaus Copernicus Polish-German Research Award 2020 (together with prof. Sebastian Faust)
- ERC Advanced Grant (the 2019 call)
- Silver Medal of the University of Warsaw for the University 200 years Anniversary (2016)
- Kazimierz Bartel Award (2016)
- Best Paper Award at the IEEE Symposium on Security and Privacy (IEEE S&P) 2014
- Best Paper Award at EUROCRYPT 2014
- ERC Starting Grant (the 2007 call)
- Foundation for Polish Science *START* fellowship (2003-04)

Publications

Journals

(note: most of these papers are extended versions or are partly based on the conference papers listed later)

- Alexandre Duc, Stefan Dziembowski, and Sebastian Faust. “Unifying Leakage Models: From Probing Attacks to Noisy Leakage”. In: *J. Cryptology* 32.1 (2019), pp. 151–177.

- Stefan Dziembowski, Tomasz Kazana, and Maciej Zdanowicz. “Quasi chain rule for min-entropy”. In: *Inf. Process. Lett.* 134 (2018), pp. 62–66.
- Stefan Dziembowski, Krzysztof Pietrzak, and Daniel Wichs. “Non-Malleable Codes”. In: *J. ACM* 65.4 (2018), 20:1–20:32.
- Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Lukasz Mazurek. “Secure multiparty computations on Bitcoin”. In: *Commun. ACM* 59.4 (2016), pp. 76–84.
- Stefan Dziembowski and Ueli M. Maurer. “The Bare Bounded-Storage Model: The Tight Bound on the Storage Requirement for Key Agreement”. In: *IEEE Trans. Information Theory* 54.6 (2008), pp. 2790–2792.
- Ran Canetti, Ivan Damgård, Stefan Dziembowski, Yuval Ishai, and Tal Malkin. “Adaptive versus Non-Adaptive Security of Multi-Party Protocols”. In: *J. Cryptology* 17.3 (2004), pp. 153–207.
- Stefan Dziembowski and Ueli M. Maurer. “Optimal Randomizer Efficiency in the Bounded-Storage Model”. In: *J. Cryptology* 17.1 (2004), pp. 5–26.

Refereed conference proceedings

- Gianluca Brian, Stefan Dziembowski, and Sebastian Faust. “From Random Probing to Noisy Leakages Without Field-Size Dependence”. In: *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part IV*. Ed. by Marc Joye and Gregor Leander. Vol. 14654. Lecture Notes in Computer Science. Springer, 2024, pp. 345–374.
- Stefan Dziembowski, Sebastian Faust, Tomasz Lizurej, and Marcin Mielniczuk. “Secret Sharing with Snitching”. In: *accepted to the 31st ACM Conference on Computer and Communications Security (ACM CCS 2024)*. 2024.
- Stefan Dziembowski, Stanisław Jarecki, Paweł Kędzior, Hugo Krawczyk, Chan Nam Ngo, and Jiayu Xu. “Password-Protected Threshold Signatures”. In: *accepted to ASIACRYPT 2024 - 30th International Conference on the Theory and Application of Cryptology and Information Security*. 2024.
- Mirza Ahad Baig, Suvradip Chakraborty, Stefan Dziembowski, Malgorzata Galazka, Tomasz Lizurej, and Krzysztof Pietrzak. “Efficiently Testable Circuits”. In: *14th Innovations in Theoretical Computer Science Conference, ITCS 2023, January 10-13, 2023, MIT, Cambridge, Massachusetts, USA*. Ed. by Yael Tauman Kalai. Vol. 251. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023, 10:1–10:23.
- Mirza Ahad Baig, Suvradip Chakraborty, Stefan Dziembowski, Malgorzata Galazka, Tomasz Lizurej, and Krzysztof Pietrzak. “Efficiently Testable Circuits Without Conductivity”. In: *Theory of Cryptography - 21st International Conference, TCC 2023, Taipei, Taiwan, November 29 - December 2, 2023, Proceedings, Part III*. Ed. by Guy N. Rothblum and Hoeteck Wee. Vol. 14371. Lecture Notes in Computer Science. Springer, 2023, pp. 123–152.
- Stefan Dziembowski, Sebastian Faust, and Tomasz Lizurej. “Individual Cryptography”. In: *Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part II*. Ed. by Helena Handschuh and Anna Lysyanskaya. Vol. 14082. Lecture Notes in Computer Science. Springer, 2023, pp. 547–579.
- Stefan Dziembowski and Pawel Kedzior. “Non-Atomic Payment Splitting in Channel Networks”. In: *5th Conference on Advances in Financial Technologies, AFT 2023, October 23-25, 2023, Princeton, NJ, USA*. Ed. by Joseph Bonneau and S. Matthew Weinberg. Vol. 282. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023, 17:1–17:23.
- Tomasz Lizurej, Tomasz Michalak, and Stefan Dziembowski. “On Manipulating Weight Predictions in Signed Weighted Networks”. In: *Thirty-Seventh AAAI Conference on Artificial Intelligence, AAAI 2023, Thirty-Fifth Conference on Innovative Applications of Artificial Intelligence, IAAI 2023, Thirteenth Symposium on Educational Advances in Artificial Intelligence, EAAI 2023, Washington, DC, USA, February 7-14, 2023*. Ed. by Brian Williams, Yiling Chen, and Jennifer Neville. AAAI Press, 2023, pp. 5222–5229.
- Suvradip Chakraborty, Stefan Dziembowski, Malgorzata Galazka, Tomasz Lizurej, Krzysztof Pietrzak, and Michelle Yeo. “Trojan-Resilience Without Cryptography”. In: *Theory of Cryptography - 19th International*

Conference, *TCC 2021*, *Raleigh*, *NC*, *USA*, *November 8-11*, *2021*, *Proceedings*, *Part II*. Ed. by Kobbi Nissim and Brent Waters. Vol. 13043. Lecture Notes in Computer Science. Springer, 2021, pp. 397–428.

- Stefan Dziembowski, Grzegorz Fabianski, Sebastian Faust, and Siavash Riahi. "Lower Bounds for Off-Chain Protocols: Exploring the Limits of Plasma". In: *12th Innovations in Theoretical Computer Science Conference*, *ITCS 2021*, *January 6-8*, *2021*, *Virtual Conference*. Ed. by James R. Lee. Vol. 185. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021, 72:1–72:20.
- Suvradip Chakraborty, Stefan Dziembowski, and Jesper Buus Nielsen. "Reverse Firewalls for Actively Secure MPCs". In: *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference*, *CRYPTO 2020*, *Santa Barbara*, *CA*, *USA*, *August 17-21*, *2020*, *Proceedings*, *Part II*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12171. Lecture Notes in Computer Science. Springer, 2020, pp. 732–762.
- Stefan Dziembowski, Lisa Eckey, Sebastian Faust, Julia Hesse, and Kristina Hostáková. "Multi-party Virtual State Channels". In: *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, *Darmstadt*, *Germany*, *May 19-23*, *2019*, *Proceedings*, *Part I*. Ed. by Yuval Ishai and Vincent Rijmen. Vol. 11476. Lecture Notes in Computer Science. Springer, 2019, pp. 625–656.
- Stefan Dziembowski, Lisa Eckey, Sebastian Faust, and Daniel Malinowski. "Perun: Virtual Payment Hubs over Cryptocurrencies". In: *2019 IEEE Symposium on Security and Privacy*, *SP 2019*, *San Francisco*, *CA*, *USA*, *May 19-23*, *2019*. IEEE, 2019, pp. 106–123.
- Stefan Dziembowski, Sebastian Faust, and Karol Zebrowski. "Simple Refreshing in the Noisy Leakage Model". In: *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security*, *Kobe*, *Japan*, *December 8-12*, *2019*, *Proceedings*, *Part III*. Ed. by Steven D. Galbraith and Shiho Moriai. Vol. 11923. Lecture Notes in Computer Science. Springer, 2019, pp. 315–344.
- Stefan Dziembowski, Lisa Eckey, and Sebastian Faust. "FairSwap: How To Fairly Exchange Digital Goods". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, *CCS 2018*, *Toronto*, *ON*, *Canada*, *October 15-19*, *2018*. Ed. by David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang. ACM, 2018, pp. 967–984.
- Stefan Dziembowski, Sebastian Faust, and Kristina Hostáková. "General State Channel Networks". In: *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, *CCS 2018*, *Toronto*, *ON*, *Canada*, *October 15-19*, *2018*. Ed. by David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang. ACM, 2018, pp. 949–966.
- Joshua Brody, Stefan Dziembowski, Sebastian Faust, and Krzysztof Pietrzak. "Position-Based Cryptography and Multiparty Communication Complexity". In: *Theory of Cryptography - 15th International Conference*, *TCC 2017*, *Baltimore*, *MD*, *USA*, *November 12-15*, *2017*, *Proceedings*, *Part I*. Ed. by Yael Kalai and Leonid Reyzin. Vol. 10677. Lecture Notes in Computer Science. Springer, 2017, pp. 56–81.
- Marcin Andrychowicz, Stefan Dziembowski, and Sebastian Faust. "Circuit Compilers with O(1/\log (n)) Leakage Rate". In: *Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, *Vienna*, *Austria*, *May 8-12*, *2016*, *Proceedings*, *Part II*. Ed. by Marc Fischlin and Jean-Sébastien Coron. Vol. 9666. Lecture Notes in Computer Science. Springer, 2016, pp. 586–615.
- Waclaw Banasik, Stefan Dziembowski, and Daniel Malinowski. "Efficient Zero-Knowledge Contingent Payments in Cryptocurrencies Without Scripts". In: *Computer Security - ESORICS 2016 - 21st European Symposium on Research in Computer Security*, *Heraklion*, *Greece*, *September 26-30*, *2016*, *Proceedings*, *Part II*. Ed. by Ioannis G. Askoxylakis, Sotiris Ioannidis, Sokratis K. Katsikas, and Catherine A. Meadows. Vol. 9879. Lecture Notes in Computer Science. Springer, 2016, pp. 261–280.
- Konrad Durnoga, Stefan Dziembowski, Tomasz Kazana, Michal Zajac, and Maciej Zdanowicz. "Bounded-Retrieval Model with Keys Derived from Private Data". In: *Information Security and Cryptology - 12th International Conference*, *Inscrypt 2016*, *Beijing*, *China*, *November 4-6*, *2016*, *Revised Selected Papers*. Ed.

by Kefei Chen, Dongdai Lin, and Moti Yung. Vol. 10143. Lecture Notes in Computer Science. Springer, 2016, pp. 273–290.

- Stefan Dziembowski, Sebastian Faust, Gottfried Herold, Anthony Journault, Daniel Masny, and François-Xavier Standaert. "Towards Sound Fresh Re-keying with Hard (Physical) Learning Problems". In: *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*. Ed. by Matthew Robshaw and Jonathan Katz. Vol. 9815. Lecture Notes in Computer Science. Springer, 2016, pp. 272–301.
- Stefan Dziembowski, Sebastian Faust, and Maciej Skórski. "Optimal Amplification of Noisy Leakages". In: *Theory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part II*. Ed. by Eyal Kushilevitz and Tal Malkin. Vol. 9563. Lecture Notes in Computer Science. Springer, 2016, pp. 291–318.
- Stefan Dziembowski, Sebastian Faust, and François-Xavier Standaert. "Private Circuits III: Hardware Trojan-Resilience via Testing Amplification". In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*. Ed. by Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi. ACM, 2016, pp. 142–153.
- Divesh Aggarwal, Stefan Dziembowski, Tomasz Kazana, and Maciej Obremski. "Leakage-Resilient Non-malleable Codes". In: *Theory of Cryptography - 12th Theory of Cryptography Conference, TCC 2015, Warsaw, Poland, March 23-25, 2015, Proceedings, Part I*. Ed. by Yevgeniy Dodis and Jesper Buus Nielsen. Vol. 9014. Lecture Notes in Computer Science. Springer, 2015, pp. 398–426.
- Marcin Andrychowicz, Ivan Damgård, Stefan Dziembowski, Sebastian Faust, and Antigoni Polychroniadou. "Efficient Leakage Resilient Circuit Compilers". In: *Topics in Cryptology - CT-RSA 2015, The Cryptographer's Track at the RSA Conference 2015, San Francisco, CA, USA, April 20-24, 2015. Proceedings*. Ed. by Kaisa Nyberg. Vol. 9048. Lecture Notes in Computer Science. Springer, 2015, pp. 311–329.
- Marcin Andrychowicz and Stefan Dziembowski. "PoW-Based Distributed Cryptography with No Trusted Setup". In: *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*. Ed. by Rosario Gennaro and Matthew Robshaw. Vol. 9216. Lecture Notes in Computer Science. Springer, 2015, pp. 379–399.
- Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Lukasz Mazurek. "On the Malleability of Bitcoin Transactions". In: *Financial Cryptography and Data Security - FC 2015 International Workshops, BITCOIN, WAHC, and Wearable, San Juan, Puerto Rico, January 30, 2015, Revised Selected Papers*. Ed. by Michael Brenner, Nicolas Christin, Benjamin Johnson, and Kurt Rohloff. Vol. 8976. Lecture Notes in Computer Science. Springer, 2015, pp. 1–18.
- Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak. "Proofs of Space". In: *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*. Ed. by Rosario Gennaro and Matthew Robshaw. Vol. 9216. Lecture Notes in Computer Science. Springer, 2015, pp. 585–605.
- Stefan Dziembowski, Sebastian Faust, and Maciej Skorski. "Noisy Leakage Revisited". In: *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part II*. Ed. by Elisabeth Oswald and Marc Fischlin. Vol. 9057. Lecture Notes in Computer Science. Springer, 2015, pp. 159–188.
- Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Lukasz Mazurek. "Fair Two-Party Computations via Bitcoin Deposits". In: *Financial Cryptography and Data Security - FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, Barbados, March 7, 2014, Revised Selected Papers*. Ed. by Rainer Böhme, Michael Brenner, Tyler Moore, and Matthew Smith. Vol. 8438. Lecture Notes in Computer Science. Springer, 2014, pp. 105–121.
- Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Lukasz Mazurek. "Modeling Bitcoin Contracts by Timed Automata". In: *Formal Modeling and Analysis of Timed Systems - 12th International Conference, FORMATS 2014, Florence, Italy, September 8-10, 2014. Proceedings*. Ed. by Axel Legay and Marius Bozga. Vol. 8711. Lecture Notes in Computer Science. Springer, 2014, pp. 7–22.

- Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Lukasz Mazurek. "Secure Multiparty Computations on Bitcoin". In: *2014 IEEE Symposium on Security and Privacy, SP 2014, Berkeley, CA, USA, May 18-21, 2014* (***Best Paper Award***). IEEE Computer Society, 2014, pp. 443–458.
- Alexandre Duc, Stefan Dziembowski, and Sebastian Faust. "Unifying Leakage Models: From Probing Attacks to Noisy Leakage". In: *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings* (***Best Paper Award***). Ed. by Phong Q. Nguyen and Elisabeth Oswald. Vol. 8441. Lecture Notes in Computer Science. Springer, 2014, pp. 423–440.
- Stefan Dziembowski and Maciej Zdanowicz. "Position-Based Cryptography from Noisy Channels". In: *Progress in Cryptology - AFRICACRYPT 2014 - 7th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 28-30, 2014. Proceedings*. Ed. by David Pointcheval and Damien Vergnaud. Vol. 8469. Lecture Notes in Computer Science. Springer, 2014, pp. 300–317.
- Konrad Durnoga, Stefan Dziembowski, Tomasz Kazana, and Michal Zajac. "One-Time Programs with Limited Memory". In: *Information Security and Cryptology - 9th International Conference, Inscrypt 2013, Guangzhou, China, November 27-30, 2013, Revised Selected Papers*. Ed. by Dongdai Lin, Shouhuai Xu, and Moti Yung. Vol. 8567. Lecture Notes in Computer Science. Springer, 2013, pp. 377–394.
- Stefan Dziembowski, Tomasz Kazana, and Maciej Obremski. "Non-malleable Codes from Two-Source Extractors". In: *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II*. Ed. by Ran Canetti and Juan A. Garay. Vol. 8043. Lecture Notes in Computer Science. Springer, 2013, pp. 239–257.
- Michal Jastrzebski and Stefan Dziembowski. "Leakage Resilience of the Blom's Key Distribution Scheme". In: *Information Theoretic Security - 7th International Conference, ICITS 2013, Singapore, November 28-30, 2013, Proceedings*. Ed. by Carles Padró. Vol. 8317. Lecture Notes in Computer Science. Springer, 2013, pp. 220–237.
- Stefan Dziembowski and 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*. Ed. by Ronald Cramer. Vol. 7194. Lecture Notes in Computer Science. Springer, 2012, pp. 230–247.
- Stefan Dziembowski and 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*. Ed. by Dong Hoon Lee and Xiaoyun Wang. Vol. 7073. Lecture Notes in Computer Science. Springer, 2011, pp. 702–721.
- Stefan Dziembowski, Tomasz Kazana, and 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. Proceedings*. Ed. by Phillip Rogaway. Vol. 6841. Lecture Notes in Computer Science. Springer, 2011, pp. 335–353.
- Stefan Dziembowski, Tomasz Kazana, and 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. Proceedings*. Ed. by Yuval Ishai. Vol. 6597. Lecture Notes in Computer Science. Springer, 2011, pp. 125–143.
- Francesco Davì, Stefan Dziembowski, and Daniele Venturi. "Leakage-Resilient Storage". In: *Security and Cryptography for Networks, 7th International Conference, SCN 2010, Amalfi, Italy, September 13-15, 2010. Proceedings*. Ed. by Juan A. Garay and Roberto De Prisco. Vol. 6280. Lecture Notes in Computer Science. Springer, 2010, pp. 121–137.
- Stefan Dziembowski. "How to Pair with a Human". In: *Security and Cryptography for Networks, 7th International Conference, SCN 2010, Amalfi, Italy, September 13-15, 2010. Proceedings*. Ed. by Juan A. Garay and Roberto De Prisco. Vol. 6280. Lecture Notes in Computer Science. Springer, 2010, pp. 200–218.

- Stefan Dziembowski, Krzysztof Pietrzak, and Daniel Wichs. “Non-Malleable Codes”. In: *Innovations in Computer Science - ICS 2010, Tsinghua University, Beijing, China, January 5-7, 2010. Proceedings*. Ed. by Andrew Chi-Chih Yao. Tsinghua University Press, 2010, pp. 434–452.
- Stefan Dziembowski. “A Lower Bound on the Key Length of Information-Theoretic Forward-Secure Storage Schemes”. In: *Information Theoretic Security, 4th International Conference, ICITS 2009, Shizuoka, Japan, December 3-6, 2009. Revised Selected Papers*. Ed. by Kaoru Kurosawa. Vol. 5973. Lecture Notes in Computer Science. Springer, 2009, pp. 19–26.
- Stefan Dziembowski, 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, Rhodes, Greece, July 10-11, 2009. Revised Selected Papers*. Ed. by Shlomi Dolev. Vol. 5804. Lecture Notes in Computer Science. Springer, 2009, pp. 52–63.
- Stefan Dziembowski and Krzysztof Pietrzak. “Leakage-Resilient Cryptography”. In: *49th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2008, October 25-28, 2008, Philadelphia, PA, USA*. IEEE Computer Society, 2008, pp. 293–302.
- Stefan Dziembowski and Krzysztof Pietrzak. “Intrusion-Resilient Secret Sharing”. In: *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2007), October 20-23, 2007, Providence, RI, USA, Proceedings*. IEEE Computer Society, 2007, pp. 227–237.
- Stefan Dziembowski. “Intrusion-Resilience Via the Bounded-Storage Model”. In: *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006, Proceedings*. Ed. by Shai Halevi and Tal Rabin. Vol. 3876. Lecture Notes in Computer Science. Springer, 2006, pp. 207–224.
- Stefan Dziembowski. “On Forward-Secure Storage”. In: *Advances in Cryptology - CRYPTO 2006, 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2006, Proceedings*. Ed. by Cynthia Dwork. Vol. 4117. Lecture Notes in Computer Science. Springer, 2006, pp. 251–270.
- Stefan Dziembowski and Ueli M. Maurer. “On Generating the Initial Key in the Bounded-Storage Model”. In: *Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004, Proceedings*. Ed. by Christian Cachin and Jan Camenisch. Vol. 3027. Lecture Notes in Computer Science. Springer, 2004, pp. 126–137.
- Stefan Dziembowski and Ueli M. Maurer. “Tight security proofs for the bounded-storage model”. In: *Proceedings on 34th Annual ACM Symposium on Theory of Computing, May 19-21, 2002, Montréal, Québec, Canada*. Ed. by John H. Reif. ACM, 2002, pp. 341–350.
- 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 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*. Ed. by Birgit Pfitzmann. Vol. 2045. Lecture Notes in Computer Science. Springer, 2001, pp. 262–279.
- Ronald Cramer, Ivan Damgård, and Stefan Dziembowski. “On the complexity of verifiable secret sharing and multiparty computation”. In: *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, May 21-23, 2000, Portland, OR, USA*. Ed. by F. Frances Yao and Eugene M. Luks. ACM, 2000, pp. 325–334.
- 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, International Conference on the Theory and Application of Cryptographic Techniques, Prague, Czech Republic, May 2-6, 1999, Proceeding*. Ed. by Jacques Stern. Vol. 1592. Lecture Notes in Computer Science. Springer, 1999, pp. 311–326.
- 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, Warsaw, Poland, June 29 - July 2, 1997*. IEEE Computer Society, 1997, pp. 99–110.

- Stefan Dziembowski. “Bounded-Variable Fixpoint Queries are PSPACE-complete”. In: *Computer Science Logic, 10th International Workshop, CSL '96, Annual Conference of the EACSL, Utrecht, The Netherlands, September 21-27, 1996, Selected Papers*. Ed. by Dirk van Dalen and Marc Bezem. Vol. 1258. Lecture Notes in Computer Science. Springer, 1996, pp. 89–105.

Edited volumes

- Orr Dunkelman and Stefan Dziembowski, eds. *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part I*. Vol. 13275. Lecture Notes in Computer Science. Springer, 2022.
- Orr Dunkelman and Stefan Dziembowski, eds. *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part II*. Vol. 13276. Lecture Notes in Computer Science. Springer, 2022.
- Orr Dunkelman and Stefan Dziembowski, eds. *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*. Vol. 13277. Lecture Notes in Computer Science. Springer, 2022.
- Amos Beimel and Stefan Dziembowski, eds. *Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part I*. Vol. 11239. Lecture Notes in Computer Science. Springer, 2018.
- Amos Beimel and Stefan Dziembowski, eds. *Theory of Cryptography - 16th International Conference, TCC 2018, Panaji, India, November 11-14, 2018, Proceedings, Part II*. Vol. 11240. Lecture Notes in Computer Science. Springer, 2018.

Membership in the Administrative Committees

- Council of the Polish National Science Centre (2021-2024).
- TrustChain (trustchain.ngi.eu) Executive Advisory Board (2023 -)
- University of Warsaw Electoral College to elect the rector for the 2024-2028 term.
- University of Warsaw Electoral College to elect the rector for the 2020-2024 term.
- Commission for the Employment of Academic Staff at the Faculty of Mathematics, Informatics and Mechanics, University of Warsaw (2021-2024).
- Scientific Council for Mathematics and Computer Science at the University of Warsaw (2019-2020).
- Faculty Council of the Faculty of Mathematics, Informatics and Mechanics, University of Warsaw.
- commission for PhD procedures in Computer Science at the University of Warsaw.
- Computer Science Committee of the Polish Academy of Sciences (2016–2019).
- advisory team for the lists of scientific journals for the Polish Ministry of Science (2019).

Grant PI

- Foundation for Polish Science, Scientific subsidy linked to the *Nicolaus Copernicus Polish-German Research Award 2020 COP/01/2020*, budget: EUR 80,000, duration: July 2020 – Jun 2023,
- National Science Centre, *Opus* grant, project: *Blockchain wallets – cryptographic theory and applications, 2019/35/B/ST6/04138* , budget: PLN 945,600, duration: Sep 2020 – Aug 2024,
- European Research Council (ERC) Advanced Grant, project: *Smart-Contract Protocols: Theory for Applications (885666-PROCONTRA)*, budget: EUR 2,496,372, duration: Jan 2021 – Dec 2025,
- Ethereum Foundation, project *Off-chain labs: formal models, constructions and proofs, FY18-0023*, budget

EUR 99,600, duration Nov 2018 – Nov 2023,

- Foundation for Polish Science. *Team* grant, project: *Cryptographic Defence Against Malicious Hardware Manufacturers*, *TEAM 2016/1/4*, budget: PLN 3,080,100, duration: Oct 2016 – Aug 2020,
- National Science Centre, *Opus* grant, project: *Foundations of Cryptocurrencies*, *2014/13/B/ST6/03540*, budget: PLN 649,600, duration: Oct 2015 – Sep 2019,
- Foundation for Polish Science. *Welcome* grant, project: *Cryptographic Protocols Provably-Secure Against Physical Attacks*, *WELCOME/2010-4/2*, budget: PLN 3,238,580, duration: Jun 2011 – Dec 2015,
- European Research Council (ERC) Starting Grant, project: *Cryptography on Non-Trusted Machines (207908-CNTM)*, budget: EUR 872,550, duration: Nov 2008 – Oct 2013,
- Marie Curie Intra European Fellowship, project MEIF-CT-2006-024300-CRYPTOSENSORS, budget: EUR 109,780, duration: Jul 2006 – Dec 2007

Project Participant

- Polish National Centre for Research and Development, NCBR, project *Bitfold* POIR.01.01.01-00-1101/20 (2021)
- The European Cooperation in Science and Technology (COST) action *Cryptography for Secure Digital Interaction* (2014 – 2018)

Service

Program Committee Chair

- Theory of Cryptography Conference (TCC) 2018 (co-chair together with Amos Beimel),
- Eurocrypt 2022 (co-chair together with Orr Dunkelman)

PC member

ACM Conference on Advances in Financial Technologies (AFT 2020), ACM Conference on Computer and Communications Security (ACM CCS 2016, 2021, 2023), ASIACRYPT (2003, 2008, 2009), BalkanCryptSec 2014, Conference on Cryptographic Hardware and Embedded Systems (CHES 2021), Conference on Security and Cryptography for Networks (SCN 2012, 2014), CRYPTO 2013, Crypto Valley Conference 2021, EUROCRYPT (2007, 2017, 2018, 2019, 2021), Financial Cryptography (2008, 2009, 2010,2022), Information-Theoretic Cryptography (2020), International Symposium on Cyber Security Cryptology and Machine Learning 2022 INSCRYPT 2008. International Colloquium on Automata, Languages, and Programming (ICALP 2007, 2008, 2012, 2015), International Conference on Information Theoretic Security (ICITS 2007, 2008, 2011, 2013, 2016), LATINCRYPT 2012, Public-Key Cryptography (PKC 2011, 2012), Stanford Blockchain Conference (2020), Theory of Cryptography Conference (TCC 2006, 2009, 2020, 2024), Workshop on Bitcoin Research (2015, 2017)

Current Editorial Board Member

- IEEE Transactions on Dependable and Secure Computing (from 2021)

Past Editorial Board Member

- Information and Computation

Scientific Event Organizer

- Organizer of the Warsaw IACR Summer School on Post-Quantum Cryptography, July 2024, Warsaw, Poland,
- Organizer of the Second IACR School on Privacy-Preserving Machine Learning, July 2023, Warsaw, Poland,
- Co-coordinator of the *Combinatorics and Cryptology* session at the *Jubilee Congress for the 100th anniversary of the Polish Mathematical Society*, September 2019, Cracow, Poland,

- General chair of the Theory of Cryptography Conference (TCC) 2015, Warsaw, Poland
- General chair of the Workshop on Leakage, Tampering and Viruses 2013, Warsaw, Poland.

Reviewer

Journals

SIAM Journal on Computing; Journal of the ACM; 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)

Grant reviewer

European Research Council (ERC), Foundation for Polish Science, Polish National Science Centre (NCN), Polish National Centre for Research and Development (NCBiR), German Research Foundation (DFG), Israel Science Foundation (ISF), Netherlands Organisation for Scientific Research (NWO), Polish National Agency for Academic Exchange, Vienna Science and Technology Fund

Grant panel member

European Coordinated Research on Long-term Challenges in Information and Communication Sciences & Technologies ERA-NET (CHIST-ERA, 2014), Foundation for Polish Science (Team and Team Tech grants, 2018), European Research Council (Consolidator Grant, 2023)

PhD, habilitation, hiring, and tenure case reviewer

Adam Mickiewicz University (Poznań)„ Carnegie Mellon University, ETH Zurich, Indian Institute of Science Bangalore, Indian Statistical Institute, Institute of Computer Science (Polish Academy of Sciences), Institute of Science and Technology Austria (IST Austria), Jagiellonian University (Cracow), National University of Singapore, Tel Aviv University, Technical University of Darmstadt, University of Edinburgh, University of Haifa, University of Warsaw

Selected research talks

- *Individual Cryptography: Secret Sharing with Snitching*, Cryptography in the Blockchain Era workshop, June 2024,
- *Non-Atomic Payment Splitting in Channel Networks*, Advances in Financial Technologies - AFT 2023, Princeton, USA, October 2023
- *Cryptography: from ancient art to modern science*, German Historical Institute Warsaw, December 2022
- *From BSM to BRM to BLM*, Ueli Maurer's Birthday Seminar, Monte Verità, Switzerland, June, 2022
- *Lower Bounds for Off-Chain Protocols: Exploring the Limits of Plasma*, Milan Theory Workshop, June 2022
- *Crypto in Crypto*, 17th SFI IT Academic Festival, Cracow, March 2022
- *Going off the blockchain*, 20th International School on Foundations of Security Analysis and Design (FOSAD), Bertinoro, Italy, August 2021
- *Lower Bounds for Off-Chain Protocols: Exploring the Limits of Plasma*, University of Lübeck (virtual seminar),

March 2021

- *Lower Bounds for Off-Chain Protocols: Exploring the Limits of Plasma*, Proofs, Consensus, and Decentralizing Society Reunion, UC Berkeley, USA, December 2020
- *Non-Atomic Payment Splitting in Channel Networks*, CS Virtual Colloquium at Purdue University, USA, December 2020
- *Theory of leakage – a look at the past two decades of research*, Conference on Cryptographic Hardware and Embedded Systems (CHES) 2020, September 2020
- *Non-Atomic Payment Splitting in Channel Networks*, Theory and Practice of Blockchains (Online Weekly Seminar Series), July 2020
- *Lower Bounds for Off-Chain Protocols: Exploring the Limits of Plasma*, The Stanford Blockchain Conference, Stanford University, February 2020
- *Position-Based Cryptography and Multiparty Communication Complexity*, Bay Area Crypto Day, UC Berkeley, Nov 2019
- *Introduction to Plasma*, Seminar at UC Berkeley, Nov 2019
- *Perun's Off-chain Channels*, Theory and Practice of Blockchains, Aarhus University, May 2019
- *Perun's Off-chain Channels*, Theory and Practice of Blockchains 2019, Aarhus University, Denmark, May 2019
- *Going off the chain*, Centre for Quantum Technologies, National University of Singapore, March 2019
- *Position-Based Cryptography and Multiparty Communication Complexity*, TCC 2017, Baltimore, USA, November 2017
- *State Channels over Cryptographic Currencies*, FACT Center Fast and Sound Cryptography Workshop, IDC Herzliya, Israel, September 2017
- *Proofs-of-space – an alternative for Proofs-of-work*, Theoretical Computer Science Forum 2017, Warsaw, Poland, July 2017
- *Private Circuits III: Hardware Trojan-Resilience via Testing Amplification*, COST Cryptoaction meeting, Amsterdam, The Netherlands, March 2017
- *Non-Malleable Codes*, MIMUW colloquium, Warsaw, Poland, January 2017
- *Private Circuits III: Hardware Trojan-Resilience via Testing Amplification*, ACM CCS 2016, Vienna, Austria, October 2016
- *Circuit compilers with O(1/log(n)) leakage rate*, Workshop on Mathematics of Information-Theoretic Cryptography Institute for Mathematical Sciences, National University of Singapore, September 2016
- *Modelling Side-Channel Leakage*, COST Cryptoaction meeting, Budapest, Hungary, April 2016
- *Proofs of Space*, Symposium on the Work of Ivan Damgård, Aarhus, Denmark, April 2016
- *Modelling Side-Channel Leakage*, Nexus of Information and Computation Theories, Henri Poincare Institute, Paris, France, March 2016
- *Non-Malleable Codes*, Theoretical Computer Science Forum, Warsaw, January 2015
- *Optimal Amplification of Noisy Leakages*, TCC 2016, Tel-Aviv, Israel, January 2016
- *Research Challenges in Cryptocurrencies*, SantaCrypt 2015, Prague, Czech Republic, December 2015
- *Modelling Side Channel Leakage*, MACIS, Berlin, Germany, November 2015
- *PoW-Based Distributed Cryptography with no Trusted Setup*, CRYPTO 2015, Santa Barbara, USA, August 2015
- *Proofs of Space*, CRYPTO 2015, Santa Barbara, USA, August 2015
- *Consensus in Peer-to-Peer Networks*, Club of the Foundation for Polish Science Scholars Symposium, Odolanów, Poland, May 2015
- *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
- *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
- *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
- *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*, Będlewo, 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.

- *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.

Panel discussion chair

- *Blockchain in a different way*, European Economic Congress, EEC, Katowice, Poland, April 2022,
- *What AI means for research assessment? – research funding organizations' perspective*, Fourth Polish-German Science Meeting, Warsaw, Poland, June 2024.

Lecturer

- University of Warsaw: *Cryptography I* (2011/12, 2012/13, 2016/17, 2017/18, 2018/19, 2019/20, 2020/21, 2021/22, 2022/23), *Financial Cryptography* (2014/15), *Information Theory* (2014/15), *Cryptography II* (2012/13,2013/14), *Practical Cryptographic Protocols* (2004/05), *Foundations of the Digital Signatures* (2004/05), *Cryptologic Protocol Theory* (2003/04), *Introduction to Applied Cryptography* (2002/03), *Cryptography, Blockchain, and Fintech (seminar)* (2021/22), *Cryptography (seminar)* (2013/14, 2014/15, 2015/16, 2016/17, 2017/18)
- *Sapienza* University of Rome: *Cryptography* (2007/08, 2008/09, 2009/10),
- Polish Academy of Sciences: *Introduction to Cryptography* (2004/05).

Short courses and tutorials

- *Introduction to Cryptocurrencies*, European Patent Office, Munich, Germany, December 2018
- *Introduction to Non-Malleable Codes*, ISC-IACR School on Cryptology, Indian Institute of Science, Bangalore, India, January 2018
- *Introduction to Cryptocurrencies*, Tokyo Institute of Technology, Tokyo, Japan, December 2017
- *Introduction to Cryptocurrencies* Workshop on Bitcoin, Introduction to Cryptocurrencies, Kfar Maccabiah, Ramat Gan, Israel, June, 2016
- *Introduction to Cryptocurrencies*, PhD Open, Warsaw, Poland, March 2016
- *Introduction to Cryptocurrencies*, Tutorial at the ACM CCS'15, Denver, USA, October 2015
- *Cryptography on Non-Trusted Machines* (short course for the PhD students University of Warsaw, Dec 2008 - Jan 2009)
- *Modern Cryptography* (short course for the PhD students, Bertinoro International Spring School, Italy, Mar 2009)
- *Methods of the Modern Theoretical Cryptography* (short course, Wrocław Information Technology Initiative, Wrocław, Poland, Sep 2009)

- *Multiparty Computations*, and *Bounded-Storage Model* (short courses, Nippon Telegraph and Telephone Corporation Laboratories, Japan, Jan 2004)

Graduated PhD students

- Francesco Davì (2012, *Sapienza* University of Rome),
- Tomasz Kazana (2013, University of Warsaw),
- Maciej Obremski (2013, University of Warsaw)
- Marcin Andrychowicz (2015, University of Warsaw),
- Michał Zając (2018, University of Warsaw).
- Maciej Skórski (2023, University of Warsaw).

Dissemination activities

Popular science talks

- *Crypto in Crypto*, 17th SFI IT Academic Festival, Cracow, March 2022
- *Layer 2 – protocols working on top of blockchains*, Cyber Week, Tel-Aviv University (virtual event), July 2021
- *Introduction to Blockchain*, a lecture for the staff of the Copernicus Science Centre, Warsaw, December 2020
- *Blockchain technology – hype vs. reality*, European Forum for Science, Research and Innovation, Dresden, June 2019
- *Crypto in Crypto*, Centre of New Technologies, University of Warsaw, May 2019
- *Cryptography: from ancient art to modern science*, 3rd PhD Student Conference, Nencki Institute of Experimental Biology, October 2018
- *What has the Blockchain ever done for us?*, Symposium "Can The World Run on Blockchains?", TU Darmstadt, Germany, September 2018
- *Basic Research in Cryptography*, From Poland with Science, Cambridge, March 2018
- *Perun – Virtual Payment Channel System*, Digital Money & Blockchain Forum, Warsaw, Poland, June 2017
- *Proofs-of-space – an alternative for Proofs-of-work*, Łazarski University, Warsaw, Poland, April 2017
- *How to order a murder using cryptocurrencies?*, "Technical Aspects of ICT Crime" Conference, Police Academy in Szczytno, Poland, May 2016
- *Technological weaknesses of Bitcoin*, Digital Money & Currency Forum, Warsaw, Poland, June 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
- *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
- *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
- *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.

Other

- Consulting on blockchain and cryptocurrencies for an exhibition *The future is today* at the *Copernicus Science Centre*, Warsaw, Poland.
- Several interviews about cryptography given to Polish media: *Gazeta Wyborcza*, *Polityka*, *Polska Zbrojna*, *TVN*, *TVP*, and others.

Consulting

Consulting on blockchain and cryptocurrencies for several blockchain companies in Germany, Poland, Singapore, and Switzerland.

Membership in professional societies

- *Association for Computing Machinery*,
- *Association of ERC Grantees*,
- *Association of the Foundation for Polish Science Scholars*,
- *International Association for Cryptologic Research (IACR)*,
- *Warsaw Scientific Society* (Polish: *Towarzystwo Naukowe Warszawskie*).

Languages

Polish: native
English: fluent
Italian: fluent
Russian: basic

Latest changes: September 2, 2024