Tal G. Malkin

Department of Computer Science
Columbia University
500 West 120th Street MC0401
New York, NY 10027

tal@cs.columbia.edu
http://www.cs.columbia.edu/∼tal

Education

Massachusetts Institute of Technology Cambridge, MA
Ph.D. in Computer Science, February 2000.
Thesis: "A Study of Secure Database Access and General Two-Party Computation".
Advisor: Prof. Shafi Goldwasser.

The Weizmann Institute of Science Rehovot, Israel
M.Sc. in Computer Science, January 1995.
Thesis: "Deductive Tableaux for Temporal Logic".
Advisor: Prof. Amir Pnueli.

Bar-Ilan University Ramat-Gan, Israel
B.S. *summa cum laude* in Mathematics and Computer Science, January 1993.

Employment

Columbia University, New York, NY **March 2020 – Current**
Professor, Department of Computer Science

Columbia University, New York, NY **July 2018 – December 2021**
Chair of Education Track, Columbia-IBM Center for Blockchain and Data Transparency

Columbia University, New York, NY **April 2016 – June 2018**
Co-chair, Cybersecurity Center, Data Science Institute (DSI)

Simons Institute for the Theory of Computing, Berkeley, CA
Visiting Scientist **Summer 2015, Spring 2023, Summer 2025**

Bar-Ilan University, Ramat-Gan, Israel **August 2013 – July 2014**
Visiting Research Professor

Columbia University, New York, NY **October 2012 – August 2013**
Inaugural Chair, Cybersecurity Center, Data Science Institute (DSI)

Columbia University, New York, NY **December 2009 – February 2020**
Associate Professor, Department of Computer Science

Microsoft Research, Redmond, CA **August 2009**
Consultant, Cryptography Group

Institute for Pure & Applied Mathematics (IPAM), UCLA
Los Angelos, CA **Fall 2006**
Visiting Scientist

Columbia University, New York, NY **January 2003 – November 2009**
Assistant Professor, Department of Computer Science

AT&T Labs, Florham Park, NJ **December 1999 – December 2002**
Senior Research Scientist, Secure Systems Research Department.

IBM T.J. Watson Research Center, Hawthorne, NY **Summer 1998**
Summer Intern, Cryptography Group, Networking Systems and Security Department.

News Datacom Research, Jerusalem, Israel **Summer 1996**
Summer Intern, Security Group.

Honors

- IACR Test-of-Time Award, Eurocrypt 2024 (for Eurocrypt 2009 paper)
- Amazon Faculty Research Award, 2024.
- IACR Fellow, 2020
- JP Morgan & Co. Faculty Research Award, 2020
- Columbia University Presidential Teaching Award, 2019
- PC Chair: CT-RSA 2008, ACNS 2015, TCC 2016, CCS 2017, CRYPTO 2021
- The Avanessians Diversity Award, Fu Foundation School of Engineering and Applied Science, Columbia University, 2013.
- Invited Keynote Speaker, Theory of Cryptography Conference (TCC), 2013.
- Google Faculty Research Award, 2010.
- Research Fellow, Columbia University Diversity Initiative, 2008.
- Distinguished Faculty Lecture, Department of Computer Science, University of Texas at Austin, 2005.
- IBM Faculty Partnership Award, 2004.
- NSF Faculty Early Career Development (CAREER) Award, 2004.
- The Knesset (Israeli Parliament) award to most promising undergraduate students in Israel, 1992.
- Graduated Summa Cum Laude, top 40 out of more than 7000 students, Bar-Ilan University, 1992
- The Knesset (Israeli Parliament) award to most promising undergraduate students in Israel, 1991.
- The Rachel and Reuben Jacobs Achievement Award for undergraduates, 1990.
- The Edith Wolfson Achievement Award for undergraduates, 1989.

Professional Service

Editorial:

- Advisory Board, TheoretiCS journal.
- Editorial Board, Theory of Computing Journal (ToC), 2004–2022.
- Associate editor, SIAM Journal of Computing (FOCS 2010 special issue).

Program Committee Chair:

- PC foundations area chair, 43rd Annual International Conference on the Theory and Applications of Crytpographic Techniques (EUROCRYPT 2024).
- PC co-chair, 41st Annual International Cryptology Conference (CRYPTO 2021).
- PC co-chair, 24th ACM Conference on Computer and Communications Security (CCS 2017).
- PC co-chair, 13th International Conference on the Theory of Cryptography (TCC 2016).
- PC chair, 13th International Conference on Applied Cryptography and Network Security (ACNS 2015).
- PC chair, the RSA Conference, Cryptographers' Track (CT-RSA 2008).

Steering and Workshop Organization:

- EATCS Presburger award committee chair, 2025
- EATCS Presburger award committee member, 2023 and 2024
- Steering committee chair, the Theory of Cryptography Conference (TCC), January 2020–current.
- Steering committee member, the Theory of Cryptography Conference (TCC), January 2017–current.
- Local organizer, IACR Real World Crytpo, 2017 and 2020.
- Organizing committee member, DIMACS/Simons Special Focus on Cryptography, September 2015–August 2017.
- Organizer, DIMACS Workshop on Complexity of Crytpographic Primitives and Assumptions, June 2017.
- Organizer, DIMACS/Columbia Data Science Institute Workshop on Cryptography for Big Data, December 2015.
- Steering committee member, the RSA Conference, Cryptographers' Track (CT-RSA), 2009, 2010, 2011.
- Organizing committee member, Applications of Internet Multi-Resolution Analysis to Cyber-Security Workshop, IPAM 2008.
- General chair, the 9th Annual workshop on Practice and Theory in Public Key Cryptography (PKC 2006).

Program Committee member:

- The 66th IEEE Symposium on Foundations of Computer Science (FOCS 2025).
- The 65th IEEE Symposium on Foundations of Computer Science (FOCS 2024).
- 13th Conference on Security and Cryptography for Network (SCN 2022).
- The 61st Annual IEEE Symposium on Foundations of Computer Science (FOCS 2020).
- The 39th Annual International Conference on the Theory and Applications of Crytpographic Techniques (EUROCRYPT 2020)

- Theory of Cryptoraphy Conference (TCC 2018).
- The 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2017)
- The 23rd ACM Conference on Computer and Communication Security (CCS 2016).
- The 6th Innovations in Theoretical Computer Science conference (ITCS 2015).
- The 32nd Annual IACR Crypto conference (Crypto 2012).
- Theory of Cryptography Conference (TCC 2012).
- The 16th International Conference on Financial Cryptography and Data Security (FC 2012).
- The 17th ACM Conference on Computer and Communication Security (CCS 2010).
- The 51st Annual IEEE Symposium on Foundations of Computer Science (FOCS 2010).
- The 10th Privacy Enhancing Technologies Symposium (PETS 2010).
- Security and Cryptography for Networks (SCN 2010).
- The RSA Conference, Cryptographers' track (CT-RSA 2010).
- The 9th Privacy Enhancing Technologies Symposium (PETS 2009).
- The 28th Annual IACR Crypto conference (Crypto 2008).
- The 26th Annual IACR Crypto conference (Crypto 2006).
- The 38th ACM Symposium on Theory of Computing (STOC 2006).
- The Theory of Cryptography Conference (TCC 2006).
- The 25th Annual IACR Crypto conference (Crypto 2005).
- The 14th USENIX Security Symposium (USENIX Security 2005).
- The RSA Conference, Cryptographers' Track (CT-RSA 2005).
- The Theory of Cryptography Conference (TCC 2005).
- The Workshop on Logical Foundations of an Adaptive Security Infrastructure (WOLFASI), affiliated with the Nineteenth Annual IEEE Symposium on Logic In Computer Science (LICS '04).
- The 24th Annual IACR Crypto Conference (Crypto 2004).
- The 36th ACM Symposium on Theory of Computing (STOC 2004).
- The Sixth International Workshop on Practice and Theory in Public Key Cryptography (PKC 2003).
- The Ninth Annual Workshop on Selected Areas in Cryptography (SAC 2002).

Other:

- Academic Program Review Committee for Boston University Department of Computer Science
- Reviewer of Doctoral dissertations for the ACM Dissertation Award
- NSF Panelist, Theory of Computation and Cyber Trust programs, multiple years

- Frequent referree for various professional journals including SIAM journal on Computing (SICOMP), SIAM journal on Discrete Mathematics, ACM Transactions on Information and System Security (TISSEC), ACM Transactions on Computer Systems (TOCS), Information Processing Letters (IPL), Journal of Cryptoglogy, Theory of Computing Systmes, Designs, Codes, and Cryptography, Discrete Applied Mathematics, and others.
- Co-organizer, IBM/NYU/Columbia Theory Day.
- Columbia Organizer, NY area Crypto Day
- Member of ACM, IEEE, IACR (International Association for Cryptologic Research).

Postdocs and visitors

- Satoshi Obana (Fall 2003, Spring 2004)
- Benoit Libert (Summer 2006, Winter 2007)
- François-Xavier Standaert (Fall 2004, Winter 2008, Spring 2011)
- Hoeteck Wee (October 2007-September 2008)
- Isamu Teranishi (January 2010 - December 2010)
- Geetha Jagannathan(May 2010 - July 2012)
- Yevgeniy Vahlis (July 2010 - July 2011)
- Dov Gordon, CIfellow (October 2010 - August 2012)
- Wesley George (January 2012 - May 2012)
- Kwangsu Lee (January 2012 - December 2012)
- Seung Geol Choi (August 2012 - July 2013)
- Benjamin Fisch (August 2013 - March 2014)
- Hoeteck Wee (March 2015 - September 2017)
- Fabrice Ben Hamouda (February 2018 - May 2018)
- Eran Tromer (July 2016 - June 2023)
- Alexander Hoover (September 2024 - May 2025)

Graduated PhD Students

- Ariel Elbaz, PhD 2009. *Thesis: "Round-Efficient Secure Computation, and Applications"*. Currently: CXO at Clay Sciences.
- Homin Lee, PhD 2009. *Thesis: "Complexity Measures and Computational Learning Theory"* (co-advised with Rocco Servedio). Currently: Data Scientist at Datadog.
- Andrew Wan, PhD 2010. *Thesis: "Learning, Cryptography, and the Average Case"* (co-advised with Rocco Servedio). Currently: Software Engineer at Snapchat.
- Seung Geol Choi, PhD 2010. *Thesis: "On Adaptive Security and Round Efficiency in Secure Multi-Party Computation"*. (co-advised with Moti Yung). Currently: Professor, Department of Computer Science, US Naval Academy.
- Dana (Glasner) Dachman-Soled, PhD 2011. *Thesis: "On the Black-Box Complexity of Basic Cryptographic Primitives and On Adaptive UC-Security"*. Currently: Tenured Associate Professor, Department of Electrical and Computer Engineering, University of Maryland.
- Mariana Raykova, PhD 2012. *Thesis: "Secure Computation for Heterogeneous Environments: How to Bring Multiparty Computation Closer to Practice?"* (co-advised with Steven Bellovin). Currently: Research Scientist, Google.

- Igor Carboni Oliveira, PhD 2015. *Thesis: "Unconditional Lower Bounds in Complexity Theory"* (co-advised with Rocco Servedio). Currently: Associate Professor and Royal Society University Research Fellow, Department of Computer Science, University of Warwick, UK.
- Fernando Krell, PhD 2016. *Thesis: "Secure Computation Towards Practical Applications"* Currently: VP Engineering, Espresso Systems.
- George Argyros, PhD 2019. *Thesis: "Symbolic Model Learning: New Algorithms and Applications"* (co-advised with Angelos Keromytis). Currently: Senior Applied Scientist and Applied Science Manager, Amazon Web Services (AWS Security).
- Lucas Kowalczyk, PhD 2019. *Thesis: "Attribute-Based Encryption for Boolean Formulas"* (co-advised with Allison Bishop). Currently: Head of Quantitative Research at IEX.
- Ghada Almashaqbeh, PhD 2019. *Thesis: "CacheCash: A Cryptocurrency-based Decentralized Content Delivery Network"* (co-advised with Allison Bishop). Currently: Assistant Professor, Department of Computer Science and Engineering, University of Connecticut.
- M. Marshall Ball, PhD 2020. *Thesis: "On Resilience to Computable Tampering"*. Currently: Assistant Professor, Department of Computer Science, Courant Institute of Mathematical Sciences, New York University.
- Chengyu Lin, PhD 2023. *Thesis: "Ring-LWE: Enhanced Foundations and Applications"*. Currently: Cryptography Engineer, Espresso Systems.
- Daniel Mitropolsky, PhD 2024. Thesis: "Towards a Computational Theory of the Brain: the Simplest Neural Models, and a Hypothesis for Language". Currently: Postdoctoral Fellow, McGovern Institute for Brain Research, MIT, Postdoctoral Fellow, Harvard University Center for Mathematical Sciences and Applications, and Visiting Assistant Professor, Tufts University.

Current PhD Students

- Miranda Christ, fifth year student (co-advised with Mihalis Yannakakis).
- Kevin Yeo, third year student (co-advised with Josh Alman and Rachel Cummings).
- Yizhi Huang, second year student (co-advisded with Josh Alman and Rocco Servedio).
- Tianqi Yang, second year student (co-advisded with Toni Pitassi and Rocco Servedio).
- Leo Orshansky, first year student (co-advised with Henry Yuen).

Other PhD Thesis Committee

- Hector Rosario *"Steganography: Historical Development and Applications at the Undergraduate Level"*, Teachers College, May 2003.
- Enav Weinreb *"Secret Sharing, Span Programs, and Secure Computation: Complexity Issues and Cryptographic Applications"*, Department of Computer Science, Ben-Gurion University, July 2007.
- Sharon Goldberg *"Towards Securing Interdomain Routing on the Internet"*, Department of Computer Science, Princeton University, July 2009.
- Elli Androulaki *"A Privacy Preserving ECommerce Oriented Identity Management System"*, Department of Computer Science, Columbia University, May 2010.

- Ilias Diakonikolas *"Approximation of Multiobjective Optimization Problems"*, Department of Computer Science, Columbia University, September 2010.
- Daniel Wichs *"Cryptographic Resilience to Continual Information Leakage"*, Department of Computer Science, Courant Institute of Mathematical Sciences, New York University, September 2011.
- Joel Alwen, *"Collusion Preserving Computation"*, Department of Computer Science, Courant Institute of Mathematical Sciences, New York University, September 2011.
- Malek Ben Salem, *"Towards Effective Masquerade Attack Detection"*, Department of Computer Science, Columbia University, October 2011.
- Mehvish Poshni, *"Genus Distributions of Graphs Constructed Through Amalgamations"*, Department of Computer Science, Columbia University, November 2011.
- Sigurd Meldgaard, *"Unconditionally Secure Protocols"*, Department of Computer Science, Aarhus University, Denmark, April 2013.
- Swapneel Sheth, *"Social Computing"*, Department of Computer Science, Columbia University, December 2013.
- Aristeidis Tentes, *"Computational Complexity Implications of Secure Coin Flipping Protocols"*, Department of Computer Science, New York University, September 2014.
- Yuan Kang, *"Combining Programs to Enhance Security Software"*, Department of Computer Science, Columbia University, February 2018.
- Mukul Kulkarni, *"Extending the Applicability of Non-Malleable Codes"*, Department of Electrical and Computer Engineering, University of Maryland, College Park, MD, July 2019.
- Pierre Meyer, *"Sublinear-communication secure multiparty computation"*, Université Paris Cité, Paris, France and Reichman University, Herzliya, Israel, September 2023.
- Guy Eichler, *"System-Level Design in the Era of Brain-Computer Interfaces"*, Department of Computer Science, Columbia University, February 2025.

Other Students

- PHD Candidacy Committee (other than advisees): Debbie Cook, Spyridon Antonakopoulos, Ilias Diakonikolas, Elli Androulaki, Swapneel Sheth, Mehvish Poshni, Binh Vo, Clement Cannone, Timothy Sun, Yuan Kang, Guy Eichler, Yuval Efron, John Bostanci.
- MSc Thesis Supervision: Ryan Moriarty, Devang Thakkar, Kevin Yeo, Zeyu Thomas Liu.
- MSc Thesis Committee Member: Joseph Sherrick, Hunning Dai, Harish Karthikeyan, Pierre Tholoniat, Yunhao Wang, Lior Attias.
- Undergrad Thesis Reader: Julia Gron (Barnard College, 2016)
- Independent study (research project class) supervisor: George Philip Atzemoglou (Spring 2003), Andrew Wan (Fall 2003), Bhargav Bhatt, Noel Codella (Spring 2004), Marzia Niccolai, Nikolai Yakovenko (Fall 2004), Catherine Lennon *(CRA Honorable Mention)*, Matthew Raibert, Nikolai Yakovenko (Spring 2005), Rajesh Venkataraman (Fall 2007). Noah Youngs (Fall 2007). Krzysztof Choromanski (Spring 2010 - Spring 2011). Christian Moscardi, Zachary Newman (Spring 2012). Steven Goldfeder (Fall 2012). Yi-Hsiu Chen (Spring 2013). Marshall Ball (Spring 2015). Hosanna Fuller (Fall 2015). Benjamin Kuykendall, Aubrey Alston (Fall 2016).

Benjamin Kuykendall, Jihaui Liu, Aubrey Alston, Kailash Meiyappan (Spring 2017), Jiahui Liu (Fall 2017), Benjamin Kuykendall (Spring 2018), Seungwook Han, Daniel Jaroslawicz, Abhishek Shah (Fall 2018), Seungwook Han, Alex Nicita, Hsin Pei Toh (Spring 2019) Lalita Devadas *(CRA Honorable Mention)*, Eli Goldin, Garrison Grogan, Alex Nicita (Fall 2019), Garrison Grogan (Fall 2020, Spring 2021),Zeyu Thomas Liu (Fall 2021), Owen Keith (Spring 2022), Andy Arditi (Summer 2022), Yunhao Wang, Alexander Lindenbaum, Walter McKelvie *(CRA Honorable Mention)*, Ashwin Padaki (Fall 2022), Sang Hun Han, Mark Chen, Kashvi Gupta, Jiaqian Li *(CRA Honorable Mention)* (Fall 2024), Maria Catarina Coelho (Spring 2025).

- PhD Students Mentored through Women In Theory program (2008-2010): Shanshan Duan (UCSD), Huijia (Rachel) Lin (Cornell).
- PhD Students Supervised while at AT&T Research (2000-2003): Yael Gertner (UPENN), Lea Kissner (UC Berkeley/CMU), Kobbi Nissim (Weizmann Institute of Science).

Books Edited

[B1] Advances in Cryptology – CRYPTO 2021. Tal Malkin, Chris Peikert (editors). Proceedings of the 41st Annual International Cryptology Conference (CRYPTO), Lecture Notes in Computer Science (LCNS) Vols 12825, 12826, 12827, 12828, Springer 2021.

[B2] Computer and Communications Security – CCS 2017. Bhavani M. Thuraisingham, David Evans, Tal Malkin, Dongyan Xu (editors). Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS), ACM 2017.

[B3] Theory of Cryptography - TCC 2016. Eyal Kushilevitz, Tal Malkin (editors). Proceedings of the 13th International Conference on the Theory of Cryptography (TCC 2016-A), Lecture Notes in Computer Science (LNCS) Vols 9562, 9563, Springer, 2016.

[B4] Applied Cryptography and Network Security - ACNS 2015. Tal Malkin, Vladimir Kolesnikov, Allison Bishop Lewko, Michalis Polychronakis (editors). Proceedings of the 13th International Conference on Applied Cryptography and Network Security (ACNS), Lecture Notes in Computer Science (LNCS) Vol 9092, Springer, 2015.

[B5] Lap Chi Lau, Tal Malkin, Ryan O'Donnell, Luca Trevisan. Special Section on the Fifty-First Annual IEEE Symposium on Foundations of Computer Science (FOCS 2010). *SIAM Journal on Computing*, 43(1), 2014.

[B6] Topics in Cryptology - CT-RSA 2008. Tal Malkin (editor). Proceedings of the Cryptographers' Track at the RSA Conference (CT-RSA), Lecture Notes in Computer Science (LNCS) Vol 4964, Springer, 2008.

[B7] Public Key Cryptography - PKC 2006. Moti Yung, Yevgeniy Dodis, Aggelos Kiayias, Tal Malkin (editors). Proceedings of the 9th International Conference on Theory and Practice of Public Key Cryptography (PKC), Lecture Notes in Computer Science (LNCS) Vol 3958, Springer, 2006.

[B8] Shai Avidan, Ariel Elbaz, Tal Malkin, Ryan Moriarty. Oblivious Image Matching. Invited book chapter to "Protecting Privacy in Video Surveillance", Andrew Senior (editor). Springer, 2009. ISBN: 978-1-84882-300-6 2009

Journal [*] ***Publications***

[J1] Marshall Ball, Elette Boyle Ran Cohen, Lisa Kohl, Tal Malkin, Pierre Meyer, Tal Moran. Topology-Hiding Communication from Minimal Assumptions. *Journal of Cryptology*, 36(4), 2023.

[J2] Ghada Almashaqbeh, Fabrice Benhamouda, Seungwook Han, Daniel Jaroslawicz, Tal malkin, Alex Nicita, Tal Rabin, Abhishek Shah, Eran Tromer. Gage MPC: Bypassing Residual function Leakage for Non-Interactive MPC. *Proceedings on Privacy Preserving Technologies (PoPETS)*, 2021(4).

[J3] Seung Geol Choi, Dana Dachman-Soled, Tal Malkin, Hoeteck Wee. Improved, Black-Box, Non-Malleable Encryption from Semantic Security. *Designs, Codes, and Cryptography*, 86(3), 2018.

[J4] Seung Geol Choi, Dana Dachman-Soled, Tal Malkin, Hoeteck Wee. A Black-Box Construction of Non-Malleable Encryption from Semantically Secure Encryption. *Journal of Cryptology*, 31(1), 2018.

[J5] Melissa Chase, Alexander Healy, Anna Lysyanskaya, Tal Malkin, Leonid Reyzin. Mercurial Commitments with Applications to Zero-Knowledge Sets. *Journal of Cryptology*, 26(2), 2013.

[J6] Dana Dachman-Soled, Tal Malkin, Mariana Raykova, Moti Yung. Efficient Robust Private Set Intersection. In *International Journal of Applied Cryptography (IJACT)*, 2(3), 2012.

[J7] Mariana Raykova, Ang Cui, Binh Vo, Bin Liu, Tal Malkin, Steven Bellovin, Salvatore Stolfo. Usable, Secure, Private Search. *IEEE Security & Privacy*, 10(5), 2012.

[J8] Amos Beimel, Tal Malkin, Kobbi Nissim, Enav Weinreb. How Should We Solve Search Problems Privately? *Journal of Cryptology*, 23(2), 2010.

[J9] Dana Dachman-Soled, Homin K. Lee, Tal Malkin, Rocco Servedio, Andrew Wan, Hoeteck Wee. Optimal Cryptographic Hardness of Learning Monotone Functions. *Theory of Computing*, 5(1), 2009.

[J10] Yuval Ishai, Tal Malkin, Martin Strauss, Rebecca Wright. Private Multiparty Sampling and Approximation of Vector Combinations. *Theoretical Computer Science*, 410(18), 2009. (invited submission, special issue for best ICALP '07 papers).

[J11] Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, Avi Rubin. Annonymity in Wireless Broadcast Networks. *International Journal of Network Security (IJNS)*, 8(1), 2009.

[J12] Jon Feldman, Tal Malkin, Cliff Stein, Rocco Servedio, Martin Wainwright. LP Decoding Corrects a Constant Fraction of Error. *IEEE Transactions on Information Theory*, 53(1), 2007.

[J13] Joan Feigenbaum, Yuval Ishai, Tal Malkin, Kobbi Nissim, Martin Strauss, Rebecca Wright. Secure Multiparty Computation of Approximations. *ACM Transactions on Algorithms*, 2005.

[J14] Ran Canetti, Ivan Damgard, Stefan Dziembowski, Yuval Ishai, Tal Malkin. On Adaptive vs. Non-Adaptive Security of Multiparty Protocols. *Journal of Cryptology*, 17(3), pages 153–207, June 2004.

[*] Students and postdocs are underlined. Authors in theory and cryptography venues are in alphabetical order, and authors in security venues have students first.

[J15] Amos Beimel, Yuval Ishai, Tal Malkin. Reducing the Servers Computation in Private Information Retrieval: PIR with Preprocessing. *Journal of Cryptology*, 17(2), pages 125–151, March 2004.

[J16] Yael Gertner, Yuval Ishai, Eyal Kushilevitz, Tal Malkin. Protecting Data Privacy in Private Information Retrieval Schemes. *Journal of Computer and System Sciences (JCSS),* 60(3), pages 592–629, June 2000 (invited submission, special issue for best STOC '98 papers).

Refereed Conferences [*]

[P1] Amos Beimel, Tal Malkin, Noam Mazor. Structural Lower Bounds on Black-Box Constructions of Pseudorandom Functions. In *Proc. of the 44th Annual IACR Crypto Conference (CRYPTO '24),* August 2024.

[P2] Miranda Christ, Kevin Choi, Walter McKelvie, Joseph Bonneau, Tal Malkin. Accountable Secret Leader Election. In *Proc. of the 6th Conference on Advances in Financial Technologies (AFT '24),* September 2024.

[P3] Chengyu Lin, Zeyu Liu, Tal Malkin. XSPIR: Efficient Symmetrically Private Information Retrieval from Ring-LWE. In *Proc. of the 27th European Symposium on Research in Computer Science (ESORICS '22),* Copenhagen, Denmark, September 2022.

[P4] Ghada Almashaqbeh, Ran Canetti, Yaniv Erlich, Jonathan Gershoni, Tal Malkin, Itsik Pe'er, Anna Roitburd-Berman, Eran Tromer. Unclonable Polymers and Their Cryptographic Applications. In *Proc. of the 41st Annual IACR Eurocrypt conference (EUROCRYPT '22),* Trondheim, Norway, June 2022.

[P5] Marshall Ball, Oded Goldreich, Tal Malkin. Randomness Extraction from Somewhat Dependent Sources. In *Proc. of the 13th Annual Innovations in Theoretical Computer Science Conference (ITCS '22),* January 2022.

[P6] Marshall Ball, Alper Cakan, Tal Malkin. Linear Threshold Secret-Sharing with Binary Reconstruction. In *Proc. of Information-Theoretic Cryptography Conference (ITC '21),* July 2021.

[P7] Marshall Ball, Oded Goldreich, Tal Malkin. Communication Complexity with Defective Randomness. In *Proc. of Computational Complexity Conference (CCC '21),* July 2021.

[P8] Marhsall Ball, Eshan Chattopadhyay, Jyun-Jie Liao, Tal Malkin, Li-Yang Tan. Non-Malleability Against Polynomial Tampering. In *Proc. of the 40th Annual IACR Crypto Conference (CRYPTO '20),* August 2020.

[P9] Marshall Ball, Elette Boyle, Ran Cohen, Lisa Kohl, Tal Malkin, Pierre Meyer, Tal Moran. Topology-Hiding Communication from Minimal Assumptions. In *Proc. of the Theory of Cryptography Conference (TCC '20),* November 2020.

[P10] Kasper Green Larsen, Tal Malkin, Omri Weinstein, Kevin Yeo. Lower Bounds for Oblivious Near-Neighbor Search. In *Proc. of the ACM-SIAM Symposium on Discrete Algorithms (SODA '20),* Salt Lake City, UT, January 2020.

[P11] Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, Tal Malkin. Limits to Non-Malleability. In *Proc. of the 11th Annual Innovations in Theoretical Computer Science Conference (ITCS '20),* Seattle, WA, January 2020.

[*] Students and postdocs are underlined. Authors in theory and cryptography venues are in alphabetical order, and authors in security venues have students first.

[P12] Marshall Ball, Justin Holmgren, Yuval Ishai, Tianren Liu, Tal Malkin On the Complexity of Decomposable Randomized Encodings, or: How Friendly Can a Garbling-Friendly PRF be? In *Proc. of the 11th Annual Innovations in Theoretical Computer Science Conference (ITCS '20),* Seattle, WA, January 2020.

[P13] James Bartusek, Brent Carmer, Abhishek Jain, Zhengzhong Jin, Tancrède Lepoint, Fermi Ma, Tal Malkin, Alex J. Malozemoff, Mariana Raykova. Public-Key Function Private Hidden Vector Encryption (and More). In *Proc. of the 25th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT '19),* Kobe, Japan, December 2019.

[P14] Marshall Ball, Elette Boyle, Ran Cohen, Tal Malkin, Tal Moran. Is Information-Theoretic Topology-Hiding Computation Possible? In *Proc. of the Theory of Cryptography Conference (TCC '19),* Nuremberg, Germany, December 2019.

[P15] Marshall Ball, Brent Carmer, Tal Malkin, Mike Rosulek, Nichole Schimanski. Garbled Neural Networks are Practical. In *Privacy Preserving Machine Learning, CCS '19 Workshop (PPML),* London, UK, November 2019, and in *Privacy Preserving Machine Learning, CRYPTO '19 Workshop,* Santa Barbara, CA, August 2019.

[P16] Allison Bishop, Lucas Kowalczyk, Tal Malkin, Valerio Pastro, Mariana Raykova, Kevin Shi. In Pursuit of Clarity In Obfuscation. Conference for Failed Approaches and Insightful Losses in Cryptology (CFAIL '19), New York, NY, June 2019.

[P17] Alexandr Andoni, Tal Malkin, Negev Shekel Nosatzki. Two Party Distribution Testing: Communication and Security. In *Proc. of the 46th International Colloquium on Automata, Languages, and Programming (ICALP 2019),* Patras, Greece, July 2019.

[P18] Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, Huijia Lin, Tal Malkin. Non-Malleable Codes Against Bounded Polynomial Time Tampering. In *Proc. of the 38th Annual IACR Eurocrypt conference (EUROCRYPT '19),* Darmstadt, Germany, May 2019.

[P19] Alexandr Andoni, Tal Malkin, Negev Shekel Nosatzki. Secure Two Party Distribution Testing. In *Privacy Preserving Machine Learning (PPML), NeurIPS '18 Workshop,* Montreal, Canada, December 2018.

[P20] Lucas Kowalczyk, Jiahui Liu, Tal Malkin, Kailash Meiyappan. Mitigating the One-Use Restriction in Attribute-Based Encryption. In *Proc. of the 21st International Conference on Information Security and Cryptography (ICISC '18),* Seoul, South Korea, November 2018.

[P21] Marshall Ball, Dana Dachman-Soled, Siyao Guo, Tal Malkin, Li-Yang Tan. Non-Malleable Codes for Small-Depth Circuits. In *Proc. of the 59th IEEE Annual Symposium on Foundations of Computer Science (FOCS '18),* Paris, France, October 2018.

[P22] Yuan Kang, Chengyu Lin, Tal Malkin, Mariana Raykova. Obfuscation from Polynomial Hardness: Beyond Decomposable Obfuscation. In *Proc. of the 11th International Conference on Security and Cryptography for Networks (SCN '18),* Amalfi, Italy, September 2018.

[P23] Lucas Kowalczyk, Tal Malkin, Jonathan Ullman, Daniel Wichs. Hardness of Non-Interactive Differential Privacy from One-Way Functions. In *Proc. of the 38th Annual IACR Crypto Conference (CRYPTO '18),* Santa Barbara, CA, August 2018.

[P24] Allison Bishop, Lucas Kowalczyk, Tal Malkin, Valerio Pastro, Mariana Raykova, Kevin Shi. A Simple Obfuscation Scheme for Pattern-Matching with Wildcards. In *Proc. of the 38th Annual IACR Crypto Conference (CRYPTO '18),* Santa Barbara, CA, August 2018.

[P25] Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, Tal Malkin. Non-Malleable Codes from Average-Case Hardness: AC0, Decision Trees, and Streaming Space-Bounded Tampering. In *Proc. of the 36th Annual IACR Eurocrypt conference (EUROCRYPT '18),* Tel Aviv, Israel, May 2018.

[P26] Marshall Ball, Elette Boyle, Tal Malkin, Tal Moran. Exploring the Boundaries of Topology-Hiding Computation. In *Proc. of the 36th Annual IACR Eurocrypt conference (EUROCRYPT '18),* Tel Aviv, Israel, May 2018.

[P27] Lucas Kowalczyk, Tal Malkin, Jonathan Ullman, Mark Zhandry. Strong Hardness of Privacy from Weak Traitor Tracing. In *Proc. of the Theory of Cryptography Conference (TCC '16B),* Beijing, China, November 2016.

[P28] Marshall Ball, Tal Malkin, Mike Rosulek. Garbling Gadgets for Boolean and Arithmetic Circuits. In *Proc. of the 23rd ACM Conference on Computer and Communications Security (CCS '16),* Vienna, Austria, October 2016.

[P29] Marshall Ball, Dana Dachman-Soled, Mukul Kulkarni, Tal Malkin. Non-malleable Codes for Bounded Depth, Bounded Fan-in Circuits. In *Proc. of the 35th Annual IACR Eurocrypt conference (EUROCRYPT '16),* Vienna, Austria, May 2016.

[P30] Ben A. Fisch, Binh Vo, Fernando Krell, Abishek Kumarasubramanian, Vladimir Kolesnikov, Tal Malkin, Steven Bellovin. Malicious Client Security in Blind Seer: A Scalable Private DBMS. In *Proc. of the 36th IEEE Symposium on Security and Privacy (Oakland '15),* San Jose, CA, May 2015.

[P31] Siyao Guo, Tal Malkin, Igor Carboni Oliveira, Alon Rosen. The Power of Negations in Cryptography. In *Proc. of the Theory of Cryptography Conference (TCC '15),* Warsaw, Poland, March 2015.

[P32] Isamu Teranishi, Moti Yung, Tal Malkin. Order-Preserving Encryption Secure Beyond One-Wayness. In *Proc. of the 20th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT '14),* Kaoshiung, Taiwan, December 2014.

[P33] Vasilis Pappas, Fernando Krell, Binh Vo, Vladimir Kolesnikov, Tal Malkin, Seung Geol Choi, Wesley George, Angelos Keromytis, Steven Bellovin. Blind Seer: A Scalable Private DBMS. In *Proc. of the 35th IEEE Symposium on Security and Privacy (Oakland '14),* San Jose, CA, May 2014.

[P34] Dana Dachman-Soled, Mohammad Mahmoody, Tal Malkin. Can Optimally-Fair Coin Tossing Be Based on One-Way Functions? In *Proc. of the Theory of Cryptography Conference (TCC '14),* San Diego, CA, February 2014.

[P35] Dana Dachman-Soled, Tal Malkin, Mariana Raykova, Muthuramakrishnan Venkitasubramaniam. Adaptive and Concurrent Secure Computation from New Adaptive, Non-malleable Commitments. In *Proc. of the 19th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT '13),* Bangalore, India, December 2013.

[P36] Dov Gordon, Tal Malkin, Mike Rosulek, Hoeteck Wee. Multi-Party Computation of Polynomials and Branching Programs without Simultaneous Interaction. In

Proc. of the 32nd Annual IACR Eurocrypt conference (EUROCRYPT '13), Athens, Greece, May 2013.

[P37] Tal Malkin. Secure Computation for Big Data. In *Proc. of the Theory of Cryptography Conference (TCC '13),* Tokyo, Japan , March 2013. Invited talk.

[P38] Dov Gordon, Jonathan Katz, Vladimir Kolesnikov, Fernando Krell, Tal Malkin, Mariana Raykova, Yevgeniy Vahlis. Secure Two Party Computation in Sublinear (Amortized) Time. In *Proc. of the 19th ACM Conference on Computer and Communications Security (CCS '12),* Raleigh, NC, October 2012.

[P39] Krzysztof Choromanski, Tal Malkin. The Power of the Dinur-Nissim Algorithm: Breaking Privacy of Statistical and Graph Databases. In *Proc. of the Symposium on Principles of Database Systems (PODS '12),* Scottsdale, Arizona, May 2012.

[P40] Dana Dachman-Soled, Rosario Gennaro, Hugo Krawczyk, Tal Malkin. Computational Extractors and Pseudorandomness. In *Proc. of the Theory of Cryptography Conference (TCC '12),* Taormina, Italy , March 2012.

[P41] Seung Geol Choi, Kyung-Wook Hwang, Jonathan Katz, Tal Malkin, Dan Rubenstein. Secure Multi-Party Computation of Boolean Circuits with Applications to Privacy in On-Line Marketplaces. In *Proc. of the Cryptographers' Track at the RSA Conference (CT-RSA '12),* San Francisco, CA, February 2012.

[P42] Seung Geol Choi, Aggelos Kiayias, Tal Malkin. BiTR: Built-in Tamper Resistance. In *Proc. of the 17th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT '11),* Seoul, South Korea, December 2011.

[P43] Vasilis Pappas, Mariana Raykova, Binh Vo, Steven Bellovin, Tal Malkin. Private Search in the Real World. In *Proc. of the Annual Computer Security Applications Conference (ACSAC '11),* Orlando, Florida, December 2011.

[P44] Dana Dachman-Soled, Tal Malkin, Mariana Raykova, Moti Yung. Secure Efficient Multiparty Computing of Multivariate Polynomials and Applications. In *Proc. of the International Conference on Applied Cryptography and Network Security (ACNS '11),* Nerja (Malaga), Spain, June 2011.

[P45] Tal Malkin, Isamu Teranishi, Moti Yung. Efficient Circuit-Size Independent Public Key Encryption with KDM Security. In *Proc. of the 30th Annual IACR Eurocrypt conference (EUROCRYPT '11),* Tallinn, Estonia, May 2011.

[P46] Dana Dachman-Soled, Yehuda Lindell, Mohammad Mahmoody, Tal Malkin. On the Black-Box Complexity of Optimally-Fair Coin Tossing. In *Proc. of the Theory of Cryptography Conference (TCC '11),* Providence, RI, March 2011.

[P47] Tal Malkin, Isamu Teranishi, Yevgeniy Vahlis, Moti Yung. Signatures Resilient to Continual Leakage on Memory and Computation. In *Proc. of the Theory of Cryptography Conference (TCC '11),* Providence, RI, March 2011.

[P48] Dov Gordon, Jonathan Katz, Vladimir Kolesnikov, Tal Malkin, Mariana Raykova, Yevgeniy Vahlis. Amortized Sublinear Secure Multi Party Computation. Workshop on Cryptography and Security in the Clouds, Zurich, Switzerland, March 2011.

[P49] Tal Malkin, Isamu Teranishi, Moti Yung. Key Dependent Message Security: Recent Results and Applications. In *Proc. of 1st ACM Conference on Data and*

Applications Security (CODASPY '11), San Antonio, TX, Feb 2011. Invited talk by Moti Yung.

[P50] Vasilis Pappas, Mariana Raykova, Binh Vo, Steven Bellovin, Tal Malkin. Trade-offs in Private Search. Poster presentation at *IEEE Symposium on Security and Privacy,* Oakland, CA, May 2010.

[P51] Seung Geol Choi, Dana Dachman-Soled, Tal Malkin, Hoeteck Wee. Improved Non-Committing Encryption with Applications to Adaptively Secure Protocols. In *Proc. of the 15th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT '09),* Tokyo, Japan, December 2009.

[P52] Seung Geol Choi, Ariel Elbaz, Tal Malkin, Moti Yung. Secure Multi-party Computation Minimizing Online Rounds. In *Proc. of the 15th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT '09),* Tokyo, Japan, December 2009.

[P53] Mariana Raykova, Binh Vo, Steven Bellovin, Tal Malkin. Secure Anonymous Database Search. In *Proc. of the ACM Cloud Computing Security Workshop (CCSW '09), in conjunction with ACM CCS '09*, Chicago, IL, November 2009.

[P54] Dana Dachman-Soled, Tal Malkin, Mariana Raykova, Moti Yung. Efficient Robust Private Set Intersection. In *Proc. of the International Conference on Applied Cryptography and Network Security (ACNS '09),* Paris-Rocquencourt, France, June 2009.

[P55] François-Xavier Standaert, Tal Malkin, Moti Yung. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks. In *Proc. of the 28th Annual IACR Eurocrypt conference (EUROCRYPT '09),* Cologne, Germany, April 2009. **EUROCRYPT Test-of-Time Award, 2024**

[P56] Seung Geol Choi, Dana Dachman-Soled, Tal Malkin, Hoeteck Wee. Simple, Black-Box Constructions of Adaptively Secure Protocols. In *Proc. of the Theory of Cryptography Conference (TCC '09),* San-Francisco, CA, March 2009.

[P57] Shai Avidan, Ariel Elbaz, Tal Malkin. Privacy Preserving Pattern Classification. In *Proc. of IEEE International Conference on Image Processing (ICIP '08)*, San Diego, CA, October 2008.

[P58] François-Xavier Standaert, Tal Malkin, Moti Yung. Does Physical Security of Cryptographic Devices Need a Formal Study? In *Proc. of the International Conference on Information Theoretic Security (ICITS '08)*, Calgary, Canada, August 2008. Invited talk by Moti Yung.

[P59] Elli Androulaki, Seung Geol Choi, Steven Bellovin, Tal Malkin. Reputation Systems for Anonymous Networks. In *Proc. of the 8th Privacy Enhancing Technologies Symposium (PETS '08),* Leuven, Belgium, July 2008.

[P60] Dana Dachman-Soled, Homin K. Lee, Tal Malkin, Rocco Servedio, Andrew Wan, Hoeteck Wee. Optimal Cryptographic Hardness of Learning Monotone Functions. In *Proc. of the 35th International Colloquium on Automata, Languages and Programming (ICALP '08),* Reykjavik, Iceland, July 2008.

[P61] Seung Geol Choi, Dana Dachman-Soled, Tal Malkin, Hoeteck Wee. Black-Box Construction of a Non-Malleable Encryption Scheme from Any Semantically Secure

One. In *Proc. of the Theory of Cryptography Conference (TCC '08),* New York, NY, March 2008.

[P62] Christophe Petit, François-Xavier Standaert, Olivier Pereira, Tal Malkin, Moti Yung. A Block Cipher based Pseudo Random Number Generator Secure Against Side-Channel Key Recovery. In *Proc. of the ACM Symposium on Information, Computer and Communication Security (ASIACCS '08),* Tokyo, Japan, March 2008.

[P63] Seung Geol Choi, Ariel Elbaz, Ari Juels, Tal Malkin, Moti Yung. Two-Party Computing with Encrypted Data. In *Proc. of the 13th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT '07),* Sarawak, Malaysia, December 2007.

[P64] Homin K. Lee, Tal Malkin, Erich Nahum. Cryptographic Strength of SSL/TLS Servers: Current and Recent Practices. In *Proc. of ACM SIGCOMM Internet Measurement Conference (IMC '07),* San Diego, CA, October 2007.

[P65] Amos Beimel, Tal Malkin, Kobbi Nissim, Enav Weinreb. How Should We Solve Search Problems Privately? In *Proc. of the 27th Annual IACR Crypto Conference (CRYPTO '07),* Santa Barbara, CA, August 2007.

[P66] Yuval Ishai, Tal Malkin, Martin Strauss, Rebecca Wright. Private Multiparty Sampling and Approximation of Vector Combinations. In *Proc. of the 34th International Colloquium on Automata, Languages and Programming (ICALP '07),* Wroclaw, Poland, July 2007.

[P67] Yael Gertner, Tal Malkin, Steven Myers. Towards a Separation of Semantic and CCA Security for Public Key Encryption. In *Proc. of the Theory of Cryptography Conference (TCC '07)*, Amsterdam, The Netherlands, February 2007.

[P68] Tal Malkin, Ryan Moriarty, Nikolai Yakovenko. Environmental Security From Number Theoretic Assumptions. In *Proc. of the Theory of Cryptography Conference (TCC '06)*, New York, NY, March 2006.

[P69] Tal Malkin, François-Xavier Standaert, Moti Yung. A Comparative Cost/Security Analysis of Fault Attack Countermeasures. In *Proc. of Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC '05)*, associated with CHES 2005, Edinburgh, Scotland, September 2005. Also included in the best papers of FDTC 2005/2006 volume, Lecture Notes in Computer Science (LNCS) Vol 4236, pages 159–172, Springer, September 2006.

[P70] Melissa Chase, Alexander Healy, Anna Lysyanskaya, Tal Malkin, Leonid Reyzin. Mercurial Commitments with Applications to Zero-Knowledge Sets. In *Proc. of the 24th Annual IACR Eurocrypt conference (EUROCRYPT '05),* Aarhus, Denmark, May 2005.

[P71] Jon Feldman, Tal Malkin, Cliff Stein, Rocco Servedio. On the Capacity of Secure Network Coding. In *Proc. 42nd Annual Allerton Conference on Communication, Control, and Computing (Allerton 2004),* Monticello, IL, September 2004 (invited paper).

[P72] Jon Feldman, Tal Malkin, Cliff Stein, Rocco Servedio, Martin Wainwright. LP Decoding Corrects a Constant Fraction of Error. In *Proc. IEEE International Symposium on Information Theory (ISIT '04)*, Chicago, IL, June 2004.

[P73] Tal Malkin, Satoshi Obana, Moti Yung. The Hierarchy of Key Evolving Signatures and a Characterization of Proxy Signatures. In *Proc. of the 22th Annual IACR Eurocrypt conference (EUROCRYPT '04),* Interlaken, Switzerland, May 2004.

[P74] Amos Beimel, Tal Malkin. A Quantitative Approach to Reductions in Secure Computation. In *Proc. of the Theory of Cryptography Conference (TCC '04)*, Cambridge, MA, February 2004. A full version is available at the Electronic Colloquium on Computational Complexity (ECCC) volume 86, 2003.

[P75] Rosario Gennaro, Anna Lysyanskaya, Tal Malkin, Silvio Micali, Tal Rabin. Algorithmic Tamper-Proof Security. In *Proc. of the Theory of Cryptography Conference (TCC '04)*, Cambridge, MA, February 2004.

[P76] Eric Cronin, Sugih Jamin, Tal Malkin, Patrick McDaniel. On the Design and Use of Forward Secure Signatures. In *Proc. of the 10th ACM Conference on Computer and Communications Security (CCS '03),* Washington, DC, October 2003.

[P77] Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, Avi Rubin. Protocols for Anonymity in Wireless Networks. In *Proc. of the 11th International Workshop on Security Protocols,* Cambridge, England, April 2003.

[P78] Tal Malkin, Daniele Micciancio, Sara Miner. Efficient Generic Forward-Secure Signatures With An Unbounded Number Of Time Periods. In *Proc. of the 20th Annual IACR Eurocrypt conference (EUROCRYPT '02),* Amsterdam, Netherlands, May 2002.

[P79] Yael Gertner, Tal Malkin, Omer Reingold. On the Impossibility of Basing Trapdoor Functions on Trapdoor Predicates. In *Proc. of the 42st IEEE Annual Symposium on Foundations of Computer Science (FOCS '01),* Las Vegas, NV, October 2001.

[P80] Joan Feigenbaum, Yuval Ishai, Tal Malkin, Kobbi Nissim, Martin Strauss, Rebecca Wright. Secure Multiparty Computation of Approximations. In *Proc. of the 28th International Colloquium on Automata, Languages and Programming (ICALP '01),* Crete, Greece, July 2001.

[P81] Ran Canetti, Ivan Damgard, Stefan Dziembowski, Yuval Ishai, Tal Malkin. On Adaptive vs. Non-Adaptive Security of Multiparty Protocols. In *Proc. of the 19th Annual IACR Eurocrypt conference (EUROCRYPT '01),* Innsbruck, Austria, May 2001.

[P82] Yael Gertner, Sampath Kannan, Tal Malkin, Omer Reingold, Mahesh Viswanathan. The Relationship between Public Key Encryption and Oblivious Transfer. In *Proc. of the IEEE 41st Annual Symposium on Foundations of Computer Science (FOCS '00),* Redondo Beach, CA, November 2000.

[P83] Amos Beimel, Yuval Ishai, Tal Malkin. Reducing the Servers Computation in Private Information Retrieval: PIR with Preprocessing. In *Proc. of the 20th Annual IACR Crypto conference (CRYPTO '00),* Santa Barbara, CA, August 2000.

[P84] Giovanni Di Crescenzo, Tal Malkin, Rafail Ostrovsky. Single Database Private Information Retrieval Implies Oblivious Transfer. In *Proc. of the 18th Annual IACR Eurocrypt conference (EUROCRYPT '00),* Bruges, Belgium, May 2000.

[P85] Amos Beimel, Tal Malkin, Silvio Micali. The All-Or-Nothing Nature of Two-Party Secure Computation. In *Proc. of the 19th Annual IACR Crypto conference (CRYPTO '99),* Santa Barbara, CA, August 1999.

[P86] Amos Beimel, Yuval Ishai, Eyal Kushilevitz, Tal Malkin. One-way Functions are Essential for Single-Server Private Information Retrieval. In *Proc. of the 31st Annual ACM Symp. on the Theory of Computing (STOC '99),* Atlanta, GA, May 1999.

[P87] Ran Canetti, Tal Malkin, Kobbi Nissim. Efficient Communication-Storage Tradeoffs for Multicast Encryption. In *Proc. of the 17th Annual IACR Eurocrypt conference (EUROCRYPT '99),* Prague, Czech Republic, May 1999.

[P88] Yael Gertner, Shafi Goldwasser, Tal Malkin. A Random Server Model for Private Information Retrieval. In *Proc. of the 2nd International Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM'98),* Barcelona, Spain, October 1998. M. Luby, J. Rolim, and M. Serna, editors, volume 1518 of *Lecture Notes in Computer Science*, Springer.

[P89] Yael Gertner, Yuval Ishai, Eyal Kushilevitz, Tal Malkin. Protecting Data Privacy in Private Information Retrieval Schemes. In *Proc. of the 30th Annual ACM Symp. on the Theory of Computing (STOC'98),* Dallas, TX, May 1998.

Other Publications

[O1] François-Xavier Standaert, Tal Malkin, Moti Yung. Lessons from the Past, Challenges for the Future: The Eurocrypt 2009 Evaluation Framework in the Deep Learning Era. In *Proc. of the Asian Hardware Oriented Security and Trust Symposium (AsianHOST '21),* December, 2021. Invited talk by François-Xavier Standaert.

[O2] Tal Malkin, Valerio Pastro, abhi shelat. An Algebraic Approach to Garbling. Manuscript, 2015.

[O3] Tal Malkin, Chris Peikert, Rocco Servedio, Andrew Wan. Learning an Overcomplete Basis: Cryptanalysis of Lattice-Based Signatures with Perturbations. Manuscript, 2009.

[O4] Homin K. Lee, Tal Malkin, Erich Nahum, Noel Codella. PSST! Are You Using a Secure SSL/TLS Server? Appeared at the 2005 IBM Security and Privacy Technology Symposium, Sponsored by IBM Research and the IBM Academy of Technology.

[O5] Michael Locasto, Janak Parekh, Sal Stolfo, Angelos Keromytis, Tal Malkin, Vishal Misra. Collaborative Distributed Intrusion Detection. Technical Report CUCS-012-04, Columbia University Comptuer Science Department, March 2004.

[O6] Tal Malkin. A Study of Secure Database Access and General Two-Party Computation. Ph.D. Thesis, Massachusetts Institute Of Technology, February 2000.

[O7] Yael Gertner, Tal Malkin. Efficient Distributed $\binom{n}{1}$ Oblivious Transfer. Technical Report MIT-LCS-TR-714, MIT Lab for Computer Science, April 1997.

[O8] Tal Malkin. Deductive Tableaux for Temporal Logic. M.Sc. Thesis, Weizmann Institute of Science, January 1995.

Patents

- Salvatore J. Stolfo, Tal Malkin, Angelos D. Keromytis, Vishal Misra, Michael Locasto, Janak Parekh. System and Methods for Correlating and Distributing Intrusion Alert Information Among Collaborating Computer Systems. US Patent Number 10,038,704. Issued on July 31, 2018.
- Salvatore J. Stolfo, Tal Malkin, Angelos D. Keromytis, Vishal Misra, Michael Locasto, Janak Parekh. System and Methods for Correlating and Distributing Intrusion Alert Information Among Collaborating Computer Systems. US Patent Number 9,135,438. Issued on September 15, 2015.

- Salvatore J. Stolfo, Tal Malkin, Angelos D. Keromytis, Vishal Misra, Michael Locasto, Janak Parekh. System and Methods for Correlating and Distributing Intrusion Alert Information Among Collaborating Computer Systems. US Patent Number 8,381,295. Issued on February 19th, 2013.
- Salvatore J. Stolfo, Tal Malkin, Angelos D. Keromytis, Vishal Misra, Michael Locasto, Janak Parekh. System and Methods for Correlating and Distributing Intrusion Alert Information Among collaborating Computer Systems. US Patent Number 7,779,463. Issued on August 17th, 2010.

Grants

- Google CyberNYC program. "Quality-Preserving Watermarking for Large Language Models" (sole PI). $80K. June 2024.
- AWS Cryptography and Privacy Amazon Research Award. "Cryptographic Techniques for Machine Learning" (sole PI). $60K. March 2024.
- NSF Algorithmic Foundations award. "Collaborative Research: AF: Medium: Foundations of Anonymous Communication in Large-Scale Networks" (sole Columbia PI, collaboration with Brown and Tufts universities). My share: $300K. September 2023 – August 2027.
- PI for NSF student travel grants for Real World Cryptography (RWC). 2023: $20K, 2024: $21K, 2025: $20K.
- Algorand Foundation Centre of Excellence. "PAVE: Privacy, Accountability, Verification, and Economics of Blockchain Systems" (lead Columbia PI, with Gur Huberman and Eran Tromer as co-PIs, and in collaboration with Yale, CUNY, and EPFL). My share: $180K. 2022–2023
- DARPA Securing Information for Encrypted Verification and Evaluation (SIEVE) program. "FROMAGER: Formal Reasoning Over Machine-code Assets, Given with Explicit Reticence" (sole Columbia PI, with Eran Tromer as co-PI). $800K. April 2020 – March 2024.
- CU-IBM Blockchain and Data Transparency Center. "Cryptographic Tools for Secure Sharing and Learning in the Wake of COVID-19" (sole PI). $100K January 2020-December 2023.
- Department of Energy, via subcontract from Brookhaven National Laboratory. "Exascale Privacy-Preserving AI" (with Roxana Geambasu). $202,394 (my share: 101,197). June 2020 – September 2021.
- JPMorgan Chase & Co. "MAGIC: Machine Learning Through a Cryptographic Lens" (sole PI). $150K. May 2020 – April 2021.
- LexisNexis Risk Solution Award. $70K. December 2019.
- IARPA Homomorphic Encryption Computing Techniques with Overhead Reduction (HECTOR) program. "VERONA: A Platform for Developing and Deploying Secure Computation for Data Scientists" (sole Columbia PI, with Eran Tromer as co-PI). $484K. June 2019 – May 2020.
- The Leona M. and Harry B. Helmsley Trust: Advanced Communication Technology Project (sole PI). $320K November 2016 – October 2018.
- Institute for Social and Economic Research and Policy (ISERP) Start-up Center. "The Center for Lifecourse Approach to Adolescent Well-Being (CLAAW)". Sole

SEAS participant in a center led by Shamus Khan of the Sociology Department and Jennifer Hirsch of the Sociomedical Sciences Department, with other faculty from different departments in the Mailman School of Public Health. $40K (budget for whole project, not divided by participants). January 2018 – December 2018.

- DARPA SafeWare Program. "CONCEAL: Cryptographic ObfuscatioN of CodE and ALgorithms" (sole Columbia PI, collaboration with IBM TJ Watson and other universities). My share: $574K (whole project: $3.9M). June 2015–May 2019.
- NSF Secure and Trustworthy Cyberspace award. "New Challenges in Functional Encryption" (sole PI, with Hoeteck Wee as coPI). $396K. April 2014 – February 2018.
- NSF Algorithmic Foundations award. "Minimalist Cryptography" (with Allison Lewko). $497K (my share: $248K). August 2014 – July 2017.
- IARPA Security and Privacy Assurance Research (SPAR) Program. "Practical and Secure Database Access Using Encrypted Bloom Filters" (lead PI, with Steve Bellovin and Angelos Keromytis as co-PIs, and Vlad Kolesnikov of Bell-Labs as a subcontractor). $2.24M (my share: 1.2M). September 2011- June 2014.
- NSF Algorithmic Foundations award. "How to Let an Adversary Compute For You". $350K. September 2011 – August 2014.
- The Columbia Artemis Project, total raised $29.5K plus $10K matching funds:
  - NSF subaward via Brown University. "Eager: The Artemis Project". $12K. August 2013
  - L'Oreal gift. $7.5K. August 2013
  - National Center for Women & Information Technology (NCWIT) Academic Alliance Microsoft Research Seed Fund Award. "The Artemis Project: An Immersive, Summer Learning Program in Computer Science For Girls" $10K. February 2013.
  - Matching funds, SEAS and CS, $10K.
- NSF Computing Innovations Fellowship postdoctoral funding for S. Dov Gordon. $273.6K. October 2010 – September 2012.
- NEC Japan, $50K gift. Spring 2010.
- Supplement for NSF Faculty Early Career Development (CAREER) Award, Theory of Computing Program. "CAREER: Strengthening Cryptography by Reducing Assumptions about the Adversary". $80K. August 2010 - August 2011.
- Supplement for NSF CyberTrust Award. "Cross-Leveraging Cryptography with Learning Theory". $20K. August 2010 - August 2011.
- Google research award. "Efficient Routing by Oblivious Nodes". $70K. Spring 2010.
- Department of Homeland Security (DHS). "Privacy Preserving Sharing of Network Trace Data" (with Steve Bellovin, Tony Jebara, Vishal Misra, Dan Rubenstein, Sal Stolfo). $830K (my share: $ 138K). September 2009 - January 2011.
- NSF Cybertrust award. "Tamper Proofing Cryptographic Operations". $230K. September 2008 - August 2011.
- IARPA Automatic Privacy Protection Program. "Secure Encrypted Search" (with Steve Bellovin, Angelos Keromytis, Sal Stolfo). $649K (my share: $162.25K). February 2009 - July 2010.

- Columbia University Diversity Initiative Research Fellowship. $25K. April 2008.
- NSF ADVANCE Program at the Earth Institute at Columbia University. "Foundations of Public-Key Encryption: From Weak Notions to Strong Ones". $35K. October 2007.
- NSF CyberTrust Award. "Cross-Leveraging Cryptography with Learning Theory" (with Rocco Servedio). $375K (my share: $187.5K). September 2007 - August 2010.
- Mitsubishi Electric Research Laboratories (MERL). "Blind Vision and Privacy Preserving Learning Algorithms". $15K. October 2006.
- NY Software Industry Association (NYSIA), Institute for Advanced Studies in Software and IT. "Key Evolving Signatures and Their Use in Mitigating Key Exposure Attacks for Secure On-Line Communication". $35K. September 2004-August 2005.
- NY Software Industry Association (NYSIA), Institute for Advanced Studies in Software and IT. "An Analysis of Server Security on the Internet". $35K. September 2004-August 2005.
- IBM Faculty Partnership Award. "The Next Generation of Cryptography: Removing Unrealistic Assumptions About the Adversary". $30K. June 2004.
- NSF Faculty Early Career Development (CAREER) Award, Theory of Computing Program. "CAREER: Strengthening Cryptography by Reducing Assumptions about the Adversary". $400K. February 2004-January 2009.
- Maryland Procurment Office (NSA). "Distributed Intrusion Detection Feasibility Study" (with Salvatore Stolfo, Angelos Keromytis, and Vishal Misra), $300K. April 2003 - March 2004.

Teaching

Columbia University New York, NY

Instructor for the following classes:

- COMS 3261 Computer Science Theory
  (undergraduate class, 204 students in two sections) Fall 2024
- COMS 6261 Advanced Cryptography: Cryptography and TFNP (advanced graduate class, 11 students, co-taught with Daniel Mitropolsky) Spring 2023
- COMS 4261 Introduction to Cryptography
  (graduate class, 79 students including CVN) Fall 2023
- COMS 3261 Computer Science Theory
  (undergraduate class, 303 students in two sections) Fall 2022
- COMS 4261 Introduction to Cryptography
  (graduate class, 136 students in two sections plus CVN) Spring 2022
- COMS 3261 Computer Science Theory
  (undergraduate class, 283 students in two sections) Fall 2020
- COMS 6261 Advanced Cryptography: Information-Theoretic Cryptography
  (advanced graduate class, 26 students) Spring 2020
- COMS 4261 Introduction to Cryptography
  (graduate class, 60 students) Fall 2019
- COMS 3261 Computer Science Theory
  (undergraduate class, 225 students in two sections) Spring 2018

- COMS 3261 Computer Science Theory
  (undergraduate class, 248 students in two sections) Spring 2017
- COMS 4261 Introduction to Cryptography
  (graduate class, 43 students) Fall 2016
- COMS 6261 Advanced Cryptography: Minimalist Cryptography
  (advanced graduate class, 17 students) Spring 2016
- COMS 3261 Computer Science Theory
  (undergraduate class, 186 students in two sections) Spring 2015
- COMS 4261 Introduction to Cryptography
  (graduate class, 45 students) Fall 2014
- COMS 6261 Advanced Cryptography: Homomorphic Encryption and Lattices
  (advanced graduate class, 10 students, co-taught with Dr. Shai Halevi) Spring 2013
- COMS 4261 Introduction to Cryptography
  (graduate class, 18 students) Fall 2012
- COMS 3261 Computer Science Theory
  (undergraduate class, 91 students) Spring 2012
- COMS 4261 Introduction to Cryptography
  (graduate class, 19 students) Fall 2011
- COMS 3261 Computer Science Theory
  (undergraduate class, 56 students) Spring 2011
- COMS W6261 Advanced Cryptography: Data Privacy
  (advanced graduate class, 10 students) Spring 2010
- COMS 4261 Introduction to Cryptography
  (introductory graduate class, 19 students) Fall 2009
- COMS W3261 Computer Science Theory
  (undergraduate class, 40 students) Spring 2009
- COMS W4261 Introduction to Cryptography
  (introductory graduate class, 21 students) Spring 2008
- COMS W6261 Advanced Cryptography: The Black-Box Complexity of Cryptographic Primitives
  (advanced graduate class, 7 students) Spring 2008
- COMS W3261 Computer Science Theory
  (undergraduate class, 29 students) Fall 2007
- COMS W3261 Computer Science Theory
  (undergraduate class, 41 students) Spring 2007
- COMS W3261 Computer Science Theory
  (undergraduate class, 40 students) Spring 2006
- COMS W4261 Introduction to Cryptography
  (introductory graduate class, 43 students) Fall 2005
- COMS E6998 Advanced Cryptography: Secure Multiparty Computation
  (advanced graduate class, 16 registered students and 5 auditors) Spring 2004
- COMS W4995 Introduction to Cryptography
  (introductory graduate class, 30 students) Fall 2003

- COMS W3261 Computability and Models of Computation (undergraduate class, 73 students) Spring 2003

Institute for Advanced Studies Princeton, NJ
Instructor for Cryptographic Complexity Theory (graduate summer class), PCMI Mentoring Program for Women in Mathematics. Summer 2000

CU/Dept Service

- At-Large Faculty Member, SEAS July 2023 - current
- TA/CA Chair July 2005 - current
- Student Nominations Committee Fall 2004 - Spring 2009, Fall 2019 - current
- WICS (Women In Computer Science) faculty Advisor Fall 2012 - current
- Chair of Education Track, Columbia-IBM Center for Blockchain and Data Transparency July 2018 - December 2021
- Faculty Recruiting Committe Spring 2003 - Spring 2004, Fall 2008 - Spring 2011, Fall 2012, Spring 2013, Fall 2020 - Spring 2021
- SEAS/Business School MS/MBA Joint Degree working group 2020 - 2021
- SEAS Ad-hoc Promotion Committee 2020
- Northeast Collegiate Cyber Defense Competition (NECCDC) Columbia University faculty coach 2019
- PhD Committee Fall 2017 - Spring 2018
- Barnard CS advisor (50 students) Fall 2015- Spring 2016
- Data Science Institute Cybersecurity Center Chair October 2012 - August 2013, April 2016 - June 2018
- Columbia Artemis Project, Founder and Faculty Advisor (summer program for rising 9th grade girls, taught by undergrad women) 2013 - 2015
- MS Foundations Track advisor Fall 2009 - Spring 2013
- MS Admission co-chair Fall 2009 - Spring 2013
- MS Admissions Committee Fall 2003 - Spring 2013
- MS Program Committee Fall 2003 - Spring 2009
- Faculty Retreat Organizer October 2003
- Events Representative Fall 2003 - 2007
- Academic Honesty Task Force Fall 2004
- Advisor for SEAS undergrads Spring 2003 - Spring 2009
- MS Security Track Advisor Spring 2004
- Organizer, Theory Reading Group 2003 - 2014
- Speaker and participant: Barnard Better, Enhance and Advance Research Series (BEARS), ACM Research Fair, Women in Computer Science (WICS), Columbia Computer Science Preprofessional Society (CCSPS), Intro to Data Science Course, Society of Women Engineers (SWE) Banquet, Data Science Day, Columbia Engineering Women's Forum for prospective SEAS undergrads.

Other Service

- Vice President, MIT Israeli Student Organization. 1997 – 1999

- Elected Officer, MIT graduate housing executive committee and other graduate housing committees. 1995 – 1997
- National Service: work with school children and children with special needs, Kedumim, Israel. 1988 – 1989