

Tal G. Malkin

Department of Computer Science
Columbia University
1214 Amsterdam Avenue MC 0401
New York, NY 10027-7003

Phone: +1-212-939-7097
Fax: +1-212-666-0140
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.
GPA 5.0/5.0
- The Weizmann Institute of Science** Rehovot, Israel
M.Sc. in Computer Science, January 1995.
Thesis: “Deductive Tableaux for Temporal Logic”.
Advisor: Prof. Amir Pnueli.
GPA 97/100
- Bar-Ilan University** Ramat-Gan, Israel
B.S. *summa cum laude* in Mathematics and Computer Science, January 1993.
GPA 96/100
- Employment**
- Columbia University, New York, NY** December 2009 – Current
Associate Professor, Department of Computer Science
- Columbia University, New York, NY** January 2003 – November 2009
Assistant Professor, Department of Computer Science
- Microsoft Research, Redmond, MA** August 2009
Consultant, Cryptography Group
- AT&T Labs, Florham Park, NJ** December 1999 – December 2002
Senior Research Scientist, Secure Systems Research Department.
- Massachusetts Institute of Technology, Cambridge, MA** 1995 – 1999
Research and Teaching Assistant, Cryptography and Information Security Group, and Theory of Computation Group, Department of Electrical Engineering and Computer Science.
- 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.
- The Weizmann Institute of Science, Rehovot, Israel** 1993 – 1994
Research Assistant and Teaching Assistant, Department of Applied Mathematics and Computer Science

Bar-Ilan University, Ramat-Gan, Israel**1992***Teaching Assistant, Department of Mathematics and Computer Science***Honors**

- Google Faculty Research Award, 2010.
- Research Fellow, Columbia University Diversity Initiative, 2008.
- PC Chair, Cryptographer's Track of the RSA Conference (CT-RSA), 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

- Guest editor, SIAM Journal of Computing (FOCS 2010 special issue).
- Editorial Board, Theory of Computing Journal (ToC).
- 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.
- PC chair, the RSA Conference, Cryptographers' Track (CT-RSA 2008).
- General chair, the 9th Annual workshop on Practice and Theory in Public Key Cryptography (PKC 2006).
- PC member, the 32nd Annual IACR Crypto conference (Crypto 2012).
- PC member, the 17th ACM Conference on Computer and Communication Security (CCS 2010).
- PC member, the 51st Annual IEEE Symposium on Foundations of Computer Science (FOCS 2010).
- PC member, the 10th Privacy Enhancing Technologies Symposium (PETS 2010).
- PC member, Security and Cryptography for Networks (SCN 2010).
- PC member, the RSA Conference, Cryptographers' track (CT-RSA 2010).
- PC member, the 9th Privacy Enhancing Technologies Symposium (PETS 2009).
- PC member, the 28th Annual IACR Crypto conference (Crypto 2008).
- PC member, the 26th Annual IACR Crypto conference (Crypto 2006).
- PC member the 38th ACM Symposium on Theory of Computing (STOC 2006).

- PC member, the Theory of Cryptography Conference (TCC 2006).
- PC member, the 25th Annual IACR Crypto conference (Crypto 2005).
- PC member, the 14th USENIX Security Symposium (USENIX Security 2005).
- PC member, the RSA Conference, Cryptographers' Track (CT-RSA 2005).
- PC member, the Theory of Cryptography Conference (TCC 2005).
- PC member, 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).
- PC member, the 24th Annual IACR Crypto Conference (Crypto 2004).
- PC member the 36th ACM Symposium on Theory of Computing (STOC 2004).
- PC member, the Sixth International Workshop on Practice and Theory in Public Key Cryptography (PKC 2003).
- PC member, the Ninth Annual Workshop on Selected Areas in Cryptography (SAC 2002).
- Frequent referee for various professional journals and 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 Cryptology, Theory of Computing Systems, Designs, Codes, and Cryptography, Discrete Applied Mathematics, and others.
- Reviewer of Doctoral dissertations for the ACM Dissertation Award
- NSF Panelist, Theory of Computation and Cyber Trust programs, multiple years
- Organizer, IBM/NYU/Columbia Theory Day (semi-annually starting Spring 2003).
- 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 - current)
- Yevgeniy Vahlis (July 2010 - current)
- Dov Gordon, CIFellow (October 2010 - current)

***Graduated
PhD Students***

- Ariel Elbaz, PhD 2009. *Thesis: "Round-Efficient Secure Computation, and Applications"*. Now at Google Inc.
- Homin Lee, PhD 2009. *Thesis: "Complexity Measures and Computational Learning Theory"* (co-advised with Rocco Servedio). Now a *CIFellow* postdoc at UT Austin.
- Andrew Wan, PhD 2010. *Thesis: "Learning, Cryptography, and the Average Case"* (co-advised with Rocco Servedio). Now an assistant professor at Tsinghua university.
- Seung Geol Choi, PhD 2010. *Thesis: "On Adaptive Security and Round Efficiency in Secure Multi-Party Computation"*. Now a postdoc at the University of Maryland.

- Current** • Dana (Glasner) Dachman-Soled, expected graduation Summer 2011.
- PhD Students** • Mariana Raykova, expected graduation February 2012 (co-advised with Steven Bellovin).
 • Krzysztof Choromanski, second year student (co-advised with Maria Chudnovsky)
 • Fernando Krell, first year student
 • Aaron Bernstein, first year student (co-advised with 3 theory faculty)
 • Igor Carboni Oliveira, first year student (co-advised with 3 theory faculty)
- PhD Thesis Committee** • Hector Rosario “*Steganography: Historical Development and Applications at the Undergraduate Level*”, Teachers College, May 2003. Now at the Department of Mathematics, University of Puerto Rico
 • Enav Weinreb “*Secret Sharing, Span Programs, and Secure Computation: Complexity Issues and Cryptographic Applications*”, Department of Computer Science, Ben-Gurion University, July 2007. Now a researcher (algorithm designer) at ClearForest, a Thomson Reuters company.
 • Sharon Goldberg “*Towards Securing Interdomain Routing on the Internet*”, Department of Computer Science, Princeton University, July 2009. Now an assistant professor at Boston University.
 • 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.
- Other Students** • PHD Candidacy Committee (other than advisees): Debbie Cook, Spyridon Antonakopoulos, Ilias Diakonikolas, Elli Androulaki, Swapneel Sheth, Mehvish Poshni, Binh Vo
 • MSc Thesis Supervision: Ryan Moriarty, Devang Thakkar
 • MSC Thesis Committee Member: Joseph Sherrick, Hunning Dai
 • Independent study supervisor: George Philip Atzemoglou (Spring 2003), Andrew Wan (Fall 2003), Bhargav Bhatt, Noel Codella (Spring 2004), Marzia Niccolai, Nikolai Yakovenko (Fall 2004), Catherine Lennon, Matthew Raibert, Nikolai Yakovenko (Spring 2005), Rajesh Venkataraman (Fall 2007). Noah Youngs (Fall 2007).
 • PhD Student 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] 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.
 [B2] 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.

* Students and postdocs working with me are underlined. Authors in theory and cryptography venues are in alphabetical order, and authors in security venues are alphabetized students, followed by alphabetized professors.

- [B3] 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] Melissa Chase, Alexander Healy, Anna Lysyanskaya, **Tal Malkin**, Leonid Reyzin. Mercurial Commitments with Applications to Zero-Knowledge Sets. Accepted subject to revisions, *Journal of Cryptology*.
- [J2] Amos Beimel, **Tal Malkin**, Kobbi Nissim, Enav Weinreb. How Should We Solve Search Problems Privately? *Journal of Cryptology*, 23(2), 2010.
- [J3] 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.
- [J4] 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).
- [J5] Matt Blaze, John Ioannidis, Angelos D. Keromytis, **Tal Malkin**, Avi Rubin. Anonymity in Wireless Broadcast Networks. *International Journal of Network Security (IJNS)*, 8(1), 2009.
- [J6] 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.
- [J7] Joan Feigenbaum, Yuval Ishai, **Tal Malkin**, Kobbi Nissim, Martin Strauss, Rebecca Wright. Secure Multiparty Computation of Approximations. *ACM Transactions on Algorithms*, 2005.
- [J8] 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.
- [J9] 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.
- [J10] 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] 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.
- [P2] **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.

* Students and postdocs working with me are underlined. Authors in theory and cryptography venues are in alphabetical order, and authors in security venues are alphabetized students, followed by alphabetized professors.

- [P3] 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.
- [P4] **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.
- [P5] 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.
- [P6] **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 Keynote talk by Moti Yung.
- [P7] 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.
- [P8] 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.
- [P9] 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.
- [P10] 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.
- [P11] 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.
- [P12] 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.
- [P13] 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.
- [P14] 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.
- [P15] 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.

- [P16] 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.
- [P17] 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.
- [P18] 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.
- [P19] 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.
- [P20] 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.
- [P21] 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.
- [P22] 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.
- [P23] 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.
- [P24] **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.
- [P25] **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.
- [P26] 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.
- [P27] 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).
- [P28] 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.
- [P29] **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.
- [P30] 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.
- [P31] 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.
- [P32] 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.
- [P33] 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.
- [P34] **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.
- [P35] Yael Gertner, **Tal Malkin**, Omer Reingold. On the Impossibility of Basing Trapdoor Functions on Trapdoor Predicates. In *Proc. of the 42st Annual Symposium on Foundations of Computer Science (FOCS '01)*, Las Vegas, NV, October 2001.
- [P36] 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.
- [P37] 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.
- [P38] Yael Gertner, Sampath Kannan, **Tal Malkin**, Omer Reingold, Mahesh Viswanathan. The Relationship between Public Key Encryption and Oblivious Transfer. In *Proc. of the 41st Annual Symposium on Foundations of Computer Science (FOCS '00)*, Redondo Beach, CA, November 2000.
- [P39] 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.

- [P40] 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.
- [P41] 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.
- [P42] 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.
- [P43] Ran Canetti, **Tal Malkin**, Kobbi Nissim. Efficient Communication-Storage Trade-offs for Multicast Encryption. In *Proc. of the 17th Annual IACR Eurocrypt conference (EUROCRYPT '99)*, Prague, Czech Republic, May 1999.
- [P44] 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.
- [P45] 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] Krzysztof Choromanski, **Tal Malkin**. The Power of the Dinur-Nissim Algorithm: Breaking Privacy of Statistical and Graph Databases. Submitted for Publication.
- [O2] Dana Dachman-Soled, Rosario Gennaro, Hugo Krawczyk, **Tal Malkin**. Computational Extractors and Pseudorandomness. Submitted for Publication.
- [O3] Dov Gordon, Jonathan Katz, Vladimir Kolesnikov, **Tal Malkin**, Mariana Raykova, Yevgeniy Vahlis. Secure Computation with Sublinear Amortized Work. Submitted for Publication.
- [O4] Seung Geol Choi, Aggelos Kiayias, **Tal Malkin**. BiTR: Built-in Tamper Resistance. Submitted for Publication.
- [O5] Seung Geol Choi, Kyung-Wook Hwang, Jonathan Katz, **Tal Malkin**, Dan Rubenstein. Distributed Private Matching for On-Line Marketplaces. Submitted for Publication.
- [O6] Vasilis Pappas, Mariana Raykova, Binh Vo, Steven Bellovin, **Tal Malkin**. Trade-offs in Private Search. Submitted for Publication.
- [O7] Mariana Raykova, Ang Cui, Binh Vo, Bin Liu, **Tal Malkin**, Steven Bellovin, Salvatore Stolfo. Usable Secure Private Search. Submitted for Publication.
- [O8] **Tal Malkin**, Chris Peikert, Rocco Servedio, Andrew Wan. Learning an Over-complete Basis: Cryptanalysis of Lattice-Based Signatures with Perturbations. Manuscript.

* Students and postdocs working with me are underlined. Authors in theory and cryptography venues are in alphabetical order, and authors in security venues are alphabetized students, followed by alphabetized professors.

- [O9] François-Xavier Standaert, **Tal Malkin**, Moti Yung. Does Physical Security of Cryptographic Devices Need a Formal Study? Invited talk by Moti Yung, appears in LNCS Proc. of the International Conference on Information Theoretic Security (ICITS '08), Calgary, Canada, August 2008.
- [O10] 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.
- [O11] Michael Locasto, Janak Parekh, Sal Stolfo, Angelos Keromytis, **Tal Malkin**, Vishal Misra. Collaborative Distributed Intrusion Detection. Technical Report CUCS-012-04, Columbia University Computer Science Department, March 2004.
- [O12] Amos Beimel, **Tal Malkin**. A Quantitative Approach to Reductions in Secure Computation. *The Electronic Colloquium on Computational Complexity (ECCC)* volume 86, 2003.
- [O13] **Tal Malkin**. A Study of Secure Database Access and General Two-Party Computation. Ph.D. Thesis, Massachusetts Institute Of Technology, February 2000.
- [O14] Yael Gertner, **Tal Malkin**. Efficient Distributed $\binom{n}{1}$ Oblivious Transfer. Technical Report MIT-LCS-TR-714, MIT Lab for Computer Science, April 1997.
- [O15] **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 7,779,463. Issued on August 17th, 2010.

Grants

- NSF Computing Innovations Fellowship postdoctoral funding for S. Dov Gordon. \$142.4K. October 2010 – September 2011.
- 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 Procurement 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, 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

Massachusetts Institute of Technology Cambridge, MA
Teaching Assistant, including teaching recitations and tutorials, preparing and grading
 homework and test assignments, and teaching several lectures, for the following classes:

- 6.875 Introduction to Cryptography (graduate class) Fall 1997
- 6.87s Cryptography and Information Security
(intensive summer class for high-tech professionals) Summer 1997
- 6.046 Introduction to Algorithms (undergraduate class) Spring 1997
- 6.041 Applied Probability (undergraduate class) Fall 1995
- 6.045 Automata, Computability and Complexity
(undergraduate class) Spring 1995

The Weizmann Institute of Science Rehovot, Israel
Teaching Assistant for Automated Deduction (graduate class) 1993

Bar-Ilan University Ramat-Gan, Israel
Teaching Assistant for Mathematical Logic (undergraduate class) 1992

*CU/Dept
 Service*

- TA Czar July 2005 - current
- Faculty Recruiting Committee Spring 2003 - Spring 2004, Fall 2008 – current
- MS Foundations Track advisor Fall 2009 - current
- MS Admission co-chair Fall 2009 - Spring 2010
- MS Program Committee Fall 2003 - Spring 2009
- MS Admissions Committee Fall 2003 - current
- Faculty Retreat Organizer October 2003
- Events Representative Fall 2003 - 2007
- Student Nominations Committee Fall 2004 - Spring 2009
- Academic Honesty Task Force Fall 2004
- Advisor for SEAS undergrads Spring 2003 - Spring 2009
- MS Security Track Advisor Spring 2004

- Organizer, Theory Reading Group Spring 2003 - current
- Speaker and participant: ACM Research Fair, Women in Computer Science (WICS)

*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 disabilities, Kedumim, Israel. 1988 – 1989

*Invited
Talks*

- *Dagstuhl Workshop on Public Key Encryption, Dagstuhl, Germany.* September 2011.
- *Association of Women in Mathematics (AWM) Meeting, Brown University.* Invited Speaker for “40 Years and Counting: AWM’s Celebration of Women in Mathematics” Providence, RI, September 2011.
- *American Mathematical Society (AMS) Meeting, Cornell University.* Invited Speaker Ithaca, NY, September 2011.
- *New York Area Crypto Day, NYU.* Efficient Circuit-Size Independent Public Key Encryption with KDM Security. New York, NY, March 2011.
- *Weizmann Institute of Science.* Efficient Circuit-Size Independent KDM Secure Public Key Encryption. Rehovot, Israel, February 2011.
- *Trends in Theoretical Cryptography Workshop.* (1) Efficient Block-Wise PKE with Key Dependent Message Security under Flexible SLP-Queries. (2) On the Black-Box Complexity of Optimally-Fair coin Tossing. ITCS, Tsinghua University, Beijing, China, January 2011.
- *Tel Aviv University.* Efficient Block-Wise PKE with Key Dependent Message Security under Flexible SLP-Queries. Tel Aviv, Israel, December 2010.
- *Massachusetts Institute of Technology.* Efficient Block-Wise PKE with Key Dependent Message Security under Flexible SLP-Queries. Cambridge, MA, December 2010.
- *New York Area Crypto Day, NYU.* Tamper Proofing Cryptographic Primitives. New York, NY, April 2010.
- *Microsoft Research.* Public Key Cryptosystems: Stronger Security from General Assumptions. Redmond, WA. August 2009.
- *Crypto In The Clouds Workshop.* Efficient and Robust Private Set Intersection and Multiparty Multivariate Polynomials. MIT Stata Center, Cambridge, MA. August 2009.
- *Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security, Institute for Pure and Applied Mathematics.* UCLA Conference Center, Lake Arrowhead, CA. June 2009.
- *Complexity and Cryptography: Status of Impagliazzo Worlds, Center for Computational Intractability,* Princeton, NJ. June 2009.
- *Workshop on Cryptographic Protocols and Public-Key Cryptography (WPK 2009).* Black-Box Adaptively Secure Protocols, Using Weaker Assumptions. Bertinoro, Italy. May 2009.

- *DARPA Information Science and Technology (ISAT) workshop on Securely Outsourcing Video*. Representing the Cryptography area. Arlington, VA. April 2009.
- *Tel-Aviv University and Weizmann Institute of Science CS Seminar*. Non-Committing Public Key Encryption and Adaptively Secure Protocols from Weaker Assumptions. Tel Aviv, Israel. January 2009.
- *Dagstuhl Workshop on Theoretical Foundations of Practical Information Security, Dagstuhl, Germany*. Adaptive Security: Non-Committing Encryption from Weaker Assumptions. December 2008.
- *Applications of Internet Multi-Resolution Analysis to Cyber-Security Workshop, Institute for Pure and Applied Mathematics, University of California at Los Angeles*. Co-Organizer and Invited Speaker. October 2008.
- *Women in Theory (WIT) Workshop, Princeton, NJ*. Public Key Encryption: From Semantic Security to Stronger Notions. June 2008.
- *BSF/DyDAn/DIMACS workshop on privacy and confidentiality, DIMACS Center, Rutgers University*. February 2008.
- *Weizmann Institute of Science*. Black-Box Construction of a Non-Malleable Encryption Scheme from Any Semantically Secure One. December 2007.
- *Workshop on Generic Case Complexity, American Institute of Mathematics (AIM), Palo Alto, California*. August 2007.
- *ADVANCE Leadership Workshop for Women Faculty in Engineering, Carolina Beach, NC*. August 2007
- *Keynote talk, FCS-ARSPA '07 workshop at ICALP/LICS'07, Wroclaw, Poland*. July 2007. (Declined)
- *IBM Research / Stevens / Columbia Security and Privacy Day, Columbia University*. Expanding the Foundations of Cryptography. June 2007.
- *IMA Workshop on Complexity, Coding, and Communications, Minneapolis, Minnesota*. April 2007.
- *International Workshop on Cryptographic Protocols, Bertinoro, Italy*, March 2007.
- *Securing Cyberspace: Application and Foundations of Cryptography and Computer Security, Institute for Pure and Applied Mathematics, University of California at Los Angeles*. Invited as a core participant for the entire program, including five workshops, and invited talks for two workshops: (1) Foundations of Secure Multi-Party Computation and Zero-Knowledge and its Applications; (2) Locally Decodable Codes, Private Information Retrieval, Privacy-Preserving Data-Mining, and Public-Key Encryption with Special Properties. September – December, 2006.
- Invited panelist on “Managing Mid-Career Changes”, *Grace Hopper Celebration of Women in Computing, San Diego*. October 2006.
- *Columbia University, talk for Army visitors, including a representative of the UK Ministry of Defense (MoD)*. September 2006.
- *ADVANCE Community Building Workshop for Women Junior Faculty in Engineering, Charlottesville, Virginia*. July 2006.
- *Princeton University*. Expanding the Foundations of Cryptography. May 2006.

- Invited panelist on *Princeton Women in Science and Engineering (WISE) Conference*. February 2006.
- *Distinguished Faculty Lecture Series, Department of Computer Science, University of Texas at Austin*. Expanding the Foundations of Cryptography. December 2005.
- *Dagstuhl Workshop on Anonymous Communication and its Applications, Dagstuhl, Germany*. October 2005.
- *University of Massachusetts, Amherst*. Algorithmic Tamper-Proof Security. October 2005.
- *ADVANCE Community Building Workshop for Women Junior Faculty in Engineering, College Park, Maryland*. July 2005.
- *Workshop on the Past, Present, and Future of Oblivious Transfer, a satellite workshop of the Fifth Haifa Workshop on Interdisciplinary Applications of Graph theory, Combinatorics, and Algorithms, Honoring Michael Rabin, Haifa, Israel*. May 2005 (declined).
- *New York University*. Mercurial Commitments with Applications to Zero-Knowledge. April 2005.
- *DIMACS working group on Network Coding*. January 2005.
- *Cryptography Workshop, Centre International de Rencontres Mathematiques (CIRM), Luminy, France*. November 2004 (declined due to maternity leave).
- *Workshop on Secure Multiparty Protocols (SMP 2004), Amsterdam, The Netherlands*. October 2004 (declined due to maternity leave).
- *Stevens Institute of Technology*. Algorithmic Tamper-Proof Security. April 2004.
- *DIMACS/PORTIA workshop and working group on Privacy Preserving Data Mining*. March 2004 (declined).
- *New York University*. A Quantitative Approach to Reductions in Secure Computation. February 2004.
- *University of Washington*. Secure Multiparty Computation of Approximations. January 2003.
- *Technion (Israel Institute of Technology)*. Relationships among the Fundamental Cryptographic Primitives. December 2002.
- *Weizmann Institute of Science*. Efficient Generic Forward-Secure Signatures With An Unbounded Number Of Time Periods. December 2002.
- *Workshop on Cryptographic Protocols in Complex Environments, Rutgers University, New Jersey*. Secure Multiparty Computation of Approximation. May 2002.
- *Massachusetts Institute of Technology*. From Minicrypt to Cryptomania: Relationships Among the Fundamental Cryptographic Primitives. April 2002.
- *Massachusetts Institute of Technology*. Secure Multiparty Computation of Approximations. April 2002.
- *Columbia University*. From Minicrypt to Cryptomania: Exploring the Foundations of Cryptography. March 2002.
- *IBM T.J. Watson Research Center*. On the Impossibility of Basing Trapdoor Functions on Trapdoor Predicates. February 2002.

- *Workshop on Contemporary Methods in Cryptography, Institute for Pure and Applied Mathematics, University of California at Los Angeles.* Exploring the Worlds Between Minicrypt and Cryptomania. January 2002.
- *AT&T Labs Research.* Secure Multiparty Protocols: The Power of Adaptive Attacks. July 2001.
- *Massachusetts Institute of Technology.* The Relationship Between Public-Key Encryption and Oblivious Transfer. November 2000.
- *University of California at San Diego.* The Relationship Between Public-Key Encryption and Oblivious Transfer. November 2000.
- *Ben-Gurion University.* Survey on Private Information Retrieval. April 2000.
- *DIMACS Workshop on Cryptography and Intractability.* The All-or-Nothing Nature of Two-Party Secure Computation. March 2000.
- *University of Maryland at College Park.* Private Information Retrieval: Protocols and Complexity. February 2000.
- *AT&T Labs Research.* Private Information Retrieval: Protocols and Complexity. April 1999.
- *University of California at San Diego.* Private Information Retrieval: Protocols and Complexity. April 1999.
- *DARPA High Confidence Nets Workshop, Space and Naval Warfare Center, San Diego.* Security for Distributed Computer Systems. April 1999.
- *University of Toronto.* Private Information Retrieval: Protocols and Complexity. April 1999.
- *Bell Labs, Lucent Technologies.* Efficient Communication-Storage Tradeoffs for Multicast Encryption. March 1999.
- *Massachusetts Institute of Technology.* Efficient Communication-Storage Tradeoffs for Multicast Encryption. February 1999.
- *Weizmann Institute of Science.* Oblivious Transfer is Essential for Single Database Private Information Retrieval. November 1998.
- *Bellcore (now Telcordia).* Survey on Private Information Retrieval. October 1998.
- *Bell Labs, Lucent Technologies.* Survey on Private Information Retrieval. August 1998.
- *IBM T.J. Watson Research Center.* Survey on Private Information Retrieval. July 1998.
- *Fields Institute Workshop on Interactive Proofs, PCP's, and Foundations of Cryptography, University of Toronto.* A Random Server Model for Private Information Retrieval. May 1998.
- *Weizmann Institute of Science.* A Random Server Model for Private Information Retrieval. April 1998.
- *Massachusetts Institute of Technology.* Protecting Data Privacy in Private Information Retrieval Schemes. September 1997.