

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** January 2003 – Current
Assistant Professor, Department of Computer Science
- 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 Assistant, Cryptography and Information Security Group, and Theory of Computation Group.
- Massachusetts Institute of Technology, Cambridge, MA** 1995 – 1998
Teaching Assistant, 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

- Teaching*
- Columbia University** New York, NY
- 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
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 classes listed.
- 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
- Refereed Publications*
- Jon Feldman, Tal Malkin, Cliff Stein, Rocco Servedio, Martin Wainwright. LP Decoding Corrects a Constant Fraction of Error. To Appear in *Proc. IEEE International Symposium on Information Theory (ISIT '04)*, Chicago, IL, June 2004.
 - Tal Malkin, Satoshi Obana, Moti Yung. The Hierarchy of Key Evolving Signatures and a Characterization of Proxy Signatures. To Appear in *Proc. of the 22th Annual IACR Eurocrypt conference (EUROCRYPT '04)*, Interlaken, Switzerland, May 2004.
 - Amos Beimel, Tal Malkin. A Quantitative Approach to Reductions in Secure Computation. In *Proc. of the First Theory of Cryptography Conference (TCC '04)*, Cambridge, MA, February 2004. A full version available at the Electronic Colloquium on Computational Complexity volume 86, 2003.
 - Rosario Gennaro, Anna Lysyanskaya, Tal Malkin, Silvio Micali, Tal Rabin. Algorithmic Tamper-Proof Security. In *Proc. of the First Theory of Cryptography Conference (TCC '04)*, Cambridge, MA, February 2004.

- 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.
- 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.
- 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.
- 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.
- 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. Submitted to the *Journal of Cryptology*.
- Ran Canetti, Ivan Damgard, Stefan Dziembowski, Yuval Ishai, Tal Malkin. On Adaptive vs. Non-Adaptive Security of Multiparty Protocols. *Journal of Cryptology*, 17(2), February, 2004.
 - An earlier version appeared in *Proc. of the 19th Annual IACR Eurocrypt conference (EUROCRYPT '01)*, Innsbruck, Austria, May 2001.
- 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.
- 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. To Appear in the *Journal of Cryptology*.
- 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.
- 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. Submitted to the *Journal of Cryptology*.
- 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.
- 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.
- 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.

- 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 (invited paper).
- An earlier version appeared in *Proc. of the 30th Annual ACM Symp. on the Theory of Computing (STOC'98)*, Dallas, TX, May 1998.

Other Publications

- Alexander Healy, Anna Lysyanskaya, Tal Malkin, Leonid Reyzin. Zero-Knowledge Sets from General Assumptions. In preparation.
- Michael Locasto, Janak Parekh, Sal Stolfo, Angelos Keromytis, Tal Malkin, Vishal Misra. Collaborative Distributed Intrusion Detection. Submitted for publication.
- Yael Gertner, Tal Malkin. Efficient Distributed $\binom{n}{1}$ Oblivious Transfer. Technical Report MIT-LCS-TR-714, MIT Lab for Computer Science, April 1997.
- Tal Malkin. A Study of Secure Database Access and General Two-Party Computation. Ph.D. Thesis, Massachusetts Institute Of Technology, February 2000.
- Tal Malkin. Deductive Tableaux for Temporal Logic. M.Sc. Thesis, Weizmann Institute of Science, January 1995.

Honors

- CAREER Award, National Science Foundation (NSF), 2004.
- The Knesset (Israeli Parliament) award to most promising undergraduate students in Israel, 1992.
- Graduated Summa Cum Laude, Bar-Ilan University, 1992
- Dean's list for top 3% of research students in the faculty of natural sciences and mathematics in Bar-Ilan university, 1991 and 1992.
- Dean's list for best 40 out of more than 7000 students, Bar-Ilan university, 1991 and 1992.
- The Knesset (Israeli Parliament) award to most promising undergraduate students in Israel, 1991.
- The Rachel and Reuben Jacobs Achievement Award, 1990.
- The Edith Wolfson Achievement Award, 1989.

Grants

- NSF CAREER award. "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.

Patents

- Tal Malkin, Daniele Micciancio, Sara Miner. Forward-Secure Digital Signatures with an Unbounded Number of Time Periods, and Methods for Composition and Efficiency Tradeoffs. Submitted June 2001.

Professional Service

- General and local arrangements chair, the 9th Annual workshop on Practice and Theory in Public Key Cryptography (PKC 2006).

- Program committee member for the RSA Conference, Cryptographers' Track (CT-RSA 2005).
- Program committee member for the 2nd Annual Theory of Cryptography Conference (TCC 2005).
- NSF Panelist, 2004
- Program committee member for 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).
- Program committee member for The 24th Annual IACR Crypto Conference (Crypto 2004).
- Program committee member for The 36th ACM Symposium on Theory of Computing (STOC 2004).
- Program committee member for The Sixth International Workshop on Practice and Theory in Public Key Cryptography (PKC 2003).
- Program committee member for The Ninth Annual Workshop on Selected Areas in Cryptography (SAC 2002).
- Organizer, IBM/NYU/Columbia Theory Day, Spring 2003, Fall 2003, Spring 2004.
- Regular referee for various professional journals and conferences, including:
 - SIAM Journal on Computing
 - SIAM Journal on Discrete Mathematics
 - ACM Transactions on Information and System Security
 - ACM Transactions on Computer Systems
 - Information Processing Letters
 - Journal of Cryptology
 - Theory of Computing Systems
 - Designs, Codes and Cryptography
 - IEEE Symposium on Foundations of Computer Science (FOCS)
 - ACM Symposium on the Theory of Computing (STOC)
 - Advances in Cryptology (CRYPTO and EUROCRYPT)
 - ACM Conference on Computer and Communications Security (CCS)
 - ACM Symposium on Principles of Distributed Computing (PODC)
- Member of ACM, IEEE, IACR (International Association for Cryptologic Research).

*CU/Dept
Service*

- Faculty Retreat Organizer October 2003.
- Events Representative Fall 2003, Spring 2004
- MS Program Committee, member Fall 2003, Spring 2004
- MS Admissions Committee, member Fall 2003, Spring 2004
- Faculty Recruiting Committee, member Spring 2003 - Spring 2004
- Advisor for Juniors in SEAS Spring 2003- Spring 2004
- MS Security Track Advisor Spring 2004
- ACM Research Fair, speaker Fall 2003

- Organizer, Theory Reading Group Spring 2003
- 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
- Students*
- PHD students: Theodore Diament, Ariel Elbaz, Eden (Yian Chee) Hoo
 - PHD Candidacy Committee: Debbie Cook
 - PHD Thesis Committee: Hector Rosario (Teachers College)
 - MS and undergraduate student research supervisor: George Philip Atzemoglou (Spring 2003), Andrew Wan (Fall 2004), Bhargav Bhatt, Noel Codella (Spring 2004)
 - Students Supervised while at AT&T Research: Yael Gertner (UPENN), Kobbi Nissim (Weizmann), Lea Kissner (CMU).
- Invited Talks*
- *Cryptography Workshop, Centre International de Rencontres Mathematiques (CIRM), Luminy, France.* November 2004.
 - Invited panelist on “Managing Mid-Career Changes”, Grace Hopper Celebration of Women in Computing, 2004.
 - *New York University.* A Quantitative Approach to Reductions in Secure Computation. February 2004.
 - *Stevens Institute of Technology.* Algorithmic Tamper-Proof Security. April 2004.
 - *DIMACS/PORTIA workshop and working group on Privacy Preserving Data Mining.* March 2004.
 - *Columbia University.* Secure Multiparty Computation of Approximations. March 2003.
 - *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.
- *Bell Communications Research (Bellcore).* 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.

References Available upon request.

Personal Israeli citizen, H1b visa. Fluent in English, Hebrew, and Russian.