Chris Peikert

Curriculum Vitae

Computer Science and AI Laboratory (CSAIL)
Massachusetts Institute of Technology
32 Vassar Street, Room 32–G608
Cambridge, MA 02139

cpeikert@mit.edu
office: +1 617 253 1499
home: +1 617 945 1208
http://theory.csail.mit.edu/~cpeikert

Research Interests

Cryptography, coding theory, computational complexity, algorithms, and lattices.

Teaching Interests

Cryptography, computer and network security, algorithms, computability and complexity.

Education

Massachusetts Institute of Technology
Ph.D. in Computer Science, June 2006 (expected).
Thesis Title: *Cryptographic Error Correction.*
Minor: Computational Biology.
GPA: 5.0/5.0

Massachusetts Institute of Technology
Bachelor of Science, Master of Engineering in Computer Science, June 2001.
GPA: 5.0/5.0

Massachusetts Institute of Technology
Bachelor of Science in Pure Mathematics, June 2000.
GPA: 4.9/5.0, 5.0 in major

Students Advised

- David A. Wilson, Fall 2004–Spring 2005.

  Advised Master of Engineering thesis, "Error-Free Message Transmission in the Universal Composability Framework."

Research Experience

Massachusetts Institute of Technology, Cambridge, MA.
Research Assistant, Laboratory for Computer Science/Computer Science and Artificial Intelligence Laboratory, September 2002 to May 2005.

Teaching Experience

Cryptography and Cryptanalysis
Teaching Assistant, 6.875, MIT, Spring 2004 (taught by Silvio Micali).
Cryptography and Computer Security
Teaching Assistant, 6.87s, MIT, Summer 2002 (taught by Shafi Goldwasser and Mihir Bellare)
Network and Computer Security
Teaching Assistant, 6.857, MIT, Fall 2005 (taught by Shafi Goldwasser)
Teaching Assistant, 6.857, MIT, Fall 2003 (taught by Ron Rivest)
Introduction to Algorithms
Head Teaching Assistant, 6.046, MIT, Fall 2002 (taught by Erik Demaine and Shafi Goldwasser)
Teaching Assistant, 6.046, MIT, Spring 2001 (taught by Madhu Sudan and Piotr Indyk)
Structure and Interpretation of Computer Programs
Teaching Assistant, 6.001, MIT, Fall 2000 (taught by Eric Grimson)

Publications

Conference Publications

[1] Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *Theory of Cryptography: Third Theory of Cryptography Conference*, New York, NY, March 2006. To appear.

[2] Chris Peikert. On error correction in the exponent. In *Theory of Cryptography: Third Theory of Cryptography Conference*, New York, NY, March 2006. To appear.

[3] Silvio Micali, Chris Peikert, Madhu Sudan, and David A. Wilson. Optimal error correction against computationally-bounded noise. In Joe Kilian, editor, *Theory of Cryptography: Second Theory of Cryptography Conference*, pages 1–16, Cambridge, MA, February 2005. Springer-Verlag.

[4] Matt Lepinski, Silvio Micali, Chris Peikert, and Abhi Shelat. Completely fair SFE and coalition-safe cheap talk. In *PODC '04: Proceedings of the twenty-third annual ACM Symposium on Principles of Distributed Computing*, pages 1–10, St. John's, Newfoundland, Canada, 2004. ACM Press.

[5] Chris Peikert, Abhi Shelat, and Adam Smith. Lower bounds for collusion-secure fingerprinting. In *SODA '03: Proceedings of the fourteenth annual ACM-SIAM Symposium on Discrete Algorithms*, pages 472–479, Baltimore, Maryland, 2003. Society for Industrial and Applied Mathematics.

[6] Anna Lysyanskaya and Chris Peikert. Adaptive security in the threshold setting: From cryptosystems to signature schemes. In *ASIACRYPT '01: Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security*, pages 331–350, Gold Coast, Australia, 2001. Springer-Verlag.

Lectures

Conference Presentations

"Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices"
TCC '06: Third Theory of Cryptography Conference, New York, NY, March 2006.
"On Error Correction in the Exponent"
TCC '06: Third Theory of Cryptography Conference, New York, NY, March 2006.
"Optimal Error Correction Against Computationally-Bounded Noise"
TCC '05: Second Theory of Cryptography Conference, Cambridge, MA, February 2005.
"Lower Bounds for Collusion-Secure Fingerprinting"
SODA '03: Fourteenth ACM-SIAM Symposium on Discrete Algorithms, Baltimore, MD, January 2003.
"Adaptive Security in the Threshold Setting"
ASIACRYPT '01: Seventh International Conference, Gold Coast, Australia, December 2001.

Seminar Presentations

"Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices"
Cryptography and Information Security Seminar, MIT, 2 December 2005.
"Optimal Error Correction Against Computationally-Bounded Noise"
Cryptography and Information Security Seminar, MIT, 15 October 2004.
"Introduction to Coding Theory"
Theory of Computation Student Seminar, MIT, 2 October 2003.
"Probabilistically Checkable Proofs (PCPs)"
Theory of Computation Student Seminar, MIT, 17 April 2003.
"Collusion-Secure Fingerprinting"
Theory of Computation Student Seminar, MIT, 19 September 2002.
"Traitor Tracing for Stateless Receivers"
Theory of Computation Student Seminar, MIT, September 2001.

Awards and Honors

- MIT Presidential Fellowship, 2001–2002.
- First Place, MIT ACM-IEEE Programming Contest (6.370), January 2001.

Professional Activities

Conference reviews	**IEEE Symposium on Foundations of Computer Science (FOCS)**, 2005
	ACM Workshop on Digital Rights Management (DRM), 2005
	International Workshop on Public Key Cryptography (PKC), 2005
	ACM Computer and Communications Security (CCS), 2005
	IACR Theory of Cryptography Conference (TCC), 2005
	IACR Advances in Cryptology — EUROCRYPT, 2004
	IACR Advances in Cryptology — CRYPTO, 2002, 2003
Journal reviews	**IACR Journal of Cryptology**, Volume 18, 2005
	IEEE Transactions on Signal Processing, Supplement on Secure Media, 2004

References

Prof. Silvio Micali

MIT Computer Science and Artificial Intelligence Laboratory
32 Vassar Street, 32-G644
Cambridge, MA 02139
(617) 253-5949
silvio@theory.csail.mit.edu

Prof. Shafi Goldwasser

MIT Computer Science and Artificial Intelligence Laboratory
32 Vassar Street, 32-G682
Cambridge, MA 02139
(617) 253-5914
shafi@theory.csail.mit.edu

Prof. Madhu Sudan

MIT Computer Science and Artificial Intelligence Laboratory
32 Vassar Street, 32-G640
Cambridge, MA 02139
(617) 253-9680
madhu@theory.csail.mit.edu

Prof. Ron Rivest

MIT Computer Science and Artificial Intelligence Laboratory
32 Vassar Street, 32-G692
Cambridge, MA 02139
(617) 253-5880
rivest@theory.csail.mit.edu