

# Chris Peikert

## *Curriculum Vitae*

School of Computer Science  
Georgia Institute of Technology  
266 Ferst Dr.  
Atlanta, GA 30332

cpeikert@cc.gatech.edu  
Phone: (404) 385-3264  
<http://www.cc.gatech.edu/~cpeikert/>

## Research Interests

Cryptography, lattices, error-correcting codes, algorithms and complexity, computer and network security.

## Education

### Massachusetts Institute of Technology

Ph.D. in Computer Science, July 2006.  
Advisor: Silvio Micali  
Thesis: *Cryptographic Error Correction*.  
GPA: 5.0/5.0

### Massachusetts Institute of Technology

Masters of Engineering in Computer Science, June 2001.  
Advisors: Ronald L. Rivest and Anna Lysyanskaya  
Thesis: *Adaptive Security in the Threshold Setting*.  
GPA: 5.0/5.0

### Massachusetts Institute of Technology

Bachelor of Science in Mathematics, June 2000.  
GPA: 4.9/5.0 (5.0 in major)

## Employment History

### Georgia Institute of Technology, Atlanta, GA.

*Assistant Professor*, School of Computer Science, College of Computing, August 2009 to present.

### SRI International (Stanford Research Institute), Menlo Park, CA.

*Research Scientist*, Computer Science Laboratory, August 2006 to August 2009.

### Massachusetts Institute of Technology, Cambridge, MA.

*Research Assistant*, Computer Science and Artificial Intelligence Laboratory, Sep 2002 to May 2006.

*Teaching Assistant*, Fall 2005, Spring 2004, Fall 2003, Summer 2002, Fall 2002, Spring 2001, Fall 2000.

Cryptography and Cryptanalysis, Network and Computer Security, Introduction to Algorithms,  
Cryptography and Computer Security, Structure and Interpretation of Computer Programs.

## Awards and Honors

- Best Paper Award at STOC 2009; invited to *Journal of the ACM*, for [6].
- Invited to *Theory of Computing Systems* special issue on STACS 2009, for [7].
- Invited to *SIAM Journal of Computing* special issue on STOC 2008, for [12].
- Invited to *Computational Complexity* special issue on CCC 2007, for [14].
- MIT Presidential Fellowship, 2001–2002.
- First Place, MIT ACM-IEEE Programming Contest (6.370), January 2001.

## Scientific Papers

### In Submission

- [1] Chris Peikert. An efficient and parallel Gaussian sampler for lattices. Submitted, 2010.
- [2] Adam O’Neill and Chris Peikert. Bidegradable public-key encryption. Submitted, 2010.
- [3] Tal Malkin, Chris Peikert, Rocco A. Servedio, and Andrew Wan. Learning an overdetermined basis: Analysis of lattice-based signatures with perturbations. Submitted, 2009.
- [4] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem. **Submitted by invitation to Journal of the ACM**, 2009.
- [5] Joël Alwen and Chris Peikert. Generating shorter bases for hard random lattices. **Submitted by invitation to Theory of Computing Systems special issue on STACS ’09**, 2009.

### Journal Articles

- [1] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. *SIAM J. Comput.*, 2010. **Accepted. By invitation to special issue on STOC ’08.**
- [2] Chris Peikert. Limits on the hardness of lattice problems in  $\ell_p$  norms. *Computational Complexity*, 17(2):300–351, May 2008. **By invitation to special issue on CCC ’07.**

### Refereed Conference Publications

- [1] David Cash, Dennis Hofheinz, Eike Kiltz, and Chris Peikert. Bonsai trees, or how to delegate a lattice basis. In *Proceedings of EUROCRYPT ’10*, 2010.
- [2] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *Proceedings of EUROCRYPT ’10*, 2010.
- [3] Yevgeniy Dodis, Shafi Goldwasser, Yael Kalai, Chris Peikert, and Vinod Vaikuntanathan. Public-key encryption schemes with auxiliary inputs. In *Proceedings of TCC ’10 (Theory of Cryptography Conference)*, pages 361–381, 2010.
- [4] Shafi Goldwasser, Yael Kalai, Chris Peikert, and Vinod Vaikuntanathan. Robustness of the learning with errors assumption. In *Proceedings of ICS ’10 (Symposium on Innovations in Computer Science)*, 2010.
- [5] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In *Proceedings of CRYPTO ’09*, pages 595–618, 2009.

- [6] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In *Proceedings of STOC '09 (Symposium on Theory of Computing)*, pages 333–342, 2009. **Awarded Best Paper.**
- [7] Joël Alwen and Chris Peikert. Generating shorter bases for hard random lattices. In *Proceedings of STACS '09 (Symposium on Theoretical Aspects of Computer Science)*, pages 75–86, 2009.
- [8] Yuriy Arbitman, Gil Dogon, Vadim Lyubashevsky, Daniele Micciancio, Chris Peikert, and Alon Rosen. SWIFFTX: A proposal for the SHA-3 standard. Submitted to NIST SHA-3 competition, 2008.
- [9] Chris Peikert, Vinod Vaikuntanathan, and Brent Waters. A framework for efficient and composable oblivious transfer. In *Proceedings of CRYPTO '08*, pages 554–571, 2008.
- [10] Chris Peikert and Vinod Vaikuntanathan. Noninteractive statistical zero-knowledge proofs for lattice problems. In *Proceedings of CRYPTO '08*, pages 536–553, 2008.
- [11] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of STOC '08 (Symposium on Theory of Computing)*, pages 197–206, 2008.
- [12] Chris Peikert and Brent Waters. Lossy trapdoor functions and their applications. In *Proceedings of STOC '08 (Symposium on Theory of Computing)*, pages 187–196, 2008.
- [13] Vadim Lyubashevsky, Daniele Micciancio, Chris Peikert, and Alon Rosen. SWIFFT: A modest proposal for FFT hashing. In *Proceedings of FSE '08 (Fast Software Encryption)*, pages 54–72, 2008.
- [14] Chris Peikert. Limits on the hardness of lattice problems in  $\ell_p$  norms. In *Proceedings of CCC '07 (Conference on Computational Complexity)*, pages 333–346, 2007.
- [15] Chris Peikert and Alon Rosen. Lattices that admit logarithmic worst-case to average-case connection factors. In *Proceedings of STOC '07 (Symposium on Theory of Computing)*, pages 478–487, 2007.
- [16] Vadim Lyubashevsky, Daniele Micciancio, Chris Peikert, and Alon Rosen. Provably secure FFT hashing. NIST 2nd Cryptographic Hash Workshop, August 2006.
- [17] Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *Proceedings of TCC '06 (Theory of Cryptography Conference)*, pages 145–166, March 2006.
- [18] Chris Peikert. On error correction in the exponent. In *Proceedings of TCC '06 (Theory of Cryptography Conference)*, pages 167–183, 2006.
- [19] Silvio Micali, Chris Peikert, Madhu Sudan, and David A. Wilson. Optimal error correction against computationally bounded noise. In *Proceedings of TCC '05 (Theory of Cryptography Conference)*, pages 1–16, 2005.
- [20] Matt Lepinski, Silvio Micali, Chris Peikert, and Abhi Shelat. Completely fair SFE and coalition-safe cheap talk. In *Proceedings of PODC '04 (Symposium on Principles of Distributed Computing)*, pages 1–10, 2004.
- [21] Chris Peikert, Abhi Shelat, and Adam Smith. Lower bounds for collusion-secure fingerprinting. In *Proceedings of SODA '03 (Symposium on Discrete Algorithms)*, pages 472–479, 2003.
- [22] Anna Lysyanskaya and Chris Peikert. Adaptive security in the threshold setting: From cryptosystems to signature schemes. In *Proceedings of ASIACRYPT '01*, pages 331–350, 2001.

# Expository Talks

## Invited Lectures

- **Recent Progress in Lattice-Based Cryptography**
  1. *Featured Tutorial*, Workshop on Public-Key Cryptography and the Geometry of Numbers, Mathematical Institute of Leiden University, May 2010 (scheduled)
  2. *Invited Tutorial*, 6th Theory of Cryptography Conference, 15 Mar 2009
- **Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem [6]**
  3. ECRYPT Workshop on Lattices and Cryptography, Jun 2010 (scheduled)
  4. Workshop on Computer Security and Cryptography, Centre de Recherches Mathématiques, Université de Montréal, Apr 2010 (scheduled)
  5. Workshop on the Status of Impagliazzo's Worlds, Princeton University, 3 June 2009
  6. Schloss Dagstuhl, Germany, 1 Dec 2008
  7. Massachusetts Institute of Technology, 21 Nov 2008
- **How to Use a Short Basis: New Lattice-Based Cryptographic Constructions [11]**
  8. Carnegie Mellon University, 5 Dec 2008
  9. Bay Area Theory Symposium, 7 Nov 2008
  10. Georgia Institute of Technology, 11 Mar 2008
  11. Massachusetts Institute of Technology, 9 Nov 2007
  12. University of Maryland, 8 Nov 2007
  13. Penn State University, 6 Nov 2007
- **Lossy Trapdoor Functions and Their Applications [12]**
  14. Microsoft Research Silicon Valley, 12 Jun 2008
  15. Columbia University, 13 Mar 2008
  16. University of California, San Diego, 21 Nov 2007
  17. University of California, Berkeley, 10 Sep 2007
- **A Framework for Efficient and Composable Oblivious Transfer [9]**
  18. Georgia Institute of Technology, 12 Mar 2008.
- **Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices [17]**
  19. Massachusetts Institute of Technology, 2 Dec 2005.
- **Optimal Error Correction Against Computationally Bounded Noise [19]**
  20. Massachusetts Institute of Technology, 15 Oct 2004.

## Conference Presentations

1. **STOC '09**: Public-Key Cryptosystems from the Worst-Case Shortest Vector Problem
2. **CRYPTO '08**: A Framework for Efficient and Composable Oblivious Transfer
3. **STOC '08**: Trapdoors for Hard Lattices and New Cryptographic Constructions
4. **Complexity '07**: Limits on the Hardness of Lattice Problems in  $\ell_p$  Norms
5. **STOC '07**: Lattices that Admit Logarithmic Worst-Case to Average-Case Connection Factors
6. **TCC '06**: Efficient Collision-Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices

7. **TCC '06**: On Error Correction in the Exponent
8. **TCC '05**: Optimal Error Correction Against Computationally Bounded Noise
9. **SODA '03**: Lower Bounds for Collusion-Secure Fingerprinting
10. **ASIACRYPT '01**: Adaptive Security in the Threshold Setting

## Grants

- Principal Investigator, NSF Grant #CNS-0716786, “Efficient Cryptography Based on Lattices,” Aug 2007 – Aug 2010
- Co-PI, NSF Grant #CNS-0749931, “Securing the Computing and Information Future: Principled Foundations and New Cryptographic Abstractions,” Sep 2007 – Sep 2009
- Co-PI, I3P Grant “Safeguarding Digital Identity,” Jul 2007 – Jul 2009

## Teaching and Advising

### Courses Taught

Term	Course	Comments
Spring 2010	CS 8803 TFC: Theoretical Foundations of Cryptography	graduate-level course
Fall 2009	CS 1332: Data Structures and Algorithms	guest lecture

### Students Supervised

#### Masters Students

- **Akash Kumar** (Georgia Tech, Spring 2010): Special problem: Decoding algorithms on lattices
- **Indranil Banerjee** (Georgia Tech, Fall 2009–Spring 2010): Efficiency of lattice-based cryptography
- **David A. Wilson** (MIT, 2004–2005): Co-advisor (with Ronald L. Rivest), Masters thesis: Error Correction in the Universal Composability Framework

#### Summer Students (at SRI)

- **Andrew Wan** (Columbia University, Summer 2008): Analysis of lattice-based signatures with perturbations
- **Joël Alwen** (New York University, Summer 2008): Generating shorter bases for cryptographic lattices
- **Vinod Vaikuntanathan** (MIT, Summer 2007): New lattice-based cryptographic constructions

## Professional Activities

*Program Committee Member*    **STOC** (Symposium of Theory of Computing) 2010  
**PQC** (Post-Quantum Cryptography) 2010  
**CRYPTO** 2009  
**TCC** (Theory of Cryptography Conference) 2008

*Journal Referee*                **Journal of the ACM**  
**IACR Journal of Cryptology**  
**IEEE Transactions on Information Theory**  
**IEEE Transactions on Signal Processing**

*Conference Referee*  
*(Selected venues)*                **FOCS** (Symposium on Foundations of Computer Science) 2005, 2007, 2008  
**STOC** (Symposium on Theory of Computing) 2009  
**SODA** (Symposium on Discrete Algorithms) 2008, 2009, 2010  
**CRYPTO** 2002, 2003, 2008  
**EUROCRYPT** 2004, 2007, 2008, 2009  
**TCC** (Theory of Cryptography Conference) 2005, 2007, 2009, 2010  
**ASIACRYPT** 2009  
**FSE** (Fast Software Encryption) 2009  
**CCS** (Computer and Communications Security) 2005