Melissa E. Chase

CONTACT INFORMATION
Computer Science Department
Brown University, Box 1910
Providence, RI 02906 USA

Phone: (310) 995-1456
E-mail: mchase@cs.brown.edu

RESEARCH INTERESTS
Cryptography
Recent work: definitions and constructions of new primitives, attribute-based encryption, simulatable verifiable random functions, NIZK proof techniques

EDUCATION

Brown University, Providence, Rhode Island (2003-present)
MS in Computer Science, May 2005
Candidate for Ph.D. (Advisor: Anna Lysyanskaya)

Harvey Mudd College, Claremont, California (1999-2003)
B.S. with High Honors in Computer Science, May 2003
B.S. with High Honors in Mathematics, May 2003

APPOINTMENTS

IBM Research, Zurich, Summer Visitor. Summer 2007

Graduate Teaching Assistant: Introduction to Cryptography. Spring 2007

NSF Graduate Research Fellow. Fall 2004 – Spring 2007

IPAM Fellow (Long program – Securing Cyberspace: Applications and Foundations of Cryptography and Computer Security, UCLA, CA). Fall 2006

PUBLICATIONS

Belenkiy, Mira, Jan Camenisch, M. Chase, Markulf Kohlweiss, Anna Lysyanskaya, Hovav Shacham. Delegatable Anonymous Credentials. (in submission)

Belenkiy, Mira, M. Chase, Markulf Kohlweiss, Anna Lysyanskaya. Non-Interactive Anonymous Credentials. In proceedings of *Theoretical Cryptography Conference 2008*. (to appear)

Belenkiy, Mira, M. Chase, Chris Erway, John Jannotti, Alptekin Kupcu, Anna Lysyanskaya, Eric Raclin. Making P2P Accountable without Losing Privacy. In proceedings of *Workshop on Privacy in the Electronic Society 2007*.

Chase, M. and Anna Lysyanskaya. Simulatable VRFs with Applications to Multi-Theorem NIZK. In proceedings of *Advances in Cryptology - CRYPTO 2007*.

Chase, M. Multi-Authority Attribute Based Encryption. In proceedings of *Theoretical Cryptography Conference 2007*.

Chase, M. and Anna Lysyanskaya. On Signatures of Knowledge. In *Advances*

in Cryptology - CRYPTO 2006.

Chase, M., Alex Healey, Anna Lysyanskaya, Tal Malkin, and Leo Reyzin. Mercurial Commitments and Applications to Zero Knowledge Sets. In *Advances in Cryptology - EUROCRYPT 2005.*

Presentations

Simulatable Verifiable Random Functions. Dagstuhl seminar on Cryptography, Saarland, Germany – Sept 2007

Simulatable VRFs with Applications to Multi-Theorem NIZK. Crypto 2007, Santa Barbara, CA – Aug 2007

Multi-Authority Attribute-Based Encryption. TCC 2007, Amsterdam, Netherlands – Feb 2007

Multi-Authority Attribute-Based Encryption. IPAM, UCLA – Nov 2006

On Signatures of Knowledge. CRYPTO 2006, Santa Barbara, CA – Aug 2006

Mercurial Commitments and Applications to Zero Knowledge Sets. Eurocrypt 2005, Aarhus, Denmark – May 2005

Other Contributions

Program Committee for CRYPTO 2008.

Local Arrangements Committee Volunteer for FOCS 2007.

External Reviewer for TCC 2005, CRYPTO 2005, TCC 2006, PKC 2006, CRYPTO 2006, PKC 2007, Eurocrypt 2007, FOCS 2007, J. Computer Security.

Brown Computer Science Theory Lunch Organizer: Jan 2005 – May 2006

Brown Ballroom Dance Team Captain: Jan 2005 – Dec 2006

Undergraduate Research

Fall 2002 - Spring 2003: Undergraduate Thesis
Shortest Path Problems: Multiple Paths in a Stochastic Graph
Advisor: Ran Libeskind-Hadas, Harvey Mudd College

Summer 2002: Research in Programming Languages
Improving Error Reporting in SML Typechecker
Advisor: Christopher Stone, Harvey Mudd College

Fall 2001 - Spring 2003: Clinic project for ESRI, Inc.
Algorithms and Data Structures for Time-Dependent Graphs
Advisor: Ran Libeskind-Hadas, Harvey Mudd College