

PAYMAN MOHASSEL

CONTACT INFO

pmohasse@cpsc.ucalgary.ca
<http://pages.cpsc.ucalgary.ca/~pmohasse>
(403) 210 6105

ADDRESS

642 ICT Building
Department of Computer Science
University of Calgary
Calgary, AB, Canada

EDUCATION

University of California, Davis Davis, CA
Ph.D. Computer Science June 2009

University of California, Davis Davis, CA
B.S. Computer Science June 2004

EXPERIENCE

Assistant Professor July 2009-Present
Department of Computer Science, University of Calgary Calgary, AB

Graduate Research Assistant Winter 2005-Spring 2009
Advisor: Matthew Franklin

Internship with SECUR-IT June 2008-Aug. 2008
<http://www.truststc.org/securit>

Internship at Sun June 2008-Aug. 2008
Sun's IT security office

Internship at Google May 2007-Aug. 2007
Adsense group

Fellow at IPAM Sept. 2006-Dec. 2006
University of California, Los Angeles

REU Research Fellow Spring and Summer 2004
Math Department, University of California, Davis

PUBLICATIONS

- [13] Payman Mohassel, and Matthew Franklin. *Secure and Efficient Evaluation of Multivariate Polynomials and Applications*. To Appear at Applied Cryptography and Network Security Conference, ACNS 2010.
- [12] Eike Kiltz, Payman Mohassel, and Adam O'Neill. *Adaptive Trapdoor Functions and Chosen Ciphertext Security*. To appear at Advances in Cryptology, EUROCRYPT 2010.
- [11] Mark Gondree, and Payman Mohassel. *Longest Common Subsequence as Private Search*. In Proceedings of ACM Workshop on Privacy in Electronic Society (WPES), 2009.
- [10] Matthew Franklin, Mark Gondree, and Payman Mohassel. *Communication-Efficient Private Protocols for Longest Common Subsequence*. In Proceedings of RSA conference, Cryptographer's Track (CT-RSA) 2009.
- [9] Payman Mohassel, and Enav Weinreb. *Efficient Secure Linear Algebra in the Presence of Covert or Computationally Unbounded Adversaries*. In Proceedings of Advances in Cryptology, CRYPTO, 2008.
- [8] Vipul Goyal, Payman Mohassel, and Adam Smith. *Secure Two-party and Multi-party Computation against Covert Adversaries*. In Proceedings of Advances in Cryptology, EUROCRYPT, 2008.
- [7] Matthew Franklin, Mark Gondree, and Payman Mohassel. *Multiparty Indirect Indexing and Applications*. In Proceedings of Advances in Cryptology, ASIACRYPT, 2007.
- [6] Nenad Dedic, and Payman Mohassel. *Constant-Round Private Database Queries*. In Proceedings of International Colloquium on Automata, Languages and Programming (ICALP), 2007.
- [5] Eike Kiltz, Payman Mohassel, and Enav Weinreb and Matthew Franklin. *Secure Linear Algebra Using Linearly Recurrent Sequences*. In Proceedings of Theory of Cryptography Conference (TCC), 2007.
- [4] Matthew Franklin, Mark Gondree, and Payman Mohassel. *Improved Efficiency for Private Stable Matching*. In Proceedings of RSA conference, cryptographer's track (CT-RSA), 2007.
- [3] Payman Mohassel, and Matthew Franklin. *Efficiency Tradeoffs for Malicious Two-Party Computation*. In Proceedings of Public Key Cryptography Conference (PKC), 2006.
- [2] Payman Mohassel, and Matthew Franklin. *Efficient Polynomial Operations in the Shared-Coefficients Setting*. In Proceedings of Public Key Cryptography Conference (PKC), 2006.
- [1] Gergei Bana, Payman Mohassel, and Till Stegers. *Computational Soundness of Formal Indistinguishability and Static Equivalence*. 11th Annual Asian Computing Conference (ASIAN'06), 2006.

TALKS

CCA Security and Trapdoor Functions. Presented at CRM Workshop, Montreal, April 2010.

Encryption Schemes and General Assumptions. Presented at Theory Seminar, Calgary, January, 2010.

Longest Common Subsequence as Private Search. Presented at ACM CCS, WPES workshop, Chicago, December, 2009.

Communication-Efficient Private Protocols for Longest Common Subsequence. Presented at RSA 2009, San Francisco, April 2009.

Towards More Practical Secure Computation. Interview talk given at Bell Labs, Microsoft Research Redmond, and University of Calgary, December-March 2009.

Efficient Secure Linear Algebra in the Presence of Covert or Computationally Unbounded Adversaries. Presented at Crypto 2008, Santa Barbara, USA, August 2008.

Secure Two-party and Multi-party Computation against Covert Adversaries. Presented at Eurocrypt 2008, Istanbul, Turkey, April 2008.

Constant-Round Private Database Queries. Presented at ICALP 2007, Wroclaw, Poland, July 2007.

Improved Efficiency for Private Stable Matching. Presented at RSA 2007, San Francisco, USA, February 2007.

Efficiency Tradeoffs for Malicious Two-Party Computation. Presented at PKC 2006, New York City, USA, April 2006.

Efficient Polynomial Operations in the Shared-Coefficients Setting. Presented at PKC 2006, New York City, USA, April 2006.

TEACHING

Winter 2011

Foundations of Modern Cryptography (CPSC 601.48)

Network Systems Security (CPSC 526)

Explorations in Information Security and Privacy (CPSC 329)

Winter 2010

Foundations of Modern Cryptography (CPSC 601.48)

Information and Network Security (CPSC 529)

ACTIVITIES

Program Committees

ASIACRYPT 2010

ACM WPES 2010