Shashank Agrawal

E-mail: sagrawl2@illinois.edu
Homepage: web.engr.illinois.edu/~sagrawl2

312 W Springfield Ave Apt 2,
Champaign, IL 61820.

Interests

Cryptography, Secure Multi-party Computation, and Computer Security.

Education

PhD in Computer Science August 2011 - May 2016 (Expected)
Advisor: Manoj Prabhakaran
University of Illinois at Urbana-Champaign (UIUC).

MS by Research in Computer Science August 2009 - May 2011
Advisor: Kannan Srinathan
International Institute of Information Technology, Hyderabad (IIIT-H).

B.Tech in Computer Science and Engineering July 2005 - May 2009
International Institute of Information Technology, Hyderabad (IIIT-H).

Publications

Cryptographic Agents: Towards a Unified Theory of Computing on Encrypted Data
Shashank Agrawal, Shweta Agrawal, Manoj Prabhakaran
To appear at Eurocrypt 2015

A Rate-Optimizing Compiler for Non-malleable Codes Against Bit-wise Tampering and Permutations
Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey, Manoj Prabhakaran
To appear at TCC 2015

On the Practical Security of Inner Product Functional Encryption
Shashank Agrawal, Shweta Agrawal, Saikrishna Badrinarayanan, Abishek Kumarasubramanian, Manoj Prabhakaran, Amit Sahai
To appear at PKC 2015

Controlled Functional Encryption
Muhammad Naveed, Shashank Agrawal, Manoj Prabhakaran, XiaoFeng Wang, Erman Ayday, Jean-Pierre Hubaux, Carl A. Gunter
ACM Conference on Computer and Communications Security (CCS) 2014

Lower Bounds in the Hardware Token Model
Shashank Agrawal, Prabhanjan Ananth, Vipul Goyal, Manoj Prabhakaran, and Alon Rosen
Theory of Cryptography (TCC) 2014

On Fair Exchange, Fair Coins and Fair Sampling
Shashank Agrawal and Manoj Prabhakaran
Advances in Cryptology (CRYPTO) 2013

Verifiable Secret Sharing in a total of three rounds
Shashank Agrawal
Information Processing Letters (IPL) 2012

Interplay between (im)perfectness, synchrony and connectivity: The Case of Reliable Message Transmission
Abhinav Mehta, Shashank Agrawal, and Kannan Srinathan
International Conference on Distributed Computing and Networking (ICDCN), 2012
Invited and accepted to a special issue of Theoretical Computer Science (TCS) journal

Secure Message Transmission in Asynchronous Directed Graphs
Shashank Agrawal, Abhinav Mehta, and Kannan Srinathan
International Conference on Cryptology in India (INDOCRYPT), 2012

Minimal Connectivity for Unconditionally Secure Message Transmission in Synchronous Directed Networks
Manan Nayak, Shashank Agrawal, and Kannan Srinathan
International Conference on Information Theoretic Security (ICITS), 2011

BA: Synchronous Las Vegas URMT Iff Asynchronous Monte Carlo URMT
Abhinav Mehta, Shashank Agrawal, and Kannan Srinathan
International Symposium on Distributed Computing (DISC), 2010

Research in Progress

A study of Pair Encodings: Predicate Encryption in prime order groups
Shashank Agrawal, Melissa Chase
Manuscript

Explicit Non-Malleable Codes Resistant to Permutations and Perturbations
Shashank Agrawal, Divya Gupta, Hemanta K. Maji, Omkant Pandey, Manoj Prabhakaran
Manuscript, available on eprint

Function Private Functional Encryption and Property Preserving Encryption: New Definitions and Positive Results
Shashank Agrawal, Shweta Agrawal, Saikrishna Badrinarayanan, Abishek Kumarasubramanian, Manoj Prabhakaran, and Amit Sahai
Manuscript, available on eprint

Experience

Research Internship at Microsoft Research, Redmond, WA. June - August 2014
Guide: Melissa Chase

Research Internship at Microsoft Research, Bangalore, India. June - July 2012
Guide: Vipul Goyal

Teaching Assistant for Fundamental Algorithms, Introduction to Computing (UIUC); Data Structures, Theory of Computation, Mathematics I, Mathematics II, Formal Methods (IIIT-H).

Participant, Google Summer of Code May - August 2009

Internship, Amazon Dev. Center, Hyderabad, India. April - July 2008

Achievements

C.L. and Jane W.-S. Liu Award: This award is given by the Computer Science department at UIUC in support of one graduate student every year, who shows exceptional research promise relatively early in their graduate studies.

Feng Chen Memorial Award: This award, given by the Computer Science department at UIUC, recognizes students who have received a Best Paper Award or whose paper was chosen for a special journal issue featuring best/top papers.

Awarded Student Travel Grants for attending

- ACM CCS 2014 in Scottsdale, AZ;
- CRYPTO 2012 and CRYPTO 2013 in Santa Barbara, CA;
- Theory and Practice of Multiparty Computation workshop in Aarhus, Denmark (June 2012).

Commendation Award by IIIT-Hyderabad for service to Yuktahaar Mess.

Talks and Presentations

Cryptographic Agents
- Microsoft Research, Redmond, July, 2014
- UIUC Theory Seminar, February, 2014

Non-Malleable Codes
- Indian Institute of Technology, Delhi, January, 2015
- Midwest Theory Day, Purdue University, May, 2014

Controlled Functional Encryption
- Microsoft Research, Redmond, June, 2014

Function Private Functional Encryption and Property Preserving Encryption
- ITI TSS Seminar, UIUC, November, 2013

Fair Exchange, Fair Coins and Fair Sampling
- Crypto 2013, August, 2013
- UIUC Theory Seminar, April, 2013

Service

External Reviewer for Asiacrypt 2012, TCC 2013, ICISC 2013, TCC 2014, Asiacrypt 2014, PKC 2015 and TCC 2015.

Student Member of the Graduate Admissions Committee 2014, Dept. of Computer Science, UIUC.