Amit Datta

Contact Information

Doctoral Student
Department of Electrical and Computer Engineering
The Carnegie Mellon University
2119B, CIC, 4720 Forbes Avenue
Pittsburgh, PA 15213-3890 USA

Mobile: +1- 412-759-6378
E-mail: amitdatta@cmu.edu
url: https://www.andrew.cmu.edu/user/amitdatt/

Research Interests

Privacy, Cryptography, Computer Security, Secret Sharing.

Education

Carnegie Mellon University, Pittsburgh, USA
Graduate Student, Department of Electrical and Computer Engineering
- Ongoing, since Fall 2012. Current GPA: 3.58/4.00
- Advisor: Prof. Anupam Datta

Indian Institute of Technology, Kharagpur, India
B.Tech. (Hons), Department of Computer Science and Engineering, August 2012
- Thesis Title: *Towards a Faster Fully Homomorphic Encryption Scheme*
- Thesis Advisor: Prof. Debdeep Mukhopadhyay
- Final GPA: 9.45/10

Ramakrishna Mission Vidyalaya, Narendrapur, India
Higher Secondary Examination, March 2008
- Stood second from the school with an aggregate score of 87.61%.

Secondary Examination, March 2006
- Topped the school with aggregate score of 93.25%. 100% score in Mathematics.

Publications

[1] Amit Datta, Michael Tschantz, Anupam Datta. Automated experiments on ad privacy settings: A tale of opacity, choice, and discrimination. In: *PETS 2015*.

[2] Amit Datta, Anupam Datta, Deirdre K. Mulligan, Michael Tschantz. Discrimination in Online Personalization: A Multidisciplinary Inquiry In: *PLSC 2015*.

[3] Michael Tschantz, Amit Datta, Anupam Datta, Jeannette Wing. A methodology for information flow experiments. In: *CSF 2015*.

[4] Amit Datta, Anupam Datta, Ariel D Procaccia, Yair Zick. Influence in Classification via Cooperative Game Theory. In: *IJCAI 2015*.

[5] Michael Backes, Amit Datta, Aniket Kate. Asynchronous Computational VSS with Reduced Communication Complexity. In: *CT-RSA 2013*.

[6] Chester Rebeiro, Rishabh Poddar, Amit Datta, Debdeep Mukhopadhyay. An Enhanced Differential Cache Attack on CLEFIA for Large Cache Lines. In: *Indocrypt 2011*.

[7] Rishabh Poddar, Amit Datta, Chester Rebeiro. A Cache Trace Attack on CAMELLIA. In: *International Conference on Security Aspects in Information Technology, High-Performance Computing and Networking 2011* .

[8] Anjan Sarkar, Rupert Reiger, Subhro Roy, Rahul Chatterjee, Amit Datta, Jai Prakash Gupta, Arvind Sowmyan SLAM using Relational-Trees and Semantics In: *International Conference on Management, Manufacturing and Material Engineering 2011* .

Internships

Exact Private Aggregation with Fault Tolerance (Summer 2015)

- Mentors: Nadia Fawaz and Marc Joye, Technicolor Personalization Lab, Los Altos.
- I worked on improving the state-of-the-art techniques for private aggregation using cryptographic and information theoretic techniques.

Identifying flows in Big Data (Summer 2014)

- Mentor: Saikat Guha, Microsoft Research, Bangalore.
- I worked on identifying data-flows in big data applications from data-logs without using the scripts generating the logs. I used C# and Scope to implement my techniques on Microsoft's big data platform - Cosmos.

Oblivious RAM (Summer 2012)

- Mentors: Michael Backes and Aniket Kate, Max Planck Intitute for Software Systems, Saarbrcken.
- Oblivious RAM aims at allowing remote access to data without giving away even the access patterns of the data to the server. The objective of this work was to explore the various algorithms for O-RAM and try and improve the current known complexities.

Asynchronous Verifiable Secret Sharing with better complexity (Summer 2011)

- Mentors: Michael Backes and Aniket Kate, Max Planck Intitute for Software Systems, Saarbrcken.
- Devised a new AVSS protocol with a communication complexity of $O(\kappa n^2)$, improving the known best complexity of $O(\kappa n^3)$, where n is the number of parties participating in the secret sharing scheme and k is the security parameter.

Online Assets Management Software (Summer 2009)

- Mentor: Prakash Tripathi, Shriram Insight Share Brokers Ltd., Kolkata.
- Developed an online software for managing the assets of the firm.

Technical Skills

- Programming Languages: C, C++, Python, Java.
- Database Management Systems: MySQL, SQL Server 2005, Oracle.
- Web Development: HTML, JavaScript, CSS, PHP.
- Productivity Applications: LaTeX, Version Control (Git, SVN).
- Operating Systems: Windows, Ubuntu, Mac OS.

Research Experience

Information Flow Experiments

- With Prof. Anupam Datta and Dr. Michael Tschantz
- This work aims to carry out Information Flow Analysis on online advertising networks and detect privacy violations that stem from the use of sensitive information in targeted advertising. Experiments were carried out on Python with bindings for Selenium, R, SciKit etc.

Asynchronous Verifiable Secret Sharing with improved communication complexity

- With Prof. Michael Backes and Dr. Aniket Kate
- Devised a new AVSS protocol with a communication complexity of $O(\kappa n^2)$, improving the known best complexity of $O(\kappa n^3)$, where n is the number of parties participating in the secret sharing scheme andκ is the security parameter.

Towards a Faster Fully Homomorphic Encryption Scheme

- With Prof. Debdeep Mukhopadhyay
- Proposed a new technique to improve the running times of Gentry's Fully Homomorphic Encryption Scheme by parallelizing the most costly operation using the CUDA architecture. This work formed the basis for my B.Tech thesis.

Differential Cache Attacks on Block Ciphers

- With Prof. Debdeep Mukhopadhyay
- Deployed an enhanced cache trace attack on CLEFIA using the differential property of the s-boxes of the cipher and the diffusion properties of the linear transformations of the underlying Feistel structures.
- Extended this attack to another cipher CAMELLIA, a block cipher jointly created by Mitsubishi and NTT.

Oblivious RAM Simulation

- Prof. Michael Backes and Dr. Aniket Kate
- Oblivious RAM allows remote access to data without giving away even the access patterns of the data to the server. I explored various algorithms for O-RAM and worked on improving the run-time complexities.

Localization and Navigation using Semantics

- With Prof. Anjan Sarkar
- Developed and simulated a method for SLAM[Simultaneous Localization and Mapping] using segmented images obtained from two sensors (optical and radar) aboard a UAV.

Development Projects

Information Flow Experiments

- For detecting information flows in advertising networks, I set up experiments involving several parallel browser instances, each simulating an online persona, and then collecting advertisements from a neutral website. The advertisements were then analyzed by carrying out statistical tests. The code is available on git: github.com/tadatitam/info-flow-experiments
- Worked with Selenium Webdriver, R, Python.

Online Assets Management Software

- As an intern at Shriram Insight Sharebrokers Ltd., I developed a web-based software solution to manage the firm's assets.
- Worked with .NET framework, SQL Server 2005, HTML, CSS, Javascript.

RailConnect

- Designed and developed a web-service to find railway connections between any two stations in India. Some of the major difficulties we faced were the sheer number of stations and trains, and long delays.
- Won second prize at Yahoo! HackU, Kharagpur, 2012.
- Languages: Python, Javascript, HTML, CSS.

Development of Mail & Chat Server/Client

- Guide: Prof. Arobinda Gupta and Prof. Indranil Sengupta
- Implemented a mail sever/client pair based on the SMTP and POP3 protocols, and a chat service with provisions for multi-user conferencing, using TCP/IP protocols.
- Work done as part of the course Computer Networks, Autumn 2011
- Language: C.

CourseForum

- Guide: Prof. Pabitra Mitra
- Designed and developed an online portal for ranking and recommending courses on the lines of CourseRank
- Work done as part of the course Database Management Systems, Spring 2011
- Language: RubyOnRails

Teaching Assistant

Foundations of Privacy (18-734), Fall 2014.
Foundations of Privacy (18-734), Fall 2015.

Awards and Recognitions

Carnegie Mellon University

- The Dean's Tuition Fellowship, 2012-2013.

Indian Institute of Technology, Kharagpur

- Singapore Technologies (ST) Engineering Scholarship, 2009-2012.
- Fellowships from the Max-Planck-Institute for Software Systems, 2011 & 2012.

Ramakrishna Mission Vidyalaya, Narendrapur

- Certificate of Merit for general proficiency in the years 2006, 2007 & 2008.
- Swami Lokeshwarananda Gold Medal for general proficiency, 2006 & 2007.
- Ranked 18th all over India in the National Science Olympiad, 2008.
- Stood 6th in the Regional Business Plan Competition, 2007.

Relevant Coursework

Carnegie Mellon University

- Introduction to Computer Security, Network Security, Applied Cryptography, Intermediate Statistics, Foundations of Privacy, Machine Learning, Advanced Statistical Theory I.

Indian Institute of Technology, Kharagpur

- Cryptography and Network Security, Foundations of Cryptography, Probability and Statistics, Machine Learning.