Amit Datta

Contact Information

Doctoral Student
Department of ECE
Carnegie Mellon University
Pittsburgh, PA 15213

Mobile: 412-759-6378
E-mail: amitdatta@cmu.edu
URL: andrew.cmu.edu/user/amitdatt/

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: 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*
- Advisor: 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.

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

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

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

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

[6] 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 .*

Relevant Coursework

Carnegie Mellon University

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

Indian Institute of Technology, Kharagpur

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

Technical Skills

- Programming Languages: Python, C, C++, C#, Java.
- Database Management Systems: MySQL, SQL Server 2005, Oracle.
- Web Development: HTML, JavaScript, CSS, PHP.
- Operating Systems: Windows, Ubuntu, Mac OS.

Internships

Technicolor, Los Altos [2015]

- Mentored by Nadia Fawaz and Marc Joye, I worked on improving the state-of-the-art techniques for private aggregation using cryptographic and information theoretic techniques.

Microsoft Research, Bangalore [2014]

- Mentored by Saikat Guha, 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.

Max-Planck-Institute for Software Systems, Saarbruecken [2011, 2012]

- Working with Michael Backes and Aniket Kate, I devised a new Asynchronous Verifiable Secret Sharing protocol with a communication complexity of $O(\kappa n^2)$, thereby improving the known best complexity of $O(\kappa n^3)$, where n is the number of parties participating in the secret sharing scheme and κ is a security parameter.

Shriram Insight Sharebrokers, Kolkata [2009]

- I developed an online Assets Management Software to manage the firm's assets using the .NET framework and SQL Server 2005.

Research Experience

Discovering Personal Data Use on the Web

- With Anupam Datta and Michael Tschantz.
- We studied how user behaviors on the web interact with Google ads and Google's transparency tool - Ad Settings. We built a tool to automate rigorously designed browser-based experiments and machine-learning based analysis techniques. Experiments were carried using Python and Selenium.

Towards a Faster Fully Homomorphic Encryption Scheme

- With Debdeep Mukhopadhyay.
- We 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 Debdeep Mukhopadhyay.
- We deployed an enhanced cache trace attack on CLEFIA using the differential property of the s-boxes in the cipher and the diffusion properties of the linear transformations of the underlying Feistel structures.
- We extended this attack to the block cipher CAMELLIA.

Development Projects

RailConnect

- As part of a team, I developed a web-service to find railway connections between any two stations in India on Python. Some of the major difficulties we faced were the sheer number of stations and trains, and long delays.
- We won the second prize at Yahoo! HackU, Kharagpur, 2012.

CourseForum

- I designed and developed an online portal for ranking and recommending courses on the RubyOnRails platform.
- This project was done for the Database Management Systems course, Spring'11.

Teaching Assistant

Foundations of Privacy (18734) - Fall 2014, Fall 2015