Amit Datta

CyLab, Carnegie Mellon University
CIC 2119B, 4720 Forbes Ave
Pittsburgh, PA 15213, USA

andrew.cmu.edu/∼amitdatt/
linkedin.com/in/dattaamit/
amitdatta@cmu.edu

Keywords

Privacy, Fairness, Statistics, Machine Learning, Cryptography.

Education

Carnegie Mellon University, Pittsburgh, PA — Dec 2017 (expected)
Ph.D., Electrical and Computer Engineering Advisor: Prof. Anupam Datta

Indian Institute of Technology, Kharagpur, India — Aug 2012
B. Tech (Hons), Computer Science and Engineering (GPA: 9.45/10.00)
Advisor: Prof. Debdeep Mukhopadhyay
Thesis: *Towards a Faster Fully Homomorphic Encryption Scheme*

Experience

Graduate Research Assistant, Carnegie Mellon University, Pittsburgh, PA — Aug 2012 – Present

Discovering Personal Data Use on the Web

- Developed an experimental methodology to detect information flow in blackbox systems.
- Implemented our methodology to evaluate privacy and fairness properties in Google's advertising system.
- Built a tool using Python and Selenium to automate browser-based information flow experiments which is freely available at [github.com/tadatitam/info-flow-experiments].

Ongoing Projects

- Enable accountability for fairness violations in the Bing advertising pipeline by explaining how violations came about in terms of inputs and intermediate outputs of the pipeline.
- Evaluate effectiveness of privacy enhancing technologies against tracking.

Research Intern, Technicolor Research, Los Altos, CA — Summer 2015

- Worked on improving private aggregation protocols.
- Successfully carried out a cryptanalysis attack on a published protocol.

Research Intern, Microsoft Research, Bangalore, India — Summer 2014

- Worked on identifying data-flows in Microsoft's big data platform using only data-logs without access to the scripts generating the logs.
- Used C# and Scope to implement my techniques on Microsoft's internal big data platform.

Research Intern, MPI for Software Systems, Saarbruecken, Germany — Summer 2011 & 2012

- Devised a new Asynchronous Verifiable Secret Sharing protocol with a communication complexity of $O(\kappa n^2)$, thereby improving the then best-known complexity of $O(\kappa n^3)$.

Undergraduate Research Assistant, IIT Kharagpur, India — Aug 2008 – May 2012

Towards a Faster Fully Homomorphic Encryption Scheme

- 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.

Differential Cache Attacks on Block Ciphers

- 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.
- Extended this attack to the block cipher CAMELLIA.

Publications

- *Cryptanalysis of a Privacy-Preserving Aggregation Protocol.* Amit Datta, Marc Joye. In the IEEE Transactions on Dependable and Secure Computing **(TDSC)**, Jan 2016.
- *Influence in Classification via Cooperative Game Theory.* Amit Datta, Anupam Datta, Ariel Procaccia, Yair Zick. In proceedings of the Twenty-Fourth International Joint Conference on Artificial Intelligence **(IJCAI)**, August 2015.
- *A Methodology for Information Flow Experiments.* Michael Tschantz, Amit Datta, Anupam Datta, Jeannette Wing. In the Twenty Eight IEEE Computer Security Foundations Symposium **(CSF)**, July 2015.
- *Automated experiments on ad privacy settings: A tale of opacity, choice, and discrimination.* Amit Datta, Michael Tschantz, Anupam Datta. In the proceedings on Privacy Enhancing Technologies **(PETS)**, June 2015.
- *Discrimination in Online Personalization: A Multidisciplinary Inquiry.* Amit Datta, Anupam Datta, Deirdre K. Mulligan, Michael Tschantz. In the Privacy Law Scholars Conference **(PLSC)**, June 2015.
- *Asynchronous Computational VSS with Reduced Communication Complexity.* Michael Backes, Amit Datta, Aniket Kate. In Topics in Cryptology **(CT-RSA)**, Feb 2013.
- *An Enhanced Differential Cache Attack on CLEFIA for Large Cache Lines.* Chester Rebeiro, Rishabh Poddar, Amit Datta, Debdeep Mukhopadhyay. In Progress in Cryptology **(IndoCrypt)**, Dec 2011.
- *A Cache Trace Attack on CAMELLIA*. Rishabh Poddar, Amit Datta, Chester Rebeiro. In the International Conference on Security Aspects in Information Technology, High-Performance Computing and Networking **(InfoSecHiComNet)**, Oct 2011.

Honors and Awards

- **Third place winner**, 3-Minute-Thesis (3MT) Competition, CMU. 2016
- **Dean's Tuition Fellowship**, Carnegie Institute of Technology, CMU 2012 – 2013
- **Singapore Technologies Engineering Scholarship**, IIT Kharagpur, India 2009 – 2012
- **Research Fellowship**, Max Planck Institute for Software Systems, Saarbruecken, Germany 2011, 2012
- **Certificate of Merit**, Ramakrishna Mission Vidyalaya, Narendrapur, Kolkata, India 2006, 2007, 2008
- **Gold Medal**, Ramakrishna Mission Vidyalaya, Narendrapur, Kolkata, India 2006, 2007
- Ranked 18^{th} all over India in the **National Science Olympiad** 2008
- Ranked 6^{th} in the **Regional Business Plan Competition**, Eastern Region, India 2007

Technical Skills

- **Programming Languages:** Python (proficient), C , C++, C#, Java (prior experience)
- **Database Management Systems:** MySQL, SQL Server 2005 (prior experience)
- **Web Development:** HTML, JavaScript, CSS, PHP (prior experience)
- **Productivity Applications:** LaTeX, SVN, Git (proficient)

Professional Activities and Service

- **External Reviewer** for ACM Transactions on Internet Tech., Privacy Enhancing Technologies Symposium
- **Sub-reviewer** for Network and Distributed System Security Symposium, ACM Conference on Computer and Communications Security, Workshop on Privacy in the Electronic Society
- **Teaching Assistant**, Foundations of Privacy (Graduate level), Carnegie Mellon University 2013, 2014
- **President** (2015), **Vice President** (2014), **Treasurer** (2013), Indian Graduate Student Association, CMU
- **Member**, International Students Concerns Task Force, Graduate Student Assembly, CMU 2016
- **Chair**, CyLab Events Committee, Carnegie Mellon University 2015 - Present

Relevant Coursework

Carnegie Mellon University

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

Indian Institute of Technology, Kharagpur

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