

DEBAYAN GUPTA

work.debayangupta.com

(+1) 203-606-5157 | debayan@debayangupta.com | debayan@mit.edu

EDUCATION

YALE UNIVERSITY | NEW HAVEN, CT, USA

PHD IN COMPUTER SCIENCE | 08/2011 – 05/2016

I worked on secure computation and its applications to various real-world problems. My advisor was Prof. Joan Feigenbaum.

M.PHIL. IN COMPUTER SCIENCE | 08/2011 – 05/2013

Automatically conferred en-route to PhD.

MS IN COMPUTER SCIENCE | 08/2010 – 05/2011

First in class with perfect scores.

CALCUTTA UNIVERSITY | KOLKATA, INDIA

BSC IN COMPUTER SCIENCE | 07/2006 – 05/2009

Majored in Computer Science with minors in Physics and Mathematics from St. Xavier's College (Kolkata), under Calcutta University, where I was the valedictorian.

ST. XAVIER'S COLLEGIATE SCHOOL | KOLKATA, INDIA

Graduated in 2006 (Indian School Certificate).

WORK

MASSACHUSETTS INSTITUTE OF TECHNOLOGY | CAMBRIDGE, MA, USA

FACULTY OF EECS | 09/2016 – CURRENT

I am teaching the '6.006' algorithms course in fall-16 and working on secure computation and homomorphic encryption with Prof. Vinod Vaikunthanathan.

YALE UNIVERSITY | NEW HAVEN, CT, USA

TEACHING FELLOW | 08/2011 – 05/2016

Assisted in teaching multiple courses at undergraduate and graduate levels, from introductory programming, to advanced databases, to computational complexity.

OPTIX GROUP | BROOKLYN, NY, USA

CO-FOUNDER | 05/2012 – CURRENT

OpTix Group is a data science company that helps media funds & media firms to maximize profits and minimize risk.

VENCORE LABS / BELLCORE | PISCATAWAY, NJ, USA

RESEARCHER | 05/2012 – 08/2012

Worked on the IARPA SPAR program, using secure computation for policy-checking encrypted database queries. (Originally part of Bell Communications Research, Inc., the R&D consulting arm is now part of Vencore and is based in Basking Ridge, NJ, USA.)

PRICEWATERHOUSECOOPERS | KOLKATA, INDIA

PROJECT MANAGEMENT INTERN | 06/2006 - 07/2006

Worked on standardized systems for estimating current and future CMMI ratings.

HONOURS

EXCELLENCE IN SCIENCE | AMERICAN ASSOCIATION FOR THE ADVANCEMENT OF SCIENCE / SCIENCE MAGAZINE, 2016

The program recognizes the achievements of selected students and young investigators.

BEST TEACHING FELLOW AWARD | YALE UNIVERSITY, 2015

KEMPNER SCHOLAR | YALE UNIVERSITY, 2014

Fellowship for exceptional PhD candidates.

RANJAN RAY AWARD | XAVIER'S / CALCUTTA UNIVERSITY, 2009

Special award for getting the highest score in every exam.

MERIT AWARD | XAVIER'S / CALCUTTA UNIVERSITY, 2009

Award for securing the highest overall score.

SKILLS

PROGRAMMING LANGUAGES I have significant experience with Assembly, C, C++, CSS, HTML, Java, Javascript, L^AT_EX, Matlab, OCaml, Perl, PHP, Python, Ruby, Scheme, Shell, SQL, and am familiar with many others.

LANGUAGES • Bengali • English • Hindi • Sanskrit

RESEARCH

WORK IN PROGRESS / IN SUBMISSION

- [1] D. Gupta, B. Mood, M. Hopkins, K. Butler, and J. Feigenbaum. Reusable Garbled Circuit Functions. In *progress*, 2016.
- [2] B. Ternier, D. Gupta, a. shelat, and J. Feigenbaum. Secure Stable Matching. In *progress*, 2016.

PUBLICATIONS

- [3] D. Gupta, B. Mood, J. Feigenbaum, K. Butler, and P. Traynor. Using intel software guard extensions for efficient two-party secure function evaluation. In *Financial Cryptography and Data Security*, in Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2016.
- [4] D. Gupta, B. Mood, J. Tian, G. Hernandez, J. Choi, K. Butler, P. Traynor, and T. Shrimpton. In Submission: Efficient, Leakage-Resistant Secure Function Evaluation Using Intel Software Guard Extensions, 2016.
- [5] B. Mood, D. Gupta, H. Carter, K. Butler, and P. Traynor. Frigate: a validated, extensible, and efficient compiler and interpreter for secure computation. *Proceedings of the 1st IEEE European Symposium on Security and Privacy*, 2016.
- [6] G. Di Crescenzo, J. Feigenbaum, D. Gupta, E. Panagos, J. Perry, and R. Wright. Practical and privacy-preserving policy compliance for outsourced data. In *Financial Cryptography and Data Security*. Vol. 8438, in Lecture Notes in Computer Science, pp. 181–194. Springer Berlin Heidelberg, 2014.
- [7] B. Mood, D. Gupta, K. Butler, and J. Feigenbaum. Reuse it or lose it: more efficient secure computation through reuse of encrypted values. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. ACM, New York, NY, USA, 2014, pp. 582–596.

- [8] J. Perry, D. Gupta, J. Feigenbaum, and R. Wright. Systematizing secure computation for research and decision support. In *Security and Cryptography for Networks*. Vol. 8642, in Lecture Notes in Computer Science, pp. 380–397. Springer International Publishing, 2014.
- [9] D. Gupta, A. Segal, A. Panda, G. Segev, M. Schapira, J. Feigenbaum, J. Rexford, and S. Shenker. A new approach to interdomain routing based on secure multi-party computation. In *Proceedings of the 11th ACM Workshop on Hot Topics in Networks*. ACM, New York, NY, USA, 2012, pp. 37–42.

AREAS OF INTEREST

Practical and fast secure computation • Deploying secure computation in the real world • Improving secure computation techniques (security and resource usage) • Reusable garbled circuits • Privacy and anonymity • Privacy-preserving protocols • Surveillance • Control of sensitive information

TEACHING

GAKKO PROJECT | TOKYO AND SHÖDOSHIMA, JAPAN

SUMMER CAMP FOR INNOVATIVE PEDAGOGY | SUMMER 2013

Taught Japanese high-school students electronics and mob psychology

YALE UNIVERSITY | NEW HAVEN, CT, USA

Teaching Fellow for the following courses:

COMPUTATIONAL COMPLEXITY | SPRING 2016, SPRING 2015

CPSC 468/568, taught by Joan Feigenbaum

DATABASE SYSTEMS | FALL 2015, SPRING 2014, FALL 2011

CPSC 437/537, taught by Avi Silberschatz

INTRODUCTION TO SYSTEMS PROGRAMMING AND COMPUTER ORGANIZATION | FALL 2014

CPSC 323, taught by Stan Eisenstat

PRINCIPLES OF OPERATING SYSTEMS | FALL 2013

CPSC 423/523, taught by Avi Silberschatz

INTRODUCTION TO PROGRAMMING | SPRING 2013

CPSC 112, taught by Yang (Richard) Yang

MATHEMATICAL TOOLS FOR COMPUTER SCIENCE | FALL 2012

CPSC 202, taught by Joan Feigenbaum

DATA STRUCTURES AND PROGRAMMING TECHNIQUES | SPRING 2012

CPSC 223, taught by James Aspnes

INTRODUCTION TO COMPUTER SCIENCE | SPRING 2011

CPSC 201, taught by Holly Rushmeier

SOCIAL

YALE • **Senator** for Physical Sciences, Graduate & Professional Student Senate | 2011-13 • **Representative** at the Graduate Student Assembly | 2013-14 • **Chair** for LOGICS, the Computer Science graduate student organization | 2011 – 2016

XAVIER'S • **Editorial Board member** for the college magazine, "The Xaverian" | 2008-09 • **Ex-officio member** of the Students' Union | 2008-09 • **Council Member** Science Association | 2008-09 • **Secretary** Debate & Quiz Club | 2008-09

OTHER • Researched *solid waste management in Kolkata for "Concern for Calcutta"* | 2006 • Taught *underprivileged children in Kolkata as part of the "Titli Project"* | 2002-06

LINKS

- ORCID | *Debayan Gupta*
- LINKEDIN | *debayanG*
- FACEBOOK | *debayan.gupta*
- GOOGLE SCHOLAR | *Debayan Gupta*

REFERENCES

JOAN FEIGENBAUM | JOAN.FEIGENBAUM@YALE.EDU

Prof. Feigenbaum is my PhD advisor.

AVI SILBERSCHATZ | AVI@CS.YALE.EDU

I have been a teaching assistant for multiple courses taught by Prof. Silberschatz.

KEVIN BUTLER | BUTLER@CISE.UFL.EDU

I have worked with Prof. Butler on multiple publications.