PRATYAY MUKHERJEE

Visa Research
385 Sherman Ave
Palo Alto, CA 94306

pratyay85@gmail.com
http://pratyaymukherjee.com

Current Employment

- Research Scientist
  Visa Research
  Duration: March 2017 - present.

Education

- Doctor of Philosophy, 2015
  Computer Science, Aarhus University (Denmark).
  Thesis: Protecting Cryptographic Memory against Tampering Attack.
  Supervisor: Jesper Buus Nielsen.

- Master of Technology, 2011
  Computer Science and Engineering, Indian Institute of Technology Kharagpur.
  Thesis: Parallelization of the Wiedemann Large Sparse System Solver over Large Prime Fields.
  Supervisor: Abhijit Das.
  CGPA: 9.85/10

- Bachelor of Engineering, 2008
  Electronics and Telecommunications Engineering, Jadavpur University, Kolkata.
  CGPA: 8.52/10.
  Duration: July 2004 - May 2008.

Past Positions/Research Visits

- Post-doctoral Researcher
  Computer Science Division, University of California, Berkeley.
  Host: Sanjam Garg.
  Duration: Dec 2015 - Mar 2017.

- Researcher
  Computer Science Division, University of California, Berkeley.
  Host: Sanjam Garg.
  Duration: Sep 2015 - Nov 2015.

- Visiting Graduate Student
  Simon's Institute of Theoretical Comp. Sc., Berkeley
  Host: Sanjam Garg.
  Duration: Jun 2015 - Aug 2015.

- Visiting Graduate Student
  Computer Science Dept., Northeastern University
  Host: Daniel Wichs.
  Duration: Sep 2014 - May 2015.

- Visiting Graduate Student
  R.C. Bose Centre for Cryptology and Security, ISI, Kolkata.
  Host: Rishiraj Bhattacharyya.
  Duration: Nov 2014 - Dec 2014.

- Visiting Graduate Student
  Courant Institute of Mathematical Science, NYU
  Host: Yevgeniy Dodis.
  Duration: Jun 2014 - Aug 2014.

- Visiting Graduate Student
  Microsoft Research, India
  Host: Vipul Goyal.
  Duration: Jan 2014.

- Researcher
  Cryptology and Data Security Group, University of Warsaw.
  Host: Stefan Dziembowski.
  Duration: Jul 2013 - Sep 2013.

- Researcher
  Center of Excellence in Cryptology, Indian Statistical Institute.
  Supervisors: Bimol Roy and Subhamoy Maitra.
  Duration: Jul 2011 - Jun 2012.

Research Interests

Broadly, all aspects of *Cryptography* and *Security*. A few recent interests are:

- Computations on Encrypted Data using techniques like *Multi-party Computations*, *Fully Homomorphic Encryptions* and *Program Obfuscations*.
- Protecting Cryptographic devices against Tampering/Fault attacks using techniques like *Non-malleable Codes*.

Publications
(*in reverse chronological order*)

- Preprints

  1. Obfuscation from Low noise Multilinear Maps
     with Nico Döttling, Divya Gupta, Sanjam Garg *and* Peihan Miao.

- Peer-reviewed Conferences

  1. Non-malleable Codes for Space-bounded Tampering
     with Sebastian Faust, Kristina Hostakova *and* Daniele Venturi.
     at 37^{th} International Cryptology Conference – CRYPTO 2017.
  2. Cryptanalysis of Indistinguishability Obfuscations of Circuits over GGH13
     with Daniel Apon, Nico Döttling *and* Sanjam Garg.
     at 44^{th} International Colloquium on Automata, Languages and Programming – ICALP 2017 (Track-A).
  3. Obfuscation without the Vulnerabilities of Multilinear Maps
     with Sanjam Garg, Eric Miles, Amit Sahai, Akshayaram Srinivasan *and* Mark Zhandry.
     at 14^{th} IACR Theory of Cryptography Conference – TCC 2016-B.

4. Block-wise Non-malleable Codes
   with Nishanth Chandran, Vipul Goyal, Omkant Pandey *and* Jalaj Upadhyay
   at 43^{th} International Colloquium on Automata, Languages and Programming – ICALP 2016 (Track-A).
5. Two Round Multiparty Computation via Multi-Key FHE
   with Daniel Wichs
   at 35^{th} Annual International Conference on the Theory and Applications of Cryptographic Techniques – EUROCRYPT 2016.
6. The Exact Round Complexity of Secure Computation
   with Sanjam Garg, Omkant Pandey *and* Antigoni Polychroniadou
   at 35^{th} Annual International Conference on the Theory and Applications of Cryptographic Techniques – EUROCRYPT 2016.
7. A Chaining Lemma and its application
   with Ivan Damgård, Sebastian Faust *and* Daniele Venturi
   at 8^{th} International Conference on Information-Theoretic Security – ICITS 2015.
8. Tamper and Leakage resilient von Neumann Architecture
   with Sebastian Faust, Jesper Buus Nielsen *and* Daniele Venturi
   at 8^{th} International Conference on Practice and Theory of Public-Key Cryptography – PKC 2015.
9. Efficient Non-Malleable Codes and Key-Derivation for Poly-Size Tampering Circuits
   with Sebastian Faust, Daniele Venturi *and* Daniel Wichs
   at 33^{rd} Annual International Conference on the Theory and Applications of Cryptographic Techniques – EUROCRYPT 2014.
10. Continuous Non-malleable Codes
    with Sebastian Faust, Jesper Buus Nielsen *and* Daniele Venturi
    at 11^{th} IACR Theory of Cryptography Conference – TCC 2014.
11. Bounded Tamper Resilience: How to go beyond the Algebraic Barrier
    with Ivan Damgård, Sebastian Faust, Daniele Venturi
    at 19^{th} Annual International Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT 2013.

- Journals

1. Bounded Tamper Resilience: How to go beyond the Algebraic Barrier
   with Ivan Damgård, Sebastian Faust *and* Daniele Venturi
   at Journal of Cryptology, 2017.
2. Efficient Non-Malleable Codes and Key-Derivation for Poly-Size Tampering Circuits
   with Sebastian Faust, Daniele Venturi *and* Daniel Wichs
   at IEEE Transactions on Information Theory, 2016.
3. Non-Adaptive Programmability of Random Oracle
   with Rishiraj Bhattacharyya
   at Theoretical Computer Science, 2015.

- Survey

1. An Overview of eSTREAM Ciphers.
   Manuscript, 2011 (Draft available online)

Citations

- h-index: 9; i-10 index: 9 (source: Google Scholar).

Service

- Served in the Program Committees of Indocrypt 2015, Asiacrypt 2017, TCC 2017, ProvSec 2017.
- Reviewed papers for the following journals: IEICE Journal ('16), Design Codes and Cryptography ('16), IEEE Transactions on Dependable and Secure Computing ('16)
- As an external reviewer reviewed papers for the following conferences: Crypto('15,'16,'17), Eurocrypt ('13,'16,'17,'18), IEEE S & P– Oakland ('18), Asiacrypt ('13,'14,'15,'16), ICALP ('17), TCC ('13,'15, '16-A,'16-B), PKC ('14,'15,'16,'17), Indocrypt ('11,'16), IWSEC ('13,'14), Africacrypt ('14), Inscrypt ('13).

Invited Talks

- The SaTC Workshop on Privacy and Security *at* University of Wisconsin, Madison (June, 2016).
- Bay Area Crypto Day *at* Stanford University (May, 2016).
- NYC Crypto Day *at* City University of New York (June, 2014).
- Crypto Seminar *at* Microsoft Research, India (Jan, 2014).
- Workshop on Block Ciphers *at* Bhaba Atomic Research Center, Mumbai (Dec, 2011).
- Workshop on eSTREAM ciphers *at* Indian Statistical Institute, New Delhi (Sept, 2011).

Awards/Achievements

- Awarded **Silver Medal** by IIT Kharagpur for the **best academic performance** in the class of M.Tech (Comp. Sc.) in 2011.
- Secured **All India Rank 77** among more than 40,000 aspirants in the post-graduate entrance exam (GATE in Comp. Sc.) in 2009.
- Secured **37**th position among more than 50,000 aspirants in the under-graduate entrance exam (West Bengal Joint Entrance in Engineering) in 2004.
- Offered to pursue **B. Stat.** at Indian Statistical Institute (**59** selected countrywide) in 2004. (Declined)

Teaching

- Worked as a teaching assistant (TA) for **Introduction to IT Security** (Aarhus; Spring, '14), **Distributed Systems** (Aarhus; Spring, '13), **Computational Number Theory** (IIT-Kgp; Spring, '11), **Algorithms Analysis & Design** (IIT-Kgp; Fall, '10).
- Taught **Discrete Maths** in the Crypto Internship Program (ISI-Kol; Feb, 2012), **Number Theory** in the Regional Math Olympiad Camp (ISI-Kol; June, 2012) and National Math Olympiad Camp (Kendriya Vidyalaya, Kolkata; Dec 2011)

Last updated on October 7, 2017.