Pratyay Mukherjee

Curriculum Vitae

VISA Research
385 Sherman Ave, Palo Alto, USA 94306
✉ *pratyay85@gmail.com*
`https://pratyay.net/`

Professional Experience

Mar 2017 – present **Research Scientist**, *Security*, VISA Research, USA.

Dec 2015 – Mar 2017 **Postdoctoral Researcher**, *Electrical Engineering & Computer Science*, University of California, Berkeley, USA, hosted by Prof. Sanjam Garg.

Sep 2015 – Nov 2015 **Research Specialist**, *Electrical Engineering & Computer Science*, University of California, Berkeley, USA, hosted by Prof. Sanjam Garg.

Aug 2012 – Aug 2015 **PhD Fellow**, *Cryptography Group*, Aarhus University, Denmark, supervised by Prof. Jesper Buus Nielsen & headed by Prof. Ivan Damgård.

Research visits:

- Simons Institute for the Theory of Computing, Berkeley, USA (Summer 2015), hosted by Prof. Sanjam Garg.
- Northeastern University, Boston, USA (Fall 2014 and Spring 2015), hosted by Prof. Daniel Wichs.
- R.C. Bose Centre for Cryptology and Security, Indian Statistical Institute Kolkata (December 2014), hosted by Dr. Rishiraj Bhattacharyya.
- New York University, New York, USA (Summer 2014), hosted by Prof. Yevgeniy Dodis.
- Microsoft Research, Bengaluru, India (January 2014), hosted by Dr. Vipul Goyal.
- University of Warsaw, Poland (Summer 2013), hosted by Prof. Stefan Dziembowski.

Jul 2011 – Jul 2012 **Project-linked Research Personnel**, *Centre of Excellence in Cryptology*, Indian Statistical Institute, Kolkata, headed by Prof. Bimal Roy.

Education

Oct 2015 **PhD in Computer Science**, *Aarhus University*, Denmark.

Supervisor: Prof. Jesper Buus Nielsen.

Thesis: Protecting Cryptographic Memory against Tampering Attack.

Aug 2011 **Master of Technology in Computer Science and Engineering**, *Indian Institute of Technology, Kharagpur*, India.

Supervisor: Prof. Abhijit Das.

Thesis: Parallelization of the Wiedemann Large Sparse System Solver over Large Prime Fields.

Final CGPA: 9.85/10.

Dec 2008 **Bachelor of Electronics and Telecommunications Engineering**, *Jadavpur University*, Kolkata, India.

Final CGPA: 8.52/10

Awards/Achievements

2011 Awarded **Silver Medal by IIT Kharagpur** for the **best academic performance** in the class of Master of Technology (Computer Science & Engineering).

2009 Secured **All India Rank 77** among more than 40,000 aspirants in the post-graduate entrance exam (Graduate Aptitude Test in Engineering/GATE in Computer Science).

2004 Secured **37^{th} position** among more than 50,000 aspirants in the under-graduate entrance exam (West Bengal Joint Entrance in Engineering).

2004 Selected **among 59 candidates** (countrywide) by Indian Statistical Institute for pursuing B.Stat (Declined).

Publications

Publications in cryptography/theory use alphabetical ordering for author names.

Conference Proceedings

[C13] Shashank Agrawal, Peihan Miao, Payman Mohassel, Pratyay Mukherjee. *PASTA: PASsword-based Threshold Authentication.* To appear in the 25^{th} ACM Conference on Computer and Communications Security – ACM CCS 2018

[C12] Shashank Agrawal, Payman Mohassel, Pratyay Mukherjee, Peter Rindal. *DiSE: Distributed DiSE: Distributed Symmetric-key Encryption.* To appear in the 25^{th} ACM Conference on Computer and Communications Security – ACM CCS 2018

[C11] Sebastian Faust, Kristina Hostáková, Pratyay Mukherjee, Daniele Venturi. *Non-malleable Codes for Space-bounded Tampering.* In the 37^{th} International Cryptology Conference – CRYPTO 2017

[C10] Daniel Apon, Nico Döttling, Sanjam Garg, Pratyay Mukherjee. *Cryptanalysis of Indistinguishability Obfuscations of Circuits over GGH13.* In the 44^{th} International Colloquium on Automata, Languages and Programming – ICALP 2017 (Track-A)

[C09] Sanjam Garg, Eric Miles, Pratyay Mukherjee, Amit Sahai, Akshayaram Srinivasan, Mark Zhandry. *Secure Obfuscation in a Weak Multilinear Map Model.* In the 14^{th} IACR Theory of Cryptography Conference – TCC 2016 (B).

[C08] Nishanth Chandran, Vipul Goyal, Pratyay Mukherjee, Omkant Pandey, Jalaj Upadhyay. *Blockwise Non-malleable Codes.* In the 43^{rd} International Colloquium on Automata, Languages and Programming – ICALP 2016 (Track-A).

[C07] Pratyay Mukherjee, Daniel Wichs. *Two Round Multiparty Computation via Multi-Key FHE.* In the 35^{th} Annual International Conference on the Theory and Applications of Cryptographic Techniques – EUROCRYPT 2016

[C06] Sanjam Garg, Pratyay Mukherjee, Omkant Pandey, Antigoni Polychroniadou. *The Exact Round Complexity of Secure Computation.* In the 35^{th} Annual International Conference on the Theory and Applications of Cryptographic Techniques – EUROCRYPT 2016

[C05] Ivan Damgård, Sebastian Faust, Pratyay Mukherjee, Daniele Venturi. *The Chaining Lemma and its Application.* In the 8^{th} International Conference on Information-Theoretic Security – ICITS 2015.

[C04] Sebastian Faust, Pratyay Mukherjee, Jesper Buus Nielsen, Daniele Venturi. *A Tamper and Leakage Resilient von Neumann Architecture.* In the 18^{th} International Conference on Practice and Theory in Public-Key Cryptography – PKC 2015.

[C03] Sebastian Faust, Pratyay Mukherjee, Daniele Venturi, Daniel Wichs. *Efficient Non-Malleable Codes and Key-Derivation for Poly-Size Tampering Circuits.* In the 33^{rd} Annual International Conference on the Theory and Applications of Cryptographic Techniques – EUROCRYPT 2014

[C02] Sebastian Faust, Pratyay Mukherjee, Jesper Buus Nielsen, Daniele Venturi. *Continuous Non-malleable Codes.* In the 11^{th} IACR Theory of Cryptography Conference – TCC 2014

[C01] Ivan Damgård, Sebastian Faust, Pratyay Mukherjee, Daniele Venturi. *Bounded Tamper Resilience: How to go beyond the Algebraic Barrier.* In the 19^{th} International Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT 2013

Journals

[J03] Ivan Damgård, Sebastian Faust, Pratyay Mukherjee, Daniele Venturi. *Bounded Tamper Resilience: How to go beyond the Algebraic Barrier.* In Journal of Cryptology 30(1): 152-190 (2017)

[J02] Sebastian Faust, Pratyay Mukherjee, Daniele Venturi, Daniel Wichs. *Efficient Non-Malleable Codes and Key-Derivation for Poly-Size Tampering Circuits.* In IEEE Transactions on Information Theory 62(12): 7179-7194 (2016)

[J01] Rishiraj Bhattacharyya, Pratyay Mukherjee. *Non-Adaptive Programmability of Random Oracle.* In Theoretical Computer Science 592: 97-114 (2015)

Indexes

Google Scholar
h-Index: 10.
Total # of citations: 517 (*as of* September 3, 2018).
Profile: `https://scholar.google.com/citations?user=hnxchQ8AAAAJ&hl=en`

Program Committee Memberships

— The 22^{nd} The International Conference on Practice and Theory in Public Key Cryptography – PKC 2019.

— The 8^{th} International Conference on Security, Privacy, and Applied Cryptography Engineering – SPACE 2018.

— The 23^{rd} Annual International Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT 2017.

— The 15^{th} IACR Theory of Cryptography Conference – TCC 2017.

— The 11^{th} International Conference on Provable Security – ProvSec 2017.

— The 16^{th} International Conference on Cryptology in India – Indocrypt 2015.

Selected Invited Talks

May 2018 **Stanford University, USA**, *DiSE: Distributed Symmetric-key Encryption*, Bay Area Crypto Day.

Jun 2016 **University of Wisconsin Madison, USA**, *Obfuscation from Multilinear Maps: Vulnerabilities and Protections*, The SaTC Workshop on Privacy and Security.

May 2016 **Stanford University, USA**, *Obfuscation without vulnerabilities of multilinear maps*, Bay Area Crypto Day.

Jun 2014 **City University of New York, USA**, *Efficient Non-malleable Codes and Key-derivations for Poly-size Tampering Circuits*, NYC Crypto Day.

Other Professional Activities

Organizer Co-organizer of the Workshop on eSTREAM Ciphers, Indian Statistical Institute, Delhi, India, Sep 30 – Oct 1, 2011.

Journal Reviews IEICE Journal ('16), Design Codes and Cryptography ('16,'18), IEEE Transactions on Dependable and Secure Computing ('16), Journal of Cryptology ('18).

Conference Sub-Reviews CRYPTO ('15,'16,'17,'18), EUROCRYPT ('13,'16,'17,'18), IEEE Security & Privacy – Oakland ('18), ASIACRYPT ('13,'14,'15,'16,'18), ICALP ('17), TCC ('13,'15, '16-A,'16-B,'18), PKC ('14,'15,'16,'17,'18), Indocrypt ('11,'16), IWSEC ('13,'14), Africacrypt ('14), Inscrypt ('13).

Teaching Experience

Spring 2014 **Teaching Assistant** of *Introduction to IT Security*, taught by Prof. Ivan Damgård at Aarhus University.

Spring 2013 **Teaching Assistant** of *Distributed Systems*, taught by Prof. Jesper Buus Nielsen at Aarhus University.

Jun 2012 **Guest Lecture** on *Discrete Mathematics* at Summer Internship Program in Cryptology, Indian Statistical Institute, Kolkata, India.

Dec 2011 **Tutorial** on *Block Cipher – AES* at Bhaba Atomic Research Centre, Mumbai, India.

Dec 2011 **Lecture** on *Basics of Number Theory* at National Maths Olympiad Camp, Kendriya Vidyalaya, Kolkata, India.

Sep 2011 **Tutorial** on *eSTREAM Cipher – Rabbit* at Indian Statistical Institute, Delhi, India.

Spring 2011 **Teaching Assistant** of *Computational Number Theory*, taught by Prof. Abhijit Das at IIT Kharagpur.

Fall 2010 **Teaching Assistant** of *Algorithms: Design and Analysis*, taught by Prof. Abhijit Das at IIT Kharagpur.

Supervision

Summer 2018 **Co-Mentor** of VISA Research intern *Biniy Chen*, PhD student at University of California, Santa Barbara, USA.

Summer 2018 **Co-Mentor** of VISA Research intern *Nicholas Genise*, PhD student at University of California, San Diego, USA.

Summer 2017 **Mentor** of VISA Research intern *Kristina Hostáková*, PhD student at Ruhr University Bochum, Germany.

Other

Citizenship India.

Languages Bengali (native), English (full proficiency), Hindi (working proficiency).

Last updated on September 3, 2018