Protik Kumar Paul, Ph.D.

protik.pmax.paul@gmail.com

Research Interest

My research is mostly related to Zero Knowledge proofs and Multi-Party Computation. I am also interested in Blockchain, Distributed computing such as Byzantine Agreement and Broadcast.

Employment History

Nov 2024 – · · · · **Postdoctoral researcher.** Encrypto Group, TU Darmstadt, Germany.

Jun 2017 – Jun 2018 **Assistant Professor.** ITER College, SoA University, Bhubaneswar, India.

Education

Aug 2018 – Oct 2024 **Ph.D. in Computer Science,** Indian Institute of Science Bangalore (IISc), India.
Specialization: *Cryptography*
Advisor: Dr. Arpita Patra
Thesis title: *Ankora: Notions of Multi-party Computation and Zero-knowledge Beyond Conventional Models.*
CGPA : 8.9/10

Jul 2015 – May 2017 **M.Sc. in Mathematics,** Indian Institute of Technology (IIT) Bombay, India.
Advisor: Dr. Gopala K. Srinivasan
CGPA : 8.83/10

Jun 2011 – Jun 2014 **B.Sc. in Mathematics,** Asutosh College, Calcutta University, Kolkata, India.
Percentage : 70.25

Jun 2009 – Jun 2011 **Ondal High School**, Andal, India.
Higher Secondary Education(WBCHSE) (12th), West Bengal
Percentage : 79.4

May 2009 **Eastern Railway High School**, Andal, India.
Madhyamik (WBBSE) (10th), West Bengal
Percentage : 82.625

Professional Experience

Internship
- Interned at IBM IRL in Blockchain group and worked on a project in zero knowledge proofs.
May – August 2019

Workshop
- *Theory And Practice of Blockchains 2019* workshop at Aarhus University, Denmark.
- *Secure Multiparty Computation: Theory and Practice 2020* workshop at IISc Bangalore, India.
- *Foundational Aspects of Blockchain Technology 2020* workshop at ICTS Bangalore, India.
- *Theory and Practice of Multi-Party Computation 2024* workshop at TU Darmstadt, Germany.

Research Publications

2025

- **Breaking the Barrier for Asynchronous MPC with a Friend.**
  Under submission
  Authors: Banashri Karmakar, Aniket kate, Shravani Patil, Arpita Patra, Sikhar Patranabis, **Protik Kumar Paul**, Divya Ravi.
- **Secure Evaluation of Authenticated Private Functions via MPC-Friendly Commitment.**
  IEEE Symposium on Security and Privacy 2026 **(IEEE S&P – Core Rank A*)**
  Authors: Jan Filipp, **Protik Kumar Paul**, Thomas Schneider

2024

- **QuickPool: Privacy-Preserving Ride-Sharing Service.**
  Under submission
  Authors: Banashri Karmakar, Shyam Murthy, Arpita Patra, **Protik Kumar Paul**.
- **Asterisk: Super-fast MPC with a Friend.**
  IEEE Symposium on Security and Privacy 2024 **(IEEE S&P – Core Rank A*)**
  Authors: Banashri Karmakar, Nishat Koti, Arpita Patra, Sikhar Patranabis, **Protik Kumar Paul**, Divya Ravi.

2022

- **Attaining GOD Beyond Honest Majority With Friends and Foes.**
  Advances in Cryptology – ASIACRYPT 2022 **(ASIACRYPT – Core Rank A)**
  Authors: Aditya Hedge, Nishat Koti, Varsha Bhat Kukkala, Shravani Patil, Arpita Patra, **Protik Kumar Paul**.
- **How to prove any NP statement jointly? Efficient Distributed-prover Zero-Knowledge Protocols.**
  Proceedings on Privacy Enhancing Technologies 2022 **(PoPETS – Core Rank A)**
  Authors: Pankaj Dayama, Arpita Patra, **Protik Kumar Paul**, Nitin Singh and Dhinakaran Vinayagamurthy.

Selected Talks

- Asterisk: Super-fast MPC with a Friend.
  TPMPC 2024. TU Darmstadt, Germany. June 2024.
- Asterisk: Super-fast MPC with a Friend.
  IEEE S&P 2024. San Francisco, USA. May 2024.
- Asterisk: Super-fast MPC with a Friend.
  EECS Research Symposium 2024. IISc Bangalore. April 2024.
- Asterisk: Super-fast MPC with a Friend.
  Bangalore Crypto Day. MSR India, Bangalore. March 2024.
- Attaining GOD Beyond Honest Majority With Friends and Foes.
  ACM ARCS 2024. NISER Bhubaneswar. February 2024.
- Attaining GOD Beyond Honest Majority With Friends and Foes.
  EECS Research Symposium 2023. IISc Bangalore. April 2023.
- How to prove any NP statement jointly? Efficient Distributed-prover Zero-Knowledge Protocols.
  PETS 2022. Sydney, Australia. July 2022.

Programming Experience

Quadsquad

- 4 party secure computation protocol in the *Friends and Foes* security model.
  `https://github.com/cris-iisc/quadsquad`

Asterisk

- Secure multiparty computation protocol for an arbitrary number of parties, in the malicious majority setting with a helper. `https://github.com/cris-coders-iisc/Asterisk`

Community Service

Organization committee

- Secure Multiparty Computation: Theory and Practice Workshop 2020, IISc Bangalore, India

Program committee

- APKC 2025

External Reviewer

- CCS (2021, 2022), PODC (2021), ITC (2021), Eurocrypt (2024, 2025), AfricaCrypt (2024), WWW (2025)

Skills

Languages	Strong reading, writing and speaking competencies for English, Hindi, Bangla.
Coding	C++, LaTeX, Matlab
Misc.	Academic research, teaching, LaTeX typesetting and publishing.

Awards and Achievements

- **ACM India Travel Grant,** for attending IEEE S&P 2024.
- JRF with **All India Rank (AIR) 5** CSIR-UGC NET in June, 2016 in *Mathematical Science* with score 149.75.
- **All India Rank (AIR) 10** out of 7765 in IIT-JAM 2015 with score 60.33 out of 100.
- Selected for NBHM M.Sc. scholarship 2015.
- Recipient of the scholarship from WBCHSE.