Arup **Mondal**

Ph.D. Scholar · Cryptographer · Security & Privacy Researcher

Ashoka University, Rajiv Gandhi Education City, Haryana, 131029, India

📱 (+91)-8116288859 | ✉ arup.mondal_phd19@ashoka.edu.in | 🏠 arupmondal.com | arupmondal-cs | in -arupmondal | 🎓 Google Scholar

"Arise, awake and stop not till the goal is reached" – Swami Vivekananda

About & Research Interest

Currently, I'm a visiting PhD student at IT University of Copenhagen (ITU Copenhagen) in the Center for Information Security and Trust (CISAT), advised by Dr. Bernardo David. I'm a fourth-year Ph.D. student in the Department of Computer Science at Ashoka University, advised by Dr. Debayan Gupta. I was a research intern at Technology Innovation Institute (TII) in the Crypto Research Center, advised by Dr. Abdelrahaman Aly.

My primary area of interest is the theory and design of secure cryptographic schemes for *Applied & Verifiable Cryptography*. In particular, I want to focus on a deeper understanding of the theory and design of scalable and efficient secure cryptographic schemes, which deals with the fundamental principles of practical and secure cryptosystem design. In addition to this, I have a great deal of interest in cryptographic verifiable delay functions and construction of variants of time-sensitive cryptographic protocols and applications.

I'm also interested in designing efficient post-quantum secure cryptographic protocols. Currently, I'm working on designing variants of post-quantum secure signature and secret sharing protocols.

Practical and fast secure computation ● Improving secure computation techniques (security and resource usage) ● Privacy-preserving protocols ● Design efficient verifiable delay functions and applications ● Post-quantum secure cryptography ● Lattice-based cryptography.

Education

Ashoka University
Haryana, India

Ph.D. in Computer Science (3rd year), **CGPA:** 3.5/4. *September 2019 - PRESENT*

- **Advisor:** Dr. Debayan Gupta
- Focusing on constructing new primitives for "verifiable cryptography" and "reusable garbled circuit" to improve the standard secure computation protocols.

Banaras Hindu University
Varanasi, India

M.Sc. (Hons) in Computer Science, **Minor:** Statistics and Mathematical Science, **CGPA:** 8.09/10 (In top 3 award). *July 2016 - July 2018*

- **Thesis Title:** Estimating Miss Ratio from the Characteristic of Algorithm in Simple Model of Cache.
- **Advisor:** Prof. Swapan Kumar Basu.

Ramakrishna Mission Residential College, Narendrapur, University of Calcutta
Kolkata, India

B.Sc. (Hons) in Computer Science, **Minor:** Mathematics and Physics, **Percentage:** 81.5% (In top 3 award). *June 2013 - June 2016*

- **Project Title:** Data Mining Based Desired Information from Resume and Store into Database.

Publications

Poster: Attestor: Simple Proof-of-Storage-Time
Copenhagen, Denmark

Arup Mondal *November 26–30, 2023*

- Proceedings of the 30th ACM Conference on Computer and Communication Security (ACM CCS 2023)

Poster: RandGener: Distributed Randomness Beacon from VDF [Zenodo]
Delft, The Netherlands

Arup Mondal, Ruthu Rooparaghunath, Debayan Gupta *July 3-7, 2023*

- Proceedings of the 8th IEEE European Symposium on Security and Privacy (EuroS&P), 2023.

Poster: Tight Short-Lived Signatures [Zenodo]
Delft, The Netherlands

Arup Mondal, Ruthu Rooparaghunath, Debayan Gupta *July 3-7, 2023*

- Proceedings of the 8th IEEE European Symposium on Security and Privacy (EuroS&P), 2023.

Poster: Fully Homomorphic Secret Sharing with Output Verifiability [Link]
Hybrid Conference

Arup Mondal, Pratyush Ranjan Tiwari, Debayan Gupta *24 – 28 April, 2022*

- Proceedings of the Network and Distributed System Security (NDSS) Symposium, 2022.

Beas: Blockchain Enabled Asynchronous & Secure Federated Machine Learning [ArXiv]
Fully Virtual Workshop

Arup Mondal, Harpreet Virk, Debayan Gupta *February 28 – March 1, 2022*

- Proceedings of the third AAAI Workshop on Privacy-Preserving Artificial Intelligence (PPAI-22), 2022.

SCOTCH: An Efficient Secure Computation Framework for Secure Aggregation [ArXiv] *Fully Virtual Workshop*

YASH MORE, PRASHANTHI R, PRIYAM PANDA, ARUP MONDAL, HARPREET VIRK, DEBAYAN GUPTA *February 28 – March 1, 2022*

- Proceedings of the third AAAI Workshop on Privacy-Preserving Artificial Intelligence (PPAI-22), 2022.

Poster: NEUROCRYPT: Coercion-Resistant Implicit Memory Authentication [Link] *Fully Virtual Workshop*

RITUL SATISH, NIRANJAN RAJESH, ARGHA CHAKRABARTY, ADITI JAIN, SRISTI BAFNA, ARUP MONDAL, DEBAYAN GUPTA *February 28 – March 1, 2022*

- Proceedings of the 36th AAAI Conference on Artificial Intelligence (AAAI-22), 2022.

FLATEE: Federated Learning Across Trusted Execution Environments [Link] [ArXiv] *Fully Virtual Conference*

ARUP MONDAL, YASH MORE, RUTHU ROOPARAGHUNATH, DEBAYAN GUPTA *September 6-10, 2021*

- Proceedings of the 6th IEEE European Symposium on Security and Privacy (EuroS&P), 2021.

S++: A Fast and Deployable Secure-Computation Framework for Privacy-Preserving Neural Network Training [PDF] [ArXiv] [Video] *Fully Virtual Workshop*

PRASHANTHI R, SHIVAM AGARWAL, ARUP MONDAL, AASTHA SHAH, DEBAYAN GUPTA *February 8 and 9, 2021*

- Proceedings of the second AAAI Workshop on Privacy-Preserving Artificial Intelligence (PPAI-21), 2021.

Secure Computation & Applications – In Progress/ Submission

Private Originator Tracing in End-to-End Encrypted Messaging (*Submitted*)

ARUP MONDAL, DEBAYAN GUPTA

- we study the idea of originator tracing in end-to-end encrypted messaging, a new cryptographic approach, SENDER ZERO, that enables platforms to simultaneously provide end-to-end encryption while also being able to track down the source of malicious content reported by users.

Fast and Secure Stable Matching using Arithmetic Circuits (*Submitted*)

ARUP MONDAL, PRIYAM PANDA, SHIVAM AGARWAL, ABDELRAHAMAN ALY, DEBAYAN GUPTA

- We study and constructed an *efficient* secure computation protocol for Stable Matching Problems using the secure arithmetic circuit.

Fast and Efficient Searchable Symmetric Encryption (*In Preparation*)

SAIKRISHNA BADRINARAYANAN, ARUP MONDAL, PRATYAY MUKHERJEE, SIKHAR PATRANABIS

Verifiable Cryptography – In Progress/ Submission

Efficient Construction of Continuous Verifiable Delay Function (*In Preparation*)

ARUP MONDAL, DEBAYAN GUPTA

- Verifiable delay function (VDF) is a publicly verifiable function that takes a pre-determined time to compute and produce a proof which convinces a verifier that the function output has been correctly computed. In this work, we construct and implement a *novel* Continuous VDF.

Intermediate Output Verifiable Time-Lock Puzzle (*In Preparation*)

ARUP MONDAL

- An intermediate output verifiable time-lock puzzle, which is essentially a verifiable TLP and having the property that intermediate steps of the evaluation are publicly verifiable.

ATTESTOR: Simple Proof-of-Storage-Time (*In Preparation*)

ARUP MONDAL

- We design a PoST scheme with simple proofs and efficient output verification without using trapdoors and incurring any extra overheads.
- This work appeared at ACM CCS 2023 as a Poster.

Research and Work Experience

Technology Innovation Institute *Abu Dabhi, UAE*

RESEARCH INTERN *January 2023 - March 2023*

- I'm working on designing a practical privacy-preserving decision tree training in the context of secure multiparty computation (MPC).

Ashoka University *Haryana, India*

RESEARCH ASSISTANCE *December 2022 - Present*

- I'm working on designing a post-quantum secure signature scheme using lattice-based cryptography.

Ashoka University *Haryana, India*

SOFTWARE DEVELOPER *April 2022 - December 2022*

- Part of the sysadmin team for the High-Performance Computing infrastructure at Ashoka University.

Indian Institutes of Technology (IIT) Kharagpur — *Kharagpur, India*

RESEARCH ASSISTANT — *July 2019 - August 2019*

- Cryptography and Hardware Security.

Ashoka University — *Haryana, India*

RESEARCH INTERN — *March 2019 - July 2019*

- Designed an efficient data prefetcher for stream and stride types of accesses of regular and irregular patterns in all levels of cache memories.

Indian Institutes of Science Education and Research (IISER) Bhopal — *Bhopal, India*

PH.D. SCHOLAR (CONTINUED AT ASHOKA UNIVERSITY) — *July 2018 - December 2018*

- Worked on the Theoretical Computer Science, particularly in the Approximation Algorithm and Combinatorial Optimization.

Banaras Hindu University (BHU) — *Varanasi, India*

MASTER STUDENT RESEARCHER — *July 2017 - June 2018*

- We study and analyze the memory reference pattern of the programs to estimate miss ratio using a simple model of the cache.

Teaching Experience

- TA – **Algorithm Design and Analysis [CS-1205]**, Spring 2022 – taught by Dr.Debayan Gupta. **[Head TA]** — *Ashoka University, India*
- TA – **Advanced Algorithm [CS-2446]**, Monsoon 2021 – taught by Dr. Dr.Debayan Gupta. — *Ashoka University, India*
- TA – **Computer Security and Privacy [CS-2362]**, Spring 2021 – taught by Dr.Debayan Gupta. — *Ashoka University, India*
- TA – **Advanced Programming [CS-1202]**, Monsoon 2020 – taught by Dr. Anirban Mondal. — *Ashoka University, India*
- TA – **Computer Security and Privacy [CS-2362]**, Spring 2020 – taught by Dr.Debayan Gupta. — *Ashoka University, India*
- TA – **Computer Organization and System [CS-1216]**, Monsoon 2019 – taught by Dr. Manu Awasthi. — *Ashoka University, India*
- TA – **Discrete Mathematics [ECS-201]**, Summer 2018 – taught by Dr. Shashank Singh. — *IISER BHOPAL, India*
- TA – **Data Structure and Algorithms**, Monsoon 2018 – taught by Prof. Swapan Kumar Basu. — *BHU, India*

Student Mentorship

Ritul Satish — *2021 – 2022*

UNDER GRADUATE [2019 - PRESENT] – RESEARCH PROJECT, ASHOKA UNIVERSITY

- **Project Title:** NEUROCRYPT: Coercion-Resistant Implicit Memory Authentication. **[AAAI 2022]**

Harpreet Virk — *September 2020 – May 2021*

UNDER GRADUATE & ASP [2017 - 2021] – RESEARCH CAPSTONE THESIS, ASHOKA UNIVERSITY

- **ASP Thesis:** Design an Asynchronous and Secure Federated and Transfer Machine Learning Framework. **[Under Submission]**
- **Project Title:** BEAS: Blockchain Enabled Asynchronous & Secure Federated Machine Learning **[PPAI 2022]**

Sona Maharjan — *September 2020 – May 2021*

UNDER GRADUATE & ASP [2017 - 2021] – RESEARCH CAPSTONE PROJECT, ASHOKA UNIVERSITY

- **ASP Project:** Study of Efficient Construction of Verifiable Delay Function. **[Under Submission]**

Skills

Programming	C, C++, C#, Java, Python, SageMath, LaTeX.
Languages	English, Hindi, Bengali (native).

Academic Service

Reviewer	ICLR 2024, NeurIPS 2023, ICML 2022, NeurIPS 2022
External Reviewer	IEEE European Symposium on Security and Privacy (Euro S&P) 2022.

Honors & Awards

- **Visiting Ph.D. Student Research Fellowship (Some Part of the Total)**, at ITU Copenhagen, Denmark.
- **Research Intern Fellowship**, at Technology Innovation Institute, UAE.
- **AAAI-22 Student Scholarship supported by Amazon Science**, ($300).
- **Junior Research Fellowship (Ph.D.)**, at Ashoka University, India.
- **Research Assistant Fellowship**, at Computer Science and Engineering Department, IIT Kharagpur, India.
- **Research Intern Fellowship**, at Computer Science Department, Ashoka University, India.
- **Ministry of Human Resource Development Research Fellowship (Ph.D.)**, at IISER Bhopal, India.
- **Joint Entrance Screening Test (JEST-2018)**, All India Rank 108 in Theoretical Computer Science.
- **In top 3 in the CS Department during M.Sc.**, Banaras Hindu University, India.
- **In top 3 in the CS Department during B.Sc.**, Ramakrishna Mission Residential College, Narendrapur.

References

Prof. Debayan Gupta | debayan.gupta@ashoka.edu.in | `www.debayangupta.com`

Faculty Member of Department of Computer Science, Ashoka University, India

Former Faculty Member of Department of EECS, MIT ● Visiting Faculty & Research Affiliate at MIT/ MIT Sloan

- Prof. Gupta is my Ph.D. advisor.

Prof. Mahavir Jhawar | mahavir.jhawar@ashoka.edu.in |
`https://sites.google.com/site/homeofmahavir`

Faculty Member of Department of Computer Science, Ashoka University, India

- I’m working with Prof. Jhawar on a Lattice Cryptography research project.