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 | -arupmondal | _arupmondal

About & Research Interest

I'm an early-stage third-year Ph.D. student in the Department of Computer Science at Ashoka University, advised by Dr. Debayan Gupta.

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. One major application area for secure computation protocols that I'm interested in is building and deploying efficient privacy-preserving AI and machine learning model training and inference protocols.

Practical and fast secure computation ● Deploying secure computation in the real world ● Privacy and anonymity ● Privacy-preserving protocols ● Privacy-preserving machine learning ● Fast, secure, and private AI protocols ● Design efficient verifiable delay functions and applications.

Education

Ashoka University

Haryana, India

Ph.D. in Computer Science (3rd year) — *September 2019 - PRESENT*

- **Advisor:** Prof. Debayan Gupta
- Focusing on constructing new verifiable cryptographic primitives, and improving the existing secure computation protocols and applications.

Banaras Hindu University

Varanasi, India

M.Sc. in Computer Science — *July 2016 - July 2018*

- **CGPA:** 8.09/10 (In top 3 award).
- **Minor Subject:** Statistics and Mathematical Science.
- **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. in Computer Science — *June 2013 - June 2016*

- **Percentage:** 81.5% (In top 3 award).
- **Minor Subject:** Mathematics and Physics.
- **Project Title:** Data Mining Based Desired Information from Resume and Store into Database.

Publications

NeuroCrypt: Coercion-Resistant Implicit Memory Authentication

Ritul Satish, Niranjan Rajesh, Argha Chakrabarty, Aditi Jain, Sristi Bafna, Arup Mondal, Debayan Gupta

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

Flatee: Federated Learning Across Trusted Execution Environments [Link]

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] [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.

Verifiable Cryptography – In Progress/ Submission

Efficient Construction of Continuous Verifiable Delay Function (*Submitted*)

Arup Mondal, Dewang Agarwal, 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.

Verifiable Delay Function using Elliptic Curve (*Submitted*)

Arup Mondal, Dewang Agarwal, Debayan Gupta

- We provide *novel* constructions of verifiable delay functions (VDFs) and continuous VDFs from repeated point multiplication on elliptic curves.

Time-Lock Puzzles from Elliptic Curves Point Doubling (*Submitted*)

Arup Mondal, Dewang Agarwal, Debayan Gupta

- Time-lock Puzzle (TLP) is a computational problem which can not be solved without running a computer continuously for at least a pre-defined amount of time. In this work, we construct the *first* elliptic curves repeated point doubling based TLP.

SoK: It's Not Too Late: Verifiable Delay Functions (*Submitted*)

Arup Mondal, Dewang Agarwal, Debayan Gupta

- We presents an analysis of existing VDFs and CVDFs, discusses recent developments, and provides a glimpse of the exciting research directions that lie ahead. We have created a publicly available github repository to allow others to experiment more easily with these VDFs and CVDFs.

Verifiable Homomorphic Secret Sharing and Applications (*Submitted*)

Arup Mondal, Pratyush Ranjan Tiwari, Debayan Gupta

- Homomorphic Secret Sharing (HSS) extends secret sharing to add the property of homomorphically evaluating public functions of the shares. We study and construct the *first* fully homomorphic secret sharing scheme with public verifiability.

Secure Computation & Applications – In Progress/ Submission

Asynchronous & Secure Federated Machine Learning Framework (*Submitted*)

Arup Mondal, Harpreet Virk, Debayan Gupta

- In this work, we present a blockchain-based framework for decentralized privacy-preserving federated learning that provides strict privacy guarantees of training data using gradient pruning.

Federated and Secure Transfer Learning (*Submitted*)

Arup Mondal, Harpreet Virk, Yash More, Debayan Gupta

- We constructed the *first* decentralized federated framework that uses transfer-learning to provide personalized learning models for every model trainer. Our framework provides five main advantages compared to existing approaches – (i) Personalization, (ii) Scalability, (iii) Byzantine Resilience, (iv) Fast Model Training, and (v) Higher Accuracy Performance.

Secure-Computation Framework for Secure Aggregation and Applications (*Submitted*)

Arup Mondal, Yash More, Prashanthi Ramachandran, Priyam Panda, Harpreet Virk, Debayan Gupta

- We propose a simple, fast, and efficient m-parties and n-servers federated learning framework that allows for decentralized gradient aggregation using *secure outsourced computation* and *secret sharing* while ensuring strict privacy guarantees of the training data.

Secure-Computation Framework for Neural Network Training (*In Preparation*)

Arup Mondal, Prashanthi Ramachandran, Shivam Agarwal, Debayan Gupta

- We *first* propose a secure protocol for exponentiation in the 3-party setting and describe protocols for the *logistic sigmoid*, *softmax*, and *tanh*.

Fast and Secure Stable Matching using Arithmetic Circuits (*In Preparation*)

Arup Mondal, Shivam Agarwal, Soham De, Debayan Gupta

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

Other Research– In Progress/ Submission

End-to-End Encryption and Traceability

Advisor: Debayan Gupta

- Currently, I'm involved with a CIPHER's Lab project – E2EE & Traceability (funded by WhatsApp India and NASSCOM). The main objective of this project is to analyze the existing proposals and flaws, and try to come up with a solution to achieve traceability in E2EE messaging platforms.

Breaking Ciphertext Indistinguishability in AES using Machine Learning (*Submitted*)

Arup Mondal, Yash More, Debayan Gupta

- We study the deep learning based cryptanalysis, in particular, we propose a neural network based distinguisher and we show that certain neural networks can act as efficient judges for breaking ciphertext indistinguishability in AES under a number of settings.

q-DPSGD: DPSGD with Activations Based on q-Derivative (*Submitted*)

Vedansh Priyadarshi, Arup Mondal, Debayan Gupta

- How is the privacy budget (ϵ) affected by the addition of external noise via lower level components (e.g., using scholastic activation functions)? We examine a novel question – what is the effect of external noise injection (apart from DPSGD) on the privacy budget (ϵ) calculation?

Research Experience

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*

- Design 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

- **Teaching Assistant for Advanced Algorithm**, Monsoon 2021 *Ashoka University, India*
- **Teaching Assistant for Computer Security and Privacy**, Spring 2021 *Ashoka University, India*
- **Teaching Assistant for Advanced Programming**, Monsoon 2020 *Ashoka University, India*
- **Teaching Assistant for Computer Security and Privacy**, Spring 2020 *Ashoka University, India*
- **Teaching Assistant for Computer Organization and System**, Monsoon 2019 *Ashoka University, India*
- **Teaching Assistant for Discrete Mathematics (ECS 201)**, Summer 2018 *IISER BHOPAL, India*
- **Teaching Assistant for Advance Courses in Data Structure and Algorithms**, Monsoon 2018 *BHU, India*

Students Unofficially Co-Supervised

Harpreet Virk

Advanced Postgraduate Diploma - Research Thesis, Ashoka University *September 2020 - May 2021*

- **Thesis Title:** Design an Asynchronous and Secure Federated Machine Learning Framework.

Sona Maharjan

Advanced Postgraduate Diploma - Research Thesis, Ashoka University *September 2020 - May 2021*

- **Thesis Title:** Study of Efficient Construction of Verifiable Delay Function.

Skills & Professional Activities

Programming C, C++, C#, Java, Python, LaTeX.
DevOps AWS, Bash scripting.
External Reviewer IEEE Euro S&P '22.

Honors & Awards

- **Junior Research Fellow (Ph.D.)**, at Ashoka University, India.
- **Research Assistant Fellow** , at Computer Science and Engineering Department, IIT Kharagpur, India.
- **Research Intern Fellow**, at Computer Science Department, Ashoka University, India.
- **Ministry of Human Resource Development (MHRD) Research Fellow (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

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

Former Faculty Member of Depertment of EECS, MIT • Research Affiliate at MIT/ MIT Sloan

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

Prof. Subhashis Banerjee | suban@ashoka.edu.in

Head of the Department of Computer Science, Ashoka University, India

Former Head of the of Department of Computer Science and Engineering, IIT Delhi, India

- I'm working with Prof. Banerjee on a research project.