SUBHRA MAZUMDAR

Contact : (+91)9547053507 ⋄ subhra.mazumdar1993@gmail.com

GitHub Profile ⋄ Personal Website

RESEARCH INTEREST

My primary research interest is in Applied Cryptography focusing mainly on Privacy and Security. My Ph.D. thesis deals with scalability in blockchains, specifically focussing on payment channel networks. Apart from that, I am also working on problems related to Blockchain interoperability.

EDUCATION

Indian Statistical Institute, Kolkata　　　　　　　　　　　　　　　　*July 2018 - Present*
Doctor of Philosophy
Cryptology and Security Research Unit
Jointly supervised by Prof. Bimal Kumar Roy and Dr. Sushmita Ruj

Indian Statistical Institute, Kolkata　　　　　　　　　　　　　　　*July 2016 - June 2018*
Master of Technology in Computer Science　　　　　　　　　　　　*Percentage: 88.7, Rank : 1*
Thesis : *Design of Anonymous Endorsement System in Hyperledger Fabric*
Advisor : Dr. Sushmita Ruj

National Institute of Technology, Durgapur　　　　　　　　　　　*August 2010 - June 2014*
Bachelor of Technology　　　　　　　　　　　　　　　　　　　　　*CGPA : 9.37, Rank : 4*
Department of Computer Science and Engineering

AWARDS & ACHIEVEMENTS

- Received *ACM India-IARCS travel grant* for attending *The 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, Guangzhou, China to be held from December 29, 2020 - January 1, 2021.

- Received *ISIAA-Rashi Ray Memorial Gold Medal* for securing First Rank in M.Tech (CS) programme 2016-18.

PROFESSIONAL EXPERIENCE

Nanyang Technological University, Singapore　　　　　　　　　　*May 2017 - July 2017*
Position : Research Assistant
School of Computer Science and Engineering

TCS Innovation Labs, Kolkata　　　　　　　　　　　　　　　　　*July 2014 - July 2016*
Position : Systems Engineer

Indian Statistical Institute Kolkata　　　　　　　　　　　　　　*May 2013 - July 2013*
Position : Summer Intern
Centre of Excellence in Cryptology

TEACHING EXPERIENCE

- Teaching Assistantship, Data and File Structures Laboratory, MTech (Computer Science)-I, August-December, 2018, Indian Statistical Institute Kolkata.

- Teaching Assistantship, Blockchain and Cryptocurrencies, MTech (Cryptology and Security)-II, September-December, 2019, Indian Statistical Institute Kolkata.

- Course Instructor, Blockchain and Cryptocurrencies, MTech (Cryptology and Security)-II, October,2021-January, 2022, Indian Statistical Institute Kolkata.

CONFERENCE PUBLICATIONS

- Subhra Mazumdar, Prabal Banerjee and Sushmita Ruj. Time is Money: Countermeasure for Griefing Attack in Lightning Network. In *The 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications(TrustCom)*, 2020.

- Subhra Mazumdar, Sushmita Ruj, Ram Goving Singh and Arindam Pal. HushRelay: A Privacy-Preserving, Efficient, and Scalable Routing Algorithm for Off-Chain Payments. In *IEEE International Conference on Blockchain and Cryptocurrency(ICBC)*, 2020

- Mayank Raikwar, Subhra Mazumdar, Sushmita Ruj, Sourav Sen Gupta, Anupam Chattopadhyay, and Kwok- Yan Lam. A Blockchain Framework for Insurance Processes. In 9th *IFIP International Conference on New Technologies, Mobility and Security*, 2018.

- Gopinath Mishra, Subhra Mazumdar, and Arindam Pal. Improved algorithms for the evacuation route planning problem. In 9th *Annual International Conference on Combinatorial Optimization and Applications (COCOA)*, 2015.

JOURNAL PUBLICATIONS

- Subhra Mazumdar and Sushmita Ruj. CryptoMaze: Privacy-Preserving Splitting of Off-Chain Payments. In *IEEE Transactions on Dependable and Secure Computing*, 7 February 2022.

- Subhra Mazumdar and Sushmita Ruj. Design of Anonymous Endorsement System in Hyperledger Fabric. In *IEEE Transactions on Emerging Topics in Computing*, Oct.-Dec. 2021, pp. 1780-1791, vol. 9.

- Gopinath Mishra, Subhra Mazumdar, and Arindam Pal. Improved algorithms for the evacuation route planning problem. In *Journal of Combinatorial Optimization, 36.1 (2018)*, pp. 280-306.

MANUSCRIPTS SUBMITTED

- Subhra Mazumdar, Prabal Banerjee and Sushmita Ruj. *Griefing-Penalty: Disincentivizing Griefing Attack in Lightning Network.*

- Subhra Mazumdar, Prabal Banerjee, Abhinandan Sinha, Sushmita Ruj and Bimal Kumar Roy. *Strategic Analysis to defend against Griefing Attack in Lightning Network.*

PATENTS

- Arindam Pal, Gopinath Mishra, and Subhra Mazumdar. Methods and systems for planning evacuation paths. U.S. Patent 9,972,176, publication date - May 15, 2018, status - granted.

- Arindam Pal, Francesco Parisi, Venkatramanan Siva Subrahmanian, and Subhra Mazumdar. Systems and methods for planning location-sensitive probabilistic behavior based evacuation paths. U.S. Patent Application 15/213,877, publication date - August 24, 2017, status granted.

TECHNICAL SKILLS

Software & Tools	GLPK Solver, CBC Solver, C++, C, MySQL, HTML, Verilog
	Go, CUDA, Java, Latex, Shell scripting, Python, R.