Sourav Das

website: https://sourav1547.github.io *email* souravd2@illinois.edu

Research

Distributed Cryptographic Systems, Security, Applied Cryptography, Consensus Algorithms

Education

University of Illinois at Urbana Champaign

Ph.D. candidate, Computer Science, August 2019 - ongoing (expected May 2025)

- Dissertation: "Theory and Practice of Distributed Cryptographic Systems"
- Advisor: Ling Ren

Indian Institute of Technology Delhi, India

B.Tech., Computer Science and Engineering, 2014 - 2018

- Thesis: "Scaling Smart Contracts in Permissionless Blockchain"
- Advisor: Vinay Ribeiro

Honors and Awards

- Chainlink Labs PhD fellowship. (Full tuition coverage + $100,000 in stipend for 2022-2024)
- Mavis Future Faculty Fellowship (awarded to 4 CS PhD students), UIUC, 2022-23.
- Meta (Facebook) PhD fellowship finalist, 2022.
- Young Researcher to the Heidelberg Laureate Forum (top 100 CS students worldwide), 2022.
- Best Paper Runner's Up at ACM CCS 2021.
- Best IIT Delhi CSE Undergraduate Thesis (1 out of 80 students), 2018.

Teaching Experience

Teaching Assistant, **Cryptography, UIUC**	Spring 2024
Guest lectures on Threshold Cryptography, **Distributed Algorithms, UIUC**	Spring 2023
Teaching Assistant, **Fault-Tolerant Distributed Algorithms, UIUC**	Spring 2022

Professional Experience

A16Z Crypto Research, NYC, USA. Summer Research Intern.	May 2024 - Aug 2024
Aptos Labs, Palo Alto, CA, USA. Summer Research Intern.	June 2023 - Dec 2023
Meta Research, Menlo Park, CA, USA. Summer Research Intern.	May 2022 - Aug 2022
Visa Research, Palo Alto, CA, USA. Summer Research Intern.	May 2021 - Aug 2021
IIT Bombay, India. Research Assistant.	Feb 2019 - July 2019
National University of Singapore, Singapore. Research Intern.	June 2018 - Jan 2019
Qualcomm Bangalore, India. Interim Software Developer.	May 2017 - July 2017
Loughborough University, UK. Visiting Research Student,	May 2016 - July 2016

Professional Services

Program Committee

- ACM CCS 2025
- Science of Blokchain Conference (SBC), 2025
- ACM CCS 2024
- Financial Cryptography 2024
- Junior PC at PODC 2024.
- Science of Blokchain Conference (SBC), 2024.

External-reviewer

- IEEE S&P (2023), CCS (2023, 2022), Financial Cryptography (2023, 2022, 2021)
- Eurocrypt (2024, 2023), Crypto (2024), STOC (2022, 2020), Asiacrypt (2021, 2019),
- PODC (2022), ICDCS (2022, 2021)

Selected Publications

[21] †Glacius: Threshold Schnorr Signatures from DDH with Full Adaptive Security
Renas Bacho, **Sourav Das**, Julian Loss, and Ling Ren.
EUROCRYPT 2025.

[20] †Distributed Randomness using Weighted VRFs
Sourav Das, Benny Pinkas, Alin Tomescu, Zhuolun Xiang.
EUROCRYPT 2025. Used in production by Aptos Blockchain.

[19] Shoal++: High Throughput DAG BFT Can Be Fast!
Balaji Arun, Zekun Li, Florian Suri-Payer, **Sourav Das**, and Alexander Spiegelman.
NSDI 2025.

[18] The Latency Price of Threshold Cryptosystem in Blockchains
Zhuolun Xiang, **Sourav Das**, Zhuojun Ma, Zekun Li, and Alexander Speigelman
FC 2025. Used in production by Aptos Blockchain.

[17] †Verifiable Secret Sharing Simplified
Sourav Das, Zhuolun Xiang, Alin Tomescu, Alexander Spiegelman, Benny Pinkas, and Ling Ren
IEEE SP 2025 Used in production by Supra Oracles.

[16] Groundhog: A Restart-based Systems Framework for Increasing Availability in Threshold Cryptosystems
Ashish Kashinath, Disha Agarwala, Gabriel Kulp, **Sourav Das**, Sibin Mohan, Radha Venkatagiri.
IEEE SP, 2025.

[15] †Adaptively Secure BLS Threshold Signatures from DDH and co-CDH
Sourav Das, and Ling Ren.
IACR Crypto 2024. Ongoing work on NIST threshold cryptography submission

[14] †Asynchronous Consensus without Trusted Setup or Public-Key Cryptography
Sourav Das, Sisi Duan, Shengqi Liu, Atsuki Momose, Ling Ren, Victor Shoup.
ACM CCS 2024, SBC 2024

[13] †Powers of Tau in Asynchrony
Sourav Das, Zhuolun Xiang, and Ling Ren
NDSS, 2024

[12] †Practical Asynchronous High-threshold Distributed Key Generation and Polynomial Sampling
Sourav Das, Zhuolun Xiang, Lefteris Kokoris-Kogias, Ling Ren.
USENIX Security 2023. Used in production by Arcana Network.

[11] †Threshold Signatures from Inner Product Argument: Succinct, Weighted, and Multi-threshold
Sourav Das, Philippe Camacho, Zhuolun Xiang, Javier Nieto, Benedikt Bunz, and Ling Ren.
ACM CCS 2023, **SBC 2023**.

[10] On the Security of KZG Commitment for VSS
Atsuki Momose, **Sourav Das**, Ling Ren.
ACM CCS 2023

[09] Distributed-Prover Interactive Proofs
Sourav Das, Rex Fernando, Ilan Komargodski, Elaine Shi, and Pratik Soni
IACR TCC 2023

[08] †Practical Asynchronous Distributed Key Generation
Sourav Das, Thomas Yurek, Zhuolun Xiang, Andrew Miller, Lefteris Kokoris-Kogias, Ling Ren.
IEEE S&P 2022. **SBC 2022**. Used in production by Arcana Network.

[07] †SPURT: Scalable Distributed Randomness Beacon with Transparent Setup
Sourav Das, Vinith Krishnan, Irene Miriam Isaac, and Ling Ren
IEEE S&P 2022.

[06] †Tuxedo: Maximizing Smart Contract computation in PoW Blockchains

Sourav Das, Nitin Awathare, Ling Ren, Vinay Joseph Ribeiro, and Umesh Bellur
ACM SIGMETRICS 2022.

[05] †Balanced Reliable Broadcast with Near-Optimal Communication and Improved Computation
Nicolas Alhaddad, **Sourav Das**, Sisi Duan, Ling Ren, Mayank Varia, Zhuolun Xiang, Haibin Zhang
ACM PODC 2022.

[04] †Asynchronous Verifiable Information Dispersal with Near-Optimal Communication,
Nicolas Alhaddad, **Sourav Das**, Sisi Duan, Ling Ren, Mayank Varia, Zhuolun Xiang, Haibin Zhang
Brief Announcement at **ACM PODC 2022**.

[03] Secret-Shared Joins with Multiplicity from Aggregation Trees
Saikrishna Badrinarayanan, **Sourav Das**, Gayathri Garimella, Srinivasan Raghuraman, Peter Rindal
ACM CCS 2022

[02] †Asynchronous Data Dissemination and its Applications
Sourav Das, Zhuolun Xiang, and Ling Ren.
ACM CCS, 2021 🎖 Best paper runners up at ACM CCS, 2021!

[01] †Enabling computationally intensive contracts on blockchains with Byzantine and Selfish nodes
Sourav Das, Vinay J. Ribeiro, Abhijeet Anand
NDSS 2019. 🎖 Suresh Chandra Memorial award for best IIT Delhi CSE Undergraduate thesis!

Patents

Method for scaling computation in blockchain by delaying transaction execution
Umesh Bellur, Nitin Awathare, **Sourav Das**, and Vinay J. Ribeiro
US11423016B2, Date of Patent: August 23, 2022; Priority Date: June 26 2019

Open source repositories

- Threshold BLS with adaptive security https://github.com/sourav1547/adaptive-bls
- Verifiable Secret Sharing https://github.com/sourav1547/e2e-vss
- Weighted Threshold Signtures https://github.com/sourav1547/wts
- Practical Asynchronous DKG https://github.com/sourav1547/adkg
- Practical High-threshold Asynchronous DKG https://github.com/sourav1547/htadkg
- Powers-of-Tau in Asynchrony https://github.com/sourav1547/qsdh-py