Sourav Das

PhD Candidate
Computer Science, University of Illinois Urbana-Champaign

CONTACT INFORMATION

4405, Thomas M. Siebel Center
201 N Goodwin Ave, Urbana, IL 61801

website: https://sourav1547.github.io
E-mail: souravd2@illinois.edu

RESEARCH INTERESTS

Applied Cryptography, Security, Consensus Algorithms

EDUCATION

University of Illinois at Urbana Champaign

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

- Advisor: Ling Ren

Indian Institute of Technology Delhi, India

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

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

HONORS AND AWARDS

- Mavis Future Faculty Fellowship, UIUC, 2022-23.
- Young Researcher to the Heidelberg Laureate Forum, 2022.
- Chainlink Labs PhD fellowship. 2022-2024
- 2022 Meta (Facebook) PhD fellowship finalist.
- Best paper runner's up at ACM CCS 2021.
- Suresh Chandra Memorial Award for Best IIT Delhi CSE Undergraduate Thesis, 2018.

PROFESSIONAL EXPERIENCE

Aptos Labs, Palo Alto, CA, USA. Summer Research Intern.	June 2023 - Dec 2023
Novi 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

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

SELECTED PUBLICATIONS

* Denotes alphabetical ordering.

[16] **Sourav Das**, Benny Pinkas, Alin Tomescu, Zhuolun Xiang.* *Distributed Randomness using Weighted VRFs*, In submission.
Used in production by Aptos Labs.

[15] **Sourav Das**, Zhuolun Xiang, Alin Tomescu, Alexander Spiegelman, Benny Pinkas, Ling Ren. *Verifiable Secret Sharing Simplified*, In submission.

[14] **Sourav Das**, Ling Ren. *Adaptively Secure BLS Threshold Signatures from DDH and co-CDH*, **IACR CRYPTO 2024**.

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

[12] **Sourav Das**, Zhuolun Xiang, Ling Ren. *Powers of Tau in Asynchrony*, **NDSS, 2024**.

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

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

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

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

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

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

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

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

[03] **Sourav Das**, Nitin Awathare, Ling Ren, Vinay Joseph Ribeiro, and Umesh Bellur. *Tuxedo: Maximizing Smart Contract computation in PoW Blockchains*. **ACM SIGMETRICS 2022**.

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

[01] **Sourav Das**, Vinay J. Ribeiro, Abhijeet Anand. YODA: *Enabling computationally intensive contracts on blockchains with Byzantine and Selfish nodes*. **NDSS 2019**.
Suresh Chandra Memorial award for best IIT Delhi CSE Undergraduate thesis, 2018!

PROFESSIONAL SERVICES

Program Committee
- 2024: ACM CCS, SBC, Financial Cryptography, Junior PC at PODC.

External-reviewer
- 2024: Eurocrypt, CRYPO
- 2023: IEEE S&P, Financial Cryptography, Eurocrypt, SBC
- 2022: Financial Cryptography, STOC, CCS, PODC, ICDCS
- 2021: Financial Cryptography, ASIACRYPT, ICDCS