

Sourav Das

PhD Candidate

Computer Science, UIUC

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	Cryptography, Blockchain and Distributed Algorithms	
EDUCATION	University of Illinois at Urbana Champaign Ph.D. candidate, Computer Science, August 2019 - May 2024 (expected) <ul style="list-style-type: none">• Advisor: Ling Ren Indian Institute of Technology Delhi, India B.Tech., Computer Science and Engineering, 2014 - 2018 <ul style="list-style-type: none">• Dissertation: “Scaling Smart Contracts in Permissionless Blockchain”• Advisor: Vinay Ribeiro	
HONORS AND AWARDS	<ul style="list-style-type: none">• Mavis Future Faculty Fellowship, UIUC, 2022-23.• Invited as Young Researcher to the Heidelberg Laureate Forum, 2022.• 2022 Chainlink Labs PhD fellowship.• 2022 Meta (Facebook) PhD fellowship finalist.• Best paper runner’s up at ACM CCS 2021.• Suresh Chandra Memorial Award for Best IITD-CSE B.Tech. Project, 2018.	
PROFESSIONAL EXPERIENCE	Novi Research, Menlo Park, CA, USA. Summer Research Intern. Visa Research, Palo Alto, CA, USA. Summer Research Intern. IIT Bombay, India. Research Assistant. National University of Singapore, Singapore. Research Intern. Qualcomm Bangalore, India. Interim Software Developer. Loughborough University, UK. Visiting Research Student,	May 2022 - Aug 2022 May 2021 - Aug 2021 Feb 2019 - July 2019 June 2018 - Jan 2019 May 2017 - July 2017 May 2016 - July 2016
TEACHING EXPERIENCE	Teaching Assistant, Fault-Tolerant Distributed Algorithms, UIUC	Jan 2022 - May 2022
SELECTED PUBLICATIONS	Saikrishna Badrinarayanan, Sourav Das , Gayathri Garimella, Srinivasan Raghuraman, Peter Rindal. <i>Secret-Shared Joins with Multiplicity from Aggregation Trees</i> , To appear at ACM CCS 2022 Nicolas Alhaddad, Sourav Das , Sisi Duan, Ling Ren, Mayank Varia, Zhuolun Xiang, Haibin Zhang. <i>Brief Announcement: Asynchronous Verifiable Information Dispersal with Near-Optimal Communication</i> , Brief Announcement at ACM PODC 2022 . Nicolas Alhaddad, Sourav Das , Sisi Duan, Ling Ren, Mayank Varia, Zhuolun Xiang, Haibin Zhang. <i>Balanced Byzantine Reliable Broadcast with Near-Optimal Communication and Improved Computation</i> , ACM PODC 2022 . Sourav Das , Thomas Yurek, Zhuolun Xiang, Andrew Miller, Lefteris Kokoris-Kogias, and Ling Ren. <i>Practical Asynchronous Distributed Key Generation</i> , IEEE S&P 2022 .	

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

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

Sourav Das, Zhuolun Xiang, and Ling Ren. *Asynchronous Data Dissemination and its Applications*. Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (**CCS**), November 2021, **Best paper runners up!**

Nitin Awathare, Sourav Das, Vinay Joseph Ribeiro, and Umesh Bellur. *Renoir: Accelerating Block Validation in Blockchains using State Caching*. In proceedings of 12th ACM/SPEC International Conference on Performance Engineering (**ICPE**), April 2021.

Sourav Das, Vinay J. Ribeiro, Abhijeet Anand. *YODA: Enabling computationally intensive contracts on blockchains with Byzantine and Selfish nodes*. In the Proceedings of the 30th Network and Distributed System Security Symposium (**NDSS**), Feb 2019.

SELECTED
PRE-PRINTS

Sourav Das, Vinith Krishnan, and Ling Ren. *Efficient Cross-Shard Transaction Execution in Sharded Blockchains*. arXiv preprint arXiv:2007.14521, 2020.

PROFESSIONAL
SERVICES

External-reviewer

- 2023: IEEE S&P
- 2022: Financial Cryptography, STOC, CCS, PODC, ICDCS
- 2021: Financial Cryptography, ASIACRYPT, ICDCS
- 2020: CCS, STOC, Stanford Blockchain Conference
- 2019: ASIACRYPT

RELEVANT
COURSES.

- **Online:** Lattices, LWE, and Post-Quantum Cryptography (CS 294-168, MIT and UCB);
- **UIUC:** Randomized Algorithms, Pseudorandomness, Quantum Information Processing; Applied Cryptography; Random Processes; Computational Complexity; Special Topics in Cryptography; Secure Processor Design;
- **IIT Delhi:** Advanced Computer Networks, Coding in Distributed System, Compiler Design, Numerical Algorithms, Internet of Things, Machine Learning.

RELEVANT
COMPUTER SKILLS

- **Languages [Advanced]:** Go, C++, Python
- **Tools:** Microsoft-SEAL, TFHE, OMNeT++, NS3, MPI, OpenMP.