

# 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: <a href="https://sourav1547.github.io">https://sourav1547.github.io</a> E-mail: <a href="mailto:souravd2@illinois.edu">souravd2@illinois.edu</a>
RESEARCH INTERESTS	Cryptography, Blockchain and Distributed Algorithms	
EDUCATION	<b>University of Illinois at Urbana Champaign</b> Ph.D. candidate, Computer Science, August 2019 - May 2024 (expected) <ul style="list-style-type: none"><li>• Advisor: <a href="#">Ling Ren</a></li></ul> <b>Indian Institute of Technology Delhi, India</b> B.Tech., Computer Science and Engineering, 2014 - 2018 <ul style="list-style-type: none"><li>• Dissertation: “Scaling Smart Contracts in Permissionless Blockchain”</li><li>• Advisor: <a href="#">Vinay Ribeiro</a></li></ul>	
HONORS AND AWARDS	<ul style="list-style-type: none"><li>• Mavis Future Faculty Fellowship, UIUC, 2022-23.</li><li>• Young Researcher to the Heidelberg Laureate Forum, 2022.</li><li>• 2022 Chainlink Labs PhD fellowship.</li><li>• 2022 Meta (Facebook) PhD fellowship finalist.</li><li>• Best paper runner’s up at ACM CCS 2021.</li><li>• Suresh Chandra Memorial Award for Best IITD-CSE B.Tech. Project, 2018.</li></ul>	
PROFESSIONAL EXPERIENCE	<b>Novi Research, Menlo Park, CA, USA.</b> Summer Research Intern. <b>Visa Research, Palo Alto, CA, USA.</b> Summer Research Intern. <b>IIT Bombay, India.</b> Research Assistant. <b>National University of Singapore, Singapore.</b> Research Intern. <b>Qualcomm Bangalore, India.</b> Interim Software Developer. <b>Loughborough University, UK.</b> 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, <b>Fault-Tolerant Distributed Algorithms, UIUC</b>	Jan 2022 - May 2022
SELECTED PUBLICATIONS	* Denotes alphabetical ordering.  <u>Sourav Das</u> , Philippe Camacho, Zhuolun Xiang, Javier Nieto, Benedikt Bunz, and Ling Ren. <i>Threshold Signatures from Inner Product Argument: Succinct, Weighted, and Multi-threshold</i> , <b>ACM CCS</b> , 2023, <b>SBC</b> 2023.  <u>Sourav Das</u> , Zhuolun Xiang, and Ling Ren. <i>Powers of Tau in Asynchrony</i> , eprint, 2022  <u>Sourav Das</u> , Zhuolun Xiang, Lefteris Kokoris-Kogias, and Ling Ren. <i>Practical Asynchronous High-threshold Distributed Key Generation and Distributed Polynomial Sampling</i> , <b>USENIX Security</b> 2023  Christoph U. Günther, <u>Sourav Das</u> , and Lefteris Kokoris-Kogias. <i>Practical Asynchronous Proactive Secret Sharing and Key-refresh</i> , eprint, 2022	

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

\*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.

\*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.

[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.

[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*. **ACM CCS** 2021

🏆 **Best paper runners up at ACM CCS, 2021!**

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*. **NDSS** 2019.

🏆 **Suresh Chandra Memorial award for best IIT Delhi CSE B.Tech thesis, 2018!**

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, Financial Cryptography, Eurocrypt
- 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.