# Sourav Das

*PhD Candidate*
*Computer Science, UIUC*


CONTACT INFORMATION

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

*Phone:* (217) 819 9864
*E-mail:* souravd2@illinois.edu


RESEARCH INTERESTS

Cryptography, Blockchain and Distributed Algorithms

EDUCATION

**University of Illinois at Urbana Champaign**

Ph.D. Student, Computer Science, August 2019 - May 2024 (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

Suresh Chandra Memorial Award for Best IITD-CSE B.Tech. Project, 2018.

PROFESSIONAL EXPERIENCE

| | |
|---|---|
| **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 |

PUBLICATIONS

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

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

Sourav Das, Zhuolun Xiang, and Ling Ren. Asynchronous Data Dissemination and its Applications. (To appear) Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security (CCS), November 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. In the Proceedings of the 30th Network and Distributed System Security Symposium (NDSS), Feb 2019.

Sourav Das, Aashish Kolluri, Prateek Saxena, Hifeng Yu. On The Security of Blockchain Consensus Protocols. In Proceedings of the International Conference on Information Systems Security (*Invited paper) (ICISS), Dec 2018.

Sourav Das, Alok Choudhary, Jenny Harding. An insight into Corporate Social Responsibility Reports: A Text mining Approach. In proceedings of the 3rd International Conference of Green Supply Chain, (ICGSC) London 2016.

**Pre-prints**

Shubham Anand Jain, Sanit Gupta, Denil Mehta, Inderjeet Jayakumar Nair, Rohan Shah, Jian Vora, Sushil Khyalia, Sourav Das, Vinay J. Ribeiro, and Shivaram Kalyanakrishnan. PAC Mode Estimation using PPR Martingale Confidence Sequences (Under review).

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

Sourav Das, Samuel Wadaj, Kolin Paul, Umesh Bellur, and Vinay Joseph Ribeiro. Airmed: Efficient Self-Healing Network of Low-End Devices. arXiv preprint arXiv:2004.12442, 2020 (*Under Review*).

**Professional Services**

External-reviewer

- 2022: Financial Cryptography
- 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.