Akhil Bandarupalli

@ Email: abandaru@purdue.edu | Website: https://akhilsb.github.io | Github: akhilsb

Education

Purdue University, West Lafayette, IN Jan 2021 – Dec 2025 (Expected)
Ph.D. in Computer Science
Advisors: Profs. Saurabh Bagchi and Aniket Kate

Purdue University, West Lafayette, IN Aug 2019 – Dec 2020
M.S. in Computer Science

Indian Institute of Technology, Madras, India Jun 2013 – Jul 2017
B.Tech. in Electrical Engineering

Research Interests

I design fault-tolerant distributed computing protocols for blockchains, privacy-preserving computation, and resource-constrained Cyber-Physical Systems. My research aims to improve the practical efficiency of such systems while ensuring they remain secure under harsh network conditions and adversarial attacks. It combines novel distributed computing techniques with cryptography to build protocols with provable security and efficiency. My current research focuses on computationally efficient distributed protocols for Multi-Party Computation, Asynchronous Random Beacons, and Convex Byzantine Agreement. I practically implement my research and aim to produce quality software artifacts that can be employed in real-world applications.

Keywords: Distributed Computing, Cryptography, Blockchains, Multi-Party Computation, Post-Quantum security, Distributed Machine Learning, Energy-efficient protocols, Cyber-Physical Systems, Sensor networks

Experience

Purdue University, West Lafayette, IN Sep 2020 – Present
Graduate Research Assistant *(Saurabh Bagchi and Aniket Kate)*

- Working on developing computationally efficient and Post-Quantum secure protocols for Multi-Party Computation.
- Working on developing efficient Convex Byzantine Agreement protocols for Cyber-Physical Systems.
- Implemented protocols and evaluated them in self-assembled embedded device testbeds and online clusters on clouds.

Adobe Research, San Jose, CA May 2021 – Aug 2021
Research Intern *(Haoliang Wang)*

- Designed a framework to reduce storage costs of Deep Learning Training (DLT) jobs.
- Utilized AWS Spot instances to store datasets and reduced storage costs by over 50% for long-running training jobs

Amazon Web Services, Dallas, TX May 2020 – Aug 2020
Software Development Intern *(Tom Jacobs)*

- Developed a data quality framework to introduce transparency in the data pipelining process of the team.

Open Insights, Pune, India Jul 2017 – Jun 2019
Senior Engineer

- Developed a data ingestion framework using Apache NiFi, Kafka, Spring Boot, and HDFS.
- Developed a stream data profiler using Apache Spark Streaming and Spring Boot.

Publications

* denotes alphabetical ordering

1. *Akhil Bandarupalli, Xiaoyu Ji, Aniket Kate, Chen-Da Liu-Zhang, Daniel Pöllmann, and Yifan Song. Computationally and Communication-Efficient Fair Asynchronous MPC: Scalable and Practical. *To Appear at* the 32nd ACM Conference on Computer and Communications Security (CCS), October 2025.

2. *Akhil Bandarupalli, Xiaoyu Ji, Aniket Kate, Chen-Da Liu-Zhang, and Yifan Song. Computationally Efficient Asynchronous MPC with Linear Communication and Low Additive Overhead. *To Appear at* the 45th Annual International Cryptology Conference (CRYPTO) 2025.

3. Akhil Bandarupalli, Adithya Bhat, Saurabh Bagchi, Aniket Kate, and Michael Reiter. Random Beacons in Monte Carlo: Efficient Asynchronous Random Beacons without Threshold Cryptographic Setup. 31st ACM Conference on Computer and Communications Security (CCS), November 2024.

4. Akhil Bandarupalli, Adithya Bhat, Somali Chaterji, Michael Reiter, Aniket Kate, and Saurabh Bagchi. SensorBFT: Energy-Efficient Target Localization for wide-area surveillance. 44th IEEE International Conference on Distributed Computing Systems (ICDCS), July 2024.

5. Akhil Bandarupalli, Adithya Bhat, Saurabh Bagchi, Aniket Kate, Chen-Da Liu-Zhang, and Michael Reiter. Delphi: Efficient Asynchronous Approximate Agreement for Distributed Oracles. 54th Annual IEEE/IFIP Conference on Dependable Systems and Networks (DSN), June 2024.

6. Adithya Bhat, Akhil Bandarupalli, Manish Nagaraj, Saurabh Bagchi, Aniket Kate, and Michael K. Reiter. EESMR: Energy Efficient BFT—SMR for the masses. In Proceedings of the 24th International Middleware Conference, pp. 1-14. 2023.

7. Adithya Bhat, Akhil Bandarupalli, Saurabh Bagchi, Aniket Kate, and Michael K. Reiter. The Unique Chain Rule and its Applications. In International Conference on Financial Cryptography and Data Security, pp. 38-55, 2023.

8. Akhil Bandarupalli, Sarthak Jain, Akash Melachuri, Joseph Pappas, and Somali Chaterji. Vega: Drone-based Multi-Altitude Target Detection for Autonomous Surveillance. In 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT), pp. 209-216. IEEE, 2023.

Software Artifacts

Asynchronous MPC: Implemented an asynchronous MPC protocol based on lightweight cryptography (CCS'25). Code available at https://github.com/akhilsb/fair-async-mpc-rs. Repository contains an implementation of anonymous broadcast using asynchronous MPC. This repository beats the previous best protocol by over 36×.

HashRand: Implemented *HashRand*, the asynchronous random beacon protocol (CCS'24), and Dfinity-DVRF, the beacon based on Threshold BLS signatures in Rust. Code available at https://github.com/akhilsb/hashrand-rs.

Asynchronous Post-Quantum State Machine Replication (PQ-SMR) : Implemented *PQ-Tusk* (CCS'24), A PQ-secure asynchronous SMR protocol (CCS'24) in Rust. Code available at https://github.com/akhilsb/pqsmr-rs.

Delphi: Implemented the *Delphi* Convex BA protocol (DSN'24), and FIN Asynchronous Common Subset (ACS) protocol in Rust. Code available at https://github.com/akhilsb/delphi-rs.

SensorBFT: Implemented *SensorBFT* (ICDCS'24), the asynchronous target localization protocol in Rust. Assembled a testbed of 20 Raspberry-Pi devices to evaluate the protocol. Code available at https://github.com/akhilsb/sensorbft-rs. Testbed access available upon request.

EESMR: Implemented *EESMR* (Middleware'23) and *Sync HotStuff*, both synchronous SMR protocols, in CPP. Assembled a testbed of 10 NUCLEO F401-RE devices to measure energy consumed by both protocols. Code available at https://github.com/akhilsb/E2C-BLE.

Projects

HashRand: Efficient Asynchronous Random Beacon without Threshold Setup | *GitHub*

- Designed HashRand, a computationally efficient random beacon protocol that avoids computationally expensive Discrete Log cryptography and uses only lightweight cryptography like Hash functions. Paper accepted to CCS'24.
- HashRand is the first beacon protocol to work in an asynchronous network, the first Post-Quantum secure beacon, and the first beacon protocol that does not require a Public Key Infrastructure (PKI)

- Implemented HashRand in Rust and evaluated it in a geo-distributed testbed on AWS with up to 160 machines, where it generated beacons at 5x the throughput of the prior State-of-the-art beacon protocol.
- Utilized HashRand to develop the first BFT asynchronous State Machine Replication (SMR) that is Post-Quantum Secure.

Delphi: Asynchronous Convex Agreement for Oracles | *GitHub*

- Designed and developed Delphi, a computationally efficient Asynchronous Convex Byzantine Agreement protocol for Oracle applications. Paper accepted to DSN'24.
- Proposed a new technique to improve communication complexity while not sacrificing computational efficiency.
- Implemented a distributed system in Rust to evaluate performance in two settings: A geo-distributed testbed in AWS, and an embedded system testbed on Raspberry Pi devices.
- Delphi has 8x and 3x lesser latency than prior protocols in the Raspberry Pi and AWS testbeds.

SensorBFT: Energy Efficient BFT Convex Agreement for Low-Powered Sensor Devices | *GitHub*

- Proposed SensorBFT, an energy-efficient Approximate Agreement protocol that avoids energy-expensive cryptography. Paper accepted to ICDCS'24.
- Utilized a novel technique to trade off accuracy offered by the protocol for communication and energy efficiency.
- Employed higher-order Voronoi diagrams to effectively scale the system over large geographic areas.
- Implemented the protocol in Rust and evaluated it in a self-assembled embedded system testbed, where it demonstrated over 50% energy savings compared to the prior State-of-the-art protocol.

Vega: Multi-Altitude Target Detection for Drone-based Autonomous Surveillance | *GitHub*

- Designed Vega, a Drone-based autonomous surveillance system that uses drones equipped with cameras to detect target objects in the area.
- Employed EfficientDet, a Deep-Learning based object detection program, to detect cars in a parking lot.
- Created a drone deployment system that uses covered area, detection latency, and detection quality as tunable parameters.
- Achieved an improved Pareto frontier between these parameters using two custom Drone maneuvers called DroneZoom and DroneCycle.

EESMR: Energy-Efficient Consensus for Cyber-Physical Systems | *GitHub*

- Implemented an energy-efficient Byzantine State Machine Replication (SMR) protocol on NUCLEO-F401RE ARM-Cortex microprocessor using MBed-OS. Paper accepted to Middleware'23.
- Used Bluetooth Low Energy (BLE) and the k-cast model to achieve communication between processors.

Side Channel Cryptanalysis of AES-128

- Conducted cryptanalysis of AES-128 running on a 22nm FPGA with a high probability by analyzing the power consumption of the chip.
- Used a co-variance optimized moving average filter to create templates from traces and attacked the cipher using three different template-matching algorithms.

Important Coursework

Distributed Systems, Randomized Algorithms, Blockchains and Cryptocurrencies, Cryptography, Distributed Convex Optimization, Network Security, Security Analytics, Data Structures and Algorithms.

Academic Service

External Review Committee (ERC) member for USENIX ATC'24

External Reviewer for the following

- 2024 - S&P'24, CCS'24, FC'24, EuroSys'24, ICDCS'24
- 2023 - S&P'23, AsiaCCS'23
- 2022 - ATC'22, CSF'22, NeurIPS'22, ICML'22
- 2021 - DSN'21

Academic References

Saurabh Bagchi sbagchi@purdue.edu
Professor in the Department of Electrical and Computer Engineering *Purdue University*

Aniket Kate aniket@purdue.edu
Associate Professor in the Department of Computer Science *Purdue University*
Chief Research Officer *Supra Research*

Chen-Da Liu-Zhang chen-da.liuzhang@hslu.ch
Faculty member *Lucerne University of Applied Sciences and Arts*

Chester Rebeiro chester@cse.iitm.ac.in
Associate Professor *Indian Institute of Technology, Madras*

Michael K. Reiter michael.reiter@duke.edu
James B. Duke Distinguished Professor in Departments of CS and ECE *Duke University*