ADITHYA BHAT

Purdue University, West Lafayette, IN
◇ Email - bhat24@purdue.edu ◇ GitHub - https://github.com/adithyabhatkajake
◇ Website - https://adithyabhatkajake.github.io

RESEARCH INTERESTS

My interests are *Byzantine fault-tolerant distributed systems*, *applied cryptography* and *blockchain protocols*. My work aims at developing and evaluating cryptographic solutions for secure, fault-tolerant distributed systems. My current research focuses on energy-efficient consensus protocols in network settings such as synchronous, asynchronous, and all intermediate models; fault-tolerant cryptographic protocols such as PVSS and Random Beacons, and secure Byzantine fault-tolerant distributed protocols.

EDUCATION

Purdue University, West Lafayette *(2018-2023)*
Advisor: Aniket Kate
Ph.D., Department of Computer Science

National Institute of Technology Karnataka, Surathkal *(2014-2018)*
Bachelor of Technology, Information Technology

WORK EXPERIENCE

Visa Research, Foster City (Aug 2023 - Present)
Staff Research Scientist *(Mahdi Zamani)*

Visa Research, Palo Alto (May 2022 - Aug 2022)
Ph.D. Research Intern *(Mahdi Zamani)*

· Developed *FastSync*: an efficient blockchain synchronization protocol
· Developed an efficient partially synchronous sharding protocol and implemented Instachain

VMware Research, Remote (May 2021 - Aug 2021)
Research Intern *(Alin Tomescu, Ittai Abraham)*

· Built a prototype of anonymous token system using Concord-BFT
· Developed *quick-pay*: a one-round trip low-latency payment system
· Developed a two-phase lock-free sharding solution using quick-pay

Purdue University, West Lafayette (Aug 2018 - Present)
Graduate Research Assistant *(Aniket Kate)*

· Researching energy efficient Byzantine fault tolerant consensus protocols.
· Developed mathematical models for protocol optimization to improve energy efficiency.
· Implemented, evaluated, and simulated cryptographic and distributed system protocols.

Indian Statistical Institute, Kolkata (July 2017 - December 2017)
Undergraduate Research Fellow *(Sushmitha Ruj)*

· Designed a storage auditing library based on compact proofs of retrievability.

· Implemented new transactions on an Ethereum client to build a publicly verifiable data-storage system.

Morgan Stanley, Bangalore (May 2017 - July 2017)
Software Analyst

· Worked on evaluating an elastic-search visualization plugin for the LevelDB database.

Indian Institute of Science, Bangalore (May 2016 - July 2016)
Indian Academy of Sciences Summer Research Fellow *(C. E. Veni Madhavan)*

· Evaluated Pollard's rho, William's $p+1$, $p-1$ factorization, and elliptic curve factorization methods for efficient batch factorization of numbers generated during the sieving phase of GGNFS.

PUBLICATIONS

1. *UTT: Decentralized Ecash with Accountable Privacy.* **Science of Blockchain Conference 2023**. Alin Tomescu, Adithya Bhat, Benny Applebaum, Ittai Abraham, Guy Gueta, Benny Pinkas, and Avishay Yanai. eprint code
2. *EESMR - Energy Efficient State Machine Replication.* **Middleware 2023**. Adithya Bhat, Akhil Bandarupalli, Manish Nagaraj, Saurabh Bagchi, Aniket Kate, Michael Reiter. conference eprint
3. *The unique chain rule and its applications.* **Financial Cryptography 2023**. Adithya Bhat, Akhil Bandarupalli, Saurabh Bagchi, Aniket Kate, Michael Reiter. pre-conference conference eprint code
4. *OptRand - Optimistically Responsive Reconfigurable Distributed Randomness.* **NDSS 2023**. Adithya Bhat, Nibesh Shrestha, Aniket Kate, Kartik Nayak. conference eprint protocol code crypto code video
5. *OpenSquare: Decentralized Repeated Modular Squaring Service.* **CCS 2021**. Sri Aravinda Krishnan Thyagarajan, Tiantian Gong, Adithya Bhat, Aniket Kate, Dominique Schroder. conference eprint code
6. *RandPiper – Reconfiguration Friendly Random Beacons with Quadratic Communication.* **CCS 2021**. Adithya Bhat, Nibesh Shrestha, Aniket Kate, Kartik Nayak. conference eprint code
7. *Reparo - Publicly Verifiable Repair Layer for any Blockchain.* **FC 2021**. Sri Aravinda Krishnan Thyagarajan, Adithya Bhat, Bernardo Magri, Daniel Tschudi, Aniket Kate. conference eprint
8. *Verifiable Timed Signatures for Blockchains.* **CCS 2020**. Sri Aravinda Krishnan Thyagarajan, Adithya Bhat, Guilio Malavolta, Nico Dottling, Aniket Kate, Dominique Schroder. conference eprint code

TECH REPORTS

1. *Synchronous Distributed Key Generation without Broadcasts.* Nibesh Shrestha, **Adithya Bhat**, Kartik Nayak, Aniket Kate. eprint
2. *Leto - Partially Synchronous Unique Chains made flexible.* **Adithya Bhat**, Saurabh Bagchi, Aniket Kate, Michael Reiter. code

3. *Using the future to verify the past.* Adithya Bhat, Mohsen Minaei, Mahdi Zamani. Appeared in CESC, 2022. **U.S. Patent pending.**

SOFTWARE ARTIFACTS

1. Developed a synchronous networking library to implement SMR protocols. code (Rust)
2. Implemented Apollo [3] (protocol node, normal client and special client) using the Rust networking library. code (Rust)
3. Implemented Sync HotStuff (normal protocol node, round robin protocol node, client) using the Rust networking library. code (Rust)
4. Developed a plug-and-play framework using libp2p to run and simulate distributed system protocols. The framework provides interfaces to aid faster prototyping of distributed system protocols. code (Go-lang)
5. Implemented Sync HotStuff using the go networking library. code (Go-lang)
6. Implemented Apollo [3] using the go networking library. code (Go-lang)
7. Implementation of E2C [2]. code (C++)
8. Developed a linearly homomorphic time-lock puzzle library. code (C)

TALKS

1. Reconfiguration-friendly Byzantine Fault-tolerant Distributed randomness. slides *(KU Leuven)*
2. Unique Chain Rule and its applications. slides *(FC 2023)*
3. Reconfiguration-friendly Byzantine Fault-tolerant Distributed randomness. slides *(Boston University)*
4. Flexible State Machine Replication. slides *(Midwest Crypto Day - Lightning session)*
5. OptRand - Optimistically Responsive Reconfigurable Distributed Randomness. *(NDSS 2023)*
6. FastSync: Using the future to verify the past. video *(CESC 2022)*
7. RandPiper - Reconfiguration friendly random beacons with quadratic communication. *(CCS 2021)*
8. Reparo - Publicly Verifiable Repair Layer for any blockchain. video *(FC 2021)*
9. Transitive network - A tokenless IOU-based Credit Network. Cryptocurrency Implementers Workshop. *(FC 2019)*

ACADEMIC SERVICE

- External Reviewer for
  - 2023: CCS, IET, Middleware, IEEE S & P
  - 2022: CCS, PODC, IEEE S & P, CESC
  - 2021: AFT, FC, PODC, IEEE S & P

- 2020: Usenix Security, IEEE S & P
- 2019: NDSS