ADITHYA BHAT

Purdue University, West Lafayette, IN
(+1) 765-476-3319 ⋄ bhat24@purdue.edu
Github - adithyabhatkajake ⋄ Linkedin - adithyabhatk

EDUCATION

Purdue University, West Lafayette *August 2018 - Present*
Ph.D. under Prof. Aniket Kate GPA: 3.90/4.0
Department of Computer Science

National Institute of Technology Karnataka (NITK) *August 2014 - May 2018*
Bachelor of Technology, Information Technology GPA: 9.50/10.0

WORK EXPERIENCE

Purdue University Aug 2018 - Present
Graduate Research Assistant *Prof. Aniket Kate*

- I am working on energy efficient byzantine fault tolerant protocols such as State Machine Replication, Byzantine Agreement and Agreement over dynamic graphs for CPS devices.

Indian Statistical Institute, Kolkata July 2017 - December 2017
Undergraduate Research Fellow *Prof. Sushmitha Ruj*

- Implemented a publicly verifiable data storage framework on Ethereum. We built an end-to-end system that takes a file, stores it on a machine and responds to challenges with efficient proofs of file storage.

Morgan Stanley May 2017 - July 2017
Software Analyst

- Worked on evaluating an elastic-search visualization plugin for key-value database (leveldb).

Indian Institute of Science, Bangalore May 2016 - July 2016
Summer Research Fellow *Prof. C. E. Veni Madhavan*

- Worked on evaluating 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.

ONGOING PROJECTS

Apollo - A best case optimal, linear, efficient SMR protocol for synchronous networks

Trustless, Efficient Random Beacon Protocols for Synchronous Networks

An empirical analysis of Ripple Ledgers

PROJECTS

E2C - Energy Efficient Consensus. (Submission under review)
Adithya Bhat, *Manish Nagaraj, Mike Reiter, Saurabh Bagchi, Aniket Kate*
E2C is an energy efficient BA protocol for Cyber-Physical systems such as IoT devices. We employ cryptographic techniques and leverage networking techniques to optimize the energy costs of performing consensus and demonstrate the improvements using a test-bed and simulations.

Verifiable Timed Signatures for Blockchains. (Accepted at CCS 2020)
Sri Aravinda Krishnan Thyagarajan, ***Adithya Bhat****, Bernardo Magri, Daniel Tschudi, Aniket Kate*
Built an efficient Verifiable Time-locked Signatures (VTS) using Linearly Homomorphic Time-lock Puzzles (LHTLP) that can be used to remove timing information from any atomic multi hop lock system. Implemented LHTLP, VTS for ECDSA, VTS for Schnorr, VTS for BLS and also implemented the range proofs of efficient packing.

Reparo - Publicly Verifiable Repair Layer for any Blockchain.
Sri Aravinda Krishnan Thyagarajan, ***Adithya Bhat****, Bernardo Magri, Daniel Tschudi, Aniket Kate*
Reparo (PDF) is a consensus agnostic, backwards compatible edit layer for blockchains that allows, for example, in Ethereum to fix buggy contracts and undo transactions securely and with accountability. Implemented a modified client for Ethereum that is reparo enabled to evaluate performance overheads.

Transitive Network - A Tokenless IOU based Credit Network.
Adithya Bhat*, Pedro Moreno Sanchez, Aniket Kate*
Transitive Network is a credit network implementation in Ethereum using smart contracts. We show that credit networks can be implemented without introducing tokens unlike Ripple and is even cheaper than using Ripple.

OTHER PROJECTS

Publicly Verifiable Data Storage in Ethereum - An academic implementation of Shachams and waters scheme in the Ethereum client as a native contract to enable publicly verifiable data storage.

Analysis of Paging and Caching overheads in the Linux Kernel (Linux Kernel, C) [2017]

K-Rack - A lightweight metadata encrypted steganographic filesystem (Linux Kernel, C) [2017]

A comparative analysis of Fast Fourier Transform using GPU and CPU. We find that 1-D FFT is faster on a CPU than on a GPU.

Daedalus - A tool implementing the attacks on RSA as proposed in Dan Boneh's survey paper *20 years of attacks on RSA* (Python) [2016]

INTERESTS

Byzantine Fault Tolerance (Distributed Systems) Familiar with the works on deterministic consensus such as PBFT, Paxos, Zyzzyva, Hotstuff, Sync Hotstuff, SBFT, ... Familiar with works on randomized protocols for consensus in dynamic graphs.

Blockchains Interested in Ethereum, implemented reparo and shachams and waters scheme in go-ethereum, familiar with Bitcoin , Lightning and ripple clients.

Applied Cryptography Implemented brainpool EC curves for mbed-os from RFC 5639 and linearly homomorphic time-lock puzzles.