

ADITHYA BHAT

Purdue University, West Lafayette, IN
(+1) 765-476-3319 \diamond bhat24@purdue.edu

Github - adithyabhatkajake \diamond Linkedin - adithyabhatk

EDUCATION

Purdue University, West Lafayette
Ph.D. under Prof. Aniket Kate
Department of Computer Science

August 2018 - Present
GPA: 4.0/4.0

National Institute of Technology Karnataka (NITK)
Bachelor of Technology, Information Technology

August 2014 - May 2018
GPA: 9.50/10.0

WORK EXPERIENCE

Indian Statistical Institute, Kolkata
Undergraduate Research Fellow

July 2017 - December 2017
Prof. Sushmitha Ruj

- Worked on implementing 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.

Morgan Stanley
Software Analyst

May 2017 - July 2017

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

Indian Institute of Science, Bangalore
Summer Research Fellow

May 2016 - July 2016
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.

PROJECTS

Time Lock Puzzles for Blockchains

We build an efficient verifiable time-locked signature scheme that can be used to remove timing information from any atomic multi hop lock system such as lightning network.

Reparo - Publicly Verifiable Repair Layer for any Blockchain

Reparo 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.

E2C - Energy Efficient Consensus

E2C is an energy efficient BA and IC protocol (derived from Sync Hotstuff) for Cyber Physical systems. We employ cryptographic techniques and also leverage networking techniques to optimize the energy costs of consensus.

Transitive Network - A Tokenless IOU based Credit Network Transitive Network is a credit network implementation in Ethereum using smart contracts. We show that it can be achieved without introducing tokens unlike Ripple and is even cheaper than using Ripple.

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.

INTERESTS

Byzantine Fault Tolerance (Distributed Systems)	Familiar with the works such as PBFT, Paxos, Fast Byzantine Consensus, Zyzzyva, Hotstuff, Sync Hotstuff, SBFT, ...
Blockchains	Expert in Ethereum, implemented reparo and shachams and waters scheme, familiar with the inner workings of Ethereum Client geth; 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.

SKILLS

Programming Languages	C, Python, NodeJS, Go-lang, Solidity, C++
Libraries	GMP, PBC, OpenSSL, NS3, Web3, Ripple-Lib, Bitcoin-RPC
Softwares	Go-ethereum, Bitcoind, Rippled, Lnd, Blocksci NVim > Vim > Emacs, Tmux
Misc. Favorites	Bash scripting

RELEVANT COURSES

Cryptography - CS555 (A)
Practical and Applied Cryptography - CS590 (A)
Complexity Theory - CS584 (A+)

OTHER PROJECTS

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]
Designing and building a Smart Mirror and its interface (Python) [2017]
Kompile - A secure light-weight online code judge using modified runtimes and chroot jail (C, Django) [2017]
Deep4MalDroid: Android Malware detection using system call graphs, Genetic Algorithm for parameter selection and Naive Bayes for Detection (Python, C, Android) [2017]
TextWalker - A natural language to RDF graph generator [Django, NLTK]
fMRI analysis using General Linear Model (R) [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]