SARISHT WADHWA

+1(984)377-1996 ⋄ sarisht.wadhwa@duke.edu ⋄ linkedin.com/in/sarisht-wadhwa/

EDUCATION

Ph.D. *Major: Computer Science* **Aug 2021 - Present**
Duke University, North Carolina 3.96/4

Dual B.Tech./M.Tech. *Major: Computer Science (Advance Standing)* **2014 - 2019**
Indian Institute of Technology (IIT), Delhi *JEE Rank:* 2781/1,200,000+ 8.43/10

PROJECTS

Modeling MEV Optimization with Preconf Transactions May 2024 - Present
Rohan Shrothrium, Prof. Kartik Nayak

- Analyzing the game behind pre-confirmations (preconfs), where a proposer decides whether to give preconf to transactions or extract MEV from them.
- Preliminary analysis shows that the fee required for the proposer to give preconf is significantly lower than the loss incurred by MEV.

An Inclusion List Design for Rational Parties Feb 2024 - Present
Prof. Kartik Nayak, Prof. Fan Zhang, Ethereum Foundation

- Working on the first formal definition for inclusion lists (ILs) and a new definition of censorship resistance for inclusion list schemes based on the amount of bribe required to censor each IL output.
- Analyzing a novel IL protocol combining a correlated equilibrium-based input list-building scheme and an auction-based multi-proposer inclusion list (AUCIL).
- Rigorously performing game theoretic security analysis for AUCIL and showing significant improvements over the state-of-the-art (e.g., FOCIL).

Differentially Private hints for MEV-Share June 2023 - Aug 2023
Jonathan Passerat-Palmbach, as an *Intern at Flashbots*

- Proposed and analyzed hints for MEV-Share and their use cases in order to enable easier backrunning-based MEV extractions.
- Used Laplace noise to create Differentially Private aggregate hints (of 3 different types) and discussed its effects on backrunning strategy.

Data Independent Order Policy Enforcement Jan 2022 - March 2024
Prof. Kartik Nayak, Prof. Fan Zhang, Ethereum Foundation

- Identified vulnerabilities based on decentralized but unaccountable trust in committee-based decentralized protocols to solve the problem of MEV (auction or reduction), which leads to undetectable incentive manipulation.
- Designed the AnimaguSwap AMM interface, along with an incentive structure that aligns rational behavior with honesty, leveraging distrust to ensure that the system disincentivizes MEV extraction.

Revisiting Incentives in Hashed Time Lock Contract (HTLC) Sep. 2021 - Feb. 2023
Jannis Stöther, Prof. Kartik Nayak, Prof. Fan Zhang

- Identified three new incentive manipulation attacks on MAD-HTLC (anti-bribery state-of-the-art HTLC), considering the newly identified actions of "active miners" (based on the 2020-21 MEV explosion).
- Proposed a fix to HTLC called He-HTLC, provably secure against any incentive manipulation attacks under all (active or passive) rational miners, with minimal user adjustable collateral without added transaction fee.

Answering Regular Simple Path Queries on Large Networks Jan 2018 - July 2019
Major Project (M.Tech.) - Prof. Sayan Ranu, Prof. Srikanta Bedathur, Prof. Amitabha Bagchi

- Designed a precise true-biased Monte Carlo algorithm with a high recall (over 96%), to answer regular simple path queries (NP-complete problem) employing a scalable random walk search method on graphs.
- Our proposed algorithm achieved 400x-2000x speedup over double-sided Breadth First Exhaustive Search, the only other method that scales to very large labeled (vertices and edges) graphs.

PUBLICATIONS

(Pending Reviews) **Wadhwa, S.**, Ma, J., Thiery, T., Mannot, B., Zanolini L., Zhang, F., and Nayak, K. (2024). *AUCIL: An inclusion list design for rational parties.* Submitted to 2025 IEEE Symposium on Security and Privacy (SP).

Wadhwa, S., Zanolini, L., D'Amato F., Asgaonkar, A., Fang, C., Zhang, F., and Nayak, K. (2023). *Data Independent Order Policy Enforcement: Limitations and Solutions.* In Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS).

Wadhwa, S., Stöter, J., Zhang, F., Nayak, K. (2022). *He-HTLC: Revisiting Incentives in HTLC.* In proceedings of the 2023 Network and Distributed Systems Symposium (NDSS).

Wadhwa, S., Prasad, A., Ranu, S., Bagchi, A., Bedathur, S. *Efficiently answering regular simple path queries on large labeled networks.* In Proceedings of the 2019 International Conference on Management of Data (SIGMOD).

BLOGS

Block Building is not just knapsack, *Eth Research*
AUCIL: An Auction-Based Inclusion List Design for Enhanced Censorship Resistance on Ethereum, *Eth Research*

TALKS

Data Independent Order Policy Enforcement, CCS 2024, EC 2024, Yale Security Group (July 2024), Patent Office Visit Day, Duke (June 2024)
He-HTLC: Revisiting Incentives in HTLC, NDSS 2023, SBC 2022, CESC 2022