

Research

- Statement** My research has spanned diverse topics in security and cryptography often leading to direct industry adoption. In particular, I am interested in building security and privacy-enhancing technologies to safely and securely manage users digital identities.
- Adoption** DECO is licensed from Cornell by Chainlink. ZkAttest is implemented and maintained by Cloudflare.

Education

- 2018-22 **Ph.D. in Computer Science, Cornell University.**
Advisor: *Ari Juels*
- Designed a decentralized identity system, CanDID, that can port legacy credentials (e.g., Driver's License), provide Sybil-resistance and accountability (e.g., sanctions checks) in a privacy-preserving manner.
 - Developed an oracle protocol, DECO, that allows users to prove that data accessed via TLS came from a particular website and prove statements about such data in zero-knowledge. Devised specialized MPC protocols and ZKP optimizations to make DECO practical.
 - Designed a new framework to model existing authentication mechanisms and proposed novel mechanisms more secure than any prior mechanism leveraging interactivity.
 - Created a new proactive secret-sharing scheme, CHURP, that makes dynamic changes to the committee nodes practical achieving 1000x lower communication costs than before.
- 2012-16 **B.Tech in Computer Science with Honors, IIT Bombay, GPA: 8.91/10.**

Experience

- 2023- **Research Scientist, Mysten Labs, Remote.**
Creating Foundational Infrastructure For Web3.0.
- 2020 **Cryptography Research Engineer Internship, Cloudflare, Remote.**
Devised and prototyped a privacy-preserving, usable alternative to CAPTCHA, ZkAttest, using a ring-signature scheme layered on top of WebAuthn in TypeScript. The scheme is based on a zero knowledge Σ -protocol.
- 2016-17 **Member of Technical Staff, Oracle, Bangalore.**
Back-end Java Developer for the GlassFish application server. Implemented several core features, bug fixes in the deployment module that released in Java EE RI 8.

Selected Projects and Publications

- 2022 **Interactive Authentication, [eprint](#).**
D. Maram, I. Eyal, M. Kelkar. In submission.
- 2021-22 **GoAT: File Geolocation via Anchor Timestamping, [github](#).**
D. Maram, I. Bentov, M. Kelkar, A. Juels. In submission.
- 2020-21 **CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability, [candid.id](#).**
D. Maram, H. Malvai, F. Zhang, N. Jean-Louis, A. Frolov, T. Kell, T. Lobban, C. Moy, A. Juels, and A. Miller. In *IEEE Symposium on Security and Privacy (S&P) 2021*.
- 2020 **ZkAttest: Ring and Group Signatures for existing ECDSA keys, [github](#).**
A. Faz-Hernandez, W. Ladd, D. Maram. In *Selected Areas in Cryptography (SAC) 2021*.

- 2019-20 **DECO: Liberating Web Data Using Decentralized Oracles**, deco.works.
F. Zhang, **D. Maram**, H. Malvai, S. Goldfeder, and A. Juels. *In Proceedings of the 2020 ACM Conference on Computer and Communications Security (CCS)*.
- 2018-19 **CHURP: Dynamic-committee Proactive Secret Sharing**, churp.io.
D. Maram, F. Zhang, L. Wang, A. Low, Y. Zhang, A. Juels, and D. Song. *In Proceedings of the 2019 ACM Conference on Computer and Communications Security (CCS)*.
- 2018 **SkinnerDB: Regret-Bounded Query Evaluation via Reinforcement Learning**.
I. Trummer, S. Moseley, **D. Maram**, S. Jo, and A. Antonakakis. *In Proceedings of the 2019 International Conference on Management of Data (SIGMOD)*.

Media Coverage

- Aug 29, 2020 *Forbes*, "Chainlinks New Acquisition From Cornell University Could Transform Blockchain For Good".
- Aug 29, 2020 *CoinDesk*, "Chainlink Acquires Blockchain Oracle Solution From Cornell University".
- Aug 29, 2020 *CoinTelegraph*, "Chainlink acquires a privacy-preserving oracle protocol from Cornell University".
- Aug 29, 2020 *PR Newswire*, "Chainlink Acquires DECO from Cornell University".
- May 14, 2019 *Wired*, "Microsoft Wants to Protect Your Identity With Bitcoin," by Gregory Barber.
- Mar 30, 2019 *MIT Tech Review China*, "The whereabouts of 4 million bitcoins worldwide are missing".

Professional Services

Program Committee

- 2023 Stanford Blockchain Conference (SBC)

Reviewer

- 2023 IEEE Symposium on Security & Privacy (Oakland)
- 2023 Financial Cryptography (FC)
- 2022 CRYPTO
- 2020 CRYPTO
- 2020 ACM Transactions on Networks
- 2020 USENIX Security

Programming Experience

Languages C++ (intermediate), Python (intermediate), Java (intermediate), JavaScript (beginner), Rust (beginner).

Honors / Awards

- 2018 Awarded University Fellowship by Cornell University
- 2012 Secured All India Rank 12 in *IIT-JEE* out of 500,000 students
- 2012 Secured All India Rank 36 in *AIEEE* out of 11,00,000 students
- 2012 Recipient of KVPY scholarship and attended VIJYOSHI Camp
- 2011 Awarded merit certificate for being in top 1% in National Standard Examination - Astronomy

Invited Talks

- 2021 **GoAT: File Geolocation via Anchor Timestamping**.
Presented at the Protocol Labs Research Seminar Series, 2021.
Presented at the Initiative for Cryptocurrencies and Contracts (IC3) Retreat, 2021

- 2020-21 **CanDID: A Decentralized Identity System.**
Presented at the IEEE Symposium on Security and Privacy (S&P), 2021.
Presented at the Facebook (Novi) Reserach Seminar, 2021.
Presented at the Hyperledger Identity Working Group, 2020.
Presented at the 31st Internet Identity Workshop, 2020.
Presented at the Travel Rule Information Sharing Architecture Forum, 2020.
- 2019 **CHURP: Dynamic-committee Proactive Secret Sharing.**
Presented at the ACM conference on Computer and Communication Security (CCS), London.
Presented at the Initiative for Cryptocurrencies and Contracts (IC3) Winter Retreat, Interlaken.
- 2018 **SkinnerDB: Regret-Bounded Query Evaluation via Reinforcement Learning.**
Presented a poster at the Conference on Very Large Data Bases (VLDB) 2018, Rio.

Graduate Course Work

Security & Privacy Technologies, Privacy in the Digital Age, Cryptocurrency and Smart Contracts, Advanced Programming Languages, Advanced Operating Systems, Intro to Computer Vision, Computational Ring Theory (UG), Graph Theory (UG)

Service / Extra-curriculars

- 2021-22 Acted as a Teaching Assistant for the courses: CS5433: Blockchains, Cryptocurrencies, and Smart Contracts (Spring 2022) and CS5435: Security and Privacy Concepts in the Wild (Fall 2021).
- 2019-20 Served as the treasurer of PhD student organization At Cornell Tech (PACT) and as the co-organizer of Cornell Tech Security Seminar.
- 2003-07 Won first prize in several district-level chess competitions and participated in state-level competitions.