Varun Madathil

206 AKW, 51 Prospect St, New Haven, Connecticut, CT-06515

+1 (919)-946-6096 • varun.madathil@yale.edu
https://varun2703.github.io

Research Interests

Applied Cryptography, with a focus on privacy-preserving computation in public systems (e.g., blockchains, telephone networks), and privacy-preserving machine learning.

Academic Experience

- **Yale University** — **New Haven, Connecticut**
  Postdoctoral Associate with Charalampos Papamanthou — *2024–Present*
  Focus Areas: Secure Aggregation for Federated Learning, Private Semantic Search, Concrete Security of SNARKs

Education

- **North Carolina State University** — **Raleigh, North Carolina**
  PhD in Computer Science, advised by Dr. Alessandra Scafuro — *2018–2024*
  Focus Area: Cryptography: privacy and anonymity of blockchains
- **Birla Institute of Technology and Sciences** — **Pilani,India**
  B.E. (Hons) Computer Science Engineering , First Class — *2012–2016*

Publications

- **Varun Madathil**, Alessandra Scafuro. *PriFHEte Payments: Full Privacy in Account Based Cryptocurrencies is Possible.* In **Asiacrypt 2025**
- Sashidhar Jakkamsetti, Zeyu Liu, **Varun Madathil.** *Scalable Private Signaling.* In **CSF 2025**
- **Varun Madathil**, Tanner Verber, Alessandra Scafuro. *Round-Optimal Compiler for Semi-Honest to Malicious Oblivious Transfer via CIH.* In **IACR Communications in Cryptology**
- David Adei, **Varun Madathil**, Sathvik Prasad, Bradley Reaves and Alessandra Scafuro. *Jager: Automated Telephone Call Traceback.* In **CCS 2024**(Distinguished Paper Award)
- Yanxue Jia, **Varun Madathil**, Aniket Kate. *HomeRun: High-efficiency Oblivious Message Retrieval, Unrestricted.* In **CCS 2024**
- **Varun Madathil**, Sri AravindaKrishnan Thyagarajan, Dimitrios Vasilopoulos, Giulio Malavolta, Lloyd Fournier, Pedro Moreno-Sanchez. *Cryptographic Oracle-Based Conditional Payments*. In **NDSS 2023**
- **Varun Madathil**, Alessandra Scafuro, Omer Shlomovits, Istvan Andras Seres, Denis Varlakov.

Private Signaling. In **USENIX 2022** (Distinguished Paper Award)

- **Varun Madathil**, Chris Orsini, Alessandra Scafuro, Daniele Venturi. *From Privacy-Only to Simulatable OT: Black-Box, Round-Optimal, Unconditional*. In **ITC 2022**
- Kemafor Anyanwu, **Varun Madathil**, Akash Pateria, Sen Qiao, Alessandra Scafuro, Binil Starly. *Preserving Buyer-Privacy in Decentralized Supply Chain Marketplaces*. In **CBT 2022**.
- Abida Haque, **Varun Madathil**, Alessandra Scafuro, Bradley Reaves. *Anonymous Device Authorization for Cellular Networks*. In **WiSec 2021**
- Markulf Kohlweiss, **Varun Madathil**, Kartik Nayak, Alessandra Scafuro. *On the Anonymity Guarantees of Anonymous Proof-of-Stake Protocols.* In **IEEE S&P 2021**
- Foteini Baldimtsi, **Varun Madathil**, Alessandra Scafuro, Linfeng Zhou. *Anonymous Lottery in the Proof-of-Stake Setting*. In **IEEE CSF 2020**
- Islam, SK Hafizul, **Varun Rajeev Madathil**, and Ruhul Amin. *A Robust and Efficient Three-Factor Authentication and Session Key Agreement Mechanism for SIP.* In **ICRTCCM (IEEE) 2017.**
- Islam, SK Hafizul, Mohammad S. Obaidat, **Varun Rajeev Madathil**, and Ruhul Amin. *Design of a certificateless designated server based searchable public key encryption scheme.* In **ICMC 2017**

Manuscripts

- Arthur Lazzaretti, Zeyu Liu, **Varun Madathil**, Charalampos Papamanthou *TACITA: Threshold Aggregation without Client Interaction for Federated Learning* In Submission
- Diego Castejon-Molina, **Varun Madathil**, Dimitrios Vasilopoulos, Sri AravindaKrishnan Thyagarajan, Pedro Moreno-Sanchez *Cryptographic Collateralized Loan without Smart Contracts* In Submission
- David Adei, **Varun Madathil**, Nithin Shyam, Brad Reaves *Sidecar: Extensible Out-of-band Signaling for Trustworthy Telephony* In Submission
- Kostas Kryptos Chalkias, Charanjit Jutla, Jonas Lindstrom, **Varun Madathil**, Arnab Roy. *Improved Polynomial Division in Cryptography* In Submission

Workshops

- Arthur Lazzaretti, Zeyu Liu, **Varun Madathil**, Charalampos Papamanthou *TACITA: Threshold Aggregation without Client Interaction for Federated Learning* **In Privacy Preserving Machine Learning Workshop 2025**
- Markulf Kohlweiss, **Varun Madathil**, Kartik Nayak, Alessandra Scafuro. On the Anonymity Guarantees of Anonymous Proof-of-Stake Protocols. *Theory and Practice of Blockchains Conference* (TPBC 2021)
- Foteini Baldimtsi, **Varun Madathil**, Alessandra Scafuro, Linfeng Zhou. A Framework for Anonymous Lottery-Based Protocols in the Proof-of-Stake Setting. *Privacy-Enhancing Cryptography in Distributed Ledgers*. (PENCIL 2019)

Internships

- **Mysten Labs** — **Remote**
  Cryptography Research — *June, 2024–Sept,2024*
  Interned with Mysten Labs and worked on problems related to faster polynomial divisions resulting in improvements to KZG commitment scheme, and worked on designs for privacy-preserving transactions
- **Purdue University** — **West Lafayette**
  Computer Science Dept — *May, 2023–Aug,2023*
  Worked with Dr. Aniket Kate on problems related to weighted secret sharing and oblivious message retrieval
- **Meta** — **Menlo Park**
  Meta Connectivity — *May, 2022–Aug,2022*
  Worked on resolving authentication related vulnerabilities for an open source project - Magma
- **IMDEA Software Institute** — **Remote**
  Blockchain Privacy — *July, 2021–Aug,2021*
  Interned with Dr. Pedro Moreno-Sanchez. and worked on formalizing security of hardware wallets and on decentralized oracle contracts.
- **KZen Networks Ltd** — **Remote**
  Cryptography Research — *June, 2020–Aug,2020*
  Came up with efficient protocols for decentralizing payment hubs on the Lightning Network, and also worked on efficient anonymous signaling using bulletin boards
- **University of Edinburgh** — **Edinburgh**
  School of Informatics — *May, 2019–Aug,2019*
  Interned with Dr. Markulf Kohlweiss and investigated network attacks to de-anonymize block proposers in privacy preserving Proof-of-Stake protocols.
- **George Mason University** — **Fairfax**
  CSC department — *May, 2018–Aug, 2018*
  Interned with Dr. Foteini Baldimtsi and worked on the security and analysis of privacy of BFT-based proof-of-stake blockchains. Also surveyed some Byzantine Agreement protocols as part of the internship.
- **Institute of Mathematical Sciences** — **Chennai**
  Summer Programme — *June, 2015–July, 2015*
  Completed a summer program in Theoretical Computer Science at the Institute of Mathematical Sciences. Learnt various concepts on Linear Algebra, Graph Coloring, Algorithms, Data Structures and Cryptography. Presented on simple digital signatures and encryption schemes at IMSc.

Previous Employment

- **Edgeverve Systems Ltd** — **Bangalore**
  Product Engineer, Research and Development team — *June, 2016–July, 2017*

Awards

- Awarded a Distinguished Paper Award at CCS 2024 for paper titled *Jager: Automated Telephone Call Traceback*.
- Awarded a Distinguished Paper Award at USENIX 2022 for paper titled *Private Signaling*
- Awarded a two-year fellowship from Protocol Labs to work on private decentralized storage

networks

Professional Service

I have served/will serve in the Program Committee for
- USENIX 2026
- S&P 2025, 2026
- Financial Cryptography 2025
- CCS 2025

Sub-reviewer for :
- EUROCRYPT 2025
- S&P 2023
- CRYPTO 2023, 2022, 2020 and 2018
- EUROCRYPT 2020 and 2022
- Tokenomics 2021
- AFT 2021
- CCS 2021 and 2018
- NDSS 2021 and 2019
- USENIX 2021
- ICALP 2019
- PKC 2019 and 2018