Varun Madathil

varun.madathil@yale.edu • https://varun2703.github.io

Short Bio

I am an applied cryptographer interested in the full stack of privacy-preserving computation – from foundational protocol design to practical implementation. My work explores privacy-preserving machine learning, zero-knowledge proofs, and efficient multiparty computation, emphasizing rigorous security analysis and deployable, high-performance constructions. I've contributed to systems that bring advanced cryptography into practice, including oblivious message retrieval, federated learning, secure telephony, and privacy-preserving blockchains, often through implementations in Rust and other performance-oriented environments. My focus is on closing the gap between provable security and real-world deployment – building robust, efficient protocols that retain their intended security properties in practice.

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

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, telephone security
- **Birla Institute of Technology and Sciences** — **Pilani,India**
  B.E. (Hons) Computer Science Engineering , First Class — *2012–2016*

Publications

1. **PriFHEte Payments: Full Privacy in Account Based Cryptocurrencies is Possible.**
   Varun Madathil, Alessandra Scafuro.
   Asiacrypt 2025
   [Paper]
2. **Scalable Private Signaling.**
   Sashidhar Jakkamsetti, Zeyu Liu, Varun Madathil
   CSF 2025
   [Paper] [Code](C/C++, ≈ 500 LoC)
3. **Round-Optimal Compiler for Semi-Honest to Malicious Oblivious Transfer via CIH.**
   Varun Madathil, Tanner Verber, Alessandra Scafuro.
   IACR Communications in Cryptology 2025
   [Paper]

4. **Jager: Automated Telephone Call Traceback.**
   David Adei, Varun Madathil, Sathvik Prasad, Bradley Reaves and Alessandra Scafuro.
   CCS 2024
   [Paper] [Code] (Python/C++, ≈ 600 LoC)
   🏆 Distinguished Paper Award 🏆 Distinguished Artifact Award

5. **HomeRun: High-efficiency Oblivious Message Retrieval, Unrestricted.**
   Yanxue Jia, Varun Madathil, Aniket Kate.
   CCS 2024
   [Paper] [Code] (Rust, ≈ 800 LoC)

6. **Cryptographic Oracle-Based Conditional Payments**
   Varun Madathil, Sri AravindaKrishnan Thyagarajan, Dimitrios Vasilopoulos, Giulio Malavolta, Lloyd Fournier, Pedro Moreno-Sanchez.
   NDSS 2023
   [Paper] [Code] (Rust, ≈ 600 LoC)

7. **Private Signaling**
   Varun Madathil, Alessandra Scafuro, Omer Shlomovits, Istvan Andras Seres, Denis Varlakov.
   USENIX 2022
   [Paper] [Code] (Rust/C++, ≈ 400 LoC)
   🏆 Distinguished Paper Award

8. **From Privacy-Only to Simulatable OT: Black-Box, Round-Optimal, Unconditional**
   Varun Madathil, Chris Orsini, Alessandra Scafuro, Daniele Venturi.
   ITC 2022
   [Paper]

9. **Preserving Buyer-Privacy in Decentralized Supply Chain Marketplaces**
   Kemafor Anyanwu, Varun Madathil, Akash Pateria, Sen Qiao, Alessandra Scafuro, Binil Starly.
   CBT 2022
   [Paper]

10. **Anonymous Device Authorization for Cellular Networks**
    Abida Haque, Varun Madathil, Alessandra Scafuro, Bradley Reaves.
    WiSec 2021
    [Paper].

11. **On the Anonymity Guarantees of Anonymous Proof-of-Stake Protocols.**
    Markulf Kohlweiss, Varun Madathil, Kartik Nayak, Alessandra Scafuro.
    IEEE S&P 2021
    [Paper]

12. **Anonymous Lottery in the Proof-of-Stake Setting.**
    Foteini Baldimtsi, Varun Madathil, Alessandra Scafuro, Linfeng Zhou.
    CSF 2020
    [Paper]

Manuscripts (In Submission)

1. **TACITA: Threshold Aggregation without Client Interaction for Federated Learning**
   Arthur Lazzaretti, Zeyu Liu, Varun Madathil, Charalampos Papamanthou
   PPML 2025
   [Paper] [Code]: (Rust, ≈ 500 LoC)

2. **Cryptographic Collateralized Loan without Smart Contracts**
   Diego Castejon-Molina, Varun Madathil, Dimitrios Vasilopoulos, Sri AravindaKrishnan Thyagarajan, Pedro Moreno-Sanchez

3. **Sidecar: Extensible Out-of-band Signaling for Trustworthy Telephony**
   David Adei, Varun Madathil, Nithin Shyam, Brad Reaves
   [Paper] [Code] (C++/Python)

4. **Improved Polynomial Division in Cryptography**
   Kostas Kryptos Chalkias, Charanjit Jutla, Jonas Lindstrom, Varun Madathil, Arnab Roy.
   [Paper] [Code] (Rust, ≈ 700 LoC)

Internships

- **Mysten Labs** — **Remote**
  Cryptography Research — *June, 2024–Sept,2024*
  Interned under Dr. Arnab Roy, focusing on accelerating polynomial division algorithms to improve the computation of opening proofs in the KZG commitment scheme, and contributing to the design of privacy-preserving transaction protocols.
- **Purdue University** — **West Lafayette**
  Computer Science Dept — *May, 2023–Aug,2023*
  Worked with Dr. Aniket Kate on research problems involving weighted secret sharing and oblivious message retrieval.
- **Meta** — **Menlo Park**
  Meta Connectivity — *May, 2022–Aug,2022*
  Resolved authentication-related vulnerabilities for the open-source project Magma, improving its overall security and robustness.
- **IMDEA Software Institute** — **Remote**
  Blockchain Privacy — *July, 2021–Aug,2021*
  Interned under Dr. Pedro Moreno-Sanchez, formalizing the security of hardware wallets and designing decentralized oracle contracts.
- **KZen Networks Ltd** — **Remote**
  Cryptography Research — *June, 2020–Aug,2020*
  Developed efficient protocols for decentralizing payment hubs in the Lightning Network and for oblivious message retrieval via bulletin boards.
- **University of Edinburgh** — **Edinburgh**
  School of Informatics — *May, 2019–Aug,2019*
  Interned under Dr. Markulf Kohlweiss, investigating network-level attacks aimed at de-anonymizing block proposers in privacy-preserving Proof-of-Stake protocols.
- **George Mason University** — **Fairfax**
  CSC department — *May, 2018–Aug, 2018*
  Interned under Dr. Foteini Baldimtsi, analyzing the security and privacy of BFT-based Proof-of-Stake blockchains, and surveying Byzantine Agreement protocols.

Awards

- Distinguished Paper Award at ACM CCS — 2024
- Distinguished Artifact Award at ACM CCS — 2024
- Distinguished Paper Award at USENIX — 2022
- Two-year fellowship from Protocol Labs — 2022

Professional Service

- Program Committee – USENIX Security 2026
- Program Committee – IEEE S&P 2026
- Program Committee – IEEE S&P 2025
- Program Committee – Financial Cryptography 2025
- Program Committee – ACM CCS 2025
- External Reviewer - EUROCRYPT 2025
- External Reviewer – IEEE S&P, CRYPTO 2023
- External Reviewer – CRYPTO, EUROCRYPT, 2022
- External Reviewer – AFT, ACM CCS, NDSS, USENIX 2021
- External Reviewer – CRYPTO, EUROCRYPT, 2020
- External Reviewer – NDSS, PKC 2019

Invited Talks

1. **Threshold Aggregation for Federated Learning**
   Sept 2025 - J.P. Morgan A.I. Research, *Invited Talk*
   Aug 2025 - Privacy-preserving Machine Learning, *Workshop Presentation*
   Aug 2025 - Microsoft Research, *Seminar Talk*

2. **Full Privacy for Account-based Cryptocurrencies**
   March 2024 - Yale University, *Invited Talk*
   March 2024 - U.C. Berkeley, *Invited Talk*
   Nov 2022 - Triangle Area Privacy and Security, *Student Talk*

3. **Oracle Based Conditional Payments** Feb 2023 - NDSS, *Conference Talk*
   Sept 2022 - Triangle BitDevs, *Invited Talk*

4. **Oblivious Message Retrieval and Friends**
   June 2023 - Purdue University, *Seminar Talk*
   Aug 2022 - USENIX Security, *Conference Talk*

5. **From Privacy Only to Simulatable Oblivious Transfer**
   July 2022 - Information Theoretic Cryptography, *Conference Talk*

6. **Anonymity Guarantees of Proof-of-Stake**
   May 2021 - IEEE S&P, *Conference Talk*

7. **Anonymous Lottery in Proof-of-Stake**
   June 2020 - IEEE CSF, *Conference Talk* May 2019 - Privacy-Enhancing Cryptography In Ledgers, *Workshop Talk*