Varun Madathil

3531 Ivy Commons Dr, Apt 302, Raleigh, North Carolina, NC-27606

+1 (919)-946-6096 • vrmadath@ncsu.edu
https://varun2703.github.io

Education

- **North Carolina State University** — **Raleigh, North Carolina**
  PhD in Computer Science, advised by Dr. Alessandra Scafuro — *2018–Present*
  Interests: Cryptography, with a focus on 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**, 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

Workshops

- 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

- **Meta** — **Menlo Park**
  Meta Connectivity — *May, 2022–Aug,2021*
  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.

Employment

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

Awards

- 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

Sub-reviewer for :

- CRYPTO 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