Varun Madathil

3512 Ivy Commons Dr, Apt 202, Raleigh, North Carolina, NC-27606

☎ +1 (919)-946-6096 • ✉ vrmadath@ncsu.edu

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*

Relevant Coursework

Cryptography, Privacy, Advanced Network Security, Advanced Distributed Systems, Automata and Computability Theory, Design and Analysis of Algorithms, Computer and Network Security, Operating Systems, Number Theory (undergraduate), Compiler Construction, Programming Languages

Research Projects

- **Efficient anonymous signaling using a public bulletin board**[May 2020 - present]
  Constructed protocols for parties to be able to efficiently signal a user while keeping the receiver of the signal anonymous
- **From Privacy-Only to Simulatable OT: Black-Box, Round-Optimal, Unconditional**[Nov 2020 - Feb 2021](In Submission)
  Constructed a black-box compiler that takes any 2 round privacy-only OT to a 4 round simulatable malicious secure OT
- **Hubba Bubba : Decentralizing Lightning Clients** [May 2020 - August 2020]
  Constructed new architectures and protocols for decentralizing hubs and clients on the lightning network using threshold cryptography
- **SmartChainDB - Decentralizing Interactive Marketplaces: Interactive Private Matching over Blockchains** [Jan 2020 - Jan 2021](In Submission)
  Constructed protocols for confidentiality and privacy of sensitive parts of partner transactions and collaborations for SmartChainDB, a platform that uses the blockchain to enable partnerships between business organizations without physical interactions.
- **Anonymous Device Authorization for Cellular Networks** [Jan 2020 - Aug 2020](In Submission)
  Proposed a protocol that allows mobile devices to anonymously attest to not being present in a blocklist without revealing their Personal Equipment Identifier.
- **On the actual anonymity guaranteed in anonymous Proof-of-Stake** [May 2019 - May 2020]
  Analyzed attacks to de-anonymize users in the Privacy-preserving proof of state ecosystem
- **Anonymous Selection in Proof-of-Stake. Accepted to S&P 2021.** [Aug 2018 - April 2019]
  Defined an ideal functionality for anonymous selection and realized it using an anonymous selection protocol inspired by the Algorand blockchain protocol. Accepted to CSF 2020.

Course Projects

- **Implementing BFT protocol with zero knowledge proofs** [Jan 2019 - May 2019]

  In this project we implement the binary BA protocol of Micali, and replace the signature scheme with a SNARK proof over the set of all public keys. We implemented this using the snarkjs library and a simple gossip protocol. Our aim was to achieve consensus with some flavors of anonymity.

- **Scheduling and memory management for resource containers** [Aug 2018 - Dec 2018]

  Added a new abstraction, resource containers, in the Linux Operating System and used that as another way to schedule computing resource as well as allocate memory for tasks (processes/threads). This project was completed as part of the Operating Systems course at NCSU.

- **Telephone security** [Aug 2017 - Dec 2017]

  This project was completed as part of the Computer and Network Security course at NCSU. We suggested improvements to the STIR Out-of-band architecture by giving more efficient and practically correct alternatives. AuthentiCall was a paper that was used for reference.

Internships

- **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.

- **Ericsson R & D** **Bangalore**
  Research and Innovation team *July, 2015–Dec, 2015*

  Interned with the research team at Ericsson R & D. Worked on disk simulations, to increase the efficiency of disks. This project involved writing kernel modules and the use of a disk simulator called DiskSim.

- **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*

In Submission

- Abida Haque, **Varun Madathil**, Alessandra Scafuro, Bradley Reaves. "Anonymous Device Authorization for Cellular Networks". In Submission

Publications

- 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 2020 IEEE 33rd Computer Security Foundations Symposium (CSF)
- Islam, SK Hafizul, **Varun Rajeev Madathil**, and Ruhul Amin. "A Robust and Efficient Three-Factor Authentication and Session Key Agreement Mechanism for SIP". In *Second International Conference on Recent Trends and Challenges in Computational Models* (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 *International Conference on Mathematics and Computing*, pp. 3-15. Springer, Singapore, 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)

Technical skills

- **Programming Languages:**
  - Proficient in: Python (500 LOC), Javascript (1000 LOC), C (500 LOC), C++, JAVA
  - Some familiarity with snarkjs

Professional Service

Sub-reviewer for :

- CCS 2021
- Network and Distributed System Security Symposium (NDSS) 2021 and 2019
- USENIX 2021
- CRYPTO 2020 and 2018
- EUROCRYPT 2020
- International Colloquium on Automata, Languages and Programming (ICALP) 2019
- Public Key Crypto (PKC) 2019 and 2018
- Conference on Computer and Communications Security (CCS) 2018