SAIKUMAR YADUGIRI

Madison, WI | saikumar@cs.wisc.edu | saikumarysk | saikumarysk

RESEARCH INTERESTS

I am interested in the theoretical aspects of classical and (post)-quantum cryptography. Particularly in advanced encryption systems, succinct and zero-knowledge proof systems, and lattice-based cryptography.

PUBLICATIONS AND MANUSCRIPTS

[1] Rishab Goyal and Saikumar Yadugiri. **Multi-Authority Functional Encryption with Bounded Collusions from Standard Assumptions.** *To appear in Theory of Cryptography - TCC 2024 - 22nd International Conference*, 2024.

[2] Abtin Afshar, Jiaqi Cheng, Rishab Goyal, Aayush Yadav, and Saikumar Yadugiri. **Encrypted RAM Delegation: Applications to Rate-1 Extractable Arguments, Homomorphic NIZKs, MPC, and more**. *Cryptology ePrint Archive, Paper 2024/1806, https://eprint.iacr.org/2024/1806*

RECENT AWARDS

2024 Student Presenter Stipend from TCC 2024
2024 CS Summer Research Assistantship from UW-Madison

RESEARCH EXPERIENCE

Research Assistant **Madison, WI**
Advisor: Prof. Rishab Goyal *May 2024 - Aug 2024*

- Designed partially-hiding RAM delegation scheme and applications to reusable MPC from LWE and DDH.
- Experimenting with various idealized oracle models to build better obfuscation schemes from lattices.
- Expanding the feasibility realm of general multi-authority functional encryption using dishonest authorities.
- Identified and achieved lower bounds in general-purpose corruption model in functional encryption.

Research Assistant **Santa Barbara, CA**
Advisor: Prof. Prabhanjan Ananth *Jun 2022 - Sep 2022*

- Worked on public-key functional encryption scheme for specific functionality improving the state-of-the-art.
- Optimizing the novel private-key functional encryption scheme for the same functionality.
- Implementing the public and private key versions using optimal choices for various blocks for efficiency.
- Surveyed FHE based Machine Learning for Privacy protocols and the feasility of FE-based solutions.

EDUCATION

Ph.D. in Computer Science **Madison, WI**
University of Wisconsin-Madison *Sep 2023 - Present*

- Cumulative GPA: 4.0/4.0.
- **Coursework:** CS 880- Cryptographic Proof Systems, CS 760 - Machine Learning, CS 710 - Computational Complexity, CS 763 - Security and Privacy for Data Science, CS 570 - Intro to Human-Computer Interaction.

Masters in Computer Science **Santa Barbara, CA**
University of California Santa Barbara *Sep 2021 - Jun 2023*

- Cumulative GPA: 4.0/4.0. **Major Area:** Foundations of Computer Science
- **Relevant Coursework:** Topics in Quantum Cryptography, Graduate Course in Quantum Computing, Quantitative Information Flow and Side Channel Analysis, Spectral Graph Theory and Laplacian Matrices.

Bachelor of Technology in Electrical Engineering **Chennai, India**
Indian Institute of Technology, Madras *Jul 2014 - May 2018*

- Cumulative GPA: 8.38/10. **Minor:** Mathematics for Computer Science.
- **Relevant Graduate Coursework:** Applied Cryptography, Foundations of Cryptography, Lattice Cryptography, Combinatorics and Number Theory, Mathematical Logic, Combinatorial Optimization, Error Control Coding.

SERVICE AS EXTERNAL REVIEWER

ITCS 2024, Eurocrypt 2024, Asiacrypt 2024, TCC 2023, CRYPTO 2022

TEACHING AND MENTORING EXPERIENCE

COMP SCI 435: Introduction to Cryptography **Madison, WI**
Instructor: Prof. Rishab Goyal *Sep 2024 - Present*

COMP SCI 536: Introduction to Programming Languages and Compilers **Madison, WI**
Instructor: Beck Hasti *Jan 2023 - May 2023*

COMP SCI 435: Introduction to Cryptography **Madison, WI**
Instructor: Prof. Somesh Jha *Sep 2023 - Dec 2023*

CMPSC 138: Automata and Formal Languages **Santa Barbara, CA**
Instructor: Prof. Ben Hardekopf *Apr 2023 - Jun 2023*

CMPSC 111: Introduction to Computational Science **Santa Barbara, CA**
Instructor: Prof. John Gilbert *Jan 2023 - Mar 2023*

CMPSC 130A: Data Structures and Graph Algorithms **Santa Barbara, CA**
Instructor: Prof. Eric Vigoda *Sep 2022 - Dec 2022*

CMPSCW 8: Introduction to Computer Science **Santa Barbara, CA**
Instructor: Prof. Yekaterina(Kate) Kharitonova *Sep 2021 - Sep 2022*

PROJECTS

Non-Interactive PSI from Functional Encryption, Master's Thesis ↗ **Santa Barbara, CA**
Advisor: Prof. Prabhanjan Ananth *Jan 2023 - May 2023*

- Created a non-interactive version of the widely-used and celebrated private set intersection problem.
- Leveraged functional encryption to encode sets in a manner that decryption reveals just the intersection.
- Worked on public- and private-key functional encryption schemes with adaptive simulation security.
- Implemented the schemes using various open-source cryptographic libraries and 128-bit AES scheme as PRF.

Blockchains in Business Networks, Undergraduate Thesis **Chennai, India**
Advisor: Prof. Shweta Agrawal *Jan 2018 - May 2018*

- Prototyped a permissioned blockchain-based business network that stores CRUD activity as a transaction.
- Worked with Hyperledger Fabric and Hyperledger Composer to model the business network.
- Developed REST APIs for the network using AngularJS and NodeJS with data stored in a LAMP stack.
- Tested the prototype business network with data of 10,000+ students in IIT Madras in various scenarios.

Block Cipher Design and Cryptanalysis **Chennai, India**
Advisor: Prof. Chester Rebeiro *Jan 2017 - Apr 2017*

- Designed and implemented a novel 128-bit Feistel cipher with 7 rounds and 4 s-boxes called 'Descartes'.
- Designed four 16x4 compression s-boxes, which obey non-linearity. Each s-box uses a 96-bit sub-key.
- Performed linear, differential cryptanalyses and a timing attack based on the size of the 128-bit key.

Oracle Software Security Projects **Bengaluru, India**
Advisor: Dan Norris *Jul 2018 - Jul 2021*

- Identified and fixed vulnerabilities in Oracle cloud database and frameworks using Oracle cloud DBSAT tool.
- Worked on Oracle cloud database credential storage to remove the usage of clear-text passwords.
- Identified and rectified Oracle Cloud and NetSuite ERP password logging after operational failures.

PROFESSIONAL EXPERIENCE

Oracle R&D India **Bengaluru, India**
Member of Technical Staff *Jun 2018 - July 2021*

Qualcomm India **Hyderabad, India**
Software Engineering Intern *May 2017 - Jul 2017*