SAIKUMAR YADUGIRI

Madison, WI | https://saikumarysk.github.io | saikumarysk | saikumarysk

RESEARCH INTERESTS

I am interested in the theoretical aspects of Functional Encryption, (Fully-)Homomorphic Encryption.

RESEARCH EXPERIENCE

Research Internship **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

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

- Working with Prof. Rishab Goyal on various flavors of multi-authority and multi-input functional encryption.
- Cumulative GPA: 4.0/4.0.

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

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

Indian Institute of Technology, Madras **Chennai, India**
Bachelor of Technology in Electrical Engineering *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.

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.

Cryptopals Challenges ↗ **Bengaluru, India**
Self-guided *Sep 2020 - Present*

Completed the 7-week online cryptography puzzles in Python, which consists of various attack patterns on real-world cryptography implementations and attacks derived from multiple academic papers.

UCSB Course Projects **Santa Barbara, CA**

Advisors: Dr. Bryce A. Boe, Prof. Benjamin Hardekopf, Prof. John Gilbert *Sep 2021 - Jun 2022*

- **HackOverflow:** Designed a mock e-commerce site to find the trade-offs and effectiveness of server scaling.
- **VYFuzz:** Created a probabilistic grammar-based coverage-guided fuzzer to discover bugs in JSON parsers.
- **Graph Coloring** Evaluated spectral heuristic approaches to solve graph coloring using SparseSuite matrices.
- **Chat Server:** Designed and implemented a group chat system with pseudo-auth using React and Javascript.

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.

TEACHING AND MENTORING EXPERIENCE

COMP SCI 536: Introduction to Programming Languages and Compilers **Madison, WI**

Instructor: Beck Hasti *Jan 2023 - Present*

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*

PROFESSIONAL EXPERIENCE

Oracle R&D India **Bengaluru, India**

Member of Technical Staff *Jun 2018 - July 2021*

- Former head of Database upgrade and RAC infrastructure upgrade in Oracle public cloud on OCI and OCI-C.
- Worked on all the major public cloud offerings, ADB-D, ExaCC, ExaCS, DBCS - Classic, and ADB on ExaCC.
- Fixed 50+ business-critical bugs in Database security, VM shape-scale performance issues, Database upgrade, RAC Infrastructure upgrade, Database home backup & recovery, and dataguard reliability.
- Completed 10+ self-guided projects used by several businesses including Verizon.
- Worked on a parallel VM upgrade to improve the time taken by upgrade scenario by over 80%.

Qualcomm India **Hyderabad, India**

Software Engineering Intern *May 2017 - Jul 2017*

- Worked on 4G LTE testing and parsing automation for on-chip devices of Qualcomm 205 Mobile Platform.
- Implemented various finite-state automaton techniques in Python that improved the workflow time by 31%.
- Completed 6 testing scenarios, including signal scattering, threshold calculation, and re-establishment.

Detect Technologies **Chennai, India**

GUMPS Platform GUI Development Intern *May 2016 - Jul 2016*

- Worked on data visualization for real-time health monitoring for pipelines at extremely high temperatures.
- Using WxPython created a GUI installation software. With WebView and three.js, created pipe and fault model rendering from the data. Used the same three.js APIs to render the models on the GUMPS website.

ACHIEVEMENTS

- Placed 6th among ~500 developers in Oracle Security Evangelist Cup organized by SCW platform. 2020
- Awarded 'Star Volunteer' for NSS IIT Madras chapter's 'Teach Your Neighbor' project. 2015
- Stood 878th among 150,000 students in JEE Advanced. 2014
- Secured a national rank of 374th in JEE Mains among 500,000+ students. 2014
- Among the top 1% of students with a rank of 7 in APRJC for the entrance into IIITs. 2012