SAIKUMAR YADUGIRI

✉ my-first-name-here@ucsb.edu | https://saikumarysk.github.io | saikumarysk | saikumarysk

RESEARCH INTERESTS

I am interested in the theoretical aspects of classical and (post-)quantum cryptography—specifically, Non-interactive Zero Knowledge systems, Multi-Party Computation, and Functional Encryption.

RESEARCH EXPERIENCE

Research Assistantship

Santa Barbara, CA

Advisor: Prof. Prabhanjan Ananth

Jun 2022 - Sep 2022

- Designed an efficient, novel public-key functional encryption scheme for specific functionality in the static collusion bound model whose time complexity and size of the ciphertexts are linear in the static query bound.
- Designed a new, efficient unbounded-collusion private-key functional encryption for the same functionality.
- Currently optimizing the private-key functional encryption scheme using secure multi-party computation.
- Implementing the public and private key FE schemes using optimal blocks for efficient execution in C/C++.
- Surveyed FHE based Private Machine Learning protocols and the feasibility of optimal FE-based solutions.
- A paper based on the work will be published soon at an undecided conference.

EDUCATION

University of California Santa Barbara

Santa Barbara, CA

Master's Degree in Computer Science

Sep 2021 - Present

- 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.

TEACHING EXPERIENCE

CMPSC 130A: Data Structures and Graph Algorithms

Santa Barbara, CA

Teaching Assistant, Instructor: Prof. Eric Vigoda

Sep 2022 - Present

Designed class projects, homework assignments, and daily quizzes. Currently handling the class forum on Ed.

CMPSCW 8: Introduction to Computer Science

Santa Barbara, CA

Teaching Assistant, Instructor: Prof. Kate Kharitonova

Sep 2021 - Sep 2022

- Lead TA for more than 10 TAs and 3 ULAs in the Spring and Summer quarters of the course in 2021-2022.
- Helped the professor to manage and improve course logistics and handled the class forum for 250+ students.

PROJECTS

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.
- Utilized Hyperledger Fabric and Hyperledger Composer to model business networks that utilize blockchains.
- 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'.
- Composed 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 and data breaches.

Heuristic Graph Coloring ↗ **Santa Barbara, CA**
Advisor: Prof. John Gilbert *Apr 2022 - Jun 2022*

- Evaluated the efficiency of NP-based and heuristic approaches for graph coloring of Sparse Suite matrices.
- Utilized PySAT's Glucose4 and Z3 SAT solvers to solve the reduced boolean formula to find correct coloring.
- Implemented BG'84 eigenvector sign bundling algorithm as a spectral heuristic approach for graph coloring.

UCSB Course Projects **Santa Barbara, CA**
Advisors: Dr. Bryce A. Boe, Prof. Benjamin Hardekopf *Sep 2021 - Jun 2022*

- **VYFuzz:** Created a probabilistic grammar-based coverage-guided fuzzer to discover bugs in JSON parsers.
- **eKirana:** Implemented a mock e-commerce site to evaluate the trade-offs and effectiveness of server scaling.
- **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.
- Mitigated the usage of clear-text passwords on Oracle cloud database credential storage and failure logs.

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.
- Involved in the development of all the major public cloud offerings, ADB-D, ExaCC, ExaCS, and ADB on ExaCC.
- Designed and implemented parallel RAC Infra and database upgrades to decrease the time by over 80%.
- Mentored 3 employees in Oracle R&D India for Oracle cloud database and Exadata grid upgrade stacks.

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

- Worked on 4G LTE testing and parsing automation for Qualcomm 205 Mobile Platform on-chip devices.
- Implemented various finite-state automaton techniques in Python that improved the workflow time by 31%.

Detect Technologies **Chennai, India**
GUMPS Platform GUI Development Intern *May 2016 - Jul 2016*

- Designed the data visualization platform for real-time health monitoring for pipes at excessive temperatures.
- Used WxPython, WebView, and three.js to create GUI installation software & fault rendering of steam pipes.

ACHIEVEMENTS

- Nominated for the Best TA Award in the computer science department at UC Santa Barbara. 2022
- 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 entrance into IIITs. 2012