Priyanka Mondal

+1-831-251-2070 • pmondal@ucsc.edu • priyanka-mondal.github.io
Priyanka-Mondal • mondalp

Summary

Conducting active research in applied cryptography and decentralized security, exploring both experimental and theoretical dimensions. Having expertise in leakage mitigation techniques for remote computation and information flow control policies. Designed and implemented advanced searchable encryption algorithms in C++. Have worked on multi-party computation, homomorphic encryption and fault-tolerant systems. Thrive in collaborative teamwork dynamics. Eager about creating practical solutions for information and storage security.

Education

PhD, *Computer Science* , University of California, Santa Cruz **GPA: 4.0** 2017–June,2024(expected)
Master of Engineering, *Computer Science* , Indian Institute of Science, Bangalore 2013-2015
Bachelor of Engineering, *Computer Science* , Bengal Engineering & Science University, Kolkata 2009-2013

Skills

Programming skills: C++, C, Java, Haskell, Coq, Dafny, HTML, CSS, Python, JavaScript, Matlab, Rust, Scala

Technical skills: Docker, Git, LaTeX, GDB, Wireshark, OpenSSL, SQL, PostgreSQL, MySQL, Django, Blockchain, AWS, VS Code, Bash, Linux, FreeBSD, IntelSGX

Relevant Coursework: Cryptography, Programming Languages, Distributed systems, Architecture, Databases, Analysis of Algorithms, Automated verification, Data Mining, Operating Systems, Soft computing

Research Experience

Research Interests: Cryptography, Decentralized Security, Language-based Security

Research projects

- **System-wide security for dynamic searchable encryption schemes** UC Santa Cruz
  - Implemented Oblivious RAM with B+ trees in C++, reducing the access time by 2-6× than the existing construction implemented with AVL trees
  - Mechanised an oblivious data-structure to mitigate information leakage during file retrieval from untrusted remote servers
- **Locality-aware dynamic searchable encryption** UC Santa Cruz
  - Designed and implemented a dynamic searchable encryption algorithm in C++, that improves the search time by 4-209×, both on disk and in memory, than the existing counterparts
- **Flow-Limited Authorization for Quorum Replication (FLAQR)** UC Santa Cruz
  - Added availability policies to Flow-Limited authorization model for the first time and implemented robustness proofs in Coq to verify its security
  - Incorporated FLAQR's fault-tolerant language features into a Haskell library called HasChor, and added information flow control policies that bolstered end-to-end information security
- **Detecting and eliminating byzantine peers on blockchain** UC Santa Cruz
  - Developed Ethereum smart contracts in Solidity, as part of a lightning payment network
  - Implemented correctness proofs in Alloy to verify blockchain fault-tolerant protocols
- **Atomicity Checking with Blame Assignment for Android Applications** IISc Bangalore
  - Designed and implemented a bug detection tool in Java, which found 21 bugs in real world Android applications (e.g. Gmail, Wikipedia, MyTracks)

Selected publications

1. ***I/O-Efficient Dynamic Searchable Encryption meets Forward & Backward Privacy*** USENIX'24
   Priyanka Mondal, Javad Ghareh Chamani, Ioannis Demertzis, and Dimitrios Papadopoulos
2. ***Flow-Limited authorization for consensus, replication, and secret sharing*** JCS'23
   Priyanka Mondal, Maximilian Algehed and Owen Arden
3. ***Applying consensus and replication securely with FLAQR*** (Distinguished Paper Award) CSF'22
   Priyanka Mondal, Maximilian Algehed and Owen Arden

Industry Experience

- **Citrix R&D Pvt. Ltd, Bangalore.** Networking & Cloud team ***Software Engineer II***, 2015-17
  - Implemented an algorithm to transmit JSON data from Packet Engines to Amazon S3, that doubled the speed of the Unified Logger Daemon
  - In-charge of implementing an algorithm to convert HAProxy to Netscaler configuration
  - Developed an Wireshark plugin that increased efficiency of internal testing by 30%
- **Nomura Research Institute, Kolkata.** Enterprise Data Warehouse team ***Summer Intern***, 2012
  - Implemented an automated parsing technique to extract information from incoming XML data packets, resulting in 70% improvement of the system in-terms of speed

Additional Information

Selected Talks

- Applying replication and consensus securely with FLAQR - CSF'22, Haifa, Israel
- Flow Limited Authorization for Quorum Replication - PLCrypt'22, Stanford Research Inst.
- Applying replication and consensus securely with FLAQR - PLAS'21 (Virtual)
- A Language for Secure Replicated Computation - CSF'19, New Jersey

Awards and Scholarships

- Distinguished paper award, CSF 2022
- Programming Languages Mentoring Worshop grant, 2019
- Oregon Programming Languages Summer School Student scholarship, 2018
- UC Santa Cruz Regents Fellowship, Winter 2018
- All India Council for Technical Education Scholarship, 2013-2015

Service and Outreach

- Vice President - Women in Cyber-security (WiCyS) students chapter, UC Santa Cruz
- Member - Women in Science and Engineering (WiSE), UC Santa Cruz
- External paper reviewer - AsiaCCS'24, Sigmod'23, FCS'22

Teaching Assistant Experience (at UC Santa Cruz)

- Foundations of Programming Languages - CSE114 (***Head Teaching Assistant***) Winter'24
  - Recursion, Data abstraction, Higher-order functions, Lammbda calculus, Haskell
- Programming Languages - CSE210 (***Graduate course***) Spring'21, Spring'23
  - Type-system and type-checking, proving program properties in Coq
- Advanced Programming - CMPS109 Spring'19, Spring'22
  - Object-oriented programming, multithreaded client/server applications