

Priyanka Mondal

☎ +1-831-251-2070 • ✉ priyanka02010@gmail.com • 🌐 priyanka-mondal.github.io
📄 Priyanka-Mondal • in mondalp

Summary

- **6+** years of experience as a **Security researcher**, and **2+** years of experience as a **Software Engineer**
- **Broader interests:** Security and Privacy in Distributed Systems, Applied Cryptography, Software Engineering
- **Experienced in:** *Design and implementation of provably secure cryptographic techniques and programming models that make distributed systems trustless*

Education

Ph.D., Computer Science, University of California, Santa Cruz, GPA: 4.0/4.0 2017–July'24(expected)
Master of Engineering, Computer Science, Indian Institute of Science, Bangalore, GPA: 6.7/8.0 2013-15
Bachelor of Engineering, Computer Science, Bengal Engineering & Science University, Kolkata, GPA: 8.1/10.0 2009-13

Skills

Programming skills: C++ (**proficient**), C, Python, Java, JavaScript, Haskell, Coq, HTML/CSS, Matlab

Technical skills: Docker, Git, \LaTeX , GDB, OpenSSL, SQL, VS Code, Linux/Unix

Experience

- **University of California, Santa Cruz** *Graduate Research Assistant*, 2018-present
 - **Secure and Efficient search on Encrypted databases ensuring Forward and Backward Privacy**
 - Designed and implemented an encrypted search algorithm that improves database search time by **4-179 \times** , both on disk (HDD/SSD) and in memory, than the existing counterparts (**15k+ LOC, C++**)
 - Implemented a secure data-structure (Oblivious RAM) using cryptographic mechanisms and B-trees, reducing the access time by **2-6 \times** than the existing AVL-tree based construction (**10k+ LOC, C++**)
 - **FLAQR: A programming model to securely implement Consensus, Replication and Secret-sharing**
 - Designed a programming model to write fault-tolerant distributed applications that are secure-by-construction
 - Worked on **type-systems** and Information Flow Control policies
 - Formally verified robustness of security policies of language models in Coq proof assistant (**7k+ LOC, Coq**)
 - Implemented a **Haskell** library to support fault-tolerance and consensus securely for distributed programs
 - **Detecting and eliminating malicious hosts in distributed consensus protocols**
 - Modelled an agreement protocol called PEACH in which replicas vote against and eliminate malicious hosts
 - Implemented formal proofs of safety and liveness for distributed byzantine protocols in **Alloy analyzer**
 - Worked on blockchain based protocols and implemented Ethereum smart contracts
 - **Program analysis and bug detection for distributed applications**
 - Implemented a program analysis tool in **Java** that inspects the flow of program variables during run-time
 - Developed a bug detection tool in **Java** which found **21 bugs** in real world Android applications (e.g. Gmail)
- **Citrix R&D Pvt. Ltd, Bangalore.** Networking & Cloud team *Software Engineer II*, 2015-17
 - Implemented an algorithm in **Python** to transmit **JSON** data from Packet Engines to Amazon S3 buckets, that **doubled** the speed of the Unified Logger Daemon
 - In-charge of implementing an algorithm (in **C++**, **shell scripts**) to convert HAProxy to Netscaler configuration
 - Fixed more than **20** existing bugs in the codebase of Netscaler load-balancer
 - Developed an **Wireshark** plugin that increased efficiency of **HTTP/TCP** packet testing by **30%**
- **Nomura Research Institute, Kolkata.** Enterprise Data Warehouse team *Summer Intern*, 2012
 - Deployed an automated parsing technique in **Java** to extract information from incoming **XML** data packets, resulting in **70%** improvement of the system in-terms of speed

Selected publications

1. [P. Mondal](#), J. G. Chamani, I. Demertzis, and D Papadopoulos. *I/O-Efficient Dynamic Searchable Encryption meets Forward & Backward Privacy*. **33rd USENIX Security**, 2024
2. [P. Mondal](#), M. Algehed and O. Arden. *Flow-Limited authorization for consensus, replication, and secret sharing*. **31st Journal of Computer Security**, 2023
3. [P. Mondal](#), M. Algehed and O. Arden. *Applying consensus and replication securely with FLAQR*. **35th IEEE Computer Security Foundations**, 2022 ([Distinguished Paper Award](#))