Radhika Garg

| | | | |

Summary

Ph.D. candidate in applied cryptography at Northwestern University, advised by Dr. Xiao Wang. My research sits at the intersection of theory and systems. I design cryptographic protocols and build the compiler infrastructure to make them deployable. I built Smaug, an LLVM-native compiler that makes secure computation accessible to developers without expertise in MPC, compiling up to 1240× faster than prior tools. My protocol work spans scalable MPC for large numbers of parties, efficient noise sampling for differentially private federated learning, certifiable DP mechanisms, and threshold signatures compatible with the standardized NIST FALCON parameters.

Education

Northwestern University September 2022 – Present
Ph.D. Computer Science GPA: 3.967/4
Advisor: Dr. Xiao Wang

Indian Institute of Technology, Roorkee July 2018 – May 2022
B.Tech. Computer Science and Engineering GPA : 9.371/10

Publications

Radhika Garg, Kang Yang, Jonathan Katz, Xiao Wang. **Scalable Mixed-Mode MPC**. *IEEE S&P 2024*. Code

Radhika Garg, Xiao Wang. **Smaug: Modular Augmentation of LLVM for MPC**. *IEEE S&P 2025*. Code

Olive Franzese, Congyu Fang, **Radhika Garg**, Xiao Wang, Somesh Jha, Nicolas Papernot, Adam Dziedzic. **Secure Noise Sampling for Differentially Private Collaborative Learning**. *ACM CCS 2025*. Code

Qi Pang, **Radhika Garg**, Ziling Liu, Hanshen Xiao, Virginia Smith, Wenting Zheng, Xiao Wang. **Noisette: Certifying Differential Privacy Mechanisms Efficiently**. *In submission.*

Research Projects

Thresholdizing Standardized FALCON Signatures February 2025 – Present

– Designed the first threshold signing protocol for NIST FALCON whose signatures verify against the *unmodified* standard; prior hash-and-sign threshold schemes produce signatures and keys too large to be compatible with FALCON's deployed parameters.

– Replaced the FFO-based sampler with an MPC-friendly Klein sampler and designed a PCG for authenticated VOLE, reducing AND gates from 1.83B to 140M (∼13×) and per-signature communication by $10^7\times$ for $N = 4$ parties.

– *Ongoing:* designing efficient distributed key generation for FALCON (including NTRU solving in MPC) and reducing online signing rounds to fewer than 10.

Noisette: Certifying Differential Privacy Mechanisms February 2024 – Present

– Proposed Noisette, a unified framework for certifying DP noise sampling across discrete and contin-

uous mechanisms, supporting arbitrary additive noise including Gaussian, Laplace, and Skellam.

– Designed a certifiable lookup-table protocol for arbitrary distributions; achieves up to 30× runtime improvement and 36× communication reduction over prior SOTA for discrete Gaussian sampling.

– Provided the first better than naive certifiable protocol for continuous Gaussian sampling, achieving ∼64× speedup and ∼15× lower communication vs. SOTA.

Work Experience

Research Intern | Silence Laboratories June 2026 – October 2026
Advisor: Dr. Yashwanth Kondi
Incoming research intern focused on threshold cryptography and MPC protocols.

Research Intern | AI4Crypto, FAIR, Meta June 2025 – November 2025
Advisor: Dr. Kristin Lauter

– Designed transformer-based neural distinguishers targeting the EA-LPN problem, achieving advantage > 0.5 against the aggressive parameters in the original EA-LPN assumption proposal (Boyle et al.).

– Reverse-engineered the learned model to derive a formal statistical distinguisher, bridging deep learning intuition with cryptographic analysis.

Research Intern | Northwestern University February 2022 – May 2022
Advisor: Dr. Xiao Wang
Extended emp-toolkit with a GMW circuit interface supporting SIMD execution, triple generation, and round-efficient Bristol circuit evaluation.

Software Engineering Intern | AI4SG, Google Research June 2021 – August 2021
Fairness analysis for RMAB-based resource allocation (Python, TensorFlow).

Software Engineering Intern | Google Maps, Bangalore May 2020 – June 2020
Time-lapse visualizer for geographic datasets (JavaScript, Google Maps API).

Achievements

Cabell first year fellowship — Selected among the 10 recipients of all applicants in the McCormick School of Engineering and Applied Sciences.

Best B.Tech. Thesis Project Award 2022 — Awarded the best BTP in the Computer Science Dept.

Joint Entrance Examination 2018 (Advanced) — Ranked in top 0.4 percentile with a rank of 669 among 150,000 candidates.

Skills

MPC & Crypto Tools emp-toolkit, OpenFHE, LLVM.
Languages C, C++, Python, Bash, JavaScript, Scala, LaTeX.
Dev Tools Git, GDB, LLDB, Docker.
Platforms Linux, Windows, WSL.

Professional Service

External Reviewer TCC 2025, Eurocrypt 2025, Crypto 2025.
Outreach Graduate Women in Computing (Northwestern) · Information Management Group (IIT Roorkee) · Student Mentorship Program (IIT Roorkee) · Technovation Girls.