Nirajan Koirala

✉ nkoirala@nd.edu ☎ 334-372-2989 LinkedIn Homepage GitHub Scholar

Research Summary

Ph.D. Candidate in Computer Science (GPA 4.00) focused on **trusted computing and applied cryptography**, translating privacy requirements into **production-grade** Python/C++/C# systems across **Nvidia Confidential Computing**, **Intel SGX**, **AMD SEV**, and privacy-preserving analytics (FHE/MPC). Identified, analyzed, and remediated real-world privacy/security threats in privacy-preserving face recognition applications, ensuring robust security and privacy measures were in place. Experienced in code maintenance/review, containerized dev/test, and **clear written narratives** (design docs, experiment reports).

Education

University of Notre Dame Notre Dame, IN
Ph.D. *in Computer Science and Engineering (University Fellow) | Advisor: Dr. Taeho Jung* *12/2026 (Expected)*
Thesis- Towards a Scalable Framework for Large-Scale Sensitive Workloads using FHE and TEEs
Research Areas: Applied Cryptography - FHE, Secure Multi-Party Computation, TEEs, Privacy Preserving ML

Villanova University Villanova, PA
M.S. *in Computer Science (GPA: 3.79) — Upsilon Pi Epsilon (Computer Science Honor Society), 3MT finalist* *05/2021*
Thesis: Adversarial Attacks against Deep Neural Networks

Troy University Troy, AL
B.S. *in Mathematics and Computer Science (GPA: 3.75) — Magna Cum Laude* *05/2019*
Pi Mu Epsilon (Mathematics Honor Society), Chancellor's Scholarship (full-tuition scholarship)

Research/Professional Experiences

University of Notre Dame — Graduate Research Assistant Notre Dame, IN
Skills: C++, Python, C#, Gramine, OpenFHE, gdb, Shell Scripting, Git, Docker, CUDA, SQL, LaTeX *06/2021 – Present*

- Architecting a **heterogeneous trusted-computing framework** that uses **Intel SGX** as a control plane to orchestrate and attest fleets of **Intel TDX**–VMs, using **Nvidia CC enabled GPUs** (H200) targeting scalable remote attestation, stronger user trust, and reduced per-client latency/overhead.
- Built privacy-preserving face recognition and record linkage applications in enclaves using **Intel SGX** and **Gramine**; implemented attested APIs and enclave-aware dataflows for scalable execution.
- Evaluated performance of enclave workloads in **Intel SGX** (SGX SDK), including *VM image integrity hashing* and *matrix multiplication* variants; built reproducible benchmarking harnesses and analysis scripts.
- **Cryptonite** (SN Computer Science 2025): developed **secure aggregation** framework using Intel SGX with rigorous privacy guarantees and fault tolerance.
- **HyDia** (PoPETs 2025): engineered an FHE-based facial matching pipeline with **hybrid approximations** and **diagonalization**; implemented evaluation harnesses, packing/rotation schedules, and throughput optimizations with assertions and trace points for reliability and debuggability.
- **HEProfiler** (Journal of Cryptographic Engineering 2024): designed and implemented a C++/Python **profiling & telemetry** framework for approximate HE libraries (OpenFHE, HElib, Microsoft SEAL, HEAAN) employing CKKS.

Intel Corporation — Homomorphic Encryption Engineer Hillsboro, OR
Skills: C++, Python, HEBench, HElib, OpenFHE, Docker, Git *05/2022 – 08/2022*

- Integrated multiple homomorphic encryption backends into HEBench; standardized configurations and result schemas to enable cross-library and cross-hardware comparisons.
- Discovered and fixed a bug in the open-source **HElib** library, delivering improvements that reinforced validation.

Crane Payment Innovations — Software Engineering Intern Malvern, PA
Skills: C#, WPF, .NET, Windows, Python, Node.js, Testuff API, AES Encryption *05/2020 – 08/2020*

- Built a Windows WPF application to orchestrate communications with IoT payment devices.
- Implemented messaging workflows, diagnostics, and API-driven testing to improve reliability and validation.
- Designed the application's core architecture across front-end and back-end for maintainability and scale using Agile/Scrum practices.

ALFA Insurance — Web Developer Intern Montgomery, AL
Skills: Mobile Application Development, Front End/Back End, DBA, QA *05/2018 – 07/2018*

- Deployed an internal mobile application for insurance agents that reduced quote time by **75%**.
- Contributed across front end, back end, DBA, and QA roles to deliver end-to-end functionality.

Mentoring/Teaching Experiences

University of Notre Dame — Graduate Teaching Assistant Notre Dame, IN
Courses: CSE 40622 (Cryptography, incl. FHE), CSE 40113 (Design/Analysis of Algorithms) *08/2021 – 05/2022*

- Held office hours, graded assignments, gave guest lectures, and proctored examinations.
- Reinforced problem-solving strategies and proof techniques; clarified cryptographic concepts and applications.
- Awarded CSE Outstanding Teaching Assistant Award (2022).

University of Notre Dame — Research Mentor, Summer Enrichment Program Notre Dame, IN
Skills: Mentoring, Applied Cryptography (FHE), Intel SGX, Gramine, SageMath *Summers 2024 & 2025*

- **2025:** Guided rising sophomores to implement a *Key Generation Authority (KGA)* using **SageMath** inside an **Intel SGX** enclave (via the **Gramine** LibOS); the enclave securely handled key generation and distribution as part of a prototype *Safety-Aware Drone Ecosystems (SADE)* framework.
- **2024:** Mentored rising sophomores to design and implement an *anonymous survey application* using **FHE**, emphasizing secure data collection and privacy-preserving analytics.

Troy University — Computer Science Tutor Troy, AL
Skills: Tutoring, CS Lab Operations, Intro CS Pedagogy *08/2018 – 05/2019*

- Supported Computer Science lab operations and assisted students in foundational programming courses.
- Tutored *Computer Science I/II* and *Nature of Programming Languages*.

Technical Skills

Languages & Tools: Python, C++, C#, WPF, .NET, SQL, Bash, LaTeX, Git, Linux, gdb, CMake, Docker
Privacy & Security Engineering: Applied cryptography (FHE, MPC); privacy-preserving systems design; threat modeling; secure coding practices; technical specifications & documentation
Trusted/Confidential Computing: Intel SGX, Intel TDX, Intel SGX SDK, Gramine (LibOS), AMD SEV–SNP, Nvidia CC
Data & Analytics: NumPy, Pandas, SciPy, Matplotlib, Weights & Biases
Software Engineering Practices: Code maintenance & review; containerized dev/test; reproducible pipelines; agile/scrum practices; metrics & reporting mechanisms

Selected Publications

- **Koirala, N.**, Paik, S., Martin, S., Berens, H., Januszewicz, T., Takeshita, J., Seo, J. H., Jung, T. *Select-Then-Compute: Encrypted Label Selection and Analytics over Distributed Datasets using FHE.* Accepted for publication, NDSS 2026.
- Paik, S., **Koirala, N.**, Nero, J., Son, H., Kim, Y., Seo, J. H., Jung, T. *Scalable Private Set Intersection over Distributed and Encrypted Data.* Accepted for publication, ACM AsiaCCS 2026.
- Paik, S., **Koirala, N.**, Nero, J., Son, H., Kim, Y., Seo, J. H., Jung, T. *DFPSI: Decoupled Fuzzy Private Set Intersection.* Under review, USENIX 2026.
- Takeshita, J., McKechney, C., Pajak, J., Karl, R., **Koirala, N.**, Jung, T. *Combining Intel SGX and Homomorphic Encryption for Trustworthy Distributed Large-Scale Data Analytics.* Under review, ADMA 2025.
- Karl, R., Takeshita, J., **Koirala, N.**, Jung, T. *Cryptonite: a framework for flexible time-series secure aggregation with online fault tolerance.* Springer Nature Journal of Computer Science, 2025.
- Martin, S., **Koirala, N.**, Berens, H., Rozgonyi, T., Brody, M., Jung, T. *HyDia: FHE-based Facial Matching with Hybrid Approximations and Diagonalization.* PoPETs, 2025.
- **Koirala, N.**, Takeshita, J., Stevens, J., Jung, T. *Summation-based Private Segmented Membership Test from Fully Homomorphic Encryption.* PoPETs, 2025.
- Januszewicz, A., Gutierrez, D., **Koirala, N.**, Zhao, J., Takeshita, J., Lee, J., Jung, T. *PPSA: Polynomial Private Stream Aggregation for Time-Series Data Analysis.* EAI SecureComm, 2024.
- **Koirala, N.**, Takeshita, J., McKechney, C., Jung, T. *HEProfiler: An In-Depth Profiler of Approximate Homomorphic Encryption Libraries.* Journal of Cryptographic Engineering, 2024.
- Wang, Z., Sheng, Y., **Koirala, N.**, Jung, T., Jiang, W. *PristiQ: A Co-Design Framework for Preserving Data Security of Quantum Machine Learning in the Cloud.* IEEE Computer Society Annual Symposium on VLSI, 2024.
- **Koirala, N.** *Adversarial Attacks Against Deep Neural Networks.* Villanova University, ProQuest, 2021.