Nirajan Koirala
nkoirala@nd.edu
https://n7koirala.github.io/

EDUCATION

Doctor of Philosophy (4.00/4.00 GPA), Computer Science and Engineering
University of Notre Dame (Notre Dame, IN) June 2021 - December 2025
Area of research: *Applied Cryptography, including Fully/Somewhat Homomorphic Encryption, Secure Multi-Party Computation techniques and Trusted Execution Environments*

Master of Science (3.79/4.00 GPA), Computer Science
Villanova University (Villanova, PA) Aug. 2019 - May. 2021
Thesis: *Adversarial Attacks against Deep Neural Networks*

Bachelor of Science (3.75/4.00 GPA - Magna Cum Laude), Mathematics and Computer Science
Troy University (Troy, AL) Aug. 2015 - May 2019

SKILLS AND COURSEWORK

Languages and Tools: **C++**, C#, Python, Git, Linux, gdb, LaTeX, Shell Scripting, CMake, Tensorflow, SQL, PHP

Homomorphic Encryption Libraries: HEAAN, HElib, Microsoft SEAL, OpenFHE (Palisade)

Computer Science: **Cryptography and Network Security**, Computer Networking, Operating Systems, Computer Architecture/Organization, **Design and Analysis of Algorithms**, **Data Structures and Algorithms**, Theory of Computing, Machine Learning, Deep Learning, High Performance Computing, IoT

Mathematics: **Abstract Algebra**, **Linear Algebra**, Topology, Real Analysis, Axiomatic Geometry, Applied Discrete Mathematics, Calculus I-III, Differential Equations, Statistics Methods and Computations, Statistics I and II

Foreign Languages: Nepalese (native), Hindi (fluent)

WORK EXPERIENCE

Graduate Research Assistant June 2021 - Present
University of Notre Dame (Notre Dame, IN), Department of Computer Science and Engineering

- Conducting research in areas including **FHE**, **SHE**, Trusted Execution Environments (Intel SGX, TDX and AMD SEV), and Secure Multi-party Computation.

Homomorphic Encryption Engineer May 2022 - Aug. 2022
Intel Corporation (Hillsboro, OR)

- Integrated HE backends into the HEBench benchmarking project
- Actively contributed to the development and improvement of the HElib library

Graduate Research Assistant Aug. 2019 - Jan. 2021
Villanova University (Villanova, PA), Department of Computing Sciences

- Researched under the technical area team for secure configurations to build and integrate new tools with ConSec System

- Tools used: Python, Prolog, Ptolemy II, ConSec Common Modeling Language (CCML)

Software Engineering Intern May 2021 - Aug. 2021
Crane Payment Innovations (Malvern, PA)
- Built a WPF-application to handle communications with IoT payment devices
- Developer on the front/back-end responsible for designing the main architecture of application
- Technologies used: C#, Python, Testuff API, Node.js, AES Encryption

Web Developer Intern May 2018 – July 2018
ALFA Insurance (Montgomery, AL)
- Deployed a mobile application to be used by insurance agents which decreased the quote providing time by 75%
- Developer on front/back-end, DBA and QA positions.

HONORS AND AWARDS

University of Notre Dame (Notre Dame, IN)
CSE Outstanding Teaching Assistant Award (2022)
University Fellow (fellowship offered to the top 10% by the Department of Computer Science and Engineering, 2021)

Villanova University (Villanova, PA)
Upsilon Pi Epsilon (Computer Science Honor Society), 3MT finalist

Troy University (Troy, AL)
Chancellor's List (2018, 2019), Provost's List (2016, 2017), Pi Mu Epsilon (Mathematics Honor Society), Chancellor's Scholarship (full-tuition scholarship)

PUBLICATIONS

Nirajan Koirala, Jonathan Takeshita, Jeremy Stevens, Sam Martin, Taeho Jung. *PSMT: Private Segmented Membership Test for Distributed Record Linkage* 2024. Under Review in IEEE Transactions on Dependable and Secure Computing (TDSC).

Nirajan Koirala, Jonathan Takeshita, Jeremy Stevens Taeho Jung. *Summation-based Private Segmented Membership Test from Fully Homomorphic Encryption.* 2024. Published in the Privacy Enhancing Technologies Symposium (PETS).

Antonia Januszewicz, Daniela Gutierrez, Nirajan Koirala, Jiachen Zhao, Jonathan Takeshita, Jaewoo Lee, Taeho Jung. *PPSA: Polynomial Private Stream Aggregation for Time-Series Data Analysis.* 2024. Published in EAI SecureComm Security and Privacy in Communication Networks.

Nirajan Koirala, Jonathan Takeshita, Colin McKechney, Taeho Jung. *HEProfiler: An In-Depth Profiler of Approximate Homomorphic Encryption Libraries.* 2024. Published in the Journal of Cryptographic Engineering.

Zhepeng Wang, Yi Sheng, Nirajan Koirala, Taeho Jung and Weiwen Jiang. *PristiQ: A Co-Design Framework for Preserving Data Security of Quantum Machine Learning in the Cloud.* 2024. Published in IEEE Computer Society Annual Symposium on VLSI.

Ryan Karl, Jonathan Takeshita, Nirajan Koirala, Taeho Jung. *Cryptonite: a frame-*

work for flexible time-series secure aggregation with online fault tolerance. 2022. Under review in Springer Nature Journal of Computer Science.

Koirala, Nirajan. *Adversarial Attacks Against Deep Neural Networks.* Villanova University, ProQuest Dissertations & Theses, 2021. 28489974.

TEACHING EXPERIENCE

Graduate Teaching Assistant Aug. 2021 - May 2022

University of Notre Dame (Notre Dame, IN), Department of Computer Science and Engineering

- CSE 40622 (Cryptography: Modern cryptographic techniques including **FHE**) and CSE 40113 (Design/Analysis of Algorithms)
- Held office hours, graded assignments, and proctored examinations

Computer Science Tutor Aug. 2018 - May. 2019

Troy University (Troy, AL), Department of Computer Science

- Responsible for the proper operation of Computer Science Lab
- Tutored freshman and sophomore students for Computer Science courses (Computer Science I and II, Nature of Programming Languages)

SERVICE

Served as a mentor and teacher for enlisted service members, both active-duty and veterans of the US Military, during a college-preparatory academic boot camp at the Warrior-Scholar Project (WSP) 2024, University of Notre Dame, IN.
Served as a research mentor for the 2024 Summer Enrichment Program to mentor undergraduate students at the Computer Science and Engineering Department, University of Notre Dame, IN.
Peer Reviewer for Securecomm 2023 & 2024 (8 papers reviewed)
Served in the 2023 Tech Industry Interns Panel for Graduate Students at the University of Notre Dame, IN
Peer Reviewer for IEEE Transactions on Cloud Computing 2021 and 2022 (6 papers reviewed)

EXTRA-CURRICULAR ACTIVITIES

University of Notre Dame (Notre Dame, IN)
Book Club Member (2021-Present)
Bengal Bouts Boxing Champion 2022 (146 lb weight division)
Intramural Soccer League Champion (Fall 2022 and Spring 2023, Notre Dame, IN)

Villanova University (Villanova, PA)
Graduate Student Ambassador

Troy University (Troy, AL)
Volunteered at the Troy University BEST Robotics Kick Off
Active member of the Computer Science Club and the Square Root C Math Club
Vice-President of Troy Nepalese Student Association
Played for the Troy's Men Soccer Club (Troy FC)