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 - May 2024
Area of research: *Applied Cryptography, including Fully/Somewhat Homomorphic Encryption, Lattice-based Cryptography, 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

PROJECTS

Profiling of Homomorphic Encryption Libraries. Computer Science and Engineering Department, University of Notre Dame.
- Performance evaluation of **HE libraries** for primitive operations (multiplication, rescaling, relinearization etc.) and application level tasks (linear transform, dot product, polynomial evaluation) using a test framework in **C++**
- Active collaboration with CryptoLab (HEAAN), Duality Technologies (Palisade), Intel (HElib) and Microsoft SEAL for measuring various operations native to each library's **CKKS** implementation
- Comparing **HEAAN**, **HElib**, **Microsoft SEAL**, **PALISADE** alongside working with all stakeholders to fine tune library's parameters for performance and security.

Implementation and Performance study of Advanced Encryption Standard. Electrical and Computer Engineering Department, Villanova University. Link: `bit.ly/AESproject0`

Applications of Deep Learning Methods in Autonomous Driving Systems. Department of Computing Sciences, Villanova University.
Link: `bit.ly/autonomous_driving_dl`

SKILLS AND COURSEWORK

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

Homomorphic Encryption Libraries: HEAAN, HElib, Microsoft SEAL, 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)

HONORS AND AWARDS

University of Notre Dame (Notre Dame, IN)
CSE Outstanding Teaching Assistant Award (2022)
Bengal Bouts Boxing Champion 2022 (146 lb weight division)
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)

WORK EXPERIENCE

Graduate Research Assistant   June 2021 - Present
University of Notre Dame (Notre Dame, IN), Department of Computer Science and Engineering
- Performing investigation with **Cryptolab**, **Duality Technologies**, **Intel** and **Microsoft Research** for profiling HE libraries
- Conducting research in areas including **FHE**, **SHE** and Trusted Execution Environments (Intel SGX, TDX and AMD SEV)

Homomorphic Encryption Engineer   May 2022 - Aug. 2022
Intel Corporation (Hillsboro, OR)
- Backend developer for adding HE backends to HEBench project
- Contributed to the HElib (an open-source HE software library)

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

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

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)

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.

EXTRA-CURRICULAR ACTIVITIES

University of Notre Dame (Notre Dame, IN)
Book Club Member (2021-Present)
Captain of multiple intramular soccer teams

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
Organized various events through Troy Nepalese Student Association
Played for the Troy's Men Soccer Club (Troy FC)