KUSHAL POKHAREL

+1 859-509-8690 ◇ Indianapolis,Indiana
kupokh@iu.com ◇ https://www.linkedin.com/in/kushal-pokharel/ ◇ https://github.com/kushalpokharel

SUMMARY

I am purusing a PhD degree in Indiana University Indianapolis under my advisor Dr. Xukai Zou. I am particularly interested in intersection of AI and privacy in fields like Secure Aggregation in Federated Learning and have also been surveying and studying the state of art in Post Quantum Cryptography especially based on Learning with Error cryptosystems. I am also developing some tools to visualize the Lattices and operations on them.

EDUCATION

PhD in Computer Science, Indiana University Indianapolis, Indiana, US 2025 - 2029(expected)
Relevant Coursework: Software Security and Information Assurance, Algorithm Design and Analysis
Full-time RA: working on researching the current state of the art in Secure MultiParty Computation applications in Federated Learning to share the model updates securely, and Post Quantum Cryptography

SKILLS

Technical Skills	Rust, Javascript, TypeScript, Haskell, React, Linux, Docker, Microservices
Soft Skills	Problem Solving, Critical Thinking, Teamwork

EXPERIENCE

Software Engineer Feb 2024 - Dec 2024
Venture23 *United States - Remote*

- Led the development of Aleo programs in Aleo Eth Bridge project, which is the primary source to bridge assets from Ethereum to Aleo.
- Led zero-knowledge research within the company and conducted multiple sessions on zero-knowledge proofs and blockchain privacy.
- Contributed in the development of a testing tool called doko-js to test out programs written in leo language.

Haskell/Cardano developer Sep 2022 - Present
Sireto Technology *Netherlands* - Remote

- Contributed to the development of KuberIDE https://kuberide.com/, an online IDE for Plutus developers to write smart contracts and compose various transactions. My contributions to the project involve the address-to-keys conversion. Writing the compiler server to compile the smart contracts written in the IDE. Copied the examples from the Plutus-use-cases repository and made them compatible with the IDE.
- Mentored interns to kickstart their journey into the Cardano world by curating the resources and assignments relating to Haskell and Plutus.
- Led the development for Chainsync notifier that notifies your API of any event that happens with your address using Cardano-streaming library. It is particularly useful when you have a pending transaction in your app, and rather than polling, you could use this service for event-based notification that triggers after your transaction is complete.

Blockchain Developer Internship Apr 2022 - Aug 2022
Nethermind *UK* - Remote

- Developed Forta bots to detect unusual transactions on Ethereum blockchain
- Completed Ethernaut's challenges and some Damn Vulnerable Defi challenges.
- Learn about L2 advancements in Ethereum and Starknet ecosystem (Cairo)

PERSONAL PROJECTS

Lattice visualization
Working on the first version of the project where users can interact and visualize different lattice instances uniquely defined by their bases, change the bases, see the dual version of the lattice and visualization of the Guassian distribution functions.

Secure Multiparty Computation
Implementation of a Paillier Cryptosystem-based Secure Multiparty Computation where n-number of clients with private data interact to receive some random numbers whose multiplication is equal to the sum of the private data. Done in Rust using the actix-actor model and the websocket connection between a relayer/server and clients.

COVID detection using Bluetooth Technology
Developed during a college minor project, the application employs Bluetooth technology to maintain a comprehensive record of interpersonal interactions. In the event where an individual tests positive for a virus, they can update their status, triggering notifications for all individuals who have been in contact within two degrees of separation. This system effectively enables timely and informed responses to potential health risks within a network of connections

SURVEY PAPERS

A survey on defenses for Poison Attack in Federated Learning
Due to the distributed nature of Federated Learning, anyone can participate in the learning process and try to poison the model either in targeted or untargeted manner. In the survey here, I study different defense mechanisms being used to prevent such poison attack in Federated Learning.

A survey on Side Channel attacks on Kyber
The cryptosystems have evolved to resist quantum attacks using different hardness assumption which is difficult even for quantum computers to solve but during this transition, other side channels like computation time can be used to leak the information. I am studying different side channel attacks being employed on Kyber (R-LWE based cryptosystem).

ACHIEVEMENTS

- **Runner Up** LOCUS Codejam, Nepal
- **Problem Solving** Hackerrank verified problem solver
- **Competitive exam** Top 0.1% All Nepal Rank in IOE examination