Research Summary

Brief Summary of Research Experiences and Publications

Vishnu Asutosh Dasu (6th January, 2024)

Security, Privacy, and Machine Learning

Trustworthy ML

- Developed secure aggregation protocols for privacy-preserving federated learning
  - *ACM AISEC Workshop CCS 2022*
- Developed attacks to extract data from language models in federated learning
  - *Under review at USENIX Security 2024*
- Developed algorithm to “repair” neurons to improve fairness in neural networks
  - *Under review at ACM ISSTA 2024*
- Helped develop privacy-preserving deduplication protocols for federated learning
  - *Tentative submission to ACM CCS 2024*
- Helped develop differentially private dataset distillation techniques with tight privacy guarantees
  - *Tentative submission to ICML 2024*
- Developed algorithms to remove FGSM and PGD noise from CNNs
- Developed algorithms to detect insider threats and anomalies from employee network logs using ML

Cryptography and Machine Learning

ML for Cryptography

- Designed a framework to perform side-channel attacks on stream ciphers using ML
  - *IACR TCHES 2022*
- Designed ML algorithms for differential cryptanalysis
  - *IEEE Access 2023, EUROCRYPT Workshops 2021*
- Developed algorithms to generate implementations of linear layers in block ciphers using XOR2 and XOR3 gates
  - *INDOCRYPT 2021, ACNS Workshops 2021*
- Developed algorithm to generate implementations of linear layer in block ciphers using XOR2 gates
  - *EUROCRYPT Workshops 2021*
- Developed algorithms to generate quantum implementations of 4x4 S-Boxes
  - *IEEE SOCC 2019*

Miscellaneous

NLP, CV, and Robotics

- Developed data pre-processing algorithms and language models for conversational task assistants
  - *Amazon Alexa Prize TaskBot Challenge 2 Proceedings*
- Developed an algorithm to identify 3-D coordinates of a human from live 2-D video feed
  - *Technical Report (Best Project Award)*
- Worked on clustering and tracking LiDAR point clouds and sensor fusion using Kalman filters for localization in autonomous vehicles.
  - *IGVC 2018*
- Reproduced GANSpace (NeurIPS 2020) during ML Reproducibility Challenge
  - *ReScience C 2022*