HONGYU REN

Yinchuan, China.750001 | +86 15109503582 | lubricantrhy@gmail.com

Education

Master of Science Artificial Iintelligence 09/2023 - Current
Guangzhou University Guangzhou, China

- **Thesis:** *Research on Score-based Black Box Adversarial Attacks*
- **Coursework in** *Pattern Recognition, Machine Learning, Privacy Preservation, Intercultural Communication, Modern Cryptography, Lectures on Frontier of Research, Blockchain Technology and Practice.etc.*
- **GPA:***85.88/100*

Bachelor of Science Computer Science and Technology 09/2019 - 06/2023
Jilin University Jilin, China

- **Thesis:** *Research and Implementation of Acceleration Methods for Deep Binary Neural Networks on Multi-core and GPU*
- **Coursework in** *Foundation of Computer Science, Calculus A, Linear Algebra, Discrete Mathematics, Algorithm Design and Analysis, Computer Organization,Data Structure, Computer Architecture,etc.*
- **GPA:** *81.61/100*

Publications

- *Yang, Y., Liang, X., Song, X., Dong, Y., Huang, L., Ren, H., Dong, C., & Zhou, J. (2025). Maliciously secure circuit private set intersection via SPDZ-compatible oblivious PRF. Proceedings on Privacy Enhancing Technologies, 2025(2), 680–696. https://doi.org/10.56553/popets-2025-0082*
- *A Flexible and Efficient PSI-CA Protocol with Malicious Security, Differential Privacy, and Fairness.(Awaiting Submission for Publication)*
- *Ren, H., Song, X., Zhang, Q., Huang, L., Cai, Q., Lin, Y., ... & Dong, C. Latency-aware (2+1)-PC and its application to secure transformer inference（submitted to USENIX Security 2026)*

Research Experiences

- **Privacy-Preserving Machine Learning under Secret Sharing (Collaborative Research with ByteDance)** 02/2025-Now
- **Explainable AI: A Method for Calculating Contribution Importance of Parameters, Neurons and Inputs** 09/2023-01/2024
  Performing explainable analysis of the pre-trained vision model on ImageNet.
- **AI Security:Black-box Adversarial Attack and Defense Algorithms** 09/2024-Now
  Improvement of score-based black box adversarial attack algorithm and improvement of the stochastic adversarial defense algorithm against adaptive attacks
- **Heterogeneous Computing Acceleration Algorithm of Neural Network Based on SYCL (Intel DPC++)** 12/2022-03/2023
  Implementation of fully connected layer inference algorithm of binary neural networks
- **The Application of Multi-omics graph Convolutional Neural Networks in Disease Classification and Biomarker Recognition** 12/2021-03/2022
  Reproduction of the experimental results of the thesis and structure improvement of GCN model
- **Simulation of Operant Conditioning reflex in Brain-Inspired Neural Networks.** 07/2019-Now
  Simulating Leaky Integrate-and-Fire (LIF) neurons, with Spike-Timing-Dependent Plasticity(STDP) employed as the learning rule instead of gradient descent, accomplishing the learning of operant conditioning reflex in the multi-armed bandit problem.

Skills

- Programming: C/C++, Python , CUDA, SYCL/DPC++, OpenMP
- Pytorch: Customizing Optimizer and Back Propagation
- AI: Deep Learning, Reinforcement Learning, Brain-Like Intelligence, XAI, Generalization.
- Fundamentals: Algorithms, Data Structures, Hardware Architecture of CPUs and GPUs.
- Privacy-preserving AI inference

Languages

English

IELTS: Overall Score 6.5

Chinese (Mandarin)

Native

GRE Score

Total Score: 320