HE Paper Summary

MPC Basics

- MPC short course [link]

HE Basics

- Introduction to the BFV encryption scheme [link]
- Introduction to the BGV encryption scheme [link]
- Introduction to the CKKS/HEAAN FHE Scheme [link]
- How to pack a convolution for HE:
    - Coefficient packing: [Slides]
- A very good HE introduction (in Chinese) [link]

Algorithm and Protocol

[Arxiv'23] HyPHEN: A Hybrid Packing Method and Optimizations for Homomorphic Encryption-Based Neural Networks

[Usenix Security'22] Cheetah: Lean and Fast Secure Two-Party Deep Neural Network Inference

[NeurIPs'22] CryptoGCN: Fast and Scalable Homomorphically Encrypted Graph Convolutional Network Inference

[ICML'22] Low-Complexity Deep Convolutional Neural Networks on Fully Homomorphic Encryption Using Multiplexed Parallel Convolutions

[NeurPs'22] Iron: Private Inference on Transformers

[CCS'17] Oblivious Neural Network Predictions via MiniONN Transformations

Compiler

[PLDI'19] CHET: An Optimizing Compiler for Fully-Homomorphic Neural-Network Inferencing

[PLDI'20] EVA: An Encrypted Vector Arithmetic Language and Compiler for Efficient Homomorphic Computation

[Arxiv'21] SoK: Fully Homomorphic Encryption Compilers

[ASPLOS'23] Coyote: A Compiler for Vectorizing Encrypted Arithmetic Circuits

[HPCA'23] TensorFHE: Achieving Practical Computation on Encrypted Data Using GPGPU

[Arxiv'23] HE-MAN: Homomorphically Encrypted MAchine learning with oNnx models

[Arxiv'23] HECO: Fully Homomorphic Encryption Compiler

Hardware

[Usenix Security'18] GAZELLE: A Low Latency Framework for Secure Neural Network Inference

[HPCA'21] Cheetah- Optimizing and Accelerating Homomorphic Encryption for Private Inference

[MICRO'21] F1: A Fast and Programmable Accelerator for Fully Homomorphic Encryption

[ISCA'22] CraterLake: a hardware accelerator for efficient unbounded computation on encrypted data

[DAC'22] MATCHA: A Fast and Energy-Efficient Accelerator for Fully Homomorphic Encryption over the Torus

[FCCM'22] FPGA Accelerator for Homomorphic Encrypted Sparse Convolutional Neural Network Inference

[Micro'22] ARK: Fully Homomorphic Encryption Accelerator with Runtime Data Generation and Inter-Operation Key Reuse

[HPCA'23] Poseidon: Practical Homomorphic Encryption Accelerator

[HPCA'23] FAB: An FPGA-based Accelerator for Bootstrappable Fully Homomorphic Encryption

[HPCA'23] FxHENN: FPGA-based acceleration framework for homomorphic encrypted CNN inference