Overview

Conversions Between All Five Protocols

- change representation of shared values
- evaluation of hybrid circuits combining Boolean and arithmetic components
- t₀ direct (→), 6 as composition (→)
- based on protocols from ABY [DSZ15], ABYv2.0 [PSSY21], and MOTION, with improvements

Improvements to ABY [DSZ15] and ABYv2.0 [PSSY21]

- security parameter ν, bit length ℓ
- B → A: using shared bits
- Y → A: without online comm.

Neural Network Building Blocks

- Idea: exploit high-level structure of networks, and do not compile to circuits
- use generic protocols, but implement them in a optimized way
- do not change the networks’ architectures

Currently Supported Tensor Operations

- fixed-point arithmetic (using with [M2Y])
- fully-connected and convolutional layers (Δ·κ)
- ReLU (multiple variants V/2//0)
- MaxPool (using optimized circuits Y/2/7)
- AveragePool (Δ/κ)

Neural Network Benchmarks

Small Network: MiniONN MNIST [LJLA17]

Larger Network: MiniONN CIFAR-10 [LJLA17]

Comparing with Prior and Concurrent Work [IVC18; MLS20; RRK20]

Neural Network Structure

more batched operations reduces disadvantage of ABYv2.0 setup
- ABYv2.0 clearly better for ReLU

Extending the MOTION Framework → MOTION2NX

Extending and Improving the Framework

- implementation of the five generic 2PC protocols and conversions
- architectural improvements to increase flexibility and performance
- clearer interfaces, decoupled components
- new system for asynchronous communication
- executors allow for different execution strategies
- single instruction multiple data (SIMD) operations
- automatic collection of run-time statistics and metadata
- support for HyCC-generated [BDK+18] hybrid circuits

Support for Neural Networks

- secure tensor data types
- neural network building blocks
- parallelized tensor operations

ONNX support for interoperability with PyTorch, TensorFlow, etc.

Open Source under an MIT License

available on GitHub: https://github.com/encrypto.cs.tu-darmstadt.de/MOTION2NX

More Information

Extended Abstract


Acknowledgments

This work is supported by the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation program under grant agreements No. 870490 (ABY) and No. 952619 (MOTION), and the German Federal Ministry of Education and Research (BMBF) under the project Open Neural Network Exchange (ONNX) and the project MOTION. MOTION is supported by the Max Planck Funding Program (MPFund) and by the Bavarian Federal Ministry of Science and Research and the Helmholtz-Deutsche Forschungsgemeinschaft. The work of Lennart Braun was supported by the “Perry van Oevelen” scholarship.

References


