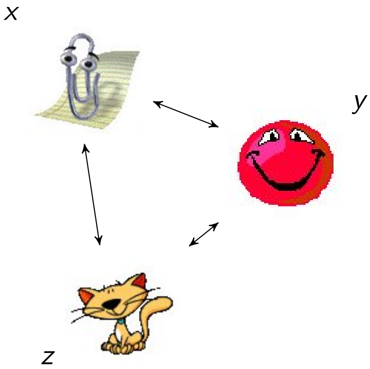
Secure Quantized Training for Deep Learning

Marcel Keller Ke Sun

CSIRO's Data61

27 June 2022

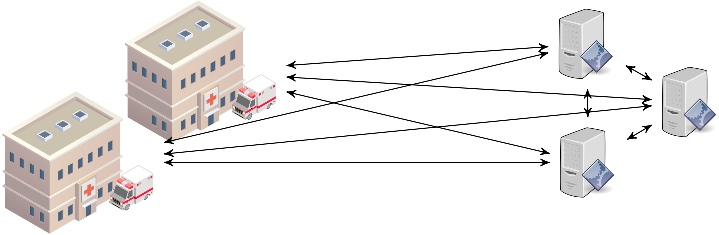
Secure Multiparty Computation



Wanted: $f(x, y, z)$

- Computation on secret inputs
- Replace trusted third party

Privacy-Preserving Machine Learning



Outsourced training

- Data owners share their inputs among computing parties
- Computing parties train a model securely using MPC
- Output model OR use it for secure inference
- Model inference attacks etc. not addressed

Quantization

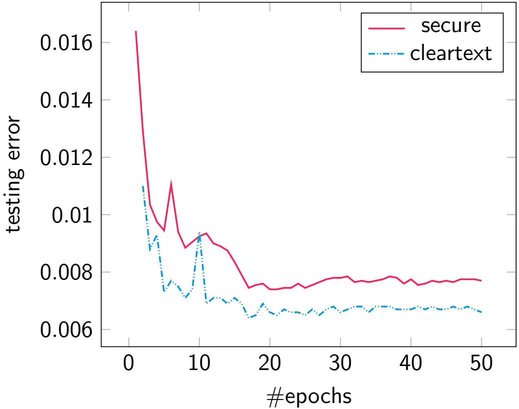
Issue

Floating-point computation is expensive in MPC

Solution

Represent x as $\lfloor x \cdot 2^f \rceil$ to use integer computation for fractional numbers

Results for LeNet on MNIST



- AMSgrad optimizer
- Co-located AWS c5.9xlarge
- 1/3 corruption (semi-honest)
- Time per epoch: 9 minutes
- 1 hour for 99% accuracy

Comparison with CrypTen

CrypTen

- Adds MPC functionality to PyTorch
- Less accurate approximations of non-linear functions
  $\Rightarrow$ More divergence

	Method	Accuracy (4 epochs)	Time per epoch (s)
CrypTen	SGD, lr 0.01	96.73%	10,940
Ours	SGD, lr 0.01	98.64%	343
Ours	AMSgrad, lr 0.001	98.97%	512

Links

https://github.com/data61/MP-SPDZ

https://github.com/csiro-mlai/mnist-mpc

https://arxiv.org/abs/2107.00501