Private Emotion Recognition with Secure Multiparty Computation

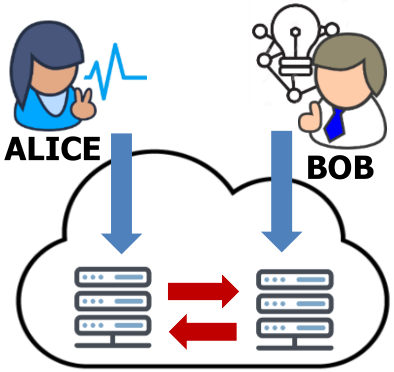
Kyle Bittner[1], Martine De Cock[1,2], Rafael Dowsley[3]

[1]University of Washington, [2]Ghent University, [3]Monash University

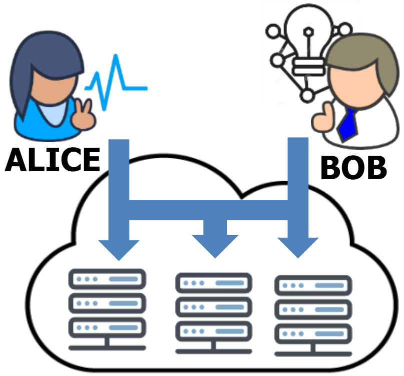
WHAT: private speech classification

- To label Alice's speech signal with Bob's classifier
- without Alice disclosing her speech signal
- without Bob disclosing his model parameters

HOW: secure multiparty computation (MPC)



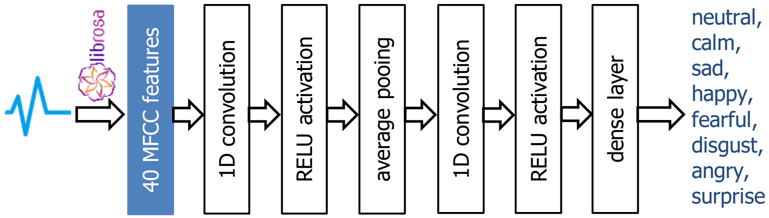
2PC
dishonest majority



3PC
honest majority

Training Bob's classifier

- RAVDESS data: 2,542 audio files, ~3.5 sec each
- 1D convolutional neural network (CNN)



librosa

40 MFCC features

1D convolution

RELU activation

average pooing

1D convolution

RELU activation

dense layer

neutral, calm, sad, happy, fearful, disgust, angry, surprise

- Post-training integer quantization
- 81.2% accuracy

TensorFlowLite

Secure inference runtime results

		2PC	3PC
Low-end F32s VMs	Passive	40.5 sec	2.06 sec
	Active	370 sec	12.72 sec
High-end F72s VMs	Passive	4.17 sec	0.26 sec
	Active	33.30 sec	1.61 sec

data61 / MP-SPDZ

Microsoft Azure