RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: CRYP-F01

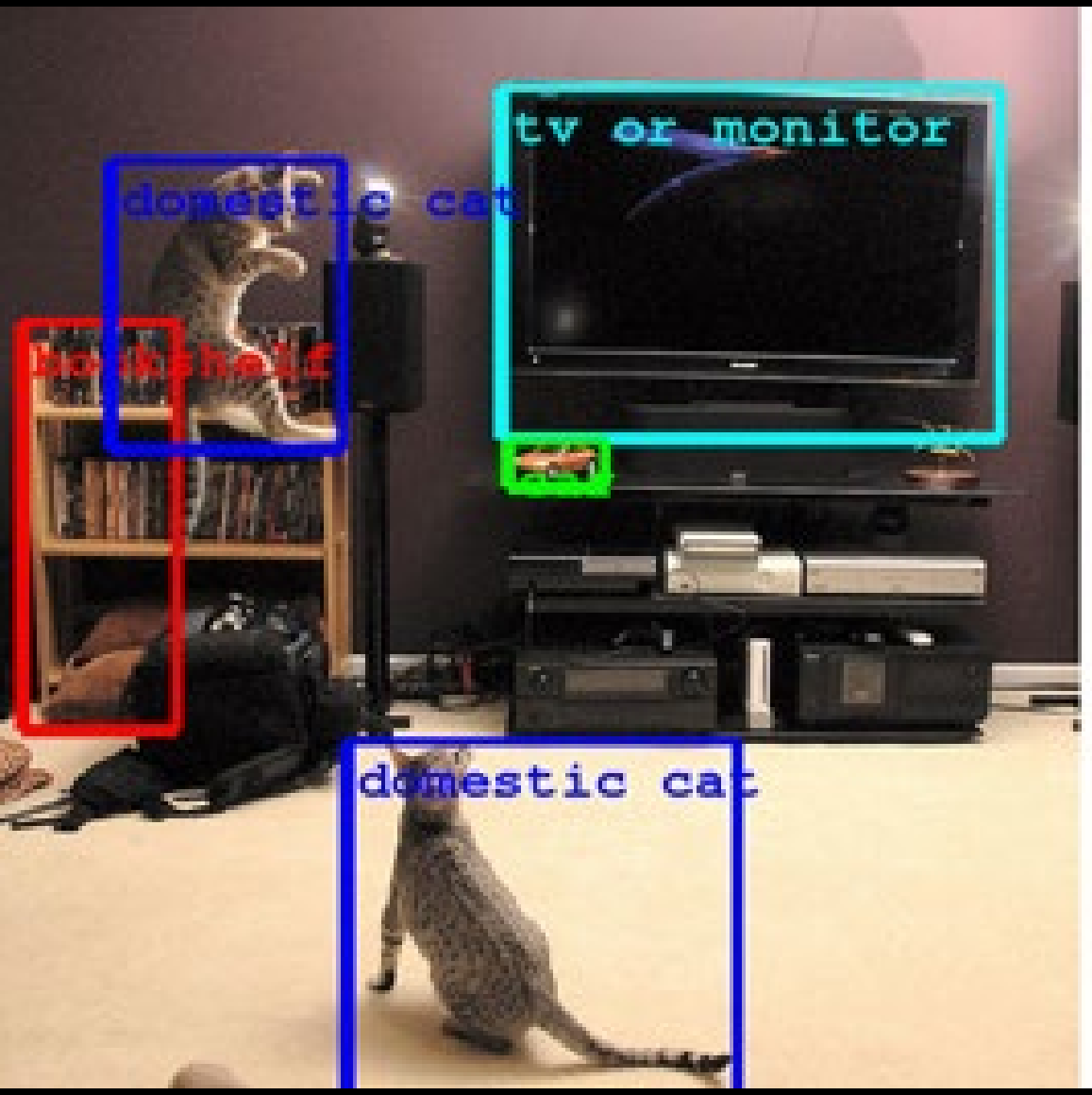
Multiparty Computation and Application

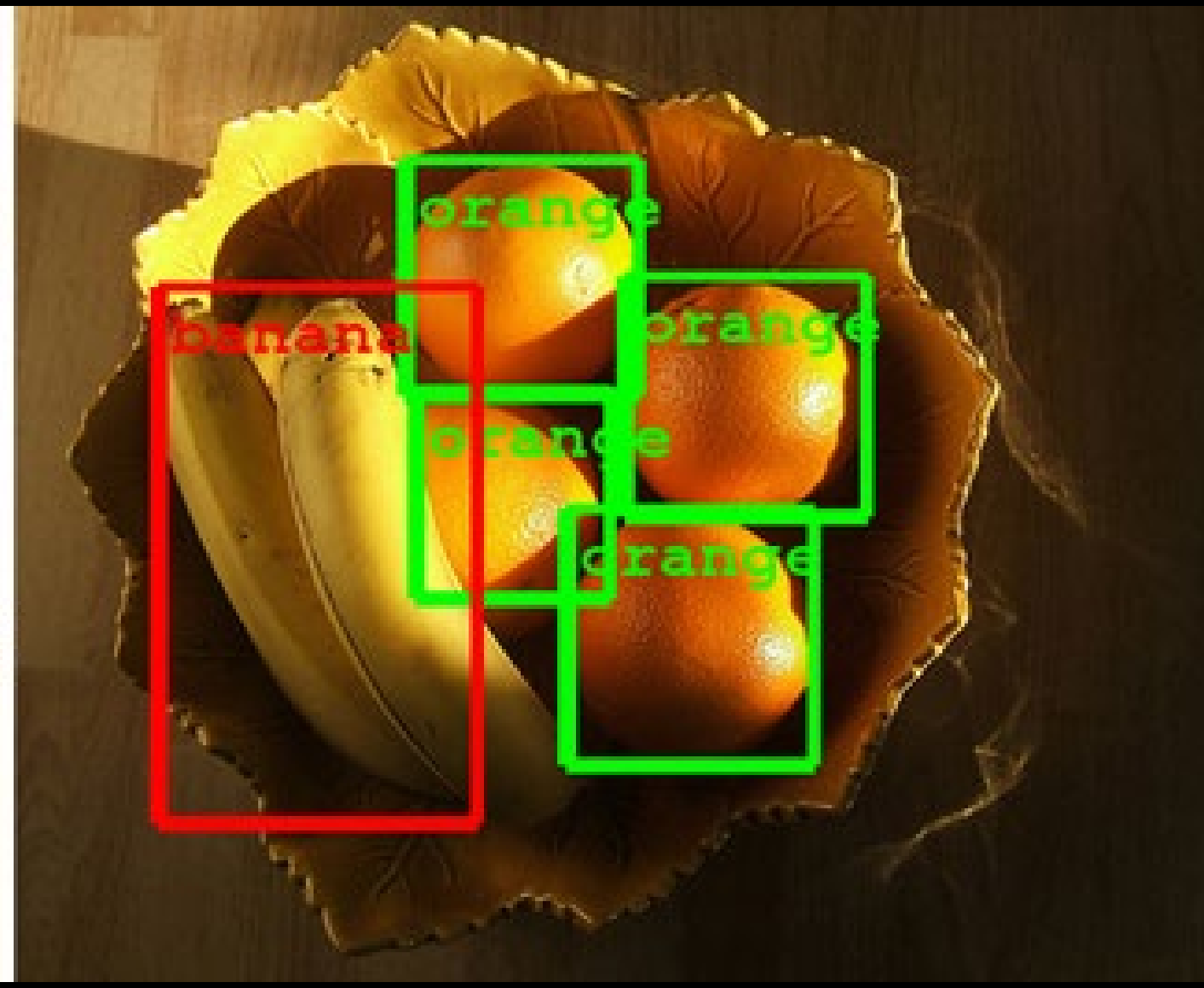
Eleftheria Makri
Lecturer/Researcher
Imec-COSIC, KU Leuven, BE &
Saxion University of Applied Sciences, NL
@MakriEleftheria

RSAConference2019

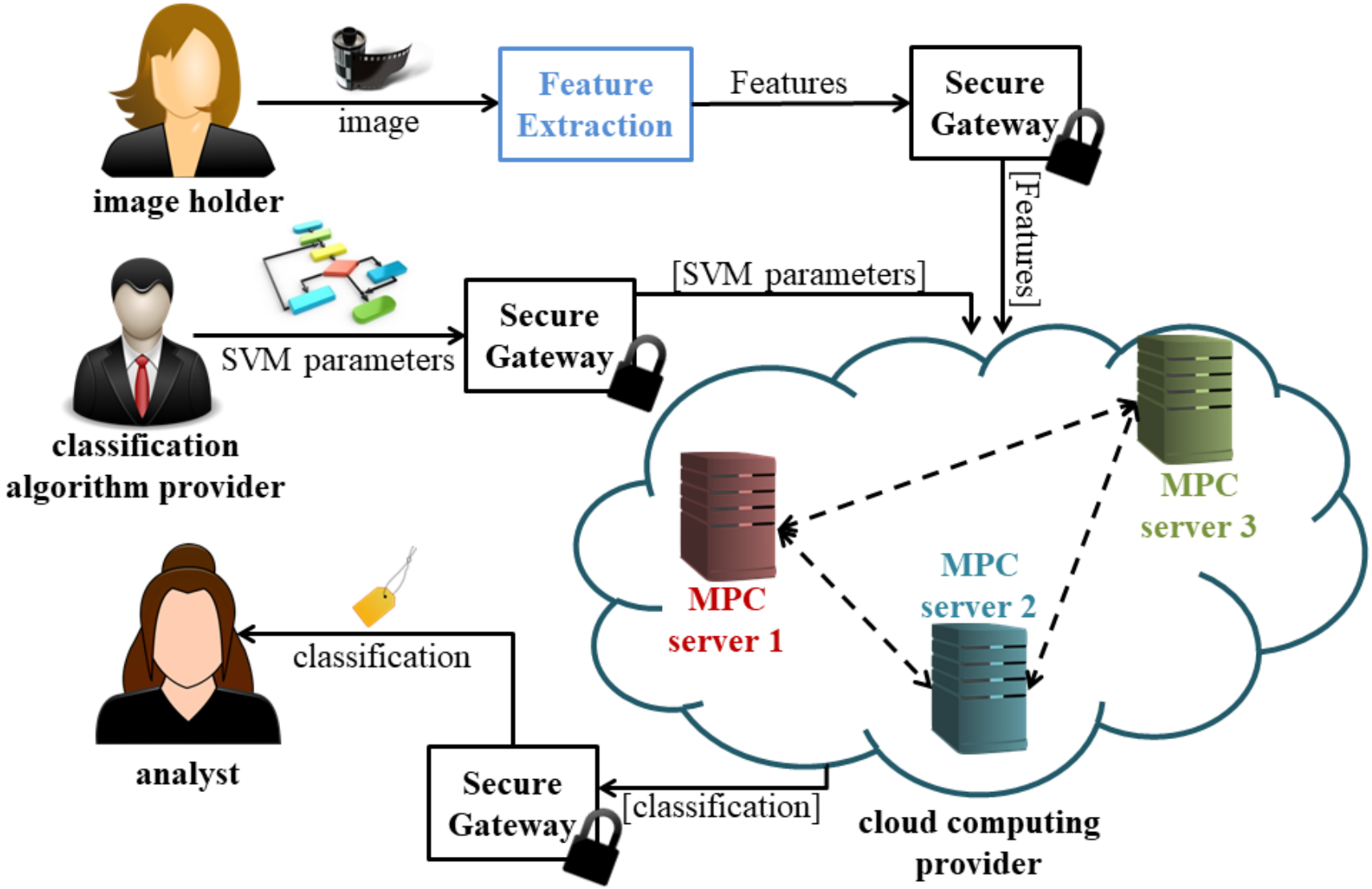
EPIC: Efficient Private Image Classification (or: Learning from the Masters)

E. Makri, *D. Rotaru, N. P. Smart, F. Vercauteren*


tv or monitor
domestic cat
domestic cat


orange
banana
orange
orange
orange

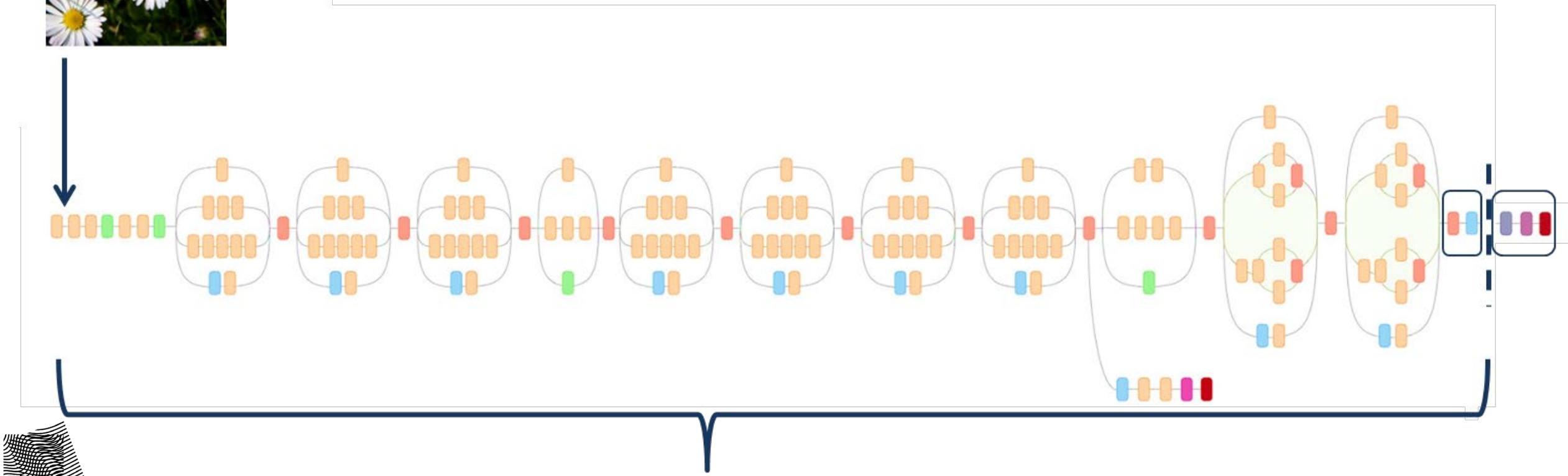
EPIC: Efficient Private Image Classification

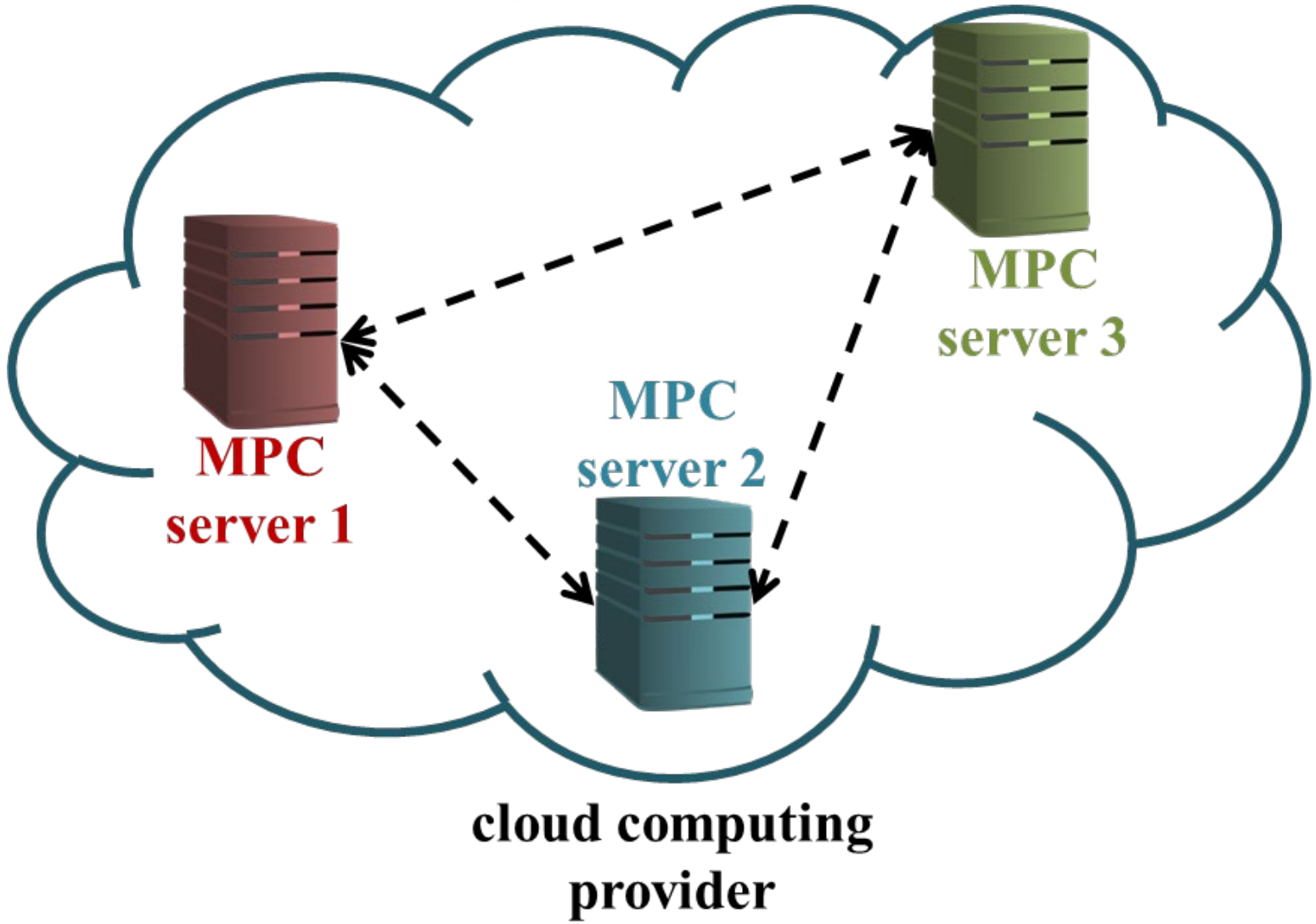



Feature
Extraction

Transfer Learning Feature Extraction (or: Learning from the Masters)

Plaintext (non-sensitive) images




MPC
server 1
MPC
server 2
MPC
server 3
cloud computing
provider

EPIC Security

Active Security **vs.** **Passive Security**

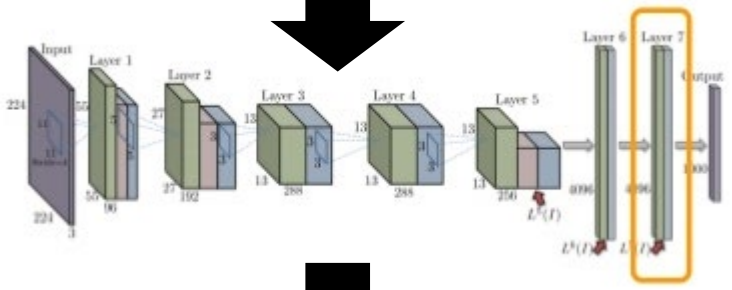
EPIC

All other protocols in the related work

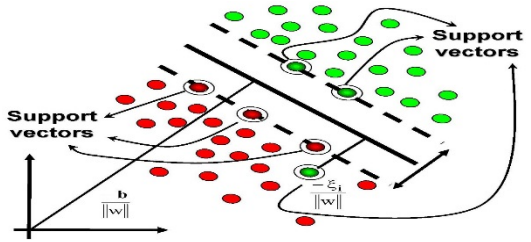
Step 1: Create the ML model

Alice

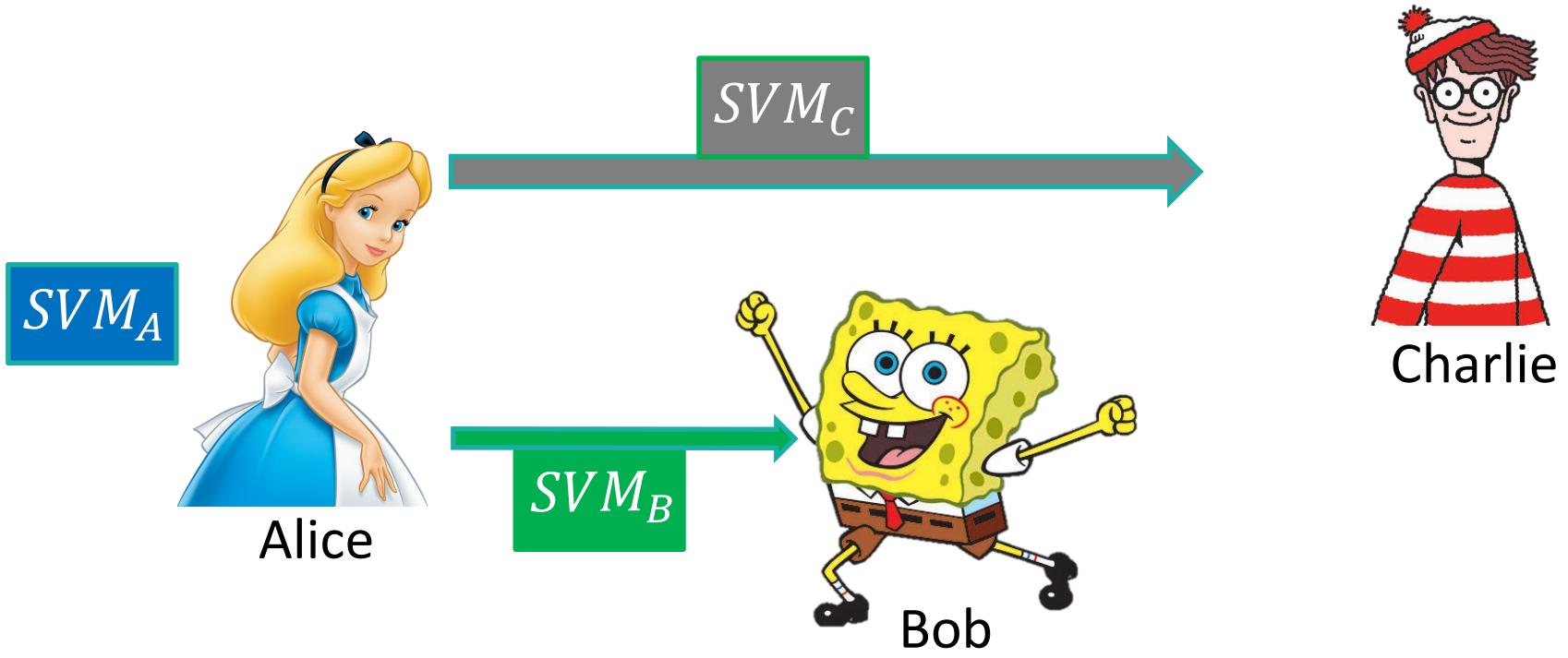
Inception–v3 CNN



Linear SVM



Step 2: Alice secret shares the ML model



Step 2: Alice secret shares the ML model

SVM_A

Alice

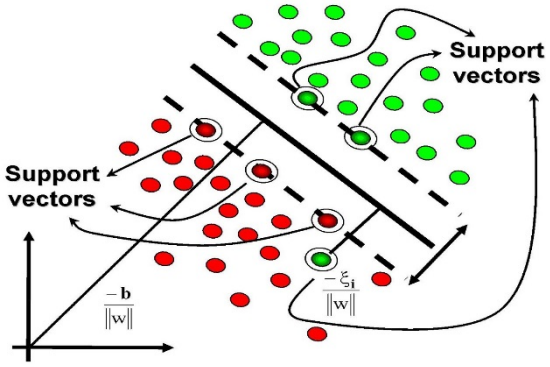
SVM_B

Bob

SVM_C

Charlie

$$SVM_A + SVM_B + SVM_C =$$

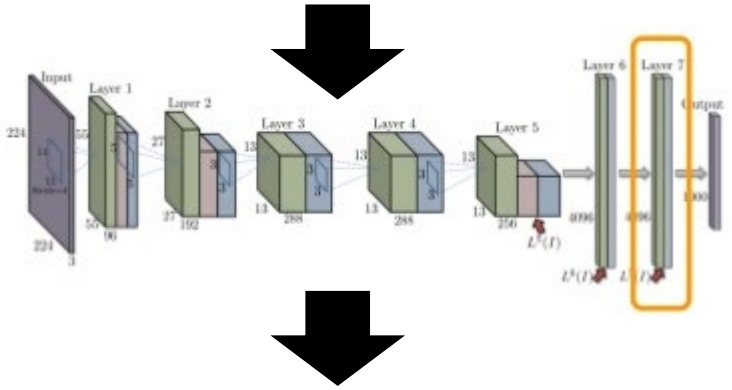


COSIC

Step 3: Bob extracts features

Bob

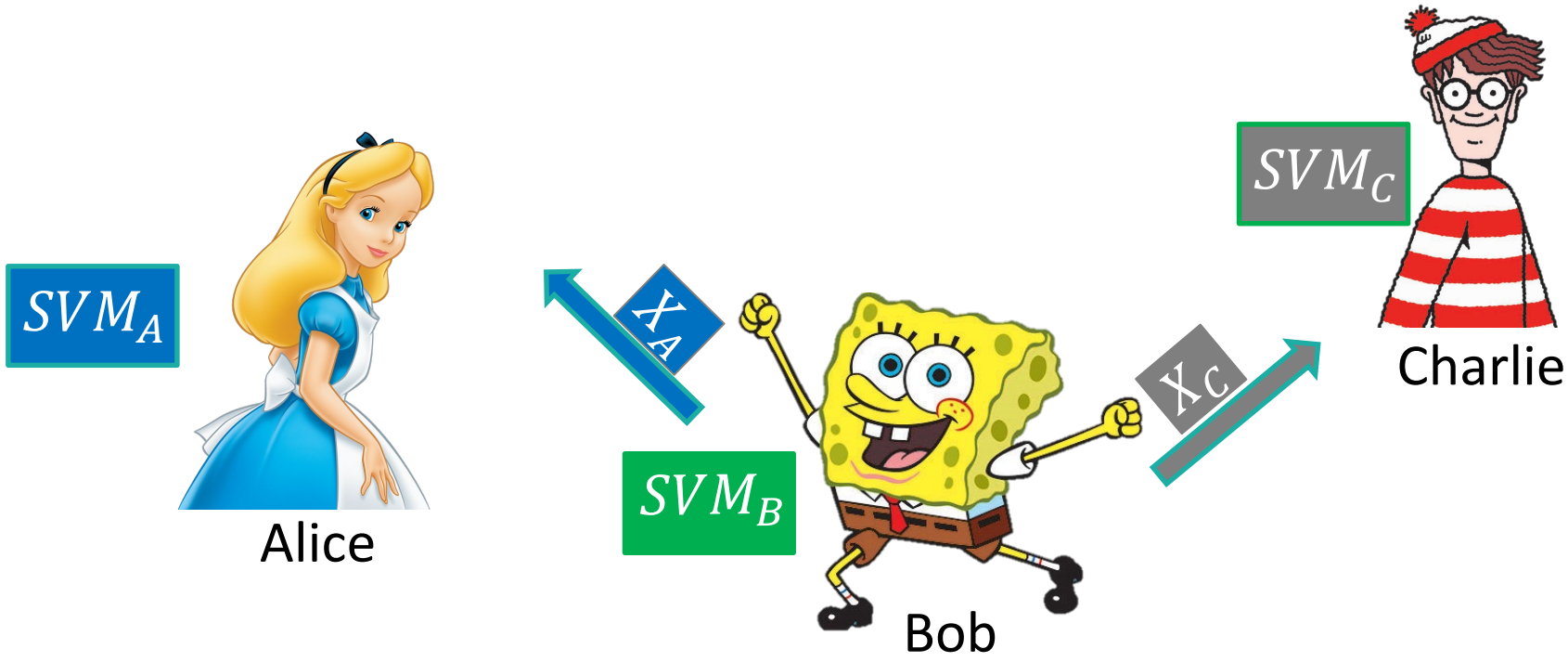
Inception–v3
CNN



Features

X

Step 4: Bob secret shares features



Step 4: Bob secret shares features

SVM_A

X_A

Alice

SVM_B

X_B

Bob

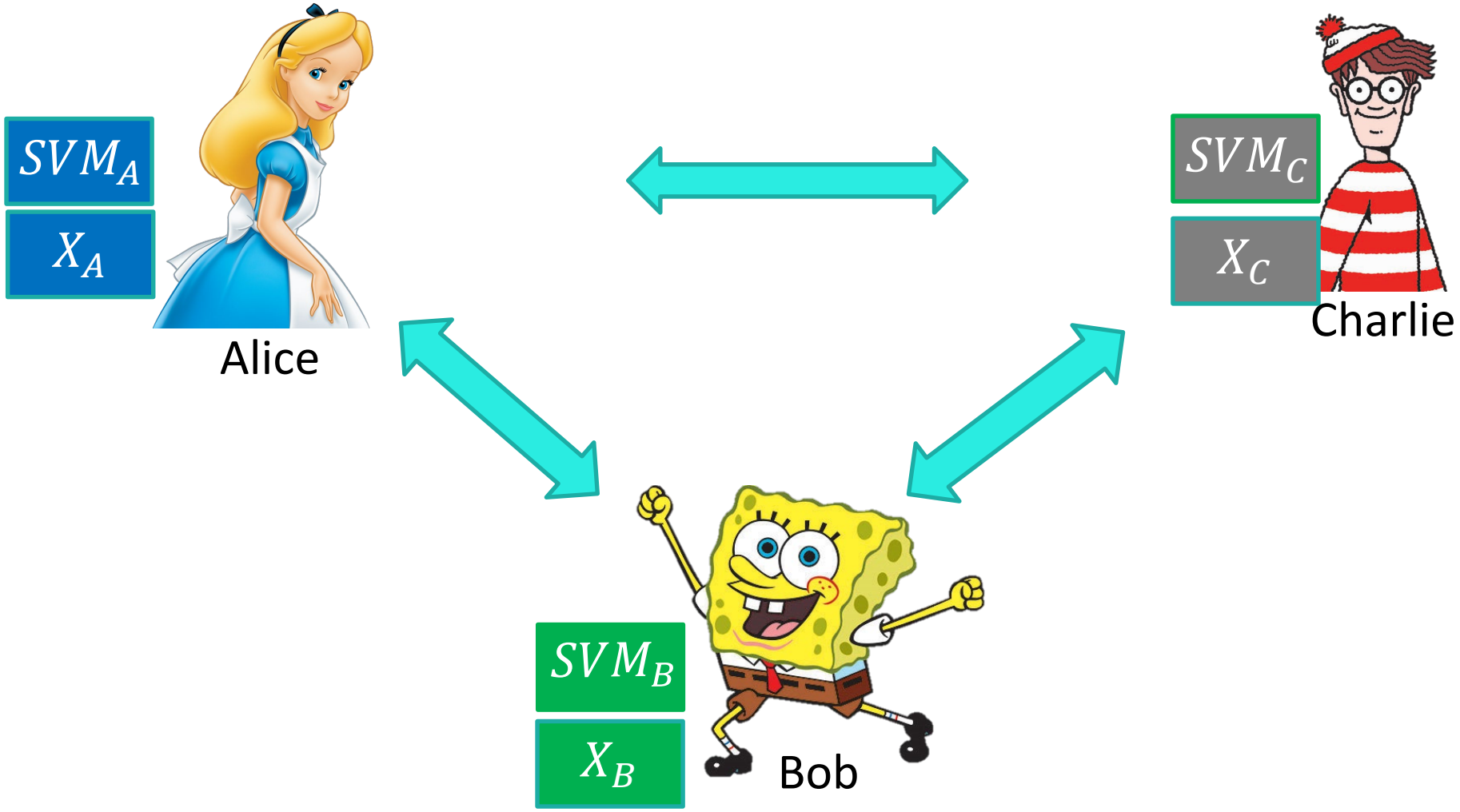
SVM_C

X_C

Charlie

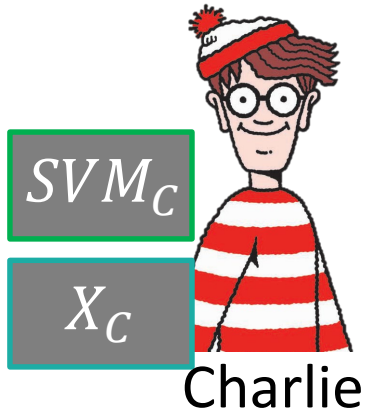
$X_A + X_B + X_C =$ CNN-Feat()

Step 5: Parties use MPC to help Charlie compute label of SVM-Alice(Bob-Image)



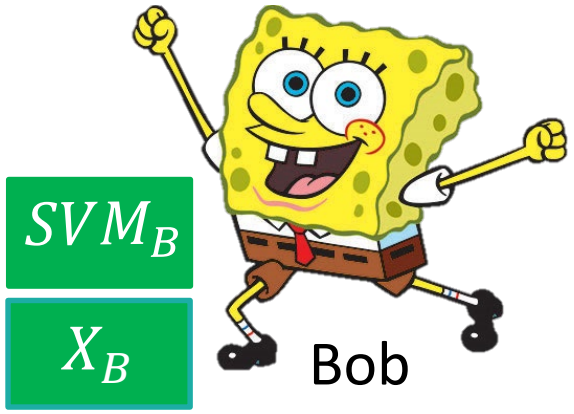
Step 5: Parties use MPC to help Charlie compute label of SVM-Alice(Bob-Image)

Alice



Charlie

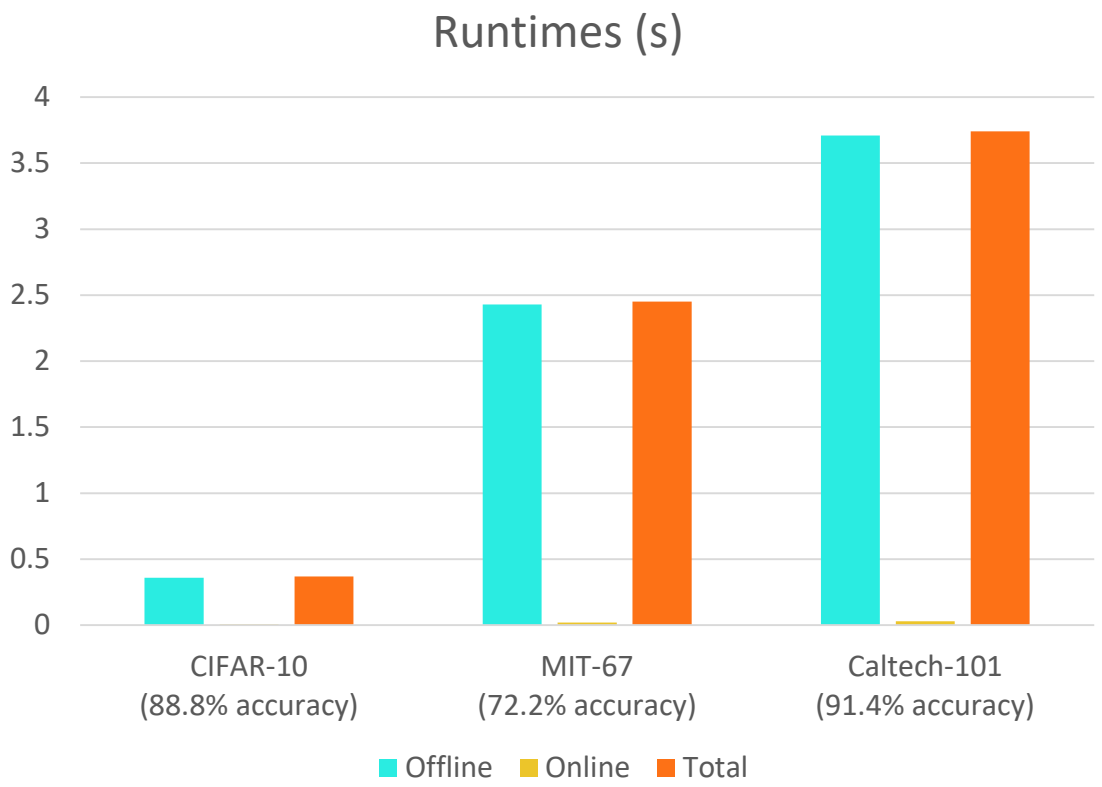
"Florist"



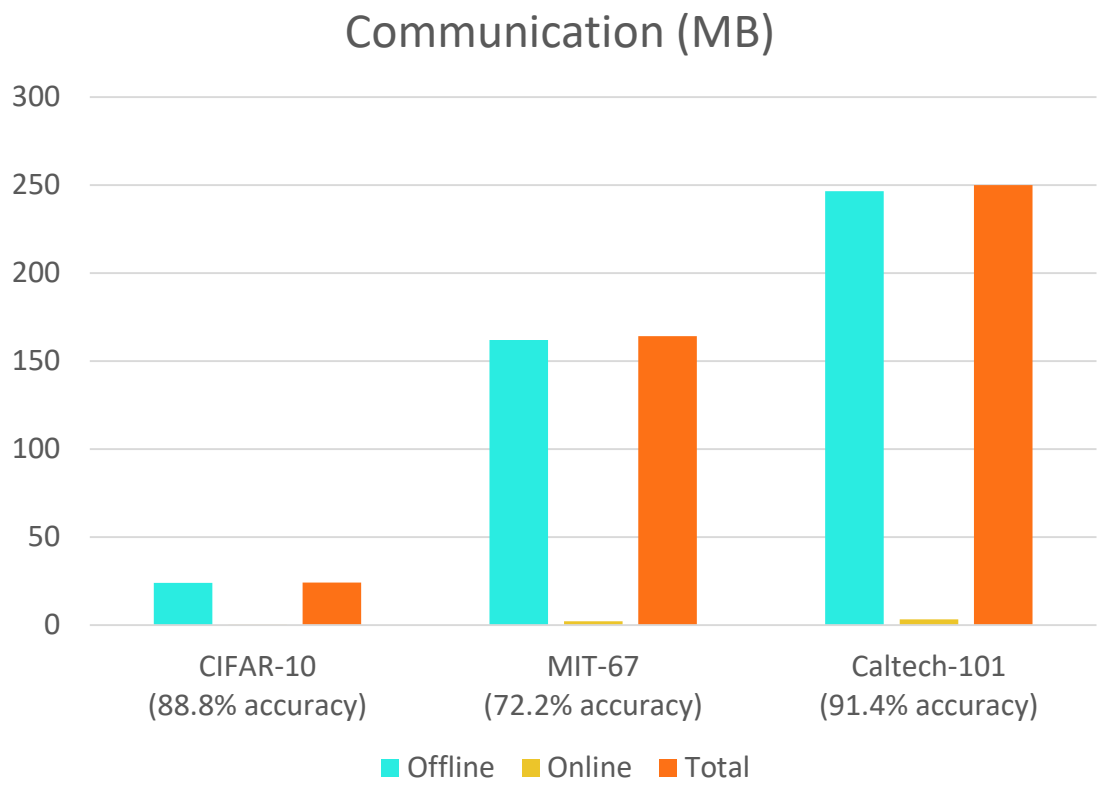
Bob

EPIC Performance – Simple Variant

Computation Cost



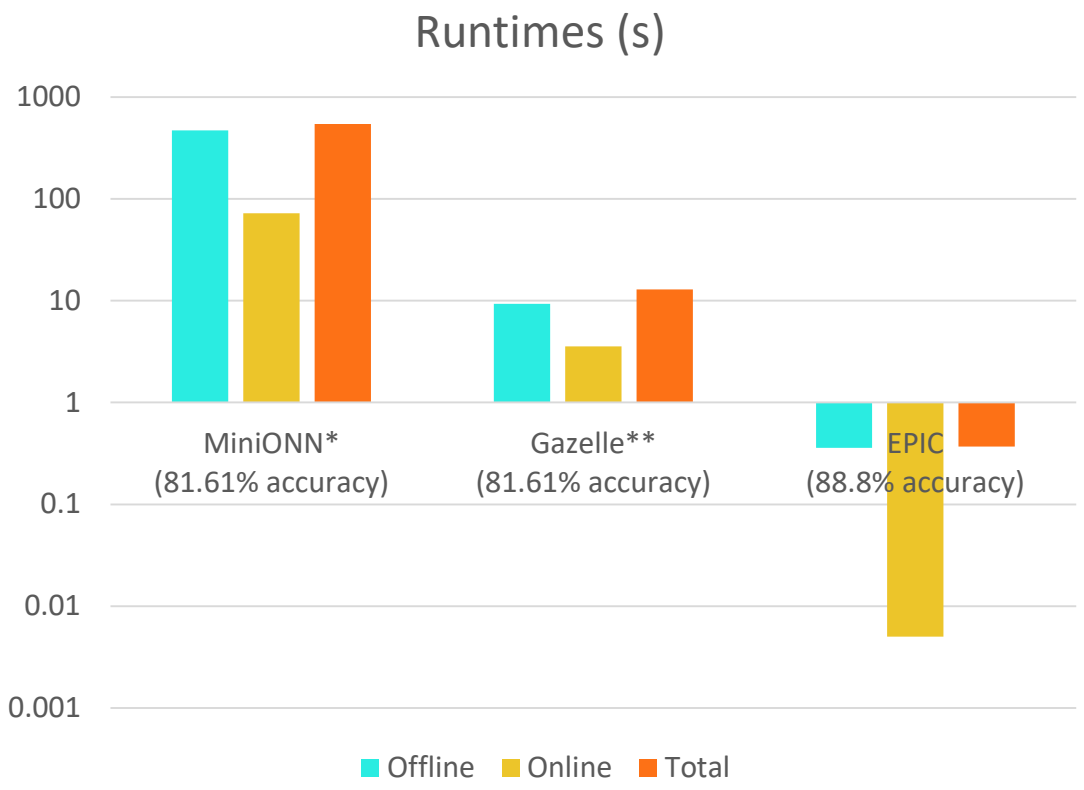
Communication Cost



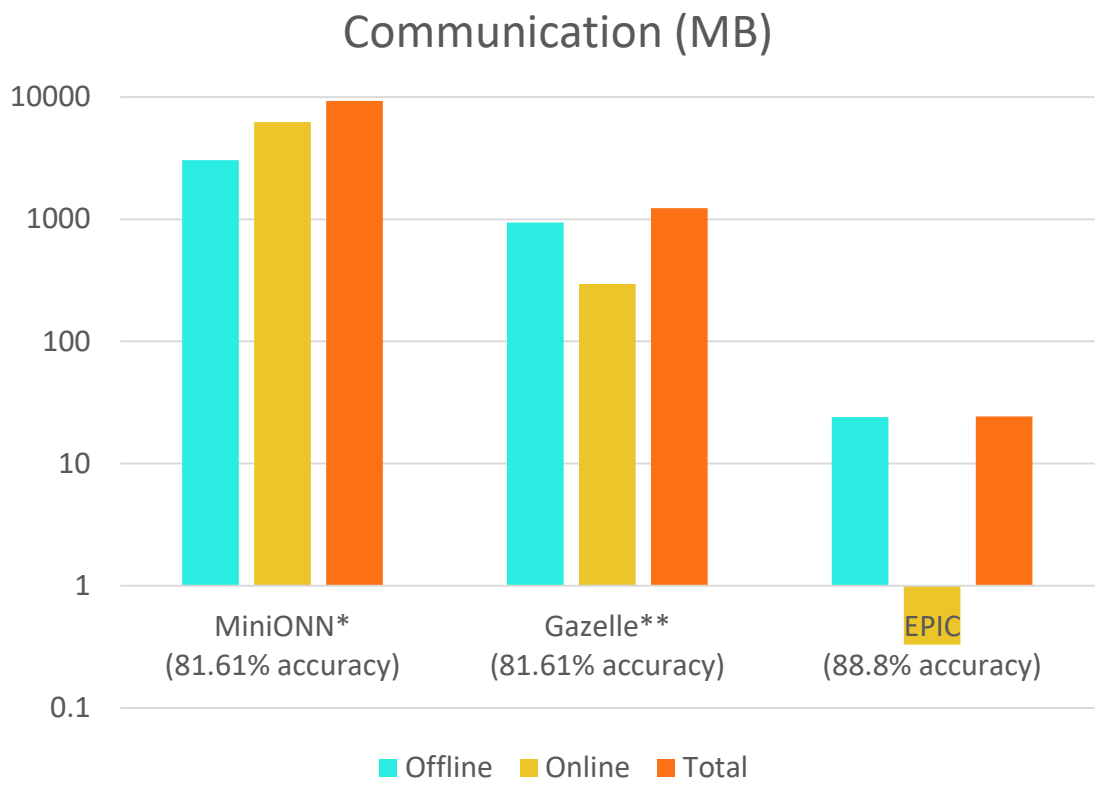
COSIC

Performance of the state-of-the-art private image classification

Computation Cost



Communication Cost



* Jian Liu, Mika Juuti, Yao Lu, N. Asokan. **Oblivious Neural Network Predictions via MiniONN Transformations**. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 619-631). ACM.*
** Chiraag Juvekar, Vinod Vaikuntanathan, and Anantha Chandrakasan. **GAZELLE: A low latency framework for secure neural network inference**. *In 27th USENIX Security Symposium (USENIX Security '18), Baltimore, MD, 2018. USENIX Association*.

COSIC

EPIC Efficiency Gain over the state-of-the-art

- EPIC vs. Gazelle[1] on CIFAR-10:
  - 34 times faster runtime;
  - 50 times improvement of communication cost;
  - 7% higher classification accuracy.

- EPIC vs. Gazelle[1] with the same accuracy:
  - 700 times faster runtime;
  - 500 times improvement of communication cost.

1 Chiraag Juvekar, Vinod Vaikuntanathan, and Anantha Chandrakasan. **GAZELLE: A low latency framework for secure neural network inference**. *In 27th USENIX Security Symposium (USENIX Security '18), Baltimore, MD, 2018. USENIX Association*.

Now what?

- What would transform EPIC to a LEGENDARY solution?
  - Maintain security
  - Maintain or increase efficiency
  - **Increase accuracy!**
- Any ideas on how to do this (using MPC)?
  - Talk to me during the break, or
  - Contact me offline at: eleftheria.makri@esat.kuleuven.be

THAT WAS

EPIC!