RSA Conference 2019
San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: CRYP-W10

Cryptography and AI

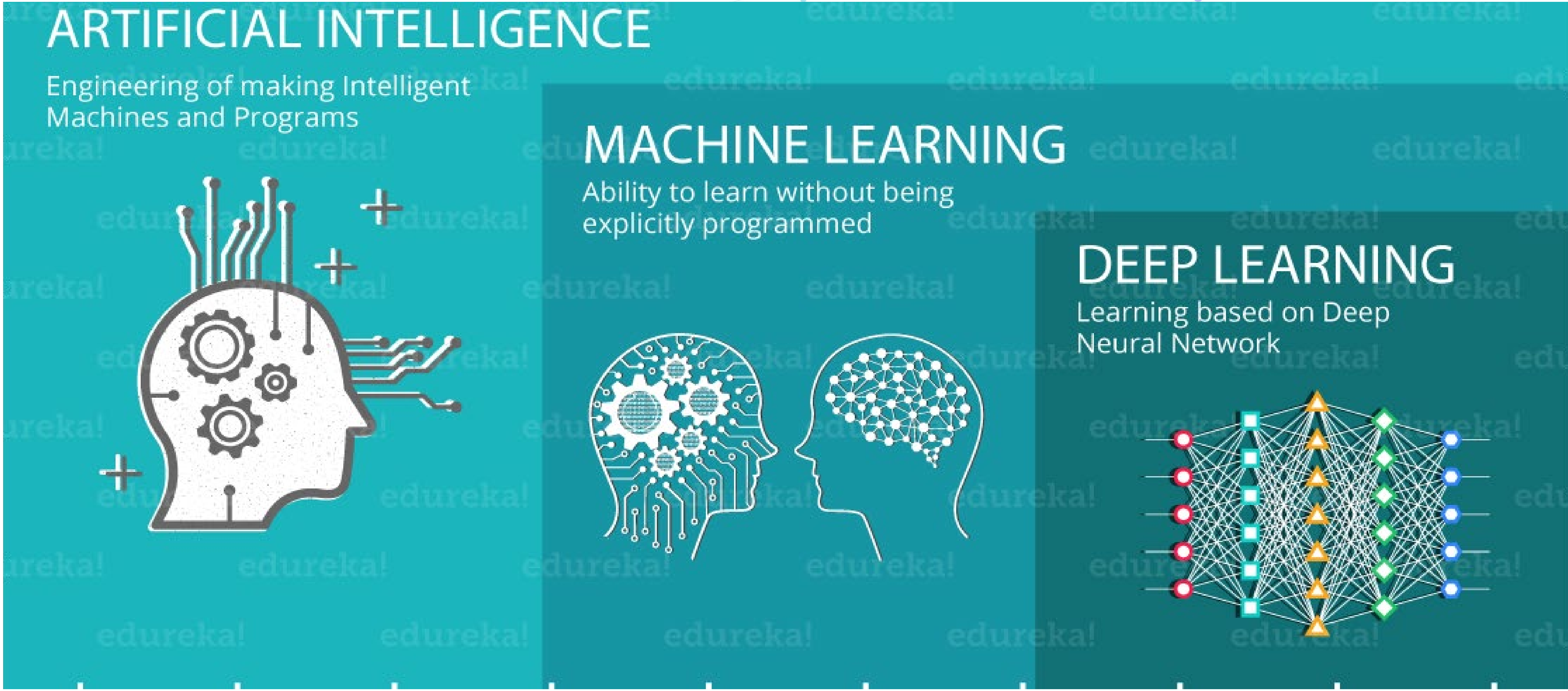
MODERATOR: **Bart Preneel**
Professor, COSIC KU Leuven
Bart.Preneel@esat.kuleuven.be, @cosic.be

PANELISTS:

Dan Boneh
Professor
Stanford University

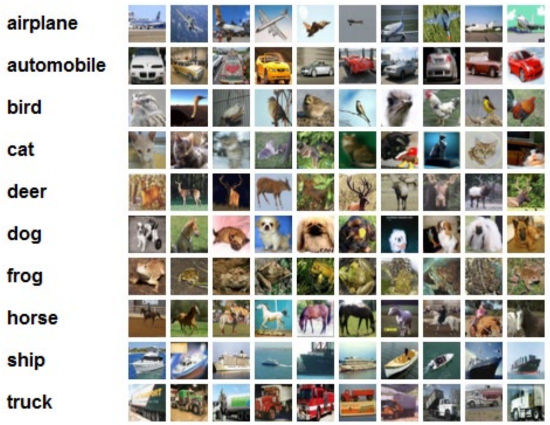
Maria Raykova
Research Scientist
Google

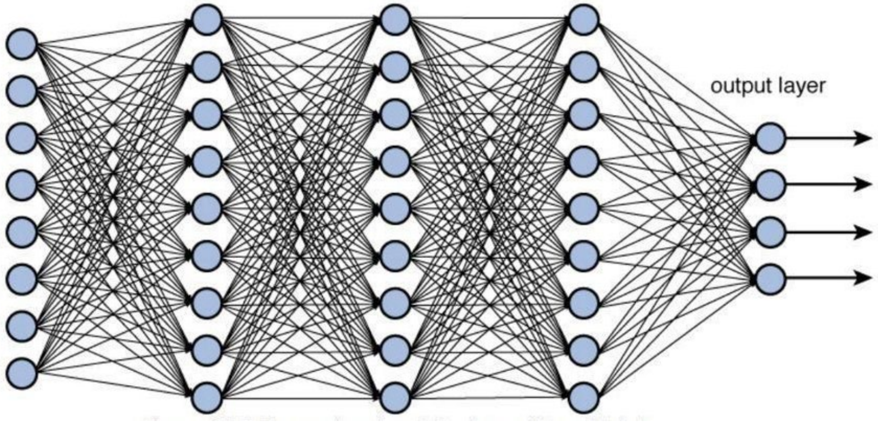
Nigel Smart
Professor
COSIC KU Leuven
@SmartCryptology


ARTIFICIAL INTELLIGENCE
Engineering of making Intelligent Machines and Programs
MACHINE LEARNING
Ability to learn without being explicitly programmed
DEEP LEARNING
Learning based on Deep Neural Network

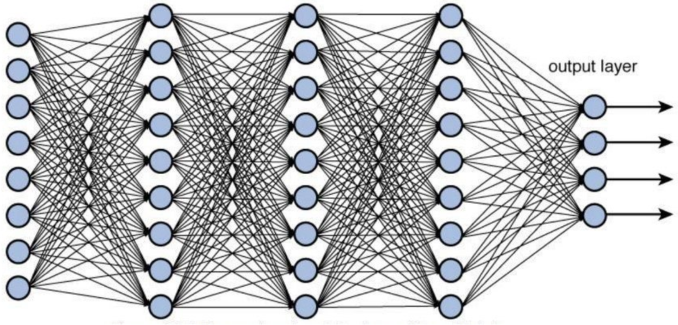
Machine Learning

Training





Evaluation



airplane

What could you protect?

- The individual data used to train the model
- The model itself
- The input data to evaluation
- The output of evaluation

- Different parties want to protect different things!

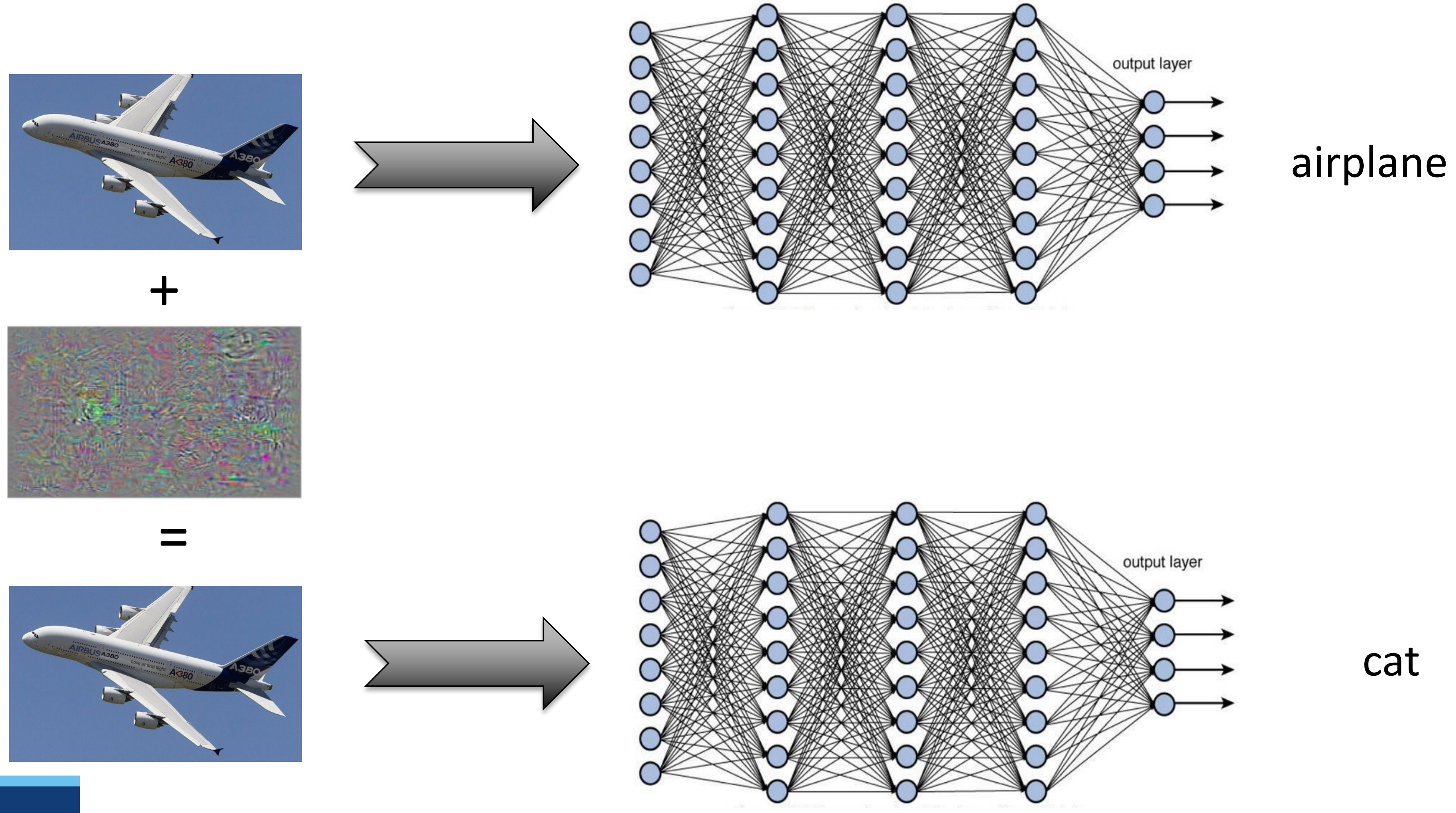
Secure Computation

- Multi Party Computation
  - A set of parties perform the computation together via a protocol
  - Relatively efficient for some functions
- Homomorphic Encryption
  - One party computes a function on data of another set of parties
  - Decryption by the party who gets output
- Differential Privacy
  - Adds randomness to the output to protect individual training samples
  - Can either add randomness to the trained model and/or the output of the evaluation

Secure Machine Learning

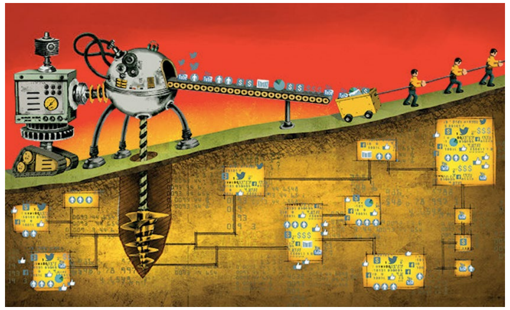
- Are you securing training or evaluation phase?
- Who gets output?
- Programming is hard
  - Branching for example is very difficult
  - Try writing programs which do few “if-then-else” statements!
- Accuracy will drop from processing clear data
- What about adversarial input to training phase
  - Adversarial learning

Adversarial machine learning



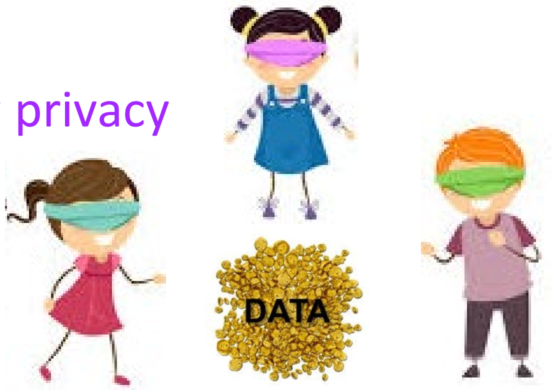
Benefits

- Data as a valuable resource
  - Why? - analyze and gain insight
    - Extract essential information
    - Build predictive models
    - Better understanding and targeting
  - **Value often comes from putting together different private data sets**



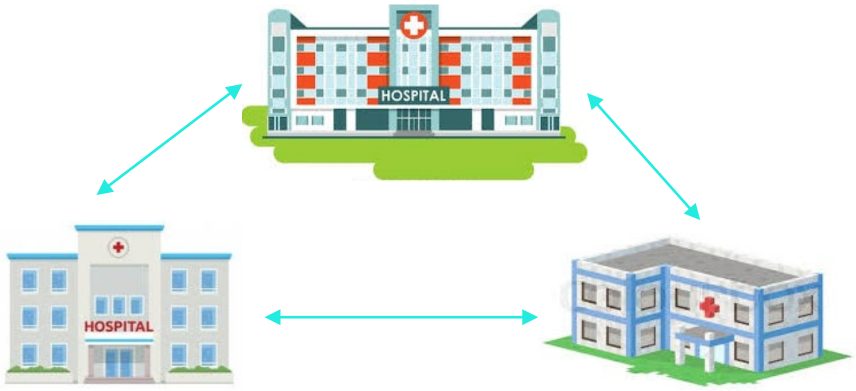
- Data use challenges
  - Liability - security breaches, rogue employees, subpoenas
  - Restricted sharing - policies and regulations protecting private data
  - Source of discrimination – unfair algorithms

- **Privacy preserving computation** – promise to obtain utility without sacrificing privacy
  - Reduce liability
  - Enable new services and analysis
  - Better user protection



Two Scenarios

Few Input Parties



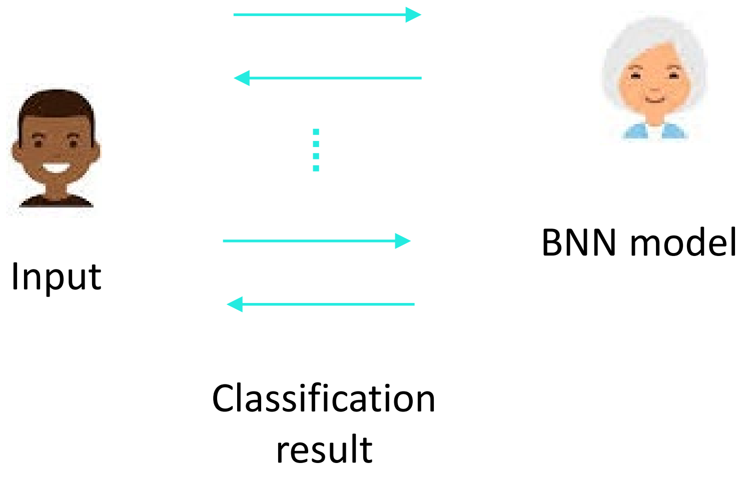
- Equal computational power
- Connected parties
- Availability

Federated Learning

- Weak devices
- Star communication
- Devices may drop out

Secure Neural Networks Evaluation Example

Compute binary neural network (BNN) prediction without revealing more about the model or the input



Two Party Passive Secure MPC Using Garbled Circuits
+ Conditional Oblivious Addition
+ Customized BNNs

- Evaluation: MNIST dataset – 60000 (28x28) images of digits

BNN Architecture	Runtime (s)	Communication (MB)	Accuracy
3FC layers + binary activation	0.13	4.27	97.6%
1-Conv and 3-FC layers + binary activation	0.16	38.28	98.64%
2-Conv, 2-MP and 3-FC layers + binary activation	0.15	32.13	99%

[RSCLLK19] XONN:XNOR-based Oblivious Deep Neural Network Inference, Riazi, Samragh, Chen, Laine, Lauter, Koushanfar, 2019

Also see talks on Friday at 08.30 for active MPC on CIFAR datasets

RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: CRYP-W10

Cryptography and AI

MODERATOR: **Bart Preneel**

Professor, COSIC KU Leuven

Bart.Preneel@esat.kuleuven.be, @cosic.be

PANELISTS:

Dan Boneh

Professor

Stanford University

Maria Raykova

Research Scientist

Google

Nigel Smart

Professor

COSIC KU Leuven

@SmartCryptology

#RSAC