UNIVERSITY
OF TWENTE.

Cybersecurity Research

Semantics, Cybersecurity & Services (SCS)

Florian Hahn (f.w.hahn@utwente.nl)

Cybersecurity research: Why?

Our society is today fully digitalized

- The amount of collected data and computational demands is ever-increasing

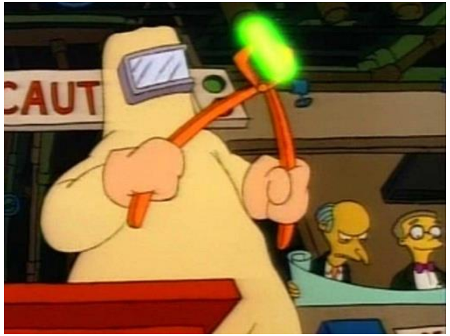
Cybersecurity research: Why?

Our society is today fully digitalized

- The amount of collected data and computational demands is ever-increasing

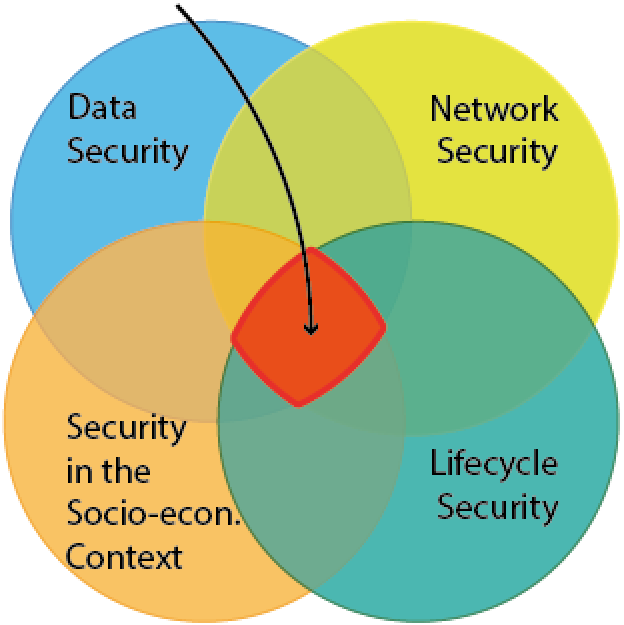
Vital digital systems are threatened by a plethora of cyber-attacks

- For instance, data exfiltration attacks & breaches exposing sensitive data
- On a daily basis, newspapers world-wide report cyber-attacks
- Cyber-attacks impact our digital society



Cybersecurity at Twente - TUCCR

UNIVERSITY OF TWENTE. | TUCCR Twente University Center for Cybersecurity Research



SCS’s research strategy

Our Data Security research strategy focuses on data from different angles

- Data Security

SCS’s research strategy

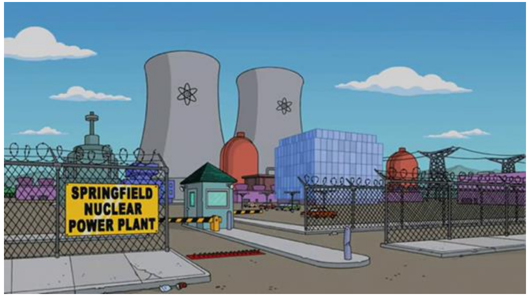
Our Data Security research strategy focuses on data from different angles

- Data Security
- AI Security

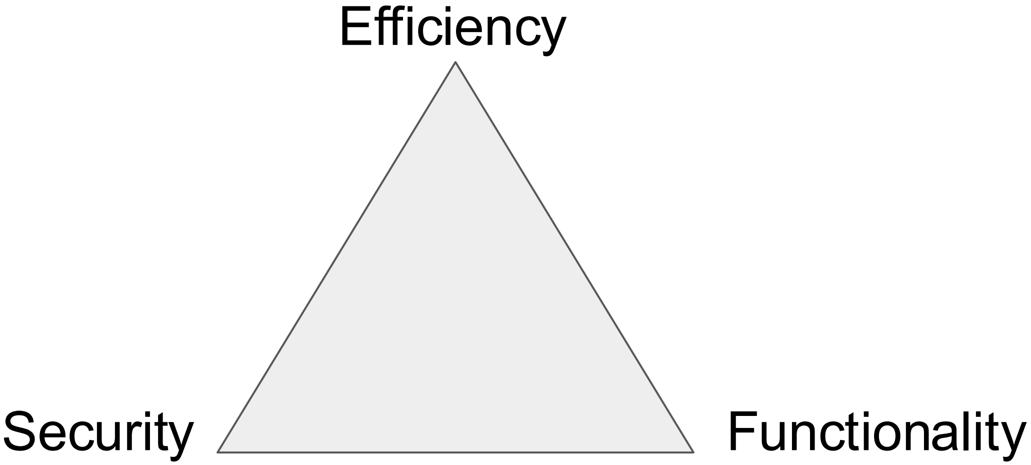
SCS's research strategy

Our Data Security research strategy focuses on data from different angles

- Data Security
- AI Security
- System Security



Trade-off challenge



Efficiency

Security

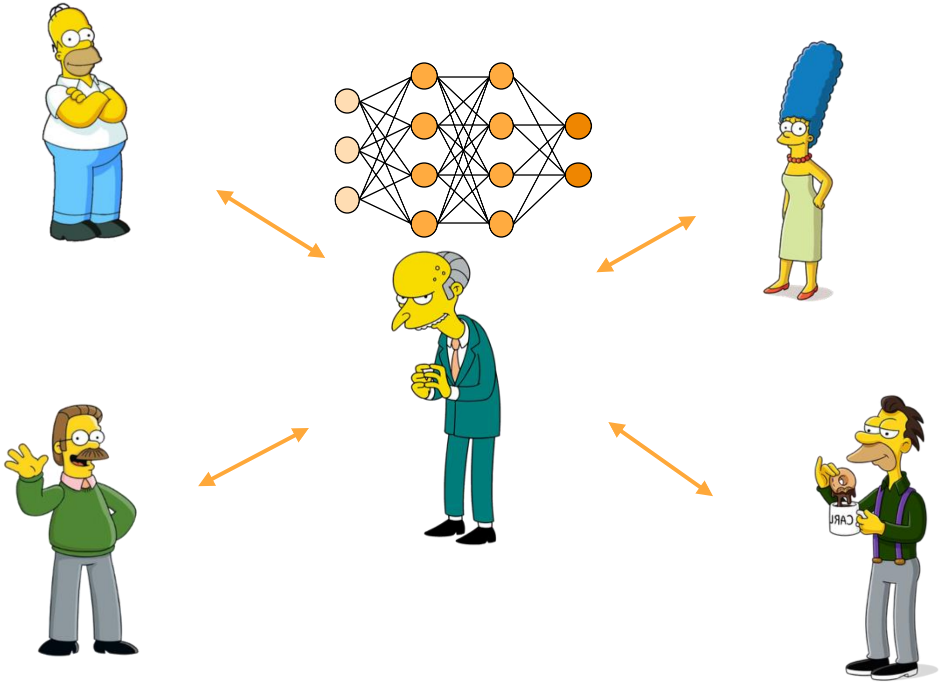
Functionality

Our functionality for today

Joint training of Neural Networks (AI!)

Status quo: trusted party

- Send data to trusted party
- Train model @ trusted party



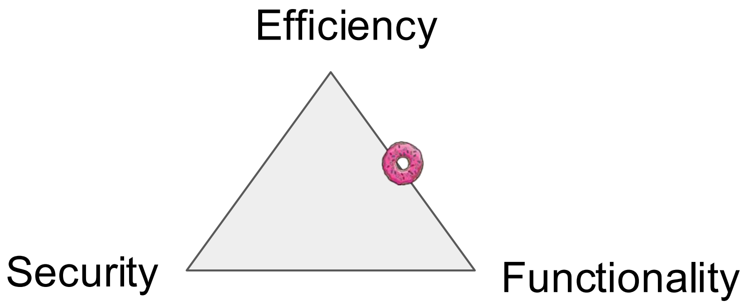
Our functionality for today

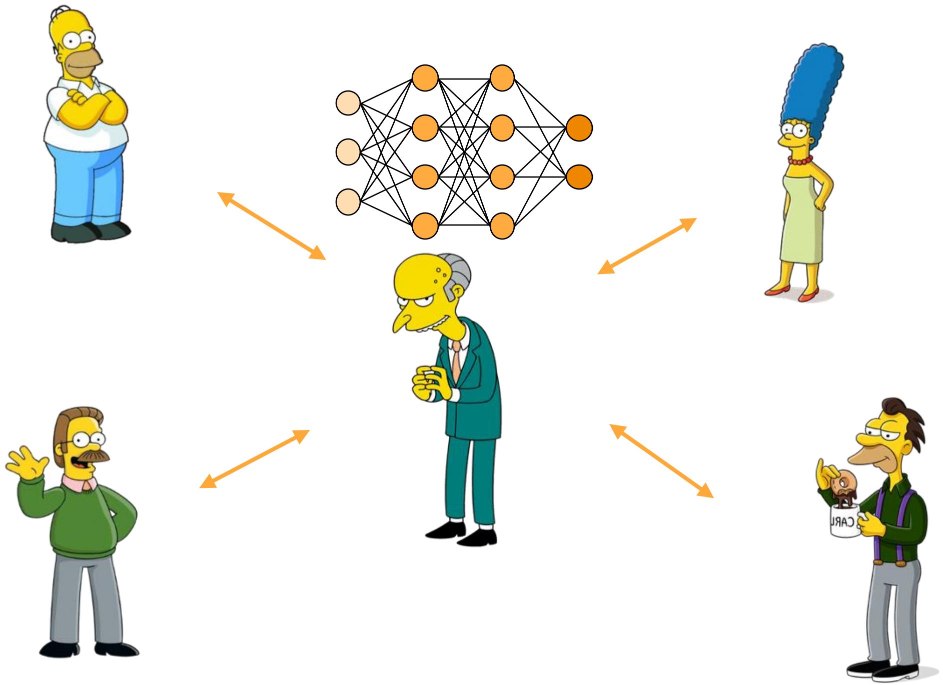
Joint training of Neural Networks (AI!)

Status quo: trusted party

- Send data to trusted party
- Train model @ trusted party

- *Send trained model back to data owners*





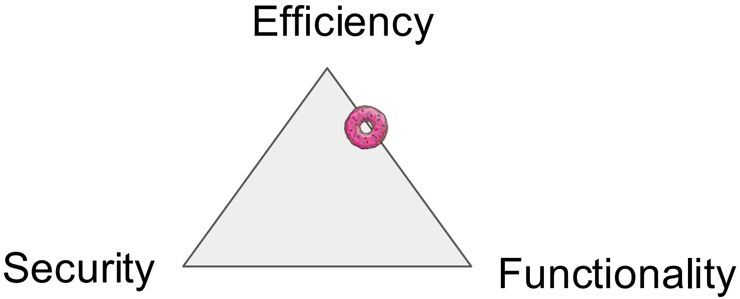
Our functionality for today

Joint training of Neural Networks (AI!)

Status quo: trusted party

- Send data to trusted party
- Train model @ trusted party

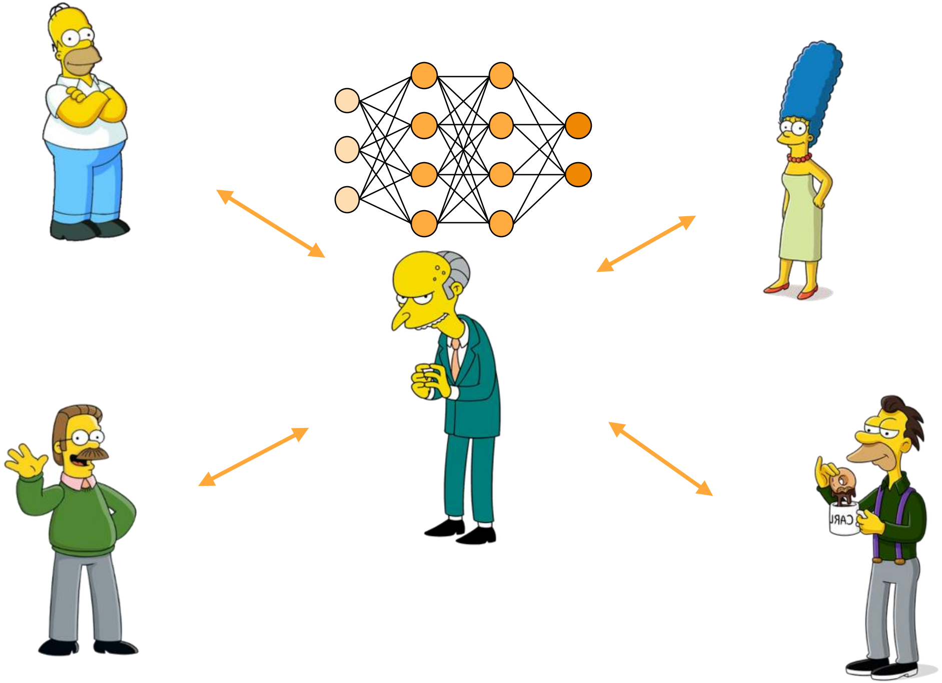
- *Data owners can query model with plaintext data*



Efficiency

Security

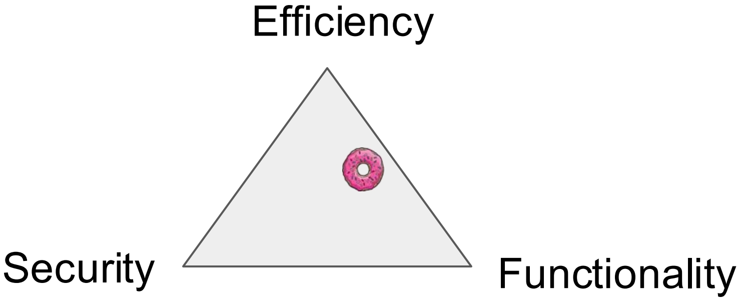
Functionality

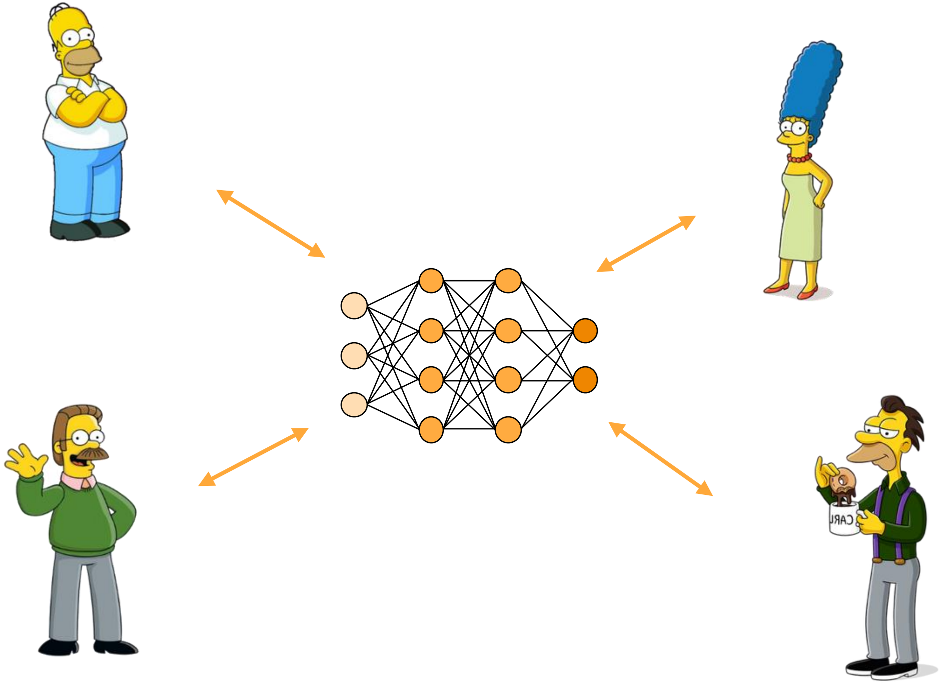


Federated Learning (FL)

Train a joint machine learning **model** over own local data

1. Train Locally
2. Aggregate
3. Map back and refine locally
4. Go to step 2 until accurate enough





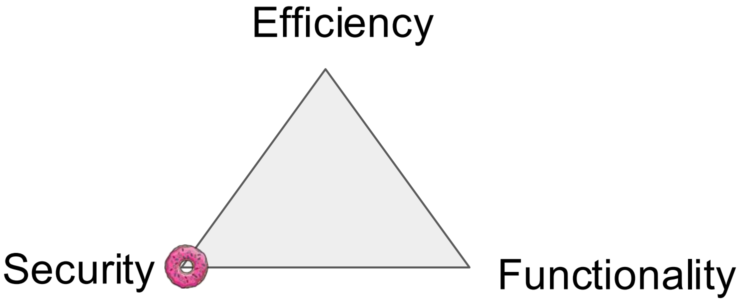
How to increase security?

Encryption of data

- With the secret key, one can encrypt plaintext data to a ciphertext

- Without the secret key, one cannot recover (sensitive) plaintext data

How to increase security?



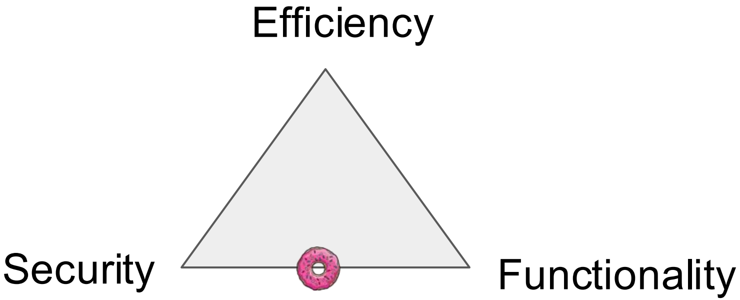
Asymmetric Encryption of data

- With the public key, one can encrypt plaintext data to ciphertexts
- With the secret key, one can recover plaintext data
  - Even with access to the public key, one cannot recover plaintext data

How to increase security?

Homomorphic encryption of data

- With the public key, one can encrypt plaintext data to ciphertexts
    - With the public key, one can compute with encrypted data (without learning plaintext data)
- With a secret key, one can recover plaintext data
    - Even with access to the public key, one cannot recover plaintext data

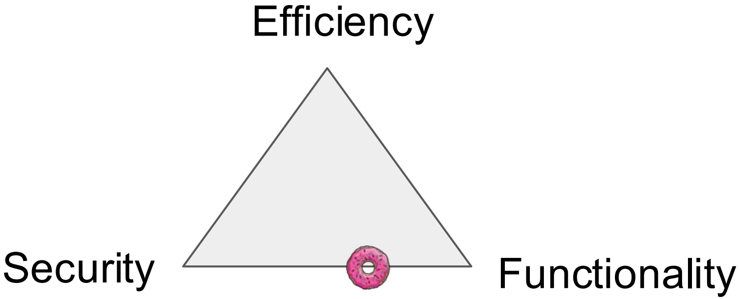


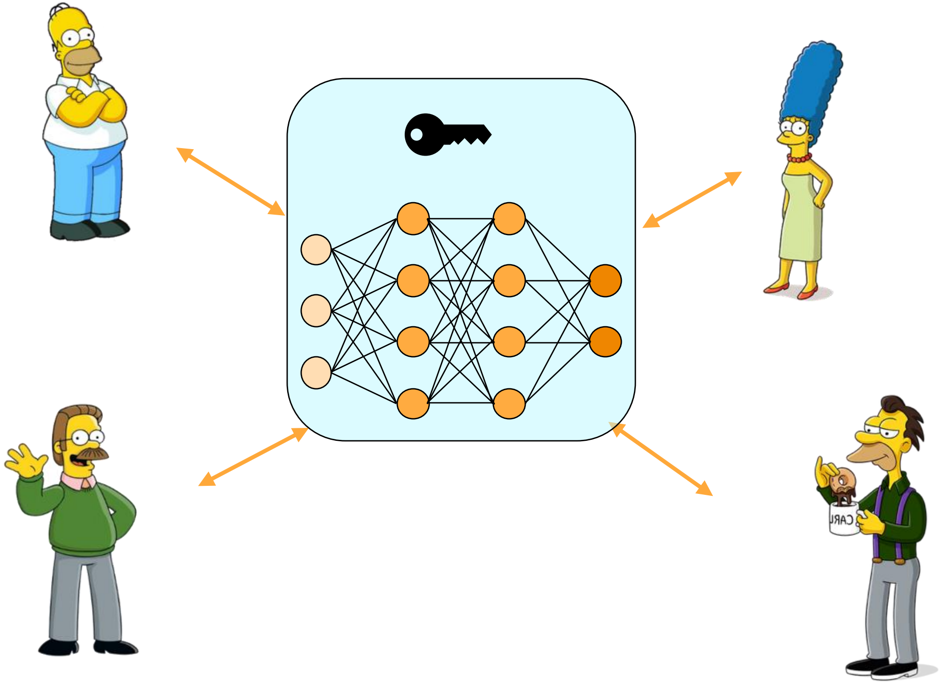
FL under encryption

Use Fully Homomorphic Encryption for training under encryption.

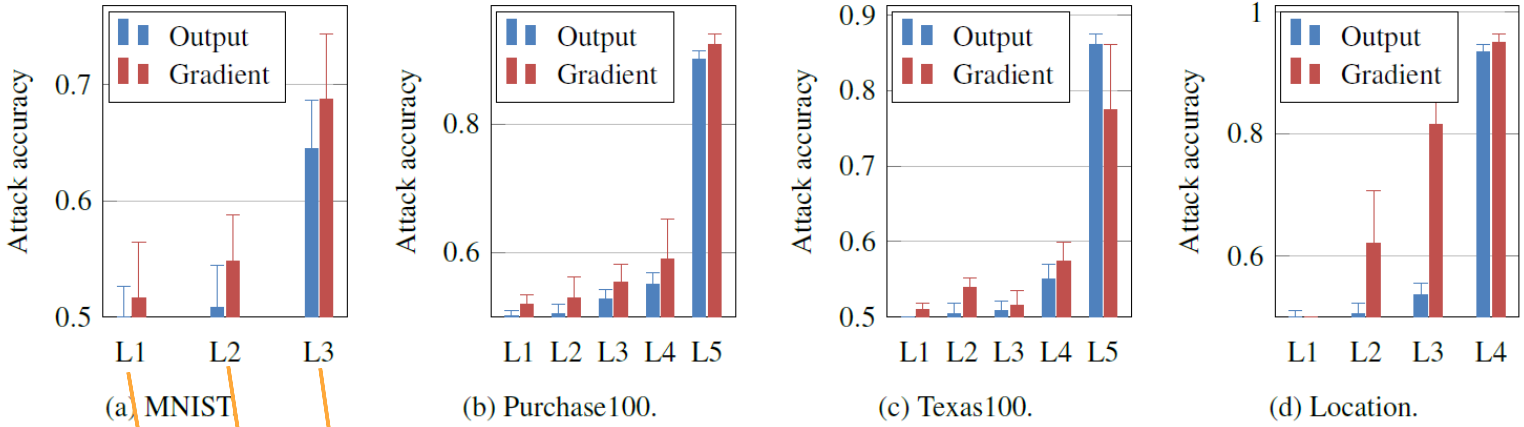
High computational and communication costs.

Impractical for deep models.





Assessing privacy attacks against model subsets



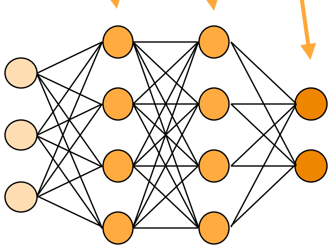
(a) MNIST.

(b) Purchase100.

(c) Texas100.

(d) Location.

Figure 1: Layer-wise accuracy of the white-box membership inference attack by Nasr et al. [54] against different datasets and models, exploiting both the layer's output and gradient.



FL under partial encryption

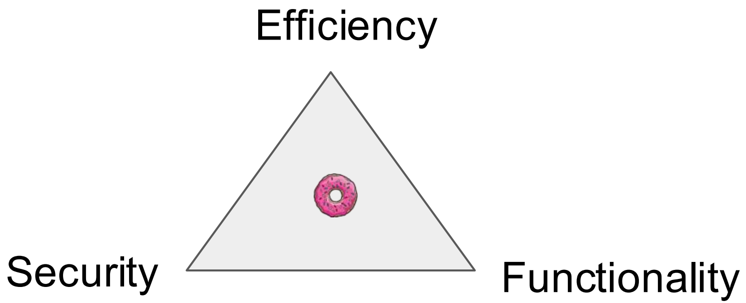
Different layers contain different information

Performances:

- The number of decryptions is independent of the neural network

Security:

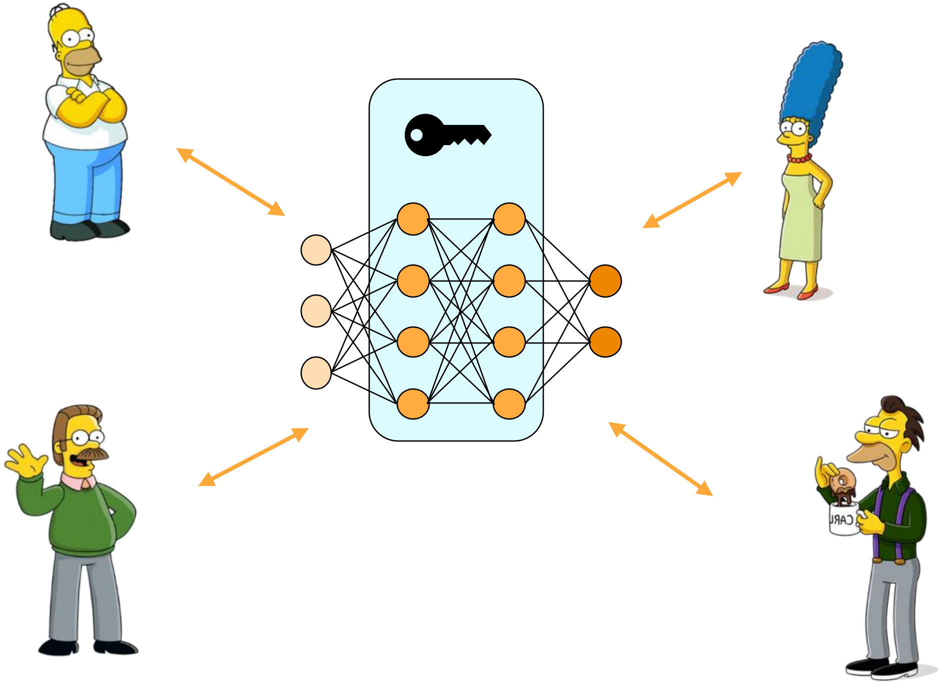
- Part of the weights are hidden



Efficiency

Security

Functionality



FL under partial encryption

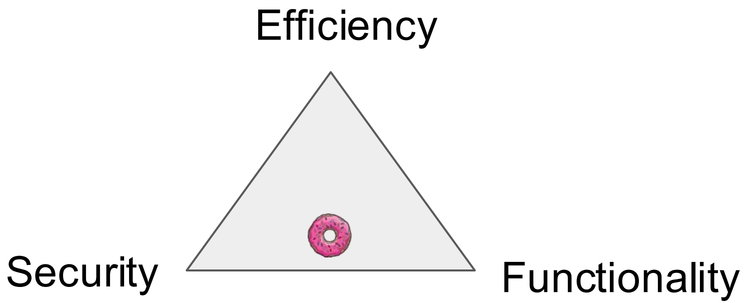
Different layers contain different information

Performances:

- The number of decryptions is independent of the neural network

Security:

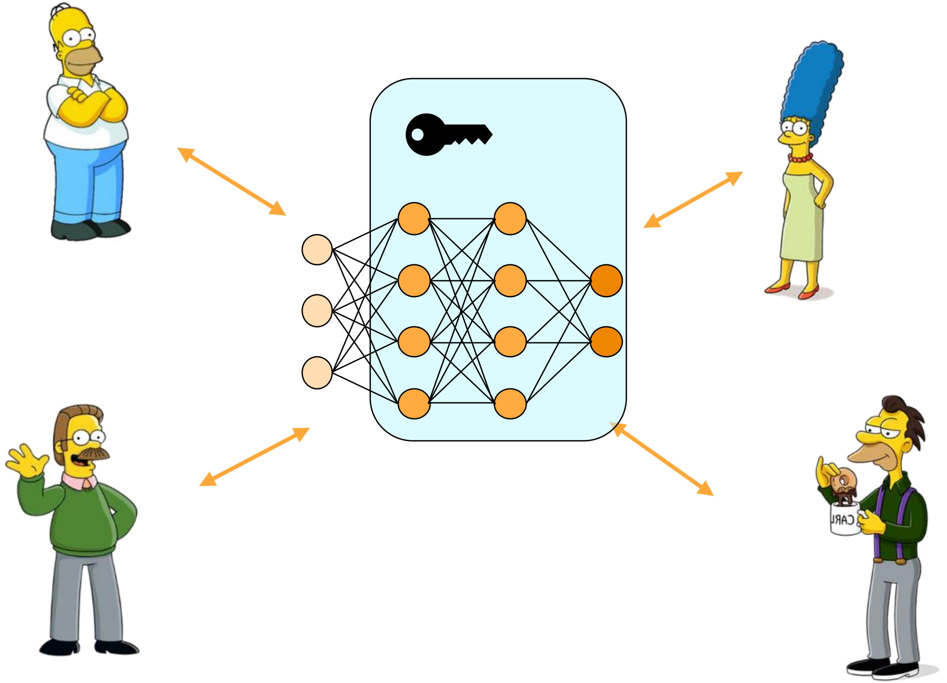
- Part of the weights are hidden



Efficiency

Security

Functionality



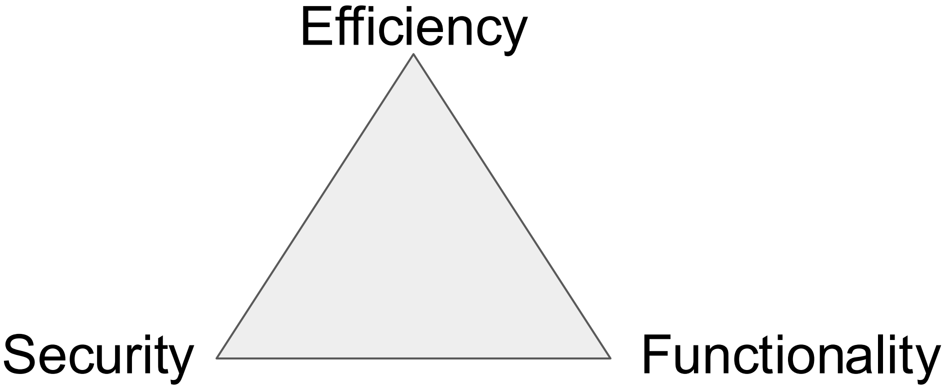
From research to real-world

There is on black-and-white (practical) solution for security threats

The shape of the trade-off figure might be different, e.g. with more dimensions

AI solutions for security also move within these boundaries and are no silver bullet

Purely technical solutions will not work without considering the human user in the system



Questions?