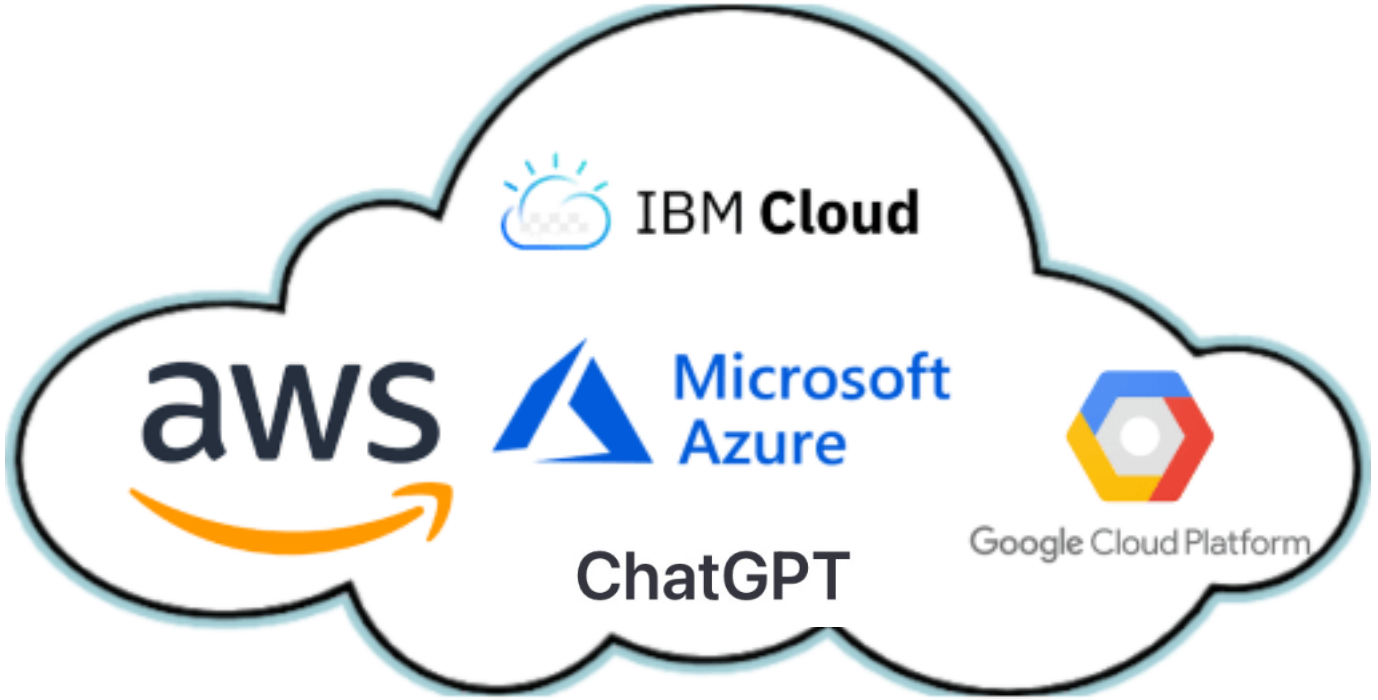
Homomorphic Evaluation of Convolutional Neural Networks

Huanhuan Chen (TU Delft)

(H.Chen-2@tudelft.nl)

October 25th, Università di Padova

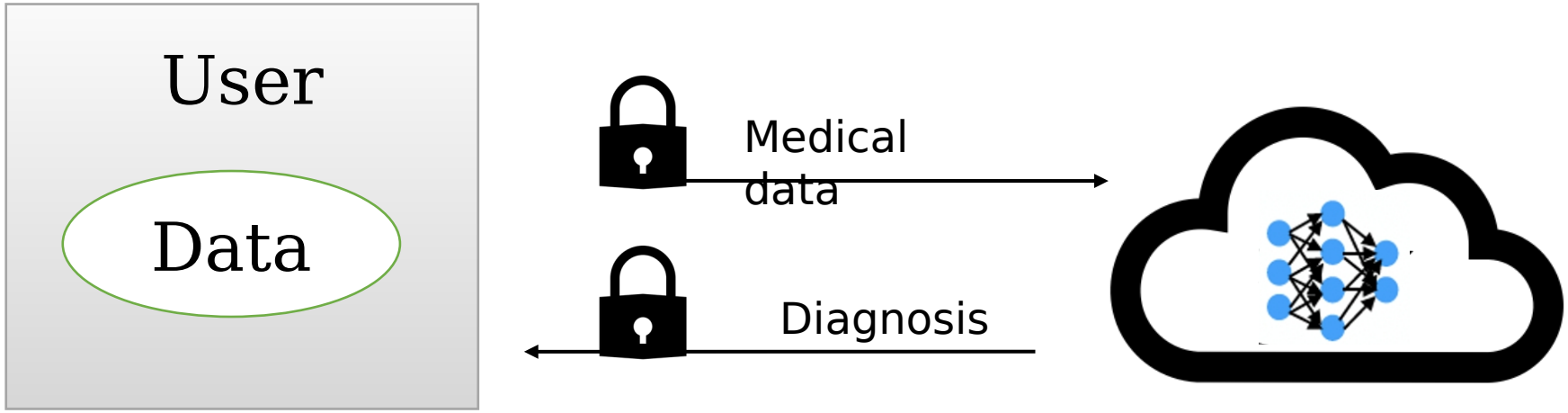
Machine Learning As a Service



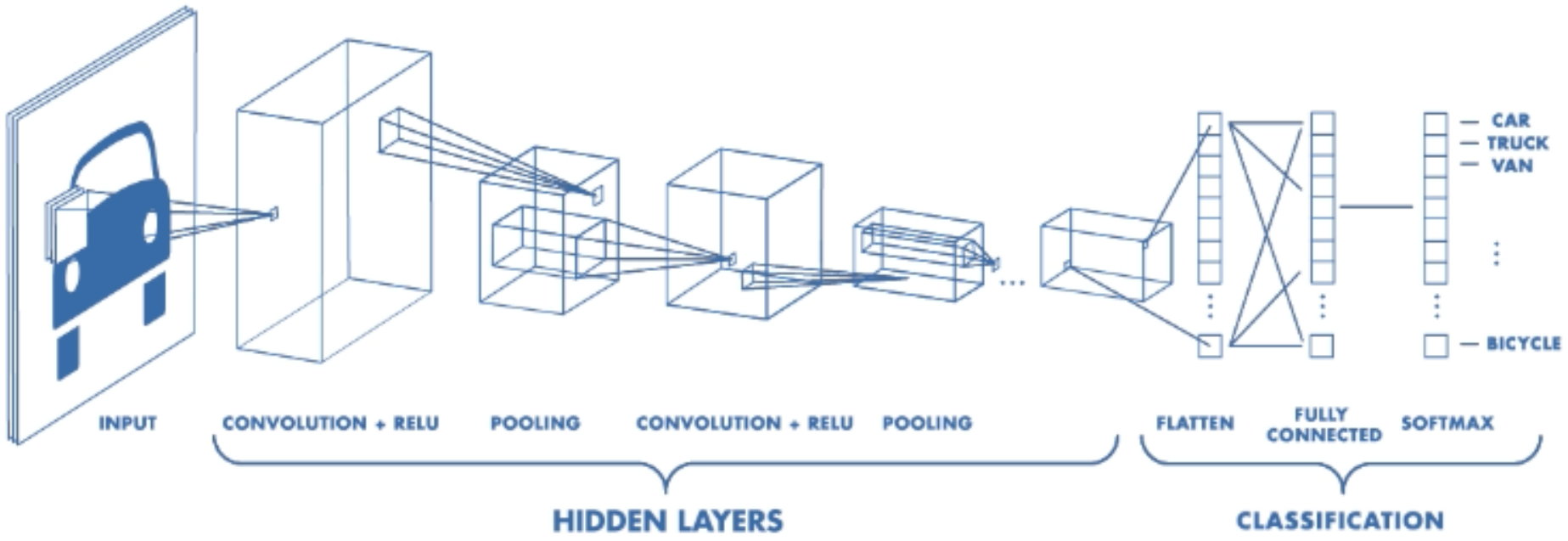
$1.0 billion in 2019 → $8.48 billion by 2025*

*https://neptune.ai/blog/machine-learning-as-a-service-what-it-is-when-to-use-it-and-what-are-the-best-tools-out-there

Privacy-Preserving Machine Learning



CNN



Activation function: ReLU, Max, sign, Sigmoid, etc.

Fully Homomorphic Encryption (FHE)

Given encrypted_data and a computation F, there exists an alternative F’ s.t.

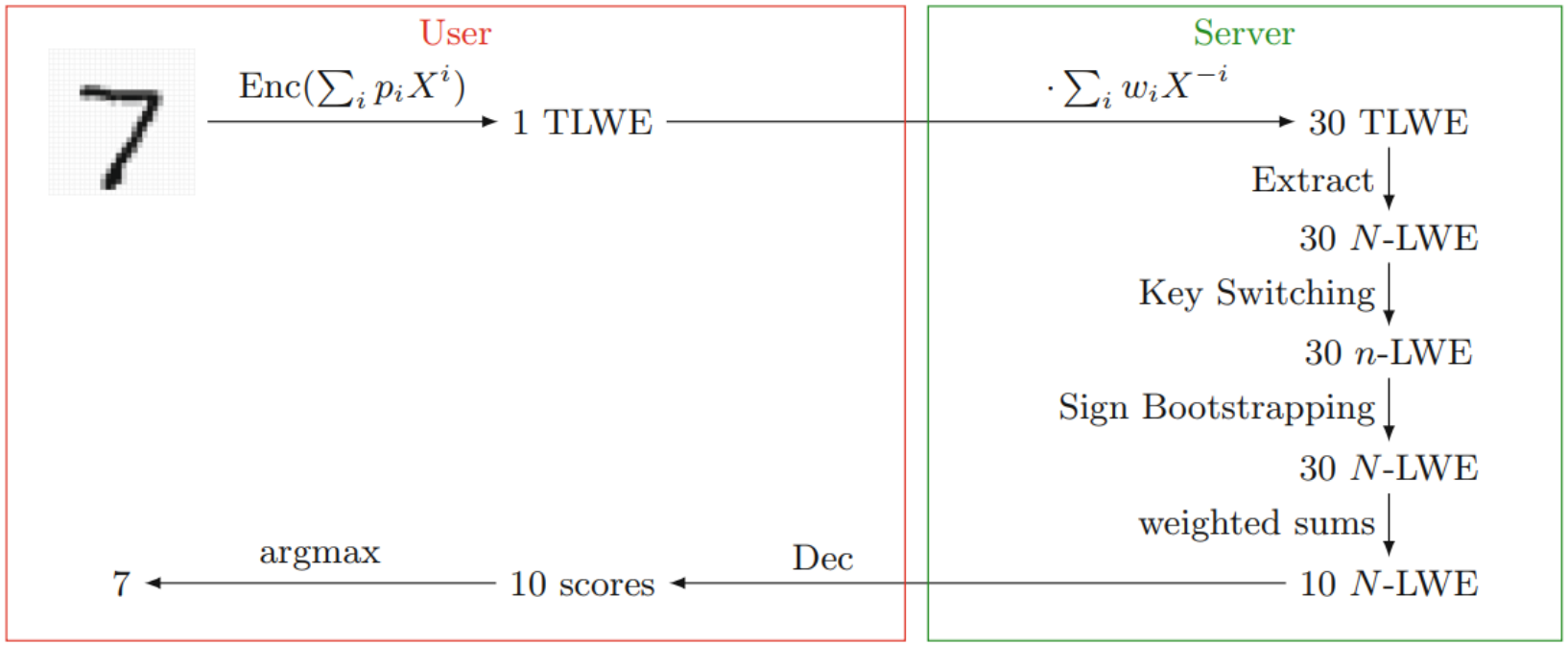


Fig. 1: homomorphic evaluation of a 784:30:10 neural network with activation function sign [Crypto 2018]

Prior Frameworks Are Not the Best

- From the activation function side
  - Only evaluate the sign function
  - Others are converted to polynomials

- From the message space side
  - Limited to 4-5 bits (eg. [0,128]→-1, [128,255]→1)

- Batch
  - Not SIMD, only SISD

We Propose a New Framework

	Activation Func.	Large MSG Space (# of Boot, if yes)	Batch
[BMMP, Crypt`18]	Sign	✗	✗
[LMP, Asiacrypt`22]	Sign	✓ (2)	✗
[LW, EUROCRYPT`23]	Sign	✗	✓ (msg: 0/1)
Our work	Sign/Max/ReLU	✓ (1)	✓

Learning With Errors (LWE)

RSA: (discrete logarithm problem)

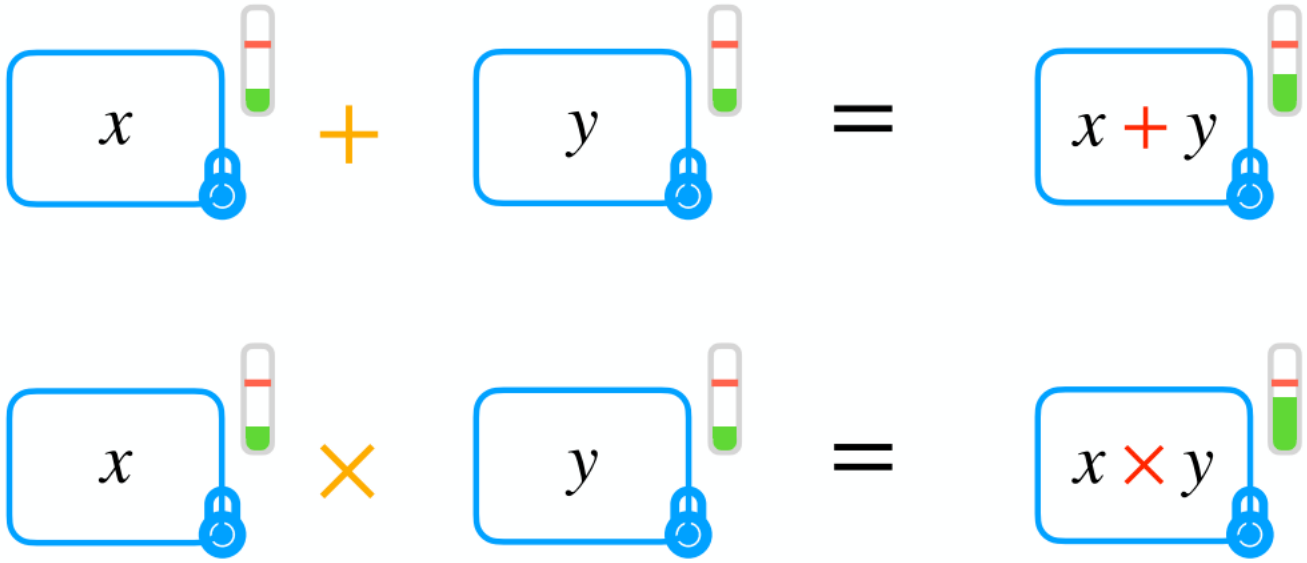
LWE hardness:

LWE encryption: mod , msg space

decryption: mod

addition homomorphism:

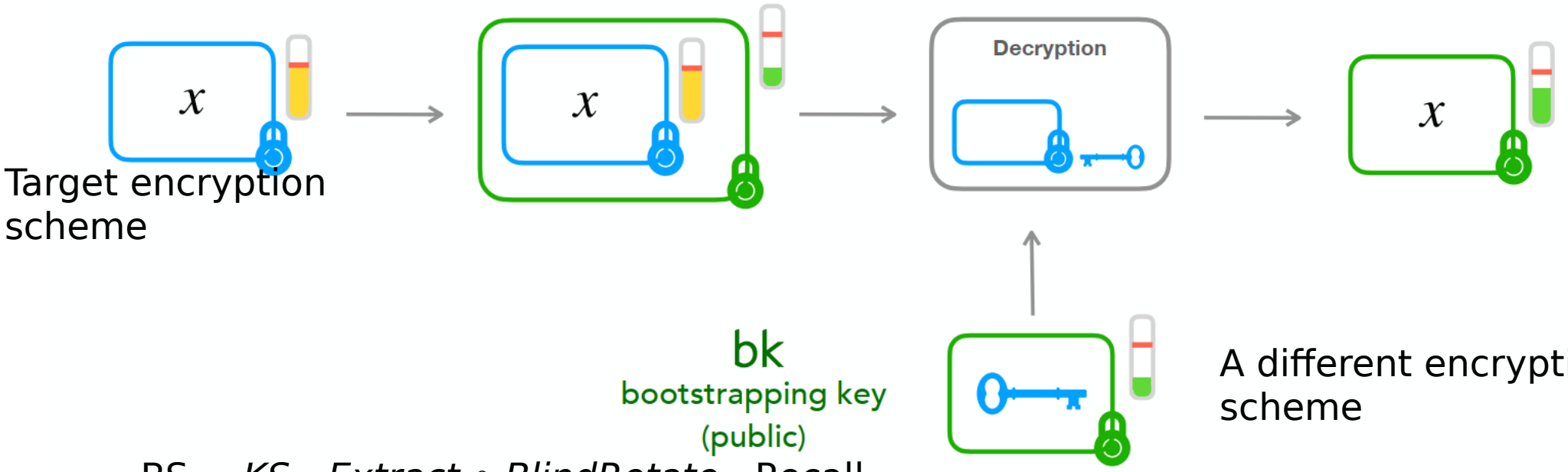
Errors Increased After Homomorphic Operations



Noise grows too much 🌡️ ⇒ decryption incorrect 🚨

[Chillotti. Introduction to FHE and the TFHE scheme]

Bootstrapping [Gen09]



BS = *KS* ∘ *Extract* ∘ *BlindRotate*, Recall

BlindRotate - Liner part: with input

(msb)Extract – Nonlinear part:

[Chillotti. Introduction to FHE and the TFHE scheme]