FHE for Machine Learning

USING TFHE [CGGI16]

Samuel Tap - Zama samuel.tap@zama.ai

LINKMEDIA SEMINAR - JANUARY 2022

Zama

2019 - 2020: Speed up homomorphic inference (Concrete Library)

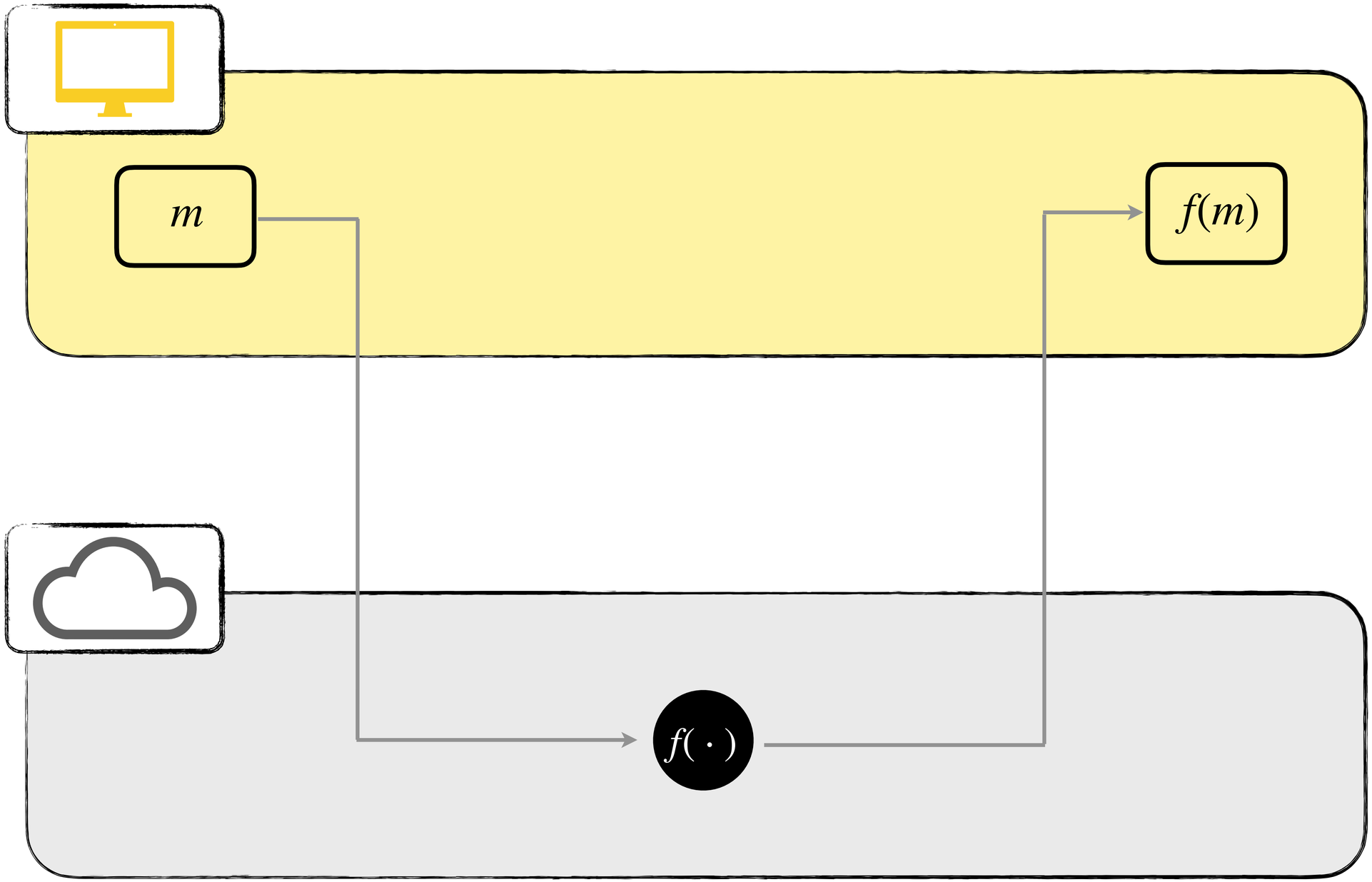
2020 - 2022: Improvement of the PBS (asiacrypt paper)

Optimization for FHE

Data Transfer

Past

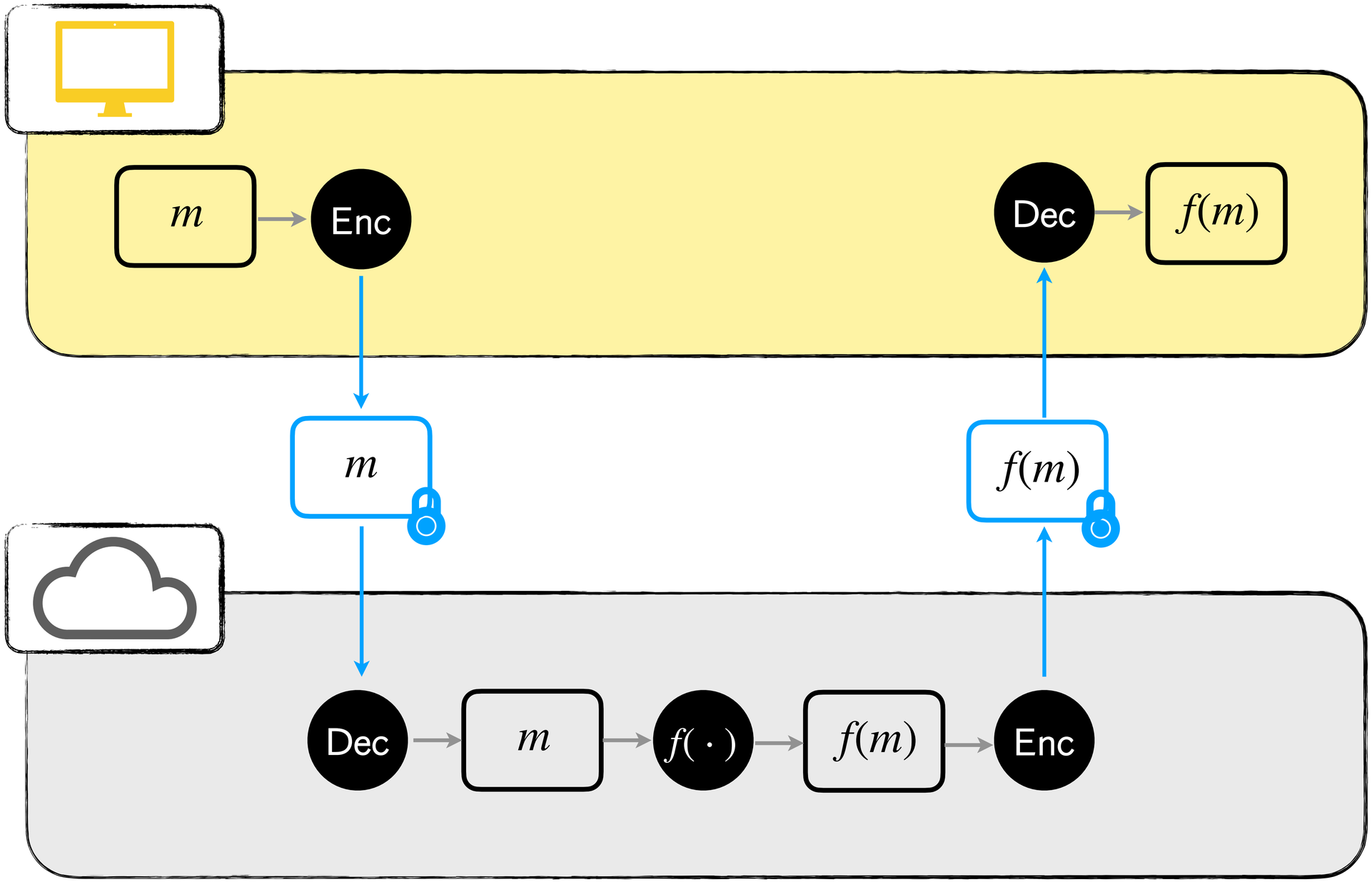
- ✗ In transit
- ✗ At rest
- ✗ In processing



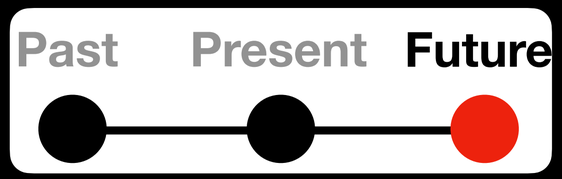
Data Transfer

Past Present

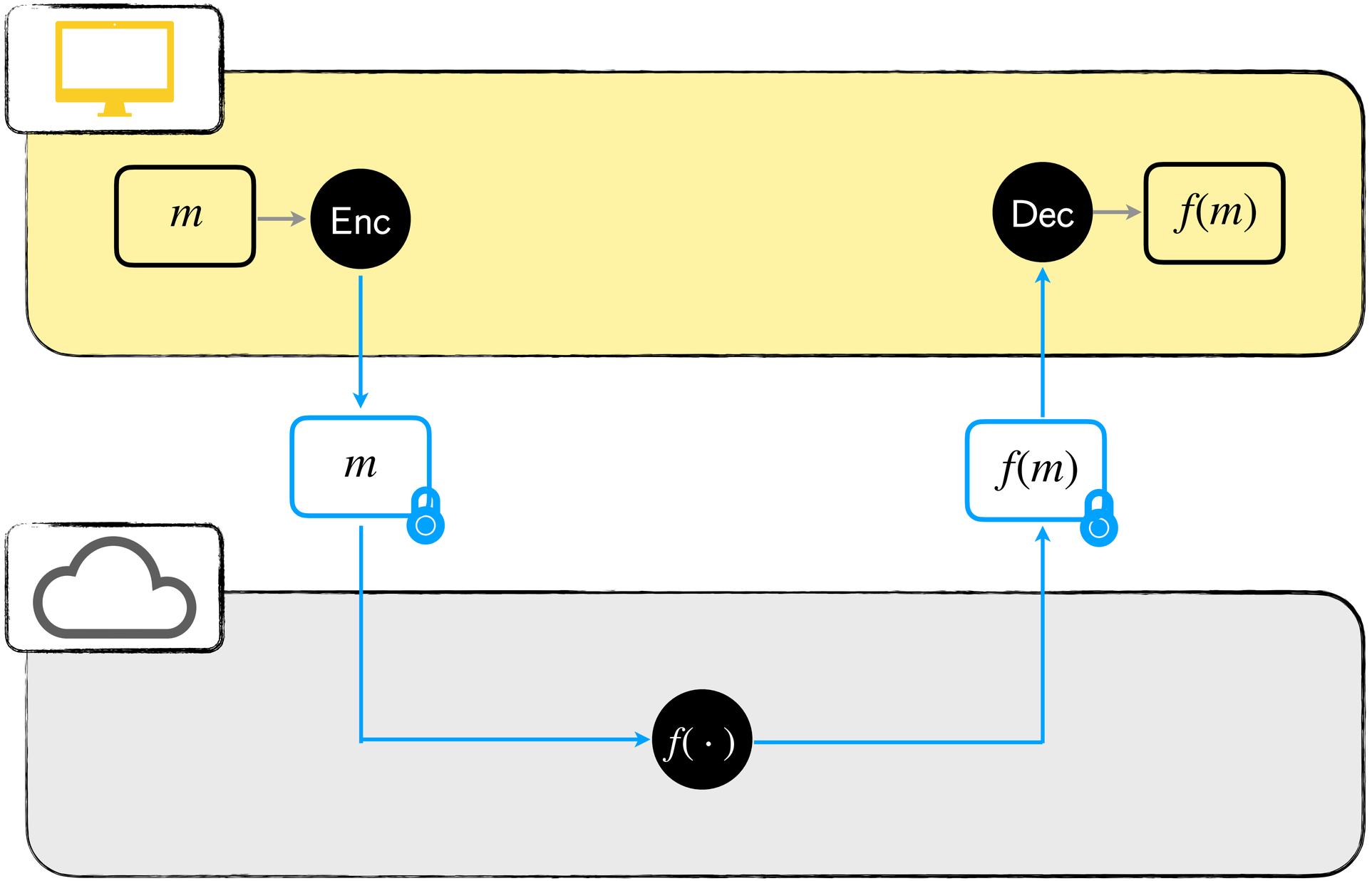
- ✅ In transit
- ✅ At rest
- ❌ In processing



Data Transfer



- ✅ In transit
- ✅ At rest
- ✅ In processing



Use Cases

Health

- Blood work
- STDs, HIV
- Genomics
- Lifestyle tracking

Gov

- Tax evasion
- Police/Justice case solving
- Crime prevention

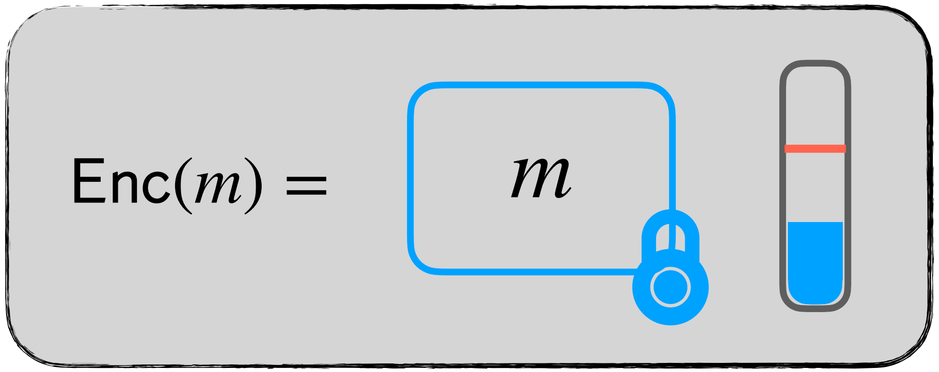
Financial

- Investments
- Transaction records
- AML regulation
- Fraud prevention

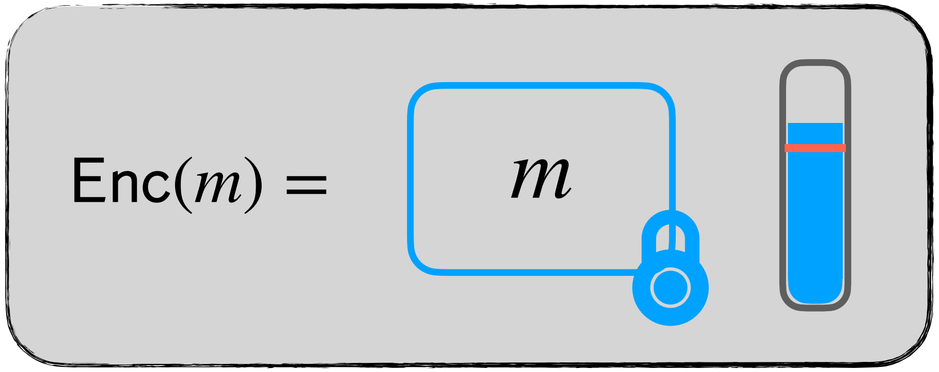
HOW ?

FHE using TFHE

Noise



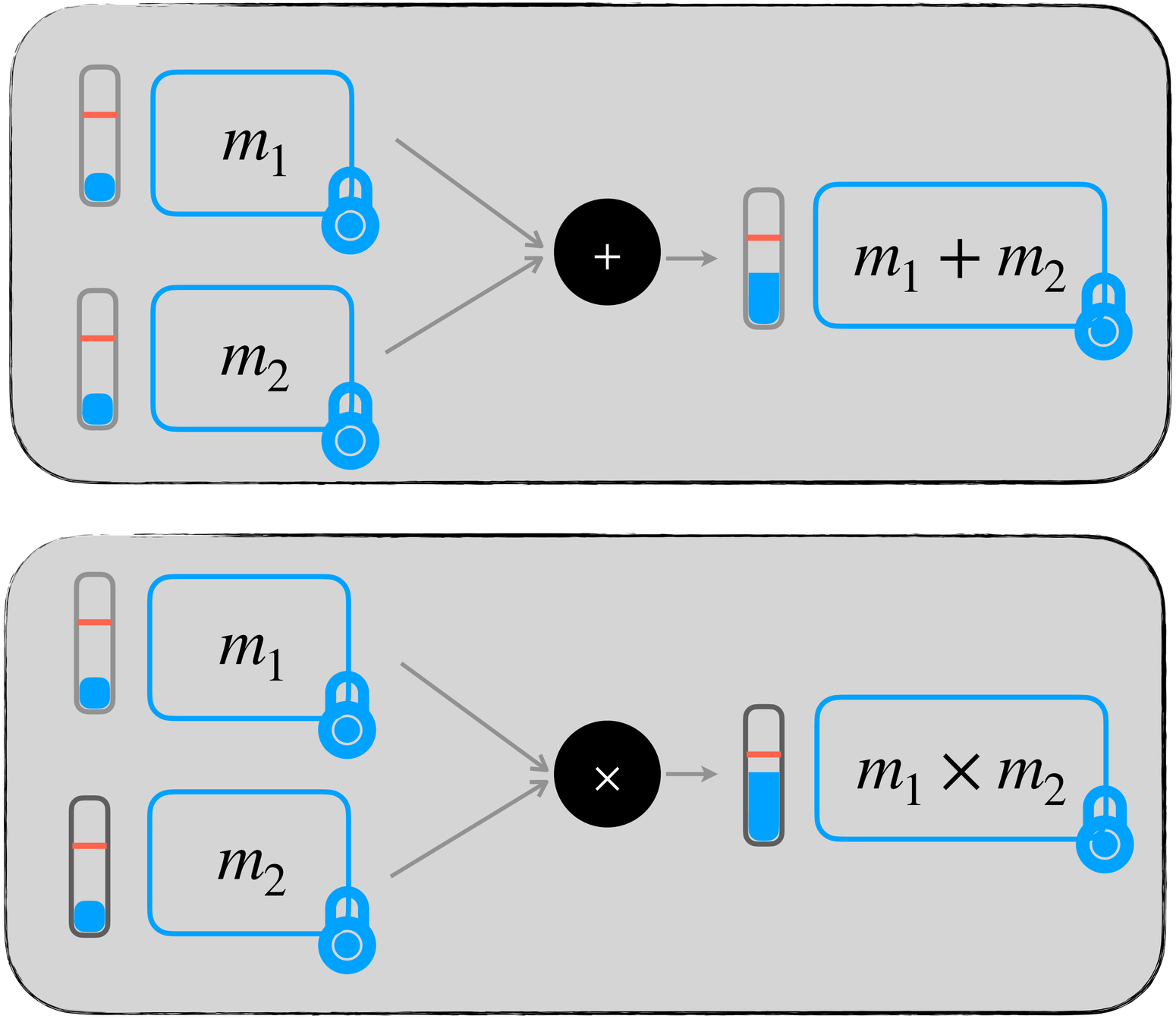
✅ decryptable



❌ incorrect decryption

Security rely on (R)LWE hardness assumption

Fully Homomorphic Encryption

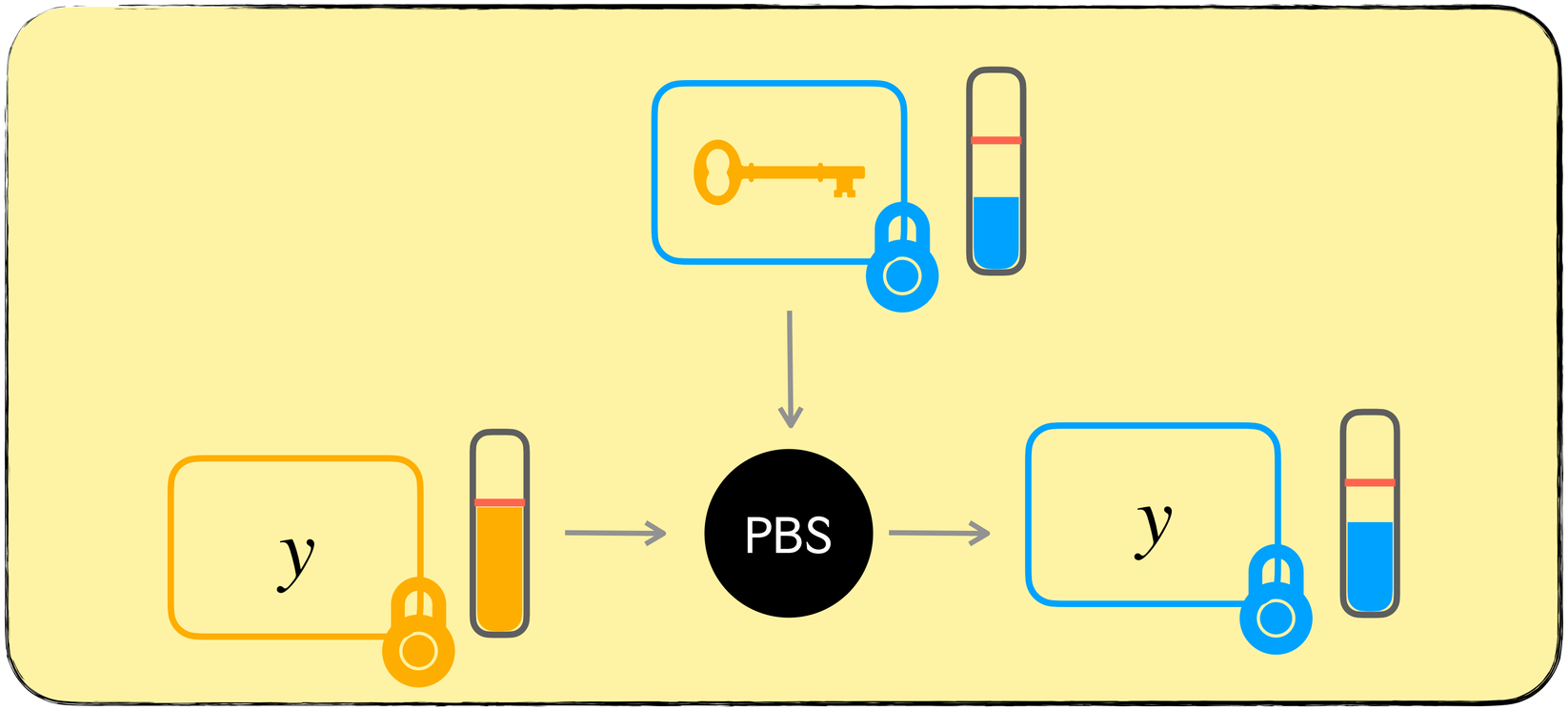


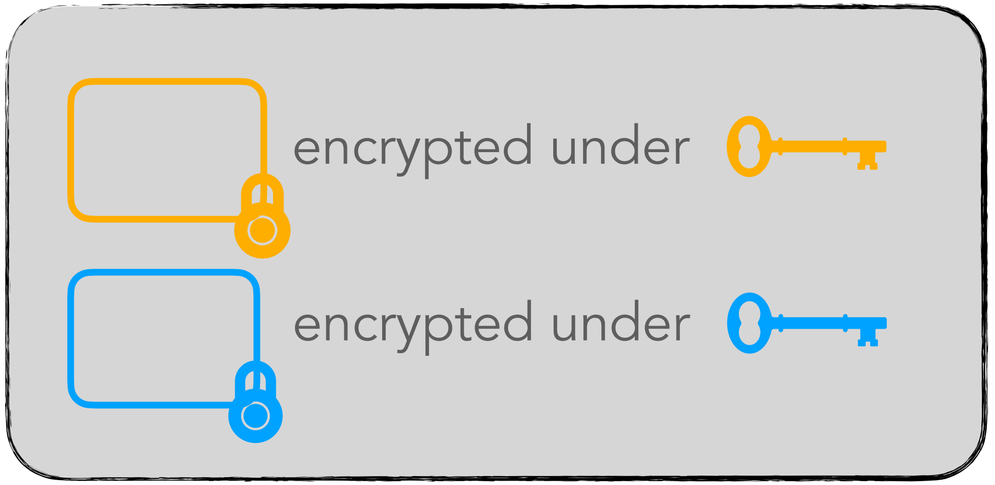
Somewhat Homomorphic Approach

1. Choose a circuit to evaluate
2. Choose cryptographic parameters large enough

Bigger parameters → Slower computation

Bootstrap [Gen09]

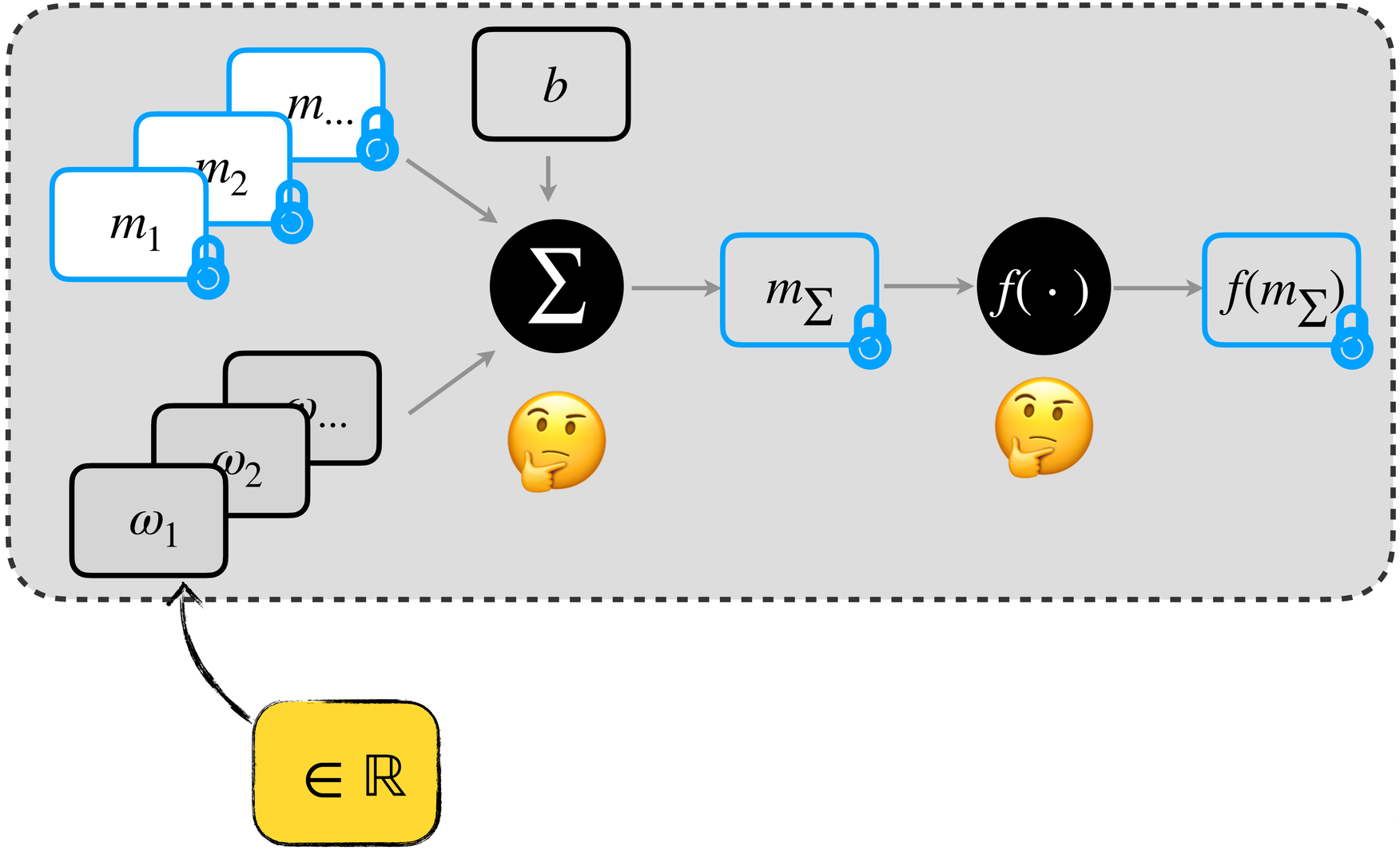




≈ Homomorphic decryption

No need to know the circuit anymore !

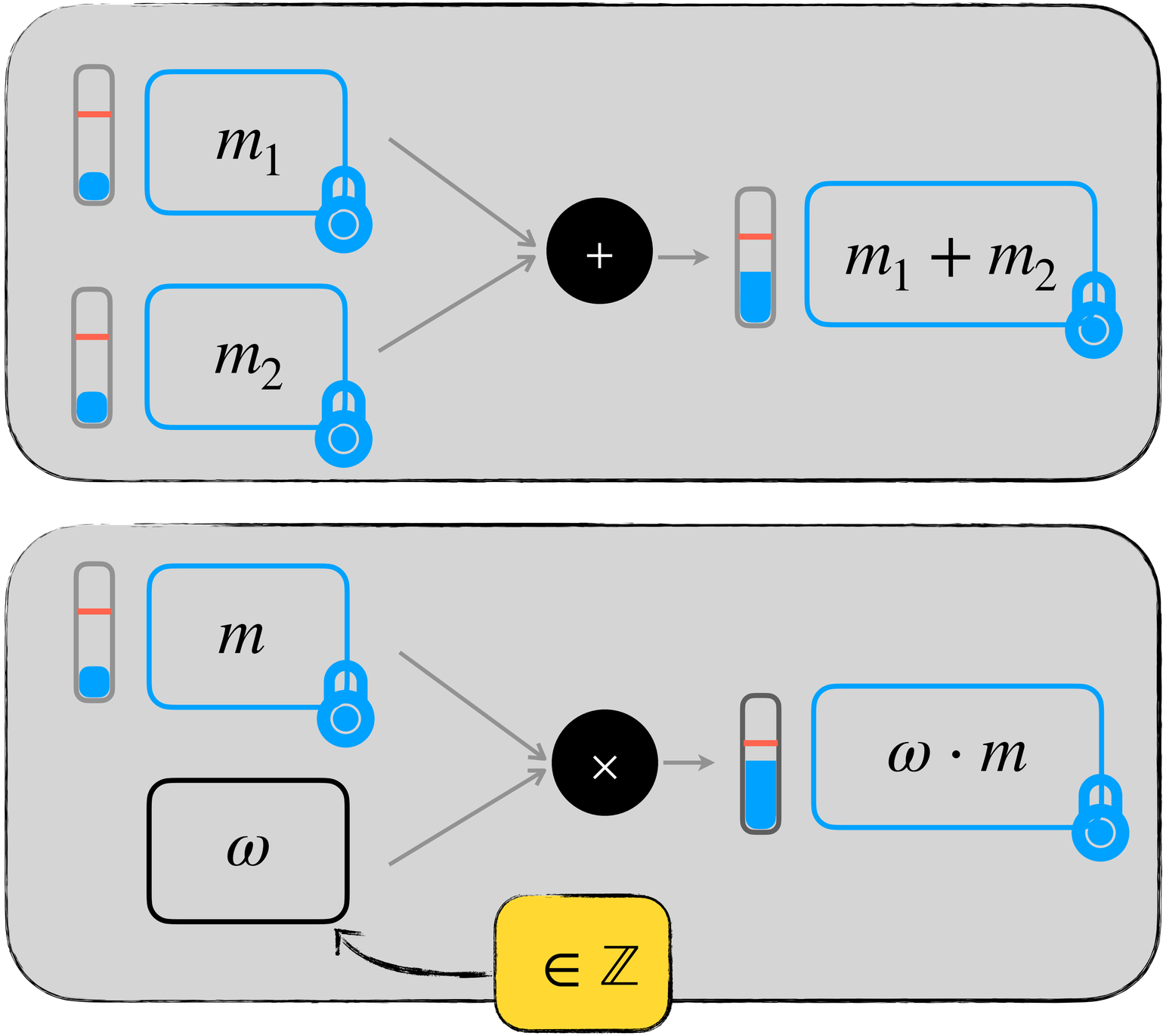
Neuron



$$m_\Sigma = \sum \omega_i \cdot m_i + b$$

Addition

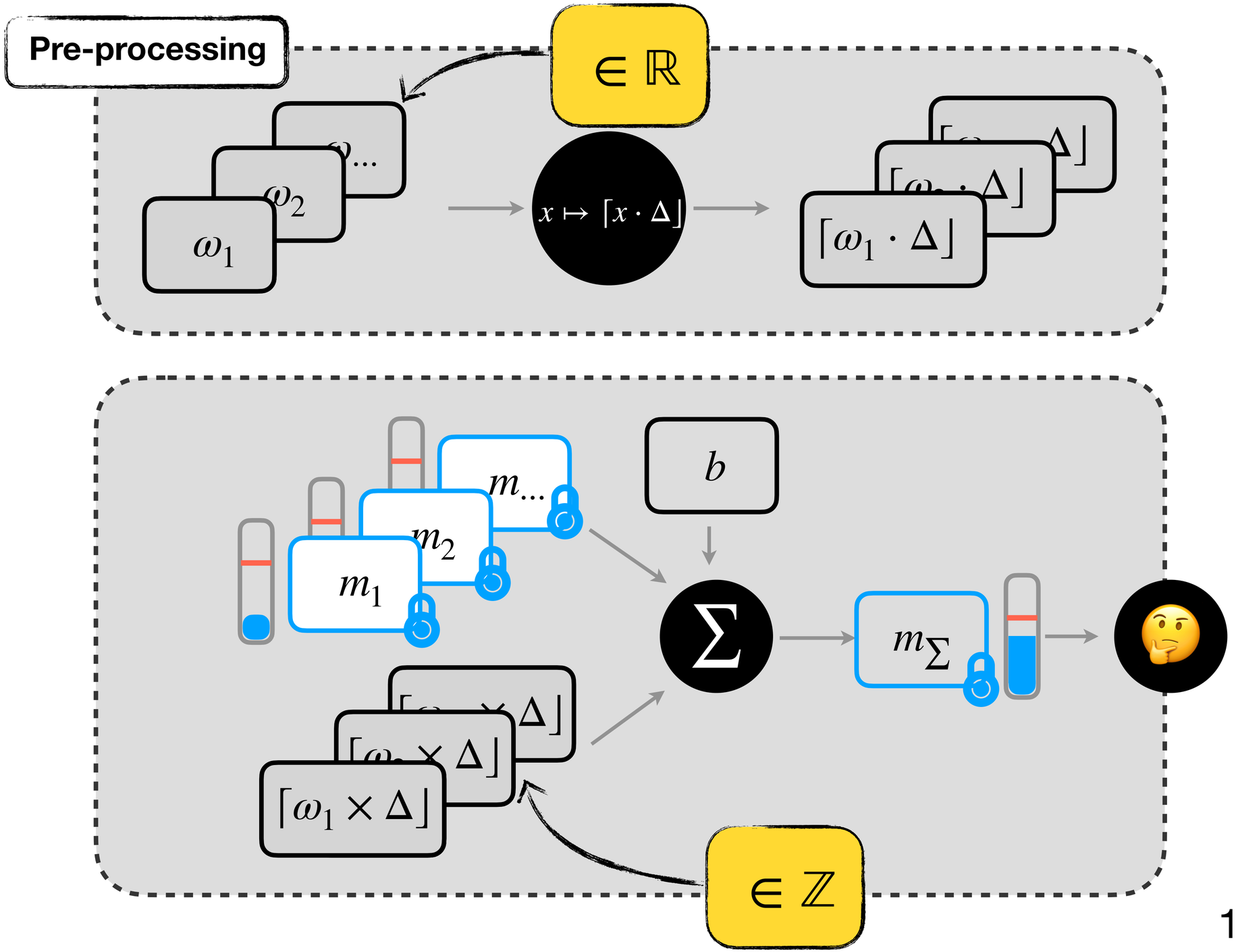
Homomorphic Addition



Homomorphic Addition

Neuron

$$\sum_{i=1}^{n} m_i \cdot \omega_i \approx \frac{1}{\Delta} \sum_{i=1}^{n} m_i \cdot \lceil \omega_i \times \Delta \rfloor$$

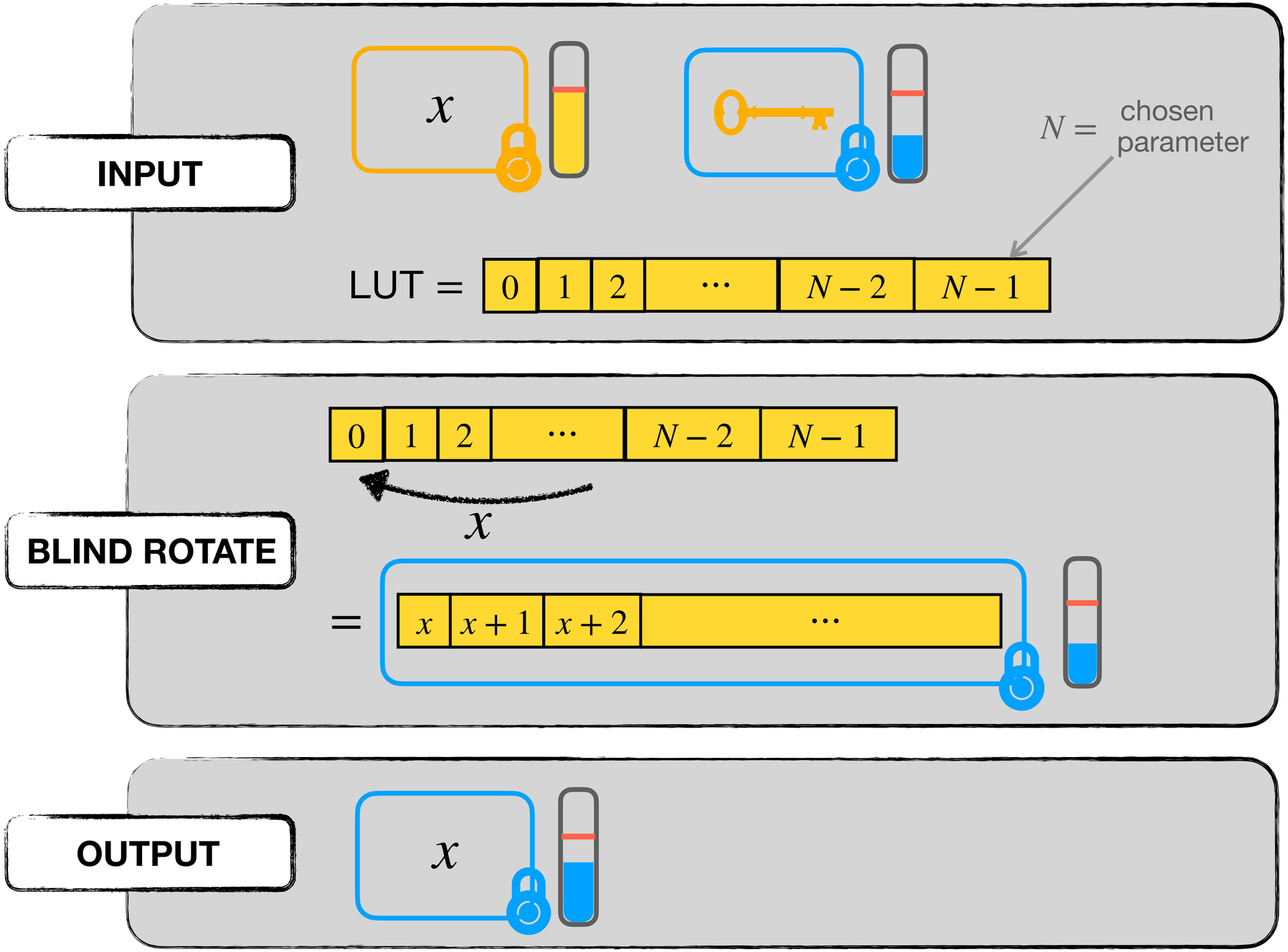


Activation function

Programmable Bootstrapping

Bootstrapping

LUT evaluation



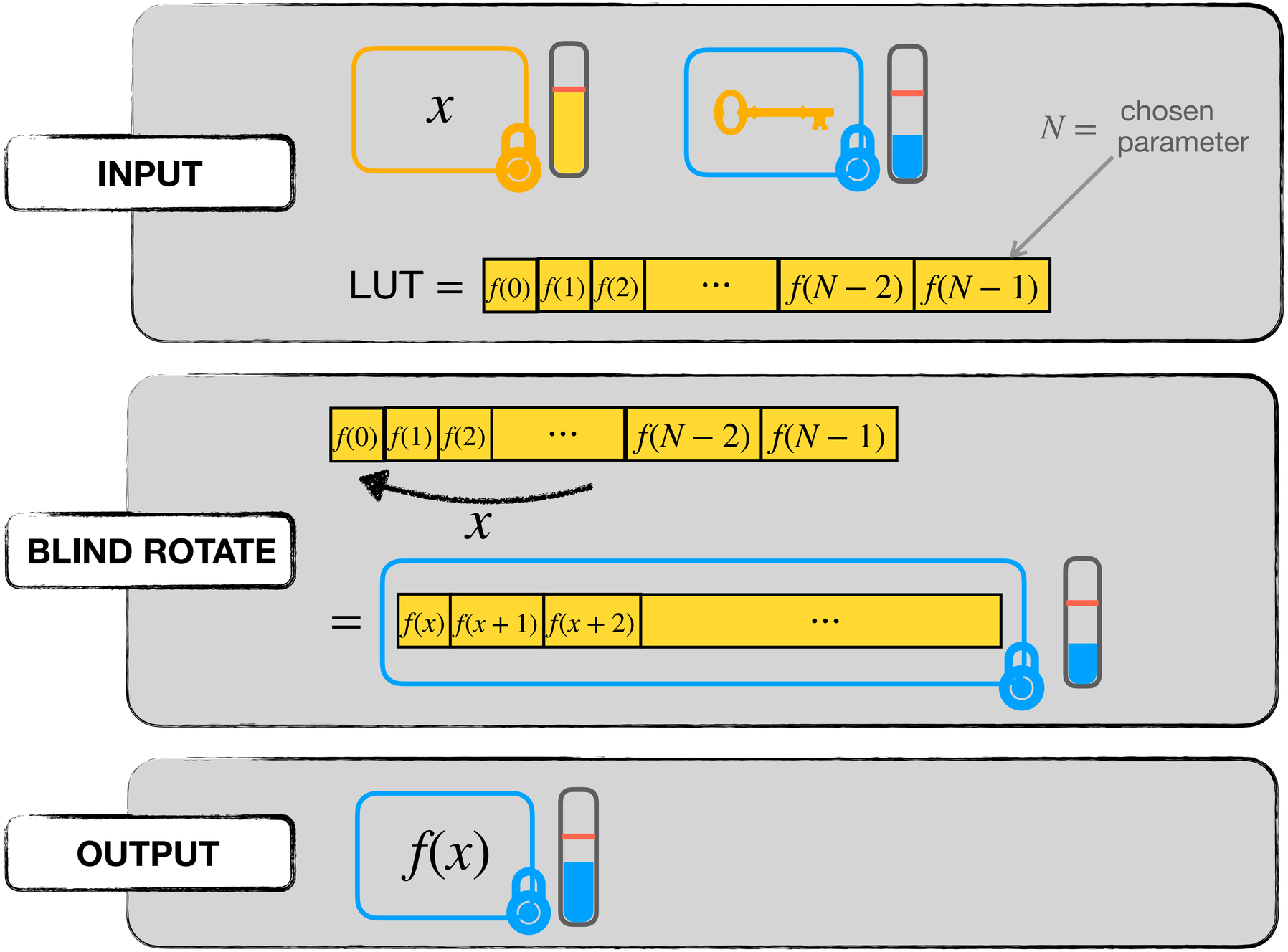
Programmable Bootstrapping

Bootstrapping

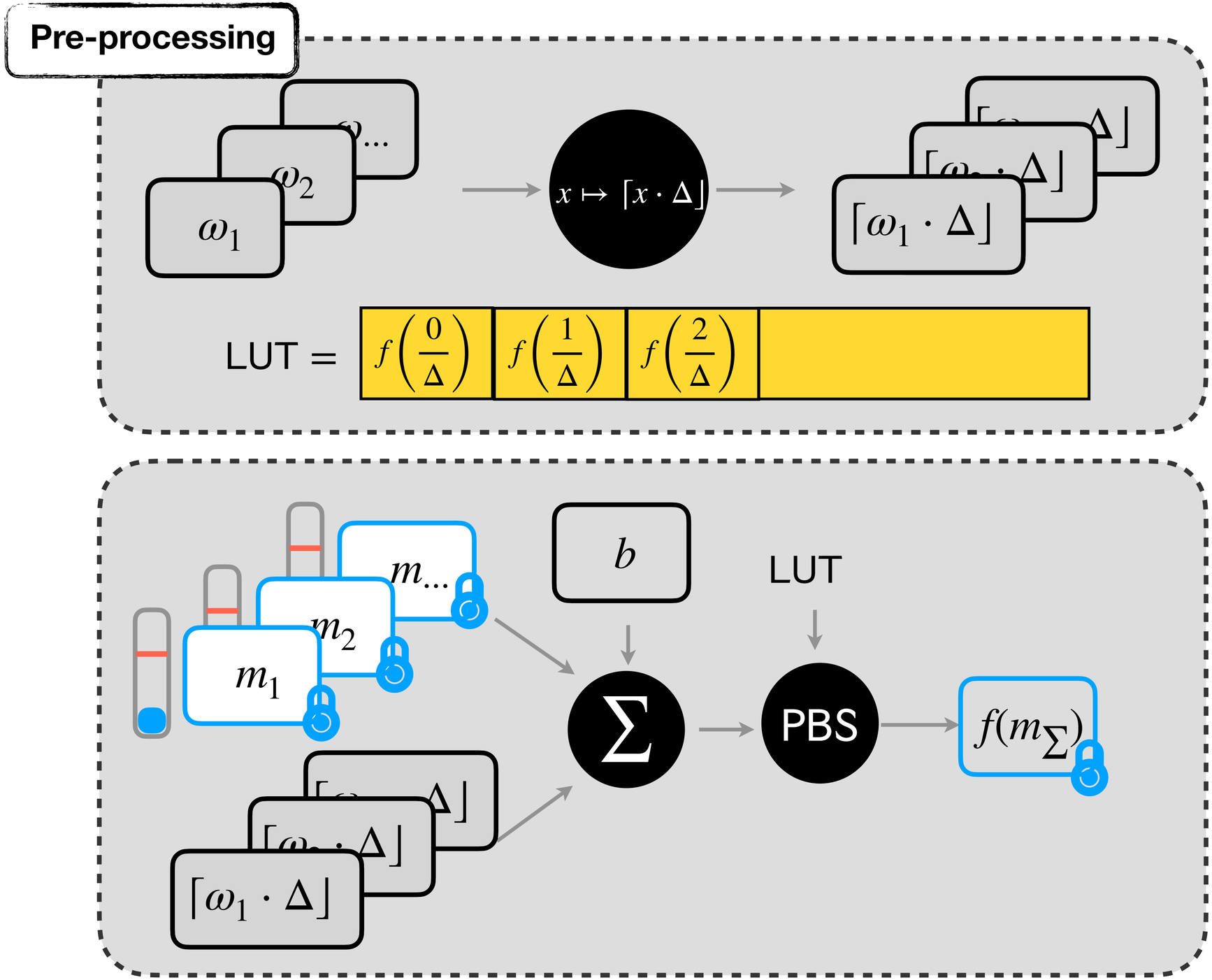
LUT evaluation

For Neural Network

$$f : x \mapsto \mathrm{ReLu}(\frac{x}{\Delta})$$

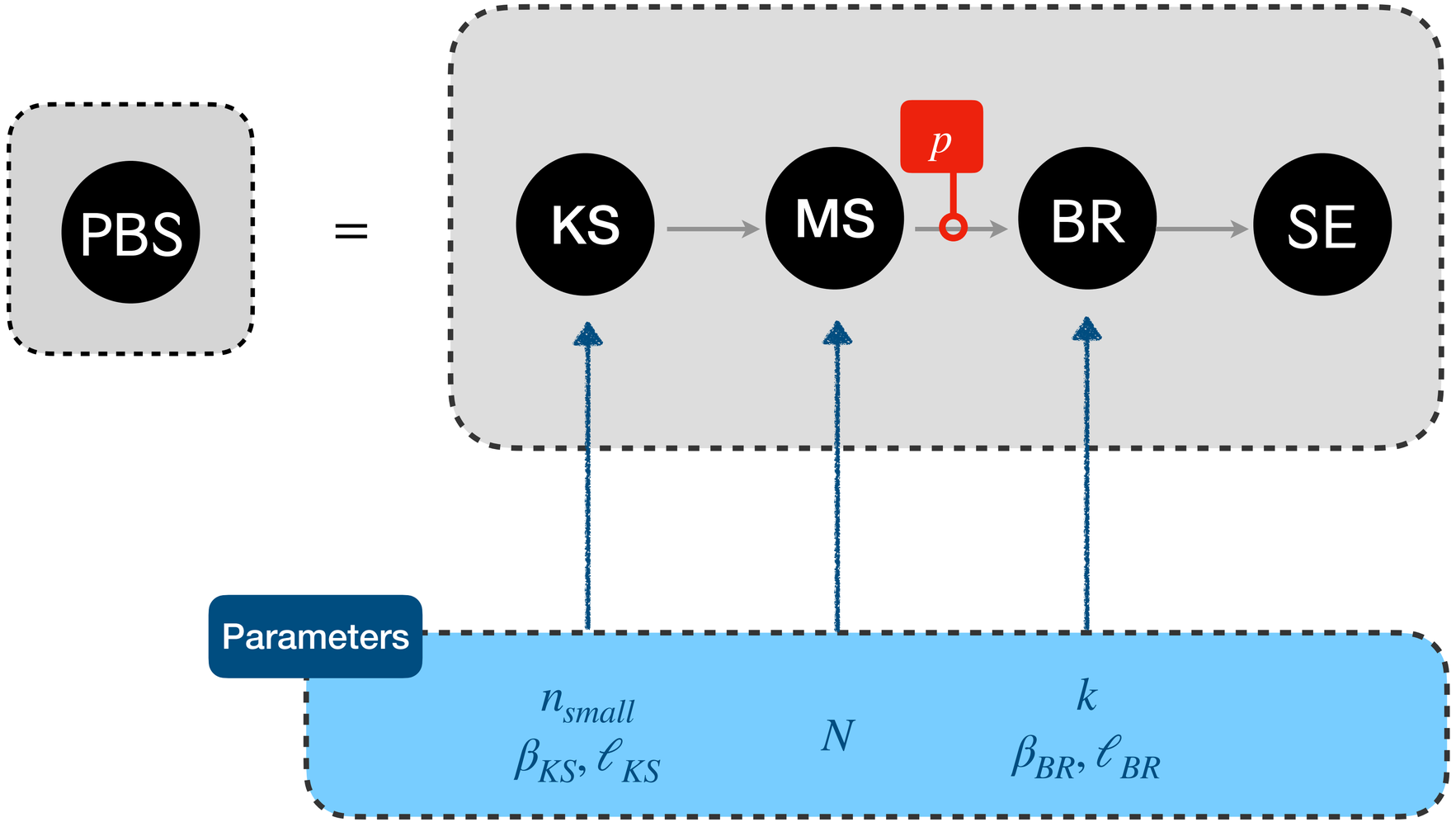


Homomorphic Neuron



Is that it ?

Optimization

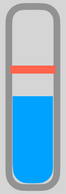


Optimization

Find **Parameters** that are

FAST

SECURE



CORRECT

Conclusion

Futur Work

Find the best FHE DAG of a given DAG

Relax the One Key Hypothesis

Bootstrap improvement

Encoding improvement