Loris Bergerat, Anas Boudi, Quentin Bourgerie, **Ilaria Chillotti**,
Damien Ligier, Jean-Baptiste Orfila & Samuel Tap

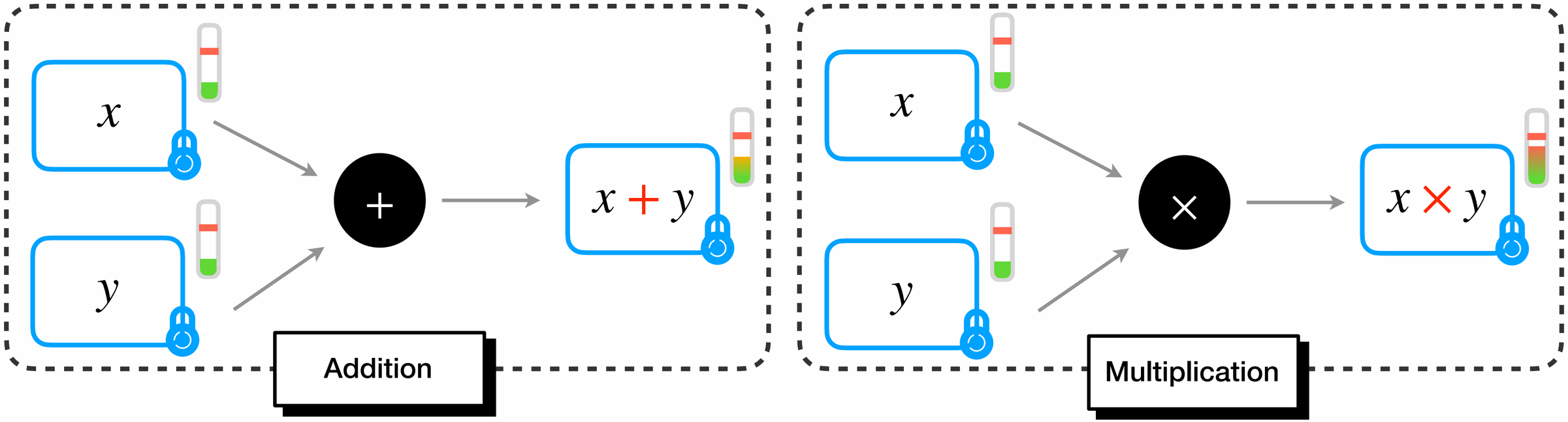
26 June 2023

Parameter Optimization & Larger Precision for (T)FHE

Agenda

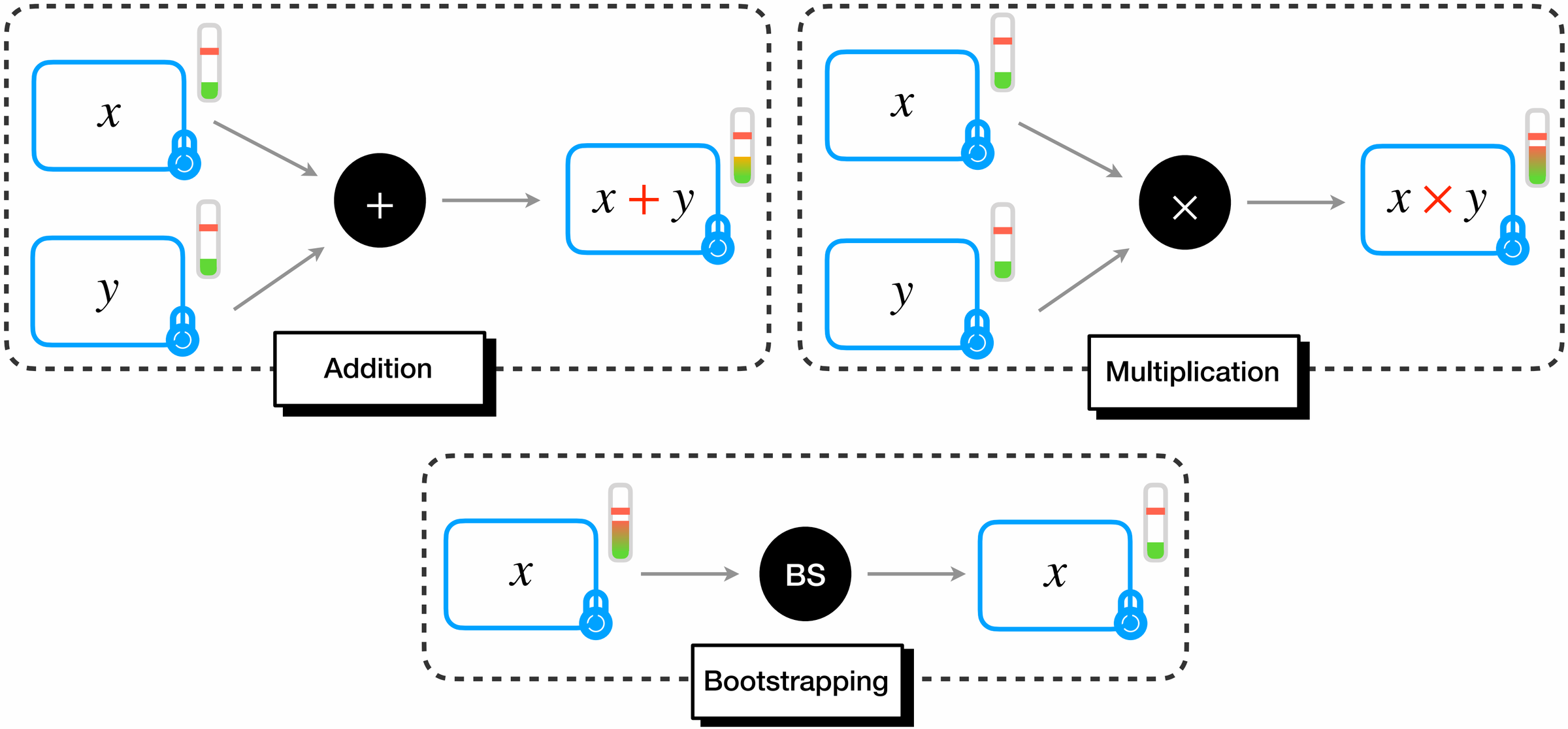
FHE and TFHE

FHE

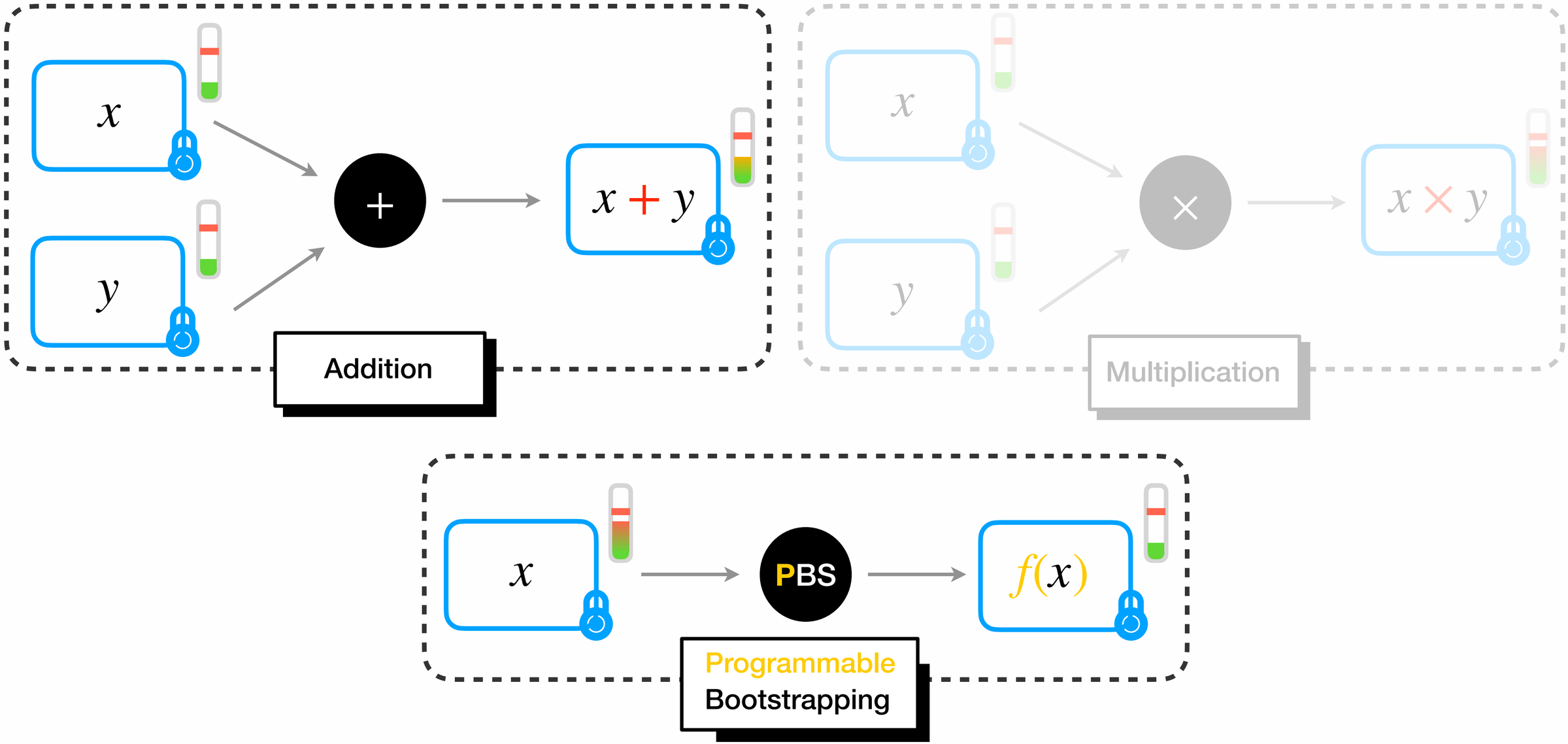


too much noise 🥵 $\Longrightarrow$ incorrect decryption

FHE

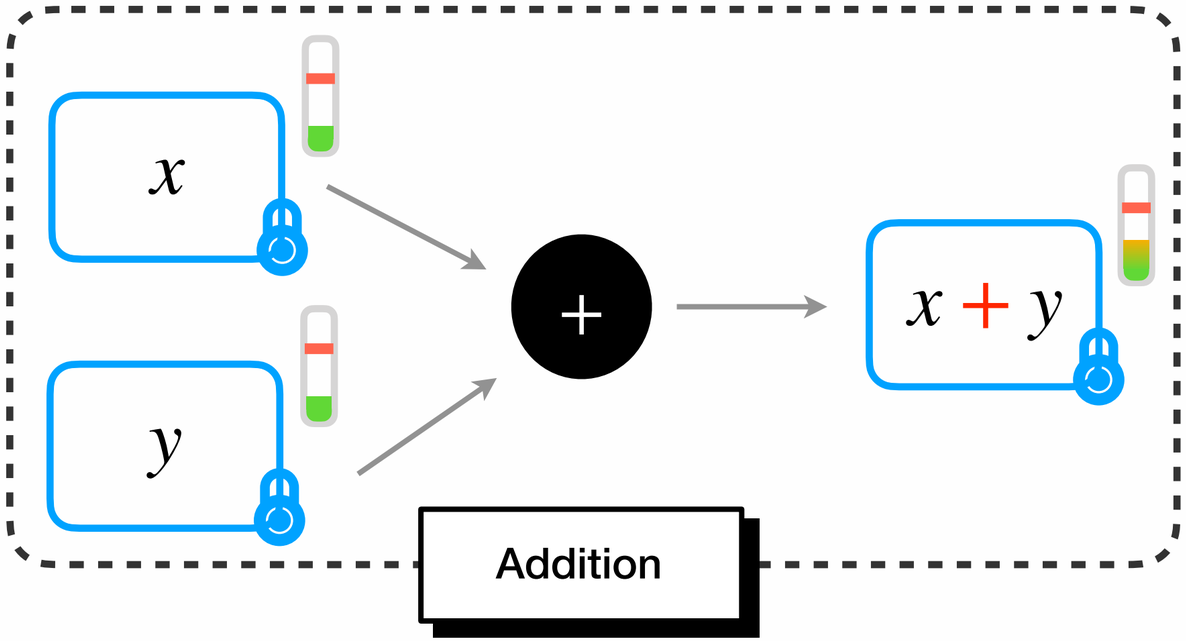


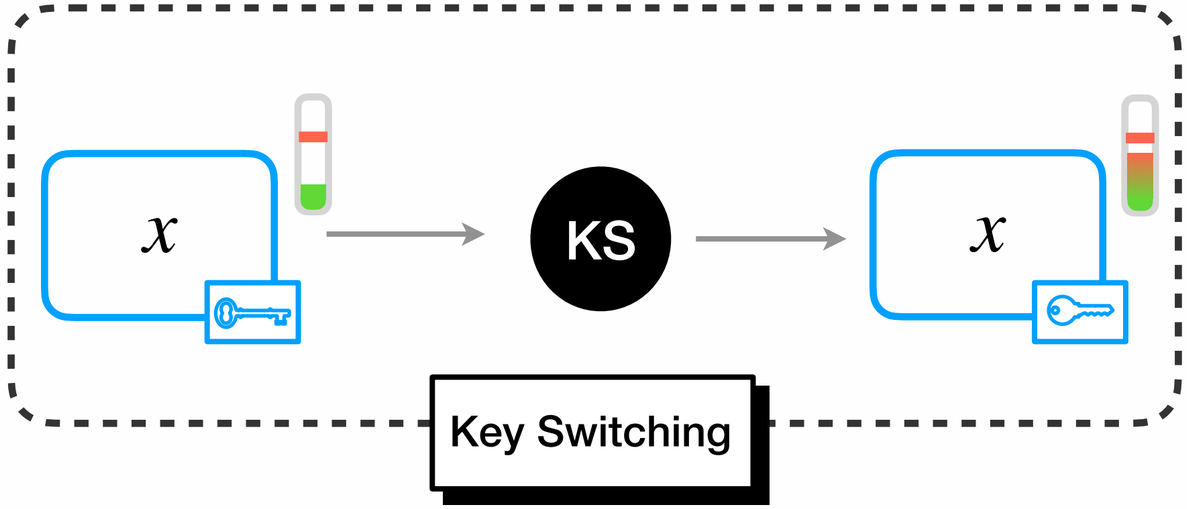
(T)FHE

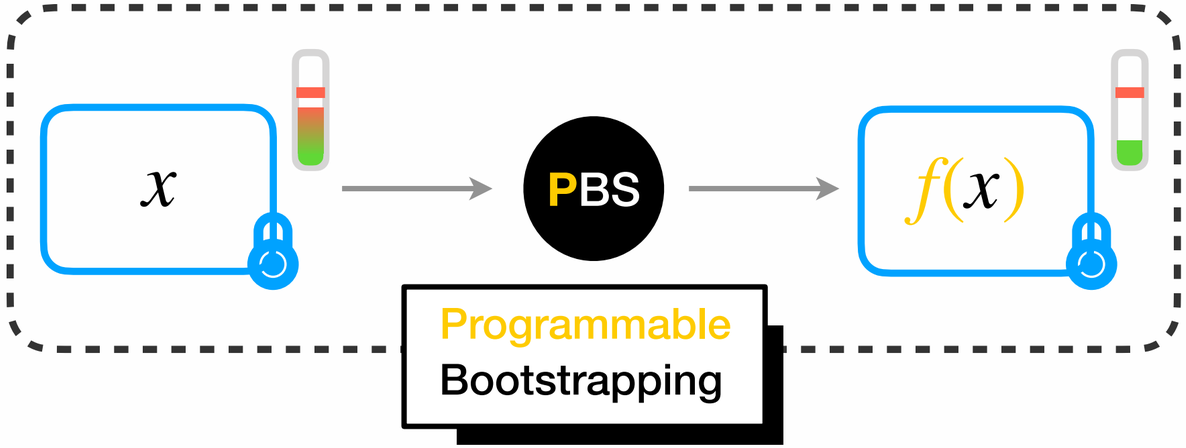


[CGGI20] I. Chillotti, N. Gama, M. Georgieva, M. Izabachène. TFHE: Fast Fully Homomorphic Encryption over the Torus. Journal of Cryptology 2020.

(T)FHE

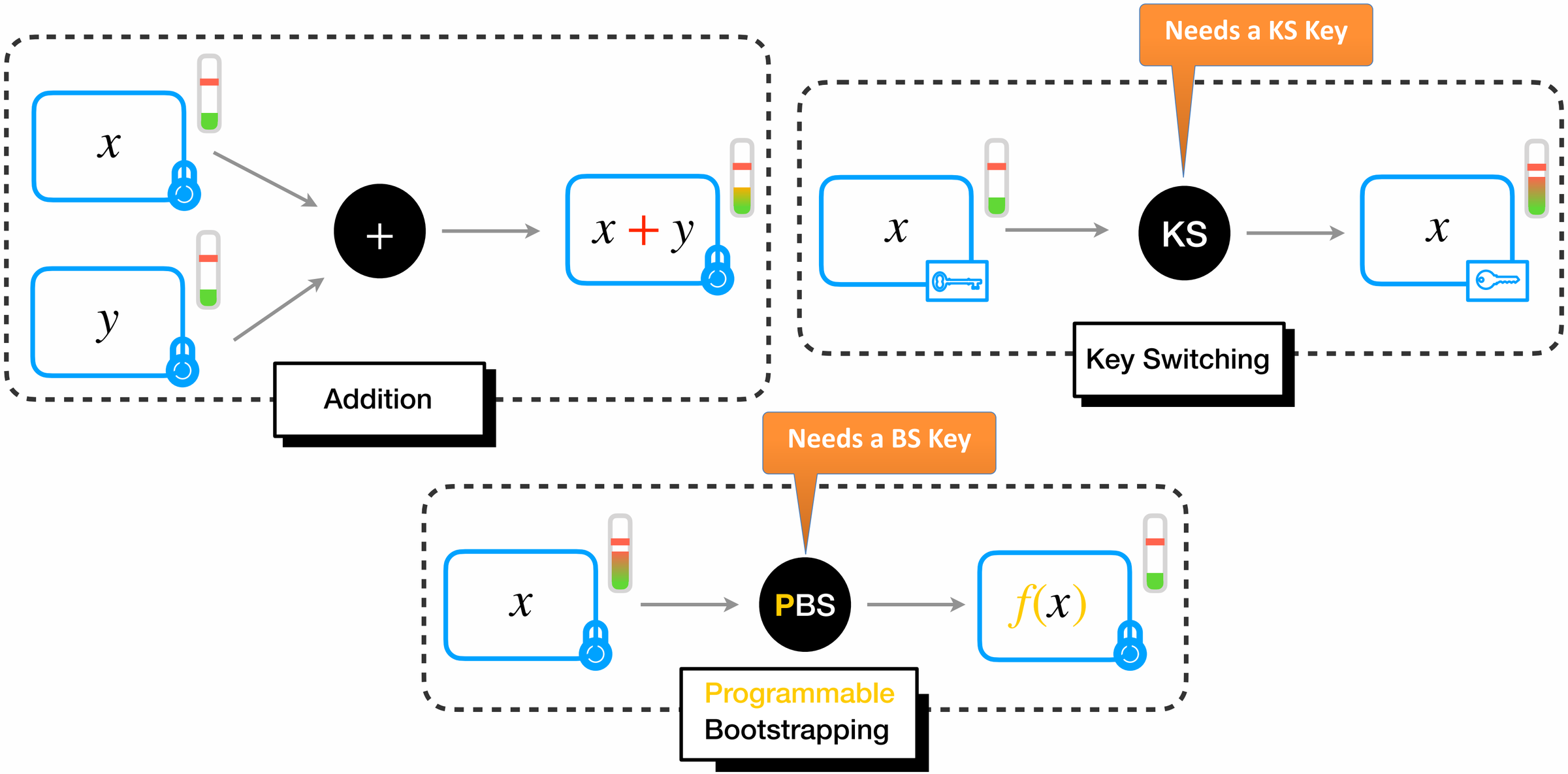






[CGGI20] I. Chillotti, N. Gama, M. Georgieva, M. Izabachène. TFHE: Fast Fully Homomorphic Encryption over the Torus. Journal of Cryptology 2020.

(T)FHE



[CGGI20] I. Chillotti, N. Gama, M. Georgieva, M. Izabachène. TFHE: Fast Fully Homomorphic Encryption over the Torus. Journal of Cryptology 2020.

$$\mathscr{R}_q = \mathbb{Z}_q[X]/(X^N + 1)$$

TFHE Ciphertexts

LWE

$$m \;\; (\vec{s}) = \vec{a} \;\; b \in \mathbb{Z}_q^{n+1}$$

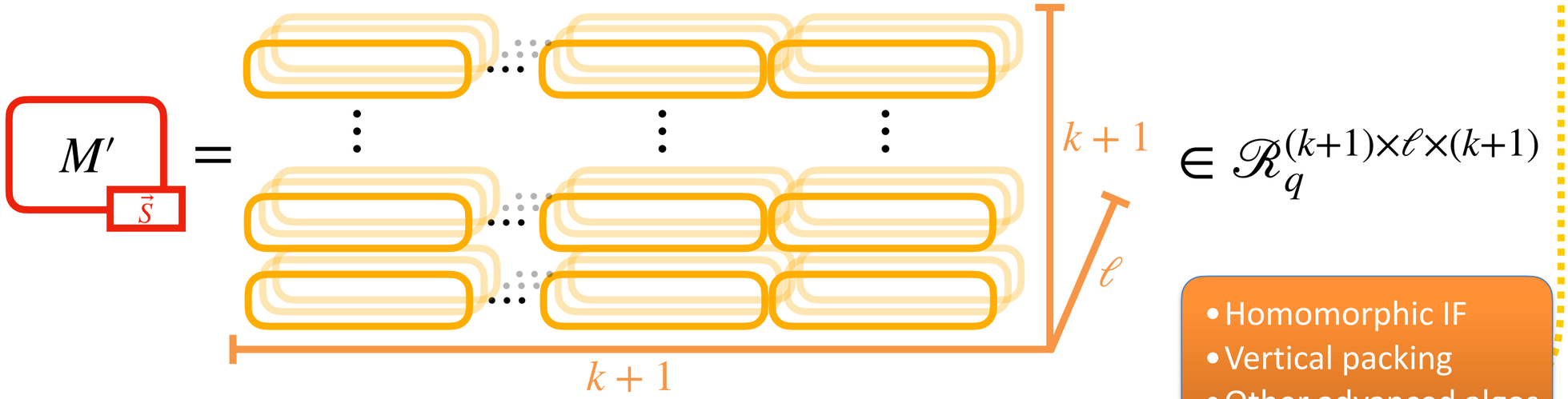
Linear Combinations

Programmable Bootstrapping

GLWE

$$M \;\; (\vec{S}) = A_0 \cdots A_{k-1} \;\; B \in \mathscr{R}_q^{k+1}$$

GGSW



$$\in \mathscr{R}_q^{(k+1)\times\ell\times(k+1)}$$

- Homomorphic IF
- Vertical packing
- Other advanced algos

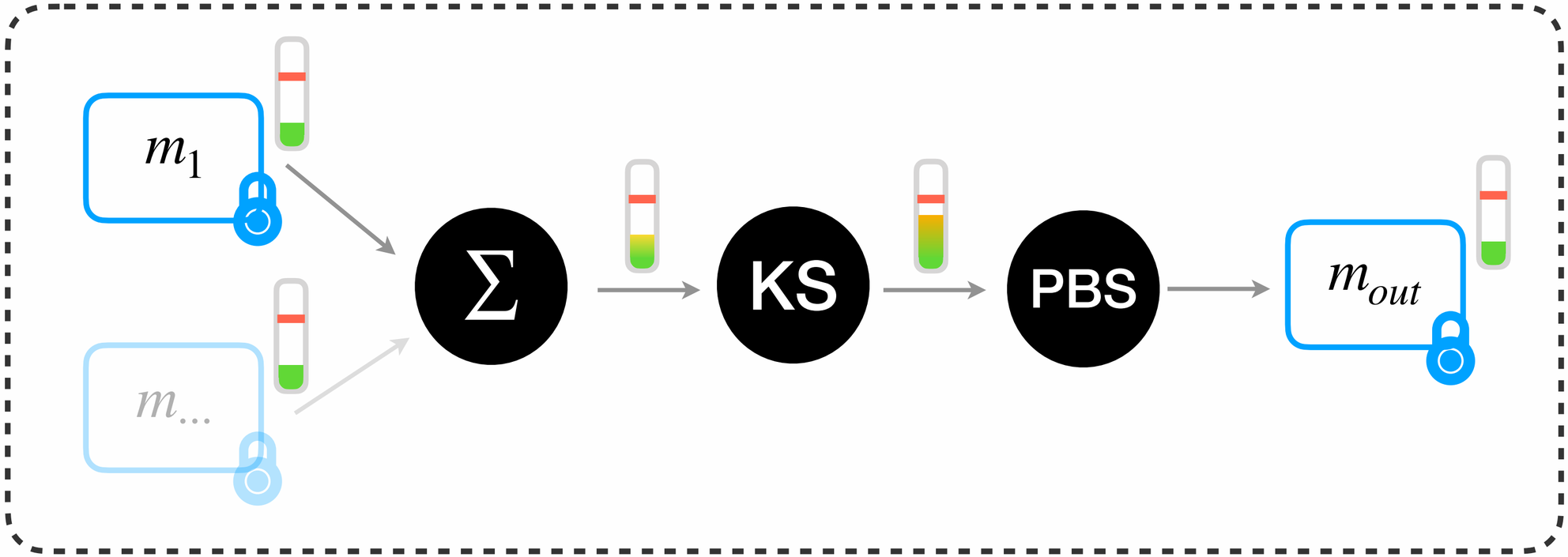
Atomic Pattern

Addition & LUT evaluation ONLY

Graph of integer operations $+$ ✅ $f(\cdot)$ ✅ $\times$ 🤔

$$x \times y = \frac{(x+y)^2}{4} - \frac{(x-y)^2}{4}$$

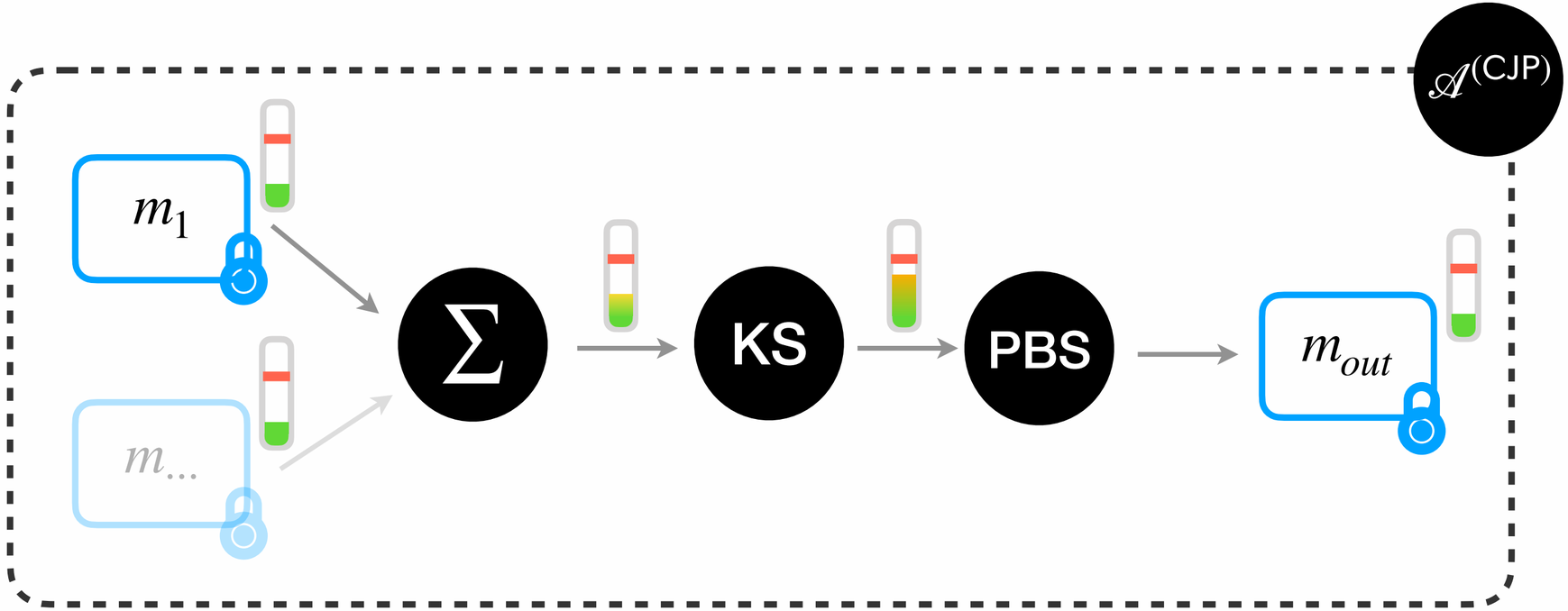
CJP Atomic Pattern



Leveled Operations | Keyswitching | Programmable Bootstrapping

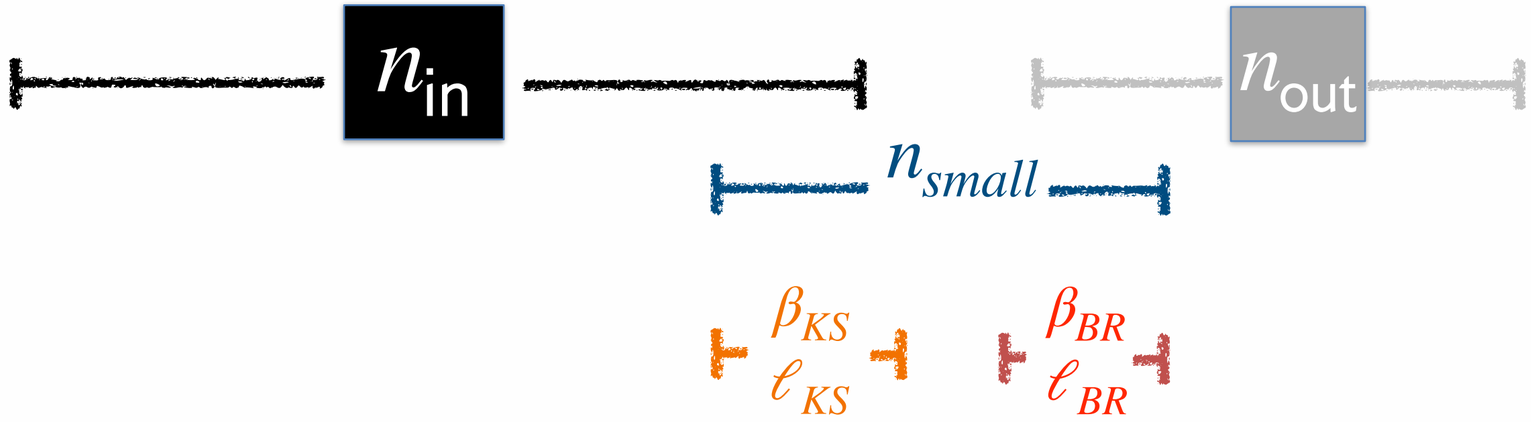
[CJP21] Ilaria Chillotti, Marc Joye, and Pascal Paillier. Programmable bootstrapping enables efficient homomorphic inference of deep neural networks. In CSCML 2021

CJP Atomic Pattern

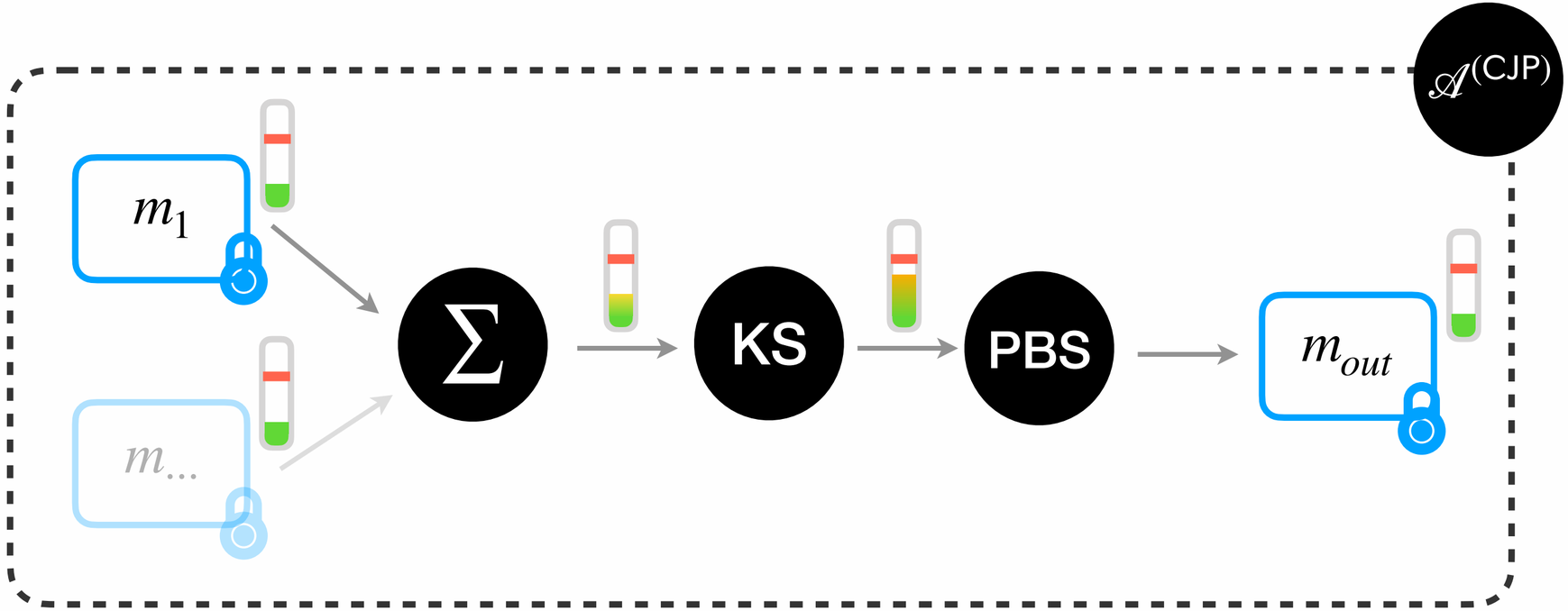


Macro
Parameters

Micro
Parameters

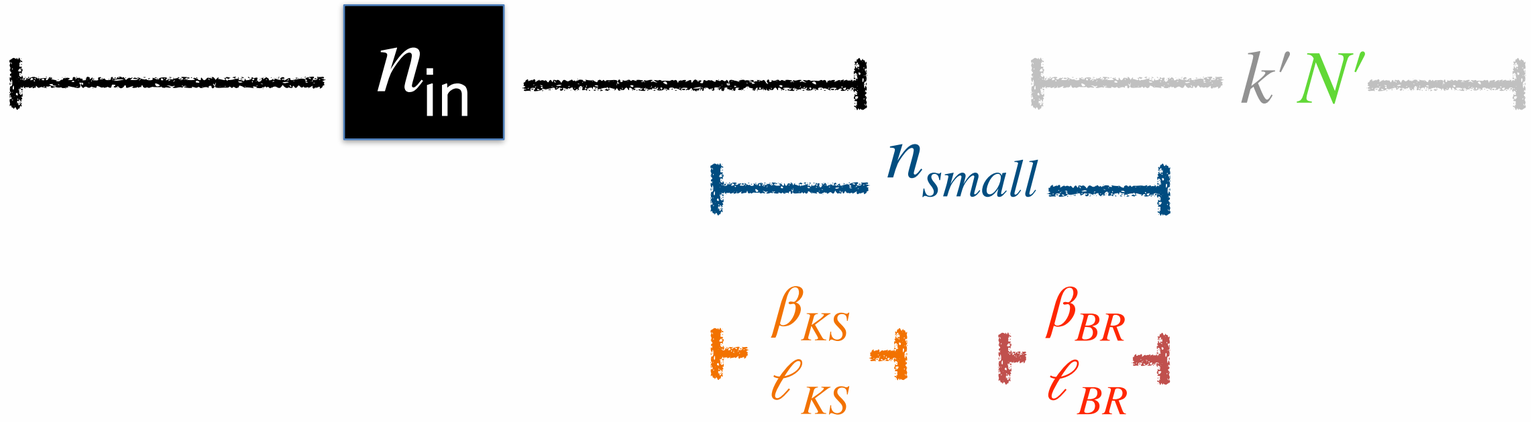


CJP Atomic Pattern

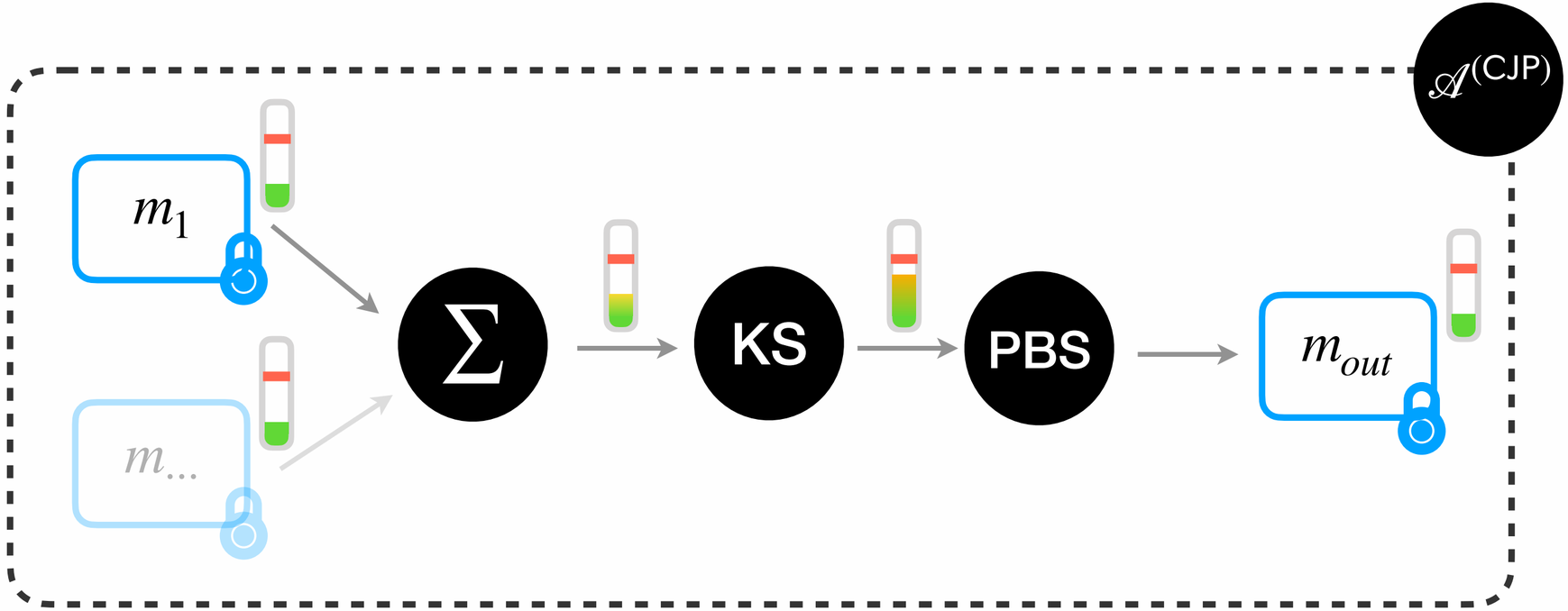


Macro Parameters

Micro Parameters

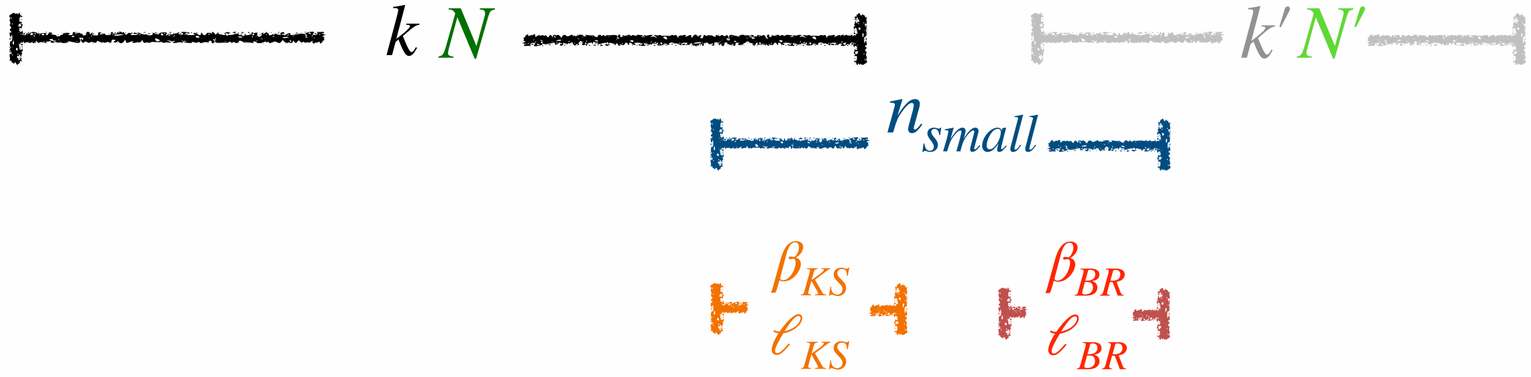


CJP Atomic Pattern

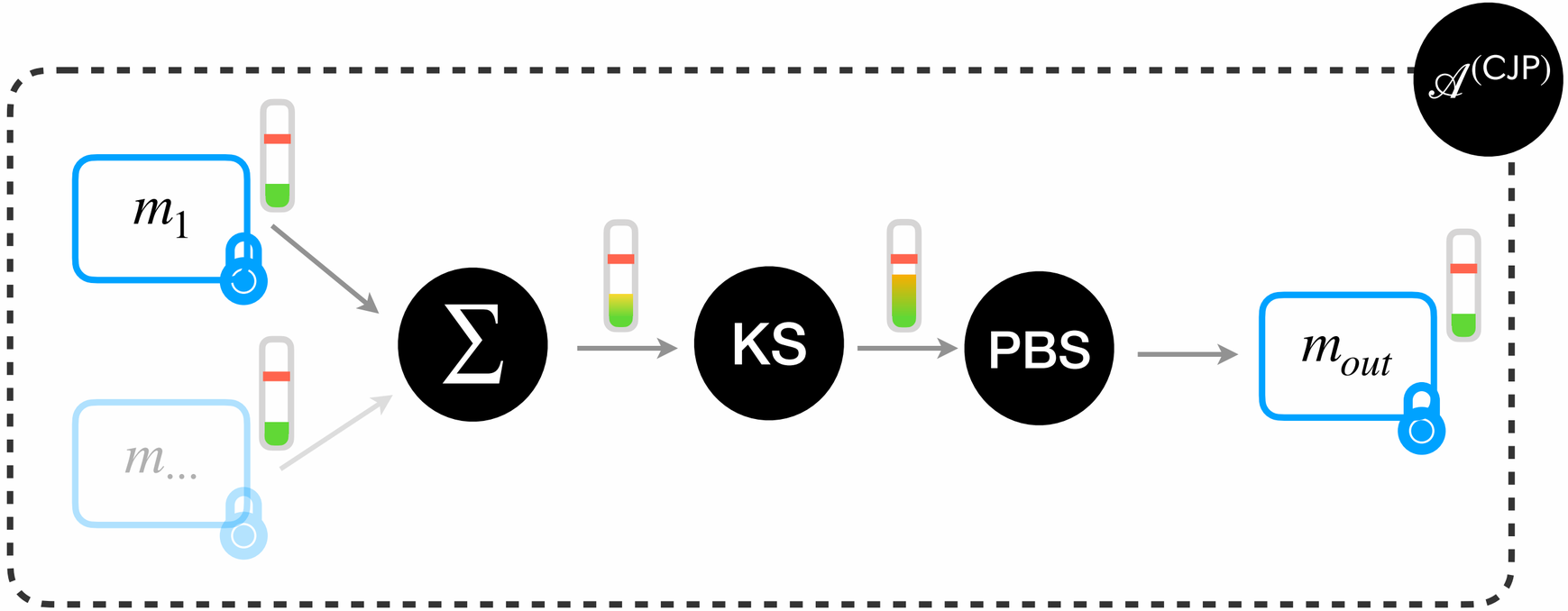


Macro
Parameters

Micro
Parameters

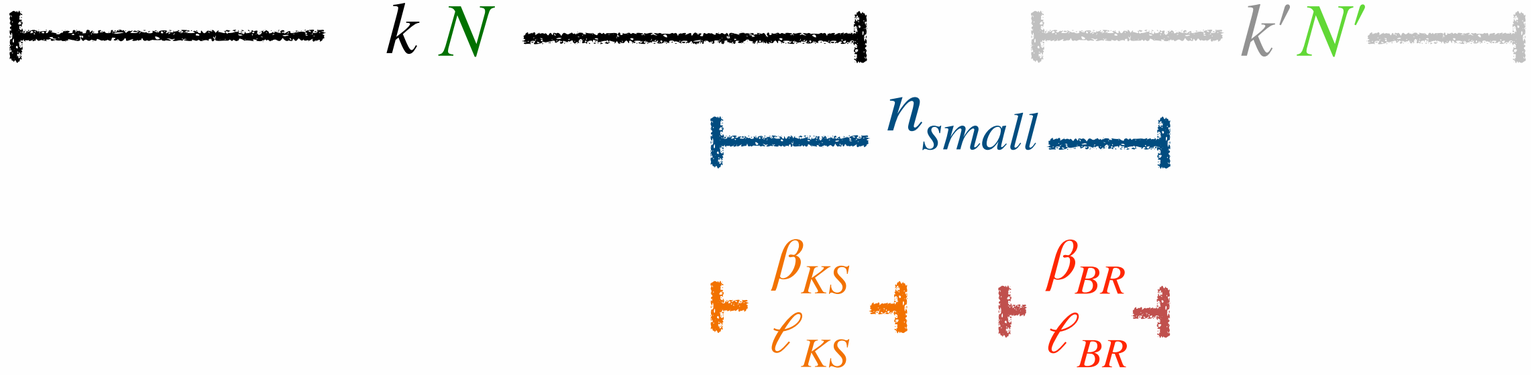


CJP Atomic Pattern



Macro Parameters

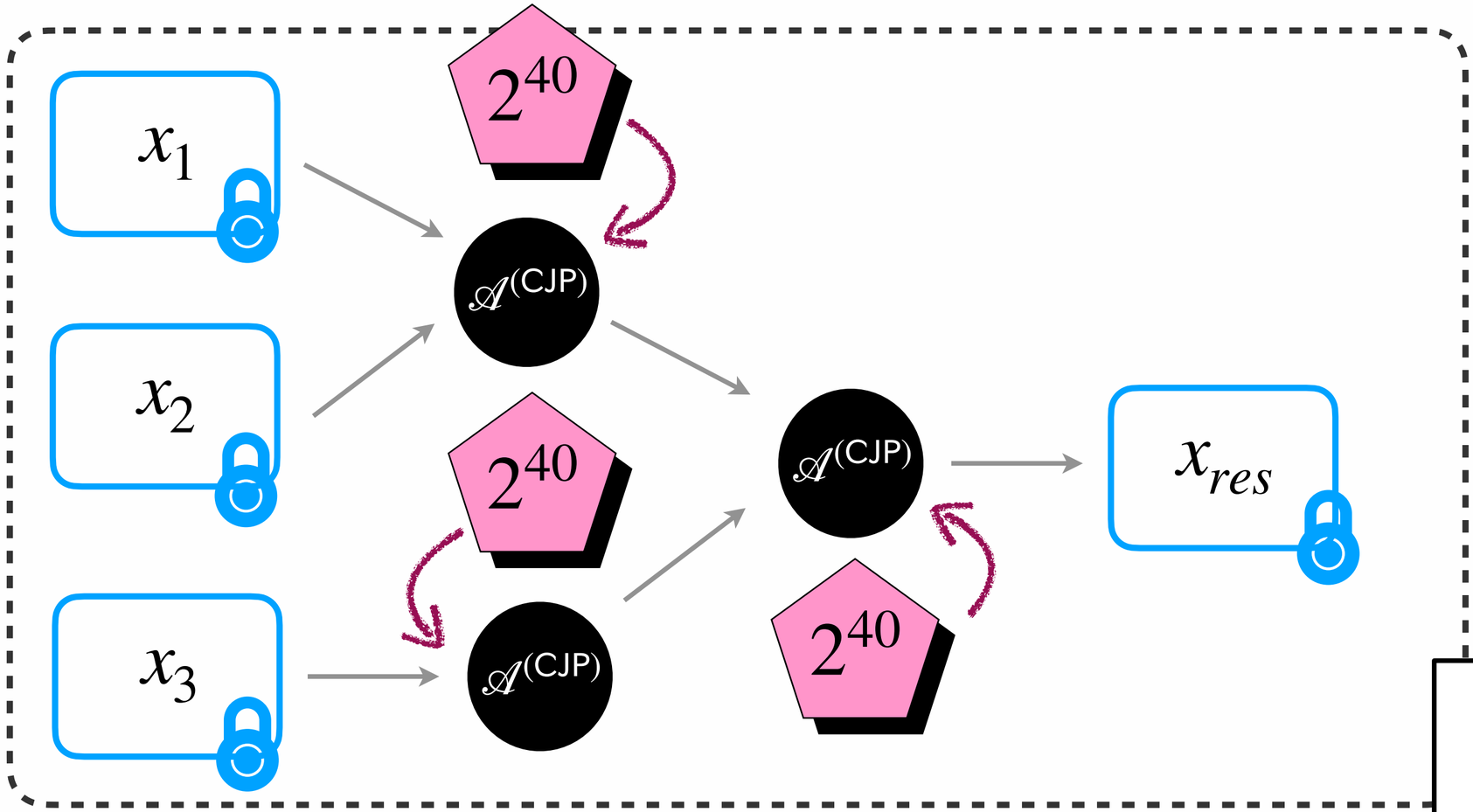
Micro Parameters



$\approx 2^{40}$

possible parameters

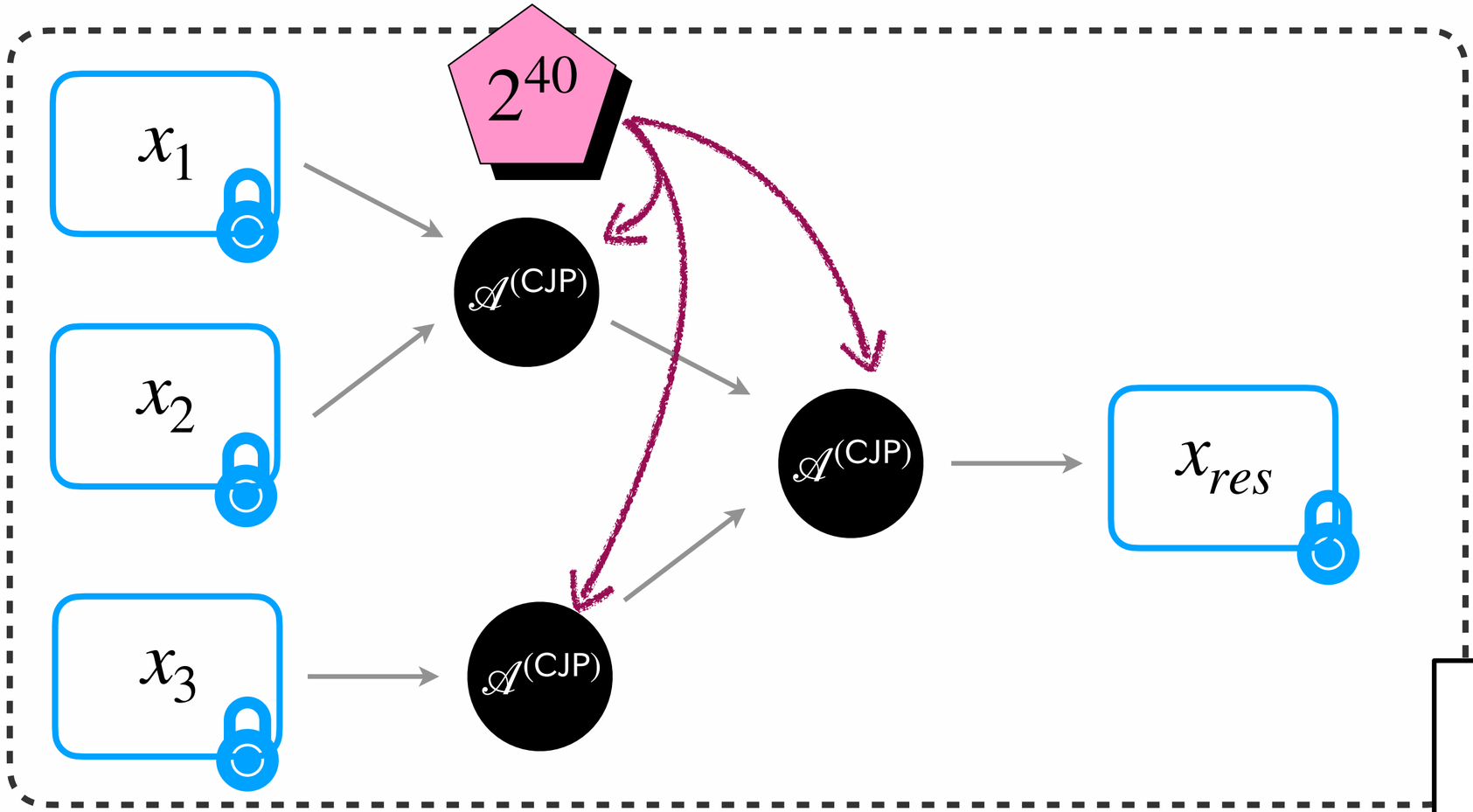
Graph of CJP AP



$\approx 2^{120}$

possible parameters

Graph of CJP AP

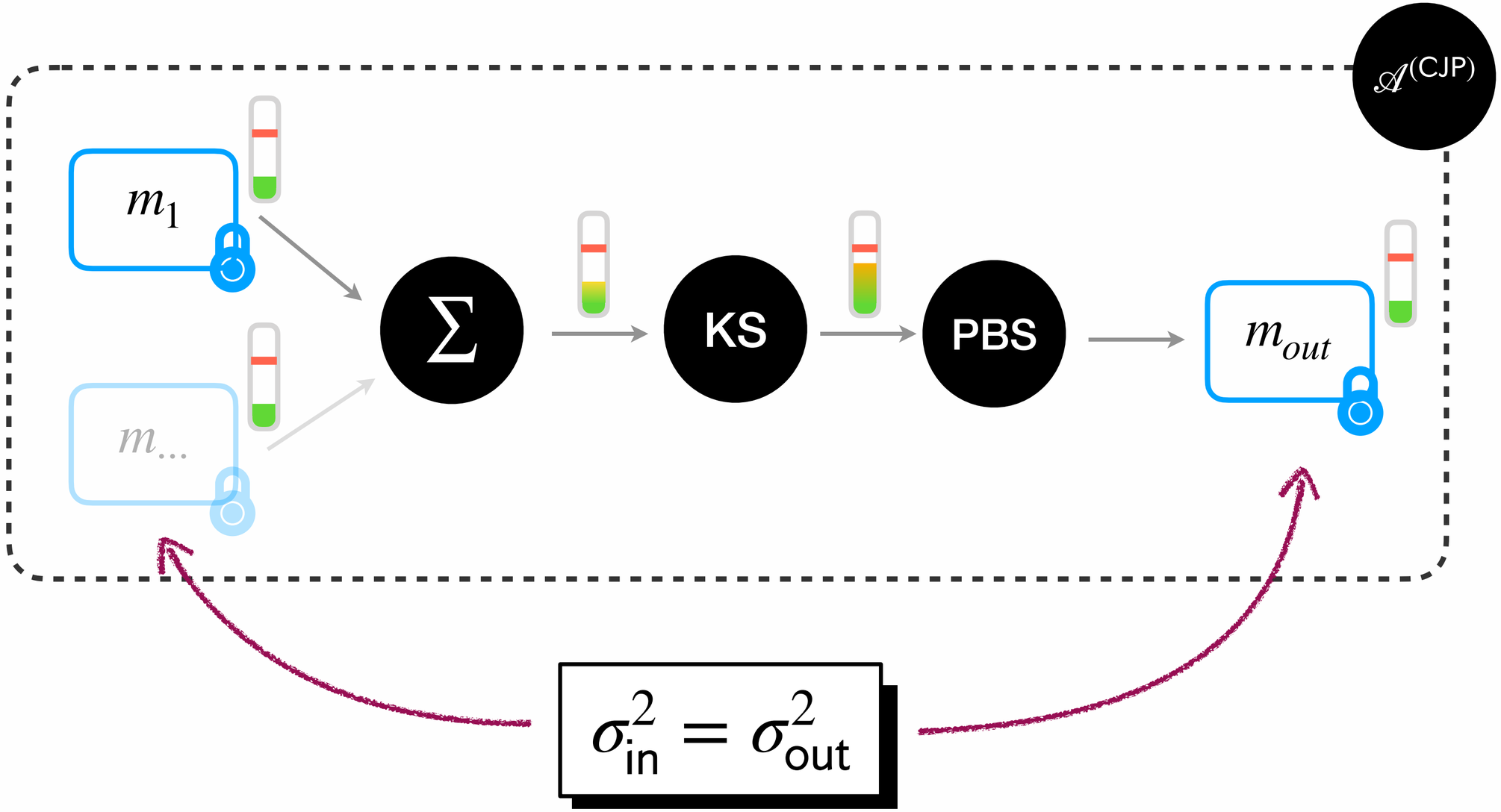


$\approx 2^{40}$

possible parameters

🧠 **1 Parameter set for the whole graph**

Graph of CJP AP



FHE Parameter Optimization

Overview

Overview: Goals

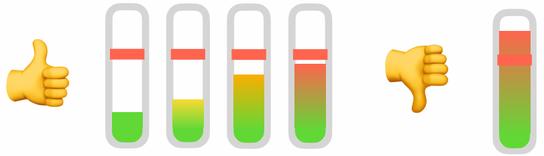
Security

$$f : (n, \lambda, q) \mapsto \sigma_{\text{enc}}$$

LWE dimension — Ciphertext Modulus — Security level — Minimal standard deviation

→ Using the **lattice estimator**

Correctness



→ **Noise Model** to track the noise along the computation

Efficiency

→ **Cost Model** as a surrogate of the execution time

Overview: Problem

Let $\mathcal{G} = \{A_i\}_{i \in I}$

$$\min \text{Cost}(\mathcal{G}) \quad \text{s.t.} \quad \begin{cases} \forall i \in I, \ \text{Noise}(A_i) \leq t^2 \\ \sigma_{\text{enc}} = f(n, \lambda, q) \end{cases}$$

✅ up to a given p_{fail}

Noise bound

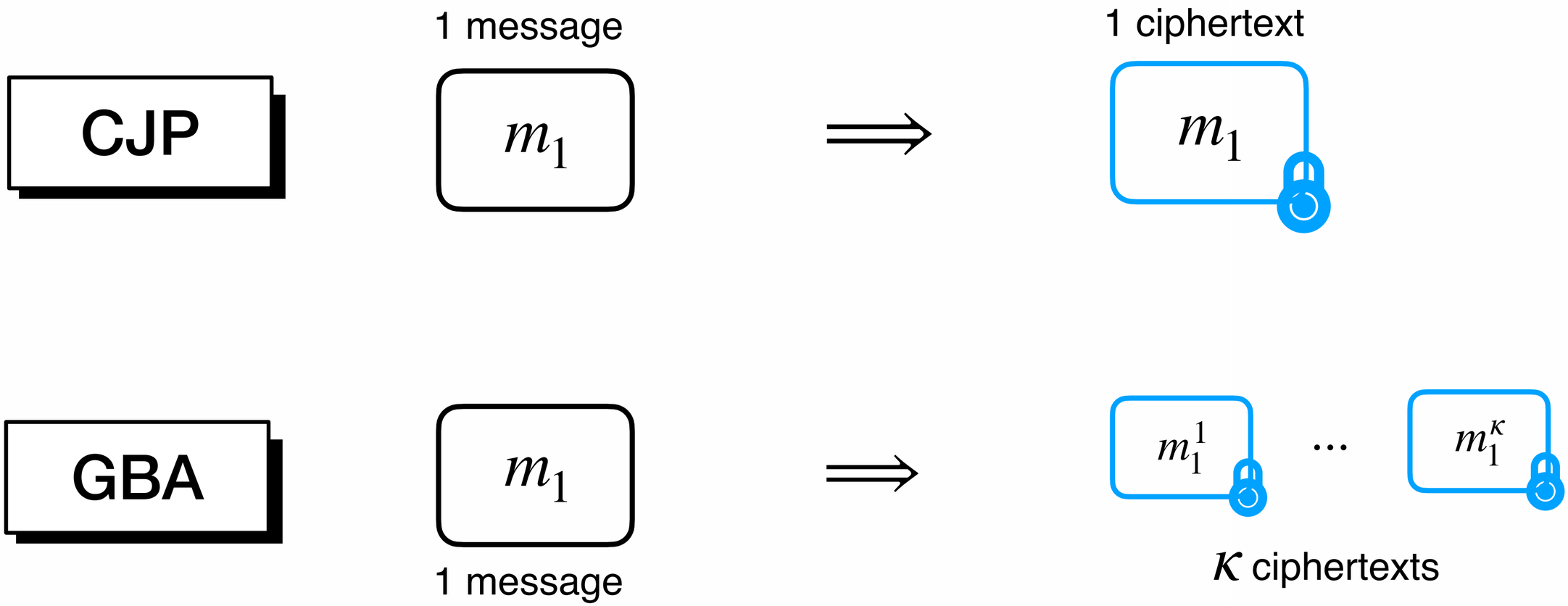
🚀

🔒 λ bits of security

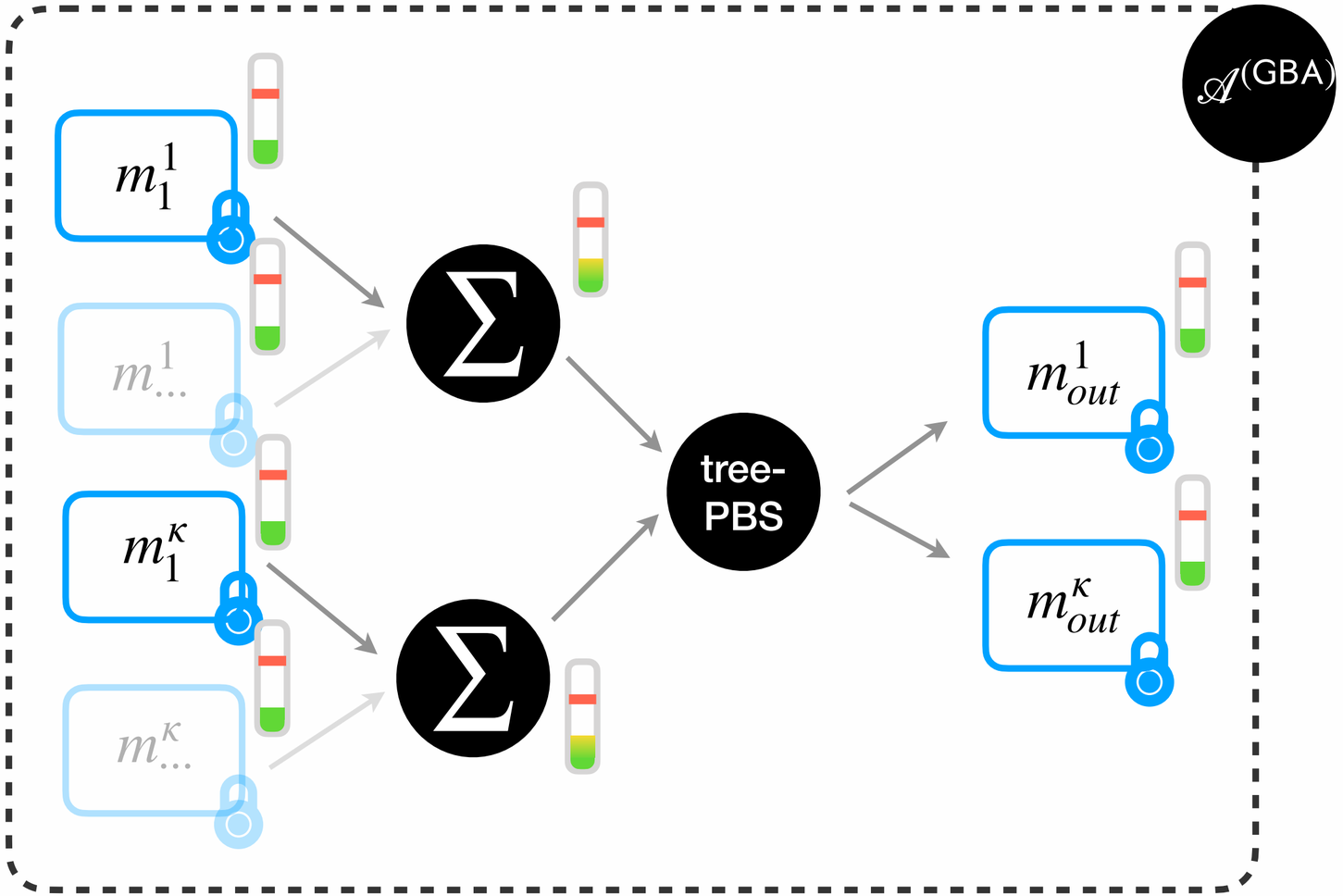
FHE Parameter Optimization

GBA Atomic Pattern

Encoding


CJP
1 message
m_1
1 ciphertext
m_1
GBA
m_1
1 message
m_1^1
...
m_1^κ
κ ciphertexts

GBA Atomic Pattern



$\approx 2^{52}$

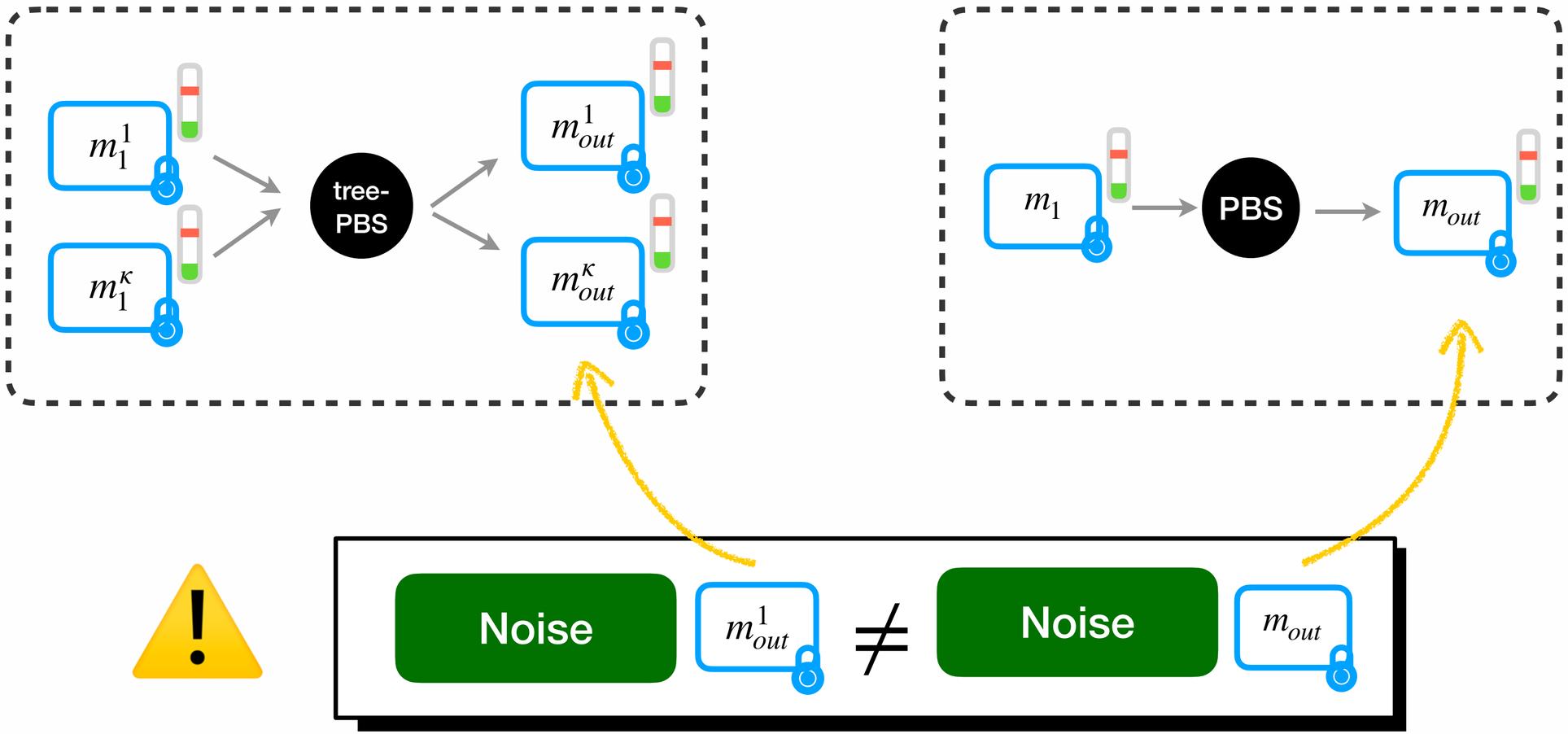
possible parameters

[GBA21] A. Guimaraes, E. Borin, D. Aranha. Revisiting the functional bootstrap in TFHE. IACR Transactions on Cryptographic Hardware and Embedded Systems

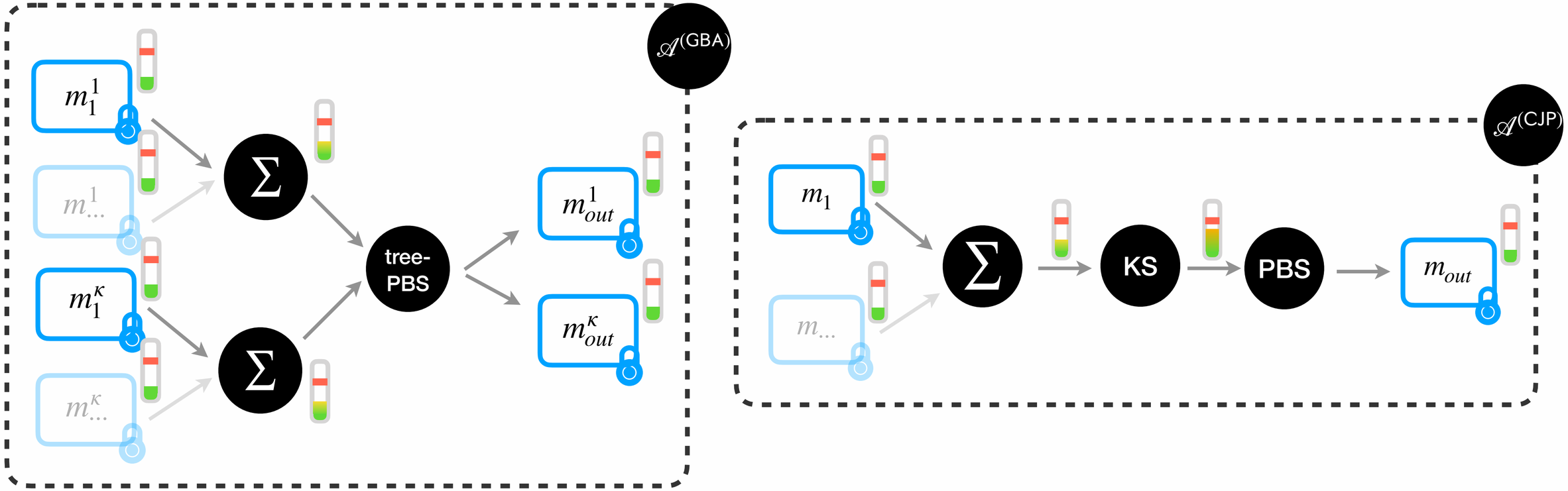
FHE Parameter Optimization

CJP vs GBA

CJP vs GBA

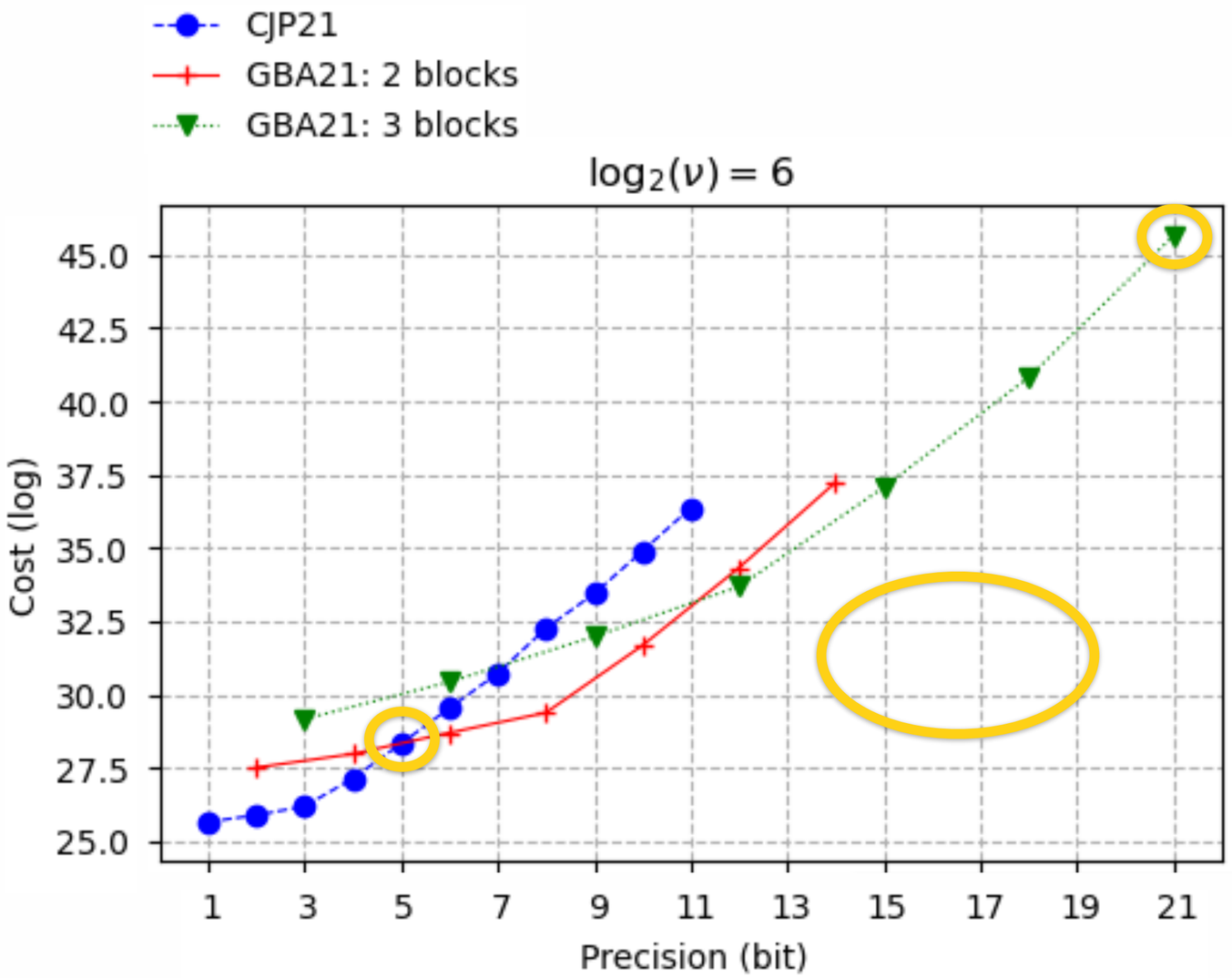

m_1^1
m_1^κ
tree-PBS
m_{out}^1
m_{out}^κ
m_1
PBS
m_{out}
Noise
m_{out}^1
≠
Noise
m_{out}

CJP vs GBA



Context-aware comparison

CJP vs GBA



Efficient alternative to TFHE PBS above **5 bits**

Allows **bigger** precision (up to **21 bits**)

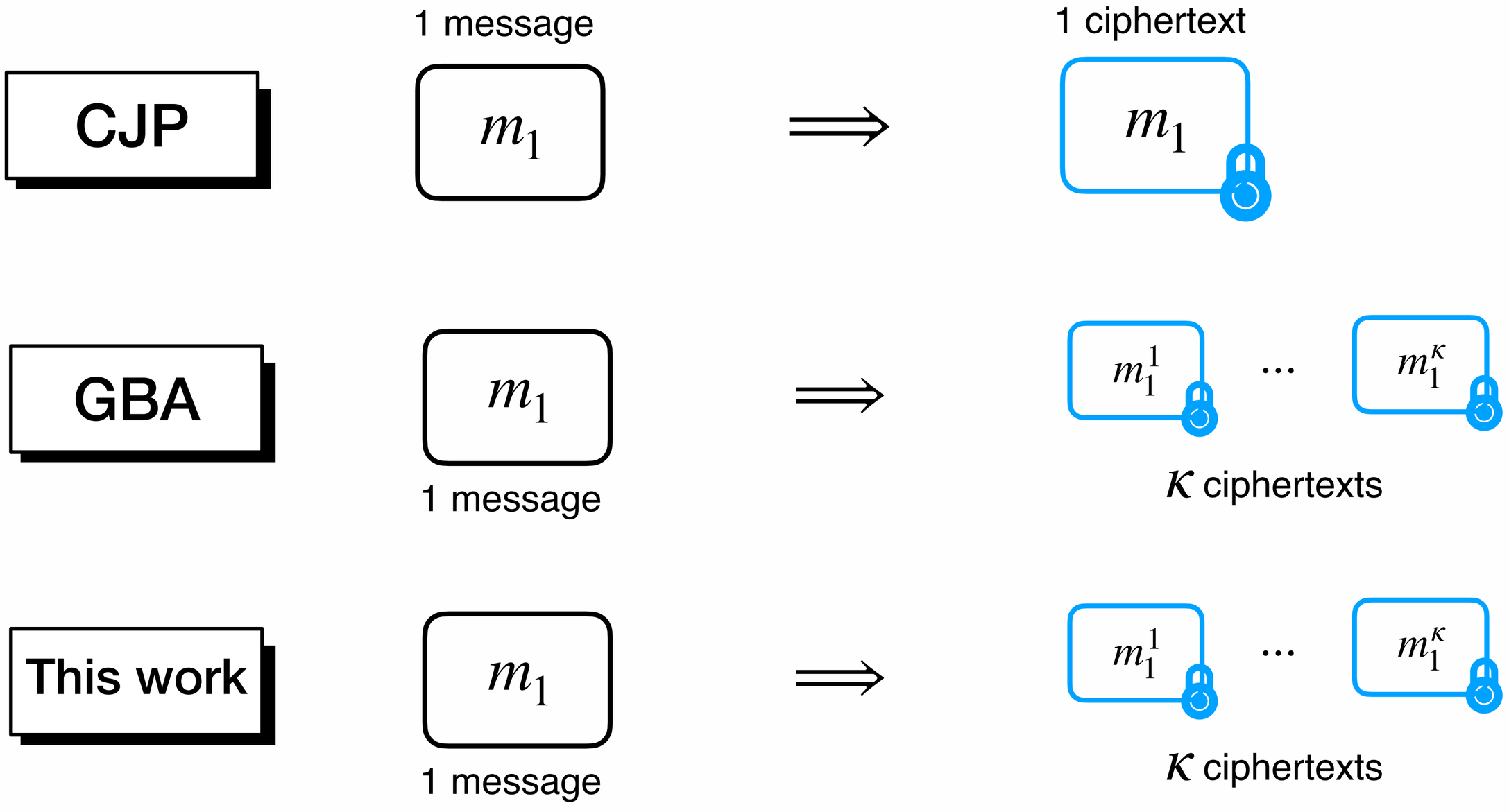
Large precision are **very costly**

$$\text{Cost}(21\ bits) \approx 2^{17} \cdot \text{Cost}(5\ bits)$$

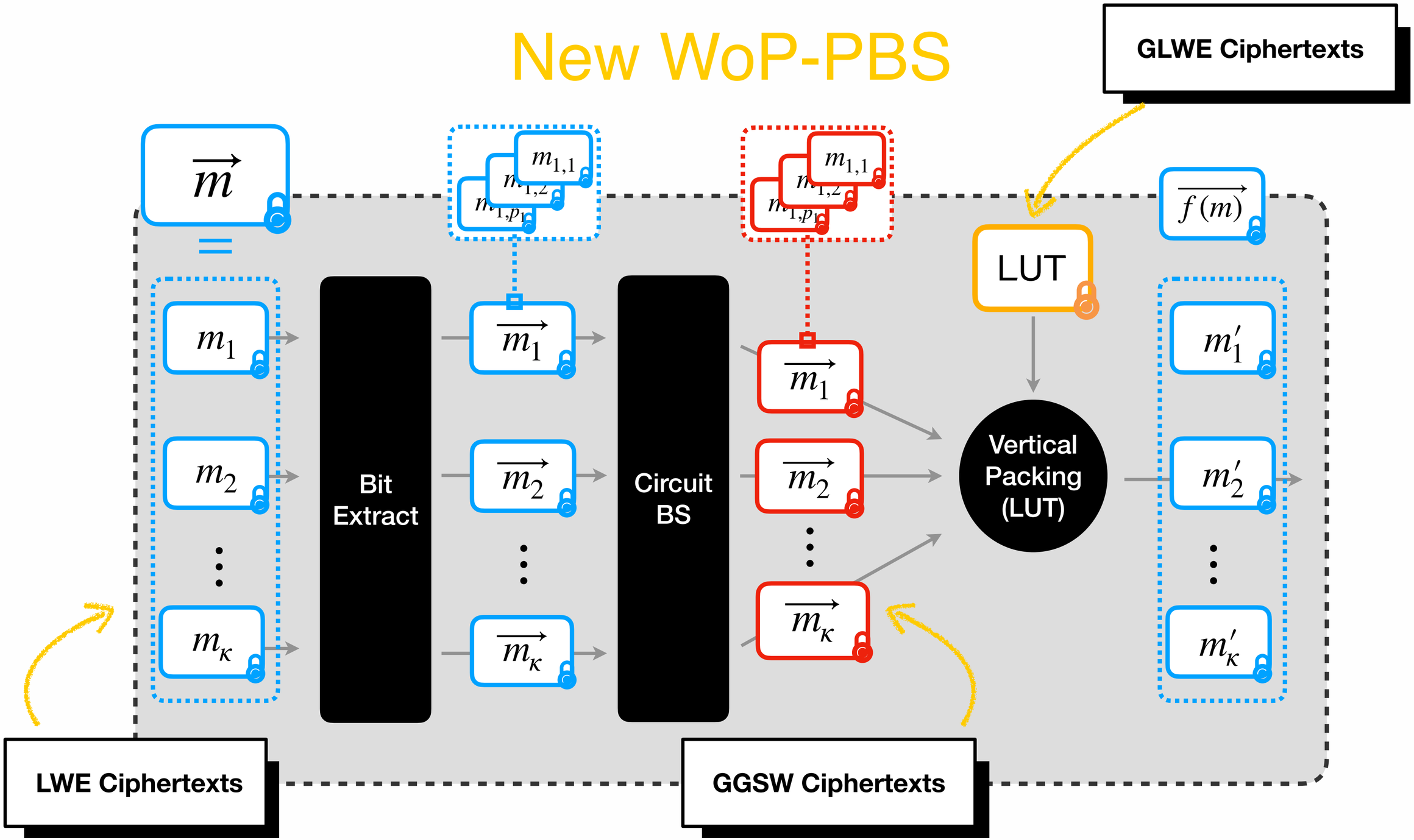
WoP-PBS

Overview

Encoding


1 message
1 ciphertext
CJP
m_1
m_1
GBA
m_1
m_1^1 ... m_1^κ
1 message
κ ciphertexts
This work
m_1
m_1^1 ... m_1^κ
1 message
κ ciphertexts

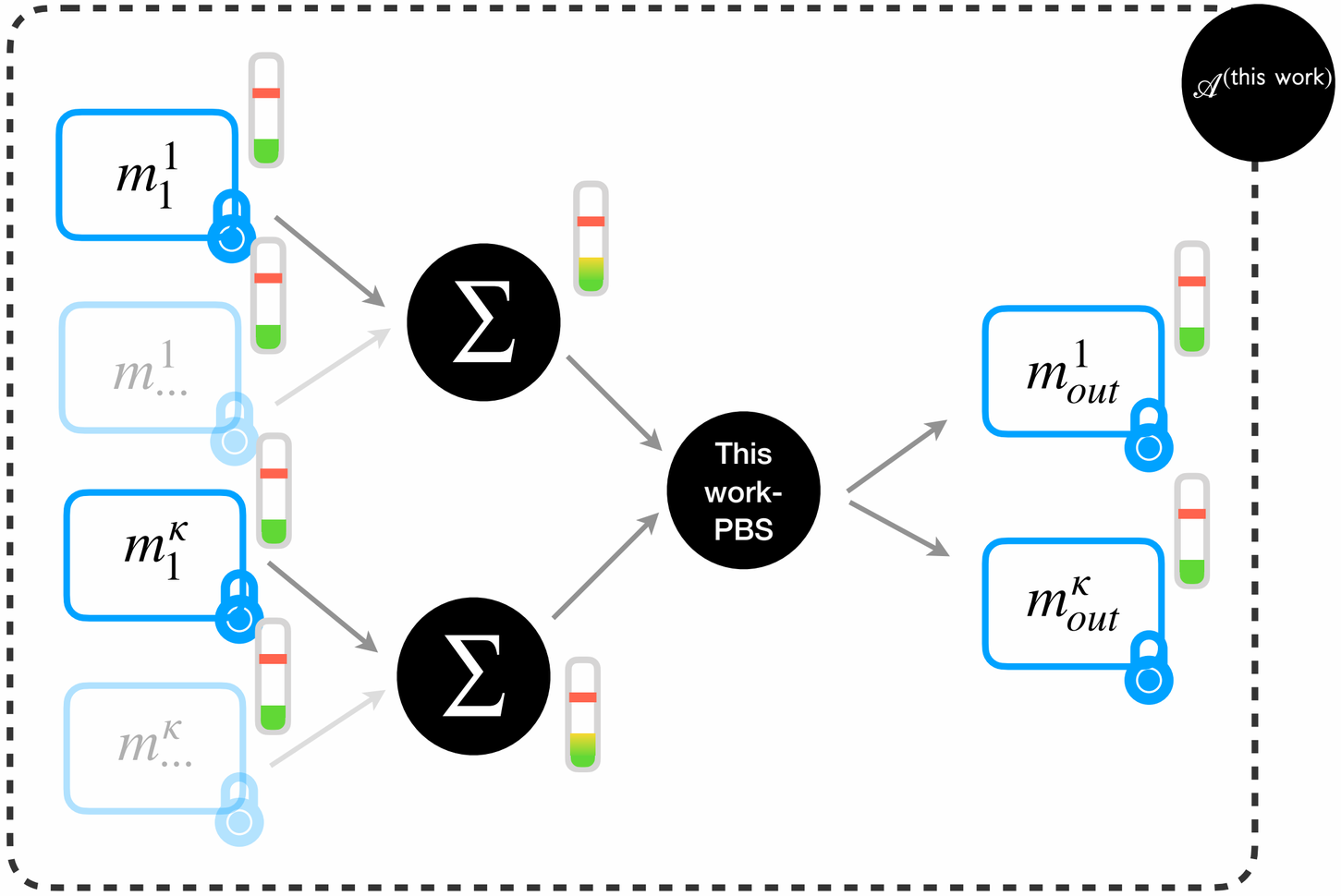
New WoP-PBS


GLWE Ciphertexts
LUT
Bit Extract
Circuit BS
Vertical Packing (LUT)
LWE Ciphertexts
GGSW Ciphertexts

WoP-PBS

Comparisons

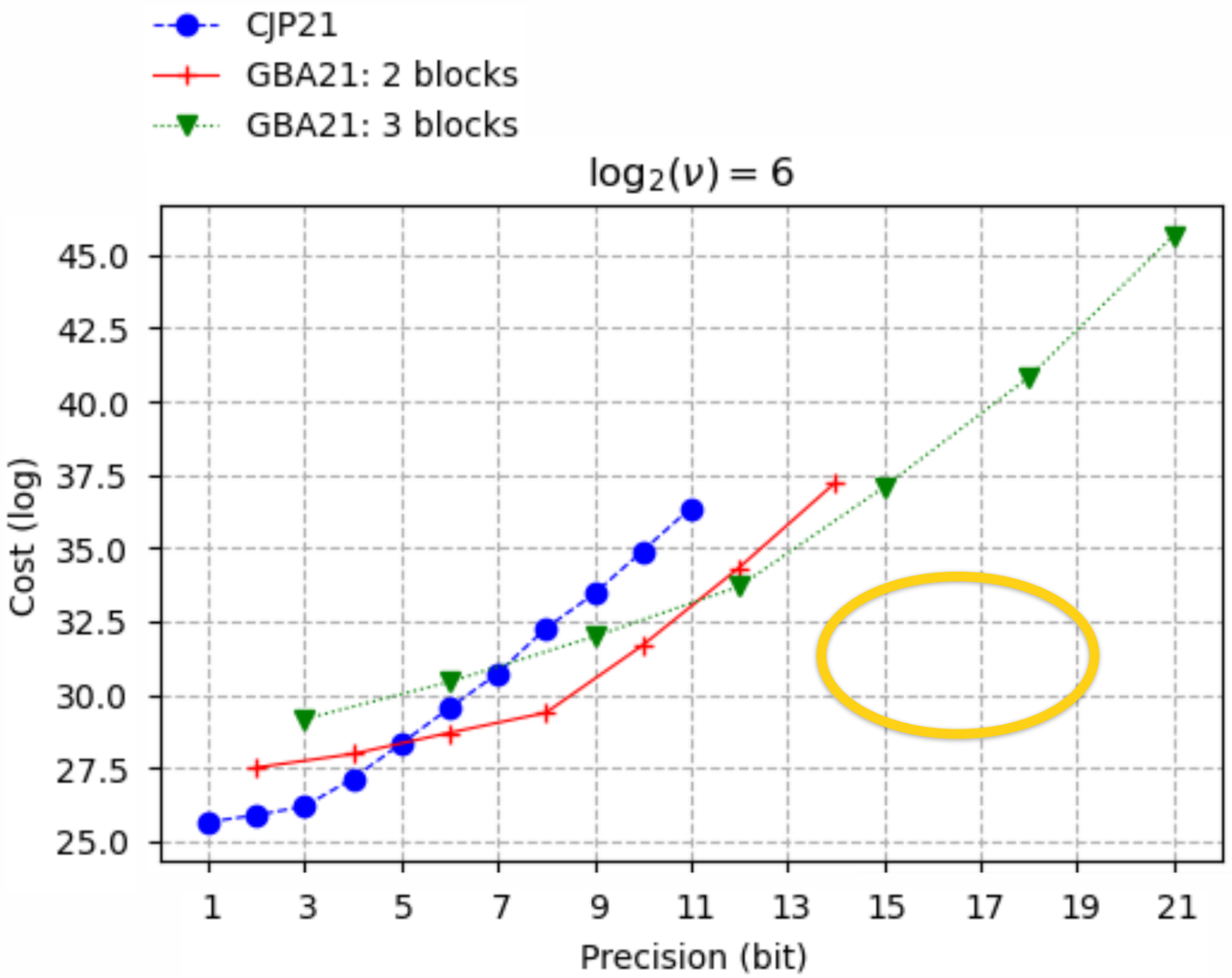
This work Atomic Pattern



$\approx 2^{64}$

possible parameters

CJP vs GBA



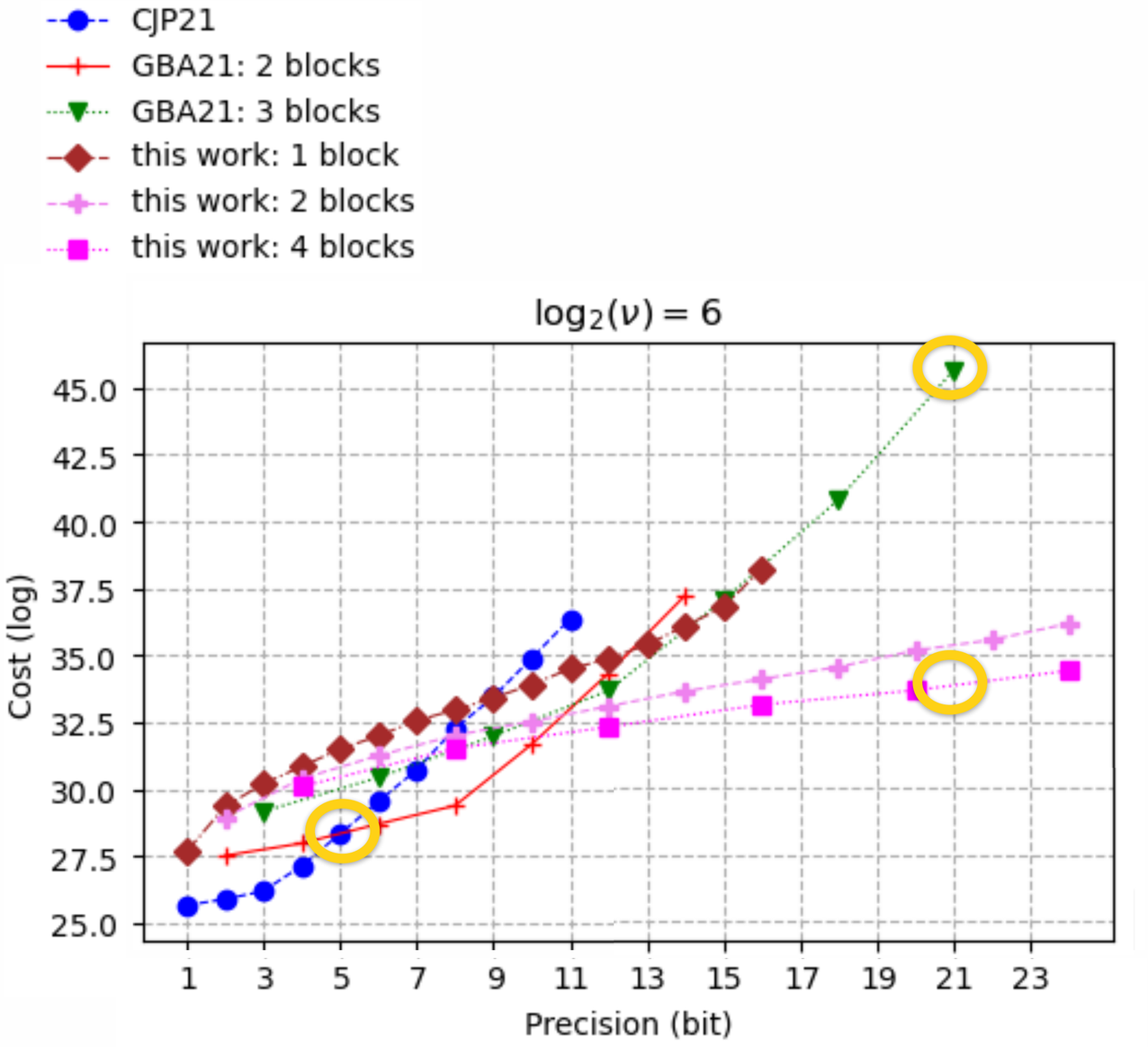
Efficient alternative to TFHE PBS above **5 bits**

Allows **bigger** precision (up to **21 bits**)

Large precision are **very costly**

$$\text{Cost}(21\ bits) \approx 2^{17} \cdot \text{Cost}(5\ bits)$$

CJP vs GBA vs this work



Efficient alternative to GBA-PBS above **10 bits**

Allows **bigger** precision (up to **24 bits**)

Large precision are **less costly**

$$\text{Cost}(21\ bits) \approx 2^{17} \cdot \text{Cost}(5\ bits)$$
$$\approx 2^{12} \cdot \text{Cost}(5\ bits)$$

Conclusion

Other results

Other results

Large Integers

CRT, radix, hybrid encoding

Failure Probability

AP and graph level

PBS Insertion

In Dot Product

WoP-PBS Analysis

LMP, this work

KS Position

CJP, CGGI, KS-free

Several KSK/BSK

CJP

Conclusion

Future Work

Future Work

Better Cost Model

In the paper: algorithmic complexities

Better Noise Model

In the paper: from [CLOT21]

Multi Parameter Sets

In the paper: only one parameter set

Graph Comparison

Real use cases

Bibliography

[CGGI20] I. Chillotti, N. Gama, M. Georgieva, M. Izabachène. TFHE: Fast Fully Homomorphic Encryption over the Torus. Journal of Cryptology 2020.

[CJP21] Ilaria Chillotti, Marc Joye, and Pascal Paillier. Programmable bootstrapping enables efficient homomorphic inference of deep neural networks. In CSCML 202

[CLOT21] I. Chillotti, D. Ligier, J-B Orfila, and S. Tap. Improved programmable bootstrapping with larger precision and efficient arithmetic circuits for tfhe. In ASIACRYPT 2021

[GBA21] A. Guimaraes, E. Borin, D. Aranha. Revisiting the functional bootstrap in TFHE. IACR Transactions on Cryptographic Hardware and Embedded Systems

[LMP21] Zeyu Liu, Daniele Micciancio, and Yuriy Polyakov. Large-precision homomorphic sign evaluation using fhew/tfhe bootstrapping. Cryptology ePrint Archive, Report 2021/1337

Thank you.

ZAMA

Contact and Links

ilaria.chillotti@zama.ai
damien.ligier@zama.ai

zama.ai

Github

Community links

Want to know more about this work?
https://eprint.iacr.org/2022/704.pdf

ZAMA