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

26 March 2023

Parameter Optimization & Larger Precision for (T)FHE

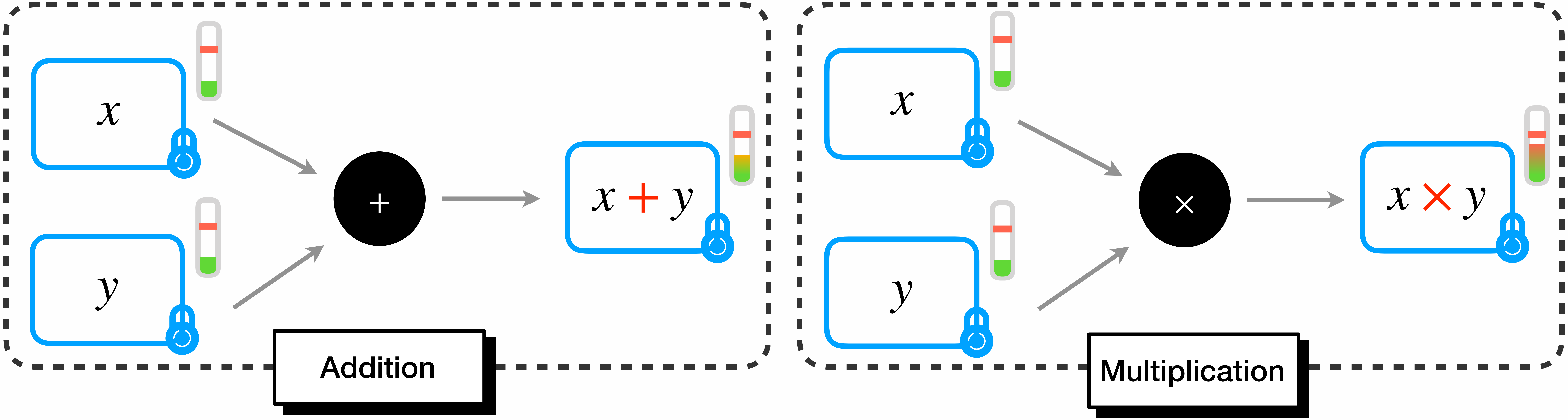
ZAMA

Agenda

Introduction	04
FHE Parameter Optimization	07
WoP-PBS	09
Conclusion	11

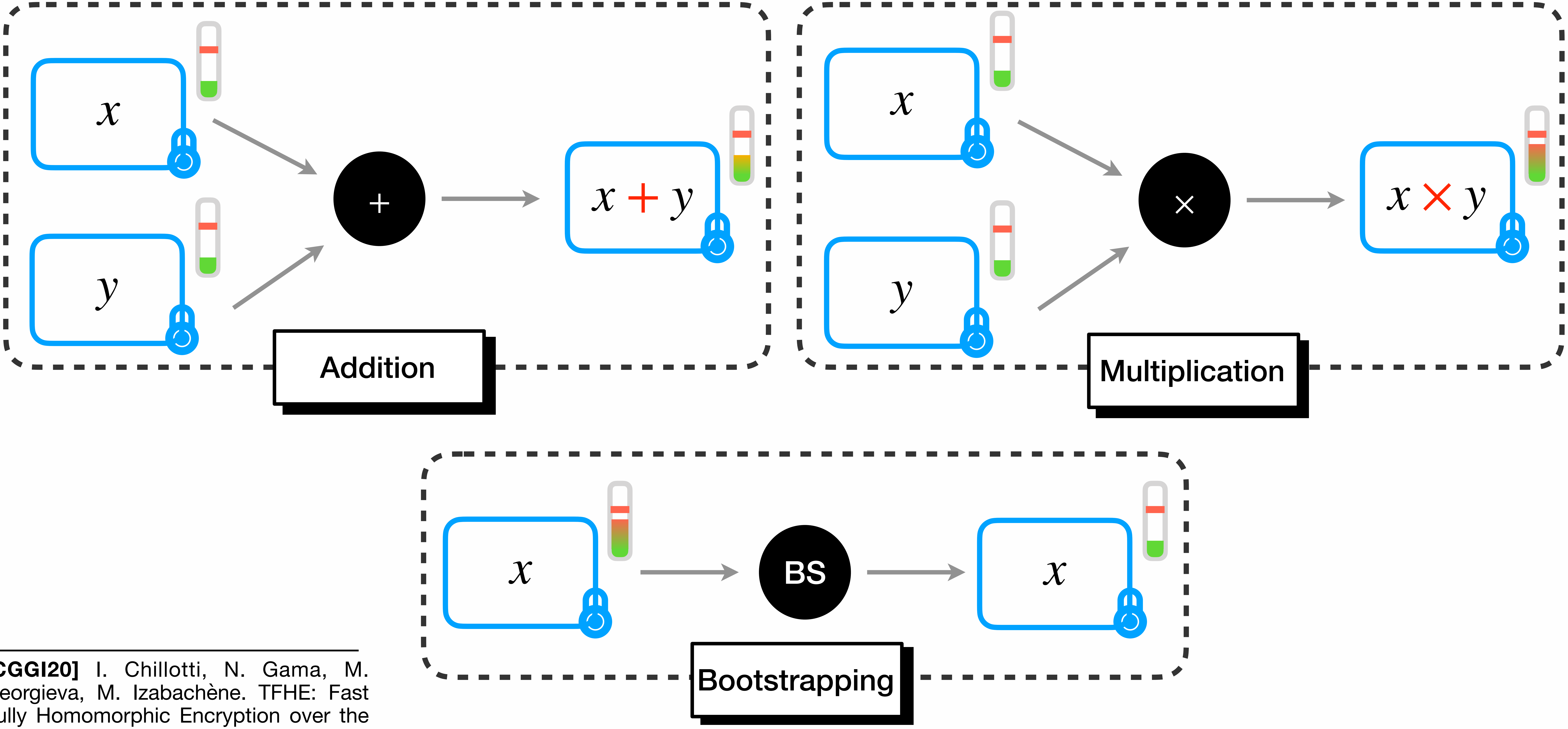
Introduction

FHE



too much noise 🥵 $\Longrightarrow$ incorrect decryption

FHE



x

y

$+$

$x + y$

Addition

x

y

$\times$

$x \times y$

Multiplication

x

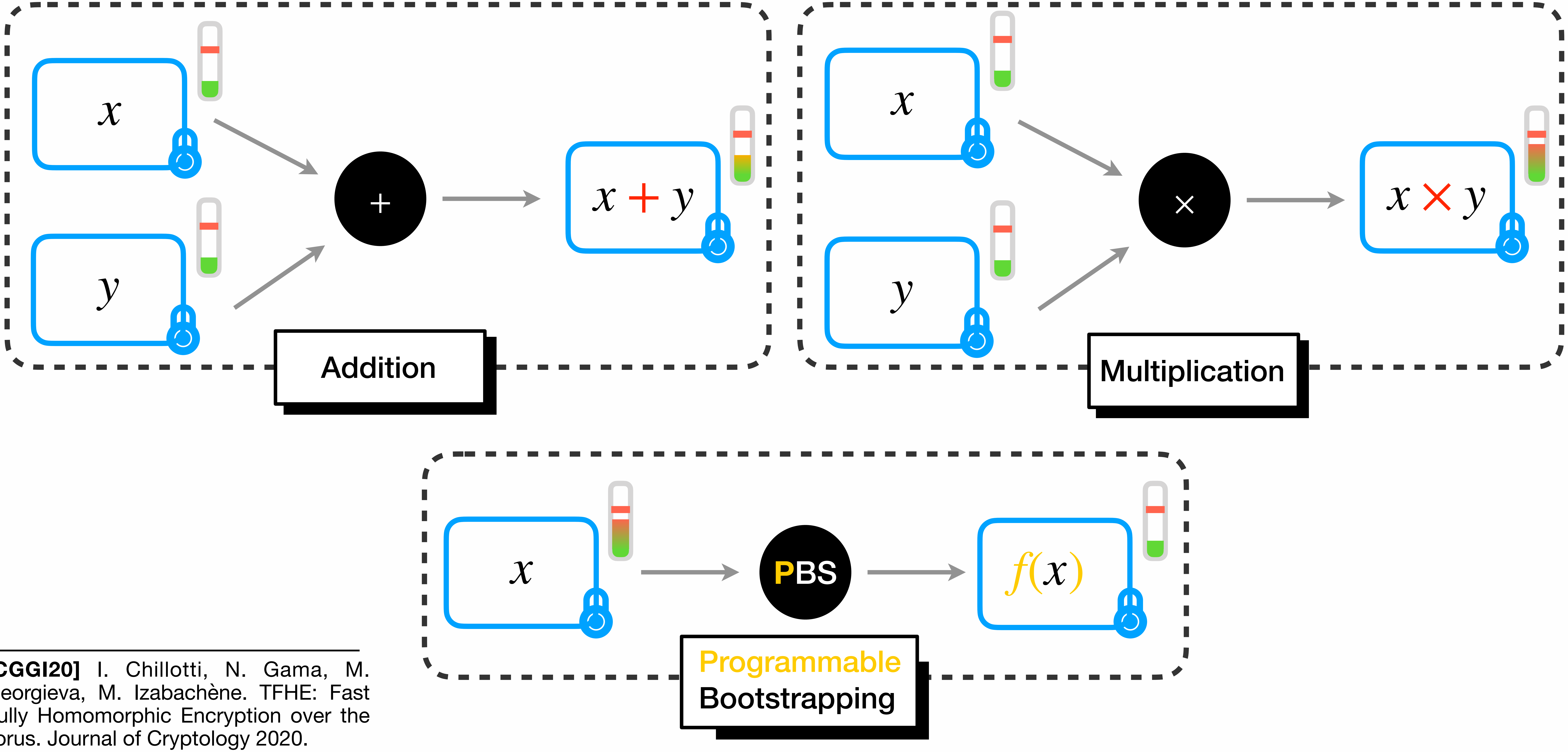
BS

x

Bootstrapping

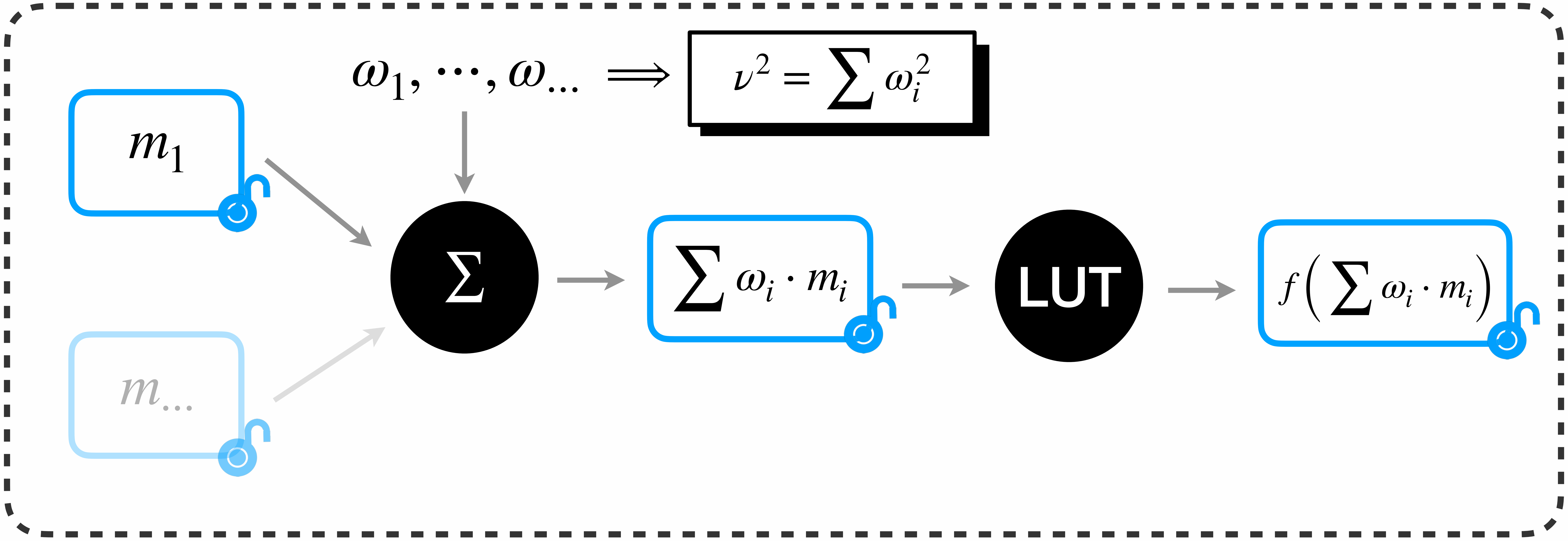
[CGGI20] I. Chillotti, N. Gama, M. Georgieva, M. Izabachène. TFHE: Fast Fully Homomorphic Encryption over the Torus. Journal of Cryptology 2020.

FHE



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

Plain Atomic Pattern



m_1
$m_{\dots}$
$\omega_1, \cdots, \omega_{\dots} \Longrightarrow$
$\nu^2 = \sum \omega_i^2$
Σ
$\sum \omega_i \cdot m_i$
LUT
$f\left(\sum \omega_i \cdot m_i\right)$

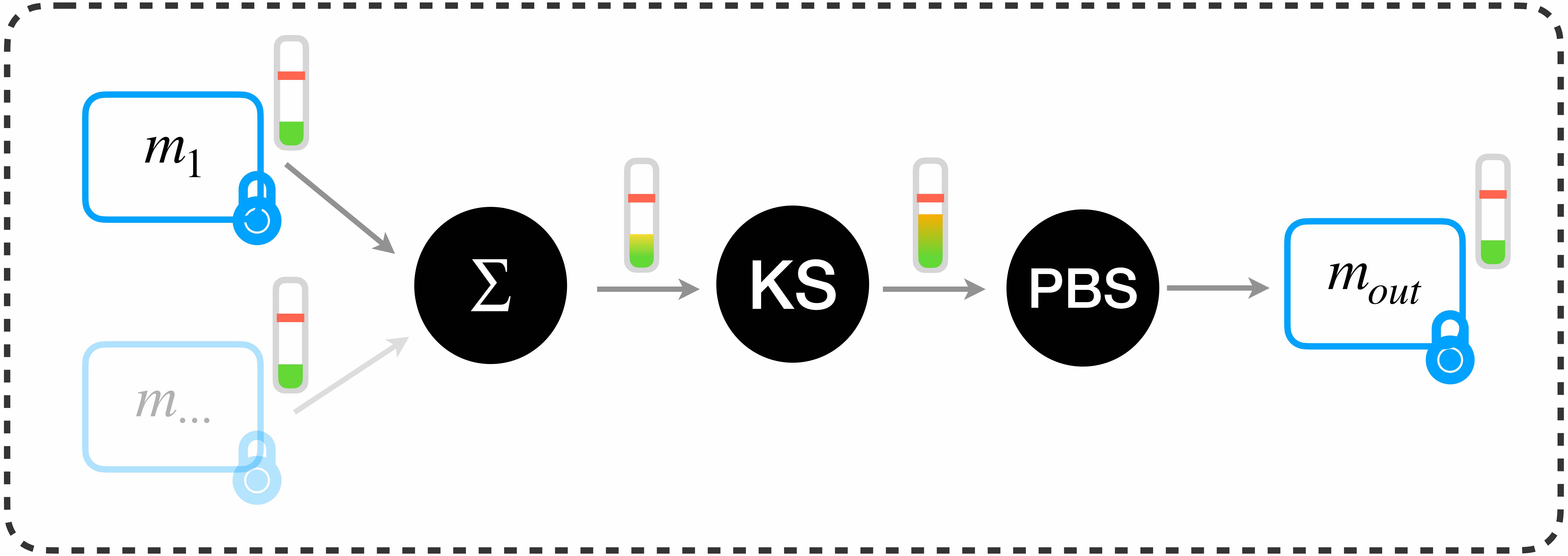
Symbolic Rewriting

Easy to transform a computation graph into a graph of atomic patterns

Recurrent Pattern

Enable simple analysis

CJP Atomic Pattern



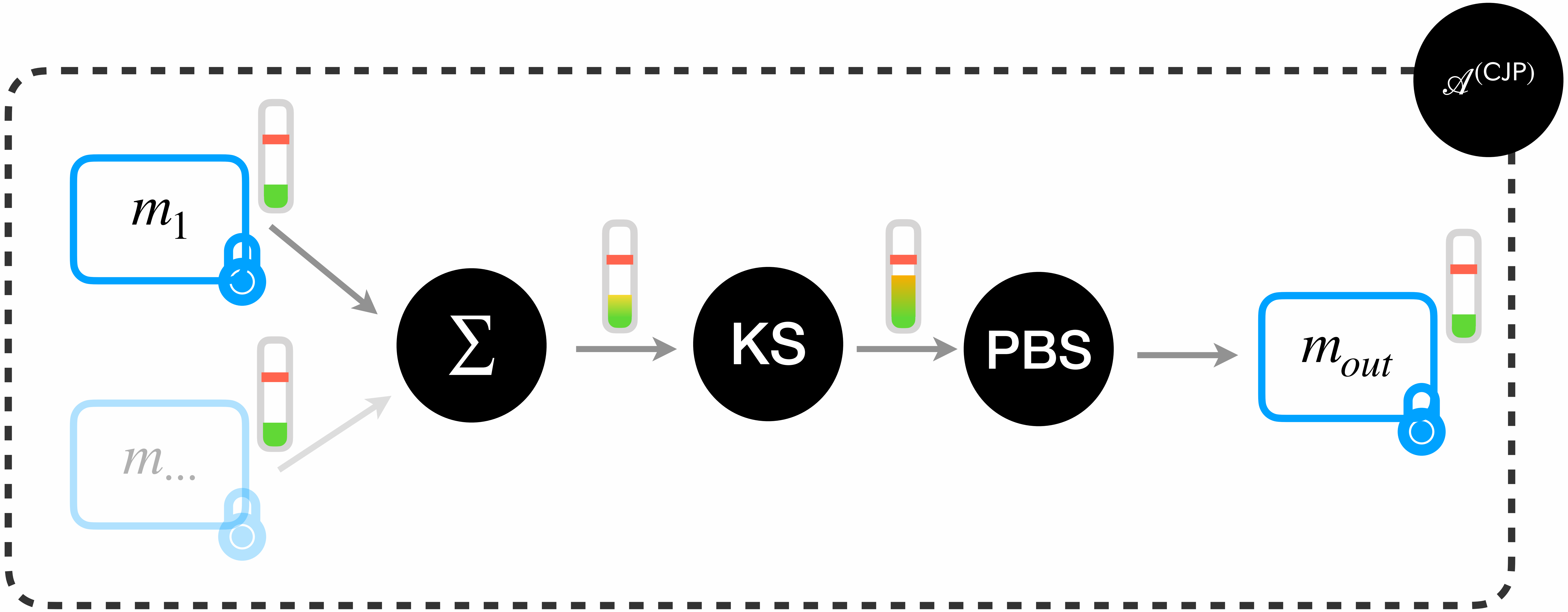
Leveled Operations

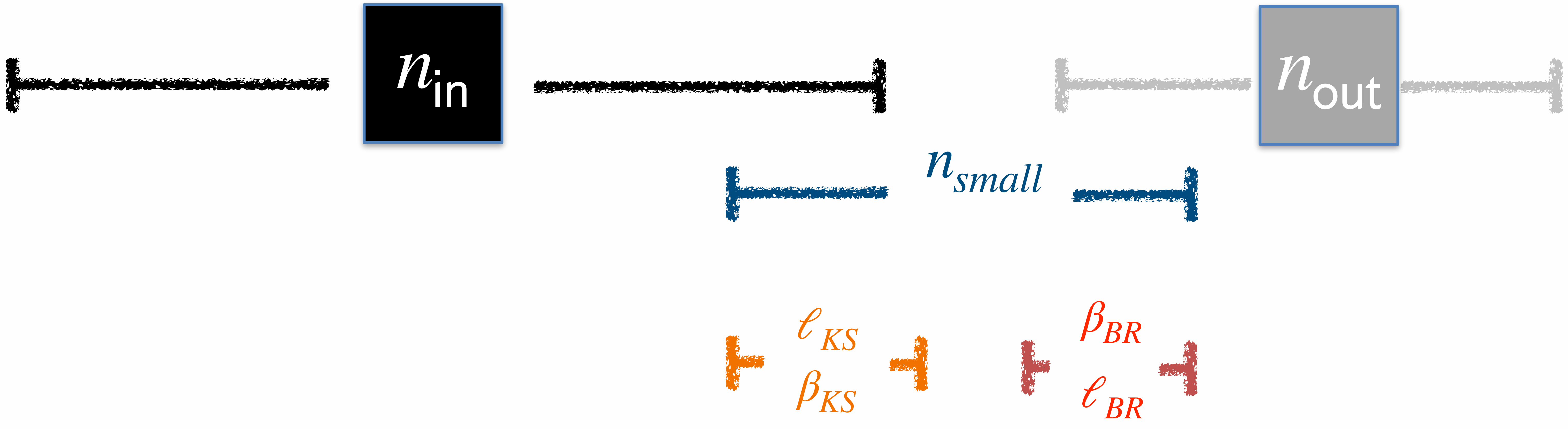
Keyswitching

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





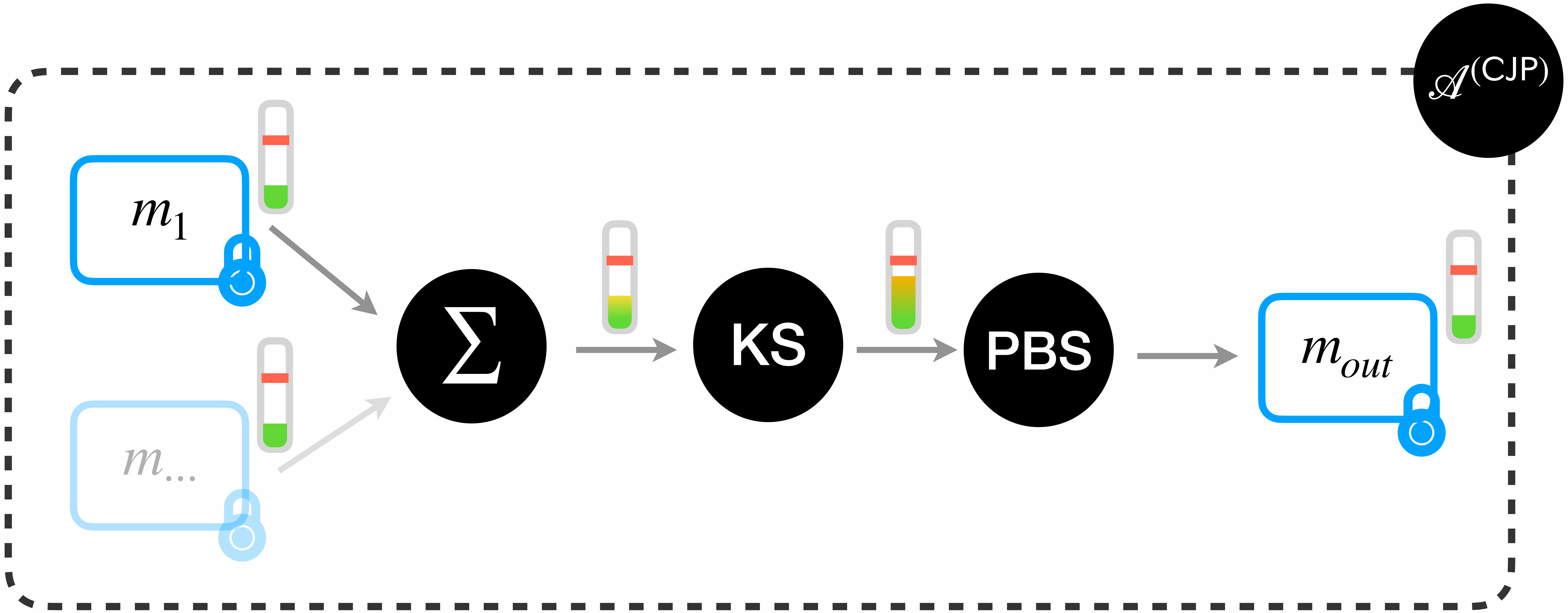
Macro
Parameters

Micro
Parameters

$\approx 2^{40}$

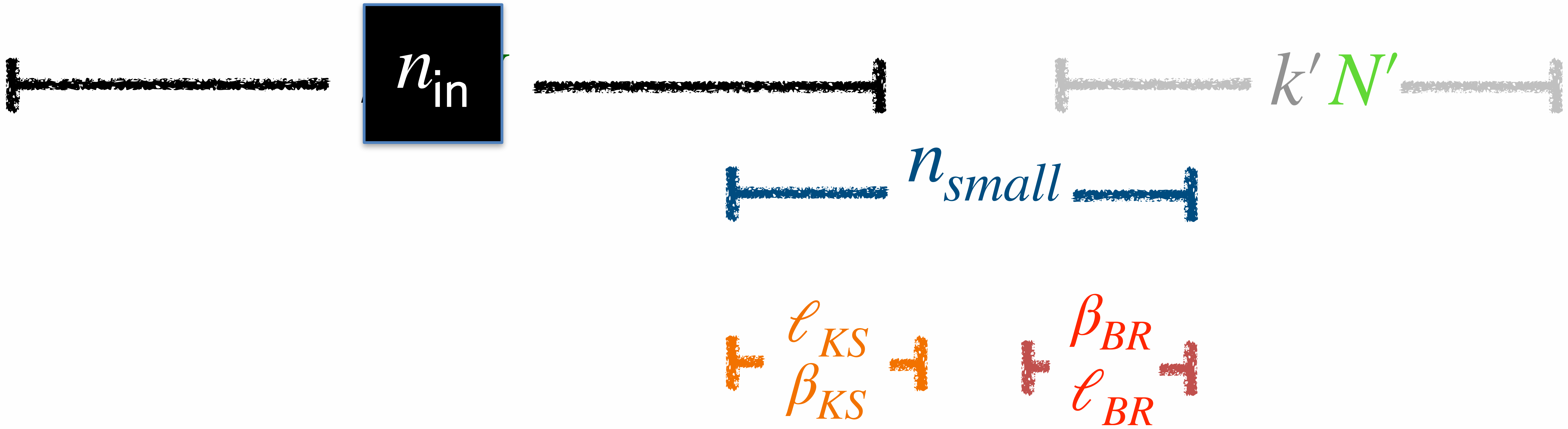
possible parameters

CJP Atomic Pattern



Macro
Parameters

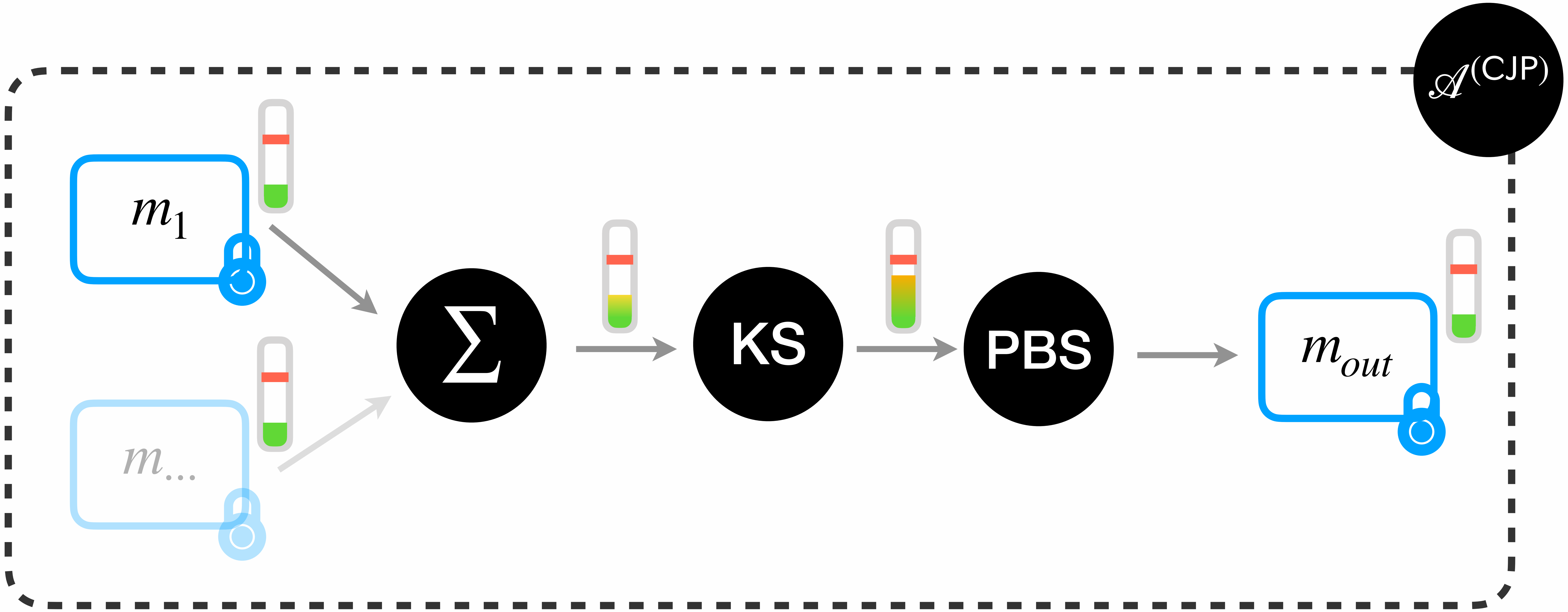
Micro
Parameters



$\approx 2^{40}$

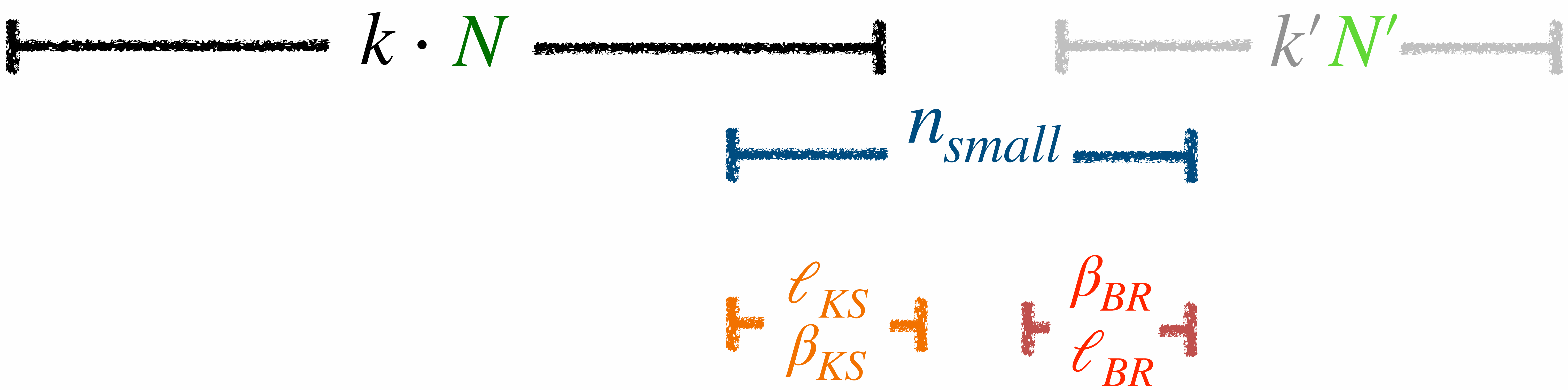
possible parameters

CJP Atomic Pattern



Macro
Parameters

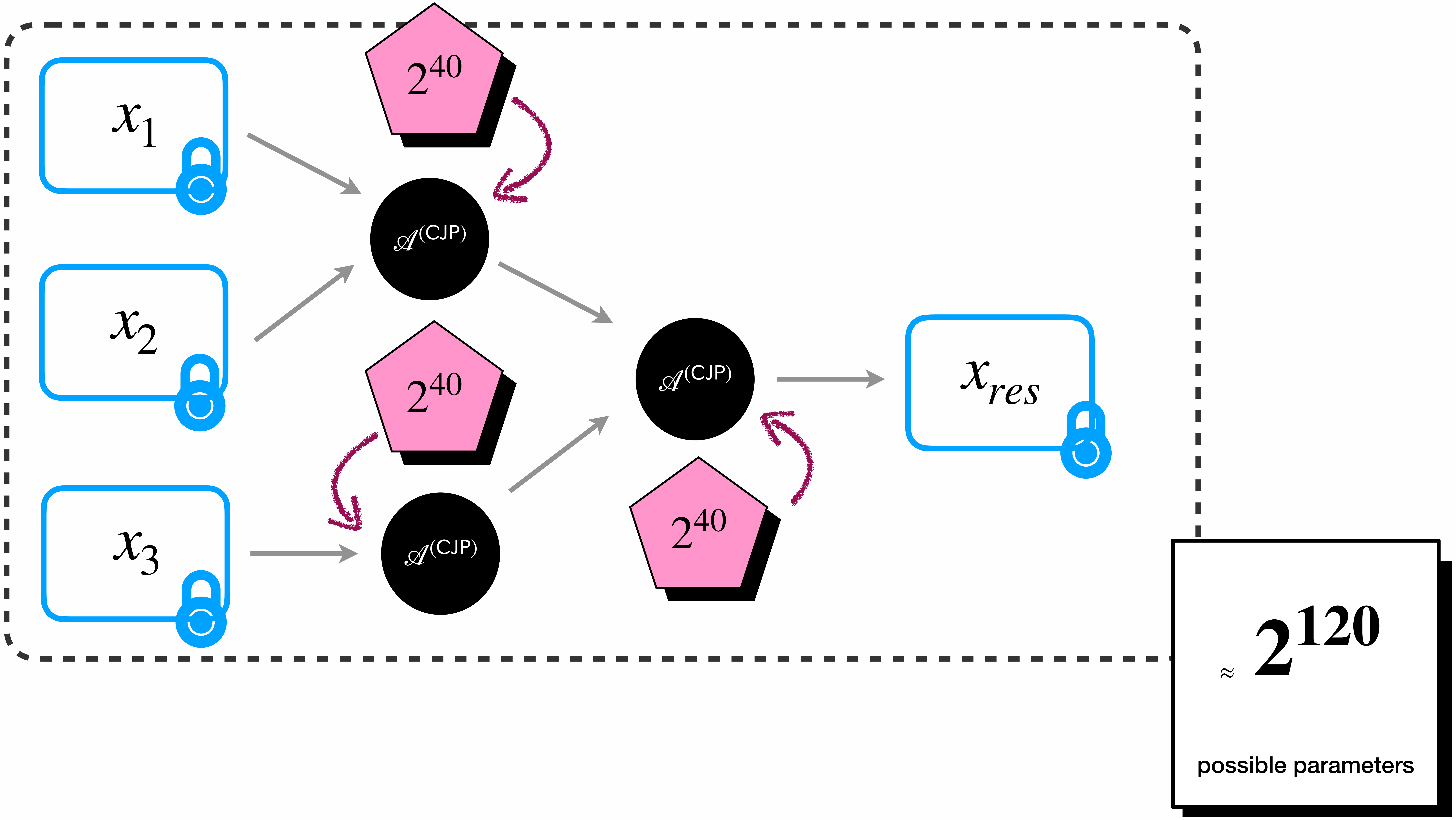
Micro
Parameters



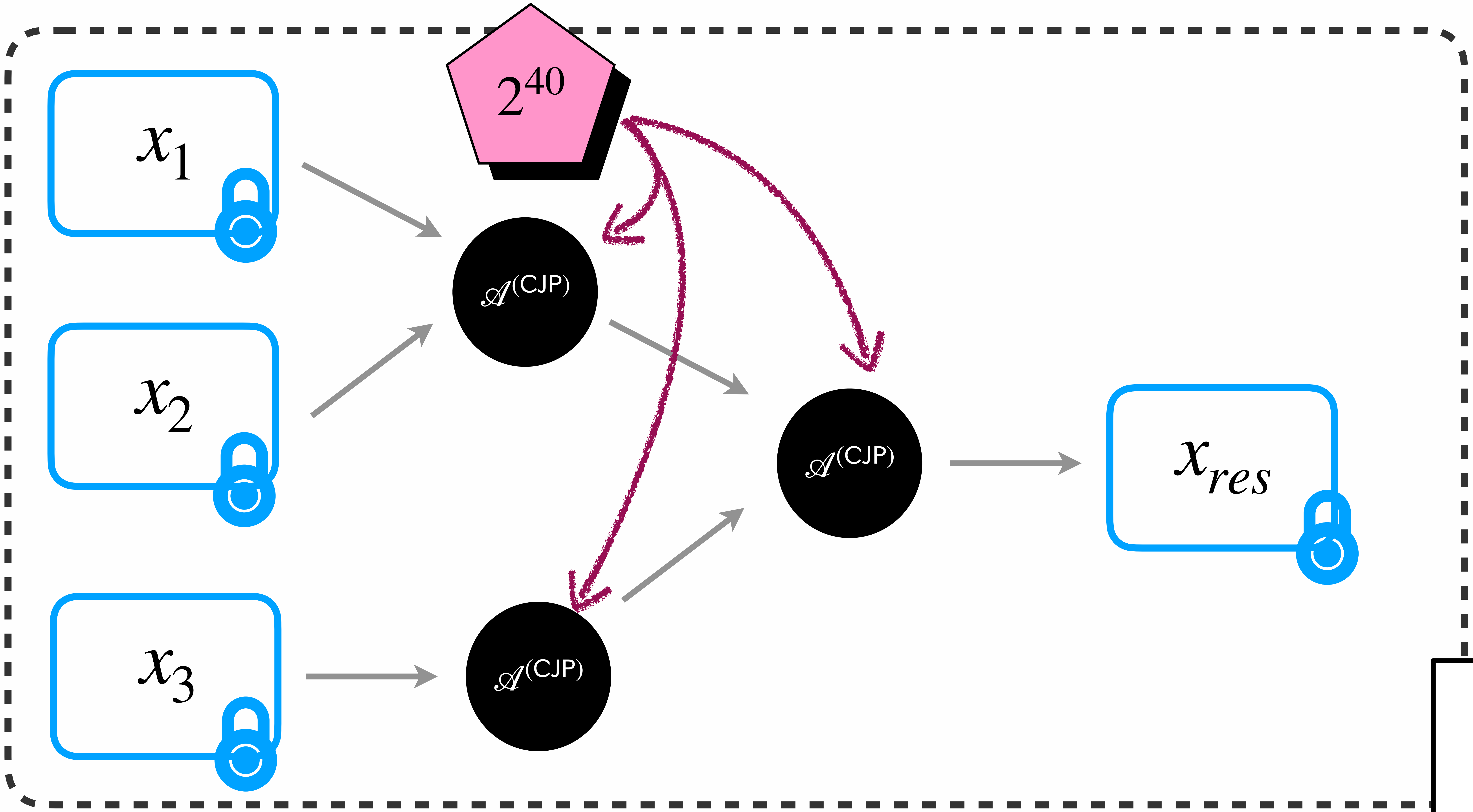
$\approx 2^{40}$

possible parameters

Graph of CJP AP


x_1
x_2
x_3
2^{40}
2^{40}
2^{40}
$\mathscr{A}^{(\text{CJP})}$
$\mathscr{A}^{(\text{CJP})}$
$\mathscr{A}^{(\text{CJP})}$
x_{res}
$\approx 2^{120}$
possible parameters

Graph of CJP AP

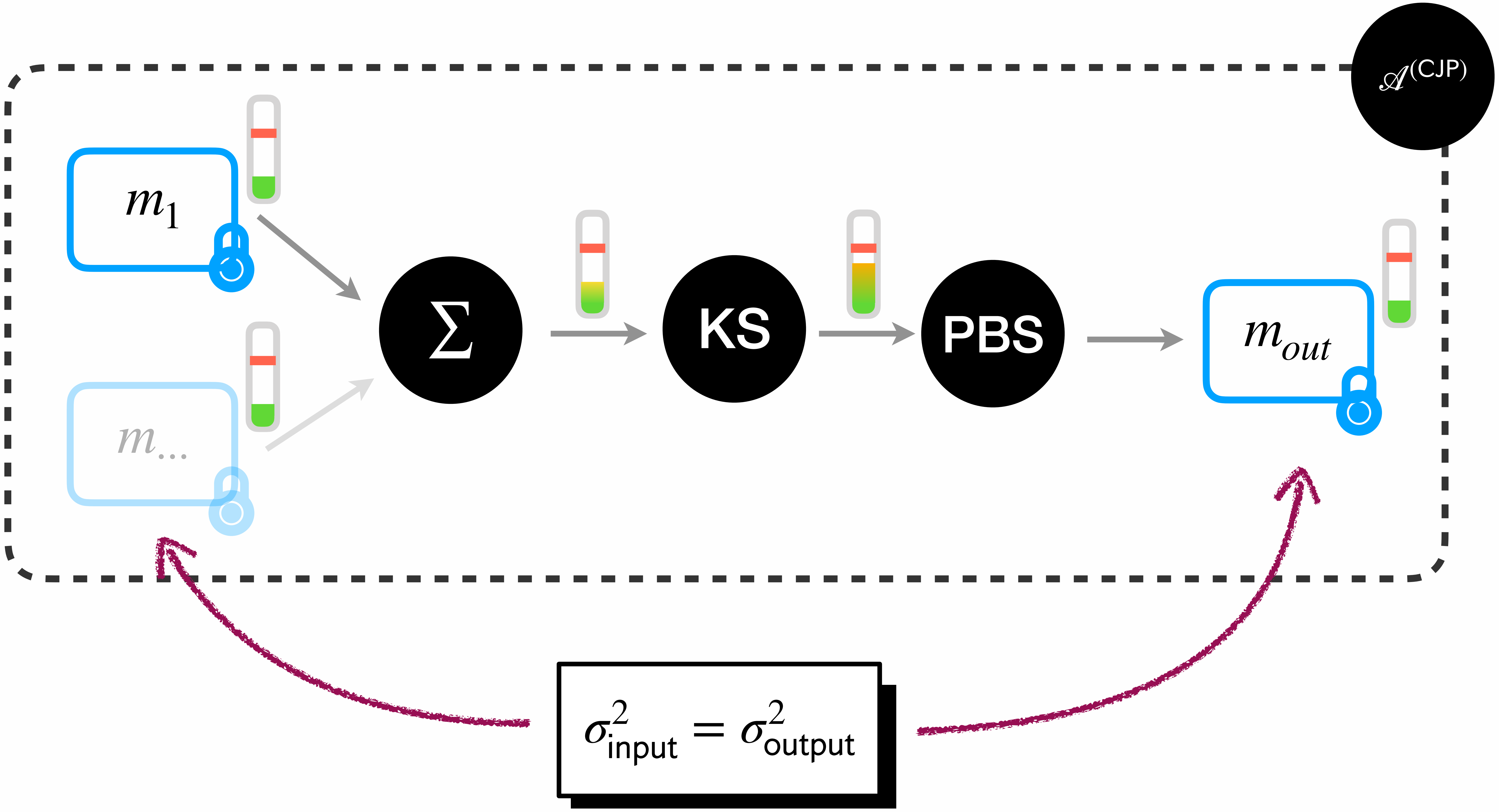

2^{40}
x_1
x_2
x_3
$\mathscr{A}^{(\mathrm{CJP})}$
$\mathscr{A}^{(\mathrm{CJP})}$
$\mathscr{A}^{(\mathrm{CJP})}$
x_{res}

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

$\approx$ $\mathbf{2^{40}}$

possible parameters

Graph of CJP AP


$\mathscr{A}^{(\text{CJP})}$
m_1
$m_{\dots}$
Σ
KS
PBS
m_{out}
$\sigma^2_{\text{input}} = \sigma^2_{\text{output}}$

FHE Parameter Optimization

Overview

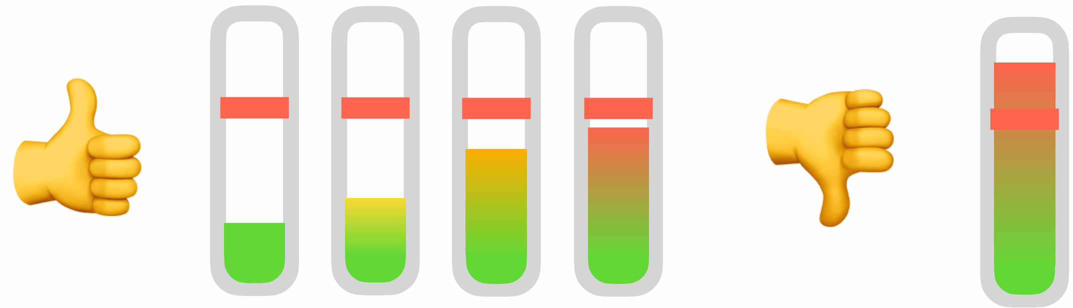
Overview: Goals

Security

$$f : \left(\overset{\substack{\text{LWE}\\ \text{dimension}}}{n}, \underset{\substack{\text{Security}\\ \text{level}}}{\lambda}, \overset{\substack{\text{Ciphertext}\\ \text{Modulus}}}{q}\right) \mapsto \underset{\substack{\text{Minimal standard}\\ \text{deviation}}}{\sigma_{\text{enc}}}$$

→ 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 $\mathscr{G} = \{A_i\}_{i \in I}$

✅ up to a given p_{fail}

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

Noise bound

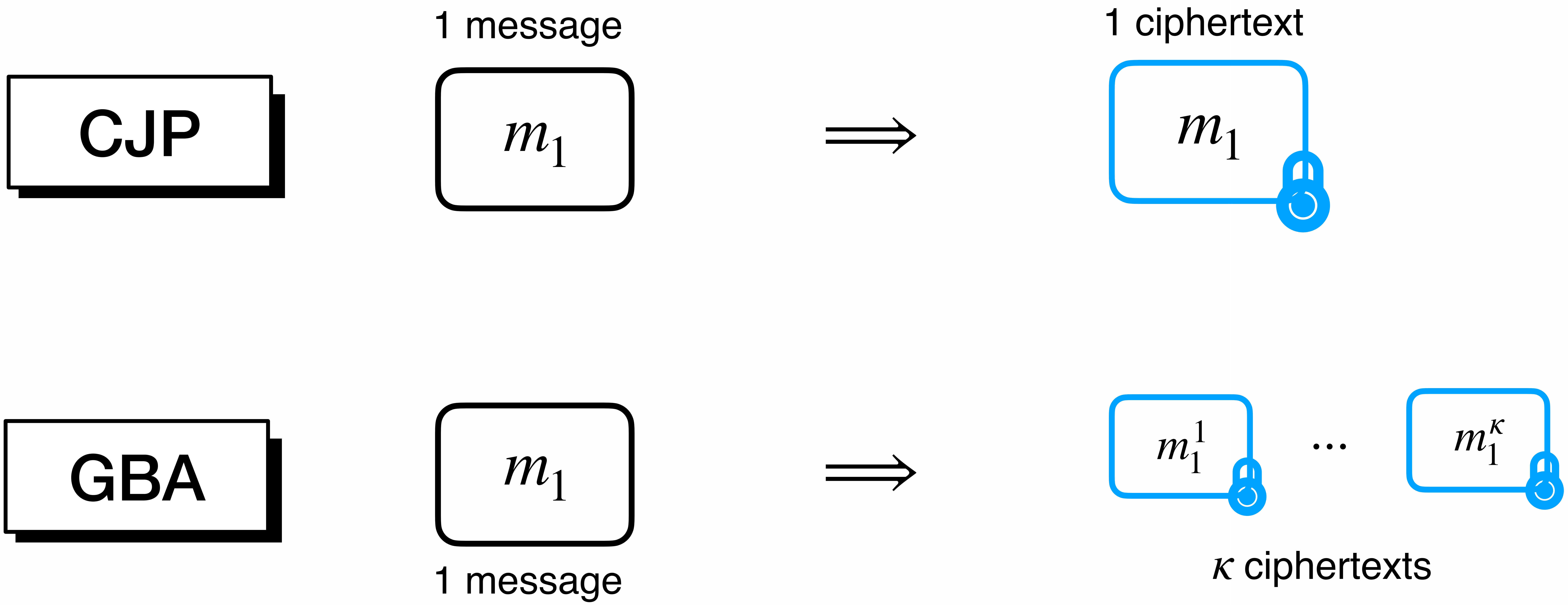
🚀

🔒 λ bits of security

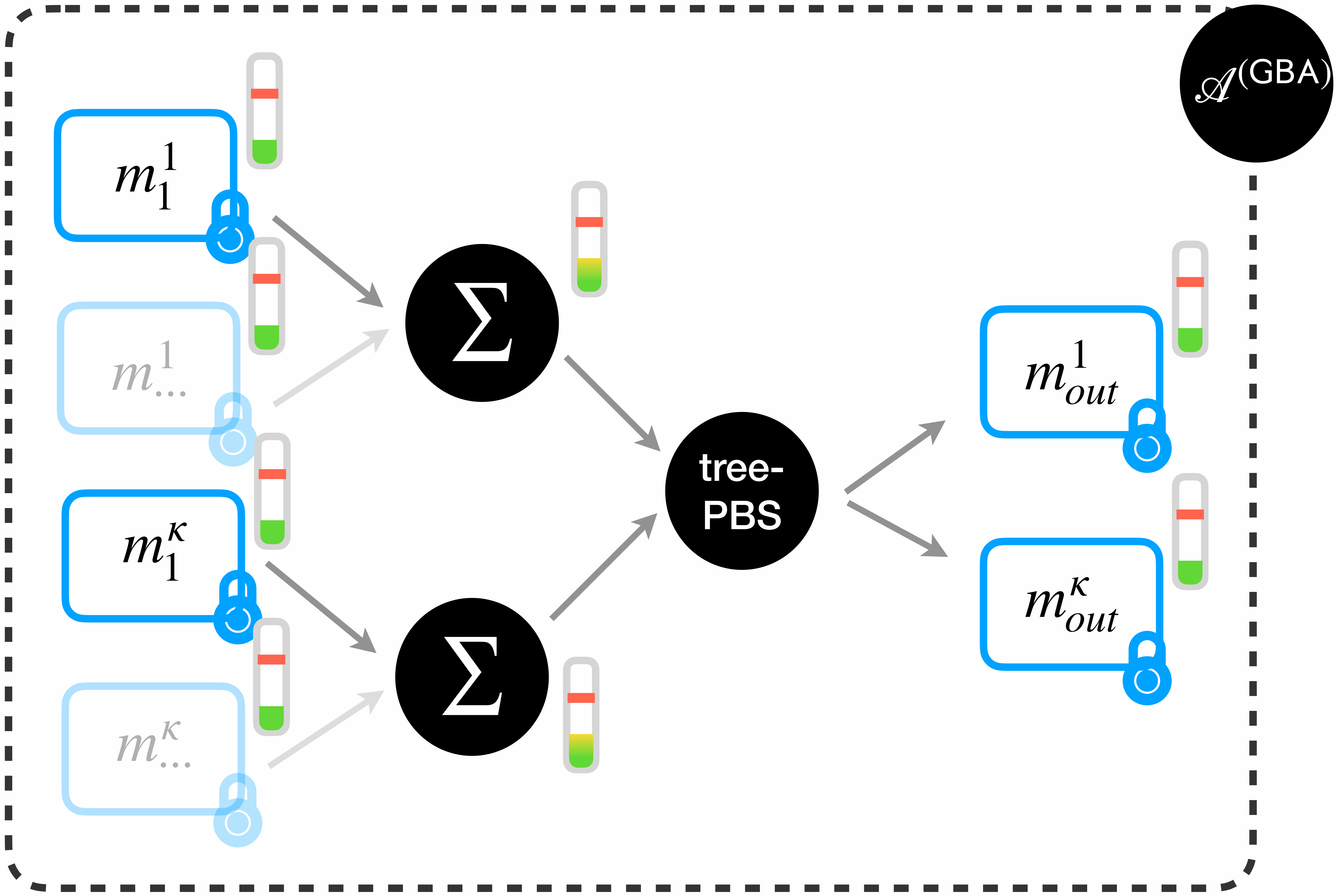
FHE Parameter Optimization

GBA Atomic Pattern

Encoding


CJP
1 message
m_1
$\Longrightarrow$
1 ciphertext
m_1
GBA
m_1
1 message
$\Longrightarrow$
m_1^1
$\cdots$
m_1^κ
κ ciphertexts

GBA Atomic Pattern



$\approx 2^{52}$

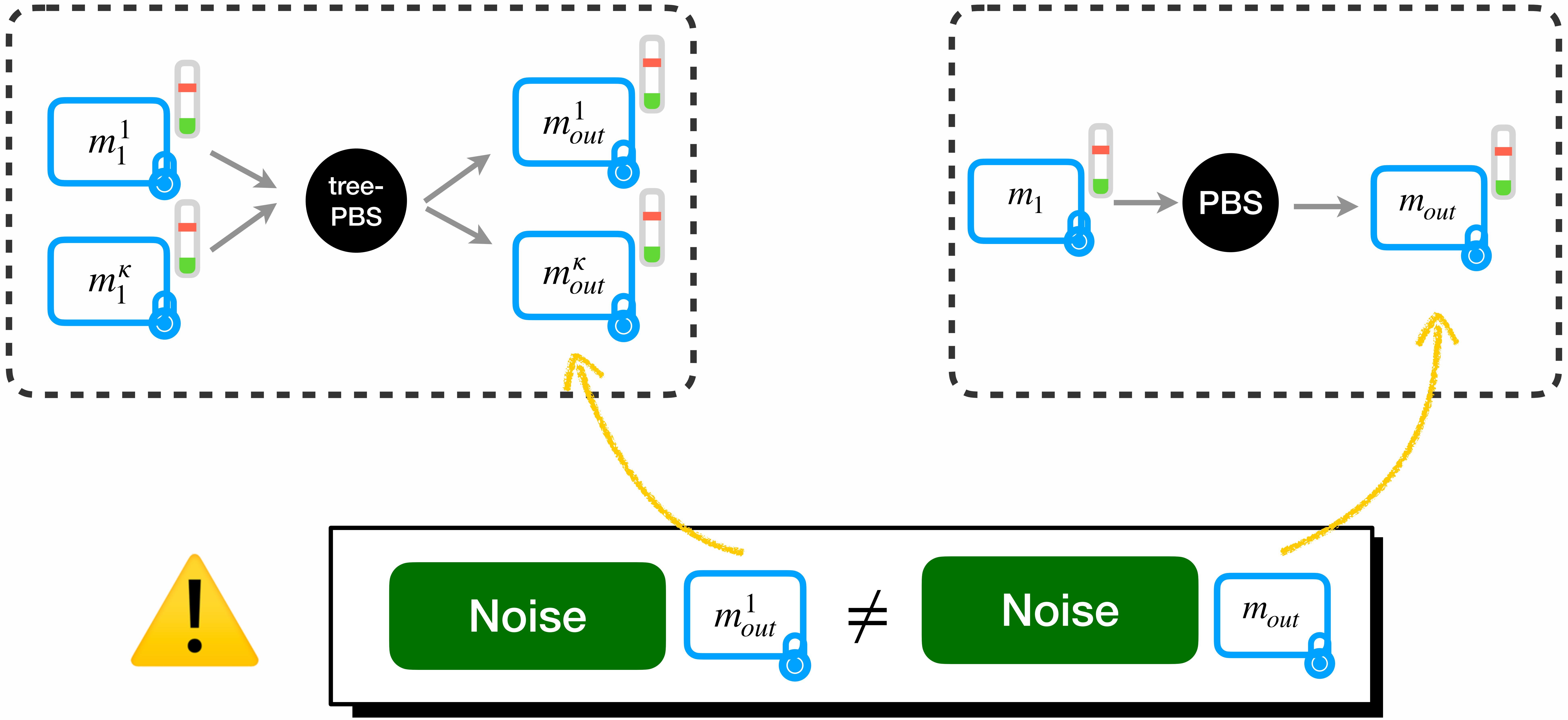
possible parameters

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

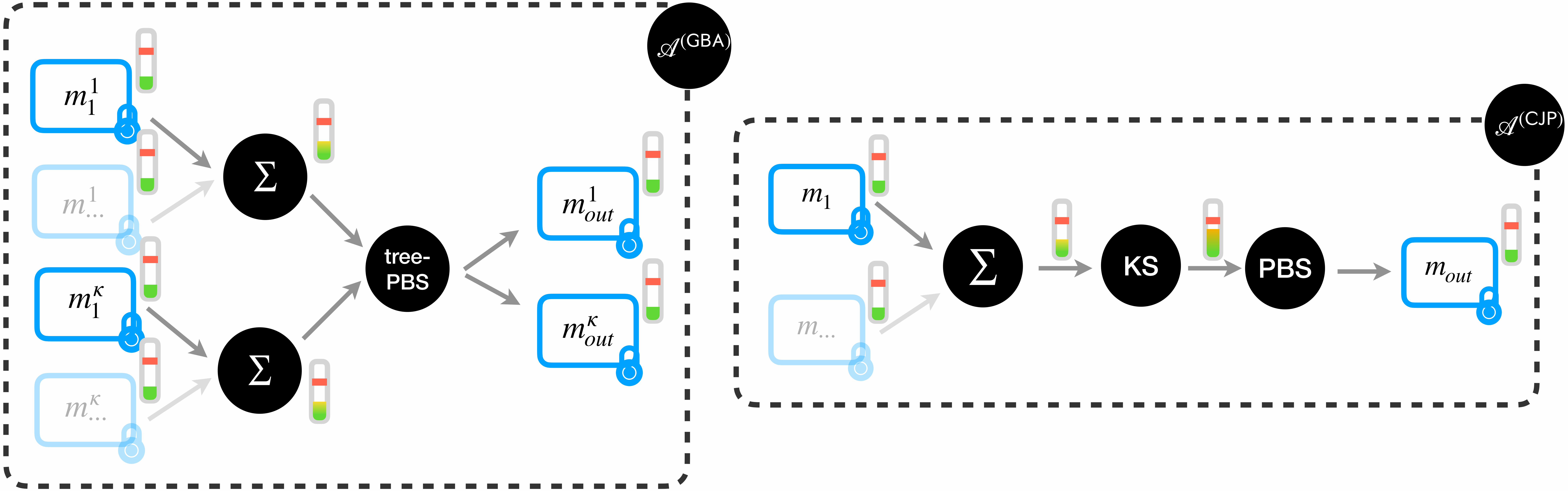
FHE Parameter Optimization

CJP vs GBA

CJP vs GBA

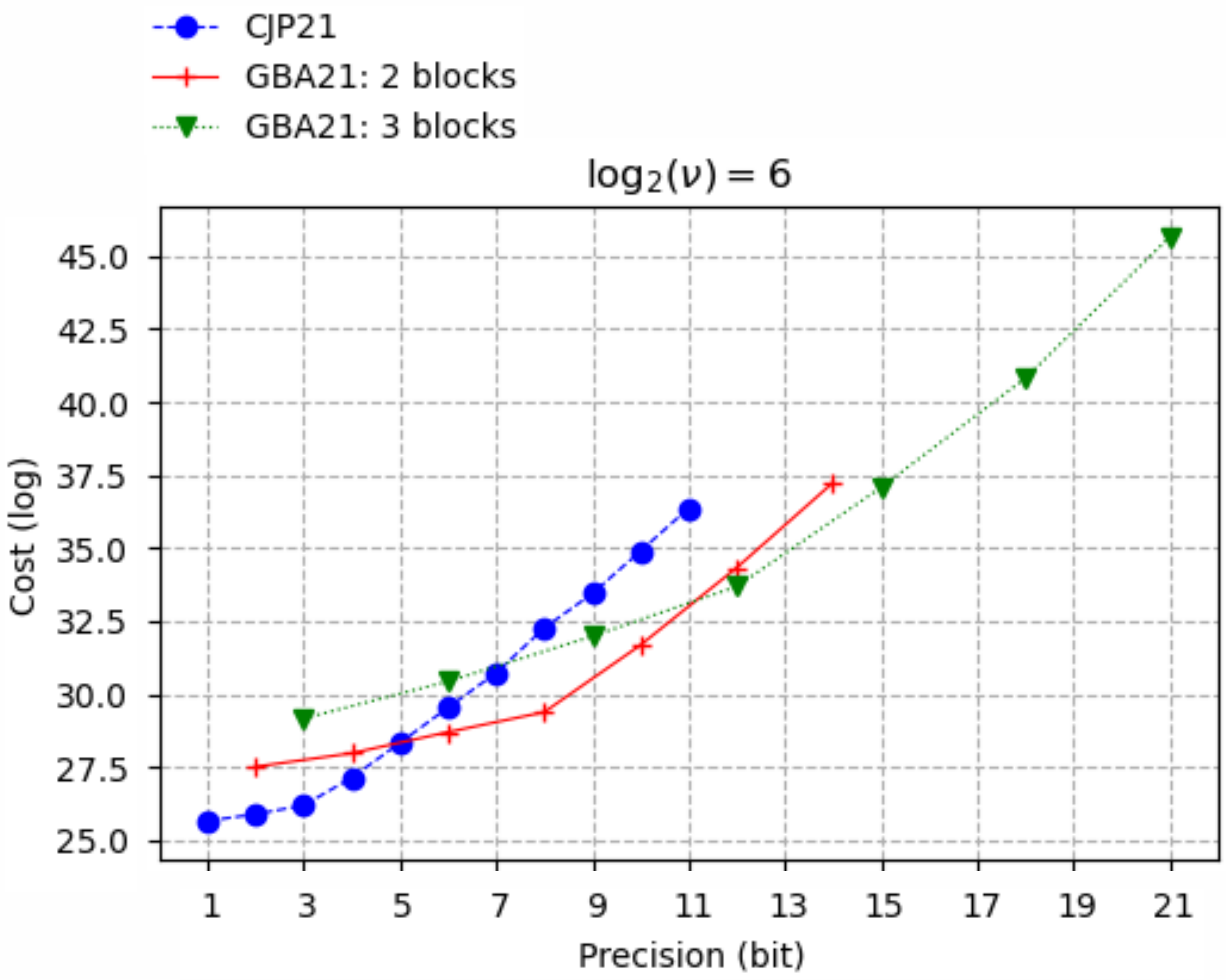

m_1^1
m_1^κ
tree-PBS
m_{out}^1
m_{out}^κ
m_1
PBS
m_{out}
Noise
m_{out}^1
$\neq$
Noise
m_{out}

CJP vs GBA



😍 Context-aware comparison

CJP vs GBA



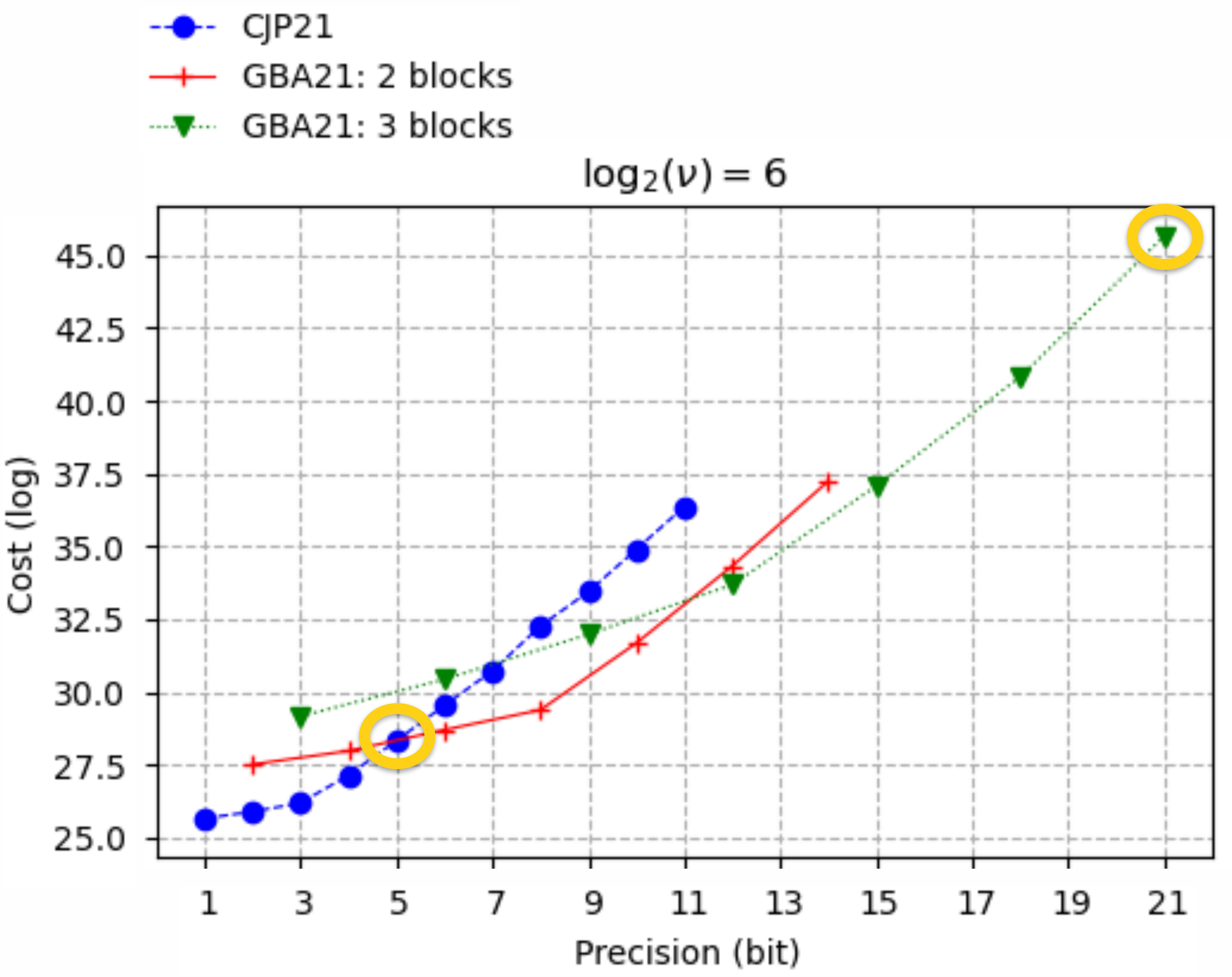
Efficient alternative to TFHE PBS above 5 bits

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

Large precision are **very costly**

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

CJP vs GBA



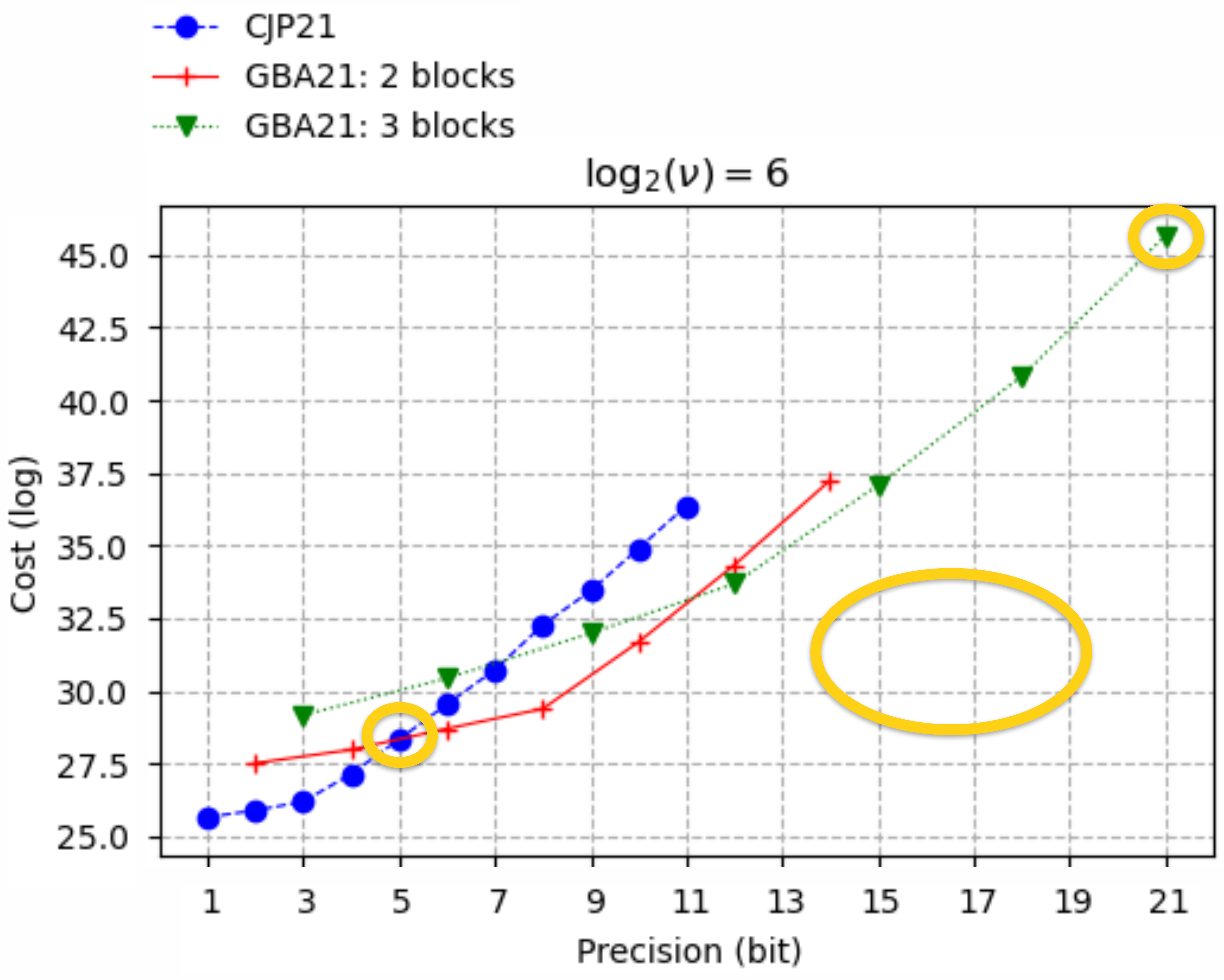
Efficient alternative to TFHE PBS above 5 bits

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

Large precision are **very costly**

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

CJP vs GBA



Efficient alternative to TFHE PBS above 5 bits

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

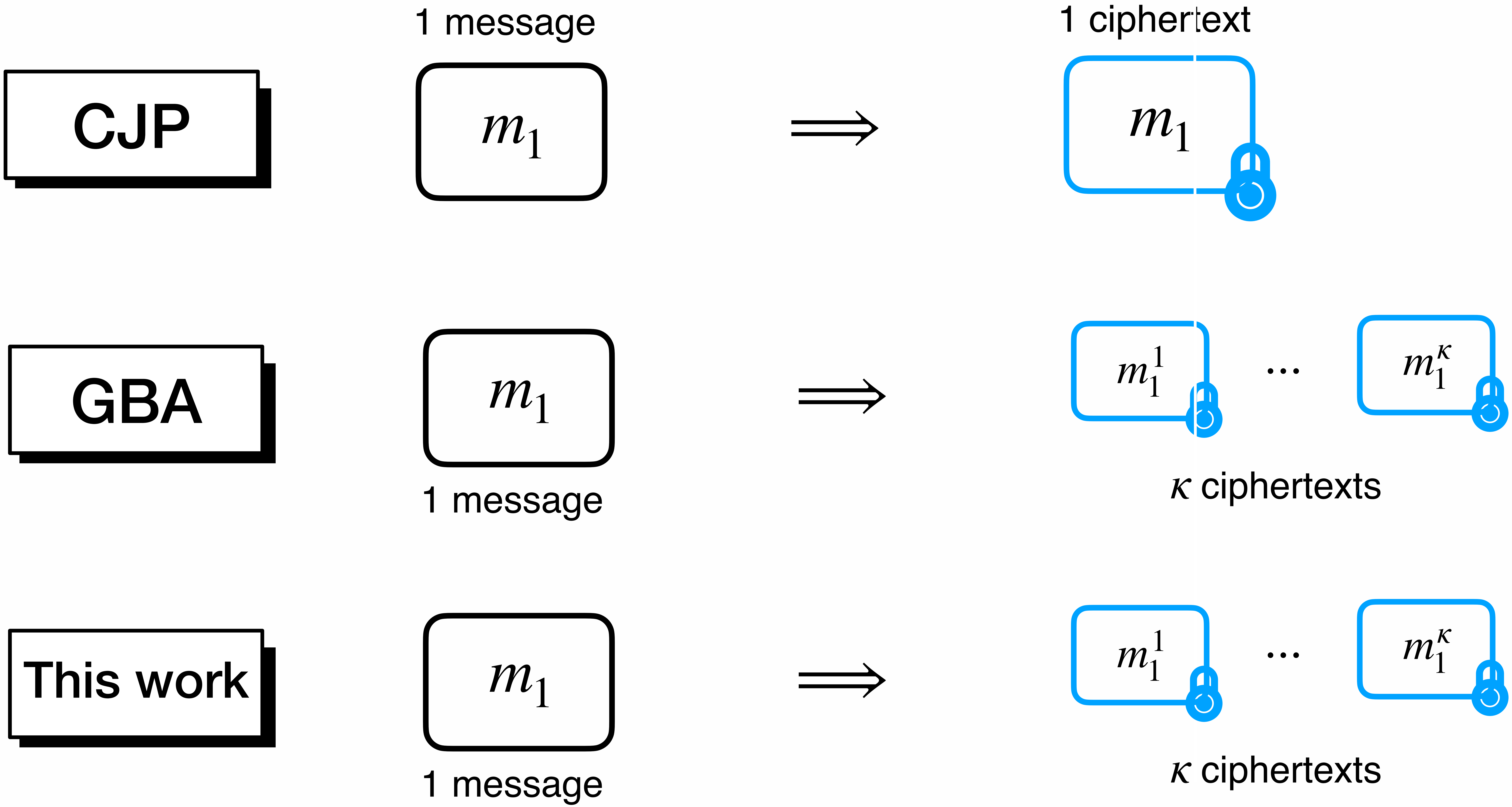
Large precision are **very costly**

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

WoP-PBS

Overview

Encoding

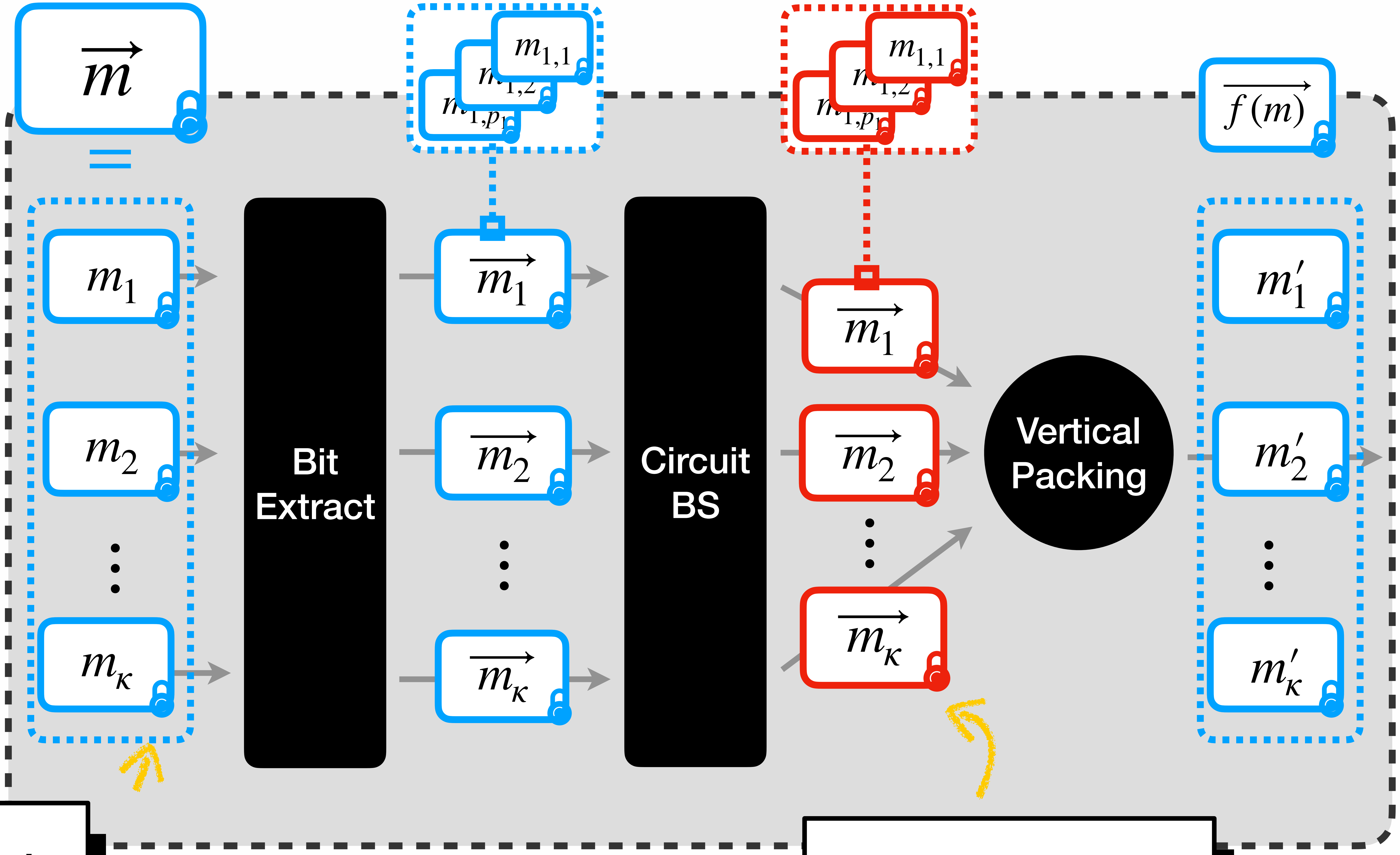


CJP: 1 message m_1 $\Longrightarrow$ 1 ciphertext m_1

GBA: m_1, 1 message $\Longrightarrow$ m_1^1 $\cdots$ m_1^κ, κ ciphertexts

This work: m_1, 1 message $\Longrightarrow$ m_1^1 $\cdots$ m_1^κ, κ ciphertexts

New WoP-PBS



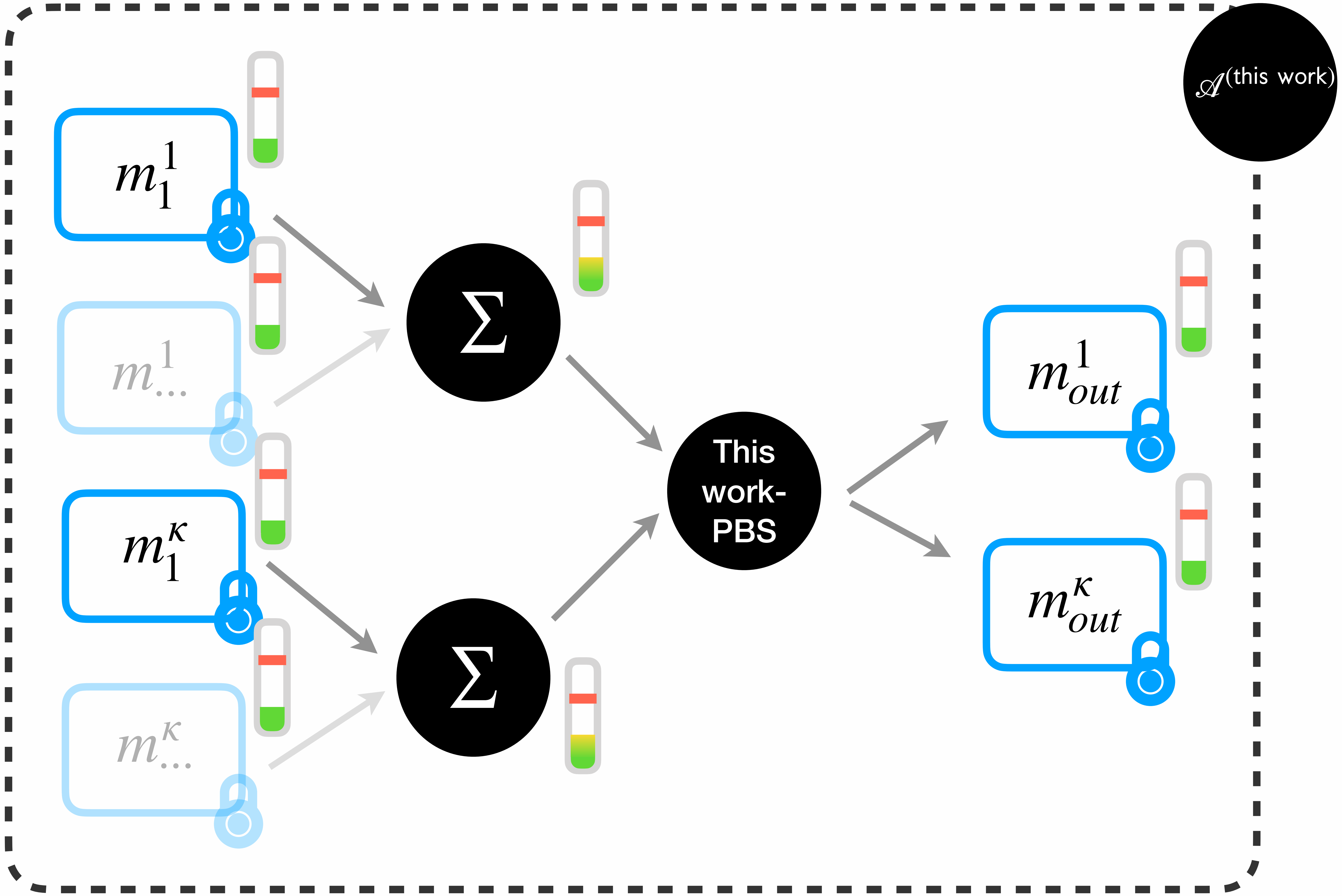
LWE Ciphertexts

GGSW Ciphertexts

WoP-PBS

Comparisons

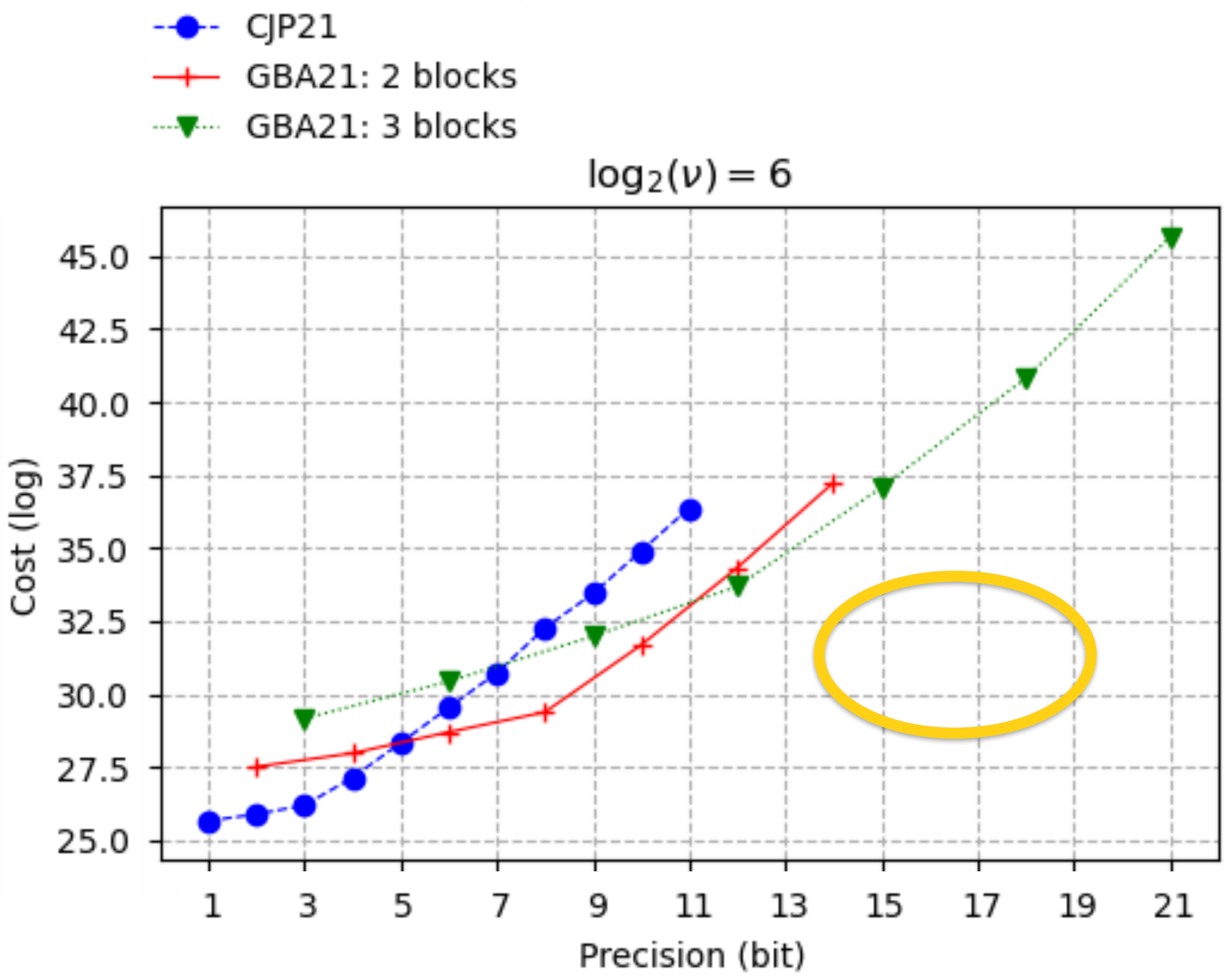
This work Atomic Pattern



$\approx 2^{64}$

possible parameters

CJP vs GBA



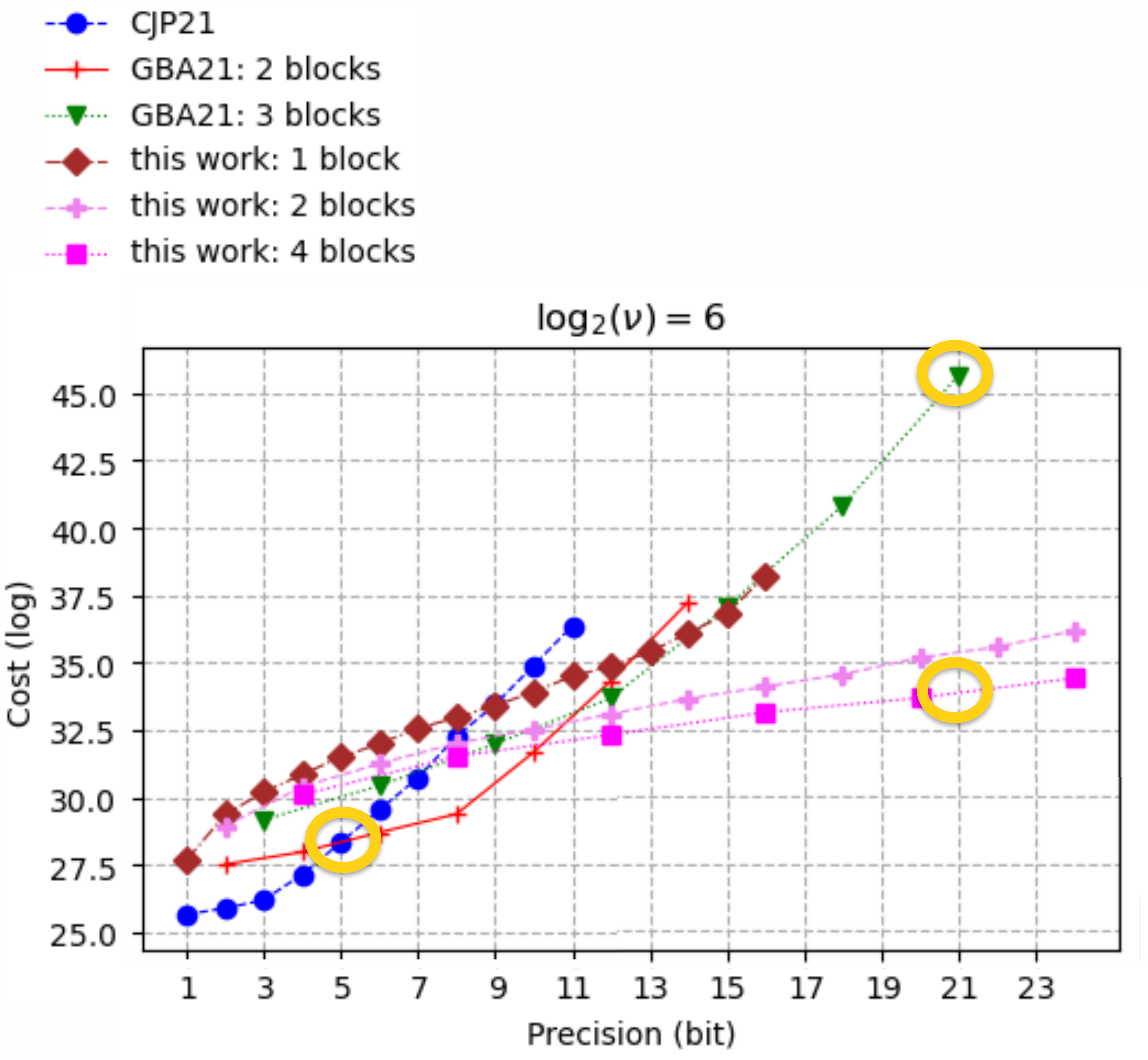
Efficient alternative to TFHE PBS above 5 bits

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

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

Conclusion

Other results

Other results

Large Integers

CRT, radix, hybrid encoding

WoP-PBS Analysis

LMP, this work

Failure Probability

AP and graph level

KS Position

CJP, CGGI, KS-free

PBS Insertion

In Dot Product

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 Set

In the paper: only one parameter set

Graph Comparison

Real use cases

Thank you.

ZAMA

Contact and Links

damien.ligier@zama.ai
samuel.tap@zama.ai

zama.ai

Github

Community links

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