ZAMA

Improved Programmable Bootstrapping with Larger Precision and Efficient Arithmetic Circuits for TFHE

Ilaria Chillotti | ilaria.chillotti@zama.ai

Damien Ligier | damien.ligier@zama.ai

Jean-Baptiste Orfila | jb.orfila@zama.ai

Samuel Tap | samuel.tap@zama.ai

Asiacrypt 2021

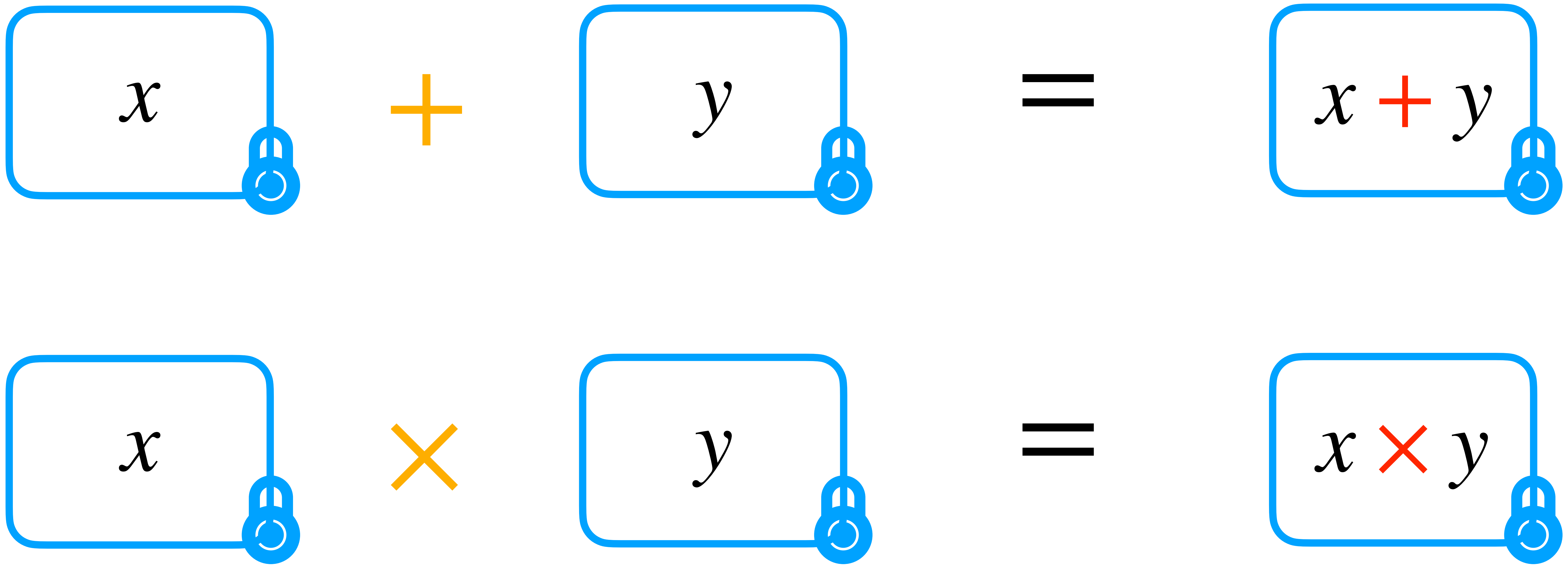
December 9, 2021

Overview

1. TFHE Scheme Overview
2. PBS Many LUTs
3. BFV Product in TFHE
4. WoP-PBS
5. Challenges & Conclusion

Overview

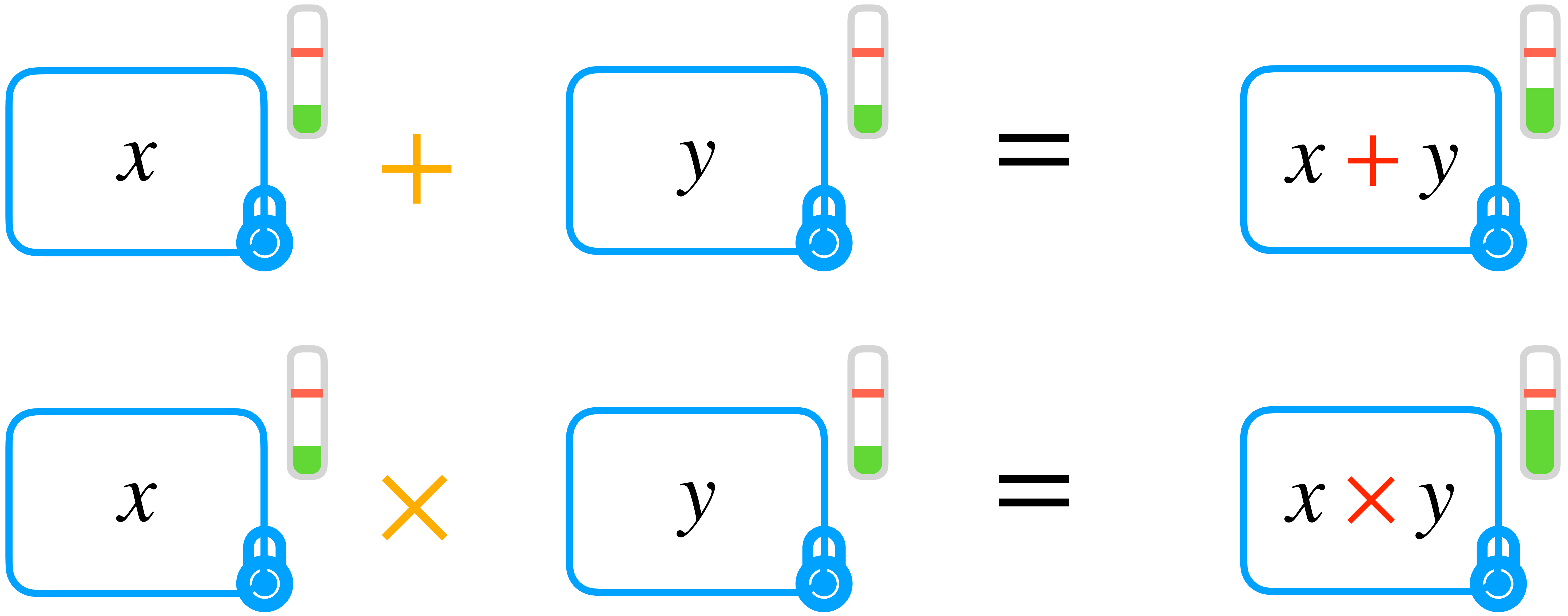
What is FHE?



Computations over Encrypted Messages!

- Possibly any function
- Possibly any type: bit, integer, real messages…

Noise Growth



too much noise 🥵 $\Longrightarrow$ incorrect decryption 💀

Bootstrapping in TFHE

Refresh the ciphertext with **less noise** ❄️ ...

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

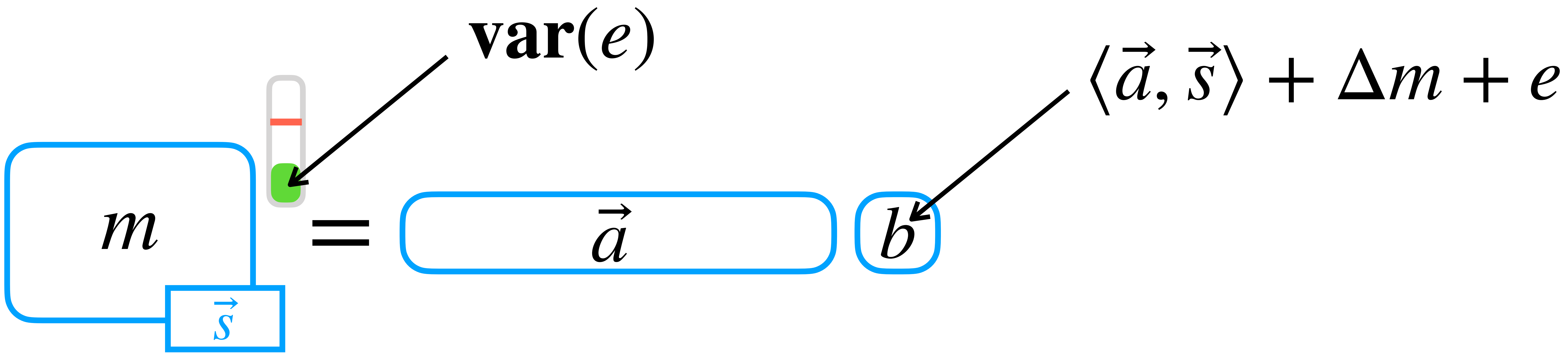
Bootstrapping in TFHE

… and can **evaluate a Lookup Table** (LUT)! 💪

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

Ciphertexts in TFHE:

LWE Ciphertexts



Easy **homomorphic addition** & **integer multiplication!**

Ciphertexts in TFHE:

Other Ciphertexts

RLWE
- Addition
- Constant multiplication

RGSW
- Addition
- Constant multiplication
- Multiplication

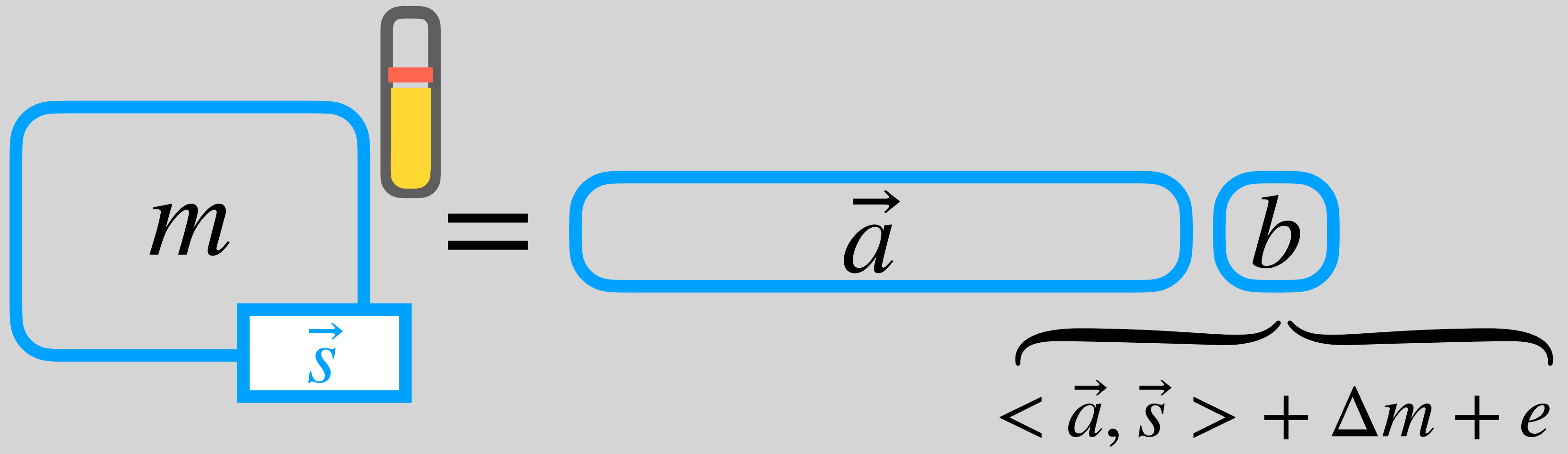
(External) **Product:**

RGSW: μ (key $S(X)$) $\boxdot$ RLWE: M (key $S(X)$) $=$ RLWE: $M \cdot \mu$ (key $S(X)$)

TFHE Bootstrapping: more details

Inputs:

1 LWE ciphertext



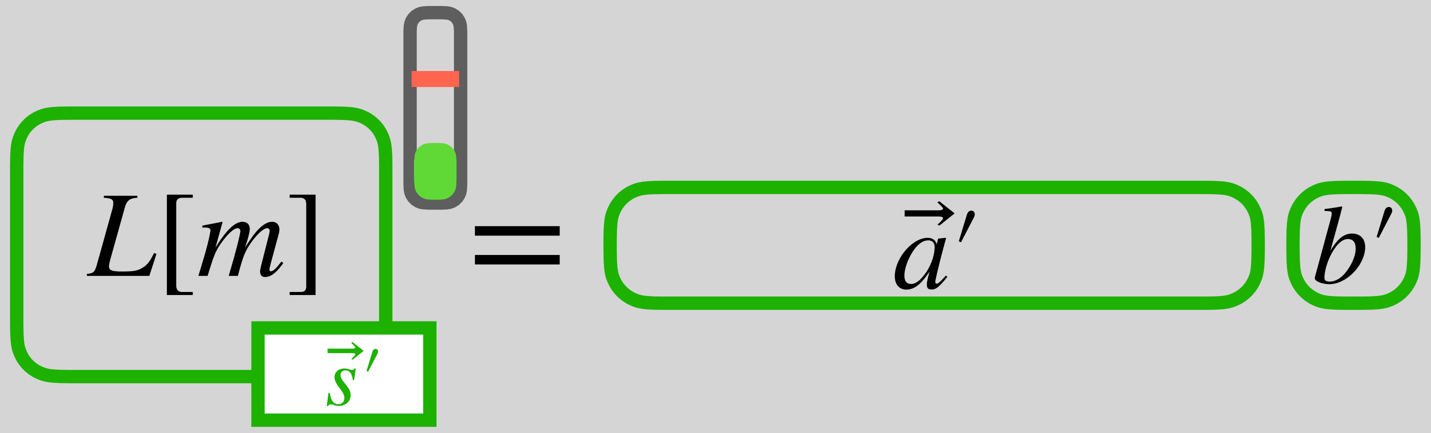
1 lookup-table

$$[L[0], \ldots, L[p-1]]$$

1 bootstrapping key

Output:

1 LWE ciphertext



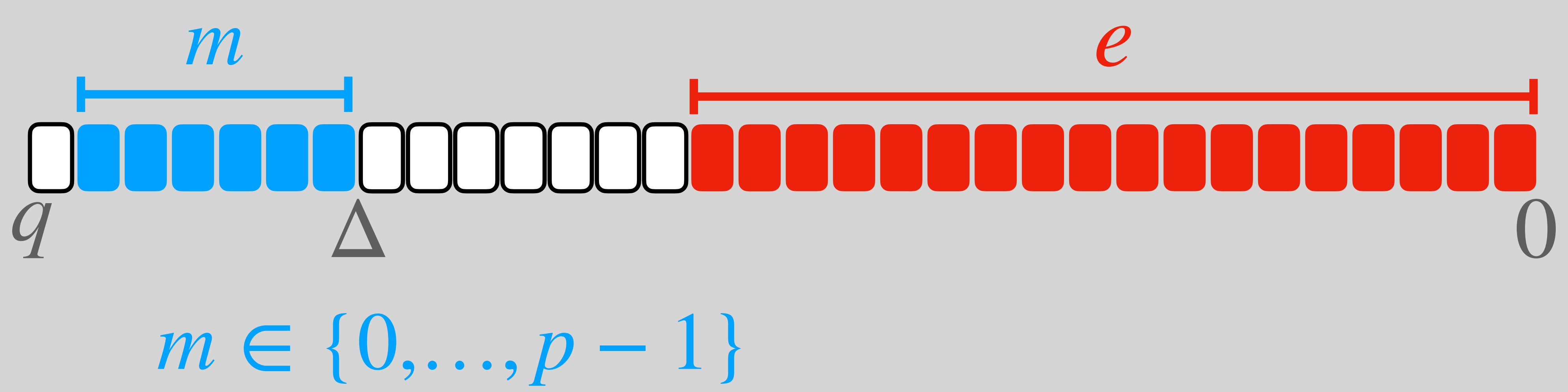
TFHE Bootstrapping: more details

Idea: homomorphically evaluate the ***decryption algorithm***

Decryption algorithm:

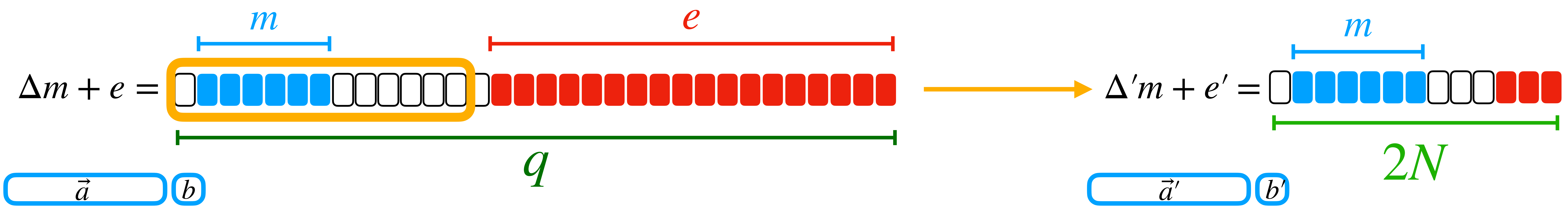
1. $b - < \vec{a}, \vec{s} > = \Delta m + e$
2. $\left\lceil \frac{\Delta m + e}{\Delta} \right\rfloor = m$

LWE Input:

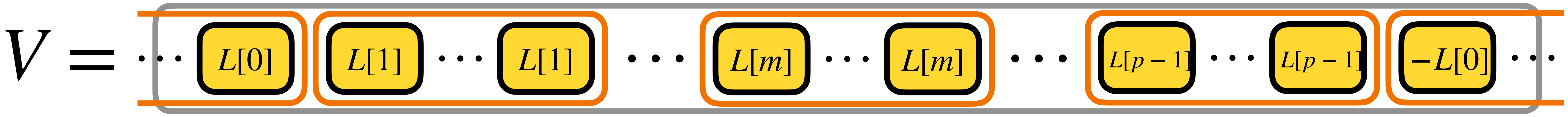


TFHE Bootstrapping: more details

1 **Modulus Switching** step from $\mathbb{Z}_q$ to $\mathbb{Z}_{2N}$

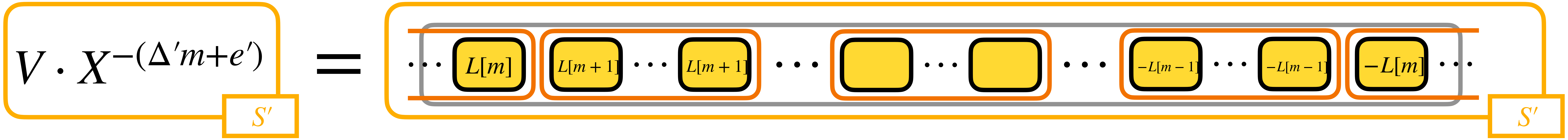


2 **Describe the LUT into a polynomial** $V \mod X^N + 1$ **with redundancy**



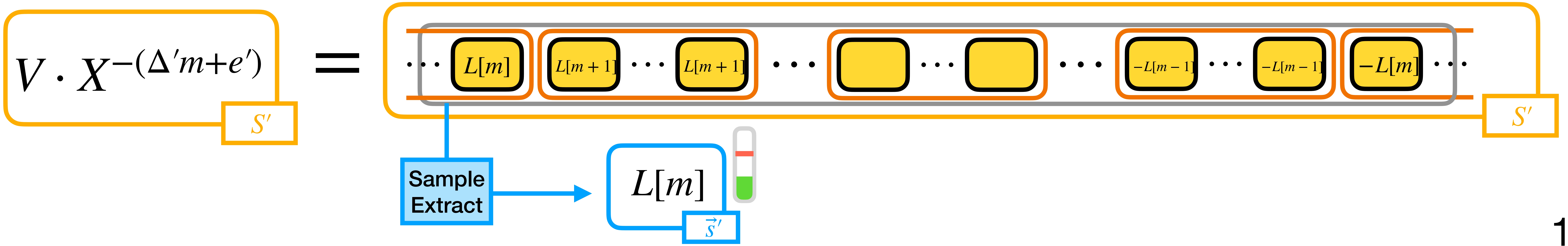
TFHE Bootstrapping: more details

3 Rotate the LUT of $\Delta' m + e'$ positions

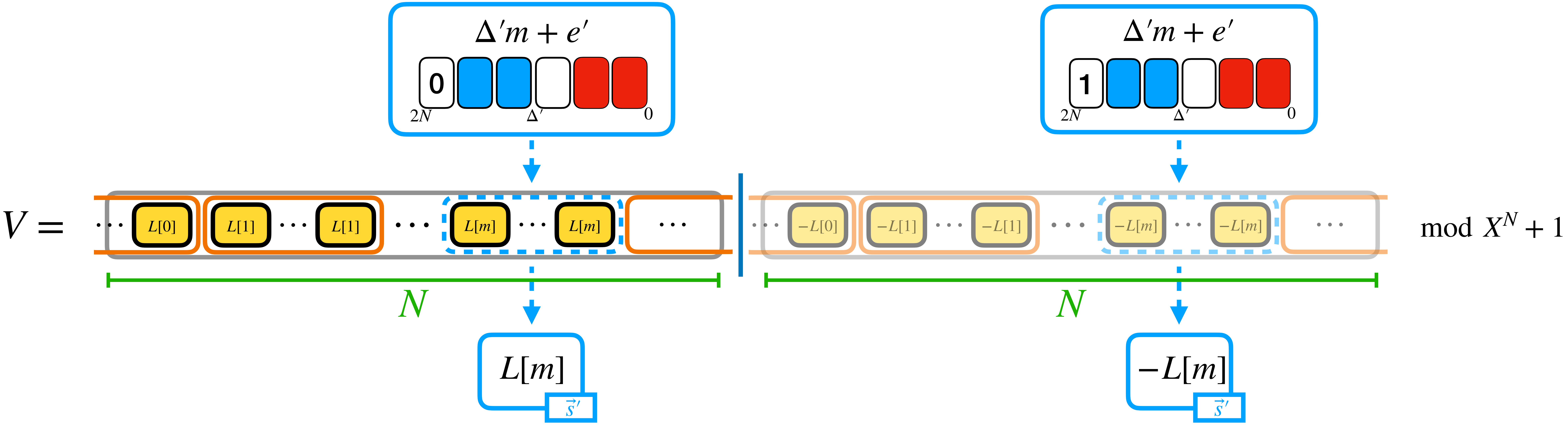


$$= V \cdot X^{-b' + \sum_{i=0}^{n-1} a'_i s_i}$$ ⟵ external products (CMux) chain

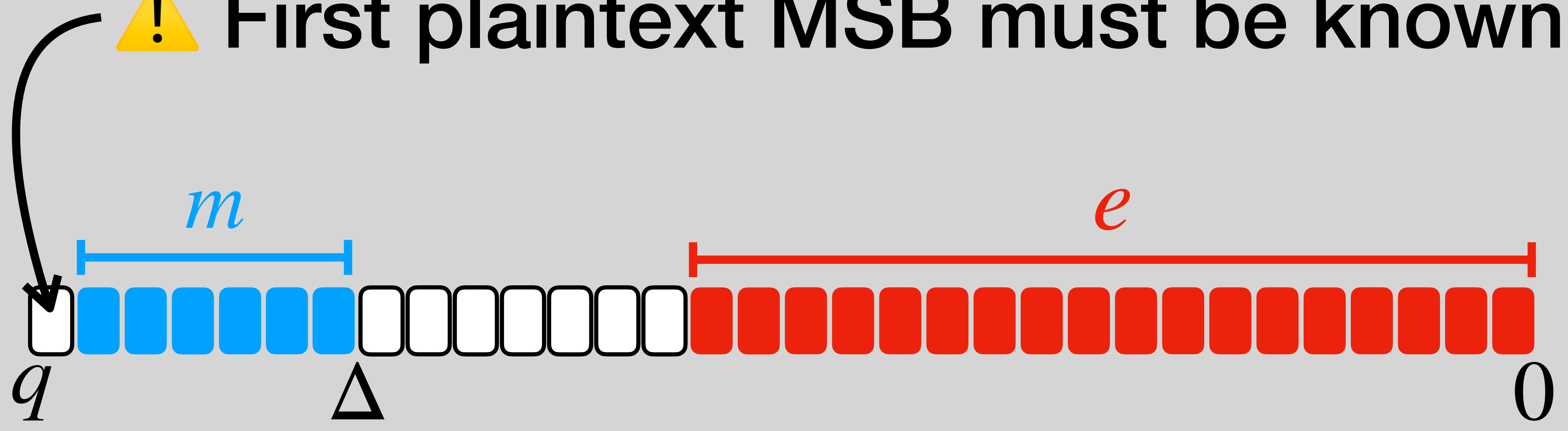
4 Extract the first coefficient as an LWE



TFHE Bootstrapping: limitations



⚠️ First plaintext MSB must be known



Our Contributions: (some of them)

1 **Several LUT per bootstrapping** on the same input ciphertext

→ PBSManyLUT

n lookup-table:

$$[L_1[0], \ldots, L_1[p-1]]$$
$$\vdots \qquad \vdots$$
$$[L_n[0], \ldots, L_n[p-1]]$$

2 Introduction of a **BFV-like Multiplication in TFHE**

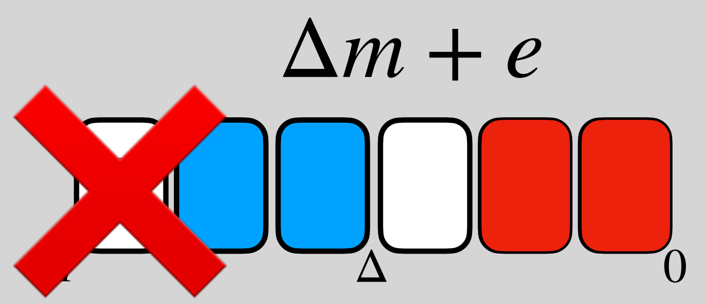
→ Tight noise analysis

$$C_1 \boxtimes C_2$$

3 PBS **without Padding**

→ 2 ideas for WoP-PBS

not anymore!

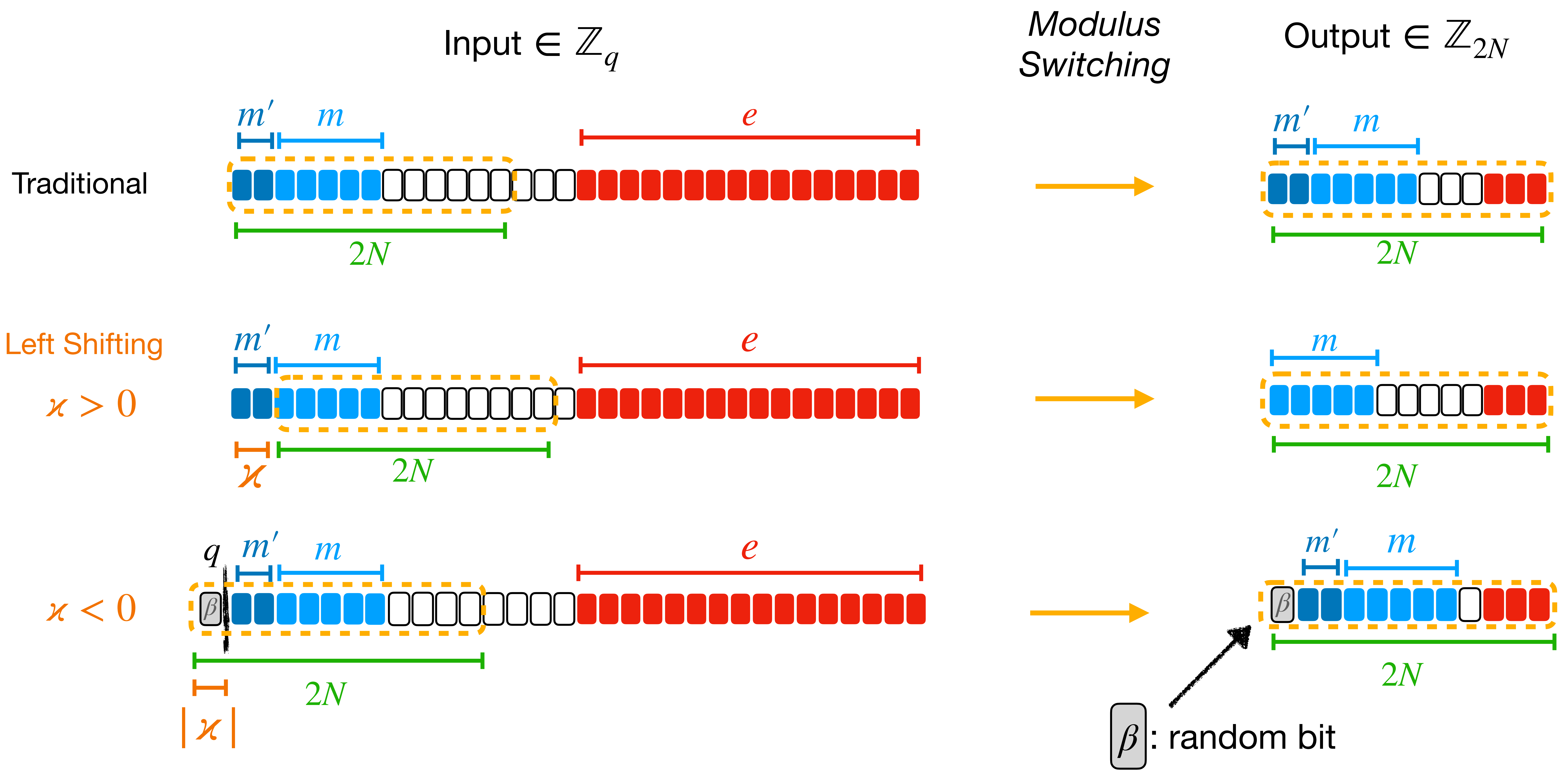


Overview

1. TFHE Scheme Overview
2. **PBS Many LUTs**
3. BFV Product in TFHE
4. WoP-PBS
6. Challenges & Conclusion

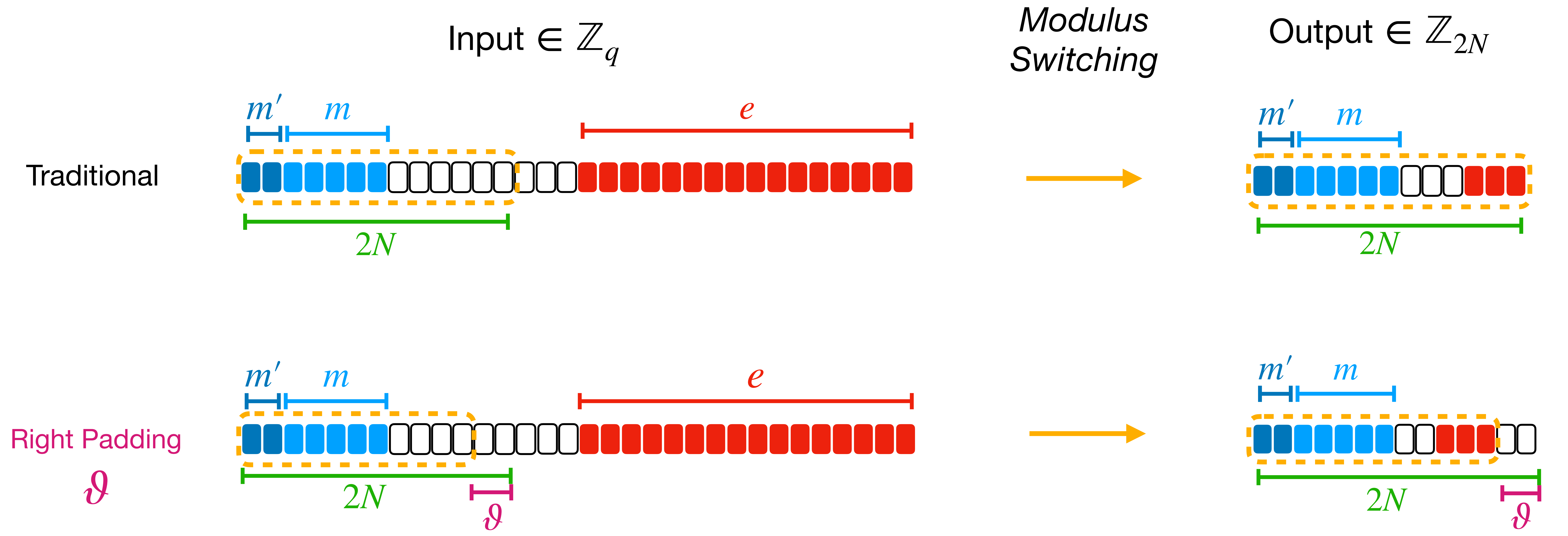
Generalized Bootstrapping

Left Shifting

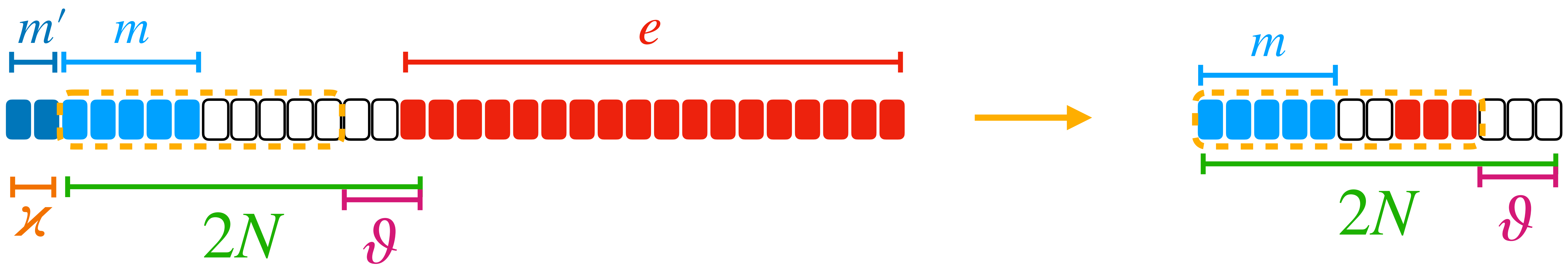


Generalized Bootstrapping

Right Padding



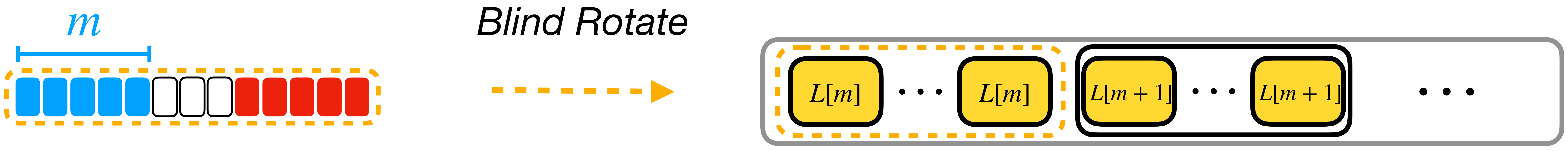
Generalized Bootstrapping



N, $\varkappa$ and ϑ defines the frame:

PBS Many LUTs

1 PBS $\leftrightarrow$ 1 LUT



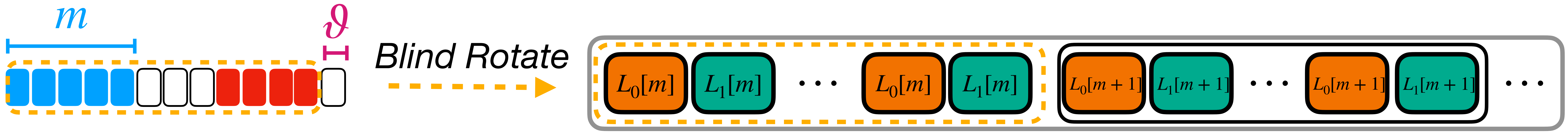
$\approx$ Select the m^{th} LUT case

PBS Many LUTs

1 Generalized PBS ↔ Many LUTs

2 lookup-tables: $[L_0[0], \ldots, L_0[p-1]]$

$[L_1[0], \ldots, L_1[p-1]]$



1 bit Right Lifting

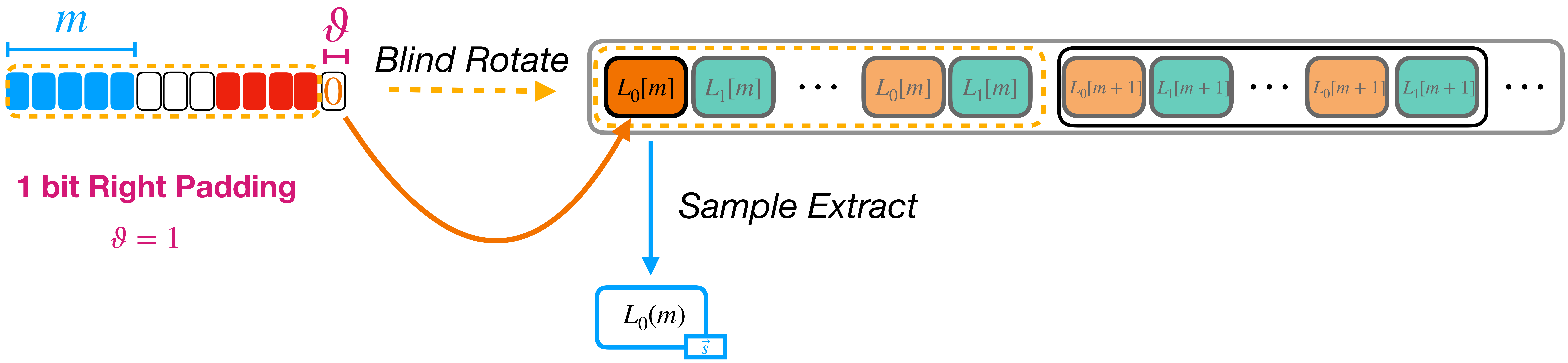
$\vartheta = 1$

PBS Many LUTs

1 Generalized PBS ↔ Many LUTs

2 lookup-tables: $[L_0[0], \ldots, L_0[p-1]]$

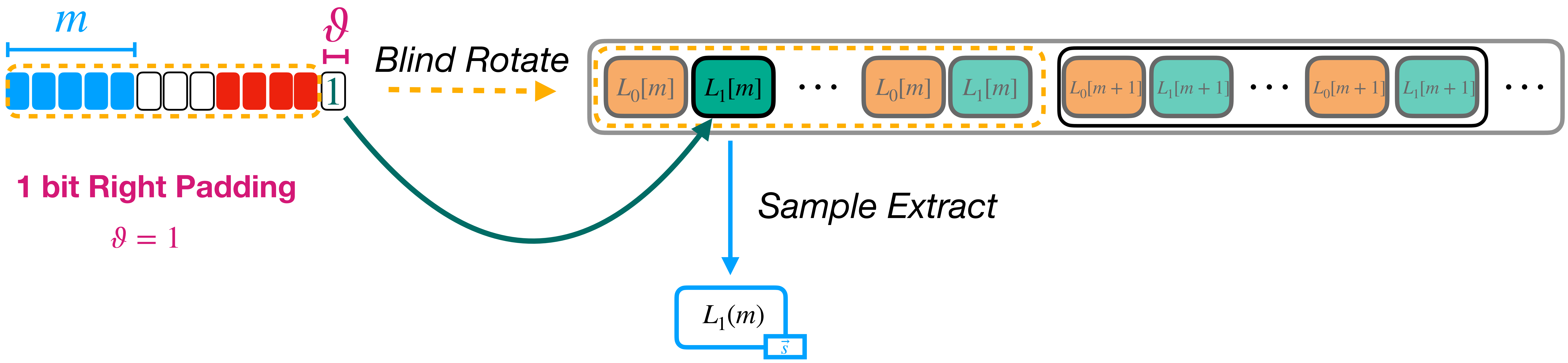
$[L_1[0], \ldots, L_1[p-1]]$



PBS Many LUTs

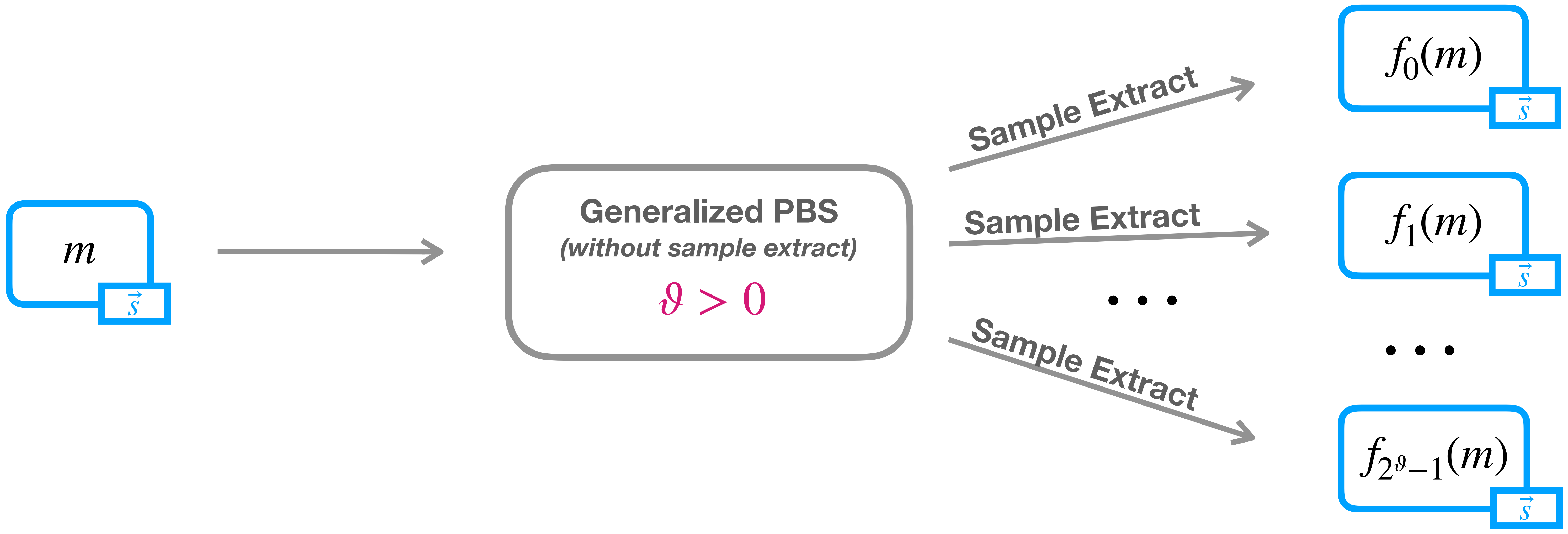
1 Generalized PBS ↔ Many LUTs

2 lookup-tables: $[L_0[0], \ldots, L_0[p-1]]$
$[L_1[0], \ldots, L_1[p-1]]$



PBS Many LUTs

Recap



Multiple Instructions, Single Data **(MISD)**

$\Rightarrow$ For a cost $\approx$ 1 PBS, evaluation of 2^ϑ functions on the same input

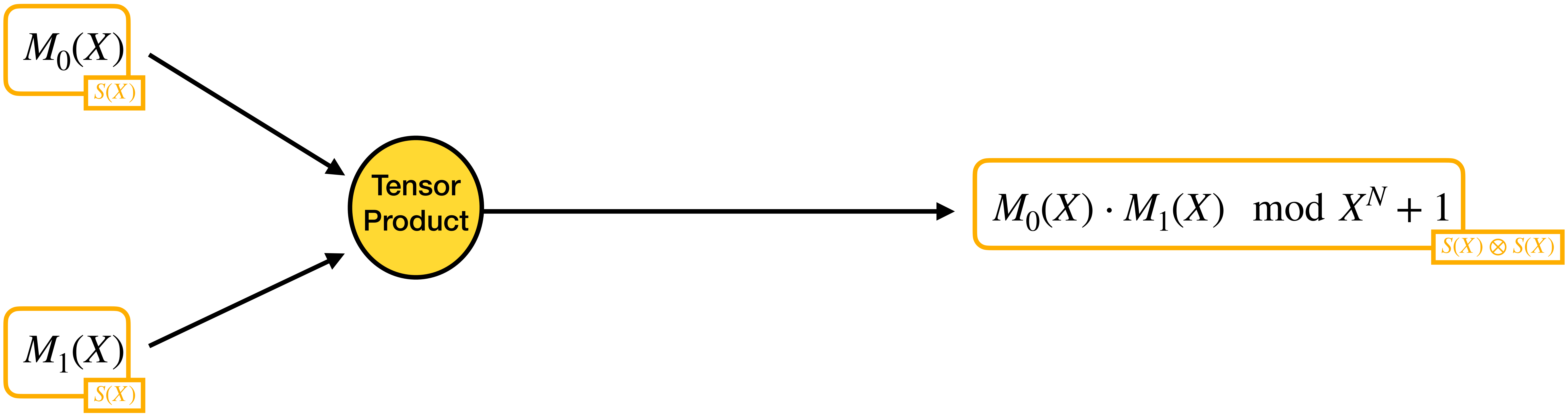
Require small messages m

Higher $\vartheta \Rightarrow$ more error

Overview

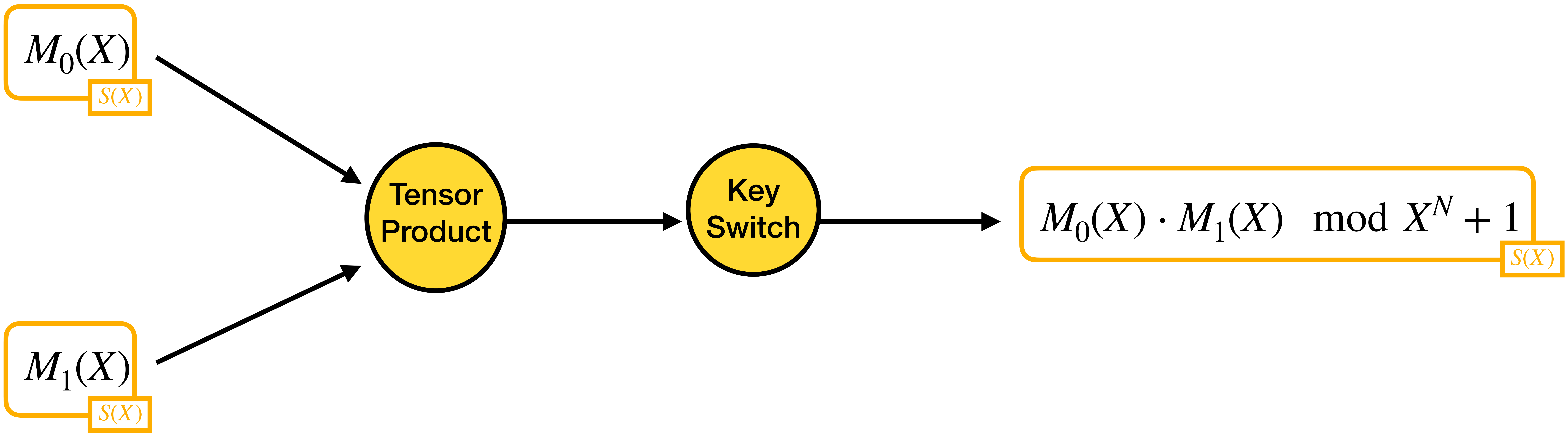
1. TFHE Scheme Overview
2. PBS Many LUTs
3. **BFV Product in TFHE**
4. WoP-PBS
6. Challenges & Conclusion

RLWE Product *a la* B/FV



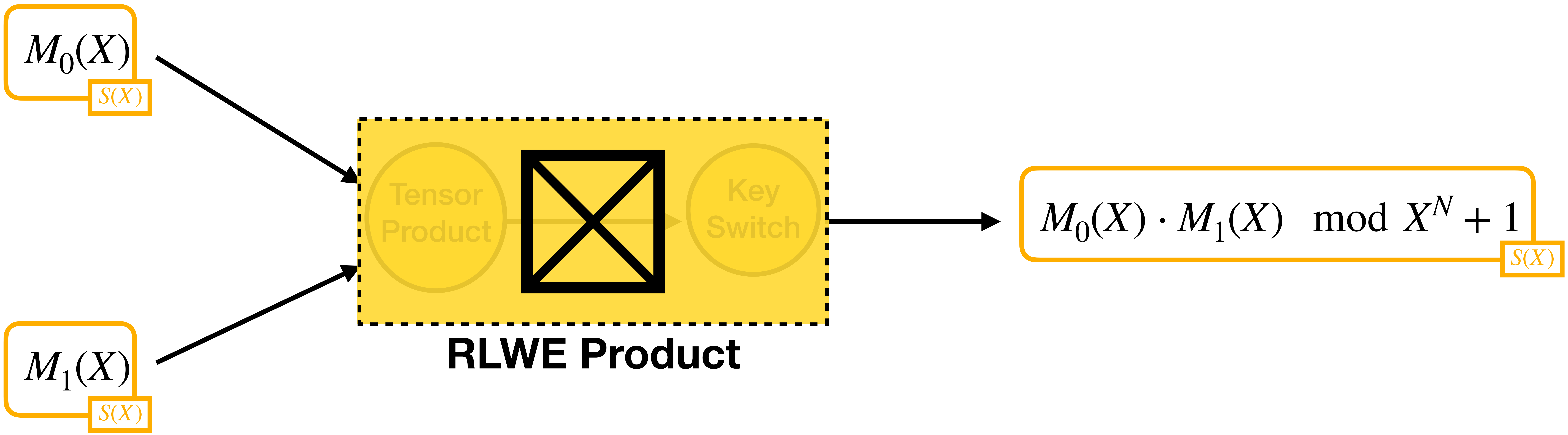
[Bra12] Z. Brakerski. Fully homomorphic encryption without modulus switching from classical gapsvp. CRYPTO 2012.
[FV12] J. Fan, F. Vercauteren. Somewhat practical fully homomorphic encryption. IACR Cryptology ePrint Archive, 2012.

RLWE Product *a la* B/FV



[Bra12] Z. Brakerski. Fully homomorphic encryption without modulus switching from classical gapsvp. CRYPTO 2012.
[FV12] J. Fan, F. Vercauteren. Somewhat practical fully homomorphic encryption. IACR Cryptology ePrint Archive, 2012.

RLWE Product *a la* B/FV



[Bra12] Z. Brakerski. Fully homomorphic encryption without modulus switching from classical gapsvp. CRYPTO 2012.
[FV12] J. Fan, F. Vercauteren. Somewhat practical fully homomorphic encryption. IACR Cryptology ePrint Archive, 2012.

Tight Noise Formulas

$$
\begin{aligned}
\mathsf{Var}(\mathsf{Mult}) = {} & \frac{N}{\Delta^2}\left(\Delta_1^2||M_1||_\infty^2\sigma_2^2+\Delta_2^2||M_2||_\infty^2\sigma_1^2+\sigma_1^2\sigma_2^2\right)+ \\
& + \frac{N}{\Delta^2}\left(\frac{q^2-1}{12}\left(1+kN\mathsf{Var}(S)+kN\mathbb{E}^2(S)\right)+\frac{kN}{4}\mathsf{Var}(S)+\frac{1}{4}(1+kN\mathbb{E}(S))^2\right)(\sigma_1^2+\sigma_2^2)+ \\
& + \frac{1}{12}+\frac{kN}{12\Delta^2}\cdot\left((\Delta^2-1)\cdot\left(\mathsf{Var}(S)+\mathbb{E}^2(S)\right)+3\cdot\mathsf{Var}(S)\right)+\frac{k(k-1)N}{24\Delta^2}\cdot\left((\Delta^2-1)\cdot\left(\mathsf{Var}(S'')+\mathbb{E}^2(S'')\right)+3\cdot\mathsf{Var}(S'')\right)+ \\
& + \frac{kN}{24\Delta^2}\cdot\left((\Delta^2-1)\cdot\left(\mathsf{Var}(S'_{\mathsf{odd}})+\mathsf{Var}(S'_{\mathsf{even}})+2\cdot\mathbb{E}^2(S'_{\mathsf{mean}})\right)+3\cdot\left(\mathsf{Var}(S'_{\mathsf{odd}})+\mathsf{Var}(S'_{\mathsf{even}})\right)\right)+ \\
& +k\ell N\sigma_{\mathsf{RLK}}^2\cdot\frac{(k+1)}{2}\cdot\frac{\mathfrak{B}^2+2}{12}+\frac{kN}{8}\cdot\left((k-1)\cdot\mathsf{Var}(S'')+\mathsf{Var}(S'_{\mathsf{odd}})+\mathsf{Var}(S'_{\mathsf{even}})\right)+ \\
& +\frac{kN}{2}\left(\frac{q^2}{12\mathfrak{B}^{2\ell}}-\frac{1}{12}\right)\left((k-1)\cdot(\mathsf{Var}(S'')+\mathbb{E}^2(S''_{\mathsf{mean}}))+\mathsf{Var}(S'_{\mathsf{odd}})+\mathsf{Var}(S'_{\mathsf{even}})+2\mathbb{E}^2(S'_{\mathsf{mean}})\right)+
\end{aligned}
$$

Tight Noise Formulas

$$
\begin{aligned}
\mathsf{Var}(\mathsf{Mult}) = & \tfrac{N}{\Delta^2}\left(\Delta_1^2||M_1||_\infty^2\sigma_2^2+\Delta_2^2||M_2||_\infty^2\sigma_1^2+\sigma_1^2\sigma_2^2\right)+ \\
& + \tfrac{N}{\Delta^2}\left(\tfrac{q^2-1}{12}\left(1+kN\mathsf{Var}(S)+kN\mathbb{E}^2(S)\right)+\tfrac{kN}{4}\mathsf{Var}(S)+\tfrac{1}{4}(1+kN\mathbb{E}(S))^2\right)(\sigma_1^2+\sigma_2^2)+ \\
& + \tfrac{1}{12}+\tfrac{kN}{12\Delta^2}\cdot\left((\Delta^2-1)\cdot\left(\mathsf{Var}(S)+\mathbb{E}^2(S)\right)+3\cdot\mathsf{Var}(S)\right)+\tfrac{k(k-1)N}{24\Delta^2}\cdot\left((\Delta^2-1)\cdot\left(\mathsf{Var}(S'')+\mathbb{E}^2(S'')\right)+3\cdot\mathsf{Var}(S'')\right)+ \\
& + \tfrac{kN}{24\Delta^2}\cdot\left((\Delta^2-1)\cdot\left(\mathsf{Var}(S'_{\mathsf{odd}})+\mathsf{Var}(S'_{\mathsf{even}})+2\cdot\mathbb{E}^2(S'_{\mathsf{mean}})\right)+3\cdot\left(\mathsf{Var}(S'_{\mathsf{odd}})+\mathsf{Var}(S'_{\mathsf{even}})\right)\right)+ \\
& + k\ell N\sigma_{\mathsf{RLK}}^2\cdot\tfrac{(k+1)}{2}\cdot\tfrac{\mathfrak{B}^2+2}{12}+\tfrac{kN}{8}\cdot\left((k-1)\cdot\mathsf{Var}(S'')+\mathsf{Var}(S'_{\mathsf{odd}})+\mathsf{Var}(S'_{\mathsf{even}})\right)+ \\
& + \tfrac{kN}{2}\left(\tfrac{q^2}{12\mathfrak{B}^{2\ell}}-\tfrac{1}{12}\right)\left((k-1)\cdot(\mathsf{Var}(S'')+\mathbb{E}^2(S''_{\mathsf{mean}}))+\mathsf{Var}(S'_{\mathsf{odd}})+\mathsf{Var}(S'_{\mathsf{even}})+2\mathbb{E}^2(S'_{\mathsf{mean}})\right)+
\end{aligned}
$$

Generic Key Type

Tight Noise Formulas

Generic Key Type

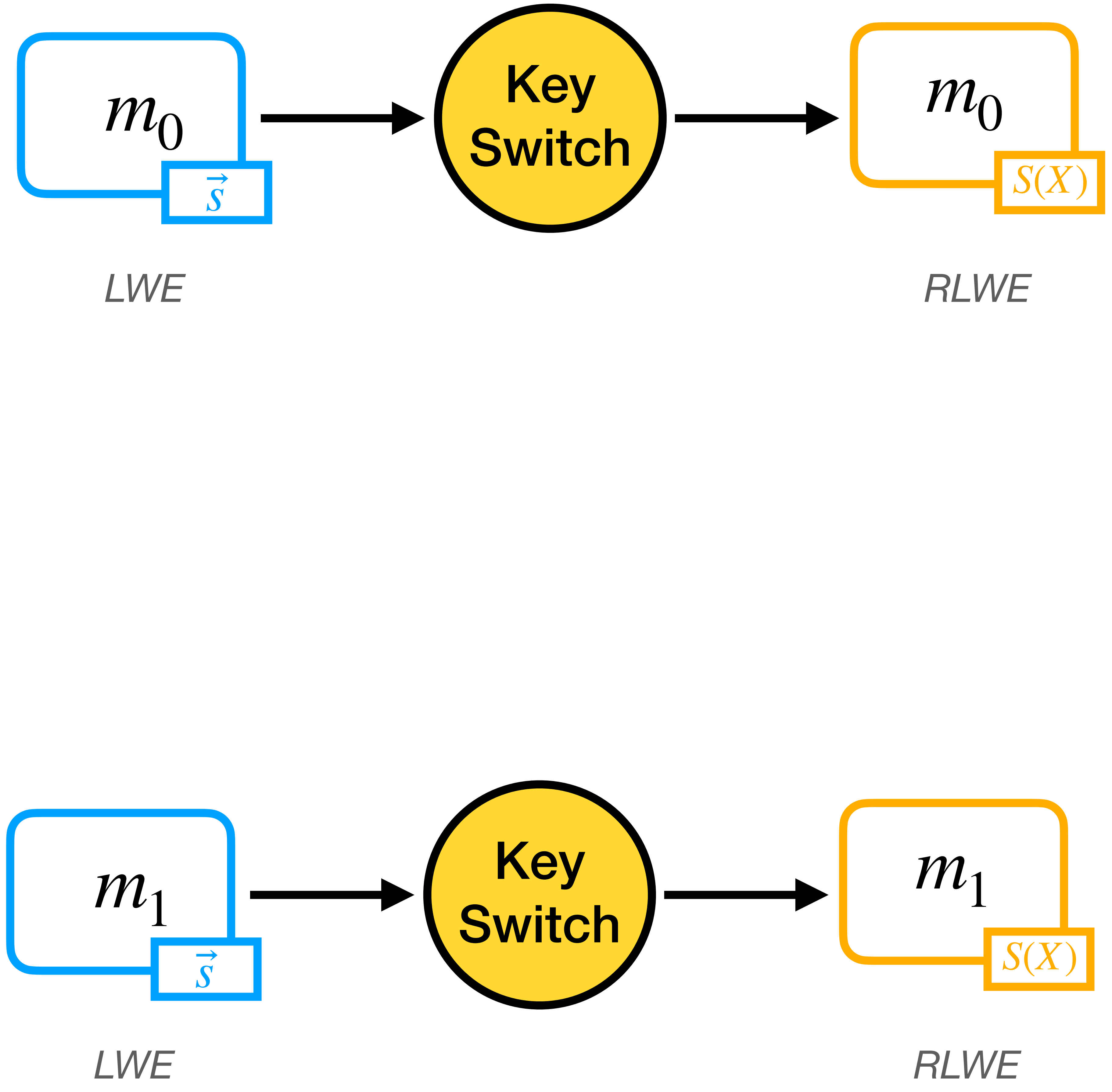
$$
\begin{aligned}
\mathsf{Var}(\mathsf{Mult}) = {} & \frac{N}{\Delta^2}\left(\Delta_1^2\|M_1\|_\infty^2\sigma_2^2+\Delta_2^2\|M_2\|_\infty^2\sigma_1^2+\sigma_1^2\sigma_2^2\right)+\\
& + \frac{N}{\Delta^2}\left(\frac{q^2-1}{12}\left(1+kN\mathsf{Var}(S)+kN\mathbb{E}^2(S)\right)+\frac{kN}{4}\mathsf{Var}(S)+\frac{1}{4}\left(1+kN\mathbb{E}(S)\right)^2\right)(\sigma_1^2+\sigma_2^2)+\\
& + \frac{1}{12}+\frac{kN}{12\Delta^2}\cdot\left((\Delta^2-1)\cdot\left(\mathsf{Var}(S)+\mathbb{E}^2(S)\right)+3\cdot\mathsf{Var}(S)\right)+\frac{k(k-1)N}{24\Delta^2}\cdot\left((\Delta^2-1)\cdot\left(\mathsf{Var}(S'')+\mathbb{E}^2(S'')\right)+3\cdot\mathsf{Var}(S'')\right)+\\
& + \frac{kN}{24\Delta^2}\cdot\left((\Delta^2-1)\cdot\left(\mathsf{Var}(S'_{\mathsf{odd}})+\mathsf{Var}(S'_{\mathsf{even}})+2\cdot\mathbb{E}^2(S'_{\mathsf{mean}})\right)+3\cdot\left(\mathsf{Var}(S'_{\mathsf{odd}})+\mathsf{Var}(S'_{\mathsf{even}})\right)\right)+\\
& + k\ell N\sigma_{\mathsf{RLK}}^2\cdot\frac{(k+1)}{2}\cdot\frac{\mathfrak{B}^2+2}{12}+\frac{kN}{8}\cdot\left((k-1)\cdot\mathsf{Var}(S'')+\mathsf{Var}(S'_{\mathsf{odd}})+\mathsf{Var}(S'_{\mathsf{even}})\right)+\\
& + \frac{kN}{2}\left(\frac{q^2}{12\mathfrak{B}^{2\ell}}-\frac{1}{12}\right)\left((k-1)\cdot(\mathsf{Var}(S'')+\mathbb{E}^2(S''_{\mathsf{mean}}))+\mathsf{Var}(S'_{\mathsf{odd}})+\mathsf{Var}(S'_{\mathsf{even}})+2\mathbb{E}^2(S'_{\mathsf{mean}})\right)+
\end{aligned}
$$

Precision	1	2	3	4	5	6	7	8
Max. depth	32	16	16	8	8	8	8	4
$\log_2(N)$	12	11	12	11	11	12	12	11
$\log_2(\mathfrak{B})$	8	5	8	12	10	8	8	20
ℓ	8	10	8	4	5	8	8	2

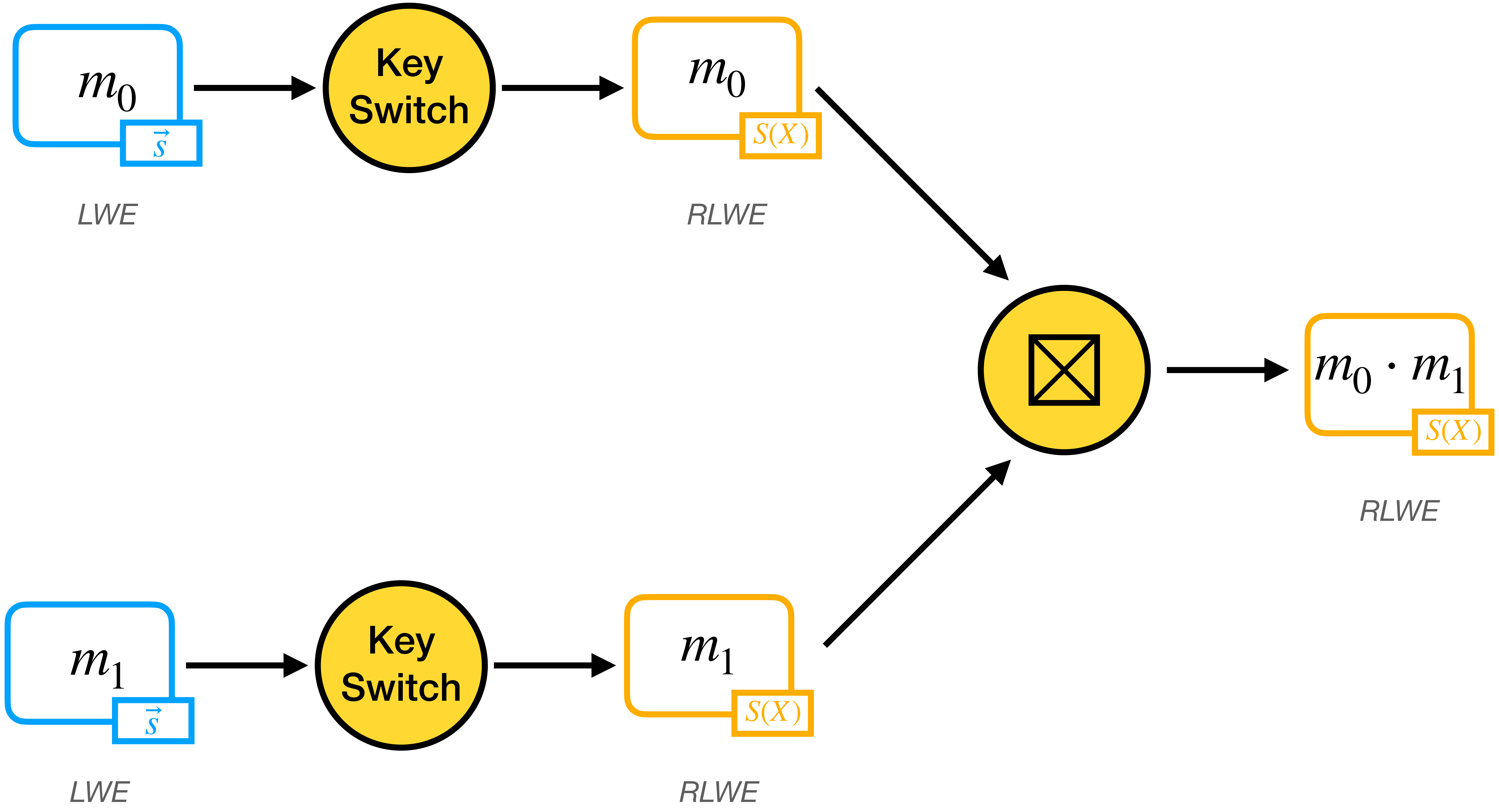
• • •

14	15	16	17	18	19	20	21	22	23	24
2	2	2	2	2	2	2	2	2	2	2
11	11	11	11	11	11	11	12	12	12	12
30	30	20	20	20	20	20	20	20	20	20
1	1	2	2	2	2	2	2	2	2	2

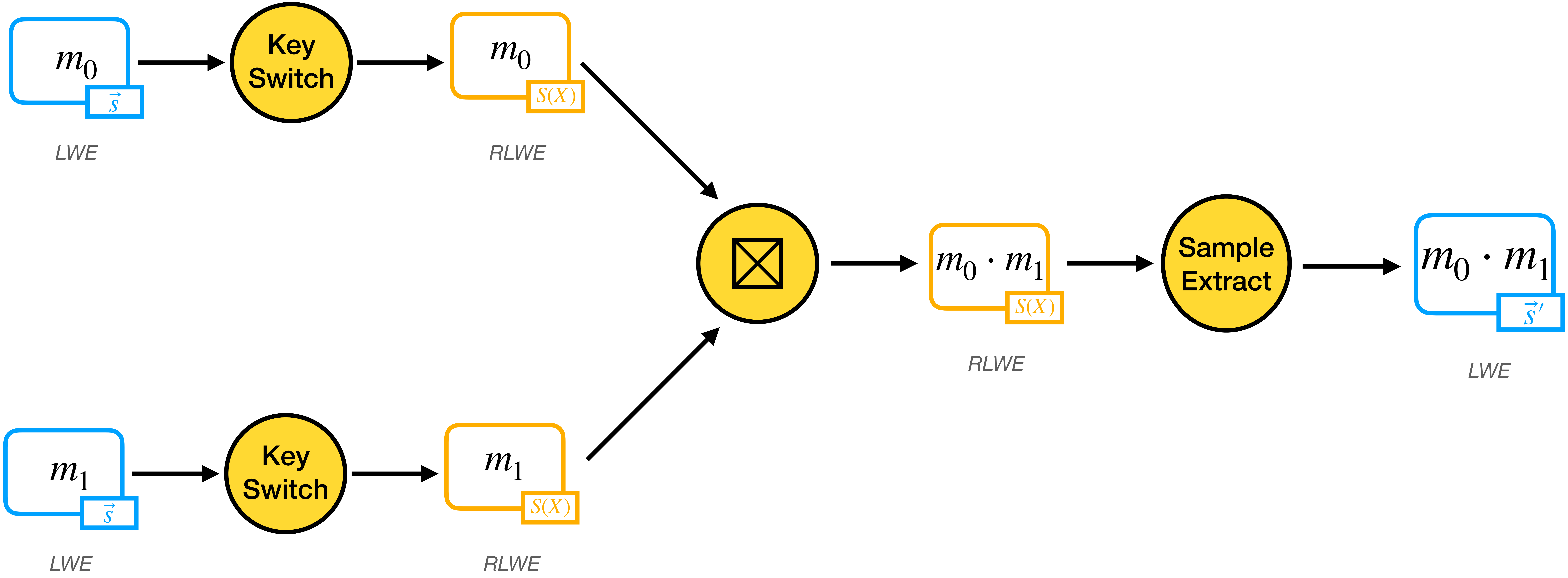
LWE Product Inside TFHE



LWE Product Inside TFHE

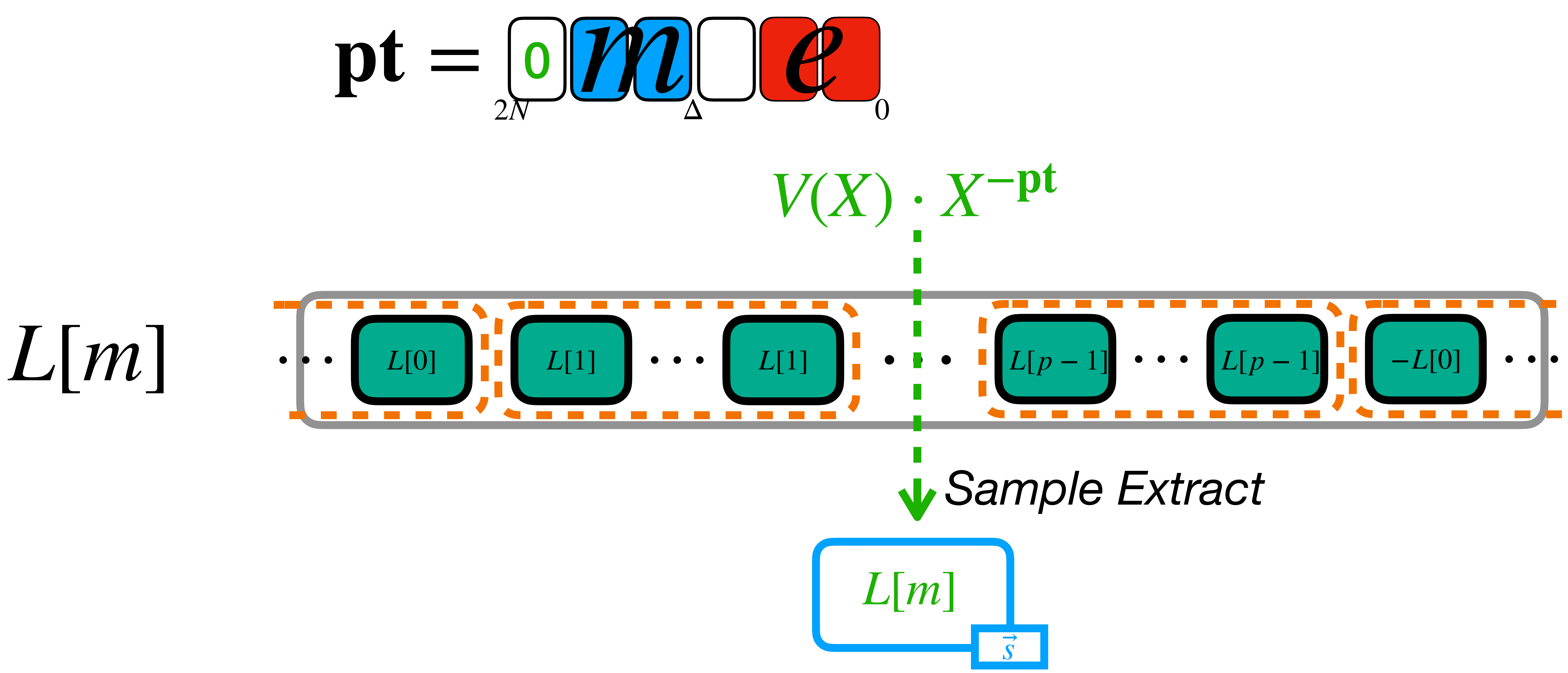


LWE Product Inside TFHE

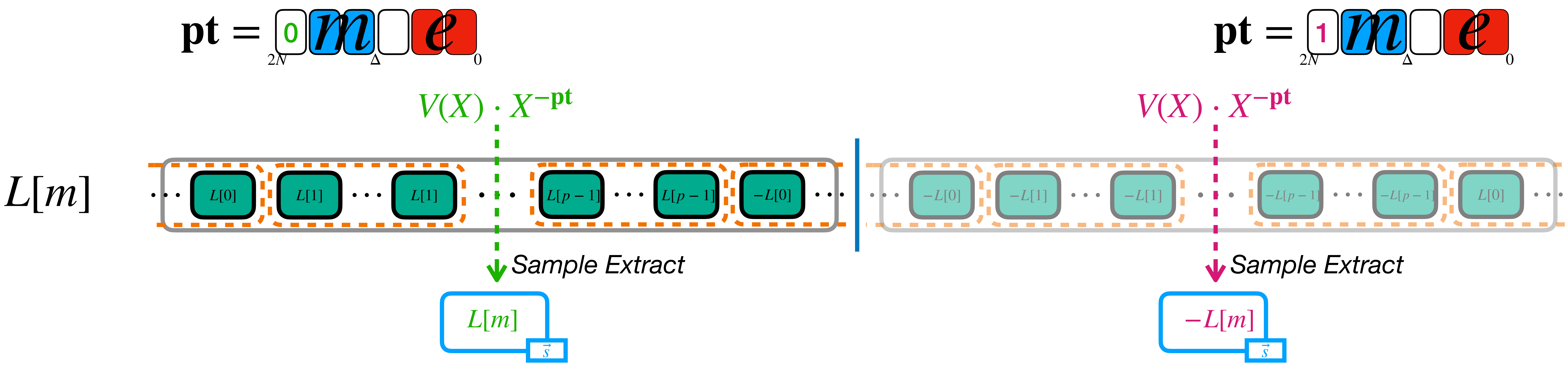


Overview

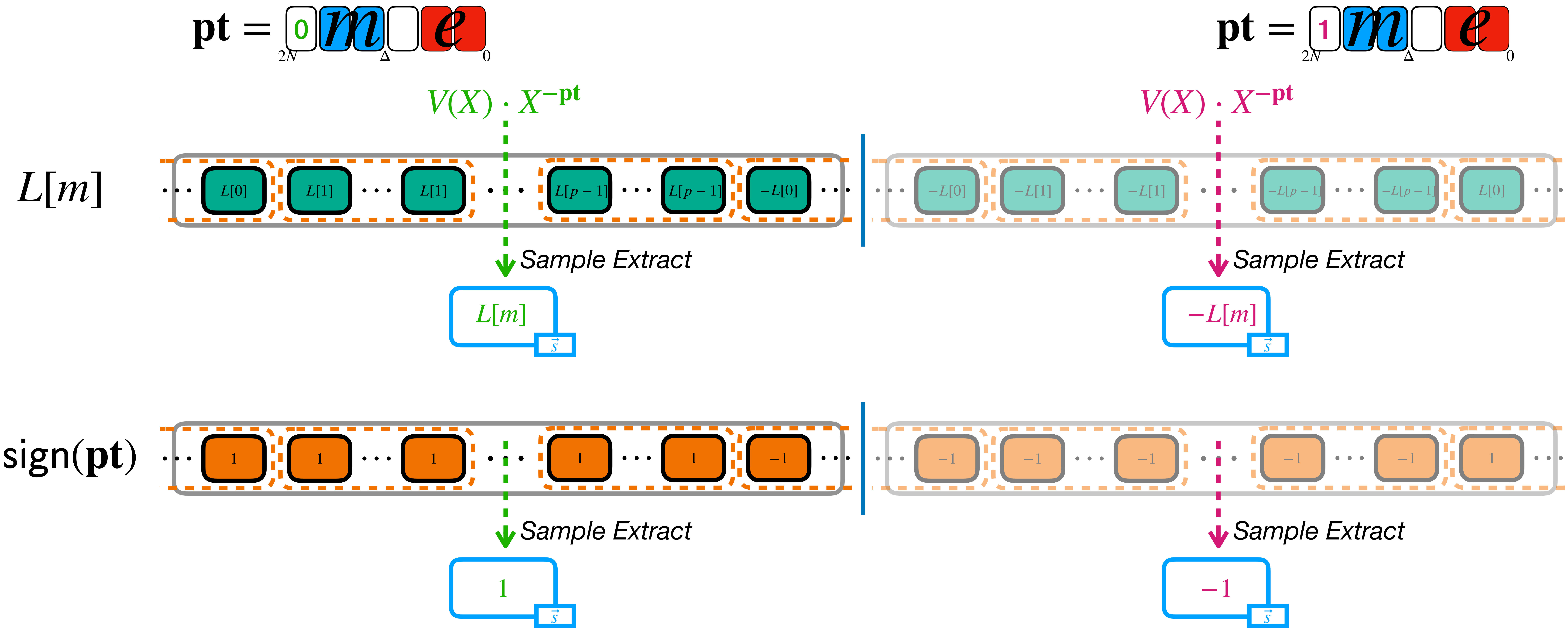
Observe that...



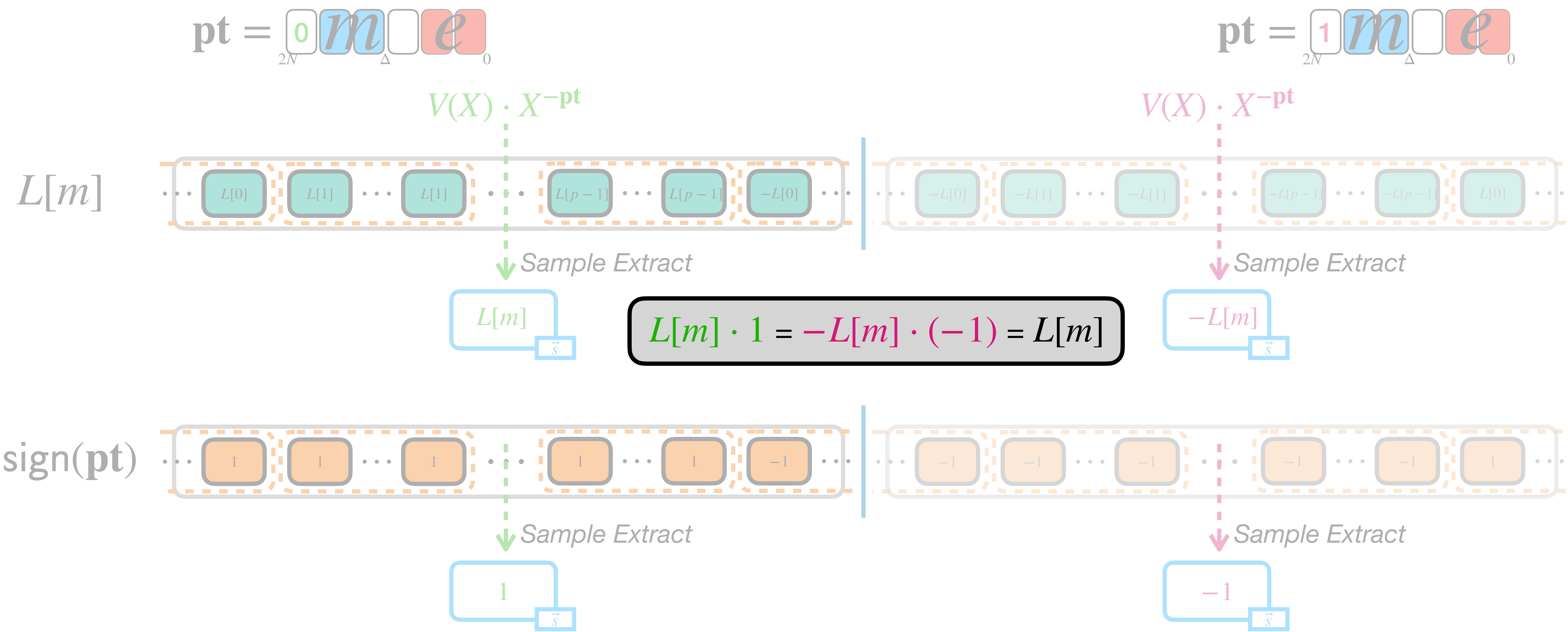
Observe that…



Observe that…



Observe that…

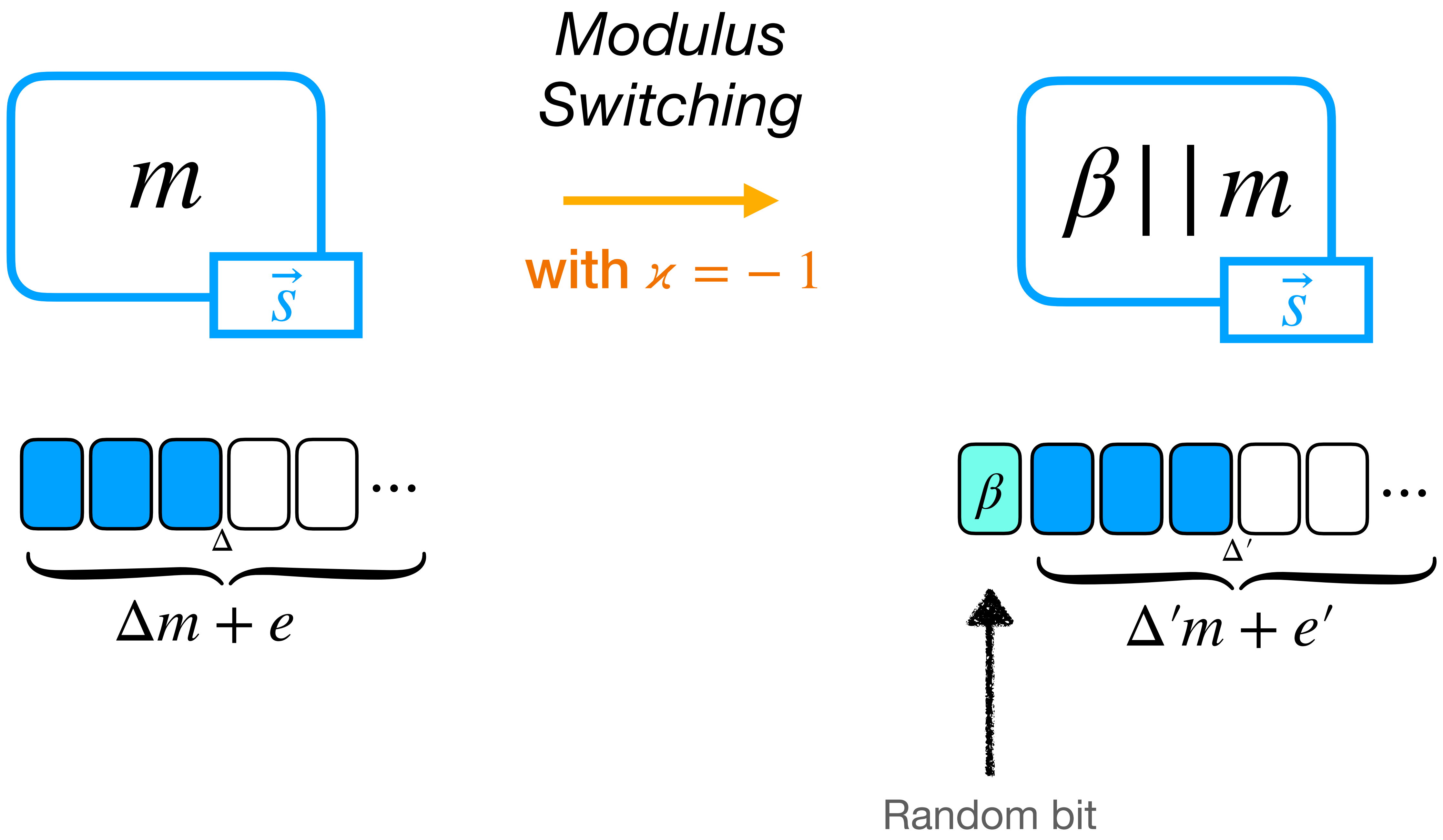


$$L[m] \cdot 1 = -L[m] \cdot (-1) = L[m]$$

WoP-PBS

PBS without padding

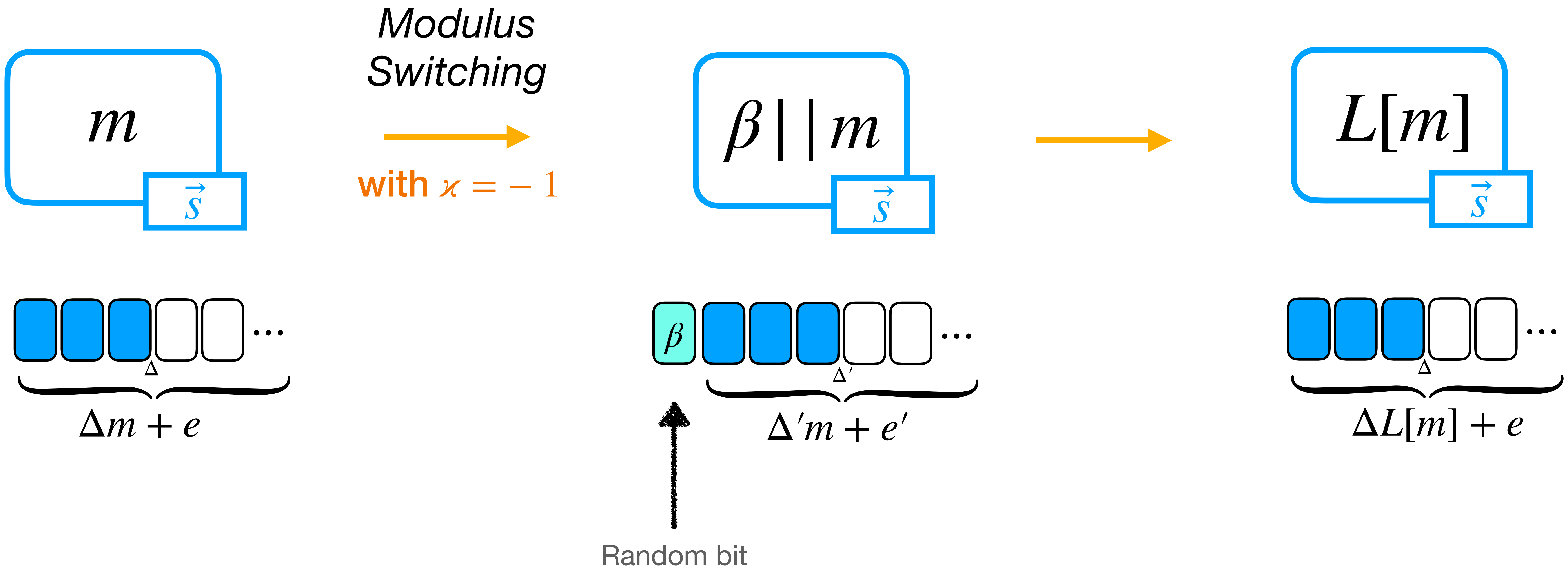
V1



WoP-PBS

PBS without padding

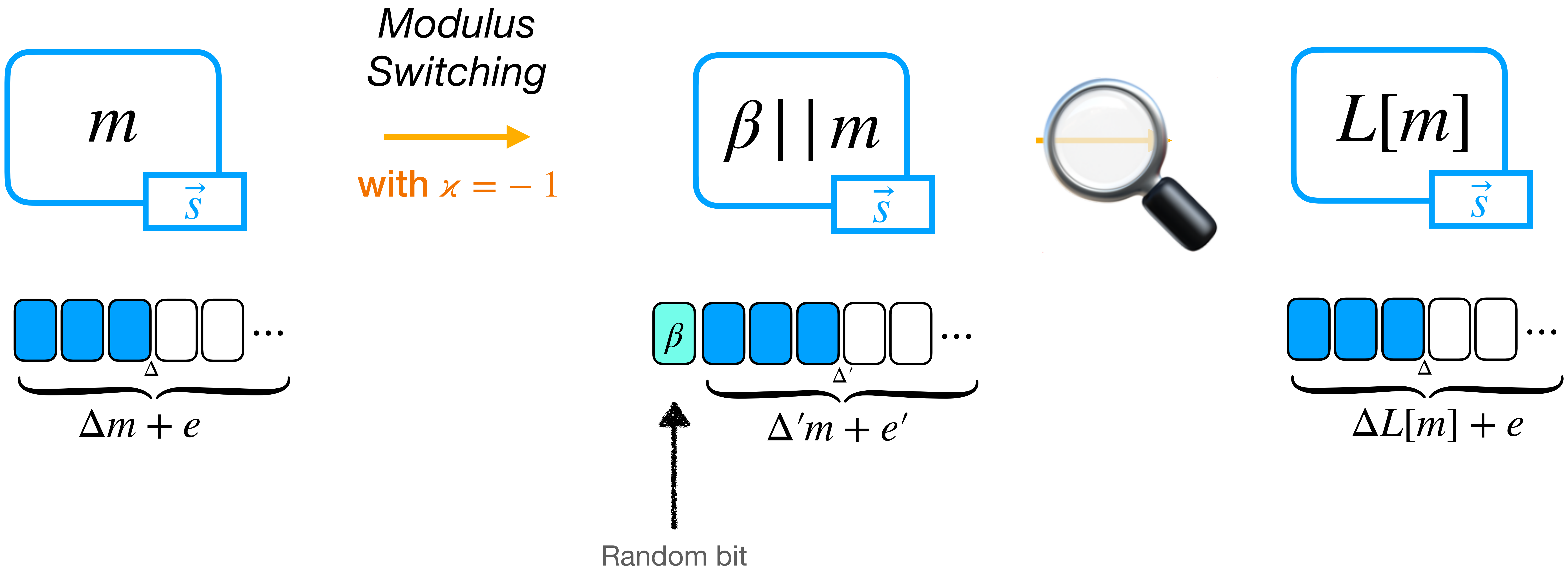
V1



WoP-PBS

PBS without padding

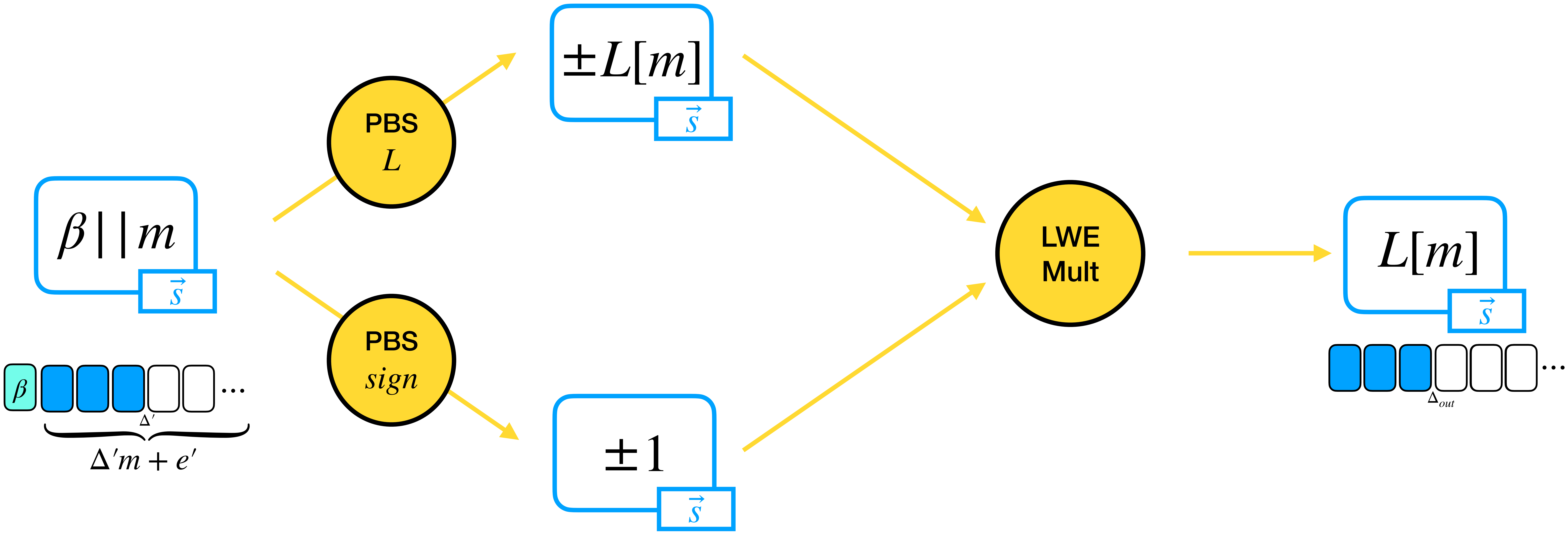
V1



WoP-PBS

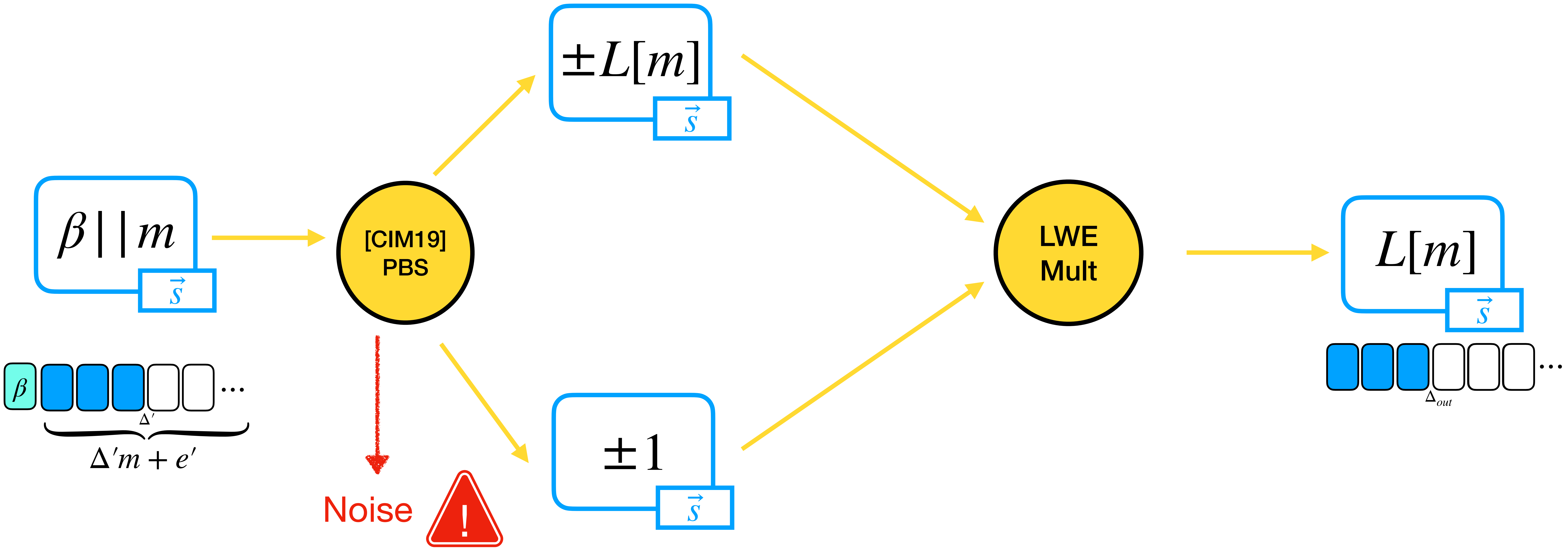
PBS without padding

V1



WoP-PBS

PBS without padding



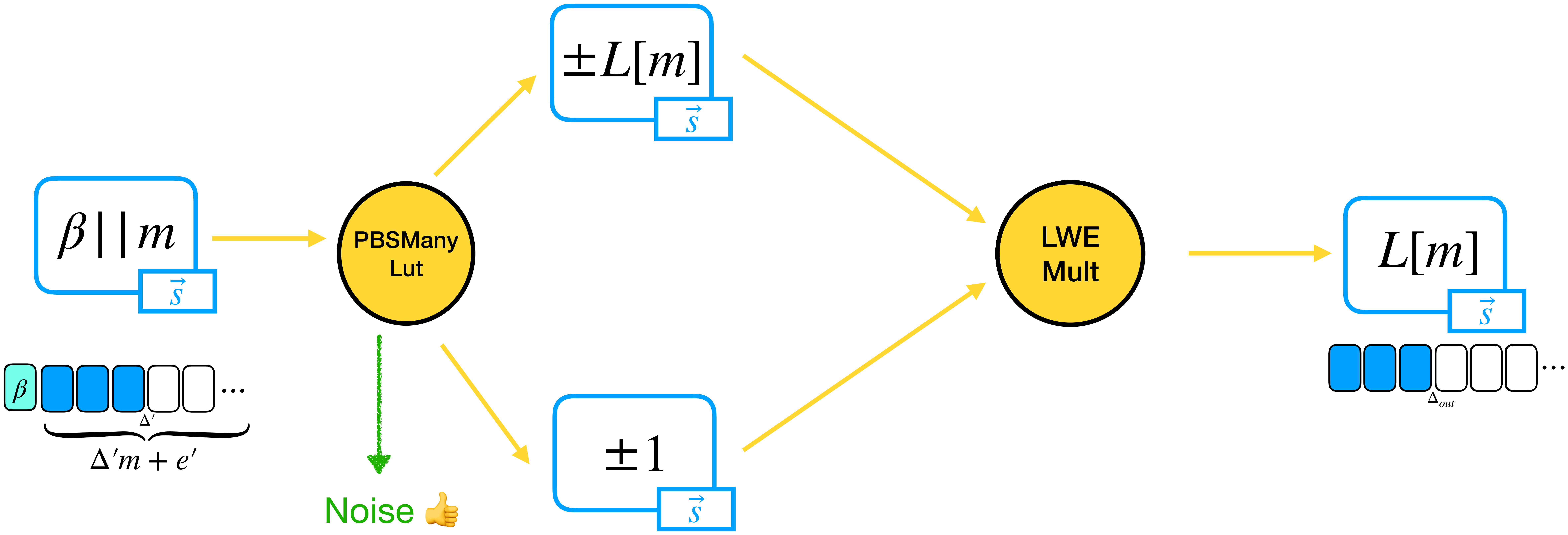
[CIM19] S. Carpov, M. Izabachène, V. Mollimard. New Techniques for Multi-value Input Homomorphic Evaluation and Applications. CT-RSA 2019.

WoP-PBS

PBS without padding

PBS ManyLUT

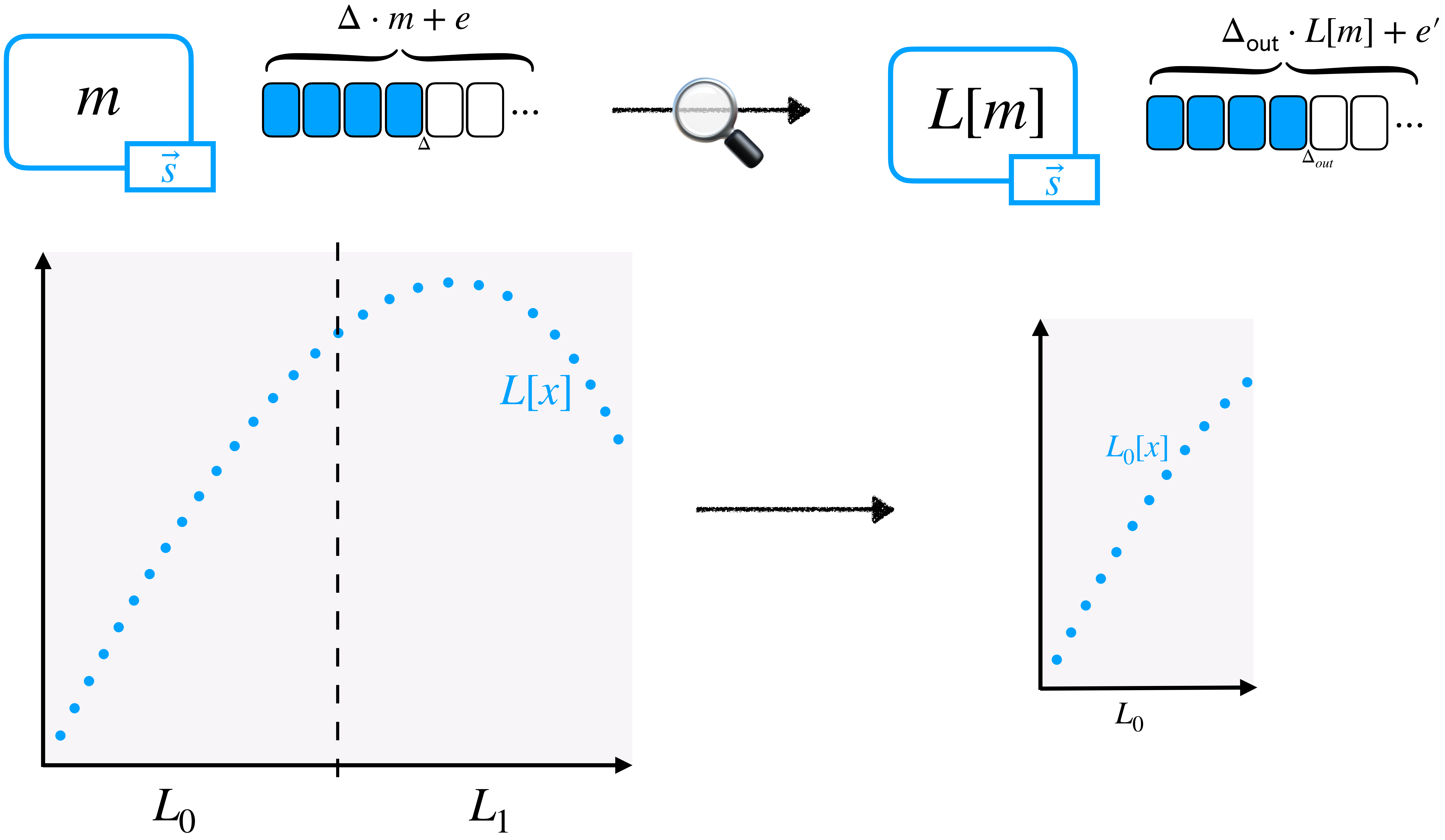
V1



WoP-PBS

PBS without padding

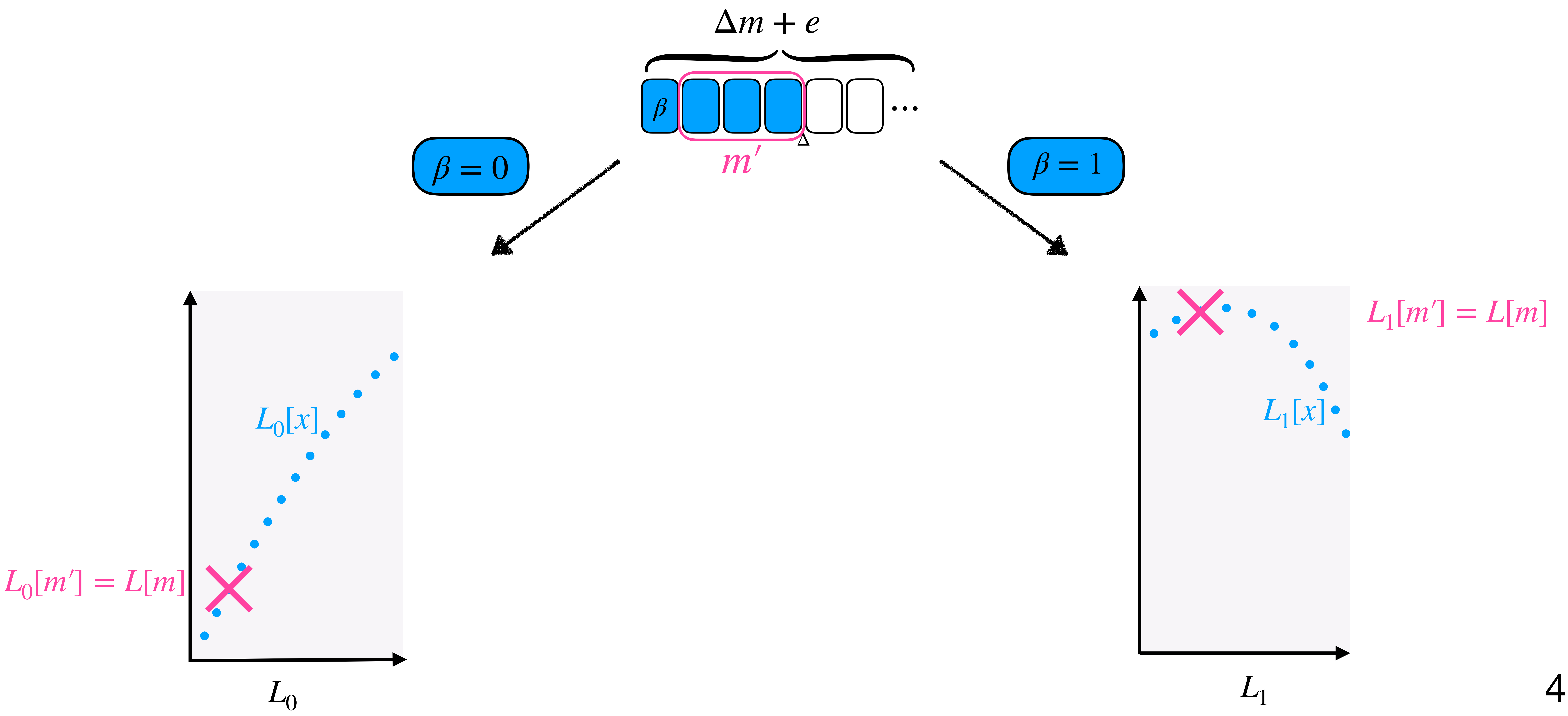
V2



WoP-PBS

PBS without padding

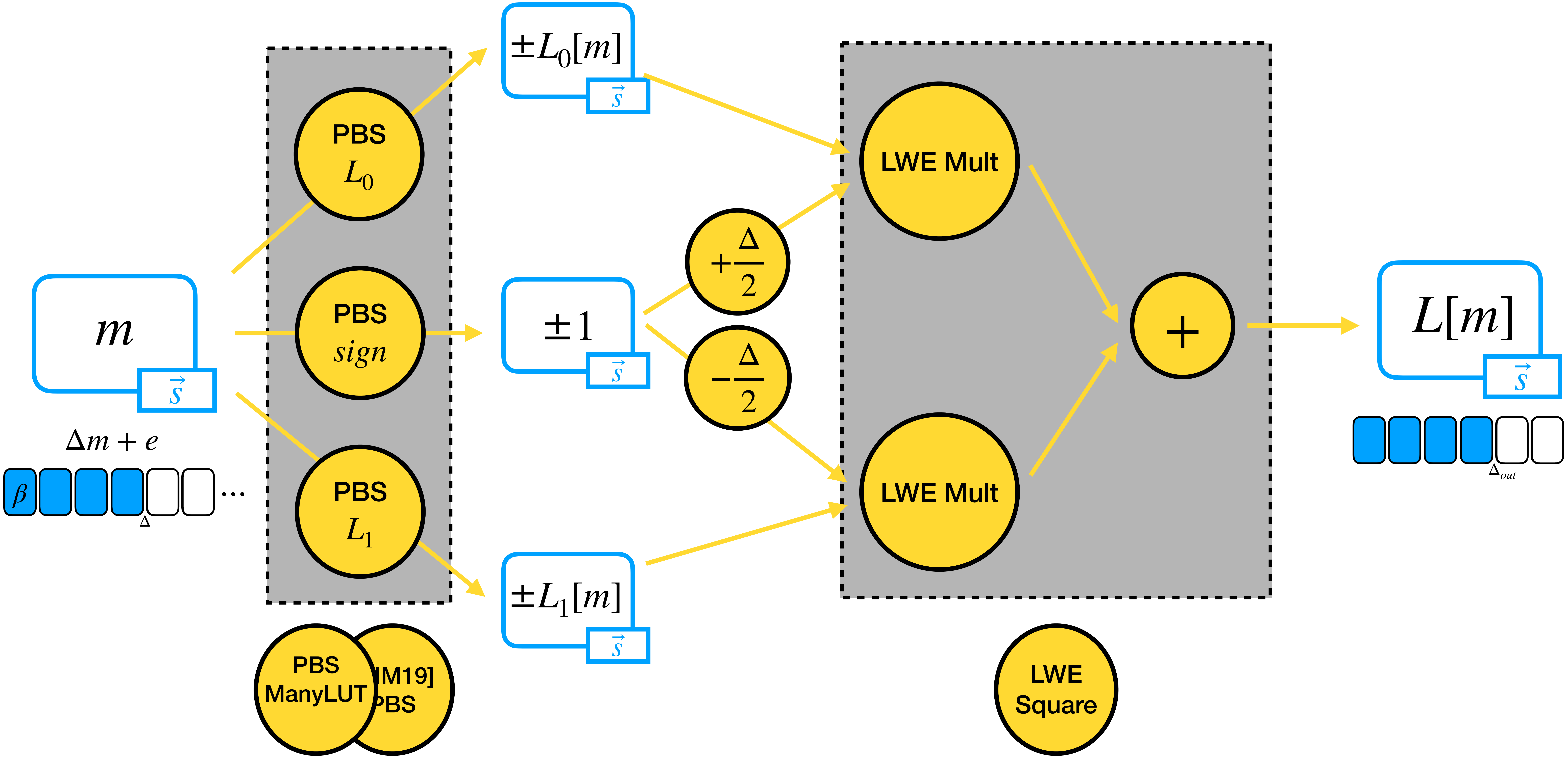
V2



WoP-PBS

PBS without padding

V2



WoP-PBS

Sequential complexity for
a p-bit message

Message / Zero Padding

PBS $= \quad 1 \times$ (PBS) for $(p + 1)$**-bit**

Message / Random Padding

WoP-PBS$_1 \approx \quad 2 \times$ (PBS) for $(p + 1)$**-bit** $+1 \times$ (LWE Mult)

Message

WoP-PBS$_2 \approx \quad 3 \times$ (PBS) for p**-bit** $+2 \times$ (LWE Mult) $+3 \times$ ($+$)

WoP-PBS

Parallel complexity for
a p-bit message

PBS $= \; 1 \times$ PBS for $(p+1)$**-bit**

WoP-PBS$_1 \approx$ ~~2~~ 1 $\times$ PBS for $(p+1)$**-bit** $+1 \times$ LWE Mult

WoP-PBS$_2 \approx$ ~~3~~ 1 $\times$ PBS for p**-bit** $+$ ~~2~~ 1 $\times$ LWE Mult $+$ ~~3~~ 2 $\times$ $+$

Easy to parallelize!

Overview

1. TFHE Scheme Overview
2. PBS Many LUTs
3. BFV Product in TFHE
4. WoP-PBS
6. Challenges & Conclusion

Conclusion

Our contributions

In this presentation

- BFV-like Multiplication in TFHE
- Evaluate several LUTs at once: PBS Many LUT
- Bootstrapping Without Padding: WoP-PBS$_1$ and WoP-PBS$_2$

More in the paper

- **Generic tight** noise analysis
- Efficient **Circuit Bootstrapping**
- Efficient **ciphertext splitting** in chunks.
  - **Large Precision PBS**
- Efficient **Gate Bootstrapping** approach and extension to **arithmetic circuits**

→ used for

Open Problems

- Fast **FFT** with higher precision
- Experiment with **hardware implementations**
- Reduce **noise growth** in WoP-PBS
- **Improve** LWE $\longrightarrow$ GLWE Key Switching

Thank you

Q&A

Ilaria Chillotti ilaria.chillotti@zama.ai

Damien Ligier damien.ligier@zama.ai

Jean-Baptiste Orfila jb.orfila@zama.ai

Samuel Tap samuel.tap@zama.ai