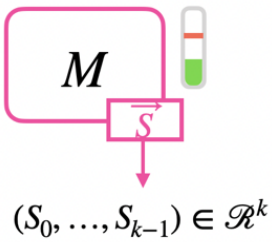
# TFHE

Rümeysa Bilik

Sabancı University PURE Summer'24

2024, July

# TLWE Encryption

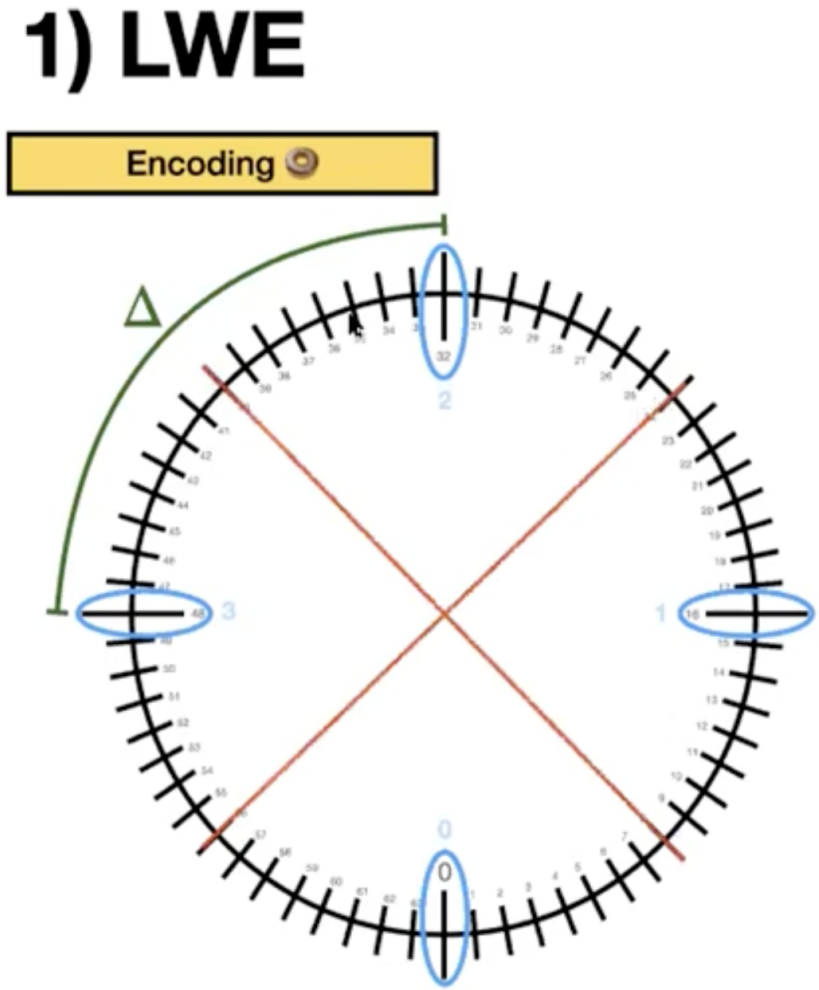



$$= \overbrace{(A_0, \ldots, A_{k-1}, B)}^{k+1} \quad \text{where} \quad B = \sum_{i=0}^{k-1} A_i \cdot S_i + \Delta M + E \in \mathcal{R}_q$$

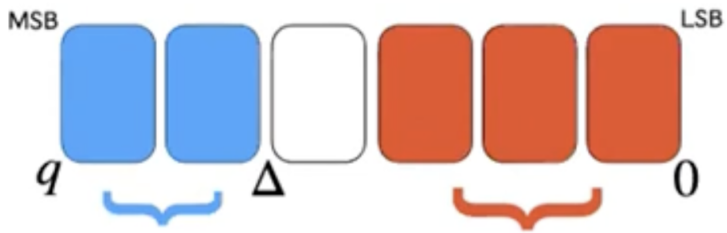
$A_i \in \mathcal{R}_q$ uniform random

$E \in \mathcal{R}_q$ Gaussian coefficients

# TLWE Torus Representation




$$\begin{cases} q = 64 = 2^6 \\ p = 4 = 2^2 \\ \Delta = \dfrac{q}{p} = 16 = 2^4 \end{cases}$$




$\mathcal{M} = \{0,1,2,3\}$

$\text{Encode}(m) = \Delta m$

$|e| < \dfrac{\Delta}{2} = 8 = 2^3$

# TLWE Decryption

**Decryption**

1. $B - \sum_{i=0}^{k-1} A_i \cdot S_i = \Delta M + E$
2. $\lfloor (\Delta M + E)/\Delta \rceil = M$

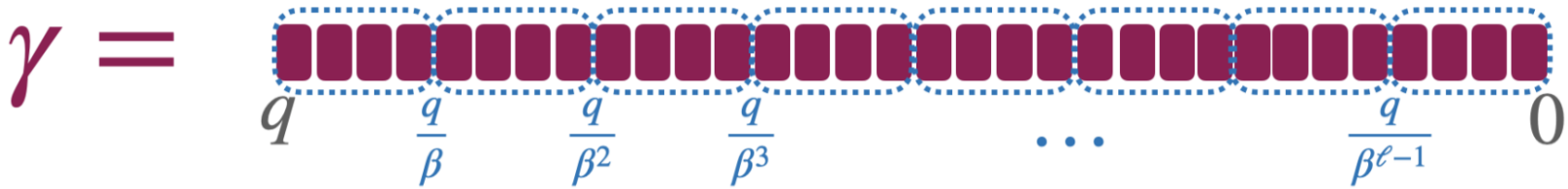
# GLev

$$\left(GLWE^{\vec{}}_{S,\sigma}\left(\frac{q}{\beta^1}M\right)\times\ldots\times GLWE^{\vec{}}_{S,\sigma}\left(\frac{q}{\beta^\ell}M\right)\right)=GLev^{\beta,\ell}_{\vec{S},\sigma}(M)\subseteq\mathcal{R}_q^{\ell\cdot(k+1)}.$$

# GGSW

$$\left(GLev^{\beta,\ell}_{\vec{S},\sigma}(-S_0 M) \times \ldots \times GLev^{\beta,\ell}_{\vec{S},\sigma}(-S_{k-1} M) \times GLev^{\beta,\ell}_{\vec{S},\sigma}(M)\right) = GGSW^{\beta,\ell}_{\vec{S},\sigma}(M) \subseteq \mathcal{R}_q^{(k+1)\times \ell(k+1)}.$$

# Decomposition Operation



# External Product

**Definition 3.12 (External product).** *We define the product* $\boxdot$ *as*

$$\boxdot : \mathsf{TGSW} \times \mathsf{TLWE} \longrightarrow \mathsf{TLWE}$$
$$(A, \boldsymbol{b}) \longmapsto A \boxdot \boldsymbol{b} = Dec_{H,\beta,\epsilon}(\boldsymbol{b}) \cdot A,$$

# Internal Product

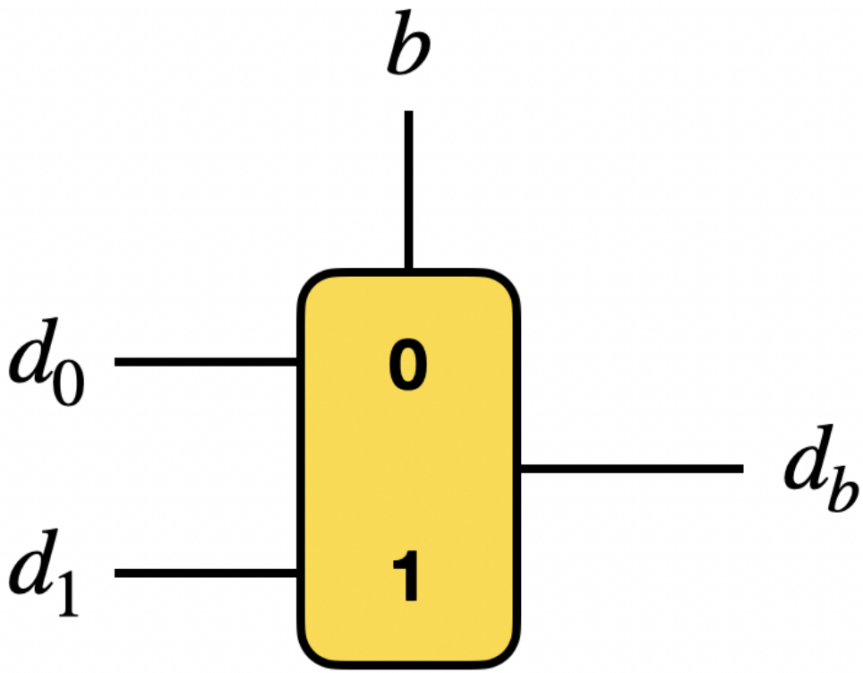
**Corollary 3.15 (Internal Product).** *Let the product*

$$\boxtimes\colon \mathsf{TGSW} \times \mathsf{TGSW} \longrightarrow \mathsf{TGSW}$$

$$(A, B) \longmapsto A \boxtimes B = \begin{bmatrix} A \boxdot \boldsymbol{b_1} \\ \vdots \\ A \boxdot \boldsymbol{b_{(k+1)\ell}} \end{bmatrix} = \begin{bmatrix} Dec_{H,\beta,\epsilon}(\boldsymbol{b_1}) \cdot A \\ \vdots \\ Dec_{H,\beta,\epsilon}(\boldsymbol{b_{(k+1)\ell}}) \cdot A \end{bmatrix},$$

*with $A$ and $B$ two valid* TGSW *samples of messages $\mu_A$ and $\mu_B$ respectively and $\boldsymbol{b_i}$ corresponding to the $i$-th line of $B$. Then $A \boxtimes B$ is a* TGSW *sample of message $\mu_A \cdot \mu_B$ and*

# CMux Gate




- $b.(d_1 - d_0) + d_0 = d_b$

# Key Switching

$$C' = \underbrace{\overbrace{(0,\ldots,0,B)}^{\text{Trivial GLWE of } B} - \sum_{i=0}^{k-1} \overbrace{\langle \mathsf{Decomp}^{\beta,\ell}(A_i), \mathsf{KSK}_i \rangle}^{\text{GLWE encryption of } A_i S_i}}_{\text{GLWE encryption of } B - \sum_{i=0}^{k-1} A_i S_i = \Delta M + E} \in GLWE^{\vec{}}_{S',\sigma'}(\Delta M) \subseteq \mathcal{R}_q^{k+1}.$$

# Sample Extraction

$$S(X) = S_0 + S_1X + \ldots + S_{N-1}X^{N-1}$$

RLWE $\quad M(X)_{S(X)} = A(X)\ B(X)$

$M_0 + M_1X + \ldots + M_{N-1}X^{N-1} \qquad (A_0 + A_1X + \ldots + A_{N-1}X^{N-1}, B_0 + B_1X + \ldots + B_{N-1}X^{N-1})$

LWE $\quad M_{0\,\vec{s}} = \vec{a}\ b$

$$\begin{cases} a_0 = A_0 \\ a_1 = -A_{N-1} \\ \vdots \\ a_{n-1} = -A_1 \\ b = B_0 \end{cases}$$

$$\begin{cases} \vec{s} = (s_0 = S_0, \ldots, s_{n-1} = S_{N-1}) \\ n = N \end{cases}$$

All the other coefficients can be extracted in a similar way

2

# Blind Rotation

## Rotation

**Rotate a polynomial $M(X)$ of $p$ positions**

$$\cdot X^{-p} \quad \begin{cases} M(X) = M_0 + M_1 X + \ldots + M_p X^p + \ldots + M_{N-1} X^{N-1} \\ M(X) \cdot X^{-p} = M_p + M_{p+1} X + \ldots + M_{N-1} X^{N-p-1} - M_0 X^{N-p} - \ldots - M_{p-1} X^{N-1} \end{cases} \quad \text{mod } X^N + 1, \; X^N = -1$$

**Rotate an encrypted polynomial $M(X)$ of $p$ positions**

$$\boxed{M}_{S} \cdot X^{-p} = \boxed{M \cdot X^{-p}}_{S}$$

$$\boxed{A}\boxed{B} \cdot X^{-p} = \boxed{A \cdot X^{-p}}\boxed{B \cdot X^{-p}}$$

# Blind Rotation

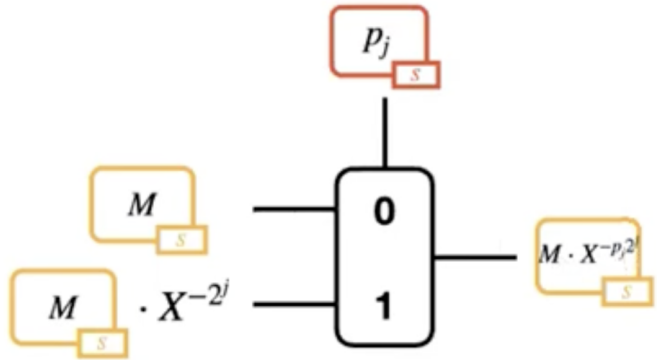
**Rotate an encrypted polynomial $M(X)$ of $p$ encrypted positions**

$$p = p_0 \cdot 2^0 + \ldots + p_j 2^j + \ldots + p_k \cdot 2^k$$

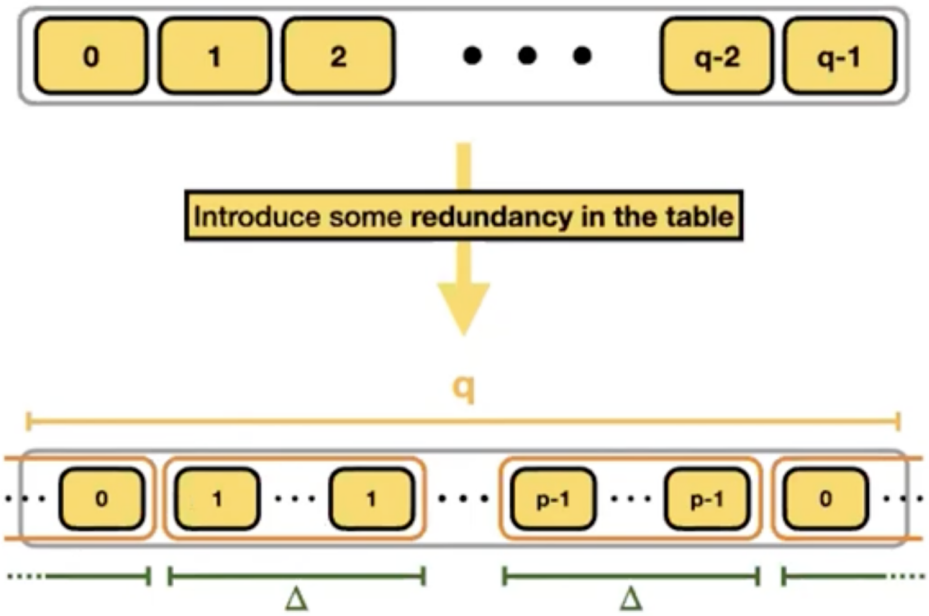
Secret — Known Constant

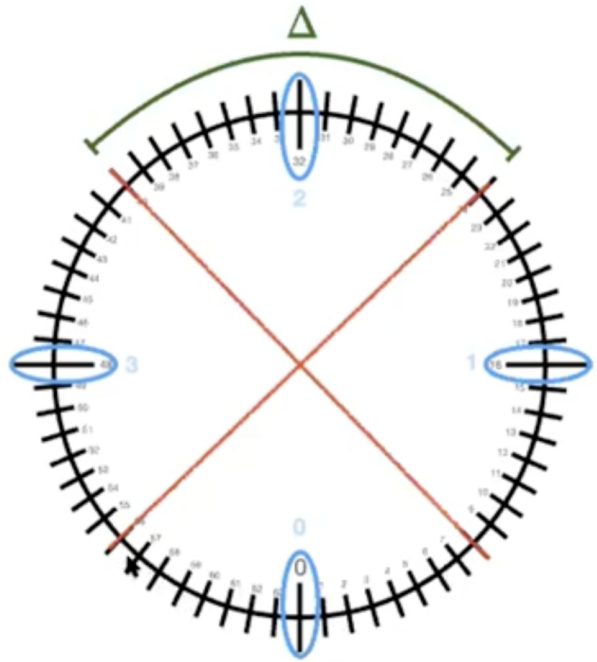

$$M \cdot X^{-p} = M \cdot X^{-p_0 \cdot 2^0 - \ldots - p_j 2^j - \ldots - p_k \cdot 2^k}$$
$$= M \cdot X^{-p_0 \cdot 2^0} \cdot \ldots \cdot X^{-p_j 2^j} \cdot \ldots \cdot X^{-p_k \cdot 2^k}$$

$$M \cdot X^{-p_j 2^j} = \begin{cases} M & \text{if } p_j = 0 \\ M \cdot X^{-2^j} & \text{if } p_j = 1 \end{cases}$$



# Bootstrapping



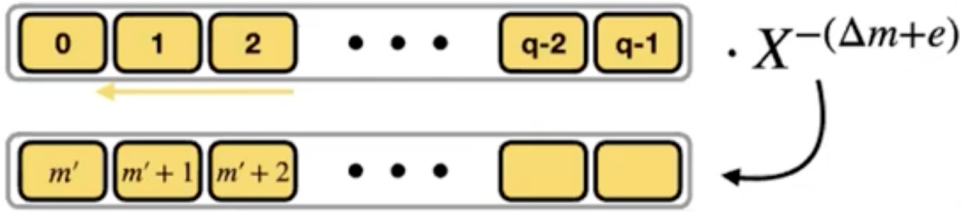



# Bootstrapping

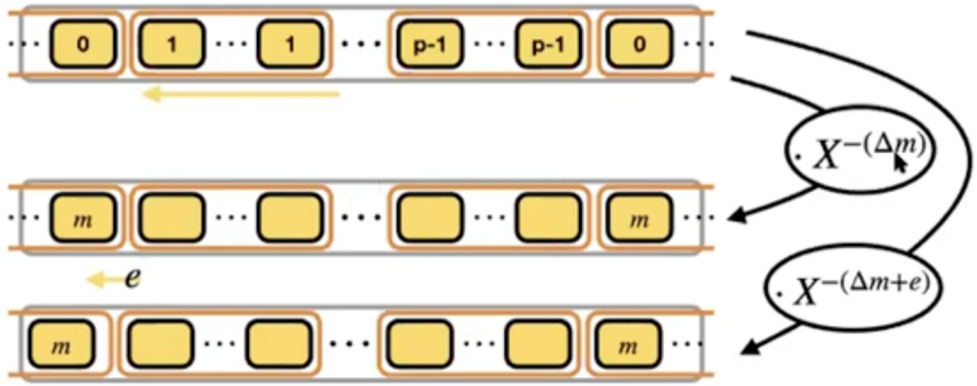
## Bootstrapping

Let's start from **step 2** (the rounding of $\Delta m + e$)

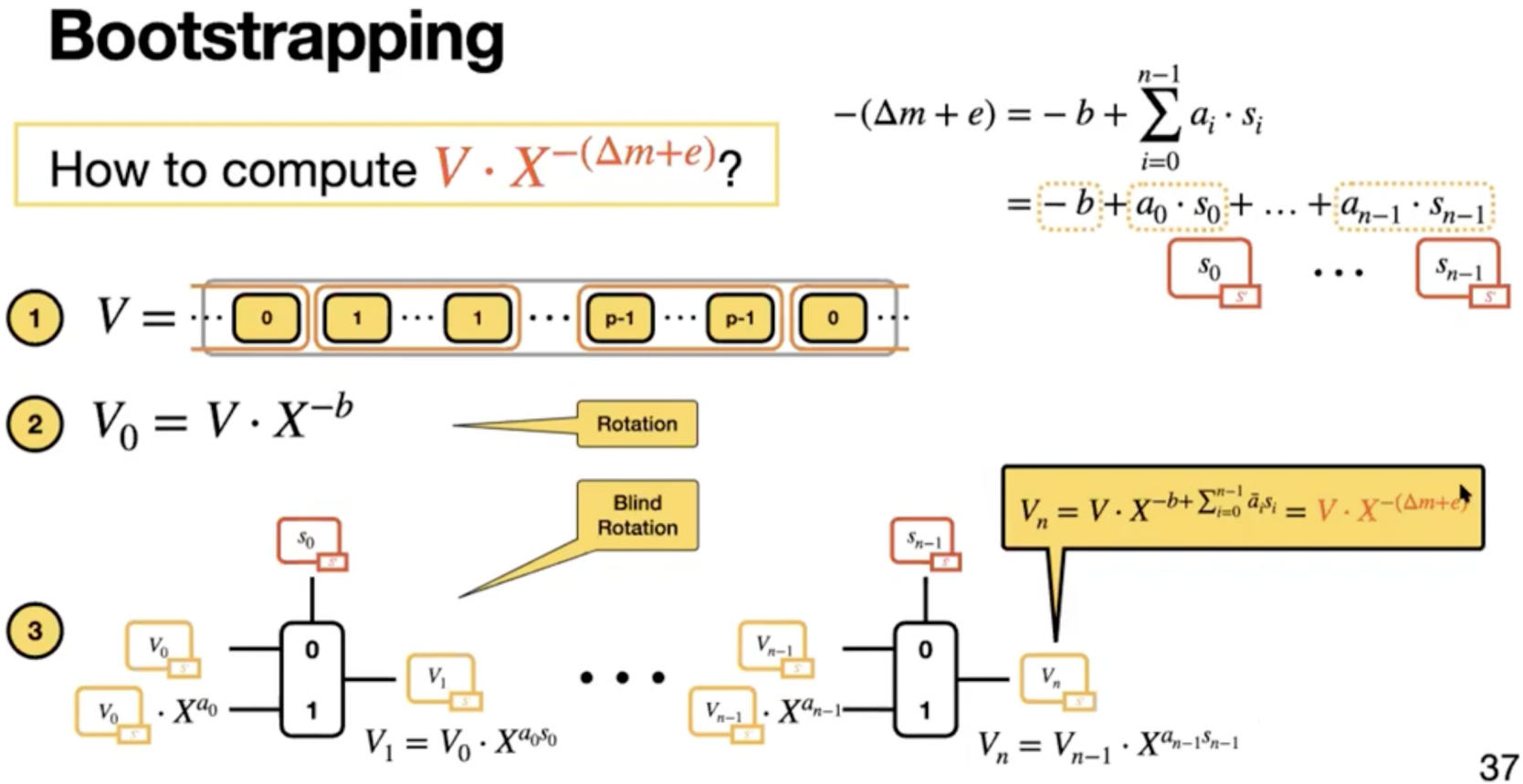
$$m' = \Delta m + e \in \{0,1,\ldots,q-1\}$$




$$\Delta m + e \to \lceil \Delta m + e \rfloor = m$$



# Bootstrapping



# Bootstrapping