$n=4 \qquad q_L = 32 \qquad h=4 \qquad p=7$

$s \leftarrow HWT(h)$ $\qquad$ $e, e' \leftarrow DG_1(\sigma^2)$

$$s = \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix} \qquad e = \begin{pmatrix} 3 \\ -2 \\ 0 \\ 1 \end{pmatrix}, \; e' = \begin{pmatrix} 2 \\ 1 \\ 4 \\ 0 \end{pmatrix} \qquad a = \begin{pmatrix} 5 \\ -7 \\ 2 \\ -3 \end{pmatrix} \qquad a' = \begin{pmatrix} 4 \\ 5 \\ 1 \\ -3 \end{pmatrix}$$

Key Generation

$$pk = (-a \odot s \oplus e, a)$$

$$= \left(-\begin{pmatrix} 5 \\ -7 \\ 2 \\ -3 \end{pmatrix} \odot \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix} \oplus \begin{pmatrix} 3 \\ -2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 5 \\ -7 \\ 2 \\ -3 \end{pmatrix} \right) \quad \text{mod } q_L$$

$$= \left(\begin{pmatrix} -2 \\ 5 \\ -2 \\ -2 \end{pmatrix}, \begin{pmatrix} 5 \\ -7 \\ 2 \\ -3 \end{pmatrix} \right) \quad \text{mod } q_L$$

$$= \left(\begin{pmatrix} 30 \\ 5 \\ 30 \\ 30 \end{pmatrix}, \begin{pmatrix} 5 \\ 25 \\ 2 \\ 29 \end{pmatrix} \right)$$

$$sk = (1, s) = \left(1, \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix}\right)$$

$$evk = (((-a' \odot s) \oplus e' \oplus (p \cdot s \otimes s)), a')$$

$$= \left(\left(\left(-\begin{pmatrix} 4 \\ 5 \\ 1 \\ -3 \end{pmatrix} \odot \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix} \right) \oplus \begin{pmatrix} 2 \\ 1 \\ 1 \\ 0 \end{pmatrix} \oplus \left(7 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix} \odot \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix} \right), \begin{pmatrix} 4 \\ 5 \\ 1 \\ -3 \end{pmatrix} \right) \quad \text{mod } p \cdot q_L$$

$$= \left(\left(\begin{pmatrix} -2 \\ -4 \\ 0 \\ -3 \end{pmatrix} \oplus \begin{pmatrix} 7 \\ 7 \\ 7 \\ 7 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 1 \\ -3 \end{pmatrix} \right) \right) \quad \text{mod } p \cdot q_L$$

$$= \left(\begin{pmatrix} 5 \\ 3 \\ 7 \\ 4 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 1 \\ -3 \end{pmatrix} \right) = \left(\begin{pmatrix} 5 \\ 3 \\ 7 \\ 4 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 1 \\ 221 \end{pmatrix} \right)$$

✓