Encryption

$$m = \begin{pmatrix} 5 \\ 11 \\ 0 \\ 4 \end{pmatrix} \qquad v = \begin{pmatrix} -1 \\ 1 \\ 1 \\ -1 \end{pmatrix} \qquad e_0 = \begin{pmatrix} 1 \\ -3 \\ 0 \\ 4 \end{pmatrix} \qquad e_1 = \begin{pmatrix} -2 \\ -3 \\ 5 \\ 1 \end{pmatrix}$$

$$\mathrm{Enc}_{pk}(m) = \left(v \odot b \oplus m \oplus e_0 ,\ v \odot a + e_1 \right)$$

$$= \left(\begin{pmatrix} -1 \\ 1 \\ 1 \\ -1 \end{pmatrix} \odot \begin{pmatrix} 30 \\ 5 \\ 30 \\ 30 \end{pmatrix} \oplus \begin{pmatrix} 5 \\ 11 \\ 0 \\ 4 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ -3 \\ 0 \\ 4 \end{pmatrix},\ \begin{pmatrix} -1 \\ 1 \\ 1 \\ -1 \end{pmatrix} \odot \begin{pmatrix} 9 \\ 25 \\ 2 \\ 29 \end{pmatrix} + \begin{pmatrix} -2 \\ -3 \\ 5 \\ 1 \end{pmatrix} \right) \bmod q_L$$

$$= \left(\begin{pmatrix} -24 \\ 13 \\ 30 \\ -22 \end{pmatrix},\ \begin{pmatrix} -7 \\ 22 \\ 7 \\ -28 \end{pmatrix} \right) \bmod q_L$$

$$= \left(\begin{pmatrix} 8 \\ 13 \\ 30 \\ 10 \end{pmatrix},\ \begin{pmatrix} 25 \\ 22 \\ 7 \\ 4 \end{pmatrix} \right) = X$$

Decryption

$$\mathrm{Dec}_{sk}(x) = x_1 \oplus x_2 \odot s$$

$$= \begin{pmatrix} 8 \\ 13 \\ 30 \\ 10 \end{pmatrix} \oplus \begin{pmatrix} 25 \\ 22 \\ 7 \\ 4 \end{pmatrix} \odot \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix} \qquad \bmod q_L$$

$$= \begin{pmatrix} 33 \\ 35 \\ 37 \\ 6 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \\ 5 \\ c \end{pmatrix}$$

Fehler

$$v \odot e \oplus e_0 \oplus e_1 \odot s$$

$$= \begin{pmatrix} -1 \\ 1 \\ 1 \\ -1 \end{pmatrix} \odot \begin{pmatrix} 3 \\ -2 \\ 0 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ -3 \\ 0 \\ 4 \end{pmatrix} \oplus \begin{pmatrix} -2 \\ -3 \\ 5 \\ 1 \end{pmatrix} \odot \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \end{pmatrix}$$

$$= \begin{pmatrix} 28 \\ 24 \\ 5 \\ 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 \\ 3 \\ 5 \\ 6 \end{pmatrix} - \begin{pmatrix} 28 \\ 24 \\ 5 \\ 2 \end{pmatrix} = \begin{pmatrix} -27 \\ -21 \\ 0 \\ 4 \end{pmatrix} = \begin{pmatrix} 5 \\ 11 \\ 0 \\ 4 \end{pmatrix}$$ ✓