Addition

$$Enc'_{pk}(m) = (b + m,\ a)$$

$$Ecd\begin{pmatrix}10+10i\\10i\end{pmatrix} = \begin{pmatrix}5\\11\\0\\4\end{pmatrix} = m \qquad Ecd\begin{pmatrix}10\\-10\end{pmatrix} = \begin{pmatrix}0\\7\\0\\-7\end{pmatrix} = m'$$

$$Enc'_{pk}(m) = \left(\begin{pmatrix}30\\5\\30\\30\end{pmatrix} \oplus \begin{pmatrix}5\\11\\0\\4\end{pmatrix},\ \begin{pmatrix}5\\25\\2\\29\end{pmatrix}\right) \mod q_L$$

$$= \left(\begin{pmatrix}3\\16\\30\\2\end{pmatrix},\ \begin{pmatrix}5\\25\\2\\29\end{pmatrix}\right) = x$$

$$Enc'_{pk}(m') = \left(\begin{pmatrix}30\\5\\30\\30\end{pmatrix} \oplus \begin{pmatrix}0\\7\\0\\-7\end{pmatrix},\ \begin{pmatrix}5\\25\\2\\29\end{pmatrix}\right)$$

$$= \left(\begin{pmatrix}30\\12\\30\\23\end{pmatrix},\ \begin{pmatrix}5\\25\\2\\29\end{pmatrix}\right) = y$$

Nur gleich mg. vereinfachter Verschlüsselung ohne Fehler

$$Add(x,y) = x \oplus y = \left(\begin{pmatrix}3\\16\\30\\2\end{pmatrix} \oplus \begin{pmatrix}30\\12\\30\\23\end{pmatrix},\ \begin{pmatrix}5\\25\\2\\29\end{pmatrix} \oplus \begin{pmatrix}5\\25\\2\\29\end{pmatrix}\right)$$

$$= \left(\begin{pmatrix}33\\28\\60\\25\end{pmatrix},\ \begin{pmatrix}10\\50\\4\\58\end{pmatrix}\right)$$

$$= \left(\begin{pmatrix}1\\28\\28\\25\end{pmatrix},\ \begin{pmatrix}10\\-18\\4\\26\end{pmatrix}\right) = z$$

$$Dec_{sk}(z) = \begin{pmatrix}1\\28\\28\\25\end{pmatrix} \oplus \begin{pmatrix}10\\-18\\4\\26\end{pmatrix} \odot \begin{pmatrix}1\\1\\1\\-1\end{pmatrix} = \begin{pmatrix}11\\14\\0\\31\end{pmatrix}$$

kommt von Vlog, zu Demozwecken

↓

Fehler abziehen: $\begin{pmatrix}11\\14\\0\\31\end{pmatrix} - \begin{pmatrix}6\\-4\\0\\2\end{pmatrix} = \begin{pmatrix}5\\18\\0\\29\end{pmatrix}$

$$Ecd\begin{pmatrix}5\\18\\0\\29\end{pmatrix} = \begin{pmatrix}-2,78 + 33,24i\\12,78 + 33,24i\end{pmatrix}$$

inaccurate because 29 too close to mod with -3 it works