Supplementary Material

1 SKINNY S_{222} TI

The expressions for the SKINNY_{222} first order TI are given here. Note that we decompose $\mathsf{S}_{222} = H \circ G \circ F$, where F, G, H are 8×8, 8×9 and 9×8 S-boxes respectively, over $GF(2)$. For F, let us have $x_0 = a_0 + a_1 + a_2$, $x_1 = b_0 + b_1 + b_2$, $x_2 = c_0 + c_1 + c_2$, $x_3 = d_0 + d_1 + d_2$, $x_4 = e_0 + e_1 + e_2$, $x_5 = f_0 + f_1 + f_2$, $x_6 = g_0 + g_1 + g_2$, $x_7 = h_0 + h_1 + h_2$. We have

$$u_{0,0} = e_2 + g_1 \cdot h_1 + g_1 \cdot h_2 + g_2 \cdot h_1 + h_1 + h_2 + 1$$
$$u_{0,1} = a_2 + c_1 \cdot d_1 + c_1 \cdot d_2 + c_2 \cdot d_1 + d_1 + d_2 + 1$$
$$u_{0,2} = b_1 + a_1 \cdot d_2 + a_2 \cdot d_1 + a_2 \cdot d_2 + a_2 + c_1 \cdot d_1 + c_1 \cdot d_2 + c_2 \cdot d_1 + c_2$$
$$u_{0,3} = b_1 \cdot c_2 + b_1 + b_2 \cdot c_1 + b_2 \cdot c_2 + b_2 + g_2 + 1$$
$$u_{0,4} = c_2,\ u_{0,5} = d_2,\ u_{0,6} = f_2,\ u_{0,7} = h_2$$

$$u_{1,0} = e_0 + g_0 \cdot h_2 + g_2 \cdot h_0 + g_2 \cdot h_2 + g_2 + h_0$$
$$u_{1,1} = a_0 + c_0 \cdot d_2 + c_2 \cdot d_0 + c_2 \cdot d_2 + c_2 + d_0$$
$$u_{1,2} = b_2 + a_0 \cdot d_0 + a_0 \cdot d_2 + a_2 \cdot d_0 + a_0 + c_0 \cdot d_2 + c_2 \cdot d_0 + c_2 \cdot d_2 + c_0$$
$$u_{1,3} = b_0 \cdot c_0 + b_0 + b_0 \cdot c_2 + b_2 \cdot c_0 + c_2 + g_0$$
$$u_{1,4} = c_0,\ u_{1,5} = d_0,\ u_{1,6} = f_0,\ u_{1,7} = h_0$$

$$u_{2,0} = e_1 + g_0 \cdot h_0 + g_0 \cdot h_1 + g_1 \cdot h_0 + g_0 + g_1$$
$$u_{2,1} = a_1 + c_0 \cdot d_0 + c_0 \cdot d_1 + c_1 \cdot d_0 + c_0 + c_1$$
$$u_{2,2} = b_0 + a_1 \cdot d_1 + a_0 \cdot d_1 + a_1 \cdot d_0 + a_1 + c_0 \cdot d_0 + c_0 \cdot d_1 + c_1 \cdot d_0 + c_1$$
$$u_{2,3} = b_1 \cdot c_1 + b_1 + c_0 \cdot c_1 + b_1 \cdot c_0 + c_1 + g_1$$
$$u_{2,4} = c_1,\ u_{2,5} = d_1,\ u_{2,6} = f_1,\ u_{2,7} = h_1$$

Arguing Uniformity: It can be verified that correctness and non-completeness are trivially satisfied for the above sharing. Uniformity is also not difficult to argue. Denote $X_i := [h_i, g_i, f_i, e_i, d_i, c_i, b_i, a_i], \forall\ i \in\ [0, 2]$. It can be seen that the input shares X_0, X_1, X_2 can be uniquely recovered given all the output shares, and thus the mapping $(X_0, X_1, X_2) \rightarrow \{u_{i,j}\}_{i=0\rightarrow 2,\ j=0\rightarrow 7}$ is a permutation over $\{0,1\}^{24}$ and so uniformity follows.

1.1 The S-box G

Again let us have $u_0 = a_0 + a_1 + a_2$, $u_1 = b_0 + b_1 + b_2$, $u_2 = c_0 + c_1 + c_2$, $u_3 = d_0 + d_1 + d_2$, $u_4 = e_0 + e_1 + e_2$, $u_5 = f_0 + f_1 + f_2$, $u_6 = g_0 + g_1 + g_2$, $u_7 = h_0 + h_1 + h_2$. We have

$$v_{0,0} = a_1 \cdot b_2 + a_1 + a_2 \cdot b_1 + a_2 \cdot b_2 + a_2 + g_2 + 1$$
$$v_{0,1} = f_1 + a_1 \cdot b_2 + a_1 \cdot g_1 + a_1 \cdot g_2 + a_2 \cdot b_1 + a_2 \cdot g_1 + a_2 \cdot g_2 + b_2 + g_2$$
$$v_{0,2} = c_1 \cdot d_2 + c_2 \cdot d_1 + c_2 \cdot d_2 + a_1$$
$$v_{0,3} = a_2,\ v_{0,4} = b_2,\ v_{0,5} = c_2,\ v_{0.6} = d_2,\ v_{0,7} = e_2,\ v_{0,8} = h_2$$

$$v_{1,0} = a_0 \cdot b_0 + a_0 \cdot b_2 + a_0 + a_2 \cdot b_0 + b_2 + g_0$$
$$v_{1,1} = a_0 \cdot b_0 + a_0 \cdot b_2 + a_0 \cdot g_2 + a_2 \cdot b_0 + a_2 \cdot b_2 + a_2 \cdot g_0 + b_0 + f_2 + g_0$$
$$v_{1,2} = c_0 \cdot d_0 + c_0 \cdot d_2 + c_2 \cdot d_0 + a_0$$
$$v_{1,3} = a_0,\ \ v_{1,4} = b_0,\ v_{1,5} = c_0,\ v_{1,6} = d_0,\ v_{1,7} = e_0,\ v_{1,8} = h_0$$

$$
\begin{aligned}
v_{2,0} &= g_1 + a_1 \cdot b_1 + a_0 \cdot b_1 + a_1 \cdot b_0 + b_0 + b_1 \\
v_{2,1} &= b_1 + g_1 + a_1 \cdot b_1 + a_0 \cdot b_1 + a_0 \cdot g_0 + a_0 \cdot g_1 + a_1 \cdot b_0 + a_1 \cdot g_0 + f_0 \\
v_{2,2} &= c_1 \cdot d_1 + c_0 \cdot d_1 + c_1 \cdot d_0 + a_1 + a_0 \\
v_{2,3} &= a_1,\ v_{2,4} = \ b_1,\ v_{2,5} = \ c_1,\ v_{2,6} = \ d_1,\ v_{2,7} = \ e_1,\ v_{2,8} = \ h_1
\end{aligned}
$$

Arguing Uniformity: The input shares $a_i, b_i, c_i, d_i, e_i, h_i$ can be uniquely recovered from the equations for $v_{i-2 \bmod 3,j}$ for $j \in [3,8]$. Since g_i is a linear term in the expression for $v_{i-2 \bmod 3,0}$ and all the other terms in this expression have already been computed, g_i also can be recovered uniquely at this point. Similarly f_i is a linear term in the expression for $v_{i-1 \bmod 3,1}$ and all the other terms in this expression have already been computed, f_i also can be recovered uniquely at this point. Denote $U_i := [h_i, g_i, f_i, e_i, d_i, c_i, b_i, a_i], \forall\ i \in\ [0,2]$. It can be seen that the mapping $(U_0, U_1, U_2) \to \{v_{i,j}\}_{i=0\to 2,\ j=0\to 1,\ 3\to 8}$ is a permutation over $\{0,1\}^{24}$. For all the input vectors in the truth-table of the permutation $v_{0,2},\ v_{1,2},\ v_{2,2}$ are uniquely determined, which implies that for any input share in $\{0,1\}^{24}$ there exists a unique output share over $\{0,1\}^{27}$.

1.2 The S-box H

Again let us have $v_0 = a_0 + a_1 + a_2$, $v_1 = b_0 + b_1 + b_2$, $v_2 = c_0 + c_1 + c_2$, $v_3 = d_0 + d_1 + d_2$, $v_4 = e_0 + e_1 + e_2$, $v_5 = f_0 + f_1 + f_2$, $v_6 = g_0 + g_1 + g_2$, $v_7 = h_0 + h_1 + h_2$, $v_8 = i_0 + i_1 + i_2$. We have

$$
\begin{aligned}
y_{0,0} &= h_1 + a_1 \cdot c_2 + a_1 \cdot f_1 + a_1 \cdot f_2 + a_1 \cdot g_1 + a_1 \cdot g_2 + a_1 + a_2 \cdot c_1 + a_2 \cdot f_1 + \\
&\quad a_2 \cdot f_2 + a_2 \cdot g_1 + a_2 + f_1 \cdot i_1 + f_1 \cdot i_2 + f_2 \cdot i_1 + g_1 + g_2 + i_2 \\
y_{0,1} &= a_1 \cdot g_2 + a_1 + a_2 \cdot g_1 + a_2 \cdot g_2 + a_2 + i_2 + 1 \\
y_{0,2} &= g_2,\ y_{0,3} = \ f_2,\ y_{0,4} = \ b_2,\ y_{0,5} = \ e_2,\ y_{0,6} = \ d_2,\ y_{0,7} = \ a_2
\end{aligned}
$$

$$
\begin{aligned}
y_{1,0} &= a_0 \cdot c_0 + a_0 \cdot c_2 + a_0 \cdot f_2 + a_0 \cdot g_0 + a_0 \cdot g_2 + a_0 + a_2 \cdot c_0 + a_2 \cdot c_2 + a_2 \cdot f_0 + \\
&\quad a_2 \cdot g_0 + a_2 \cdot g_2 + c_2 + f_0 \cdot i_2 + f_2 \cdot i_0 + f_2 \cdot i_2 + h_2 + i_0 \\
y_{1,1} &= a_0 \cdot g_0 + a_0 \cdot g_2 + a_0 + a_2 \cdot g_0 + g_2 + i_0 \\
y_{1,2} &= g_0,\ y_{1,3} = \ f_0,\ y_{1,4} = \ b_0,\ y_{1,5} = \ e_0,\ y_{1,6} = \ d_0,\ y_{1,7} = \ a_0
\end{aligned}
$$

$$
\begin{aligned}
y_{2,0} &= g_0 + i_1 + a_1 \cdot c_1 + a_0 \cdot c_1 + a_0 \cdot f_0 + a_0 \cdot f_1 + a_0 \cdot g_1 + a_1 \cdot c_0 + a_1 \cdot f_0 + \\
&\quad a_1 \cdot g_0 + c_0 + c_1 + f_0 \cdot i_0 + f_0 \cdot i_1 + f_1 \cdot i_0 + h_0 \\
y_{2,1} &= i_1 + a_1 \cdot g_1 + a_0 \cdot g_1 + a_1 \cdot g_0 + g_0 + g_1 \\
y_{2,2} &= g_1,\ y_{2,3} = \ f_1,\ y_{2,4} = \ b_1,\ y_{2,5} = \ e_1,\ y_{2,6} = \ d_1,\ y_{2,7} = \ a_1
\end{aligned}
$$

Arguing Uniformity: The input shares $a_k, b_k, d_k, e_k, f_k, g_k$ can be uniquely recovered from the equations for $y_{k-2 \bmod 3,j}$ for $j \in [2,7]$. Since i_k is a linear term in the expression for $y_{k-2 \bmod 3,1}$ and all the other terms in this expression have already been computed, i_k also can be recovered uniquely at this point. Denote $V_k := [i_k, g_k, f_k, e_k, d_k, b_k, a_k], \forall\ k \in\ [0,2]$. It can be seen that the mapping $(V_0, V_1, V_2) \to \{y_{k,l}\}_{k=0\to 2,\ l=1\to 7}$ is a permutation over $\{0,1\}^{21}$. Let us now inspect the expressions for $y_{k,0}$. Each input vector in $\{0,1\}^{21}$ of the above permutation gives rise to a specific mapping between $(c_0, c_1, c_2, h_0, h_1, h_2) \to (y_{0,0}, y_{1,0}, y_{2,0})$. Since h_k is a linear term in all 3 expressions that define all these maps, it is not difficult to verify that for every $(y_{0,0}, y_{1,0}, y_{2,0}) \in \{0,1\}^3$ there exist exactly 2^3 input pre-images $(c_0, c_1, c_2, h_0, h_1, h_2)$. Uniformity thus follows.

2 SKINNY S_{33} TI

Note that we decompose $\mathsf{S}_{33} = \mathsf{S}'_{\mathsf{Red}} \circ \mathsf{S}'_{\mathsf{Blue}}$, where $\mathsf{S}'_{\mathsf{Blue}}, \mathsf{S}'_{\mathsf{Red}}$ are 9×8, 8×9 S-boxes respectively, over $GF(2)$. For $\mathsf{S}'_{\mathsf{Blue}}$, let's denote $x_0 = a_0 + a_1 + a_2 + a_3$, $x_1 = b_0 + b_1 + b_2 + b_3$, $x_2 = c_0 + c_1 + c_2 + c_3$, $x_3 = d_0 + d_1 + d_2 + d_3$,

$x_4 = e_0 + e_1 + e_2 + e_3$, $x_5 = f_0 + f_1 + f_2 + f_3$, $x_6 = g_0 + g_1 + g_2 + g_3$, $x_7 = h_0 + h_1 + h_2 + h_3$. We have

$$
\begin{aligned}
u_{0,0} &= e_1 + g_1 \cdot h_1 + g_1 \cdot h_2 + g_1 \cdot h_3 + g_1 + g_2 \cdot h_3 + h_1 + 1\\
u_{0,1} &= a_1 + c_1 \cdot d_1 + c_1 \cdot d_2 + c_1 \cdot d_3 + c_1 + c_2 \cdot d_3 + d_1 + 1\\
u_{0,2} &= a_1 \cdot d_1 + a_1 \cdot d_2 + a_1 \cdot d_3 + a_1 + a_2 \cdot d_3 + b_1 + c_1 \cdot d_1 + c_1 \cdot d_2 + c_1 \cdot d_3 + c_1 + c_2 \cdot d_3\\
u_{0,3} &= b_1 \cdot c_1 + b_1 \cdot c_2 + b_1 \cdot c_3 + b_1 + b_2 \cdot c_3 + c_1 + g_1 + 1\\
u_{0,4} &= e_1 + a_1 \cdot b_1 + a_1 \cdot b_2 + a_1 \cdot b_3 + a_2 \cdot b_3 + a_3 \cdot b_3 + b_1 \cdot c_1 \cdot d_1 + b_1 \cdot c_1 \cdot d_2 + b_1 \cdot c_1 \cdot d_3 + b_1 \cdot c_1 + b_1 \cdot c_2 \cdot d_1 +\\
&\quad b_1 \cdot c_2 \cdot d_2 + b_1 \cdot c_2 \cdot d_3 + b_1 \cdot c_2 + b_1 \cdot c_3 \cdot d_1 + b_1 \cdot c_3 \cdot d_2 + b_1 \cdot c_3 \cdot d_3 + b_1 \cdot c_3 + b_1 \cdot d_3 + b_1 + b_2 \cdot c_1 \cdot d_1 +\\
&\quad b_2 \cdot c_1 \cdot d_3 + b_2 \cdot c_2 \cdot d_1 + b_2 \cdot c_3 \cdot d_1 + b_2 \cdot c_3 \cdot d_3 + b_2 \cdot d_3 + b_3 \cdot c_1 \cdot d_2 + b_3 \cdot c_2 \cdot d_1 + b_3 \cdot c_2 \cdot d_3 + b_3 \cdot c_3 \cdot d_2 + b_3 \cdot d_1\\
u_{0,5} &= c_1,\ u_{0,6} = d_1,\ u_{0,7} = f_1,\ u_{0,8} = h_1
\end{aligned}
$$

$$
\begin{aligned}
u_{1,0} &= e_0 + g_0 \cdot h_0 + g_0 \cdot h_3 + g_0 + g_2 \cdot h_2 + g_3 \cdot h_2 + h_0\\
u_{1,1} &= a_0 + c_0 \cdot d_0 + c_0 \cdot d_3 + c_0 + c_2 \cdot d_2 + c_3 \cdot d_2 + d_0\\
u_{1,2} &= a_0 \cdot d_0 + a_0 \cdot d_3 + a_0 + a_2 \cdot d_2 + a_3 \cdot d_2 + b_0 + c_0 \cdot d_2 + c_0 \cdot d_3 + c_0 + c_2 \cdot d_2 + c_3 \cdot d_2\\
u_{1,3} &= b_0 \cdot c_0 + b_0 \cdot c_3 + b_0 + b_2 \cdot c_2 + b_3 \cdot c_2 + c_0 + g_0\\
u_{1,4} &= e_0 + a_0 \cdot b_0 + a_0 \cdot b_3 + a_2 \cdot b_2 + a_3 \cdot b_2 + b_0 \cdot c_0 \cdot d_2 + b_0 \cdot c_0 \cdot d_3 + b_0 \cdot c_2 \cdot d_0 + b_0 \cdot c_2 \cdot d_2 + b_0 \cdot c_2 \cdot d_3 + b_0 \cdot c_3 \cdot d_2 +\\
&\quad b_0 \cdot c_3 \cdot d_3 + b_0 \cdot d_2 + b_0 + b_2 \cdot c_0 \cdot d_0 + b_2 \cdot c_0 \cdot d_2 + b_2 \cdot c_0 \cdot d_3 + b_2 \cdot c_0 + b_2 \cdot c_2 \cdot d_0 + b_2 \cdot c_2 \cdot d_2 + b_2 \cdot c_2 \cdot d_3 + b_2 \cdot c_2 +\\
&\quad b_2 \cdot c_3 \cdot d_0 + b_2 \cdot c_3 \cdot d_2 + b_2 \cdot c_3 + b_3 \cdot c_0 \cdot d_2 + b_3 \cdot c_2 \cdot d_0 + b_3 \cdot c_2 \cdot d_2 + b_3 \cdot c_2 + b_3 \cdot c_3 + b_3 \cdot d_2\\
u_{1,5} &= c_0,\ u_{1,6} = d_0,\ u_{1,7} = f_0,\ u_{1,8} = h_0
\end{aligned}
$$

$$
\begin{aligned}
u_{2,0} &= e_3 + g_0 \cdot h_1 + g_1 \cdot h_0 + g_3 \cdot h_0 + g_3 \cdot h_1 + g_3 \cdot h_3 + g_3 + h_3\\
u_{2,1} &= a_3 + c_0 \cdot d_1 + c_1 \cdot d_0 + c_3 \cdot d_0 + c_3 \cdot d_1 + c_3 \cdot d_3 + c_3 + d_3\\
u_{2,2} &= a_0 \cdot d_1 + a_1 \cdot d_0 + a_3 \cdot d_0 + a_3 \cdot d_1 + a_3 \cdot d_3 + a_3 + b_3 + c_1 \cdot d_0 + c_3 \cdot d_0 + c_3 \cdot d_1 + c_3 \cdot d_3 + c_3\\
u_{2,3} &= b_0 \cdot c_1 + b_1 \cdot c_0 + b_3 \cdot c_0 + b_3 \cdot c_1 + b_3 \cdot c_3 + b_3 + c_3 + g_3\\
u_{2,4} &= e_1 + a_0 \cdot b_1 + a_1 \cdot b_0 + a_3 \cdot b_0 + a_3 \cdot b_1 + b_0 \cdot c_0 \cdot d_1 + b_0 \cdot c_1 \cdot d_0 + b_0 \cdot c_1 \cdot d_3 + b_0 \cdot c_1 + b_0 \cdot c_3 \cdot d_0 + b_0 \cdot c_3 \cdot d_1 +\\
&\quad b_0 \cdot c_3 + b_0 \cdot d_3 + b_1 \cdot c_0 \cdot d_1 + b_1 \cdot c_0 \cdot d_3 + b_1 \cdot c_1 \cdot d_0 + b_1 \cdot c_3 \cdot d_0 + b_1 \cdot d_1 + b_3 \cdot c_0 \cdot d_0 + b_3 \cdot c_0 \cdot d_1 + b_3 \cdot c_0 \cdot d_3 +\\
&\quad b_3 \cdot c_0 + b_3 \cdot c_1 \cdot d_0 + b_3 \cdot c_1 \cdot d_1 + b_3 \cdot c_1 \cdot d_3 + b_3 \cdot c_1 + b_3 \cdot c_3 \cdot d_0 + b_3 \cdot c_3 \cdot d_1 + b_3 \cdot c_3 \cdot d_3 + b_3 \cdot d_0 + b_3 \cdot d_3 + b_3\\
u_{2,5} &= c_3,\ u_{2,6} = d_3,\ u_{2,7} = f_3,\ u_{2,8} = h_3
\end{aligned}
$$

$$
\begin{aligned}
u_{3,0} &= e_2 + g_0 \cdot h_2 + g_2 \cdot h_0 + g_2 \cdot h_1 + g_2 + h_2\\
u_{3,1} &= a_2 + c_0 \cdot d_2 + c_2 \cdot d_0 + c_2 \cdot d_1 + c_2 + d_2\\
u_{3,2} &= a_0 \cdot d_2 + a_2 \cdot d_0 + a_2 \cdot d_1 + a_2 + b_2 + c_0 \cdot d_0 + c_0 \cdot d_1 + c_2 \cdot d_0 + c_2 \cdot d_1 + c_2\\
u_{3,3} &= b_0 \cdot c_2 + b_2 \cdot c_0 + b_2 \cdot c_1 + b_2 + c_2 + g_2\\
u_{3,4} &= e_0 + a_0 \cdot b_2 + a_2 \cdot b_0 + a_2 \cdot b_1 + b_0 \cdot c_0 \cdot d_0 + b_0 \cdot c_0 + b_0 \cdot c_1 \cdot d_1 + b_0 \cdot c_1 \cdot d_2 + b_0 \cdot c_2 \cdot d_1 + b_0 \cdot c_2 + b_0 \cdot d_0 + b_0 \cdot d_1 +\\
&\quad b_1 \cdot c_0 \cdot d_0 + b_1 \cdot c_0 \cdot d_2 + b_1 \cdot c_0 + b_1 \cdot c_2 \cdot d_0 + b_1 \cdot d_0 + b_1 \cdot d_2 + b_2 \cdot c_0 \cdot d_1 + b_2 \cdot c_1 \cdot d_0 + b_2 \cdot c_1 \cdot d_2 + b_2 \cdot c_1 +\\
&\quad b_2 \cdot d_0 + b_2 \cdot d_1 + b_2 \cdot d_2 + b_2\\
u_{3,5} &= c_2,\ u_{3,6} = d_2,\ u_{3,7} = f_2,\ u_{3,8} = h_2
\end{aligned}
$$

Arguing Uniformity: The input shares c_i, d_i, f_i, h_i can be uniquely recovered from the equations for $u_{i,j}$ for $j \in [5, 8]$. Since a_i's are linear terms in the expressions for $u_{i,1}$ and all the other terms in this expression have already been computed, a_i's also can be recovered uniquely at this point. Similarly b_i's are the only unknown linear terms the expressions for $u_{i,2}$, and so these can also be recovered. Similarly the g_i's can be recovered from $u_{i,3}$. And then the e_i's can be recovered from $u_{i,0}$. Denote $X_i := [h_i, g_i, f_i, e_i, d_i, c_i, b_i, a_i], \forall\ i \in\ [0, 3]$. It can be seen that the mapping $(X_0, X_1, X_2, X_3) \to \{v_{i,j}\}_{i=0\to 2,\ j=0\to 3,\ 5\to 8}$ is a permutation over $\{0,1\}^{32}$. For all the input vectors in the truth-table of the permutation $v_{0,4},\ v_{1,4},\ v_{2,4},\ v_{3,4}$ are uniquely determined, which implies that for any input share in $\{0,1\}^{32}$ there exists a unique output share over $\{0,1\}^{36}$.

2.1 The S-box $\mathsf{S}'_{\mathsf{Red}}$

Again let us have $u_0 = a_0 + a_1 + a_2 + a_3$, $u_1 = b_0 + b_1 + b_2 + b_3$, $u_2 = c_0 + c_1 + c_2 + c_3$, $u_3 = d_0 + d_1 + d_2 + d_3$, $u_4 = e_0 + e_1 + e_2 + e_3$, $u_5 = f_0 + f_1 + f_2 + f_3$, $u_6 = g_0 + g_1 + g_2 + g_3$, $u_7 = h_0 + h_1 + h_2 + h_3$, $u_8 = i_0 + i_1 + i_2 + i_3$.

We have

$$
\begin{aligned}
y_{0,0} = {} & a_1 \cdot b_1 \cdot d_1 + a_1 \cdot b_1 \cdot d_2 + a_1 \cdot b_1 \cdot d_3 + a_1 \cdot b_1 + a_1 \cdot b_2 \cdot d_1 + a_1 \cdot b_2 \cdot d_2 + a_1 \cdot b_2 \cdot d_3 + a_1 \cdot b_2 + a_1 \cdot b_3 \cdot d_1 + \\
& a_1 \cdot b_3 \cdot d_2 + a_1 \cdot b_3 \cdot d_3 + a_1 \cdot b_3 + a_1 \cdot c_1 \cdot d_1 + a_1 \cdot c_1 \cdot d_2 + a_1 \cdot c_1 \cdot d_3 + a_1 \cdot c_1 + a_1 \cdot c_2 \cdot d_1 + a_1 \cdot c_2 \cdot d_2 + \\
& a_1 \cdot c_2 \cdot d_3 + a_1 \cdot c_2 + a_1 \cdot c_3 \cdot d_1 + a_1 \cdot c_3 \cdot d_2 + a_1 \cdot c_3 \cdot d_3 + a_1 \cdot c_3 + a_1 \cdot d_1 \cdot e_1 + a_1 \cdot d_1 \cdot e_2 + a_1 \cdot d_1 \cdot e_3 + \\
& a_1 \cdot d_1 + a_1 \cdot d_2 \cdot e_1 + a_1 \cdot d_2 \cdot e_2 + a_1 \cdot d_2 \cdot e_3 + a_1 \cdot d_2 + a_1 \cdot d_3 \cdot e_1 + a_1 \cdot d_3 \cdot e_2 + a_1 \cdot d_3 + a_1 \cdot e_3 + a_1 + \\
& a_2 \cdot b_1 \cdot d_1 + a_2 \cdot b_1 \cdot d_3 + a_2 \cdot b_2 \cdot d_1 + a_2 \cdot b_3 \cdot d_1 + a_2 \cdot c_1 \cdot d_1 + a_2 \cdot c_1 \cdot d_3 + a_2 \cdot c_2 \cdot d_1 + a_2 \cdot c_3 \cdot d_1 + \\
& a_2 \cdot c_3 \cdot d_3 + a_2 \cdot d_1 \cdot e_1 + a_2 \cdot d_1 \cdot e_2 + a_2 \cdot d_1 \cdot e_3 + a_2 \cdot d_2 \cdot e_1 + a_2 \cdot d_3 \cdot e_1 + a_2 \cdot d_3 \cdot e_2 + a_2 \cdot d_3 + a_2 \cdot e_3 + \\
& a_3 \cdot b_1 \cdot d_2 + a_3 \cdot b_2 \cdot d_1 + a_3 \cdot b_2 \cdot d_3 + a_3 \cdot b_3 \cdot d_2 + a_3 \cdot c_1 \cdot d_2 + a_3 \cdot c_2 \cdot d_1 + a_3 \cdot c_2 \cdot d_3 + a_3 \cdot c_3 \cdot d_2 + a_3 \cdot d_1 \cdot e_1 + \\
& a_3 \cdot d_1 \cdot e_2 + a_3 \cdot d_1 + a_3 \cdot d_2 \cdot e_1 + a_3 \cdot d_2 + a_3 \cdot d_3 + a_3 \cdot e_2 + b_1 \cdot c_3 + b_1 \cdot d_3 + b_1 + b_2 \cdot d_3 + b_3 \cdot d_1 + b_3 \cdot d_2 + \\
& c_1 \cdot d_1 \cdot h_1 + c_1 \cdot d_1 \cdot h_2 + c_1 \cdot d_1 \cdot h_3 + c_1 \cdot d_2 \cdot h_1 + c_1 \cdot d_2 \cdot h_2 + c_1 \cdot d_2 \cdot h_3 + c_1 \cdot d_3 \cdot h_1 + c_1 \cdot d_3 \cdot h_2 + \\
& c_1 \cdot d_3 \cdot h_3 + c_1 \cdot h_1 + c_1 \cdot h_2 + c_1 \cdot h_3 + c_1 \cdot i_3 + c_1 + c_2 \cdot d_1 \cdot h_1 + c_2 \cdot d_1 \cdot h_3 + c_2 \cdot d_3 \cdot h_1 + c_2 \cdot h_1 + c_2 \cdot h_3 + \\
& c_2 \cdot i_3 + c_3 \cdot d_1 \cdot h_2 + c_3 \cdot d_2 \cdot h_1 + c_3 \cdot d_2 \cdot h_3 + c_3 \cdot h_2 + c_3 \cdot i_1 + d_1 \cdot e_1 + d_1 \cdot e_2 + d_1 \cdot e_3 + d_1 \cdot h_3 + d_2 \cdot e_3 + \\
& d_2 \cdot h_2 + d_3 \cdot e_2 + d_3 \cdot h_2 + f_1 + h_1 + i_1 + 1 \\
y_{0,1} = {} & a_1 \cdot b_1 \cdot d_1 + a_1 \cdot b_1 \cdot d_2 + a_1 \cdot b_1 \cdot d_3 + a_1 \cdot b_1 + a_1 \cdot b_2 \cdot d_1 + a_1 \cdot b_2 \cdot d_2 + a_1 \cdot b_2 \cdot d_3 + a_1 \cdot b_2 + a_1 \cdot b_3 \cdot d_1 + \\
& a_1 \cdot b_3 \cdot d_2 + a_1 \cdot b_3 \cdot d_3 + a_1 \cdot b_3 + a_1 \cdot d_1 + a_1 \cdot d_3 + a_1 + a_2 \cdot b_1 \cdot d_1 + a_2 \cdot b_1 \cdot d_3 + a_2 \cdot b_2 \cdot d_1 + a_2 \cdot b_3 \cdot d_1 + \\
& a_2 \cdot b_3 \cdot d_3 + a_2 \cdot d_3 + a_3 \cdot b_1 \cdot d_2 + a_3 \cdot b_2 \cdot d_1 + a_3 \cdot b_2 \cdot d_3 + a_3 \cdot b_3 \cdot d_2 + a_3 \cdot d_1 + b_1 \cdot d_2 + b_1 \cdot d_3 + b_1 + b_2 \cdot d_3 + \\
& d_1 \cdot h_1 + d_1 \cdot h_2 + d_1 \cdot h_3 + d_2 \cdot h_3 + d_3 \cdot h_3 + h_1 + i_1 \\
y_{0,2} = {} & d_1 \\
y_{0,3} = {} & c_1 \\
y_{0,4} = {} & a_1 \cdot b_1 + a_1 \cdot b_2 + a_1 \cdot b_3 + a_1 \cdot h_1 + a_1 \cdot h_3 + a_2 \cdot b_3 + a_2 \cdot h_2 + a_3 \cdot b_2 + a_3 \cdot h_2 + b_1 + g_1 + h_1 \\
y_{0,5} = {} & b_1 \\
y_{0,6} = {} & a_1 \\
y_{0,7} = {} & a_1 \cdot b_1 + a_1 \cdot b_2 + a_1 \cdot b_3 + a_1 + a_2 \cdot b_3 + b_1 + h_1 + 1
\end{aligned}
$$

$$
\begin{aligned}
y_{1,0} = {} & a_0 \cdot b_0 \cdot d_0 + a_0 \cdot b_0 \cdot d_3 + a_0 \cdot b_2 \cdot d_0 + a_0 \cdot b_2 \cdot d_2 + a_0 \cdot b_2 \cdot d_3 + a_0 \cdot b_2 + a_0 \cdot b_3 \cdot d_2 + a_0 \cdot b_3 + a_0 \cdot c_0 + \\
& a_0 \cdot c_2 \cdot d_0 + a_0 \cdot c_2 \cdot d_2 + a_0 \cdot c_2 \cdot d_3 + a_0 \cdot c_3 \cdot d_2 + a_0 \cdot c_3 \cdot d_3 + a_0 \cdot d_0 \cdot e_2 + a_0 \cdot d_2 \cdot e_0 + a_0 \cdot d_2 \cdot e_2 + \\
& a_0 \cdot d_2 \cdot e_3 + a_0 \cdot d_2 + a_0 \cdot d_3 \cdot e_2 + a_0 \cdot d_3 \cdot e_3 + a_0 \cdot e_3 + a_0 + a_2 \cdot b_0 \cdot d_0 + a_2 \cdot b_0 \cdot d_2 + a_2 \cdot b_0 \cdot d_3 + a_2 \cdot b_0 + \\
& a_2 \cdot b_2 \cdot d_0 + a_2 \cdot b_2 \cdot d_2 + a_2 \cdot b_2 \cdot d_3 + a_2 \cdot b_2 + a_2 \cdot b_3 \cdot d_0 + a_2 \cdot b_3 \cdot d_2 + a_2 \cdot b_3 \cdot d_3 + a_2 \cdot b_3 + a_2 \cdot c_0 \cdot d_0 + \\
& a_2 \cdot c_0 \cdot d_2 + a_2 \cdot c_0 \cdot d_3 + a_2 \cdot c_0 + a_2 \cdot c_2 \cdot d_0 + a_2 \cdot c_2 \cdot d_2 + a_2 \cdot c_2 \cdot d_3 + a_2 \cdot c_2 + a_2 \cdot c_3 \cdot d_0 + a_2 \cdot c_3 \cdot d_2 + \\
& a_2 \cdot c_3 + a_2 \cdot d_0 \cdot e_3 + a_2 \cdot d_2 \cdot e_0 + a_2 \cdot d_2 \cdot e_2 + a_2 \cdot d_2 \cdot e_3 + a_2 \cdot d_3 \cdot e_0 + a_2 \cdot d_3 \cdot e_3 + a_2 \cdot e_2 + a_3 \cdot b_0 \cdot d_2 + \\
& a_3 \cdot b_2 \cdot d_0 + a_3 \cdot b_2 \cdot d_2 + a_3 \cdot b_2 + a_3 \cdot c_0 \cdot d_2 + a_3 \cdot c_2 \cdot d_0 + a_3 \cdot c_2 \cdot d_2 + a_3 \cdot c_2 + a_3 \cdot d_0 \cdot e_2 + a_3 \cdot d_0 + \\
& a_3 \cdot d_2 \cdot e_0 + a_3 \cdot d_2 \cdot e_2 + a_3 \cdot d_2 \cdot e_3 + a_3 \cdot d_3 \cdot e_2 + a_3 \cdot e_0 + a_3 \cdot e_3 + b_0 \cdot c_3 + b_0 + b_2 \cdot c_3 + b_3 \cdot c_2 + b_3 \cdot d_0 + \\
& c_0 \cdot d_0 \cdot h_2 + c_0 \cdot d_0 \cdot h_3 + c_0 \cdot d_2 \cdot h_0 + c_0 \cdot d_2 \cdot h_2 + c_0 \cdot d_2 \cdot h_3 + c_0 \cdot d_3 \cdot h_2 + c_0 \cdot h_3 + c_0 \cdot i_2 + c_0 + c_2 \cdot d_0 \cdot h_0 + \\
& c_2 \cdot d_0 \cdot h_2 + c_2 \cdot d_0 \cdot h_3 + c_2 \cdot d_2 \cdot h_0 + c_2 \cdot d_2 \cdot h_2 + c_2 \cdot d_2 \cdot h_3 + c_2 \cdot d_3 \cdot h_0 + c_2 \cdot d_3 \cdot h_2 + c_2 \cdot d_3 \cdot h_3 + c_2 \cdot h_2 + \\
& c_2 \cdot i_2 + c_3 \cdot d_0 \cdot h_2 + c_3 \cdot d_2 \cdot h_0 + c_3 \cdot d_2 \cdot h_2 + c_3 \cdot d_3 \cdot h_2 + c_3 \cdot h_3 + c_3 \cdot i_2 + d_0 \cdot e_3 + d_0 \cdot h_3 + d_2 \cdot e_0 + d_2 \cdot e_2 + \\
& d_2 \cdot h_0 + d_2 \cdot h_3 + d_3 \cdot h_0 + d_3 \cdot h_3 + f_0 + h_0 + i_0 \\
y_{1,1} = {} & a_0 \cdot b_0 \cdot d_0 + a_0 \cdot b_0 \cdot d_3 + a_0 \cdot b_2 \cdot d_0 + a_0 \cdot b_2 \cdot d_2 + a_0 \cdot b_2 \cdot d_3 + a_0 \cdot b_2 + a_0 \cdot b_3 \cdot d_2 + a_0 \cdot b_3 + a_0 + a_2 \cdot b_0 \cdot d_0 + \\
& a_2 \cdot b_0 \cdot d_2 + a_2 \cdot b_0 \cdot d_3 + a_2 \cdot b_0 + a_2 \cdot b_2 \cdot d_0 + a_2 \cdot b_2 \cdot d_2 + a_2 \cdot b_2 \cdot d_3 + a_2 \cdot b_2 + a_2 \cdot b_3 \cdot d_0 + a_2 \cdot b_3 \cdot d_2 + \\
& a_2 \cdot b_3 + a_3 \cdot b_0 \cdot d_2 + a_3 \cdot b_2 \cdot d_0 + a_3 \cdot b_2 \cdot d_2 + a_3 \cdot b_2 + a_3 \cdot b_3 + a_3 \cdot d_2 + b_0 \cdot d_3 + b_0 + b_2 \cdot d_2 + b_3 \cdot d_2 + d_0 \cdot h_2 + \\
& d_0 \cdot h_3 + d_2 \cdot h_2 + d_3 \cdot h_2 + h_0 + i_0 \\
y_{1,2} = {} & d_0 \\
y_{1,3} = {} & c_0 \\
y_{1,4} = {} & a_0 \cdot b_0 + a_0 \cdot b_3 + a_0 \cdot h_2 + a_2 \cdot b_0 + a_2 \cdot b_2 + a_2 \cdot h_0 + a_2 \cdot h_3 + a_3 \cdot h_0 + a_3 \cdot h_3 + b_0 + g_0 + h_0 \\
y_{1,5} = {} & b_0 \\
y_{1,6} = {} & a_0 \\
y_{1,7} = {} & a_0 \cdot b_0 + a_0 \cdot b_3 + a_0 + a_2 \cdot b_2 + a_3 \cdot b_2 + b_0 + h_0
\end{aligned}
$$

$$y_{2,0} = a_0 \cdot b_0 \cdot d_1 + a_0 \cdot b_0 + a_0 \cdot b_1 \cdot d_1 + a_0 \cdot b_1 \cdot d_3 + a_0 \cdot b_3 \cdot d_0 + a_0 \cdot b_3 \cdot d_1 + a_0 \cdot b_3 \cdot d_3 + a_0 \cdot c_0 \cdot d_3 + a_0 \cdot c_1 \cdot d_0 + a_0 \cdot c_1 \cdot d_3 + a_0 \cdot c_1 + a_0 \cdot c_3 \cdot d_0 + a_0 \cdot c_3 \cdot d_1 + a_0 \cdot c_3 + a_0 \cdot d_0 \cdot e_3 + a_0 \cdot d_1 \cdot e_0 + a_0 \cdot d_1 \cdot e_3 + a_0 \cdot d_1 + a_0 \cdot d_3 \cdot e_0 + a_0 \cdot d_3 \cdot e_1 + a_0 \cdot d_3 + a_1 \cdot b_0 \cdot d_0 + a_1 \cdot b_0 \cdot d_3 + a_1 \cdot b_0 + a_1 \cdot b_3 \cdot d_0 + a_1 \cdot c_0 \cdot d_0 + a_1 \cdot c_0 \cdot d_3 + a_1 \cdot c_0 + a_1 \cdot c_3 \cdot d_0 + a_1 \cdot d_0 \cdot e_0 + a_1 \cdot d_0 \cdot e_3 + a_1 \cdot d_0 + a_1 \cdot d_3 \cdot e_0 + a_1 \cdot d_3 \cdot e_3 + a_1 \cdot e_1 + a_3 \cdot b_0 \cdot d_0 + a_3 \cdot b_0 \cdot d_1 + a_3 \cdot b_0 \cdot d_3 + a_3 \cdot b_0 + a_3 \cdot b_1 \cdot d_0 + a_3 \cdot b_1 \cdot d_1 + a_3 \cdot b_1 \cdot d_3 + a_3 \cdot b_1 + a_3 \cdot b_3 \cdot d_0 + a_3 \cdot b_3 \cdot d_1 + a_3 \cdot b_3 \cdot d_3 + a_3 \cdot b_3 + a_3 \cdot c_0 \cdot d_0 + a_3 \cdot c_0 \cdot d_1 + a_3 \cdot c_0 \cdot d_3 + a_3 \cdot c_0 + a_3 \cdot c_1 \cdot d_0 + a_3 \cdot c_1 \cdot d_1 + a_3 \cdot c_1 \cdot d_3 + a_3 \cdot c_1 + a_3 \cdot c_3 \cdot d_0 + a_3 \cdot c_3 \cdot d_1 + a_3 \cdot c_3 \cdot d_3 + a_3 \cdot c_3 + a_3 \cdot d_0 \cdot e_0 + a_3 \cdot d_0 \cdot e_1 + a_3 \cdot d_0 \cdot e_3 + a_3 \cdot d_1 \cdot e_0 + a_3 \cdot d_1 \cdot e_3 + a_3 \cdot d_3 \cdot e_0 + a_3 \cdot d_3 \cdot e_1 + a_3 \cdot d_3 \cdot e_3 + a_3 \cdot e_1 + a_3 + b_0 \cdot d_3 + b_3 \cdot c_0 + b_3 \cdot c_1 + b_3 \cdot c_3 + b_3 \cdot d_3 + b_3 + c_0 \cdot d_1 \cdot h_1 + c_0 \cdot d_1 \cdot h_3 + c_0 \cdot d_3 \cdot h_0 + c_0 \cdot d_3 \cdot h_1 + c_0 \cdot d_3 \cdot h_3 + c_0 \cdot i_0 + c_0 \cdot i_3 + c_1 \cdot d_0 \cdot h_1 + c_1 \cdot d_0 \cdot h_3 + c_1 \cdot d_3 \cdot h_0 + c_1 \cdot h_0 + c_1 \cdot i_1 + c_3 \cdot d_0 \cdot h_0 + c_3 \cdot d_0 \cdot h_1 + c_3 \cdot d_0 \cdot h_3 + c_3 \cdot d_1 \cdot h_0 + c_3 \cdot d_1 \cdot h_1 + c_3 \cdot d_1 \cdot h_3 + c_3 \cdot d_3 \cdot h_0 + c_3 \cdot d_3 \cdot h_1 + c_3 \cdot d_3 \cdot h_3 + c_3 \cdot h_0 + c_3 \cdot h_1 + c_3 \cdot i_0 + c_3 \cdot i_3 + c_3 + d_1 \cdot e_0 + d_1 \cdot h_1 + d_3 \cdot e_0 + d_3 \cdot e_1 + d_3 \cdot e_3 + d_3 \cdot h_1 + f_3 + h_3 + i_3$$

$$y_{2,1} = a_0 \cdot b_0 \cdot d_1 + a_0 \cdot b_0 + a_0 \cdot b_1 \cdot d_1 + a_0 \cdot b_1 \cdot d_3 + a_0 \cdot b_3 \cdot d_0 + a_0 \cdot b_3 \cdot d_1 + a_0 \cdot b_3 \cdot d_3 + a_0 \cdot d_3 + a_1 \cdot b_0 \cdot d_0 + a_1 \cdot b_0 \cdot d_3 + a_1 \cdot b_0 + a_1 \cdot b_3 \cdot d_0 + a_1 \cdot d_0 + a_3 \cdot b_0 \cdot d_0 + a_3 \cdot b_0 \cdot d_1 + a_3 \cdot b_0 \cdot d_3 + a_3 \cdot b_0 + a_3 \cdot b_1 \cdot d_0 + a_3 \cdot b_1 \cdot d_1 + a_3 \cdot b_1 \cdot d_3 + a_3 \cdot b_1 + a_3 \cdot b_3 \cdot d_0 + a_3 \cdot b_3 \cdot d_1 + a_3 \cdot b_3 \cdot d_3 + a_3 \cdot d_0 + a_3 \cdot d_3 + a_3 + b_3 \cdot d_0 + b_3 \cdot d_1 + b_3 \cdot d_3 + b_3 + d_1 \cdot h_0 + d_3 \cdot h_0 + d_3 \cdot h_1 + h_3 + i_3$$

$$y_{2,2} = d_3$$

$$y_{2,3} = c_3$$

$$y_{2,4} = a_0 \cdot b_1 + a_0 \cdot h_0 + a_0 \cdot h_3 + a_1 \cdot h_0 + a_3 \cdot b_0 + a_3 \cdot b_1 + a_3 \cdot b_3 + a_3 \cdot h_1 + b_3 + g_3 + h_3$$

$$y_{2,5} = b_3$$

$$y_{2,6} = a_3$$

$$y_{2,7} = a_0 \cdot b_1 + a_1 \cdot b_0 + a_3 \cdot b_0 + a_3 \cdot b_1 + a_3 \cdot b_3 + a_3 + b_3 + h_3$$

$$y_{3,0} = a_0 \cdot b_0 \cdot d_2 + a_0 \cdot b_1 \cdot d_0 + a_0 \cdot b_1 \cdot d_2 + a_0 \cdot b_1 + a_0 \cdot b_2 \cdot d_1 + a_0 \cdot c_0 \cdot d_0 + a_0 \cdot c_0 \cdot d_1 + a_0 \cdot c_0 \cdot d_2 + a_0 \cdot c_1 \cdot d_1 + a_0 \cdot c_1 \cdot d_2 + a_0 \cdot c_2 \cdot d_1 + a_0 \cdot c_2 + a_0 \cdot d_0 \cdot e_0 + a_0 \cdot d_0 \cdot e_1 + a_0 \cdot d_0 + a_0 \cdot d_1 \cdot e_1 + a_0 \cdot d_1 \cdot e_2 + a_0 \cdot d_2 \cdot e_1 + a_0 \cdot e_0 + a_0 \cdot e_1 + a_0 \cdot e_2 + a_1 \cdot b_0 \cdot d_1 + a_1 \cdot b_0 \cdot d_2 + a_1 \cdot b_1 \cdot d_0 + a_1 \cdot b_2 \cdot d_0 + a_1 \cdot c_0 \cdot d_1 + a_1 \cdot c_0 \cdot d_2 + a_1 \cdot c_1 \cdot d_0 + a_1 \cdot c_2 \cdot d_0 + a_1 \cdot d_0 \cdot e_1 + a_1 \cdot d_0 \cdot e_2 + a_1 \cdot d_1 \cdot e_0 + a_1 \cdot d_2 \cdot e_0 + a_1 \cdot e_0 + a_1 \cdot e_2 + a_2 \cdot b_0 \cdot d_1 + a_2 \cdot b_1 \cdot d_0 + a_2 \cdot b_1 \cdot d_2 + a_2 \cdot b_1 + a_2 \cdot c_0 \cdot d_1 + a_2 \cdot c_1 \cdot d_0 + a_2 \cdot c_1 \cdot d_2 + a_2 \cdot c_1 + a_2 \cdot d_0 \cdot e_0 + a_2 \cdot d_0 \cdot e_1 + a_2 \cdot d_0 \cdot e_2 + a_2 \cdot d_0 + a_2 \cdot d_1 \cdot e_0 + a_2 \cdot d_1 + a_2 \cdot d_2 + a_2 \cdot e_0 + a_2 \cdot e_1 + a_2 + b_0 \cdot c_0 + b_0 \cdot c_1 + b_0 \cdot c_2 + b_0 \cdot d_0 + b_0 \cdot d_1 + b_0 \cdot d_2 + b_1 \cdot c_0 + b_1 \cdot c_1 + b_1 \cdot c_2 + b_1 \cdot d_0 + b_1 \cdot d_1 + b_1 \cdot d_2 + b_2 \cdot c_0 + b_2 \cdot c_1 + b_2 \cdot c_2 + b_2 \cdot d_0 + b_2 \cdot d_1 + b_2 \cdot d_2 + b_2 + c_0 \cdot d_0 \cdot h_0 + c_0 \cdot d_0 \cdot h_1 + c_0 \cdot d_1 \cdot h_0 + c_0 \cdot d_1 \cdot h_2 + c_0 \cdot d_2 \cdot h_1 + c_0 \cdot h_0 + c_0 \cdot h_1 + c_0 \cdot h_2 + c_0 \cdot i_1 + c_1 \cdot d_0 \cdot h_0 + c_1 \cdot d_0 \cdot h_2 + c_1 \cdot d_1 \cdot h_0 + c_1 \cdot d_2 \cdot h_0 + c_1 \cdot i_0 + c_1 \cdot i_2 + c_2 \cdot d_0 \cdot h_1 + c_2 \cdot d_1 \cdot h_0 + c_2 \cdot d_1 \cdot h_2 + c_2 \cdot d_2 \cdot h_1 + c_2 \cdot h_0 + c_2 \cdot i_0 + c_2 \cdot i_1 + c_2 + d_0 \cdot e_0 + d_0 \cdot e_1 + d_0 \cdot e_2 + d_0 \cdot h_0 + d_0 \cdot h_1 + d_0 \cdot h_2 + d_1 \cdot h_0 + d_1 \cdot h_2 + d_2 \cdot e_1 + d_2 \cdot h_1 + f_2 + h_2 + i_2$$

$$y_{3,1} = a_0 \cdot b_0 \cdot d_2 + a_0 \cdot b_1 \cdot d_0 + a_0 \cdot b_1 \cdot d_2 + a_0 \cdot b_1 + a_0 \cdot b_2 \cdot d_1 + a_0 \cdot d_0 + a_0 \cdot d_1 + a_0 \cdot d_2 + a_1 \cdot b_0 \cdot d_1 + a_1 \cdot b_0 \cdot d_2 + a_1 \cdot b_1 \cdot d_0 + a_1 \cdot b_2 \cdot d_0 + a_1 \cdot d_2 + a_2 \cdot b_0 \cdot d_1 + a_2 \cdot b_1 \cdot d_0 + a_2 \cdot b_1 \cdot d_2 + a_2 \cdot b_1 + a_2 \cdot d_0 + a_2 \cdot d_1 + a_2 \cdot d_2 + a_2 + b_0 \cdot d_0 + b_0 \cdot d_1 + b_0 \cdot d_2 + b_1 \cdot d_0 + b_1 \cdot d_1 + b_2 \cdot d_0 + b_2 \cdot d_1 + b_2 + d_0 \cdot h_0 + d_0 \cdot h_1 + d_2 \cdot h_0 + d_2 \cdot h_1 + h_2 + i_2$$

$$y_{3,2} = d_2$$

$$y_{3,3} = c_2$$

$$y_{3,4} = a_0 \cdot b_2 + a_0 \cdot h_1 + a_1 \cdot b_0 + a_1 \cdot h_2 + a_2 \cdot b_1 + a_2 \cdot h_1 + b_2 + g_2 + h_2$$

$$y_{3,5} = b_2$$

$$y_{3,6} = a_2$$

$$y_{3,7} = a_0 \cdot b_2 + a_2 \cdot b_0 + a_2 \cdot b_1 + a_2 + b_2 + h_2$$

Arguing Uniformity: The input shares a_k, b_k, c_k, d_k can be uniquely recovered from the equations for $y_{k,l}$ for $l \in \{2,3,5,6\}$. The h_k's are then recovered from $y_{k,7}$, and then the g_k's from $y_{k,4}$ and then the i_k's from $y_{k,1}$. Denote $U_k := [i_k, h_k, g_k, d_k, c_k, b_k, a_k], \forall\ k \in\ [0,3]$. It can be seen that the mapping $(U_0, U_1, U_2) \rightarrow \{y_{k,l}\}_{k=0\rightarrow 3,\ l=1\rightarrow 7}$ is a permutation over $\{0,1\}^{28}$. Let us now inspect the expressions for $y_{k,0}$. Each input vector in $\{0,1\}^{28}$ of the above permutation gives rise to a specific mapping between $(e_0, e_1, e_2, e_3, f_0, f_1, f_2, f_3) \rightarrow (y_{0,0}, y_{1,0}, y_{2,0}, y_{3,0})$. Since f_k is a linear term in all 4 expressions that define all these maps, it is not difficult to verify that for every $(y_{0,0}, y_{1,0}, y_{2,0}, y_{3,0}) \in \{0,1\}^4$ there exist exactly 2^4 input pre-images $(e_0, e_1, e_2, e_3, f_0, f_1, f_2, f_3)$. Uniformity thus follows.