Supplementary Material

Anonymous Submission

1 First-Order PRINCE S-box Inverse without Randomness

$F(a,b,c,d)$: B732FD89A6405EC1

$$x = f(a,b,c,d) = 1 + d + ab + bc + cd + abd + acd$$
$$y = g(a,b,c,d) = 1 + ac + bc + bd + cd + abc$$
$$z = h(a,b,c,d) = a + c + ab + ac + bc + bd + abc + abd$$
$$t = k(a,b,c,d) = 1 + a + b + ab + ac + bc + cd + abc + acd + bcd$$

$$\begin{array}{ll}
f_0(a_0,b_0,c_0,d_1) = 1 + d_1 + a_0c_0 + b_0d_1 + a_0b_0d_1 + a_0c_0d_1 & \rightarrow x'_0 \\
f_1(a_0,b_0,c_1,d_0) = a_0 + d_0 + a_0b_0 + c_1d_0 + a_0b_0d_0 + a_0c_1d_0 & \rightarrow x'_1 \\
f_2(a_0,b_1,c_0,d_0) = c_0 + a_0c_0 + c_0d_0 + a_0b_1d_0 + a_0c_0d_0 & \rightarrow x'_2 \\
f_3(a_0,b_1,c_1,d_1) = a_0 + b_1 + a_0b_1 + b_1d_1 + a_0b_1d_1 + a_0c_1d_1 & \rightarrow x'_3 \\
\hline
f_4(a_1,b_0,c_0,d_0) = b_0 + c_0 + a_1c_0 + b_0c_0 + a_1d_0 + a_1b_0d_0 + a_1c_0d_0 & \rightarrow x'_4 \\
f_5(a_1,b_0,c_1,d_1) = b_0 + c_1 + a_1b_0 + a_1c_1 + b_0c_1 + b_0d_1 + c_1d_1 + a_1b_0d_1 + a_1c_1d_1 & \rightarrow x'_5 \\
f_6(a_1,b_1,c_0,d_1) = a_1 + a_1b_1 + a_1c_0 + b_1c_0 + b_1d_1 + c_0d_1 + a_1b_1d_1 + a_1c_0d_1 & \rightarrow x'_6 \\
f_7(a_1,b_1,c_1,d_0) = a_1 + b_1 + c_1 + a_1c_1 + b_1c_1 + a_1d_0 + a_1b_1d_0 + a_1c_1d_0 & \rightarrow x'_7
\end{array}$$

$$\begin{array}{ll}
g_0(a_0,b_1,c_1,d_0) = b_1 + c_1 + d_0 + a_0b_1 + a_0c_1 + a_0d_0 + b_1c_1 + b_1d_0 & \rightarrow y'_0 \\
g_1(a_0,b_1,c_0,d_0) = 1 + a_0b_1 + a_0c_0 + a_0d_0 + b_1c_0 + b_1d_0 & \rightarrow y'_1 \\
g_2(a_0,b_0,c_0,d_1) = b_0 + c_0 & \rightarrow y'_2 \\
g_3(a_0,b_1,c_1,d_0) = 1 + a_0 + b_1 + d_0 + a_0b_1 + a_0c_1 + a_0d_0 + b_1c_1 + b_1d_0 & \rightarrow y'_3 \\
\hline
g_4(a_0,b_1,c_1,d_1) = b_1 + c_1 & \rightarrow y'_4 \\
g_5(a_1,b_0,c_0,d_0) = 1 + a_1 + c_0 & \rightarrow y'_5 \\
g_6(a_1,b_0,c_1,d_1) = a_1 + c_1 + d_1 + a_1b_0 + a_1c_1 + a_1d_1 + b_0c_1 + b_0d_1 & \rightarrow y'_6 \\
g_7(a_1,b_0,c_0,d_1) = b_0 + c_0 + a_1b_0 + a_1c_0 + a_1d_1 + b_0c_0 + b_0d_1 & \rightarrow y'_7
\end{array}$$

$$\begin{array}{ll}
h_0(a_0,b_0,c_0,d_1) = a_0 + c_0 + a_0b_0 + a_0d_1 + a_0b_0c_0 + a_0b_0d_1 & \rightarrow z'_0 \\
h_1(a_0,b_0,c_1,d_0) = a_0b_0c_1 + a_0b_0d_0 & \rightarrow z'_1 \\
h_2(a_0,b_1,c_0,d_0) = a_0b_1 + a_0c_0 + b_1c_0 + b_1d_0 + a_0b_1c_0 + a_0b_1d_0 & \rightarrow z'_2 \\
h_3(a_0,b_1,c_1,d_1) = c_1 + d_1 + a_0c_1 + b_1c_1 + a_0d_1 + b_1d_1 + a_0b_1c_1 + a_0b_1d_1 & \rightarrow z'_3 \\
\hline
h_4(a_1,b_0,c_0,d_0) = b_0c_0 + b_0d_0 + a_1b_0c_0 + a_1b_0d_0 & \rightarrow z'_4 \\
h_5(a_1,b_0,c_1,d_1) = d_1 + a_1b_0 + a_1c_1 + b_0c_1 + a_1d_1 + b_0d_1 + a_1b_0c_1 + a_1b_0d_1 & \rightarrow z'_5 \\
h_6(a_1,b_1,c_0,d_1) = a_1b_1 + a_1c_0 + a_1d_1 + a_1b_1c_0 + a_1b_1d_1 & \rightarrow z'_6 \\
h_7(a_1,b_1,c_1,d_0) = a_1 + a_1b_1c_1 + a_1b_1d_0 & \rightarrow z'_7
\end{array}$$

$$\begin{array}{ll}
k_0(a_0,b_0,c_0,d_1) = 1 + b_0 + a_0b_0 + b_0c_0 + a_0d_1 + b_0d_1 + a_0b_0c_0 + a_0c_0d_1 + b_0c_0d_1 & \rightarrow t'_0 \\
k_1(a_0,b_0,c_1,d_0) = c_1d_0 + a_0b_0c_1 + a_0c_1d_0 + b_0c_1d_0 & \rightarrow t'_1 \\
k_2(a_0,b_1,c_0,d_0) = b_1 + a_0c_0 + b_1c_0 + c_0d_0 + a_0b_1c_0 + a_0c_0d_0 + b_1c_0d_0 & \rightarrow t'_2 \\
k_3(a_0,b_1,c_1,d_1) = a_0 + a_0b_1 + a_0c_1 + a_0d_1 + b_1d_1 + a_0b_1c_1 + a_0c_1d_1 + b_1c_1d_1 & \rightarrow t'_3 \\
\hline
k_4(a_1,b_0,c_0,d_0) = a_1c_0 + a_1b_0c_0 + a_1c_0d_0 + b_0c_0d_0 & \rightarrow t'_4 \\
k_5(a_1,b_0,c_1,d_1) = a_1 + d_1 + a_1b_0 + a_1c_1 + b_0c_1 + a_1d_1 + b_0d_1 + c_1d_1 + a_1b_0c_1 + & \\
\qquad a_1c_1d_1 + b_0c_1d_1 & \rightarrow t'_5 \\
k_6(a_1,b_1,c_0,d_1) = d_1 + a_1b_1 + a_1d_1 + b_1d_1 + c_0d_1 + a_1b_1c_0 + a_1c_0d_1 + b_1c_0d_1 & \rightarrow t'_6 \\
k_7(a_1,b_1,c_1,d_0) = b_1c_1 + a_1b_1c_1 + a_1c_1d_0 + b_1c_1d_0 & \rightarrow t'_7
\end{array}$$

$$\begin{array}{ll}
x'_0 + x'_1 + x'_2 + x'_3 = x_0 & x'_4 + x'_5 + x'_6 + x'_7 = x_1 \\
y'_0 + y'_3 + y'_0y'_1 + y'_0y'_2 + y'_0y'_3 + y'_1y'_2 + & y'_4 + y'_5 + y'_6 + y'_4y'_5 + y'_4y'_6 + y'_4y'_7 + \\
y'_1y'_3 = y_0 & y'_5y'_6 + y'_5y'_7 = y_1 \\
z'_0 + z'_1 + z'_2 + z'_3 = z_0 & z'_4 + z'_5 + z'_6 + z'_7 = z_1 \\
t'_0 + t'_1 + t'_2 + t'_3 = t_0 & t'_4 + t'_5 + t'_6 + t'_7 = t_1
\end{array}$$

2 First-Order PRINCE S-box without Randomness

$F(a, b, c, d) :$ BF32AC916780E5D4

$x = f(a, b, c, d) = 1 + c + d + ab + bc + ad + cd + abc$

$y = g(a, b, c, d) = 1 + ac + bc + bd + abc + bcd$

$z = h(a, b, c, d) = a + d + ab + ad + bd + abd + bcd$

$t = k(a, b, c, d) = 1 + b + d + bc + cd + abc + abd + acd$

$$\begin{array}{lr}
f_0(a_0, b_0, c_0, d_1) = 1 + c_0 + d_1 + b_0c_0 + a_0d_1 + a_0b_0c_0 & \rightarrow x'_0 \\
f_1(a_0, b_0, c_1, d_0) = a_0b_0 + a_0d_0 + a_0b_0c_1 & \rightarrow x'_1 \\
f_2(a_0, b_1, c_0, d_0) = b_1 + d_0 + a_0b_1 + b_1c_0 + a_0d_0 + a_0b_1c_0 & \rightarrow x'_2 \\
f_3(a_0, b_1, c_1, d_0) = c_1 + a_0d_0 + a_0b_1c_1 & \rightarrow x'_3 \\
\hline
f_4(a_1, b_0, c_0, d_0) = a_1b_0 + a_1d_0 + c_0d_0 + a_1b_0c_0 & \rightarrow x'_4 \\
f_5(a_1, b_0, c_1, d_0) = b_0c_1 + c_1d_0 + a_1b_0c_1 & \rightarrow x'_5 \\
f_6(a_1, b_1, c_0, d_1) = d_1 + a_1d_1 + c_0d_1 + a_1b_1c_0 & \rightarrow x'_6 \\
f_7(a_1, b_1, c_1, d_1) = b_1 + d_1 + a_1b_1 + b_1c_1 + c_1d_1 + a_1b_1c_1 & \rightarrow x'_7
\end{array}$$

$$\begin{array}{lr}
g_0(a_0, b_0, c_0, d_1) = 1 + a_0c_0 + c_0d_1 + a_0b_0c_0 + b_0c_0d_1 & \rightarrow y'_0 \\
g_1(a_0, b_0, c_1, d_0) = b_0c_1 + a_0b_0c_1 + b_0c_1d_0 & \rightarrow y'_1 \\
g_2(a_0, b_1, c_0, d_0) = a_0b_1 + b_1d_0 + a_0b_1c_0 + b_1c_0d_0 & \rightarrow y'_2 \\
g_3(a_0, b_1, c_1, d_1) = d_1 + a_0b_1 + a_0c_1 + b_1c_1 + b_1d_1 + c_1d_1 + a_0b_1c_1 + b_1c_1d_1 & \rightarrow y'_3 \\
\hline
g_4(a_1, b_0, c_0, d_0) = a_1 + c_0 + a_1b_0 + b_0c_0 + b_0d_0 + a_1b_0c_0 + b_0c_0d_0 & \rightarrow y'_4 \\
g_5(a_1, b_0, c_1, d_1) = a_1 + d_1 + a_1b_0 + a_1c_1 + b_0d_1 + c_1d_1 + a_1b_0c_1 + b_0c_1d_1 & \rightarrow y'_5 \\
g_6(a_1, b_1, c_0, d_1) = c_0 + a_1c_0 + b_1c_0 + c_0d_1 + a_1b_1c_0 + b_1c_0d_1 & \rightarrow y'_6 \\
g_7(a_1, b_1, c_1, d_0) = a_1b_1c_1 + b_1c_1d_0 & \rightarrow y'_7
\end{array}$$

$$\begin{array}{lr}
h_0(a_0, b_0, c_0, d_1) = a_0b_0 + b_0c_0 + b_0d_1 + a_0b_0d_1 + b_0c_0d_1 & \rightarrow z'_0 \\
h_1(a_0, b_1, c_0, d_1) = d_1 + a_0d_1 + a_0b_1d_1 + b_1c_0d_1 & \rightarrow z'_1 \\
h_2(a_1, b_0, c_1, d_1) = a_1b_0d_1 + b_0c_1d_1 & \rightarrow z'_2 \\
h_3(a_1, b_1, c_1, d_1) = b_1 + c_1 + a_1b_1 + b_1c_1 + a_1d_1 + b_1d_1 + a_1b_1d_1 + b_1c_1d_1 & \rightarrow z'_3 \\
\hline
h_4(a_0, b_0, c_1, d_0) = a_0 + c_1 + a_0d_0 + b_0d_0 + a_0b_0d_0 + b_0c_1d_0 & \rightarrow z'_4 \\
h_5(a_0, b_1, c_1, d_0) = a_0b_1 + b_1c_1 + a_0b_1d_0 + b_1c_1d_0 & \rightarrow z'_5 \\
h_6(a_1, b_0, c_0, d_0) = a_1 + a_1b_0 + b_0c_0 + a_1d_0 + a_1b_0d_0 + b_0c_0d_0 & \rightarrow z'_6 \\
h_7(a_1, b_1, c_0, d_0) = b_1 + d_0 + b_1d_0 + a_1b_1d_0 + b_1c_0d_0 & \rightarrow z'_7
\end{array}$$

$$\begin{array}{lr}
k_0(a_0, b_0, c_0, d_0) = 1 + a_0b_0 + a_0b_0c_0 + a_0b_0d_0 + a_0c_0d_0 & \rightarrow t'_0 \\
k_1(a_0, b_1, c_1, d_0) = b_1 + a_0b_1 + b_1c_1 + b_1d_0 + c_1d_0 + a_0b_1c_1 + a_0b_1d_0 + a_0c_1d_0 & \rightarrow t'_1 \\
k_2(a_1, b_0, c_1, d_0) = a_1 + d_0 + a_1c_1 + a_1b_0c_1 + a_1b_0d_0 + a_1c_1d_0 & \rightarrow t'_2 \\
k_3(a_1, b_1, c_0, d_0) = c_0 + a_1c_0 + b_1c_0 + b_1d_0 + c_0d_0 + a_1b_1c_0 + a_1b_1d_0 + a_1c_0d_0 & \rightarrow t'_3 \\
\hline
k_4(a_0, b_0, c_1, d_1) = b_0 + a_0b_0 + b_0c_1 + b_0d_1 + c_1d_1 + a_0b_0c_1 + a_0b_0d_1 + a_0c_1d_1 & \rightarrow t'_4 \\
k_5(a_0, b_1, c_0, d_1) = a_0b_1 + a_0b_1c_0 + a_0b_1d_1 + a_0c_0d_1 & \rightarrow t'_5 \\
k_6(a_1, b_0, c_0, d_1) = c_0 + a_1c_0 + b_0c_0 + b_0d_1 + c_0d_1 + a_1b_0c_0 + a_1b_0d_1 + a_1c_0d_1 & \rightarrow t'_6 \\
k_7(a_1, b_1, c_1, d_1) = a_1 + d_1 + a_1c_1 + a_1b_1c_1 + a_1b_1d_1 + a_1c_1d_1 & \rightarrow t'_7
\end{array}$$

$$\begin{array}{ll}
x'_0 + x'_1 + x'_2 + x'_3 = x_0 & x'_4 + x'_5 + x'_6 + x'_7 = x_1 \\
y'_0 + y'_1 + y'_2 + y'_3 = y_0 & y'_4 + y'_5 + y'_6 + y'_7 = y_1 \\
z'_0 + z'_1 + z'_2 + z'_3 = z_0 & z'_4 + z'_5 + z'_6 + z'_7 = z_1 \\
t'_0 + t'_1 + t'_2 + t'_3 = t_0 & t'_4 + t'_5 + t'_6 + t'_7 = t_1
\end{array}$$

3 First-Order SKINNY S-box without Randomness

$F(a,b,c,d)$: C6901A2B385D4E7F

$x = f(a,b,c,d) = b + c + d + ab + ac + ad + bd + abc + bcd$

$y = g(a,b,c,d) = a + d + ab + bc + bd + cd + bcd$

$z = h(a,b,c,d) = 1 + b + c + d + bc$

$t = k(a,b,c,d) = 1 + a + c + d + cd$

$$\begin{array}{lr}
f_0(a_0,b_0,c_1,d_1) = 1 + a_0 + c_1 + d_1 & \rightarrow x'_0 \\
f_1(a_0,b_0,c_0,d_1) = b_0 + c_0 + d_1 + a_0b_0 + a_0c_0 + a_0d_1 + b_0c_0 + b_0d_1 & \rightarrow x'_1 \\
f_2(a_0,b_0,c_0,d_0) = b_0 + d_0 & \rightarrow x'_2 \\
f_3(a_0,b_1,c_0,d_1) = a_0 + b_1 + c_0 + a_0b_1 + a_0c_0 + a_0d_1 + b_1c_0 + b_1d_1 & \rightarrow x'_3 \\
\hline
f_4(a_1,b_0,c_1,d_0) = a_1 + c_1 + d_0 & \rightarrow x'_4 \\
f_5(a_1,b_1,c_0,d_0) = a_1b_1 + a_1c_0 + a_1d_0 + b_1c_0 + b_1d_0 & \rightarrow x'_5 \\
f_6(a_1,b_1,c_0,d_1) = a_1 + b_1 + d_1 & \rightarrow x'_6 \\
f_7(a_1,b_0,c_0,d_0) = 1 + d_0 + a_1b_0 + a_1c_0 + a_1d_0 + b_0c_0 + b_0d_0 & \rightarrow x'_7
\end{array}$$

$$\begin{array}{lr}
g_0(a_0,b_1,c_0,d_0) = b_1 + c_0 & \rightarrow y'_0 \\
g_1(a_1,b_0,c_0,d_0) = c_0 + a_1b_0 + a_1c_0 + b_0d_0 + c_0d_0 & \rightarrow y'_1 \\
g_2(a_1,b_0,c_0,d_1) = 1 + a_1 + b_0 + d_1 + a_1b_0 + a_1c_0 + b_0d_1 + c_0d_1 & \rightarrow y'_2 \\
\hline
g_3(a_0,b_1,c_1,d_0) = b_1 + c_1 & \rightarrow y'_3 \\
g_4(a_0,b_0,c_1,d_1) = c_1 + a_0b_0 + a_0c_1 + b_0d_1 + c_1d_1 & \rightarrow y'_4 \\
g_5(a_0,b_0,c_1,d_0) = 1 + a_0 + b_0 + d_0 + a_0b_0 + a_0c_1 + b_0d_0 + c_1d_0 & \rightarrow y'_5
\end{array}$$

$$\begin{array}{lr}
h_0(a_0,b_1,c_1,d_0) = 1 + b_1c_1 + c_1d_0 & \rightarrow z'_0 \\
h_1(a_0,b_0,c_1,d_0) = b_0 + c_1 + d_0 + b_0c_1 + c_1d_0 & \rightarrow z'_1 \\
\hline
h_2(a_0,b_0,c_0,d_1) = c_0 + b_0c_0 + c_0d_1 & \rightarrow z'_2 \\
h_3(a_0,b_1,c_0,d_1) = b_1 + d_1 + b_1c_0 + c_0d_1 & \rightarrow z'_3
\end{array}$$

$$\begin{array}{lr}
k_0(a_0,b_1,c_1,d_0) = 1 + b_1c_1 + c_1d_0 & \rightarrow t'_0 \\
k_1(a_0,b_1,c_1,d_1) = a_0 + c_1 + d_1 + b_1c_1 + c_1d_1 & \rightarrow t'_1 \\
\hline
k_2(a_0,b_0,c_0,d_1) = c_0 + b_0c_0 + c_0d_1 & \rightarrow t'_2 \\
k_3(a_1,b_0,c_0,d_0) = a_1 + d_0 + b_0c_0 + c_0d_0 & \rightarrow t'_3
\end{array}$$

$$\begin{array}{ll}
x'_1 + x'_0x'_1 + x'_0x'_2 + x'_0x'_3 = x_0 & x'_5 + x'_4x'_5 + x'_4x'_6 + x'_4x'_7 = x_1 \\
y'_2 + y'_0y'_1 + y'_0y'_2 = y_0 & y'_5 + y'_3y'_4 + y'_3y'_5 = y_1 \\
z'_0 + z'_1 = z_0 & z'_2 + z'_3 = z_1 \\
t'_0 + t'_1 = t_0 & t'_2 + t'_3 = t_1
\end{array}$$

4 First-Order Mysterion S-box without Randomness

$F(a,b,c,d)$: 086D5F7C4E2391BA

$x = f(a,b,c,d) = c + ab$

$y = g(a,b,c,d) = b + ab + ac + ad + abc$

$z = h(a,b,c,d) = b + c + d + bc$

$t = k(a,b,c,d) = a + cd + abd$

$$f_0(a_0,b_0,c_1,d_1) = b_0 + c_1 + a_0b_0 + b_0c_1 + b_0d_1 \qquad \to x'_0$$
$$\underline{f_1(a_0,b_1,c_0,d_0) = a_0b_1 + b_1c_0 + b_1d_0 \qquad \to x'_1}$$
$$f_2(a_1,b_1,c_0,d_0) = c_0 + a_1b_1 + b_1c_0 + b_1d_0 \qquad \to x'_2$$
$$f_3(a_1,b_0,c_1,d_1) = b_0 + a_1b_0 + b_0c_1 + b_0d_1 \qquad \to x'_3$$

$$g_0(a_0,b_1,c_1,d_1) = b_1 + c_1 + d_1 + a_0c_1 + a_0d_1 + b_1c_1 + b_1d_1 \qquad \to y'_0$$
$$g_1(a_1,b_1,c_0,d_0) = a_1 + b_1 \qquad \to y'_1$$
$$\underline{g_2(a_0,b_1,c_0,d_1) = a_0 + a_0c_0 + a_0d_1 + b_1c_0 + b_1d_1 \qquad \to y'_2}$$
$$g_3(a_0,b_0,c_1,d_0) = a_0 + a_0c_1 + a_0d_0 + b_0c_1 + b_0d_0 \qquad \to y'_3$$
$$g_4(a_1,b_0,c_0,d_0) = 1 + a_1 + b_0 \qquad \to y'_4$$
$$g_5(a_0,b_0,c_0,d_0) = b_0 + c_0 + d_0 + a_0c_0 + a_0d_0 + b_0c_0 + b_0d_0 \qquad \to y'_5$$

$$h_0(a_0,b_0,c_1,d_1) = b_0 + c_1 + a_0b_0 + b_0c_1 + b_0d_1 \qquad \to z'_0$$
$$\underline{h_1(a_0,b_0,c_0,d_1) = d_1 + a_0b_0 + b_0c_0 + b_0d_1 \qquad \to z'_1}$$
$$h_2(a_1,b_1,c_0,d_0) = c_0 + a_1b_1 + b_1c_0 + b_1d_0 \qquad \to z'_2$$
$$h_3(a_1,b_1,c_1,d_0) = b_1 + d_0 + a_1b_1 + b_1c_1 + b_1d_0 \qquad \to z'_3$$

$$k_0(a_0,b_0,c_0,d_0) = 1 + a_0 + d_0 \qquad \to t'_0$$
$$k_1(a_0,b_0,c_1,d_1) = 1 + a_0 + d_1 + a_0b_0 + a_0c_1 + a_0d_1 + b_0d_1 + c_1d_1 \qquad \to t'_1$$
$$\underline{k_2(a_0,b_1,c_1,d_1) = a_0 + b_1 + c_1 + a_0b_1 + a_0c_1 + a_0d_1 + b_1d_1 + c_1d_1 \qquad \to t'_2}$$
$$k_3(a_1,b_1,c_0,d_1) = a_1 + b_1 + c_0 + a_1b_1 + a_1c_0 + a_1d_1 + b_1d_1 + c_0d_1 \qquad \to t'_3$$
$$k_4(a_1,b_0,c_0,d_0) = a_1 + d_0 \qquad \to t'_4$$
$$k_5(a_1,b_0,c_0,d_1) = a_1 + d_1 + a_1b_0 + a_1c_0 + a_1d_1 + b_0d_1 + c_0d_1 \qquad \to t'_5$$

$$\begin{array}{ll}
x'_0 + x'_1 = x_0 & x'_2 + x'_3 = x_1 \\
y'_2 + y'_0y'_1 + y'_1y'_2 = y_0 & y'_5 + y'_3y'_4 + y'_4y'_5 = y_1 \\
z'_0 + z'_1 = z_0 & z'_2 + z'_3 = z_1 \\
t'_0 + t'_2 + t'_0t'_1 + t'_0t'_2 = t_0 & t'_5 + t'_3t'_4 + t'_4t'_5 = t_1
\end{array}$$

5 First-Order GIFT S-box without Randomness

$F(a,b,c,d)$: 1A4C6F392DB7508E

$x = f(a,b,c,d) = 1 + a + b + c + d + ab$

$y = g(a,b,c,d) = a + c + d + ab + ac$

$z = h(a,b,c,d) = b + c + ad + bd + bcd$

$t = k(a,b,c,d) = a + bd + acd$

$f_0(a_1,b_1,c_1,d_0) = a_1 + b_1 + a_1b_1 + a_1c_1 \quad \rightarrow x'_0$

$f_1(a_1,b_0,c_1,d_0) = b_0 + c_1 + d_0 + a_1b_0 + a_1c_1 \quad \rightarrow x'_1$

$f_2(a_0,b_0,c_0,d_0) = a_0 + c_0 + a_0b_0 + a_0c_0 \quad \rightarrow x'_2$

$f_3(a_0,b_1,c_0,d_1) = 1 + d_1 + a_0b_1 + a_0c_0 \quad \rightarrow x'_3$

$g_0(a_1,b_1,c_1,d_0) = a_1 + b_1 + a_1b_1 + a_1c_1 \quad \rightarrow y'_0$

$g_1(a_1,b_0,c_0,d_1) = d_1 + a_1b_0 + a_1c_0 \quad \rightarrow y'_1$

$g_2(a_0,b_0,c_0,d_0) = a_0 + c_0 + a_0b_0 + a_0c_0 \quad \rightarrow y'_2$

$g_3(a_0,b_1,c_1,d_0) = b_1 + c_1 + d_0 + a_0b_1 + a_0c_1 \quad \rightarrow y'_3$

$h_0(a_0,b_0,c_1,d_0) = d_0 + a_0c_1 + a_0d_0 + b_0d_0 + c_1d_0 + b_0c_1d_0 \quad \rightarrow z'_0$

$h_1(a_0,b_0,c_1,d_1) = c_1 + a_0c_1 + a_0d_1 + b_0d_1 + c_1d_1 + b_0c_1d_1 \quad \rightarrow z'_1$

$h_2(a_1,b_0,c_0,d_0) = a_1b_0 + a_1c_0 + a_1d_0 + b_0c_0d_0 \quad \rightarrow z'_2$

$h_3(a_1,b_0,c_0,d_1) = b_0 + c_0 + d_1 + a_1b_0 + a_1c_0 + a_1d_1 + b_0c_0d_1 \quad \rightarrow z'_3$

$h_4(a_0,b_1,c_0,d_0) = b_1d_0 + b_1c_0d_0 \quad \rightarrow z'_4$

$h_5(a_0,b_1,c_0,d_1) = d_1 + b_1d_1 + b_1c_0d_1 \quad \rightarrow z'_5$

$h_6(a_0,b_1,c_1,d_0) = b_1 + d_0 + c_1d_0 + b_1c_1d_0 \quad \rightarrow z'_6$

$h_7(a_0,b_1,c_1,d_1) = c_1d_1 + b_1c_1d_1 \quad \rightarrow z'_7$

$k_0(a_0,b_0,c_0,d_1) = a_0 + d_1 \quad \rightarrow t'_0$

$k_1(a_0,b_1,c_1,d_0) = 1 + d_0 + a_0b_1 + a_0c_1 + b_1d_0 + c_1d_0 \quad \rightarrow t'_1$

$k_2(a_0,b_1,c_0,d_0) = b_1 + c_0 + d_0 + a_0b_1 + a_0c_0 + b_1d_0 + c_0d_0 \quad \rightarrow t'_2$

$k_3(a_1,b_0,c_0,d_0) = a_1 + d_0 \quad \rightarrow t'_3$

$k_4(a_1,b_0,c_0,d_1) = 1 + d_1 + a_1b_0 + a_1c_0 + b_0d_1 + c_0d_1 \quad \rightarrow t'_4$

$k_5(a_1,b_0,c_1,d_1) = b_0 + c_1 + d_1 + a_1b_0 + a_1c_1 + b_0d_1 + c_1d_1 \quad \rightarrow t'_5$

$$\begin{array}{ll}
x'_0 + x'_1 = x_0 & x'_2 + x'_3 = x_1 \\
y'_0 + y'_1 = y_0 & y'_2 + y'_3 = y_1 \\
z'_0 + z'_1 + z'_2 + z'_3 = z_0 & z'_4 + z'_5 + z'_6 + z'_7 = z_1 \\
t'_1 + t'_0t'_1 + t'_0t'_2 = t_0 & t'_4 + t'_3t'_4 + t'_3t'_5 = t_1
\end{array}$$

6 First-Order PRINCE-like S-box S_1 without Randomness

$F(a,b,c,d)$: 3158C2D9A4F0E6B7

$$x = f(a,b,c,d) = 1 + c + d + ab + bc + bd + cd + abc + bcd$$
$$y = g(a,b,c,d) = 1 + a + b + c + ab + bc + bd + cd + abd + acd + bcd$$
$$z = h(a,b,c,d) = b + c + ab + ac + ad + bc + abc + abd + bcd$$
$$t = k(a,b,c,d) = c + d + ab + ac + ad + cd + abd + acd$$

$$\begin{array}{lr}
f_0(a_0,b_0,c_0,d_1) = 1 + c_0 + b_0c_0 + c_0d_1 + a_0b_0c_0 + b_0c_0d_1 & \to x'_0 \\
f_1(a_0,b_1,c_0,d_0) = b_1 + a_0b_1 + b_1c_0 + b_1d_0 + a_0b_1c_0 + b_1c_0d_0 & \to x'_1 \\
f_2(a_1,b_0,c_0,d_0) = a_1c_0 + c_0d_0 + a_1b_0c_0 + b_0c_0d_0 & \to x'_2 \\
f_3(a_1,b_1,c_0,d_1) = a_1 + a_1b_1 + a_1c_0 + b_1d_1 + a_1b_1c_0 + b_1c_0d_1 & \to x'_3 \\
\hline
f_4(a_0,b_0,c_1,d_0) = c_1 + a_0b_0 + b_0d_0 + a_0b_0c_1 + b_0c_1d_0 & \to x'_4 \\
f_5(a_0,b_1,c_1,d_0) = b_1 + d_0 + b_1c_1 + c_1d_0 + a_0b_1c_1 + b_1c_1d_0 & \to x'_5 \\
f_6(a_1,b_0,c_1,d_1) = a_1 + d_1 + a_1b_0 + a_1c_1 + b_0c_1 + b_0d_1 + a_1b_0c_1 + b_0c_1d_1 & \to x'_6 \\
f_7(a_1,b_1,c_1,d_1) = a_1c_1 + c_1d_1 + a_1b_1c_1 + b_1c_1d_1 & \to x'_7
\end{array}$$

$$\begin{array}{lr}
g_0(a_0,b_0,c_0,d_1) = 1 + a_0 + a_0d_1 + a_0b_0d_1 + a_0c_0d_1 + b_0c_0d_1 & \to y'_0 \\
g_1(a_0,b_1,c_0,d_0) = a_0 + b_1d_0 + a_0b_1d_0 + a_0c_0d_0 + b_1c_0d_0 & \to y'_1 \\
g_2(a_1,b_0,c_0,d_0) = c_0 + a_1b_0 + a_1c_0 + b_0c_0 + c_0d_0 + a_1b_0d_0 + a_1c_0d_0 + b_0c_0d_0 & \to y'_2 \\
g_3(a_1,b_1,c_0,d_1) = b_1 + d_1 + a_1b_1 + a_1c_0 + b_1c_0 + a_1d_1 + b_1d_1 + c_0d_1 + & \\
\qquad\qquad\qquad\qquad a_1b_1d_1 + a_1c_0d_1 + b_1c_0d_1 & \to y'_3 \\
\hline
g_4(a_0,b_0,c_1,d_0) = a_0 + b_0 + a_0b_0 + a_0c_1 + b_0c_1 + b_0d_0 + a_0b_0d_0 + a_0c_1d_0 + b_0c_1d_0 & \to y'_4 \\
g_5(a_0,b_1,c_1,d_1) = a_0b_1 + a_0c_1 + b_1c_1 + a_0d_1 + a_0b_1d_1 + a_0c_1d_1 + b_1c_1d_1 & \to y'_5 \\
g_6(a_1,b_0,c_1,d_1) = a_1 + c_1 + d_1 + a_1d_1 + b_0d_1 + c_1d_1 + a_1b_0d_1 + a_1c_1d_1 + b_0c_1d_1 & \to y'_6 \\
g_7(a_1,b_1,c_1,d_0) = c_1d_0 + a_1b_1d_0 + a_1c_1d_0 + b_1c_1d_0 & \to y'_7
\end{array}$$

$$\begin{array}{lr}
h_0(a_0,b_0,c_0,d_0) = c_0 + a_0c_0 + b_0c_0 + a_0d_0 + c_0d_0 + a_0b_0c_0 + a_0b_0d_0 + b_0c_0d_0 & \to z'_0 \\
h_1(a_0,b_1,c_0,d_1) = b_1 + a_0b_1 + b_1c_0 + b_1d_1 + a_0b_1c_0 + a_0b_1d_1 + b_1c_0d_1 & \to z'_1 \\
h_2(a_1,b_0,c_0,d_1) = b_0d_1 + a_1b_0c_0 + a_1b_0d_1 + b_0c_0d_1 & \to z'_2 \\
h_3(a_1,b_1,c_0,d_0) = a_1b_1 + a_1c_0 + a_1d_0 + c_0d_0 + a_1b_1c_0 + a_1b_1d_0 + b_1c_0d_0 & \to z'_3 \\
\hline
h_4(a_0,b_0,c_1,d_1) = b_0 + c_1 + d_1 + a_0b_0 + a_0c_1 + b_0c_1 + a_0d_1 + b_0d_1 + c_1d_1 + & \\
\qquad\qquad\qquad\qquad a_0b_0c_1 + a_0b_0d_1 + b_0c_1d_1 & \to z'_4 \\
h_5(a_0,b_1,c_1,d_0) = b_1c_1 + a_0b_1c_1 + a_0b_1d_0 + b_1c_1d_0 & \to z'_5 \\
h_6(a_1,b_0,c_1,d_0) = a_1b_0 + a_1b_0c_1 + a_1b_0d_0 + b_0c_1d_0 & \to z'_6 \\
h_7(a_1,b_1,c_1,d_1) = d_1 + a_1c_1 + a_1d_1 + b_1d_1 + c_1d_1 + a_1b_1c_1 + a_1b_1d_1 + b_1c_1d_1 & \to z'_7
\end{array}$$

$$\begin{array}{lr}
k_0(a_0,b_0,c_1,d_0) = c_1 + a_0c_1 + c_1d_0 + a_0b_0d_0 + a_0c_1d_0 & \to t'_0 \\
k_1(a_0,b_1,c_0,d_0) = d_0 + a_0b_1 + a_0d_0 + c_0d_0 + a_0b_1d_0 + a_0c_0d_0 & \to t'_1 \\
k_2(a_1,b_0,c_1,d_0) = a_1c_1 + a_1b_0d_0 + a_1c_1d_0 & \to t'_2 \\
k_3(a_1,b_1,c_0,d_0) = a_1b_1 + a_1d_0 + a_1b_1d_0 + a_1c_0d_0 & \to t'_3 \\
\hline
k_4(a_0,b_0,c_1,d_1) = a_0b_0 + a_0d_1 + a_0b_0d_1 + a_0c_1d_1 & \to t'_4 \\
k_5(a_0,b_1,c_0,d_1) = a_0c_0 + a_0b_1d_1 + a_0c_0d_1 & \to t'_5 \\
k_6(a_1,b_0,c_1,d_1) = d_1 + a_1b_0 + a_1d_1 + c_1d_1 + a_1b_0d_1 + a_1c_1d_1 & \to t'_6 \\
k_7(a_1,b_1,c_0,d_1) = c_0 + a_1c_0 + c_0d_1 + a_1b_1d_1 + a_1c_0d_1 & \to t'_7
\end{array}$$

$$\begin{array}{ll}
x'_0 + x'_1 + x'_2 + x'_3 = x_0 & \qquad x'_4 + x'_5 + x'_6 + x'_7 = x_1 \\
y'_0 + y'_1 + y'_2 + y'_3 = y_0 & \qquad y'_4 + y'_5 + y'_6 + y'_7 = y_1 \\
z'_0 + z'_1 + z'_2 + z'_3 = z_0 & \qquad z'_4 + z'_5 + z'_6 + z'_7 = z_1 \\
t'_0 + t'_1 + t'_2 + t'_3 = t_0 & \qquad t'_4 + t'_5 + t'_6 + t'_7 = t_1
\end{array}$$

7 First-Order PRINCE-like S-box S_1 Inverse without Randomness

$F(a, b, c, d)$: B15092DF378E46CA

$$x = f(a, b, c, d) = 1 + ab + ac + bd + cd + abd + acd + bcd$$
$$y = g(a, b, c, d) = 1 + a + b + c + ab + ad + bc + abc + acd$$
$$z = h(a, b, c, d) = b + ab + ad + bd + cd + abc + abd + acd$$
$$t = k(a, b, c, d) = 1 + a + b + d + ab + ad + bc + abd + bcd$$

$$f_0(a_0, b_0, c_0, d_1) = 1 + a_0d_1 + a_0b_0d_1 + a_0c_0d_1 + b_0c_0d_1 \qquad \rightarrow x'_0$$
$$f_1(a_0, b_0, c_1, d_0) = c_1 + a_0b_0 + a_0c_1 + b_0c_1 + c_1d_0 + a_0b_0d_0 + a_0c_1d_0 + b_0c_1d_0 \qquad \rightarrow x'_1$$
$$f_2(a_1, b_0, c_0, d_0) = b_0d_0 + a_1b_0d_0 + a_1c_0d_0 + b_0c_0d_0 \qquad \rightarrow x'_2$$
$$f_3(a_1, b_0, c_1, d_1) = a_1 + c_1 + d_1 + a_1b_0 + a_1c_1 + b_0c_1 + a_1d_1 + b_0d_1 + c_1d_1 + a_1b_0d_1 + a_1c_1d_1 + b_0c_1d_1 \qquad \rightarrow x'_3$$

$$f_4(a_0, b_1, c_0, d_0) = c_0 + a_0b_1 + a_0c_0 + b_1c_0 + c_0d_0 + a_0b_1d_0 + a_0c_0d_0 + b_1c_0d_0 \qquad \rightarrow x'_4$$
$$f_5(a_0, b_1, c_1, d_1) = a_0d_1 + a_0b_1d_1 + a_0c_1d_1 + b_1c_1d_1 \qquad \rightarrow x'_5$$
$$f_6(a_1, b_1, c_0, d_1) = a_1 + c_0 + d_1 + a_1b_1 + a_1c_0 + b_1c_0 + a_1d_1 + b_1d_1 + c_0d_1 + a_1b_1d_1 + a_1c_0d_1 + b_1c_0d_1 \qquad \rightarrow x'_6$$
$$f_7(a_1, b_1, c_1, d_0) = b_1d_0 + a_1b_1d_0 + a_1c_1d_0 + b_1c_1d_0 \qquad \rightarrow x'_7$$

$$g_0(a_0, b_0, c_0, d_1) = 1 + b_0c_0 + a_0b_0c_0 + a_0c_0d_1 \qquad \rightarrow y'_0$$
$$g_1(a_0, b_1, c_0, d_0) = b_1 + a_0b_1 + b_1c_0 + a_0d_0 + a_0b_1c_0 + a_0c_0d_0 \qquad \rightarrow y'_1$$
$$g_2(a_1, b_0, c_0, d_0) = a_1b_0c_0 + a_1c_0d_0 \qquad \rightarrow y'_2$$
$$g_3(a_1, b_1, c_0, d_1) = a_1 + c_0 + a_1b_1 + a_1d_1 + a_1b_1c_0 + a_1c_0d_1 \qquad \rightarrow y'_3$$

$$g_4(a_0, b_0, c_1, d_1) = a_0b_0 + a_0d_1 + a_0b_0c_1 + a_0c_1d_1 \qquad \rightarrow y'_4$$
$$g_5(a_0, b_1, c_1, d_0) = a_0 + b_1c_1 + a_0b_1c_1 + a_0c_1d_0 \qquad \rightarrow y'_5$$
$$g_6(a_1, b_0, c_1, d_0) = b_0 + a_1b_0 + b_0c_1 + a_1d_0 + a_1b_0c_1 + a_1c_1d_0 \qquad \rightarrow y'_6$$
$$g_7(a_1, b_1, c_1, d_1) = c_1 + a_1b_1c_1 + a_1c_1d_1 \qquad \rightarrow y'_7$$

$$h_0(a_0, b_0, c_0, d_1) = a_0b_0 + a_0b_0c_0 + a_0b_0d_1 + a_0c_0d_1 \qquad \rightarrow z'_0$$
$$h_1(a_0, b_1, c_0, d_0) = b_1 + a_0b_1 + b_1c_0 + b_1d_0 + c_0d_0 + a_0b_1c_0 + a_0b_1d_0 + a_0c_0d_0 \qquad \rightarrow z'_1$$
$$h_2(a_1, b_0, c_0, d_0) = a_1d_0 + a_1b_0c_0 + a_1b_0d_0 + a_1c_0d_0 \qquad \rightarrow z'_2$$
$$h_3(a_1, b_1, c_0, d_1) = a_1 + b_1c_0 + a_1d_1 + b_1d_1 + c_0d_1 + a_1b_1c_0 + a_1b_1d_1 + a_1c_0d_1 \qquad \rightarrow z'_3$$

$$h_4(a_0, b_0, c_1, d_0) = d_0 + b_0c_1 + a_0d_0 + b_0d_0 + c_1d_0 + a_0b_0c_1 + a_0b_0d_0 + a_0c_1d_0 \qquad \rightarrow z'_4$$
$$h_5(a_0, b_1, c_1, d_1) = a_0d_1 + a_0b_1c_1 + a_0b_1d_1 + a_0c_1d_1 \qquad \rightarrow z'_5$$
$$h_6(a_1, b_0, c_1, d_1) = b_0 + a_1b_0 + b_0c_1 + b_0d_1 + c_1d_1 + a_1b_0c_1 + a_1b_0d_1 + a_1c_1d_1 \qquad \rightarrow z'_6$$
$$h_7(a_1, b_1, c_1, d_0) = a_1 + d_0 + a_1b_1 + a_1b_1c_1 + a_1b_1d_0 + a_1c_1d_0 \qquad \rightarrow z'_7$$

$$k_0(a_0, b_0, c_1, d_0) = 1 + b_0 + a_0b_0 + a_0b_0d_0 + b_0c_1d_0 \qquad \rightarrow t'_0$$
$$k_1(a_0, b_0, c_1, d_1) = c_1 + b_0c_1 + a_0d_1 + c_1d_1 + a_0b_0d_1 + b_0c_1d_1 \qquad \rightarrow t'_1$$
$$k_2(a_1, b_0, c_0, d_0) = a_1b_0 + b_0c_0 + a_1d_0 + c_0d_0 + a_1b_0d_0 + b_0c_0d_0 \qquad \rightarrow t'_2$$
$$k_3(a_1, b_0, c_0, d_1) = a_1b_0d_1 + b_0c_0d_1 \qquad \rightarrow t'_3$$

$$k_4(a_0, b_1, c_0, d_0) = a_0 + d_0 + a_0b_1 + a_0d_0 + c_0d_0 + a_0b_1d_0 + b_1c_0d_0 \qquad \rightarrow t'_4$$
$$k_5(a_0, b_1, c_0, d_1) = b_1 + d_1 + b_1c_0 + a_0b_1d_1 + b_1c_0d_1 \qquad \rightarrow t'_5$$
$$k_6(a_1, b_1, c_1, d_0) = a_1 + c_1 + a_1b_1d_0 + b_1c_1d_0 \qquad \rightarrow t'_6$$
$$k_7(a_1, b_1, c_1, d_1) = a_1b_1 + b_1c_1 + a_1d_1 + c_1d_1 + a_1b_1d_1 + b_1c_1d_1 \qquad \rightarrow t'_7$$

$$\begin{array}{ll}
x'_0 + x'_1 + x'_2 + x'_3 = x_0 & x'_4 + x'_5 + x'_6 + x'_7 = x_1 \\
y'_0 + y'_1 + y'_2 + y'_3 = y_0 & y'_4 + y'_5 + y'_6 + y'_7 = y_1 \\
z'_0 + z'_1 + z'_2 + z'_3 = z_0 & z'_4 + z'_5 + z'_6 + z'_7 = z_1 \\
t'_0 + t'_1 + t'_2 + t'_3 = t_0 & t'_4 + t'_5 + t'_6 + t'_7 = t_1
\end{array}$$