X_0 SC AC Y_0 $\gg 1$ $\gg 2$ $\gg 3$ W_0 W'_0 ETK_0 0 1 2 3 0 1 2 3 7 4 5 6 0 1 2 3 X_1 SC AC Y_1 STK_1 9 f 8 d a e c b Z_1 $\gg 1$ $\gg 2$ $\gg 3$ W_1 X_2
X_2 SC AC Y_2 STK_2 1 7 0 5 2 6 4 3 Z_2 $\gg 1$ $\gg 2$ $\gg 3$ W_2 X_3 SC AC Y_3 STK_3 f b 9 e 8 c a d Z_3 $\gg 1$ $\gg 2$ $\gg 3$ W_3 X_4
X_4 SC AC Y_4 STK_4 7 3 1 6 0 4 2 5 Z_4 $\gg 1$ $\gg 2$ $\gg 3$ W_4 X_5 SC AC Y_5 STK_5 b d f c 9 a 8 e Z_5 $\gg 1$ $\gg 2$ $\gg 3$ W_5 X_6
X_6 SC AC Y_6 STK_6 3 5 7 4 1 2 0 6 Z_6 $\gg 1$ $\gg 2$ $\gg 3$ W_6 X_7 SC AC Y_7 STK_7 d e b a f 8 9 c Z_7 $\gg 1$ $\gg 2$ $\gg 3$ W_7 X_8
X_8 SC AC Y_8 STK_8 5 6 3 2 7 0 1 4 Z_8 $\gg 1$ $\gg 2$ $\gg 3$ W_8 X_9 SC AC Y_9 STK_9 e c d 8 b 9 f a Z_9 $\gg 1$ $\gg 2$ $\gg 3$ W_9 X_{10}
X_{10} SC AC Y_{10} STK_{10} 6 4 5 0 3 1 7 2 Z_{10} $\gg 1$ $\gg 2$ $\gg 3$ W_{10} X_{11} SC AC Y_{11} STK_{11} c a e 9 d f b 8 Z_{11} $\gg 1$ $\gg 2$ $\gg 3$ W_{11} X_{12}
X_{12} SC AC Y_{12} STK_{12} 4 2 6 1 5 7 3 0 Z_{12} $\gg 1$ $\gg 2$ $\gg 3$ W_{12} X_{13} SC AC Y_{13} STK_{13} a 8 c f e b d 9 Z_{13} $\gg 1$ $\gg 2$ $\gg 3$ W_{13} X_{14}
X_{14} SC AC Y_{14} STK_{14} 2 0 4 7 6 3 5 1 Z_{14} $\gg 1$ $\gg 2$ $\gg 3$ W_{14} X_{15} SC AC Y_{15} STK_{15} 8 9 a b c d e f Z_{15} $\gg 1$ $\gg 2$ $\gg 3$ W_{15} X_{16}
X_{16} SC AC Y_{16} STK_{16} 0 1 2 3 4 5 6 7 Z_{16} $\gg 1$ $\gg 2$ $\gg 3$ W_{16} X_{17} SC AC Y_{17} STK_{17} 9 f 8 d a e c b Z_{17} $\gg 1$ $\gg 2$ $\gg 3$ W_{17} X_{18}
X_{18} SC AC Y_{18} STK_{18} 1 7 0 5 2 6 4 3 Z_{18} $\gg 1$ $\gg 2$ $\gg 3$ W_{18} X_{19} SC AC Y_{19} STK_{19} f b 9 e 8 c a d Z_{19} $\gg 1$ $\gg 2$ $\gg 3$ W_{19} X_{20}
X_{20} SC AC Y_{20} STK_{20} 7 3 1 6 0 4 2 5 Z_{20} $\gg 1$ $\gg 2$ $\gg 3$ W_{20} X_{21} SC AC Y_{21} STK_{21} b d f c 9 a 8 e Z_{21} $\gg 1$ $\gg 2$ $\gg 3$ W_{21} X_{22}
X_{22} SC AC Y_{22} STK_{22} 3 5 7 4 1 2 0 6 Z_{22} $\gg 1$ $\gg 2$ $\gg 3$ W_{22} X_{23}
nonzero
any
involved in key-recovery
diff. value is needed
value is needed