

*input bytes*

$in_0$	$in_4$	$in_8$	$in_{12}$
$in_1$	$in_5$	$in_9$	$in_{13}$
$in_2$	$in_6$	$in_{10}$	$in_{14}$
$in_3$	$in_7$	$in_{11}$	$in_{15}$



*State array*

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$



*output bytes*

$out_0$	$out_4$	$out_8$	$out_{12}$
$out_1$	$out_5$	$out_9$	$out_{13}$
$out_2$	$out_6$	$out_{10}$	$out_{14}$
$out_3$	$out_7$	$out_{11}$	$out_{15}$