

64
state
$_{ m bits}$

 $p_{0.0}$ $p_{0,1}$ $p_{15,1}$ $p_{0.1}$ $p_{0,63}$ $p_{0,2}$ $p_{15,2}$ $p_{1,0}$ $p_{1,1}$ $p_{1.63}$ $p_{15,0}$ $p_{15,1}$ $p_{15.63}$ $p_{0,14}$ $p_{15,62}$. . . $p_{0.15}$

64 state bits

16 plaintexts

 $p_{15,63}$

 $p_{15,0}$

. . .

16 plaintexts

 $p_{0,0}$