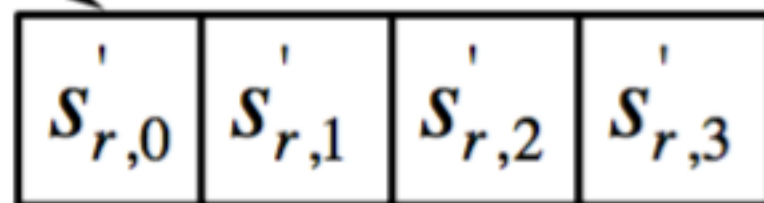
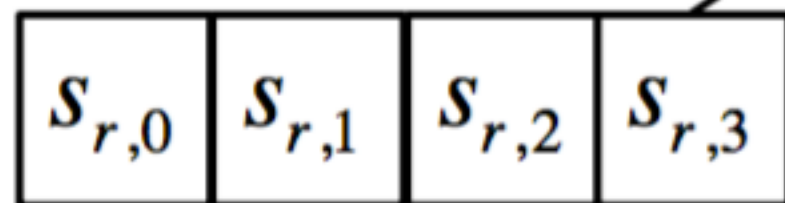
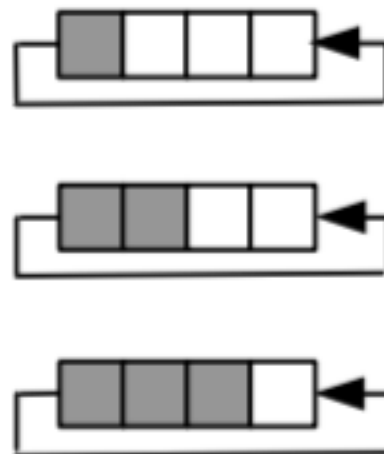


ShiftRows ()



S

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



S'

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