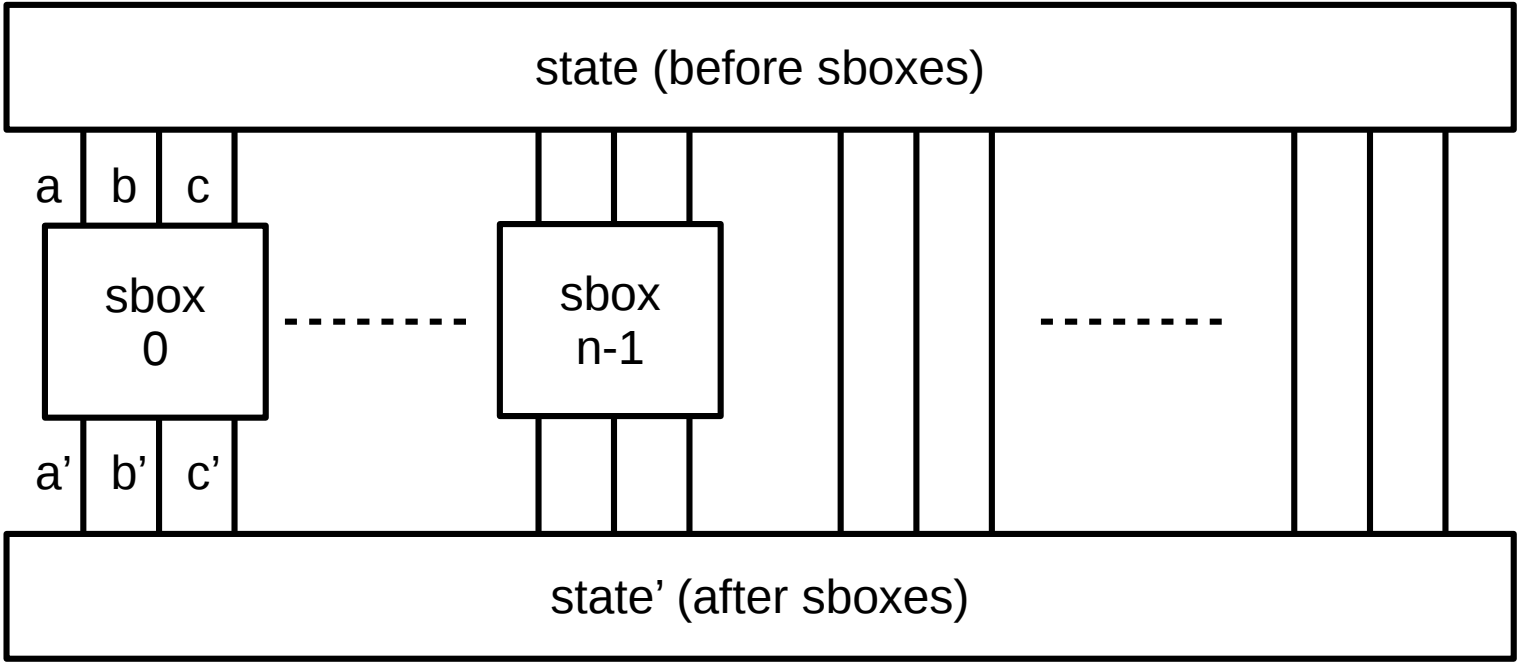
state (before sboxes)
a
b
c
sbox
0
sbox
n-1
a'
b'
c'
state' (after sboxes)