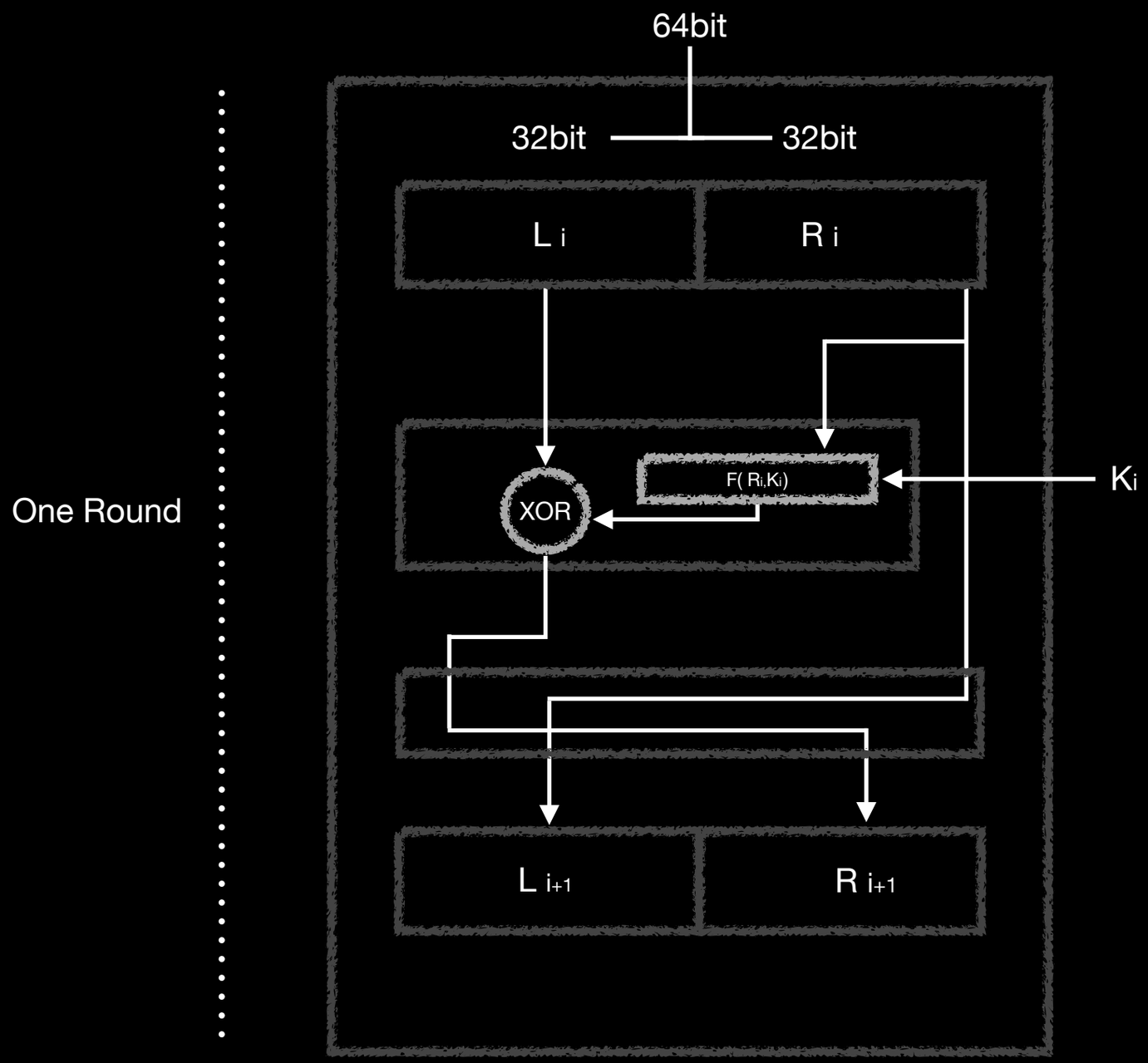
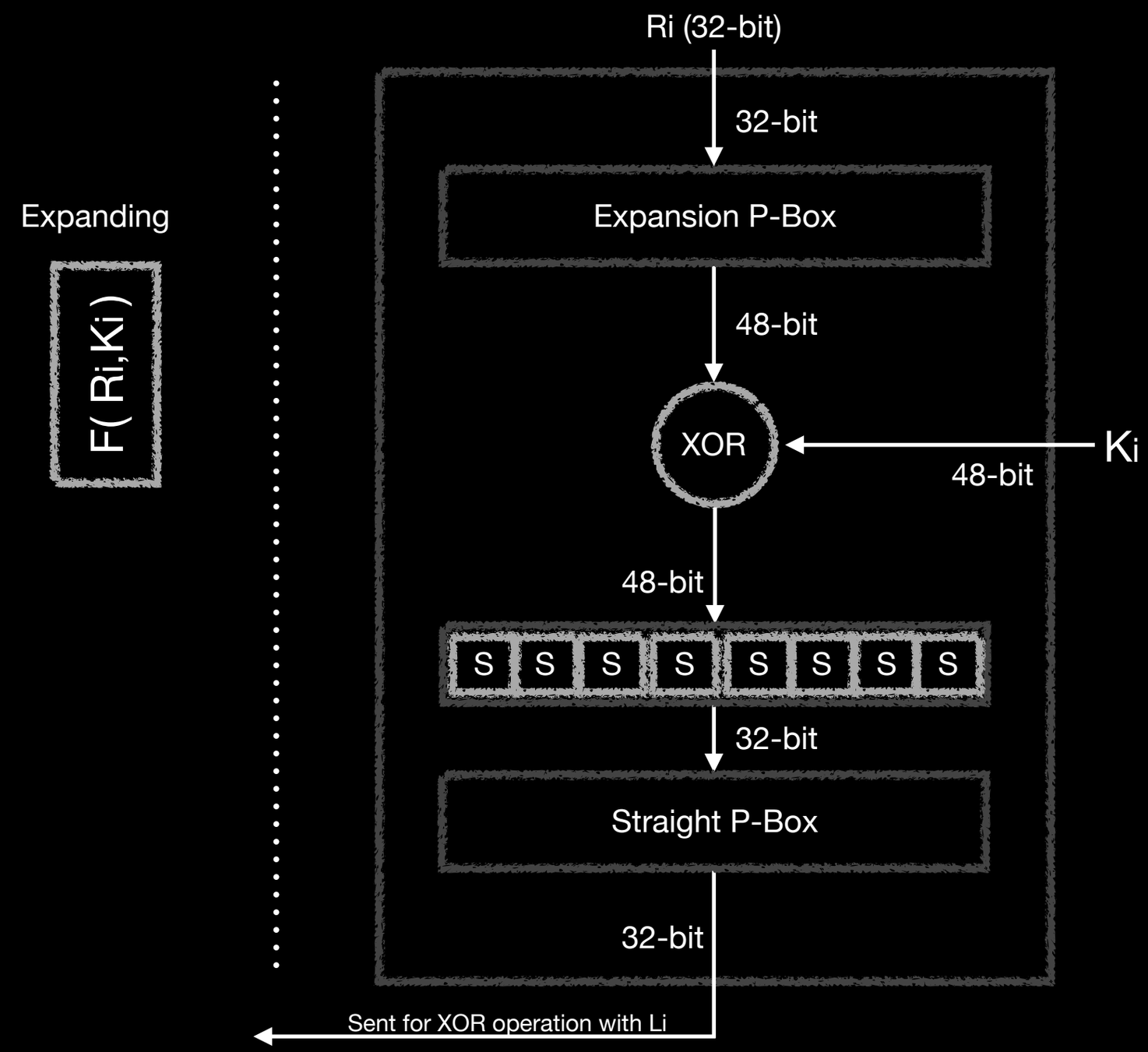
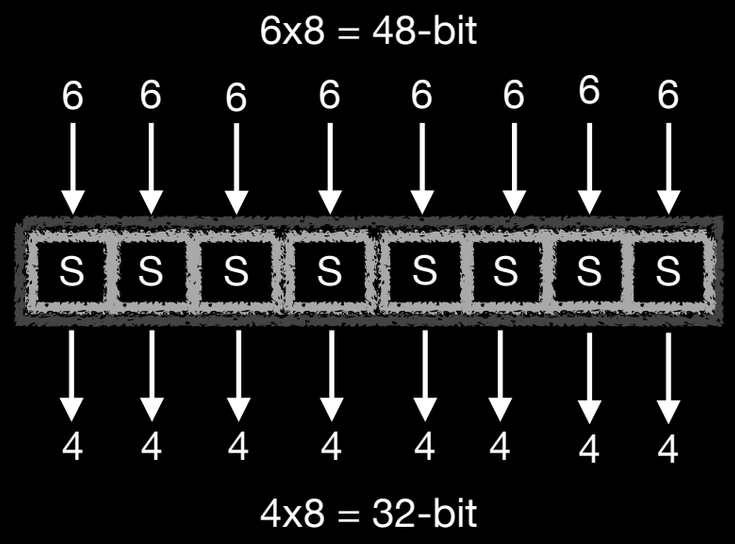
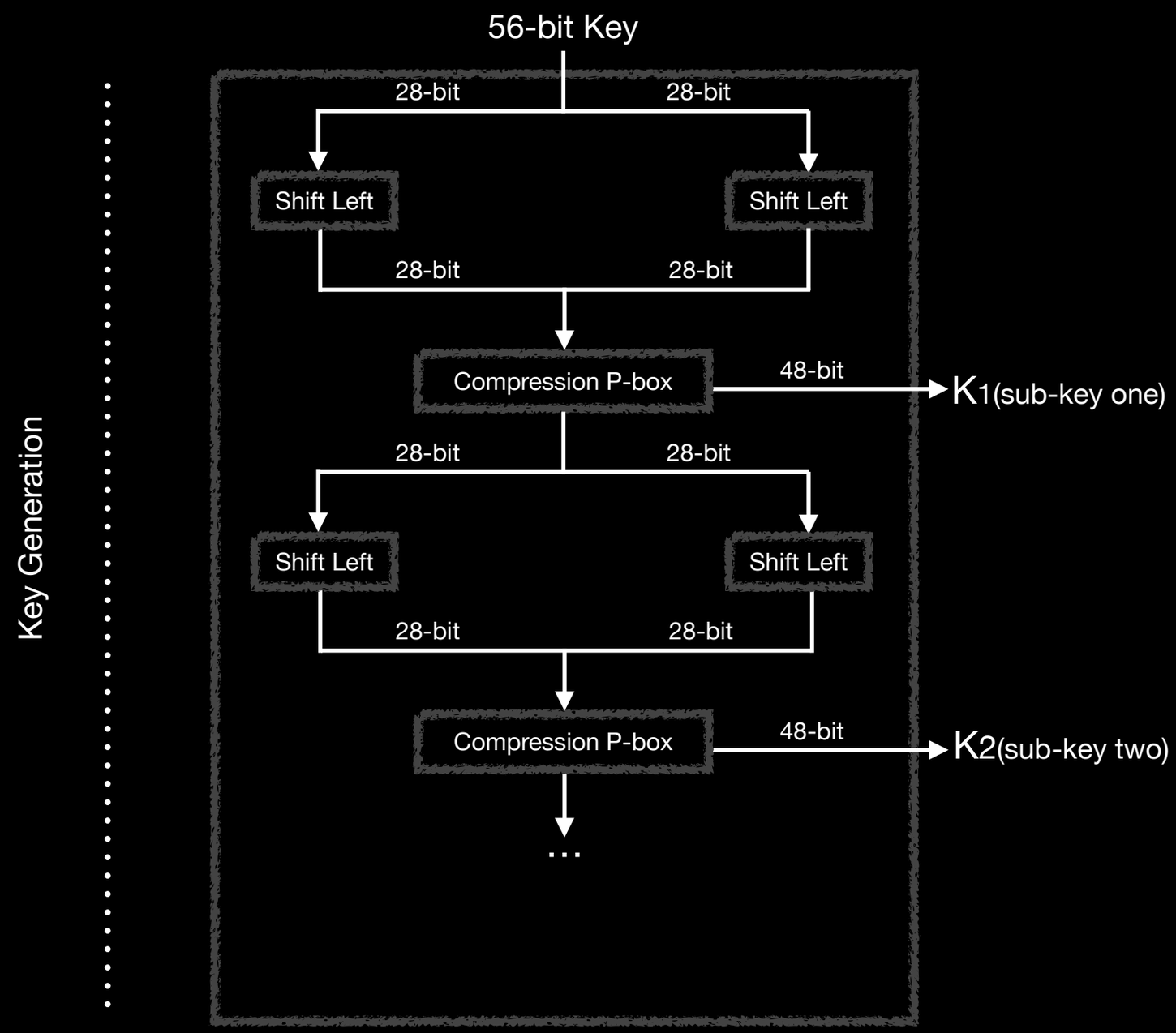

One Round
64bit
32bit
32bit
L i
R i
XOR
F(Ri,Ki)
Ki
L i+1
R i+1


Ri (32-bit)
32-bit
Expansion P-Box
48-bit
XOR
Ki
48-bit
48-bit
S S S S S S S S
32-bit
Straight P-Box
32-bit
Sent for XOR operation with Li
Expanding
F(Ri,Ki)


6x8 = 48-bit
6 6 6 6 6 6 6 6
S S S S S S S S
4 4 4 4 4 4 4 4
4x8 = 32-bit


56-bit Key
28-bit
28-bit
Shift Left
Shift Left
28-bit
28-bit
Compression P-box
48-bit
K1(sub-key one)
28-bit
28-bit
Shift Left
Shift Left
28-bit
28-bit
Compression P-box
48-bit
K2(sub-key two)
...
Key Generation