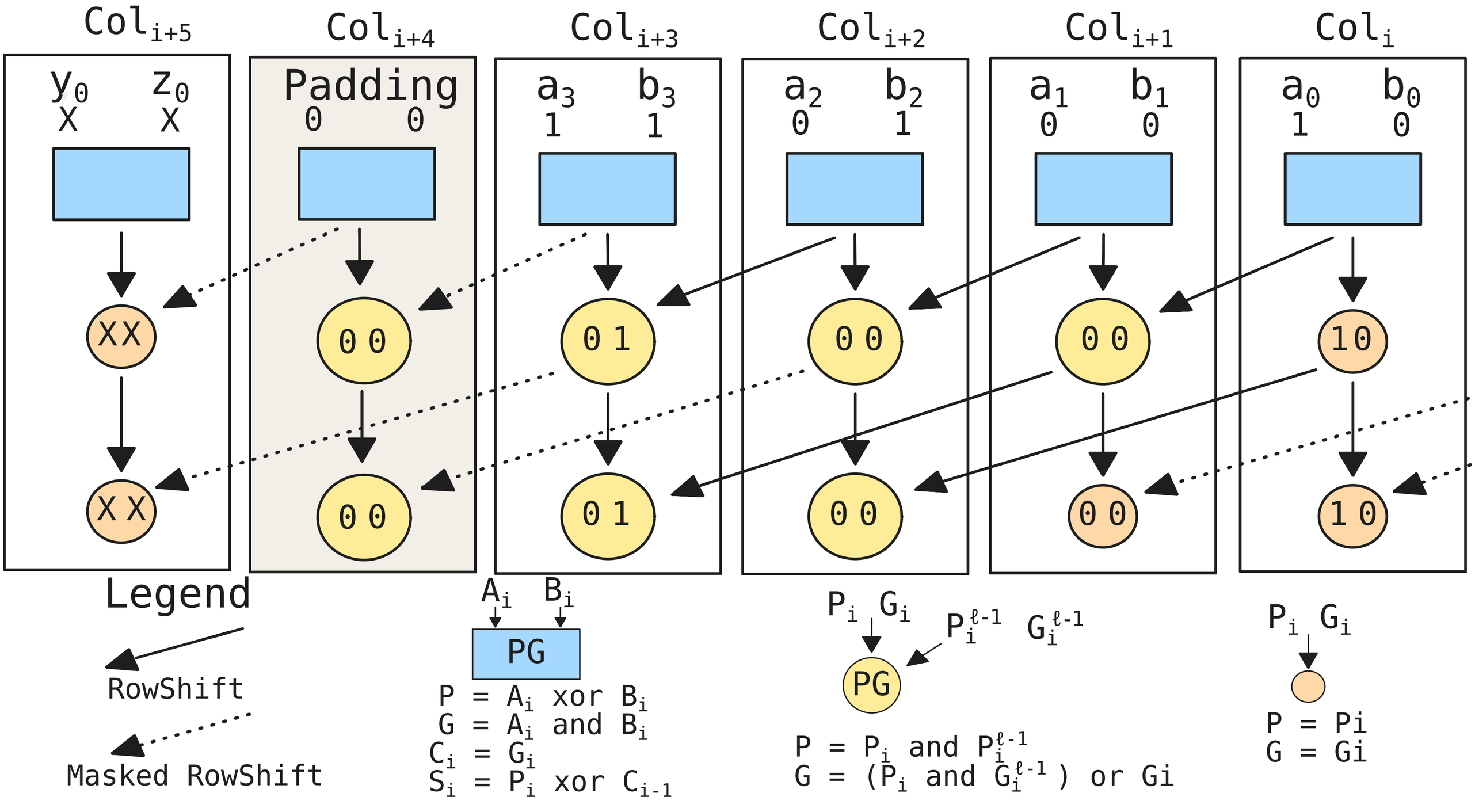

Col i+5
Col i+4
Col i+3
Col i+2
Col i+1
Col i
y0 z0
X X
Padding
0 0
a3 b3
1 1
a2 b2
0 1
a1 b1
0 0
a0 b0
1 0
XX
00
01
00
00
10
XX
00
01
00
00
10
Legend
RowShift
Masked RowShift
Ai Bi
PG
P = Ai xor Bi
G = Ai and Bi
Ci = Gi
Si = Pi xor Ci-1
Pi Gi
Pi ℓ-1 Gi ℓ-1
PG
P = Pi and Pi ℓ-1
G = (Pi and Gi ℓ-1) or Gi
Pi Gi
P = Pi
G = Gi