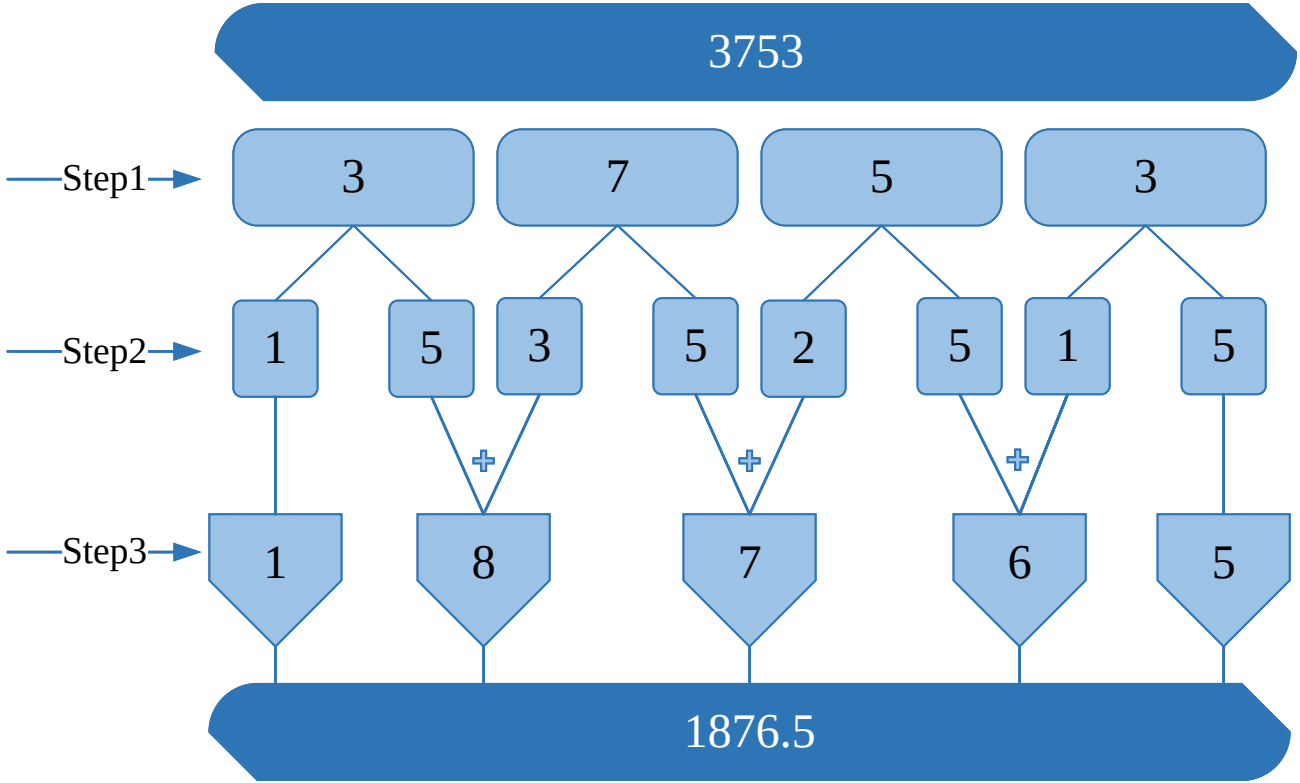
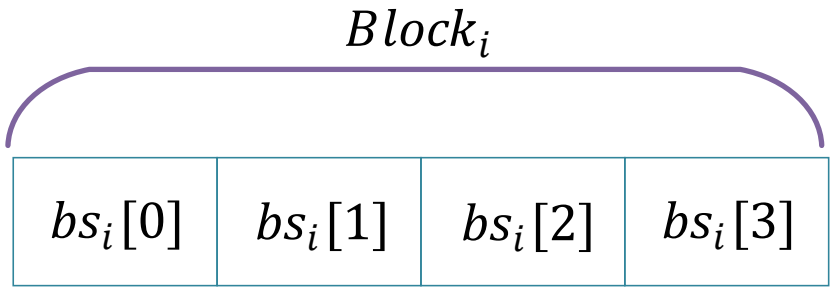
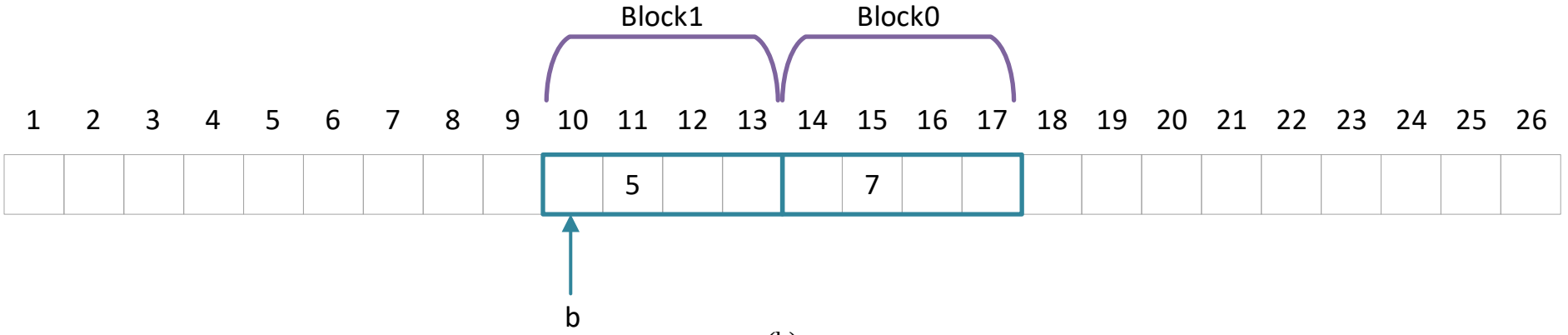
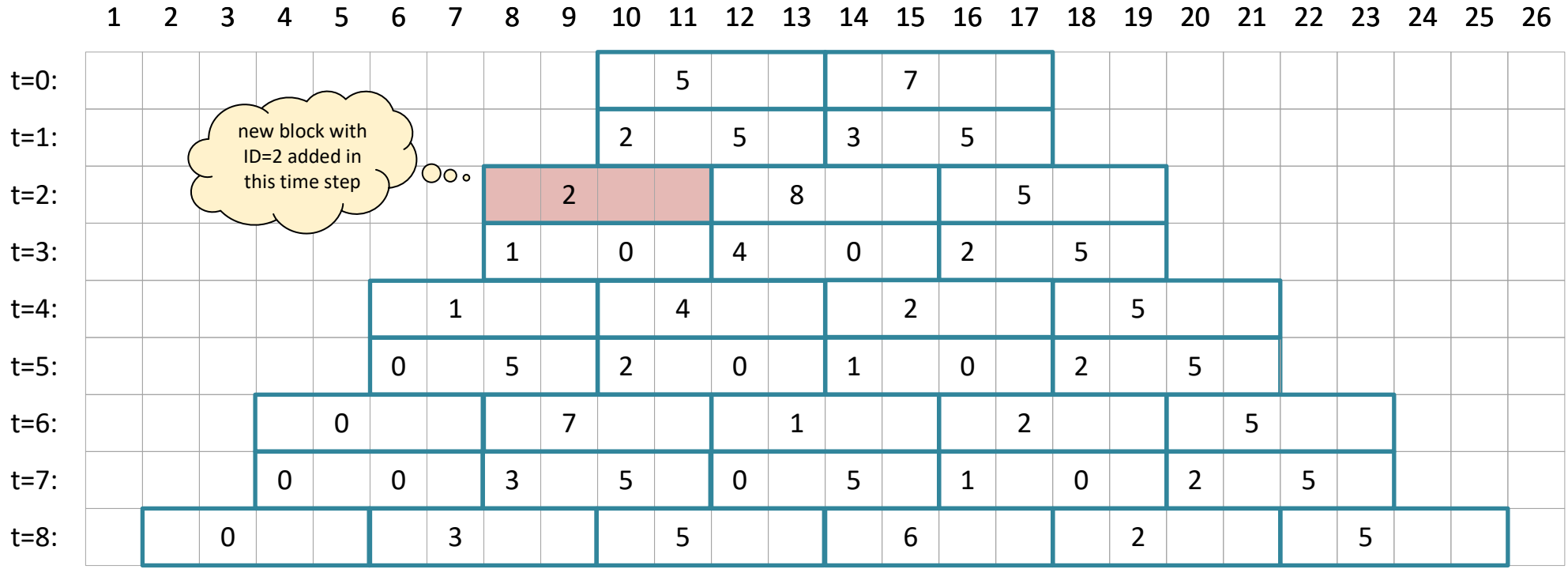

3753
Step1
3
7
5
3
Step2
1
5
3
5
2
5
1
5
Step3
1
8
7
6
5
1876.5

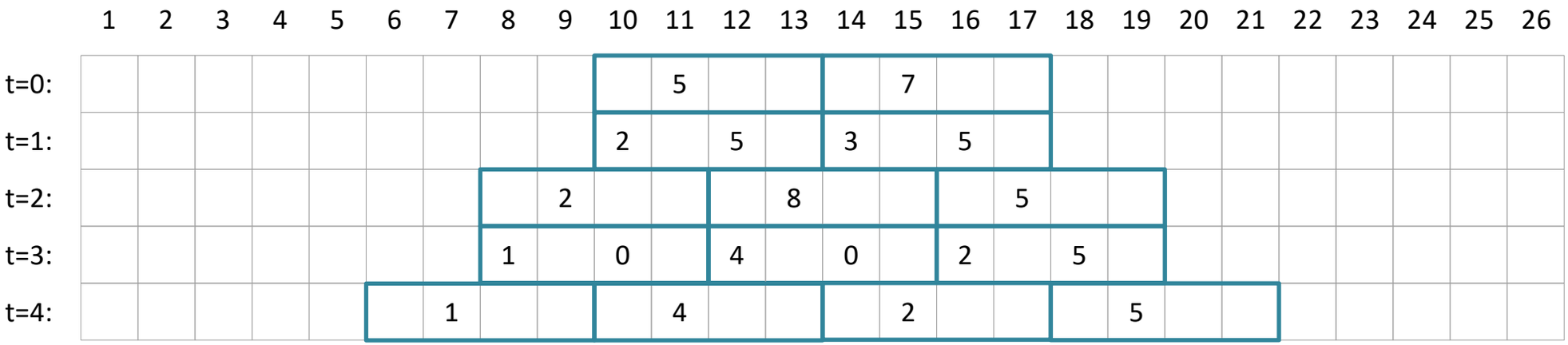

$Block_i$
$bs_i[0]$
$bs_i[1]$
$bs_i[2]$
$bs_i[3]$

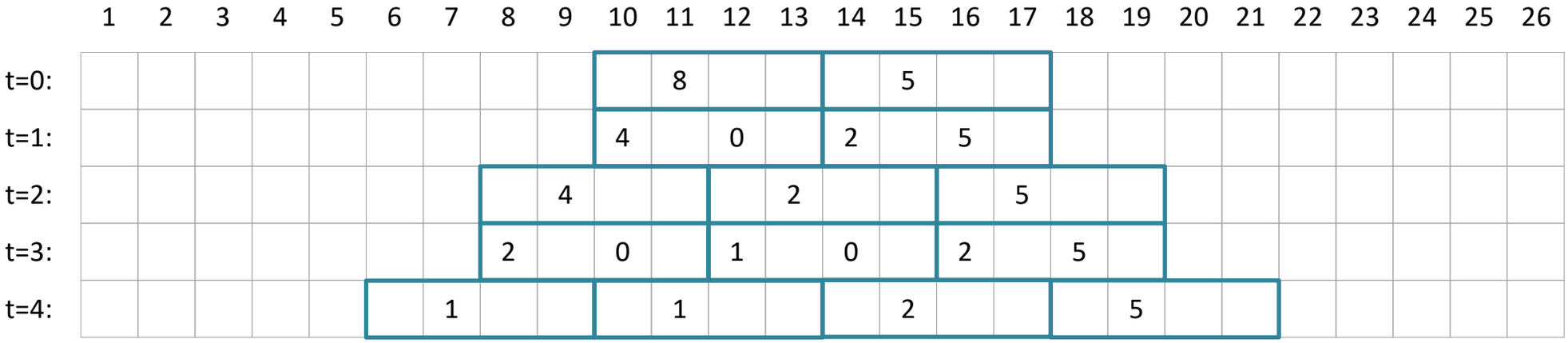
(a)

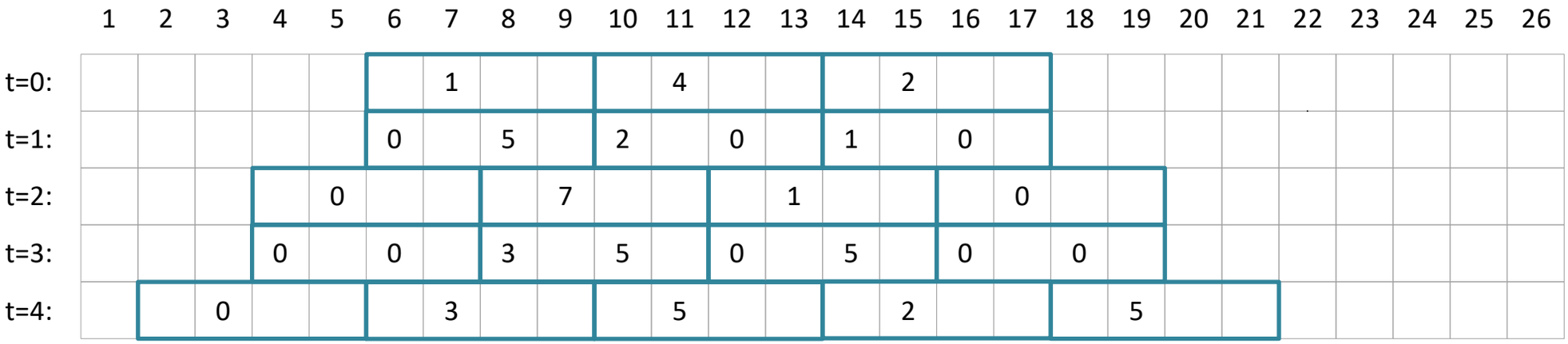

Block1
Block0
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
5
7
b

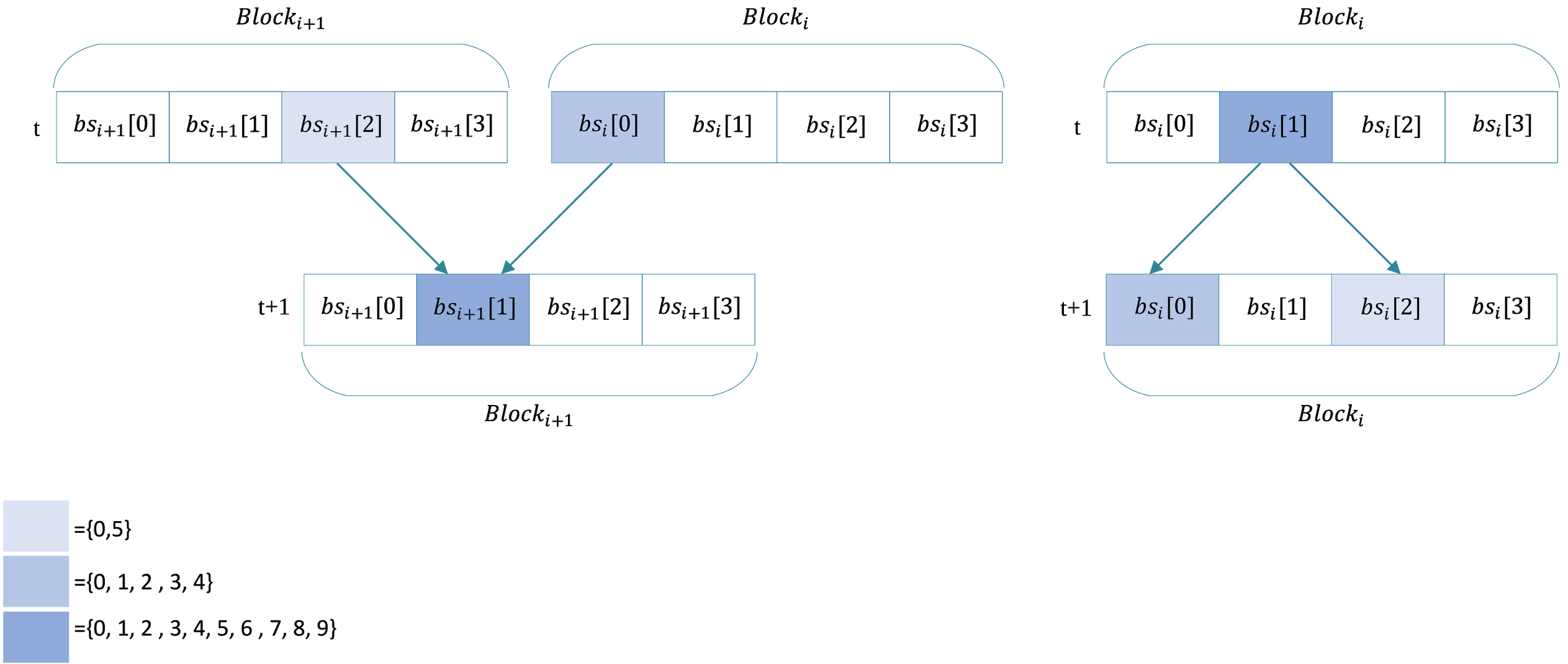
(b)

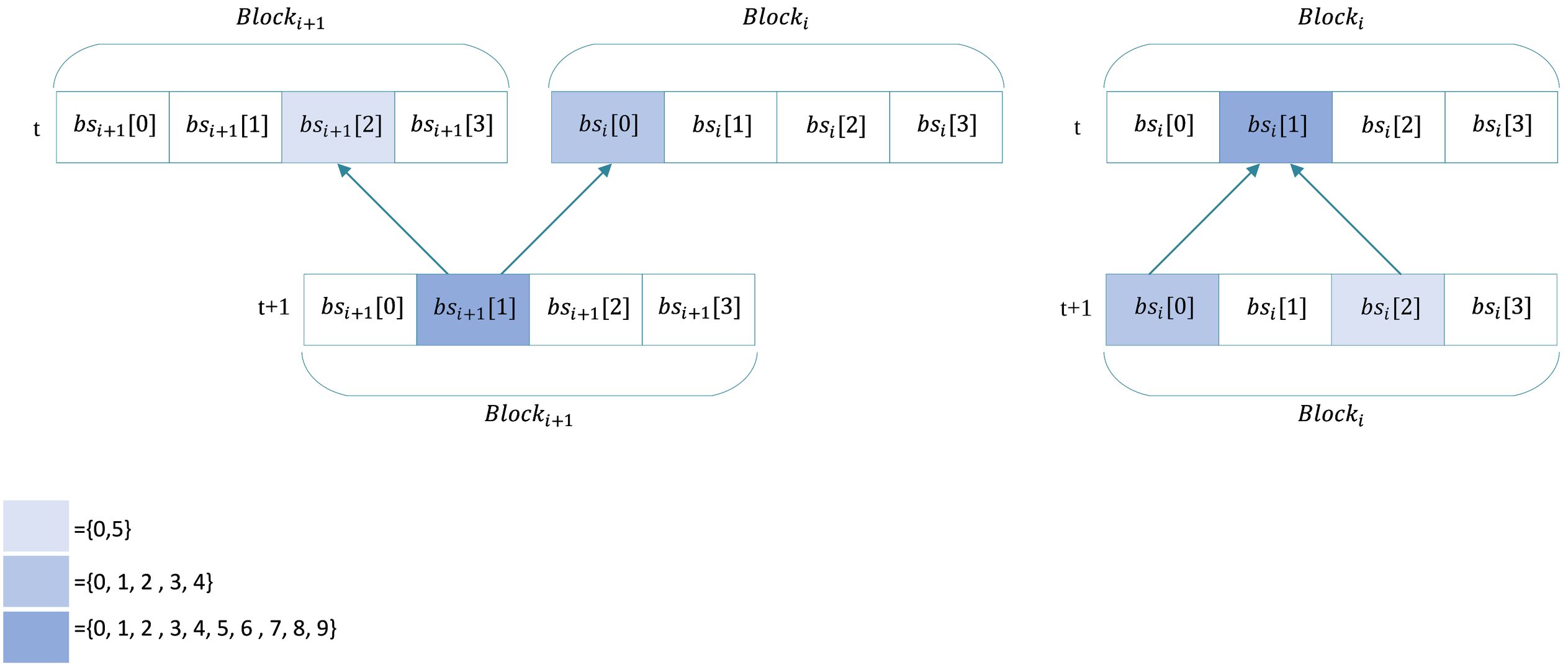

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
t=0:
t=1:
t=2:
t=3:
t=4:
t=5:
t=6:
t=7:
t=8:
new block with ID=2 added in this time step

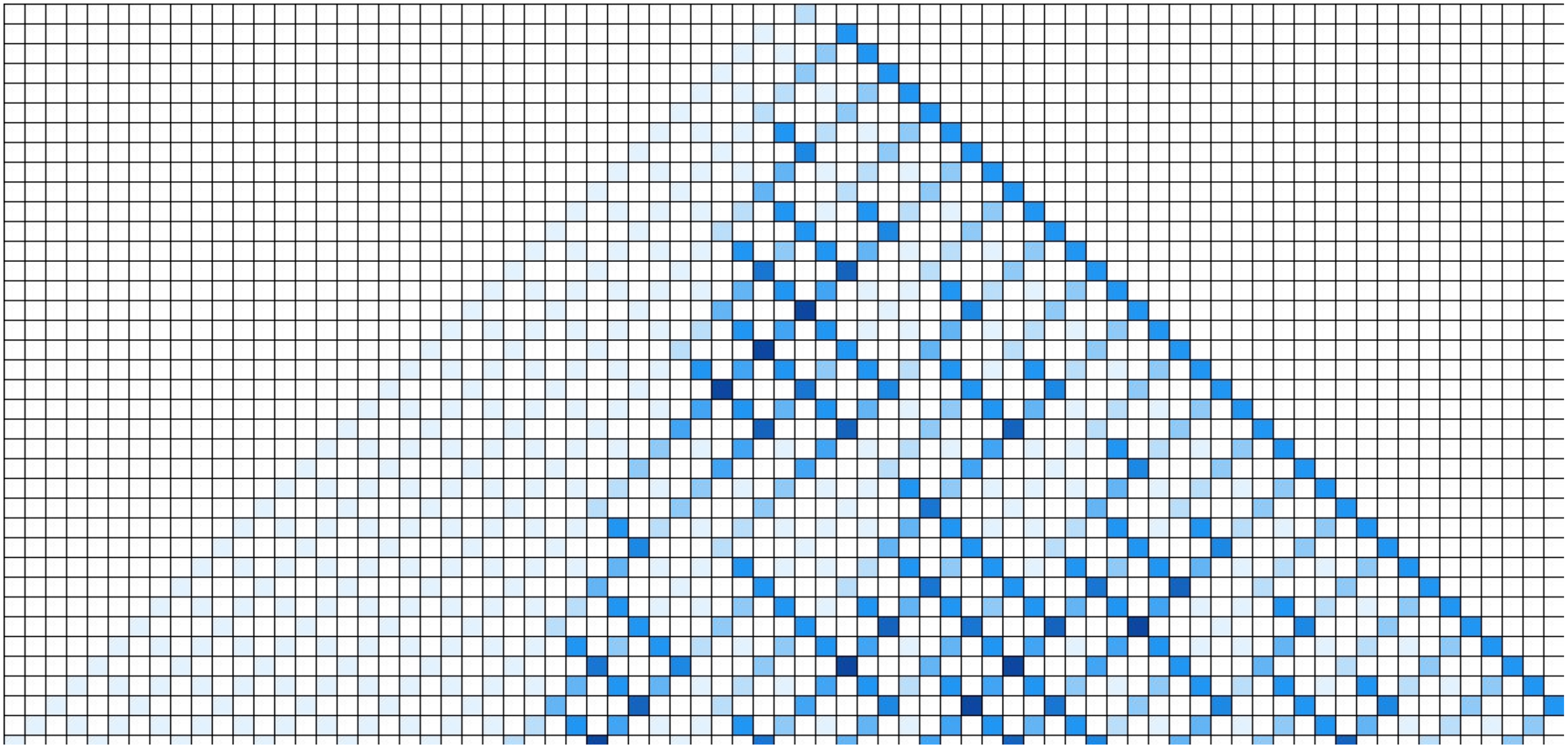

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
t=0: 5 7
t=1: 2 5 3 5
t=2: 2 8 5
t=3: 1 0 4 0 2 5
t=4: 1 4 2 5


1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
t=0: 8 5
t=1: 4 0 2 5
t=2: 4 2 5
t=3: 2 0 1 0 2 5
t=4: 1 1 2 5

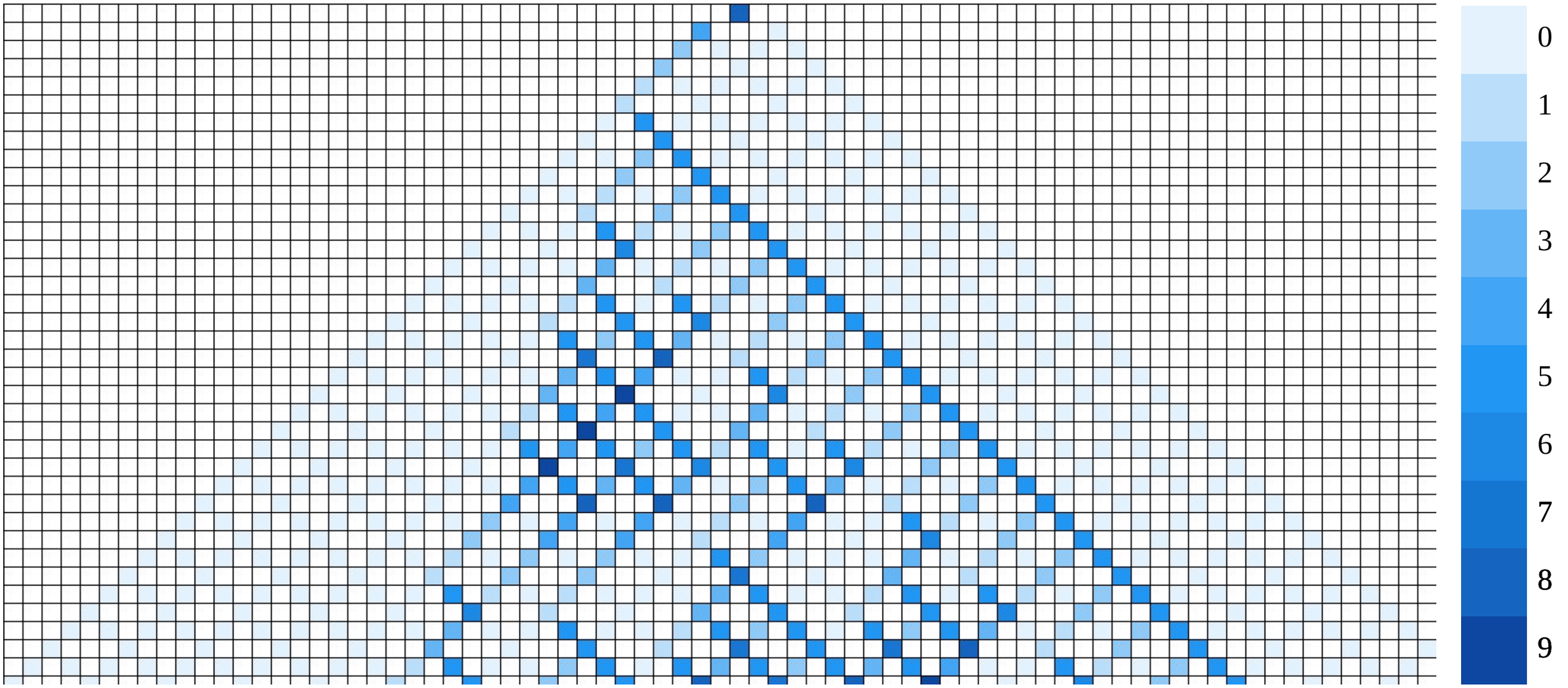

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26
t=0: 1 4 2
t=1: 0 5 2 0 1 0
t=2: 0 7 1 0
t=3: 0 0 3 5 0 5 0 0
t=4: 0 3 5 2 5


$Block_{i+1}$
$Block_i$
t
$bs_{i+1}[0]$
$bs_{i+1}[1]$
$bs_{i+1}[2]$
$bs_{i+1}[3]$
$bs_i[0]$
$bs_i[1]$
$bs_i[2]$
$bs_i[3]$
t+1
$bs_{i+1}[0]$
$bs_{i+1}[1]$
$bs_{i+1}[2]$
$bs_{i+1}[3]$
$Block_{i+1}$
$Block_i$
t
$bs_i[0]$
$bs_i[1]$
$bs_i[2]$
$bs_i[3]$
t+1
$bs_i[0]$
$bs_i[1]$
$bs_i[2]$
$bs_i[3]$
$Block_i$
={0,5}
={0, 1, 2 , 3, 4}
={0, 1, 2 , 3, 4, 5, 6 , 7, 8, 9}

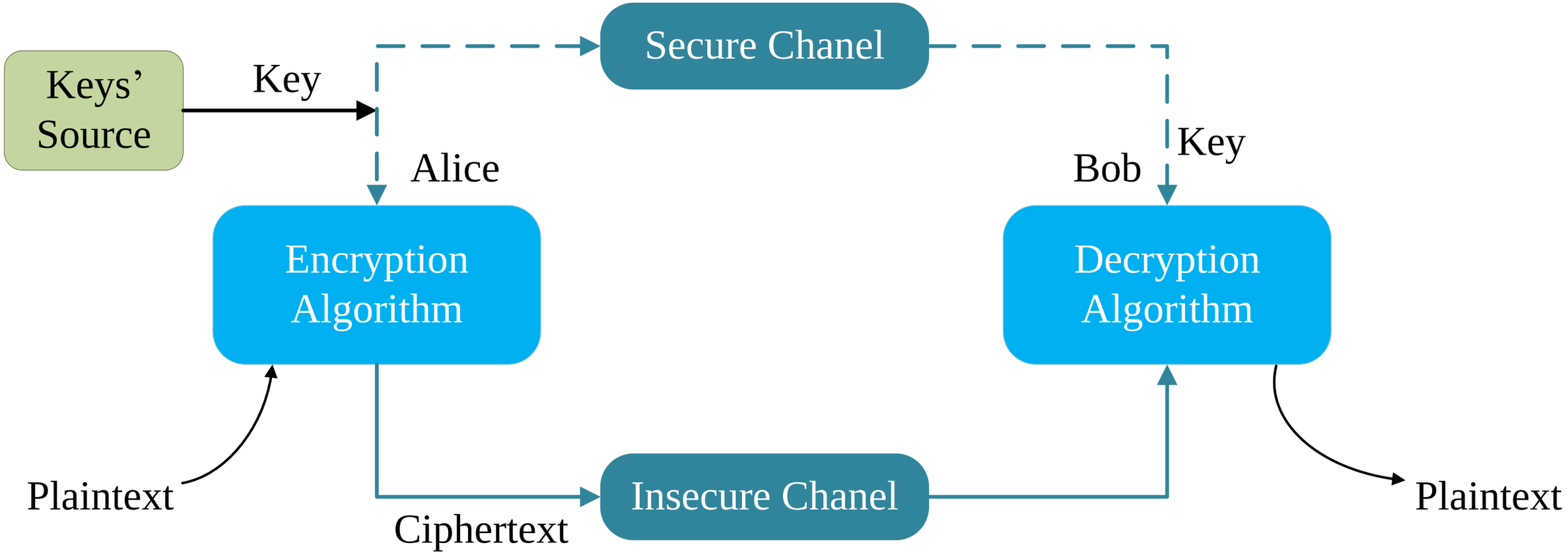

$Block_{i+1}$
$Block_i$
t
$bs_{i+1}[0]$
$bs_{i+1}[1]$
$bs_{i+1}[2]$
$bs_{i+1}[3]$
$bs_i[0]$
$bs_i[1]$
$bs_i[2]$
$bs_i[3]$
t+1
$bs_{i+1}[0]$
$bs_{i+1}[1]$
$bs_{i+1}[2]$
$bs_{i+1}[3]$
$Block_{i+1}$
$Block_i$
t
$bs_i[0]$
$bs_i[1]$
$bs_i[2]$
$bs_i[3]$
t+1
$bs_i[0]$
$bs_i[1]$
$bs_i[2]$
$bs_i[3]$
$Block_i$
={0,5}
={0, 1, 2 , 3, 4}
={0, 1, 2 , 3, 4, 5, 6 , 7, 8, 9}



(a)



(b)


Keys'
Source
Key
Secure Chanel
Alice
Bob
Key
Encryption
Algorithm
Decryption
Algorithm
Plaintext
Ciphertext
Insecure Chanel
Plaintext

Encryption Process

Decryption Process

Sender

Generate key2 as initial value and request Key1 from reciver

Key1

Reciver

Generate key1 as a primary key and sent it to the sender

Key1

Key2

Evolve D2CA(key1)

Evolve D2CA(key2)

Produce sub-keys using Algorithm 4

Sub-keys

Generate ciphertext c
ci=|(sub-keyi mod 255) – AsciiCode(pi)|

Plaintext p

Key2

ciphertext c

Key2

Evolve D2CA(key2)

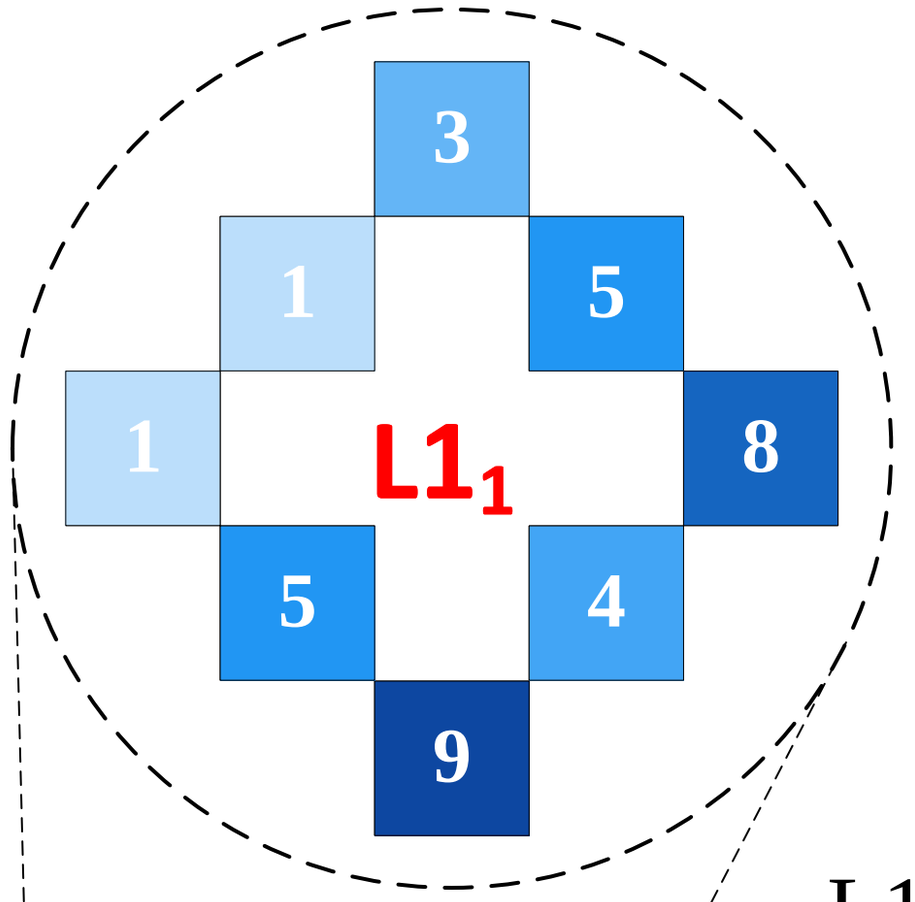
Evolve D2CA(key1)

Produce sub-keys using Algorithm 4

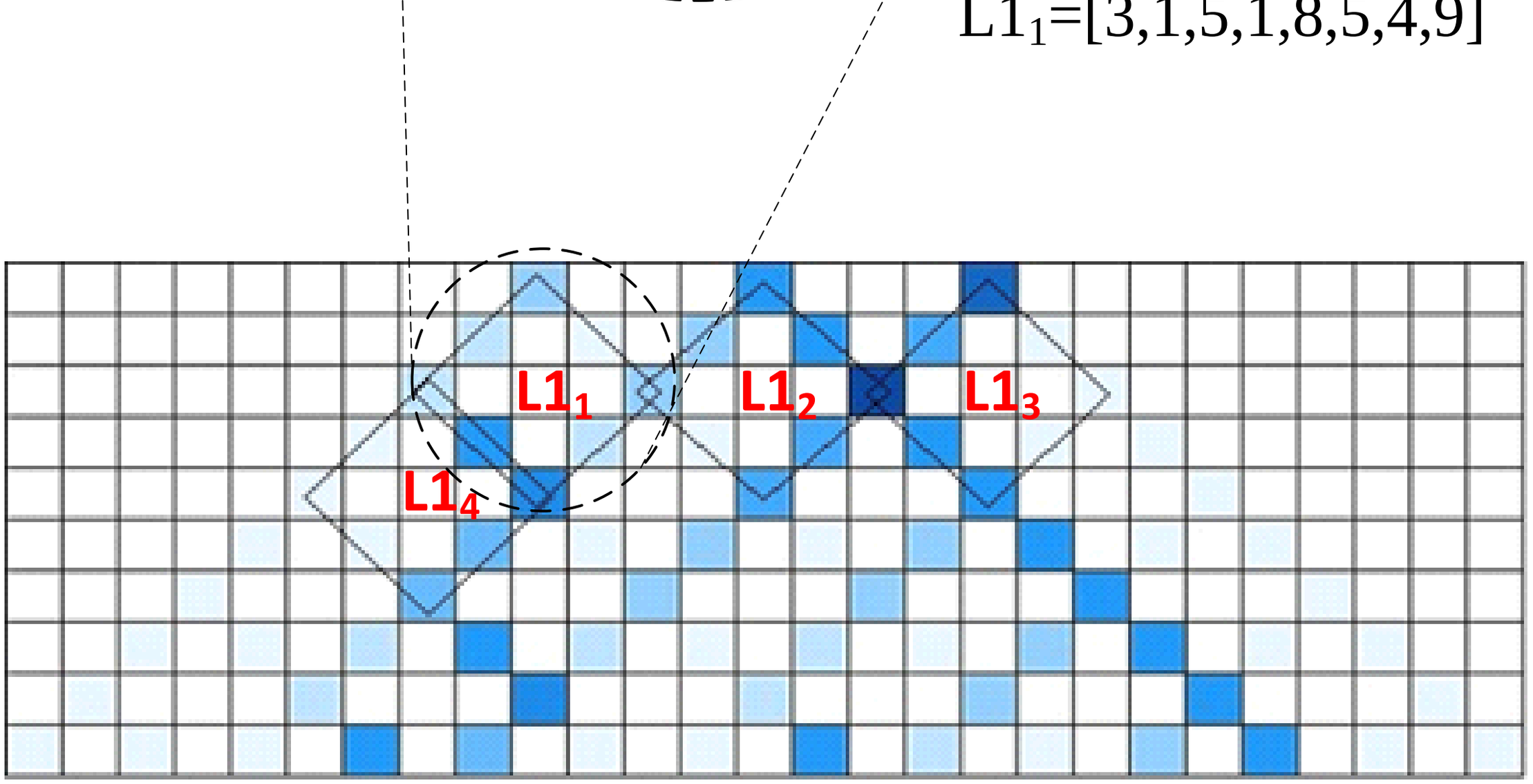
Sub-keys

Generate plaintext p
pi=char(|sub-keyi – ci|)

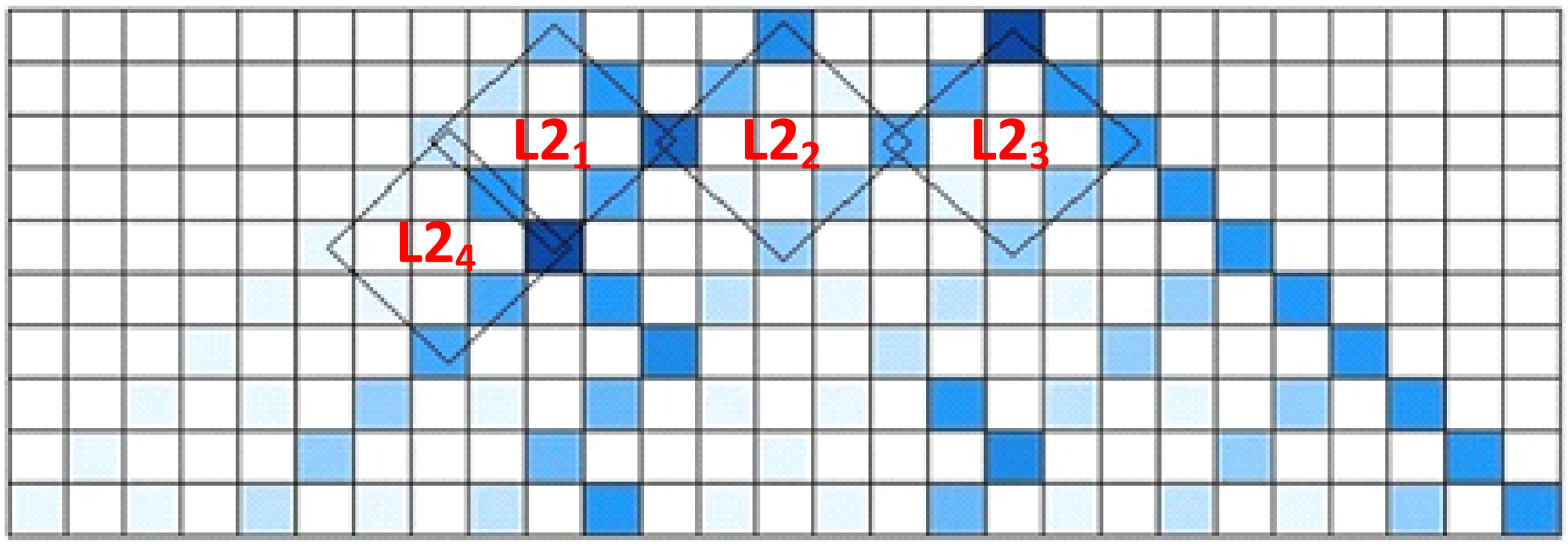
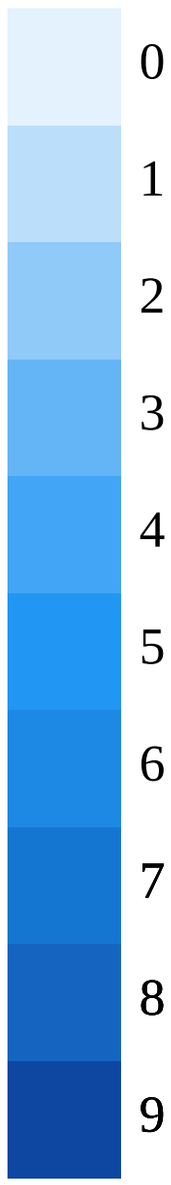
p



$L1_1=[3,1,5,1,8,5,4,9]$



a)



b)