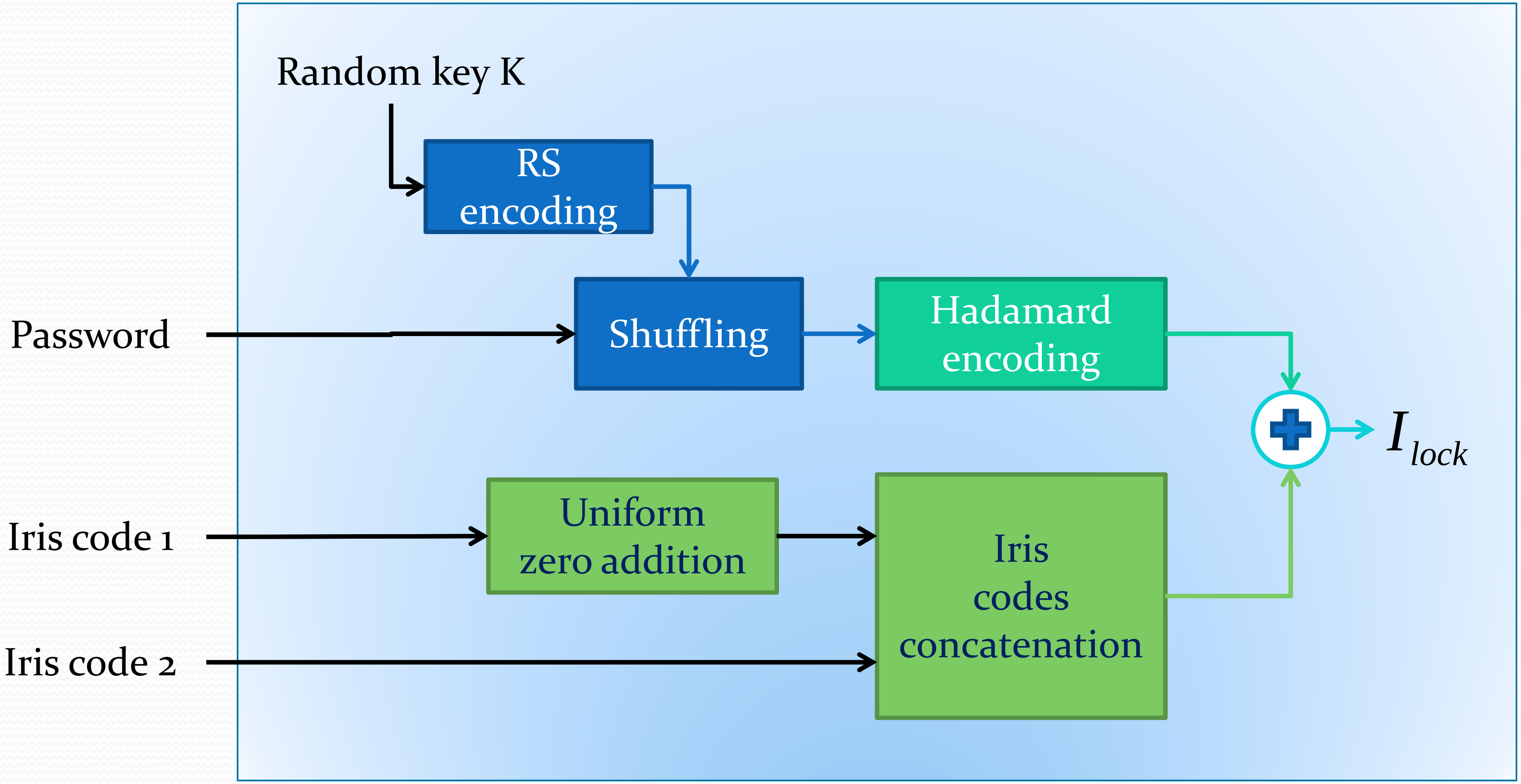
제목 : Cancelable biometric scheme에서 사용된 shuffle 함수의 안전성 분석

저자 : 박정열, 김재희, 송홍엽

소속 : 연세대학교

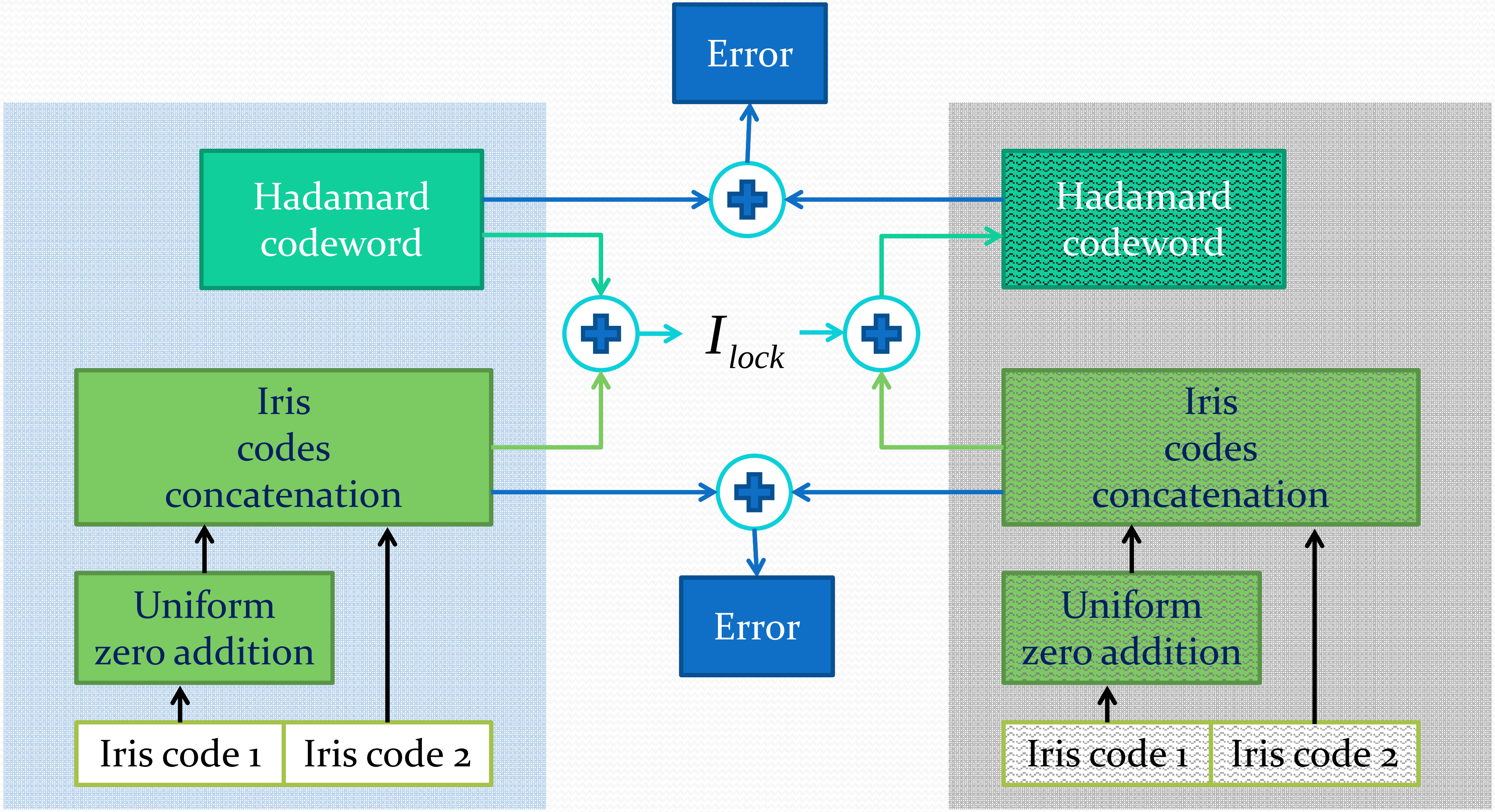
Overview of the Kanade et al.'s scheme:

User enrollment module & Key generation module (backward)

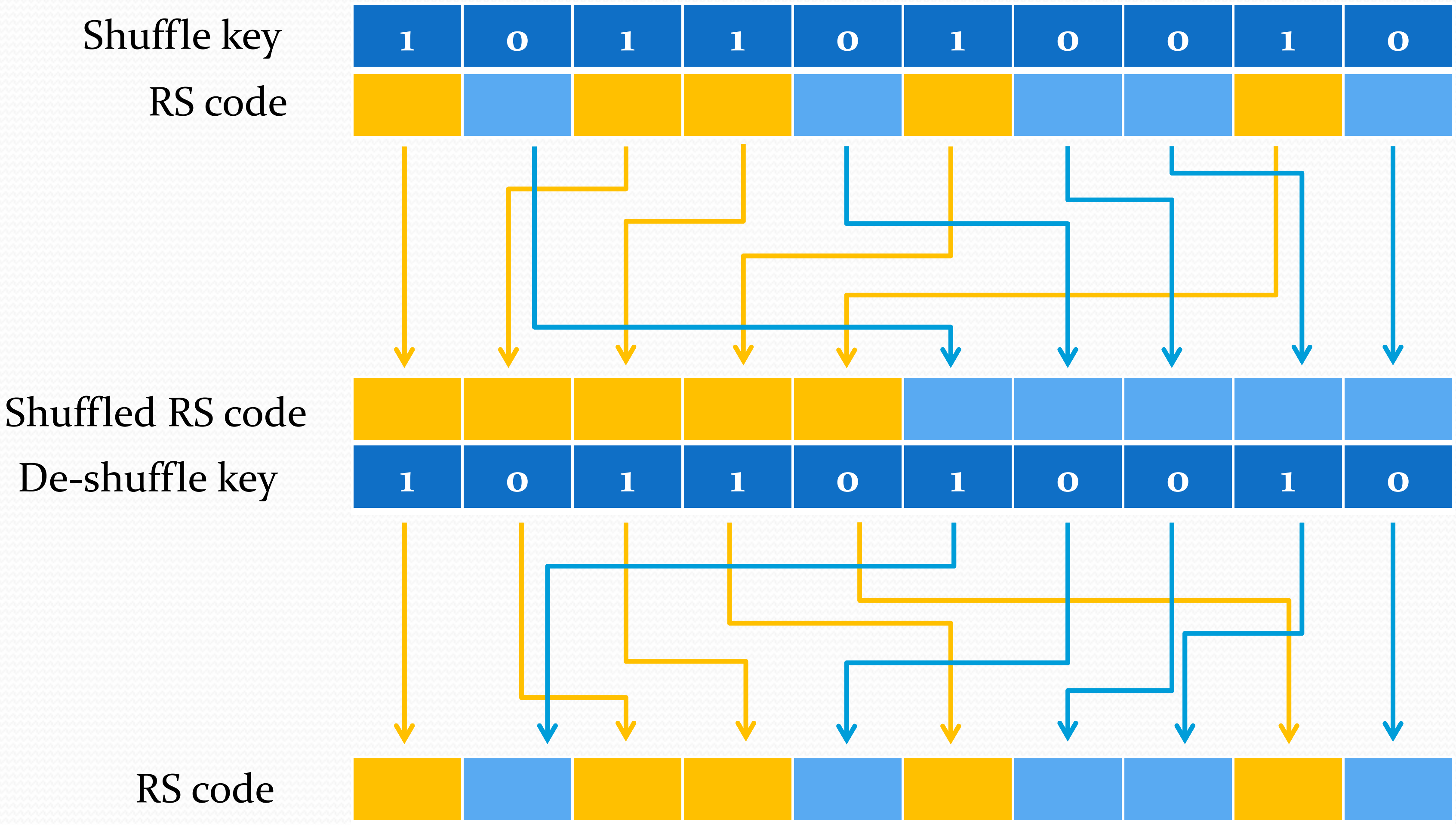


Overview of the Kanade et al.'s scheme:

Overall structure



Shuffling & De-shuffling



Shuffle key

1	0	1	1	0	1	0	0	1	0

RS code

Shuffled RS code

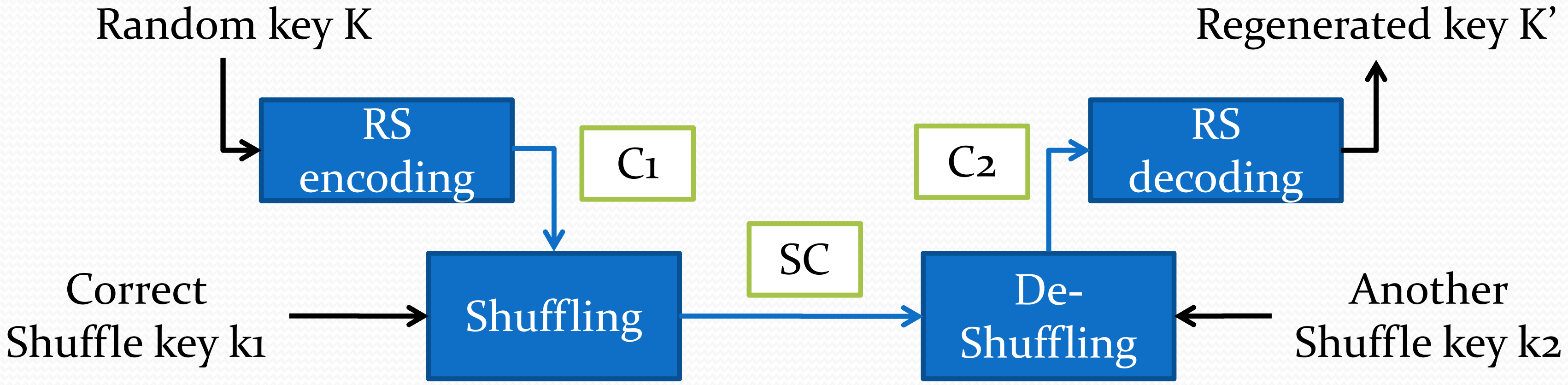
De-shuffle key

1	0	1	1	0	1	0	0	1	0

RS code

Weakness of shuffling

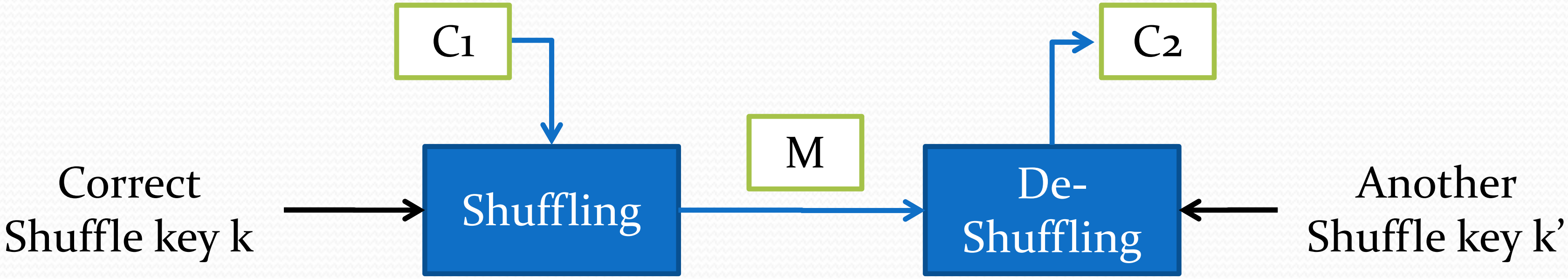
- Assume that there is no error in biometric data



- Can C2 be decoded to K?
  - Yes, since some bits of C2 are allowed to be different from those of C1

Similar keys

- Suppose that C[n,k,d] code is used & there is no error in biometric data
- A key k' is t-similar to k if d(C1, C2) <= t, where t is the error capacity of C[n,k,d]
- Actually k' has no difference from k



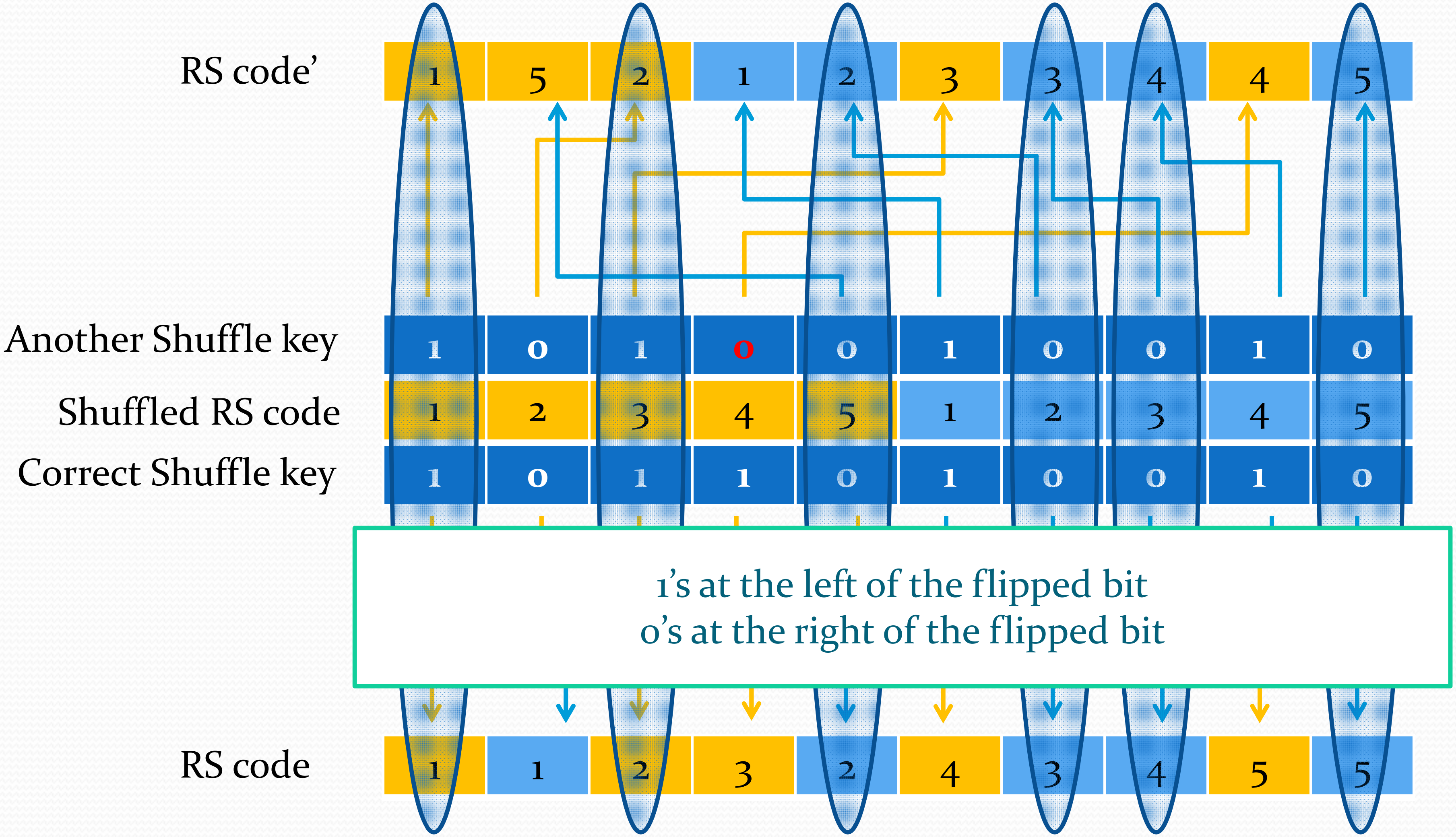
How many similar keys?

- There should be no similar key
  (it’s a security flaw!)

- Unfortunately there are many of them…

- How to count their number?
  - Observation – changing some bits of the key
  - Counting

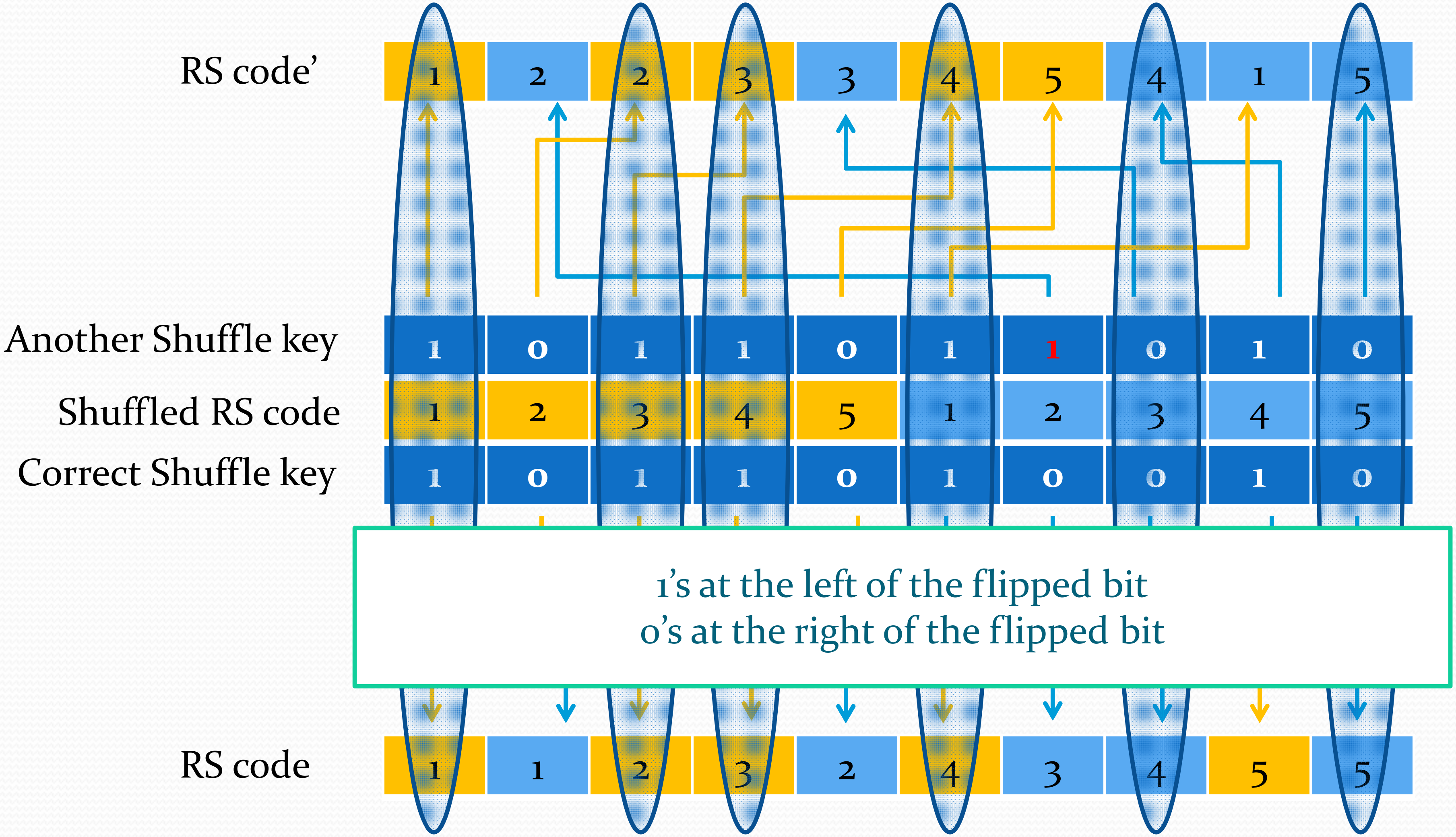
Flipping a bit : 1 to 0



RS code’	1	5	2	1	2	3	3	4	4	5
Another Shuffle key	1	0	1	0	0	1	0	0	1	0
Shuffled RS code	1	2	3	4	5	1	2	3	4	5
Correct Shuffle key	1	0	1	1	0	1	0	0	1	0
RS code	1	1	2	3	2	4	3	4	5	5

1’s at the left of the flipped bit
0’s at the right of the flipped bit

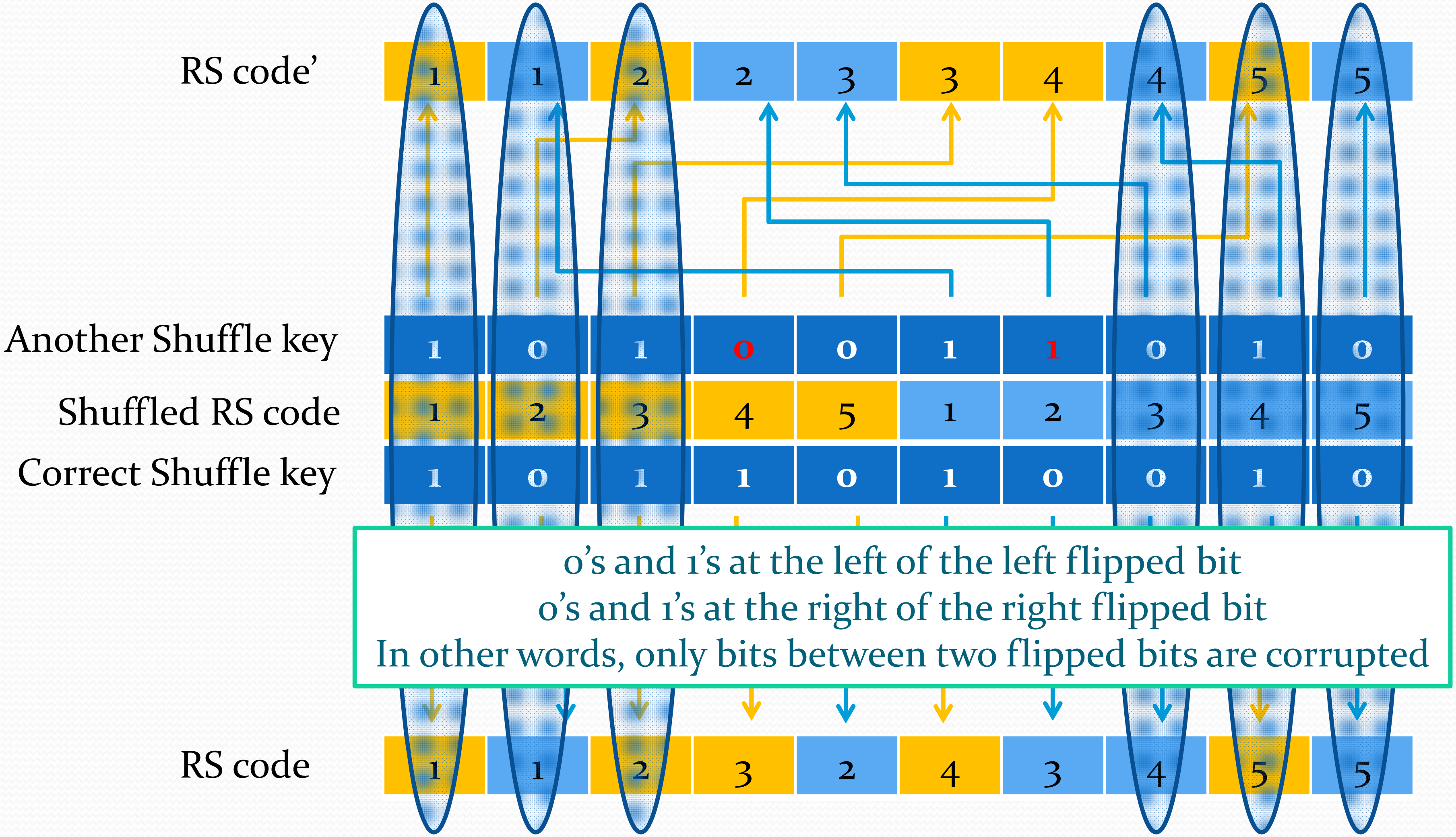
Flipping a bit : 0 to 1



RS code’	1	2	2	3	3	4	5	4	1	5
Another Shuffle key	1	0	1	1	0	1	1	0	1	0
Shuffled RS code	1	2	3	4	5	1	2	3	4	5
Correct Shuffle key	1	0	1	1	0	1	0	0	1	0
RS code	1	1	2	3	2	4	3	4	5	5

1’s at the left of the flipped bit
0’s at the right of the flipped bit

Flipping two bits : 1 to 0, 0 to 1



RS code’	1	1	2	2	3	3	4	4	5	5
Another Shuffle key	1	0	1	0	0	1	1	0	1	0
Shuffled RS code	1	2	3	4	5	1	2	3	4	5
Correct Shuffle key	1	0	1	1	0	1	0	0	1	0
RS code	1	1	2	3	2	4	3	4	5	5

0’s and 1’s at the left of the left flipped bit
0’s and 1’s at the right of the right flipped bit
In other words, only bits between two flipped bits are corrupted

Flipping one bit or two bits…

- Only limited number of blocks of the code are affected!

- We can limit the number of distinct blocks (error blocks) by flipping bits carefully
  - Flipping two consecutive bits complementarily
  - Flipping the rightmost 1 to 0
  - Flipping the leftmost 0 to 1

Example

1	0	1	1	0	1	1	1	1	0
1	0	1	0	1	1	1	1	1	0
1	1	0	0	1	1	1	1	1	0
1	1	0	0	1	1	1	1	0	1
1	1	0	0	1	1	1	0	0	1
1	1	0	0	1	1	1	0	0	1
1	1	0	0	1	1	0	0	0	1
1	1	0	0	1	0	0	0	0	1
0	1	0	0	1	0	0	0	0	1

Conclusion

- If (n, k, d) codes are applied in the scheme…
  - Error capacity = ${}^{d-1}/_{2}$
  - # of similar keys = $2^{{}^{d-1}/_{4}}$
  - Thus if one uses an l-bit key,
    then it is indeed a $\left(l - \frac{d-1}{4}\right)$-bit key

- Security is reduced greatly!