

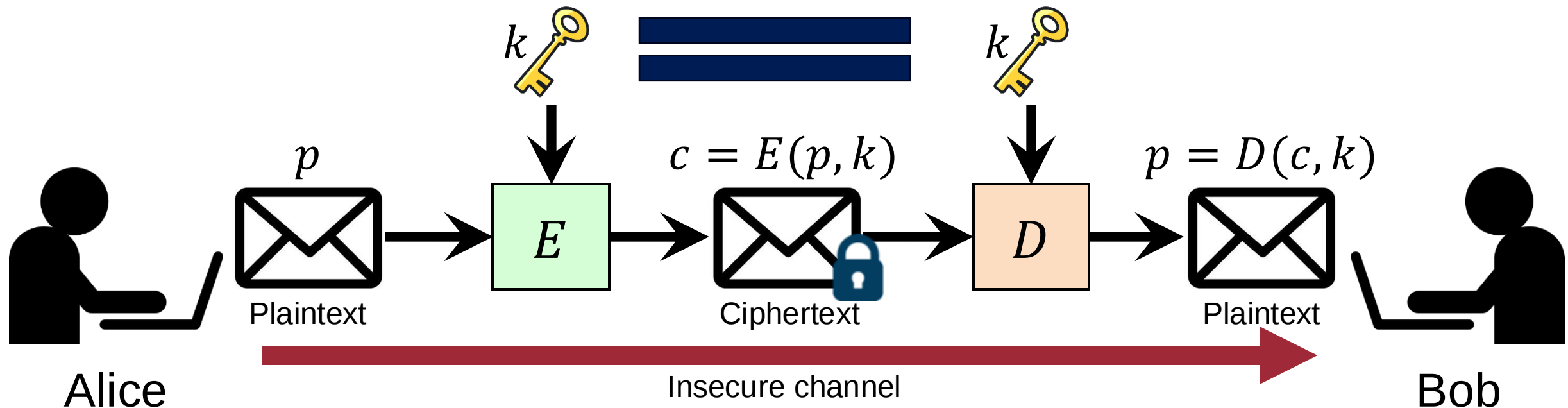
CSE467: Computer Security

5. Symmetric-key Encryption (2)

Seongil Wi

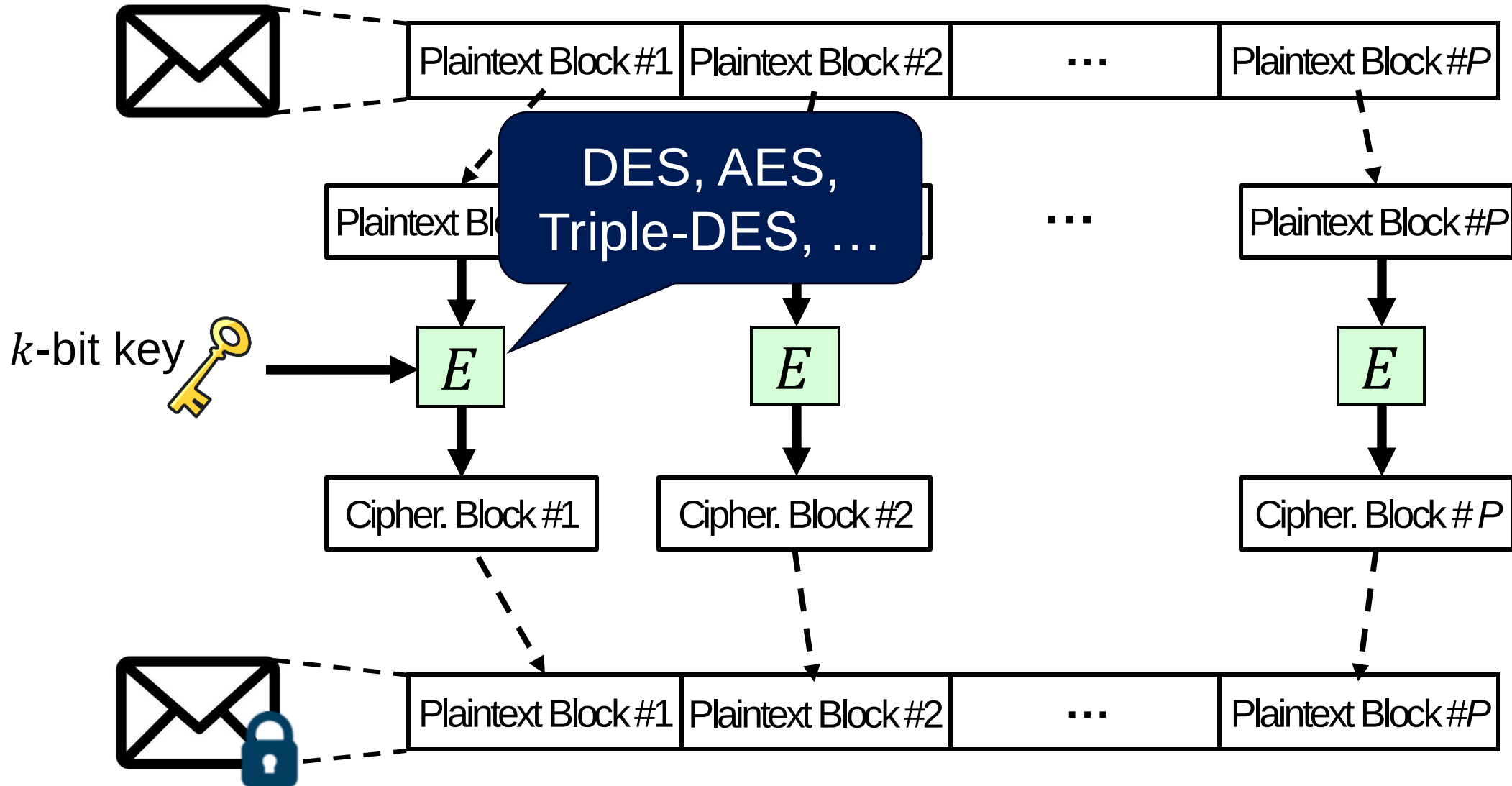
Recap: Symmetric-key Encryption

- **Symmetric:** the encryption and decryption keys *are the same*



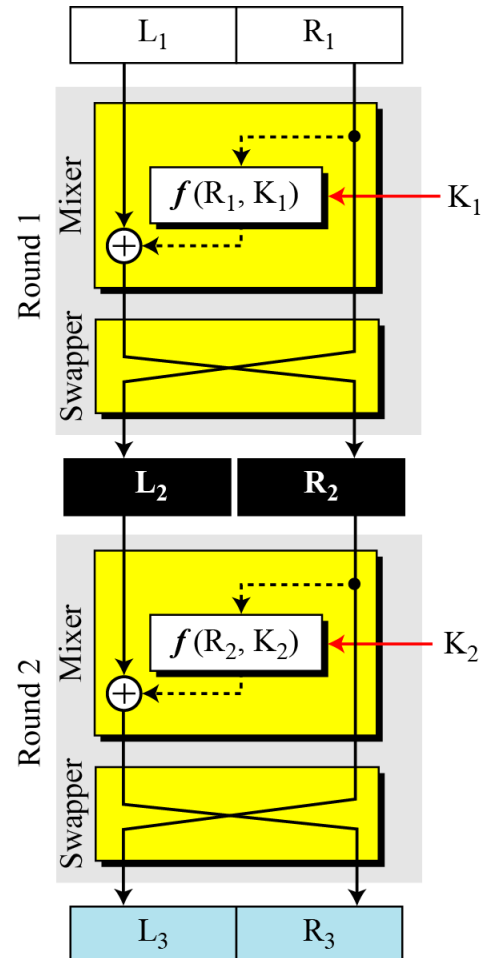
Recap: Block Cipher

3

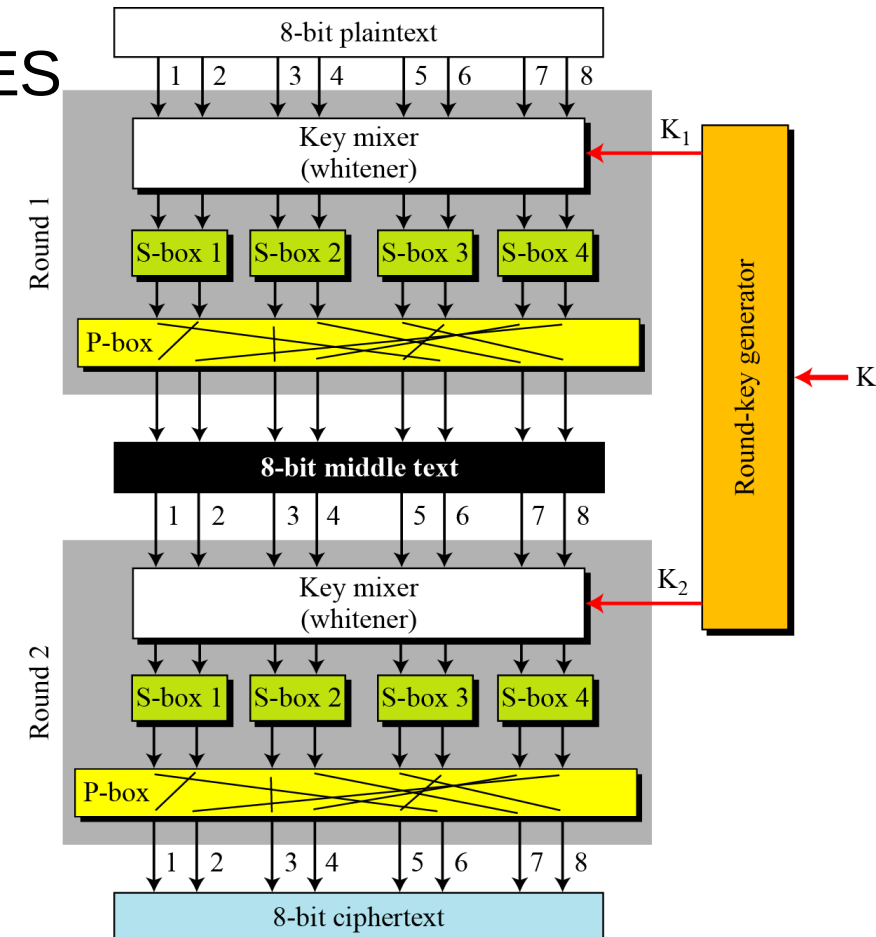


Recap: Two Classes of Block Ciphers

- Feistel ciphers
 - E.g., DES

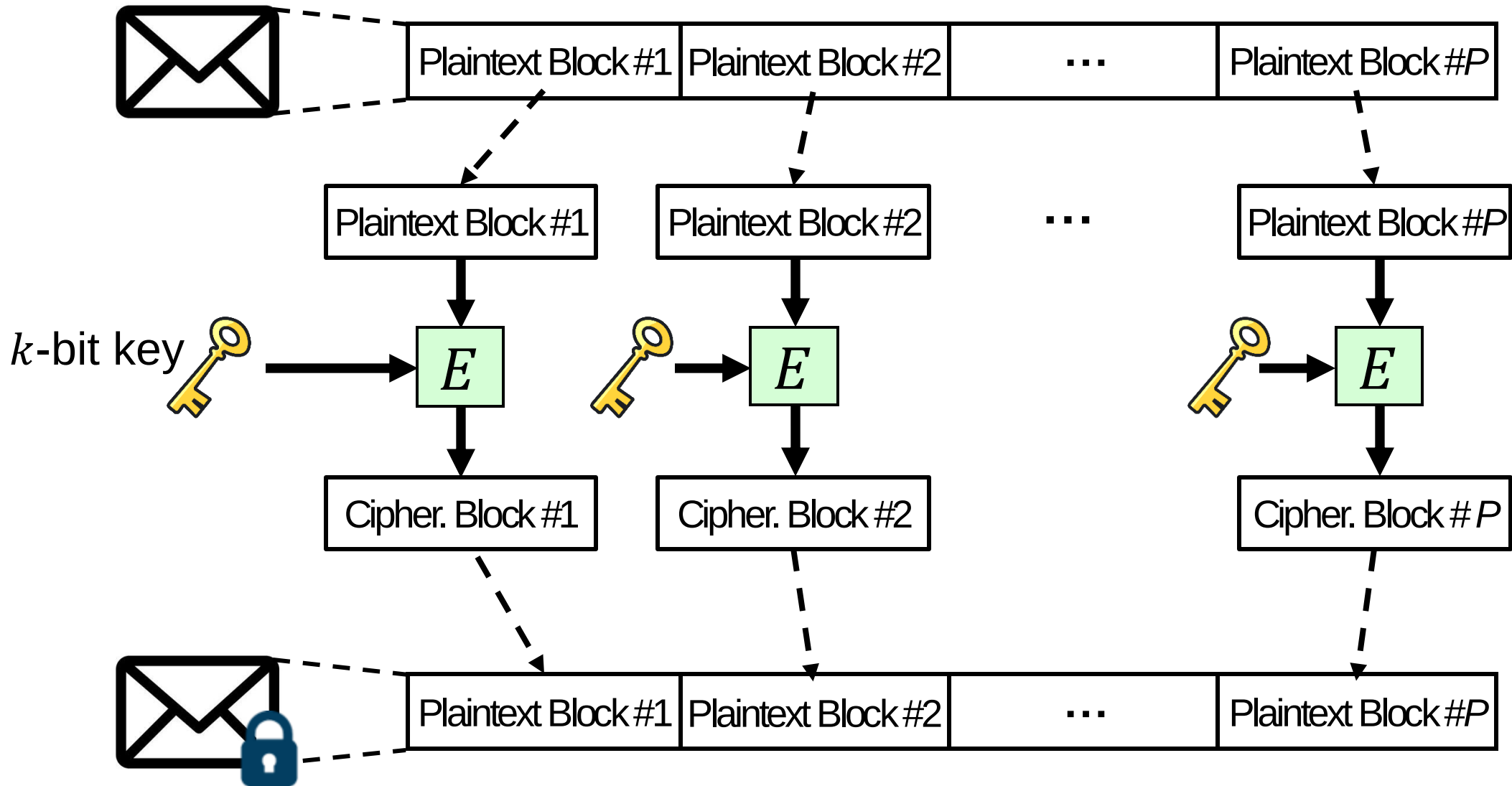


- Substitution-permutation (SP) ciphers
 - E.g., AES

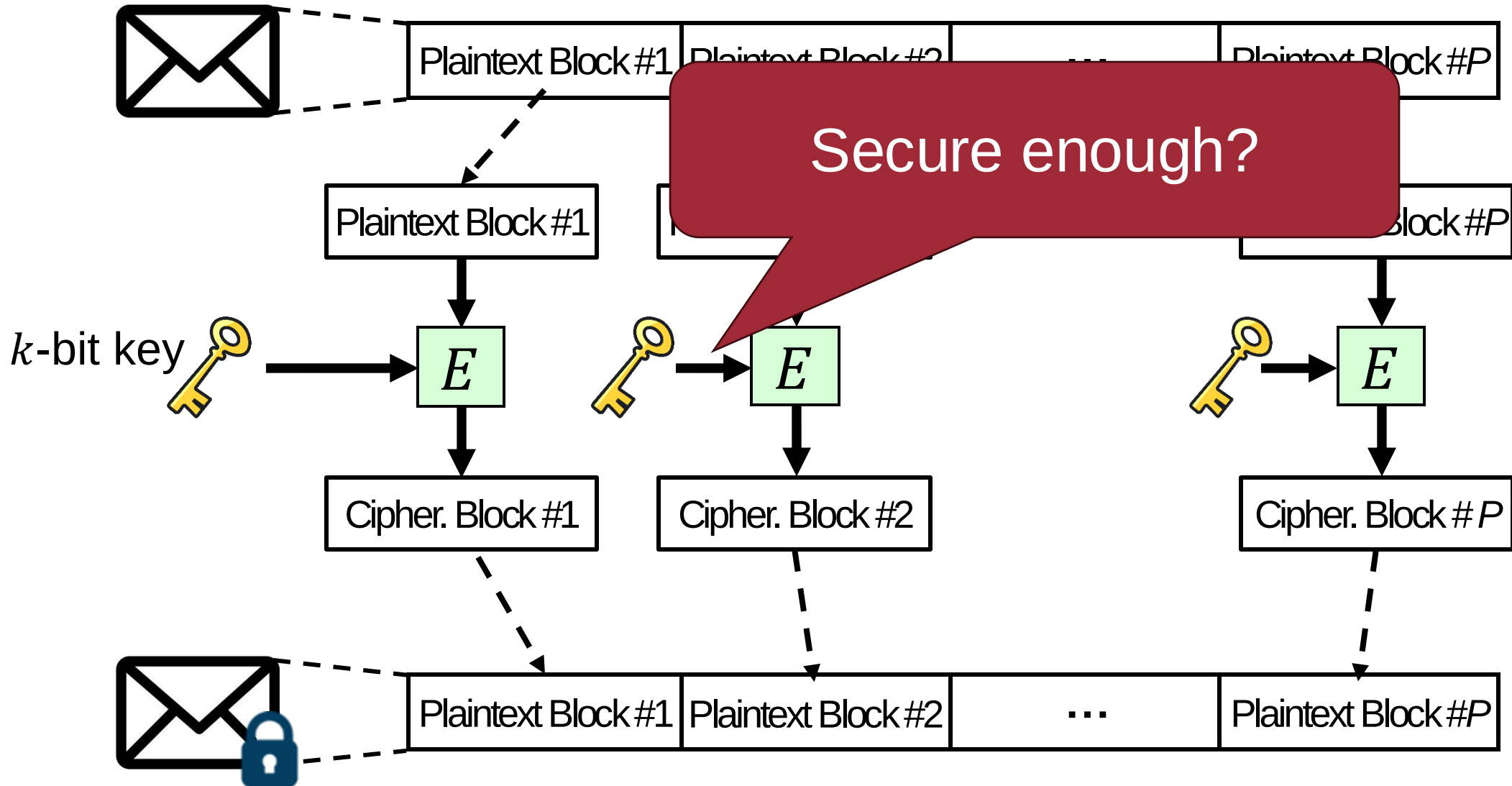


Practical Use of Block Cipher

5



Practical Use of Block Cipher

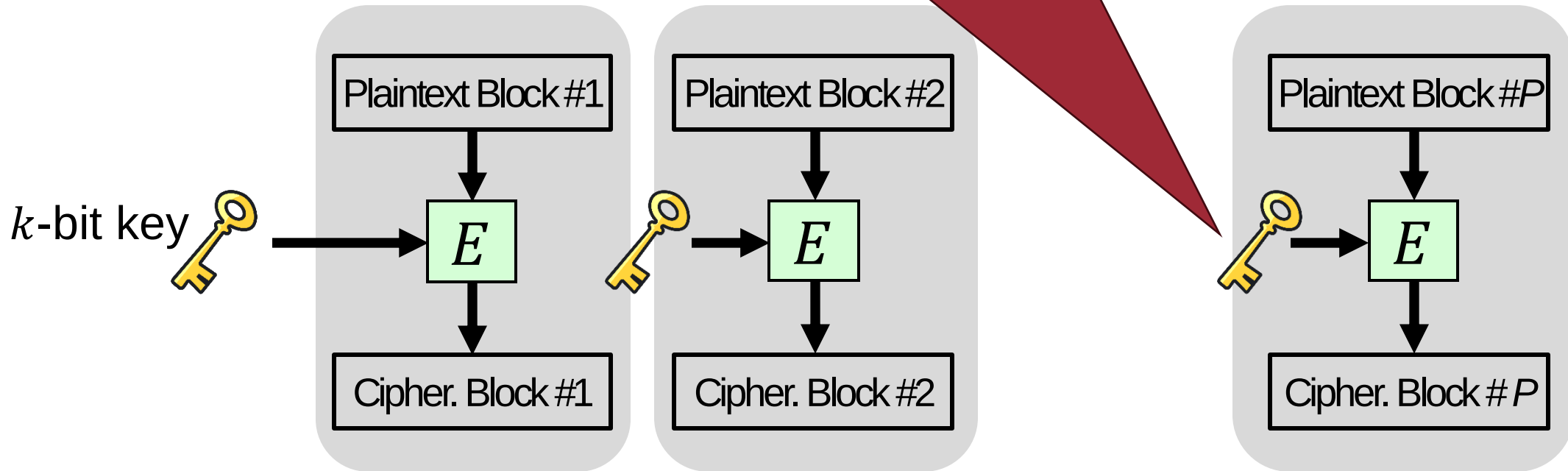


Problems for ECB mode

7



Use the **same key**
for multiple blocks

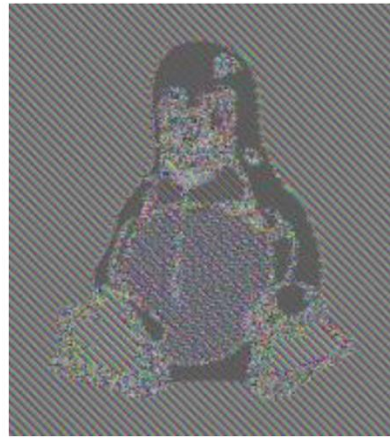


Problems for the Example

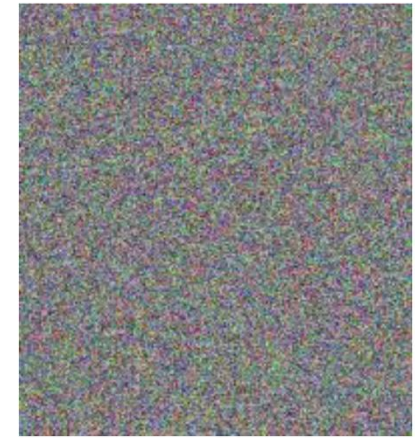
- Identical plaintext blocks $\rightarrow$ identical ciphertext blocks



Plaintext



**Ciphertext of
the Naive block cipher**



**Ciphertext
we want!**

How to generate different ciphertexts
for the same plaintext?

Modes of Operation

Block Cipher Modes of Operation

- Determine **how to repeatedly apply a single-block operation** to a sequence of blocks
- Different modes of operations
 - ECB: Electronic Code Book (The naïve one we've just discussed)
 - CBC: Cipher Block Chaining
 - CFB: Cipher FeedBack
 - OFB: Output FeedBack
 - CTR: CounTeR mode

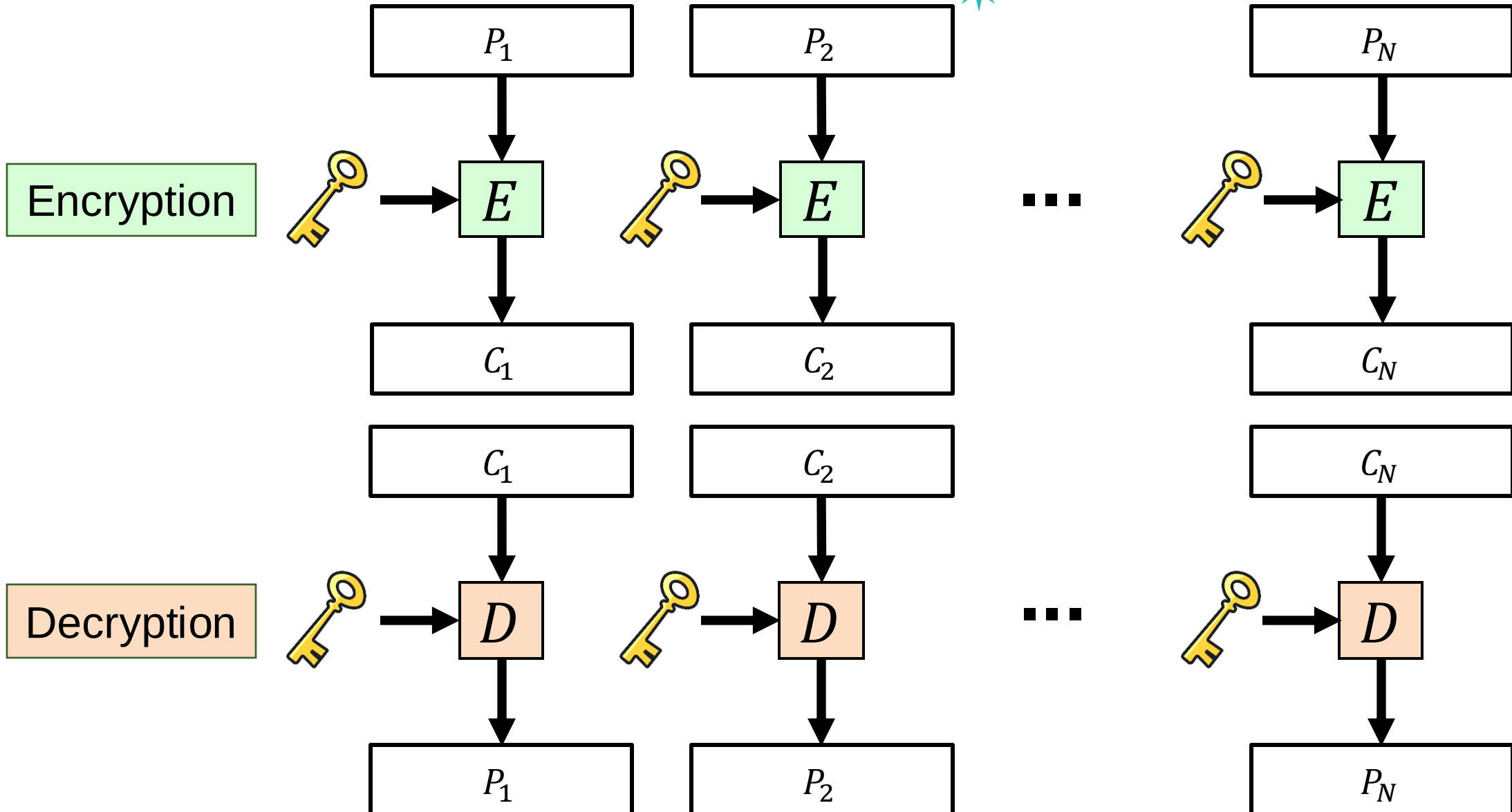
Shell Command

```
$ openssl enc -aes-128-cfb -e -in plain.bin -out cipher.bin -K
```

Block cipher mode

ECB: Electronic Code Book

11

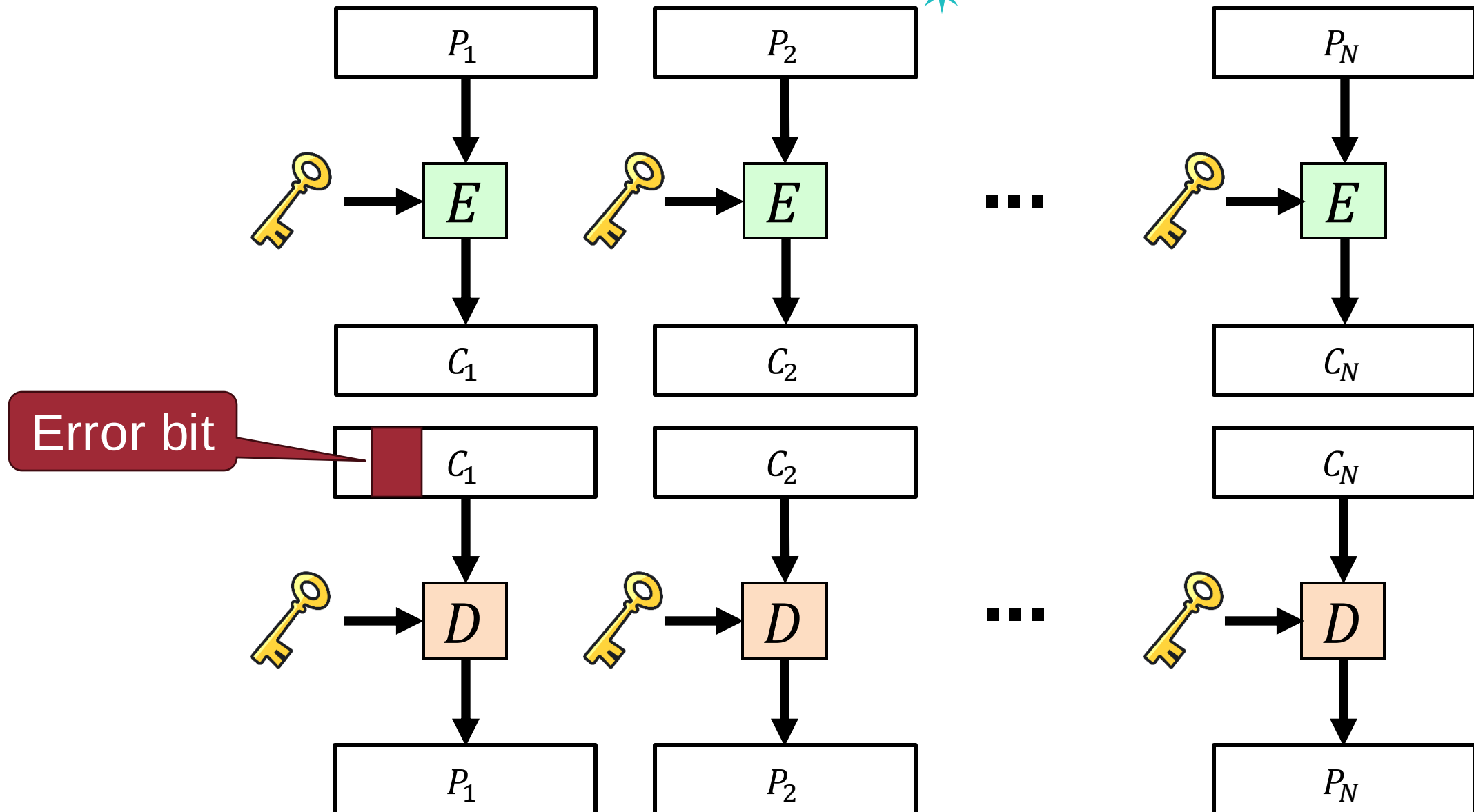


ECB: Electronic Code Book

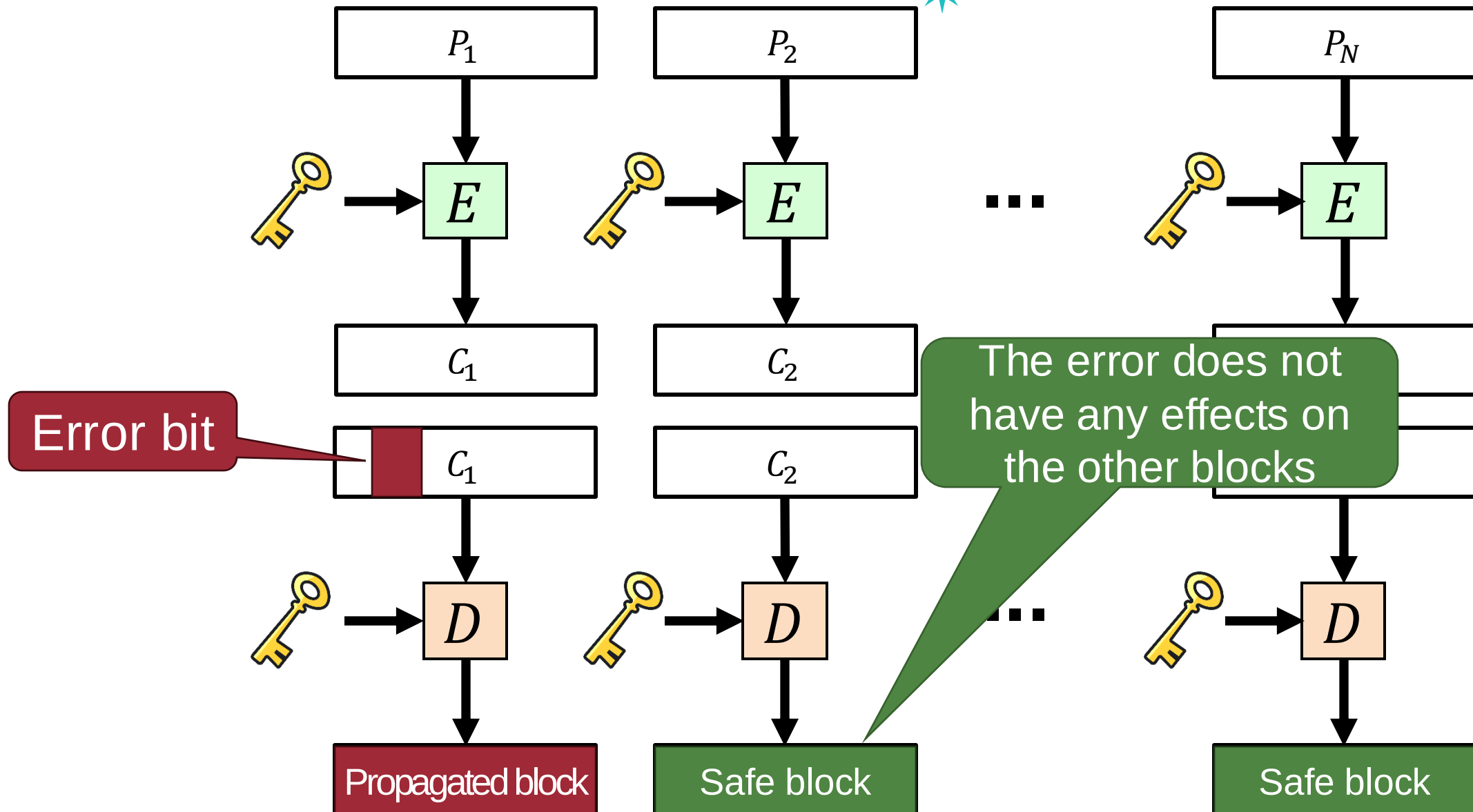


- Each block is encoded independently of the other blocks
- Advantages
 - Simple and efficient (i.e., parallelizable) to compute
 - The error does not have any effects on the other blocks

Error Propagation in ECB



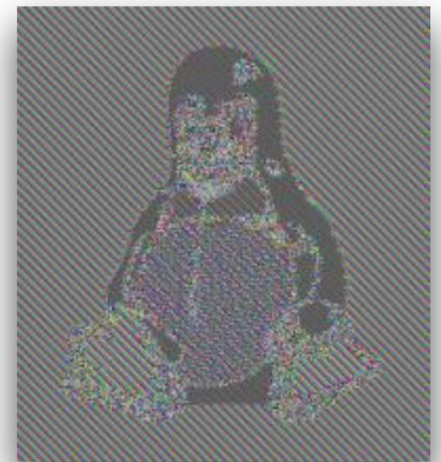
Error Propagation in ECB



ECB: Electronic Code Book

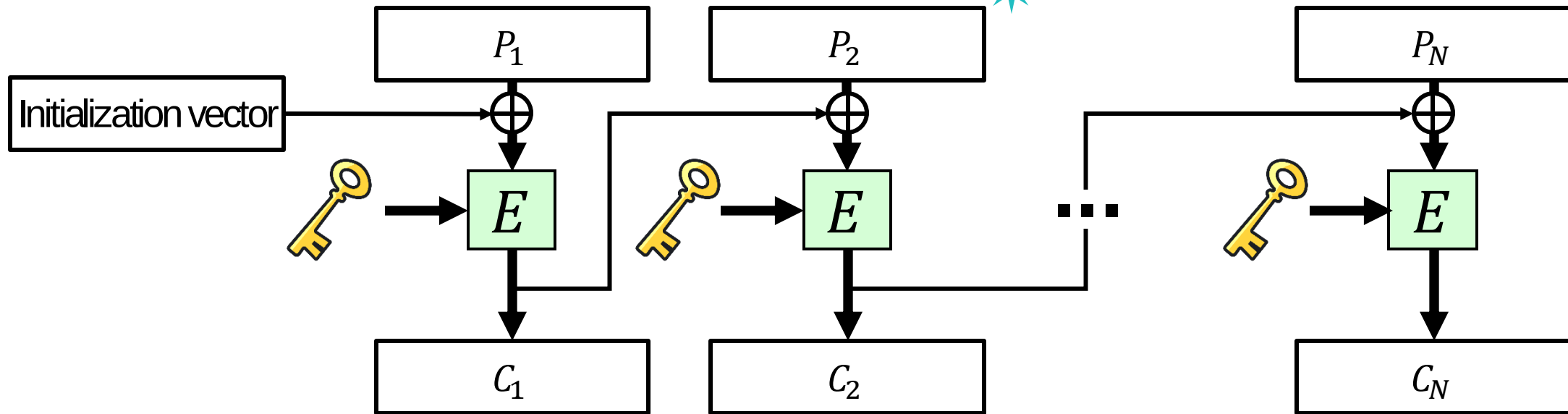


- Each block is encoded independently of the other blocks
- Advantages
 - Simple and efficient (i.e., parallelizable) to compute
 - The error does not have any effects on the other blocks
- Disadvantages
 - Same plaintext always corresponds to same ciphertext

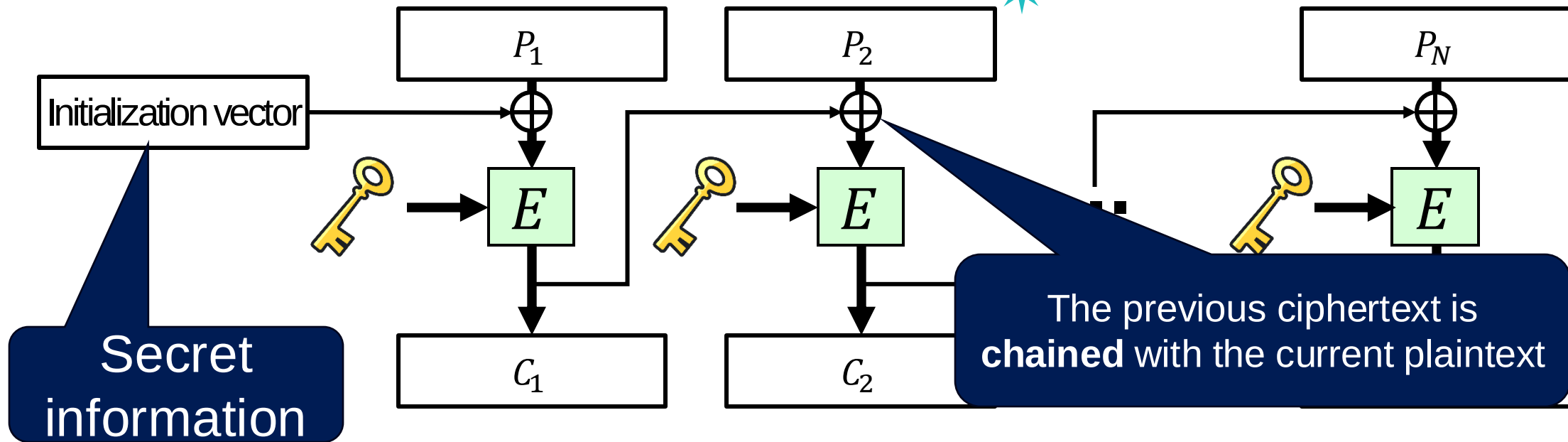


CBC: Cipher Block Chaining

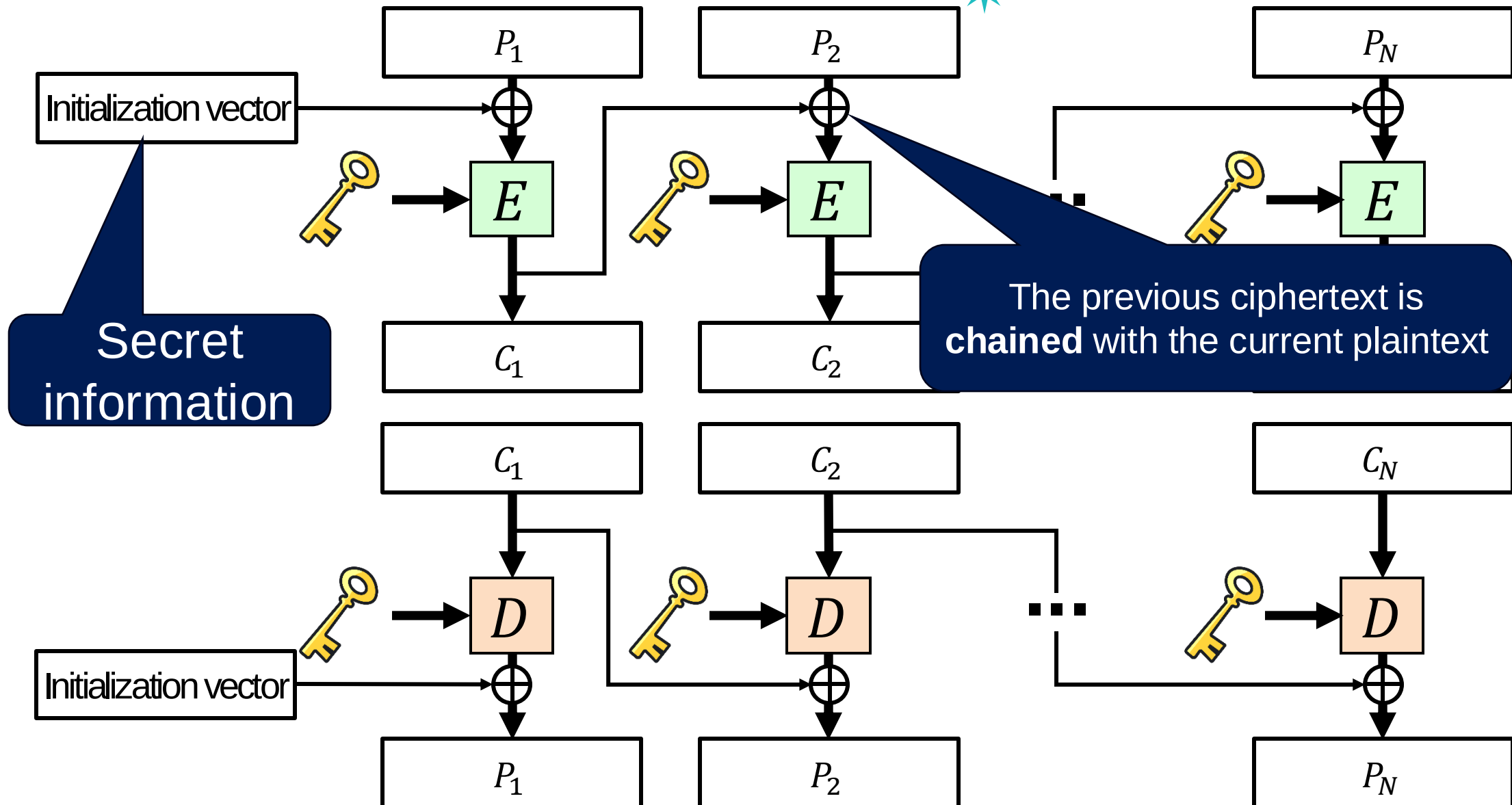
16



CBC: Cipher Block Chaining



CBC: Cipher Block Chaining

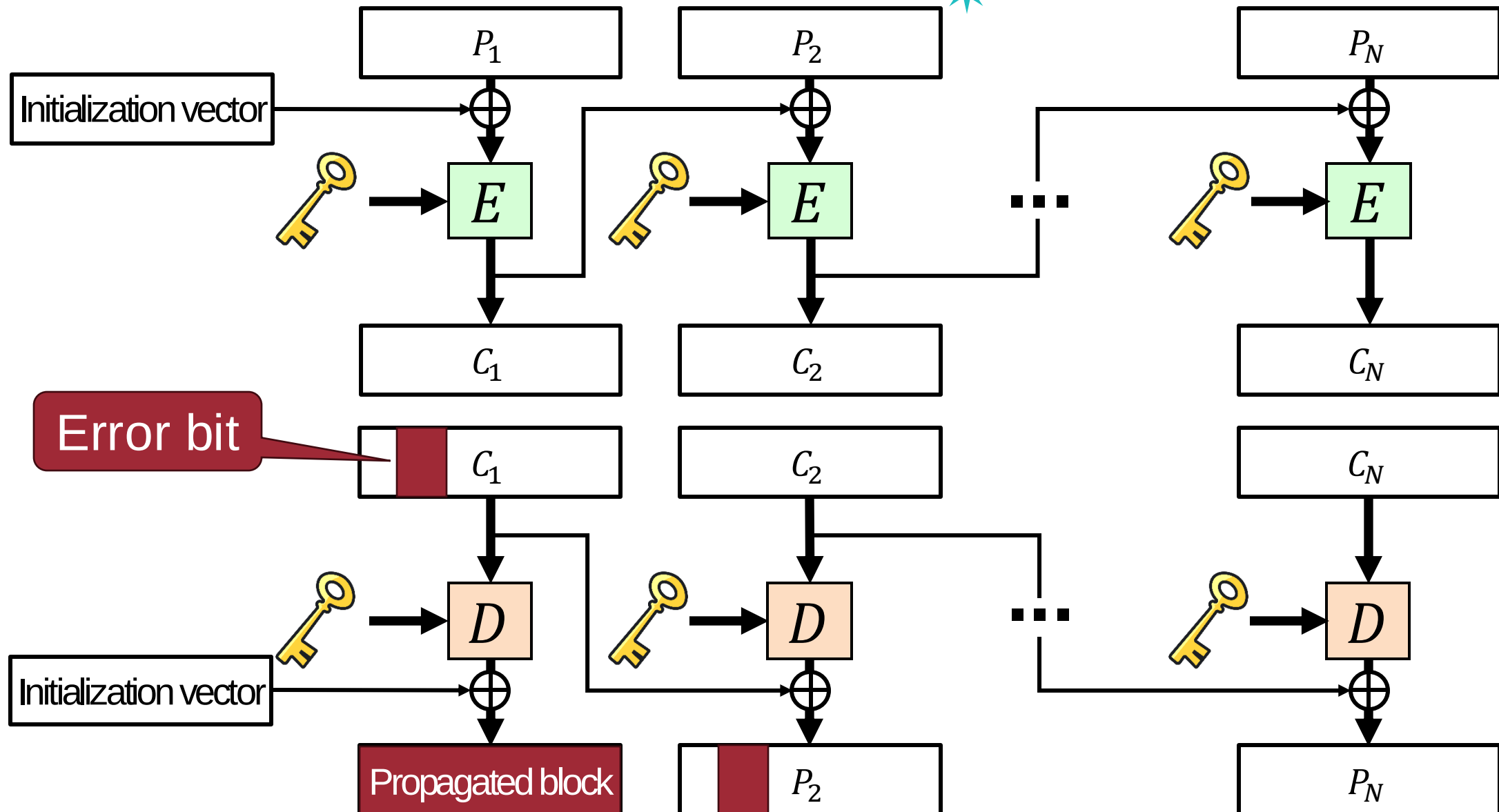


CBC: Cipher Block Chaining

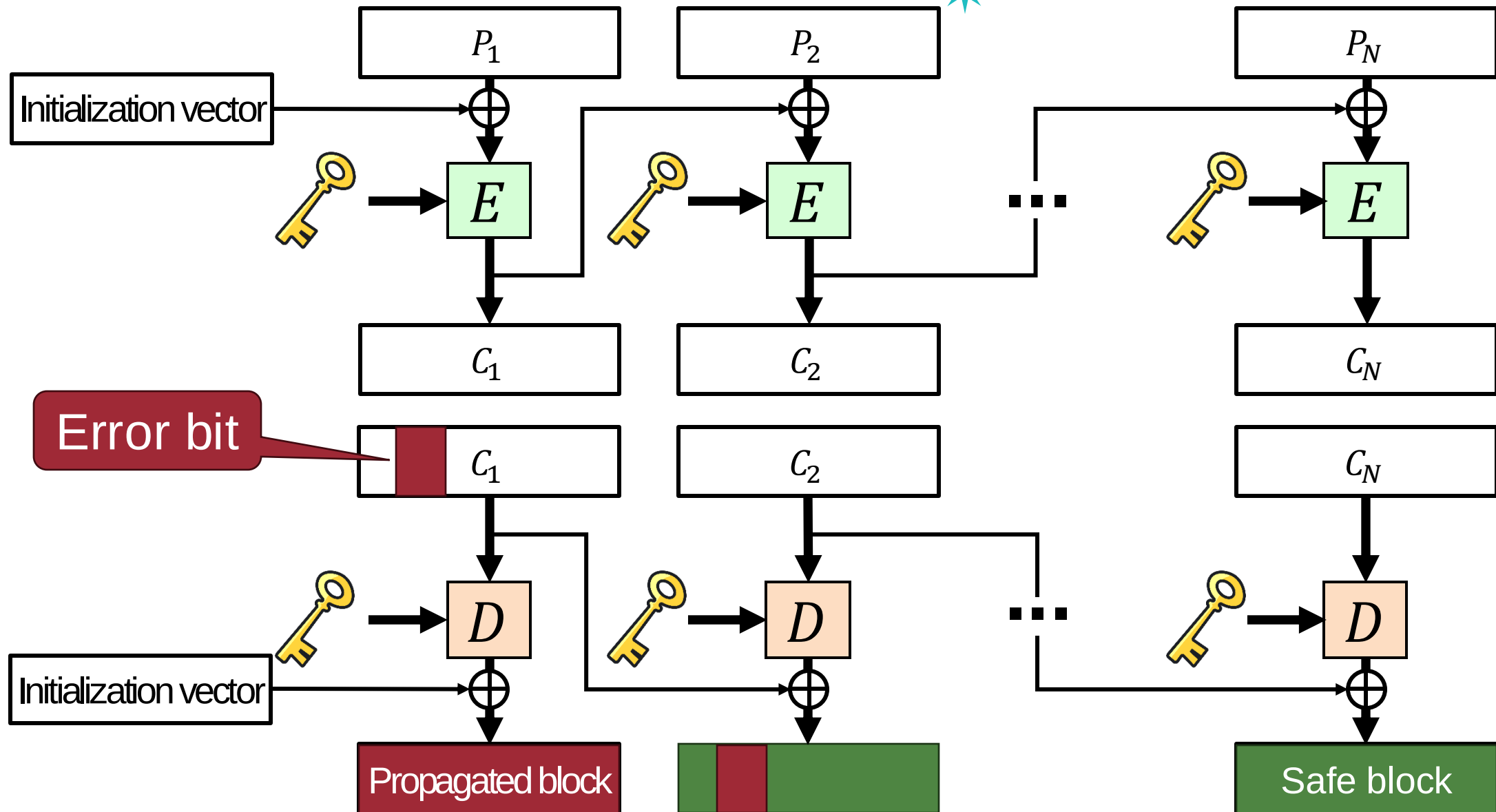


- Each previous cipher block is chained with current plaintext block
- Advantages
 - Does not reveal any patterns the plaintext may have
- Disadvantages
 - Cannot parallelize encryption
 - An error affects one other block (Toggles only one bit in the next block)

Error Propagation in CBC



Error Propagation in CBC



CBC: Cipher Block Chaining

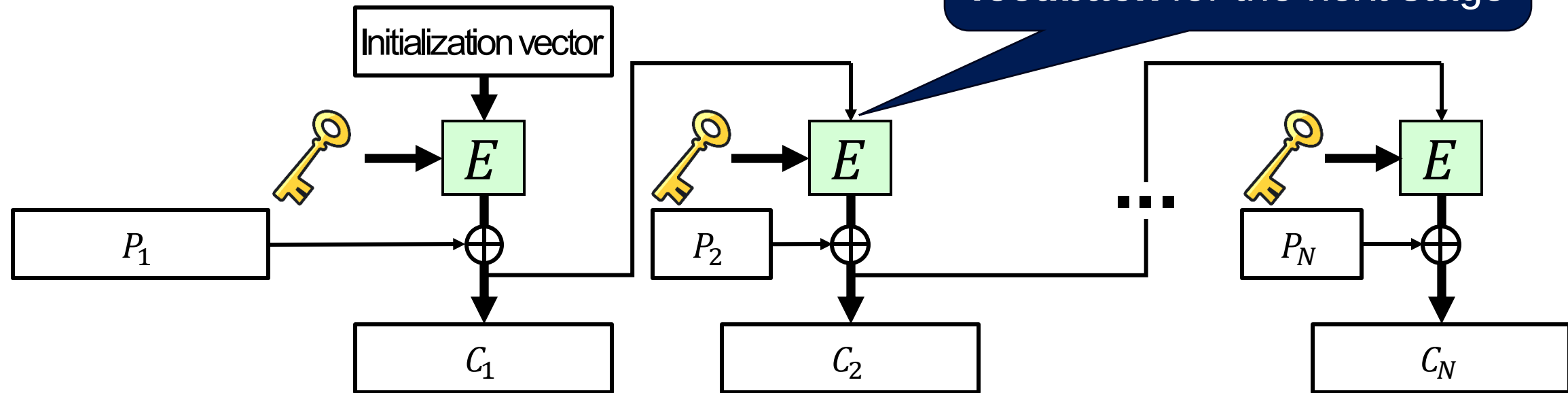


- Each previous cipher block is chained with current plaintext block
- Advantages
 - Does not reveal any patterns the plaintext may have
- Disadvantages
 - Cannot parallelize encryption
 - An error affects one other block (Toggles only one bit in the next block)

CFB: Cipher Feedback

The previous ciphertext is **feedback** for the next stage

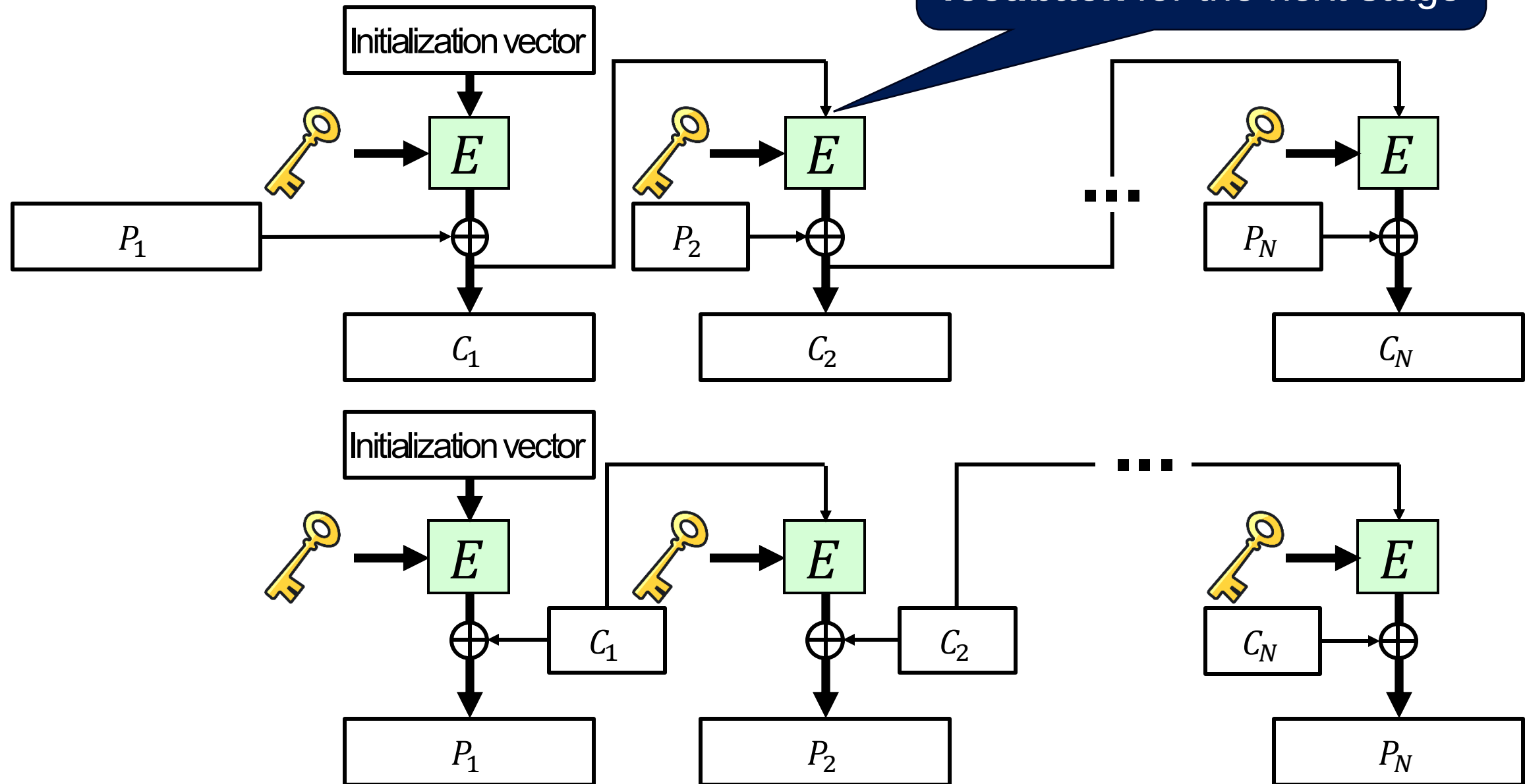
23



CFB: Cipher Feedback

The previous ciphertext is **feedback** for the next stage

24

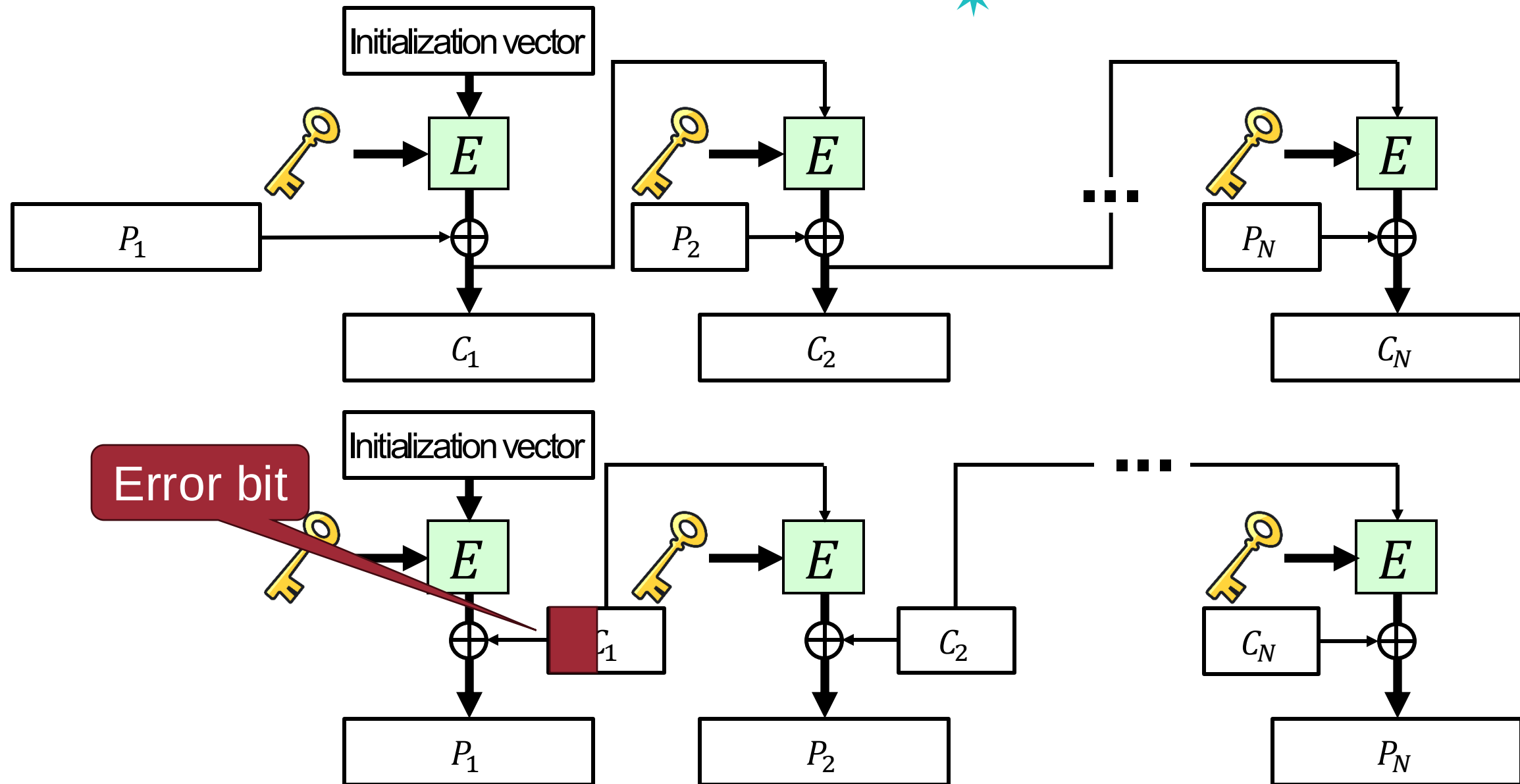


CFB: Cipher Feedback

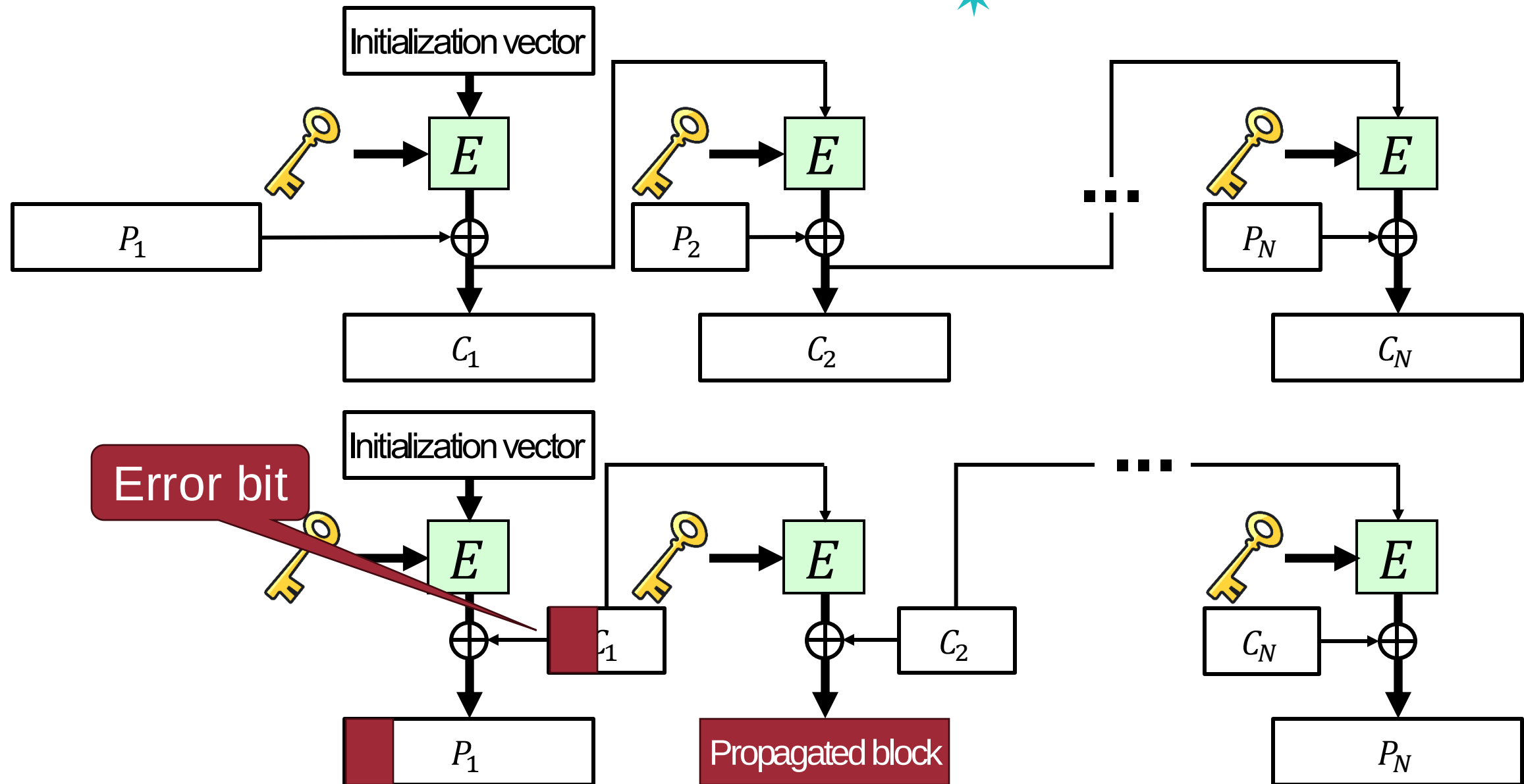


- Each previous cipher block is feedback for the next stage
- Advantages
 - Does not reveal any patterns the plaintext may have
 - Does not use a decryption algorithm (The implementation is efficient)
- Disadvantages
 - Cannot parallelize encryption
 - An error affects one other block

Error Propagation in CFB



Error Propagation in CFB



CFB: Cipher Feedback

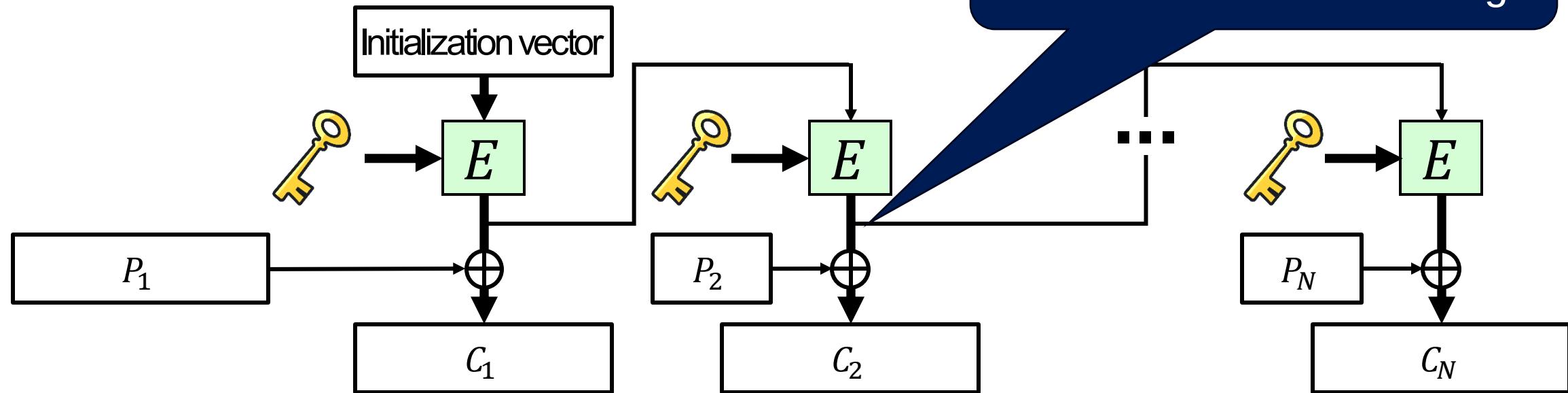


- Each previous cipher block is feedback for the next stage
- Advantages
 - Does not reveal any patterns the plaintext may have
 - Does not use a decryption algorithm (The implementation is efficient)
- Disadvantages
 - Cannot parallelize encryption (How about the decryption process?)
 - An error affects one other block

OFB: Output Feedback

The encrypted output is
feedback for the next stage

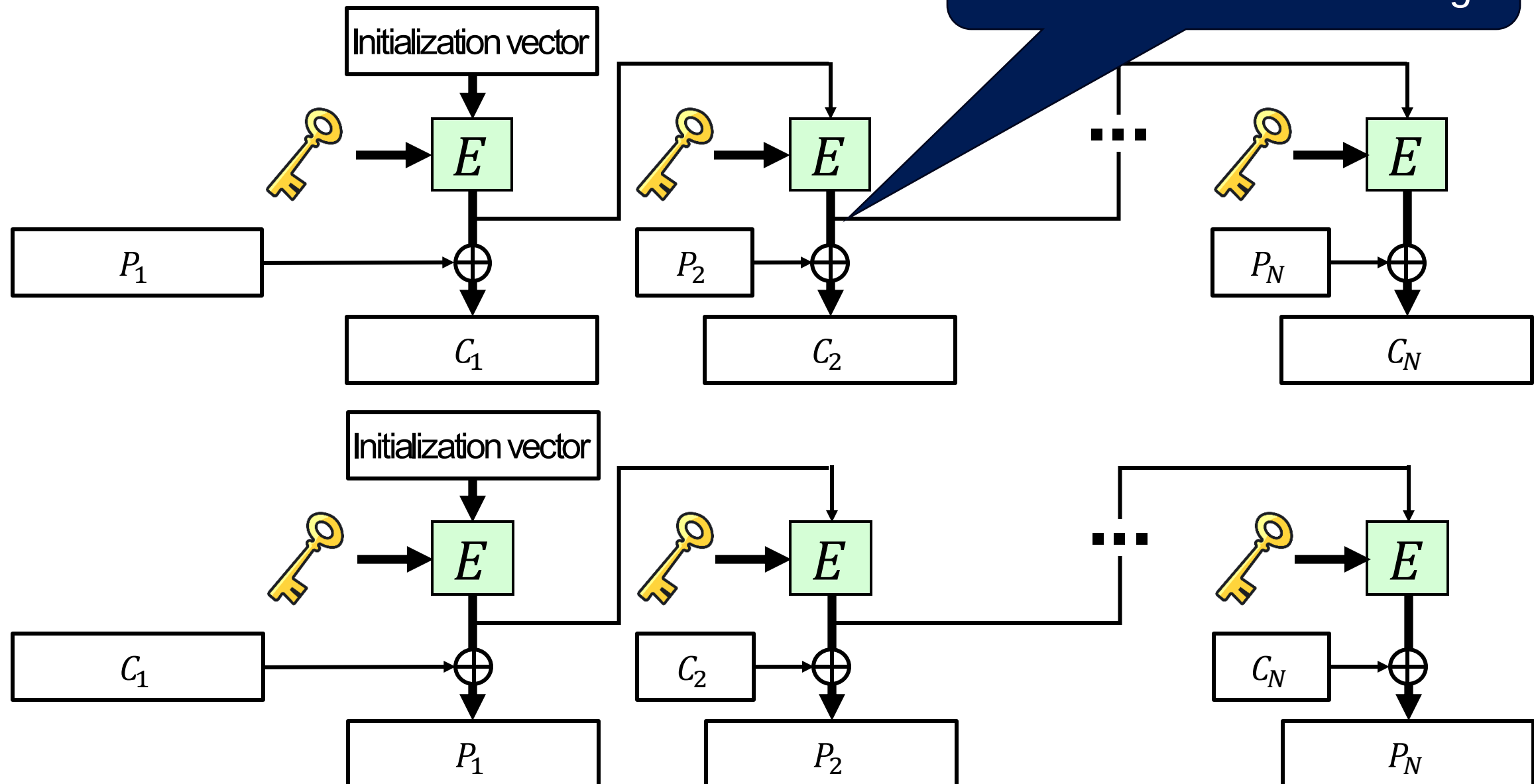
29



OFB: Output Feedback

The encrypted output is
feedback for the next stage

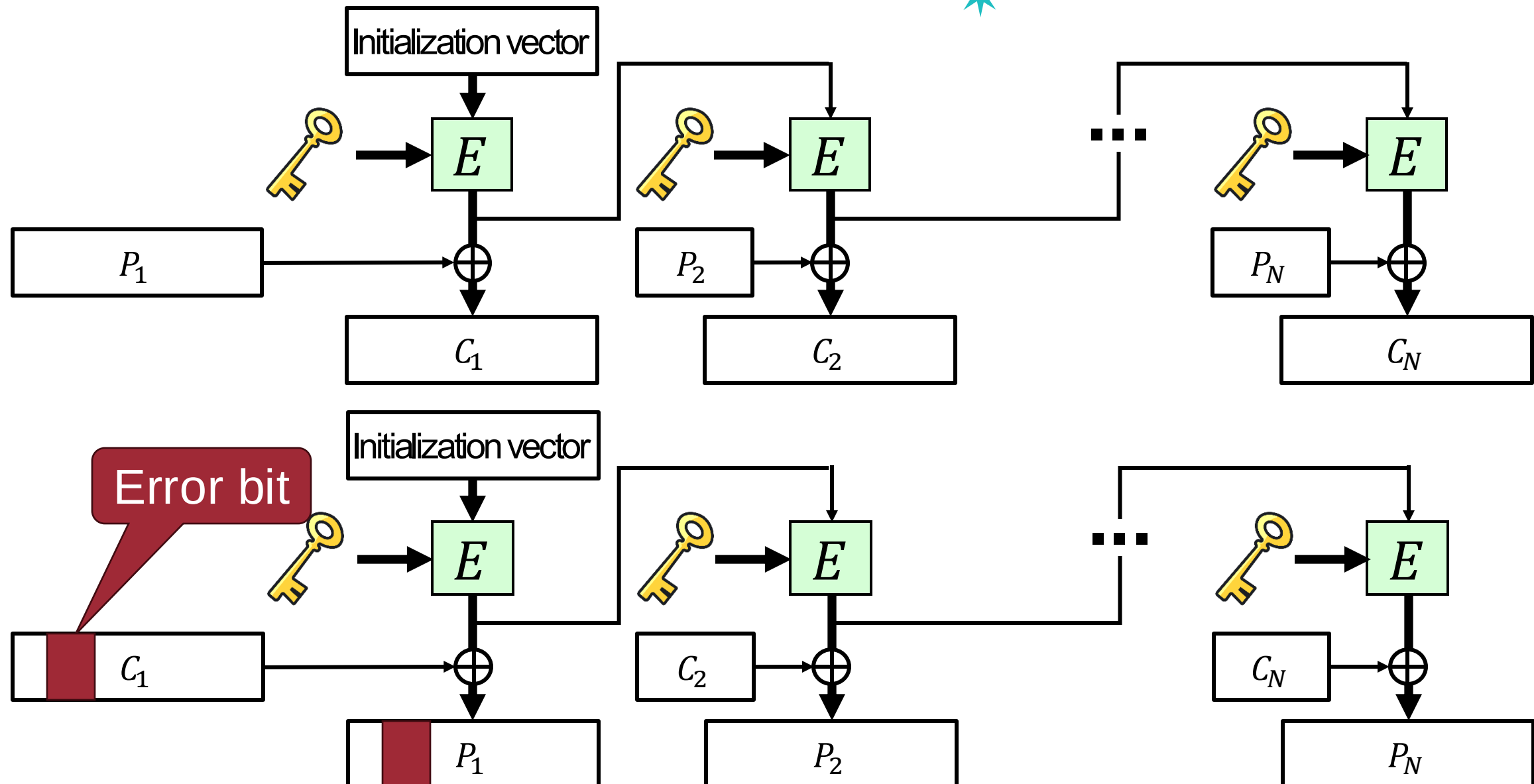
30



OFB: Output Feedback

- Each encrypted output is feed back for next stage
- Advantages
 - Does not reveal any patterns the plaintext may have
 - Does not use a decryption algorithm (+ Extra benefit?)
 - An error has no effect on other blocks (+ Error of one bit in ciphertext affects only one bit in the plaintext block)

Error Propagation in OFB



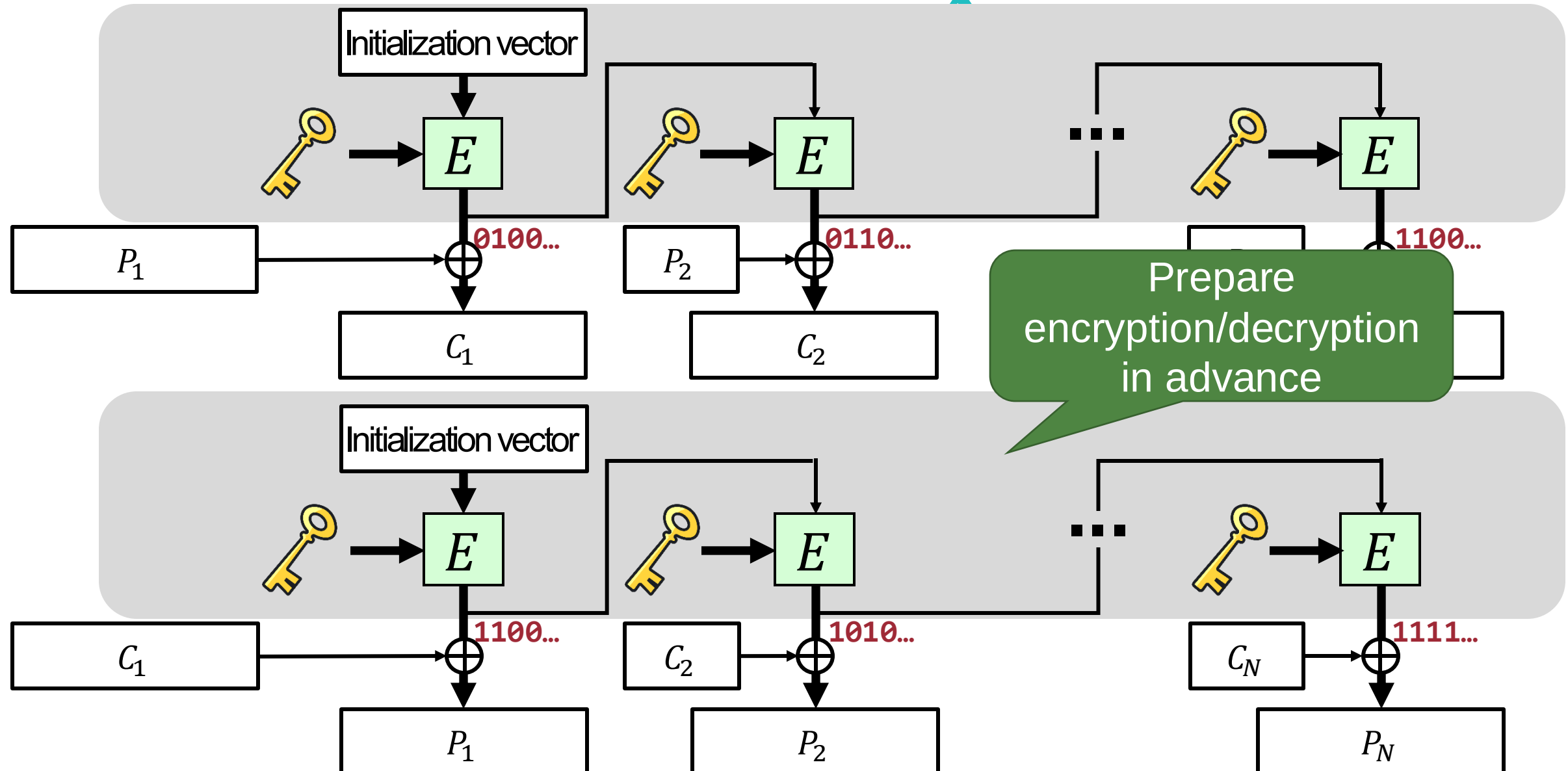
OFB: Output Feedback

- Each encrypted output is feed back for next stage
- Advantages
 - Does not reveal any patterns the plaintext may have
 - Does not use a decryption algorithm (+ Extra benefit?)
 - An error has no effect on other blocks (+ Error of one bit in ciphertext affects only one bit in the plaintext block)
- Disadvantages
 - Cannot parallelize encryption and decryption

However, we can overcome this disadvantage by preparing encryption/decryption in advance

Boost Up OFB Mode

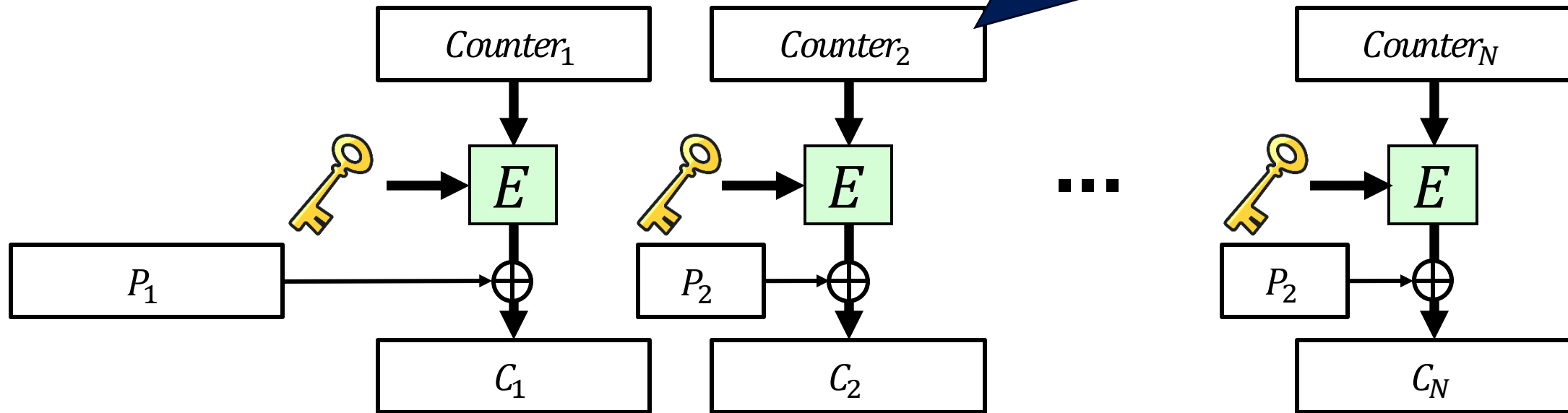
34



CTR: Counter Mode

Encrypt counter value rather than any feedback value

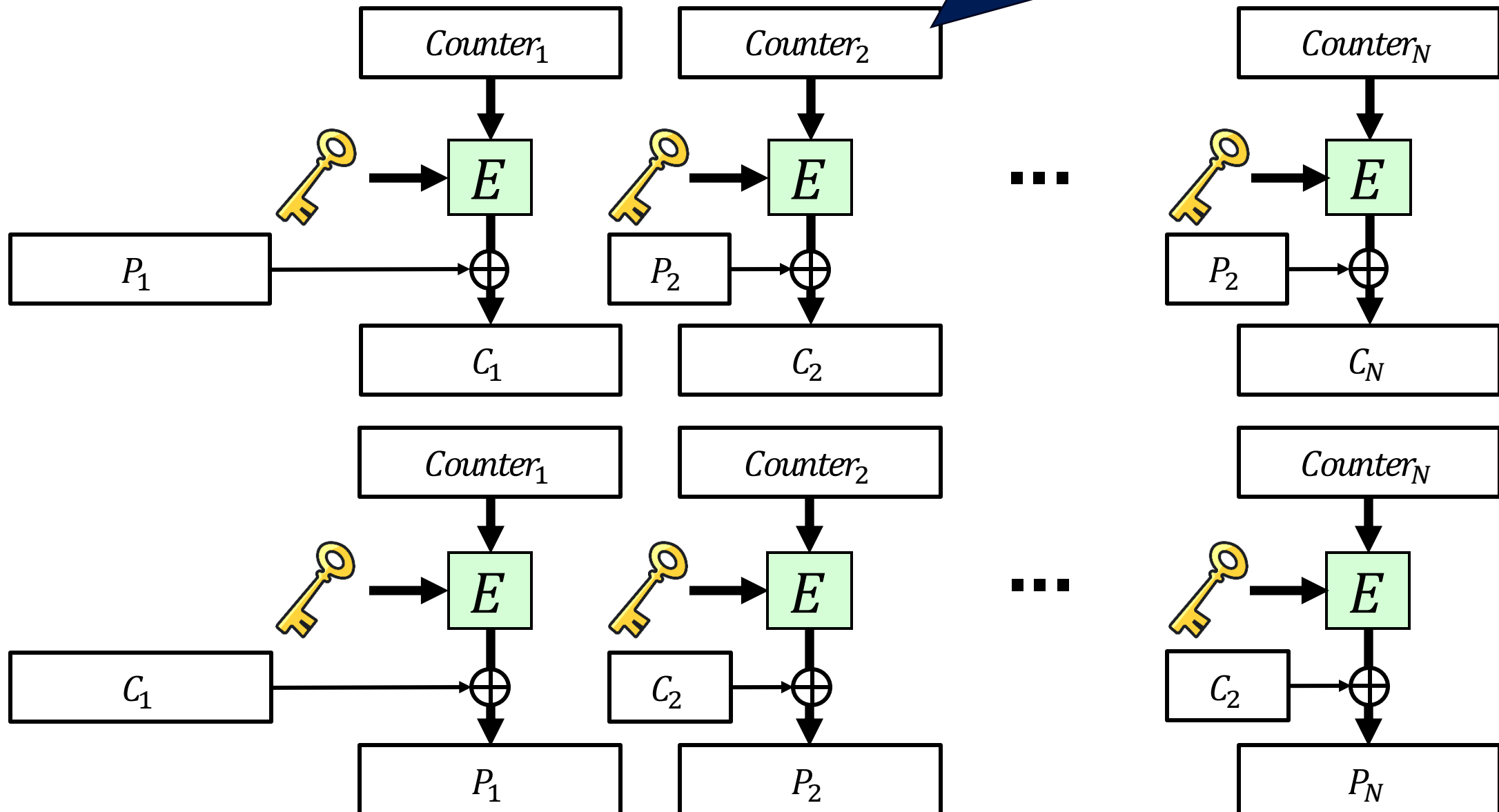
35



CTR: Counter Mode

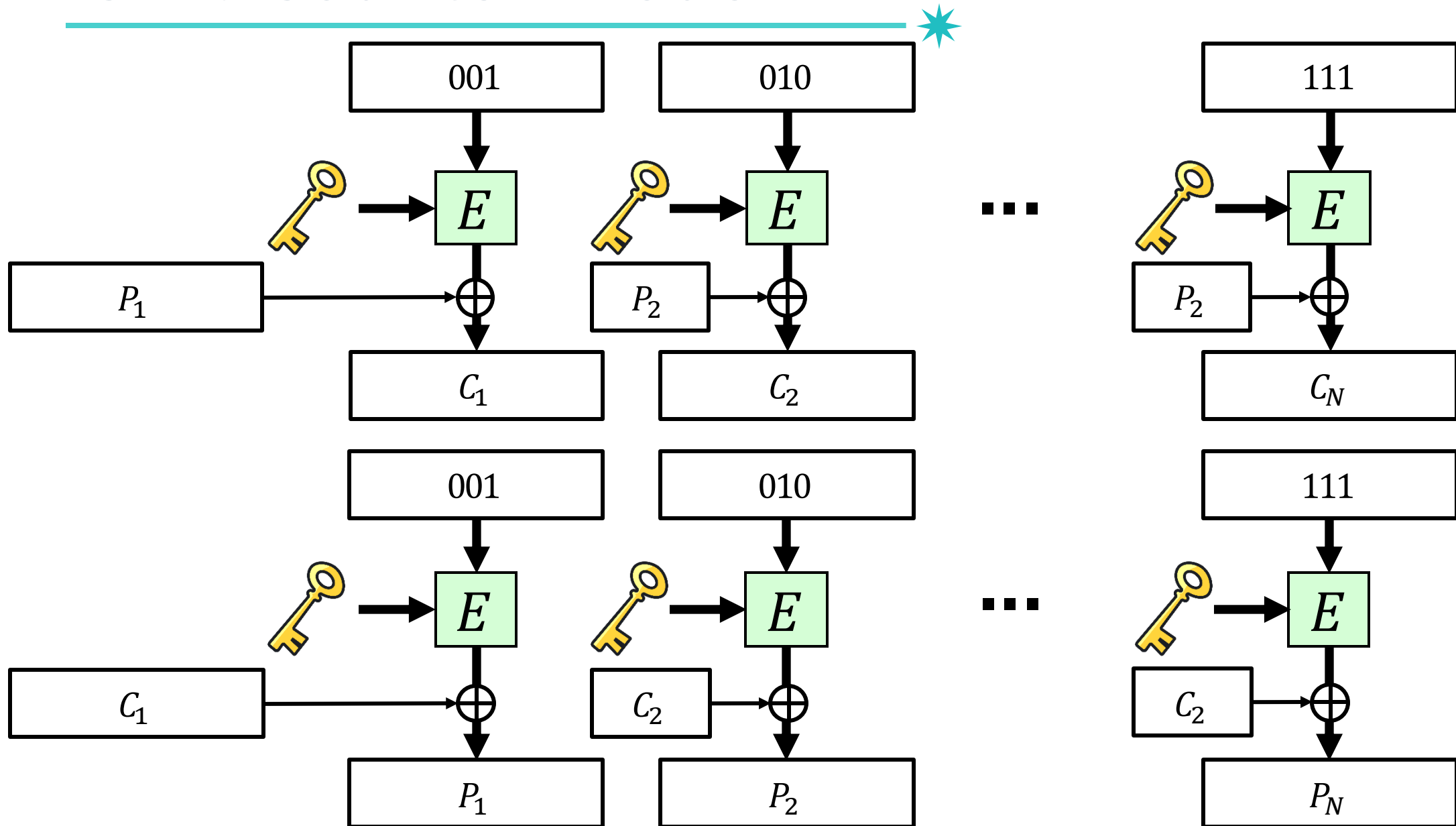
Encrypt counter value rather than any feedback value

36



CTR: Counter Mode

37



CTR: Counter Mode



- Encrypt **counter value** rather than any feedback value
- Advantages
 - Does not reveal any patterns the plaintext may have
 - Can do parallel encryption/decryption in H/W or S/W (+ can preprocess in advance of need)
 - Does not use a decryption algorithm (+ Use the same structure for both encryption and decryption)
 - An error has no effect on other blocks (+ Error of one bit in ciphertext affects only one bit in the plaintext block)
- Disadvantages
 - Must ensure never reuse key/counter values, otherwise could break

Summary



- Symmetric-key cryptography: the same key for encryption and decryption
- Block cipher: basic building block of many cipher schemes
 - DES, Triple-DES, AES
- Block cipher mode of operations
 - ECB: Electronic Code Book
 - CBC: Cipher Block Chaining
 - CFB: Cipher FeedBack
 - OFB: Output FeedBack
 - CTR: CounTeR mode

Question?