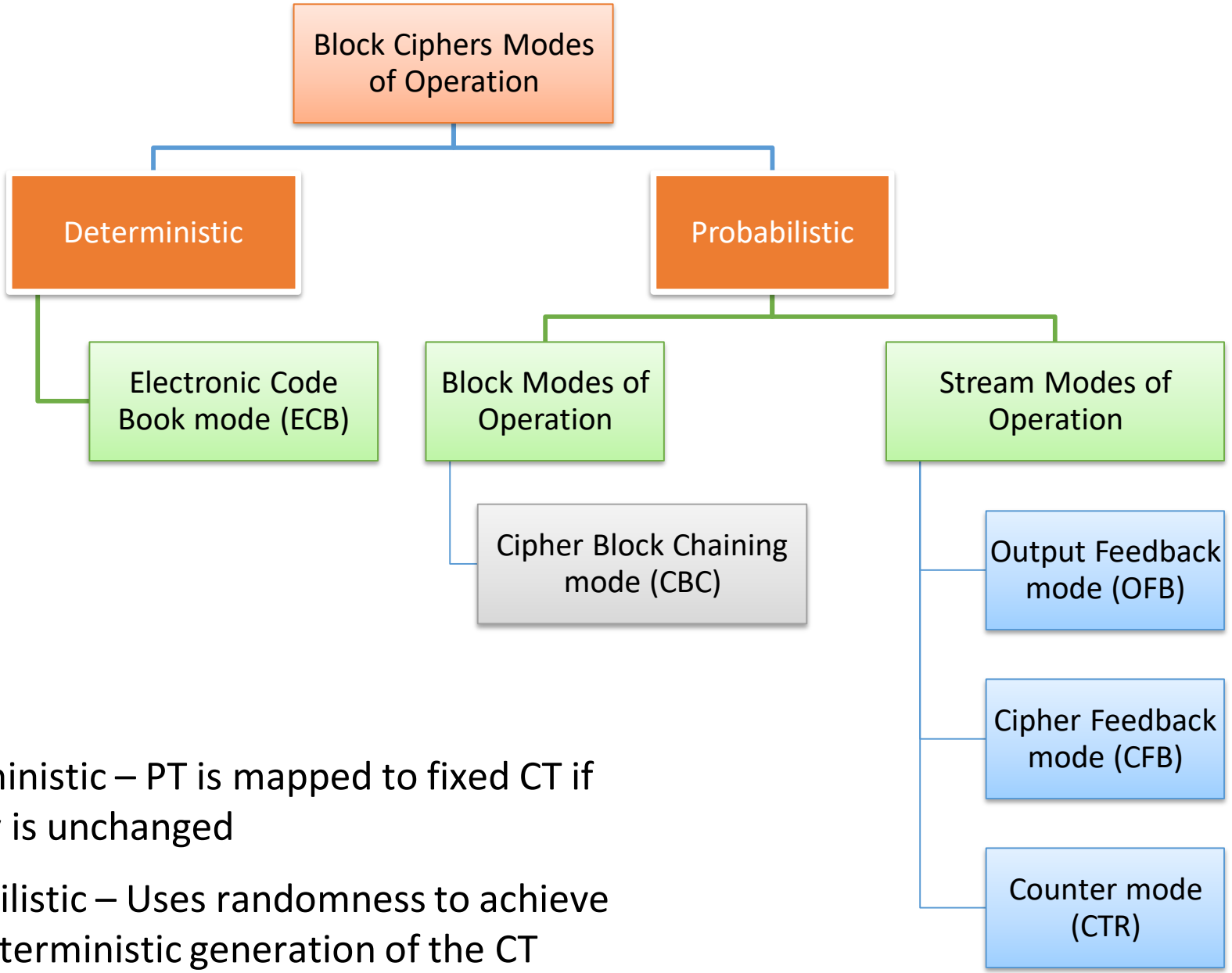
Block Ciphers Modes of Operation

Outline



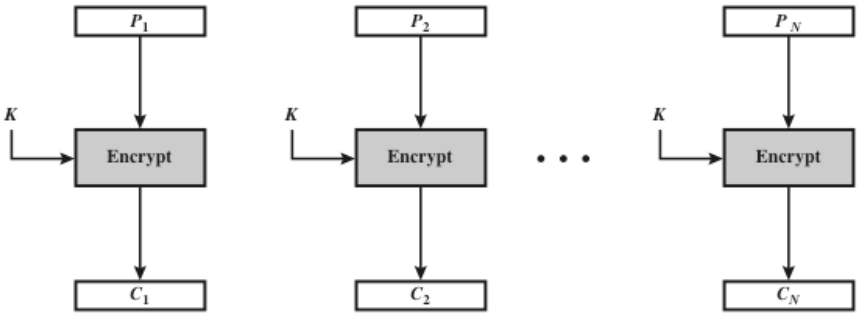
- Deterministic – PT is mapped to fixed CT if the key is unchanged
- Probabilistic – Uses randomness to achieve non-deterministic generation of the CT

ECB & CBC

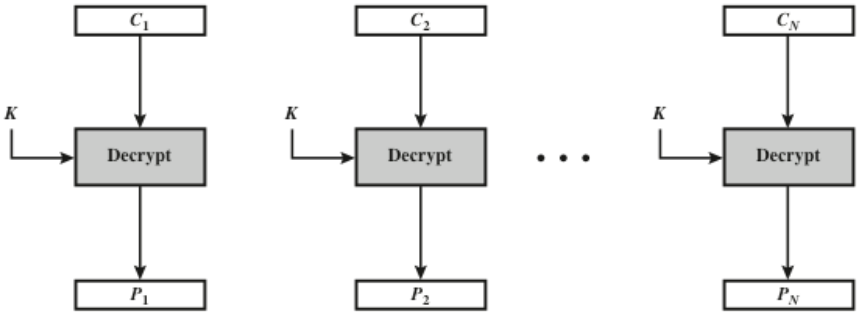
Electronic Code Book mode (ECB)

- How to encode multiple blocks of a long message?
- Each block is encrypted independently of the others

$$C_i = E_K(P_i)$$



(a) Encryption



(b) Decryption

ECB: advantages/disadvantages

- **Advantages**
  - no block synchronization between sender and receiver is required
  - bit errors caused by noisy channels only affect the corresponding block but not succeeding blocks
  - Encryption/decryption can be parallelized => high-speed
- **Disadvantages**
  - ECB encrypts highly deterministically
    - identical plaintexts result in identical ciphertexts
    - an attacker recognizes if the same message has been sent twice

Substitution Attack on ECB

- Once a particular plaintext to ciphertext block mapping $P_i \rightarrow C_i$ is known, a sequence of ciphertext blocks can easily be manipulated
- Suppose an *electronic bank transfer*

Block #	1	2	3	4	5
	Sending Bank A	Sending Account #	Receiving Bank B	Receiving Account #	Amount $

  - the encryption key between the two banks does not change too frequently
  - The attacker sends $1 transfers from his account at bank A to his account at bank B repeatedly
    - He can check for ciphertext blocks that repeat, and he stores blocks 1,3 and 4 of these transfers
  - He now simply replaces block 4 of other transfers with the block 4 that he stored before
    - *all transfers* from some account of bank A to some account of bank B are redirected to go into the attacker's B account!

Cipher Block Chaining mode (CBC)

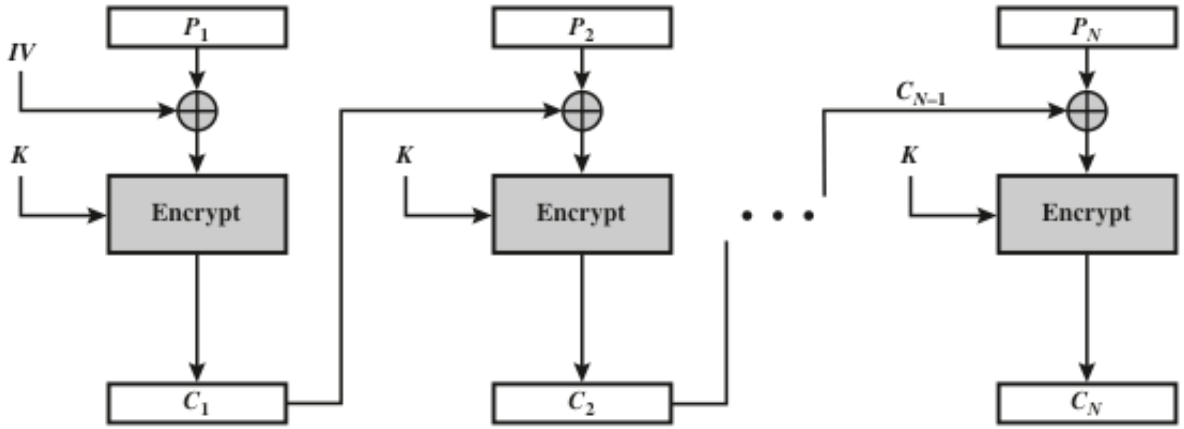
- There are two main ideas behind the CBC mode:
  - Previous cipher block is chained with current plaintext block
    - ciphertext C_i depends not only on block P_i but on ciphertext block C_{i-1} as well
    - Any change to a block affects all following ciphertext blocks
  - The encryption is randomized by using an Initialization Vector (IV)

$$C_1 = E_K(P_1 \oplus IV)$$

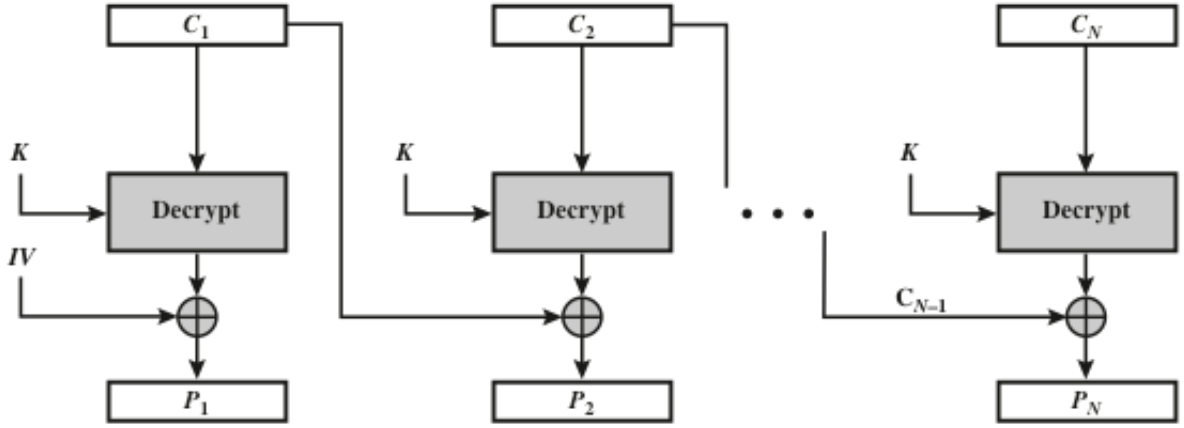
$$C_i = E_K(P_i \oplus C_{i-1})$$

- IV should be a **non-secret nonce** (used only once) value => the CBC mode becomes a probabilistic encryption scheme, i.e., two encryptions of the same plaintext look entirely different

Cipher Block Chaining mode (CBC)



(a) Encryption



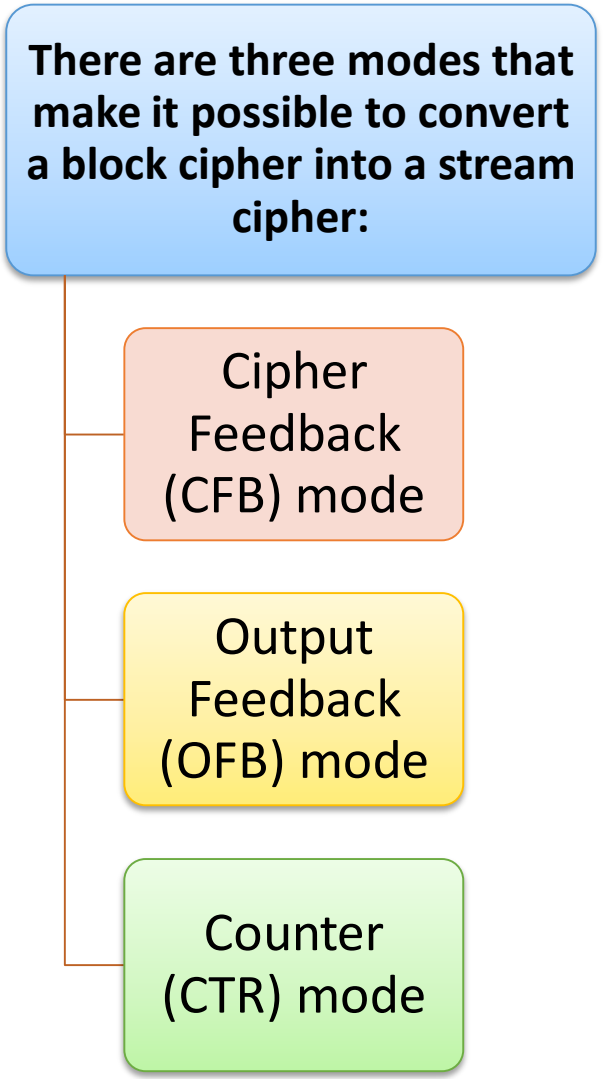
(b) Decryption

Sequential implementation. Cannot be parallelized.

Stream Modes of Operation

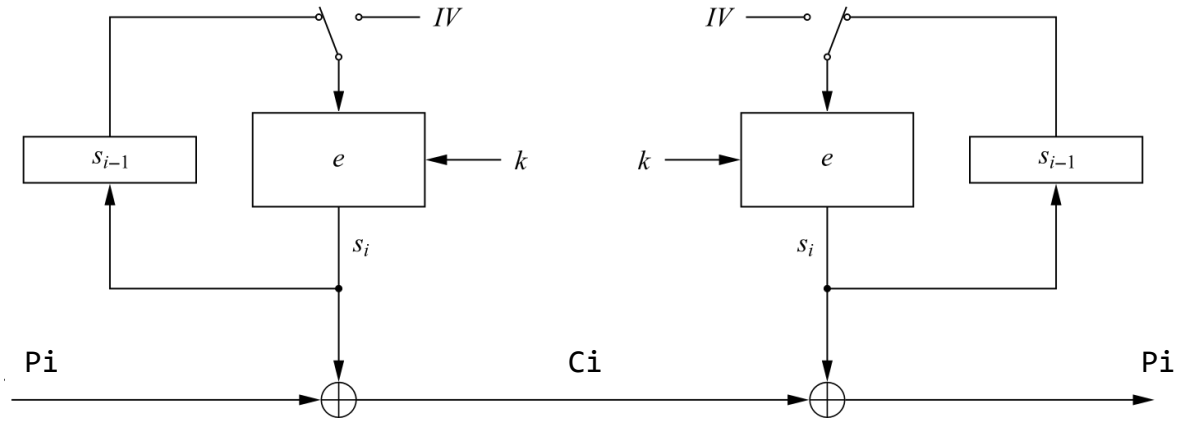
Stream Modes of Operation

- Use block cipher as some form of pseudo-random number generator
  - The random number bits are then XOR'ed with the plaintext (as in stream cipher)
  - The key stream is computed in a **blockwise** fashion
  - The key stream block has the same size as the plaintext block



Output Feedback mode (OFB)

- It is used to build a **stream cipher** from a block cipher
  - The key stream is generated in a blockwise fashion (instead of bitwise)
- The output of the cipher gives us key stream bits S_i with which we can encrypt plaintext bits using the XOR operation.
  - Output of the cipher is feed back for next stage

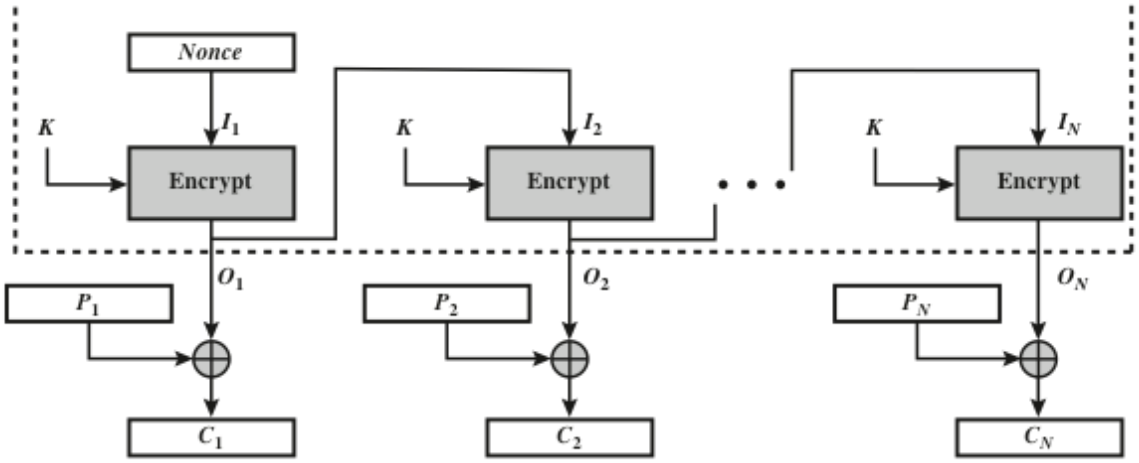


Encryption (first block): $S_1 = e_k(\text{IV}) \quad and \quad C_1 = S_1 \oplus P_1$

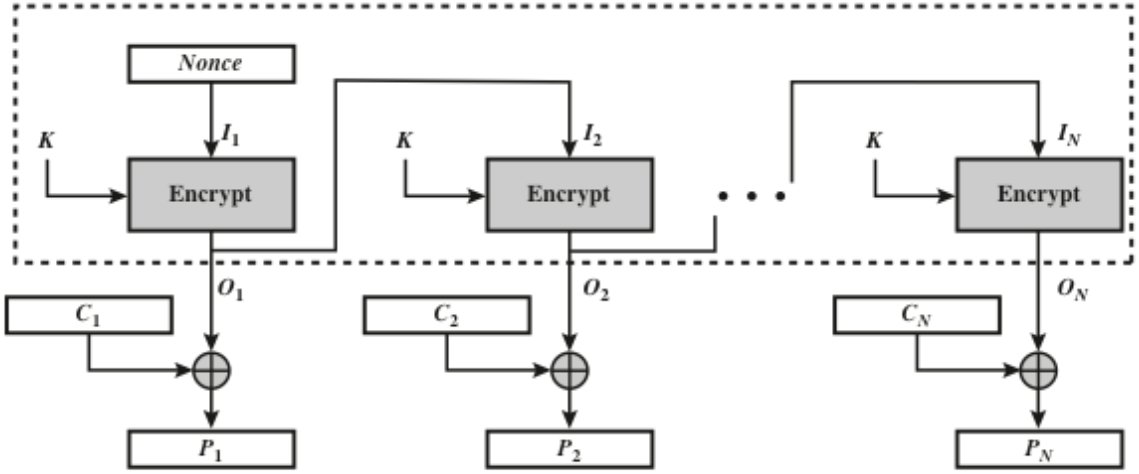
Encryption (general block): $S_i = e_k(S_{i-1}) \quad and \quad C_i = S_i \oplus P_i, \quad i \geq 2$

Decryption (first block): $S_1 = e_k(\text{IV}) \quad and \quad P_1 = S_1 \oplus C_1$

Decryption (general block) : $S_i = e_k(S_{i-1}) \quad and \quad P_i = S_i \oplus C_i, \quad i \geq 2$



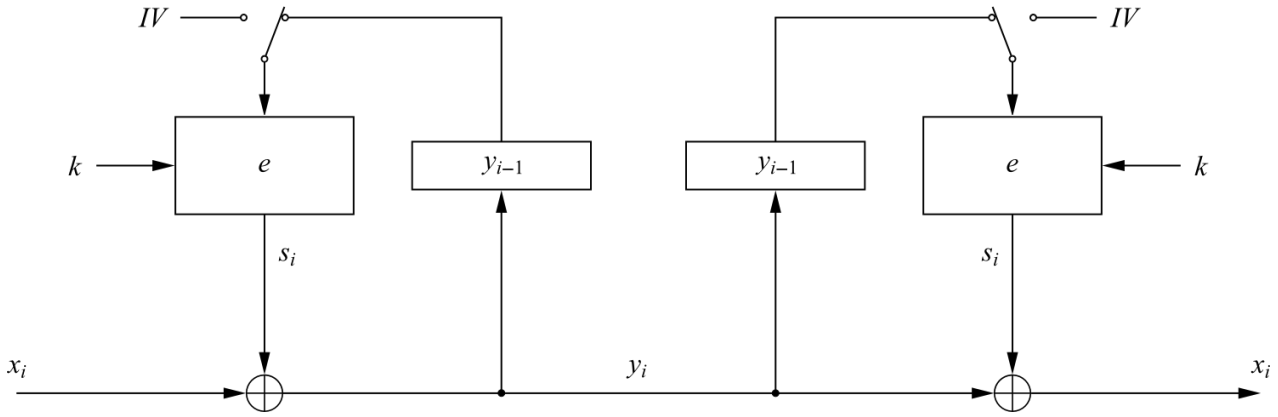
(a) Encryption



(b) Decryption

Cipher Feedback mode (CFB)

- It uses a block cipher as a building block for a **stream cipher** (similar to the OFB mode), more accurate name: “Ciphertext Feedback Mode”
- The key stream S_i is generated in a blockwise fashion and is also a function of the ciphertext y_{i-1}
- As a result of the use of an IV, the CFB encryption is also nondeterministic



Encryption (first block): $y_1 = e_k(\text{IV}) \oplus x_1$
Encryption (general block): $y_i = e_k(y_{i-1}) \oplus x_i, \quad i \geq 2$
Decryption (first block): $x_1 = e_k(\text{IV}) \oplus y_1$
Decryption (general block) : $x_i = e_k(y_{i-1}) \oplus y_i, \quad i \geq 2$

- It can be used in situations where short plaintext blocks are to be encrypted

Counter mode (CTR)

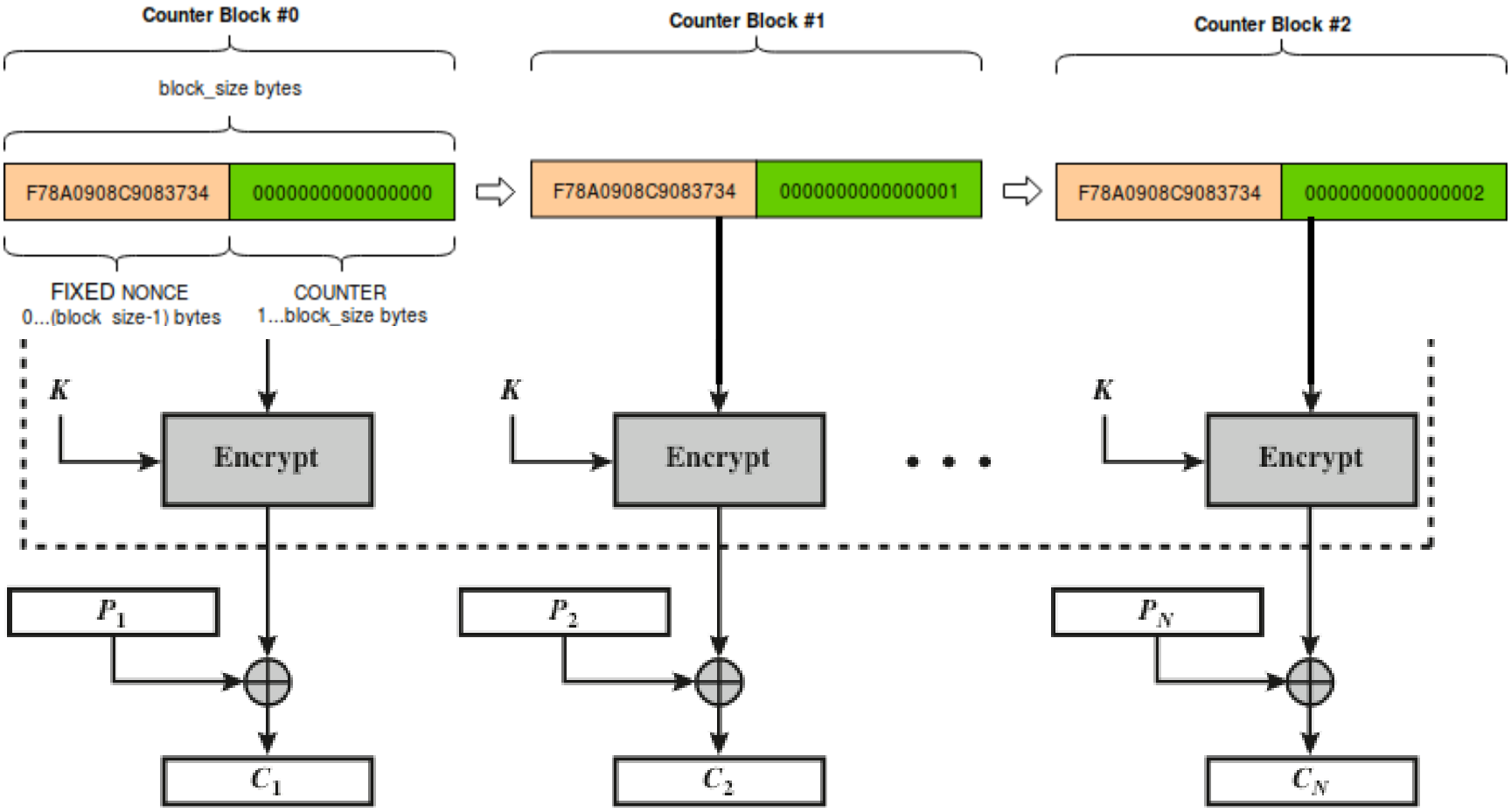
- It uses a block cipher as a **stream cipher** (like the OFB and CFB modes)
- Encrypt counter value rather than any feedback value
- The input to the block cipher is a counter value (same size as the plaintext block size) which must be different for each plaintext block that is encrypted

$$S_i = E_K(CTR_i)$$
$$C_i = P_i \oplus S_i$$

- The *keystream* is generated by encrypting a sequence of *counter blocks*
- Unlike CFB and OFB modes, the CTR mode can be parallelized since the 2nd encryption can begin before the 1st one has finished
  - Desirable for high-speed implementations, e.g., in network routers

Counter mode (CTR)

- A counter block consists of the concatenation of two pieces: **a fixed nonce**, set at initialization + **a variable counter**, which gets increased by 1 for any subsequent counter block.



Summary

Mode	Description
Electronic Codebook (ECB)	Each block of plaintext bits is encoded independently using the same key.
Cipher Block Chaining (CBC)	The input to the encryption algorithm is the XOR of the next block of plaintext and the preceding block of ciphertext.
Cipher Feedback (CFB)	Preceding ciphertext is used as input to the encryption algorithm to produce pseudorandom output, which is XORed with plaintext to produce next unit of ciphertext.
Output Feedback (OFB)	Similar to CFB, except that the input to the encryption algorithm is the preceding encryption output, and full blocks are used.
Counter (CTR)	Each block of plaintext is XORed with an encrypted counter. The counter is incremented for each subsequent block.

Summary

- There are many different ways to encrypt with a block cipher. Each mode of operation has some advantages and disadvantages
- The straightforward ECB mode has security weaknesses, independent of the underlying block cipher
- Several modes turn a block cipher into a stream cipher
- The counter mode allows parallelization of encryption and is thus suited for high speed implementations

References

- Wikipedia
  - http://en.wikipedia.org/wiki/Modes_of_operation