Modes
ECB
CBC
CFB
OFB
CTR
Feedback
XTS-AES

COMP412 Computer Security

Lec 04
Block Cipher Operation

Dr. Xiaochen Yuan
2021/2022

Modes
ECB
CBC
CFB
OFB
CTR
Feedback
XTS-AES

Contents

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

XTS-AES

Modes of Operation

- Block cipher: operates on fixed length b-bit **input** to produce b-bit **ciphertext**
- What about encrypting plaintext longer than b bits?
  - Break plaintext into b-bit blocks (padding if necessary) and apply cipher on each block
- Security issues arise: different modes of operation have been developed

Contents

Modes of Operation

Electronic Code Book (ECB)

Cipher Block Chaining Mode

Cipher Feedback Mode

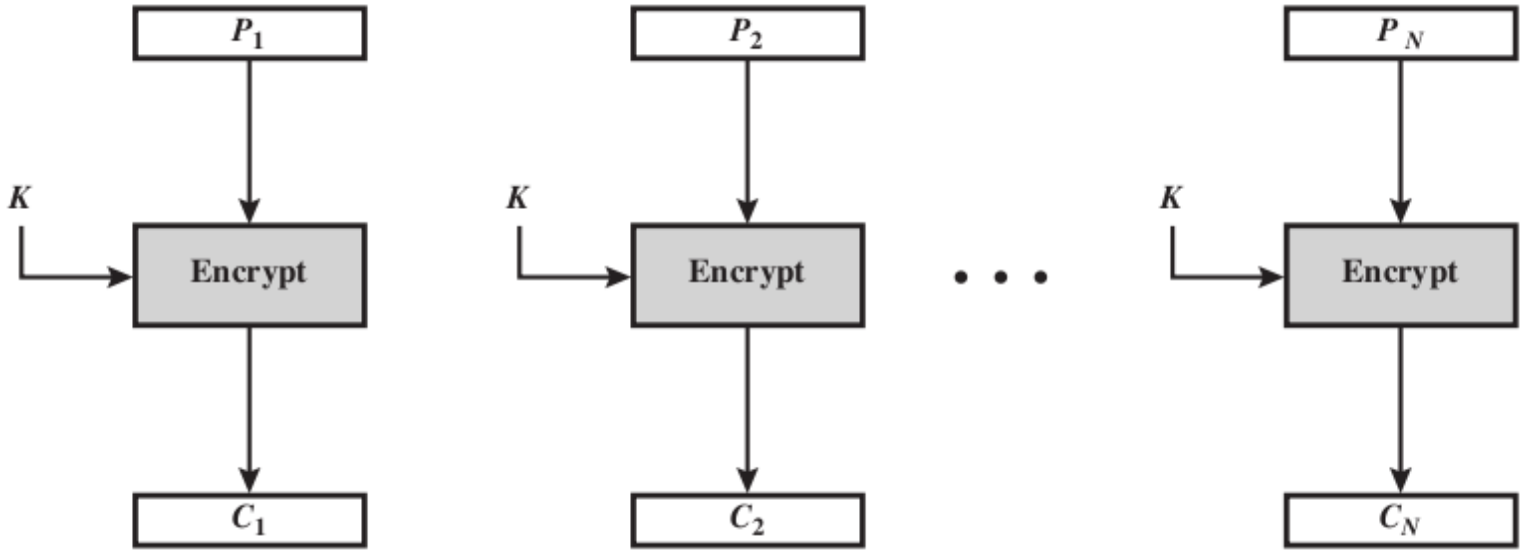
Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

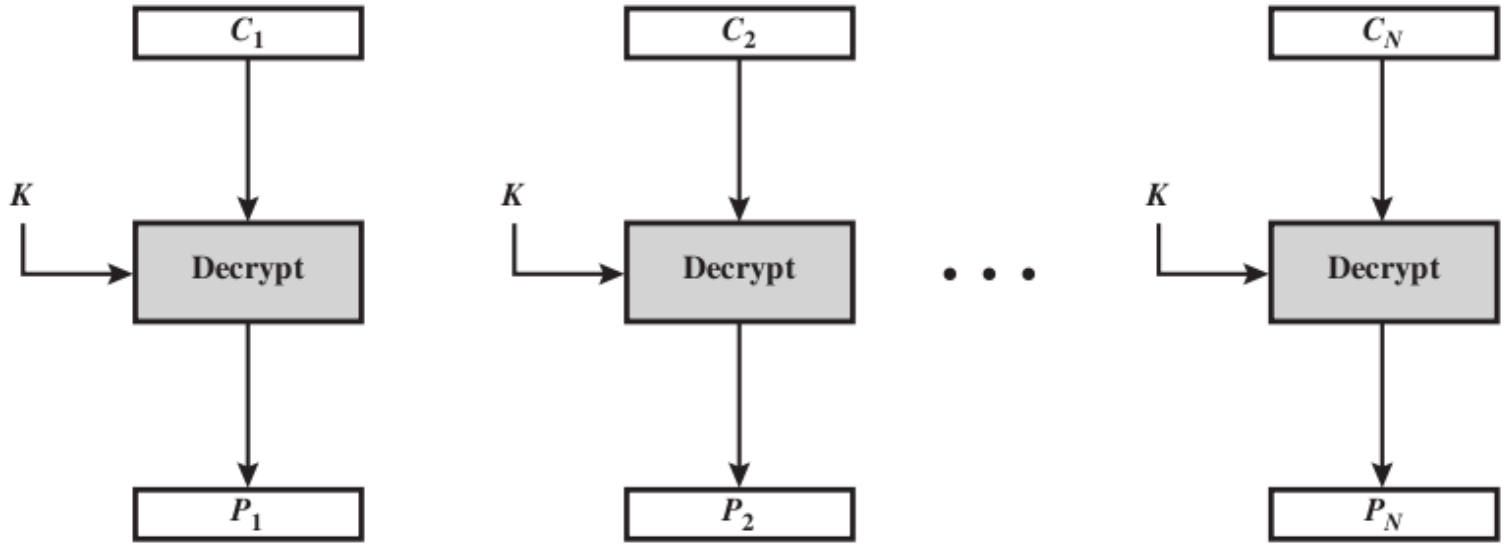
XTS-AES

Electronic Code Book (ECB) Encryption



- Each block: 64 bits
- Same key in each block
- Independently

Electronic Code Book (ECB) Decryption



Summary

- Each block of 64 plaintext bits is encoded independently using same key
- Typical applications: secure transmission of single values (e.g. encryption key)
- Problem: with long message, repetition in plaintext may cause repetition in ciphertext

Modes
ECB
CBC
CFB
OFB
CTR
Feedback
XTS-AES

Contents

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode (CBC)

Cipher Feedback Mode

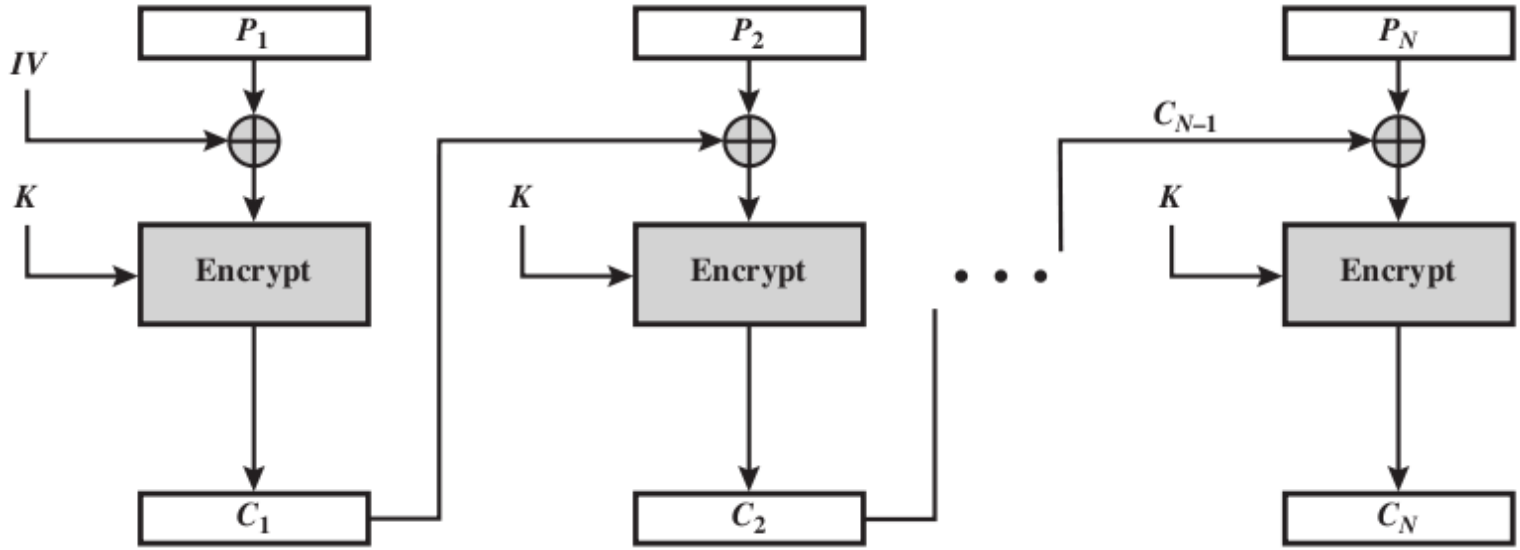
Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

XTS-AES

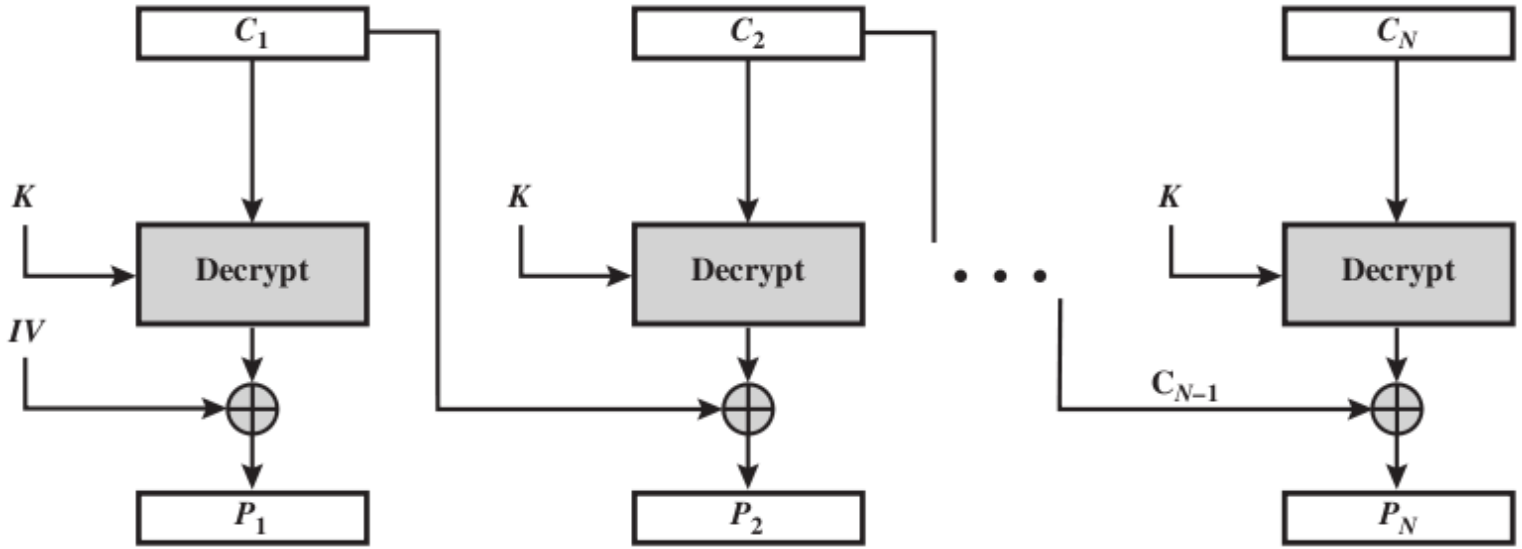
Cipher Block Chaining Mode (CBC) Encryption



- Each block: 64 bits
- Same key in each block
- Initialization Vector (IV) necessarily
- IV XORed P_1, Ci XORed P_{i+1}

Question: *How to avoid the repetition in ciphertext for repetition in plaintext?*

Cipher Block Chaining Mode (CBC) Decryption



CBC Summary

- Input to encryption algorithm is XOR of next 64-bits plaintext and preceding 64-bits ciphertext
- Typical applications: General-purpose block-oriented transmission; authentication
- Initialisation Vector (IV) must be known by sender/receiver, but secret from attacker
  - In particular, it must be impossible to predict the IV for any given plaintext;
  - For maximum security, IV should be protected against unauthorized changes.
    - E.g., send the IV using ECB encryption.

Contents

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode (CFB)

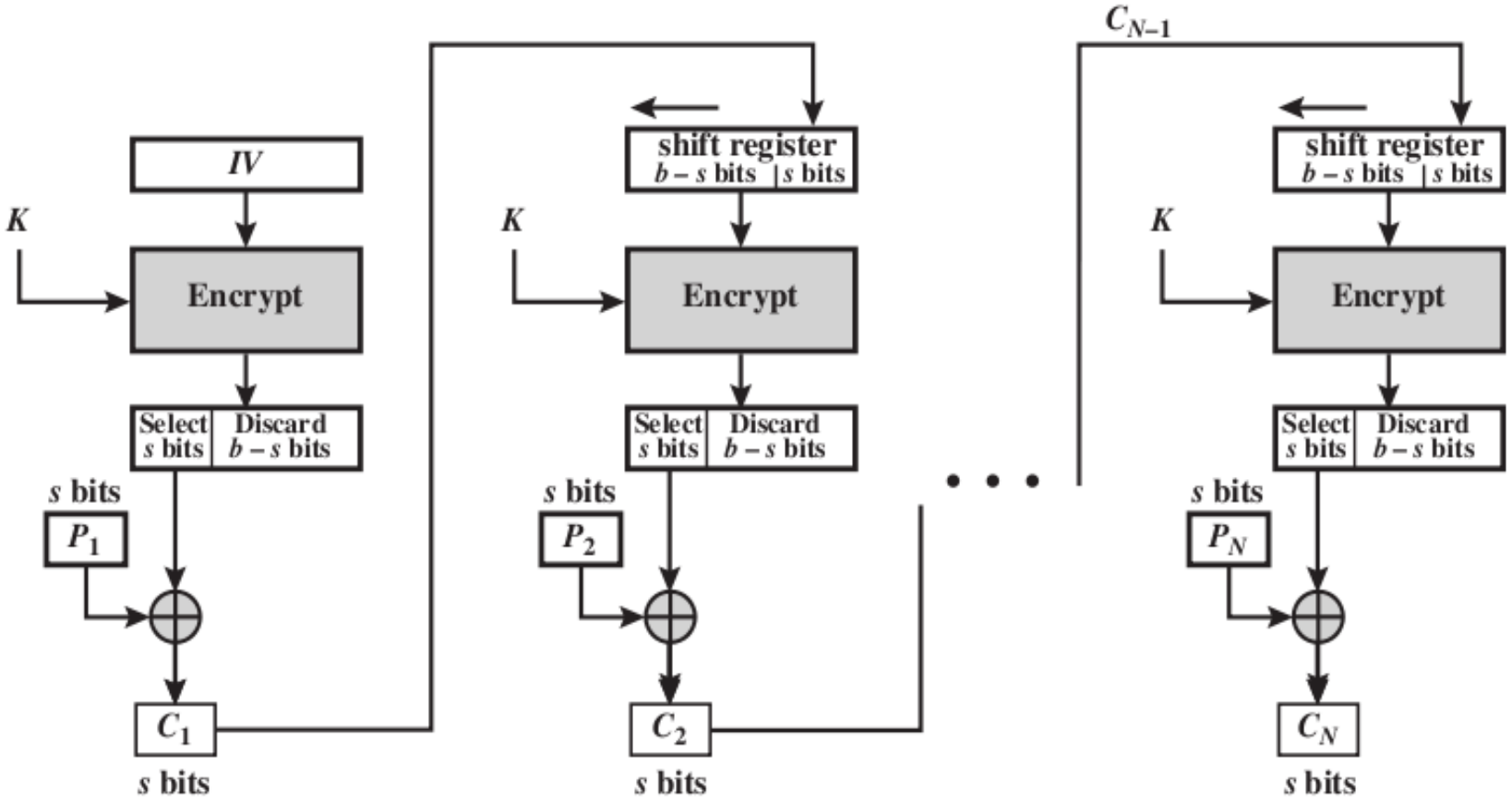
Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

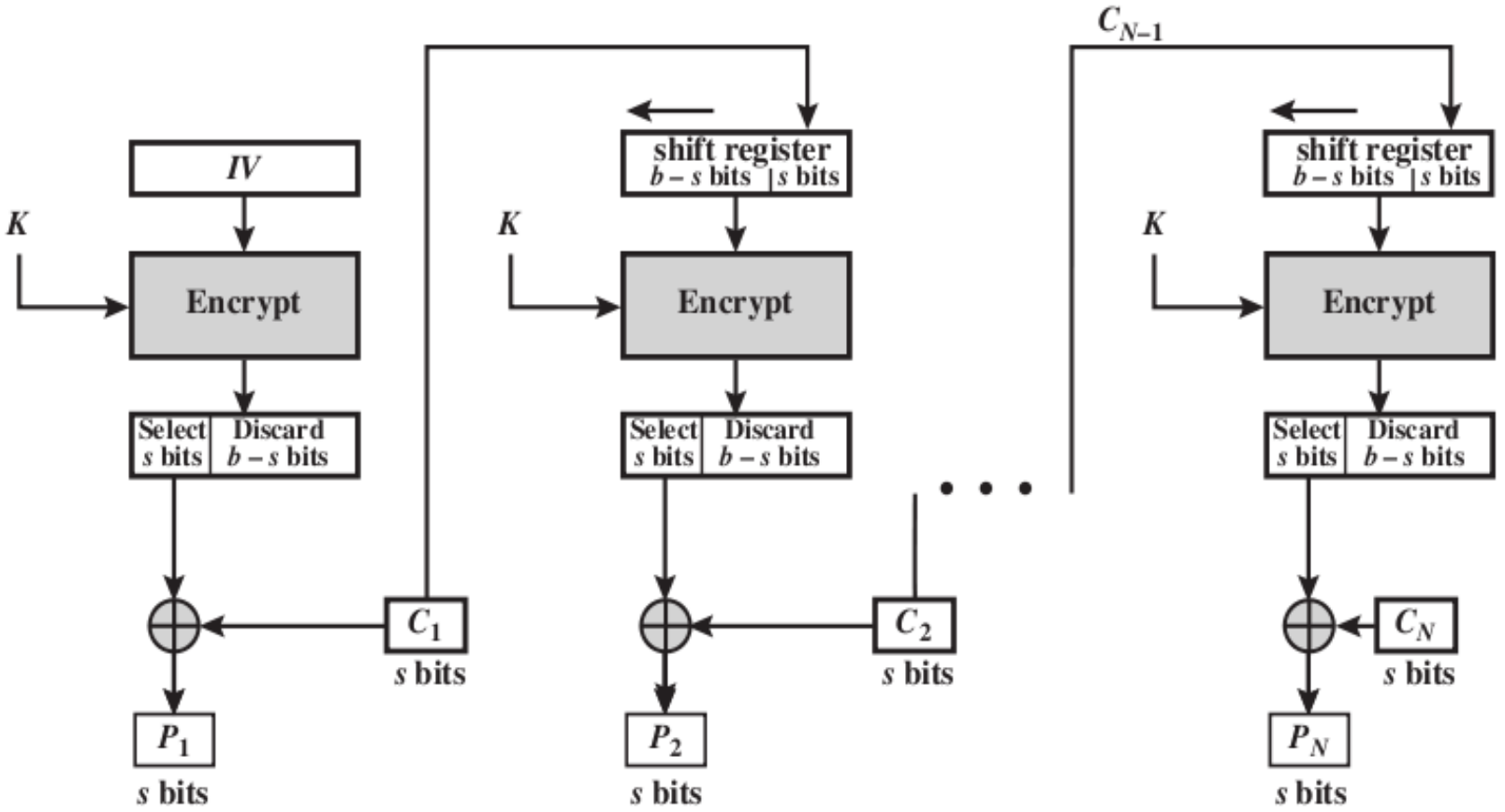
XTS-AES

Cipher Feedback Mode (CFB) Encryption



- Totally: ***b*** bits
- Each time process ***s*** bits
- Shift register applied each time
- Initialization Vector (IV) necessarily

Cipher Feedback Mode (CFB) Decryption



CFB Summary

- Converts **block cipher** into **stream cipher**
  - No need to pad message to integral number of blocks
  - Operate in real-time: each character encrypted and transmitted immediately
- Input processed s bits at a time
- **Preceding ciphertext** used as input to cipher to produce pseudo-random output
- XOR **output** with **plaintext** to produce ciphertext
- Typical applications: General-purpose stream-oriented transmission; authentication

Contents

Modes
ECB
CBC
CFB
OFB
CTR
Feedback
XTS-AES

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

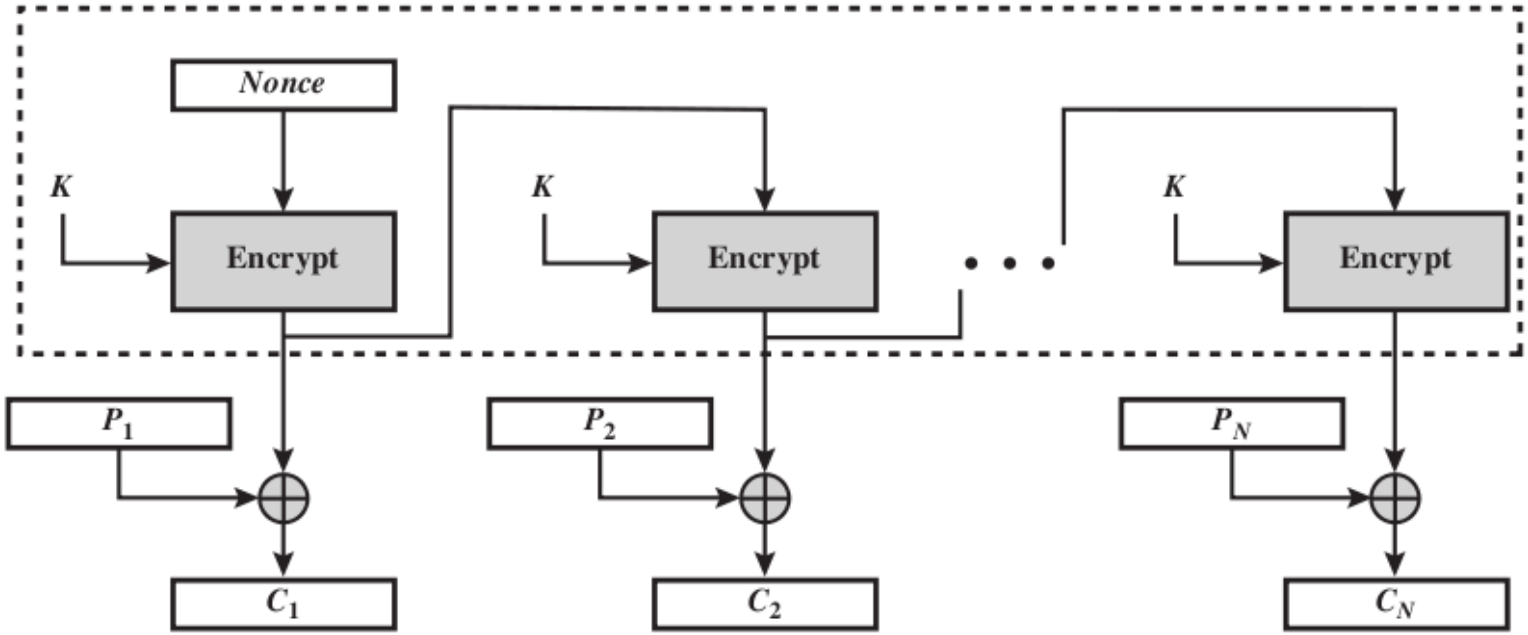
Output Feedback Mode (OFB)

Counter Mode

Feedback Characteristics of Modes

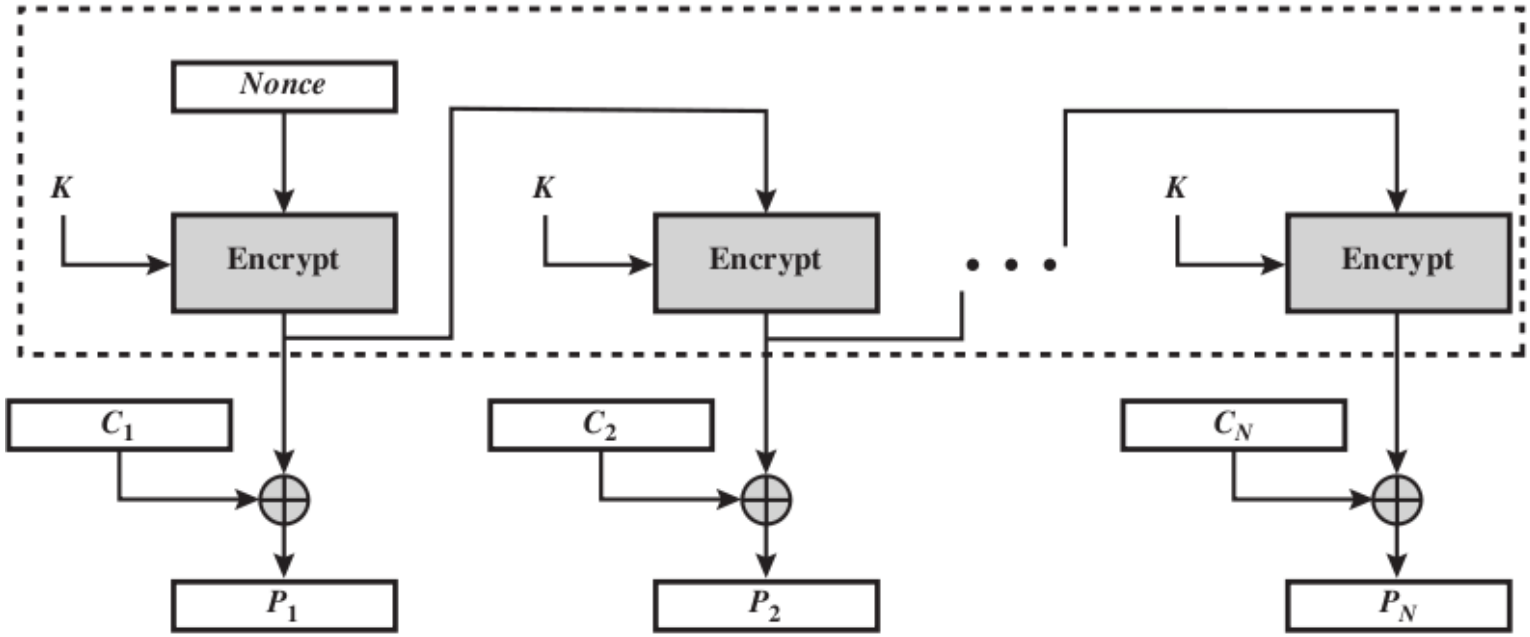
XTS-AES

Output Feedback Mode (OFB) Encryption



- Initialization Vector (IV) necessarily
  - IV must be a nonce,
  - must be unique to each execution of the encryption operation
  - Because each encryption output depends only on the key and the IV.

Output Feedback Mode (OFB) Decryption



OFB Summary

- Converts **block cipher** into **stream cipher**
  - OFB has structure of a typical stream cipher;
  - Distinction from the stream cipher is OFB encrypts a full block at a time; while many stream ciphers encrypt one byte at a time.
- Similar to CFB, except input to encryption algorithm is **preceding encryption output**
- Typical applications: stream-oriented transmission over noisy channels (e.g. satellite communications)
- Advantage compared to CFB: bit errors do not propagate
- Disadvantage: more vulnerable to message stream modification attack

Contents

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

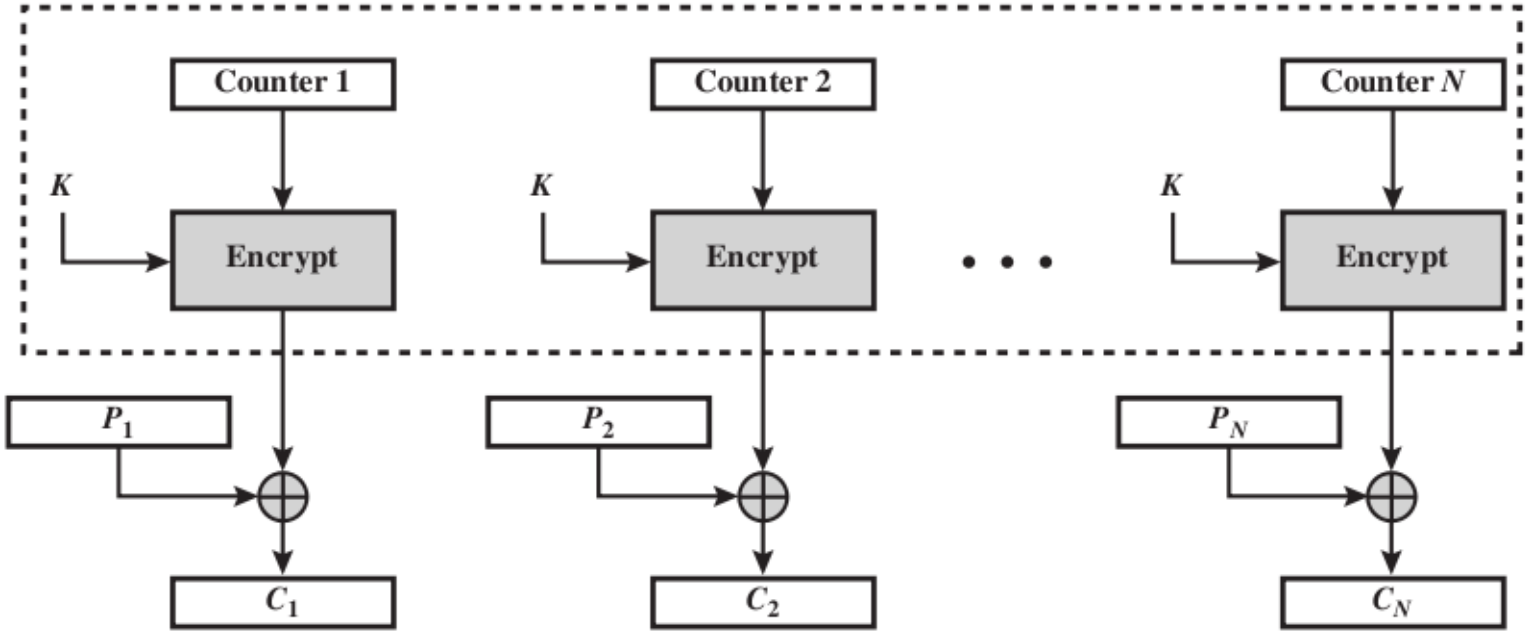
Output Feedback Mode

Counter Mode (CTR)

Feedback Characteristics of Modes

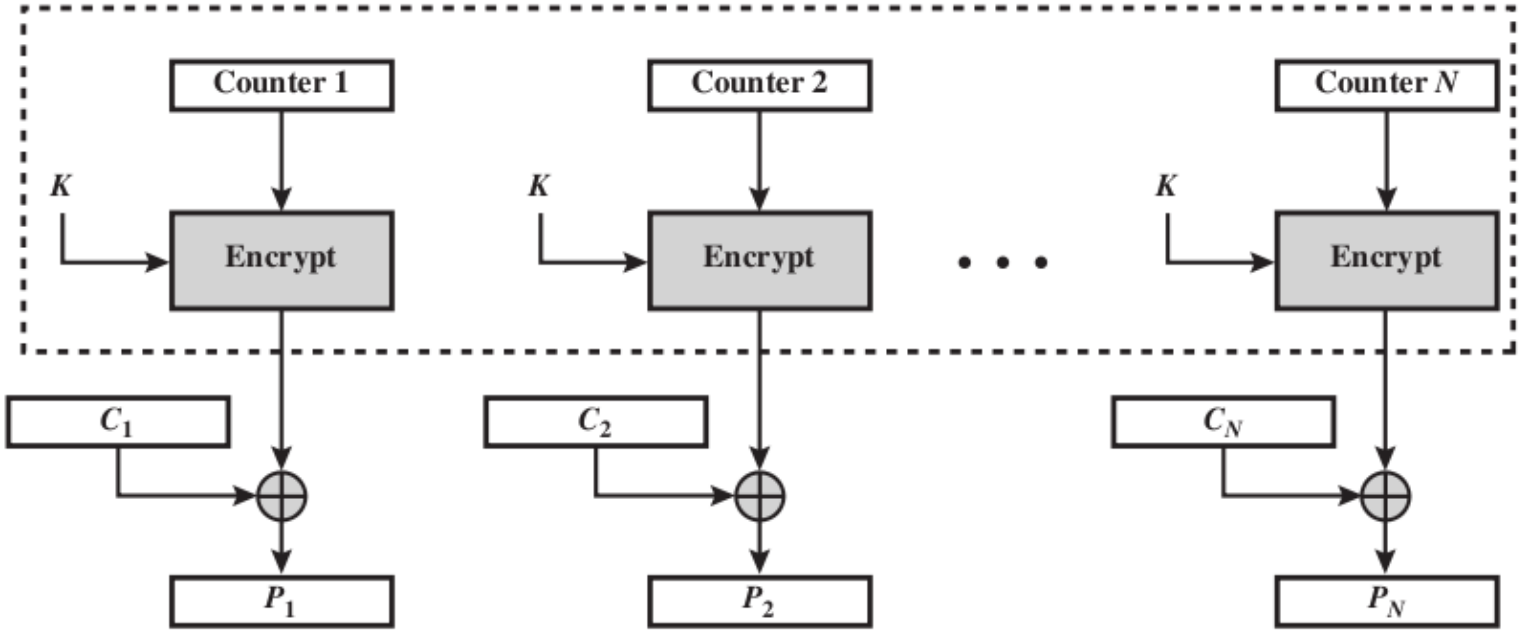
XTS-AES

Counter Mode (CTR) Encryption



- Initial Counter value must be a **nonce**
- All the counter values across all the messages should be **unique**.
- Same key in each block

Counter Mode (CTR) Decryption



CTR Summary

- Converts **block cipher** into **stream cipher**
- Each block of plaintext XORed with encrypted counter
- Typical applications: General-purpose block-oriented transmission; useful for high speed requirements
- Efficient hardware and software implementations
- Simple and secure

Contents

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

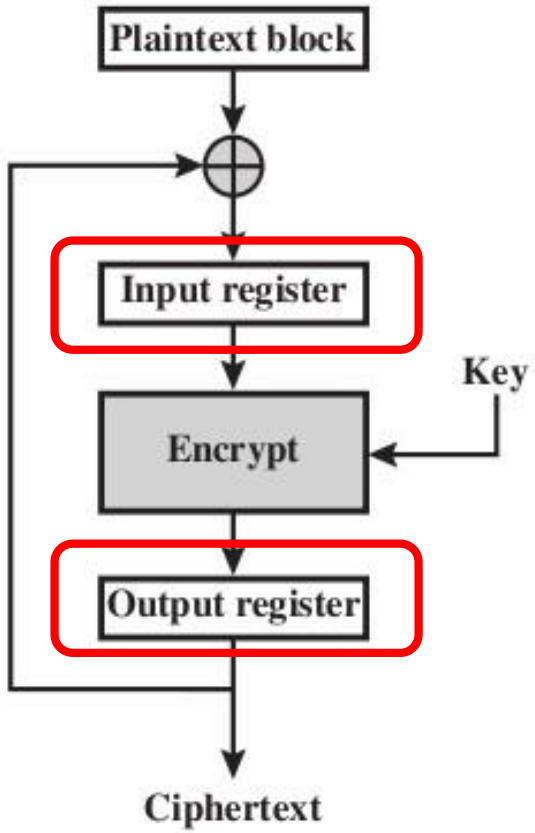
Output Feedback Mode

Counter Mode

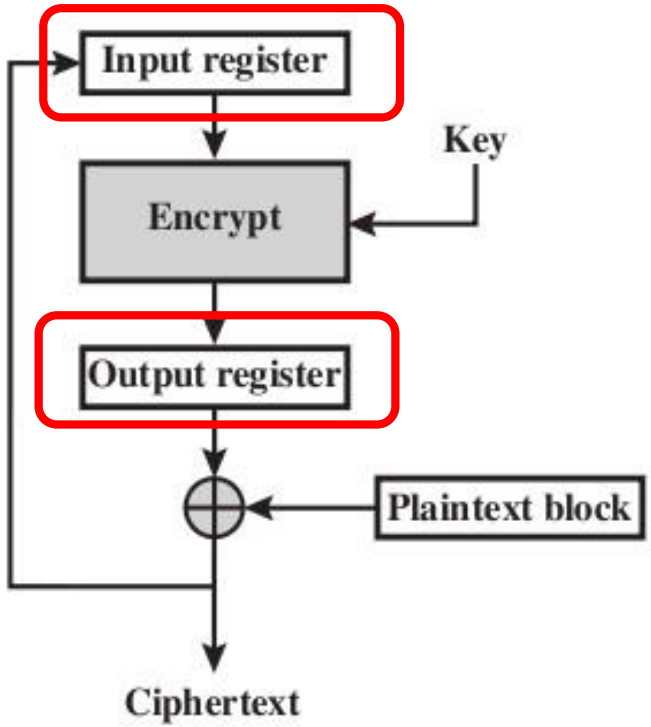
Feedback Characteristics of Modes

XTS-AES

Feedback: CBC and CFB

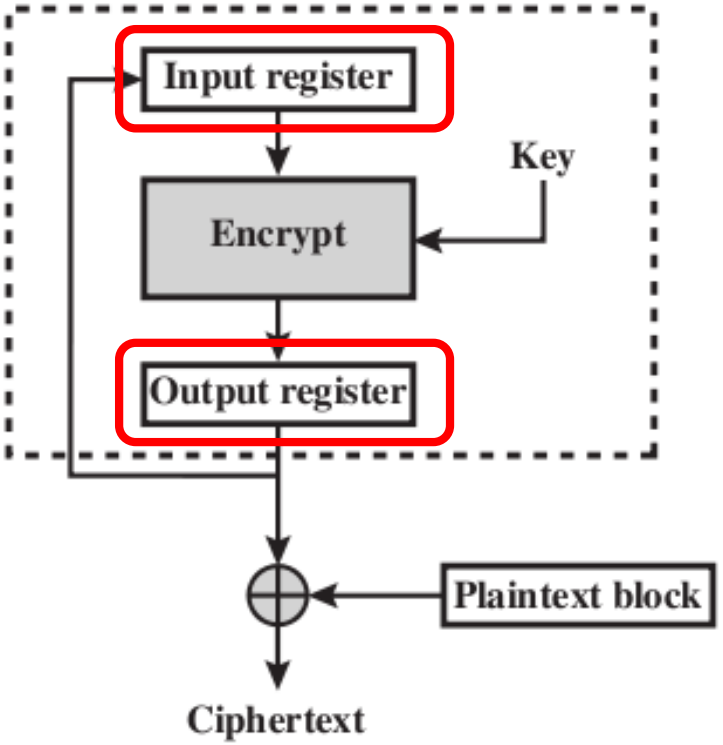


(a) Cipher block chaining (CBC) mode

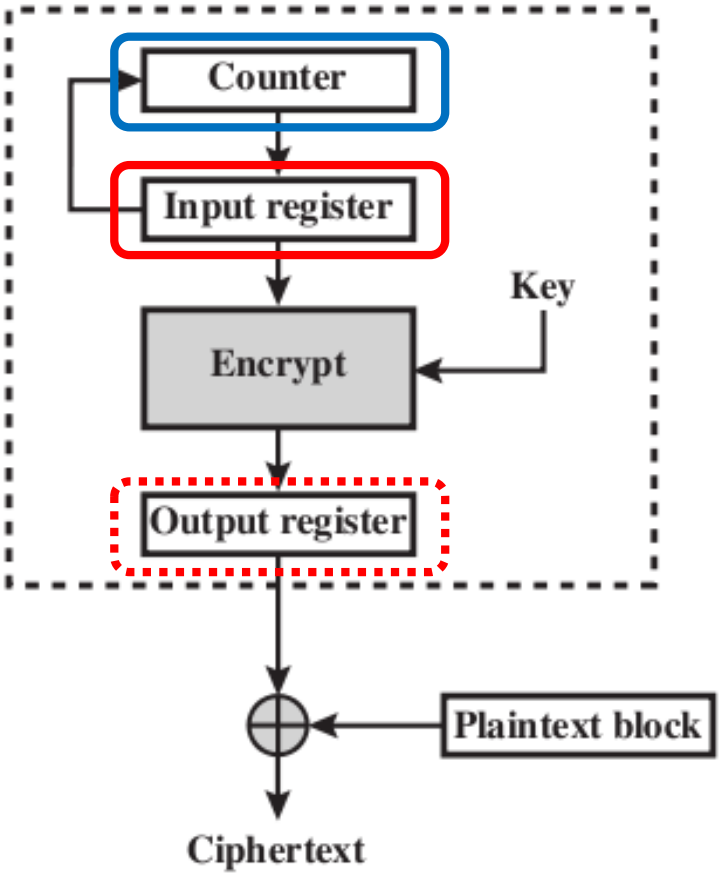


(b) Cipher feedback (CFB) mode

Feedback: OFB and CTR



(c) Output feedback (OFB) mode



(d) Counter (CTR) mode

Modes
ECB
CBC
CFB
OFB
CTR
Feedback
XTS-AES

Contents

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

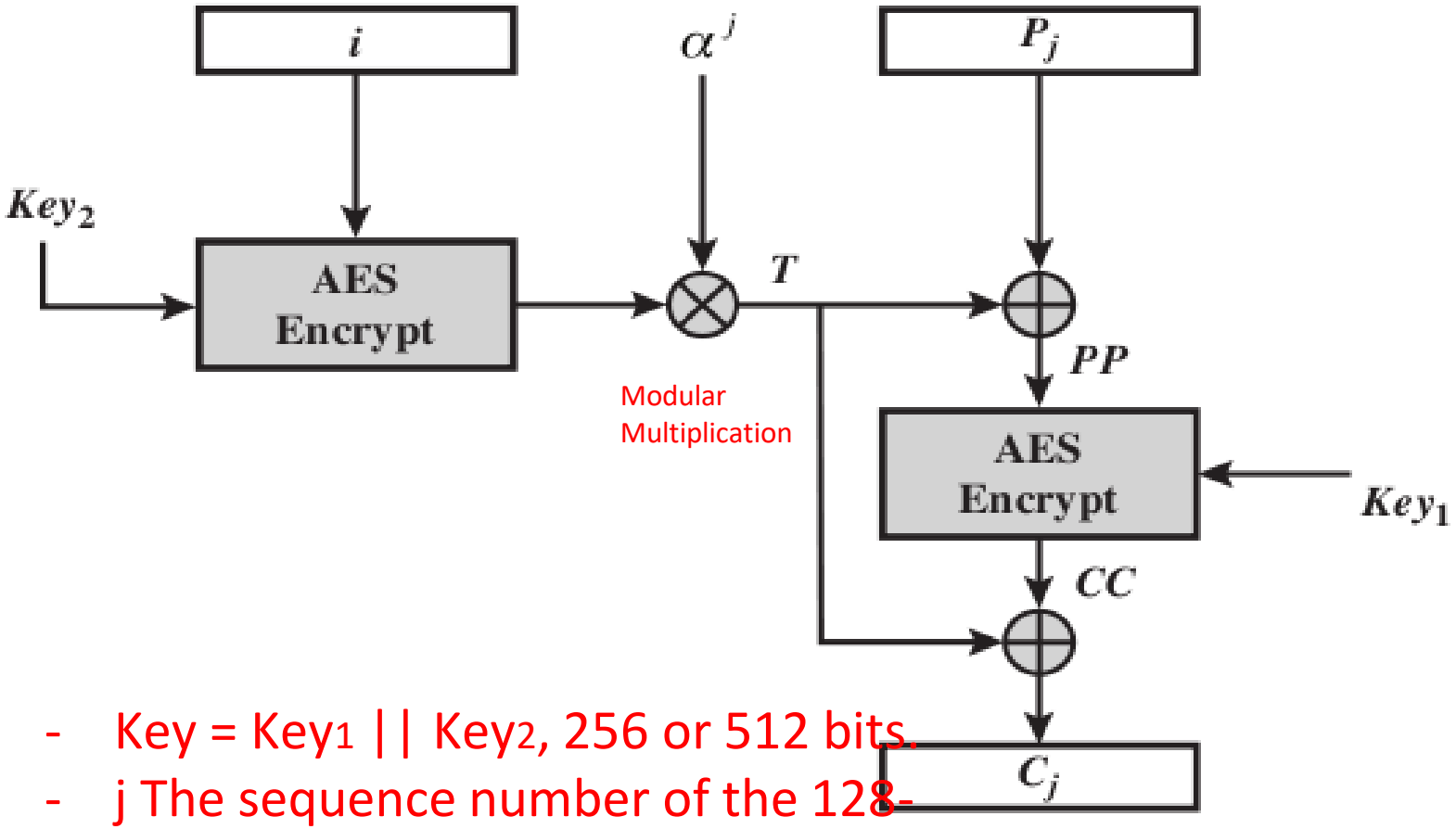
Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

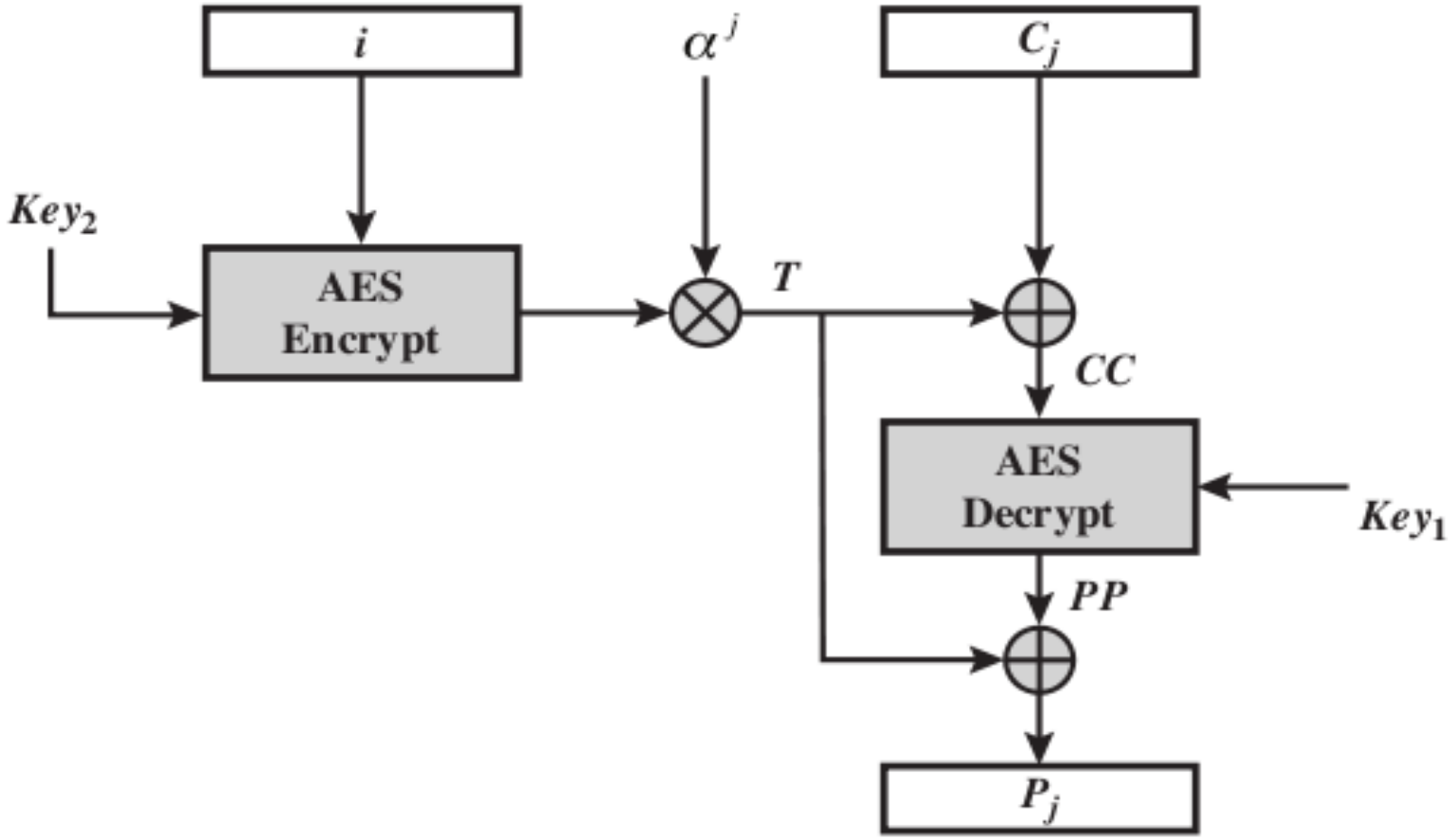
XTS-AES

XTS-AES Encryption of Single Block



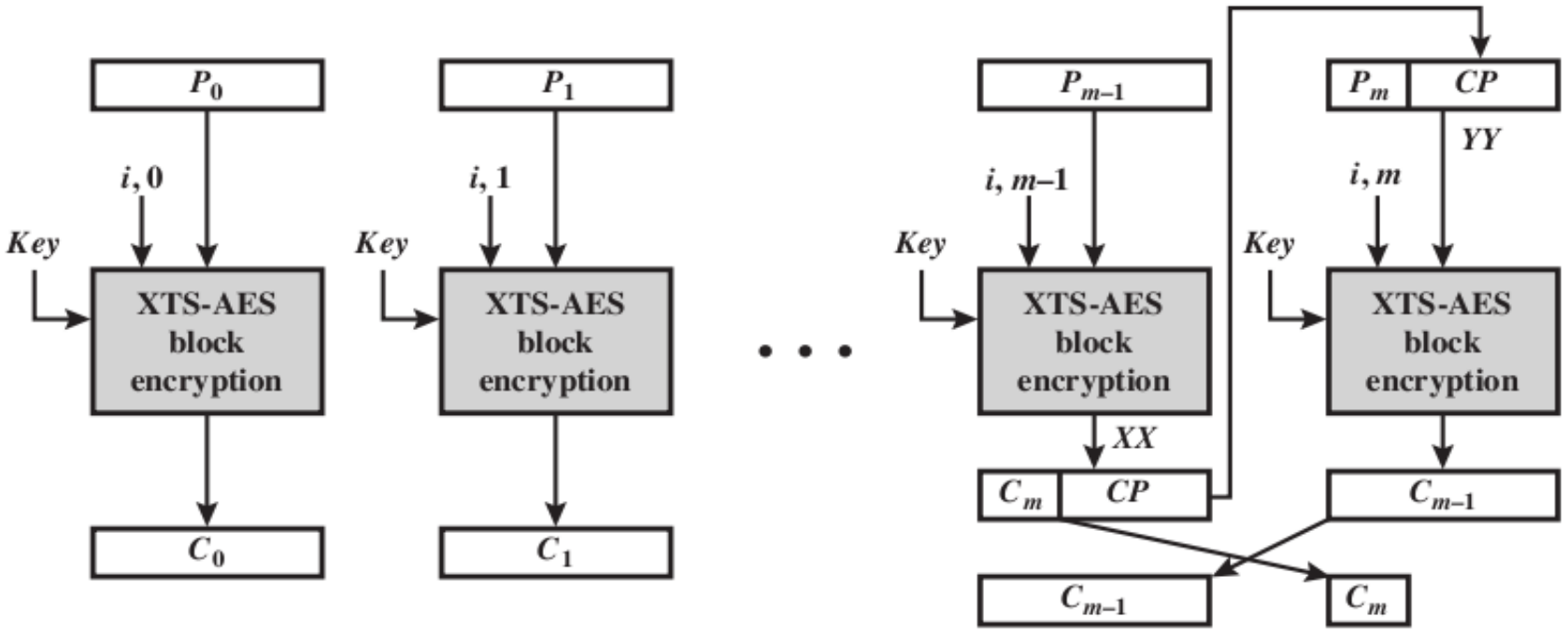
- Key = Key_1 || Key_2, 256 or 512 bits.
- j The sequence number of the 128-bit block.
- P_j The jth block of plaintext
- i The value of the 128-bit tweak; a nonnegative integer.

XTS-AES Decryption of Single Block

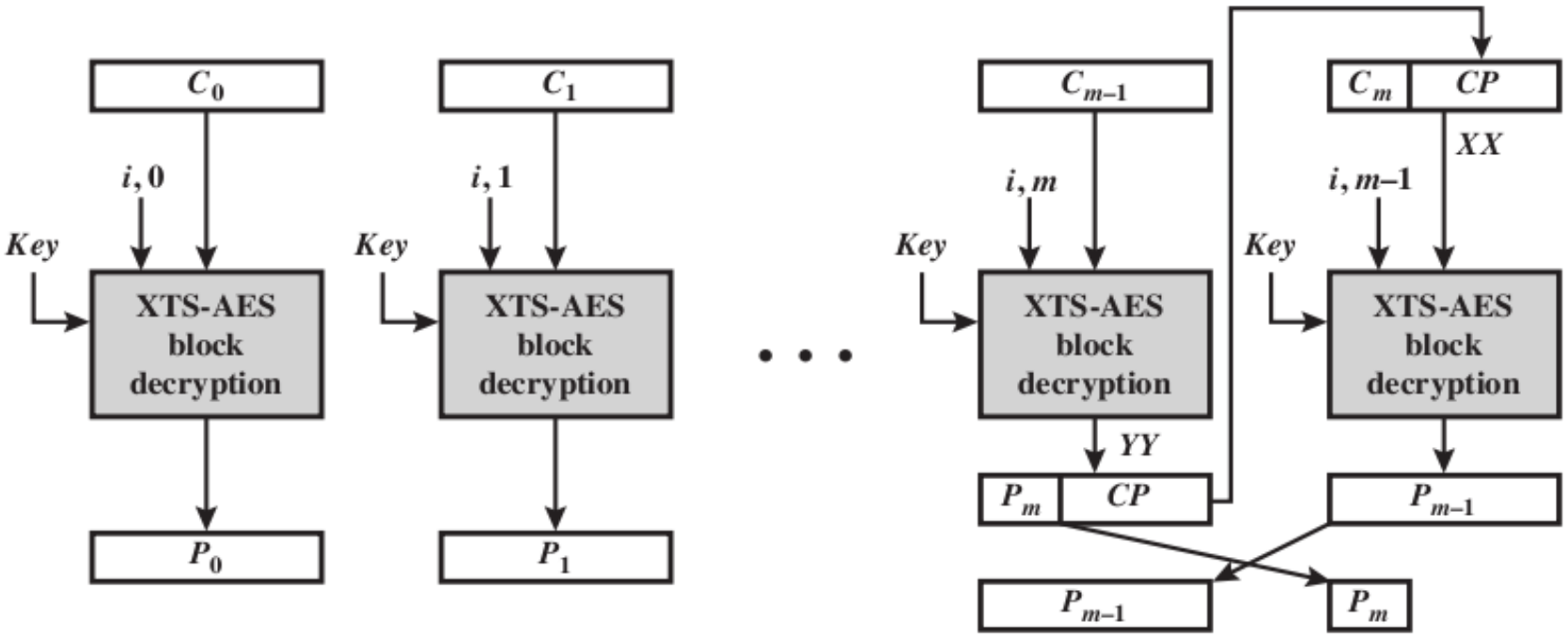


Prove: Decrypted P = Plaintext P?

XTS-AES Encryption



XTS-AES Decryption



Encryption for Stored Data

- XTS-AES designed for encrypting stored data (as opposed to transmitted data)

- The P1619 standard was designed to specify the requirement for encrypting stored data.

  "data at rest" differ somewhat from those for transmitted data.

Storage Encryption Requirements

- The **ciphertext** is freely available for an attacker.
- The data layout is not changed on the storage medium and in transit. The encrypted data must be the same size as the plaintext data.
- **Data** are assessed in fixed sized blocks, independently from each other.
- Encryption is performed in 16-byte blocks, independently from other blocks.
- There are no other metadata used, except the location of the data blocks within the whole data set.
- The same plaintext is encrypted to different ciphertexts at different locations, but always to the same ciphertext when written to the same location again.
- A standard conformant device can be constructed for decryption of data encrypted by another standard conformant device.