Block Cipher Operation

CSS322: Security and Cryptography

Sirindhorn International Institute of Technology
Thammasat University

1

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

2

CSS322

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

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

CSS322

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

Contents

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode
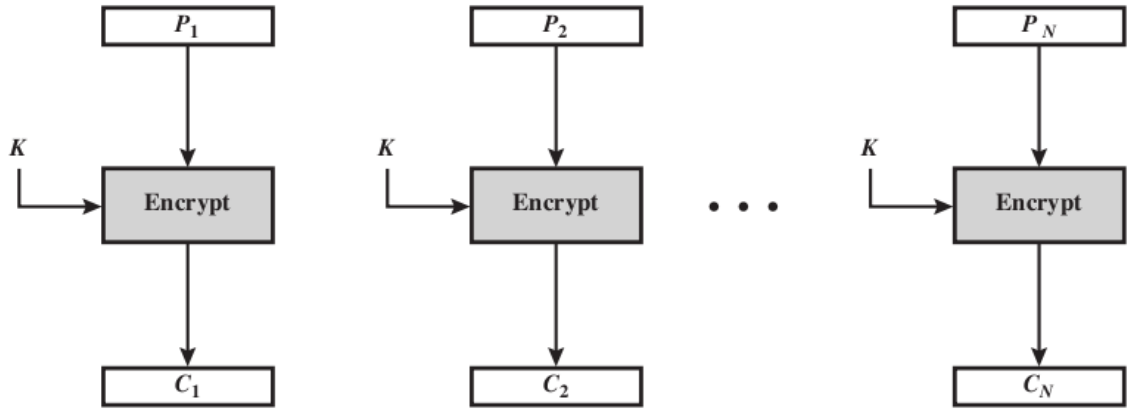
Cipher Feedback Mode

Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes
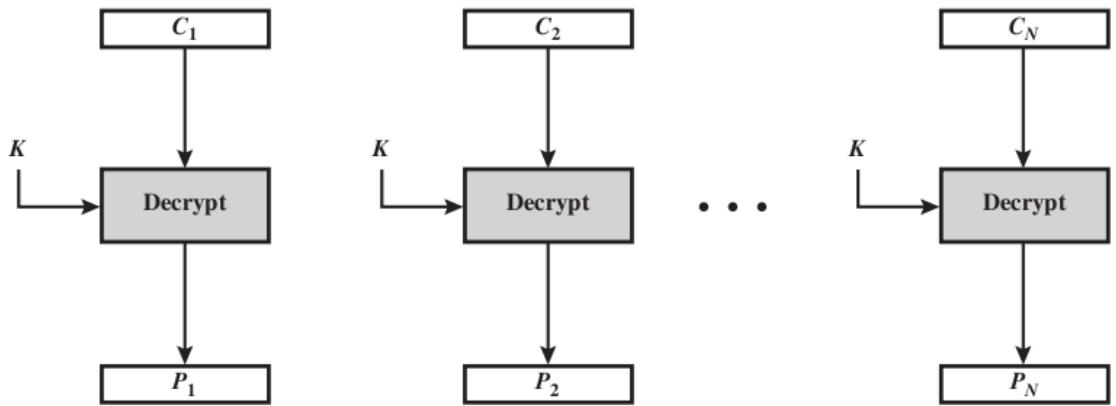
XTS-AES

ECB Encryption

ECB Decryption

CSS322

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

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

7

CSS322

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

Contents

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode
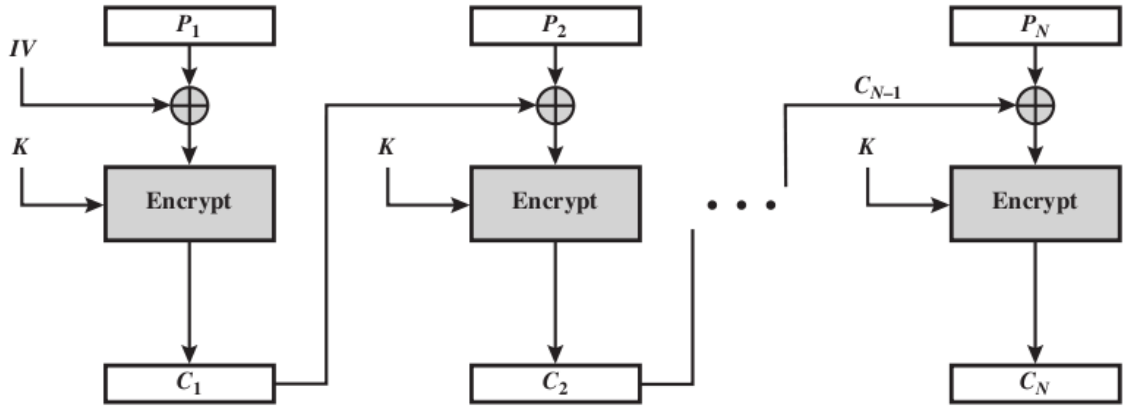
Cipher Feedback Mode

Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

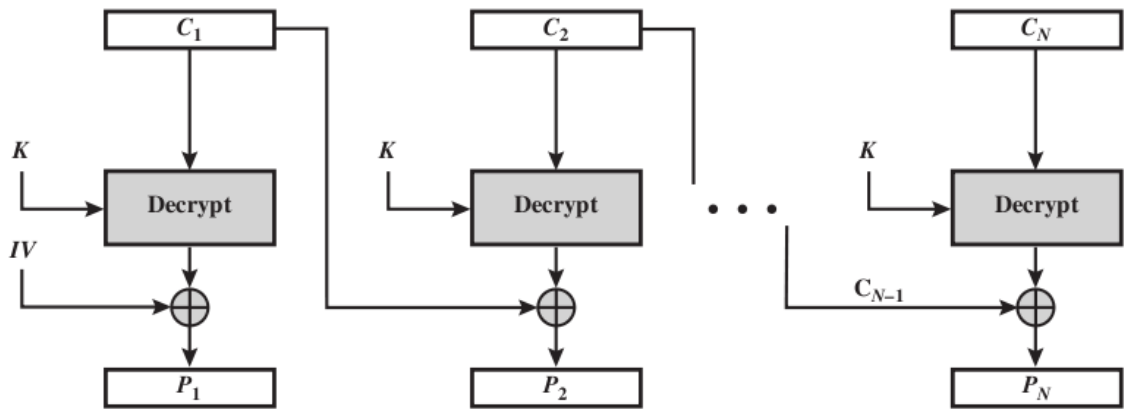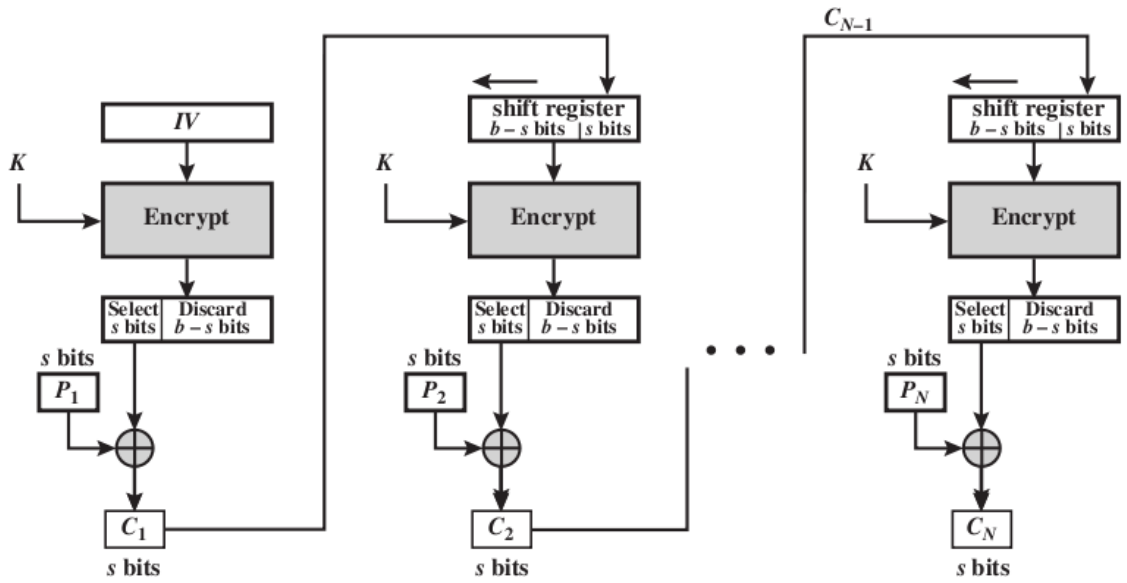XTS-AES

CBC Encryption

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

CBC Decryption

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

CSS322

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

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

CSS322

Block Cipher
Operation

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

CFB Encryption

CFB Decryption

CSS322

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES
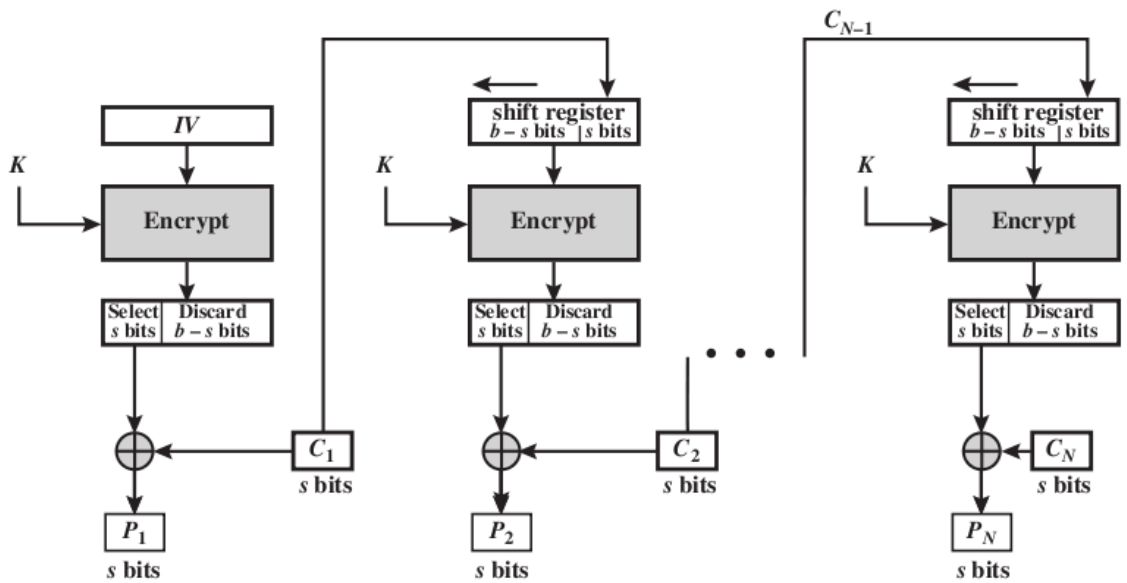
CFB Summary

- ▶ 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

CSS322

Block Cipher
Operation

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
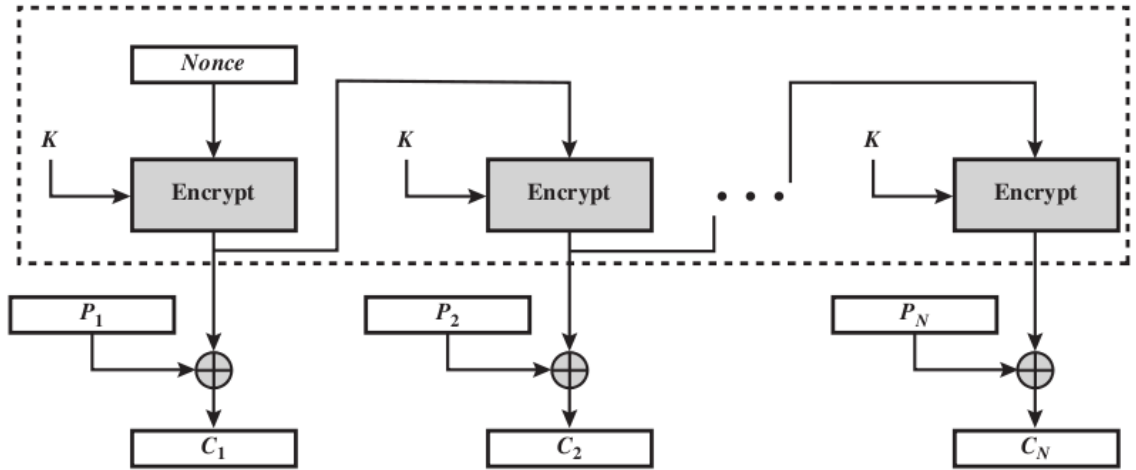
Counter Mode

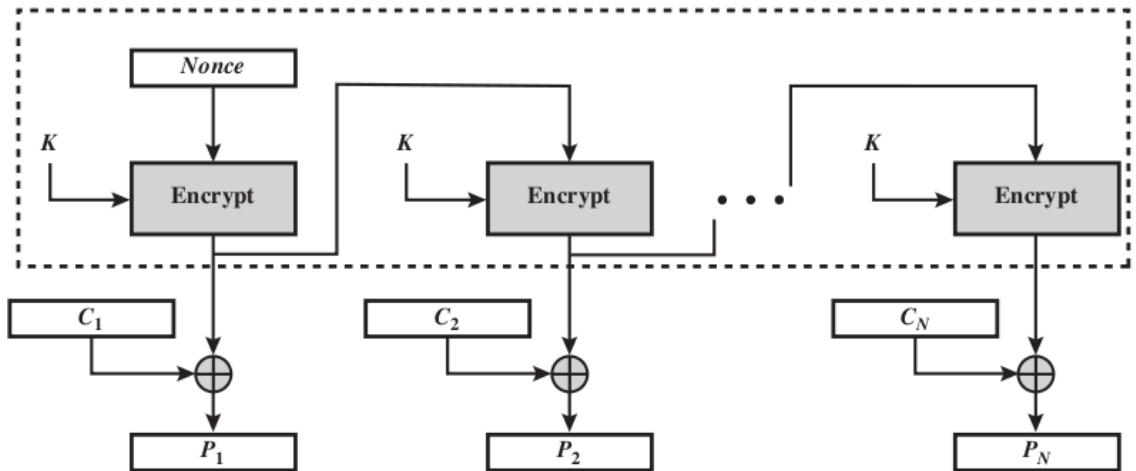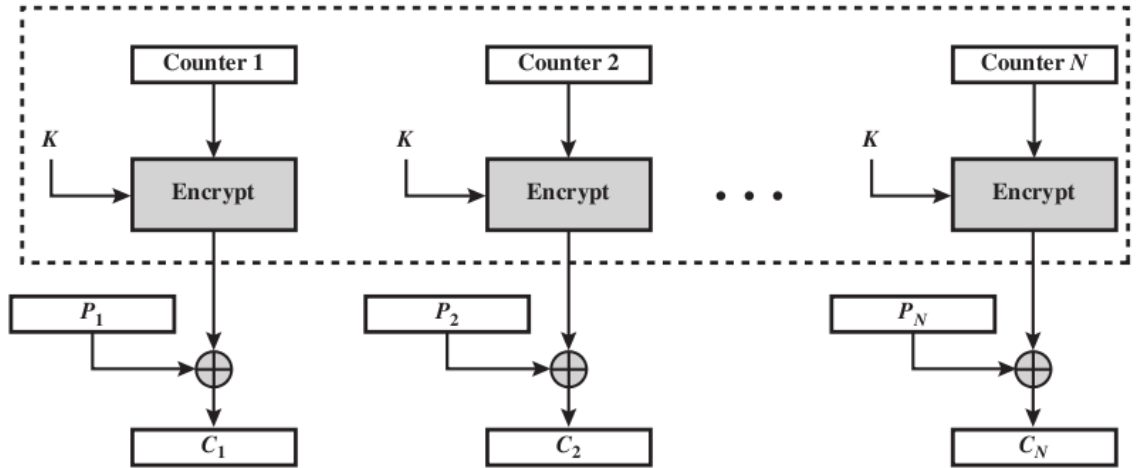Feedback Characteristics of Modes

XTS-AES

CSS322

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

OFB Encryption

CSS322

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

OFB Decryption

CSS322

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

OFB Summary

- ▶ Converts block cipher into stream cipher

- ▶ 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 OFB: bit errors do not propagate

- ▶ Disadvantage: more vulnerable to message stream modification attack

CSS322

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

Contents

CTR Encryption

| Counter 1 | Counter 2 | | Counter N |

$K \rightarrow$ Encrypt $\qquad$ $K \rightarrow$ Encrypt $\qquad \bullet\bullet\bullet \qquad$ $K \rightarrow$ Encrypt

$P_1 \rightarrow \oplus \qquad P_2 \rightarrow \oplus \qquad P_N \rightarrow \oplus$

$C_1 \qquad C_2 \qquad C_N$

CTR Decryption

| Counter 1 | Counter 2 | | Counter N |

$K \rightarrow$ Encrypt $\qquad$ $K \rightarrow$ Encrypt $\qquad \bullet\bullet\bullet \qquad$ $K \rightarrow$ Encrypt

$C_1 \rightarrow \oplus \qquad C_2 \rightarrow \oplus \qquad C_N \rightarrow \oplus$

$P_1 \qquad P_2 \qquad P_N$

CSS322

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES
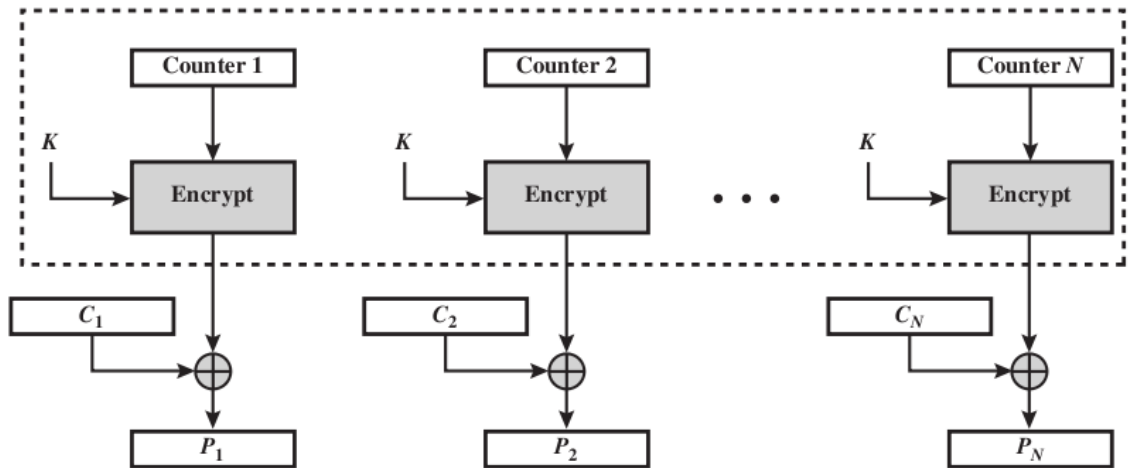
CTR Summary

- ▶ 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

CSS322

Block Cipher
Operation

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

Feedback: CBC and CFB

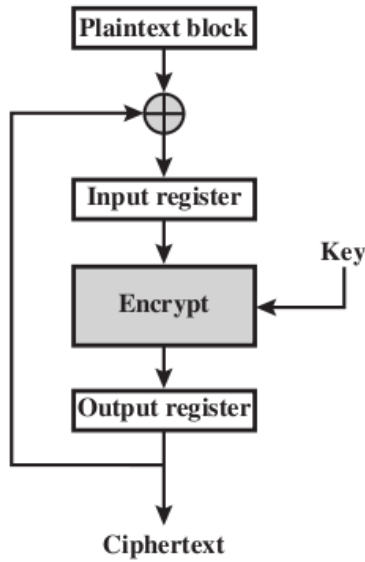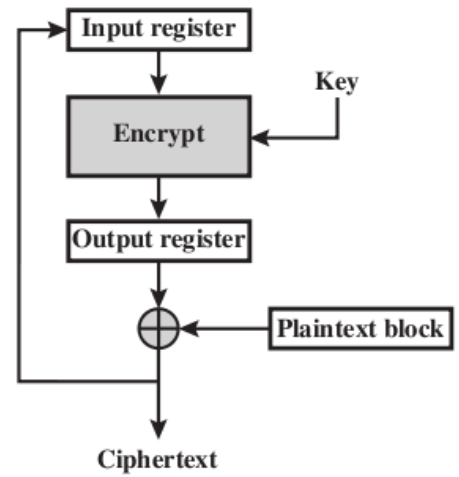Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

(a) Cipher block chaining (CBC) mode

(b) Cipher feedback (CFB) mode

Feedback: OFB and CTR

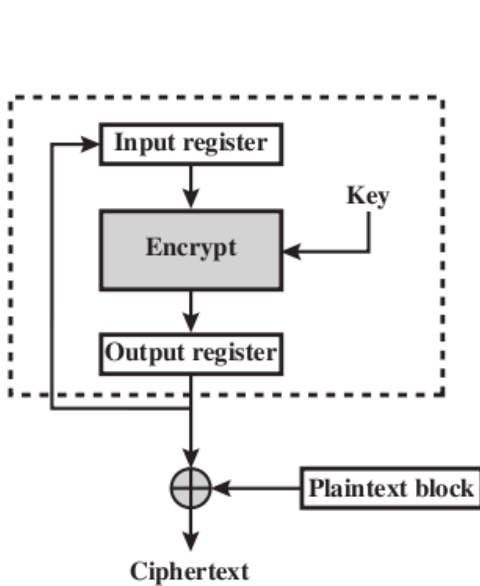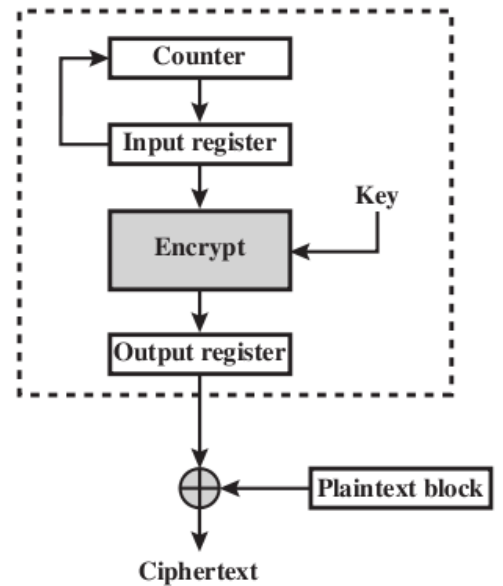Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

(c) Output feedback (OFB) mode

(d) Counter (CTR) mode

CSS322

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

Contents

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

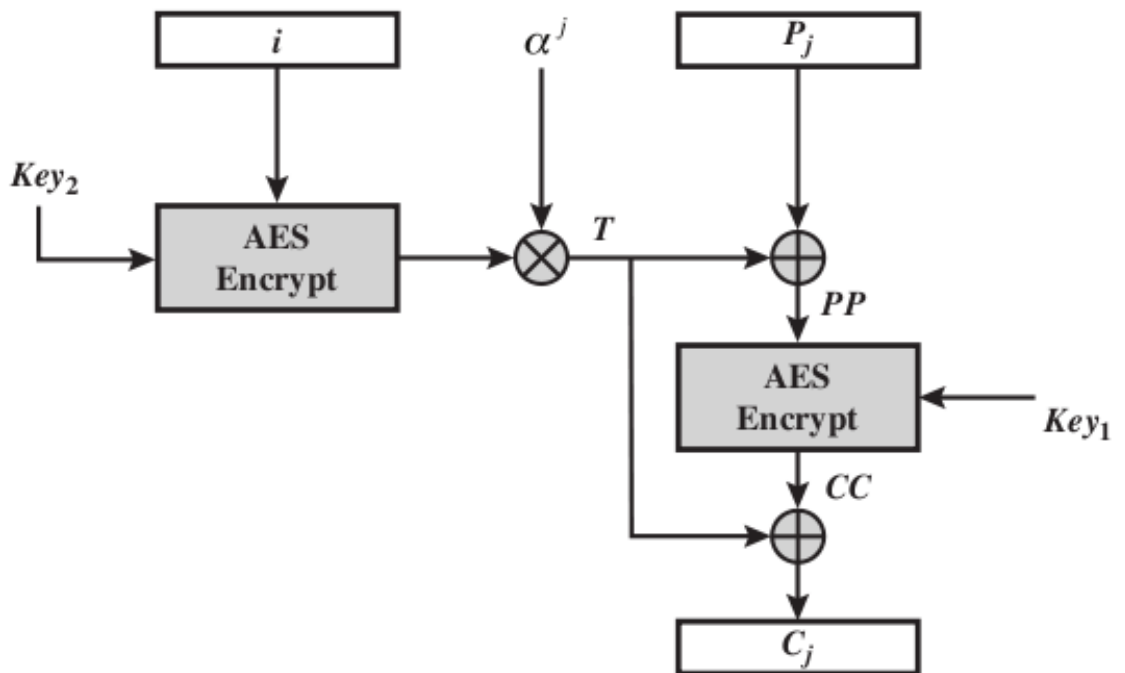Cipher Feedback Mode

Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

XTS-AES

27

CSS322

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

XTS-AES Encryption of Single Block

CSS322

Block Cipher
Operation
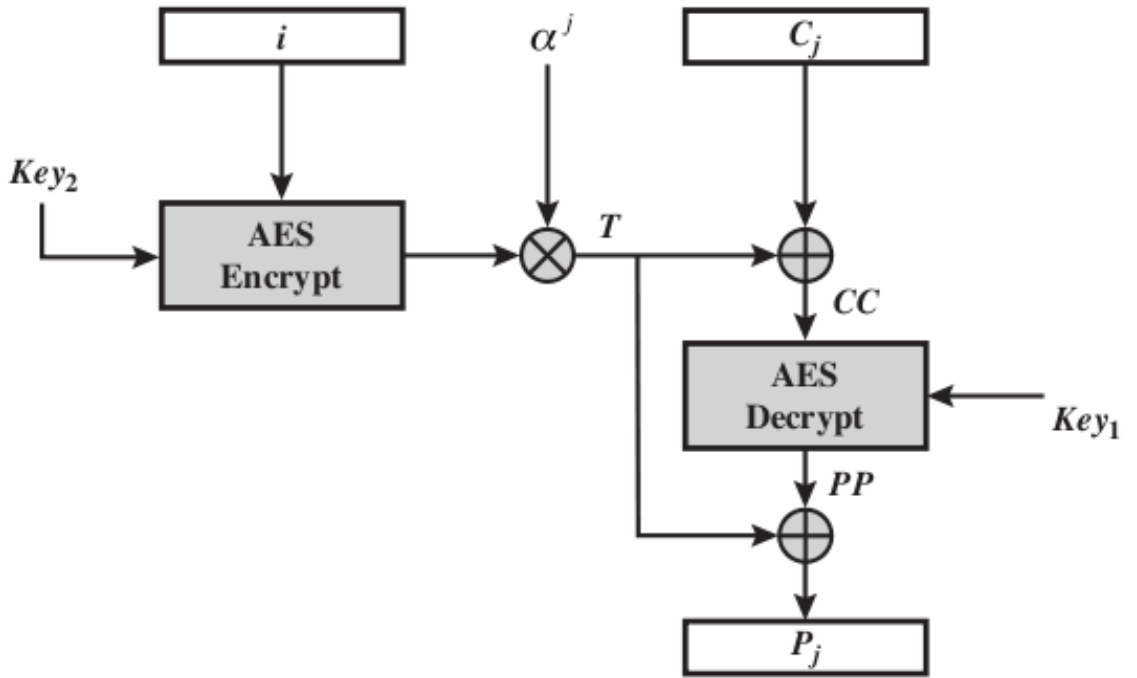
Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

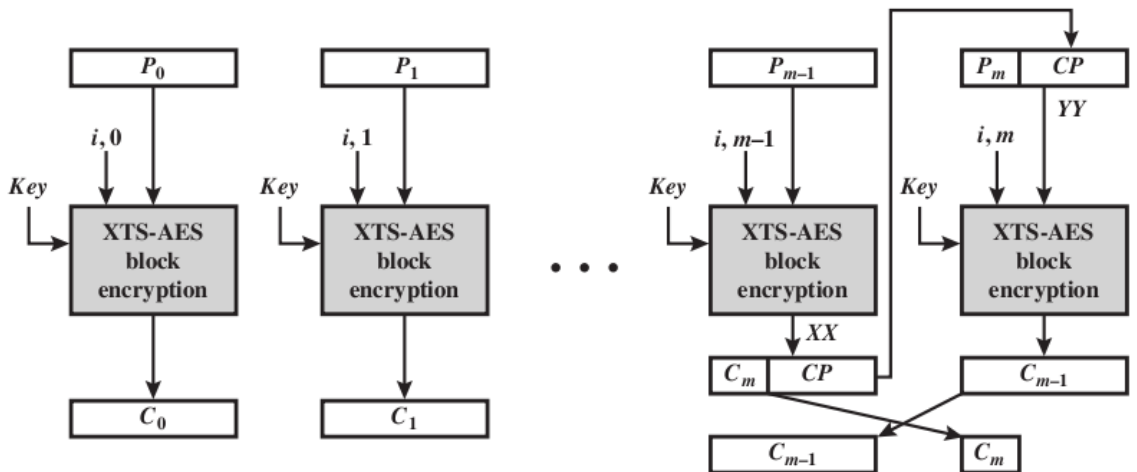# XTS-AES Decryption of Single Block

CSS322

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

XTS-AES Encryption

CSS322

Block Cipher
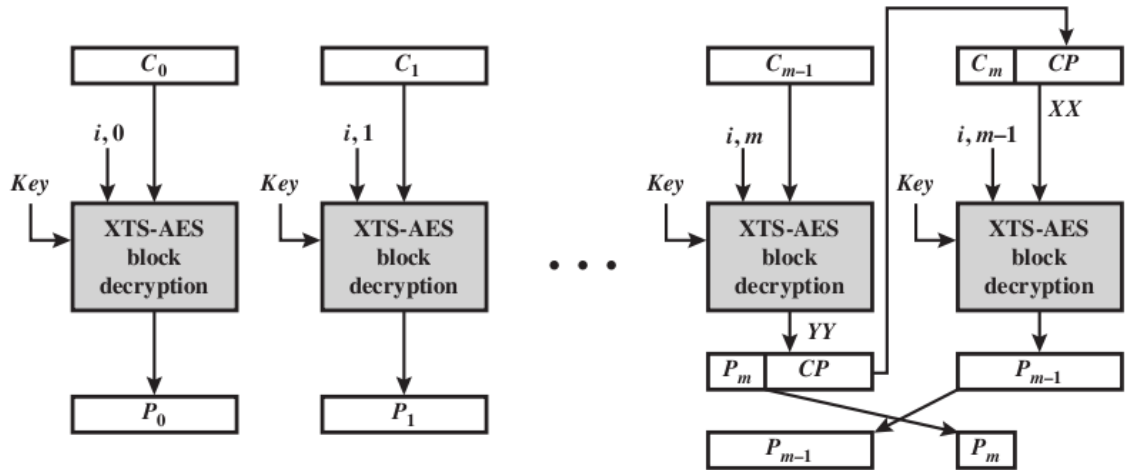Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

XTS-AES Decryption

| C_0 | C_1 | C_{m-1} | C_m | CP |

$i, 0$ $i, 1$ i, m $i, m-1$ XX

Key **XTS-AES block decryption** Key **XTS-AES block decryption**   • • • Key **XTS-AES block decryption** Key **XTS-AES block decryption**

YY

| P_0 | P_1 | P_m | CP | P_{m-1} |

| P_{m-1} | P_m |

31

CSS322

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

Encryption for Stored Data

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

▸ See Chapter 6.7 for details and differences to transmitted data encryption