Block Cipher Operation

CSS322: Security and Cryptography

Sirindhorn International Institute of Technology
Thammasat University

Prepared by Steven Gordon on 28 October 2013
css322y13s2l04, Steve/Courses/2013/s2/css322/lectures/modes.tex, r2963

Contents

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

ECB Encryption

CSS322

Block Cipher
Operation

Modes
ECB
CBC
CFB
OFB
CTR
Feedback
XTS-AES

ECB Decryption

CSS322

Block Cipher
Operation

Modes
ECB
CBC
CFB
OFB
CTR
Feedback
XTS-AES
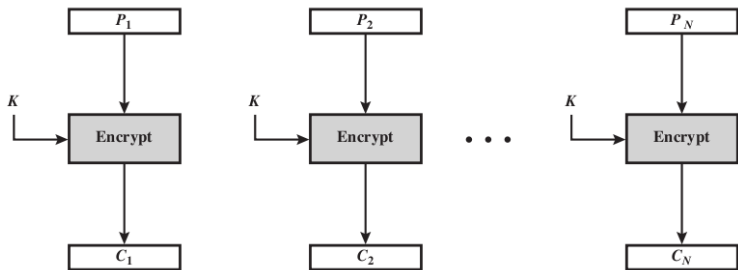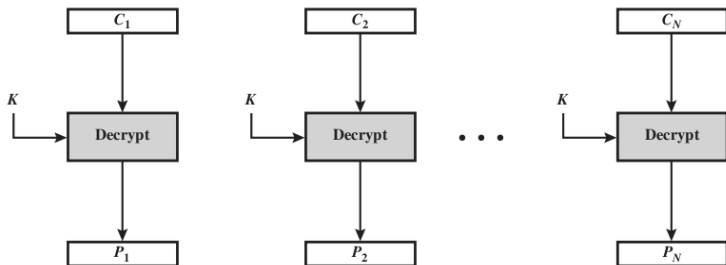
Summary

- 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

CSS322

Block Cipher
Operation

Modes
ECB
CBC
CFB
OFB
CTR
Feedback
XTS-AES
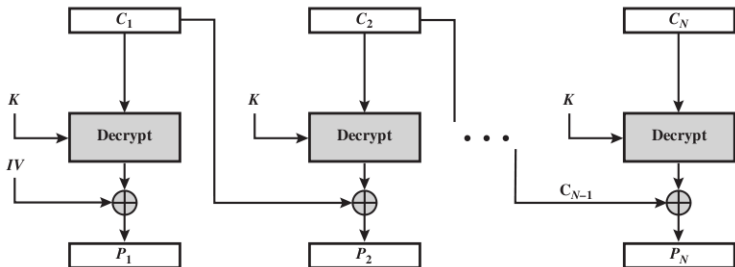
Contents

CBC Encryption

CBC Decryption

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

CSS322

Block Cipher
Operation

Modes

ECB

CBC

CFB

OFB

CTR

Feedback

XTS-AES

CFB Encryption

CFB Decryption

CSS322

Block Cipher
Operation

Modes
ECB
CBC
CFB
OFB
CTR
Feedback
XTS-AES
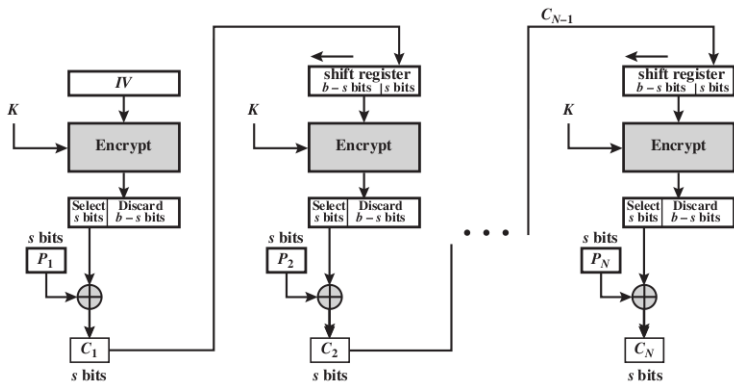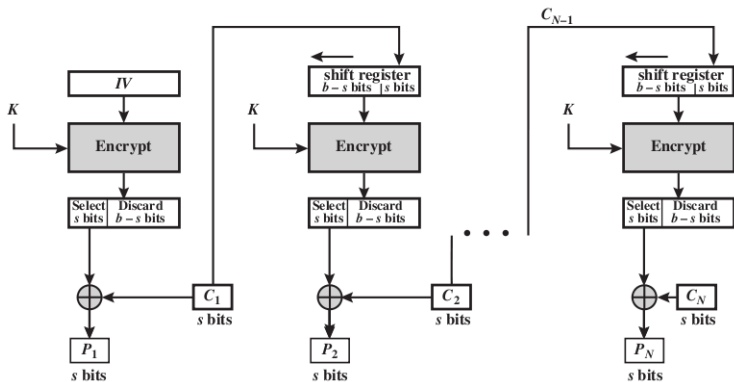
CFB Summary

- ▶ 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

Contents

OFB Encryption

OFB Decryption

CSS322

Block Cipher
Operation

Modes
ECB
CBC
CFB
OFB
CTR
Feedback
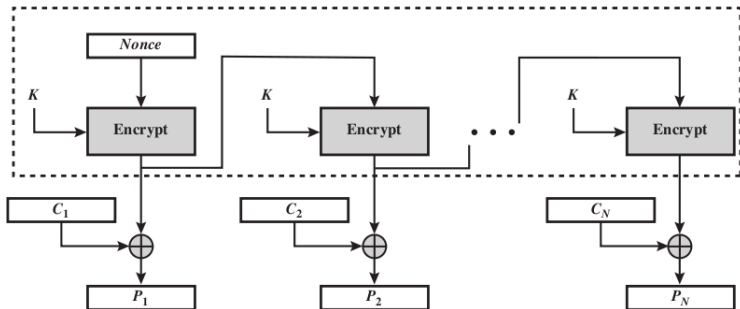XTS-AES
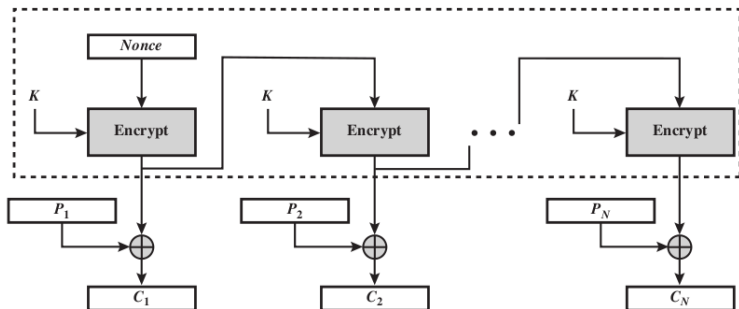
OFB Summary

- ▶ 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
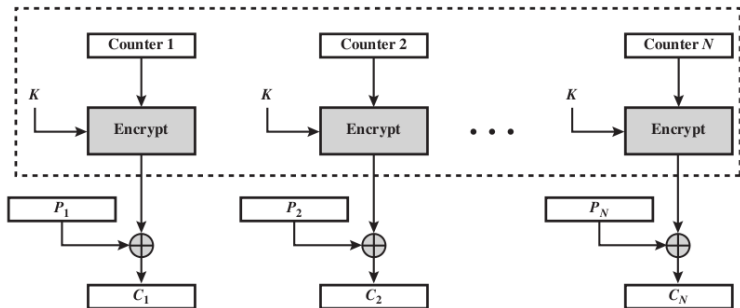
CTR Encryption

CTR Decryption
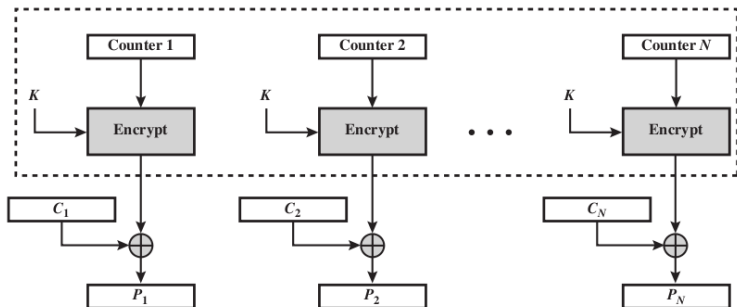
CTR Summary

- 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

CSS322

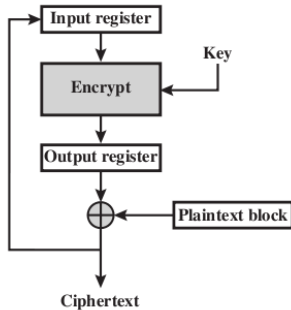Block Cipher
Operation

Modes
ECB
CBC
CFB
OFB
CTR
Feedback
XTS-AES

Contents

Feedback: CBC and CFB

(a) Cipher block chaining (CBC) mode

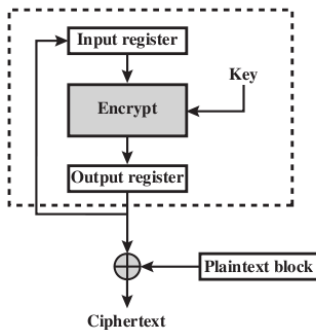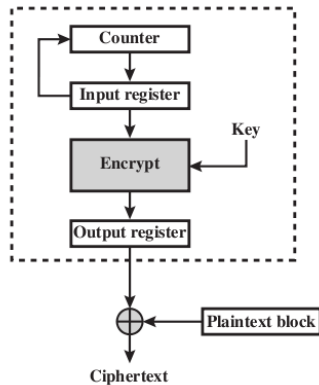(b) Cipher feedback (CFB) mode

Feedback: OFB and CTR

(c) Output feedback (OFB) mode

(d) Counter (CTR) mode

Contents

CSS322

Block Cipher Operation

Modes

ECB

CBC

CFB

OFB

CTR
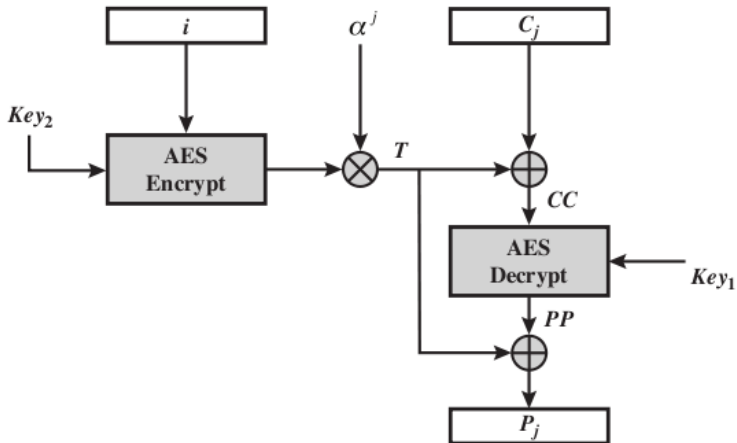
Feedback

XTS-AES
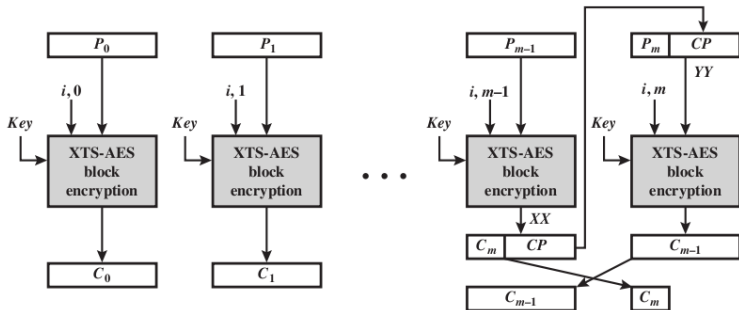
XTS-AES Encryption of Single Block
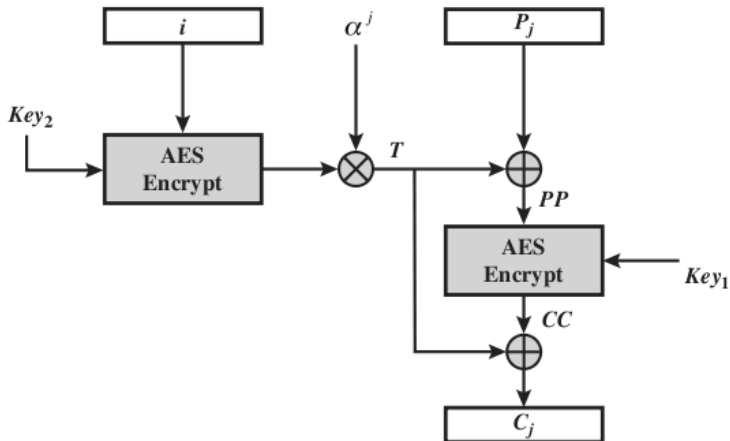
XTS-AES Decryption of Single Block

XTS-AES Encryption

XTS-AES Decryption

CSS322

Block Cipher
Operation

Modes
ECB
CBC
CFB
OFB
CTR
Feedback
XTS-AES
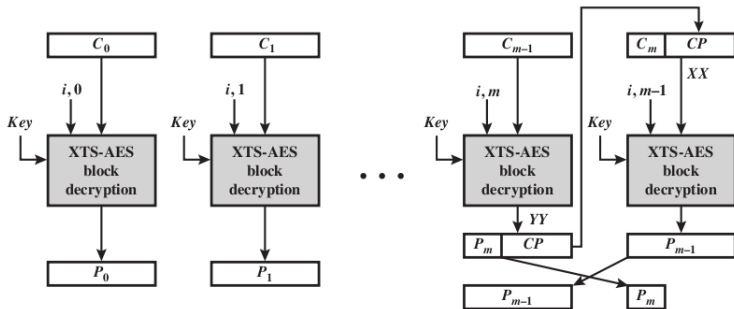
Encryption for Stored Data

- ▶ XTS-AES designed for encrypting stored data (as opposed to transmitted data)
- ▶ See Chapter 6.7 for details and differences to transmitted data encryption