Block Cipher Operation

Modes

ECR.

CBC

CFE

OFE

CTR

Feedback

XTS-AES

Block Cipher Operation

CSS441: Security and Cryptography

Sirindhorn International Institute of Technology
Thammasat University

 $Prepared \ by \ Steven \ Gordon \ on \ 20 \ December \ 2015 \\ css441y15s2l04, \ Steve/Courses/2015/s2/css441/lectures/modes-of-operation.tex, \ r4295$

Contents

Modes

ECE

CBC

CF

CT

-

YTS AF

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

Block Cipher Operation

Modes

ECB

CBO

CFI

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

Block Cipher Operation

ECB

Contents

Electronic Code Book

Block Cipher Operation

Mode

ECB

CD

CEE

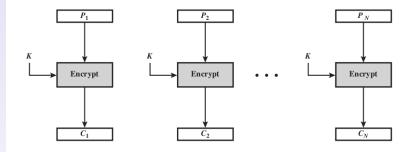
CIL

CIF

Feedbac

XTS-AF

ECB Encryption



Block Cipher Operation

Modes

ECB

CD

CEF

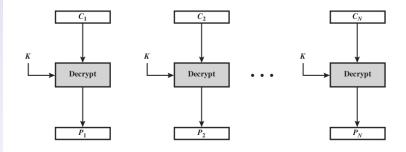
CIL

CIR

Feedbac

XTS_AF

ECB Decryption



Block Cipher Operation

Mode

ECB

СВ

CF

_ ...

VTC AEC

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

Contents

Modes

ECE

CBC

CFI

0.5

СТІ

_

reedbaci

XTS-AES

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

Block Cipher Operation

Modes

ECD

CBC

CEF

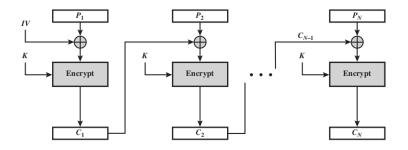
0. .

CTR

Feedbac

XTS-AES

CBC Encryption



Block Cipher Operation

Modes

ECE

CBC

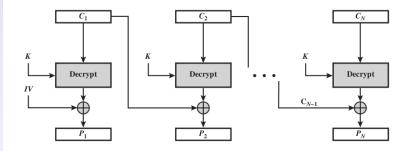
CFF

CIR

Feedbac

XTS-AES

CBC Decryption



Block Cipher Operation

Mode

FCF

CBC

CF

СТІ

Feedbac

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

Contents

Modes

ECE

CBC

CFB

OIL

CIF

геепрас

X I S-AE

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

Block Cipher Operation

Modes

ECR

CPC

CFB

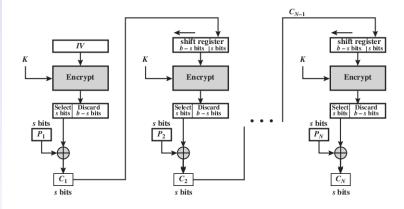
CIL

CIR

Feedbac

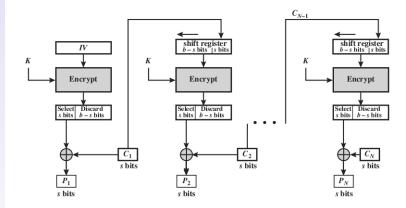
YTS AF

CFB Encryption



CFB

CFB Decryption



Block Cipher Operation

Mode

ECE

СВО

CFB

OF

CTI

Feedbac

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

Output Feedback Mode

Block Cipher Operation

Modes

ECP

CP

CEF

CFB

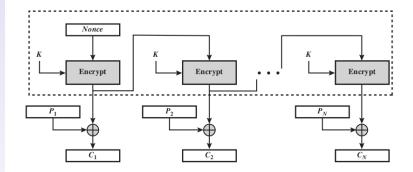
OFB

CTR

Feedbac

XTS-AF

OFB Encryption



Block Cipher Operation

Modes

ECB

CRO

CEF

CFE

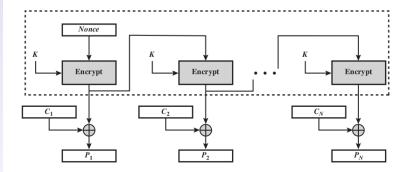
OFB

CTR

Feedbac

XTS-AES

OFB Decryption



Block Cipher Operation

Mode

ECD

CB

CFI

OFB

CTF

Feedbad

XTS-AF

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

Block Cipher Operation

Mode

ECI

CBO

CF

OF

CTR

_ ..

YTC AE

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

Block Cipher Operation

Modes

ECD

CDO

CEE

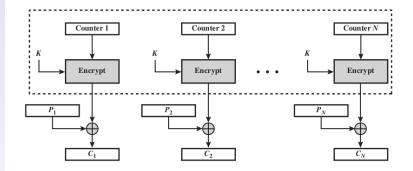
CIL

CTR

Feedbac

XTS-AF

CTR Encryption



Block Cipher Operation

Modes

ECD

CDC

CEL

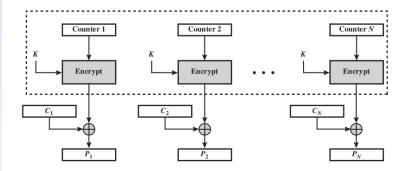
CIL

CTR

Feedbac

YTS AF

CTR Decryption



Block Cipher Operation

Mode

FCF

CBO

CF

__

CTR

E. . . II. . .

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

Mode

ECE

CBC

CFI

OF

CTF

Feedback

XTS-AES

Modes of Operation

Electronic Code Book

Cipher Block Chaining Mode

Cipher Feedback Mode

Output Feedback Mode

Counter Mode

Feedback Characteristics of Modes

Block Cipher Operation

Modes

ECR

CDO

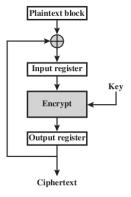
CEL

CIK

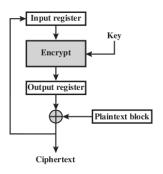
Feedback

XTS-AES

Feedback: CBC and CFB



(a) Cipher block chaining (CBC) mode



(b) Cipher feedback (CFB) mode

Block Cipher Operation

Modes

ECP

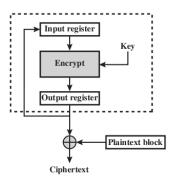
CEF

CIII

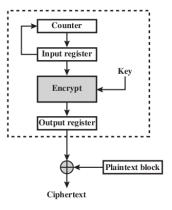
Feedback

XTS-AES

Feedback: OFB and CTR



(c) Output feedback (OFB) mode



(d) Counter (CTR) mode

CSS441 Block Cipher Operation

/lodes

EC

CBO

CF

OF

CIF

VTC A

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

Block Cipher Operation

Mode

ECP

CD/

CEL

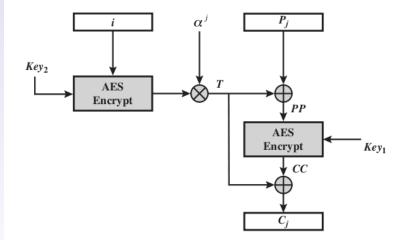
CIL

CTR

Feedbac

XTS-AES

XTS-AES Encryption of Single Block



Block Cipher Operation

Mode

ECD

CDA

CEL

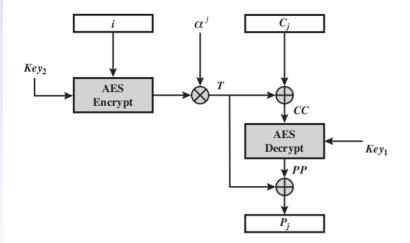
CIL

CTR

Feedback

XTS-AES

XTS-AES Decryption of Single Block



Block Cipher Operation

Modes

ECB

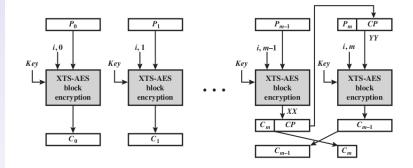
CRO

CEE

CIK

Feedbac





Block Cipher Operation

Modes

ECB

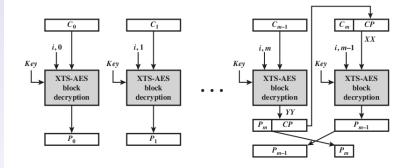
CRO

CFF

CIII

Feedbac





Block Cipher Operation

Mode

ECE

CB

CF

0-

СТІ

Feedbac

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