Comparing Cryptographic Modes of Operation using Flow Diagrams

October 20, 2000

Lyndon G. Pierson

Sandia National Laboratories

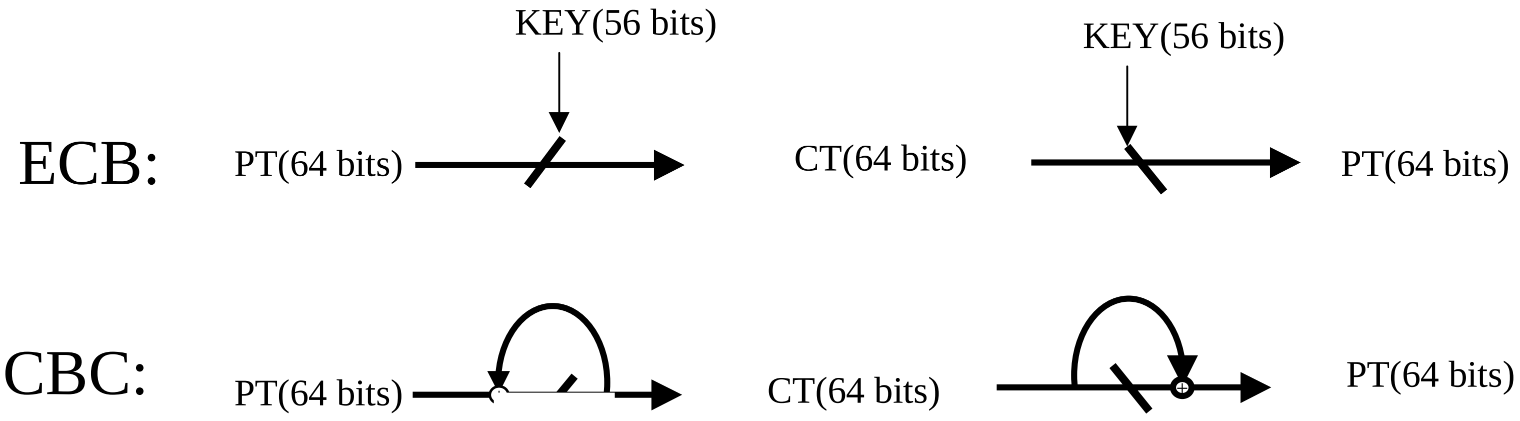
Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under contract DE-AC04-94AL85000.

Simplified Flow Diagrams for study of Cryptographic “Modes of Operation”

- To contrast and understand the major characteristics of standard and proposed standard modes
  - Gloss over some of the fine details such as:
    - Initial Variables
    - Checksum Calculations
    - Key Management/Manipulation Details

Encryption usually involves a Nonlinear “Block Cipher”

- The Nonlinear Block Cipher is depicted here by a “slanted line”: /
- The inverse (Decryption) is depicted by the “opposite slant”: \
- Data flows through the Nonlinear Block Cipher in various “modes of operation”. For example, with DES:



KEY(56 bits)

KEY(56 bits)

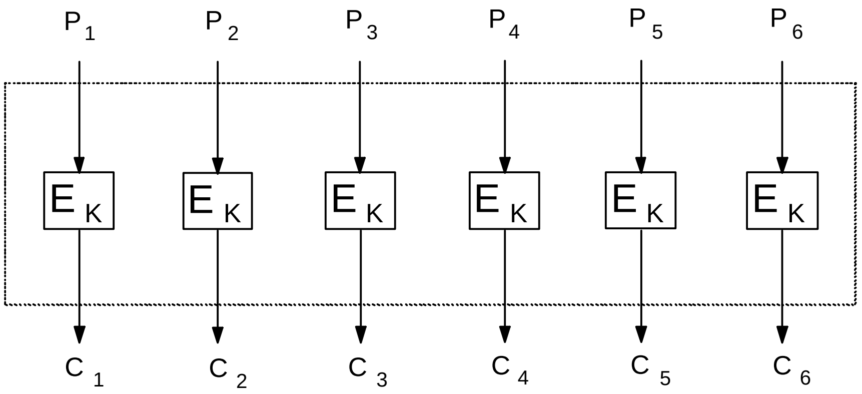
ECB: PT(64 bits) CT(64 bits) PT(64 bits)

CBC: PT(64 bits) CT(64 bits) PT(64 bits)

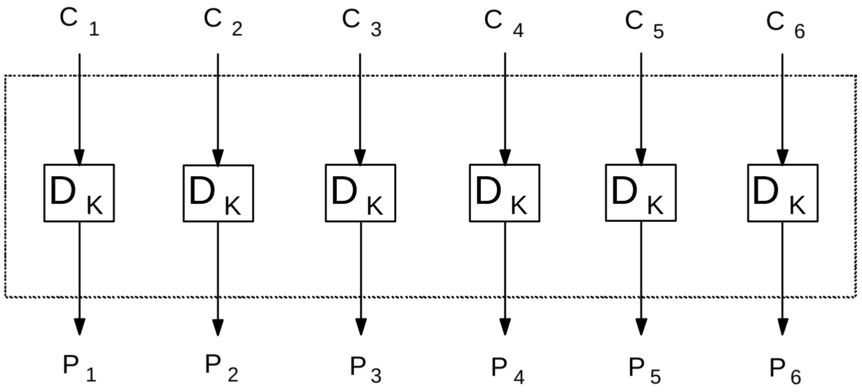
Electronic CodeBook (ECB)

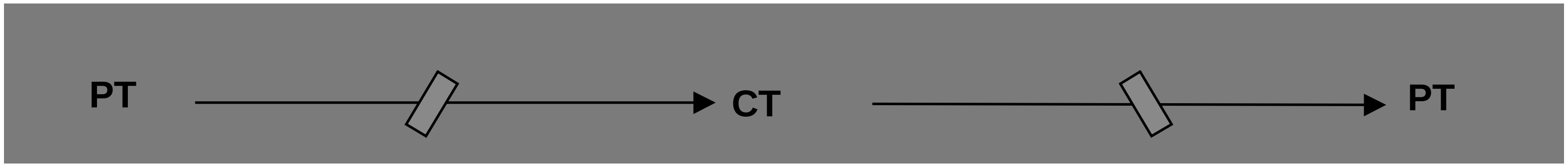
ECB Mode

Encryption


P_1 P_2 P_3 P_4 P_5 P_6
E_K E_K E_K E_K E_K E_K
C_1 C_2 C_3 C_4 C_5 C_6

Decryption

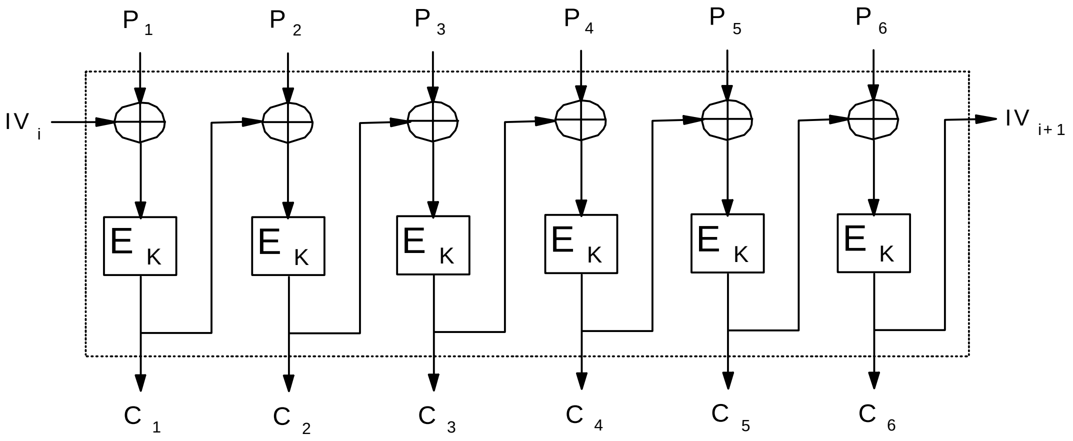

C_1 C_2 C_3 C_4 C_5 C_6
D_K D_K D_K D_K D_K D_K
P_1 P_2 P_3 P_4 P_5 P_6



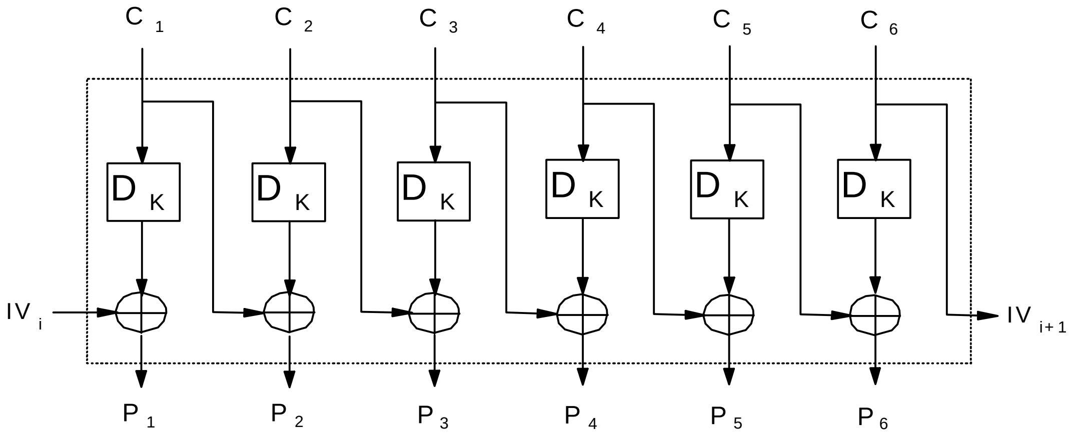
Cipher Block Chaining (CBC)

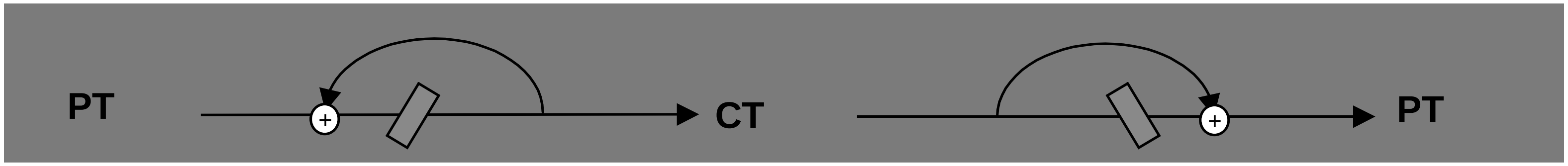
CBC Mode

Encryption


P_1 P_2 P_3 P_4 P_5 P_6
IV_i
IV_{i+1}
E_K
C_1 C_2 C_3 C_4 C_5 C_6

Decryption

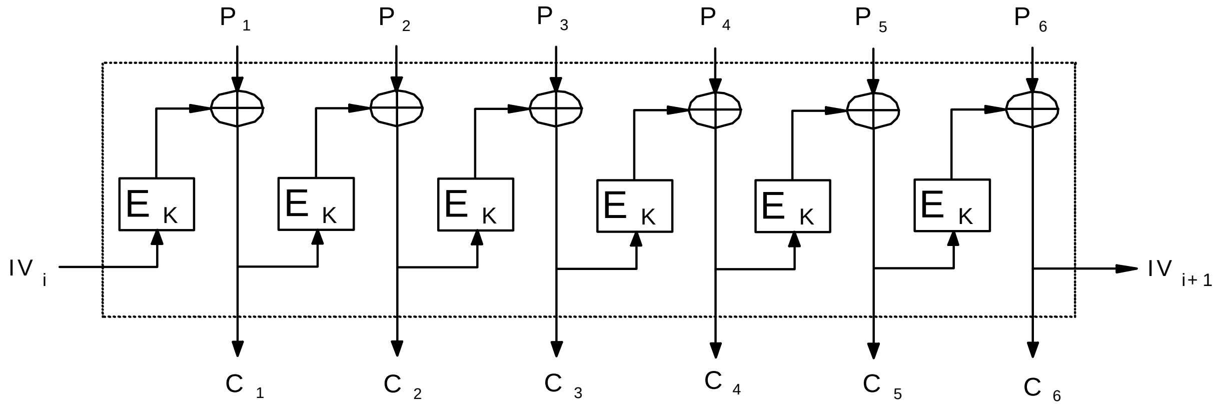

C_1 C_2 C_3 C_4 C_5 C_6
D_K
IV_i
IV_{i+1}
P_1 P_2 P_3 P_4 P_5 P_6



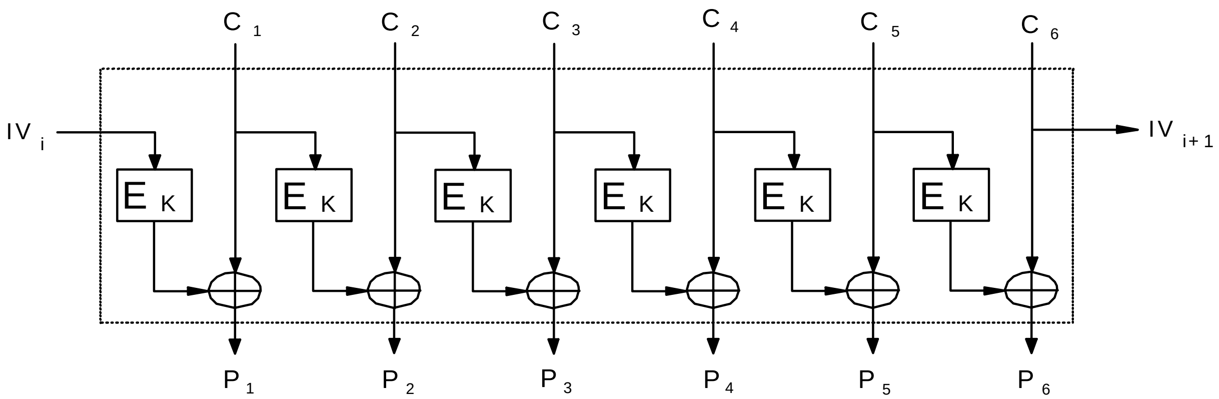
Cipher FeedBack (CFB)

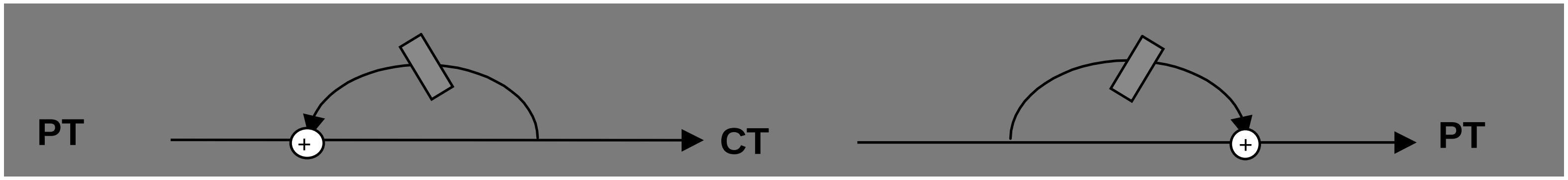
CFB Mode

Encryption

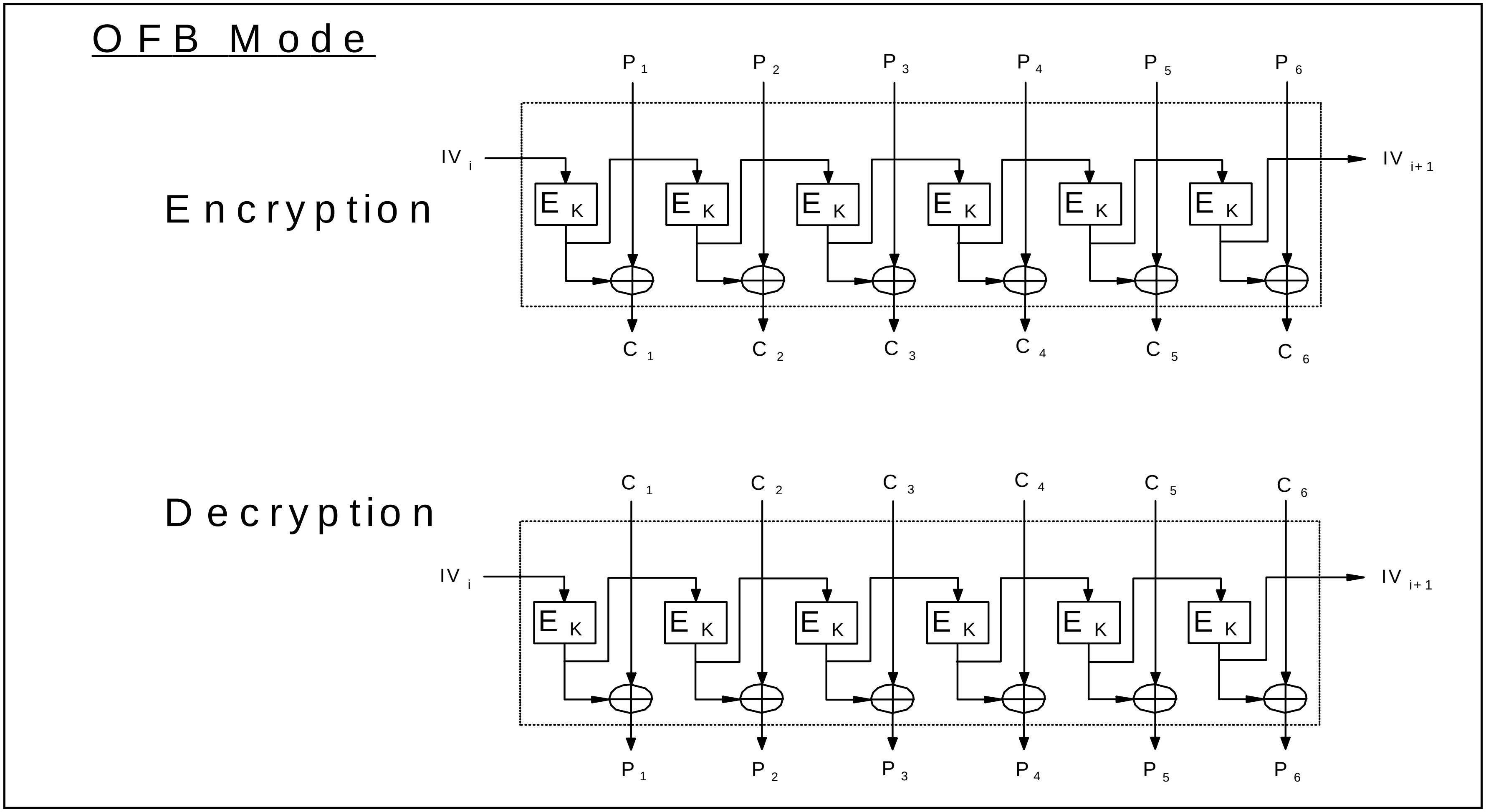


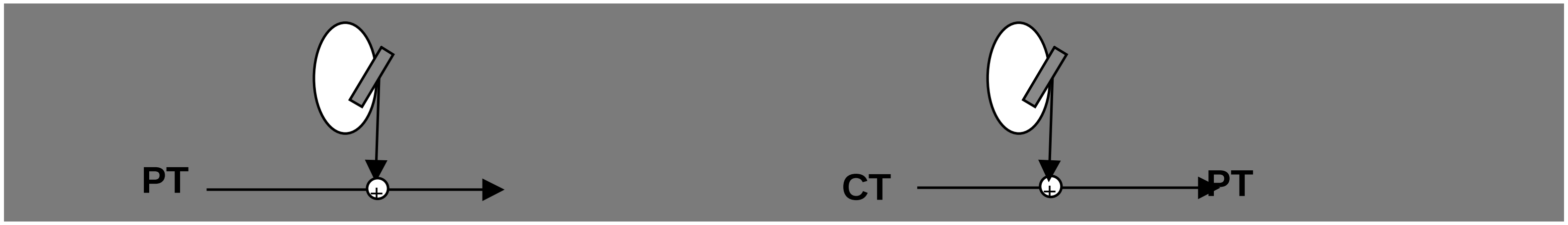
Decryption





Output FeedBack

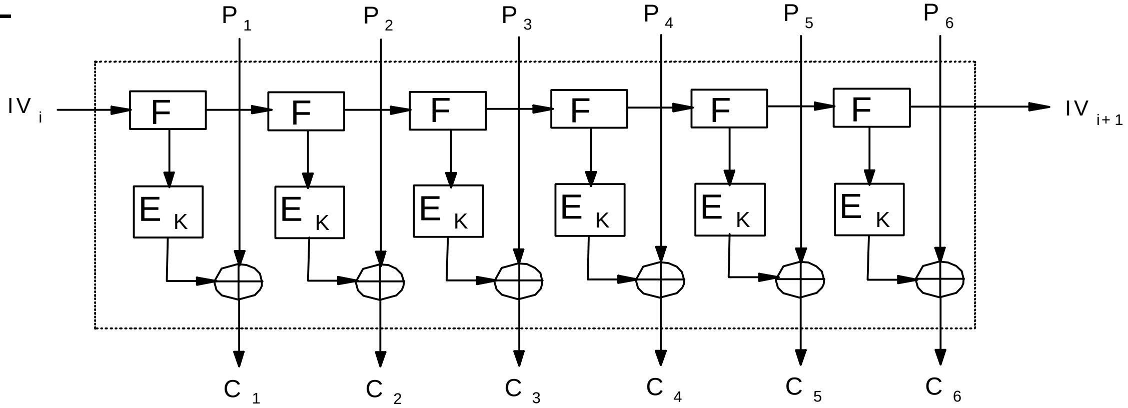




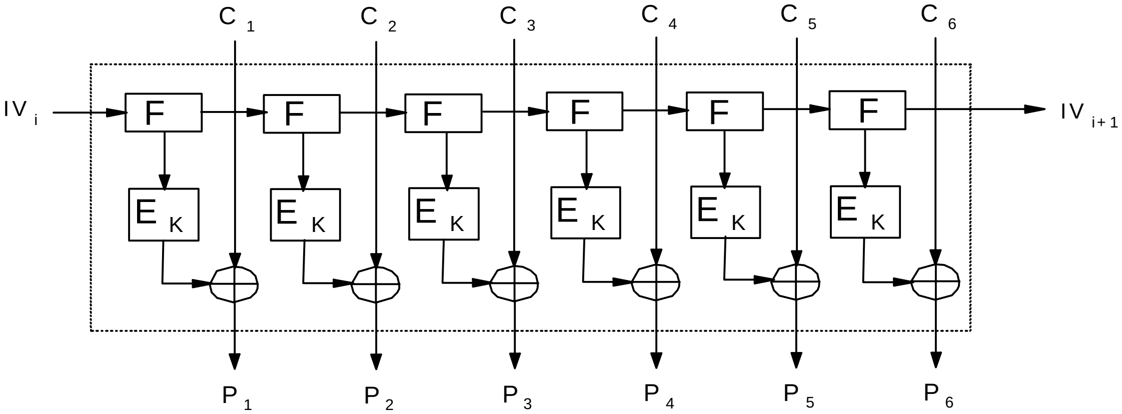
Counter Mode

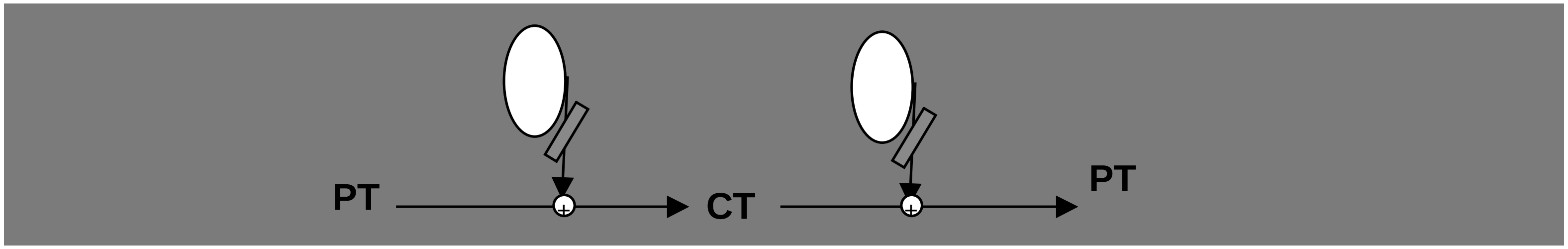
Counter Mode

Encryption

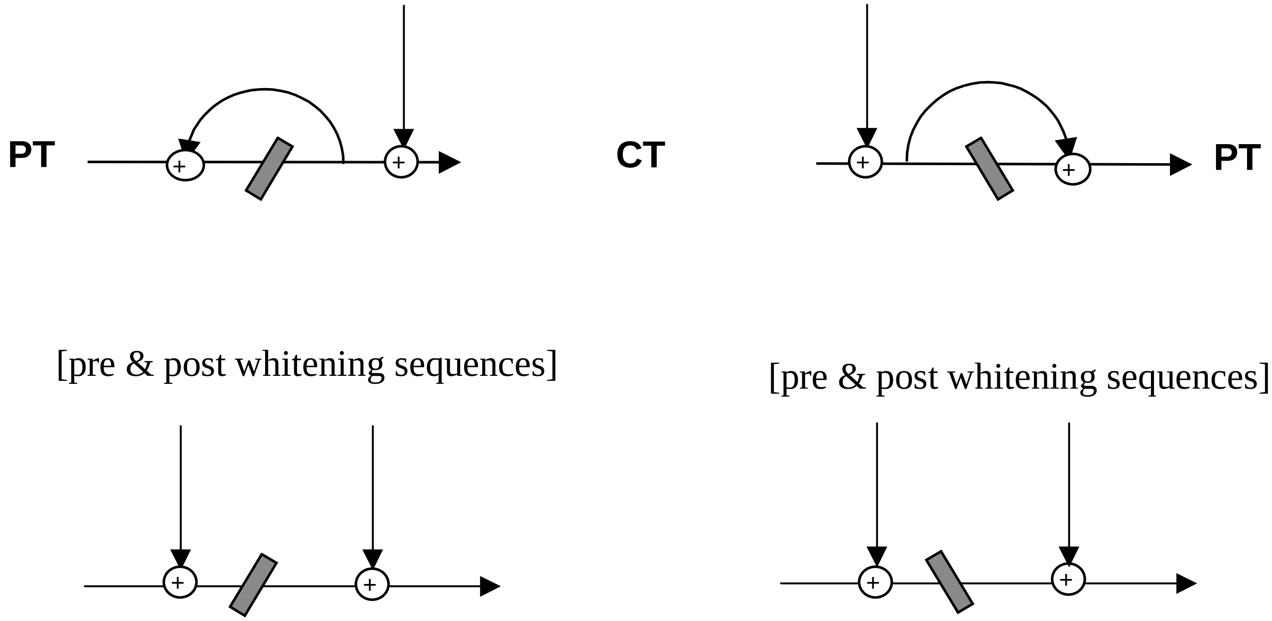


Decryption





“Almost Free Integrity” Modes



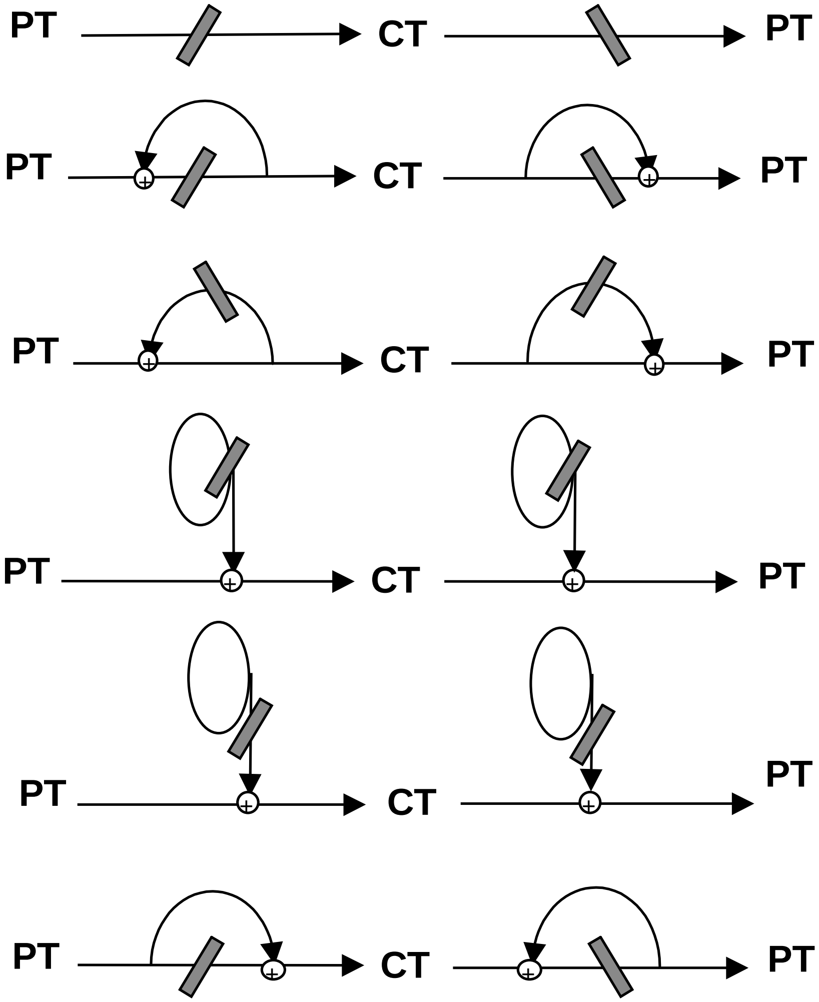
[pre-whitening sequence]

[pre-whitening sequence]

[pre & post whitening sequences]

[pre & post whitening sequences]

Encryption Modes of Operation



- Electronic CodeBook (ECB)
- Cipher Block Chaining (CBC)
- Cipher FeedBack (CFB)
- Output FeedBack (OFB)
- Counter Mode (Filter Generator)
- Plaintext Block Chaining

Mode	Security	Implementation	Fault Tolerance	Crypto Sync
ECB	- plaintext patterns are not concealed	+ no feedback + no IV storage + encryption and decryption are parallelizable	+ bit loss has no additional negative effects - ciphertext error magnification	+ self synchronizing
CBC	+ plaintext patterns are concealed	- feedback from encryption output - IV storage - encryption is not parallelizable + decryption is parallelizable	+ bit loss causes 1 additional block of plaintext to be corrupted - ciphertext error magnification	+ self synchronizing
CFB	+ plaintext patterns are concealed	- feedback from encryption output - IV storage - encryption is not parallelizable + decryption is parallelizable	+ bit loss causes 1 additional block of plaintext to be corrupted - ciphertext error magnification	+ self synchronizing
OFB	+ plaintext patterns are concealed	- feedback from encryption output - IV storage - encryption and decryption are not parallelizable	- bit loss causes loss of crypto synchronization + no ciphertext error magnification	- requires periodic resynch