Modes d'opération

Tristan Bertin
Jonathan Thieuleux

École Supérieure d'Informatique, Électronique, Automatique

16 novembre 2015

esiea
ECOLE D'INGENIEURS
DU MONDE NUMERIQUE

Sommaire

Sommaire

Présentation

C'est quoi un mode ?

- Traiter les blocs chiffrés/clairs
- Utilise un algorithme de chiffrement par bloc
- Indépendant de l'algorithme de chiffrement
- En théorie, indépendant de la taille des blocs

Présentation

Ça sert à quoi dans la vie de tous les jours ?

- Ajoute une sécurité en plus du chiffrement
  - Propagation d'erreurs (pas tous les modes)
  - Sécurité adaptée au média
- Protection de l'intégrité des données
- Certains modes associent chiffrement et authentification.

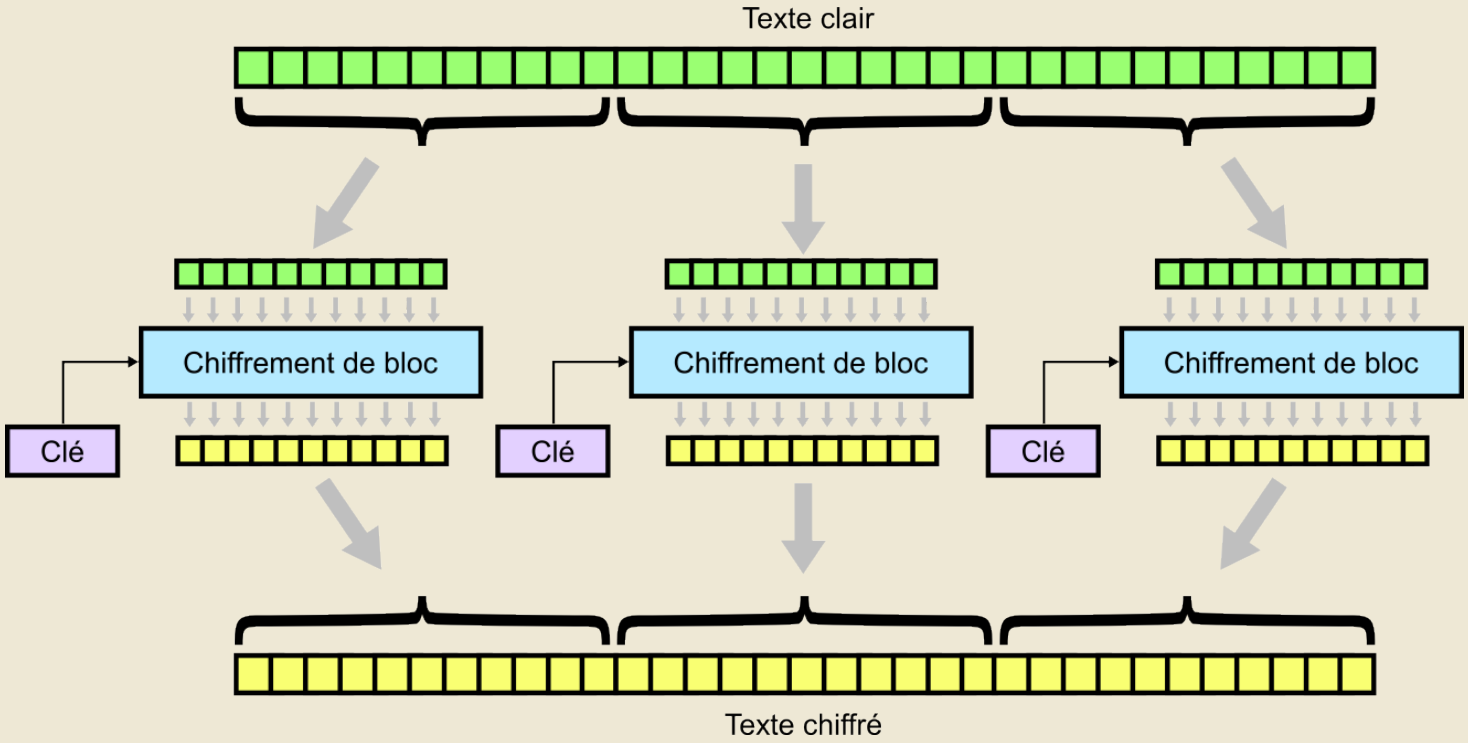
Sommaire

ECB

ECB

- Electronic CodeBook
- Mode intuitif

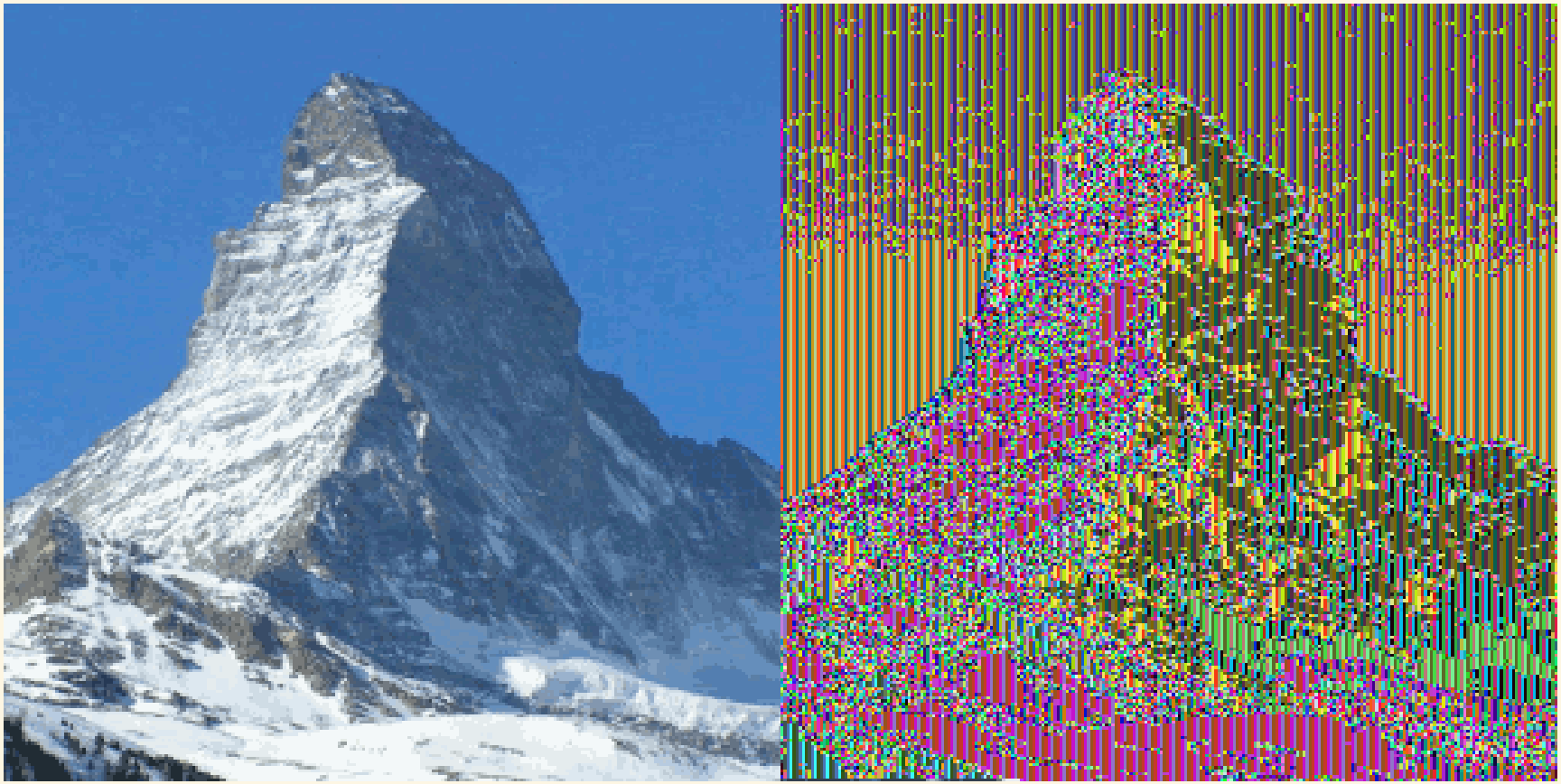
Fonctionnement



ECB

Problèmes

- La Redondance

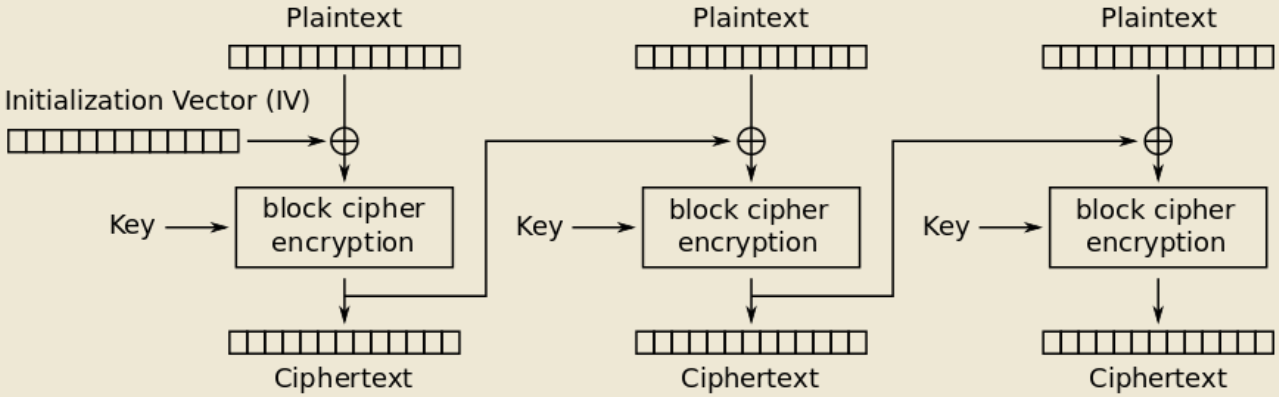


CBC

- Cipher Block Chaining
- Application d'un OU exclusif sur chaque bloc
- Vecteur d'initialisation
- Utilisé dans les communications

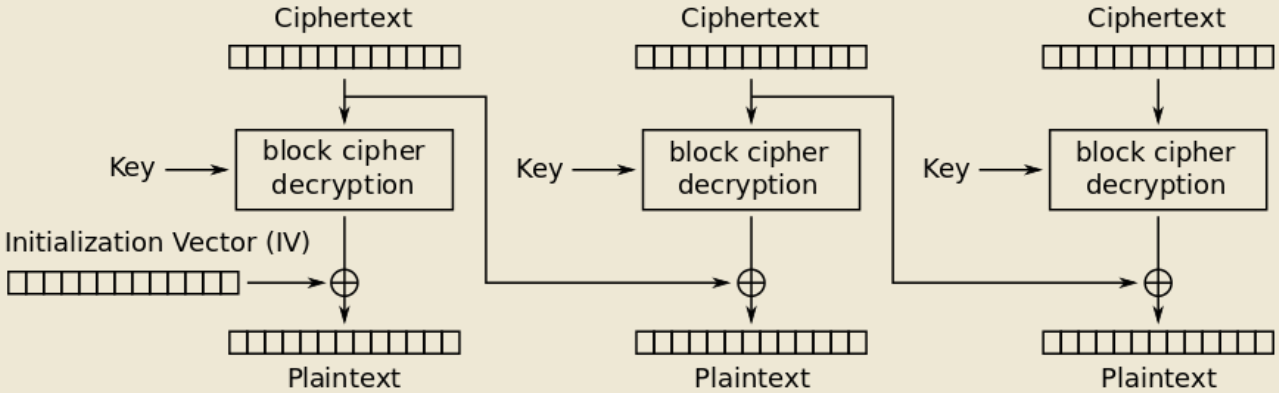
CBC

Chiffrement



Cipher Block Chaining (CBC) mode encryption

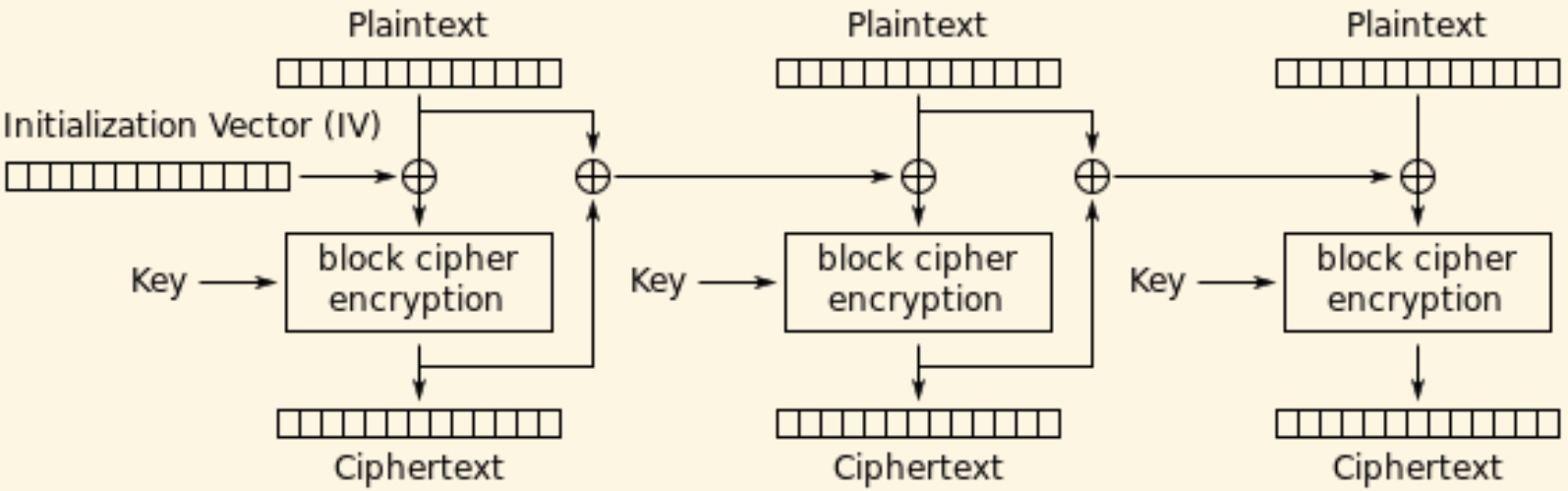
Déchiffrement



Cipher Block Chaining (CBC) mode decryption

PCBC : Propagating CBC

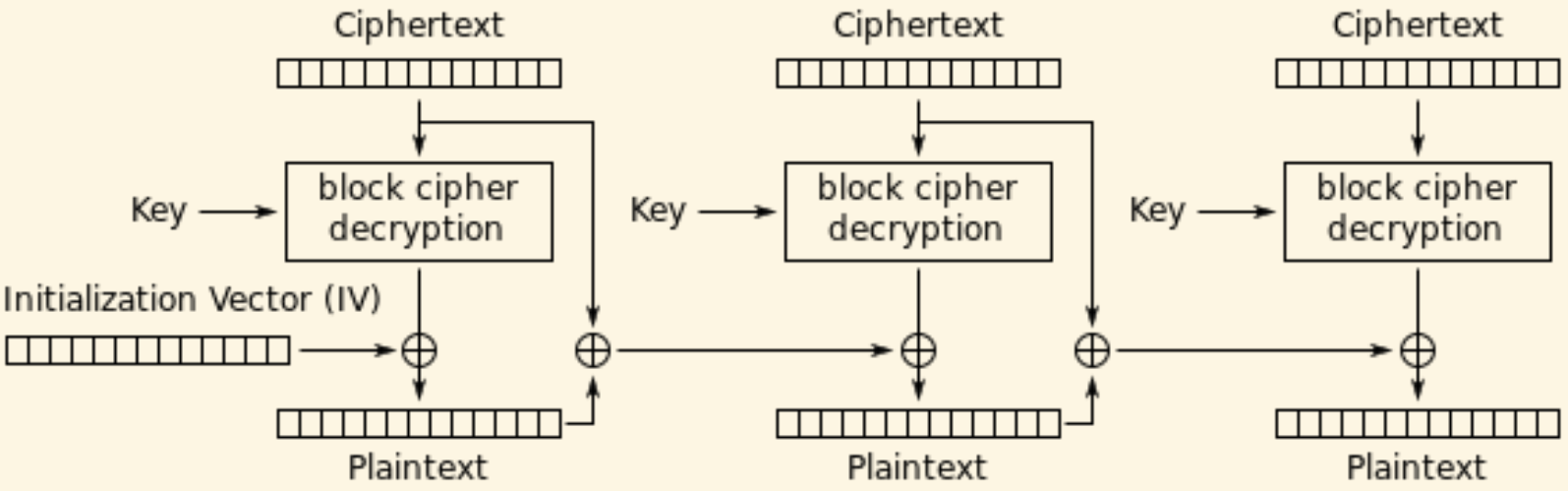
Chiffrement :



Propagating Cipher Block Chaining (PCBC) mode encryption

PCBC : Propagating CBC

Déchiffrement :



Propagating Cipher Block Chaining (PCBC) mode decryption

PCBC : Propagating CBC

Conclusion :

- Non parallélisation
- Propagation d'erreurs
- Indépendant de l'algorithme de chiffrement

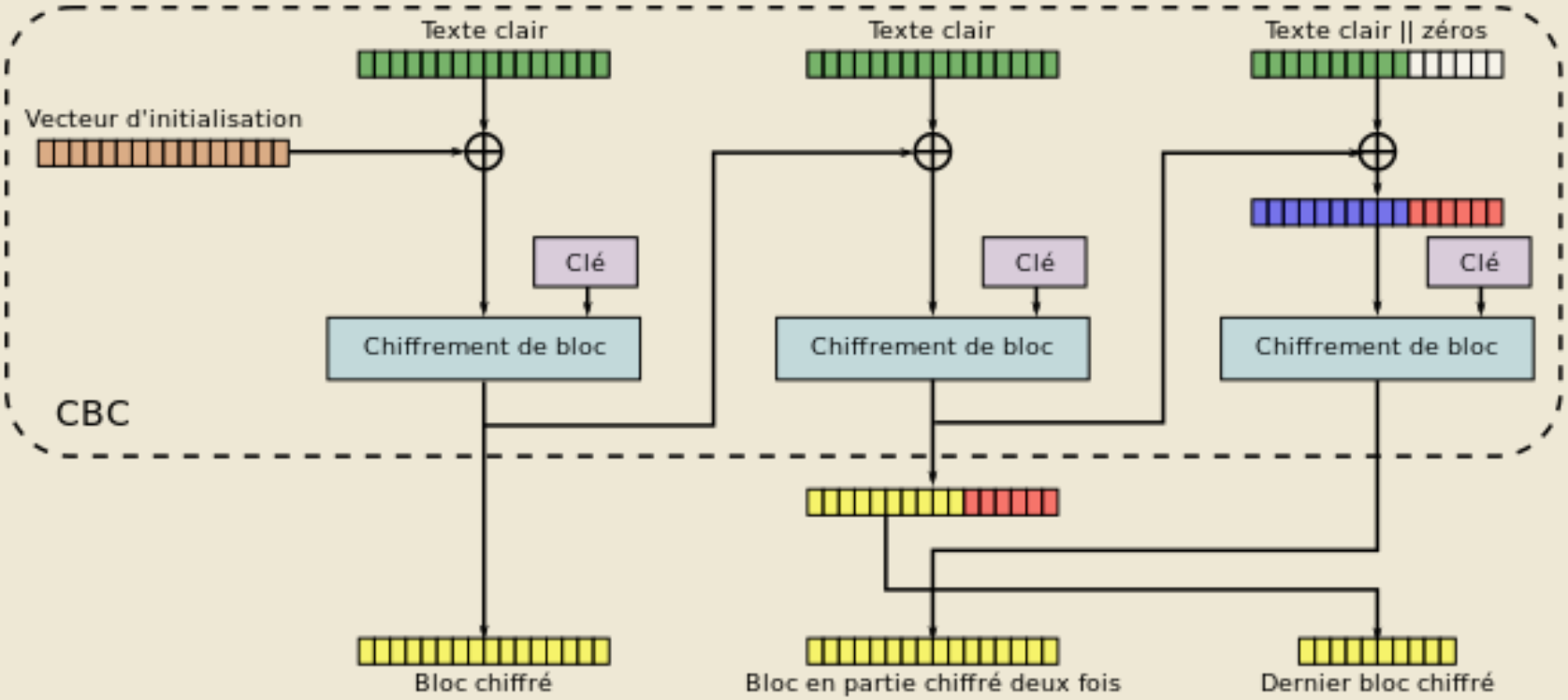
CTS

CTS

- CipherText Stealing
- CBC + Stealing
- Permet de travailler avec un message à taille variable (Message % taille de bloc != 0)

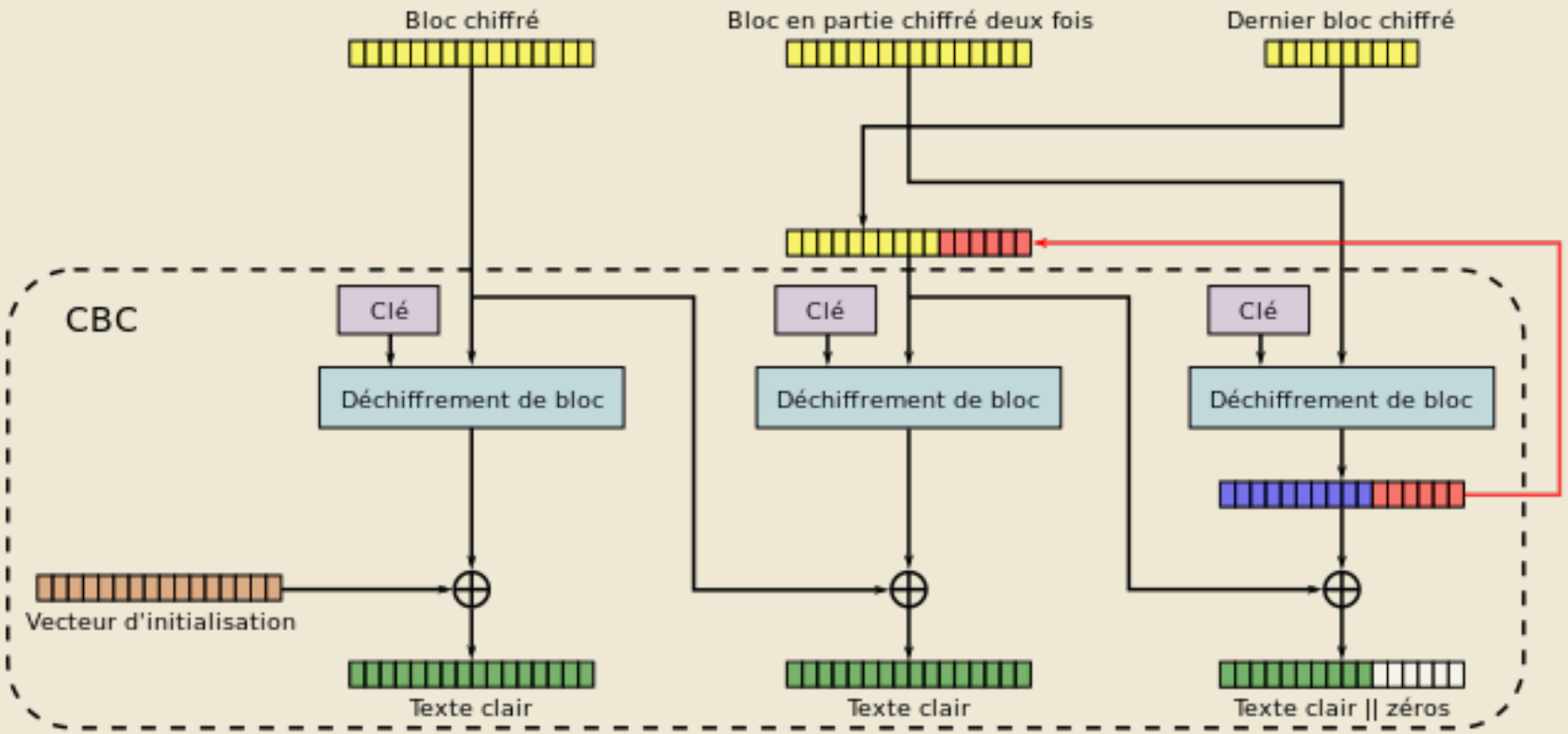
CTS

Chiffrement



CTS

Déchiffrement



XEX

- Xor-Encrypt-Xor
- Créé par Rogaway
- Utilise la propriété mathématique $(a \oplus b) \oplus b = a$
- XEX est souvent utilisé avec d'autres modes
- Permet un traitement efficace des blocs
- Créé pour le stockage de données sur un périphérique (USB, Disque dur, etc..)

XEX

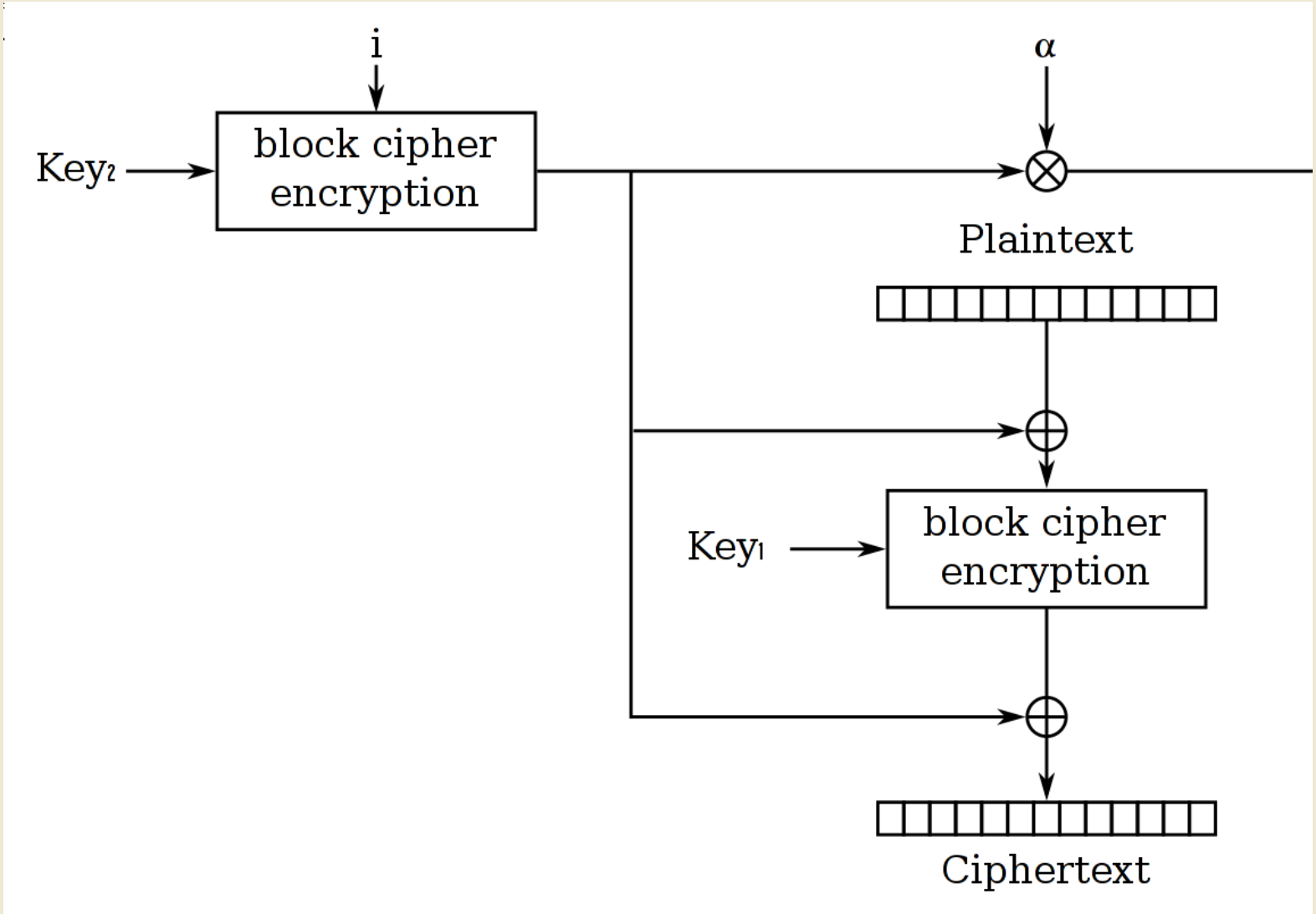
Fonctionnement

$$X = Enc(I) \otimes \alpha^j$$
$$C = Enc(P \oplus X) \oplus X$$

- P est le texte clair
- I est le numéro du secteur (avantage pour le stockage)
- α est un élément primitif du corps de Galois $GF(2^{128})$ défini par un polynôme (ex : 2)
- j Nombre de blocs par secteur

XEX

Fonctionnement



XTS

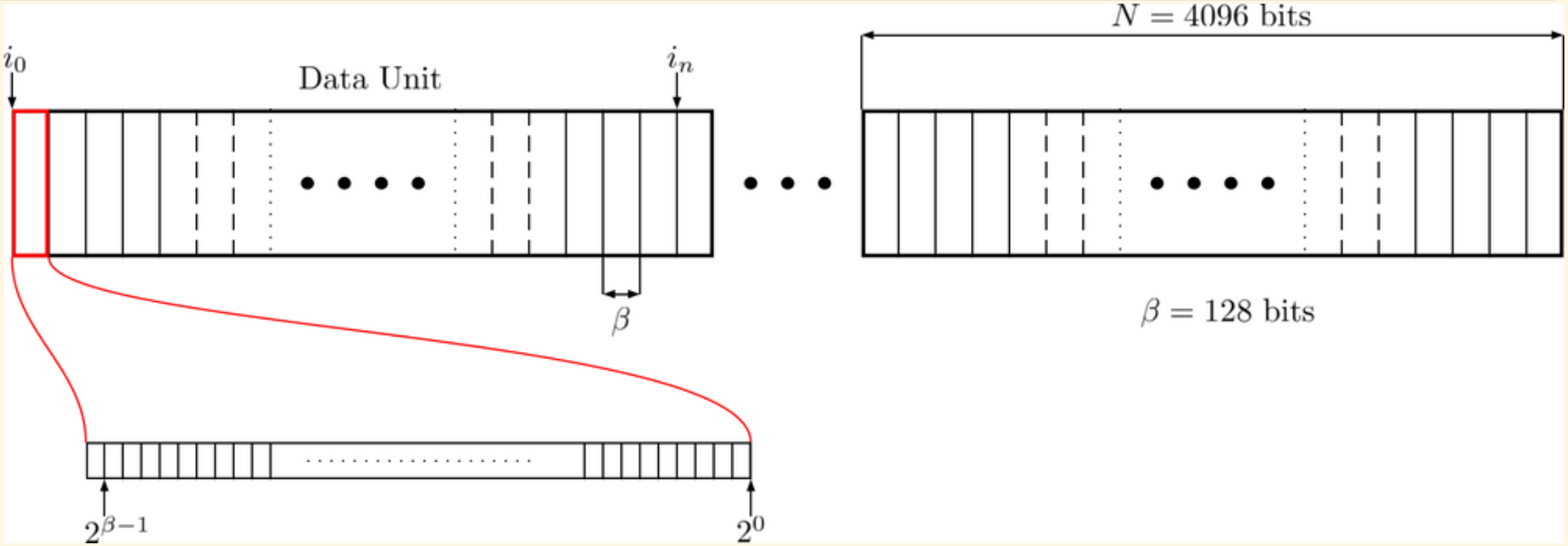
XTS

- XEX-based Tweaked-codebook mode with ciphertext Stealing
- XEX + Stealing
- Apparu en 2007
- Mise au point par l'IEEE (Std. 1619-2007)
- Créé pour l'AES [1]
- Utilisé pour le stockage de données sur un périphérique.
- Mode le plus présent dans les outils de chiffrement (Truecrypt, zulucrypt, etc)

1. Advanced Encryption Standard

XTS Chiffrement

Unité de données



XTS Chiffrement

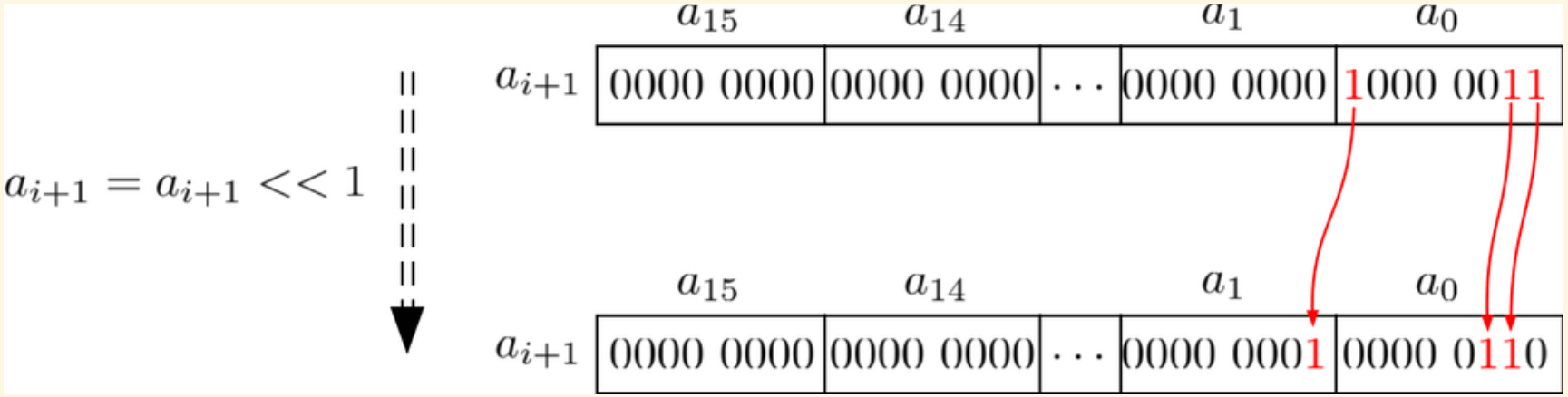
Multiplication par un élément primitif

$$a_{i+1}[0] \leftarrow (\alpha \cdot (a_i[0] \ mod \ 128)) \oplus (135 \cdot \lfloor \frac{a_i[15]}{128} \rfloor)$$

$$a_{i+1}[k] \leftarrow (\alpha \cdot (a_i[k] \ mod \ 128)) \oplus \cdot \lfloor \frac{a_i[k-1]}{128} \rfloor$$

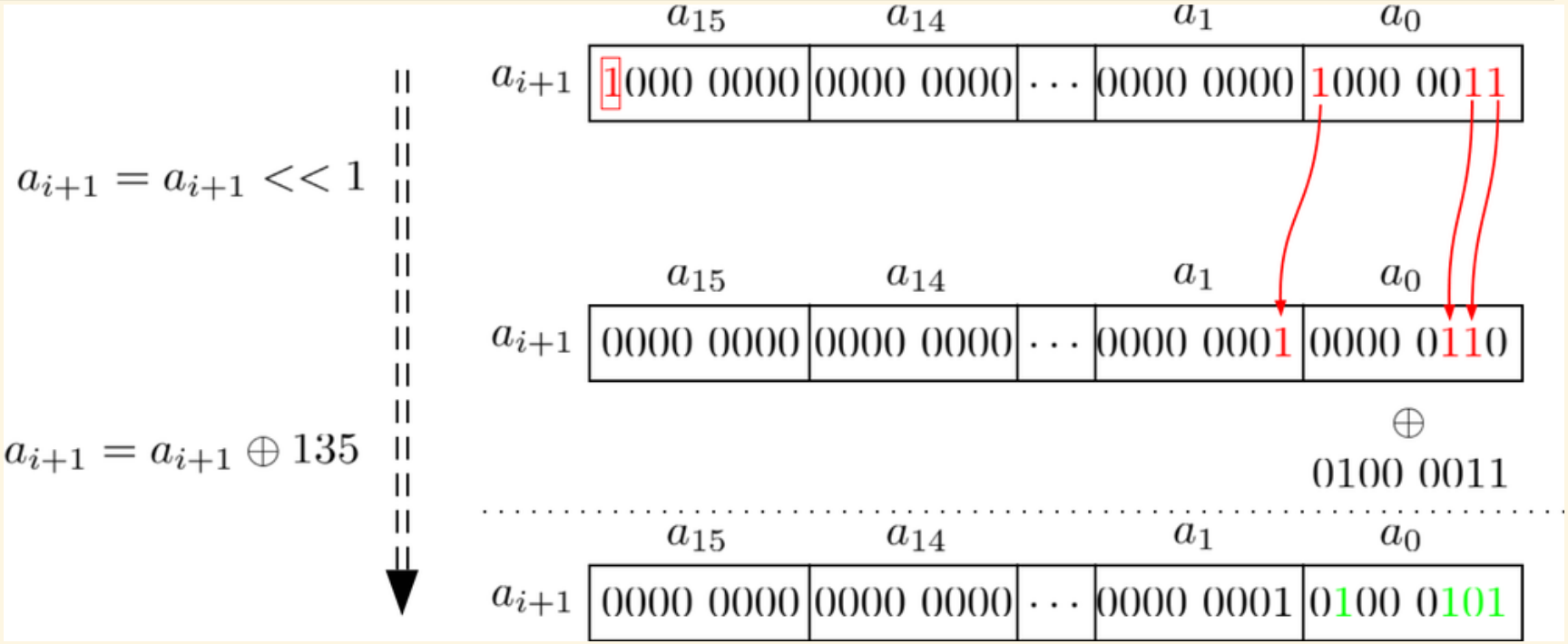
$$\text{où} \quad k = \{1, 2, \cdots, 15\}, \quad \alpha = 2$$

Multiplication dans $GF(2^{128})$ sans débordement



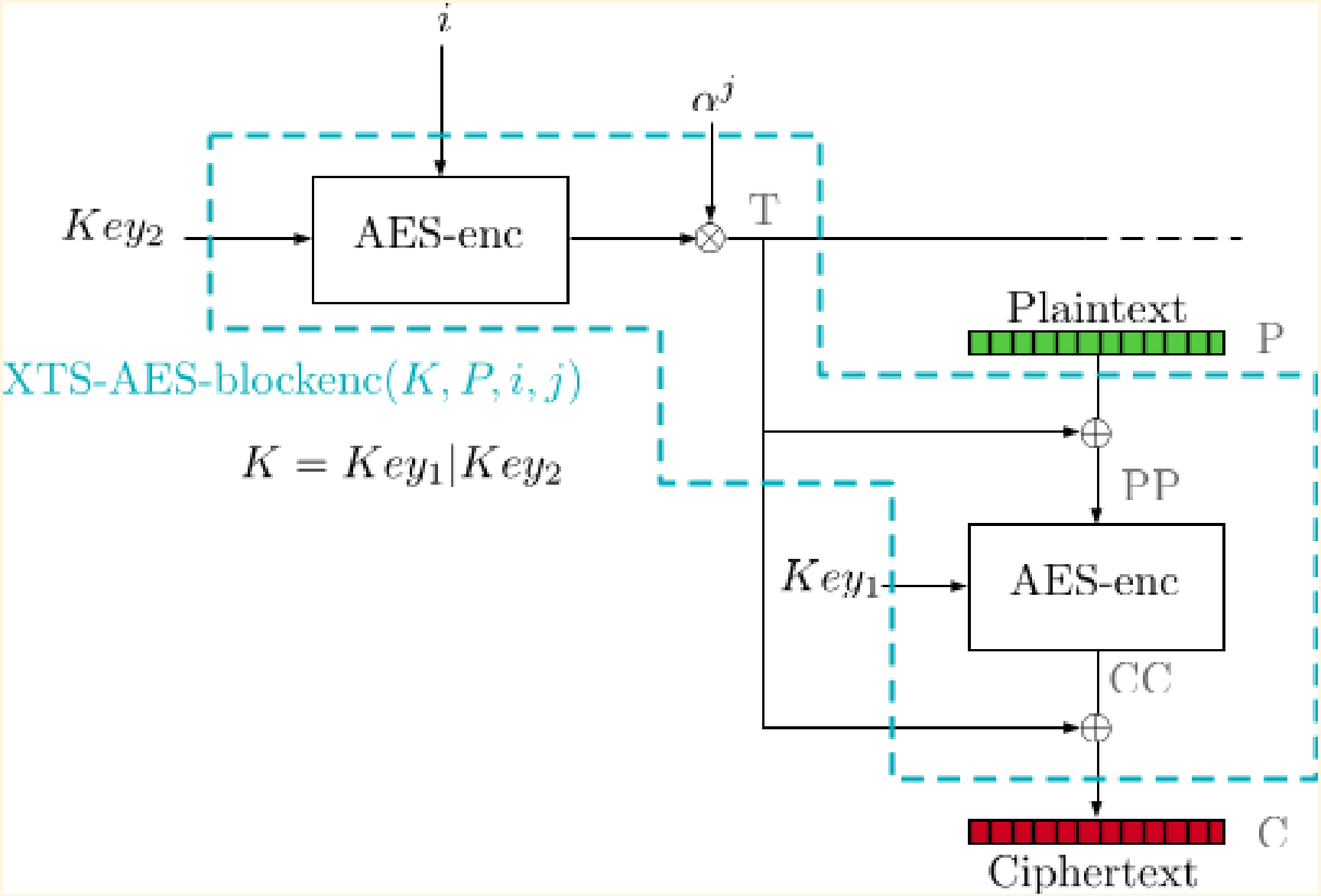
XTS Chiffrement

Multiplication dans $GF(2^{128})$ avec débordement



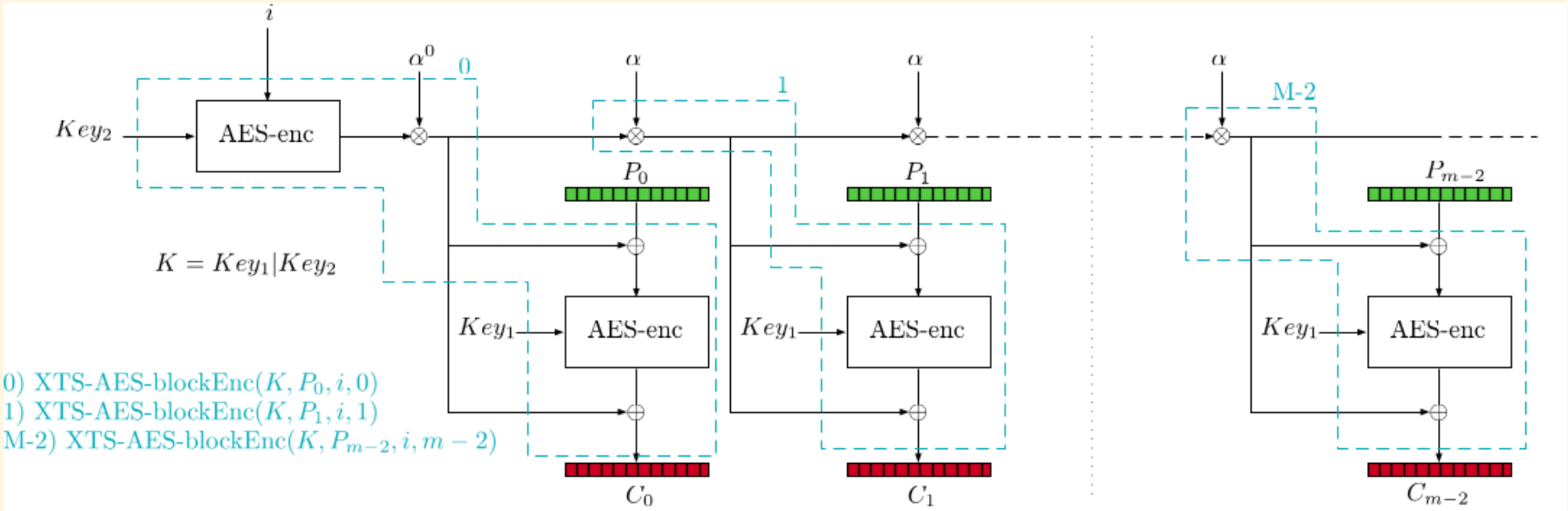
XTS Chiffrement

Chiffrement d'un bloc de 128 bits



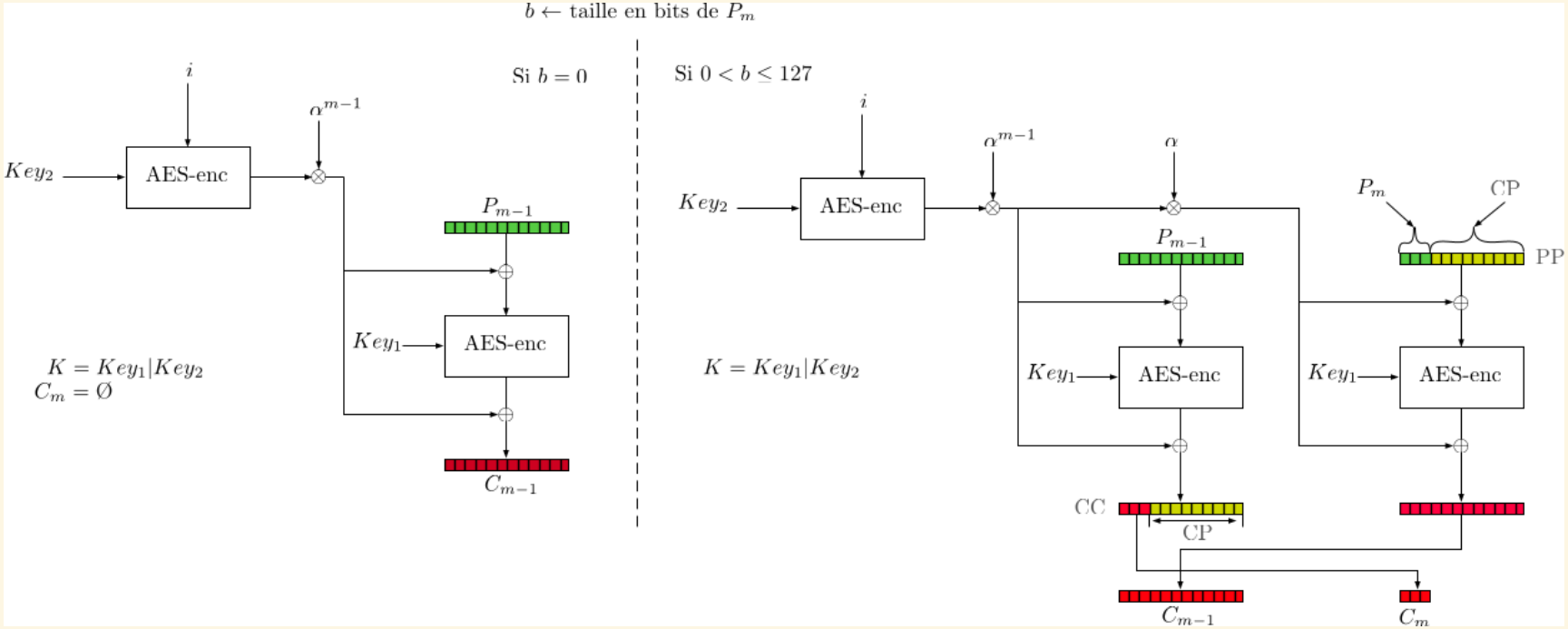
XTS Chiffrement

Chiffrement d'une unité de données



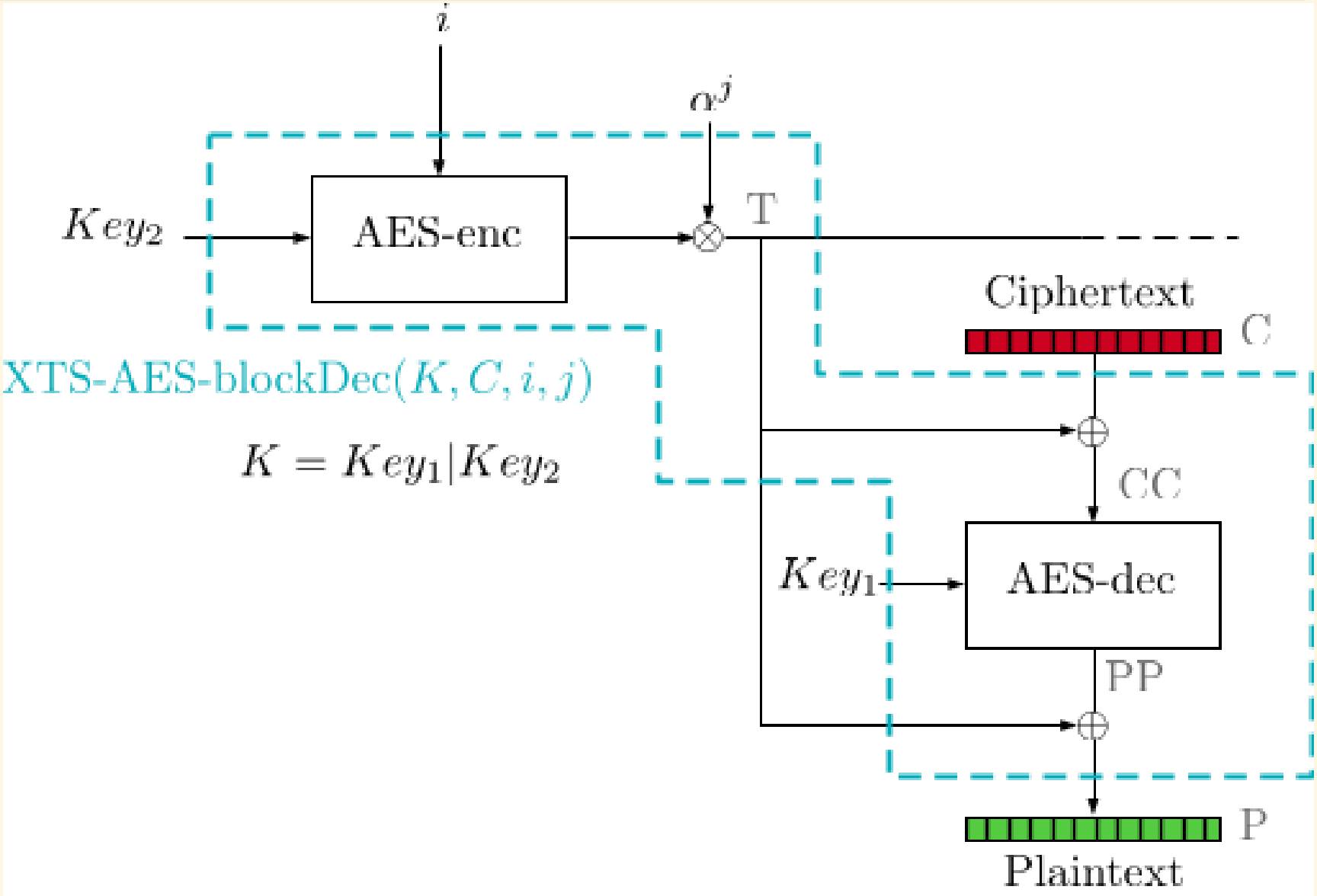
XTS Chiffrement

Texte Stealing



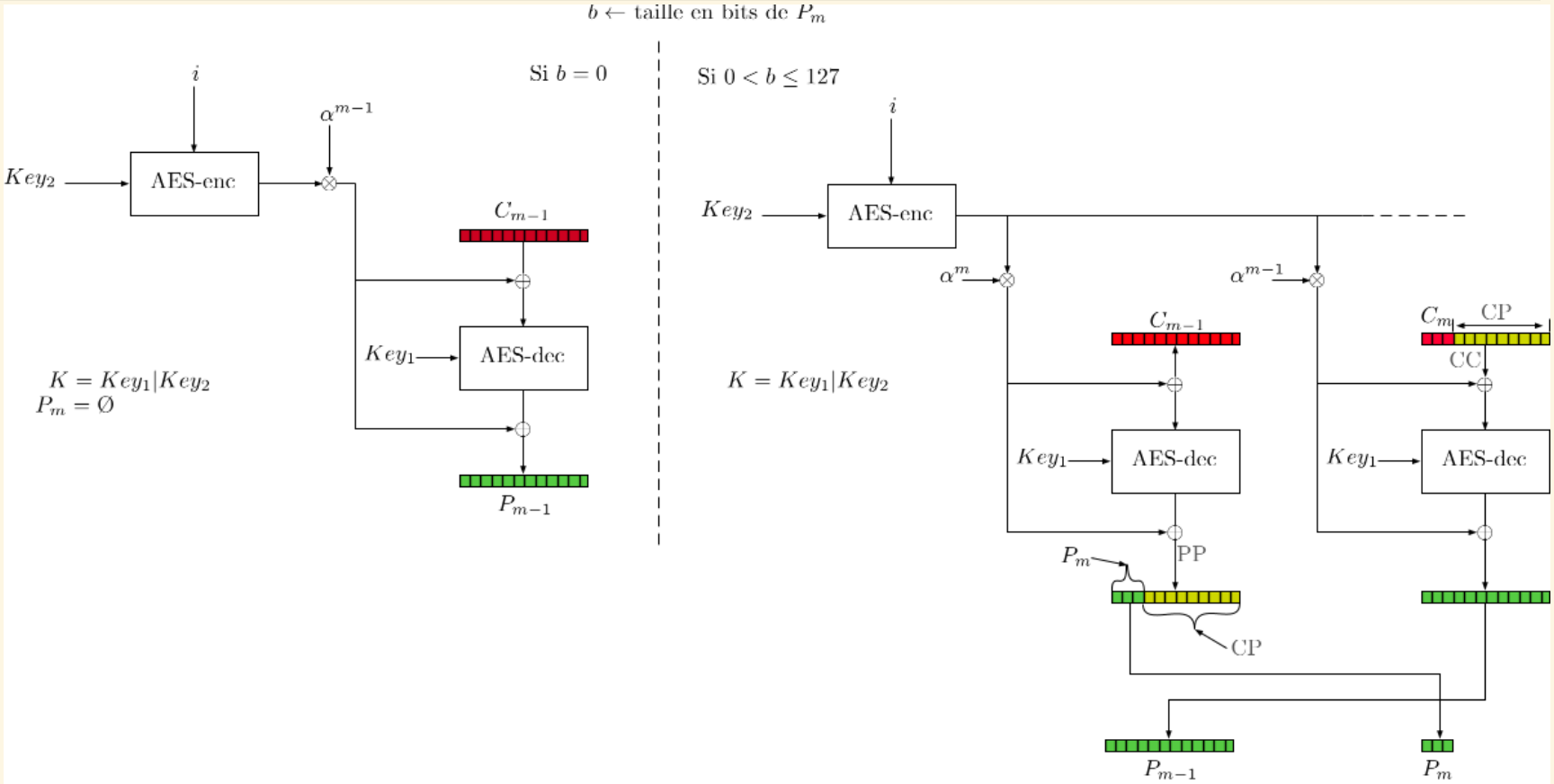
XTS Déchiffrement

Déchiffrement d'un bloc de 128 bits



XTS Déchiffrement

Texte Stealing



XTS

Conclusion :

- Parallélisable
- Pas de propagation d'erreurs
- Indépendant de l'algorithme de chiffrement

GCM

Présentation :

Mode de chiffrement en deux parties :

- Counter mode
- Galois authentication

Pour des blocs de 128 et 64 bits.

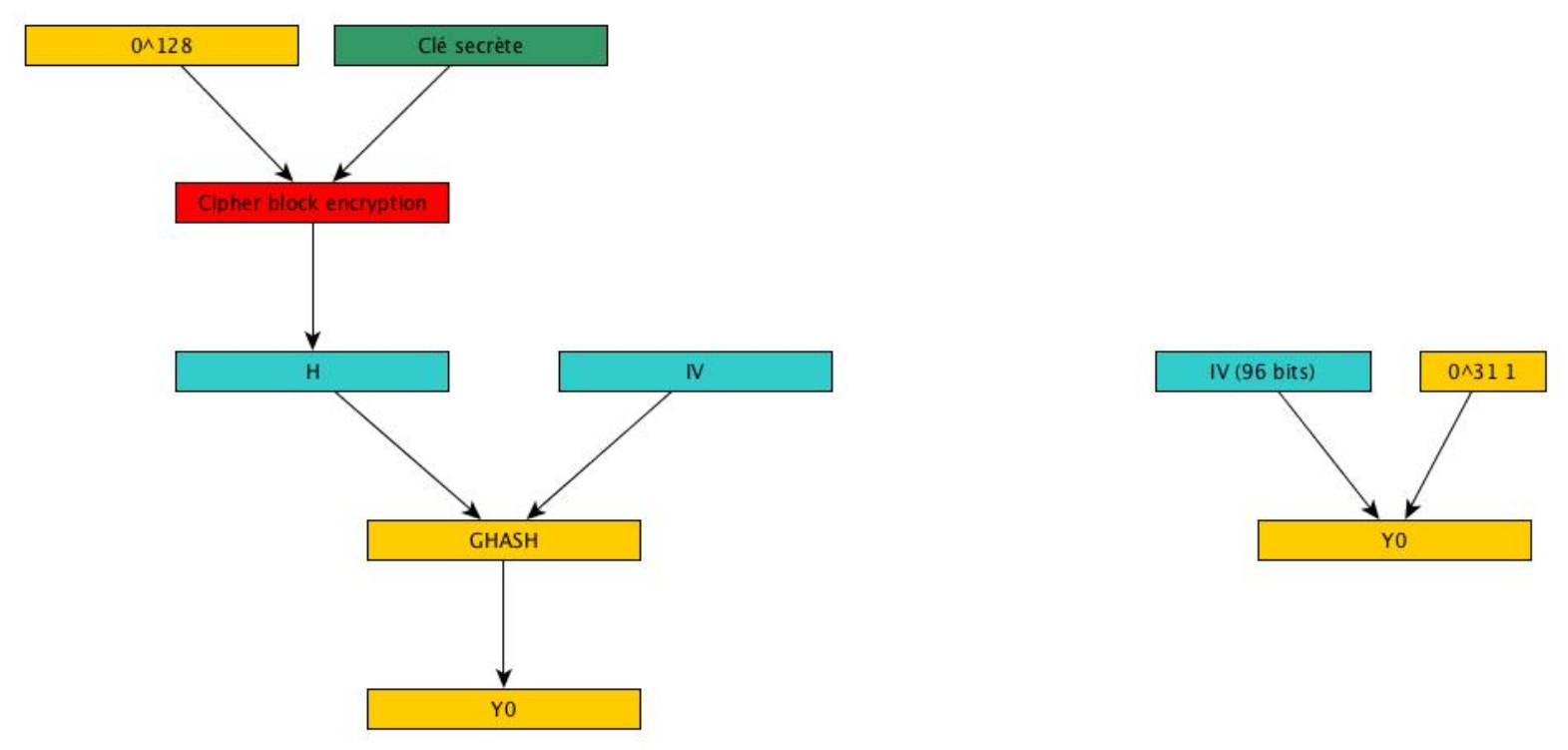
Counter mode

Explications :

Compteur initialisé au début, incrémenté à chaque nouveau bloc.
Chiffré avec l'algorithme choisi puis xoré avec le bloc de texte chiffré.
Deux méthodes d'initialisation.

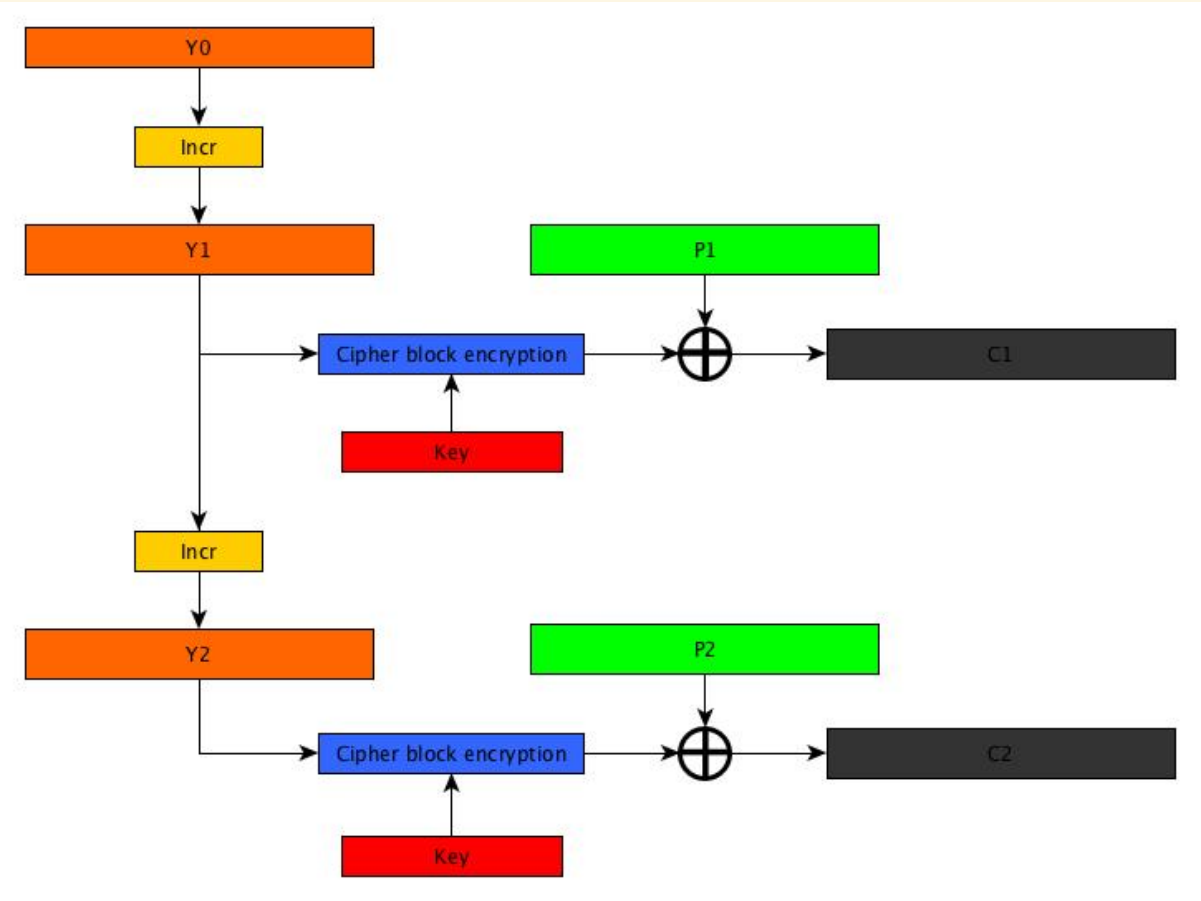
Counter mode

Initialisations :



Counter mode

Chiffrement :



Counter mode

Conclusion :

- Parallélisable
- Pas de propagation d'erreurs
- Indépendant de l'algorithme de chiffrement

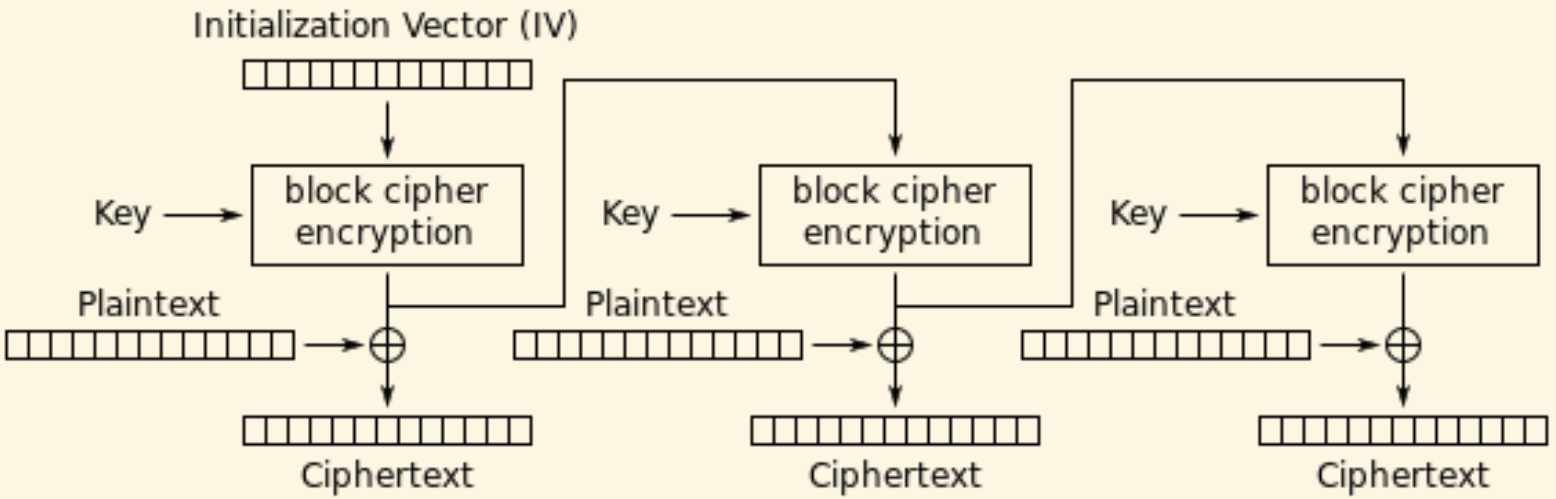
OFB : Output FeedBack

Fonctionnement :

- La longueur des blocs dépend de l'algorithme de chiffrement,
- Chiffre un vecteur d'initialisation,
- Le résultat est xoré avec le premier bloc de texte clair et donne le chiffré,
- Le résultat du chiffrement est utilisé comme bloc d'entrée dans le second cycle.
- **Pas de fonction de déchiffrement**

OFB : Output FeedBack

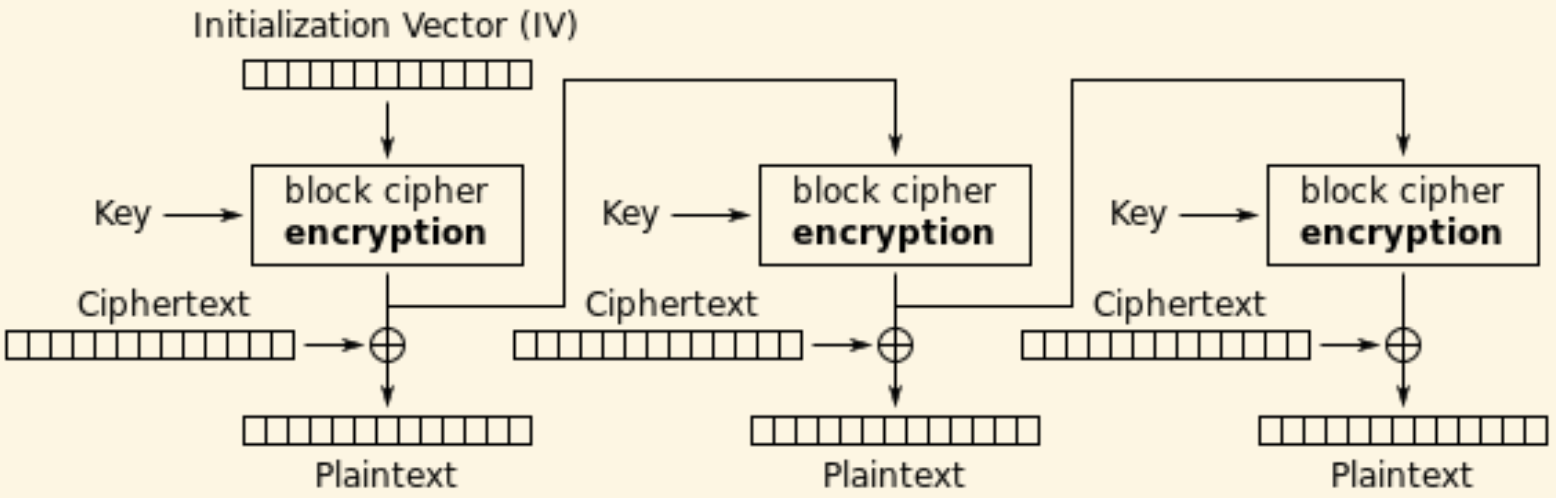
Chiffrement :



Output Feedback (OFB) mode encryption

OFB : Output FeedBack

Déchiffrement :



Output Feedback (OFB) mode decryption

OFB : Output FeedBack

Conclusions :

- Non parallélisable
- Pas de propagation d'erreurs
- Dépendant de l'algorithme de chiffrement

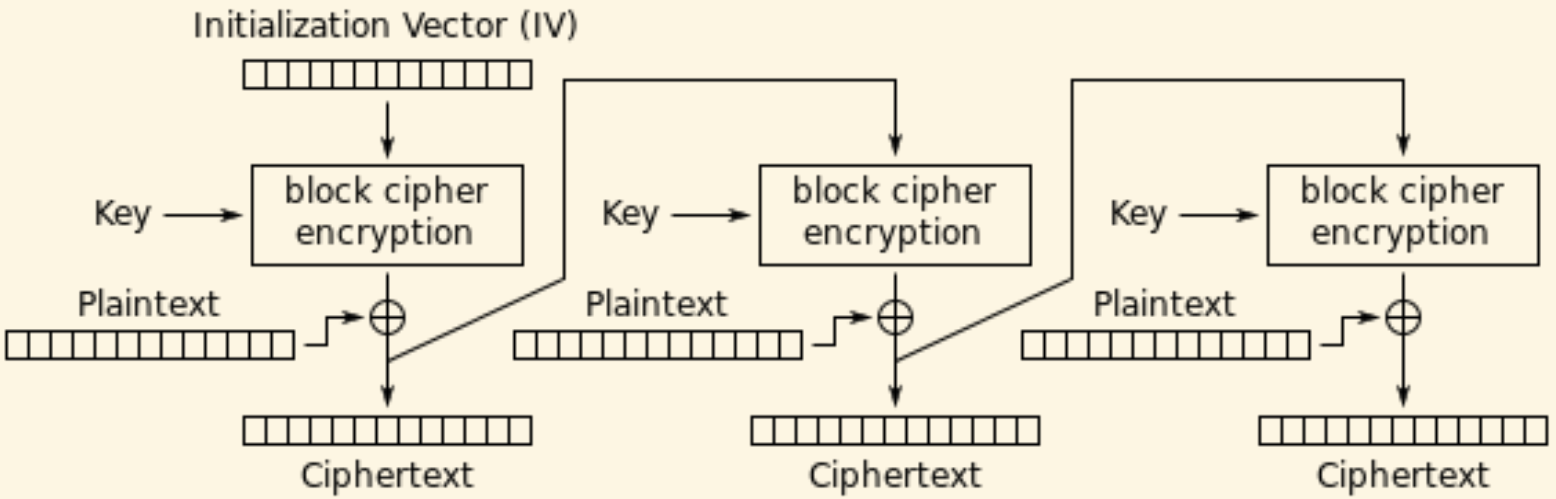
CFB : Cipher FeedBack

Présentation :

- Semblable au OFB
- Seul le bloc d'entrée du cycle suivant change. Il s'agit du chiffré du bloc actuel

CFB : Cipher FeedBack

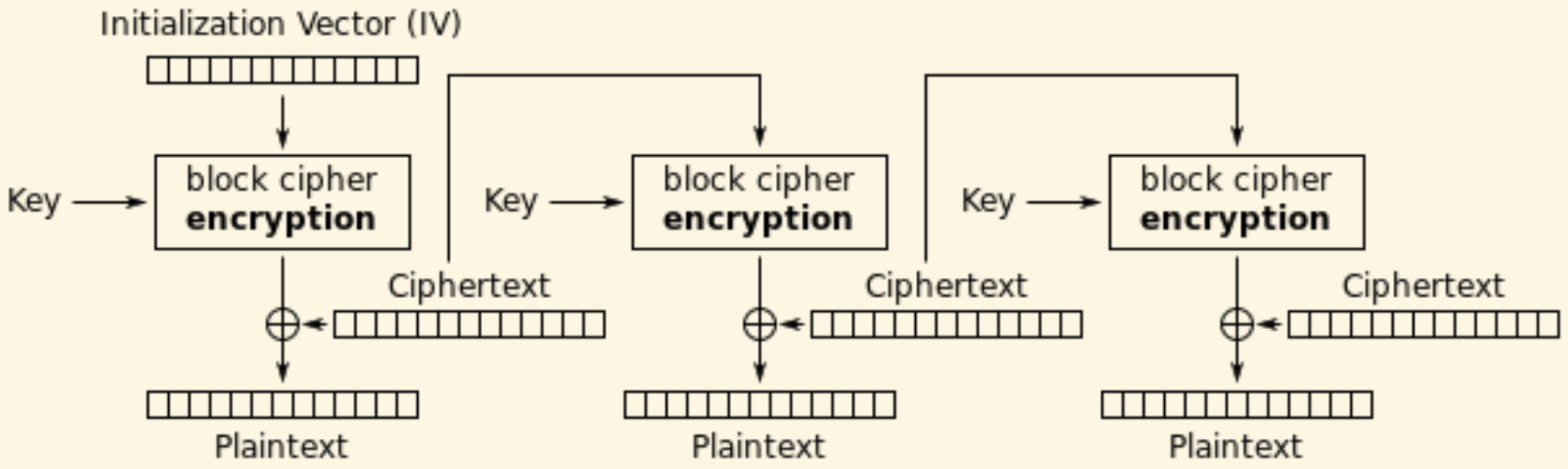
Chiffrement :



Cipher Feedback (CFB) mode encryption

CFB : Cipher FeedBack

Déchiffrement :



Cipher Feedback (CFB) mode decryption

CFB : Cipher FeedBack

Conclusion :

- Chiffrement non parallélisable / Déchiffrement oui
- Propagation d'erreurs
- Dépendant de l'algorithme de chiffrement

Sources

Sources

- Wikipedia : Mode d'opération
- Evaluation of Some Blockcipher Modes of Operation : NIST

Questions