Modes opératoires de chiffrement

Fouque Pierre-Alain

Equipe de Cryptographie

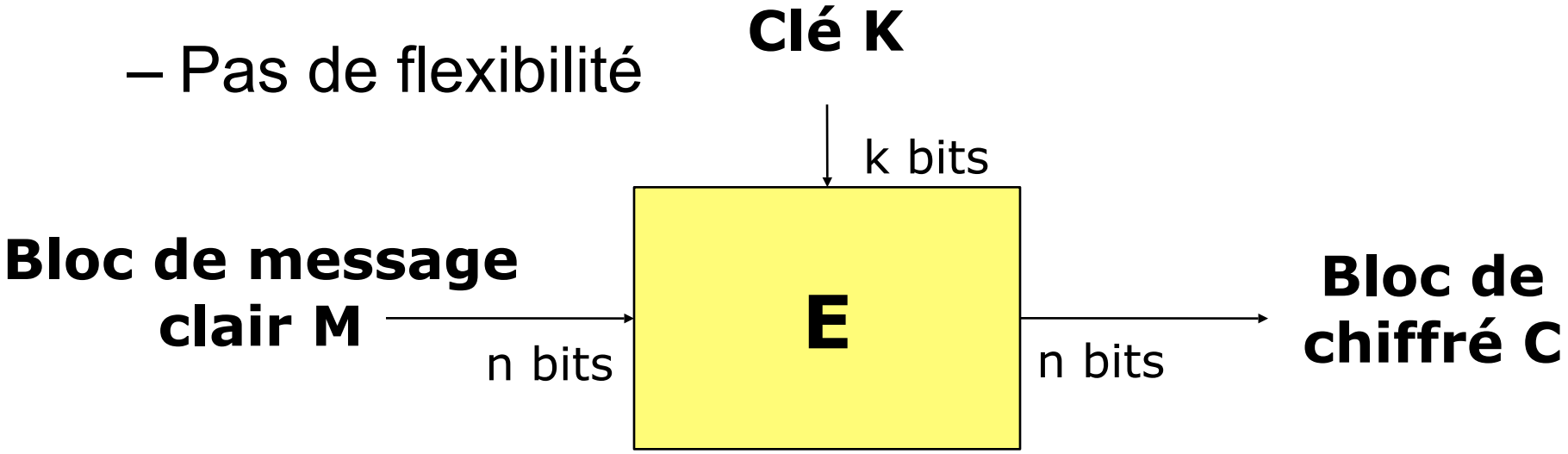
Ecole normale supérieure

Introduction

- Construction de modes opératoires
  - Assurer la confidentialité sur des messages de taille variable
  - Block cipher se comporte comme une permutation aléatoire

Problématique

- Des primitives de base sont définies
  - Chiffrement de blocs de taille fixe
  - Pas de flexibilité



Exemples : DES, n=64, k=56
3DES, n=64, k=112
AES, n=128, k=128

Le chiffrement en pratique

- En pratique :
  - Messages de taille quelconque, variable
  - Utilisation des briques de base
- Quelle hypothèse de sécurité sur la primitive ?

Confidentialité

- Comment savoir si un mécanisme assure correctement la confidentialité
  - Notion de sécurité à définir
  - Comment assurer que la notion définie est atteinte
    - Quantification de la sécurité
    - Modélisation des adversaires
    - Preuve de sécurité

Confidentialité

- Quelle « fuite » d'information peut-on tolérer ?
  - Dépend du contexte
- En général, mauvais signe
  - Selon la probabilité de cette fuite
  - Selon son importance

Notion de sécurité plus ou moins forte à définir

Confidentialité

- Intuitivement :
  - Un attaquant n’est pas capable de retrouver la clé secrète
  - Un attaquant n’est pas capable de déchiffrer sans la clé secrète
  - Un attaquant n’apprend aucune information sur le message clair à la vue de son chiffré

Confidentialité

- Intuitivement :
  - Un attaquant n'est pas capable de retrouver la clé secrète
  - Un attaquant n'est pas capable de déchiffrer sans la clé secrète
  - Un attaquant n'apprend aucune information sur le message clair à la vue de son chiffré

Attaque de plus en plus faible

Confidentialité

- Intuitivement :
  - Un attaquant n'est pas capable de retrouver la clé secrète
  - Un attaquant n'est pas capable de déchiffrer sans la clé secrète
  - Un attaquant n'apprend aucune information sur le message clair à la vue de son chiffré

Attaque de plus en plus faible

Sécurité dans ce sens = Sécurité maximale

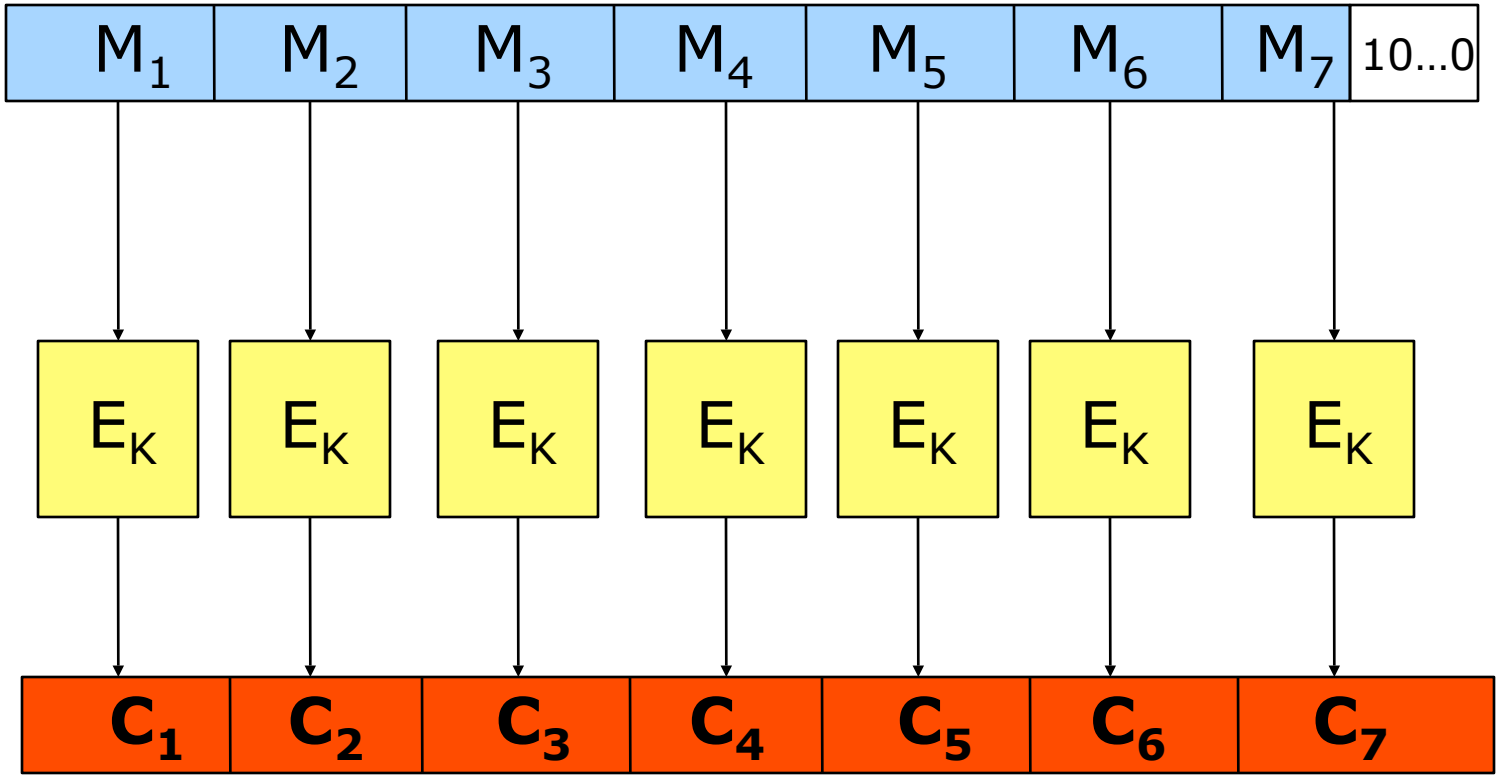
Attaques mises en oeuvre

- **À chiffrés seuls** : l'adversaire ne connaît que des chiffrés, interception par exemple
- **À clairs connus** : l'adversaire a accès à des couples (M,C) de messages chiffrés
- **À clairs choisis** : l'adversaire a accès à des couples (M,C) de messages chiffrés, pour M de son choix
- **À chiffrés connus/choisis** : l'adversaire demande le déchiffrement de chiffrés

  - Attaque non adaptative : l'ensemble des messages est choisi a priori
  - Attaque adaptative : l'adversaire choisit les messages en fonction des réponses de l'oracle

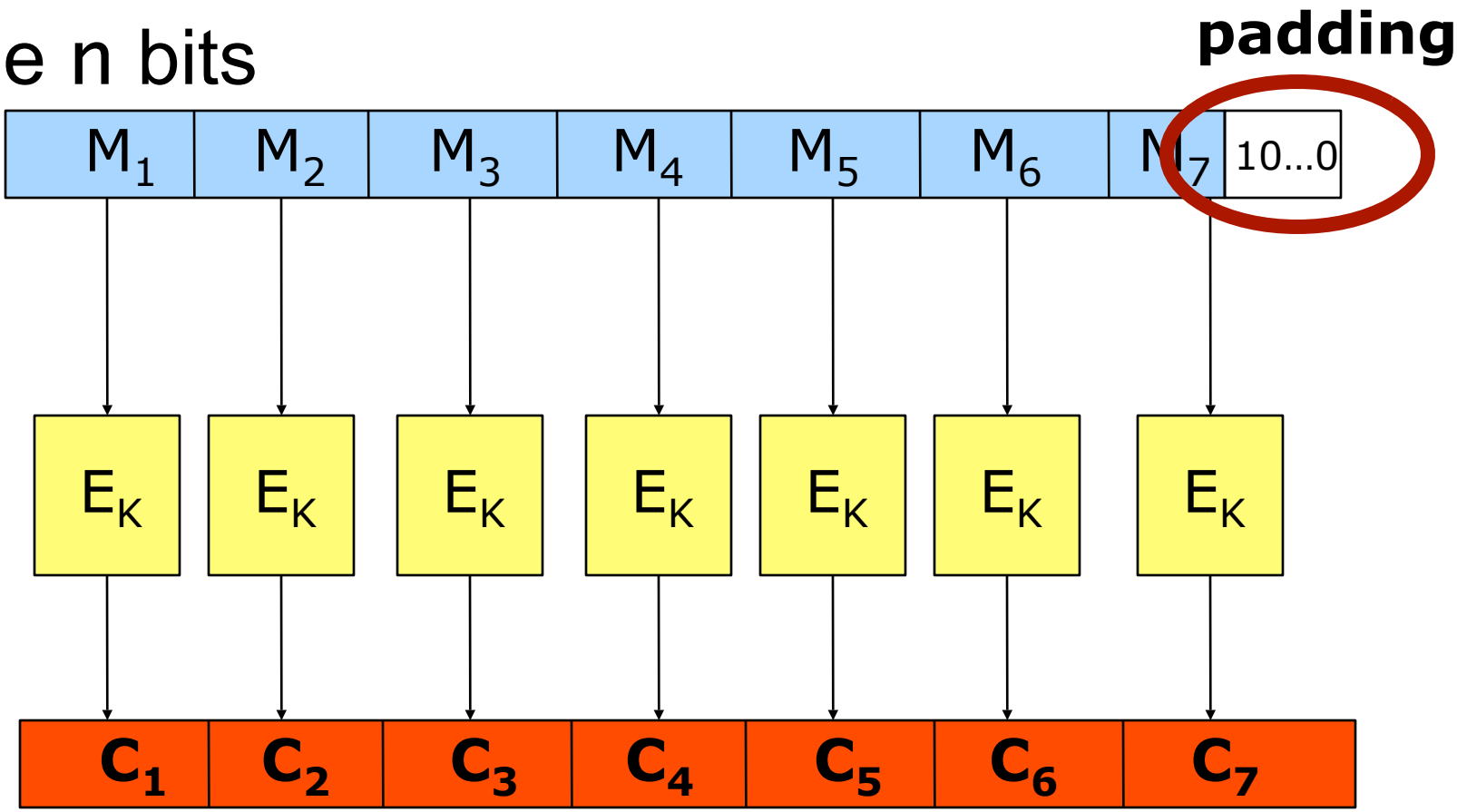
Un exemple basique

- Message de taille quelconque, non multiple de n bits



Un exemple basique

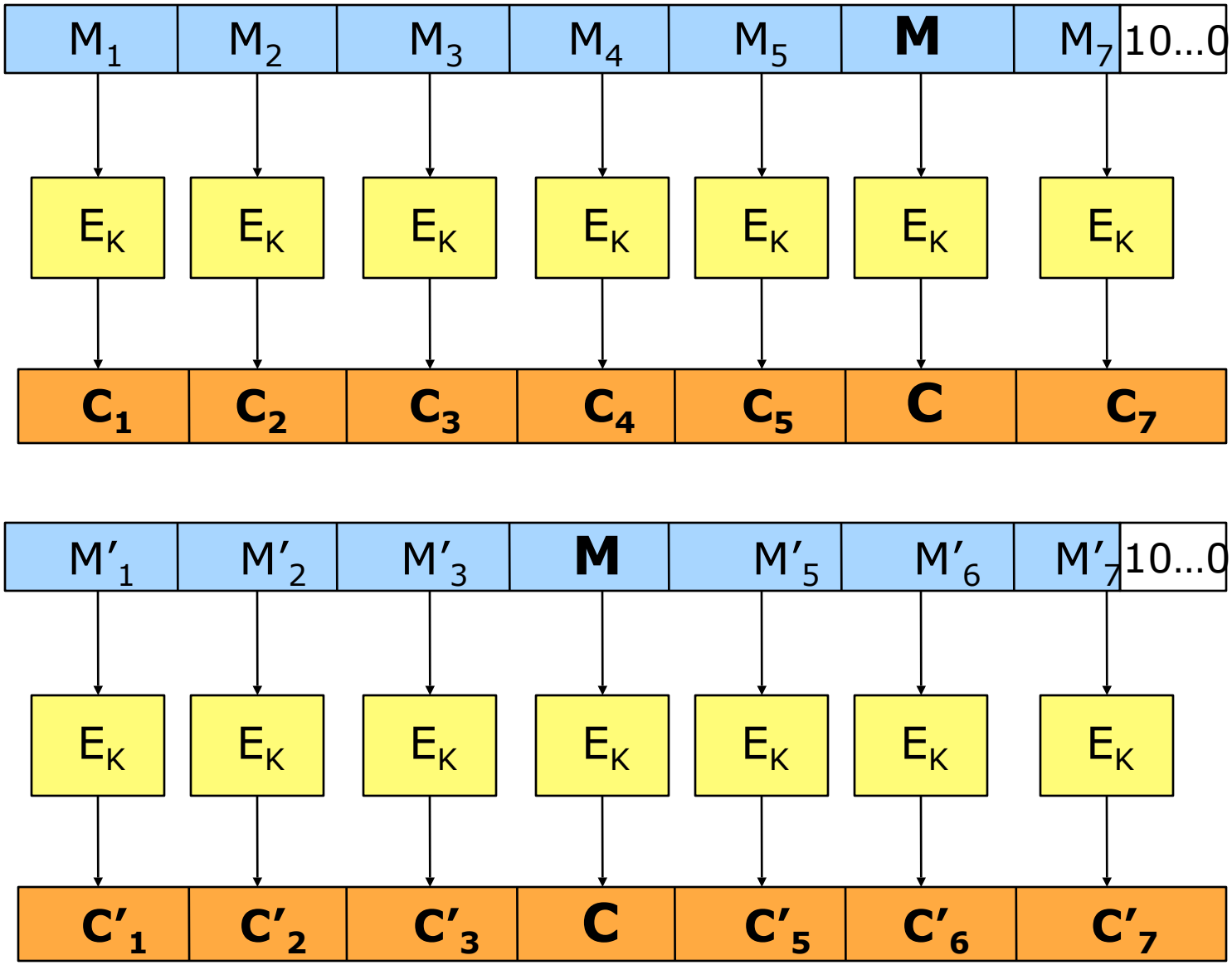
- Message de taille quelconque, non multiple de n bits



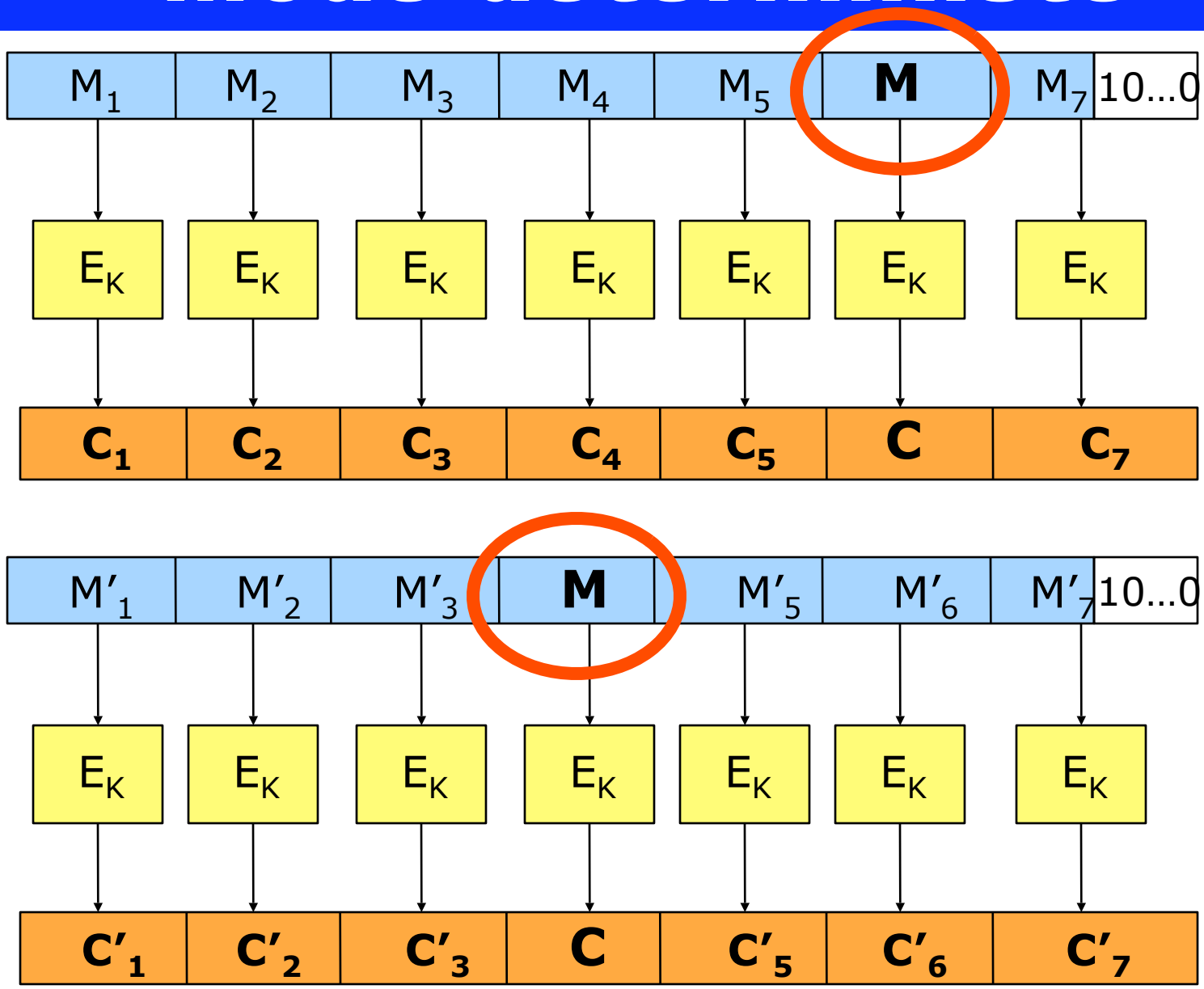
Un exemple basique

- Mode ECB : Electronic CodeBook
- Chaque bloc est chiffré indépendamment des autres
  - Interversion possible des blocs
  - Suppression d'un bloc
  - Un attaquant peut créer un dictionnaire
  - Attaque statistique parfois possible
  - Un même bloc de chiffré correspond toujours au même bloc de clair

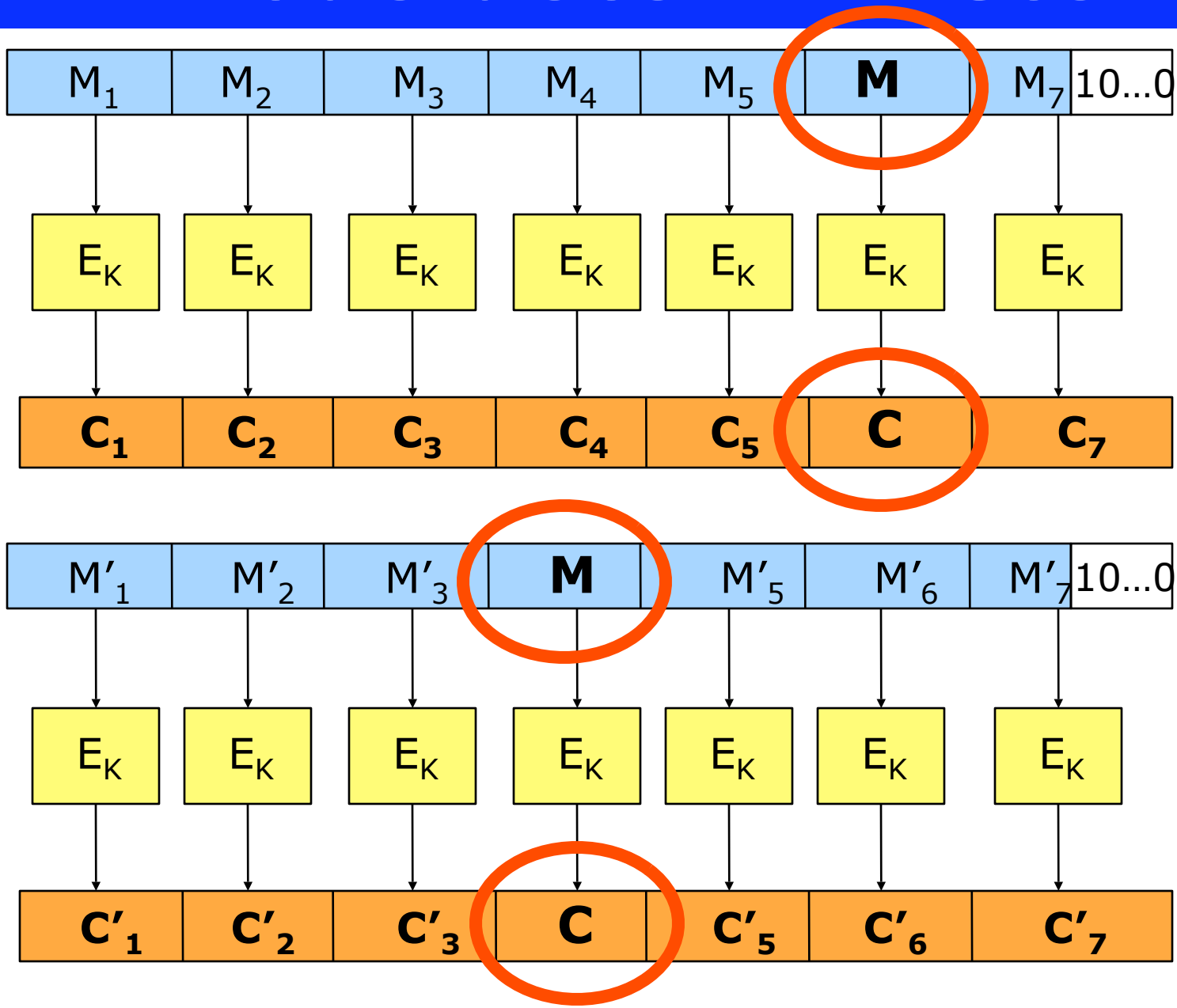
Mode déterministe



Mode déterministe

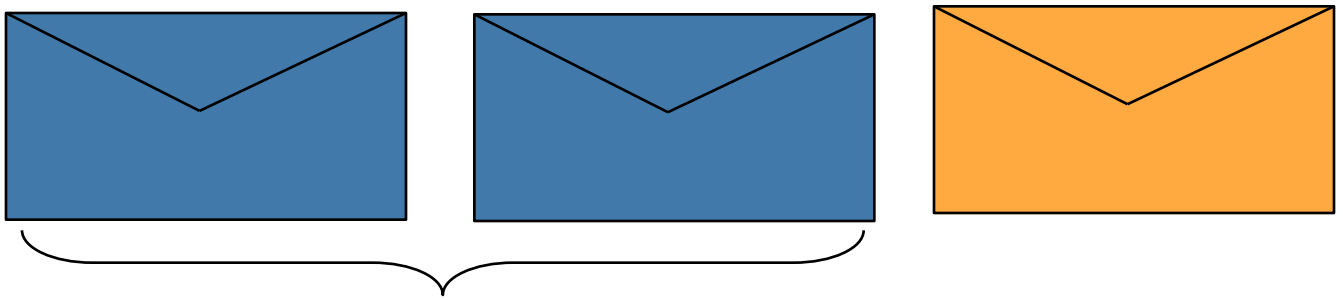


Mode déterministe



Mode déterministe

- Problématique dans certains contextes
- Exemple : vote en ligne
  - Même vote = même bulletin = même chiffré



Même enveloppe
=
Même vote

Attaque basique sur ECB

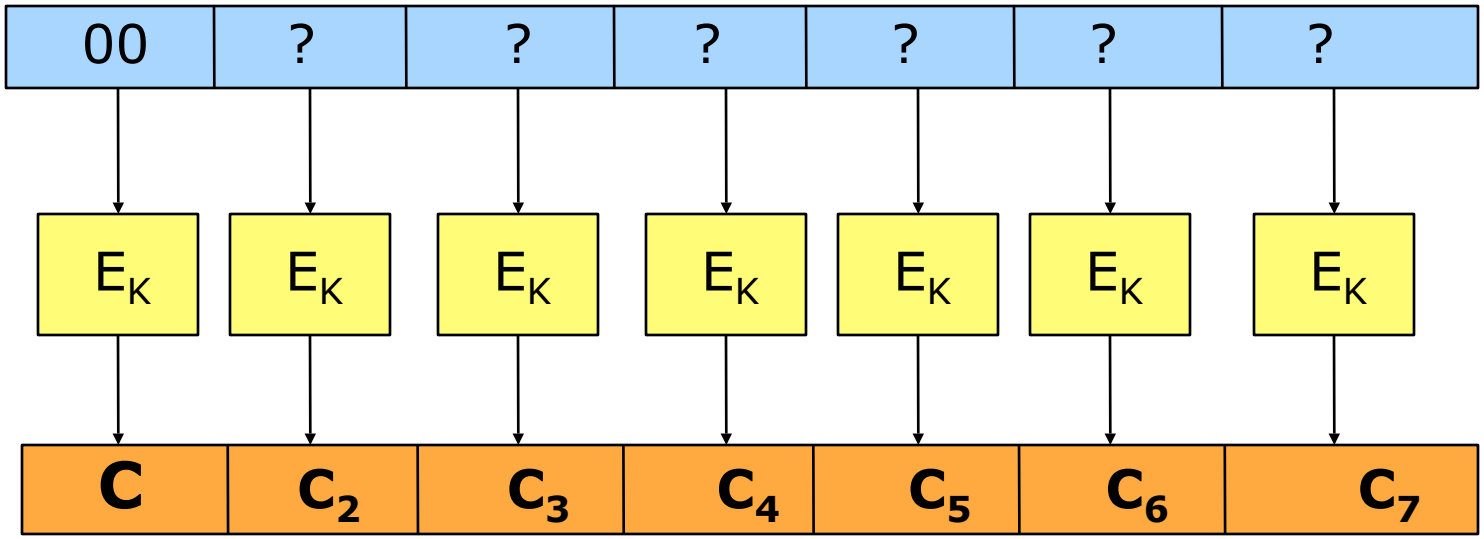
- Chiffrement de texte Unicode
  - 16 bits par caractère
- La primitive de chiffrement est le DES
  - Blocs de clair de 64 bits
- 4 caractères seulement par bloc !
- Attaque statistique : permet de retrouver le clair

Attaque statistique sur ECB

- Chaque quartet de lettres a une fréquence différente selon la langue
  - En français :
    - « tion » est très fréquent
    - « kzjx » n'apparaît jamais
- Fréquence d'apparition des blocs chiffrés
- Le clair peut être retrouvé par comparaison des tables de fréquence !

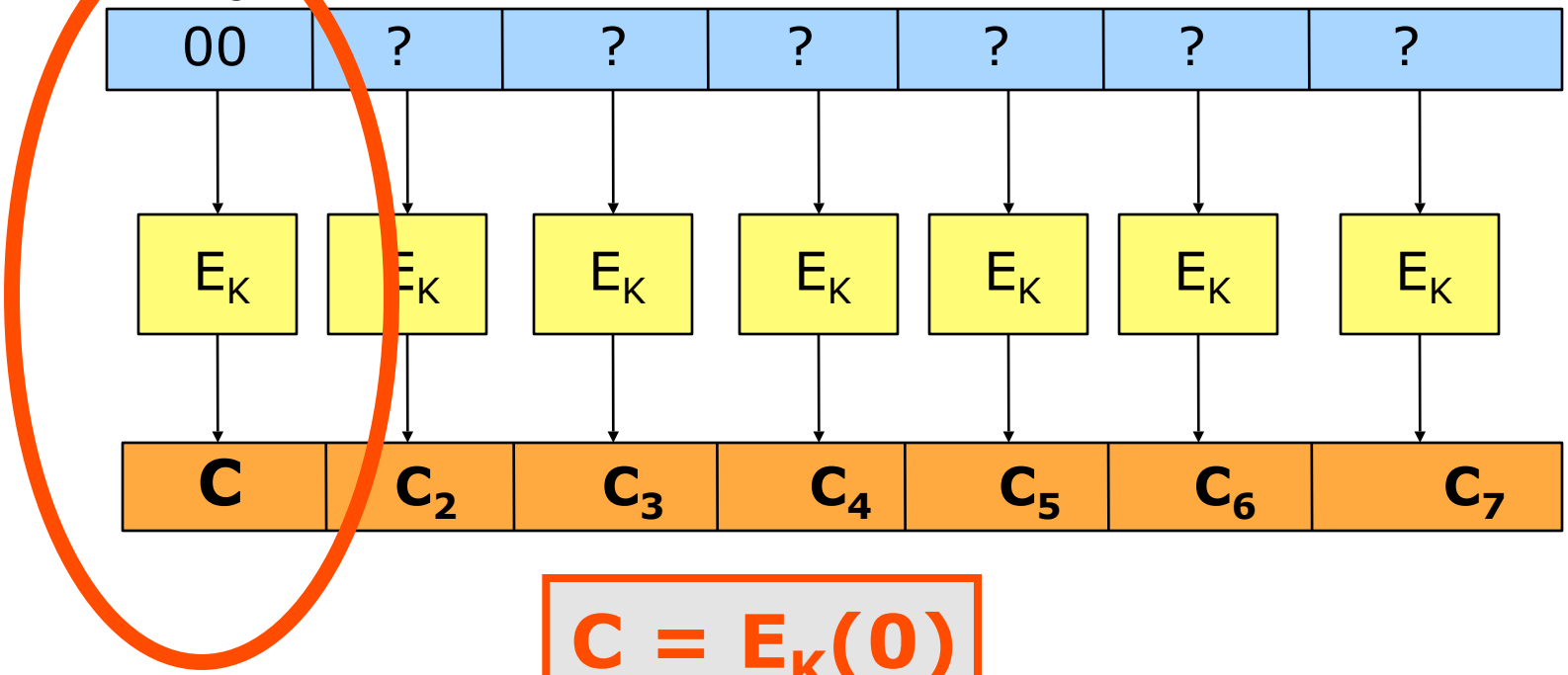
Dictionnaire

- On sait que le clair est un fichier word
  - Entête connue = clair connu !
  - Par exemple le premier bloc de clair est toujours le même



Dictionnaire

- On sait que le clair est un fichier word
  - Entête connue = clair connu !
  - Par exemple le premier bloc de clair est toujours le même



$$C = E_K(0)$$

Dictionnaire

$E_K(0)$	Clé K
C_0	0x00 … 0x00
C_1	0x00… 0x01
C_2	0x00…0x02
C	0xA6…0x3F
C_{2^k-2}	0xFF…0xFE
C_{2^k-1}	0xFF…0xFF

Dictionnaire

$E_K(0)$	Clé K
C_0	0x00 … 0x00
C_1	0x00… 0x01
C_2	0x0
C	0xA6…0x3F
C_{2^k-2}	0xFF…0xFE
C_{2^k-1}	0xFF…0xFF

On a trouvé la clé K
On peut tout déchiffrer

Dictionnaire

$E_K(0)$	Clé K
C_0	0x00 … 0x00
C_1	0x00… 0x01
C_2	0x0
C	0xA6…0x3F
C_{2^k-2}	0xFF…0xFE
C_{2^k-1}	0xFF…0xFF

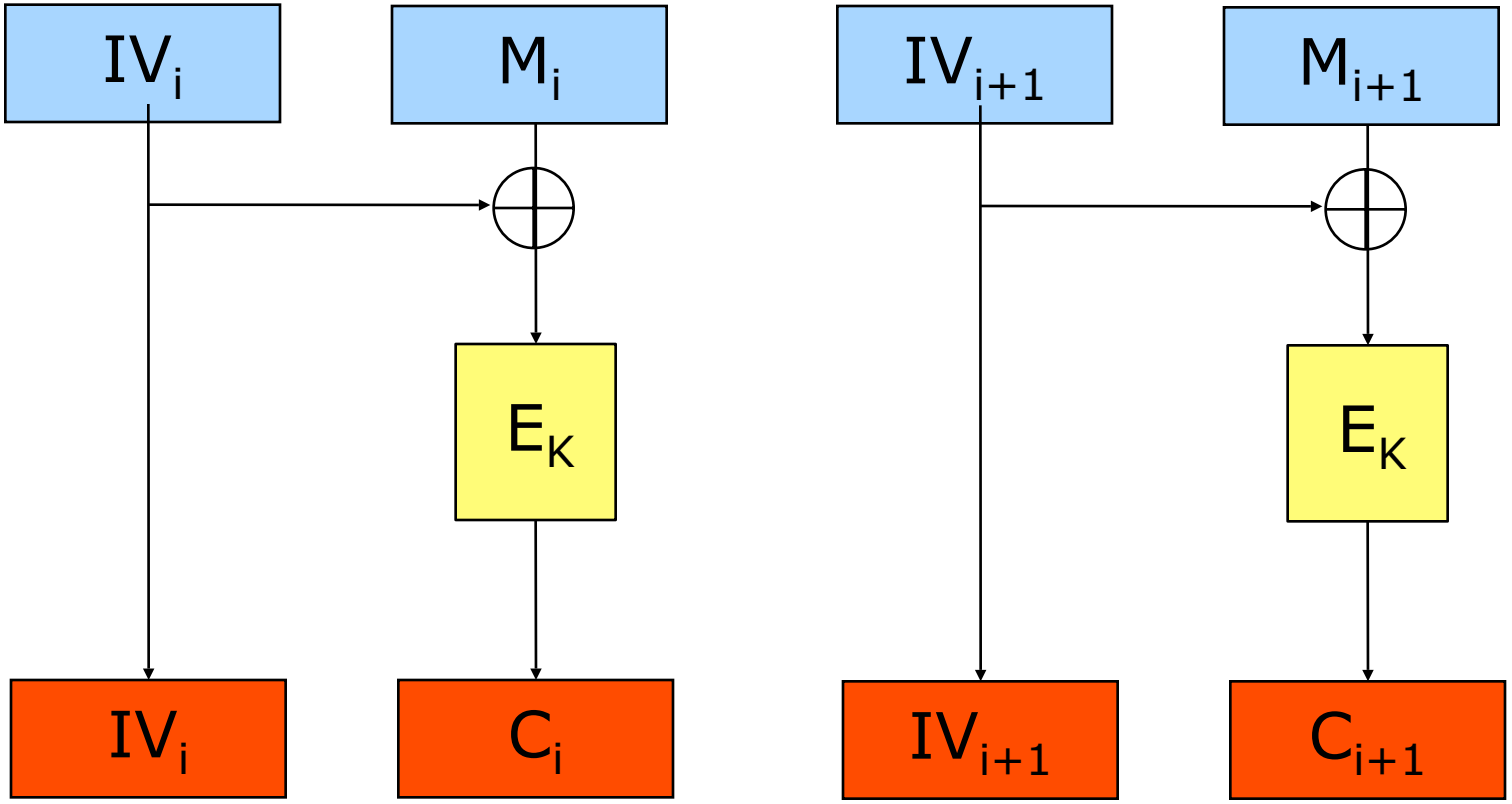
On a trouvé la clé K
On peut tout déchiffrer

Pour tous les chiffrés ultérieurs, une simple recherche dans la table permet de retrouver la clé

Solution

- « Randomiser » chaque bloc de clair
  - Chaque bloc de clair est masqué à l'aide d'une valeur aléatoire
  - Les attaques statistiques ne s'appliquent plus
    - Tous les blocs d'entrée sont équiprobables
    - Toutes les valeurs de sortie peuvent être atteinte avec même probabilité
  - Pour chaque chiffré, une recherche exhaustive doit être faite : attaque par dictionnaire évitée

Vers le mode CBC

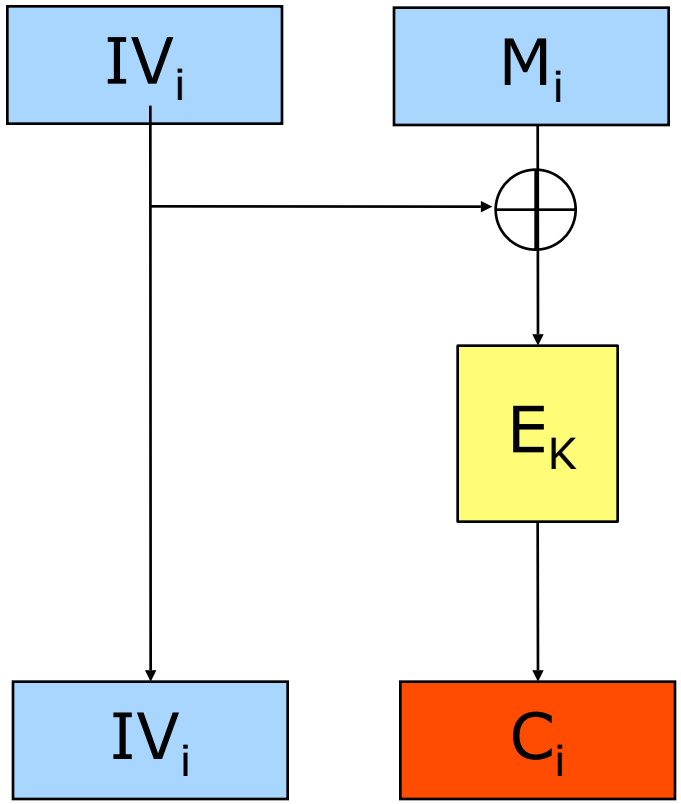


Vers le mode CBC

- Chiffrement du même message avec IV différents : chiffrés différents, impossible de savoir qu'ils correspondent au même clair
- **Problème** : le chiffré est deux fois plus long que le clair
- **Idée** : si la primitive est « sûre » ses sorties peuvent être considérées comme des valeurs aléatoires

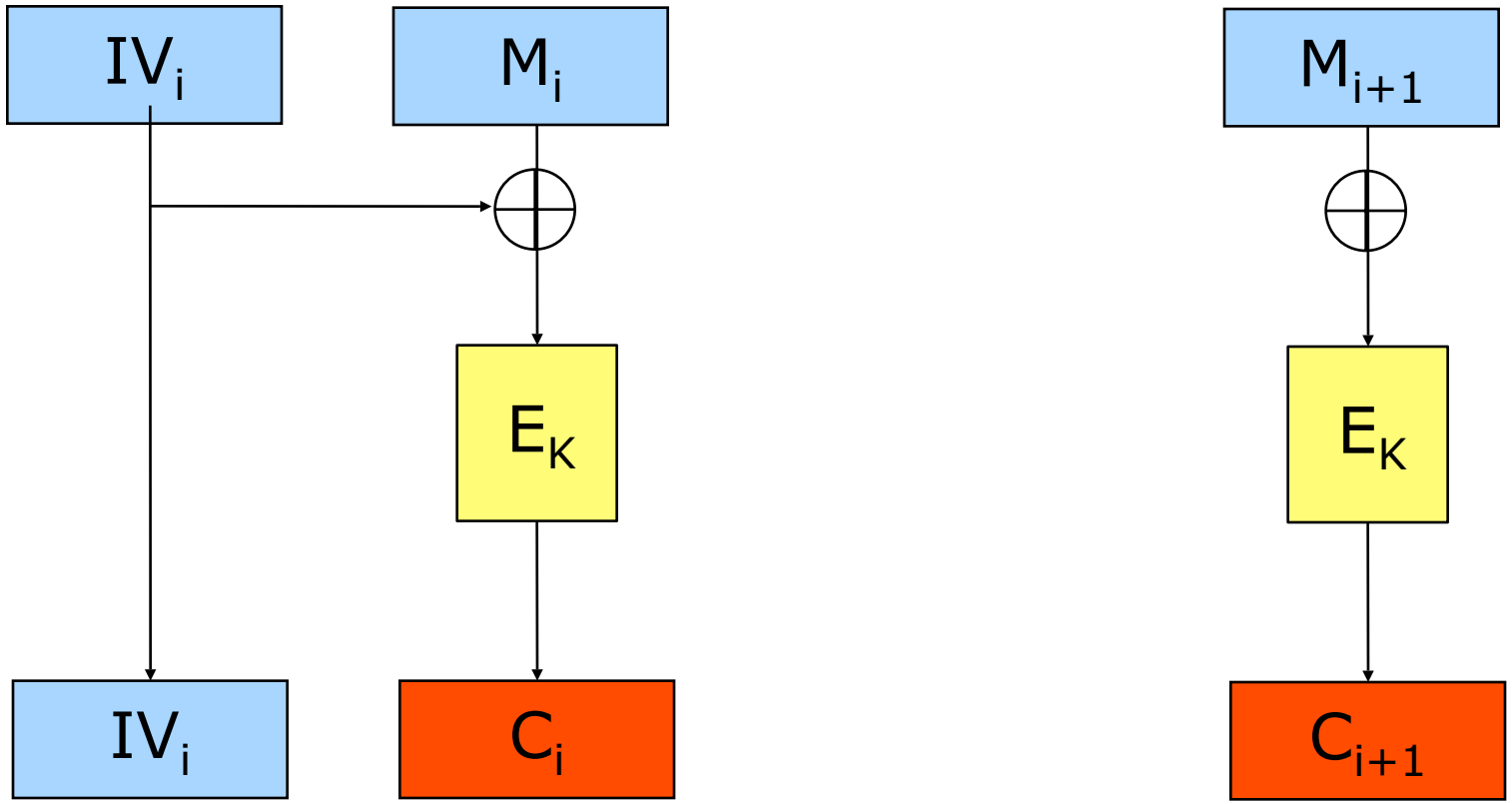
Le mode CBC

- On pose donc $IV_{i+1} = C_i$



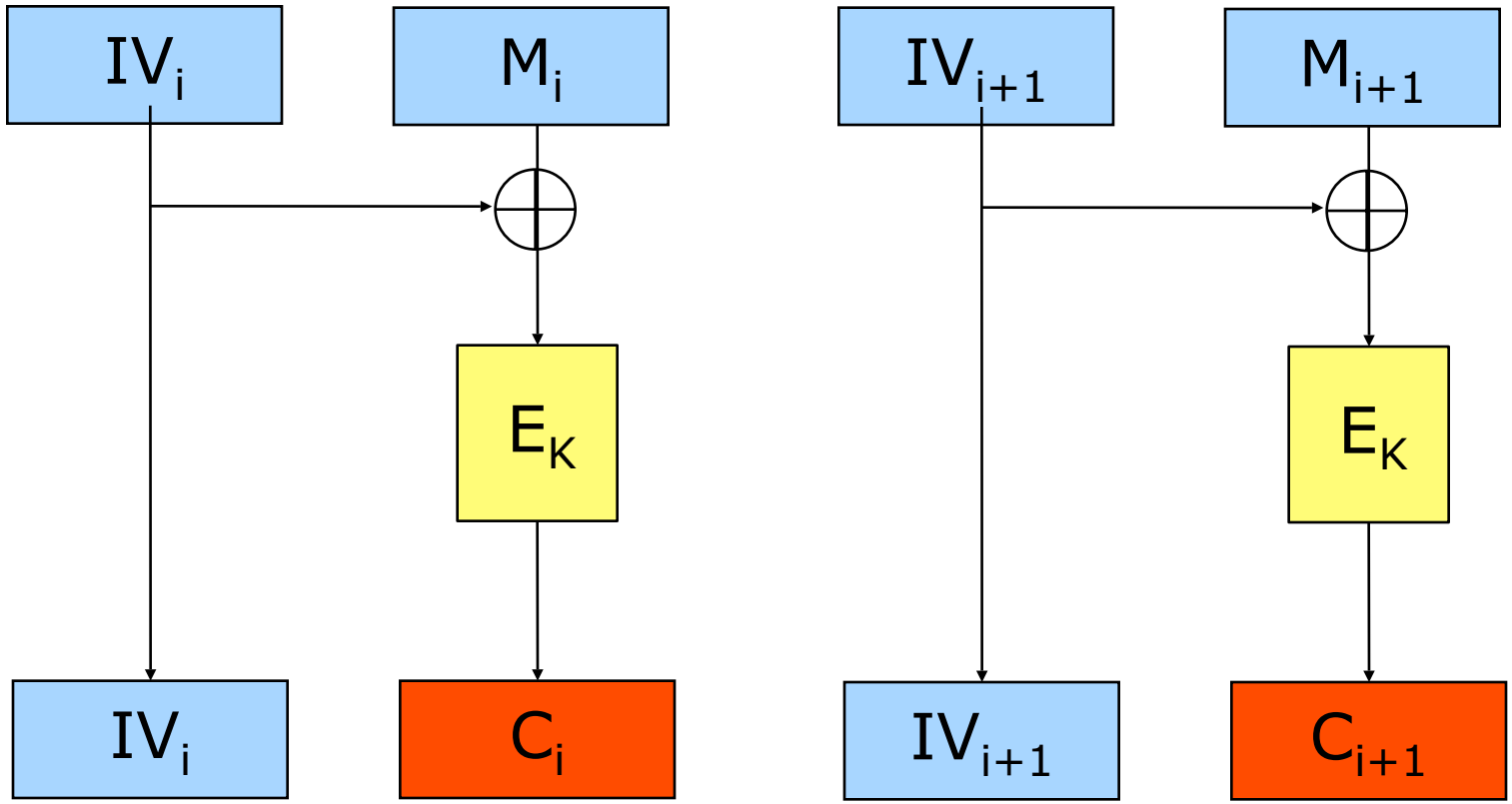
Le mode CBC

- On pose donc $IV_{i+1} = C_i$



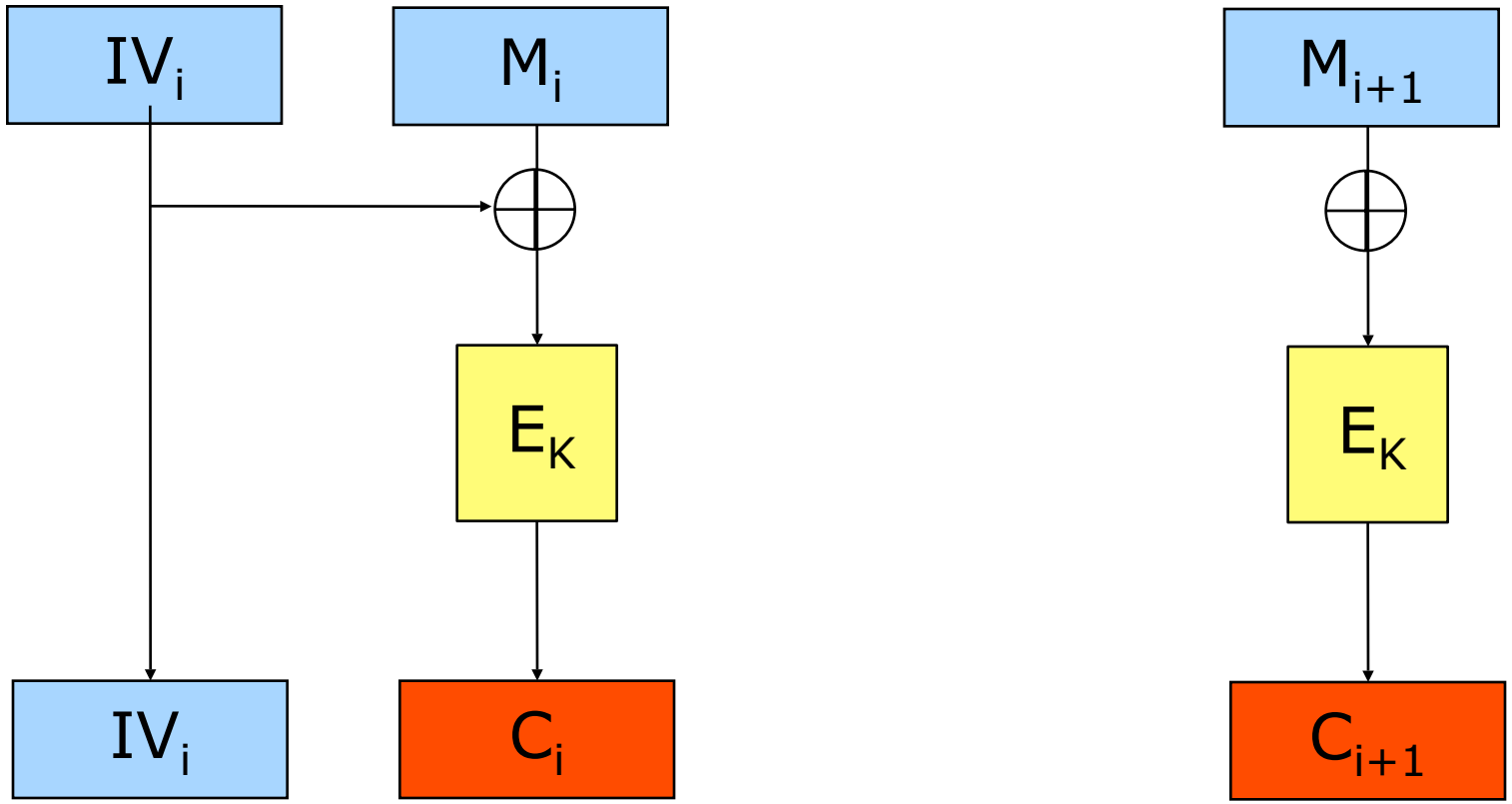
Le mode CBC

- On pose donc $IV_{i+1} = C_i$



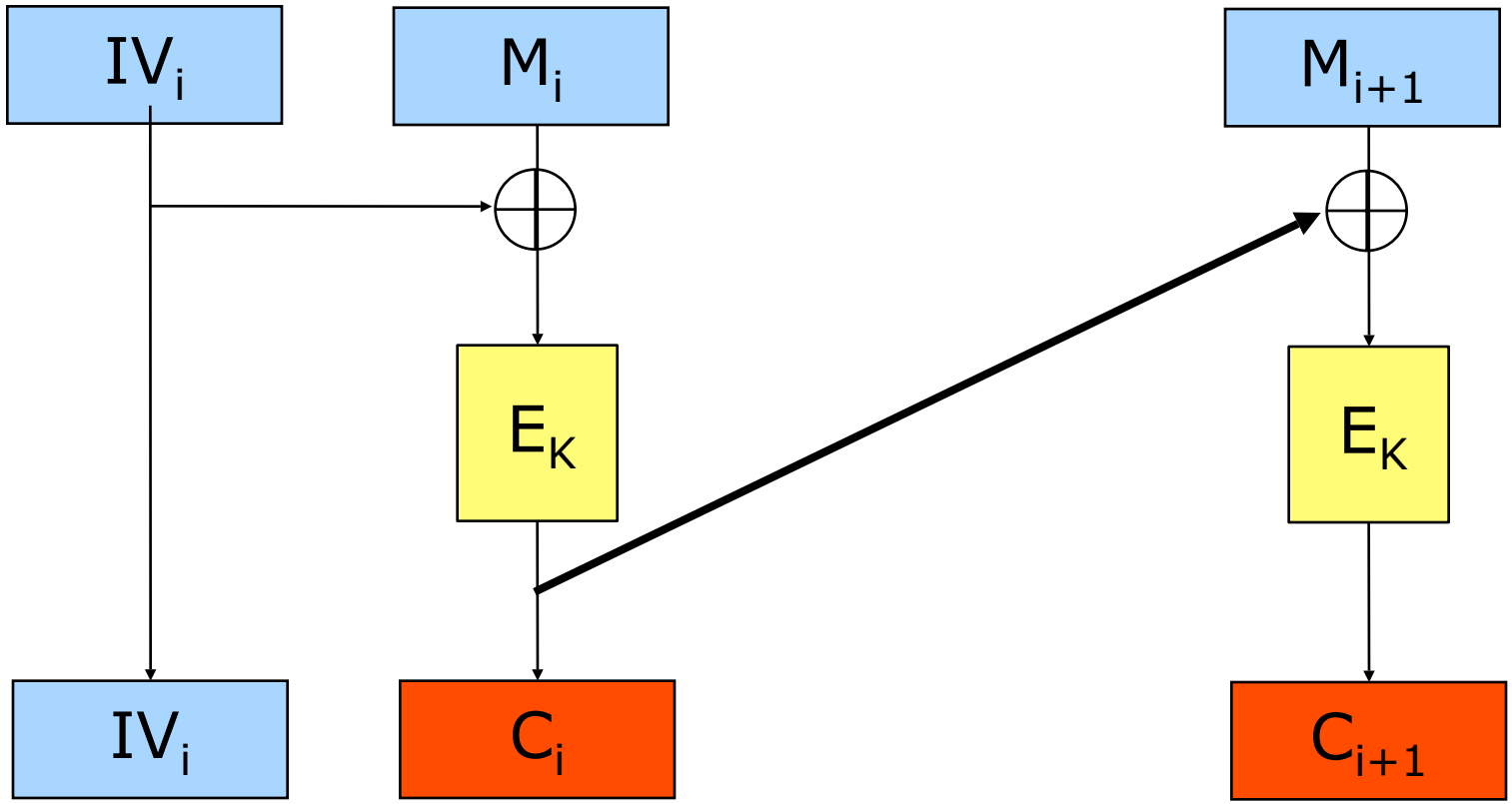
Le mode CBC

- On pose donc $IV_{i+1} = C_i$



Le mode CBC

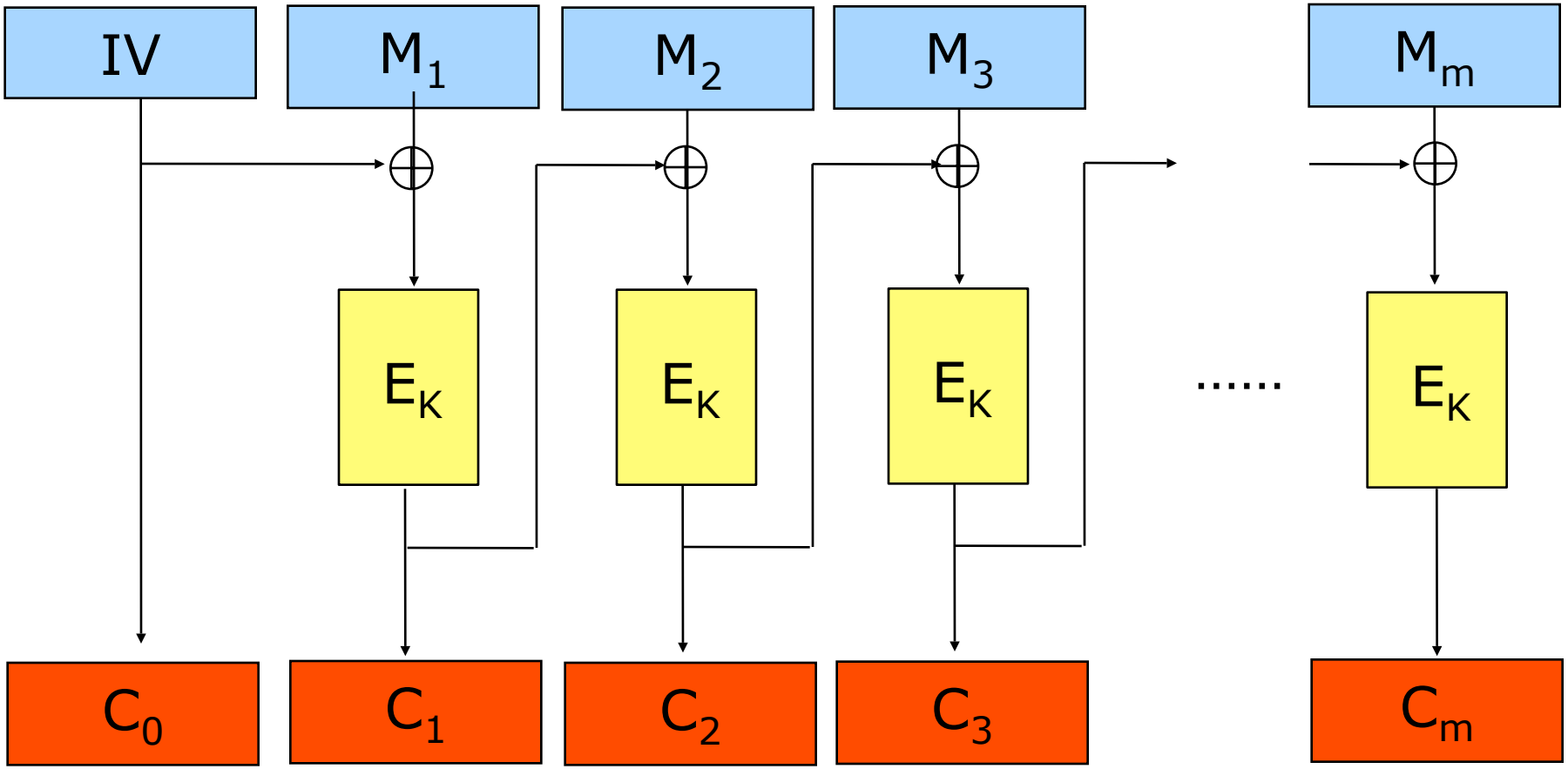
- On pose donc $IV_{i+1} = C_i$



Amélioration

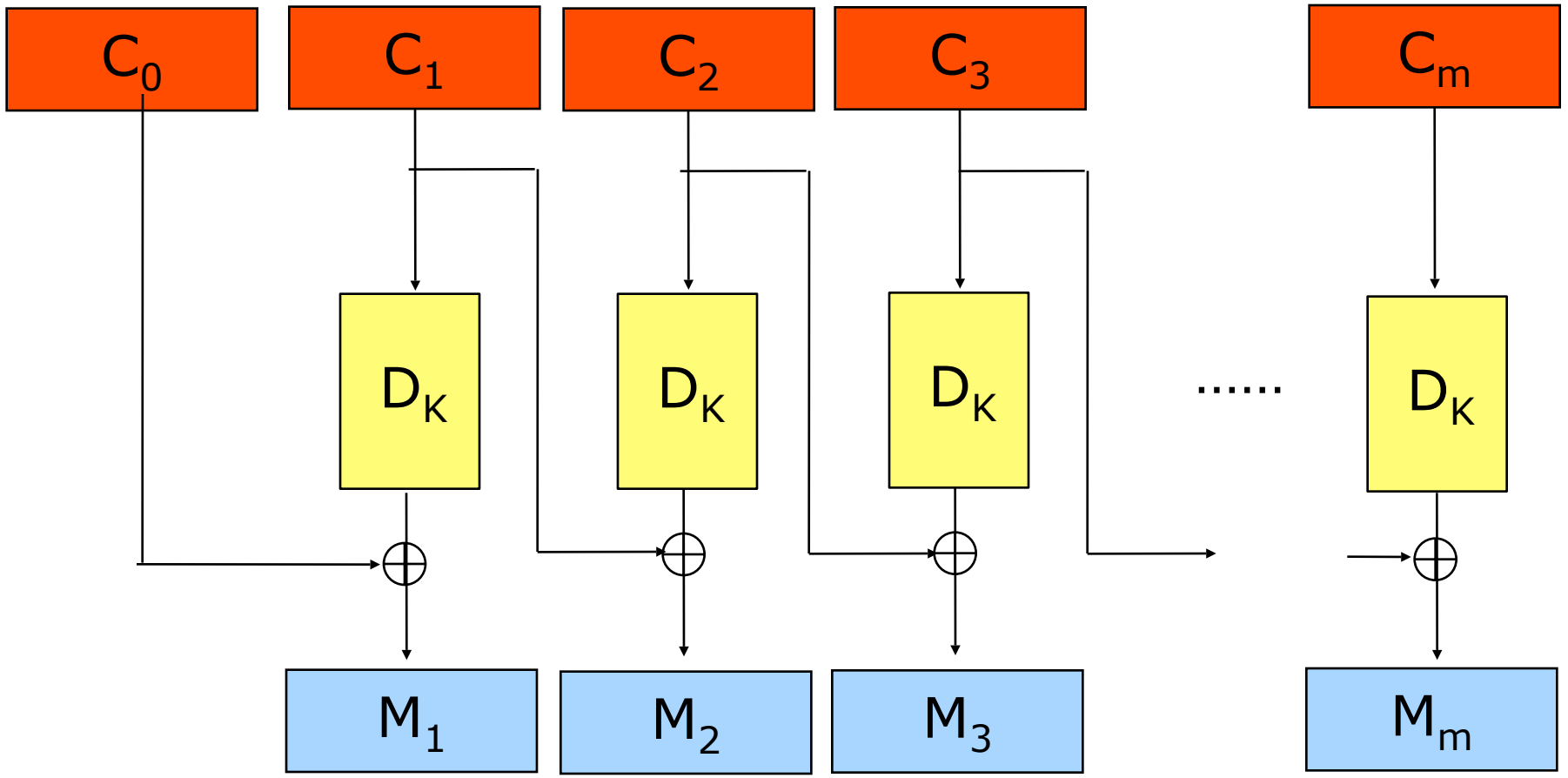
- Le bloc de chiffré précédent est utilisé pour randomiser le bloc de clair
- Optimisation de la bande passante
- Correct si la primitive a de bonnes propriétés cryptographiques
  - **indistinguabilité entre les sorties de la primitive et celles d'une permutation aléatoire**

Le mode CBC

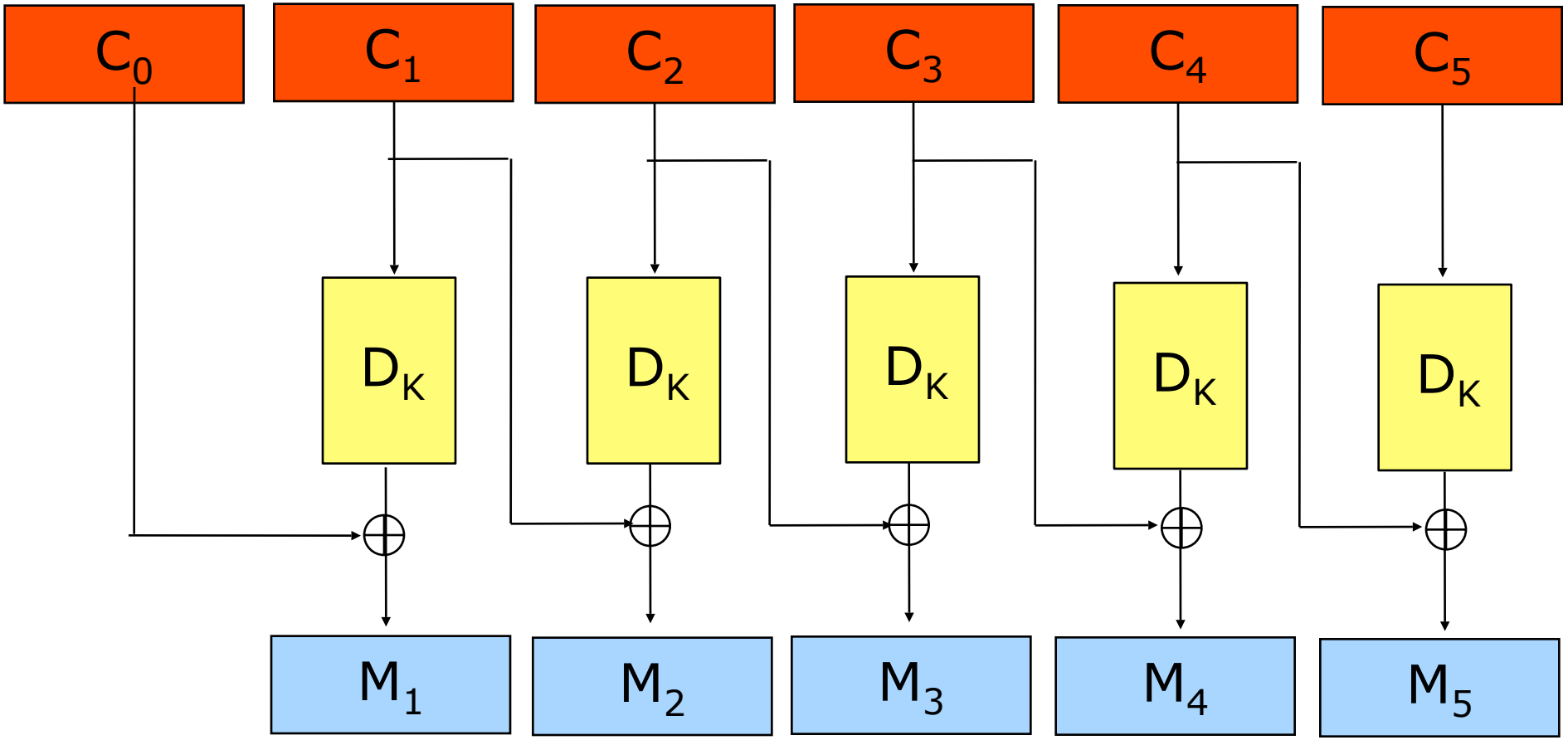


$C_0 = IV \quad et \quad C_i = E_K(C_{i-1} \oplus M_i)$

Déchiffrement CBC

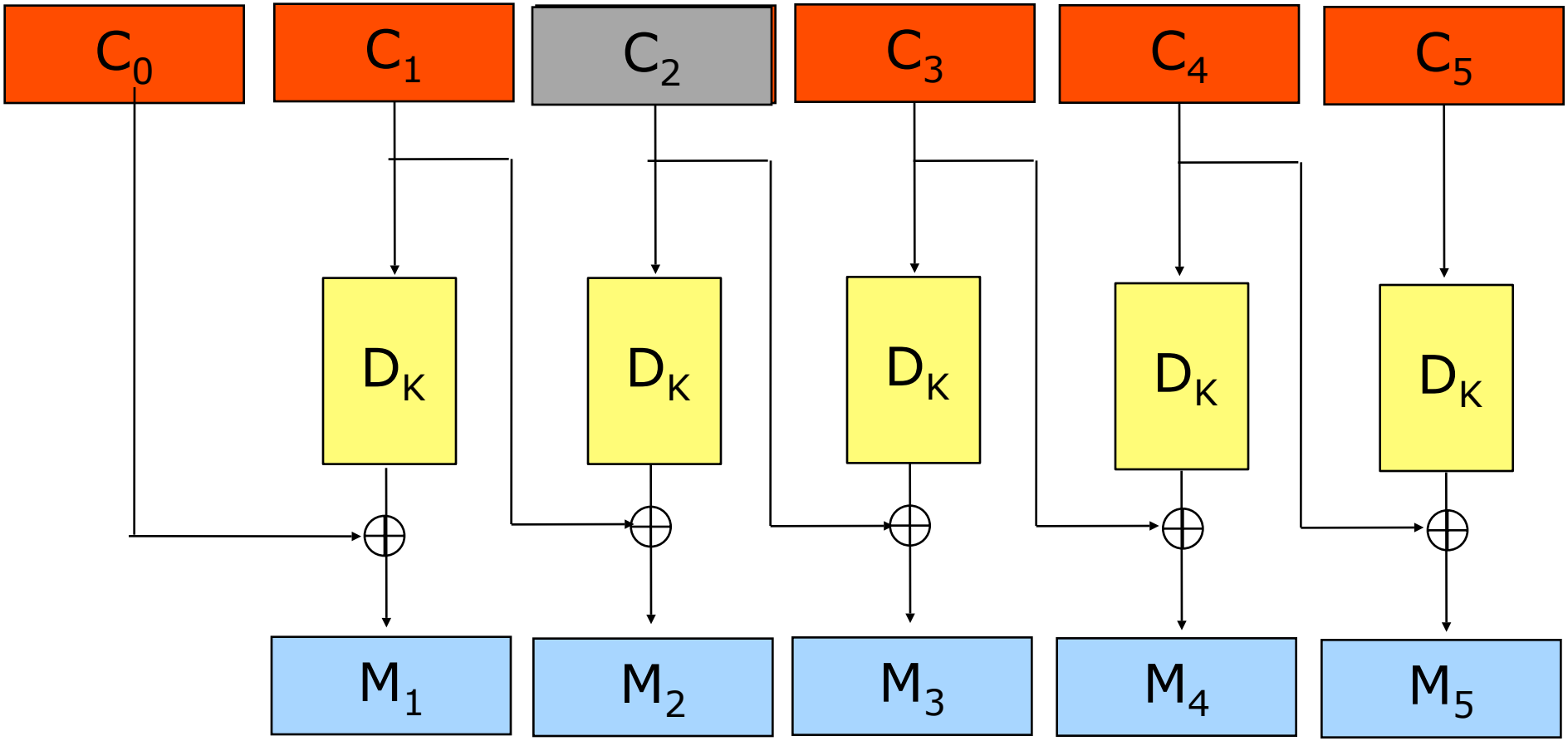


Propagation d'erreur



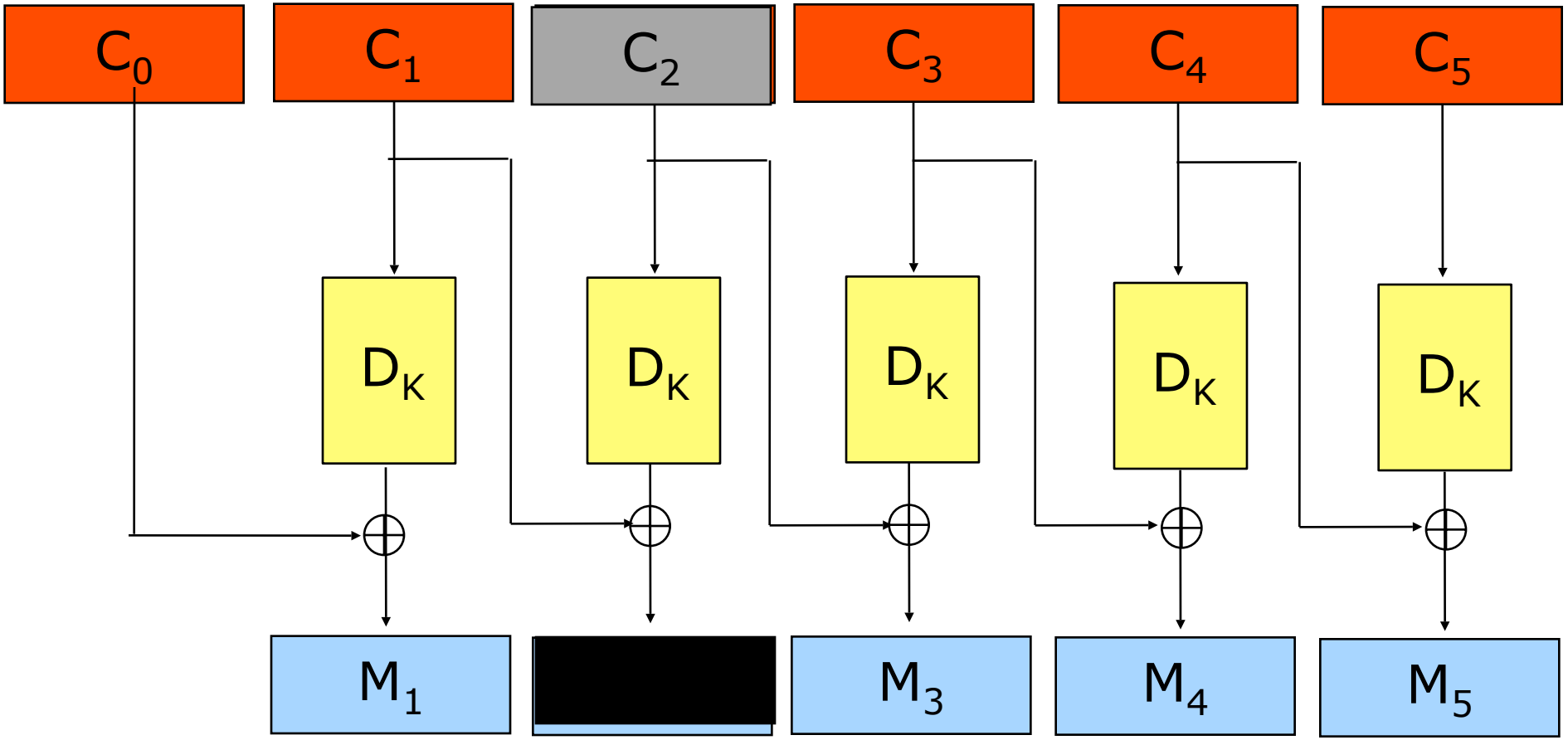
Propagation d'erreur limitée en déchiffrement

Propagation d'erreur



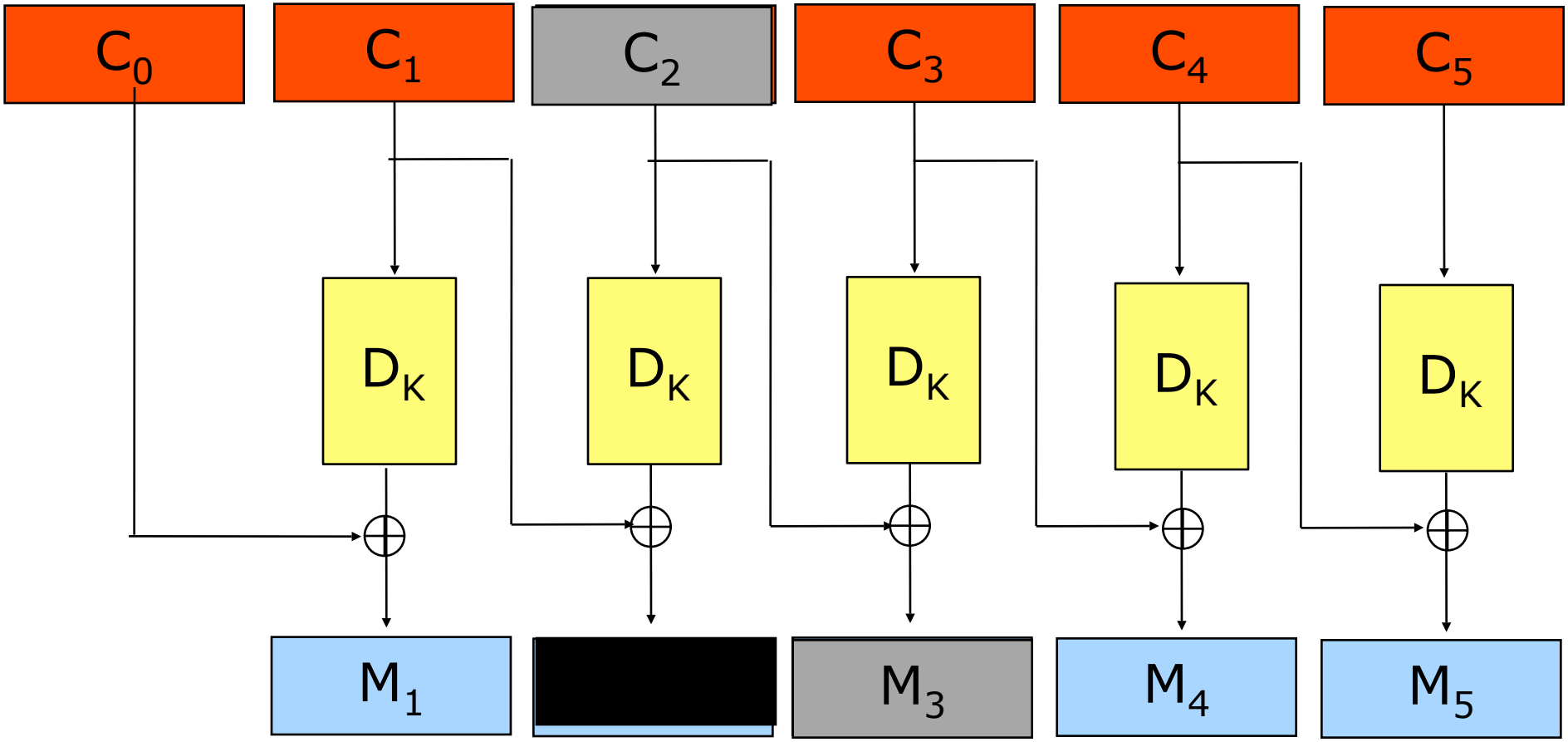
Propagation d'erreur limitée en déchiffrement

Propagation d'erreur



Propagation d'erreur limitée en déchiffrement

Propagation d'erreur



Propagation d'erreur limitée en déchiffrement

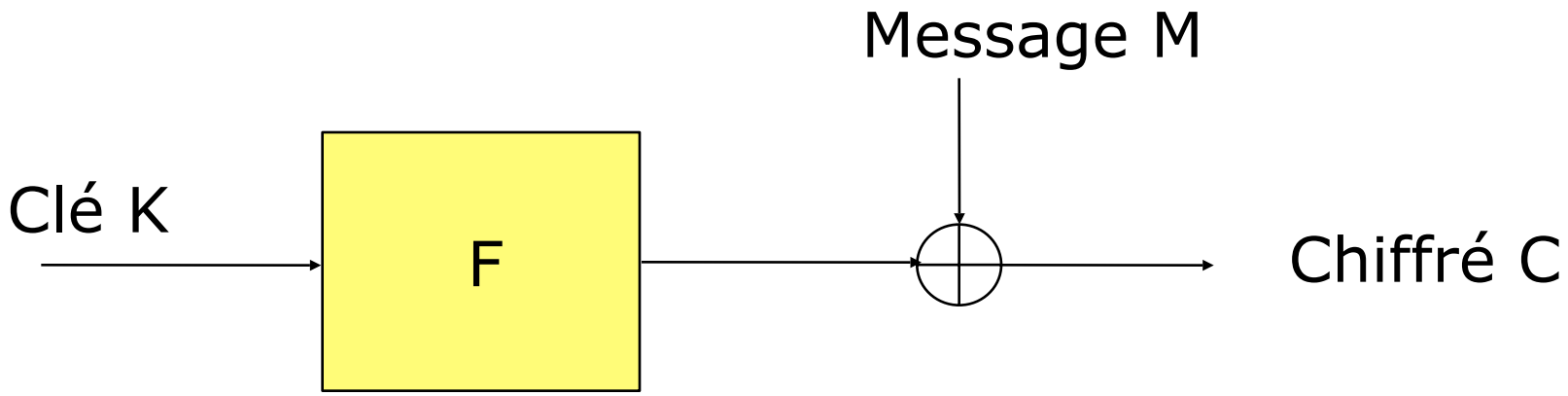
Propriétés du mode CBC

- **Pas d'état, mode probabiliste** (randomisé) : pour un même clair, chiffrés différents si l'IV choisi est différent
- **Non parallélisable**
- **Expansion** : le chiffré possède un bloc de plus que le clair
- **Gestion de l'IV** : transmis en clair avec le chiffré, valeur non prédictible
- **Propagation d'erreurs limitée en déchiffrement** : une erreur sur le bloc chiffré C_i modifie les clairs M_i et M_{i+1} seulement

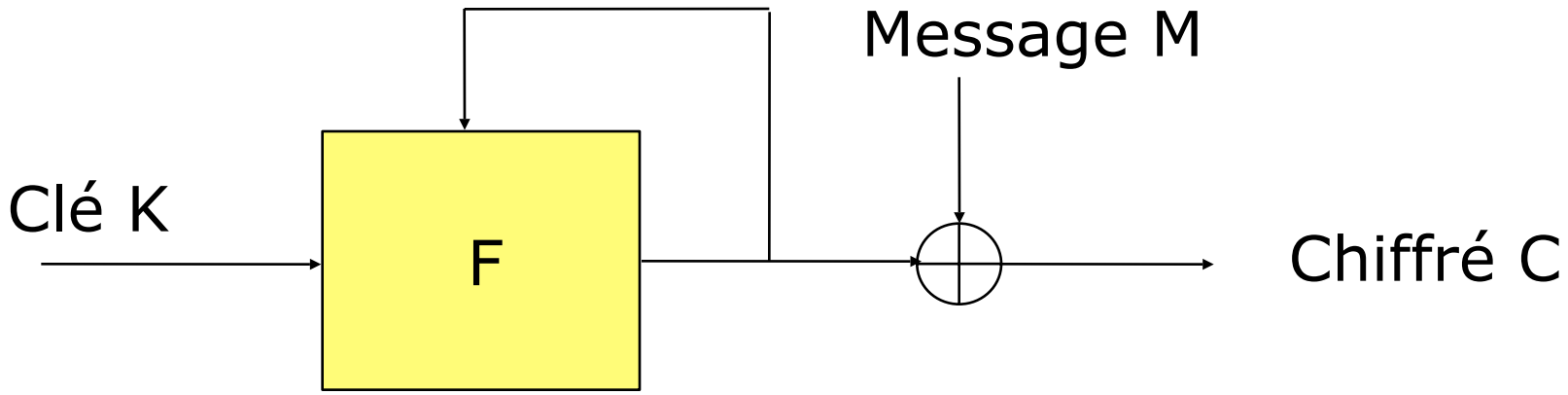
Autres modes

- Normalisation du NIST : modes pour le DES, puis modes pour l'AES
- Modes stream :
  - on génère un flux additionné bit à bit avec le message clair
  - Plus coûteux qu'un stream
  - Sécurité souvent meilleure (pas de bonnes pratiques pour les stream ciphers)
  - La fonction $D=E^{-1}$ n'est pas utilisée

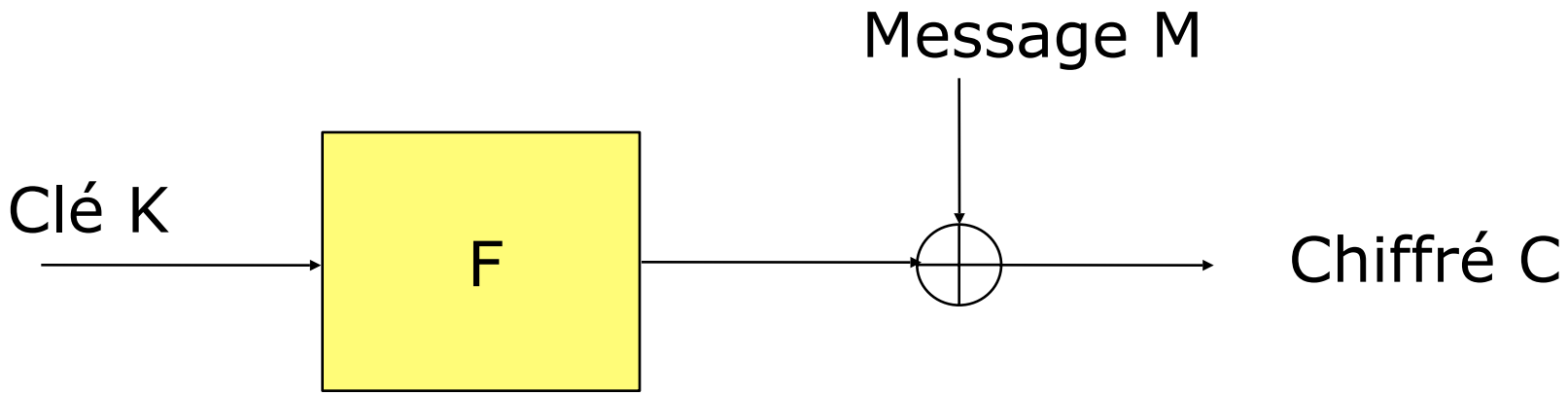
Modes stream



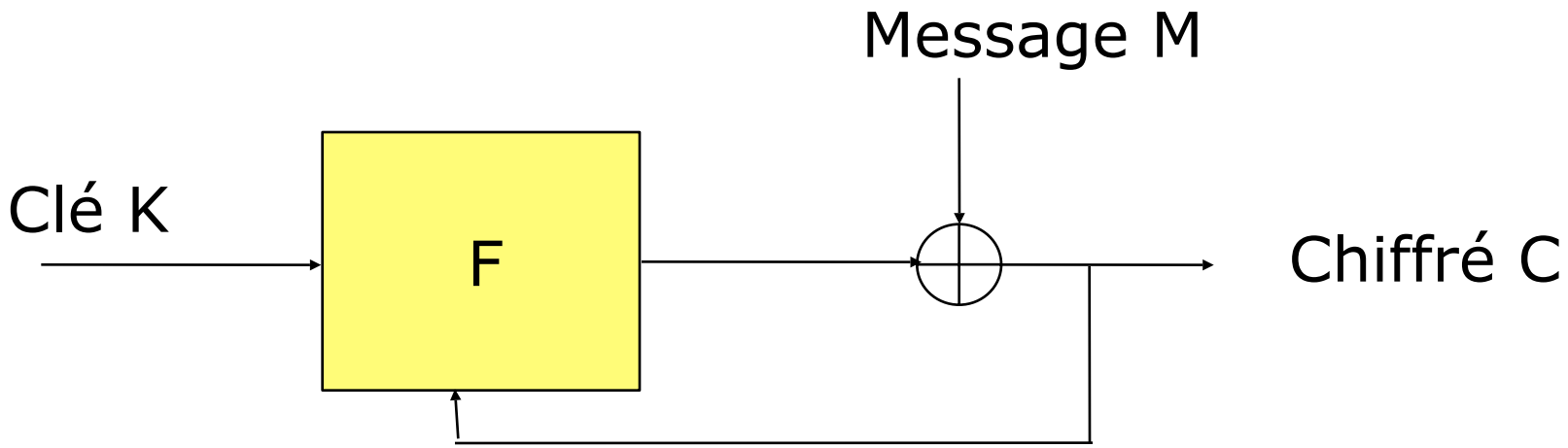
Modes stream



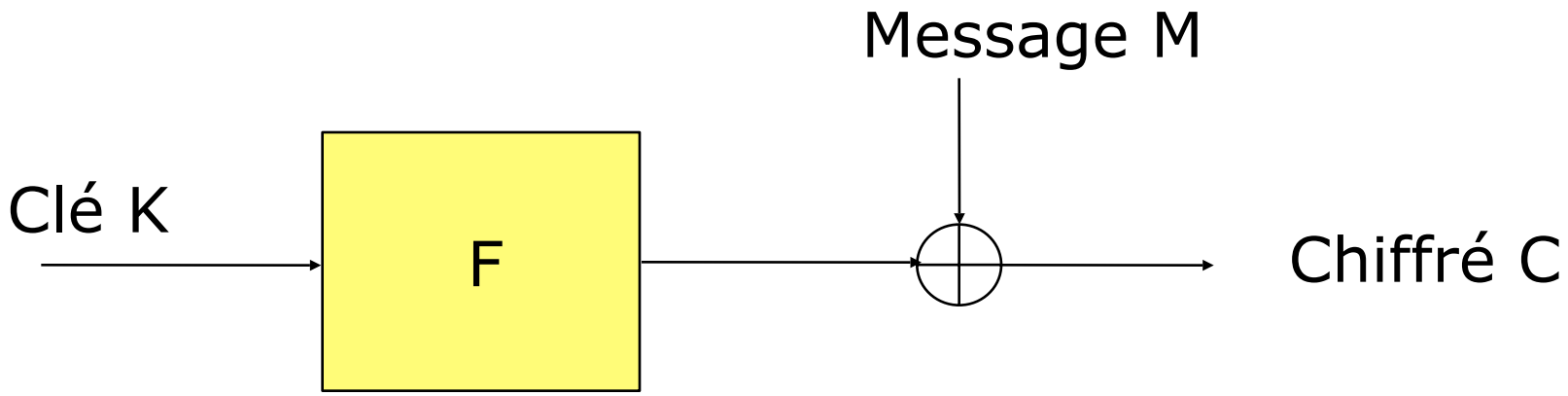
Modes stream



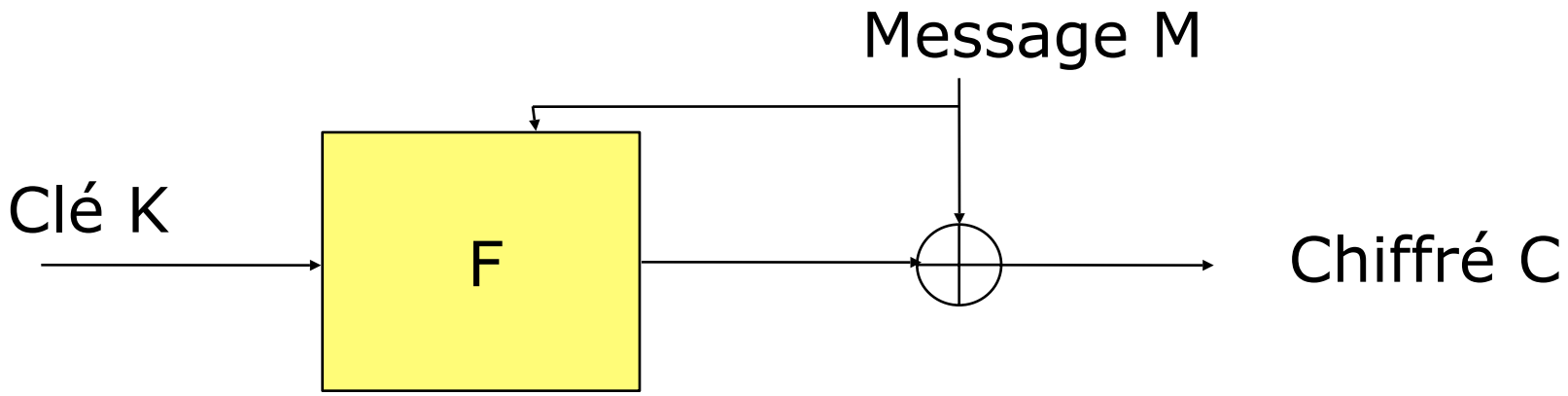
Modes stream



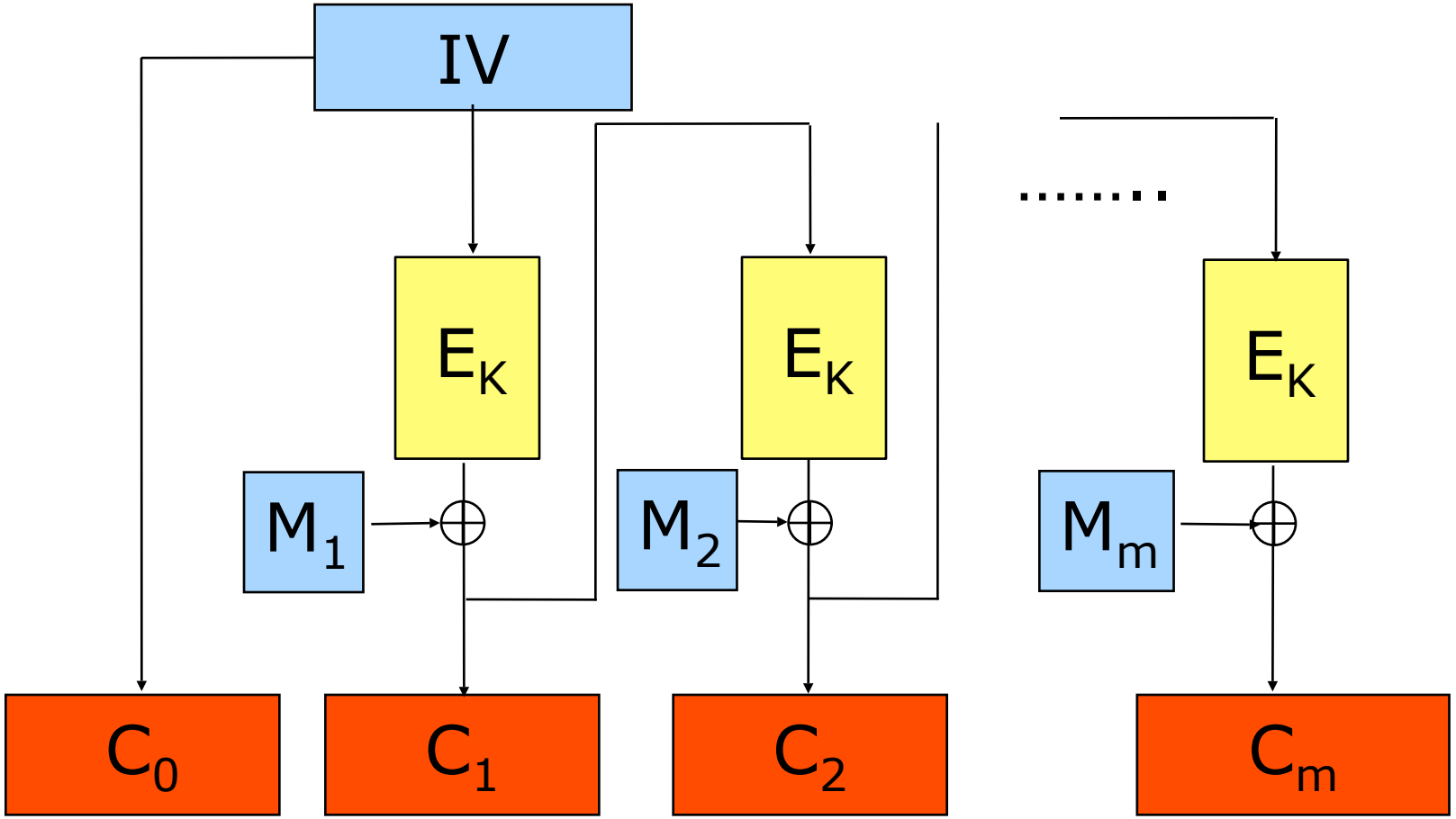
Modes stream



Modes stream



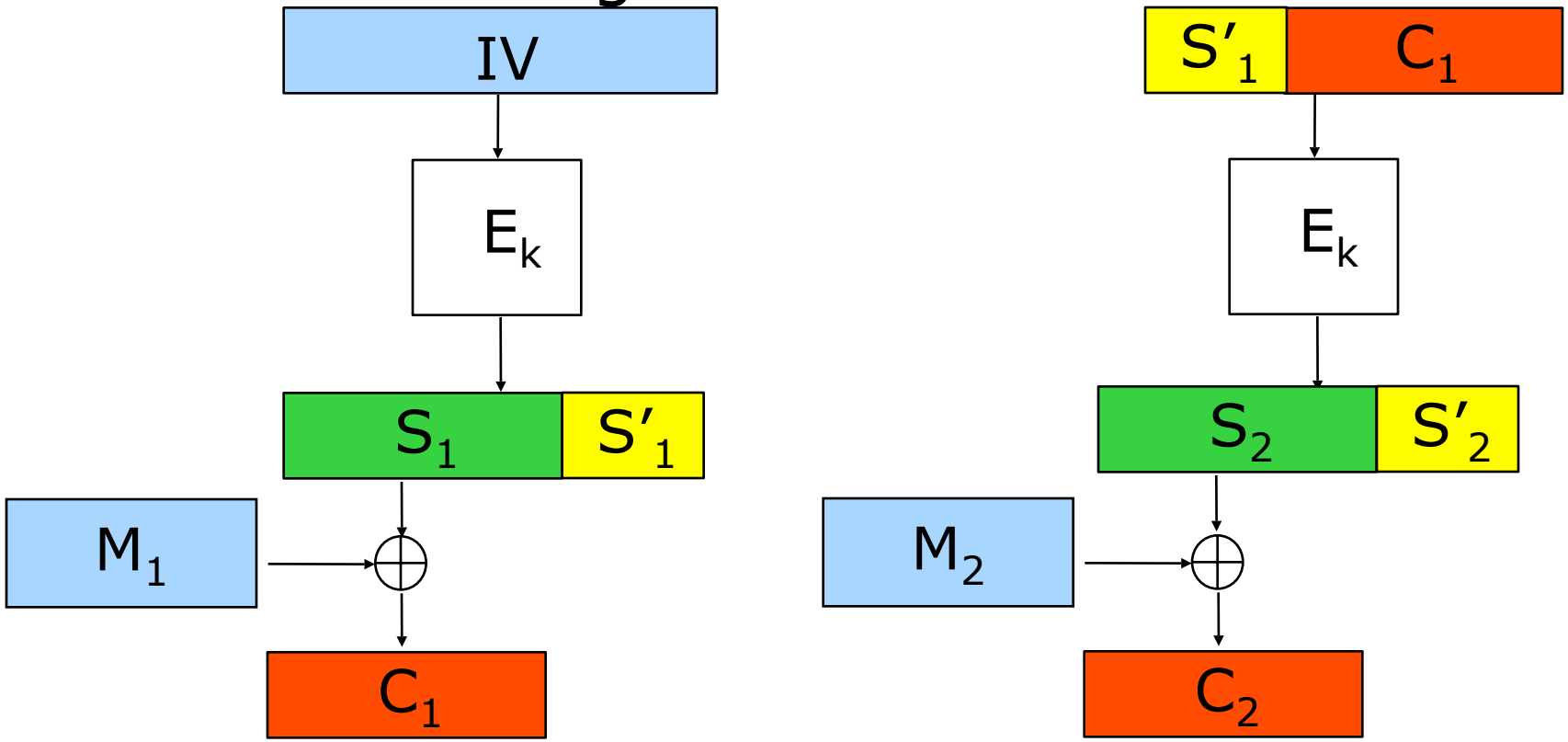
CFB : Cipher FeedBack



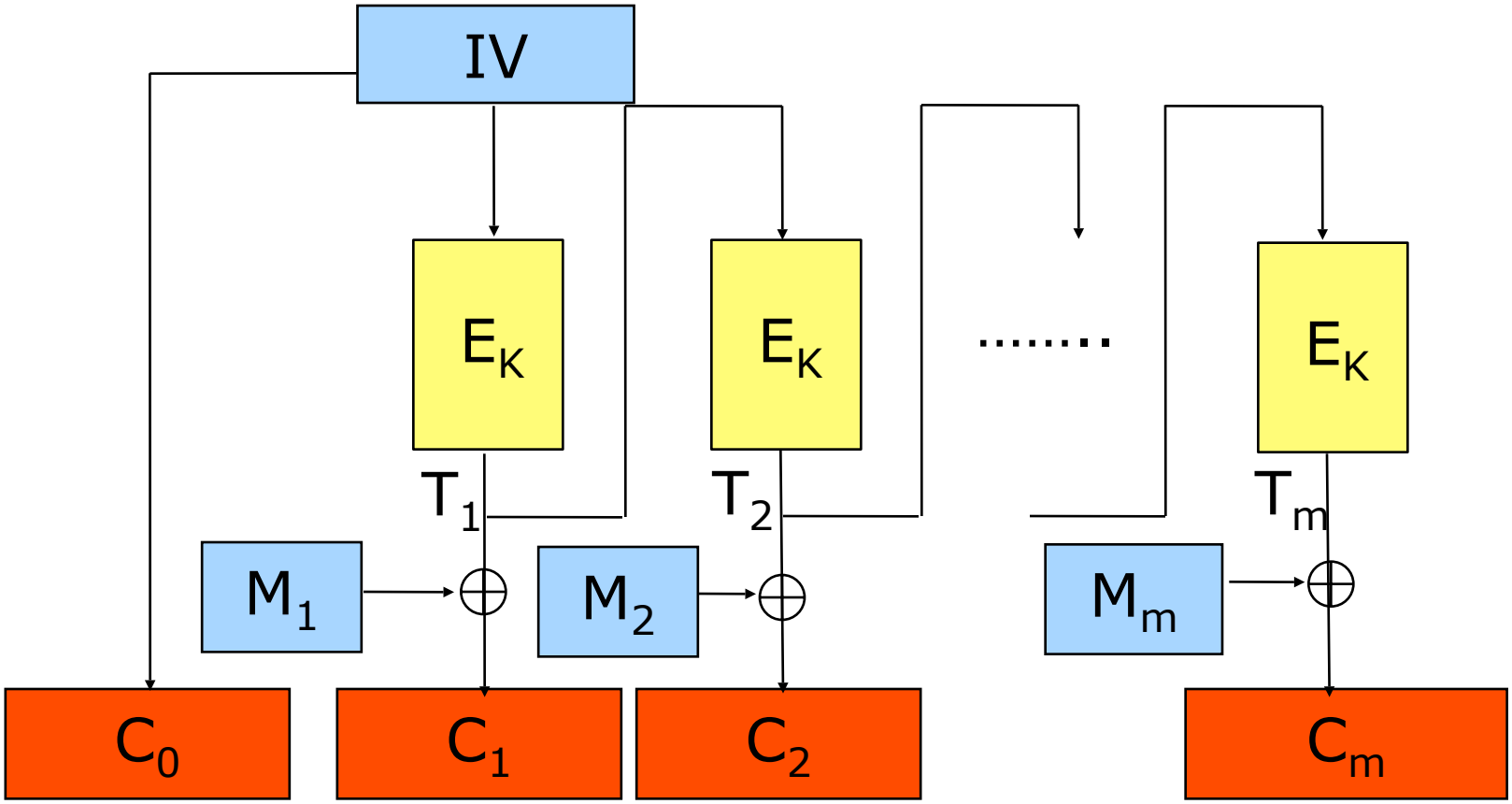
$$C_0 = IV \quad et \quad C_i = E_K(C_{i-1}) \oplus M_i$$

Variante du CFB

- Sorties du block cipher tronquées à r bits, r<n,
- Blocs de messages de r bits



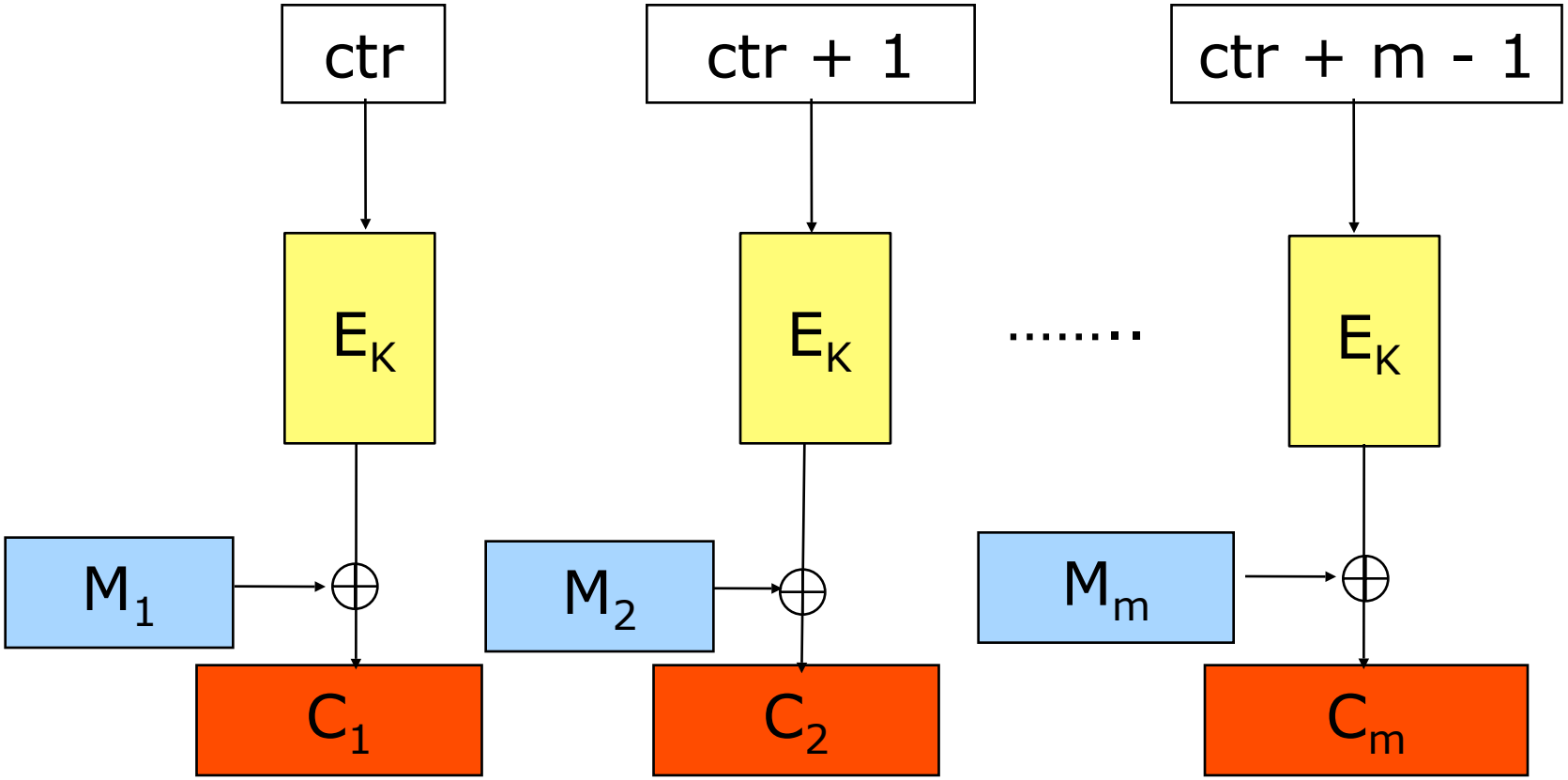
Mode OFB



$$T_0 = IV,\ T_i = E_K(T_{i-1})$$

$$C_0 = IV \text{ et } C_i = T_i \oplus M_i$$

Mode compteur



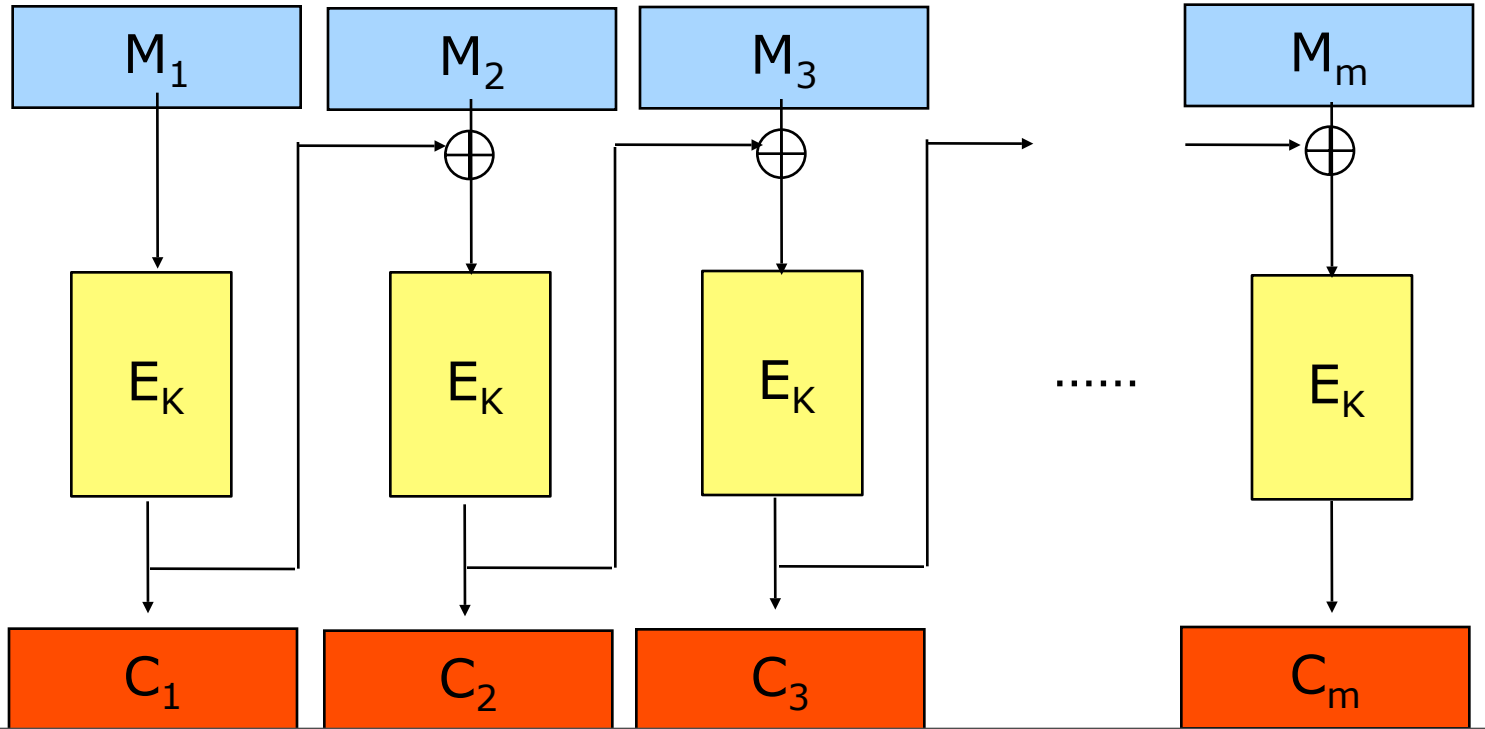
$$C_i = E_K (ctr + i - 1) \oplus M_i$$

$$M_i = E_K(ctr + i - 1) \oplus C_i$$

Le mode de chiffrement CBC

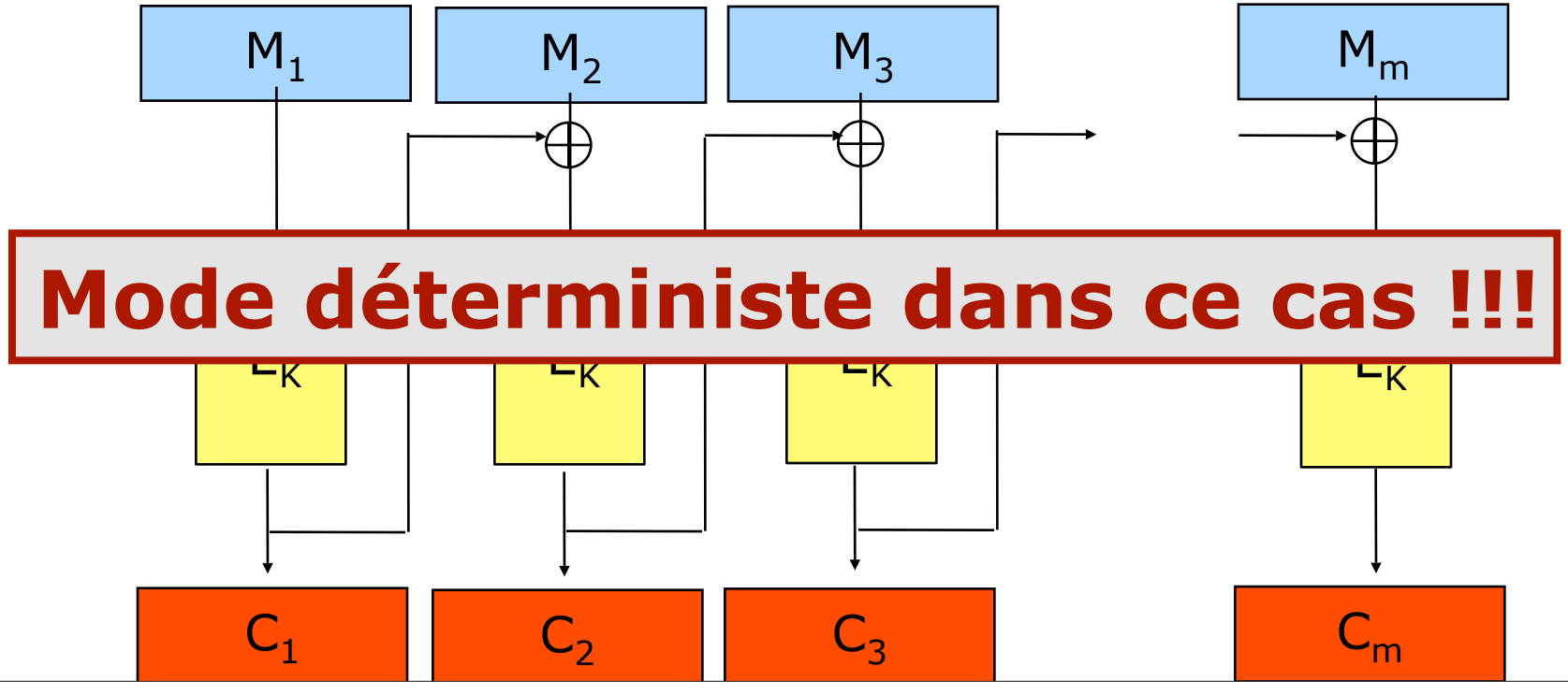
Gestion de la valeur initiale

- Confidentialité non nécessaire pour l'IV : transmis en clair
- Doit être imprédictible : pas de valeur constante ou nulle !



Gestion de la valeur initiale

- Confidentialité non nécessaire pour l'IV : transmis en clair
- Doit être imprédictible : pas de valeur constante ou nulle !

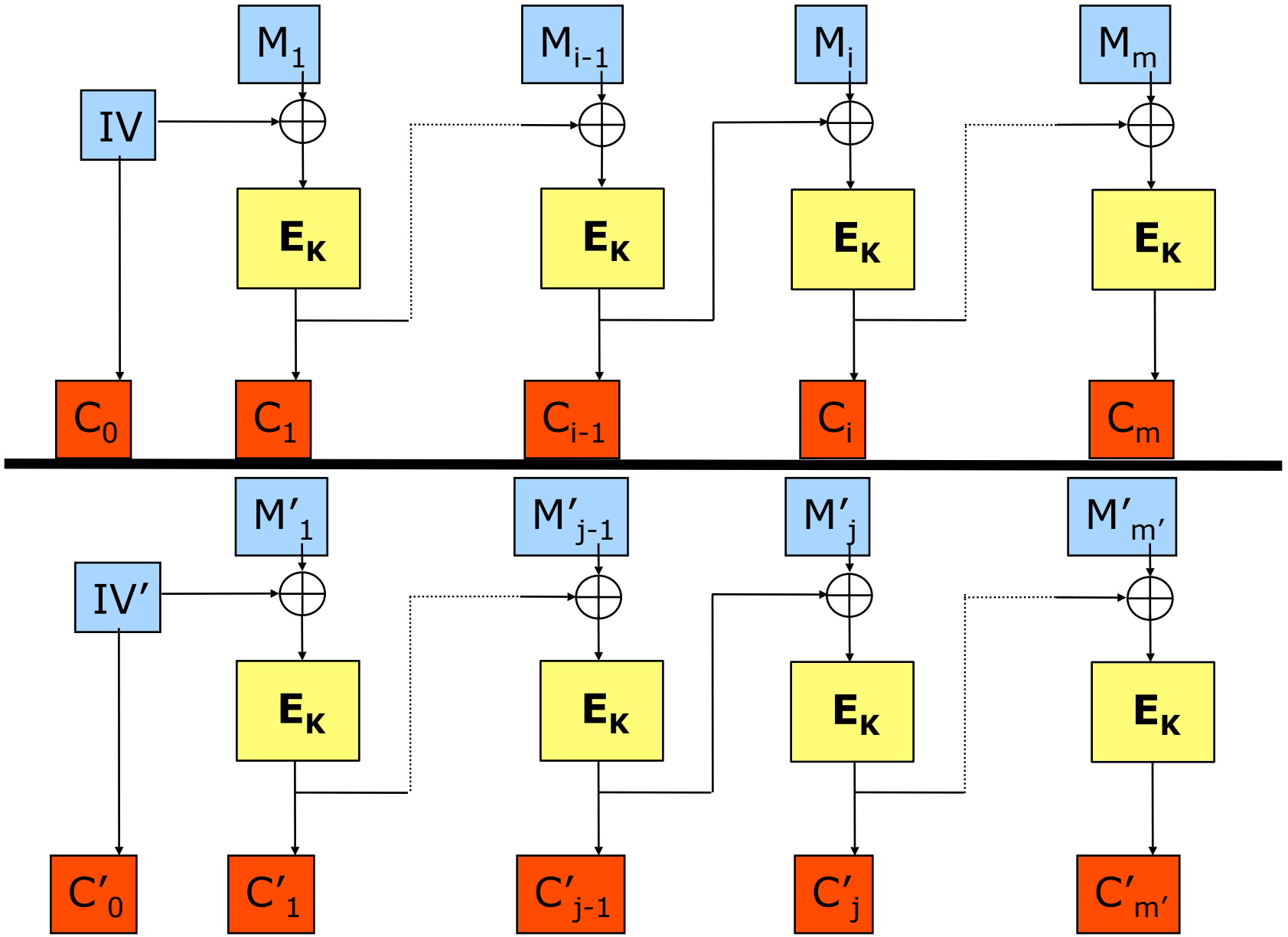


Sécurité du mode de chiffrement CBC

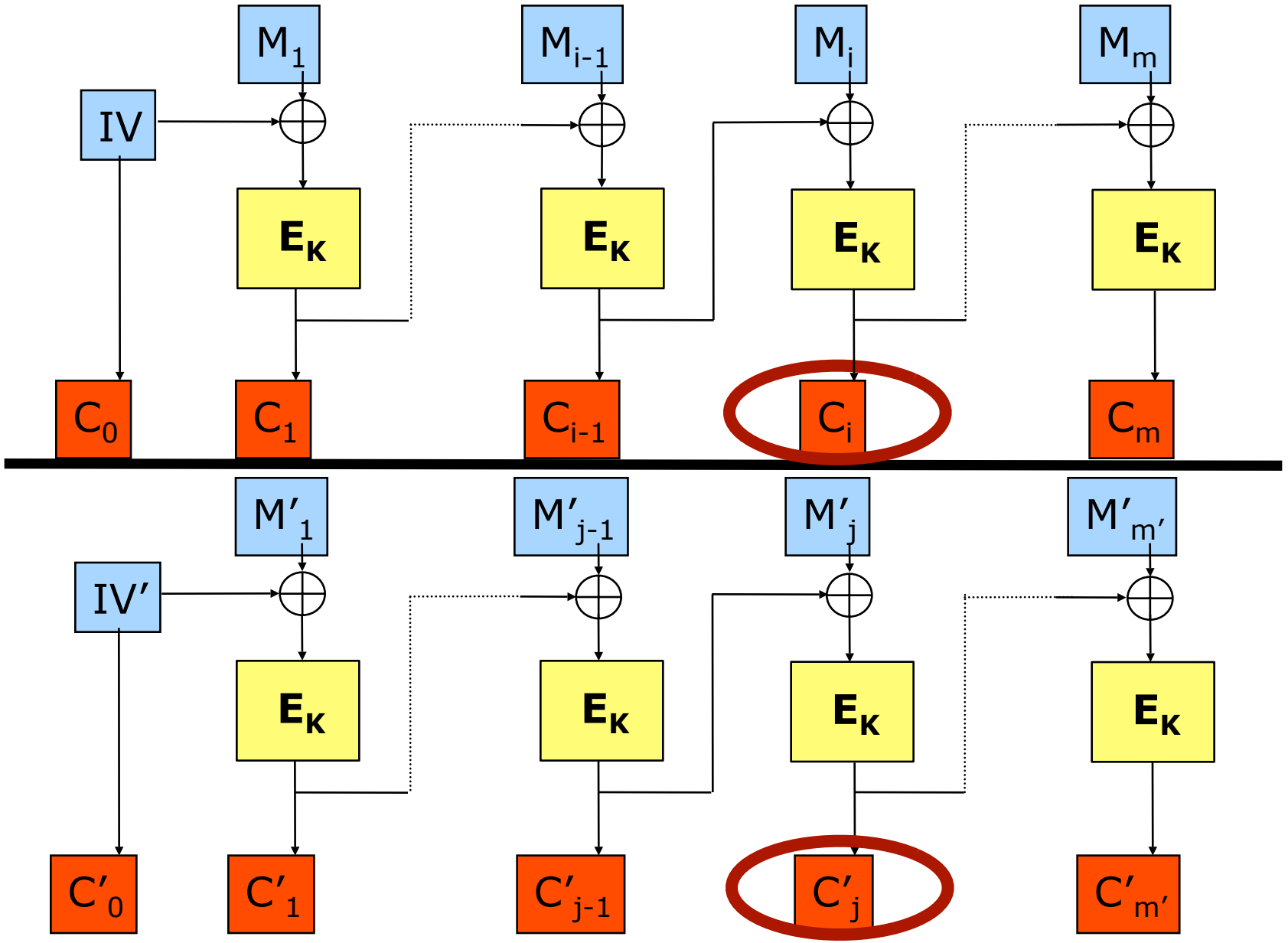
Sécurité du mode CBC

- Que se passe-t-il si deux blocs de chiffré collisionnent ?
- Quelle fuite d'info peut-on tolérer ?

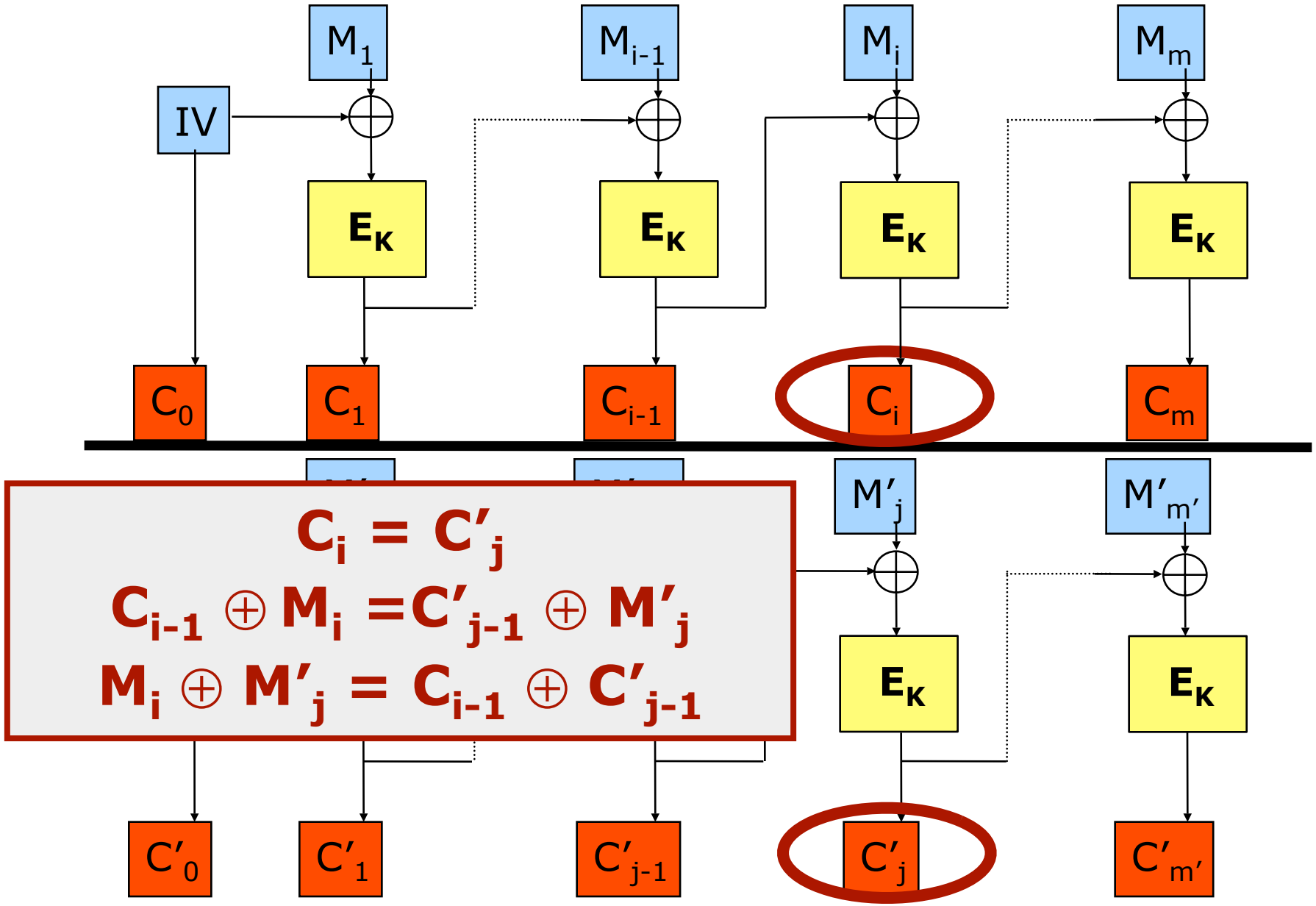
Sécurité du mode CBC



Sécurité du mode CBC



Sécurité du mode CBC



$$C_i = C'_j$$

$$C_{i-1} \oplus M_i = C'_{j-1} \oplus M'_j$$

$$M_i \oplus M'_j = C_{i-1} \oplus C'_{j-1}$$

Sécurité du CBC

- Si deux blocs collisionnent, de l'information fuit : on obtient une relation linéaire entre deux blocs de clair

$$M_i \oplus M_j = C_{i-1} \oplus C_{j-1}$$

- La confidentialité au sens le plus fort n'est plus assurée
- Quelle est la probabilité qu'une telle collision se produise ?

Paradoxe des anniversaires

- Les collisions se font sur des blocs de n bits
  - 2^n valeurs possibles
  - La primitive E est « sûre » : toutes ces valeurs sont équiprobables

- Dès que $\sqrt{2^n} = 2^{n/2}$ blocs ont été chiffrés, deux d'entre eux collisionnent avec forte probabilité

Sécurité du mode CBC

- Quand $2^{n/2}$ blocs ont été chiffrés, de l'information fuit
- **Importance de la taille des blocs pour la primitive E**
- En pratique :
  - Pour le DES : 2^{32} blocs avant une collision
    - Très réaliste sur un réseau gigabit
    - Discutable sur une carte à puce
  - Pour l'AES : 2^{64} blocs avant collision, pas de risque pratique

Paradoxe des anniversaires

- Permet d'estimer la quantité de données à traiter avant qu'une collision n'aie lieu
  - Fort intérêt en crypto :
    - Cryptanalyse de modes opératoires de chiffrement
    - Reste à exploiter les collisions
    - Impact pratique : dépend fortement du contexte
- La sécurité au delà de la borne est très difficile à atteindre

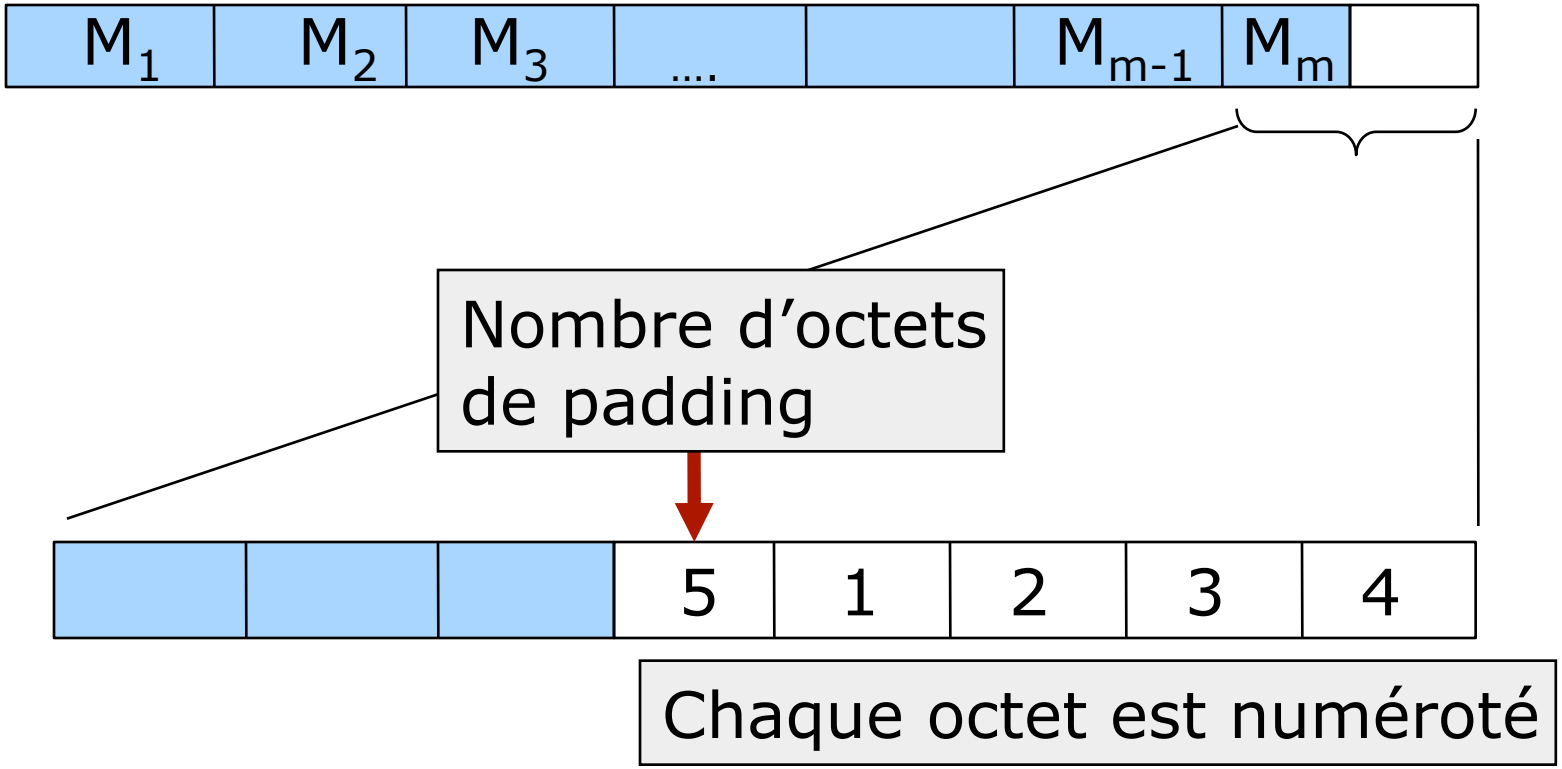
Cryptanalyse de modes opératoires de chiffrement

Padding

- Nécessité de compléter les messages à un multiple de n bits
- Nombreuses propositions
- Un mauvais choix peut conduire à une implémentation vulnérable à certaines attaques !

Exemple de padding faible

- On complète avec :
  - Nombre d'octets à compléter sur 1 octet
  - Chaque octet suivant est numéroté



Contexte d'attaque

Attaquant : cherche à déchiffrer C

C* : modification astucieuse de C

Serveur

Contexte d'attaque

Attaquant : cherche à déchiffrer C

Serveur

Chiffré C*

C* : modification astucieuse de C

Contexte d'attaque

Attaquant : cherche à déchiffrer C

C* : modification astucieuse de C

Chiffré C* →

Serveur

Déchiffrement de C*

Vérification de conformité

Contexte d'attaque

Attaquant : cherche à déchiffrer C

Serveur

Chiffré C*

Déchiffrement de C*

C* : modification astucieuse de C

Vérification de conformité

erreur

Le dernier bloc de clair ne contient pas le bon padding

Contexte d'attaque

Attaquant : cherche à déchiffrer C

C* : modification astucieuse de C

Chiffré C* →

Serveur

Déchiffrement de C*

Vérification de conformité

Contexte d'attaque

Attaquant : cherche à déchiffrer C

Serveur

Chiffré C* →

Déchiffrement de C*

C* : modification astucieuse de C

Vérification de conformité

OK

Le dernier bloc de clair contient le bon padding

Contexte d'attaque

Attaquant : cherche à déchiffrer C

C* : modification astucieuse de C

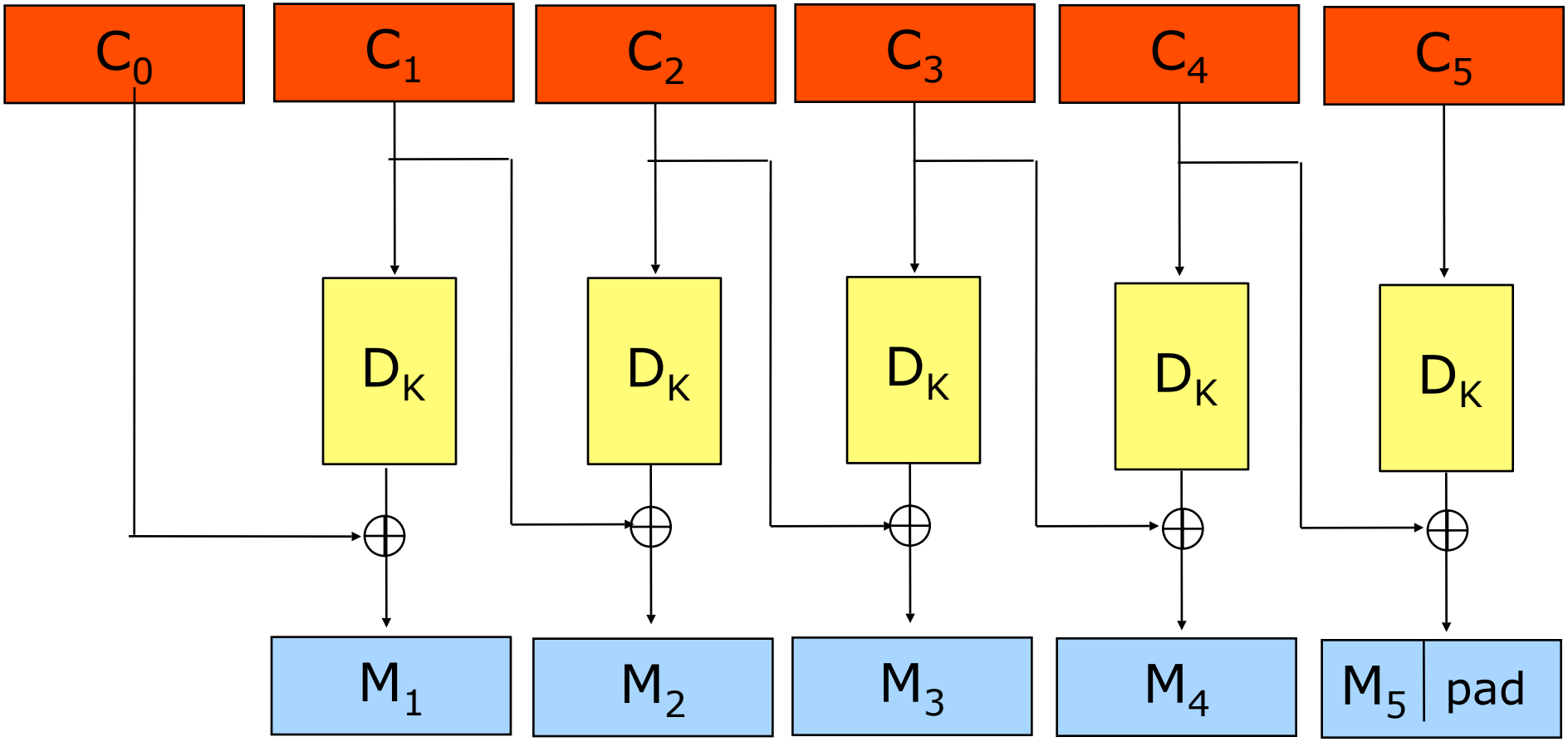
Chiffré C* →

Serveur

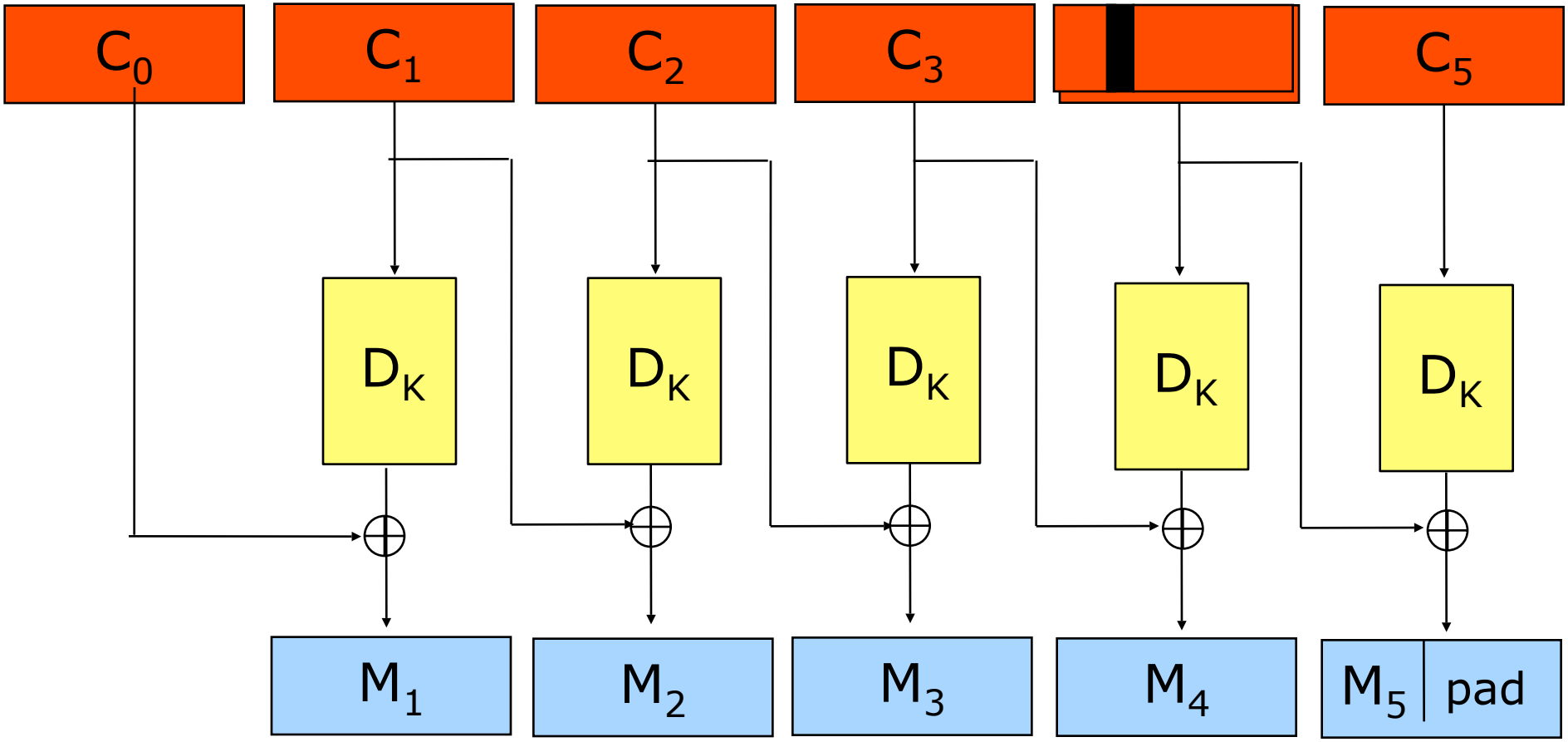
Déchiffrement de C*

Vérification de conformité

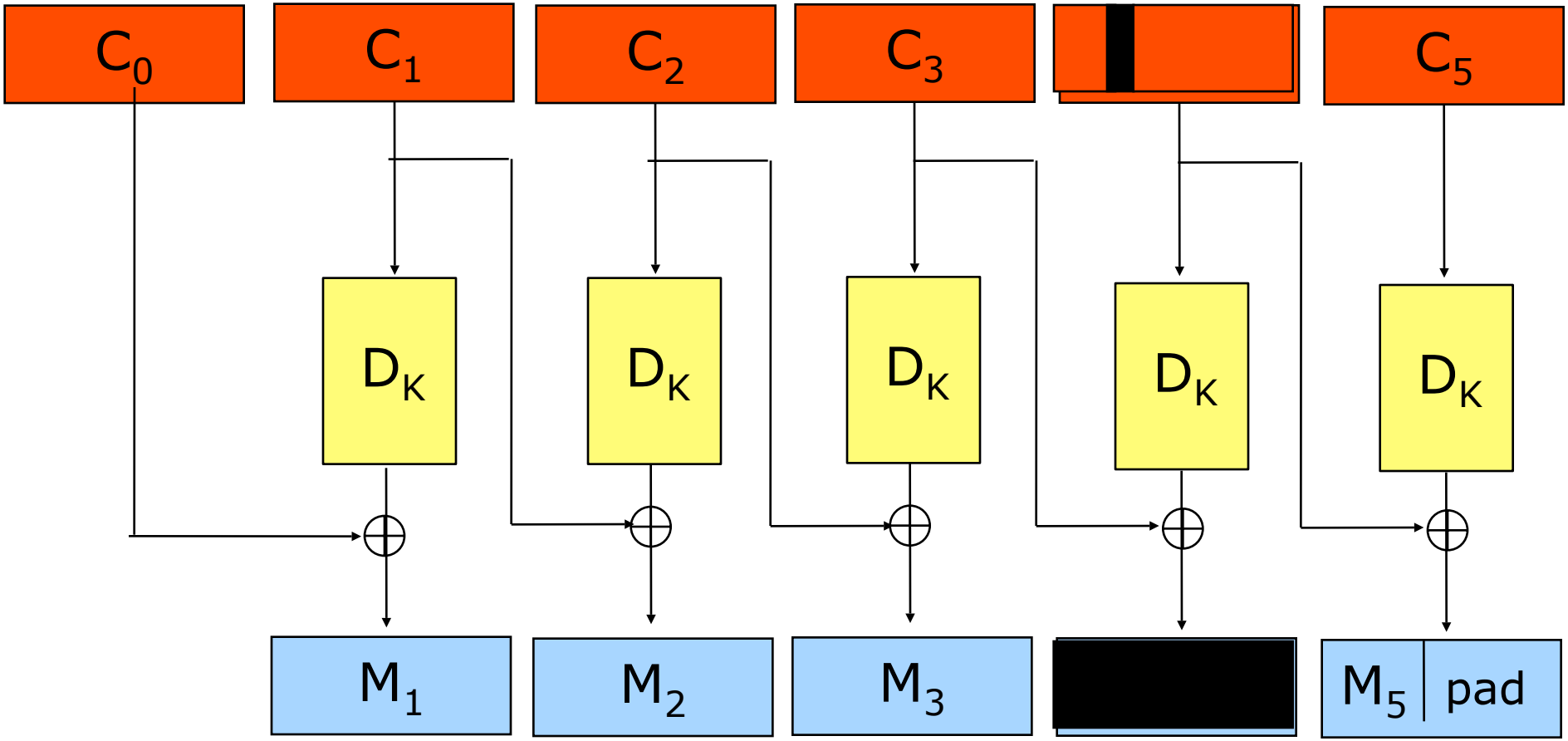
Cryptanalyse



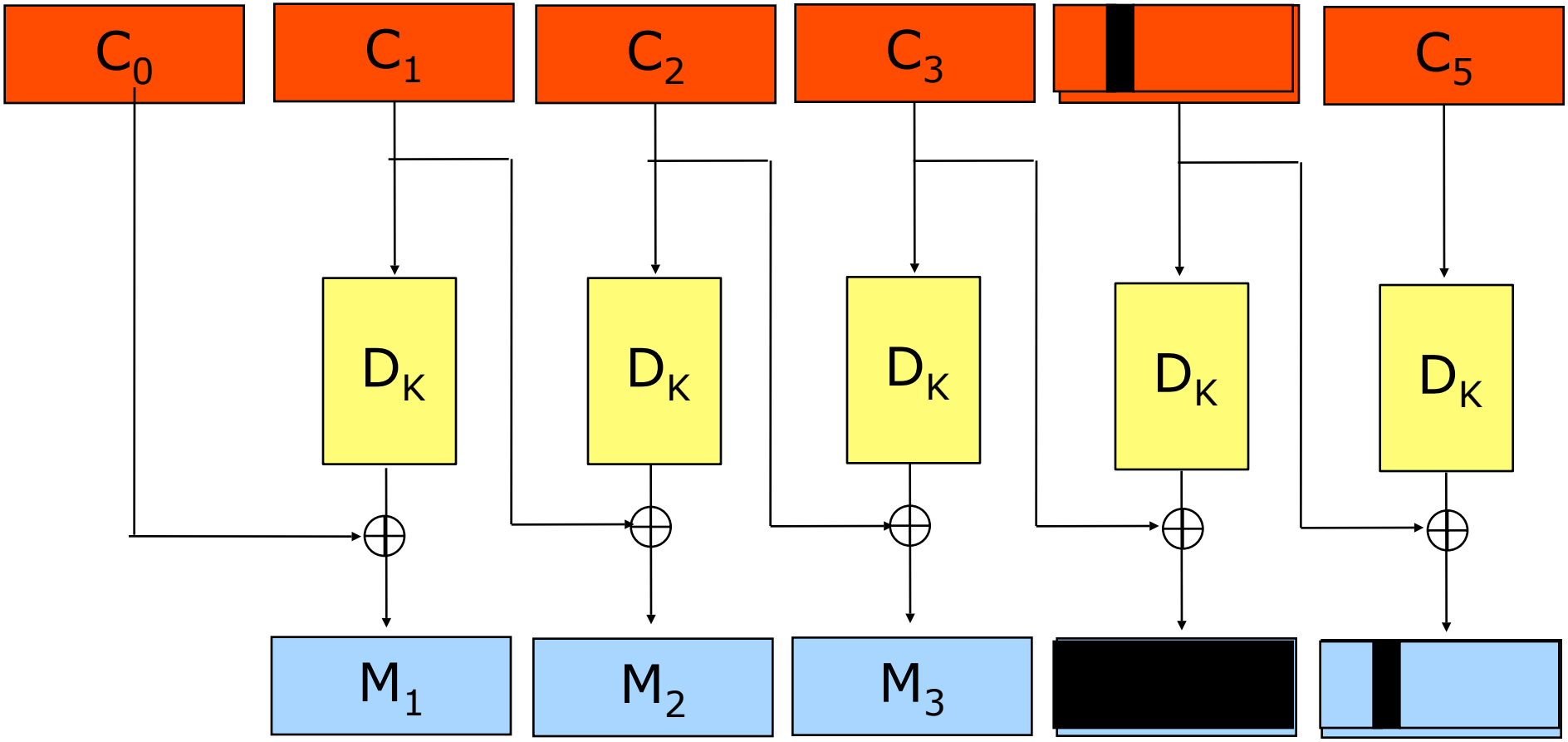
Cryptanalyse



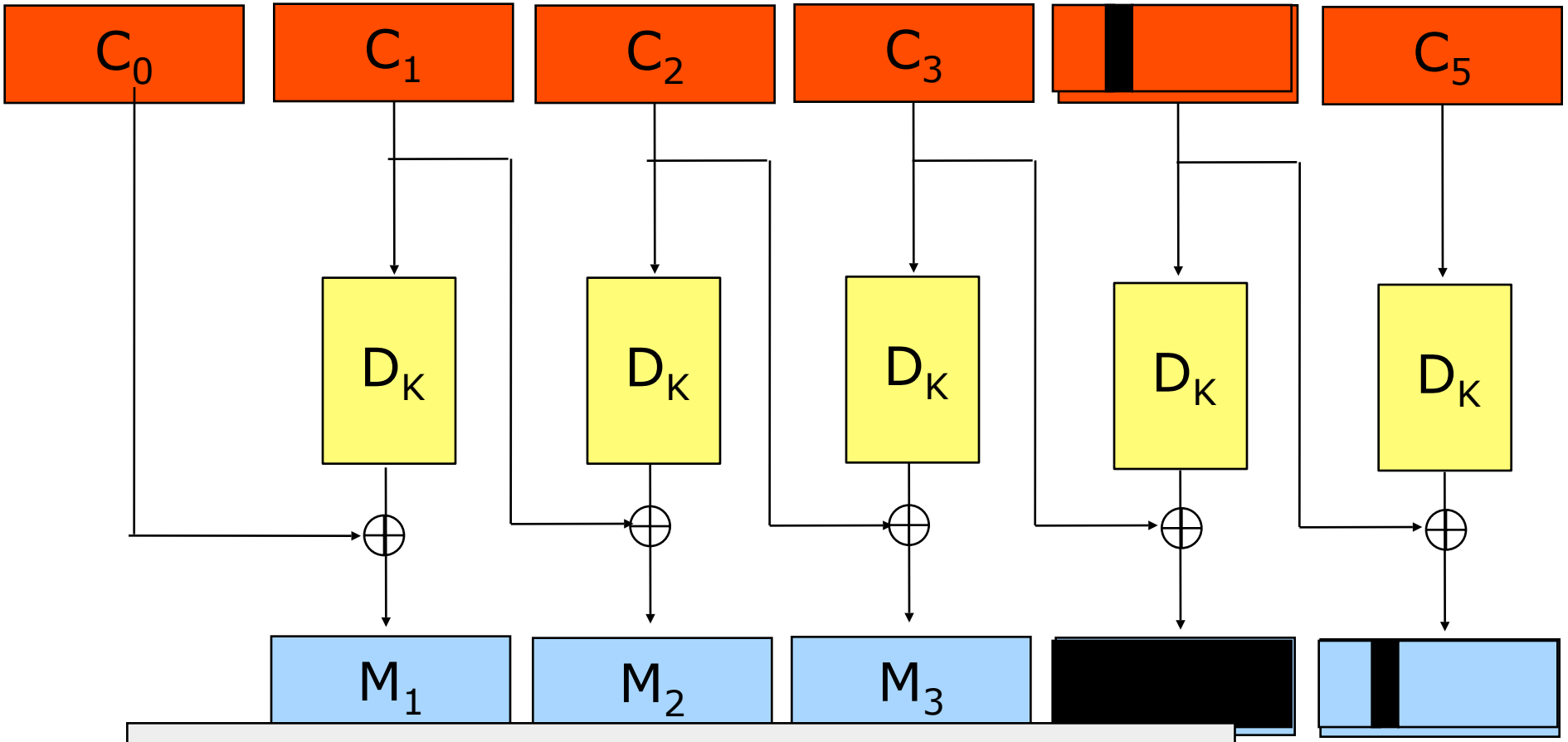
Cryptanalyse



Cryptanalyse



Cryptanalyse



Si la différence n'est pas dans le padding, le clair est encore valide

Cryptanalyse

- On trouve d'abord la taille du padding utilisé, et donc sa valeur
- Chaque octet du dernier bloc peut ensuite être obtenu
  - On modifie C_{m-1} pour modifier le padding : on attend qu'il soit valide
  - On apprend ainsi chaque octet du dernier bloc de clair
- On tronque le chiffré et on réitère

Modes opératoires multiples

Multiples modes d'opération

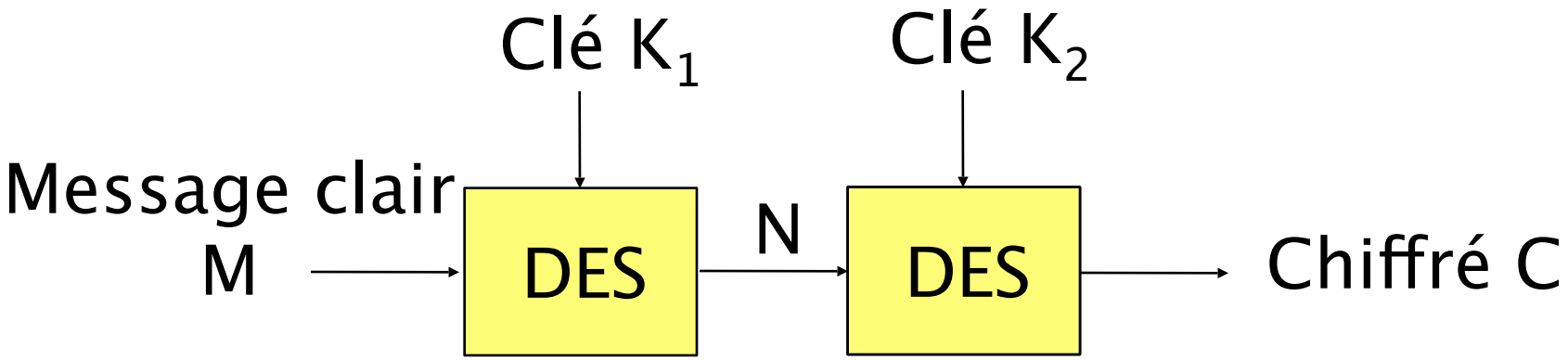
- But : parer aux faiblesses du DES
- Idée : combiner plusieurs modes opératoires
- Avantages « attendus » :
  - Meilleure sécurité que les modes opératoires simples
    - Face à la recherche exhaustive des clés
    - Pas d'entrée/sortie connue pour la primitive
  - Aussi rapides grâce à la parallélisation
  - Une attaque à clairs ou chiffrés choisis ne doit pas permettre une attaque « efficace »

Différentes techniques

- Cryptanalyse différentielle
  - ECB – CBC - CBC
- Cryptanalyse linéaire
  - CBC – ECB - CBC
- Recherche exhaustive clé par clé
  - CBC – CBC – ECB
  - CBC^{-1} – ECB - CBC
- Application du paradoxe des anniversaires
  - Triple CBC
  - CBC – CBC^{-1} - CBC

Pré-requis : le double DES

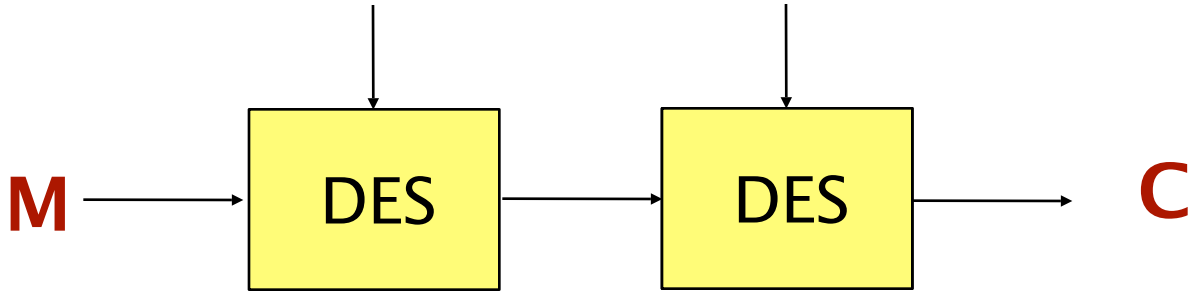
- Soit K_1 et K_2 deux clés DES indépendantes de 56 bits chacune
- Soit E le chiffrement suivant :
- $E_{K1,K2}(M) = DES_{K1}(DES_{K2}(M))$



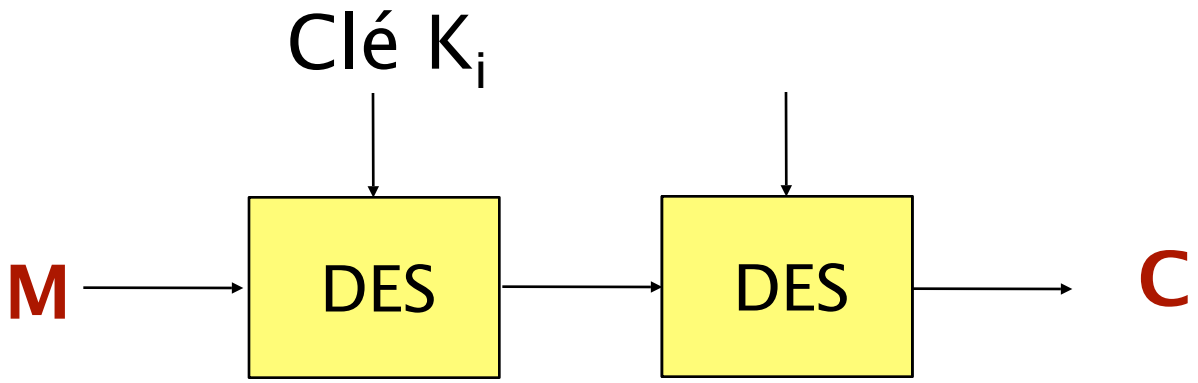
Sécurité du double DES

- Attaque naïve : recherche exhaustive des 2^{2k} clés possibles
- Attaque par le milieu : compromis temps-mémoire
  - Étant donné un couple clair-chiffré (M,C) :
  - Calculer tous les $N_i = DES_{Ki}(M)$ pour les 2^k clés K_i possibles
  - Déchiffrer C sous toutes les 2^k clés K_j possibles :
    - $P_j = DES^{-1}_{Kj}(C)$
  - Si $N_i = P_j$ alors le bi-clé (K_i,K_j) est candidat

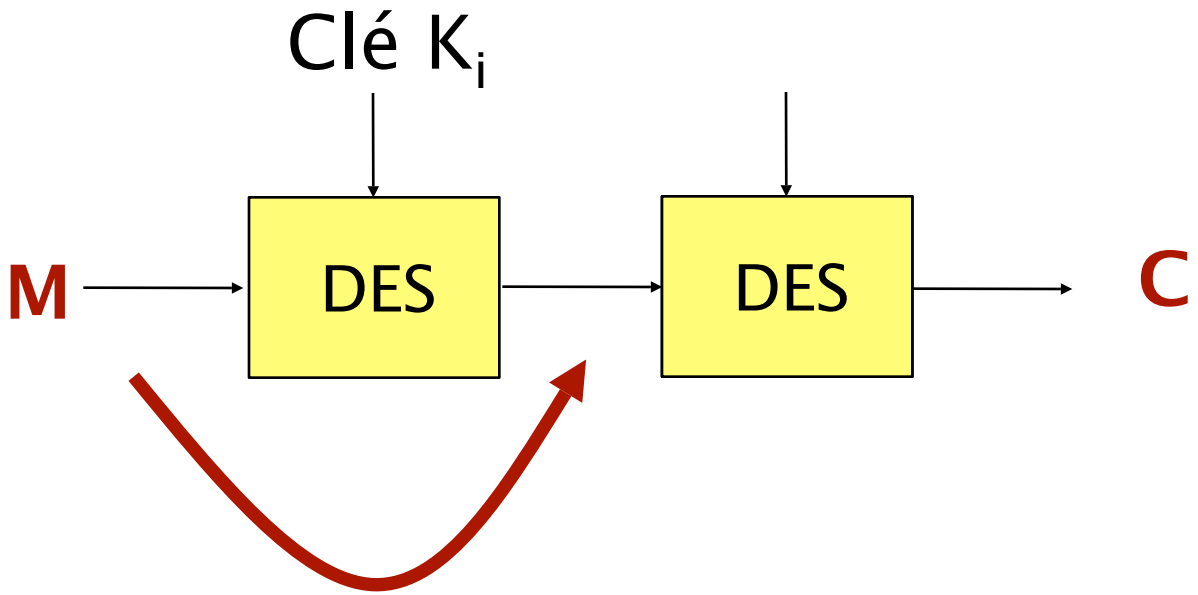
Sécurité du double DES



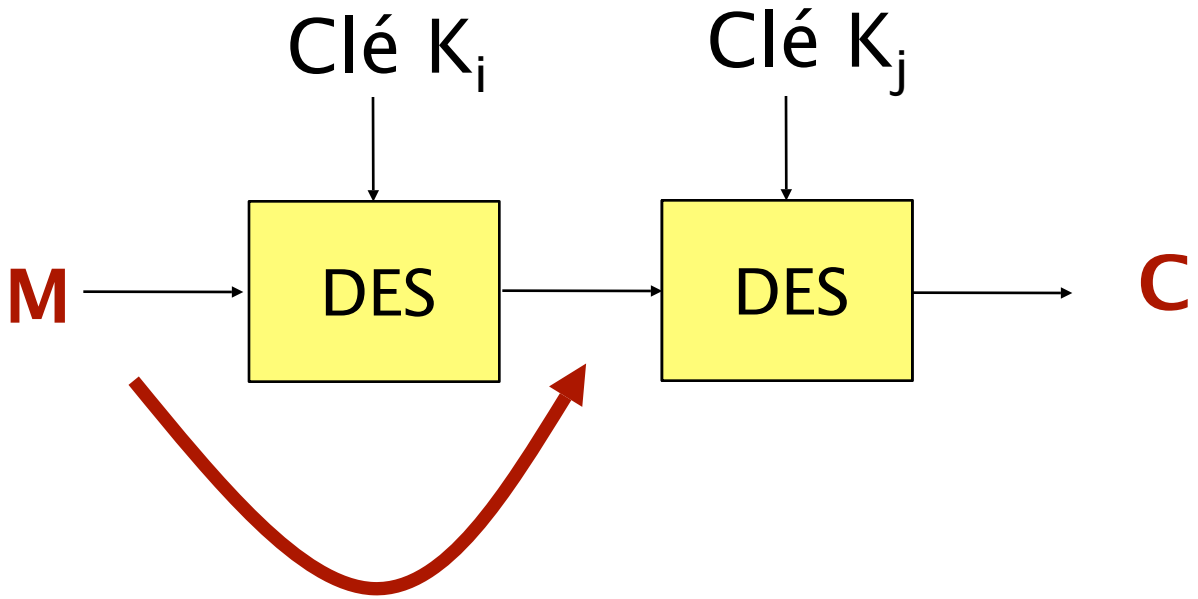
Sécurité du double DES



Sécurité du double DES



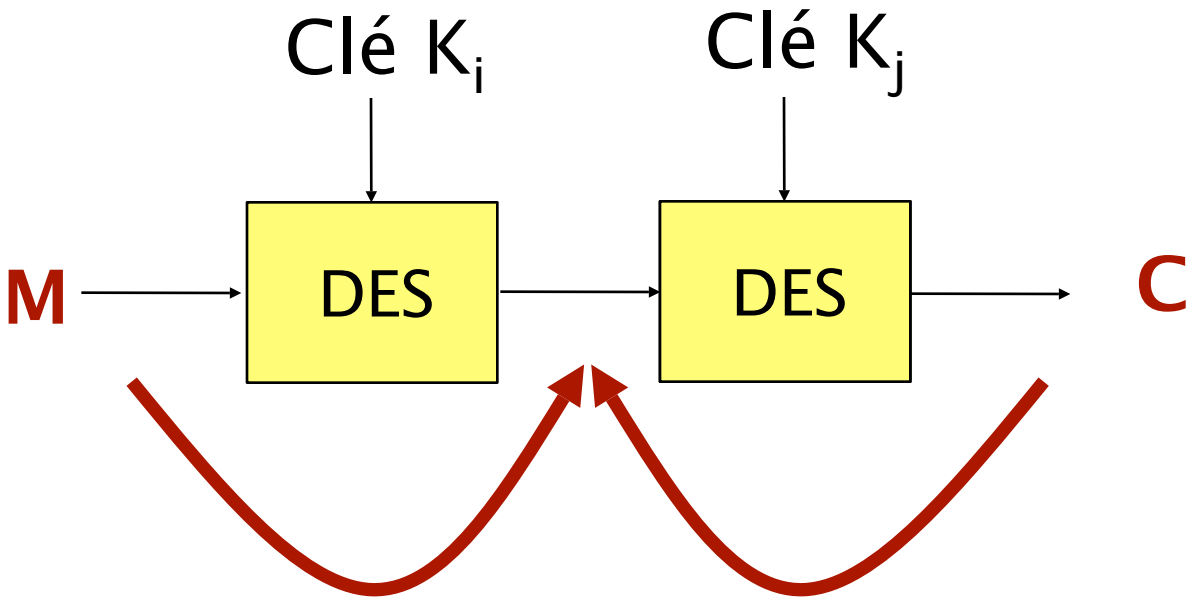
Sécurité du double DES



2^{56} calculs

$N_i = DES(K_i, M)$

Sécurité du double DES



2^{56} calculs
$N_i = DES(K_i,M)$

Pour chaque
$P_j = DES^{-1}(K_j,C)$,
on cherche $N_i = P_j$

Sécurité du double DES

- On a :
  - 2^{56} chiffrés N_i
  - 2^{56} déchiffrés P_j
  - Valeurs de 64 bits
- Par le paradoxe des anniversaires, on a :

  $(2^{56} \times 2^{56}) / 2^{64} = 2^{48}$ collisions en moyenne
- Il existe donc 2^{48} couples (i,j) tels que $N_i=P_j$
- Donc 2^{48} bi-clés possibles

Sécurité du double DES

- On cherche toutes les collisions $N_i = P_j$ et on obtient 2^{48} bi-clés possibles

- À l'aide d'un second couple (M',C'), on chiffre M' avec les 2^{48} bi-clés en C_i'
- Quand on obtient C_i' = C', on a trouvé le couple (K_1,K_2) correct

Sécurité du double DES

- Attaque en 2^k en temps et en mémoire
  - Compromis temps/mémoire possible
- La sécurité du double DES n'atteint pas 2^{2k} mais seulement 2^k, comme le DES

- Remarque :
  - deux clés de 28 bits : 56 bits de secret,
  - 2 fois plus de tours que le DES
  - **sécurité en 2^{28} seulement**

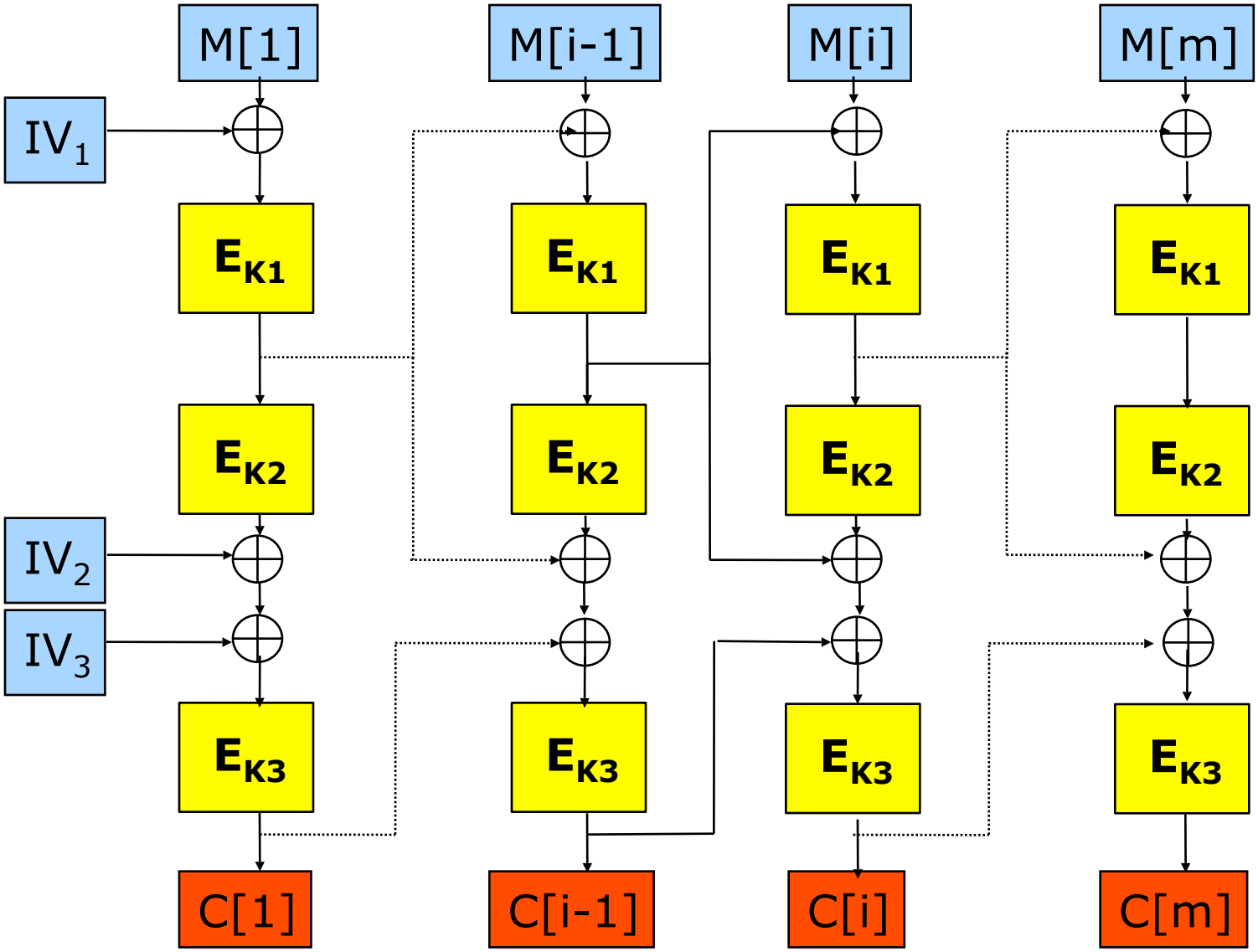
Multiples modes d'opération

- But : parer aux faiblesses du DES
- Idée : combiner plusieurs modes opératoires
- Avantages « attendus » :
  - Meilleure sécurité que les modes opératoires simples
    - Face à la recherche exhaustive des clés
    - Sécurité sémantique
  - Aussi rapides grâce à la parallélisation
  - Une attaque à clairs ou chiffrés choisis ne doit pas permettre une attaque « efficace »

Différentes techniques

- Recherche exhaustive
- Application du paradoxe des anniversaires
- Cryptanalyses linéaires et différentielles
- Nouveaux types d'adversaires
- Dans chaque cas, on cherche
  - À retrouver la clé
  - À casser la sécurité sémantique
  - Les moyens mis en œuvre sont souvent variés

Exemple : CBC / CBC^{-1} / CBC



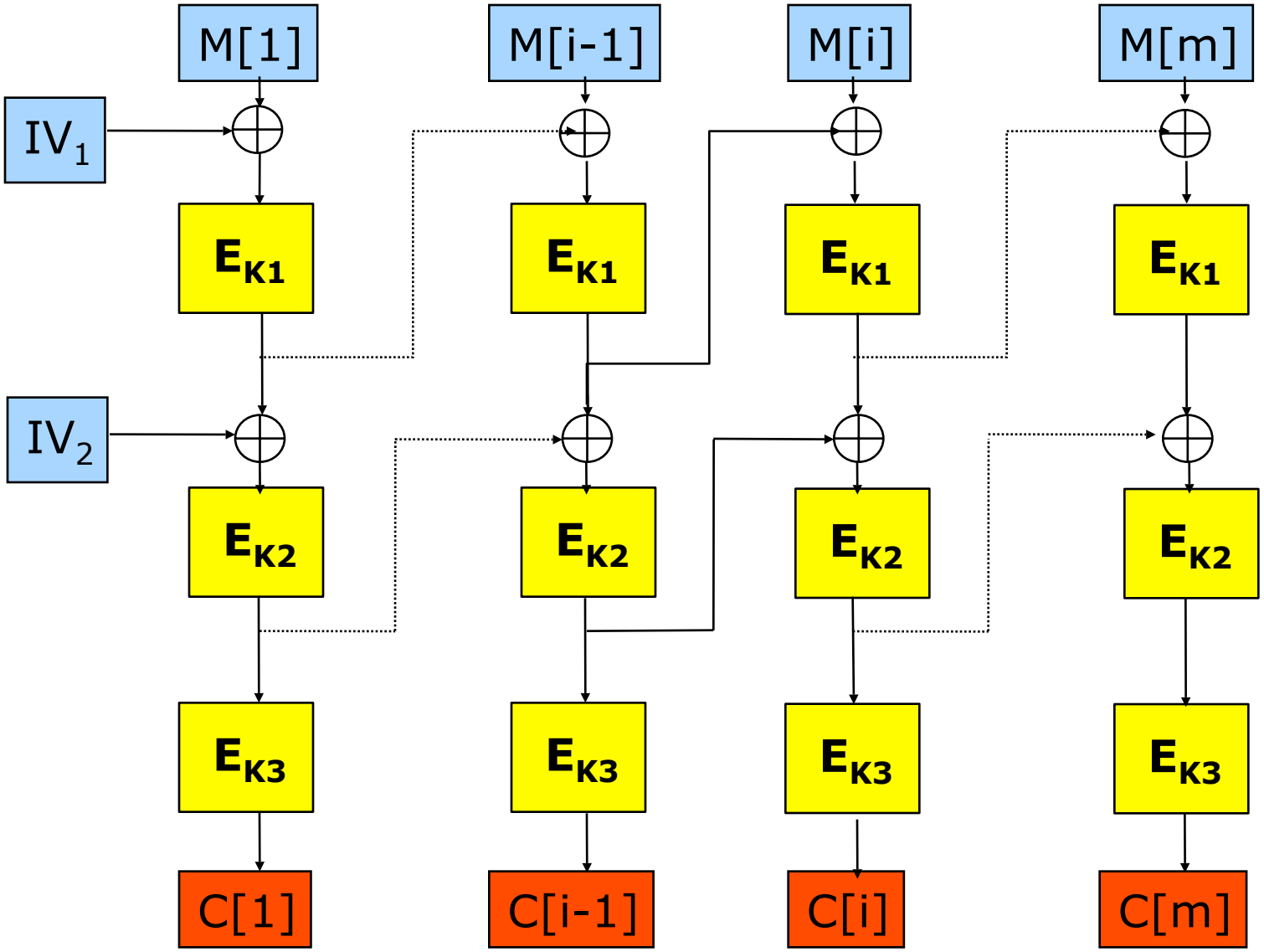
Observation principale

- Contrôle de certaines valeurs chaînées
- Choix des entrées de la primitives grâce à ce contrôle
- Attaques à clairs ou chiffrés choisis

Recherche exhaustive

- On se ramène a la recherche exhaustive de chaque clé utilisée
  - Exemple basique : attaque sur le 2DES
- **Problème** : trouver un « test d'arrêt », càd un couple (P,C) tel que $C=E_K(P)$
  - Un tel couple permet une recherche exhaustive de la clé K
  - Relations parfois plus complexes mais qui ne dépendent que d'une seule clé

Mode CBC-CBC-ECB



Mode CBC-CBC-ECB

- Attaque à chiffrés choisis : 2 requêtes seulement
- L'adversaire demande le déchiffrement de

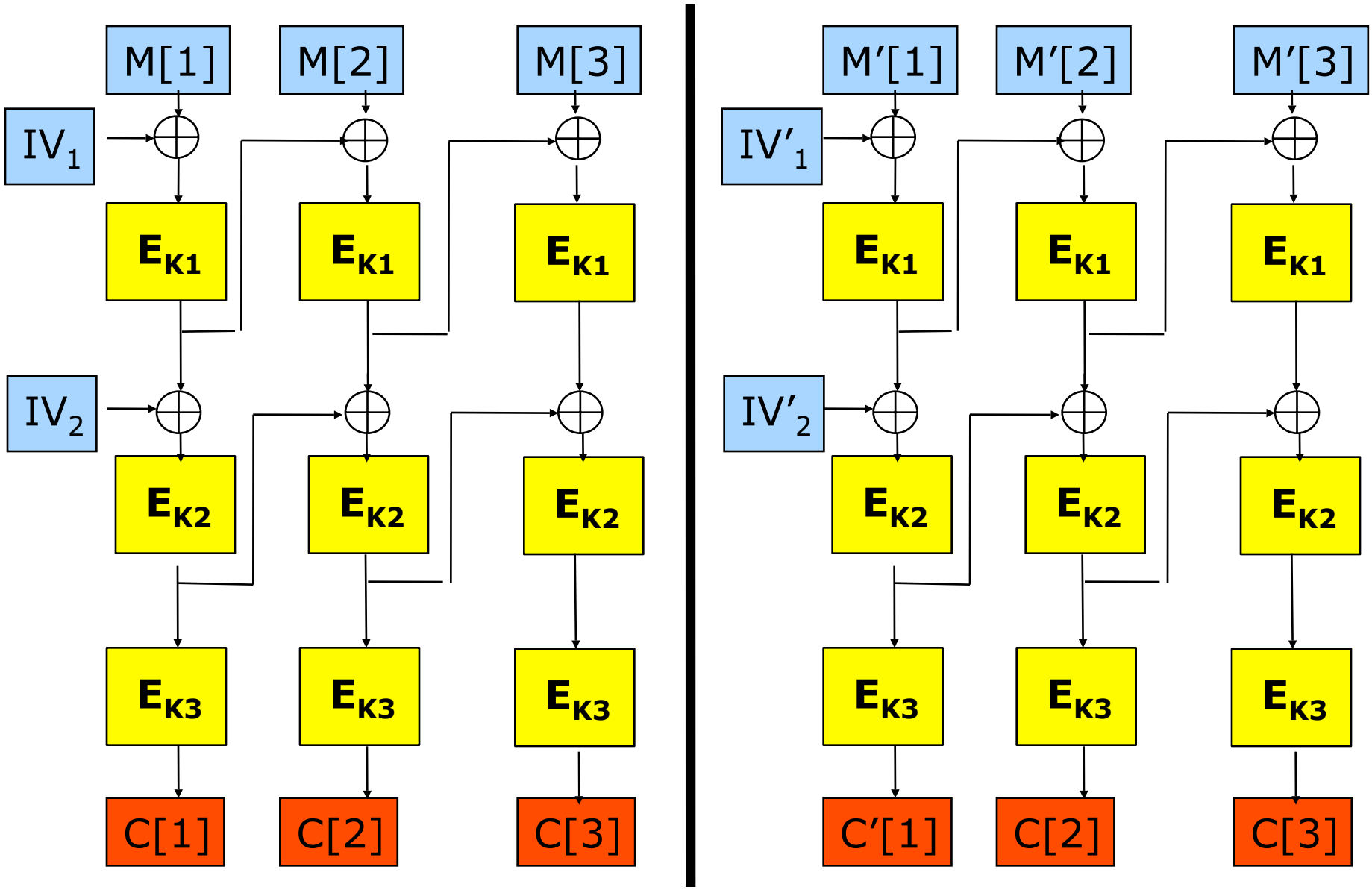
  $C=(IV_1,IV_2,C_1,C_2,C_3)$ $C'=(IV'_1,IV'_2,C'_1,C_2,C_3)$
- Il obtient $M=M_1\,M_2\,M_3$ et $M'=M'_1\,M'_2\,M'_3$
- La valeur $M_3 \oplus M'_3$ est celle en entrée de E_{K3} au premier tour

Mode CBC-CBC-ECB

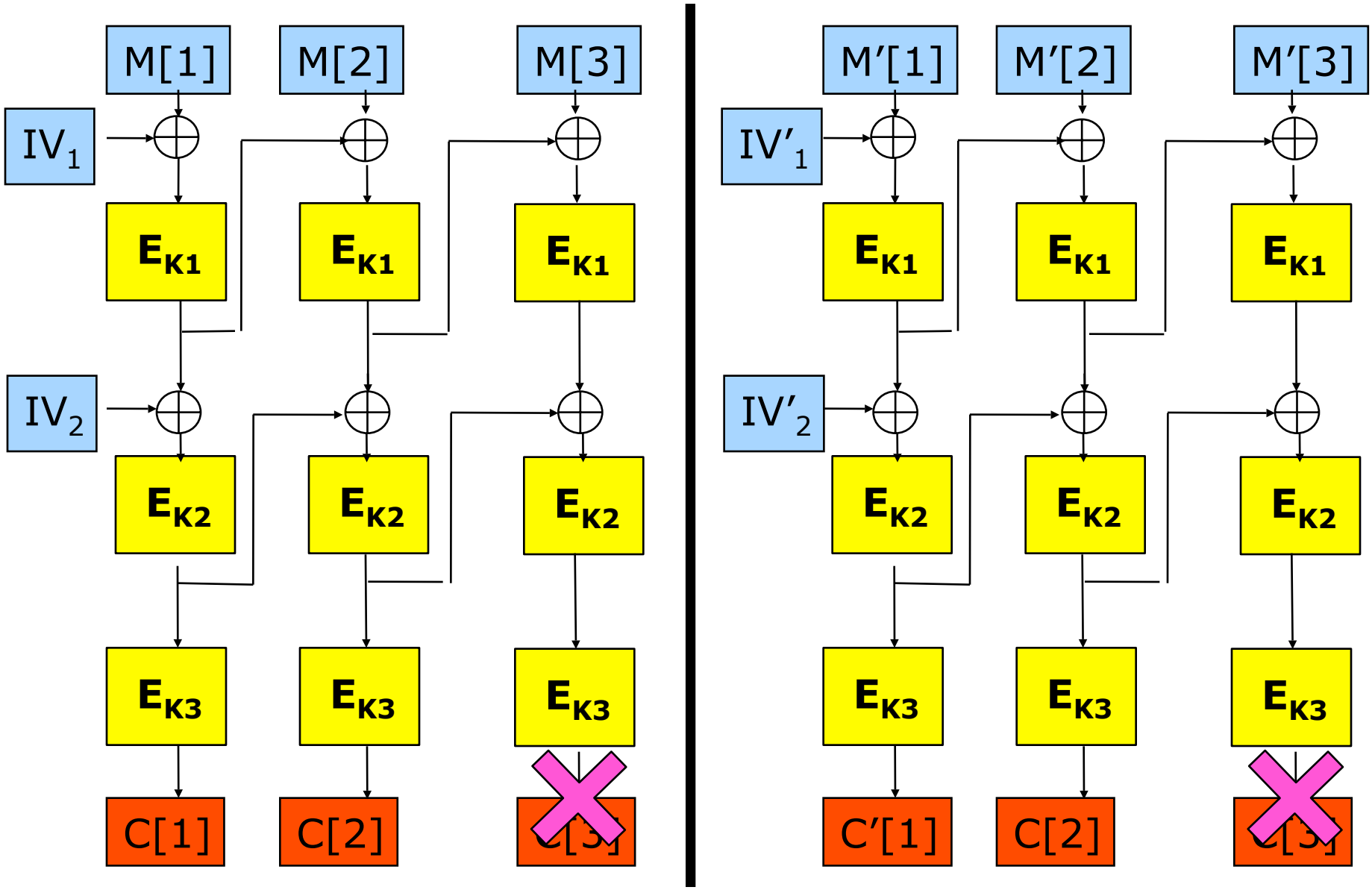
- Attaque à chiffrés choisis : 2 requêtes seulement
- L'adversaire demande le déchiffrement de

  $C=(IV_1, IV_2, C_1, C_2, C_3)$ $C'=(IV'_1, IV'_2, C'_1, C_2, C_3)$
- Il obtient $M=M_1\, M_2\, M_3$ et $M'= M'_1\, M'_2\, M'_3$
- La valeur $M_3 \oplus M'_3$ est celle en entrée de E_{K3} au premier tour

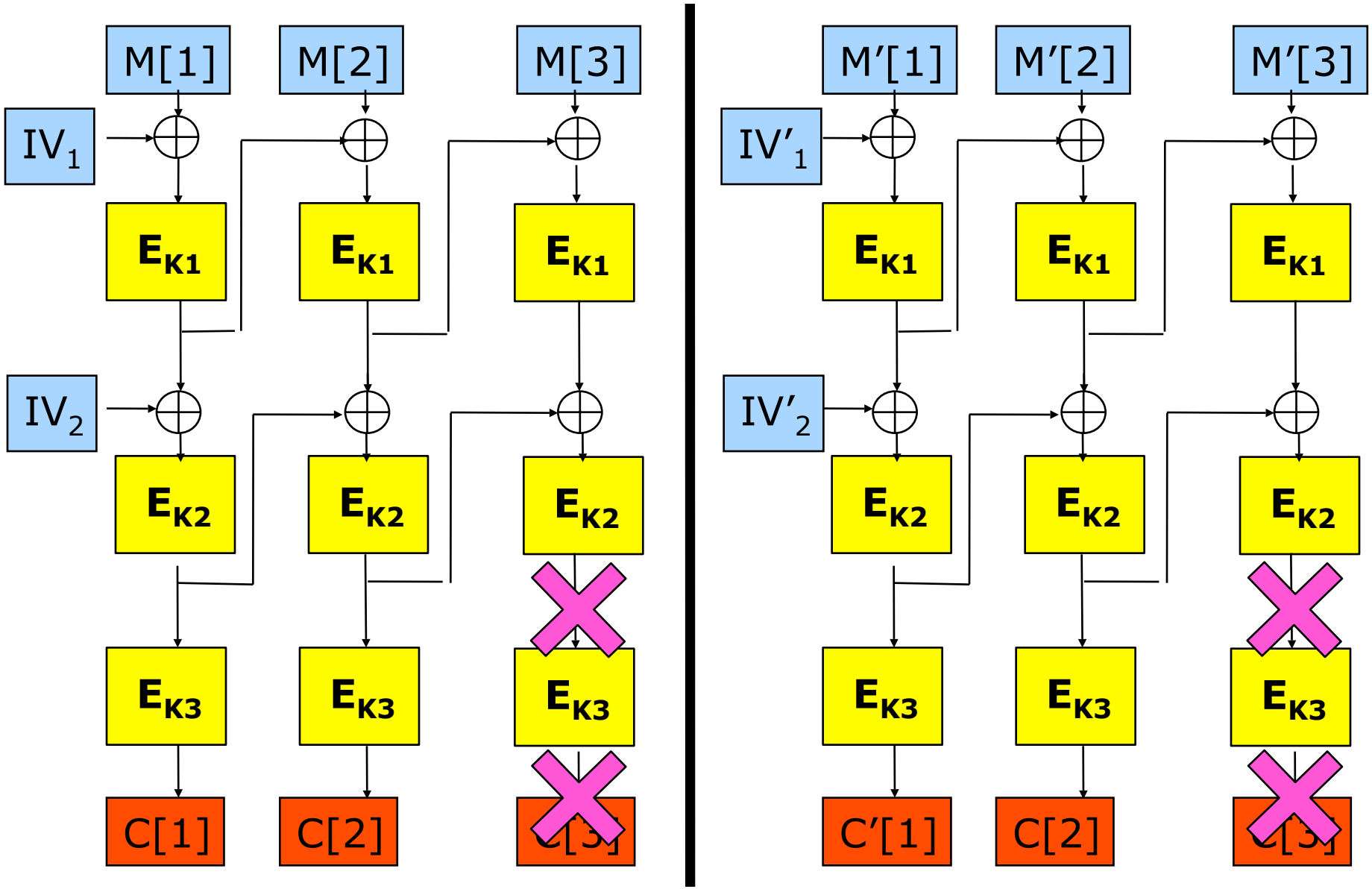
Mode CBC-CBC-ECB



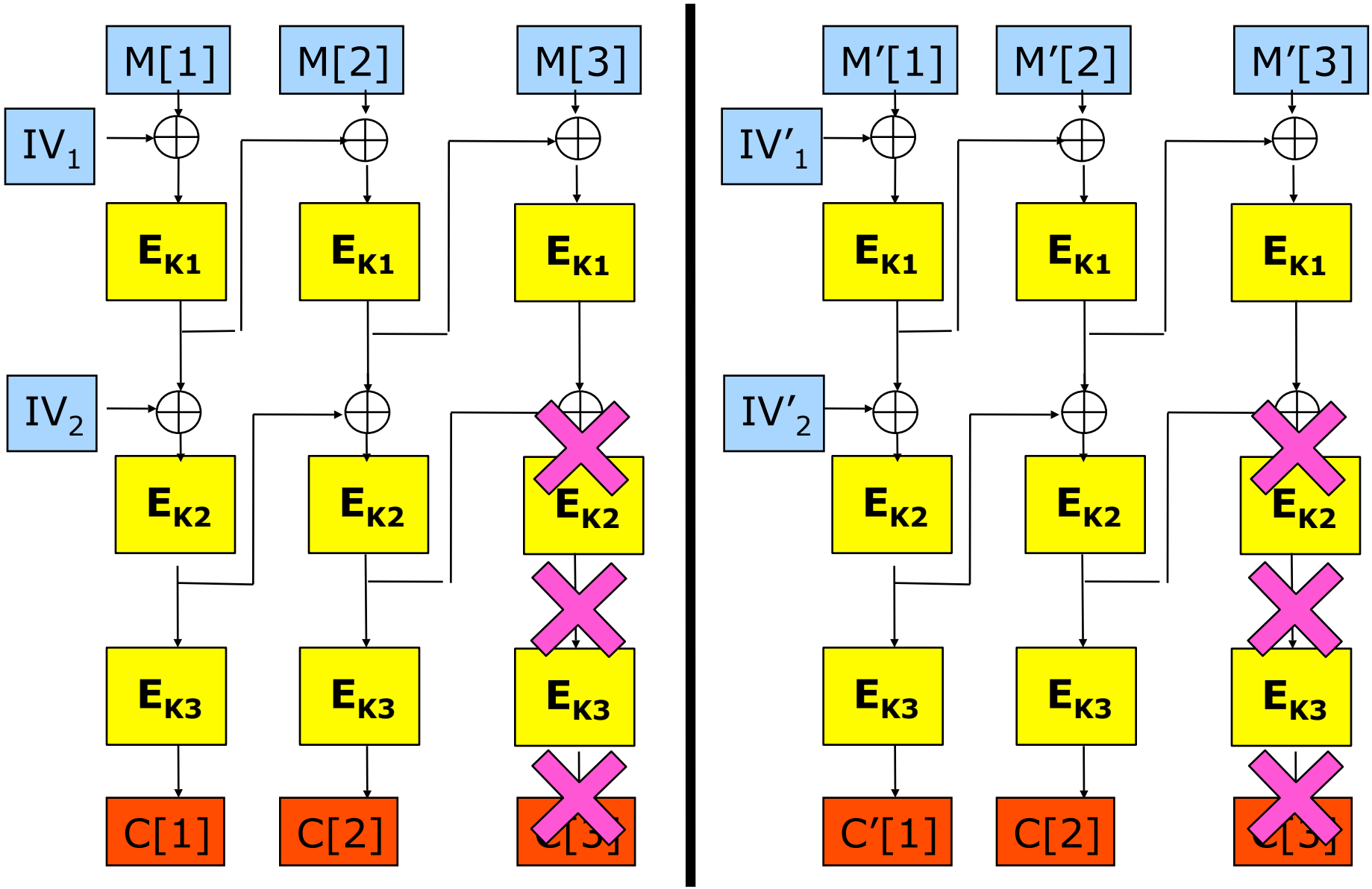
Mode CBC-CBC-ECB



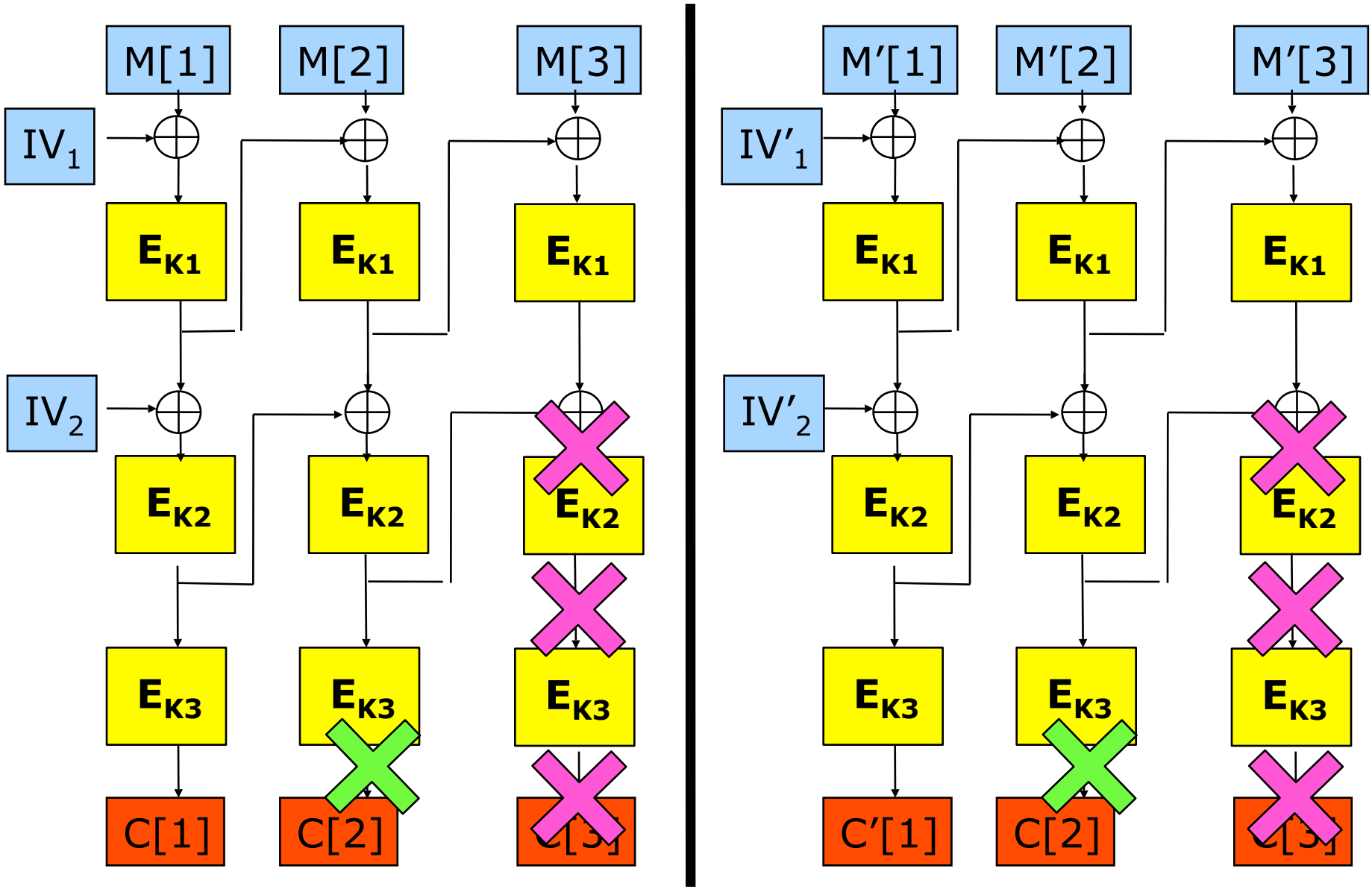
Mode CBC-CBC-ECB



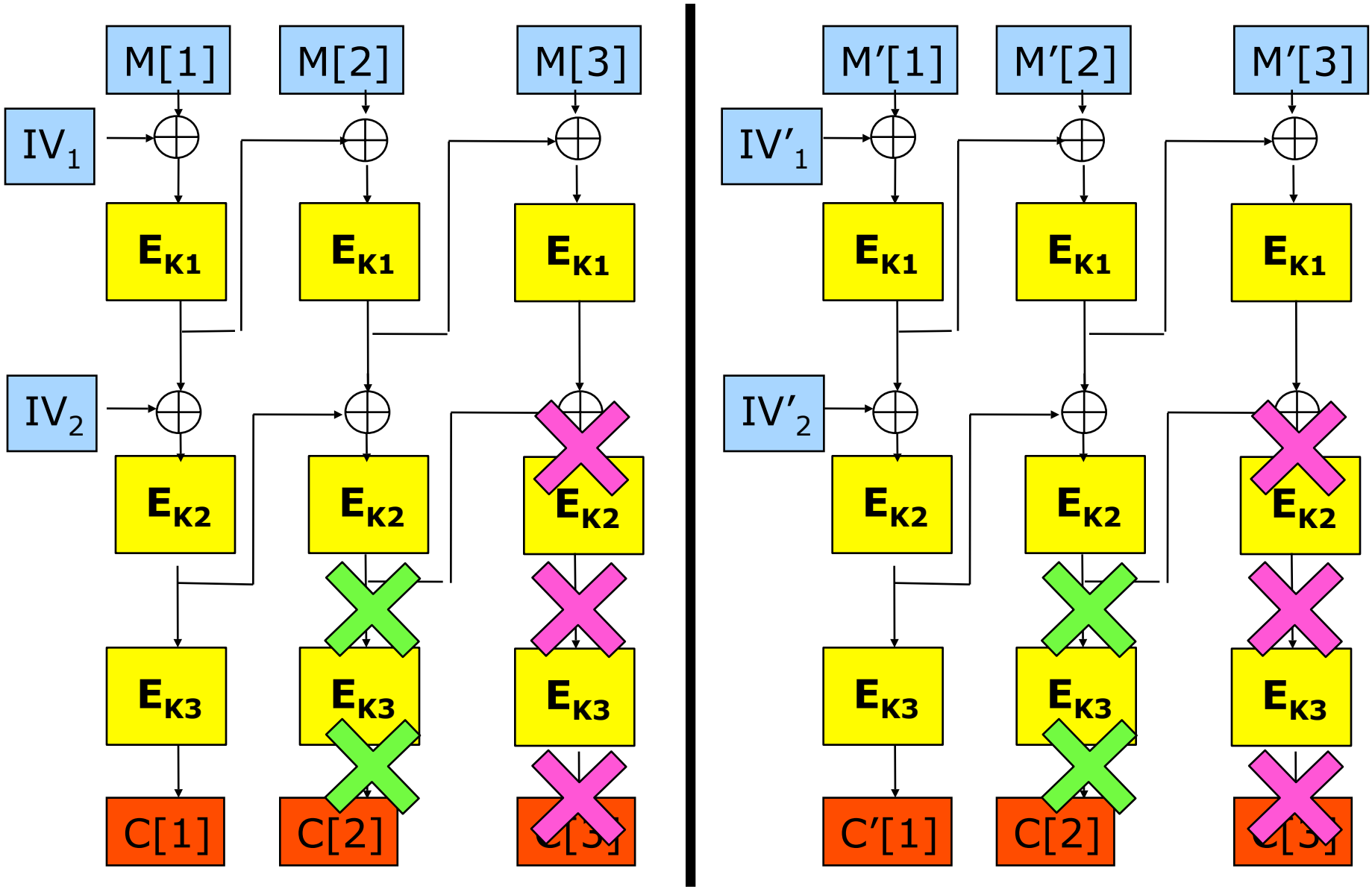
Mode CBC-CBC-ECB



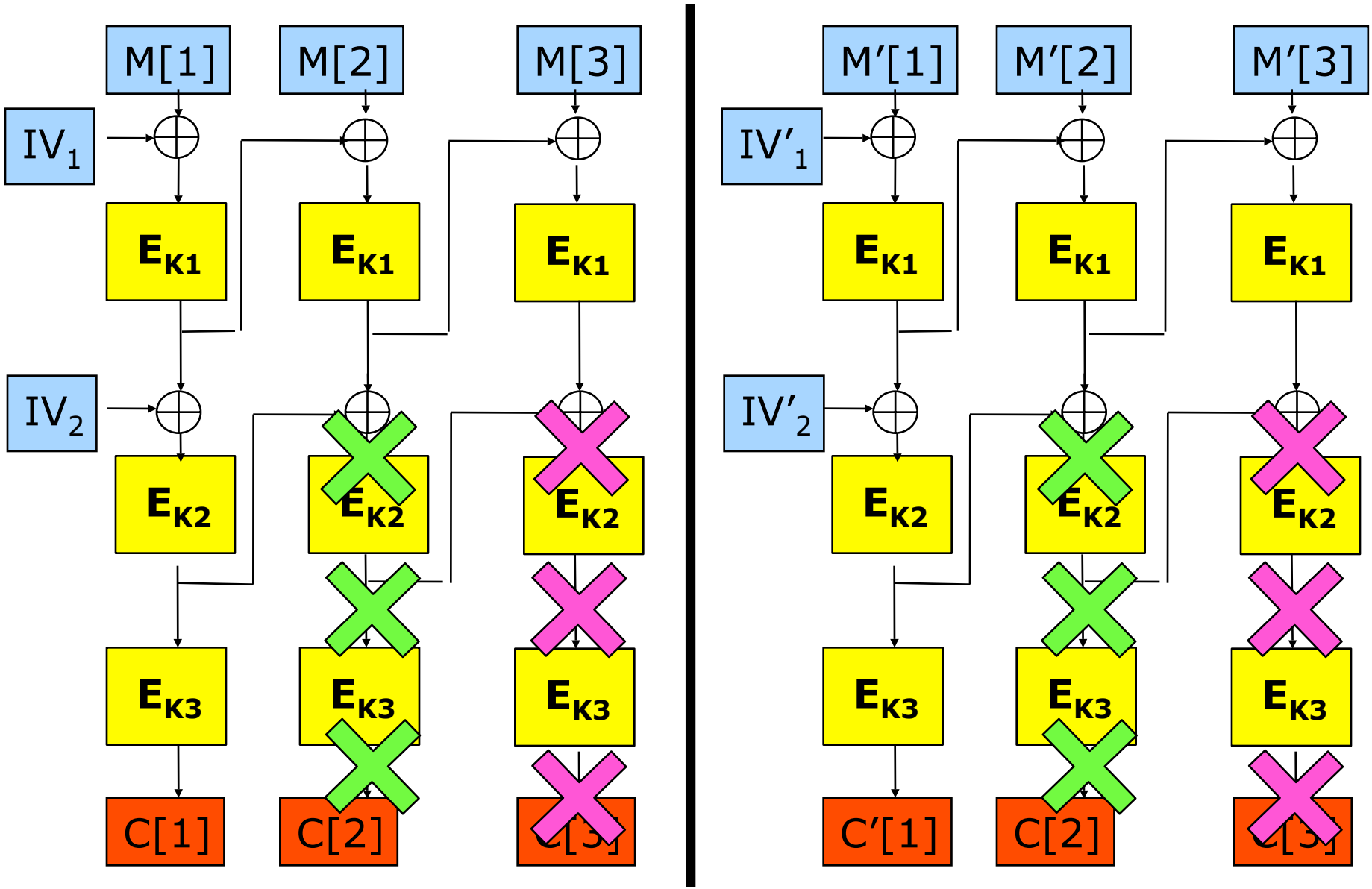
Mode CBC-CBC-ECB



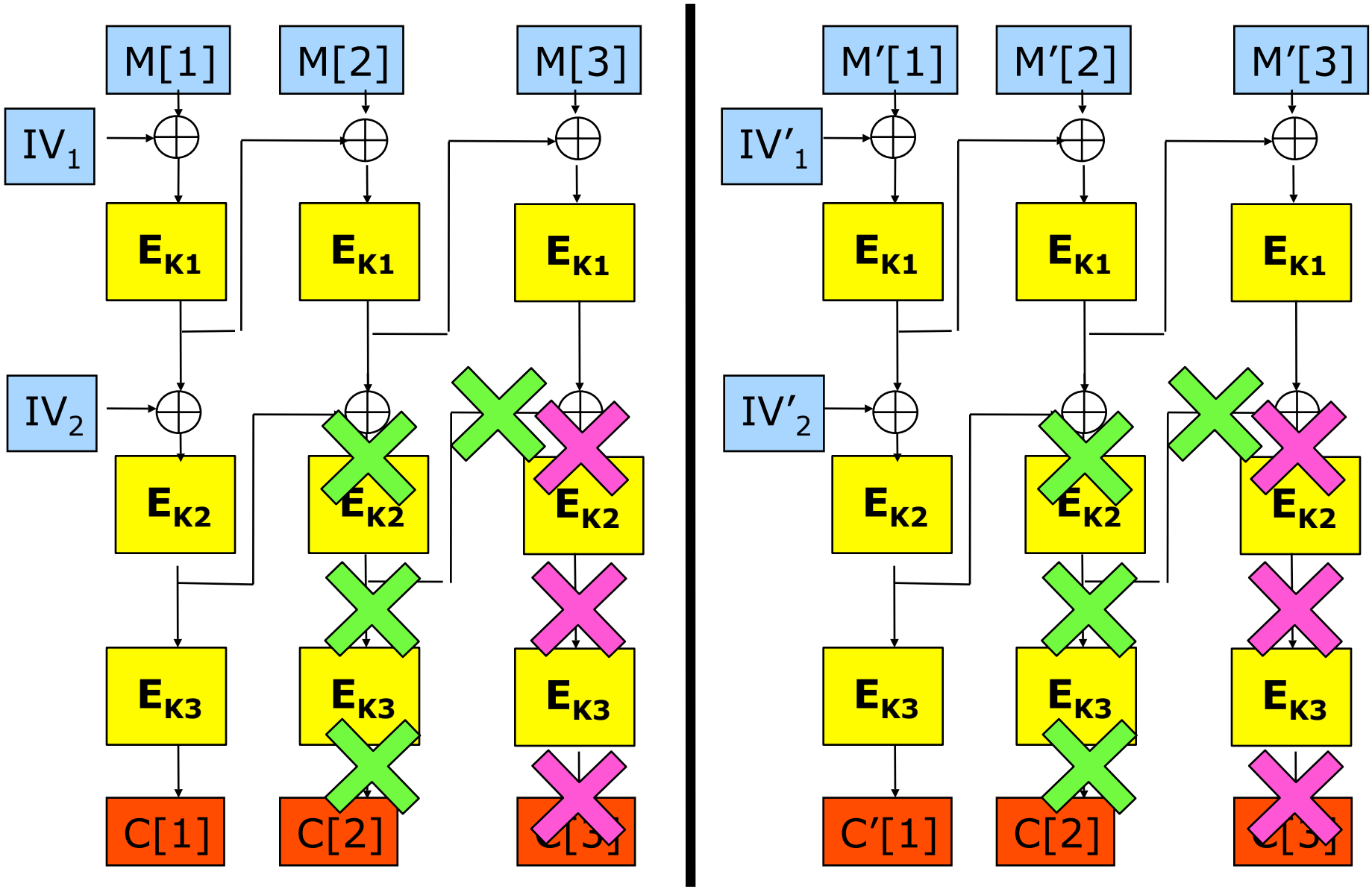
Mode CBC-CBC-ECB



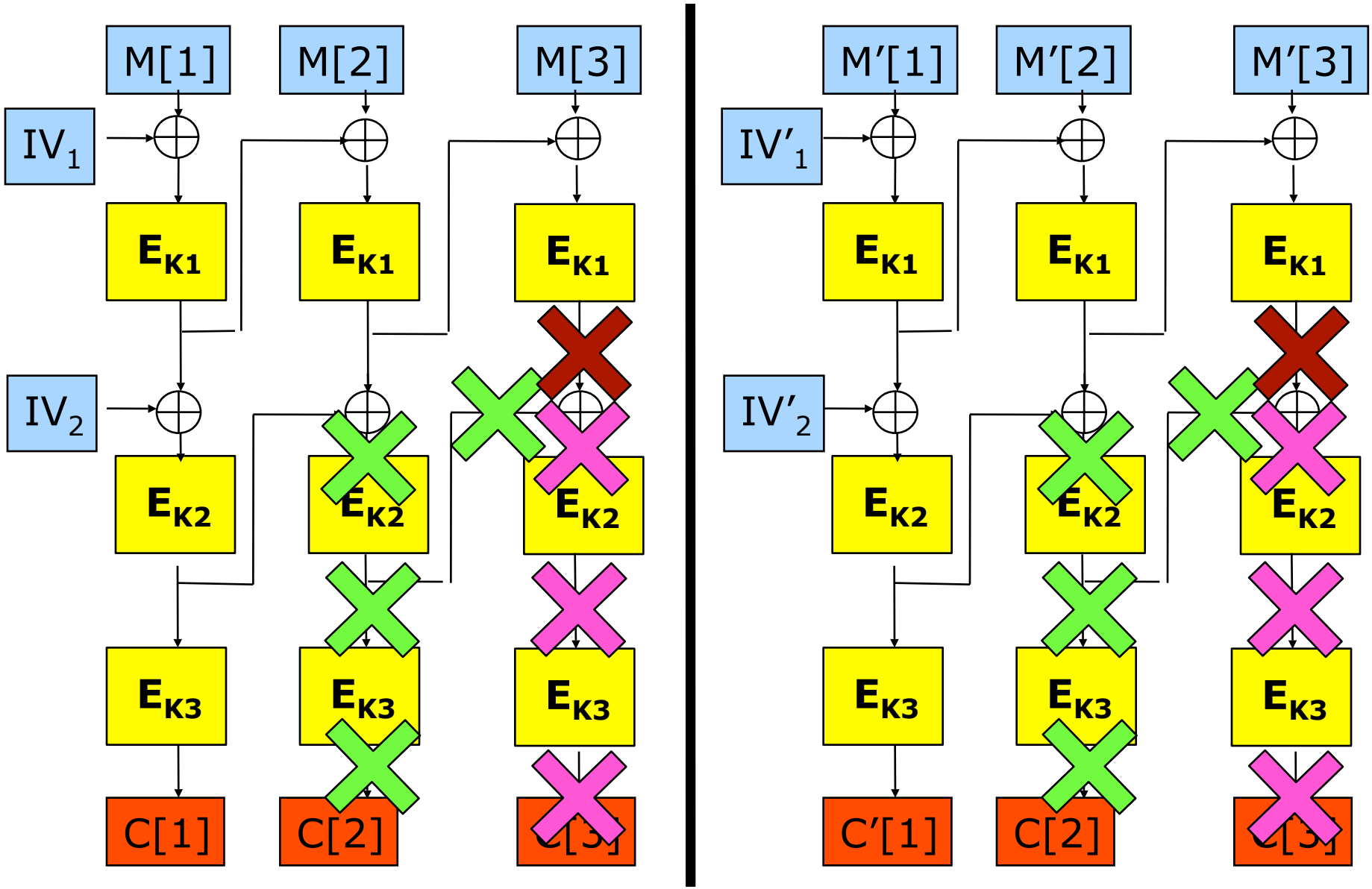
Mode CBC-CBC-ECB



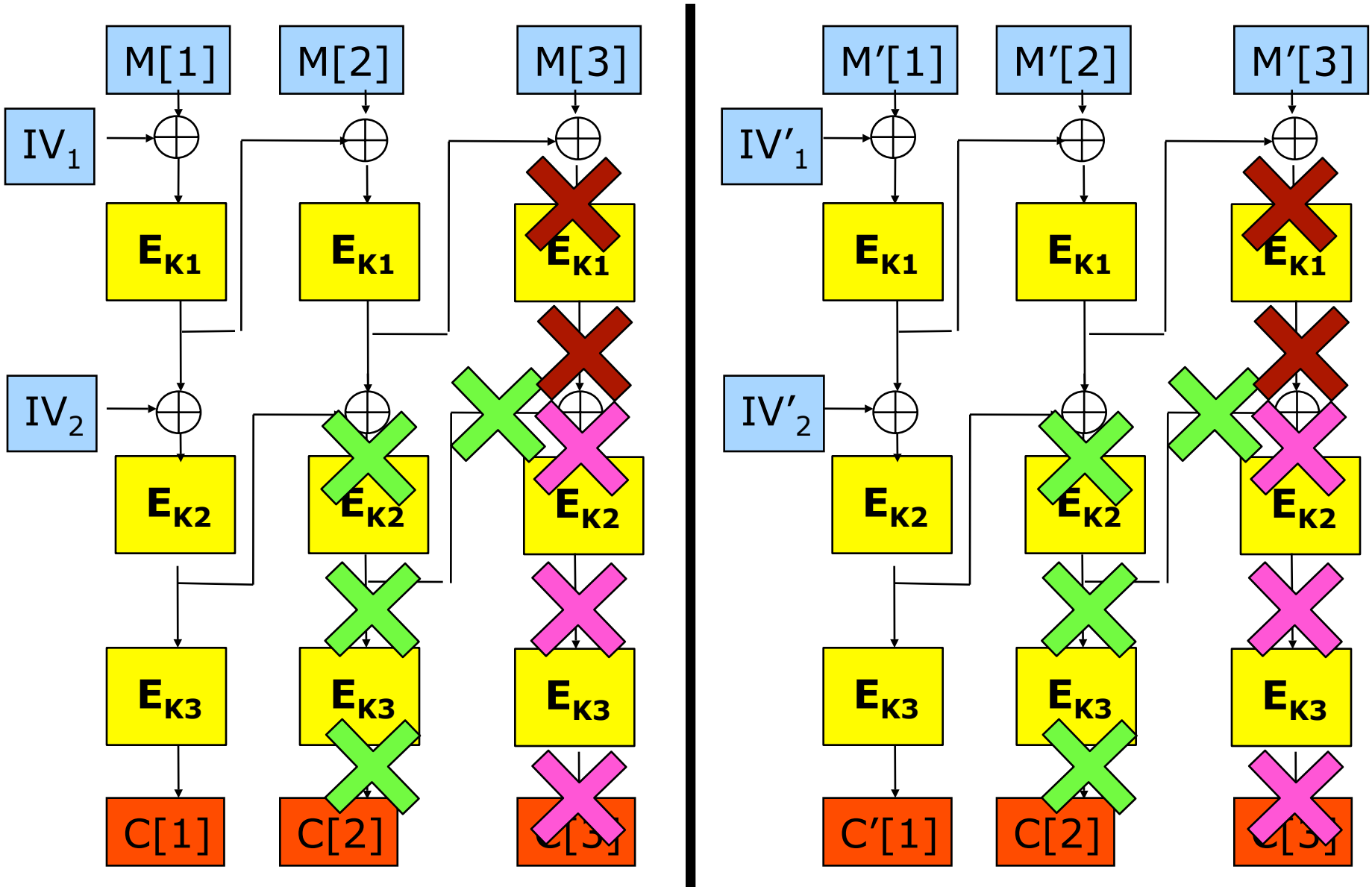
Mode CBC-CBC-ECB



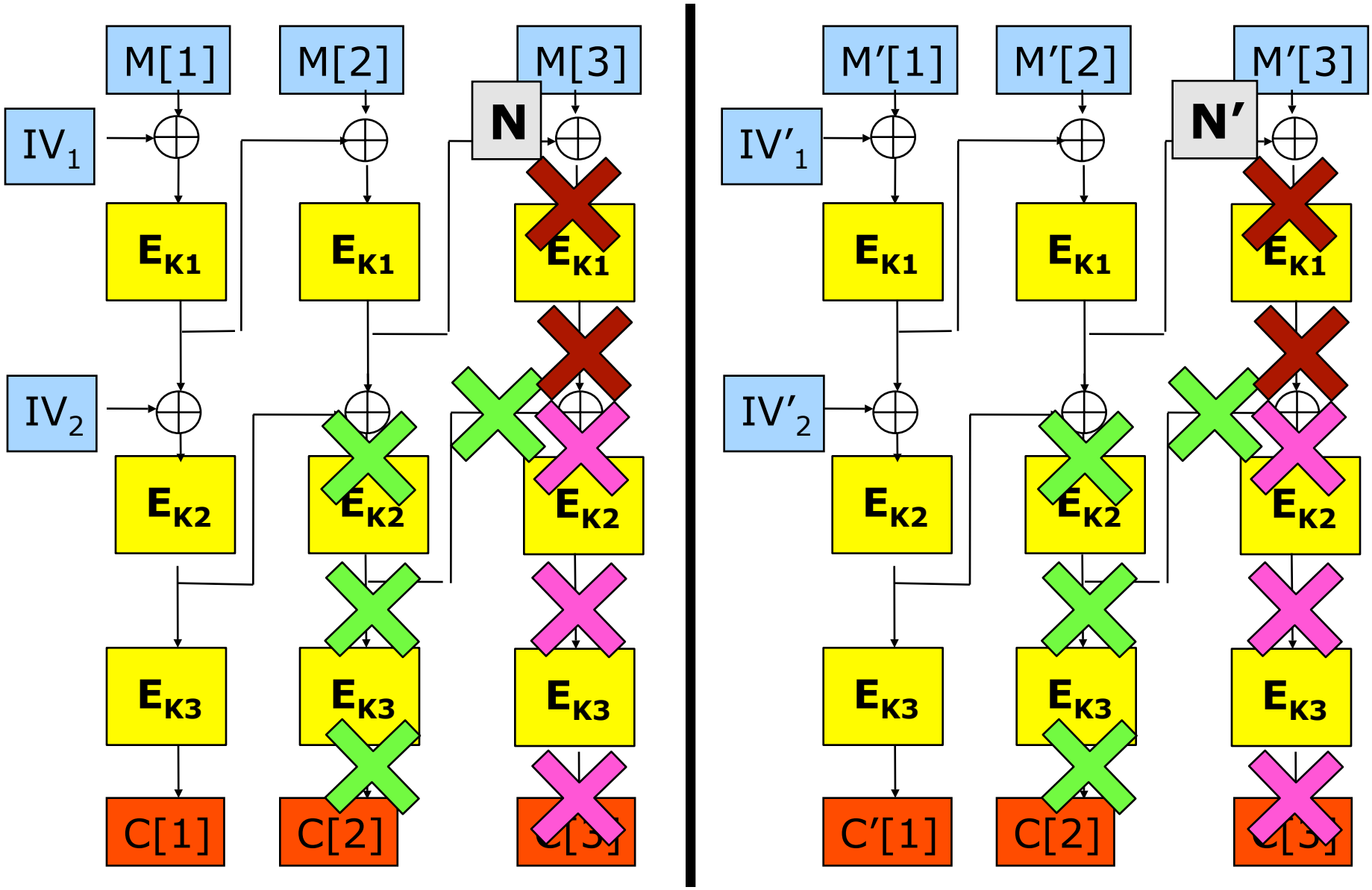
Mode CBC-CBC-ECB



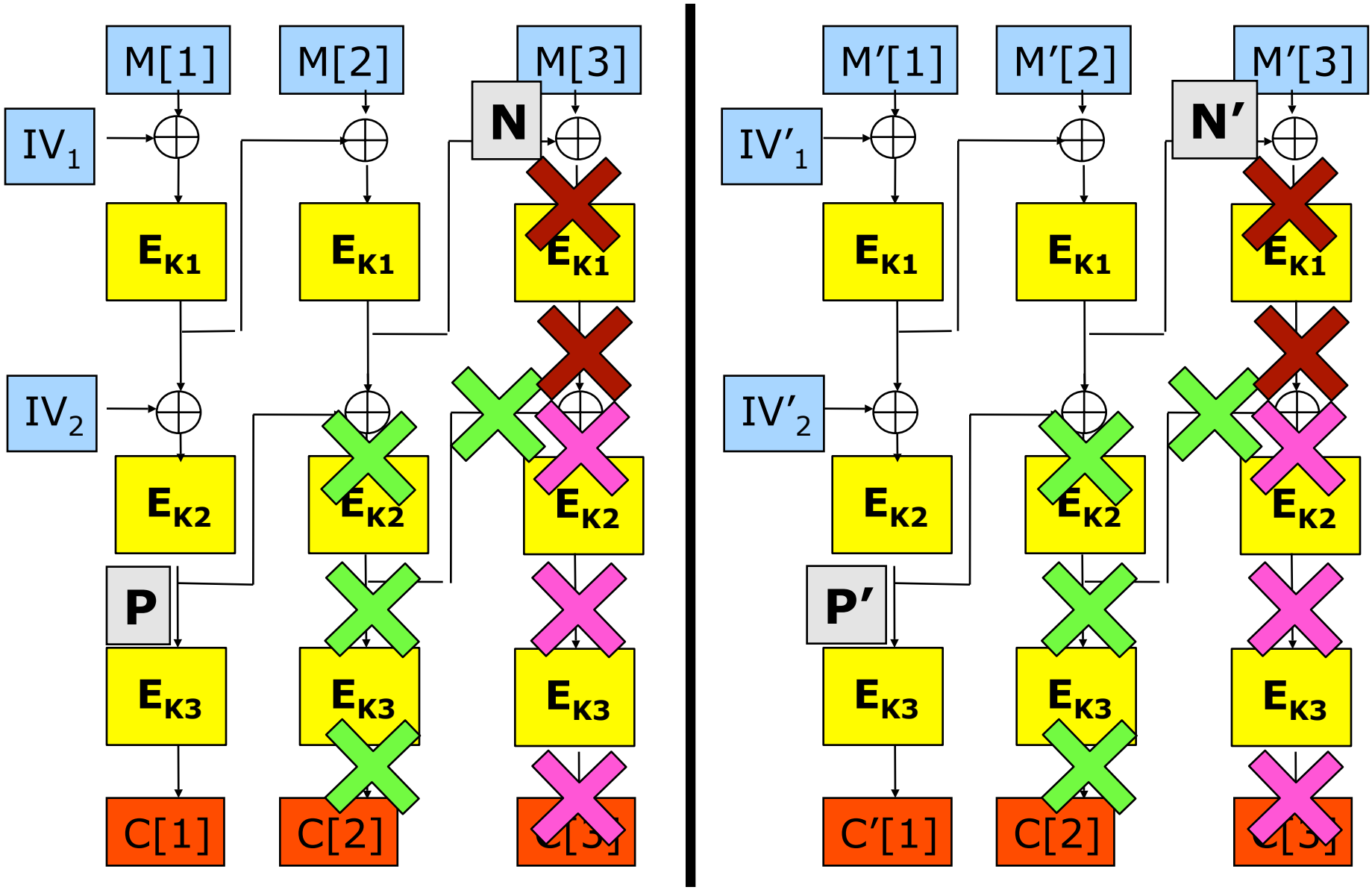
Mode CBC-CBC-ECB



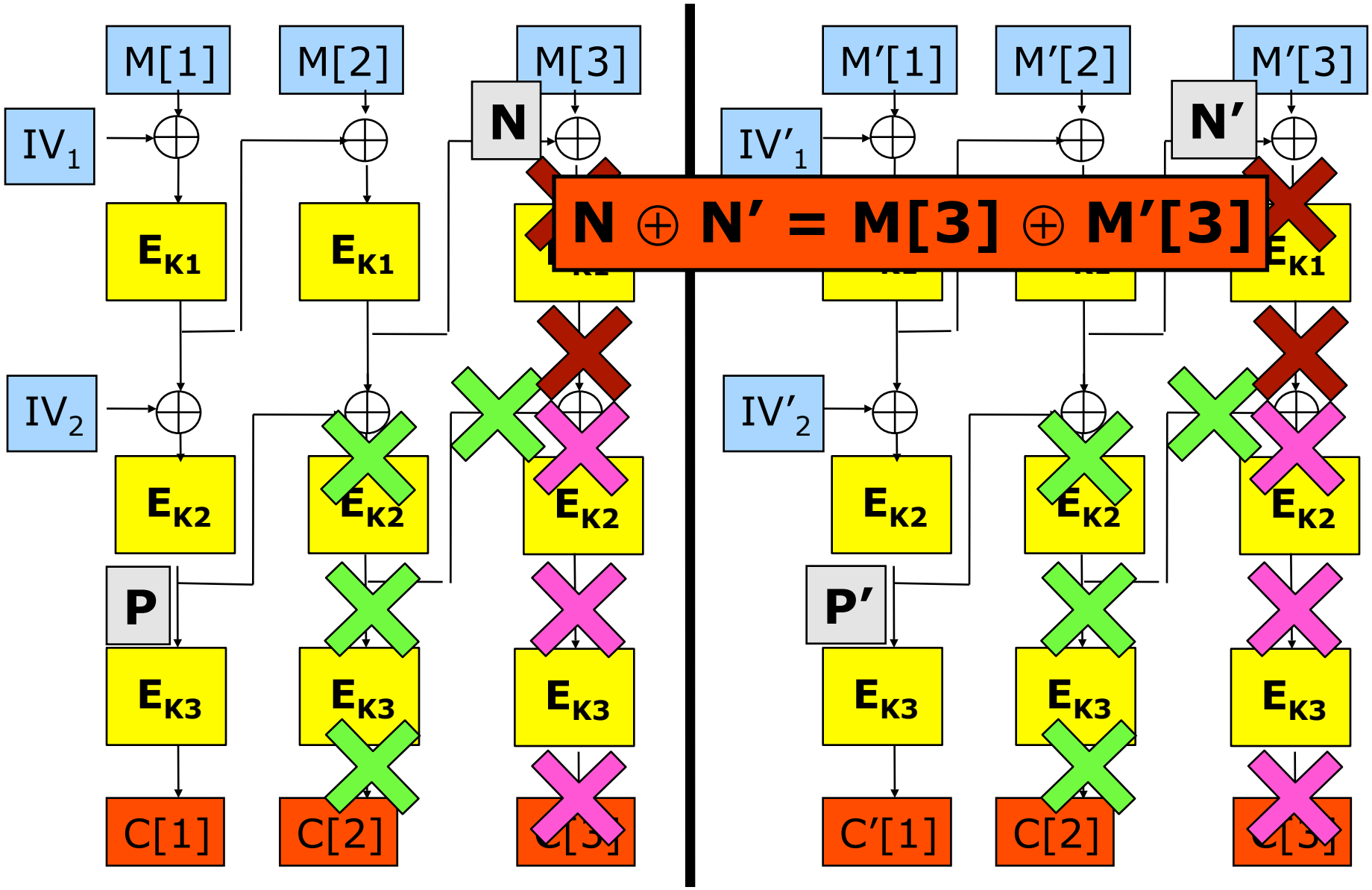
Mode CBC-CBC-ECB



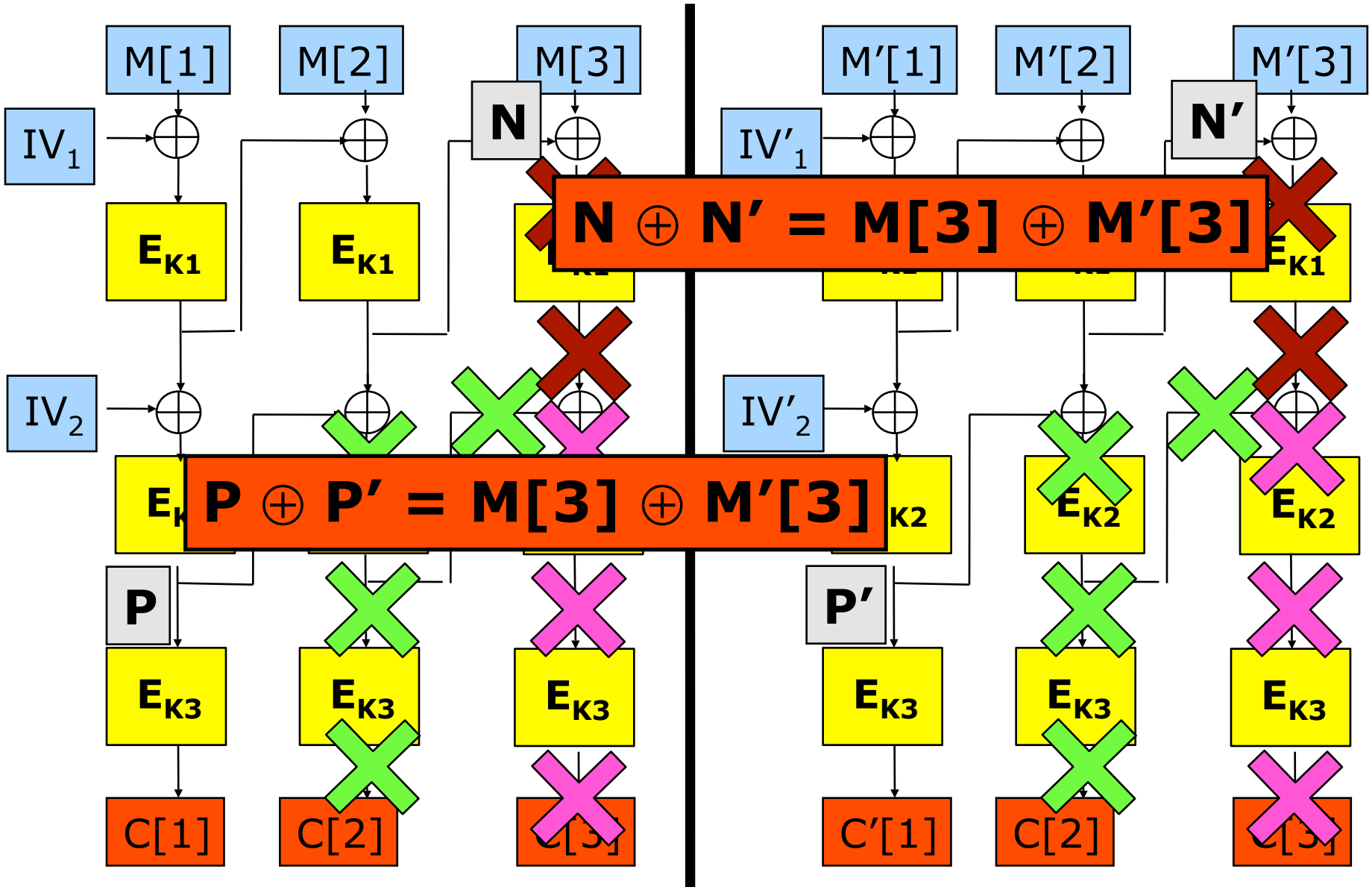
Mode CBC-CBC-ECB



Mode CBC-CBC-ECB



Mode CBC-CBC-ECB



Algorithme d'attaque

- 2 requêtes de déchiffrement
  - $C=(IV_1,IV_2,C_1,C_2,C_3)$
  - $C'=(IV'_1,IV'_2,C'_1,C_2,C_3)$
- Recherche exhaustive de K_3 :
  - Essai des 2^{56} clés K jusqu'à ce que

    $D_K(C_1) \oplus D_K(C'_1) = M_3 \oplus M'_3$
- Recherche exhaustive de K_1 et K_2

Mode CBC-CBC-ECB

- La clé K_3 peut être retrouvée avec une recherche exhaustive grâce à l'équation

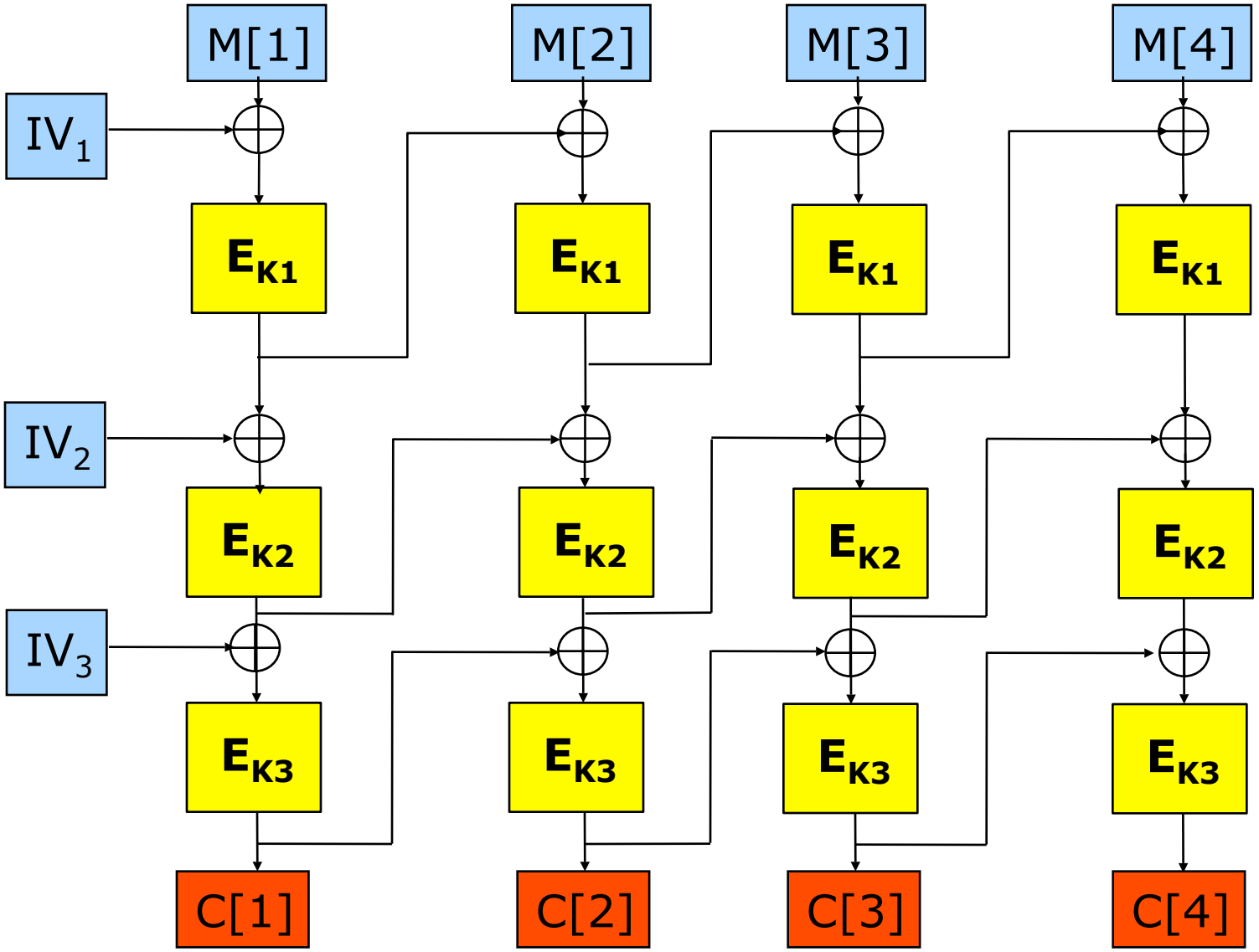
$$D_{K3}(C_1) \oplus D_{K3}(C'_1) = M_3 \oplus M'_3$$

- Variante : attaque à clairs choisis
  - Après 2^n chiffrements de clairs connus, il existe 2 chiffrés C et C' tels que $C_2=C'_2$ et $C_3=C'_3$
  - Si chiffrement DES, n=64

- Il faut ensuite retrouver K_1 et K_2 : attaque similaire à une attaque Double DES
- Optimisation possible

Autre technique

Exemple : CBC-CBC-CBC



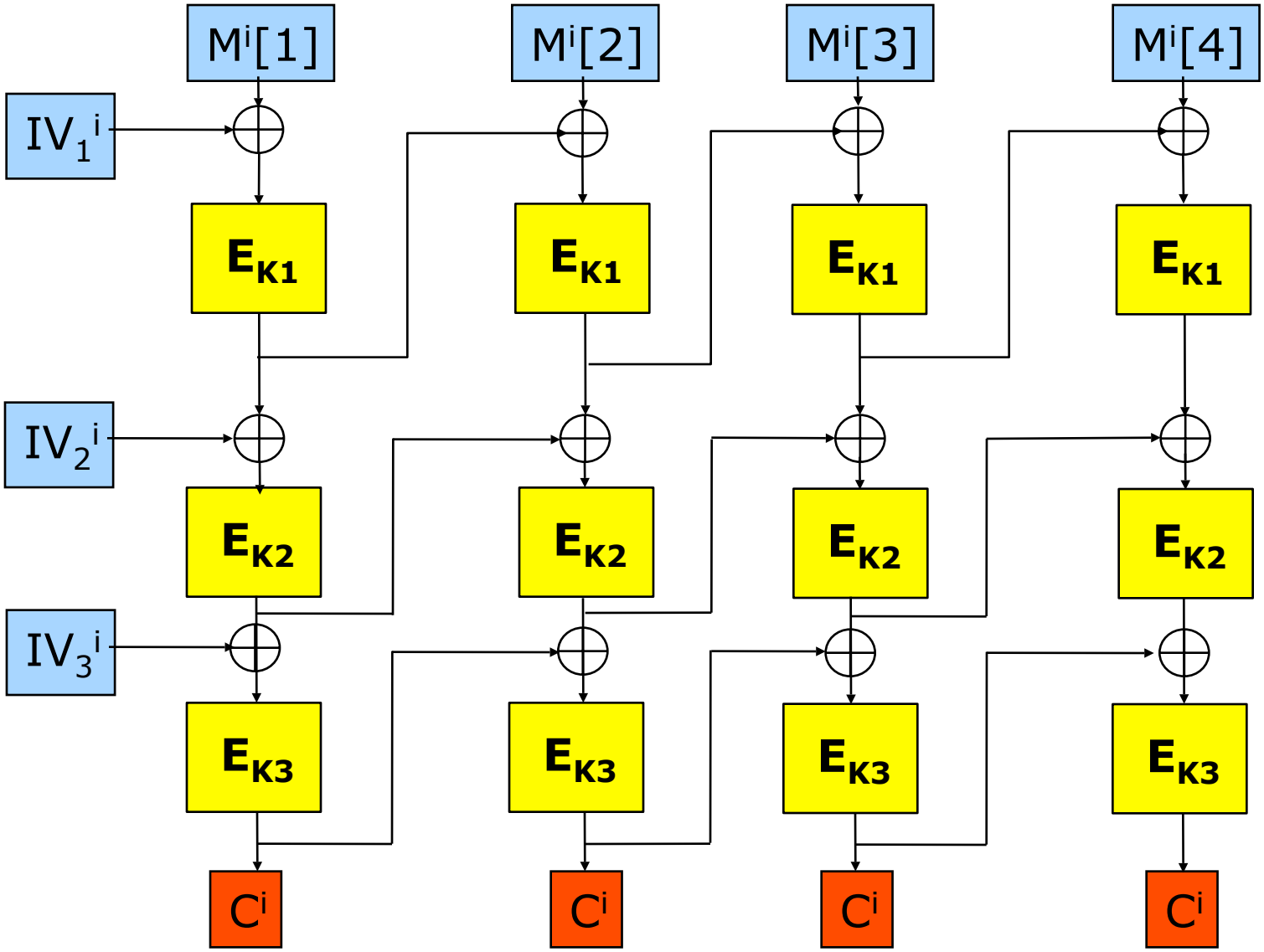
Attaque

- Attaque à chiffrés choisis
  - Requêtes de la forme (C^i, C^i, C^i, C^i)
- On veut détecter une collision de la forme

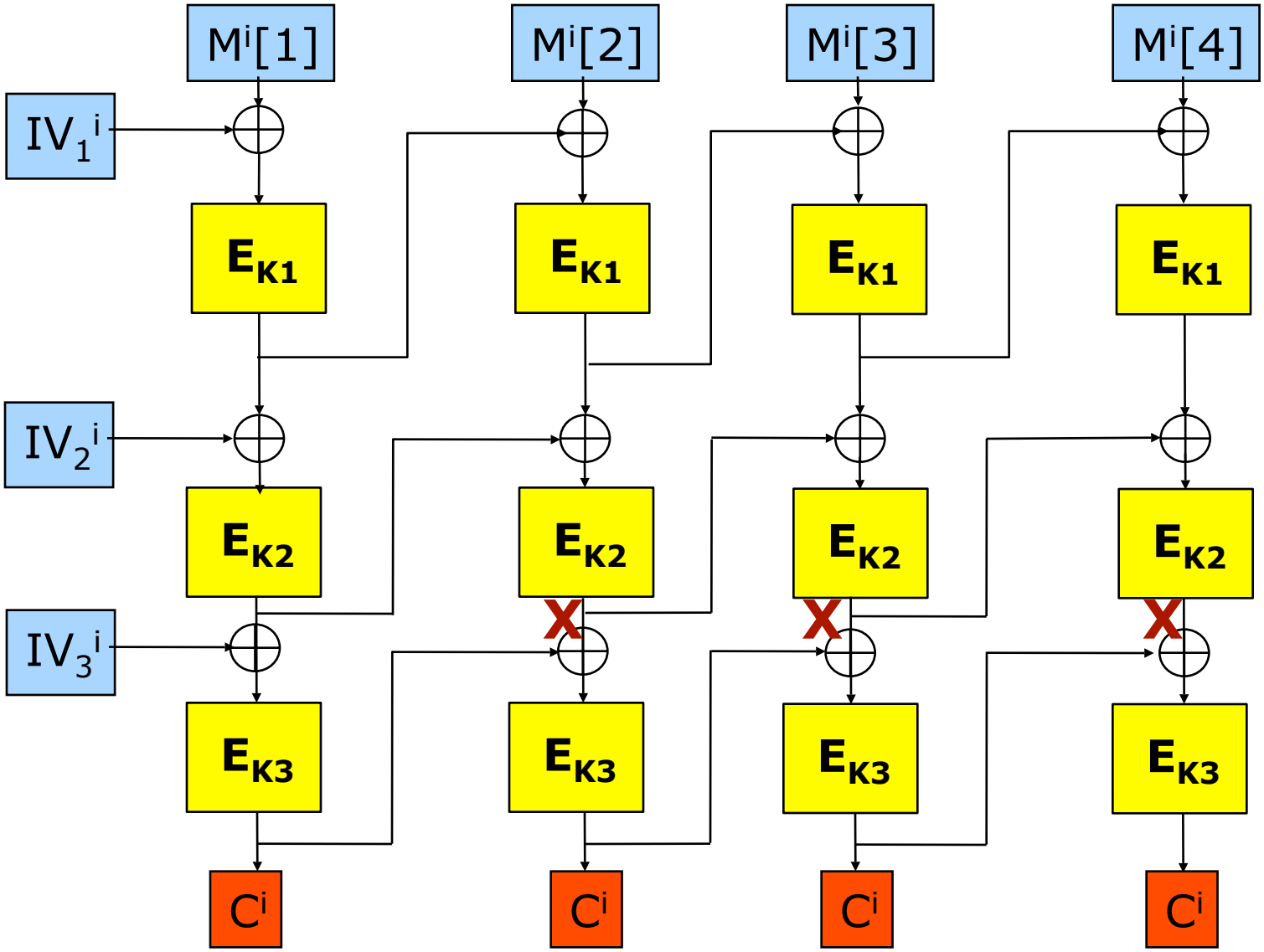
$$D_{k3}(C^i) \oplus C^i = D_{k3}(C^j) \oplus C^j$$

- Il faut ensuite l'exploiter pour retrouver la clé K_3
  - On teste toutes les clés K_3 et on cherche pour laquelle la collision a lieu
  - Restent les clés K_2 et K_3 à retrouver : attaque similaire à une attaque 2DES

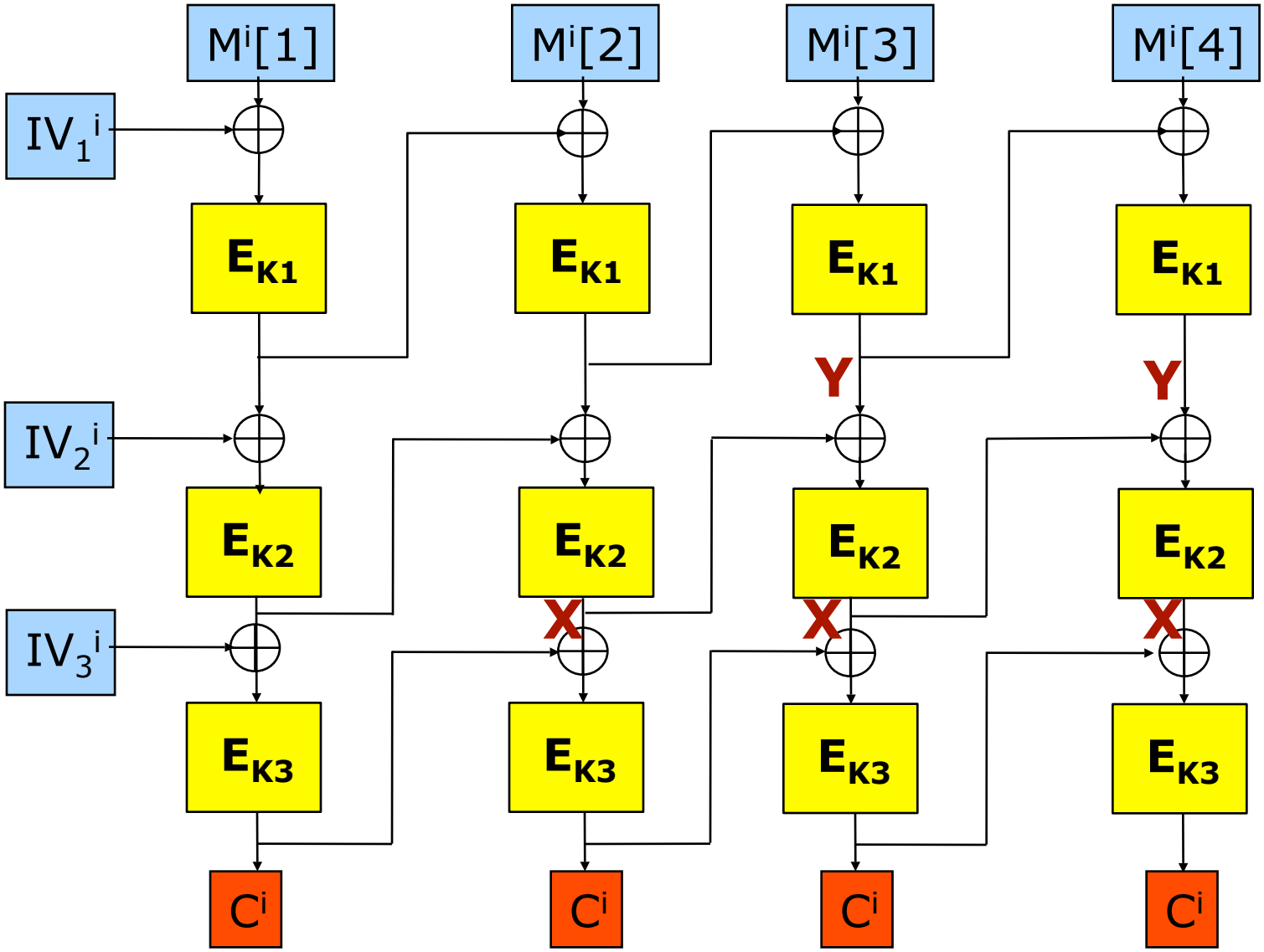
Détection de la collision



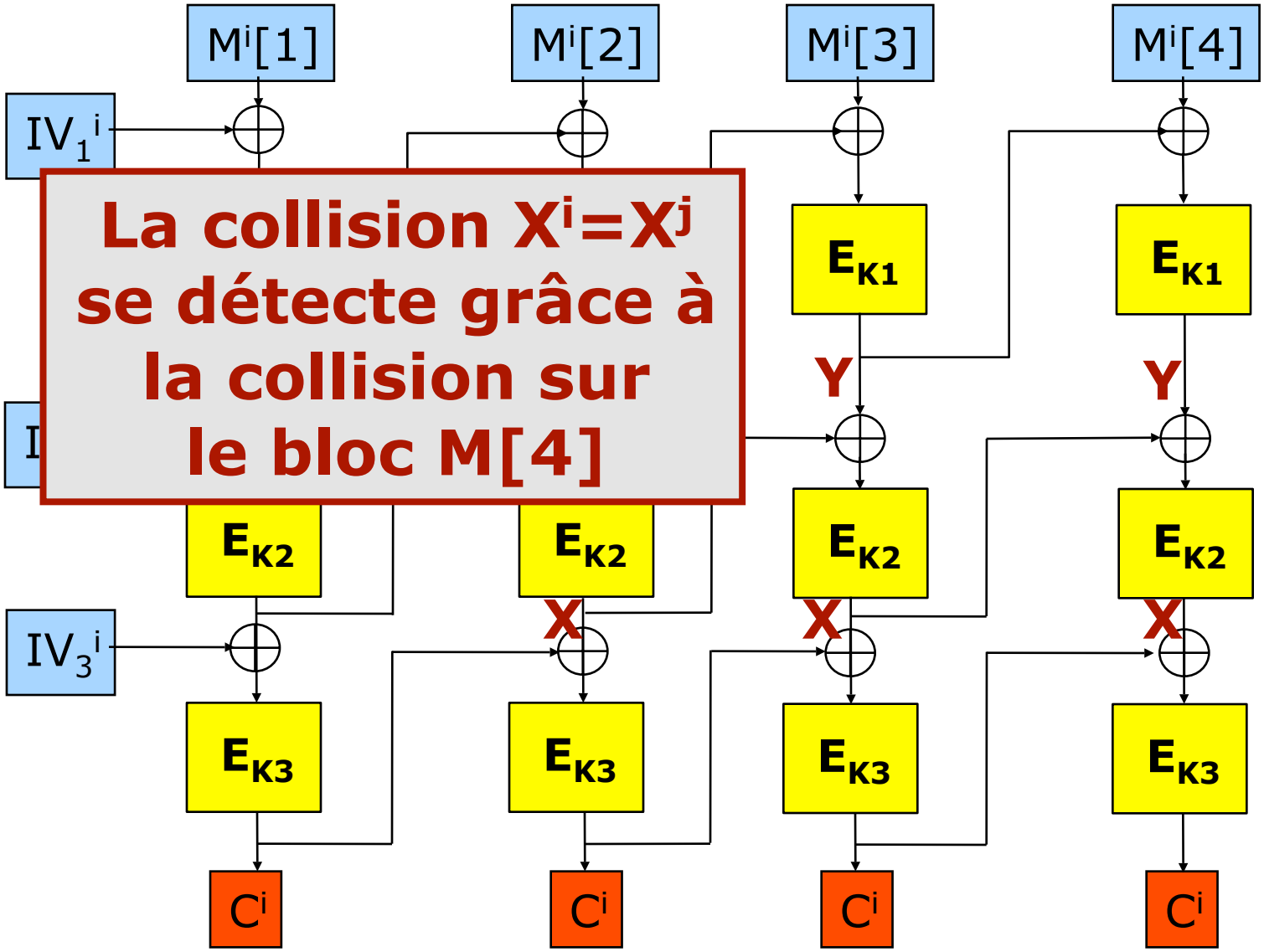
Détection de la collision



Détection de la collision



Détection de la collision



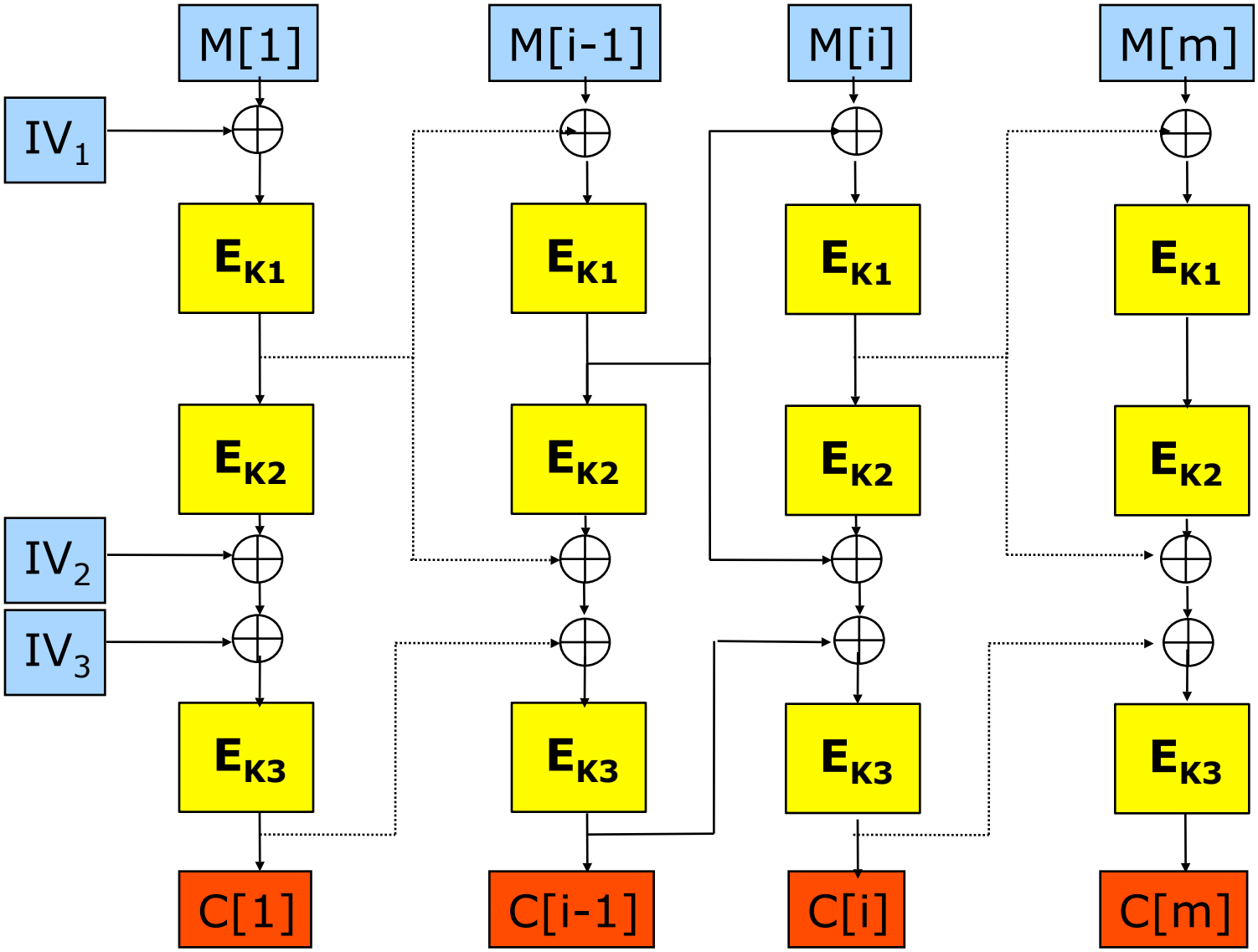
Attaque

- $2^{n/2}$ requêtes de déchiffrement de la forme (C,C,C,C)
  - collision sur X pour deux d'entre deux
  - On peut la détecter grâce à la collision sur le bloc de clair M[4]
- Recherche des clés :
  - On cherche K_3 telle que

$$D_{K3}(C^i) \oplus C^i = D_{K3}(C^j) \oplus C^j$$

  - Puis on cherche K_2 et K_3 avec une attaque similaire à celle sur le double DES

CBC-CBC^{-1}-CBC



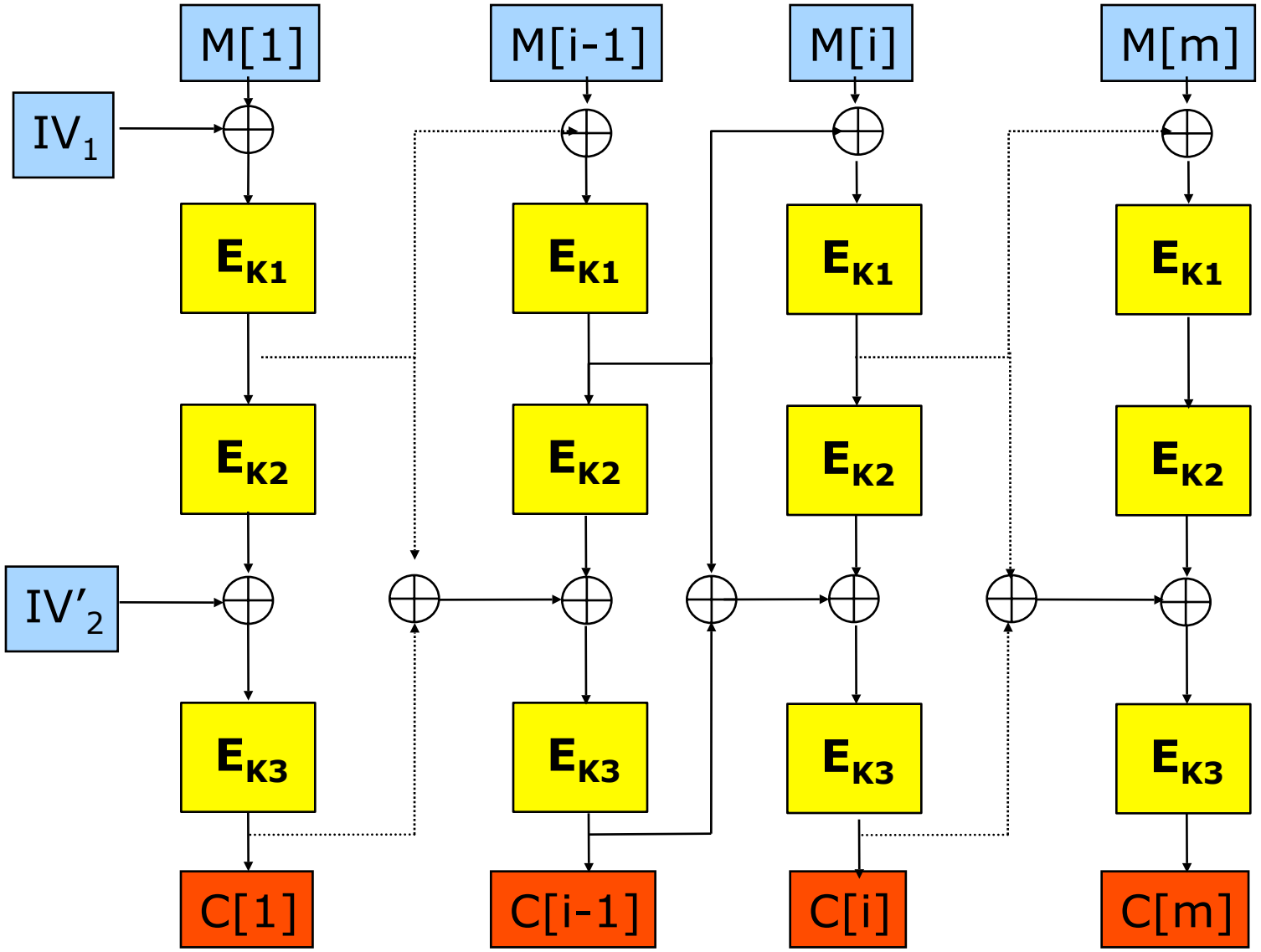
Remarque

- Il faut voir que :

$$(A \oplus B) \oplus C = A \oplus (B \oplus C)$$

- Par conséquent, on peut redessiner le mode

CBC-CBC^{-1}-CBC



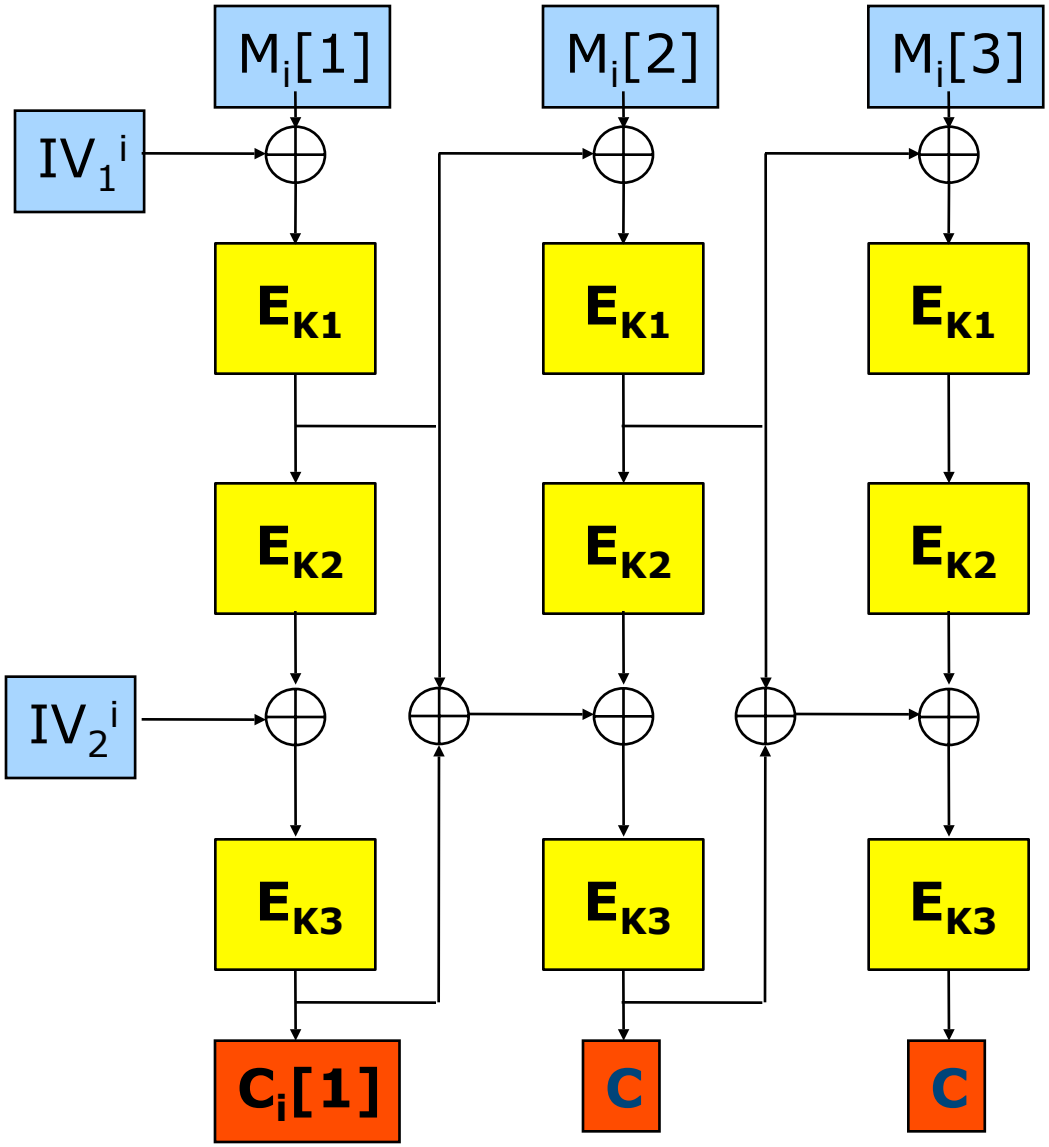
Attaque

- Attaque à chiffrés choisis
- Requêtes de déchiffrement pour des chiffrés de la forme

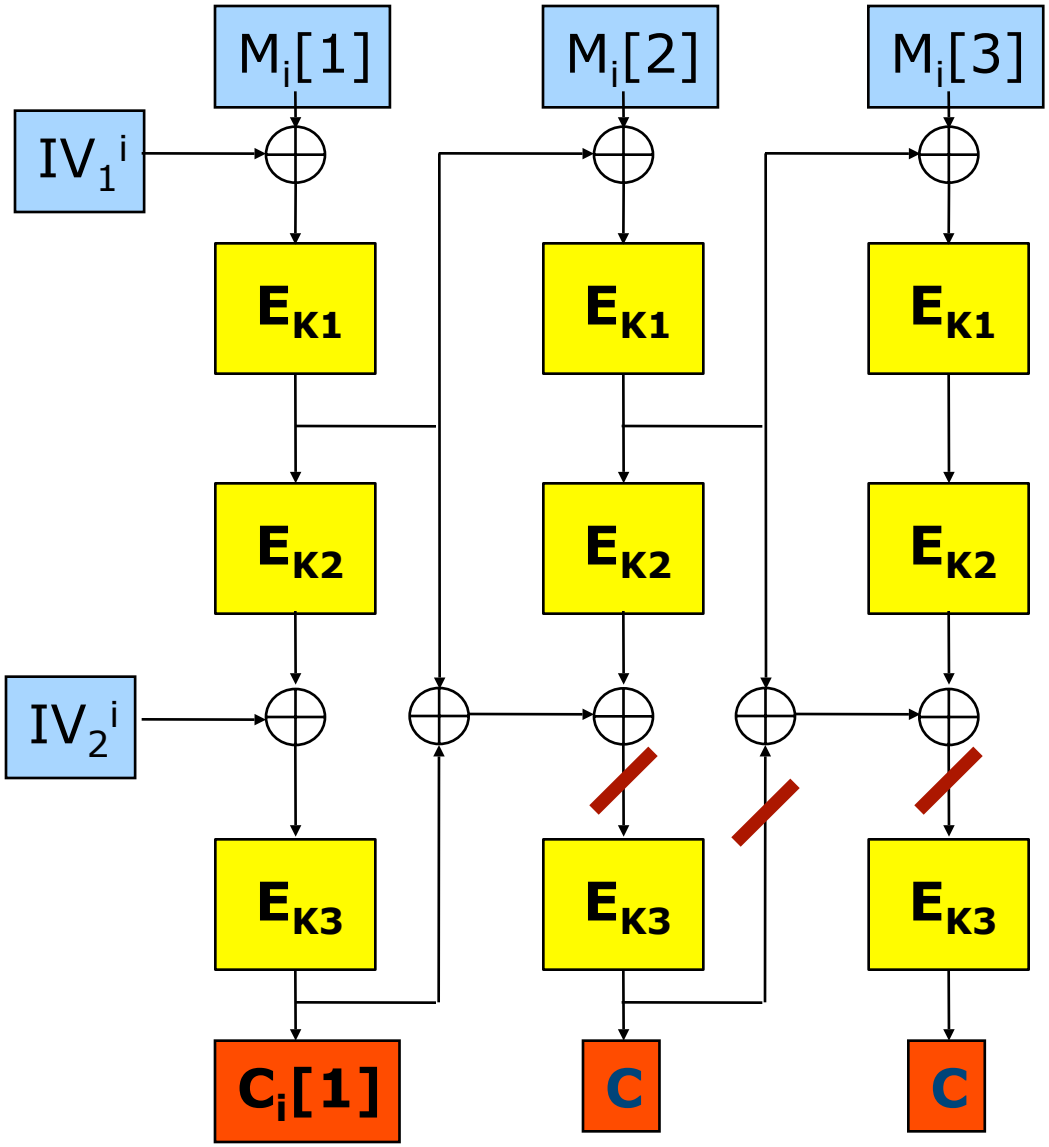
$$(IV^i_1, IV^i_2, C^i_1, C_2, C_3)$$

- On attend une collision sur la valeur X
  - Comment la détecter
  - Comment une telle collision peut permettre de retrouver les clés

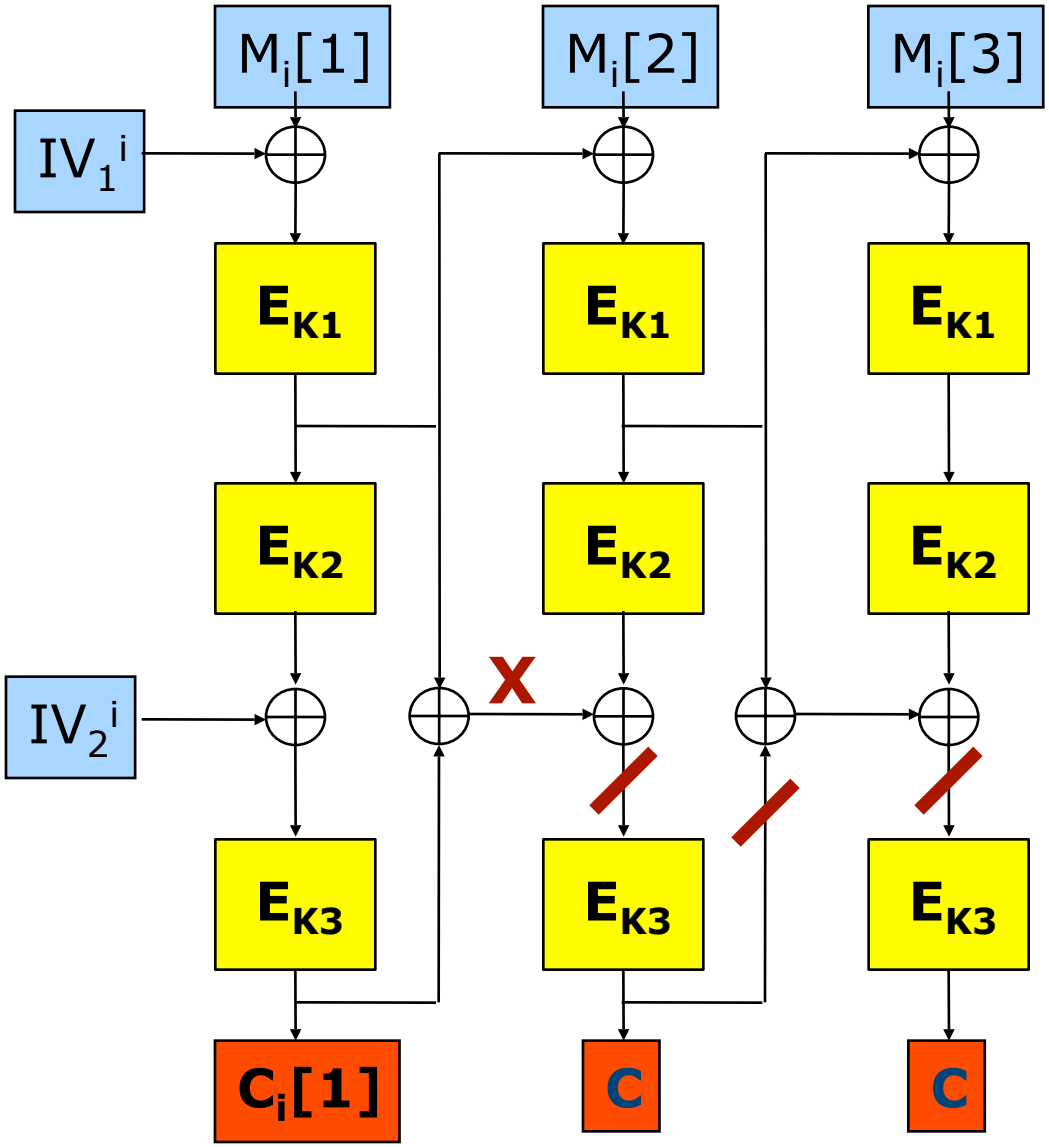
Détection de la collision



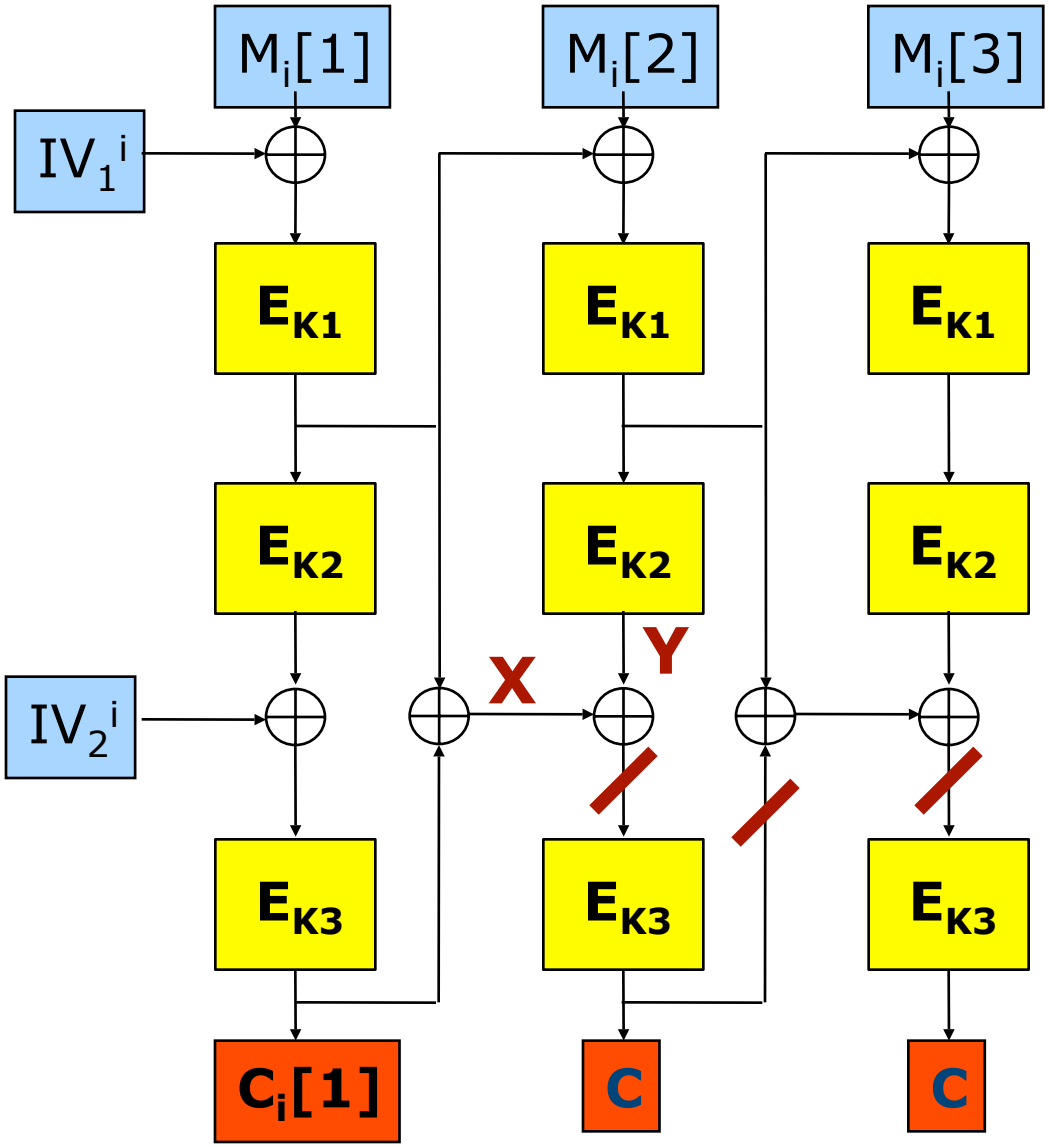
Détection de la collision



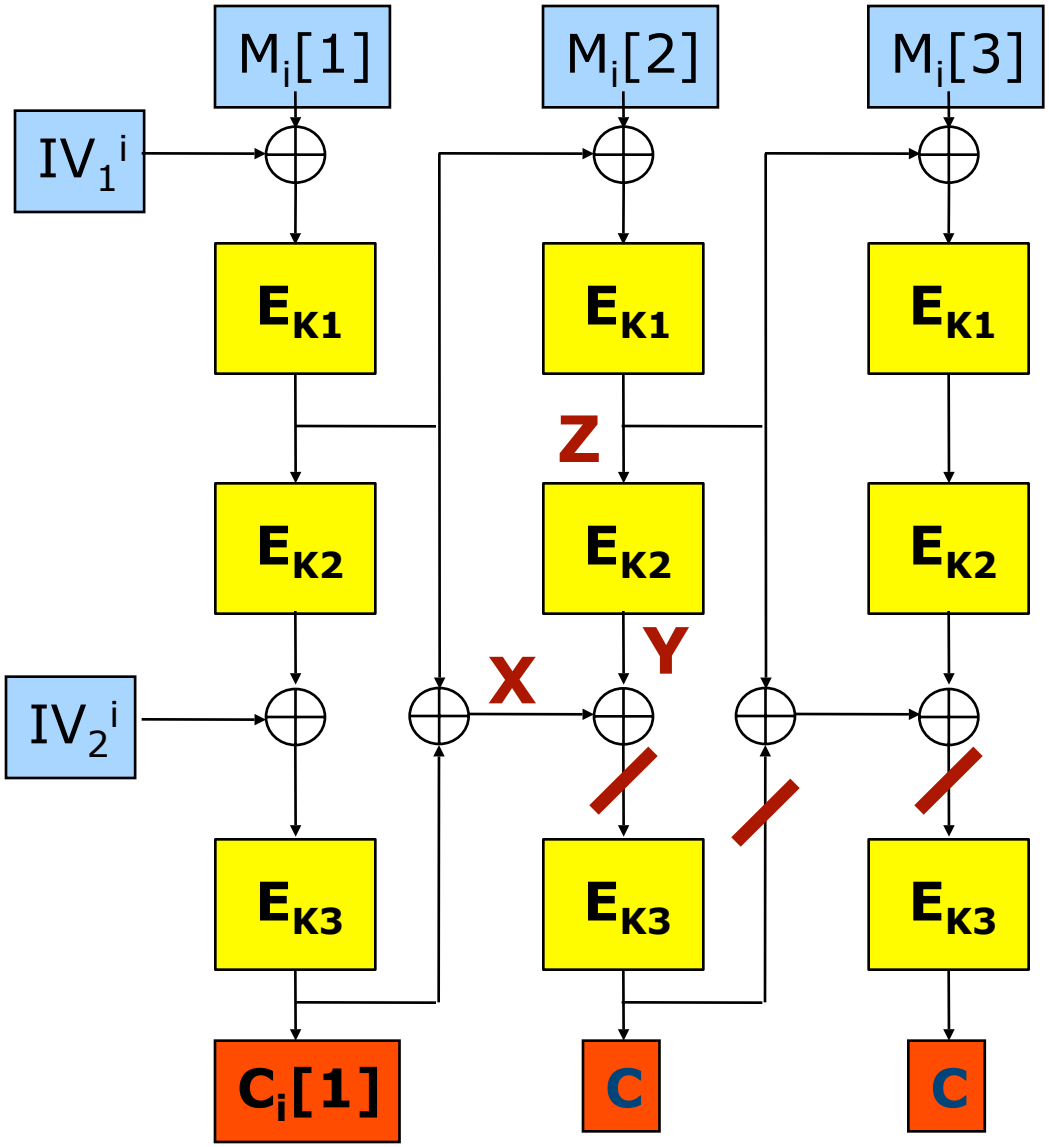
Détection de la collision



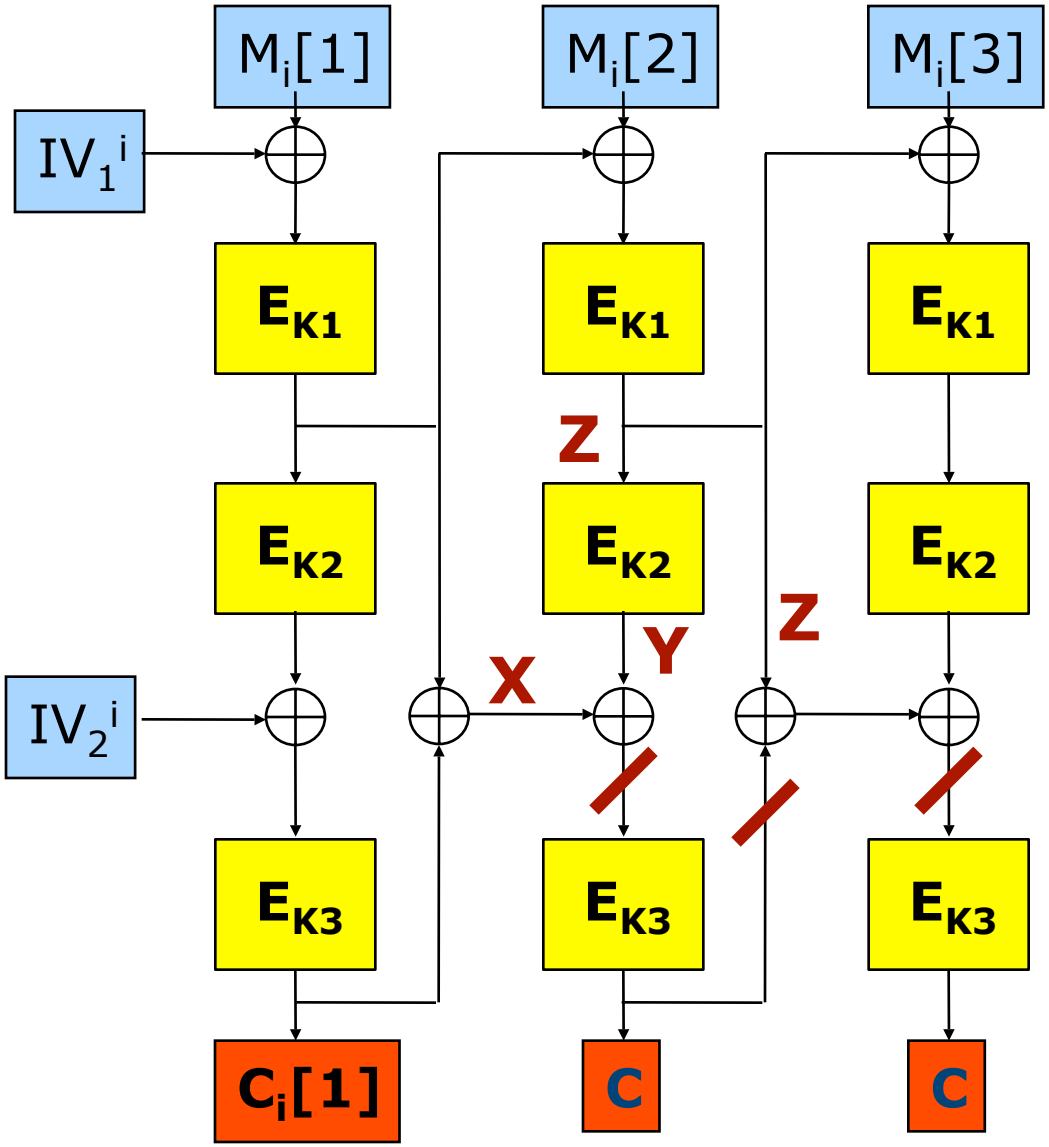
Détection de la collision



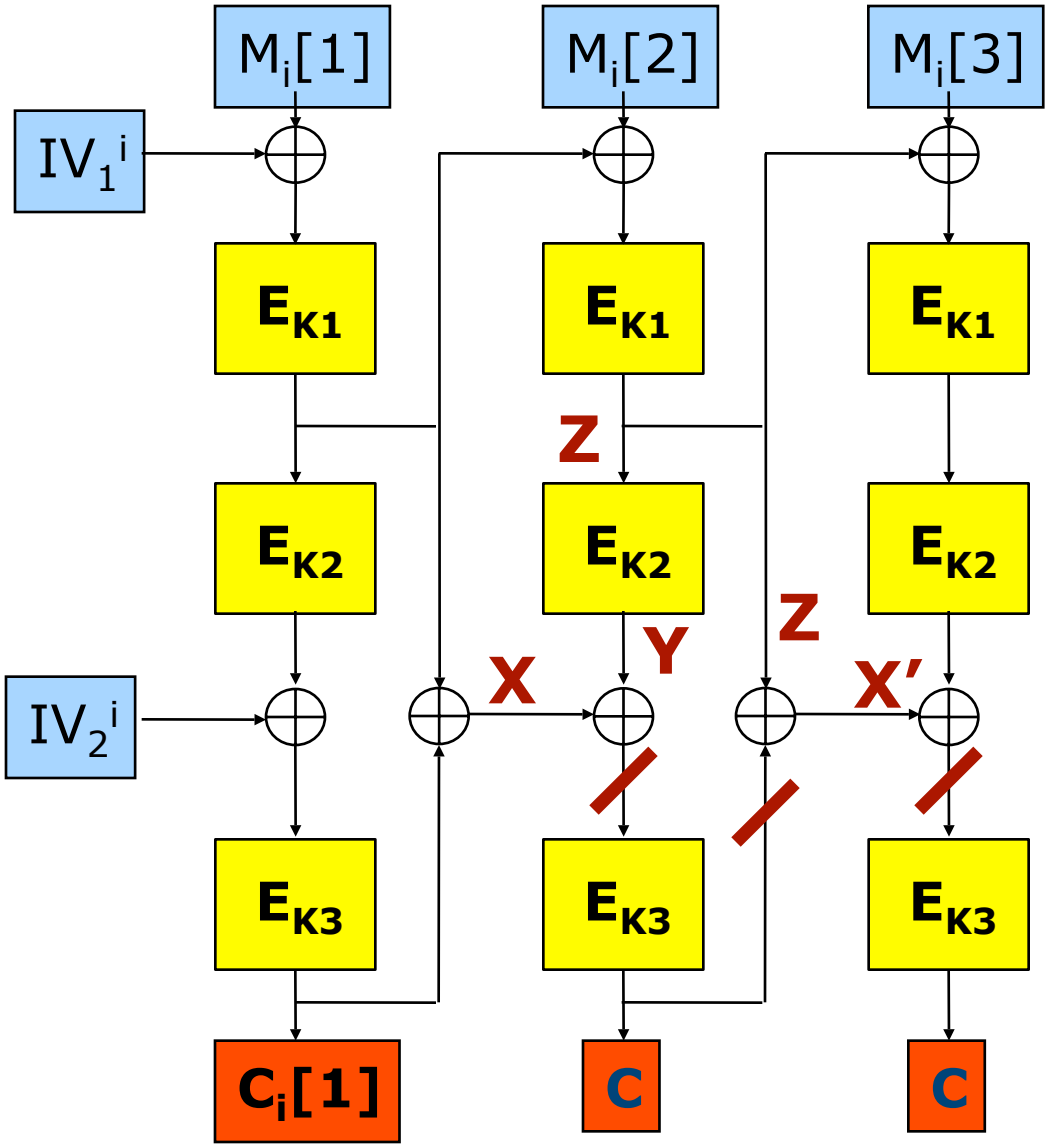
Détection de la collision



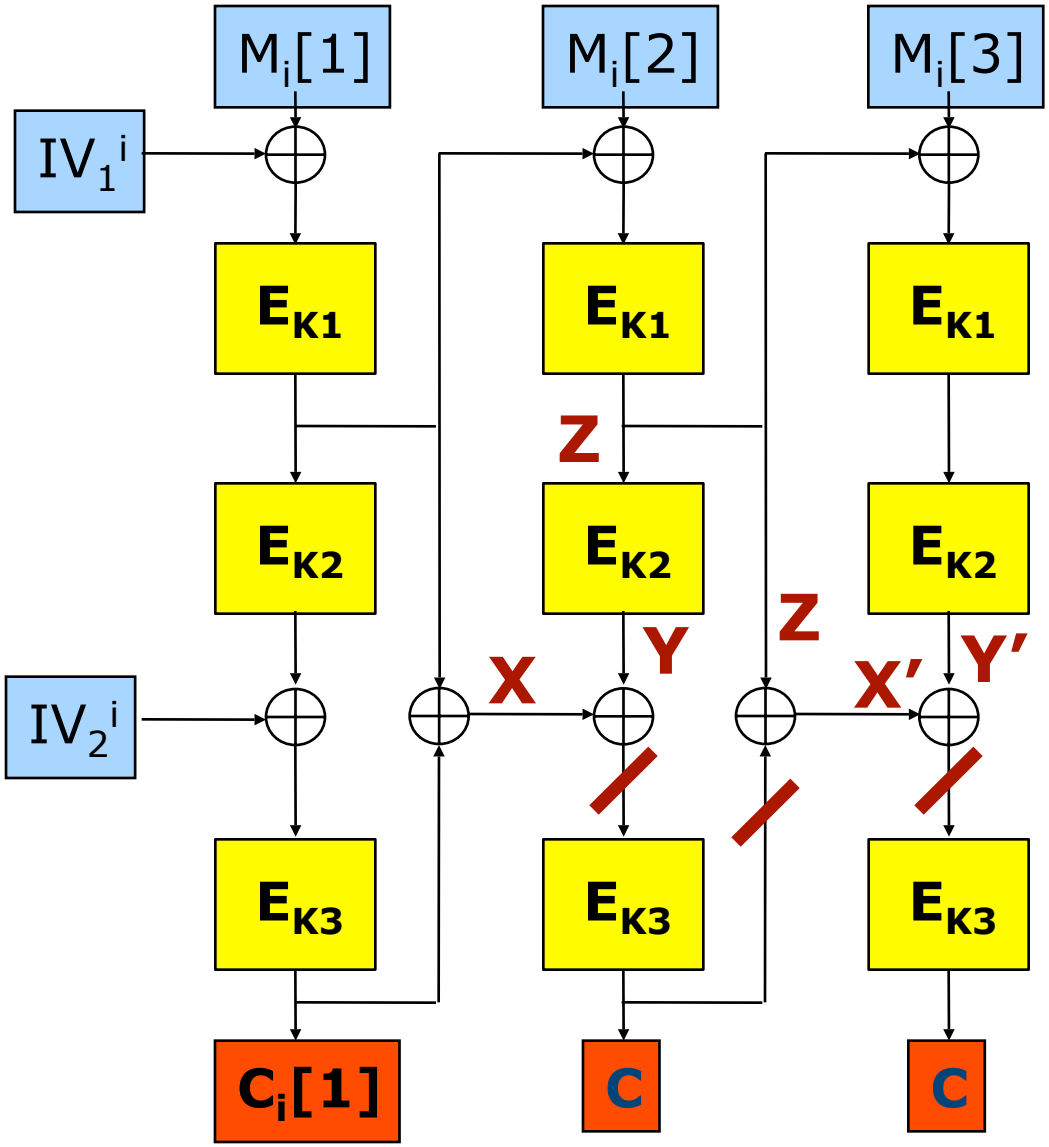
Détection de la collision



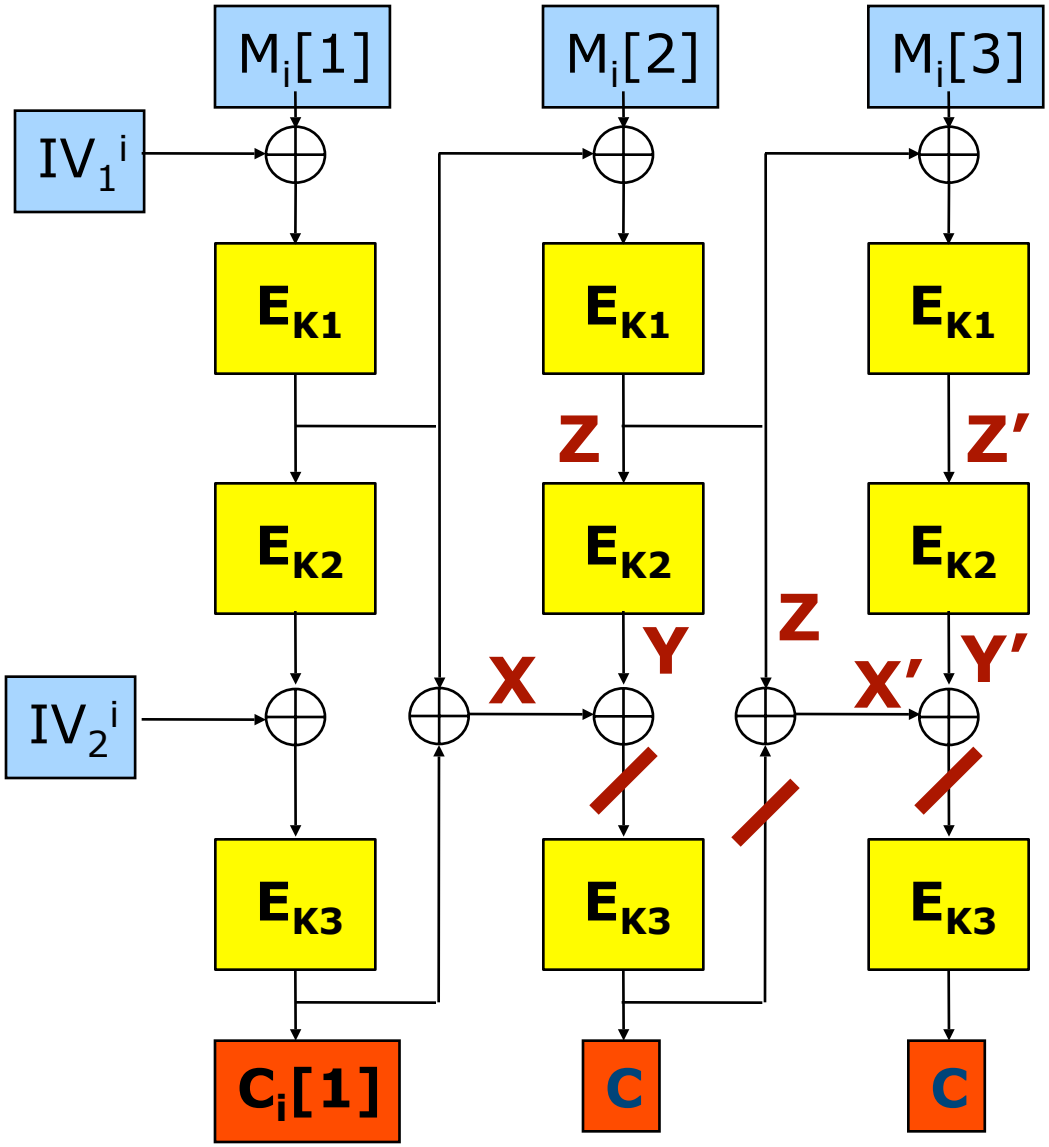
Détection de la collision



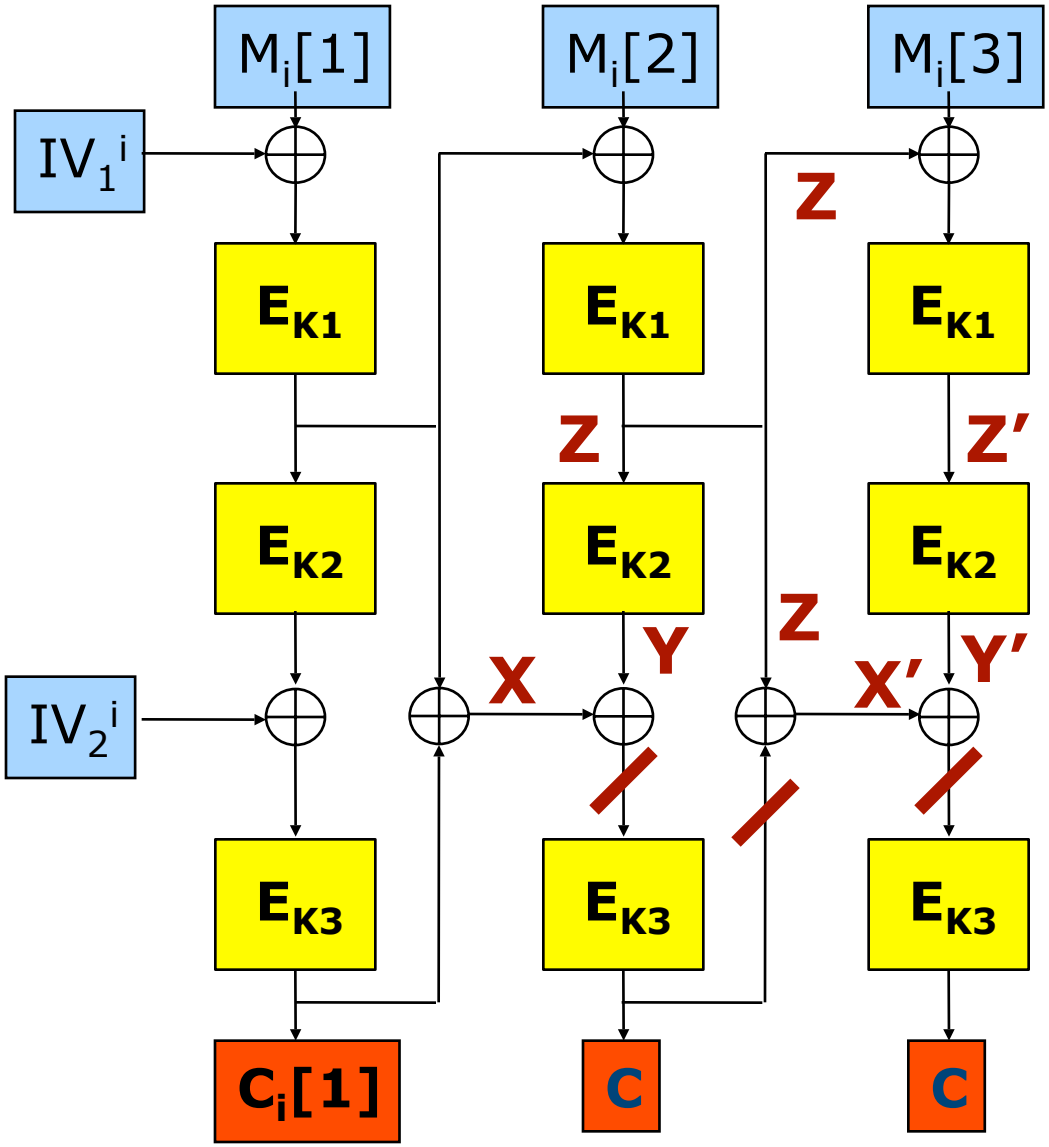
Détection de la collision



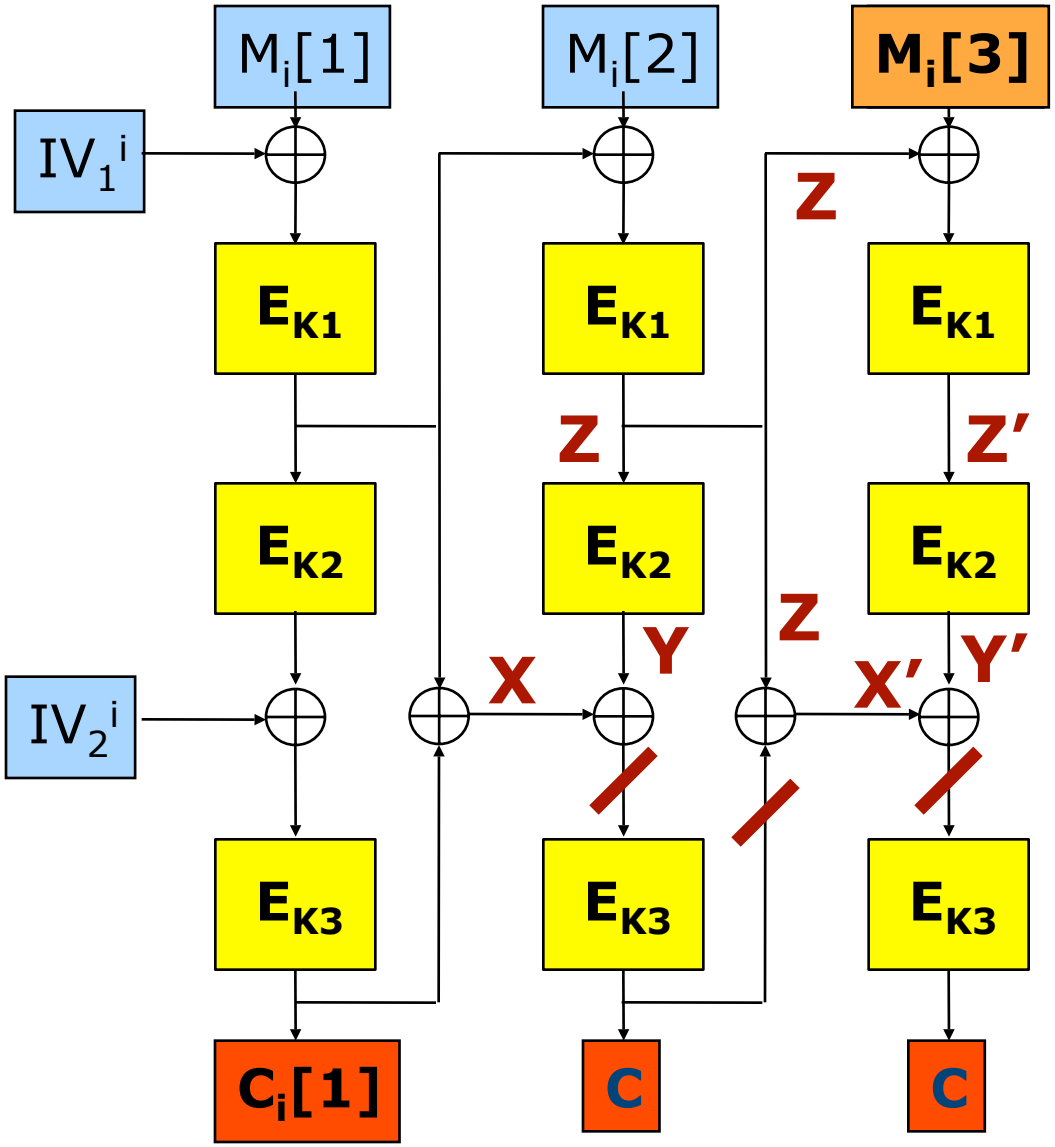
Détection de la collision



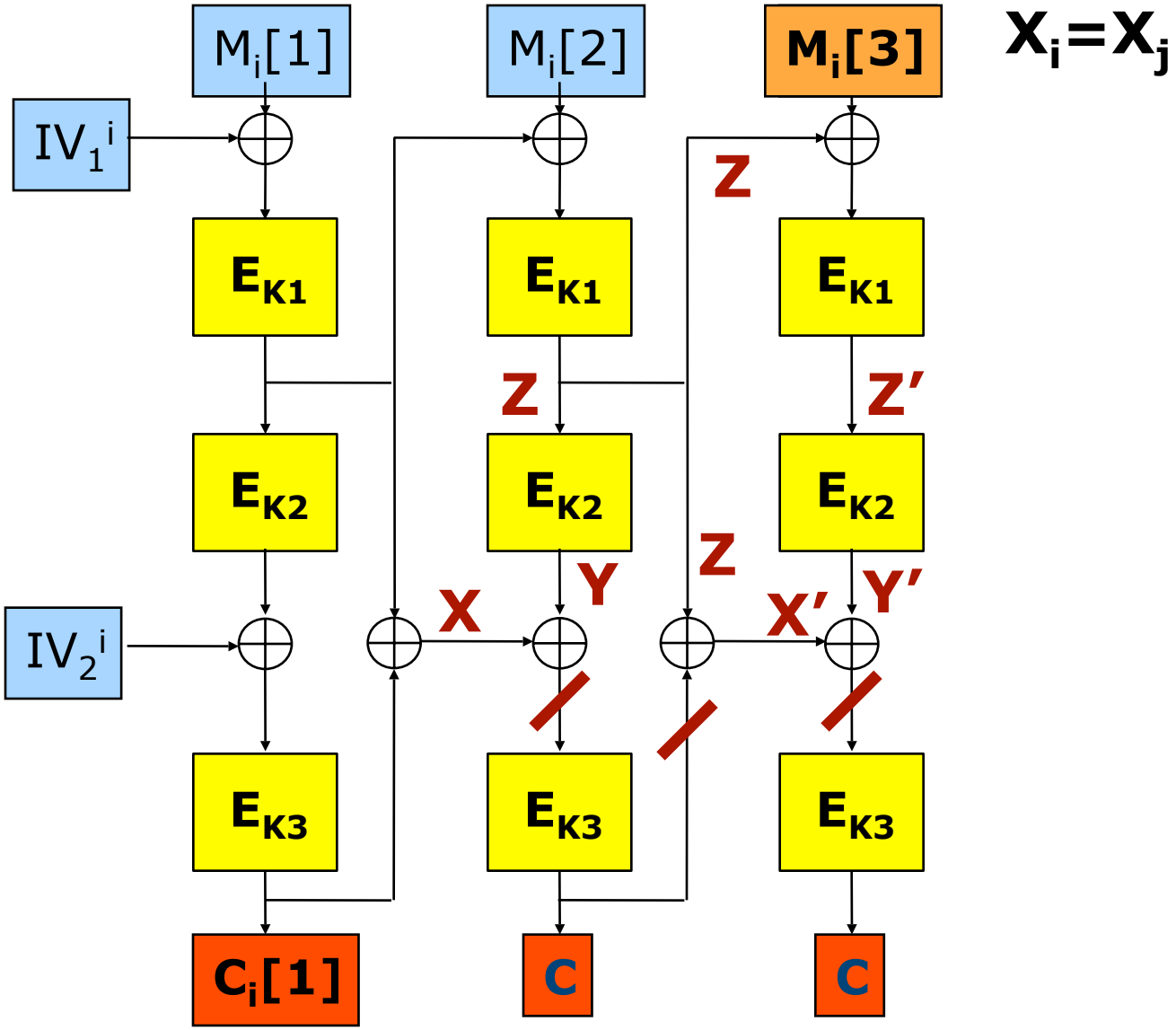
Détection de la collision



Détection de la collision

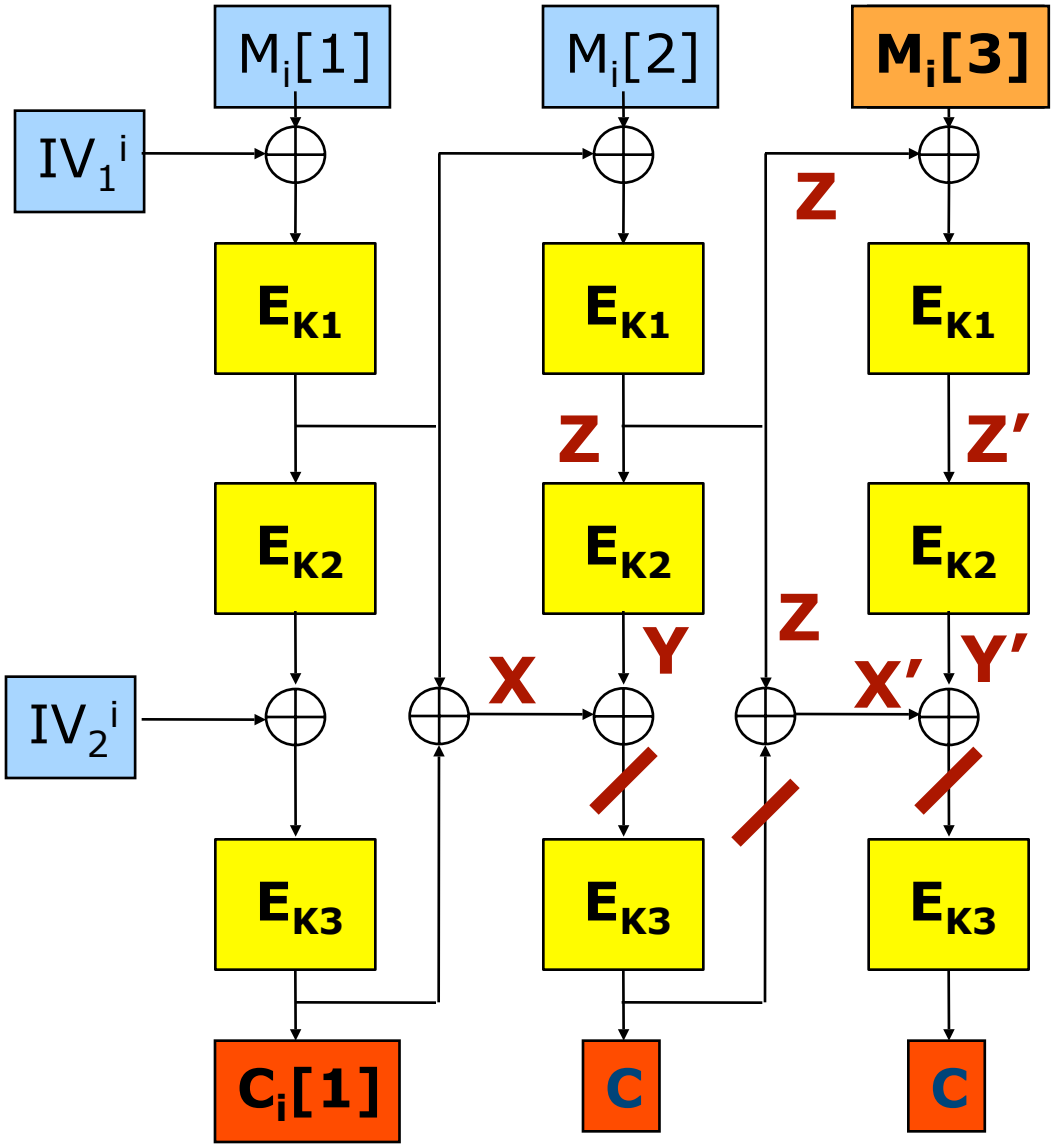


Détection de la collision



$X_i = X_j$

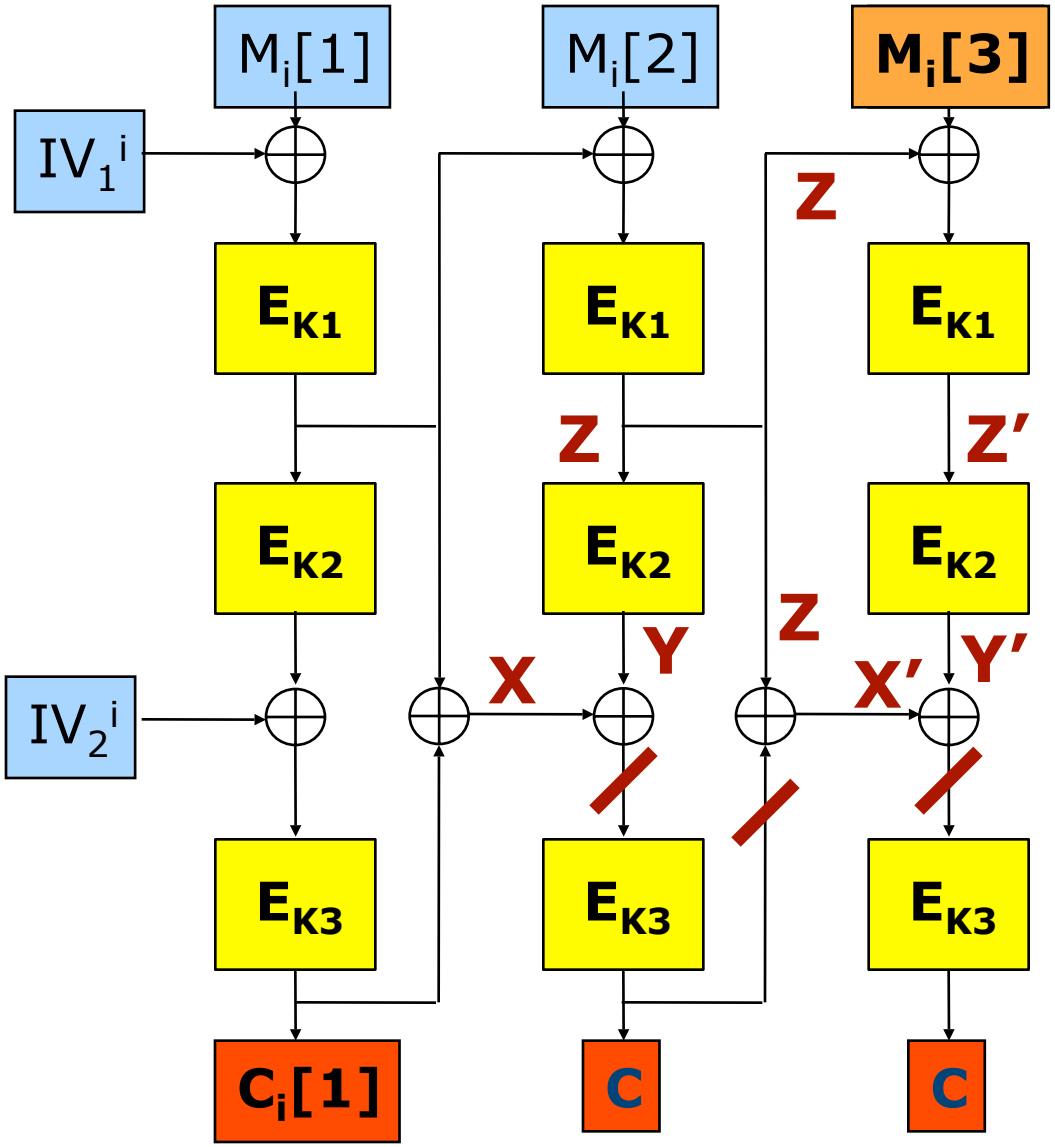
Détection de la collision



$X_i = X_j$

$Y_i = Y_j$

Détection de la collision

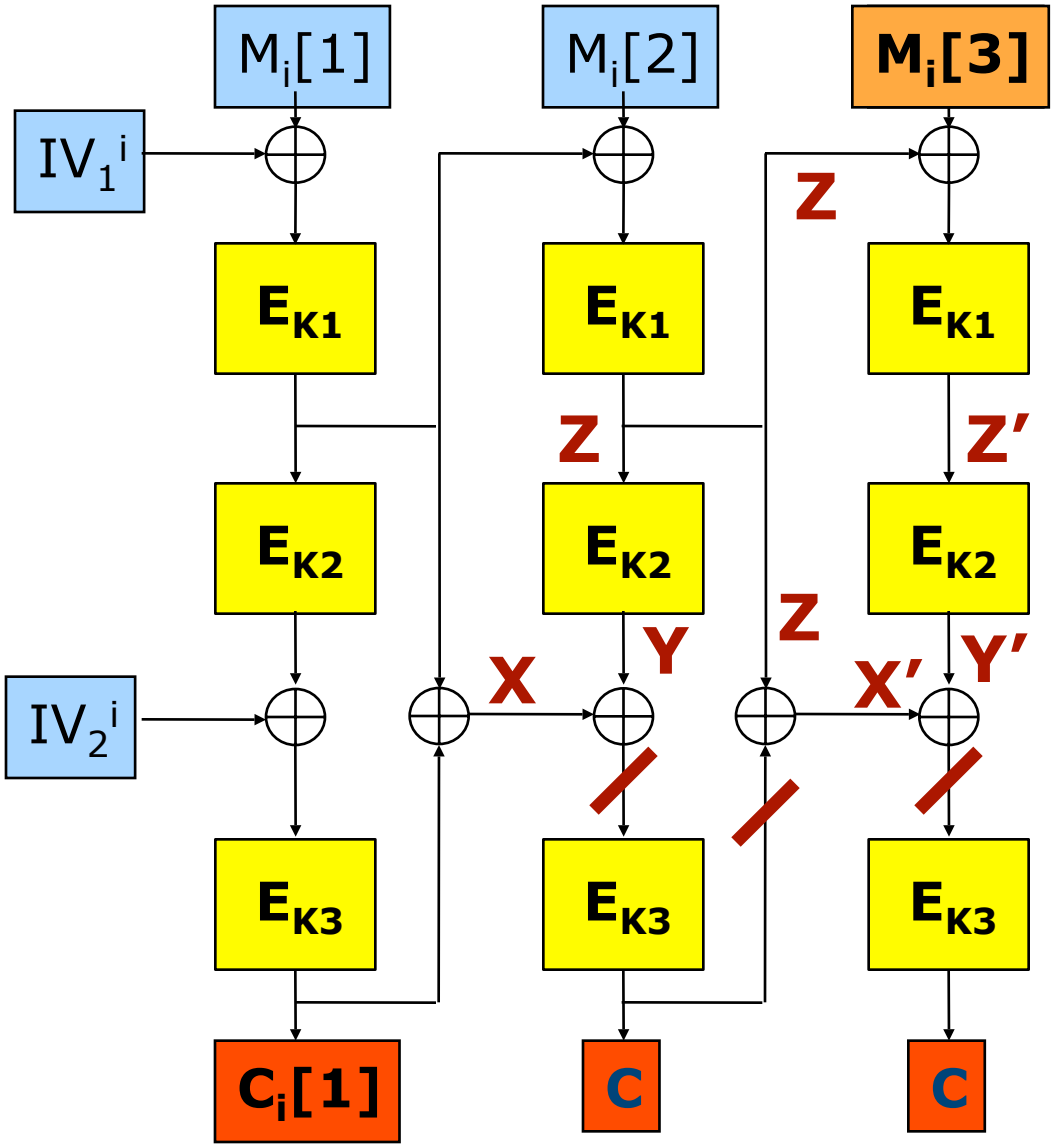


$X_i = X_j$

$Y_i = Y_j$

$Z_i = Z_j$

Détection de la collision



$X_i = X_j$

$Y_i = Y_j$

$Z_i = Z_j$

$M_i[3] = M_j[3]$

Détection de la collision

- On sait que :
  - $X_i = X_j$
  - $C_2^i = C_2^j$
- Donc
  - $Y_i = Y_j$ et $Z_i = Z_j$
  - Et $M_3^i = M_3^j$
- La collision peut donc être détectée

Recherche des clés

- Dès que la collision est détectée, il faut l'exploiter
- Recherche de la clé K_1
  - On sait que $Z_i=Z_j$
  - On connaît les clairs M^i et M^j correspondants
  - Par conséquent :

$$E_{K1}(E_{K1}(M_1^i \oplus IV_1^i) \oplus M_2^i) = E_{K1}(E_{K1}(M_1^j \oplus IV_1^j) \oplus M_2^j)$$

Recherche des clés

- Dès que K_1 est retrouvée, on peut retrouver K_2 et K_3 avec une attaque similaire à celle sur le double DES