Modes Opératoires et Authentification

Confidentialité, Intégrité et Authenticité

Yann Rotella

UVSQ - Université Paris-Saclay

19 mars 2026

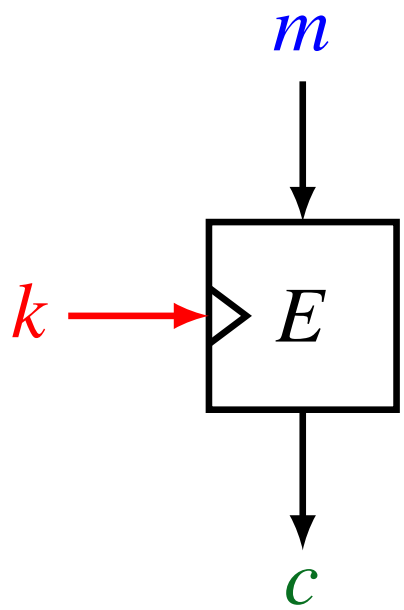
Plan du Cours

Modes Opératoires

Les MAC

Le Chiffrement Authentifié avec Données Associées - AEAD

MODES DE CHIFFREMENT

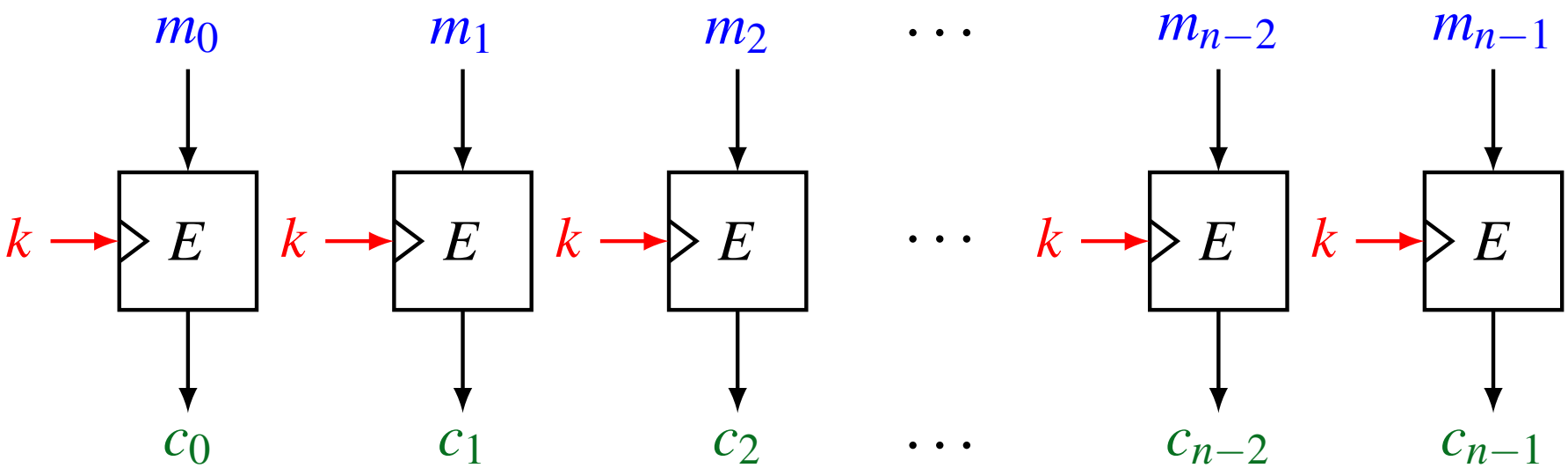


- On sait construire des chiffrements par bloc
- On sait transformer n'importe quelle chaîne de bits en une chaîne de bits de longueur multiple de la taille des blocs (padding).

PROBLÈME

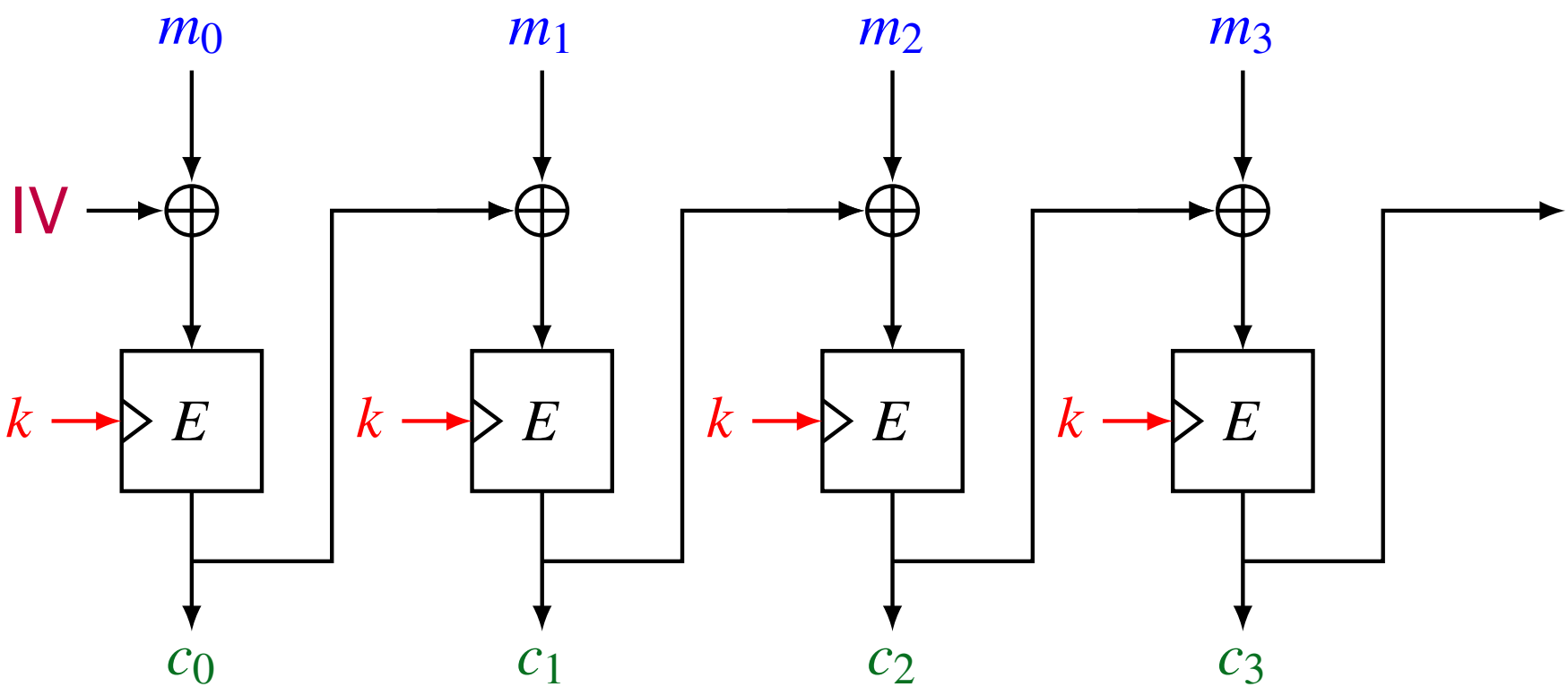
Comment combiner les chiffrements par bloc afin de chiffrer n'importe quelle taille de message ?

Le mode ECB (Electronic Code Block)



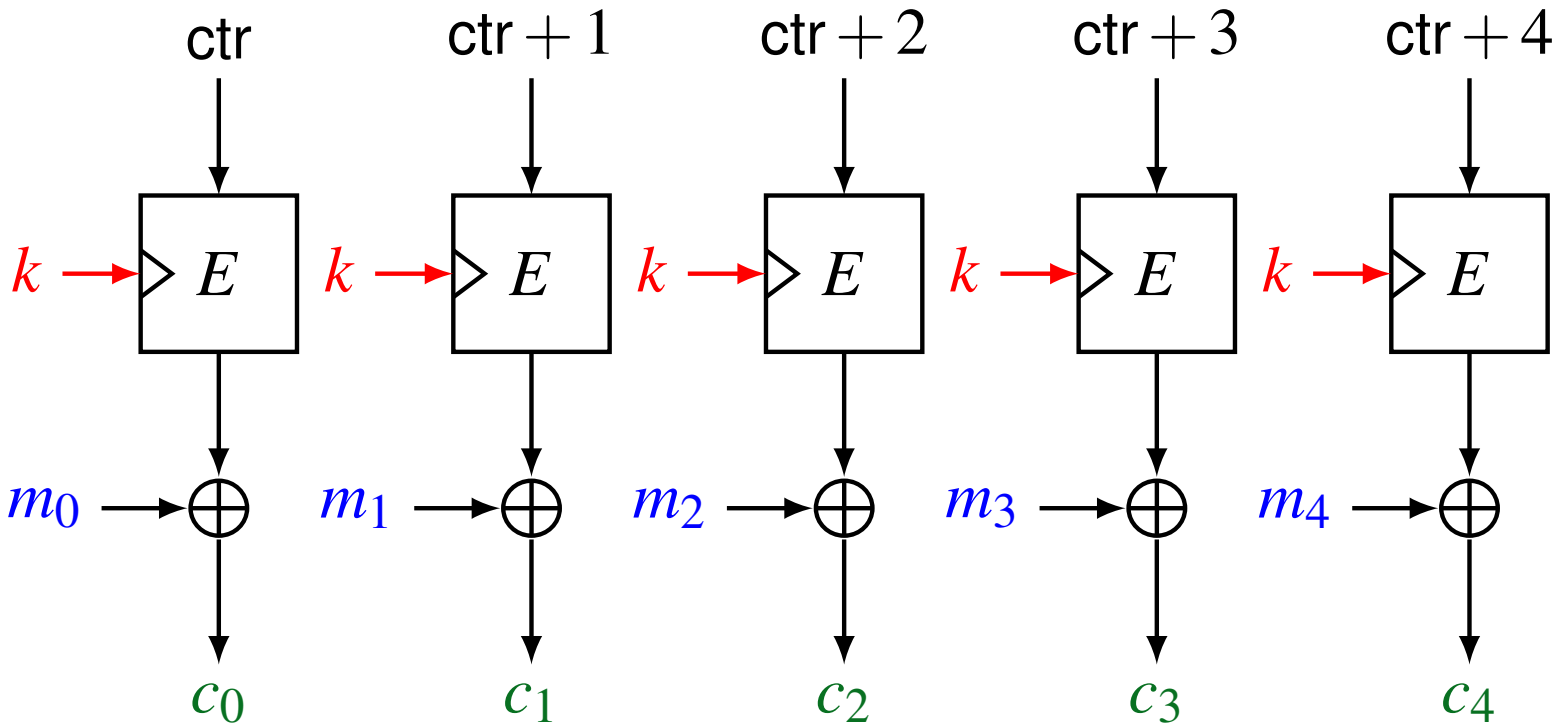
✍ Donner plusieurs problèmes liés à ce mode de chiffrement.

Le mode CBC (Cipher Block Chaining)



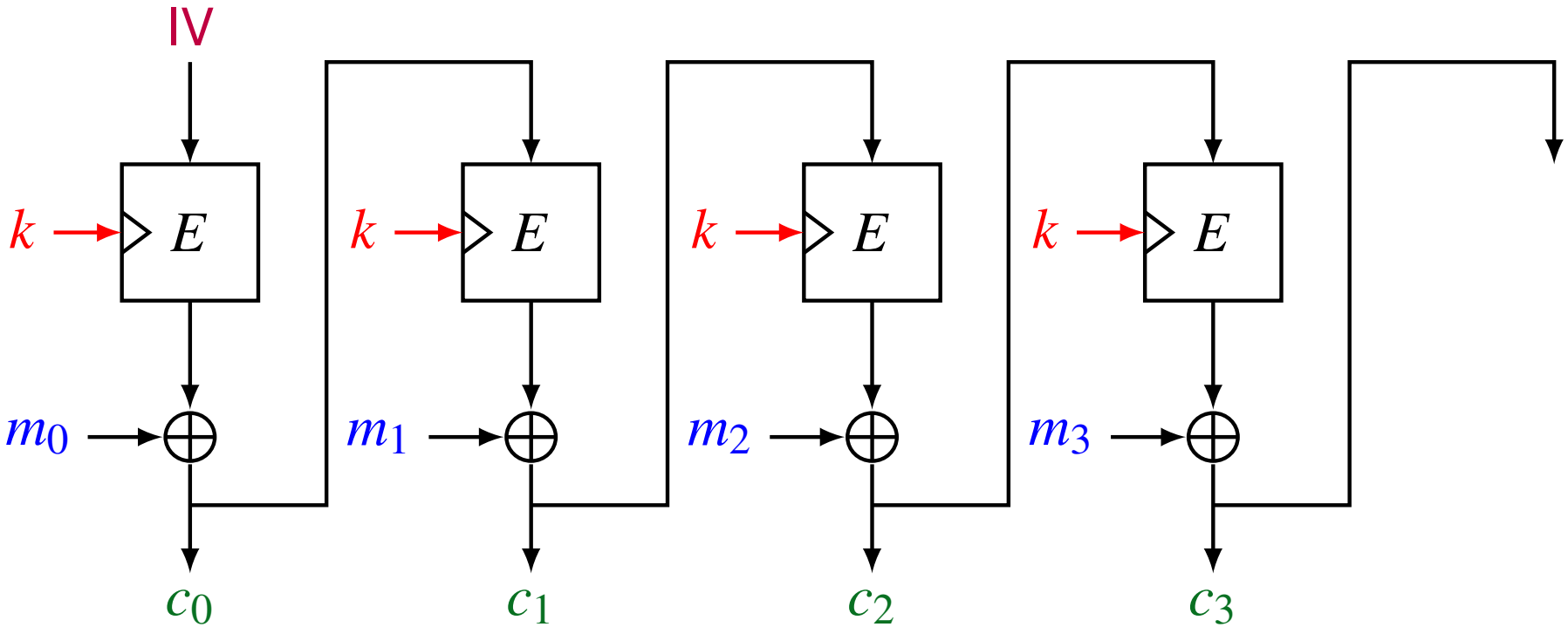
✍ Comment fonctionne le déchiffrement ? Dessiner le schéma de déchiffrement.

LE MODE CTR (COMPTEUR)



- ✍ Est-ce que la valeur initiale du compteur est fixée à l'avance ?
- ✍ Quelle sécurité avons-nous si le compteur est initialisé au vecteur d'initialisation ?
- ✍ Comment déchiffrer ?

LE MODE CFB (CIPHER FEEDBACK)



Les modes de chiffrement seuls

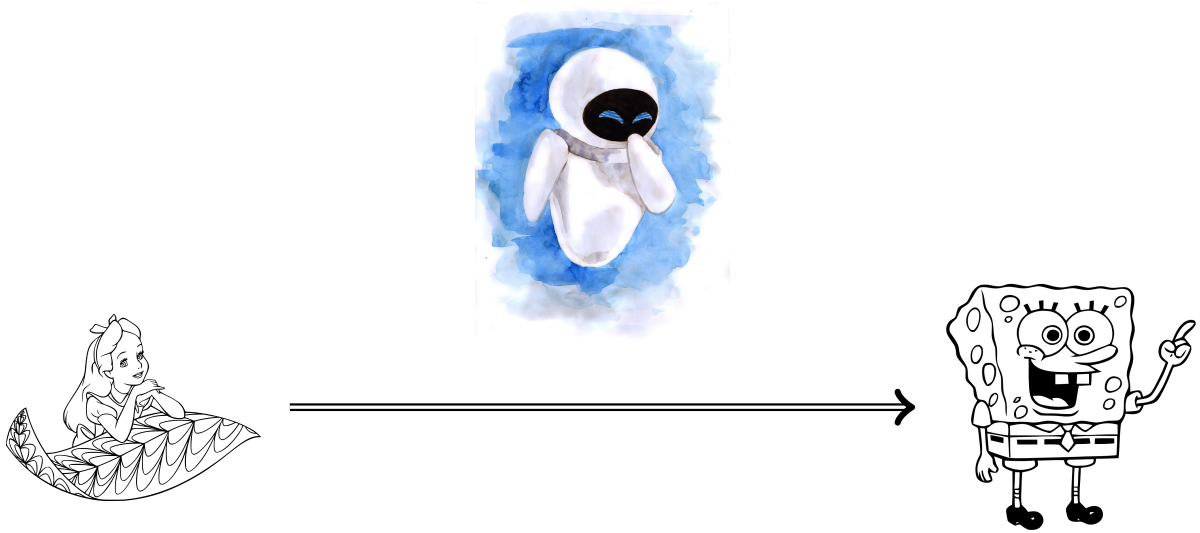
- Les autres standards sont OFB (Output FeedBack) et XTS (pour le stockage).
- le vecteur d'initialisation (IV) est public et doit parfois être « aléatoire ». (cf TD modes) Celui-ci sert en particulier à rendre le chiffrement non-déterministe.
- Les modes présentés sont prouvés sûrs si les bonnes pratiques sont respectées (borne des anniversaires, IV non-prédictible, etc).
- Ces modes protègent la confidentialité et non l'intégrité des messages.

Problème

Comment garantir l'intégrité et la confidentialité en même temps ?

L'INTÉGRITÉ

- Confidentialité : protéger les informations échangées, les données (sensibles)
- Authenticité : s'assurer de la légitimité de l'expéditeur du message
- Intégrité : s'assurer de la non-modification d'un message (intentionnellement ou non)



Solution : les MAC (Message Authentication Code)

En cryptographie symétrique, un MAC (aussi appelé Tag) est une valeur permettant d'assurer à la fois l'intégrité et l'authenticité.
(Dans notre contexte de cryptographie symétrique, on a les deux propriété en même temps. Ce n'est pas toujours le cas).
Idée : Construire une fonction de la forme

$$f : \mathcal{K} \times \mathcal{M} \to \{0,1\}^{\tau}$$

telle que cela soit « facile »à calculer si est un utilisateur légitime, i.e. on a la clef secrète.
... Et que cela soit « difficile sinon ».

Les MACS - Définition

Un MAC est un couple d'algorithmes :

- `Aut` (pour « Authentifier », souvent « signer ») : prend en entrée k, m) et sort une valeur de taille τ appelée le tag (T).
- `Ver` (pour « Vérifier ») : prend en entrée k, $T \in \{0,1\}^\tau$, x et renvoie `vrai` ou `faux`.

Propriété (d'un bon MAC)

Un MAC cryptographique doit vérifier les propriétés suivantes :

- *pour toute clef k,*

$$\Pr[\texttt{Ver}(k, \texttt{Aut}(k,x),x) = \mathit{Vrai}] = 1$$

- *Il n'existe pas d'adversaire, qui, ayant connaissance de plusieurs couples (m,T) puisse engendrer « facilement » un couple (m',T') qui soit vérifié, et ce avec probabilité négligeable.*

- Formaliser le jeu de sécurité et l'oracle permettant d'assurer l'intégrité et l'authenticité.

Les MACS - Complexité générique

Propriété (d'un bon MAC)

Un MAC cryptographique doit vérifier les propriétés suivantes :

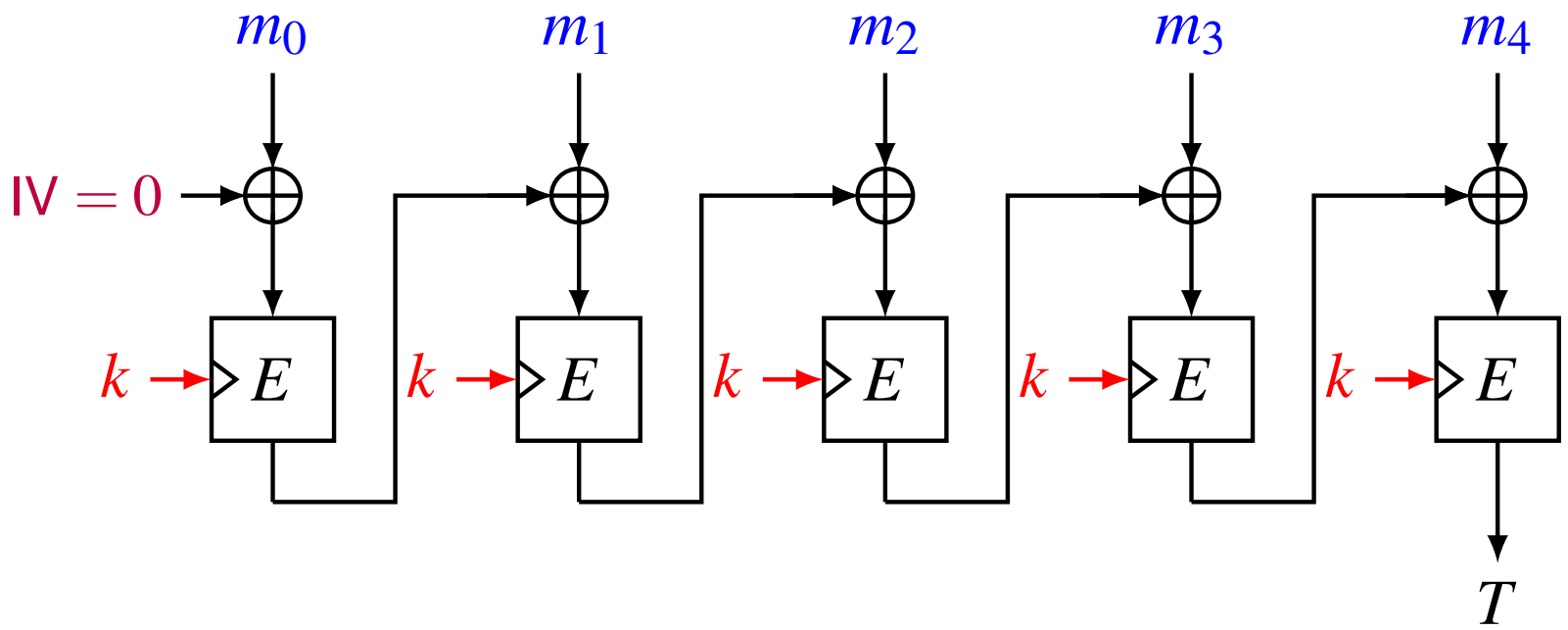
- *pour toute clef k,*

$$\Pr[\texttt{Ver}(k, \texttt{Aut}(k, x), x) = \texttt{Vrai}] = 1$$

- *Il n'existe pas d'adversaire, qui, ayant connaissance de plusieurs couples (m, T) puisse engendrer « facilement » un couple (m', T') qui soit vérifié, et ce avec probabilité négligeable.*

✍ Si le tag T est de taille τ, et que l'on en précise rien, quelle complexité générique peut-on atteindre pour « casser » l'intégrité ?

CBC-MAC



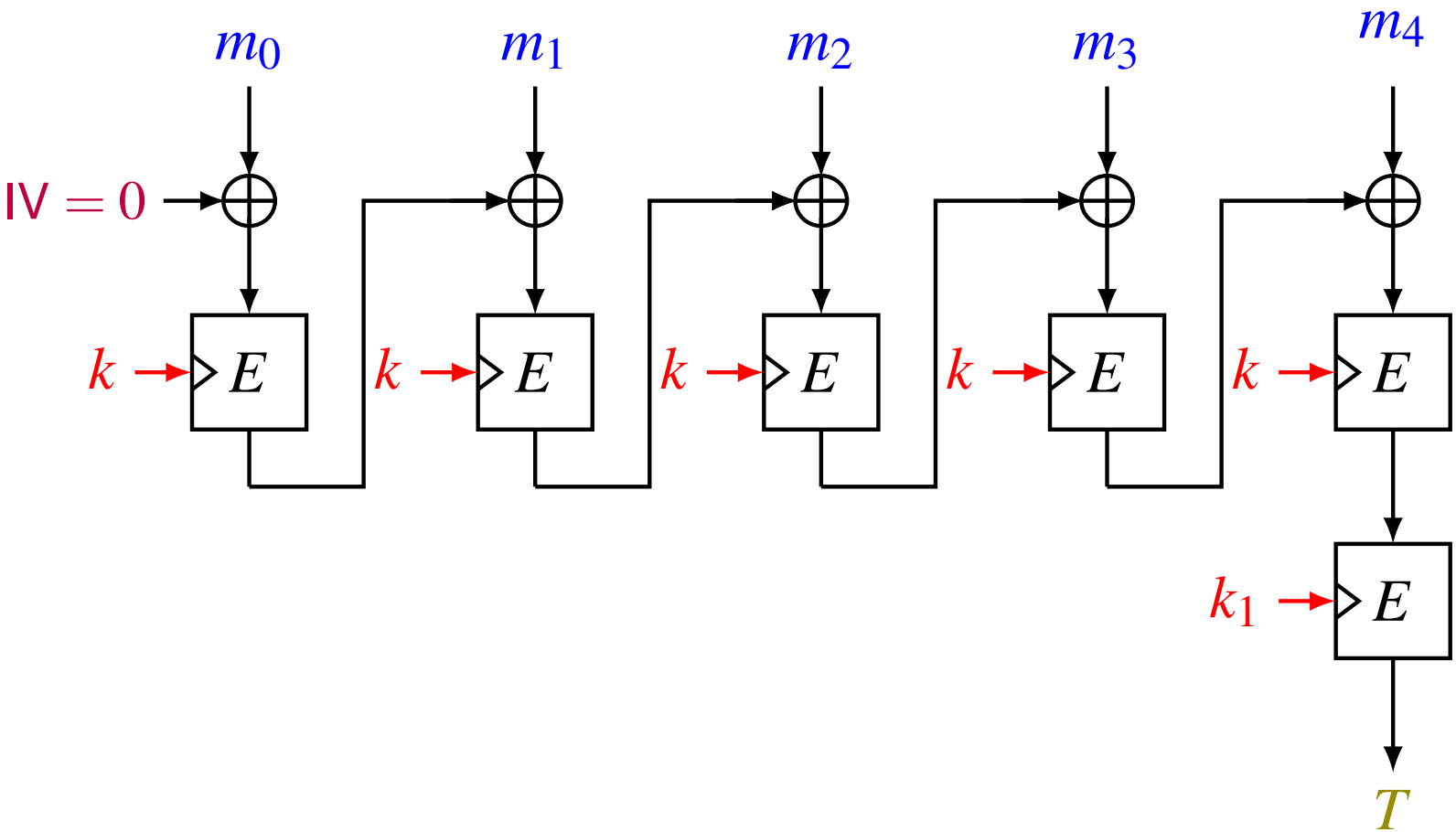
On suppose que l'on connaît un couple (m, T) valide ainsi que $E_k(m_0)$.

✍ Réfléchissons ensemble à comment produire un autre couple valide sans avoir la clef secrète.

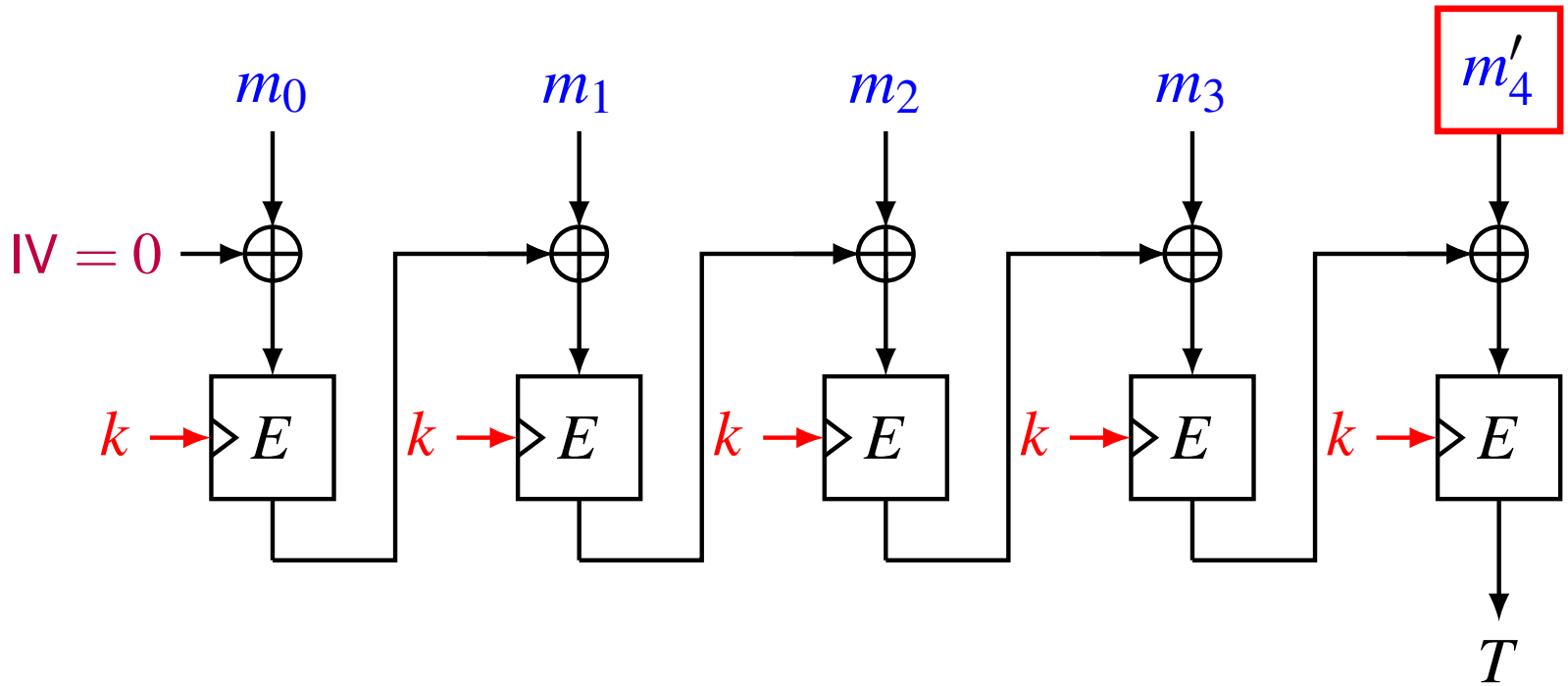
PROBLÈME

CBC-MAC n'est pas sûr avec des messages de longueurs différentes.

TMAC



C-MAC (OMAC - ONE-KEY MAC)



Calcul de m'_n :

- $m'_n = m_n \oplus k_1$ (ou k_2)
- Dérivées par $E_k(0)$

HMAC

PROBLÈME

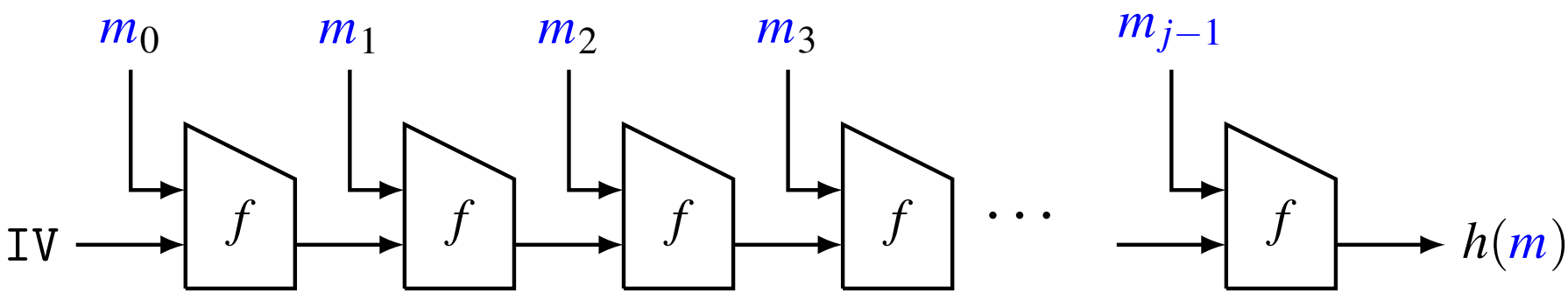
Construire un MAC avec une fonction de hachage.

✍ Parmi les deux solutions avancées, la (ou les) quelle(s) sont sûres ou non ? (On suppose que H est construite à partir de Merkle Damgård)

1. $H(k||m)$
2. $H(m||k)$

RAPPEL : LA CONSTRUCTION MERKLE DAMGARD

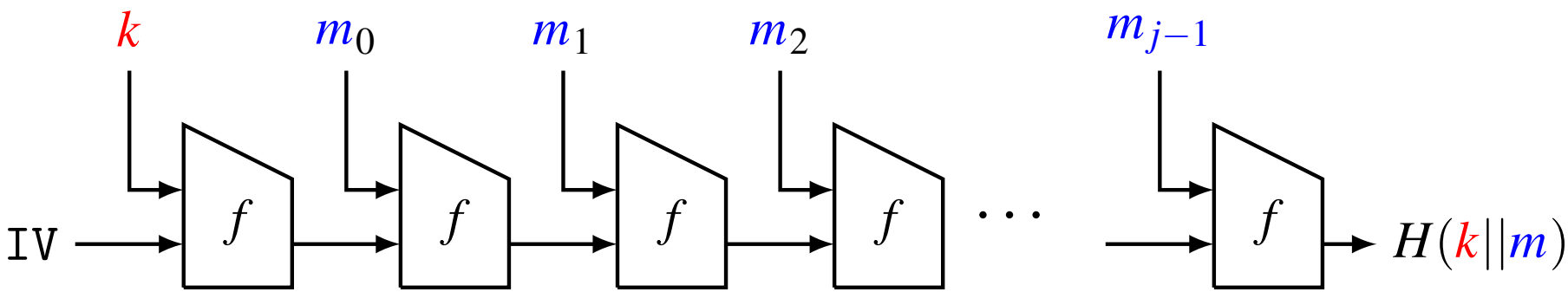
$$f : \{0,1\}^{n+\ell} \to \{0,1\}^n$$



On peut montrer que s'il est « difficile » de trouver des collisions sur f,
il l'est aussi pour H construite à partir de f.

Cas 1

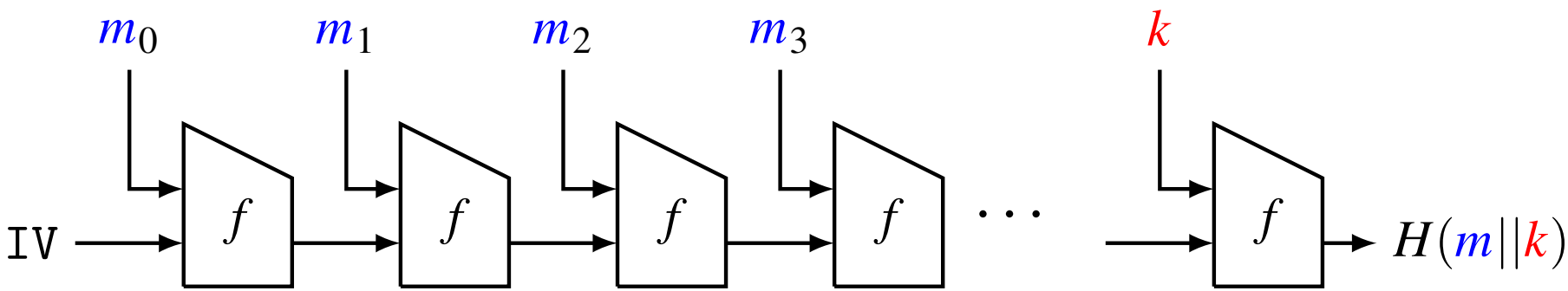
$$H(k||m)$$



✍ Montrer pourquoi ce n'est pas sûr.

Cas 2

$$H(m||k)$$



✍ Montrer pourquoi ce n'est pas sûr et donner la complexité.

HMAC - Solution (simplifiée)

Il faut protéger le début et l'entrée !

$$H\left(k_2 || H\left(k_1 || m\right)\right)$$

- On peut prouver la sécurité de cette construction, si k_1 et k_2 sont indépendantes et si H est une bonne fonction de hachage.
- Dans la pratique, k_1 et k_2 ne sont pas indépendantes, mais on n'a a priori pas d'attaque exploitant cela à ce jour.

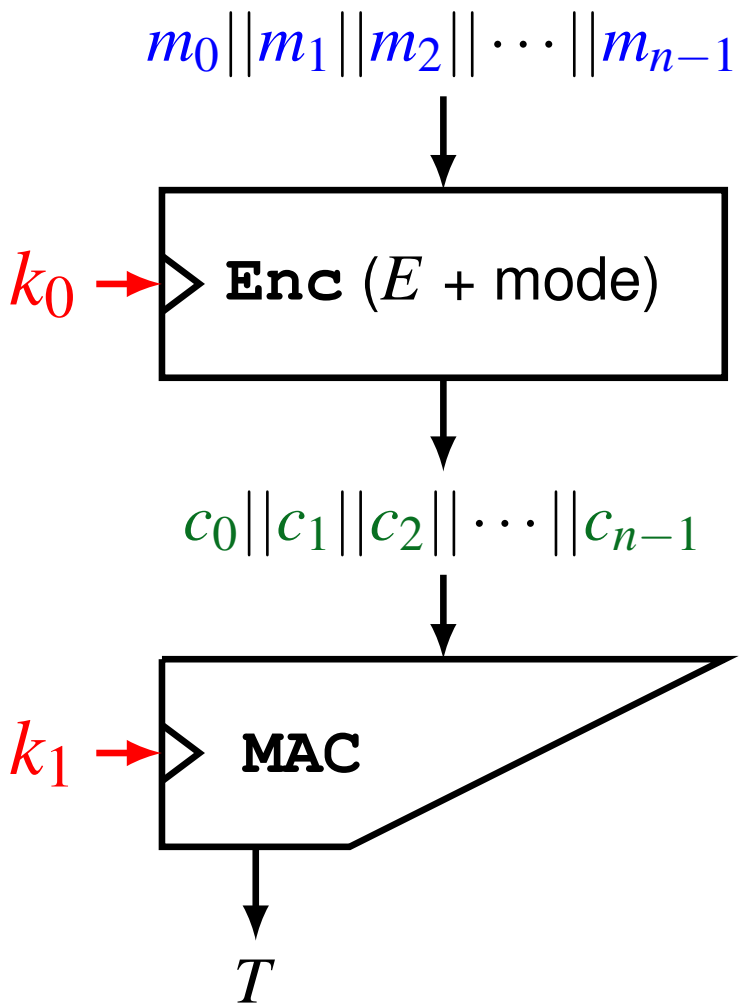
Chiffrement, Intégrité et Authentification

Qu'est-ce qu'on a ?

- Des chiffrements par bloc
- Des fonction de hachage cryptographiques
- Des modes opératoires de chiffrement (confidentialité)
- Des MACs (intégrité et authenticité)

Comment avoir les trois propriétés en même temps ?

SOLUTION 1 : ENCRYPT-THEN-MAC



- ✍ Que manque t'il dans ce schéma ?
- **Dans tous vos schémas faites tout apparaître**
- Alice envoie le couple (c, T).
- ✍ Donner la procédure de vérification de Bob.
- Si le message et/ou le tag est modifié (intentionnellement ou non), vérifier que la procédure de vérification échoue.

Solutions 2 et 3

- Encrypt-and-Mac
- Mac-then-Encrypt
- Détail en TD

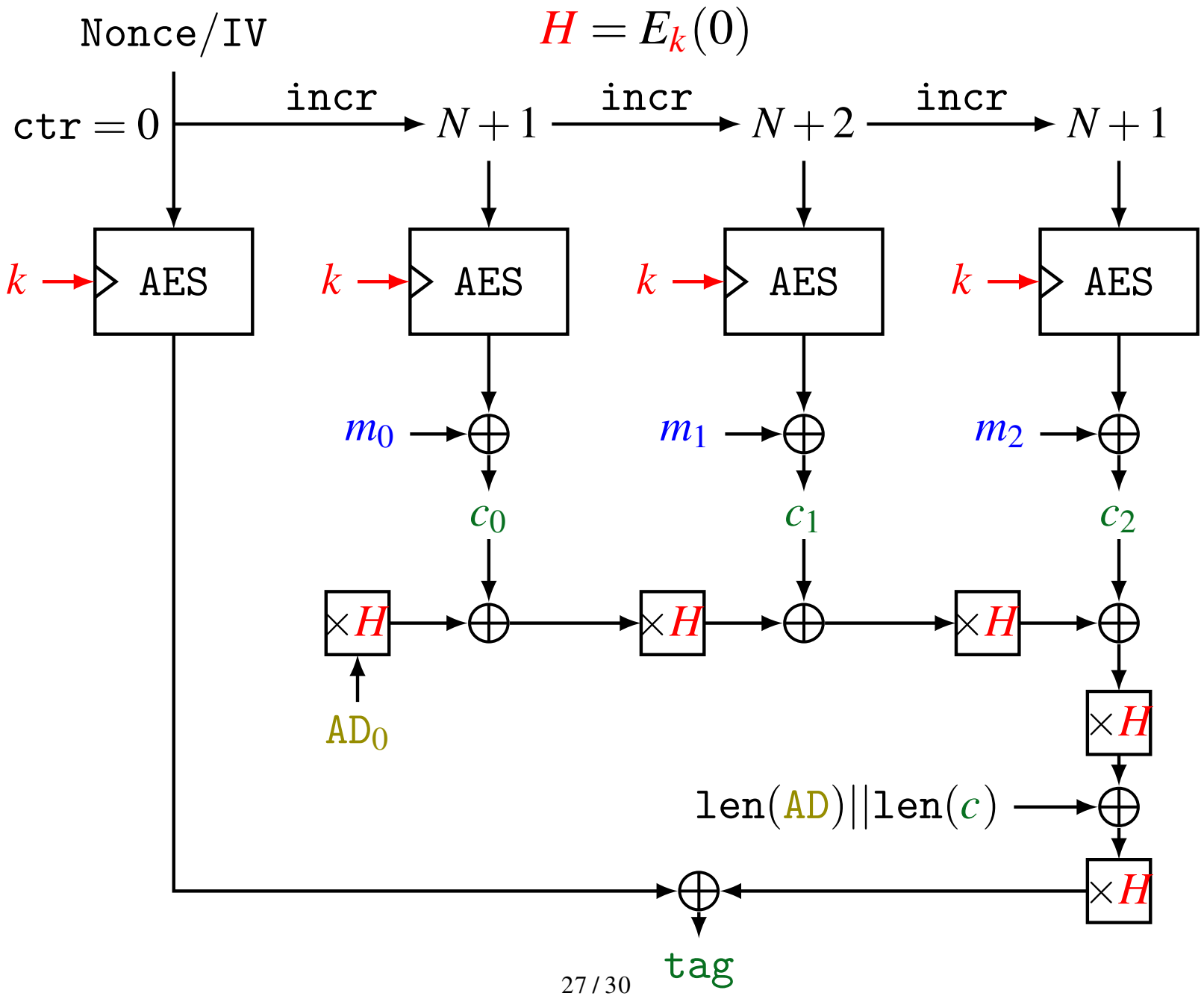
SOLUTION 4 : TOUT EN MÊME TEMPS - AEAD

1. On sait assurer confidentialité et authenticité (intégrité) séparément ;
2. Problématiques : implémentation dans les protocoles, i.e. padding, nonce, combinaison correcte des chiffrements, ... (qq exemples vus en TD)
3. Solution : Produire directement des chiffrements qui garantissent tout en même temps.

Authenticated Encryption with Associated Data

Le Chiffrement Authentifié avec Données Associées - AEAD

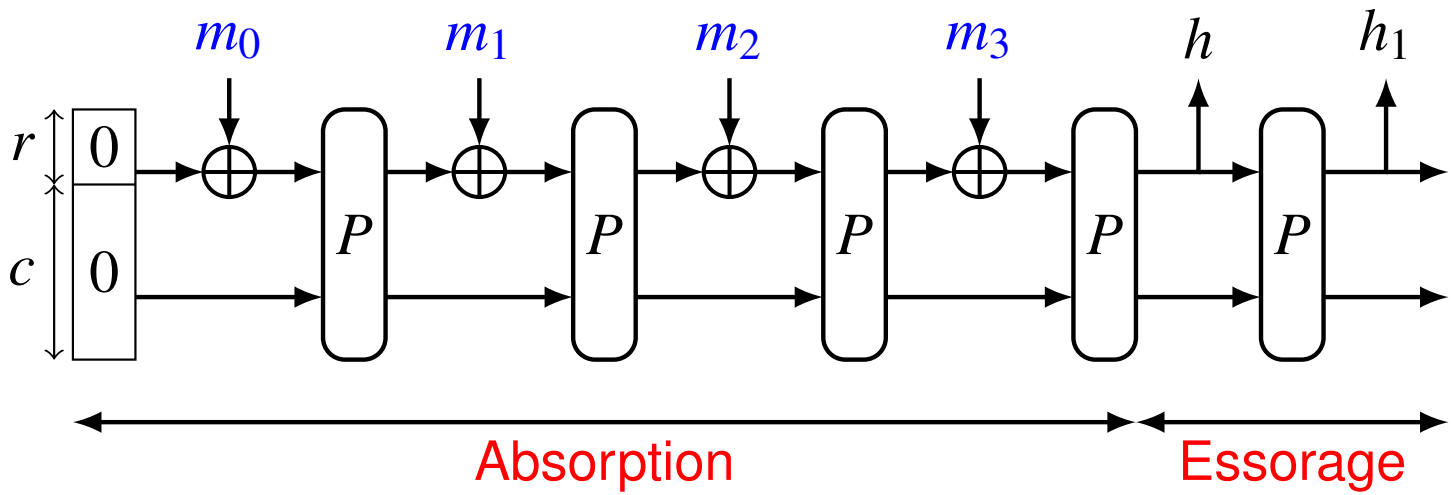
AES-GCM - Galois Counter Mode



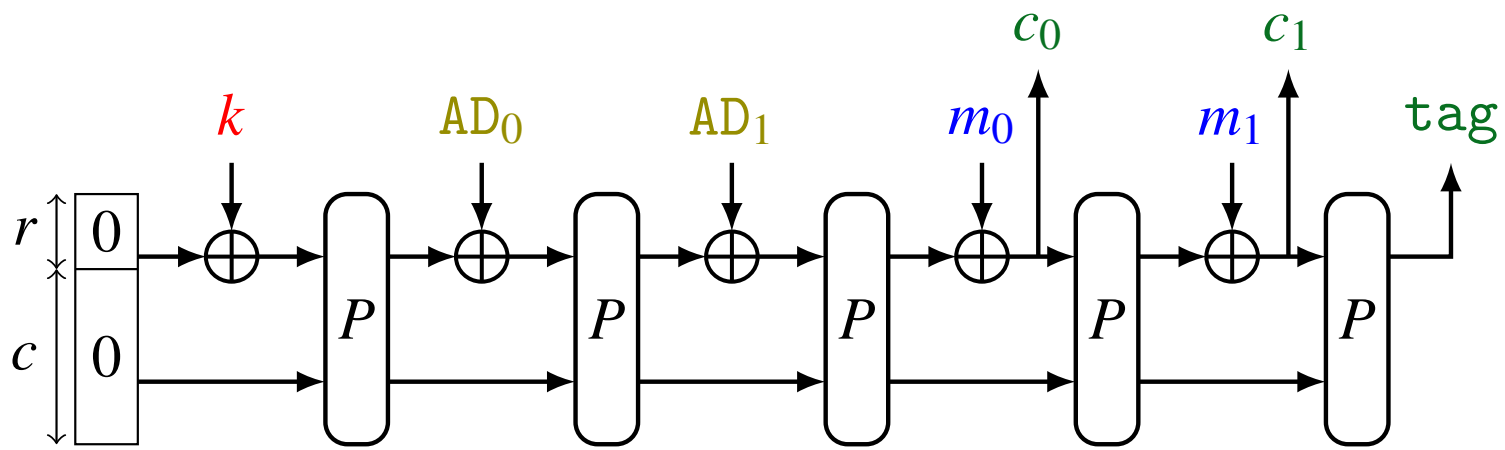
Solution 5 : Et avec une permutation - le mode Duplex

$$P : \{0,1\}^{r+c} \to \{0,1\}^{r+c}$$

Rappel : la construction en éponge



Solution 5 : Et avec une permutation - le mode Duplex



Conclusion

Important

- *Un chiffrement seul (sans authentification) n'est pas recommandé (sauf cas particulier)*
- *On a plusieurs solutions pour réaliser la confidentialité, l'authenticité et l'intégrité*
- *MACs + Chiffrements combinés*
- *AEAD - avec modes de chiffrements par blocs ou des permutations*