Cryptanalyse des Chiffrements par Bloc

Un critère nécessaire (mais toujours pas suffisant)

Yann Rotella

UVSQ - Université Paris-Saclay

26 février 2026

Plan du Cours

Cryptanalyse - Les bases

- Définition
- Le « paradoxe » des anniversaires
- Attaque de type Meet-In-the-Middle

Les slide attacks

Cryptanalyse différentielle - principe

Attaques intégrales

Cryptanalyse

Définition

Domaine de la cryptologie qui étudie la sécurité des systèmes de chiffrement. Il s'agit d'analyser toutes les stratégies possibles qu'un attaquant potentiel peut utiliser pour « casser »un système.

- On ne peut pas prouver inconditionnellement la sécurité d'un chiffrement.
- On considère un système de chiffrement sûr si aucune stratégie ne permet de casser ledit système.
- On se place généralement dans le modèle le plus fort : attaques à chiffrés choisis.

✍ Rappeler ce modèle d'attaque.

Le « paradoxe » des anniversaires

On considère E un ensemble fini de taille N.

- On tire aléatoirement selon la distribution uniforme n éléments de E un à un (potentiellement le même).

Problème

Quelle est la probabilité $p(n)$ que, parmi les n éléments tirés, deux soient identiques ?

CALCUL ET PREUVE

E, $\#E = N$, choix de n éléments. $p(n)$ est la probabilité qu'au moins deux éléments tirés soient identiques.
$\bar{p}(n) = 1 - p(n)$ est la probabilité que tous les éléments tirés soient différents.

- ✍ Que vaut $\bar{p}(1)$, $\bar{p}(2)$, $\bar{p}(3)$ et $\bar{p}(N+1)$?
- ✍ Généraliser et trouver une formule pour $\bar{p}(n)$.

Astuce d'Analyse : au voisinage de 0, on a

$$e^x = 1 + x + o(x)$$

Ainsi,

$$\bar{p}(n) \equiv \prod_{k=0}^{n-1} e^{-\frac{k}{N}}$$

- ✍ Donner alors une estimation de $p(n)$.
- ✍ Quand est-ce que cette estimation n'est plus correcte ?

Le « paradoxe » des anniversaires

Cas exact classique : Pour $n = 23$ et $N = 365$, la probabilité est supérieure à 50%. **Cas cryptographique :**

- Pour N grand, la probabilité de trouver une **collision** en tirant aléatoirement $\sqrt{N}$ éléments dans E est de 50%.
- En tirant $c\sqrt{N}$ éléments pour c une petite constante, la probabilité approche très vite de 1.
- Sans utiliser le terme, on a déjà vu cela en cours. Vous en souvenez-vous ?

Ce n'est pas un paradoxe

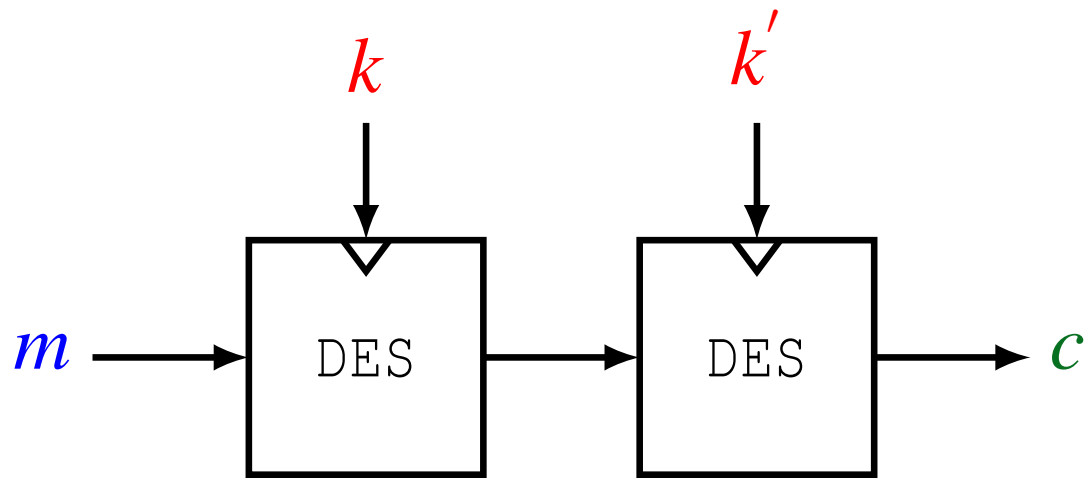
Un autre point de vue :

- Avec n valeurs tirées aléatoirement $\{v_1, v_2, \ldots, v_n\}$, combien de valeurs avons-nous de la forme $v_i + v_j$ avec $i \neq j$?
- Quand trouvons-nous une collision ?

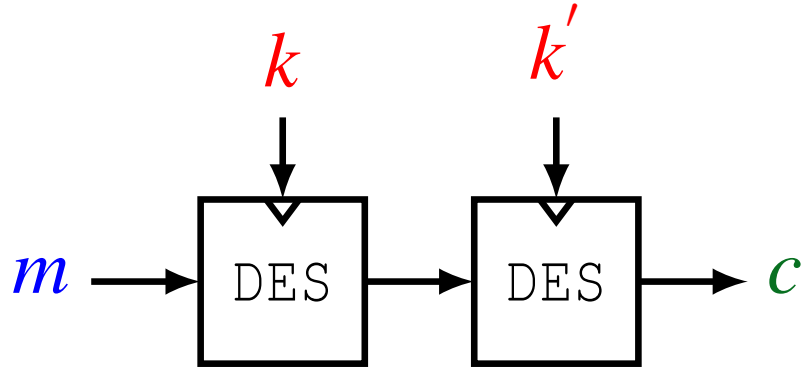
Attaque de type Meet-in-the-Middle

Le DES est un chiffrement par bloc opérant sur 64 bits et avec 56 bits de clefs.

- Rappeler pourquoi il n'est plus à utiliser.
- On considère alors la technique du double chiffrement :



Attaque de type Meet-in-the-Middle



Stratégie d'attaque :

1. Connaissant m, c, calculer et trier selon $\mathtt{DES}_k(m)$

$$\mathtt{Liste} = \{(k, \mathtt{DES}_k(m), k \in \{0,1\}^{56}\}$$

2. Pour tout $k' \in \{0,1\}^{56}$, chercher

$$\mathtt{DES}_{k'}^{-1}(c)$$

dans la liste `Liste`

- Coût de l'attaque en nombre de `DES` ?
- Coût mémoire ?
- Combien de couples de clefs possibles restent-ils en moyenne ?
- Comment régler ce problème ?

Les slide attacks ou l'importance du cadencement de clefs

On suppose que l'on a un chiffrement par bloc de type SPN sans cadencement de clef : à chaque tour c'est la même valeur k inconnue qui est ajoutée.

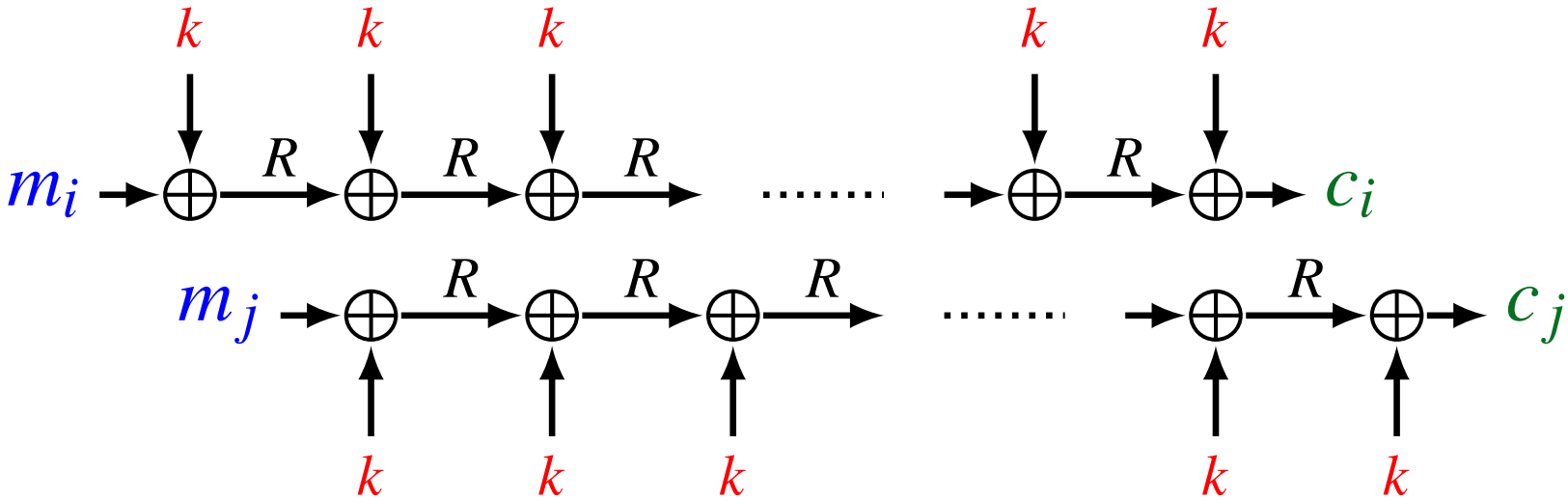
$$E_k(m) = c = R_k^r$$

où R est la fonction de tour et r le nombre de tours.
On suppose que m_1 et m_2 sont tels que

$$R_k(m_1) = m_2$$

- ✍ Quelle relation avons-nous sur c_1 et c_2 ?
- ✍ Est-ce une équivalence ?

Les slide attacks



On cherche donc $((m_i, c_i), (m_j, c_j))$ tels que

$$\begin{cases} m_j = R(k \oplus m_i) \\ c_j = R(c_i) \oplus k \end{cases}$$

Problème

Comment détecter cela sans avoir la clef ?

✍ Modifier le système pour trouver un critère indépendant de la clef secrète k.

Les slide attacks

1. Récupérer $2^{\frac{n}{2}}$ couples clairs chiffrés

$$\{(m_i, c_i), 0 \leq i \leq 2^{\frac{n}{2}}\}$$

2. Calculer et trier

$$\texttt{Liste} = \{m_i \oplus R(c_i), 0 \leq i \leq 2^{\frac{n}{2}}\}$$

3. Pour tout $0 \leq j \leq 2^{\frac{n}{2}}$, chercher

$$c_j \oplus R^{-1}(m_j)$$

   dans la liste et renvoyer le couple (I, J).

4. Renvoyer $R(c_I) \oplus c_J$.

Cryptanalyse Différentielle

On considère un chiffrement par bloc E de type SPN opérant sur n bits.

- Introduite en 1980 par Eli Biham et Adi Shamir
- Attaque à clairs choisis

Principe général : Trouver $(a,b) \in \{0,1\}^n \times \{0,1\}^n$ tels que

$$\Pr[E_k(m \oplus a) \oplus E_k(m) = b] \gg \frac{1}{2^n}$$

où la probabilité est prise sur l'ensemble des clefs et l'ensemble des clairs possibles.

- ✍ Pourquoi $\frac{1}{2^n}$?
- Comment trouver ces valeurs a et b ?

Cryptanalyse Différentielle sur SPN

Les chiffrements considérés sont les SPNs. Nous allons regarder pas à pas les probabilités de transition différentielles.
Pour une fonction $F : \{0,1\}^n \to \{0,1\}^n$, on note

$$p_F(a \to b) = \Pr[F(m \oplus a) \oplus F(m) = b]$$

- ✍ Passage par l'addition de clef ($\texttt{Add}_k$) ?
- ✍ Passage par la couche linéaire ($\mathcal{L}$) ?
- ✍ Passage par la couche de boîte-S ?

CRYPTANALYSE DIFFÉRENTIELLE - HYPOTHÈSE

Soient F et G deux fonctions de $\{0,1\}^n$ dans lui-même.

HYPOTHÈSE (INDÉPENDANCE POUR LA COMPOSITION)

On suppose que pour tout $(a,b,\delta) \in \{0,1\}^{3n}$,

$$\Pr[G(F(x \oplus a) \oplus G(F(x)) = b \text{ et } F(x \oplus a) \oplus F(x) = \delta]$$

$$= p_F(a \to \delta) \times p_G(\delta \to b)$$

CHEMIN DIFFÉRENTIEL ET CLUSTER

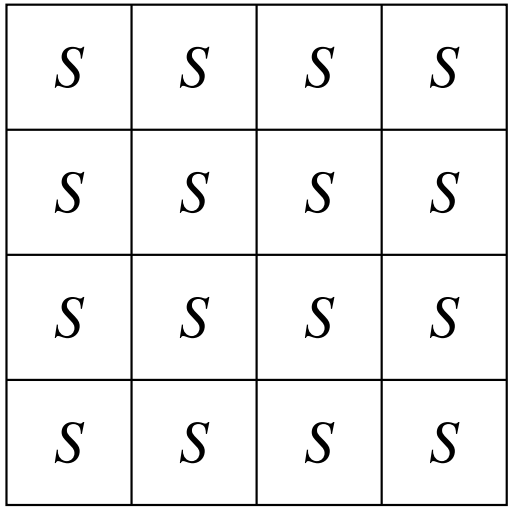
Sous l'hypothèse précédente, on peut écrire

$$p_{E_k}(a \to b) = \sum_{(\delta_i)_{1 \leq i \leq r-1}} \prod_{i=1}^{r} p_{R_i}(\delta_{i-1}, \delta_i)$$

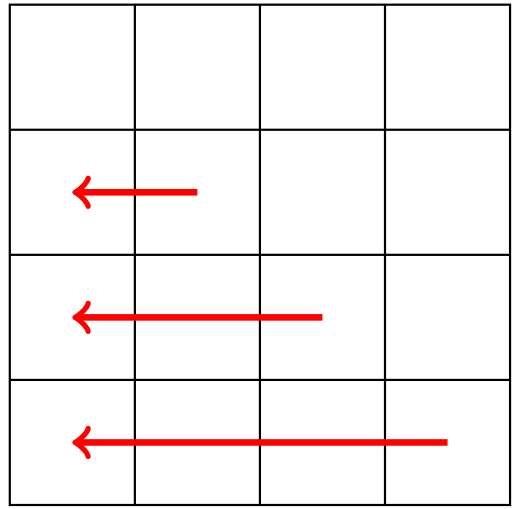
avec $\delta_0 = a$ et $\delta_r = b$ et r le nombre de tours.

- Une seule famille de δ_i pour laquelle le produit des probabilités est $> \frac{1}{2^n}$ casse le chiffrement.
- Cet argument n'est pas suffisant.
- Problème ouvert en général.
- On sait aujourd'hui s'assurer de l'absence de chemins.

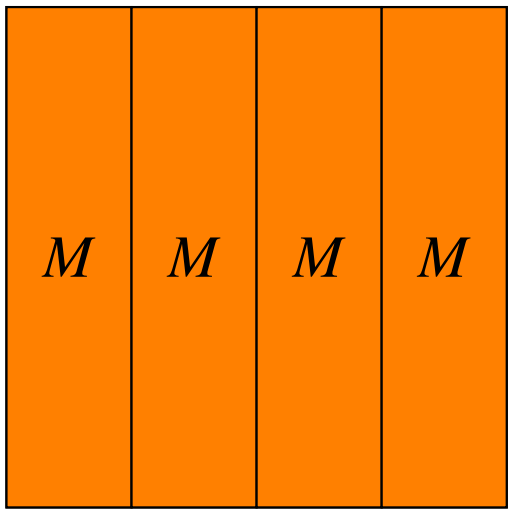
LE CAS DE L'AES - CRYPTANALYSE DIFFÉRENTIELLE



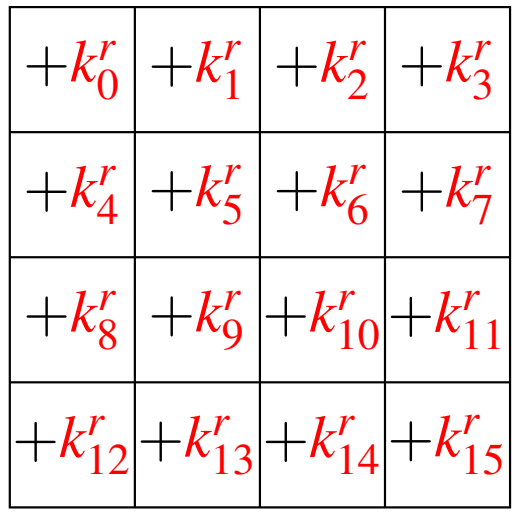
SubBytes (1)



ShiftRows (2)



MixColumns (3)



AddRoundKey (4)

Le cas de l'AES (différentielle)

- On regarde les 16 octets (et non bit à bit).
- Pour $a \in \{0,\ldots,255\}^{16}$, on note

$$w_H(a) = \#\{a_i \neq 0, 1 \leq i \leq 16\}$$

- Pour une boîte-S seule, on peut tout exhauster et, dans le cas de l'AES,

$$\max_{a,b} \#\{x \in \{0,\ldots,255\}, S(x \oplus a) \oplus S(x) = b\} = 4$$

- On peut borner $p_S(a \to b)$ par

$$\left(\frac{4}{256}\right)^{w_H(a)}$$

- On peut aussi montrer que

$$\min_{a,b \neq 0} \{w_H(a) + w_H(b), b = \mathcal{L}(a)\} = 5$$

LE CAS DE L'AES (DIFFÉRENTIELLE)

THÉORÈME

Tout chemin différentiel sur deux tours de l'AES active 5 boîtes-S

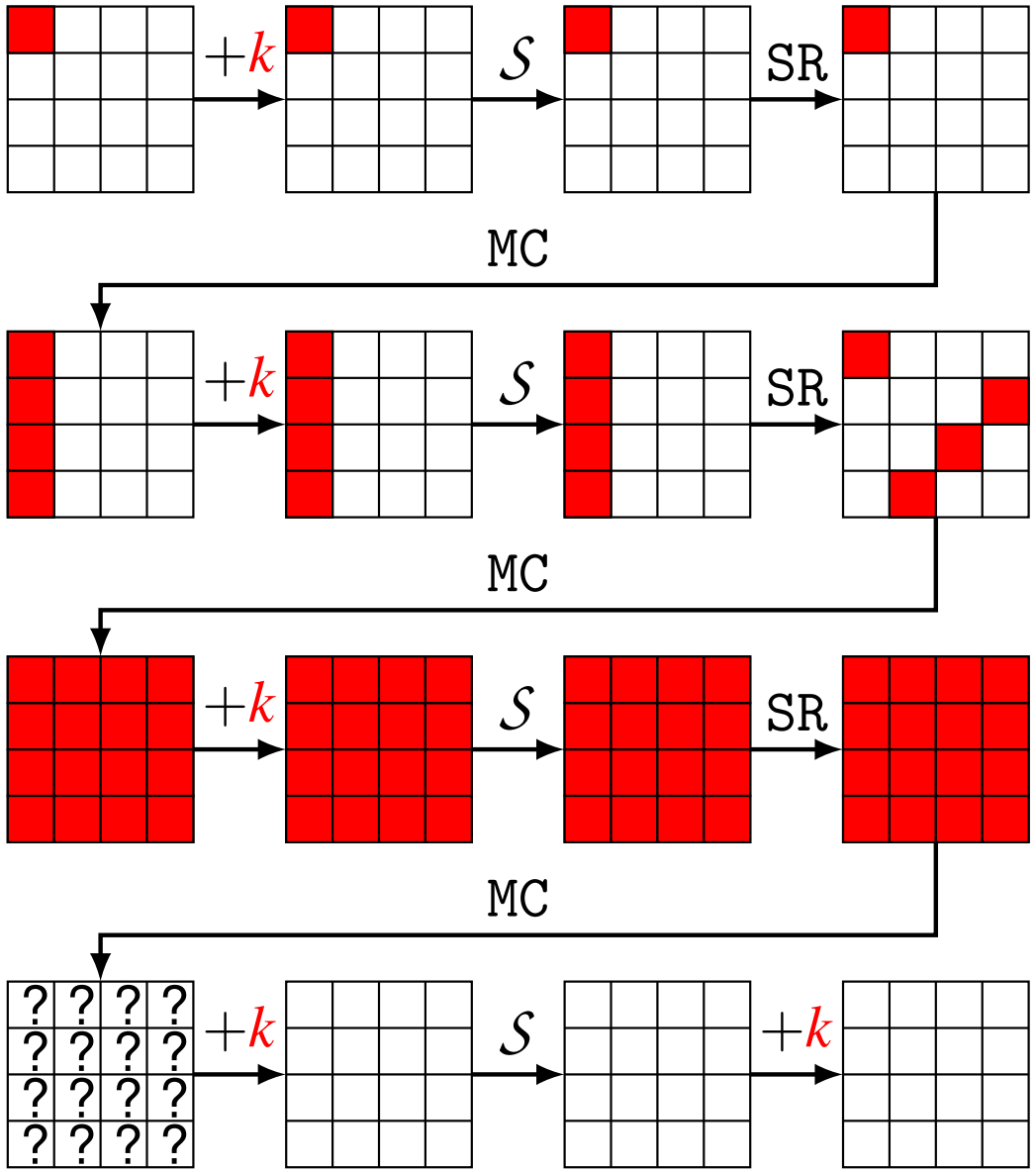
Et sur 4 tours ?

THÉORÈME

Tout chemin différentiel sur quatre tours de l'AES active au moins 5×5 boîtes-S

$$\left(\frac{4}{256}\right)^{25} = 2^{-150}$$

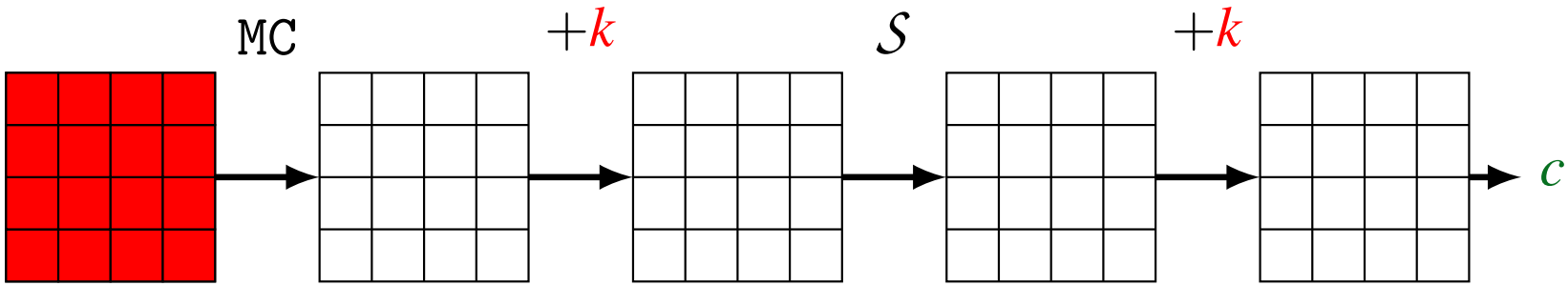
ATTAQUES INTÉGRALES - LE CAS AES (4 TOURS)



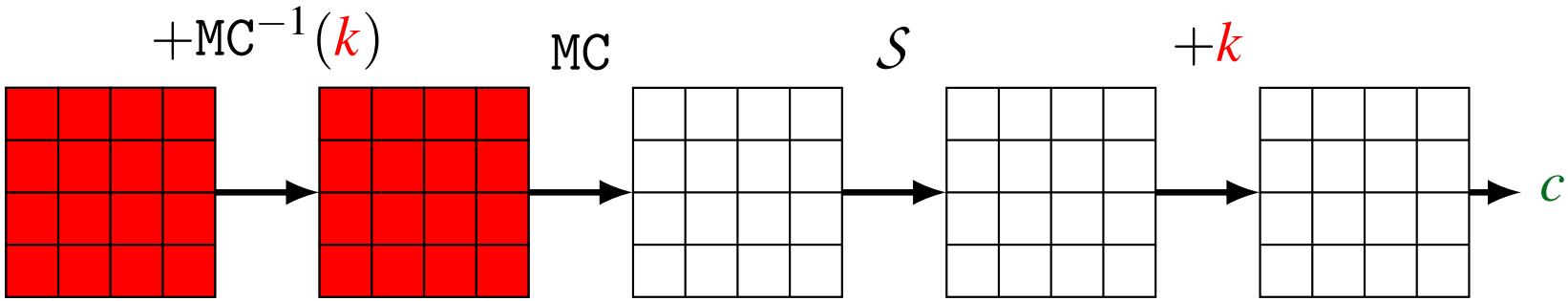
Octet saturé

Octet constant

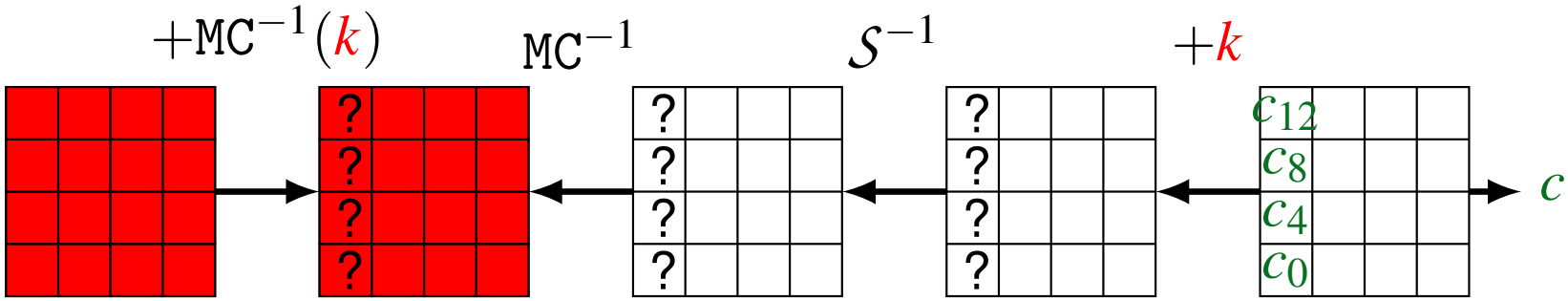
CONCENTRONS-NOUS SUR LE DERNIER TOUR



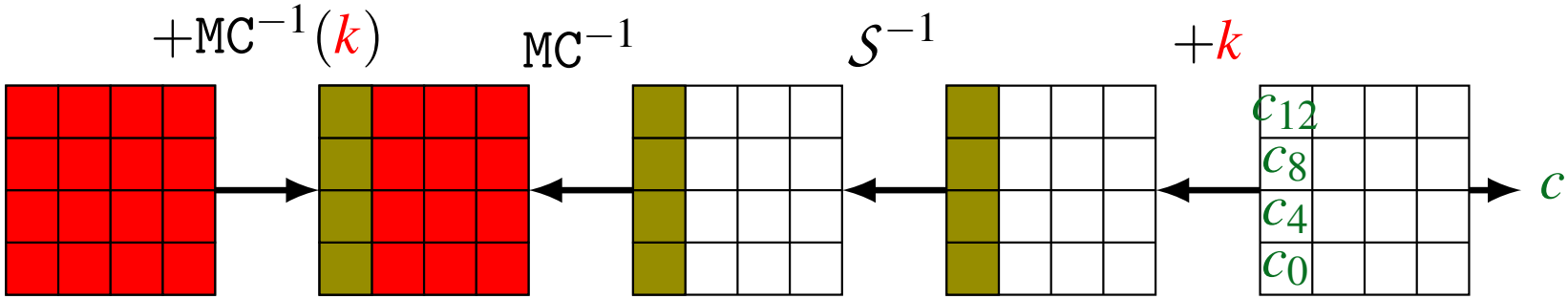
CONCENTRONS-NOUS SUR LE DERNIER TOUR



CONCENTRONS-NOUS SUR LE DERNIER TOUR



CONCENTRONS-NOUS SUR LE DERNIER TOUR



- Coût : 2^{32} hypothèses sur la clef en calculant à chaque fois sur 2^8 entrées- sorties choisies.

Résumé et conclusion

Résumé

- *« paradoxe » des anniversaires : Collision en $\sqrt{N}$*
- *MitM : chiffrer deux fois n'augmente pas le niveau de sécurité générique*
- *Slide Attacks : attaque en $2^{n/2}$ où n est la taille du bloc*
- *Cryptanalyse : plusieurs techniques, hypothèses*
- *Chercher un distingueur pour toutes les clefs*
- *Le combiner avec une diffusion non-complète pour retrouver la clef.*

Conclusion

La cryptanalyse est un domaine de recherche qui s'intéresse à analyser la sécurité des chiffrements. Plusieurs techniques existent et peuvent être complexes. C'est à ce jour le seul argument de sécurité pour les primitives cryptographiques.