Stratégies de Conception

Pseudo Random Permutations : Chiffrements par Bloc

Yann Rotella

UVSQ - Université Paris-Saclay

19 février 2026

Plan du Cours

Pseudo Random Permutations

La confusion et la diffusion

Les Réseaux de Substitution Permutation (SPN)

Pseudo Random Permutations

La confusion et la diffusion

Les Réseaux de Substitution Permutation (SPN)

Pseudo Random Permutations

- On peut construire des chiffrements sécurisés sur des tailles de message arbitraires ($\mathcal{M} = \{0,1\}^*$) si l'on a des PRP, PRF et PRG.
- On peut construire des PRF ou des PRG à partir de PRP.
- On ne sait pas construire (aujourd'hui) des PRF sans utiliser de PRP.
- On ne connaît pas de primitive plus « petite » que les PRP.

Nous allons donc construire des Pseudo Random Permutations, aussi appelés Block Ciphers : les chiffrements par bloc.

Qu'est ce qu'on veut ?

- Une famille de **permutations** de $\{0,1\}^n$ paramétrée par une clef $k \in \{0,1\}^\kappa$.
- ✍ Quelles valeurs aujourd'hui pour κ ?
- ✍ Quelles valeurs aujourd'hui pour n ?
- ✍ Donner la définition ensembliste de notre famille de fonctions ainsi que la définition de sécurité que l'on souhaite atteindre.

Pseudo Random Permutations

La confusion et la diffusion

Les Réseaux de Substitution Permutation (SPN)

Théorie de Shannon

Propriété (Confusion)

La relation entre les bits de la clef k, les bits du message clair m et les bits du message chiffré c doit être la plus complexe possible.

Propriété (Diffusion)

Chaque bit du texte clair et chaque bit de la clef doivent influencer chaque bit du texte chiffré.

IMPORTANCE DE LA DIFFUSION

Soit n, κ deux entiers et soit

$$\mathcal{P} = \{P(k,\cdot), k \in \{0,1\}^{\kappa}\}$$

une famille de bijections sur $\{0,1\}^n$ paramétrées par une clef k. On suppose que la diffusion n'est pas atteinte.

- ✍ Donner un exemple de propriété mathématique non-triviale sur $\mathcal{P}$ qui contredirait la propriété de diffusion.
- ✍ En déduire un distingueur sur la famille $\mathcal{P}$ et montrer pourquoi, dans ce cas, ce n'est pas une PRP.

IMPORTANCE DE LA CONFUSION

Soit n, κ deux entiers et soit

$$\mathcal{P} = \{P(k,\cdot), k \in \{0,1\}^\kappa\}$$

une famille de bijections paramétrées par une clef k.
La confusion est un peu plus difficile à définir, la notion de *complexité* étant elle-même peu comprise.
On peut cependant donner de mauvais exemples plus facilement, par exemple si pour toute clef $k \in \{0,1\}^\kappa, P(k,\cdot)$ est linéaire.

- ✍ Rappeler la définition d'une fonction linéaire (identifier avant l'espace vectoriel en entrée et en sortie).
- ✍ Comment peuvent être représentées les applications linéaires ?
- ✍ Comme $P(k,\cdot)$ est une bijection, que pouvons-nous dire sur sa matrice ?
- ✍ Montrer pourquoi une telle famille de bijections n'est pas sécurisée (on pourra casser IND-CPA, le jeu Réel ou aléatoire avec le mode CTR directement). Détailler la réponse et expliquer informellement pourquoi une telle construction pourrait atteindre une grande diffusion.

Idée de Shannon

Combiner la diffusion et la confusion
pour obtenir un chiffrement robuste.

ASSURER LA CONFUSION

- Relation non-linéaire
- Boîtes-S

$$S : \{0,1\}^{\ell} \to \{0,1\}^{\ell}$$

Représentée souvent par une table de vérité

Exemple :

$$S : \{0,1\}^{4} \to \{0,1\}^{4}$$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$S(x)$	8	6	7	9	3	12	10	15	13	1	14	4	0	11	5	2

✍ En pratique, quelle taille est acceptable pour une boîte-S si elle est représentée avec une table de vérité.

✍ Est-ce une taille raisonnable pour un chiffrement par bloc ?

Pseudo Random Permutations

La confusion et la diffusion

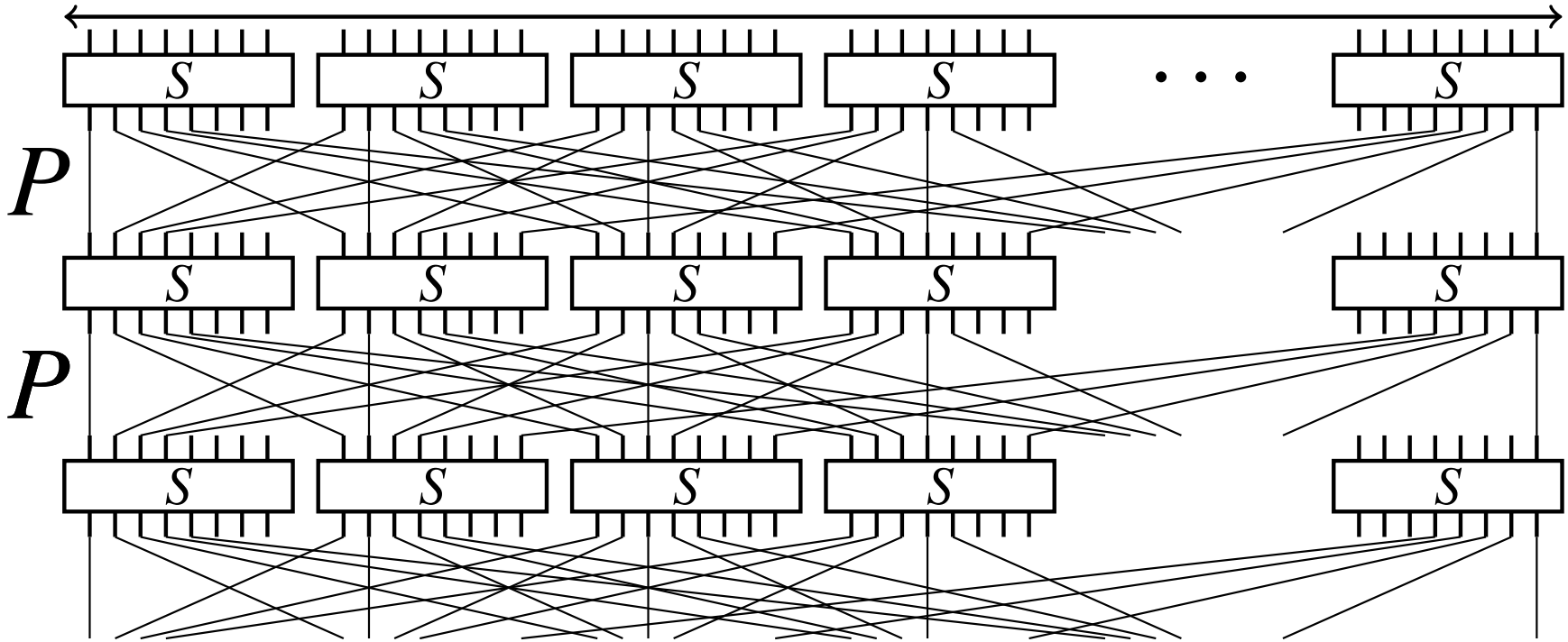
Les Réseaux de Substitution Permutation (SPN)

SPN (Substitution Permutation Network)

$$m \in \{0,1\}^n$$

$$\downarrow$$

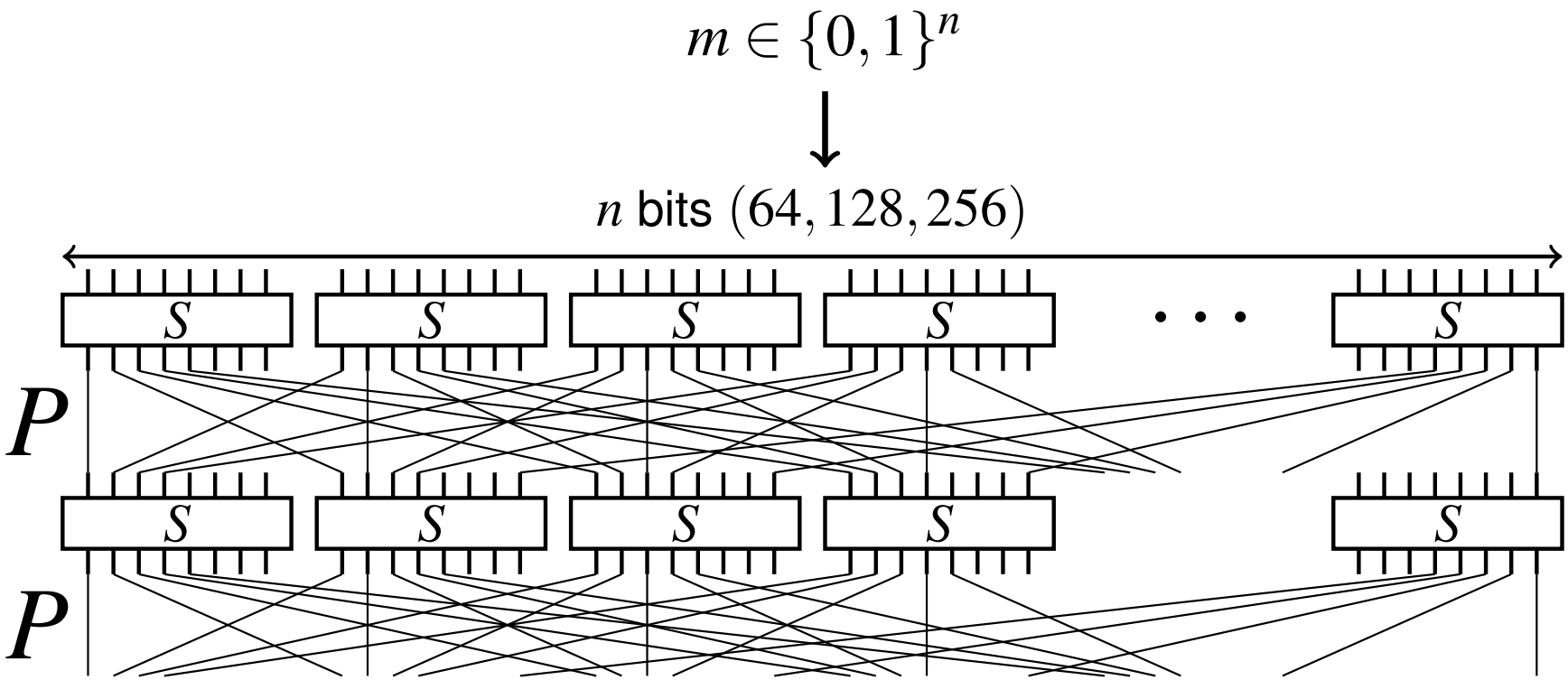
n bits $(64, 128, 256)$



Combien de fois ?

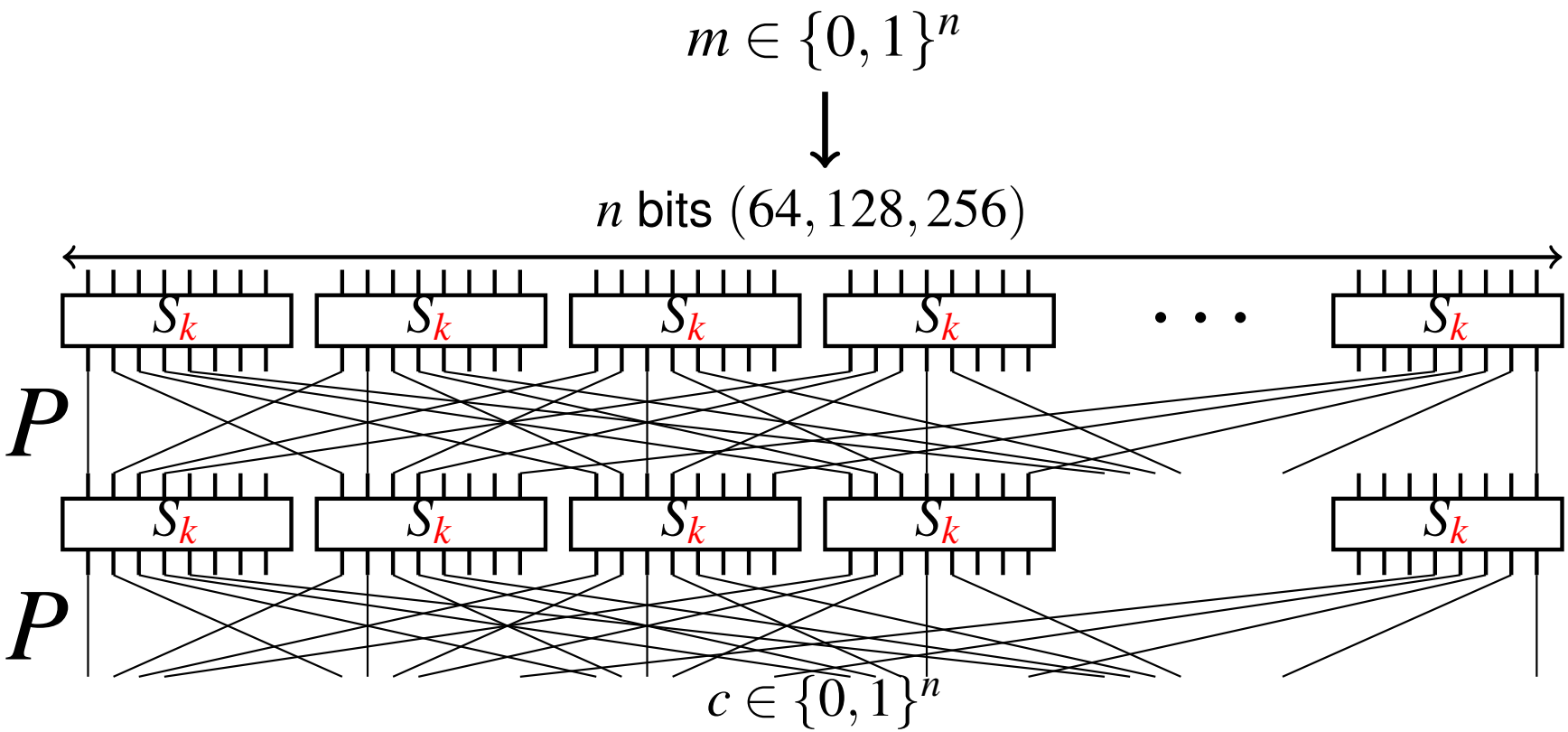
QUELLES PROPRIÉTÉS ?

- S non-linéaire (confusion)
- P doit mélanger (diffusion)
- Définir le nombre de tours est complexe.



✍ Qu'est-ce qu'il manque ?

Où rajouter la clef ?

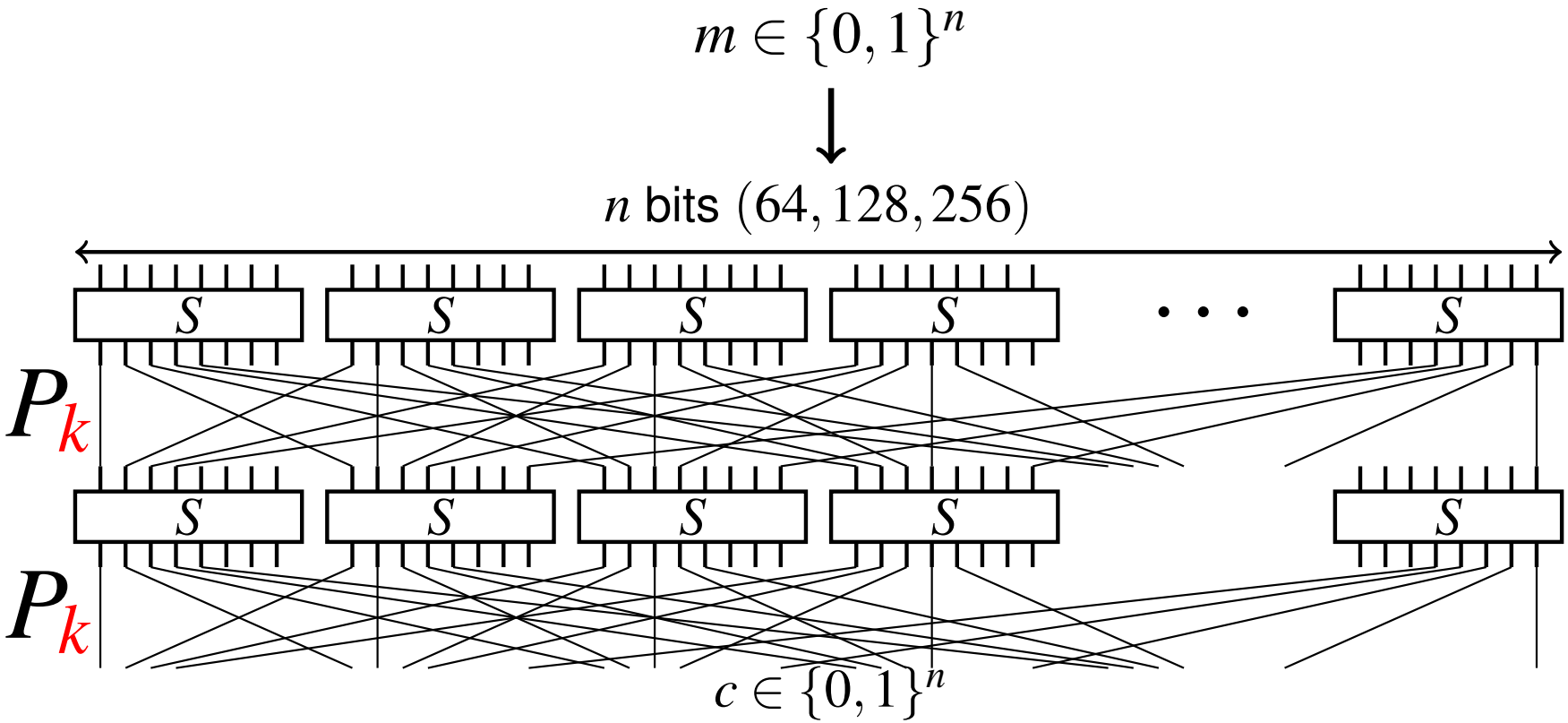


Où rajouter la clef ?

- **Implémentation :** S est représenté par une table. Si S dépend de la clef quelle est la taille mémoire ?
- **Sécurité :** Si pour certaines clefs S_k est « mauvaise », on peut avoir des attaques pour une certaine classe de clefs (clefs faibles).
- On préfère avoir des arguments de sécurité pour toutes les clefs.
- L'analyse est déjà compliquée, si on doit en faire une pour chaque classe de clef, ça l'est encore plus.
- Il faut aussi que S soit bijective (ce qui n'est pas forcément simple).

✍ Est-ce que la dernière permutation est utile ?

Où rajouter la clef ?



✍ Donner les problèmes possibles si la permutation dépend de la clef secrète.

Parenthèse sur les Attaques par canaux cachés

- Un algorithme peut se comporter différemment en fonction des entrées données.
- En cryptographie, une des entrées est la clef secrète k.
- En observant des comportements **physiques** différents, on peut en déduire de l'**information** sur la clef secrète.

✍ Quelles observations physiques vous imaginez ?

✍ Et si les opérations réalisées dépendent du secret ?

Schéma général d'un SPN

- Shannon propose initialement un croisement de fils.
- ✍ Quelle est la différence avec la composition d'une substitution et d'une transposition ?
- ✍ Pouvons-nous remplacer cela par autre chose ?

Schéma général d'un SPN

1. Définir une application linéaire sur tout l'état (e.g. 128 bits)

$$\mathcal{L} : \{0,1\}^n \to \{0,1\}^n$$

2. Choisir une boîte-S non-linéaire, bijective sur un petit nombre de bits (4 ou 8 par exemple), diviseur de la taille de l'état

$$S : \{0,1\}^\ell \to \{0,1\}^\ell$$

   On définit alors

$$\begin{aligned} \mathcal{S} : \{0,1\}^n &\to \{0,1\}^n \\ (X_0, X_1, \ldots, X_{n/\ell-1}) &\longmapsto (S(X_0), S(X_1), \ldots, S(X_{n/\ell-1})) \end{aligned}$$

   où pour tout $0 \leq i < \frac{n}{\ell}$, $X_i = x_{0+i\ell} || x_{1+i\ell} || \cdots || x_{\ell-1+i\ell}$

3.

$$R = \mathcal{L} \circ \mathcal{S} \circ \mathtt{Add}_k$$

CADENCEMENT DE CLEF

$$\texttt{KeySchedule} : \{0,1\}^{\kappa} \to \{0,1\}^{n \times r}$$

où r est le nombre de tours, κ le nombre de bits de la clef et n la taille de l'état.

- Si les tours sont identiques, on peut avoir des problèmes (cf. TD).
- Il faut plusieurs tours (on ne sais pas actuellement faire un chiffrement symétrique **performant** sans une structure itérative).
- Les critères précis sur le candencement de clef sont aujourd'hui peu compris.
- Certains cadencement de clef sont très simples : $k_i = k + c_i$

✍ Dessin au tableau du schéma général d'un chiffrement par bloc de type SPN.

Data Encryption Standard

- `Lucifer`, conçu par une équipe d'IBM (1971)
- Modifié par la NSA en vue du standard (National Bureau of Standards, NIST)
- DES
- Résistant à plusieurs attaques
- $\kappa = 56$...

JUIN 97 96 jours (Deschall Project, 78 000 PC)

FEV 98 39 jours (Distributed.net, 8 millions de processeurs)

JUIL 98 56 h (EFF, DES cracker, 250 000 $)

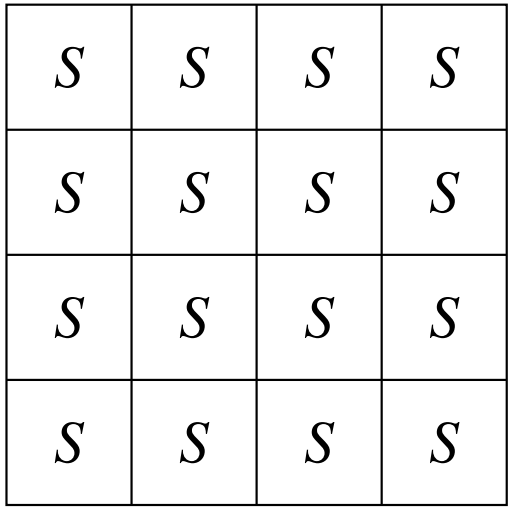
JANV 99 22h15 (EFF DES cracker + 100 000 processeurs)

MARS 07 6 jours (Copacabana, 9000 euros)

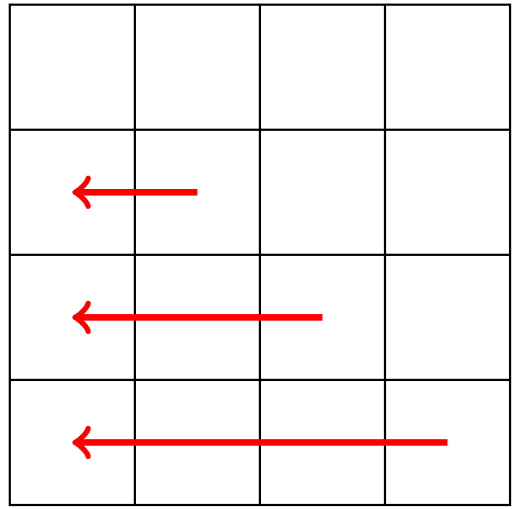
ADVANCED ENCRYPTION STANDARD - 1997

- Standardisé en 2001. `Rijndael`, conçu par Joan Daemen et Vincent Rijmen.
- Taille des clefs : 128, 192 et 256.
- Nombre de tours : 10 pour $\texttt{AES} - 128$, 12 pour $\texttt{AES} - 192$ et 14 pour $\texttt{AES} - 256$.
- Travaille sur des octets (8 bits), état du bloc : 128 bits.
- Quatre opérations :
  - **`SubBytes`**
  - **`ShiftRows`**
  - **`MixColumns`**
  - **`AddRoundKey`**

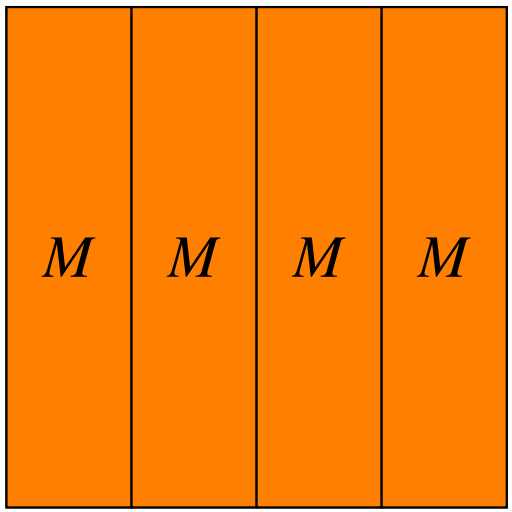
DÉTAIL DES OPÉRATIONS DANS L'AES



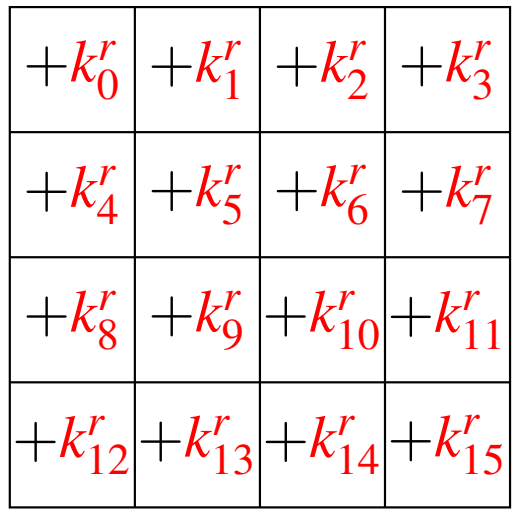
SubBytes (1)



ShiftRows (2)



MixColumns (3)



AddRoundKey (4)

Recherche exhaustive

Soit E un chiffrement par bloc opérant sur n bits et avec κ bits de clef.

- La recherche exhaustive fonctionne en testant toutes les clefs possibles.
- ✍ Donner le pseudo-code de la recherche exhaustive. De quoi avons-nous besoin ? Quel est le modèle d'attaque ?
- ✍ Que se passe t'il quand $n < \kappa$?
- ✍ Comment régler ce problème ?

Recherche Exhaustive et PRP

- ✍ Rappeler la définition de PRP (ce qu'on cherche à construire).
- ✍ Donner l'avantage de l'attaquant lorsque celui-ci réalise la recherche exhaustive en supposant $n = \kappa$. Une hypothèse est peut-être nécessaire pour se simplifier la vie.
- ✍ Casser IND-CPA avec la recherche exhaustive et le mode compteur.

Conclusion (Construction des chiffrements par bloc)

- On sait construire des chiffrements par bloc, dont on suppose que ce sont des PRPs.
- L'avantage pour distinguer une PRP est toujours supérieur à $\frac{1}{2^\kappa}$.
- La recherche exhaustive fonctionne toujours, on se compare donc à cela.
- Définir le nombre de tours n'est pas chose aisée (cryptanalyse).
- On cherche à concevoir des choses « simples »et « sécurisés »en respectant les propriétés de confusion et de diffusion
- Construire et analyser les chiffrements par bloc sont deux champs de recherche complexes en soi et permettent de gagner en confiance sur le caractère « PRP »
- Le DES est à proscrire. L'AES est actuellement encore supposé être une PRP.