Quelques propriétés de Rijndael

Marine Minier
Laboratoire CITI
INSA de Lyon

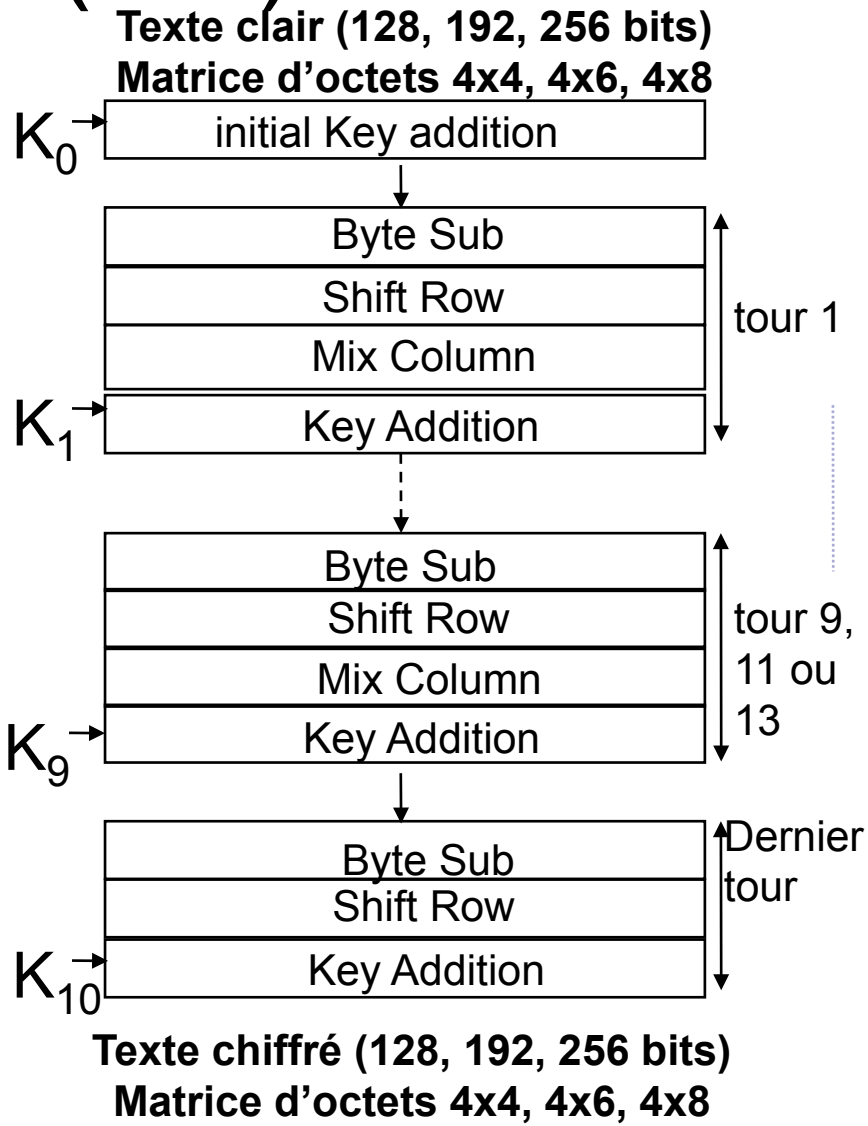
Plan de la présentation

- Description de l'AES et de ses frères
- Propriété intégrale de l'AES
- Propriétés intégrales des Rijndaels
- Distingueurs déduits
  - A clés inconnus
  - A clés connus
- LANE
- Conclusion

L’AES et ses frères

L'AES et Rijndael (1/3)

- Rijndael, créé par V. Rijmen et J. Daemen, choisi comme AES en octobre 2000.
  - Algorithme de chiffrement par blocs utilisant une structure parallèle.
  - **Taille des blocs** :
    128, 192 ou 256 bits.
  - **Longueurs des clés** :
    128, 192, ou 256 bits.
  - Le **nombre de tours varie** entre 10 et 14 selon la taille des blocs et la longueur des clés.



L'AES (2/3) : : La Fonction Étage 1/2

① **Byte Substitution**

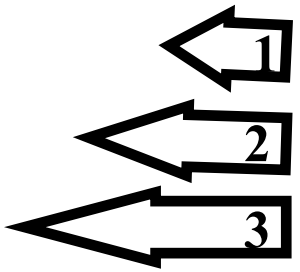
a_{00}	a_{01}	a_{02}	a_{03}
a_{10}	a_{11}	a_{12}	a_{13}
a_{20}	a_{21}	a_{22}	a_{23}
a_{30}	a_{31}	a_{32}	a_{33}

(8x8 S-box S) ↓

$S(a_{00})$	$S(a_{01})$	$S(a_{01})$	$S(a_{00})$
$S(a_{13})$	$S(a_{12})$	$S(a_{11})$	$S(a_{10})$
$S(a_{23})$	$S(a_{22})$	$S(a_{21})$	$S(a_{20})$
$S(a_{33})$	$S(a_{32})$	$S(a_{31})$	$S(a_{30})$

② **Shift Row**

a_{00}	a_{01}	a_{02}	a_{03}
a_{10}	a_{11}	a_{12}	a_{13}
a_{20}	a_{21}	a_{22}	a_{23}
a_{30}	a_{31}	a_{32}	a_{33}

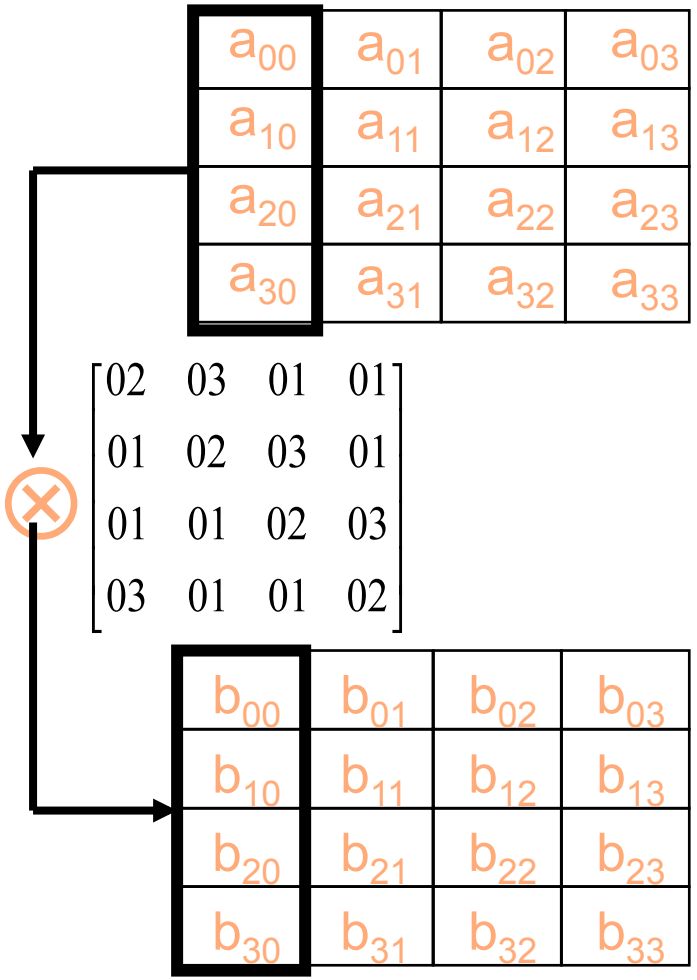


↓

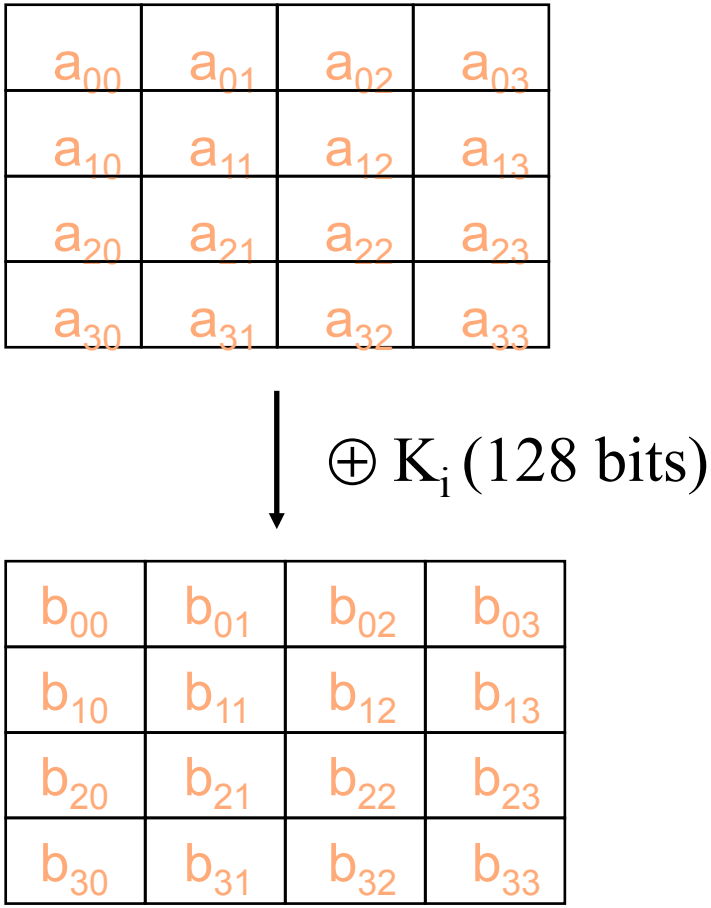
a_{00}	a_{01}	a_{02}	a_{03}
a_{11}	a_{12}	a_{13}	a_{10}
a_{22}	a_{23}	a_{20}	a_{21}
a_{32}	a_{30}	a_{33}	a_{31}

L'AES (3/3) : : La Fonction Étage 2/2

③ Mix Column

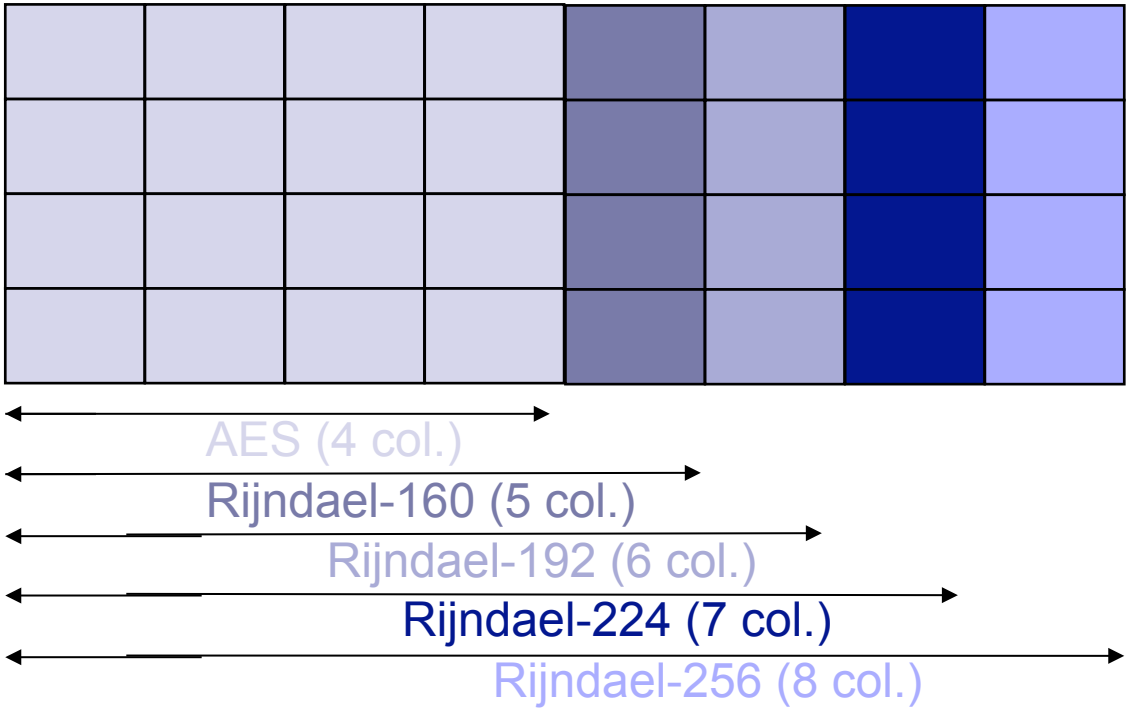


④ Key Addition



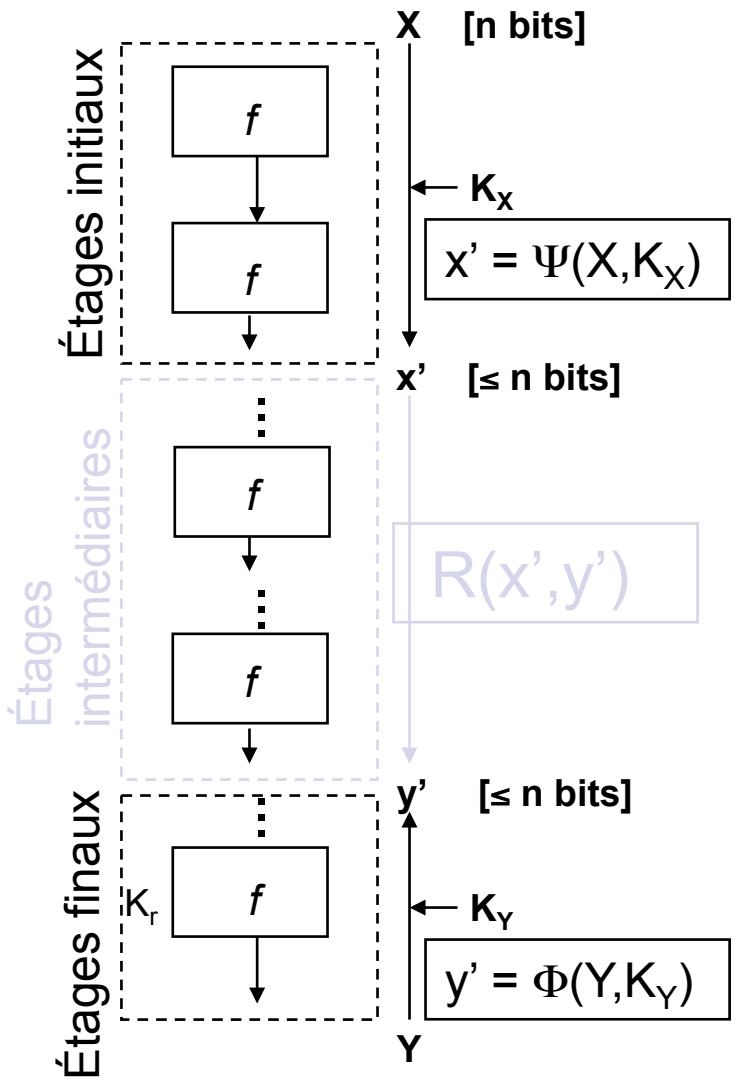
Rijndael : les différences

- Change :
  - Le nb de tours
  - Les ShiftRows



	AES	Rijndael-160	Rijndael-192	Rijndael-224	Rijndael-256
ShiftRows	(1,2,3)	(1,2,3)	(1,2,3)	(1,2,4)	(1,3,4)
Nb rounds (Nk=128)	10	11	12	13	14
Nb rounds (Nk=192)	12	12	12	13	14
Nb rounds (Nk=256)	14	14	14	14	14

Principe Général de la Cryptanalyse



- **Distingueur A :**
  recherche d'une relation **R(x',y')** sur les étages intermédiaires qui ait une probabilité *p* de se produire aussi éloignée que possible de la probabilité uniforme *p* :*

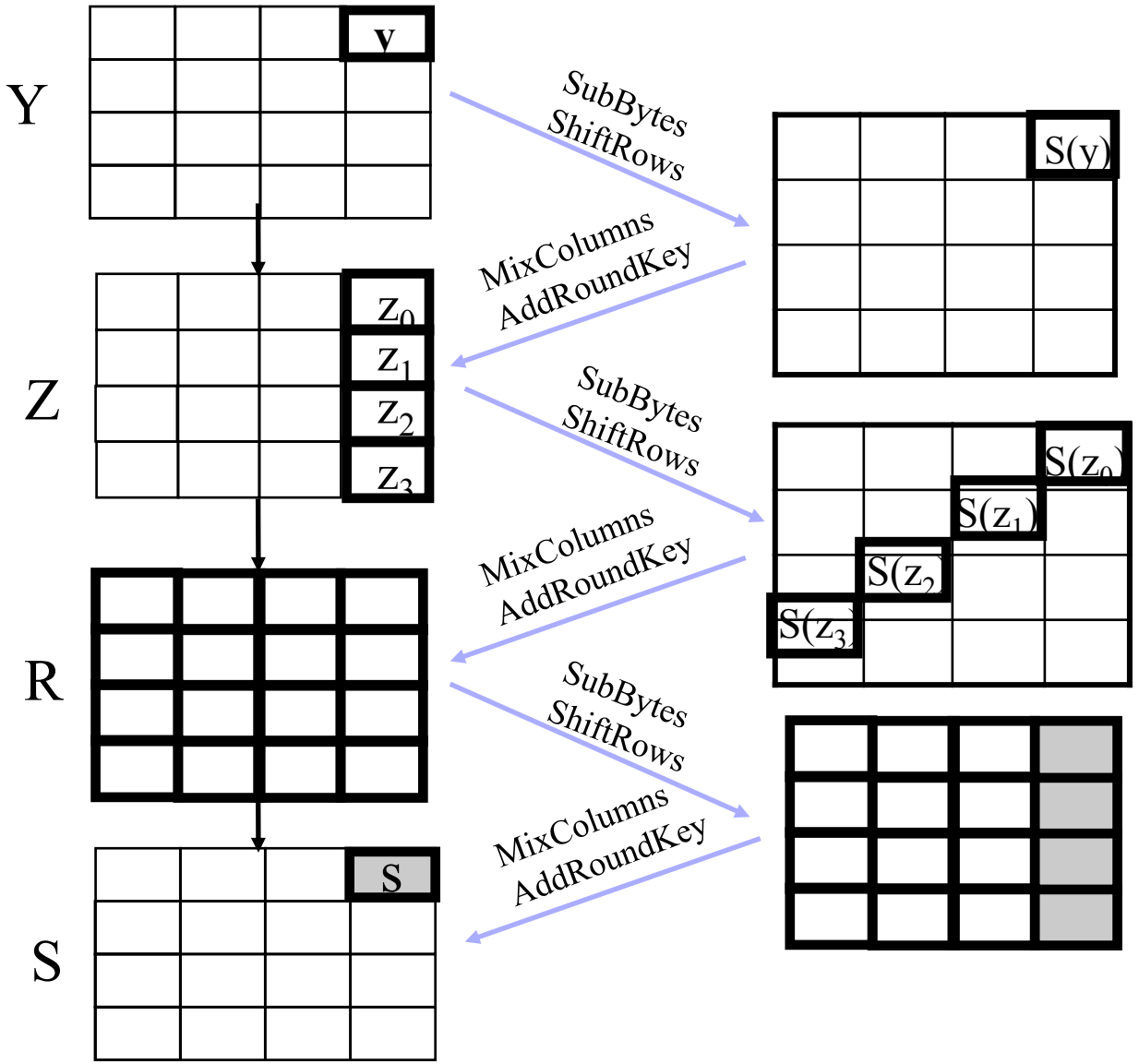
$$Pr[A]=Adv(A)=|p-p^*|$$

- **Test de clés** sur (K_X, K_Y)

Propriétés intégrales

Propriétés intégrales de l'AES (1/2)

- **octet y = 0…255**
- autres octets = **constants**



$$\bigoplus_{y=0}^{255} s(y) = 0$$

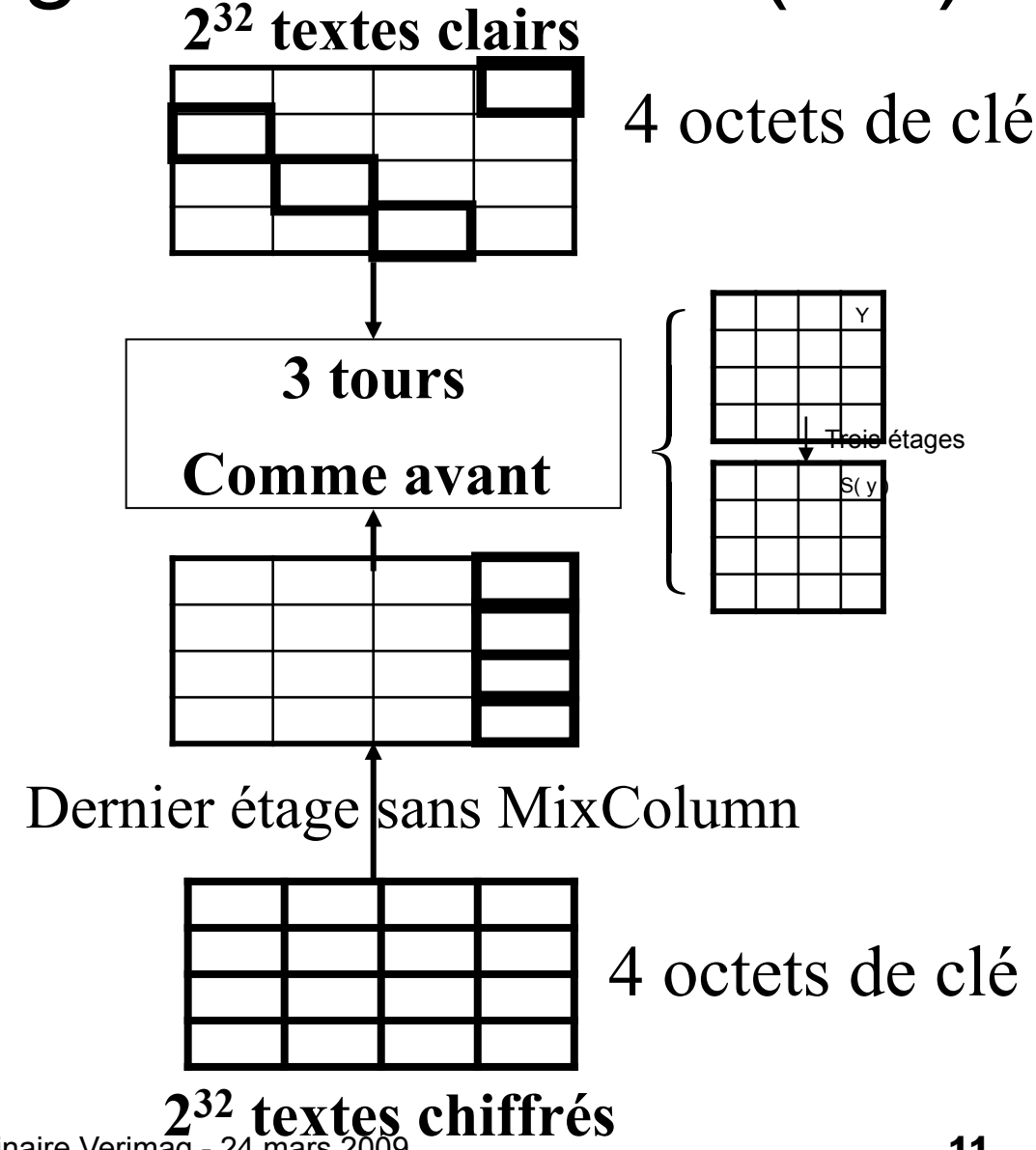
Propriétés intégrales de l'AES (2/2)

- **Pour chaque valeurs des 9 octets des sous-clés :**
- **Tester :**

$$\bigoplus_{y=0}^{255} s(y) =? \ 0$$

Les bonnes clés passent le test.

- **Attention aux fausses alarmes.**



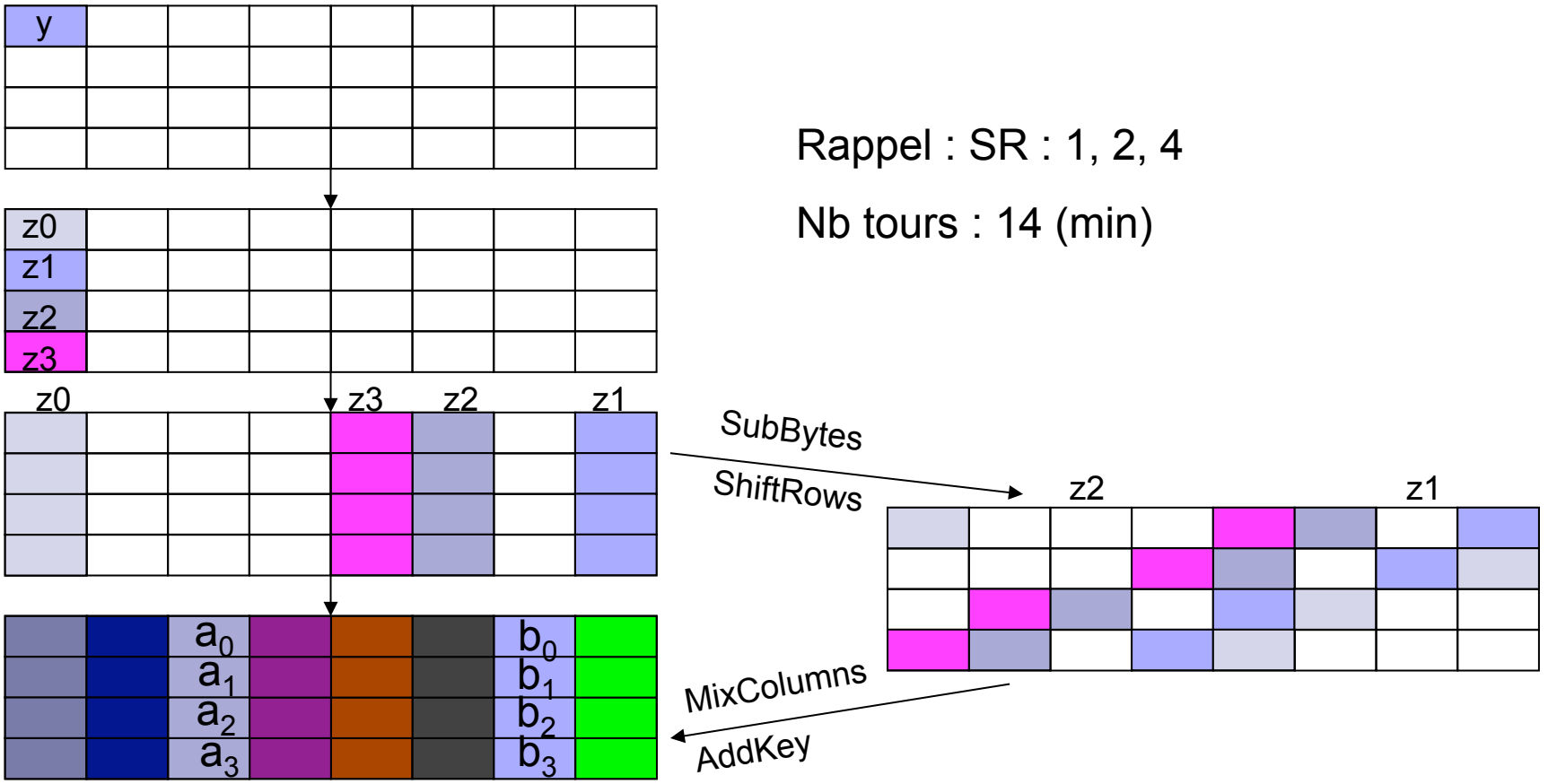
Complexité des attaques intégrales

- Avec l'amélioration de Ferguson :
  - Pour **6 tours : Nb clairs = $6*2^{32}$,**
    Complexité = 2^{46}
  - Pour **7 tours : Nb clairs = $2^{128} - 2^{119}$,**
    Complexité = 2^{120}

Pour Rijndael

- Le même genre de propriétés
- Mais en raison de la diffusion plus lente, plus d'étages + meilleures extensions

Rijndael-256 : 1ère remarque



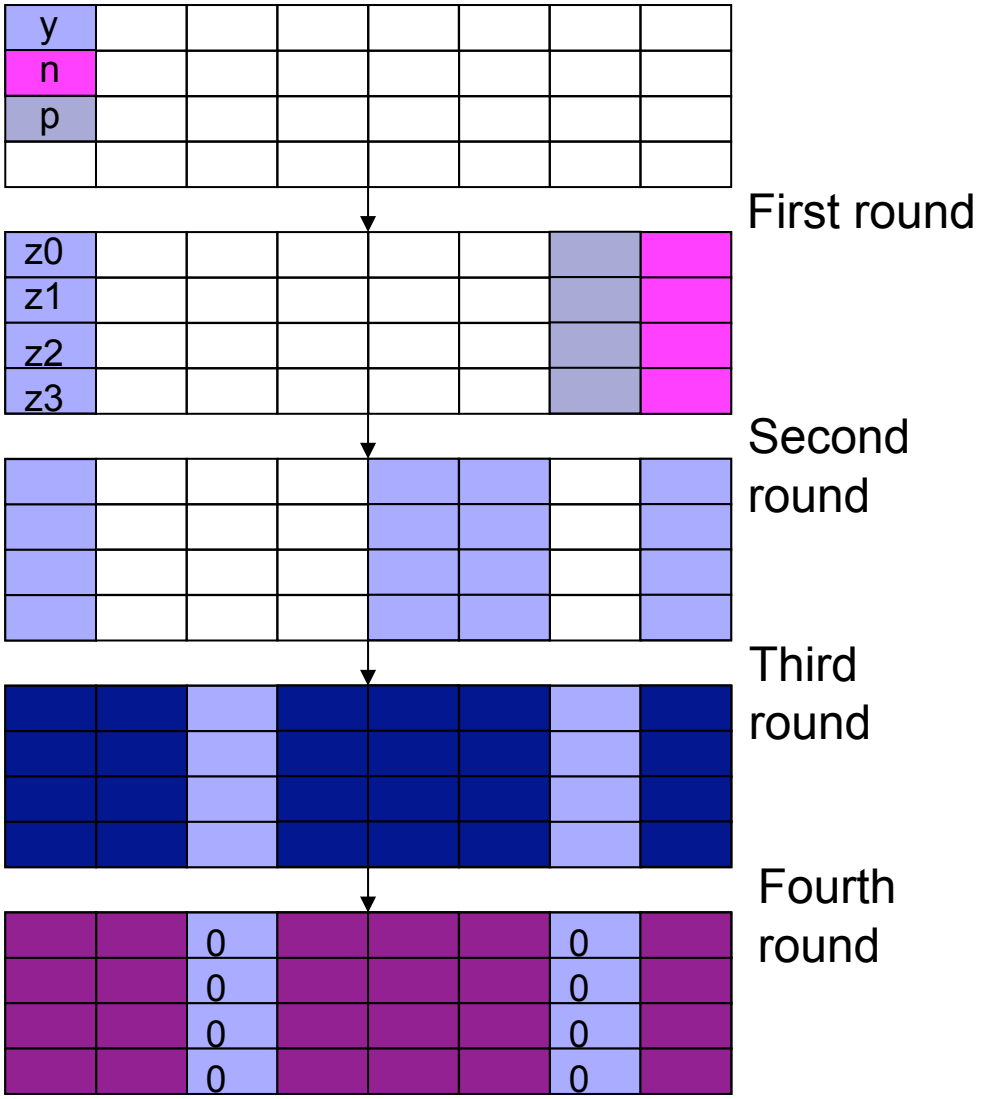
Rappel : SR : 1, 2, 4

Nb tours : 14 (min)

Rijndael 256 Propriété Intégrale

Distingueur sur 4 étages :

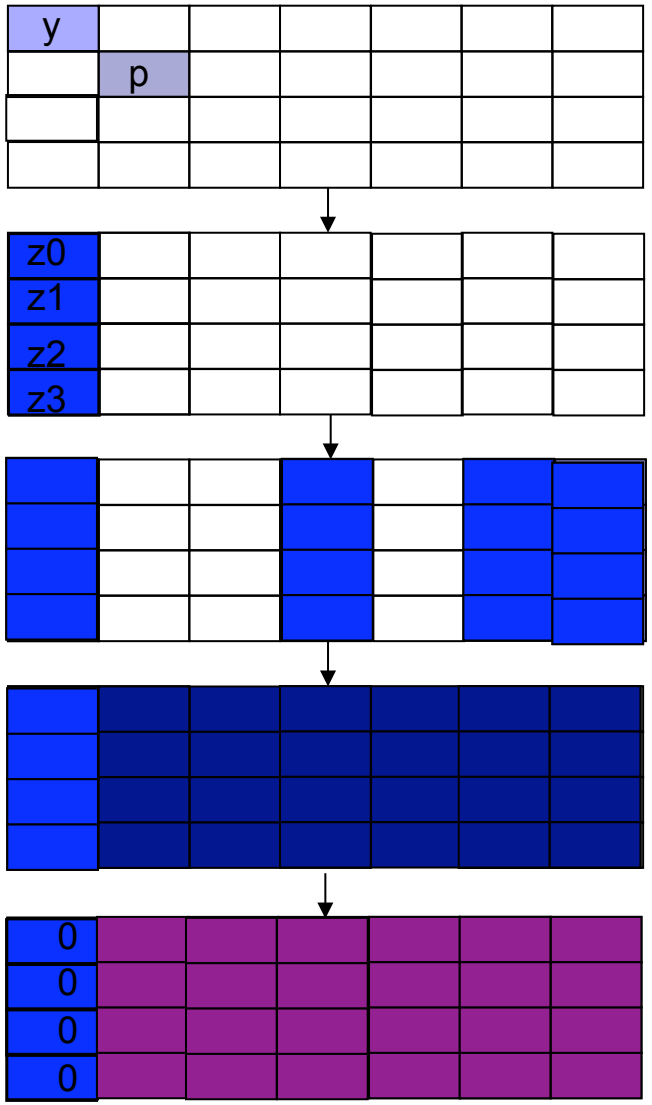
- Saturation de 3 octets
- => Complexité : 2^{24} chiffrements



Rijndael 224 Propriété Intégrale

Distingueur sur 4 étages :

- Saturation de 2 octets
- => Complexité : 2^{16} chiffrements



First round

Second round

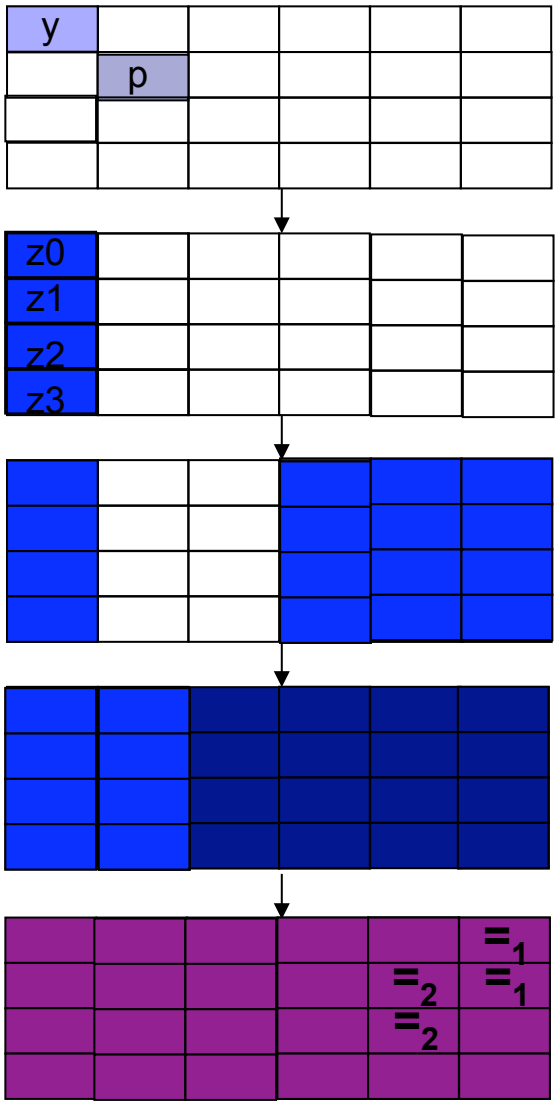
Third round

Fourth round

Rijndael 192 Propriété Intégrale (1)

Distingueur sur 4 étages :

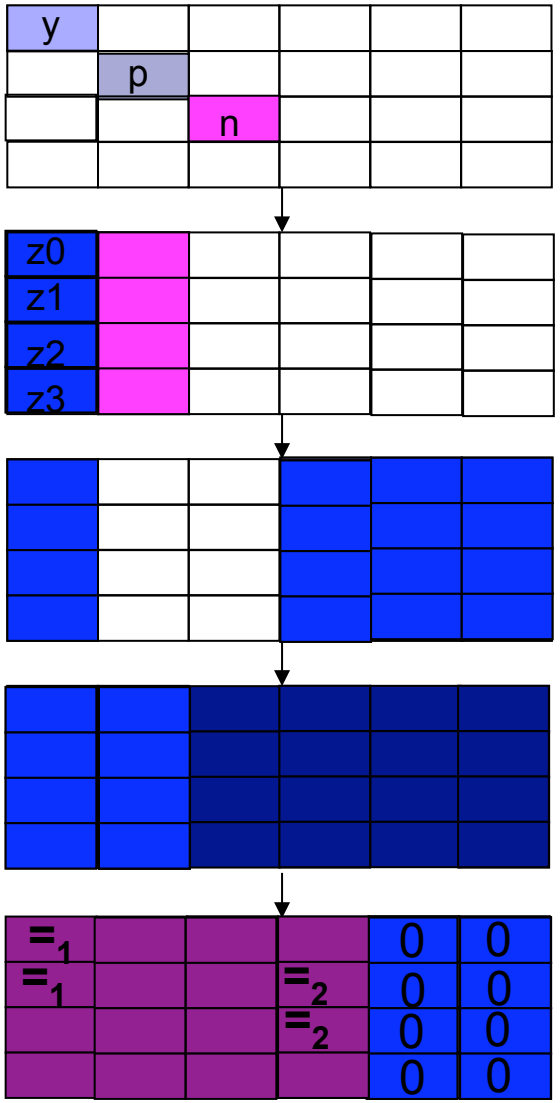
- Saturation de 2 octets
- => Complexité : 2^{16} chiffrements



Rijndael 192 Propriété Intégrale (2)

Distingueur sur 4 étages :

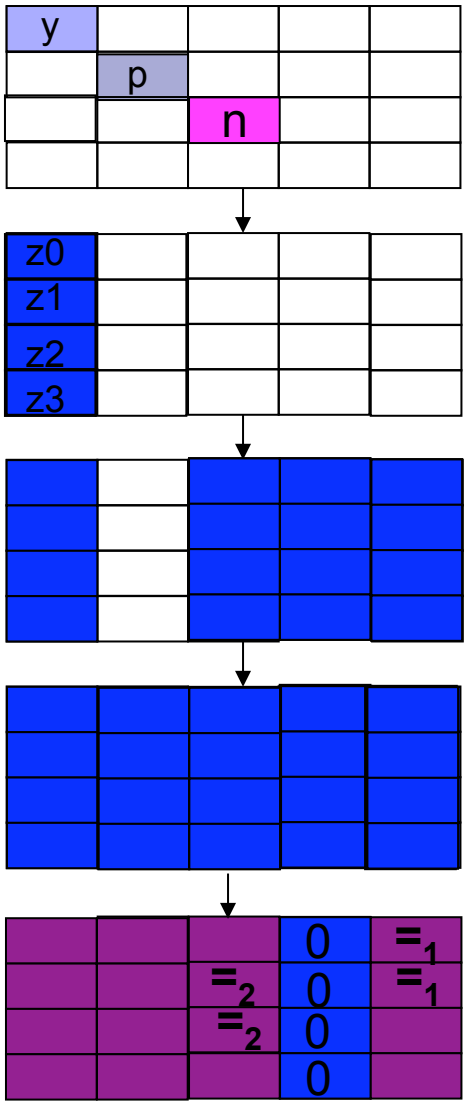
- Saturation de 2 octets
- => Complexité : 2^{16} chiffrements



Rijndael 160 Propriété Intégrale

Distingueur sur 4 étages :

- Saturation de 2 octets
- => Complexité : 2^{16} chiffrements

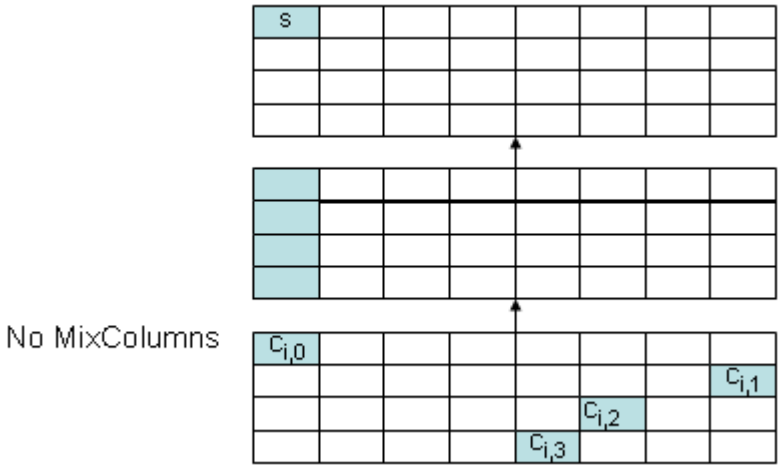


Distingueurs à clés inconnues

Extension de 2 tours à la fin

- [Ferguson et al. -00] : sommes partielles
- s directement déduit des $c_{i,j}$

$$\bigoplus_i S^{-1}\left[S_0\left[c_{i,0} \oplus k_0\right] \oplus S_1\left[c_{i,1} \oplus k_1\right] \oplus S_2\left[c_{i,2} \oplus k_2\right] \oplus S_3\left[c_{i,3} \oplus k_3\right] \oplus k_4\right]$$



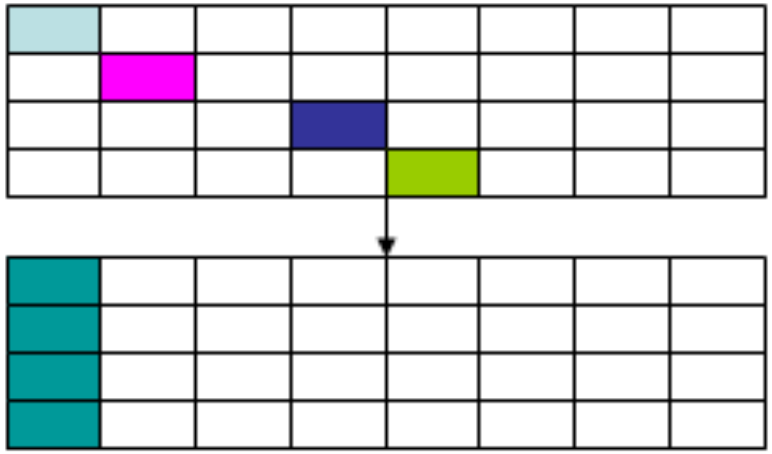
- À chaque chiffré c, on associe la somme partielle :

$$x_k := \sum_{j=0}^{k} S_j\left[c_j \oplus k_j\right] \text{ for } k \text{ from } 0 \text{ to } 3$$

- Utiliser $(c_0, c_1, c_2, c_3) \longrightarrow (x_k, c_{k+1}, \cdots, c_3)$
  Pour déterminer k_k séquentiellement
  => partage du calcul global en 4 étapes

Extension au début : 2 méthodes

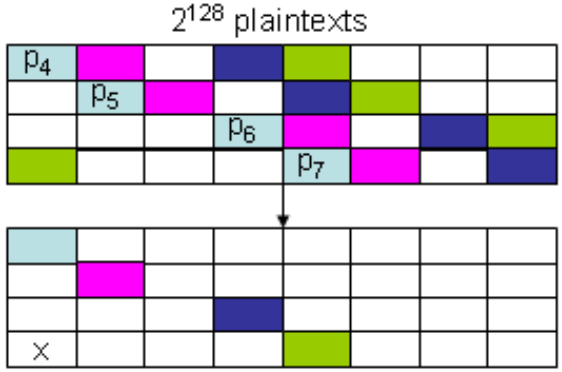
- [Ferguson et al. - 00] : un tour au début



- => Attaque sur 5 tours avec 2^{32} plaintexts

The herd technique

- Un tour de plus au début :
  - Naïvement 2^{128} plaintexts (marche, cf Nakhara et al.)
  - Octet particulier x fixé => a herd : ensemble de 2^{120} chiffrés de 2^{88} structures
  - Test sur un herd.



- X dépend de $(p_4,\ldots,p_7)$ et de 4 octets de 4 K_0
  1. En utilisant 2^{64} compteurs m_y
  2. 2^{32} compteurs n_z
  3. Filtrer les infos sur le key guess

Combiner tout cela…

- Attaque sur 2+4+2=8 étages
  1. Incrémenter les 64 bits (c_0,…,c_3,p_4,…, p_7)
  2. Devinez les 4 octets de K_0, calculer x, séparer les compteurs en herds.
  3. Choisir un single herd, mettre à jour n_z en ajoutant (c_0,…,c_3) pour chaque y correct
  4. Devinez les 5 octets de K_7 et de K_6 des deux derniers tours pour déchiffrer chaque z en un seul octet. Sommer cet octet sur les 2^{32} valeurs de z et regarder pour les 0.
  5. Répéter le dernier point pour chaque valeur des octets de K_0.

- => les 4 octets (p_4,…, p_7) et les 4 octets de K_0 fournissent 4 octets
- => 2^{24} herds plus petits,réduit la recherche exhaustive à 2^{128}-2^{119} plaintexts.

Complexité et attaques sur 9 étages

- Coût total :
  - 2^{128}-2^{119} plaintexts
  - 2^{120} chiffrements

- => ajout d'un étage en plus par recherche exhaustive complète de la clé K_9

Résumé des attaques

Rijndael-256	6	(all)	2^{32} CP	2^{72}	[4] (Integral)
	7	(all)	$2^{128} - 2^{119}$ CP	$2^{128} - 2^{119}$	[6] (Part. Sum)
	7	(all)	6×2^{32} CP	2^{44}	this paper
	8	(all)	$2^{128} - 2^{119}$ CP	$2^{128} - 2^{119}$	this paper
	9	(192)	$2^{128} - 2^{119}$ CP	2^{188}	this paper
	9	(256)	$2^{128} - 2^{119}$ CP	2^{204}	this paper

Cipher	nb rounds	Key sizes	Data	Time Complexity	Memory	Attack
Rijndael-256	6	(all)	$2 \cdot 2^{16}$ CP	2^{32}	2^{16}	2th-order integral
	7	(all)	$6 \cdot 2^{64}$ CP	2^{80}	2^{64}	8th-order integral
	8	> 192	$6 \cdot 2^{192}$ CP	2^{208}	2^{192}	24th-order integral
	8	(192)	$19 \cdot 2^{64}$ CP	2^{191}	2^{64}	8th-order integral
	8	(256)	$21 \cdot 2^{64}$ CP	2^{207}	2^{64}	8th-order integral
Rijndael-224	6	(all)	$2 \cdot 2^{16}$ CP	2^{32}	2^{16}	2th-order integral
	7	(all)	$6 \cdot 2^{64}$ CP	2^{80}	2^{64}	8th-order integral
	8	> 192	$6 \cdot 2^{192}$ CP	2^{208}	2^{192}	24th-order integral
	8	(192)	$19 \cdot 2^{64}$ CP	2^{191}	2^{64}	8th-order integral
	8	(256)	$21 \cdot 2^{64}$ CP	2^{207}	2^{64}	8th-order integral
Rijndael-192	6	(all)	$2 \cdot 2^{16}$ CP	2^{33}	2^{16}	2th-order integral
	7	(all)	$6 \cdot 2^{64}$ CP	2^{81}	2^{104}	8th-order integral
	6	(all)	$2 \cdot 2^{24}$ CP	2^{40}	2^{24}	3th-order integral
	7	(all)	$6 \cdot 2^{92}$ CP	2^{108}	2^{92}	12th-order integral
	8	(256)	$21 \cdot 2^{64}$ CP	2^{208}	2^{104}	8th-order integral
Rijndael-160	6	(all)	$2 \cdot 2^{24}$ CP	2^{40}	2^{24}	3th-order integral
	7	(all)	$6 \cdot 2^{92}$ CP	2^{108}	2^{92}	12th-order integral

Table 2. Summary of Attacks on Rijndael-b using the partial sums technique

Distingueurs à clés connues

[Knudsen – Rijmen 07]

- Notion de distingueur à clés connues
  - Principe, création d'un distingueur partant du milieu du chiffrement
  - Puis détermination d'une propriété particulière liant les clairs et les chiffrés
  - Comparaison avec la complexité nécessaire pour trouver la même propriété pour une permutation aléatoire

- Intérêt : cas des chiffrements par blocs utilisés comme fonction de hashage => distingueur

Modèle théorique [Africacrypt 09]

- Avantage des distingueurs [Vaudenay 97]: $Adv_E(A)$

$$Adv_E^{PRP}(\mathcal{A}) = \Pr\left[K \xleftarrow{\$} \mathcal{K} : A^{E_K(\cdot)} = 1\right] - \Pr\left[G \xleftarrow{\$} \mathrm{Perm}(\mathcal{M}) : A^{G(\cdot)} = 1\right]$$

$$Adv_E^{SPRP}(\mathcal{A}) = \Pr\left[K \xleftarrow{\$} \mathcal{K} : A^{E_K(\cdot),E_K^{-1}(\cdot)} = 1\right] - \Pr\left[G \xleftarrow{\$} \mathrm{Perm}(\mathcal{M}) : A^{G(\cdot),G^{-1}(\cdot)} = 1\right]$$

- Deux cas en plus : non-adaptatif, adaptatif

Cas d'un distingueur SPRP adaptatif

Algorithm 2 An n-limited generic adaptive distinguisher with chosen input plaintexts or output ciphertexts

Parameters: functions $g_1, \cdots, g_n$, a set $A^{(n)}$
Oracle: an oracle $\mathcal{O}$ implementing permutations c and c^{-1}
Select a fixed direction and message $(B_1, Z_1^0) = g_1()$ and get $Z_1^1 = c(Z_1^0)$ if $B_1 = 0$ or $Z_1^1 = c^{-1}(Z_1^0)$ otherwise
Calculate a direction and a message $(B_2, Z_2^0) = g_2(Z_1^1)$ and get $Z_2^1 = c(Z_2^0)$ if $B_2 = 0$ or $Z_2^1 = c^{-1}(Z_2^0)$ otherwise
...
Calculate a direction and a message $(B_n, Z_n^0) = g_n(Z_1^1, \cdots, Z_{n-1}^1)$ and get $Z_n^1 = c(Z_n^0)$ if $B_n = 0$ or $Z_n^1 = c^{-1}(Z_n^0)$ otherwise
if $(Z_1^1, \cdots, Z_n^1) \in A^{(n)}$ **then**
  Output 1
else
  Output 0
end if

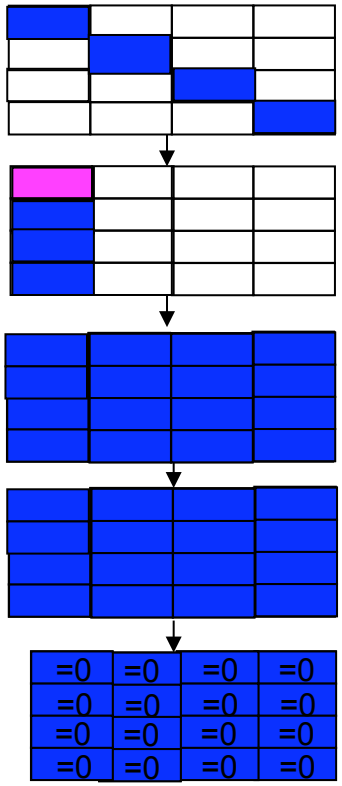
Cas d'un distingueur à clés connues

Algorithm 3 An n-limited generic non-adaptive chosen middletexts distinguisher ($NA\text{-}CMA$)

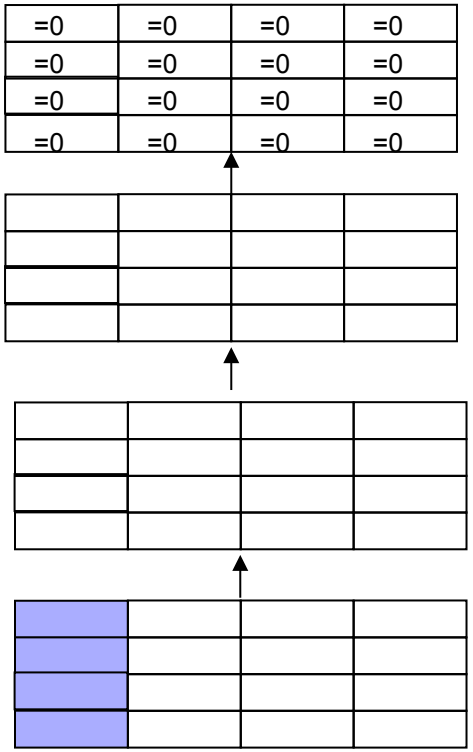
Parameters: a complexity n, an acceptance set $A^{(n)}$
Oracle: an oracle $\mathcal{O}$ implementing internal functions f_1 (resp. f_2) of permutation c that process input middletexts to the plaintext (resp. ciphertext) end
Compute some middletexts $\mathbf{M} = (M_1, \cdots, M_n)$
Query $\mathbf{P} = (P_1, \cdots, P_n) = (f_1(M_1), \cdots, f_1(M_n))$ and $\mathbf{C} = (C_1, \cdots, C_n) = (f_2(M_1), \cdots, f_2(M_n))$ to $\mathcal{O}$
if $(\mathbf{P}, \mathbf{C}) \in A^{(n)}$ **then**
  Output 1
else
  Output 0
end if

Etude de cas : l'AES [Knu-Rij 07]

- Sens descendant

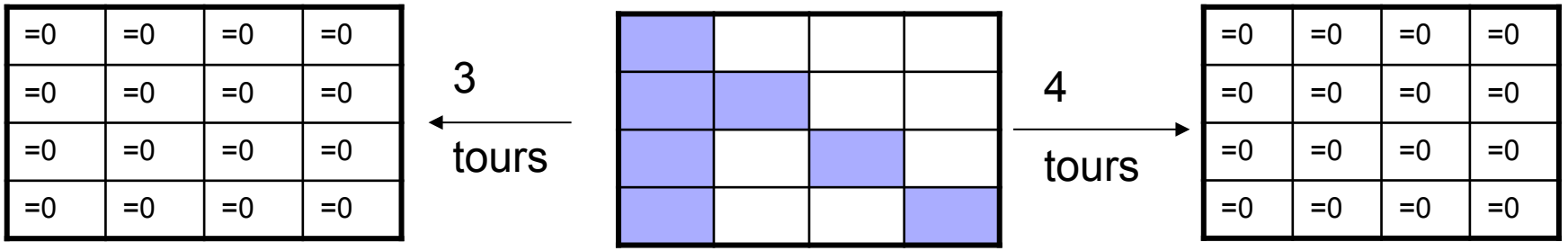


- Sens Montant



KK distinguisher pour l'AES

- KK distinguisher sur 7 étages
  - 3 dans un sens, 4 dans l'autre



  - Nécessitant 2^{56} middletexts et 2^{56} chiffrements
  - Pour une permutation aléatoire => k-sum problem, complexité : 2^{58} operations
- => KK distinguisher pour l'AES

KK distinguisher pour Rijndael

- Mêmes types de propriétés dans le sens montant

- Résumé des KK distinguishers pour Rijndael [Africacrypt 2009] :

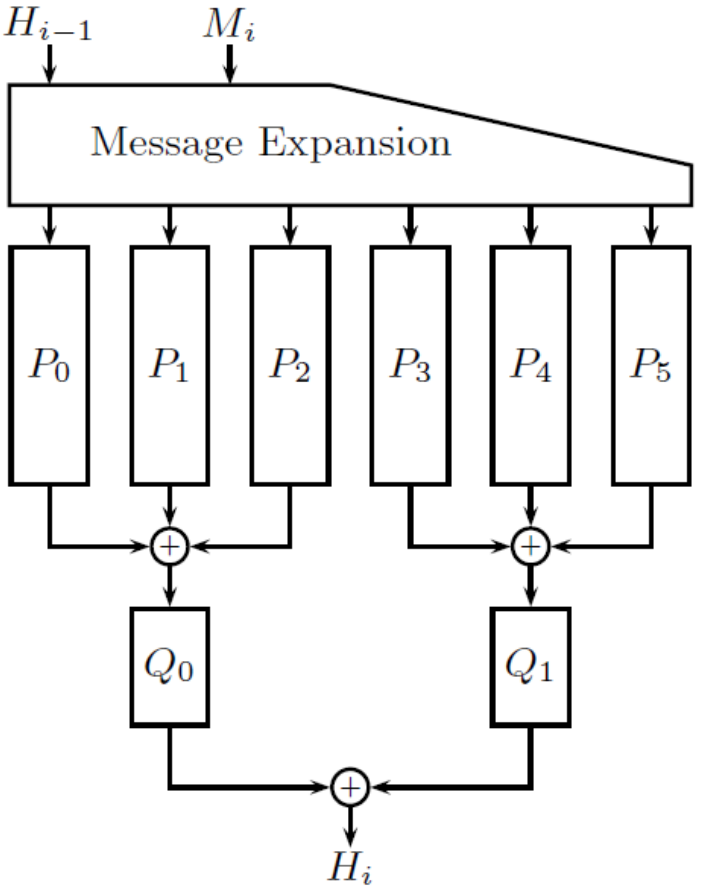
Cipher	nb rounds	Key sizes	Data	Time Complexity	Memory	Source
AES	7	(all)	2^{56} CM	2^{56}	small	[12]
Rijndael-256	8	(all)	2^{40} CM	2^{40}	small	this paper
Rijndael-224	8	(all)	2^{72} CM	2^{72}	small	this paper
Rijndael-192	7	(all)	2^{32} CM	2^{32}	small	this paper
Rijndael-160	7	(all)	2^{40} CM	2^{40}	small	this paper

Table 2. Summary of known-key distinguishers on Rijndael-b. CM means Chosen Middle-texts.

Encore une idée…

LANE : fonction de hashage soumise à SHA 3

- $H_i = h_0 \| h_1 = 256$ bits
- $M_i = m_0 \| m_1 \| m_2 \| m_3 = 512$ bits
- P_i = 6 tours AES modifié
- Q_i = 3 tours AES modifié

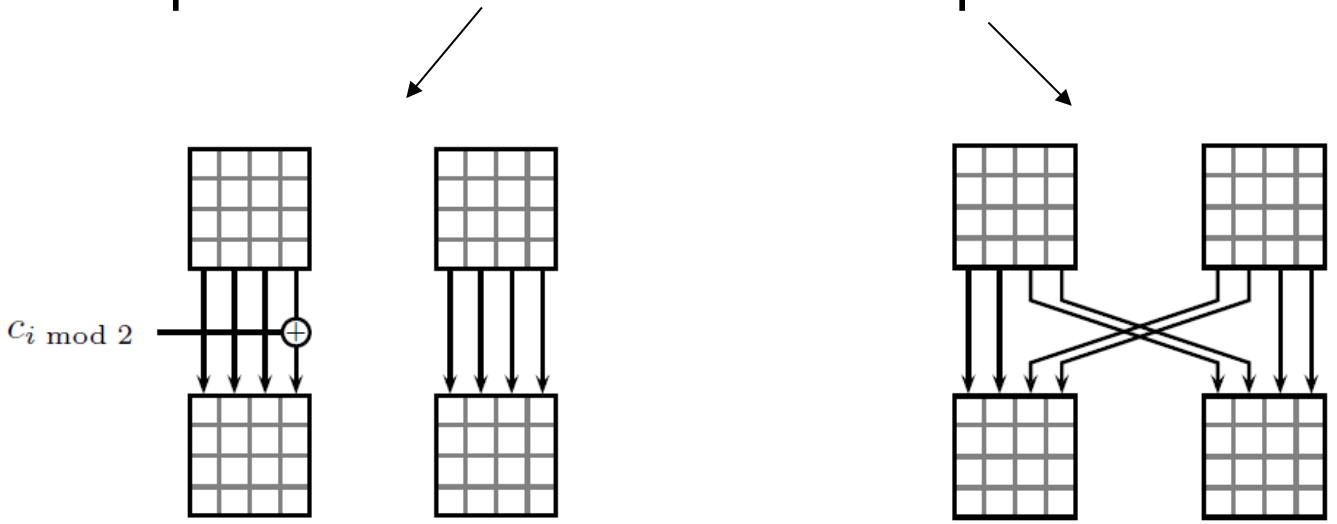


Ce qui rentre dans les P_i

$$
\begin{array}{l|l}
W_0 = h_0 \oplus m_0 \oplus m_1 \oplus m_2 \oplus m_3 & h_1 \oplus m_0 \oplus m_2 \\
W_1 = h_0 \oplus h_1 \oplus m_0 \oplus m_2 \oplus m_3 & h_0 \oplus m_1 \oplus m_2 \\
W_2 = h_0 \oplus h_1 \oplus m_0 \oplus m_1 \oplus m_2 & h_0 \oplus m_0 \oplus m_3 \\
W_3 = h_0 & h_1 \\
W_4 = m_0 & m_1 \\
W_5 = m_2 & m_3
\end{array}
$$

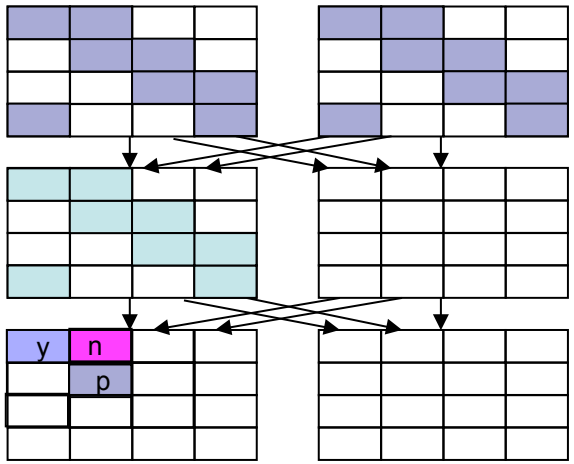
Les P_i et les Q_i (LANE 256)

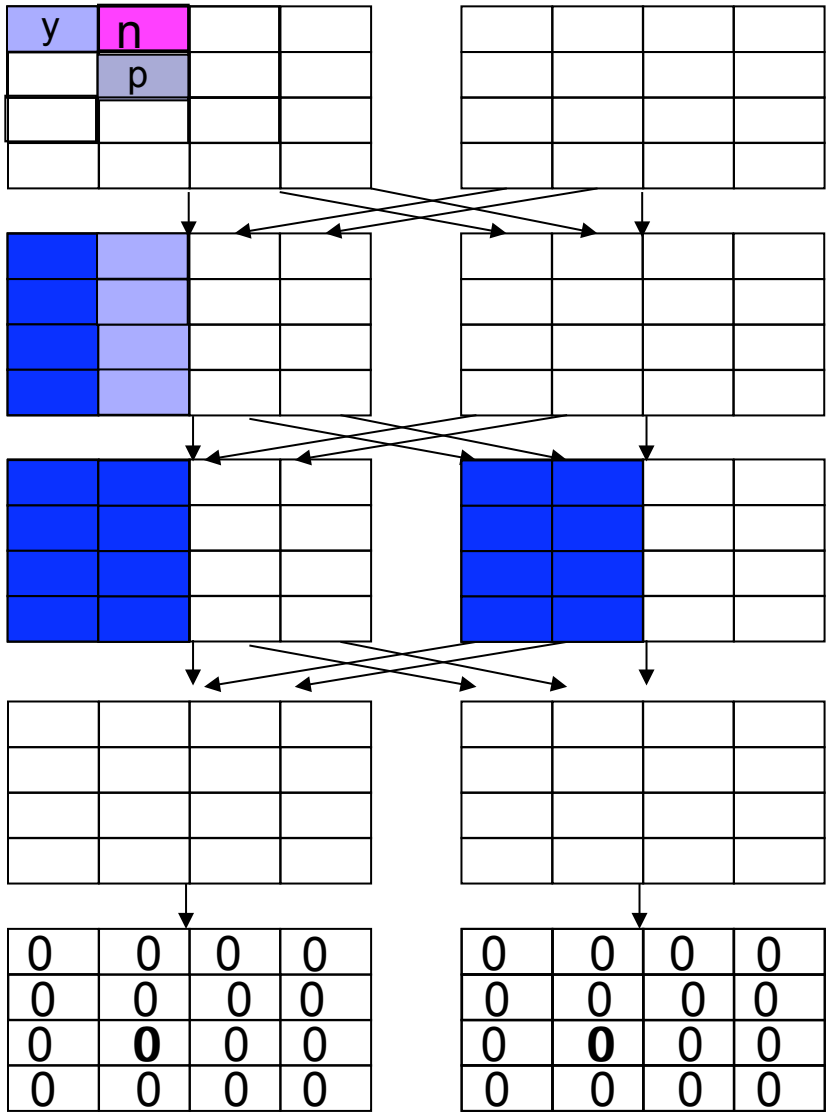
- Les mêmes opérations que l'AES en 256 bits
  - SubBytes, ShiftRows, MixColumns, KeyAdd (with constants)
  - En plus : AddConstants et SwapColumns



Propriétés intégrales de LANE-256

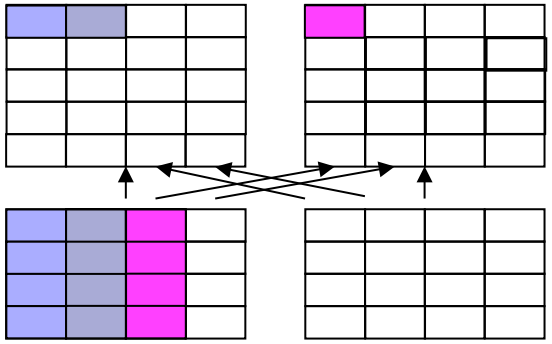
- 3 tours + extension au début :

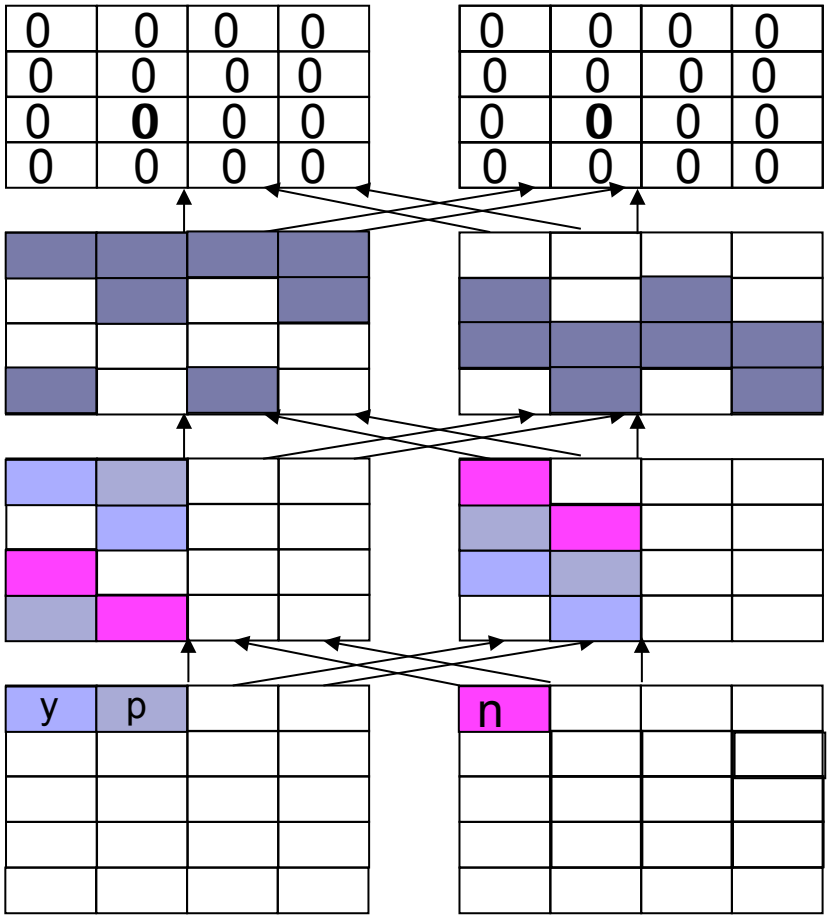




Propriété intégrale de LANE-256 sens indirect

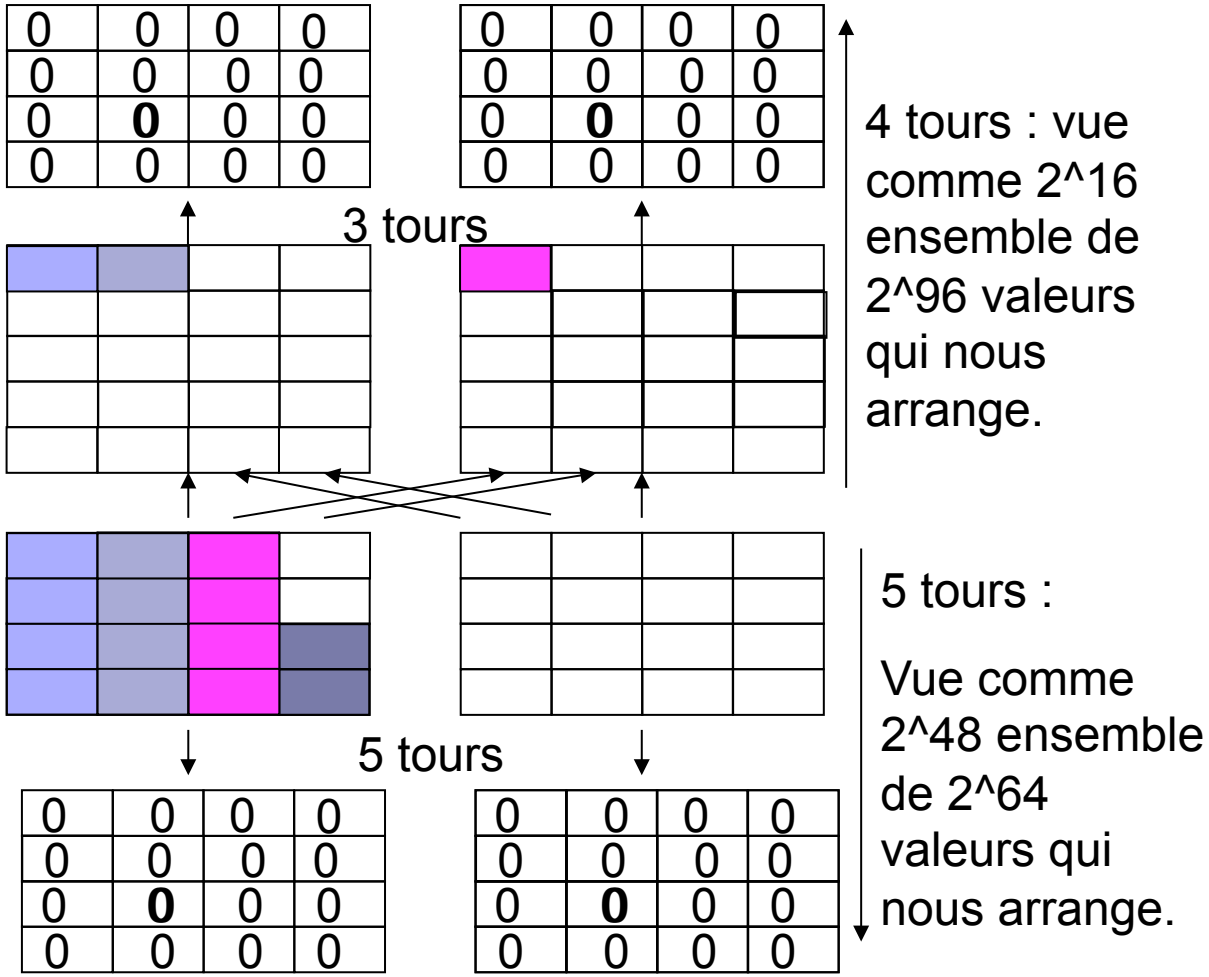
- Propriété intégrale sur 3 tours + extension au début :





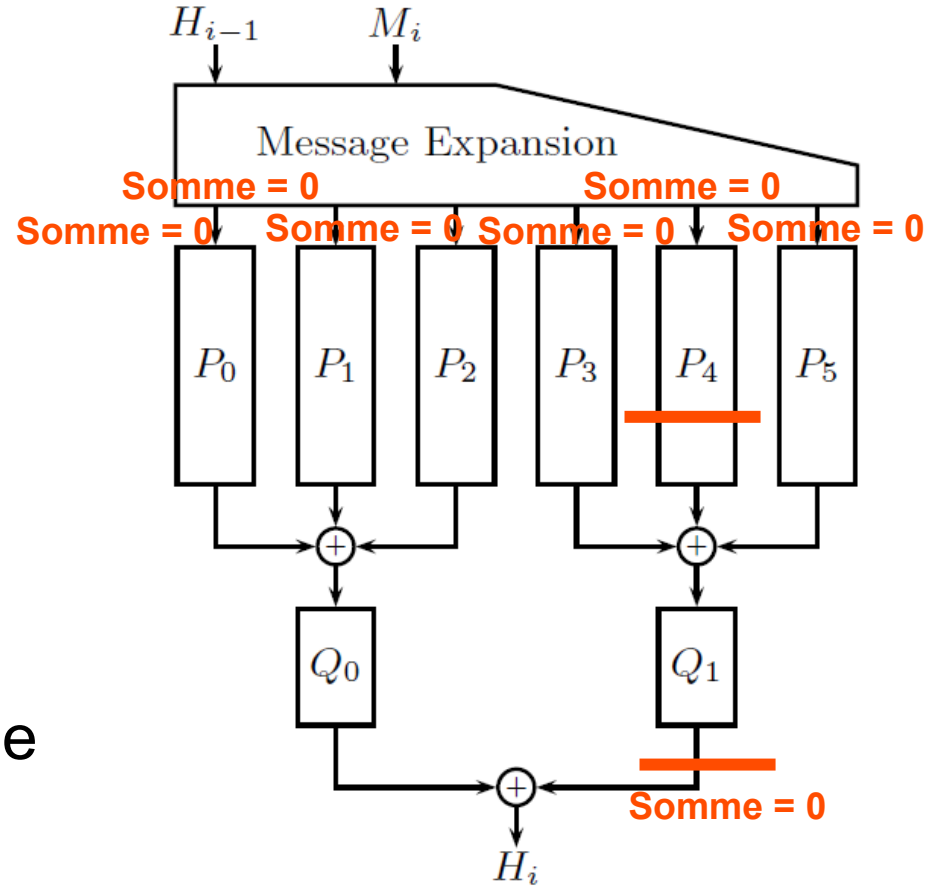
On combine les deux

- Distingueur en 2^{112} de la moitié de LANE…



Pourquoi la moitié ?

- Si $h_0=h_1=m_2=m_3$ = cte :
  - W0 = m0 + m1 || m0
  - W1 = m0 || m1
  - W2 = m0 + m1 || m0
  - W3 = 0 || 0
  - W4 = m0 || m1
  - W5 = 0 || 0
- Alors :
  - Sur 2^{112} messages, un certain nombre de somme valent 0…



Conclusion

- Les propriétés intégrales sur Rijndael n'avait pas été bien étudiées
  - Distingueurs à clés inconnues
  - Distingueurs à clés connues

- Dernier modèle prometteur et important pour la compétition SHA-3 (cf : LANE)