Cryptanalyse

Cours 4 - Chiffrement par Blocs

Maxime Bombar

Mardi 24 Septembre 2024

Rappels de la Semaine Dernière

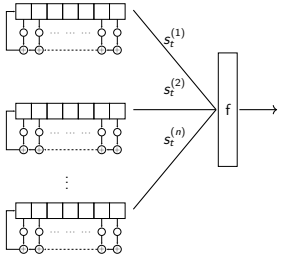
LFSR : Avantages et Inconvénients

- Ils sont extrêmement rapides et peu gourmands en ressources (implémentation matérielle, peu de mémoire).
- La suite produite possèdes de bonnes propriétés statistiques.
- La suite produite a une très grosse période.

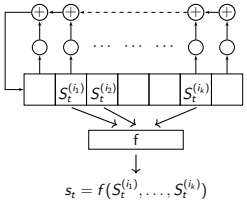
Leur complexité linéaire est logarithmique en la période...
$\Rightarrow$ Application directe de l'algorithme de Berlekamp-Massey.

Augmenter la Complexité Linéaire

On a vu deux façons d'augmenter la complexité linéaire :



LFSR Combinés



LFSR Filtrés

Il faut tenir compte de nouvelles gammes d'attaques (e.g., correlations, algébriques...)

Eprint, le Vendredi 20 Septembre

Quantum Algorithms for Fast Correlation Attacks on LFSR-Based Stream Ciphers*

Akinori Hosoyamada

NTT Social Informatics Laboratories, Tokyo, Japan
NTT Research Center for Theoretical Quantum Information, Atsugi, Japan
akinori.hosoyamada@ntt.com

À paraître, ASIACRYPT 2024.

Chiffrement par bloc

Objectifs du jour

- Rappels chiffrements par blocs et modes d'opération.
- Rappels construction de Feistel (e.g., DES)
- Rappels construction par réseaux de permutation (e.g., AES).

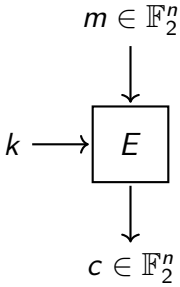
En TD

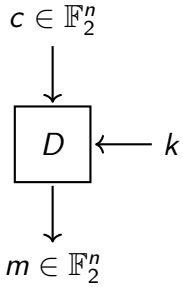
Une attaque par canaux auxiliaires sur le mode CBC.

Chiffrement par bloc

Définition

Soient n, κ deux entiers. Un **chiffrement par blocs** de taille de bloc n et de taille de clé κ est une famille de 2^κ permutations $(E_k, D_k = E_k^{-1})$ de $\mathbb{F}_2^n$, indexée par une clé $k \in \mathbb{F}_2^\kappa$.





Critères de sécurité

- **Confusion** : La structure du chiffrement doit être cachée.
- **Diffusion** : La modification d'un bit de clair doit affecter tout le chiffré.

- En général, la diffusion est assurée par les parties (bijectives) **linéaires**.
- La confusion est assurée par les parties **non-linéaires**, qu'on appelle aussi **S-box** (Substition box).

Cryptanalyse d'un chiffrement par blocs

En général, la clé est le seul élément secret d'un chiffrement par blocs.

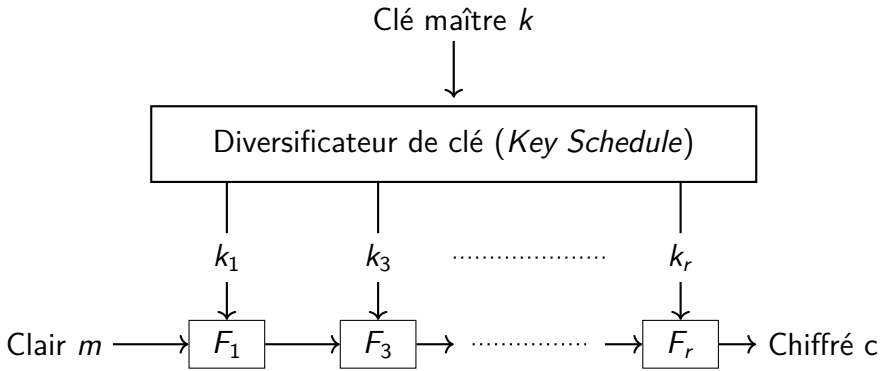
Objectif de sécurité

Il ne doit pas y avoir d'algorithme retrouvant la clé secrète à partir de couples $(\text{clairs}, \text{chiffrés})$ qui soit plus efficace que la recherche exhaustive sur l'espace des clés.

Objectif plus fort

Si $k \leftarrow \mathbb{F}_2^\kappa$, E_k doit être **indistinguable** d'une permutation aléatoire de $\mathbb{F}_2^n$.

Chiffrement par blocs iterés



Slide attack (Biryukov, Wagner 1999)

Les fonctions de tours F_i doivent être **différentes** (par exemple différentes clés).

Directions de recherches contemporaines

Cryptographie « légère » (*Lightweight Competition*)

- AES est relativement gourmand en ressources.
- Pour l'embarqué (*e.g.*, IoT) on cherche des chiffrements « à bas coût »
- Chiffrements « maison » souvent très faibles (*e.g.*, KeeLoq) $\rightarrow$ Standardisation.
- Exemple de chiffrement par blocs léger : Saturnin (2020).

Basse complexité multiplicative

Pour certaines applications cryptographiques avancées (MPC, FHE, zk-SNARKs...) la complexité est très largement dominée par le **nombre de multiplications**.

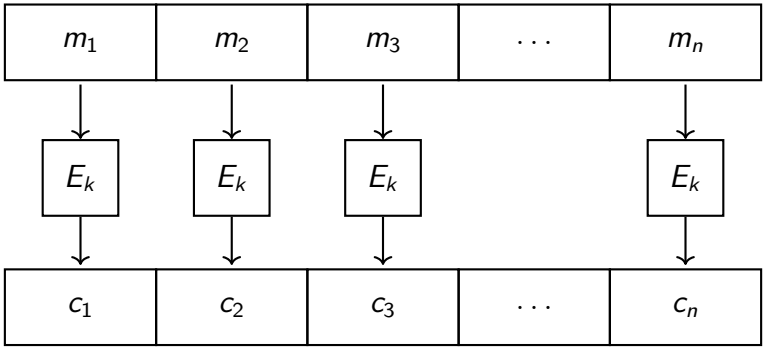
- LowMC (2015) est un chiffrement par blocs avec une très faible complexité multiplicative.
- À la base de la signature post-quantique Picnic (Finaliste compétition du NIST).

Modes d'Opération

Modes d'opération

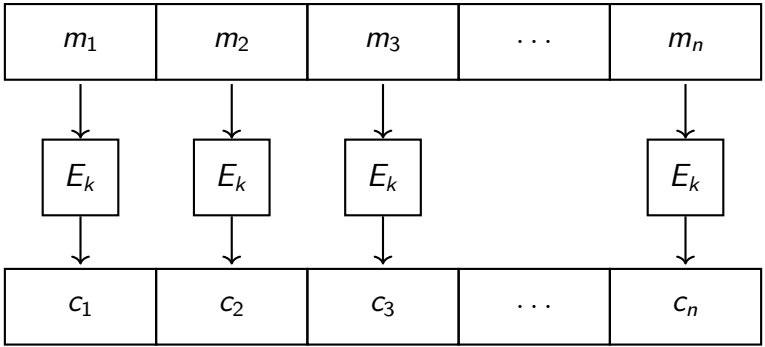
Comment chiffrer un message plus gros que la taille d'un bloc ?

Mode ECB (*Electronic Code-Book*)



Voyez-vous un potentiel problème ?

Mode ECB (*Electronic Code-Book*)

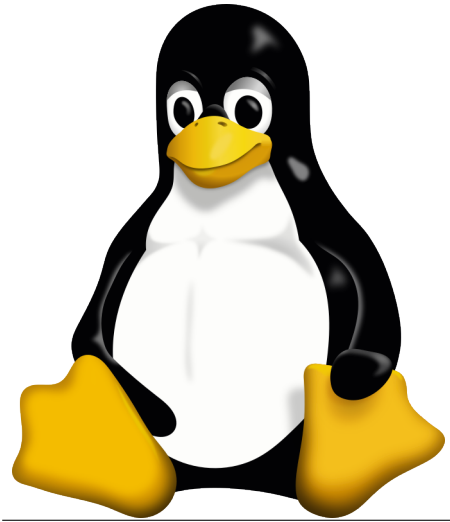


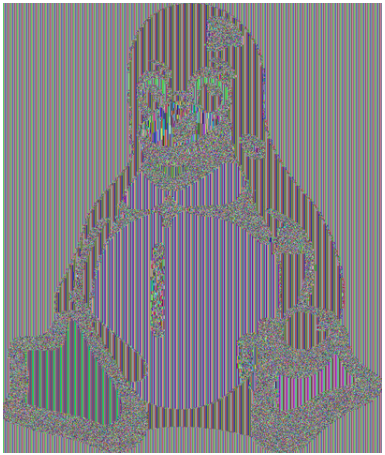
Deux blocs identiques (m, m) vont donner deux blocks du chiffré identiques (c, c)

$\rightarrow$ on peut reconnaître des motifs dans le chiffré.

$\rightarrow$ à n'utiliser que sur des données aléatoires....

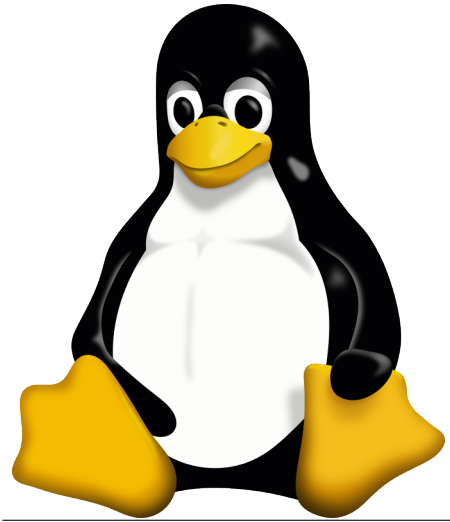
Chiffrement de Tux (Mode ECB) [1]

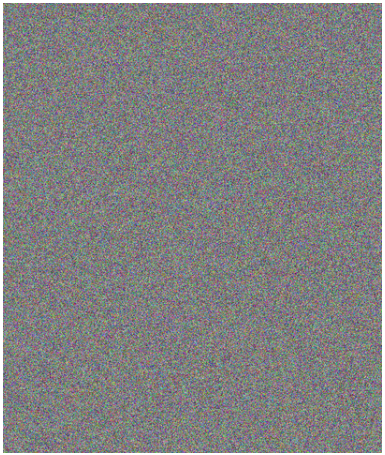




1. https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

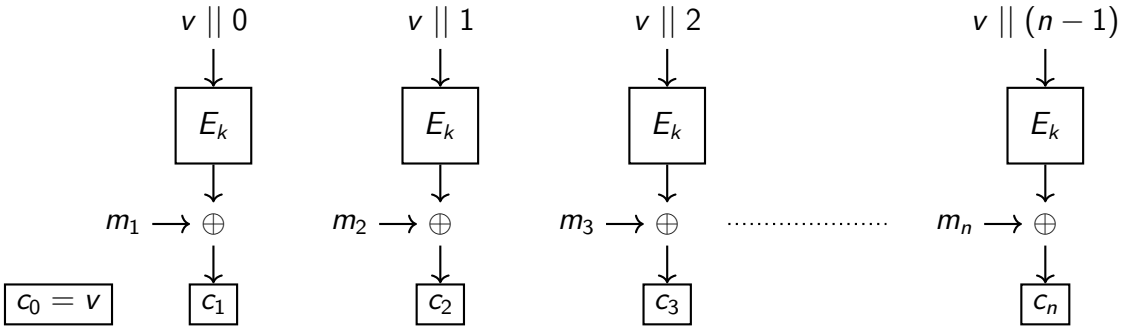
Chiffrement de Tux (Mode CTR) [1]





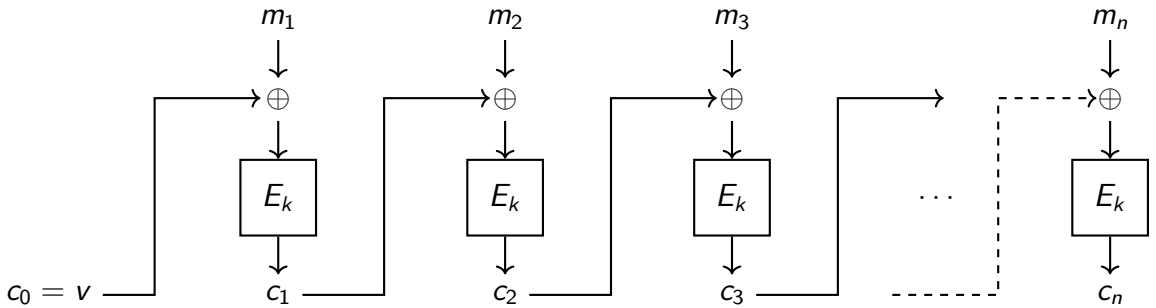
1. https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Mode CTR (*Counter Mode*)



On chiffre un vecteur d'initialisation v et un compteur pour obtenir une **suite chiffrante**, à la manière d'un chiffrement par flot.

Mode CBC (*Cipher Block Chaining*)



$$c_1 = E_k(v + m_1) \qquad c_{i+1} = E_k(c_i + m_{i+1})$$

Cryptanalyse du mode CBC par canaux auxiliaires

En TD : Attaque de Vaudenay (S. Vaudenay 2002)

Vous implémenterez une attaque dévastatrice contre le mode ECB s'il est utilisé avec un mauvais système de padding. Il s'agira de l'une des seules attaques par canaux auxilaires que l'on verra dans ce cours.

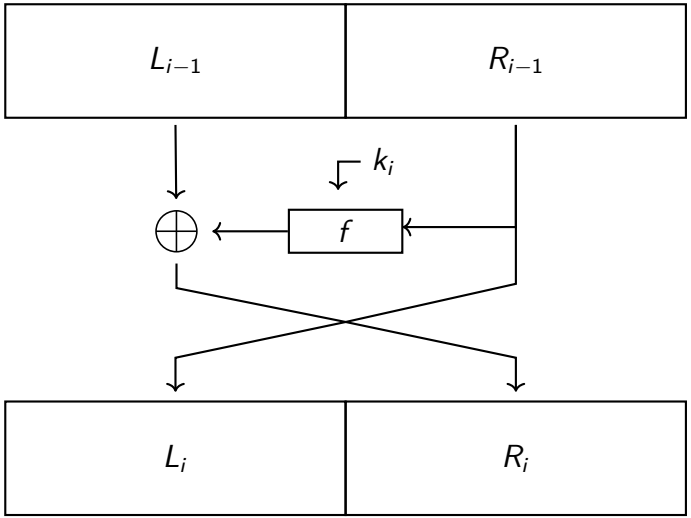
D'autres modes ?

Pour protéger l'intégrité des messages

- AEAD (*Authenticated Encryption with Addition Data*)
- GCM (*Galois Counter Mode*), utilisé dans TLS1.2 et TLS1.3, SSH, ...
- CBC-MAC
- CCM (*Counter with CBC-MAC*)
- ...

Schémas de Feistel

La construction



- $m = L_0 \,||\, R_0$ de $2n$ bits
- $L_i = R_{i-1}$
- $R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$

où $f : \mathbb{F}_2^n \times \mathbb{F}_2^\kappa \to \mathbb{F}_2^n$
est une fonction booléenne, décrite comme la composition de S-Box et de fonctions linéaires.

Cryptanalyse d'un schéma de Feistel à un tour

Exercice

Décrire une attaque à **clairs connus** pour distinguer un schéma de Feistel à un tour d'une permutation aléatoire de $\mathbb{F}_2^{2n}$.

Cryptanalyse d'un schéma de Feistel à un tour

Réponse

Il suffit de remarquer que les n premiers bits du chiffré sont **toujours** les n derniers bits du clair, ce qui n'arrive **typiquement pas** pour une permutation aléatoire de $\mathbb{F}_2^{2n}$ sur une entrée aléatoire.

Cryptanalyse Feistel à deux tours

Exercice

Décrire une attaque à **clairs choisis** pour distinguer un schéma de Feistel à deux tours d'une permutation aléatoire de $\mathbb{F}_2^{2n}$.

Cryptanalyse Feistel à deux tours

Réponse

On tire uniformément L_0, L'_0 et X dans $\mathbb{F}_2^n$ et on construit les deux messages

$$m = (L_0 \,||\, X) \quad \text{et} \quad m' = (L'_0 \,||\, X),$$

dont on obtient les chiffrés

$$c = (L_2 \,||\, R_2) \quad \text{et} \quad c' = (L'_2 \,||\, R'_2).$$

On vérifie alors qu'on a **toujours**

$$L_2 \oplus L'_2 = L_0 \oplus L'_0$$

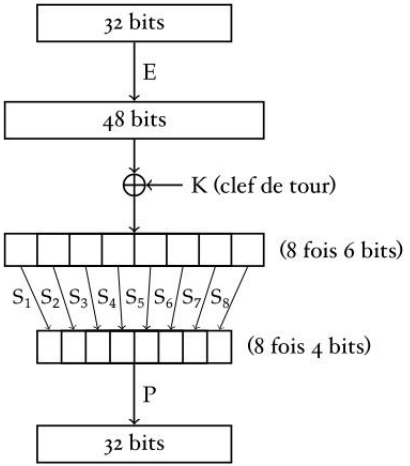
ce qui n'arrive **typiquement pas** pour une permutation aléatoire de $\mathbb{F}_2^{2n}$.

Un résultat théorique sur les schémas de Feistel à 3 tours

(M. Luby, C. Rackoff, 1988)

Si les fonctions de tours f_i sont des fonctions booléennes **aléatoires**, alors il n'existe pas de distingueur efficace pour un schéma de Feistel à 3 tours.

Un exemple : DES (*Data Encryption Standard*)



- Chiffrement standardisé en 1977
- Feistel à 16 tours sur des blocs de 64 bits.

Fonction de tour :

- $E : \mathbb{F}_2^{32} \to \mathbb{F}_2^{48}$ est linéaire.
- La clé de tour possède 48 bits, et est obtenue à partir d'une clé maître de 56 bits (=64 bits - 1 octet de redondance).

Faiblesses

Quel est le coût de l'attaque par recherche exhaustive sur DES ?

Faiblesses

- Espace des clé trop petit pour les standards de sécurité modernes.
- Cryptanalyse différentielle (Biham, Shamir 1991) : Retrouve la clé avec 2^{47} clairs choisis.
- Cryptanalyse linéaire (Matsui, 1993) : Retrouve la clé avec entre 2^{39} et 2^{43} clairs choisis.

- En 1998, *Electronic Frontier Foundations* construit une machine (le *DES Cracker*) à \$250,000 qui permet de retrouver une clé DES en **3 jours**.
- **Emergeance d'Internet** : En 1999, un réseau de 10^5 PC et le *DES cracker* permet de retrouver la clé en **22 heures**.

Itérer les DES

Pour augmenter la taille de l'espace des clés, on pourrait considérer un couple de deux clés maîtres $K = (K_1, K_2)$, et chiffrer deux fois :

$$E_K(m) \stackrel{\text{def}}{=} E_{K_2}(E_{K_1}(m)).$$

On espère alors obtenir un chiffré offrant une sécurité de $2n = 112$ bits.

Attaque de Rencontre au Milieu (*Meet in the Middle*)

Identité fondamentale

Pour un couple (M, C) de type $(\text{clair}, \text{chiffré})$, on a

$$D_{K_2}(C) = E_{K_1}(M)$$

- On calcule $E_{K_1}(M)$ et $D_{K_2}(M)$pour toutes les clés K_1 et K_2
- Dès qu'on trouve une collision, on a retrouvé $K = (K_1, K_2)$.

Coût total :

- $2^{56} + 2^{56} = 2^{57}$ évaluations de DES.
- **Remarque :** On a besoin de stocker 2^{56} paires $(\text{Clé}, \text{Chiffré})$, et de **rechercher** dedans...

Triple-DES

Double-DES n'apporte pas un gain significatif de sécurité par rapport à DES. À la place, pendant longtemps **Triple-DES** a été utilisé :

$$C = E_{K_3}(D_{K_2}(E_{K_1}(M)))$$

Exercice

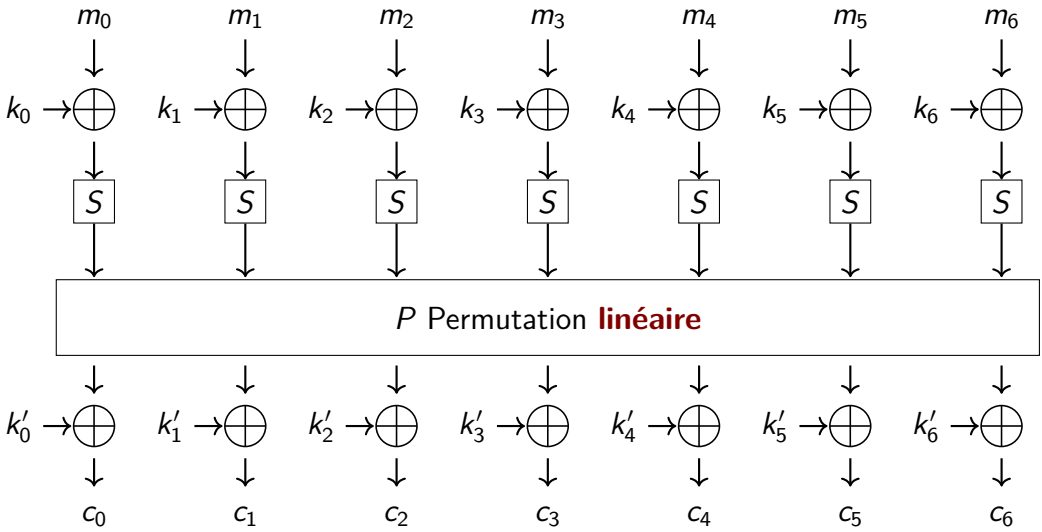
Montrer que la sécurité du triple-DES est d'au plus 112 bits. [a]

a. En ignorant les coûts non cryptographiques.

- Certains services de paiement en ligne utilisaient encore Triple-DES après 2010.
- Microsoft n'utilise plus Triple-DES que depuis Décembre 2018.

Réseaux de Substitutions-Permutations

Une fonction de tour **bijective**



AES : *Advanced Encryption Standard*

- Créé par Daemen et Rijmen en 1997 pour une compétition organisée par le NIST.
- Standardisé en 2001, et **très largement** utilisé aujourd'hui.
- Nom original : *Rijndael Cipher*.

AES opère sur des blocs de 128 bits, et trois variantes sont possibles :

- AES-128 : Clés de 128 bits, 10 tours.
- AES-192 : Clés de 192 bits, 12 tours.
- AES-256 : Clés de 256 bits, 14 tours.

Attaques sur AES, en 2024

AES avec $\leqslant 6$ tours : Complètement cassé.

Cryptanalyse de AES avec 6 tours

Improved Boomerang Attacks on 6-Round AES

Augustin Bariant[1,2], Orr Dunkelman[3], Nathan Keller[4], Gaëtan Leurent[2], and Victor Mollimard[3]

[1] ANSSI, Paris, France
augustin.bariant@ssi.gouv.fr
[2] Inria, Paris, France
gaetan.leurent@inria.fr
[3] Computer Science Department, University of Haifa, Haifa, Israel
orrd@cs.haifa.ac.il, victor.mollimard@gmail.com
[4] Department of Mathematics, Bar Ilan University, Ramat Gan, Israel
Nathan.Keller@biu.ac.il

- Connu pour être complètement cassé
- Toujours un sujet de recherche en 2024.

Cryptanalyse de AES avec 7 tours

New Key-Recovery Attack on Reduced-Round AES

Navid Ghaedi Bardeh[1,2] and Vincent Rijmen[3,4]

[1] Norwegian University of Science and Technology, Trondheim, Norway, navid.ghaedibardeh@gmail.com
[2] iagon, Oslo, Norway
[3] imec-COSIC KU Leuven, Leuven, Belgium, vincent.rijmen@kuleuven.be
[4] University of Bergen, Bergen, Norway

Table 1: Current best cryptanalysis of 7-round AES-128 in the secret-key model.

Attack	Rounds	Data	Time	Memory	Key schedule	Ref.
Impossible Differential	7	$2^{112.2}$	$2^{117.2}$	$2^{112.2}$	yes	[LDKK08]
Meet-in-the-Middle	7	2^{116}	2^{116}	2^{116}	yes	[DKS10]
Impossible Differential	7	$2^{105.1}$	2^{113}	$2^{74.1}$	yes	[BLNS18]
Impossible Differential	7	$2^{104.9}$	$2^{110.9}$	$2^{71.9}$	yes	[LP21]
Zero-Difference	7	$2^{110.2}$	$2^{110.2}$	$2^{110.2}$	no	**Section 5**
Meet-in-the-Middle	7	2^{97}	2^{99}	2^{98}	yes	[DFJ13]

Cryptanalyse de AES avec 8 tours

Improved Single-Key Attacks on 8-round AES-192 and AES-256*

Orr Dunkelman[1,2], Nathan Keller[2], and Adi Shamir[2]

[1] Computer Science Department
University of Haifa
Haifa 31905, Israel
orrd@cs.haifa.ac.il
[2] Faculty of Mathematics and Computer Science
Weizmann Institute of Science
P.O. Box 26, Rehovot 76100, Israel
{nathan.keller,adi.shamir}@weizmann.ac.il

$\approx 2^{172}$ bits de sécurité pour AES-192
$\approx 2^{177}$ bits de mémoire
ASIACRYPT 2010.

Cryptanalyse complète de l'AES (2015)

Improving the Biclique Cryptanalysis of AES

Biaoshuai Tao(✉) and Hongjun Wu(✉)

Nanyang Technological University, Singapore, Republic of Singapore
taob0001@e.ntu.edu.sg, wuhj@ntu.edu.sg

Abstract. Biclique attack is currently the only key-recovery attack on the full AES with a single key. Bogdanov *et al.* applied it to all the three versions of AES by constructing bicliques with size $2^8 \times 2^8$ and reducing the number of S-boxes computed in the matching phase. Their results were improved later by better selections of differential characteristics in the biclique construction. In this paper, we improve the biclique attack by increasing the biclique size to $2^{16} \times 2^8$ and $2^{16} \times 2^{16}$. We have a biclique attack on each of the following AES versions:

- AES-128 with time complexity $2^{126.13}$ and data complexity 2^{56},
- AES-128 with time complexity $2^{126.01}$ and data complexity 2^{72},
- AES-192 with time complexity $2^{189.91}$ and data complexity 2^{48}, and
- AES-256 with time complexity $2^{254.27}$ and data complexity 2^{40}.

Our results have the best time complexities among all the existing key-recovery attacks with data less than the entire code book.

Exploiter l'algorithme de diversification des clés

G. Leurent, C. Pernot - *New Representations of the AES Key Schedule* - EUROCRYPT 2021.

Dans les prochaines séances

- Cryptanalyse Linéaire
- Cryptanalyse Différentielle
- Cryptanalyse Algébrique