Analyse du Rayonnement Électromagnétique pour la Rétro-conception d'Algorithmes Secrets

GDR SOC-SIP

Denis Réal [1]

1 DGA Maîtrise de l'Information, 35 Bruz, France.

version : 17 mai 2011

Principe de Kerckhoffs

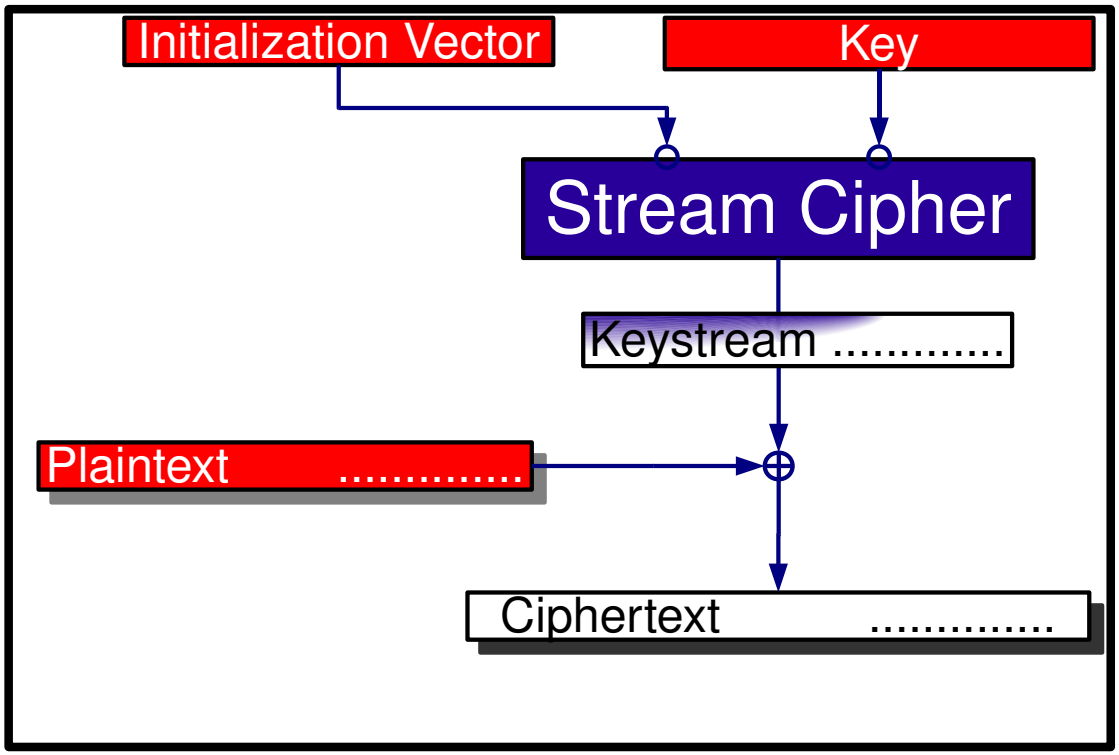
Il faut qu'il (le système) n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.

Cependant...

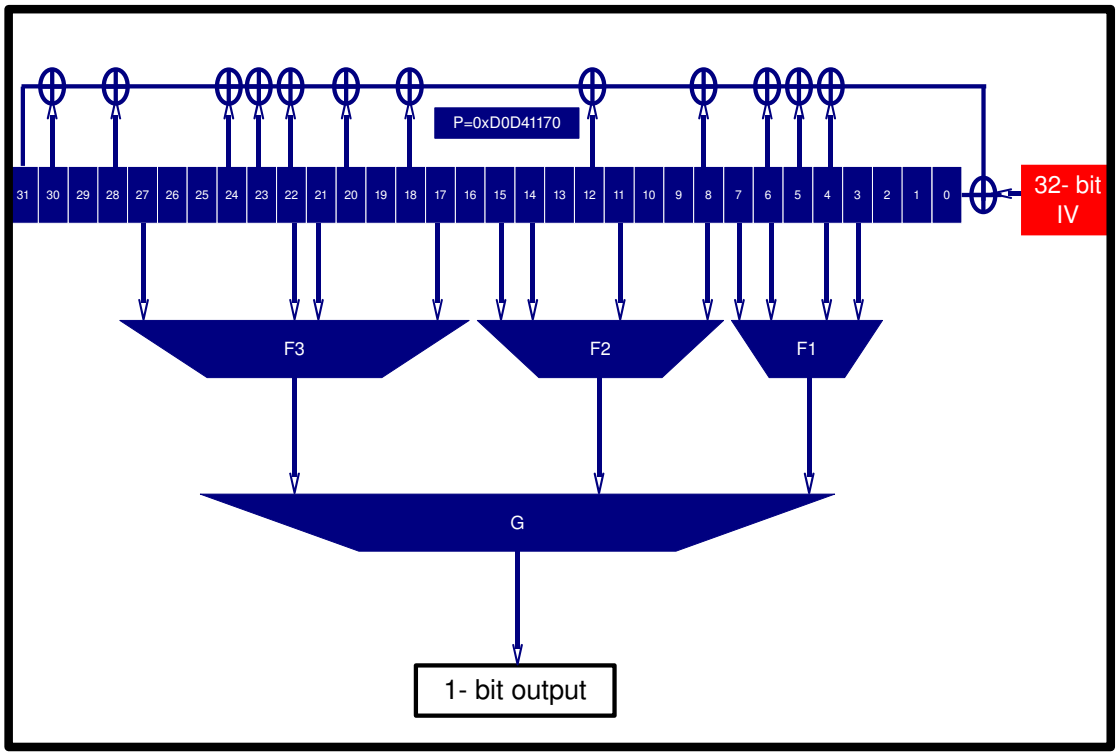
Le monde industriel fournit parfois des algorithmes propriétaires et dédiés à certaines applications.

Sommaire

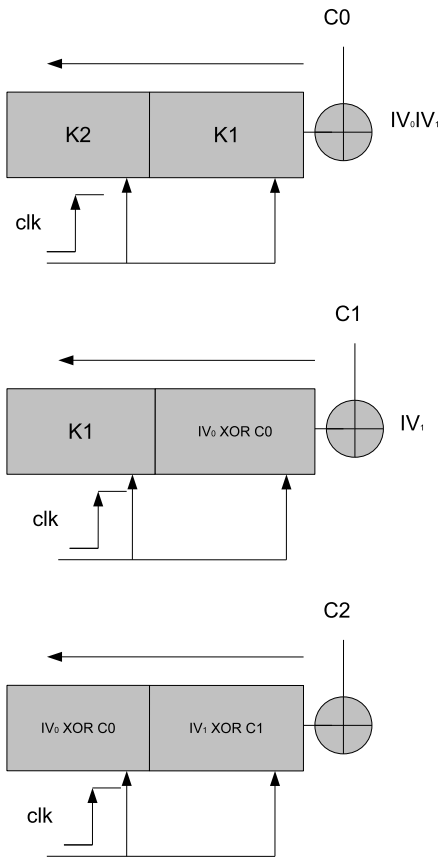
Chiffrement par flot



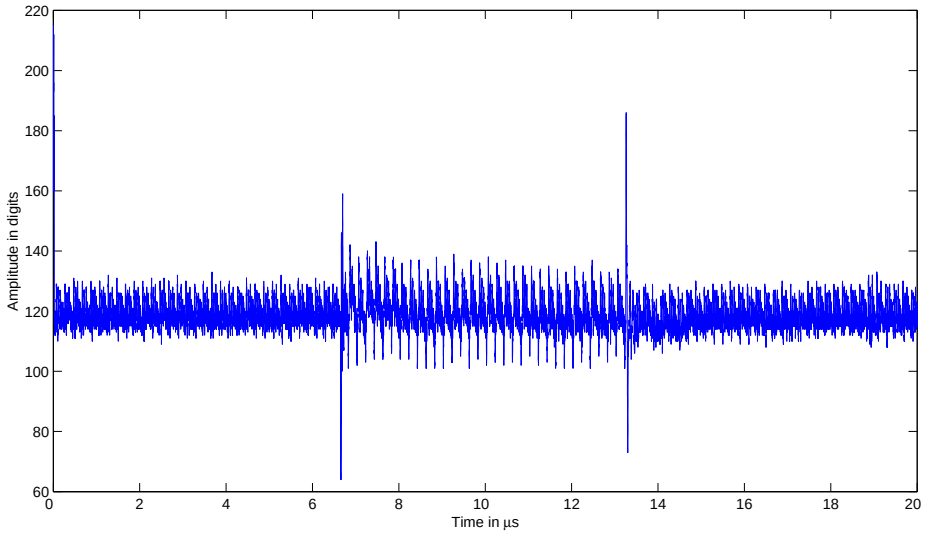
Design du LFSR



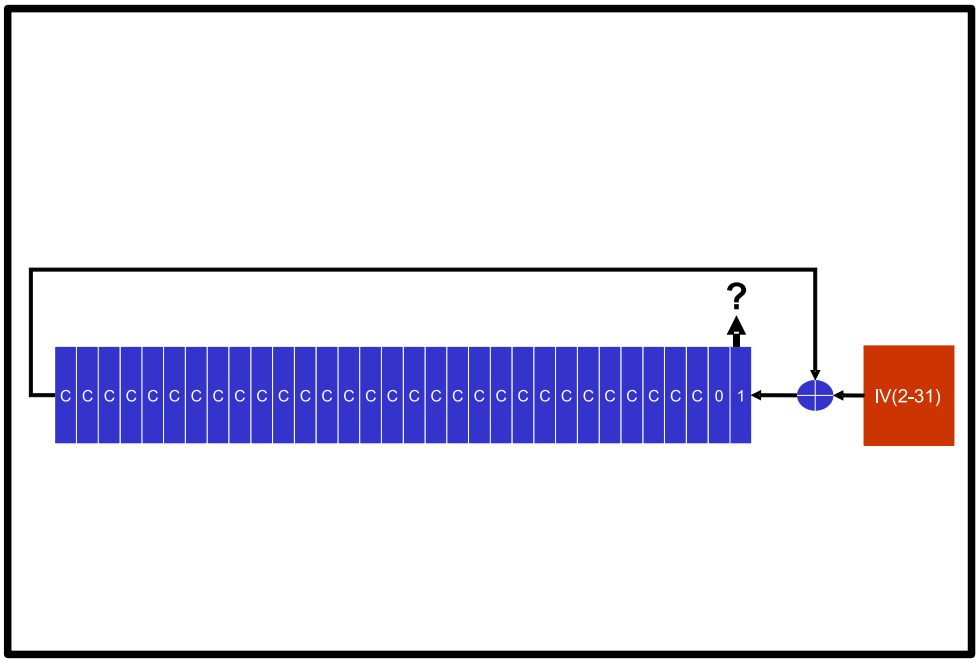
Hypothèse sur la radiation



Acquisition

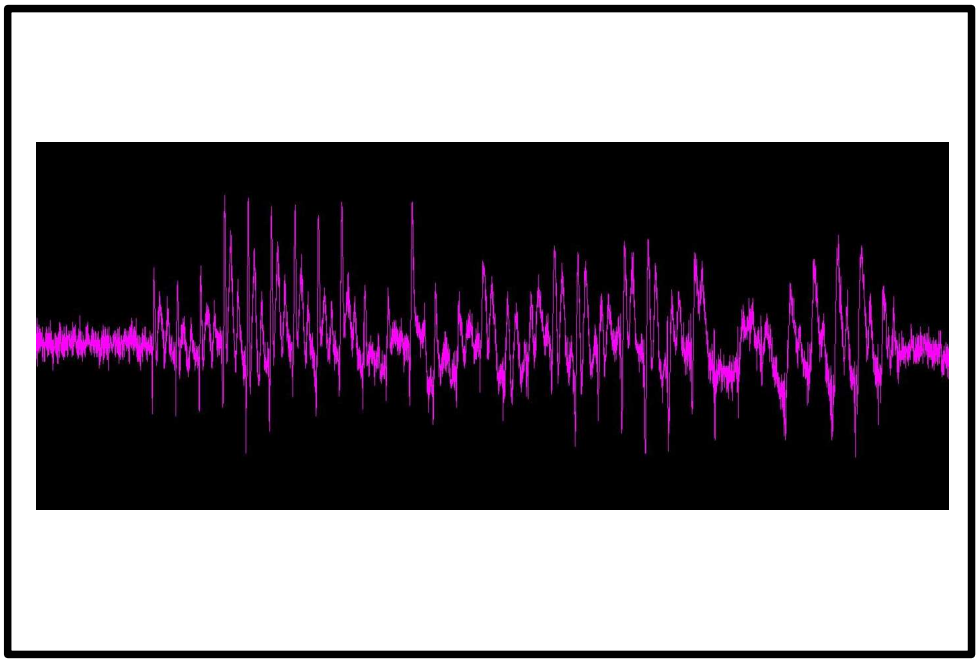


Rebouclage sur le bit 0 ?



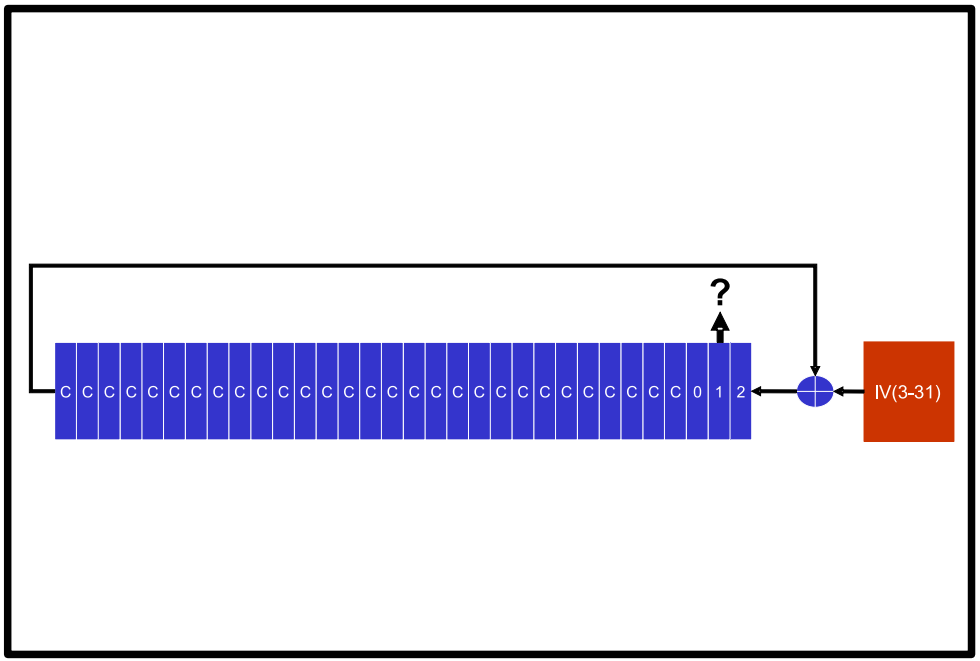
CEMA on $IV(1) \oplus IV(0)$

CEMA sur $IV(1) \oplus IV(0)$



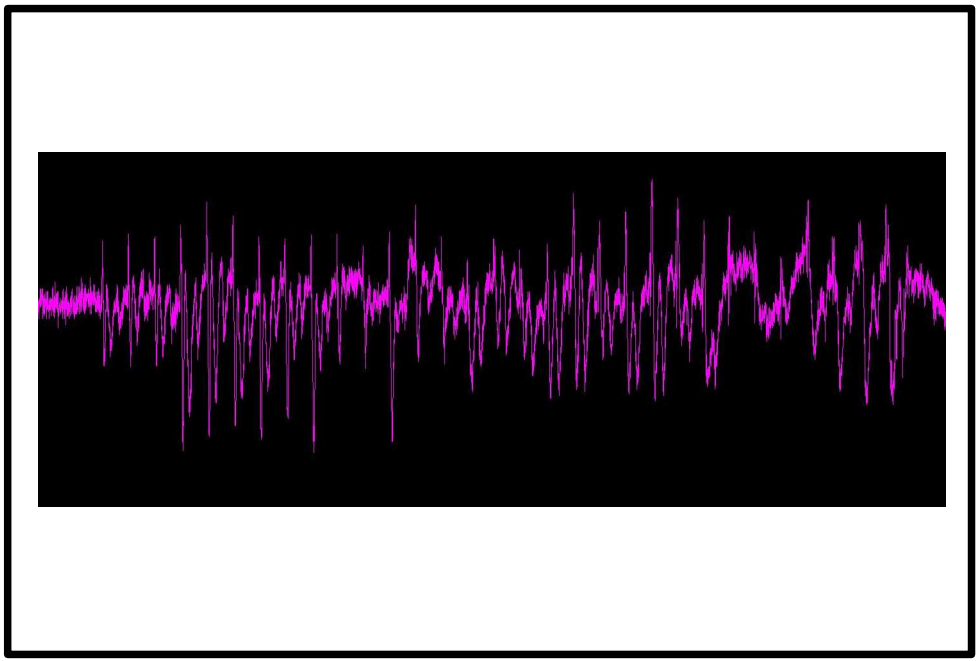
Pas de rebouclage sur le bit 0.

Rebouclage sur le bit 1 ?



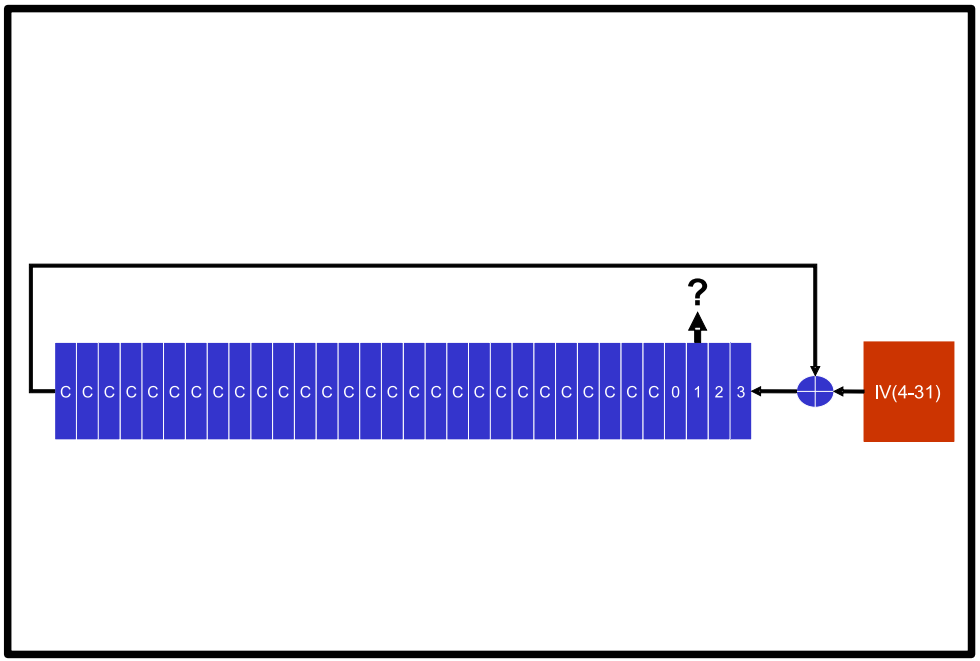
CEMA sur $IV(2) \oplus IV(1)$

CEMA sur $IV(2) \oplus IV(1)$



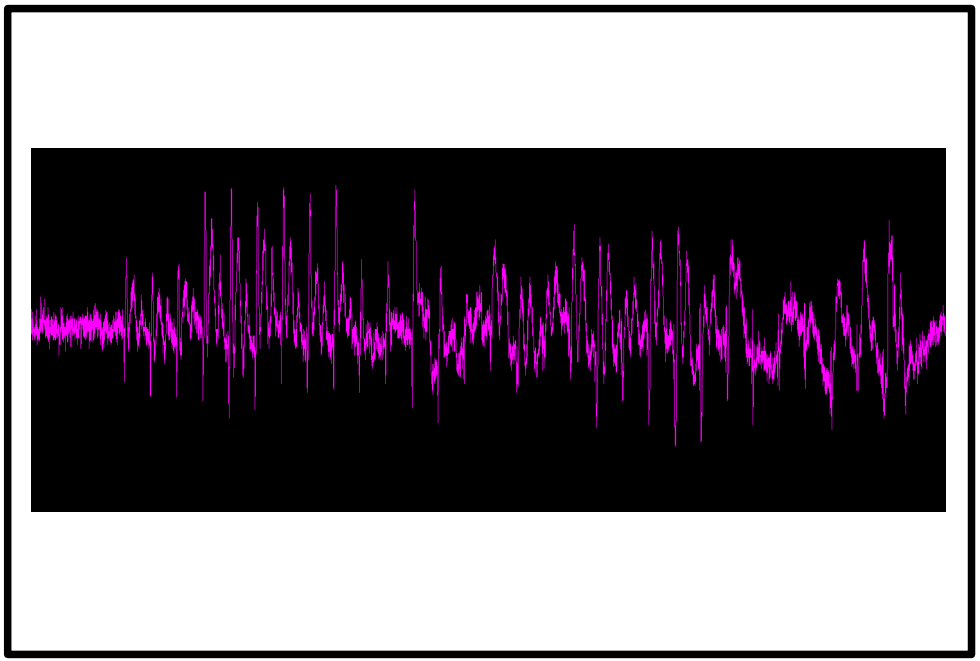
Pas de rebouclage sur le bit 1.

Rebouclage sur le bit 2 ?



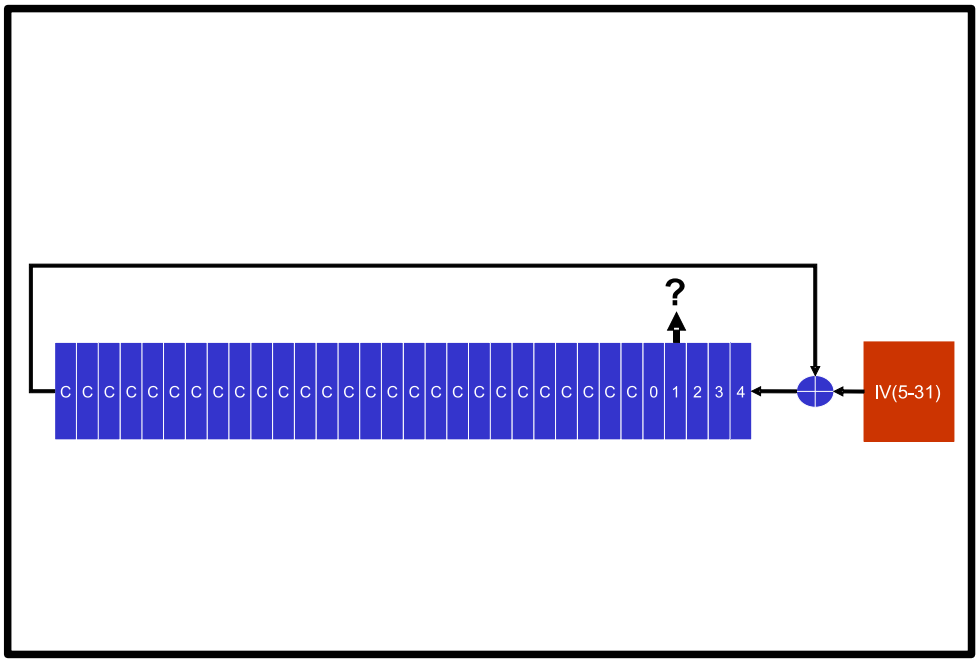
CEMA sur $IV(3) \oplus IV(2)$

CEMA sur $IV(3) \oplus IV(2)$



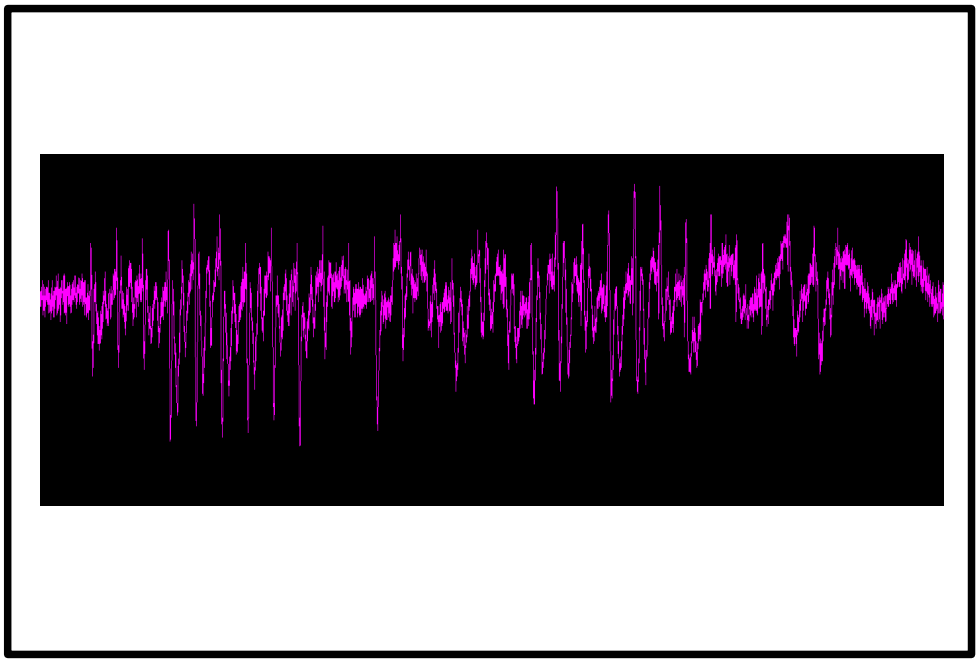
Pas de rebouclage sur le bit 2.

Rebouclage sur le bit 3 ?



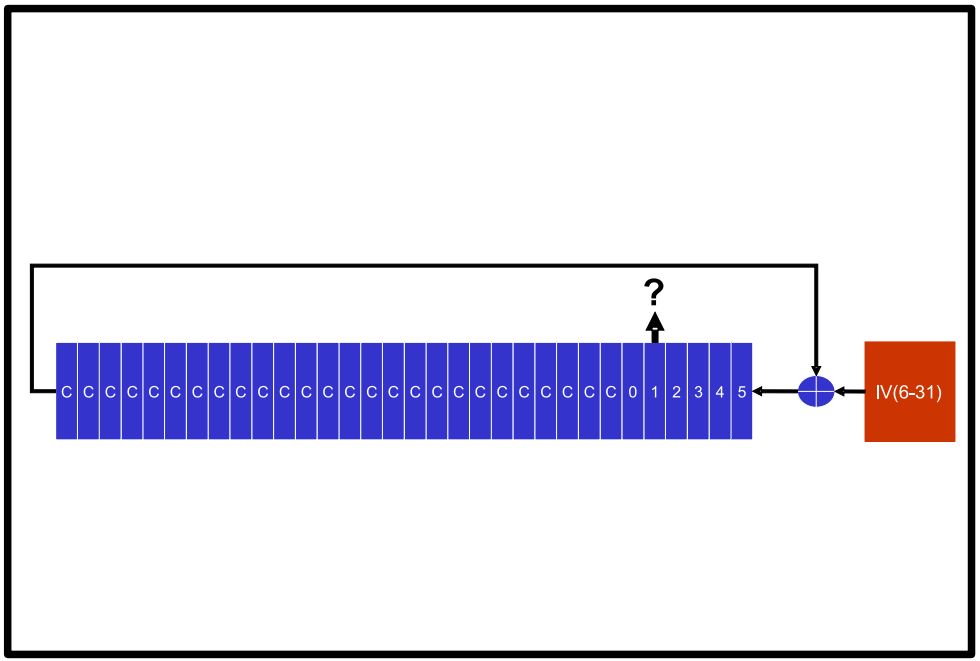
CEMA sur $IV(4) \oplus IV(3)$

CEMA sur $IV(4) \oplus IV(3)$



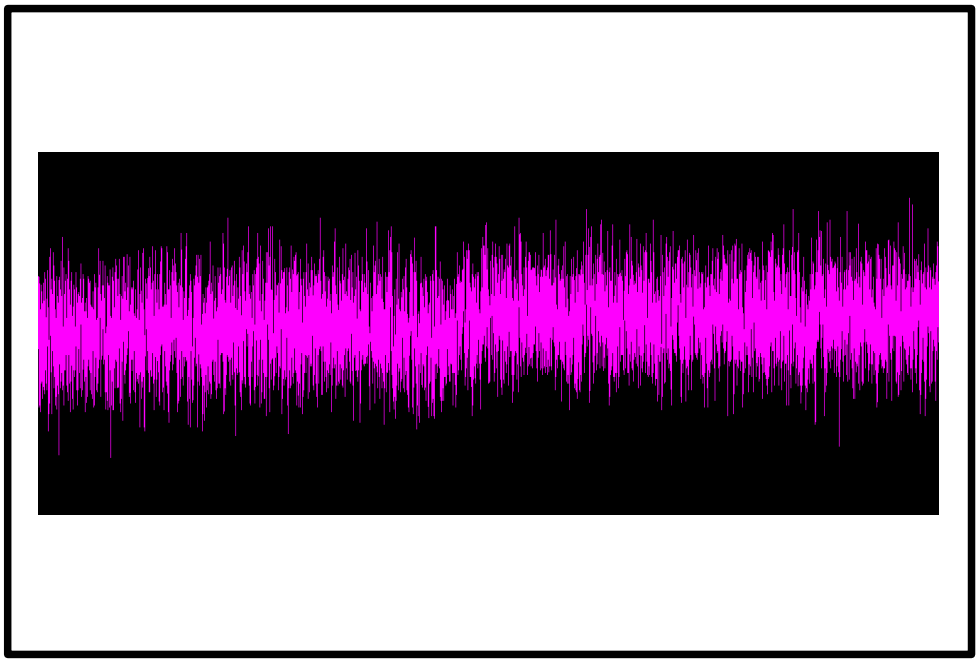
Pas de rebouclage sur le bit 3.

Rebouclage sur le bit 4 ?



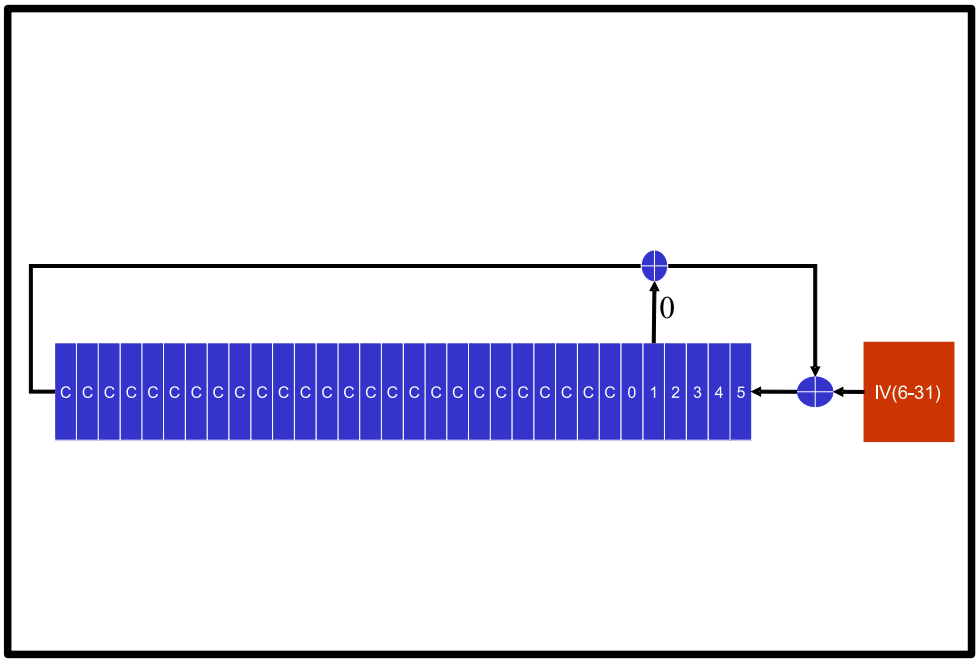
CEMA sur $IV(5) \oplus IV(4)$

CEMA sur $IV(5) \oplus IV(4)$



Rebouclage possible sur le bit 4.

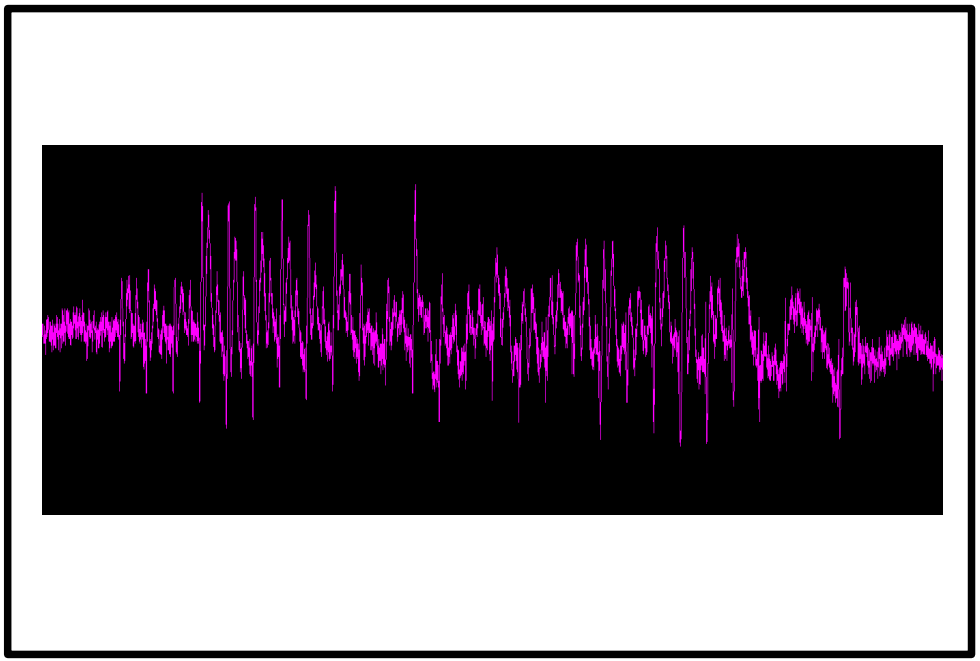
Confirmation du rebouclage sur le bit 4



CEMA sur $IV(5) \oplus IV(4) \oplus IV(0)$

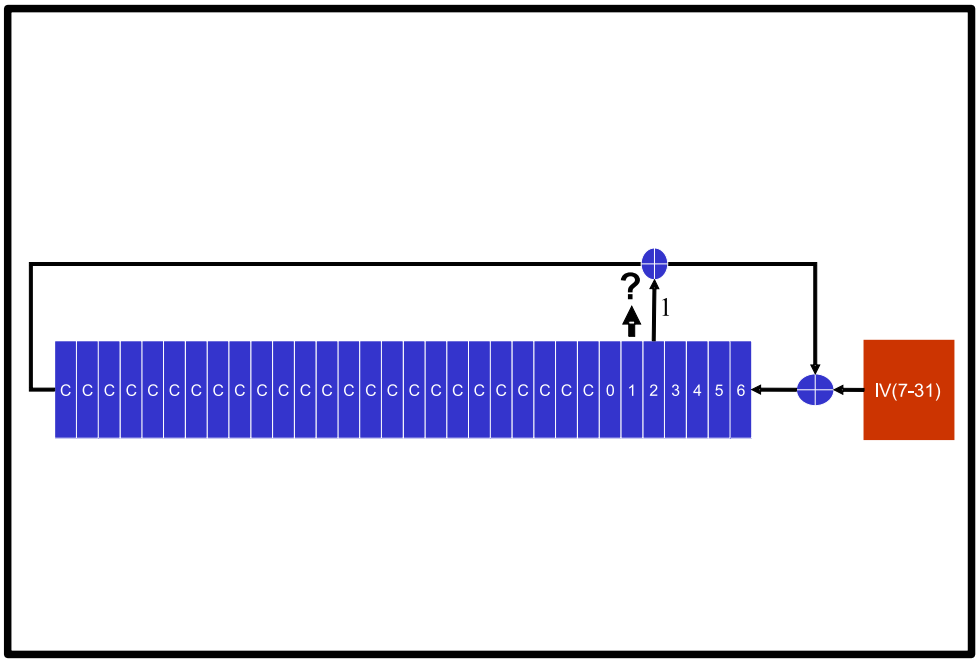
MINISTÈRE DE LA DÉFENSE
DGA

CEMA sur $IV(5) \oplus IV(4) \oplus IV(0)$



Rebouclage sur le bit 4.

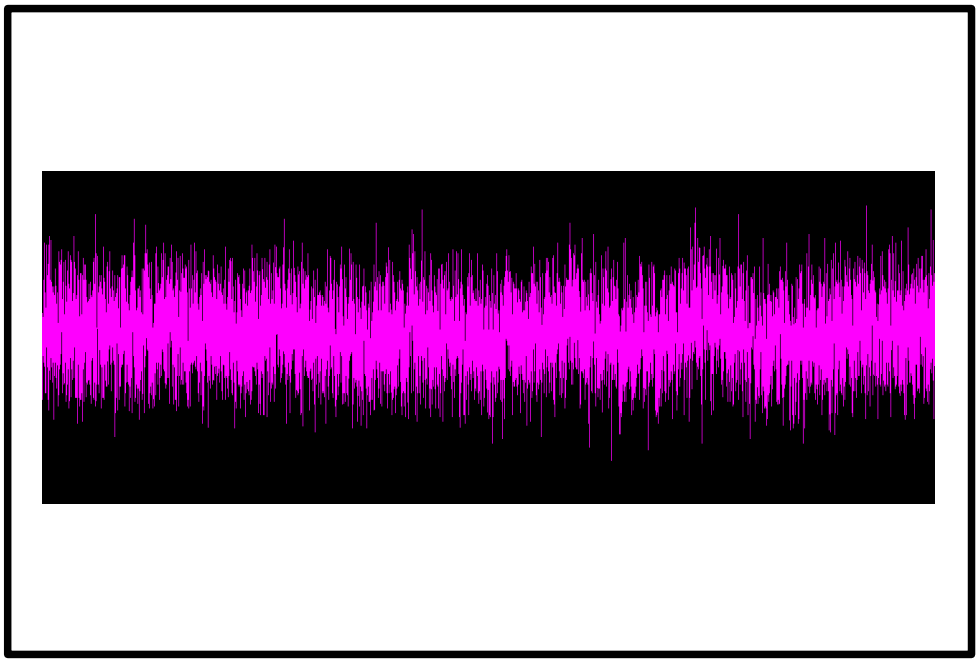
Rebouclage sur le bit 5 ?



CEMA sur $IV(6) \oplus IV(5) \oplus IV(1)$

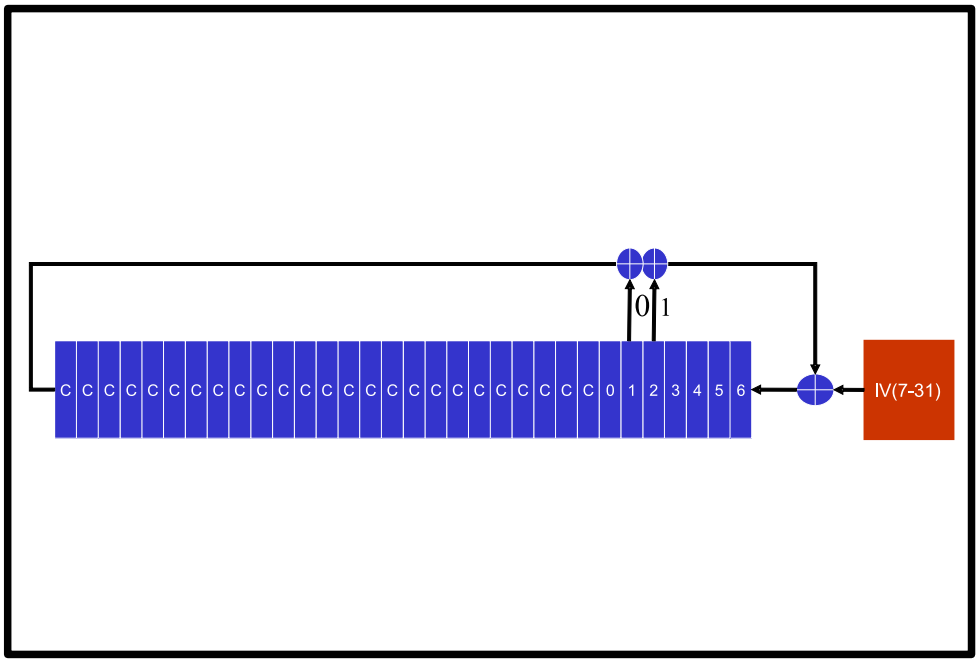
MINISTÈRE DE LA DÉFENSE
DGA

CEMA sur $IV(6) \oplus IV(5) \oplus IV(1)$



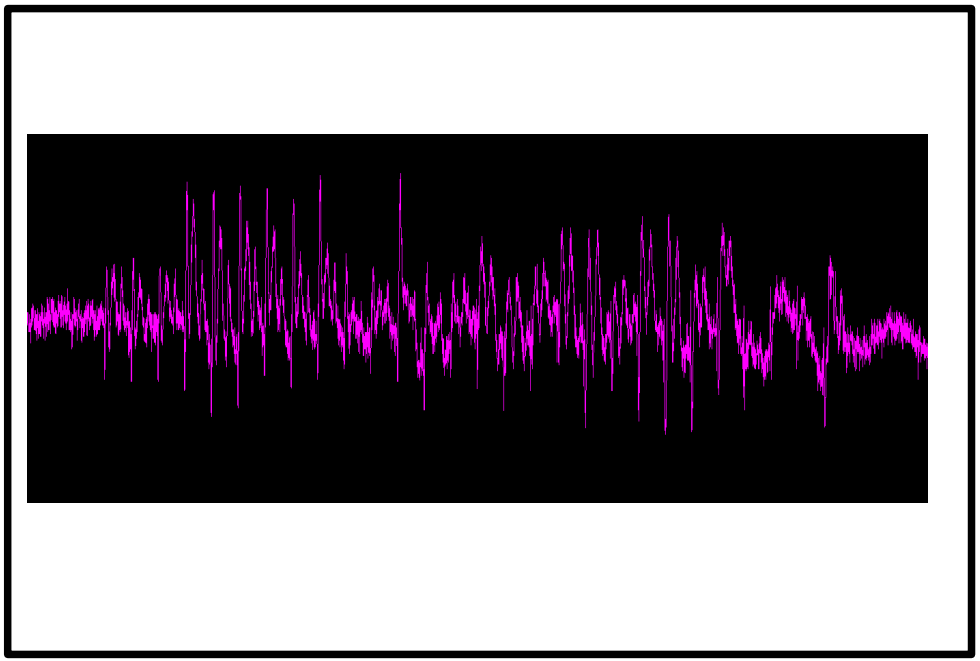
Rebouclage possible sur le bit 5.

Confirmation du rebouclage sur le bit 5



CEMA sur $IV(6) \oplus IV(5) \oplus IV(1) \oplus IV(0)$

CEMA sur $IV(6) \oplus IV(5) \oplus IV(1) \oplus IV(0)$



Rebouclage sur le bit 5.

Conclusion sur la recherche du polynome

Figure 1: CEMA with a right assumption

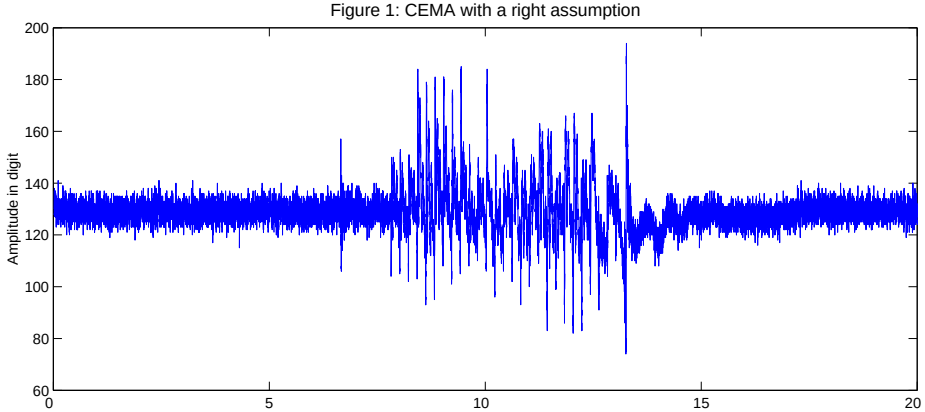
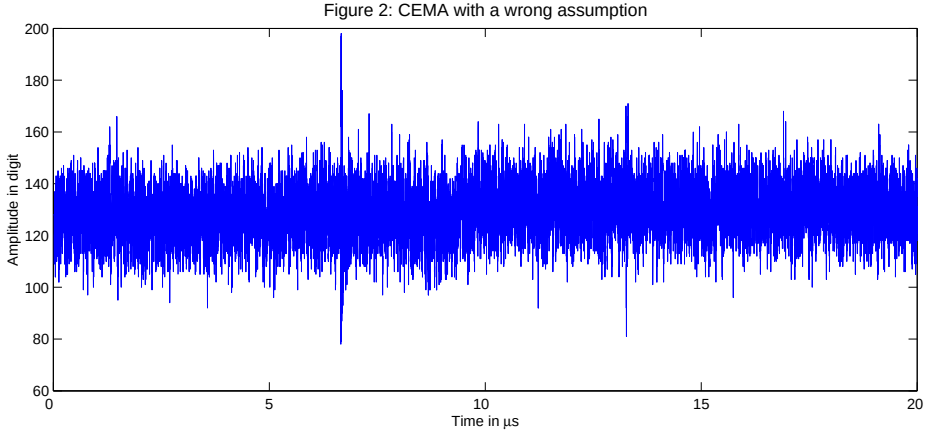


Figure 2: CEMA with a wrong assumption



Sommaire

Inversion de la Signature

Figure 1: CEMA with reversed signature

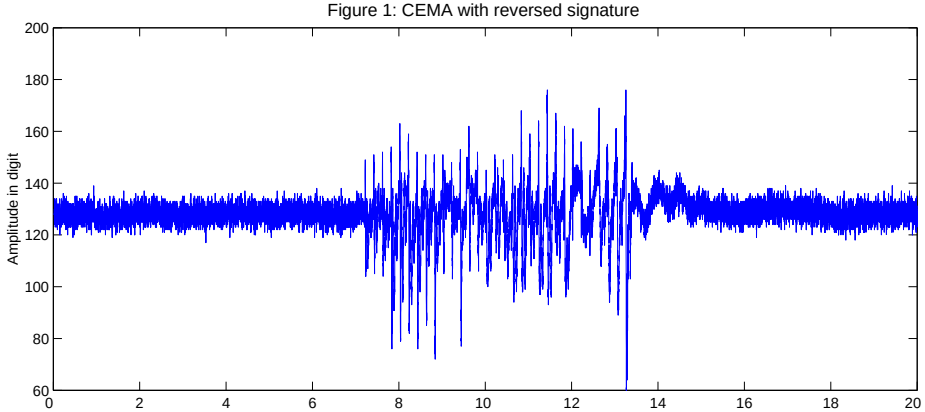
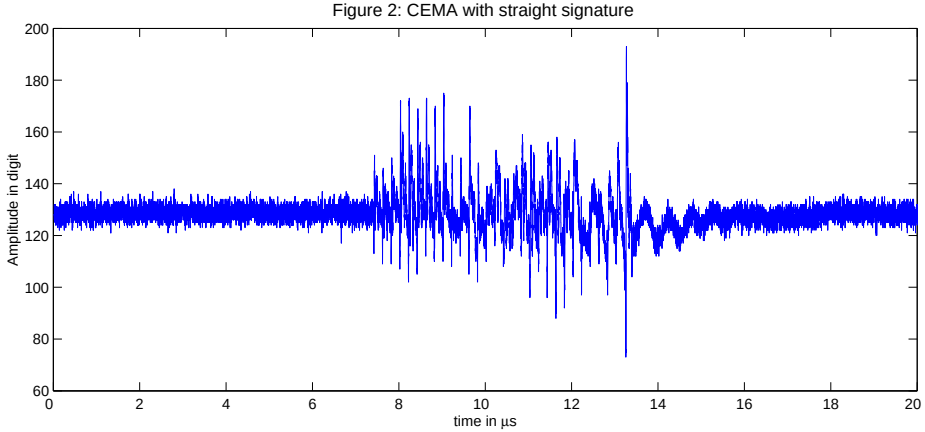


Figure 2: CEMA with straight signature



Sommaire

Conclusion

Attaque SCARE

- Polynôme du LFSR.
- Clé.

Améliorations

- Fonctions non linéaires.

Conclusion

Attaque SCARE

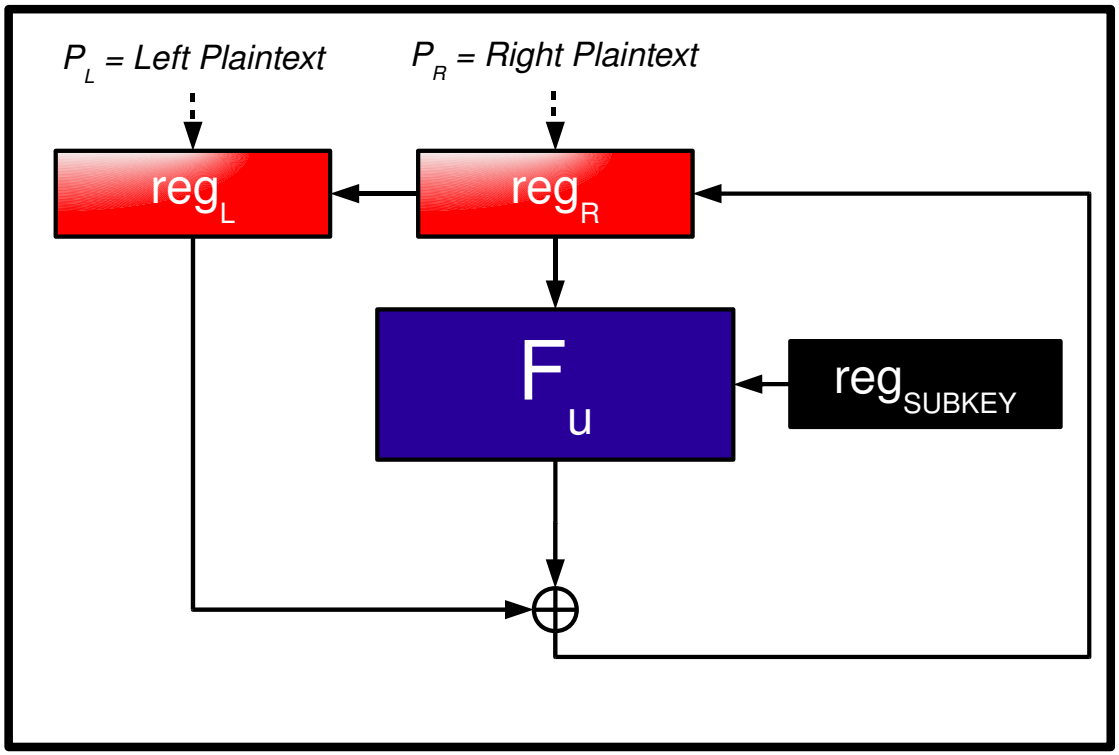
- Polynôme du LFSR.
- Clé.

Améliorations

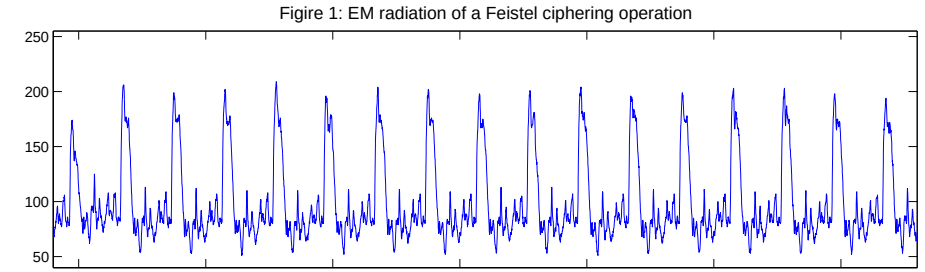
- Fonctions non linéaires.

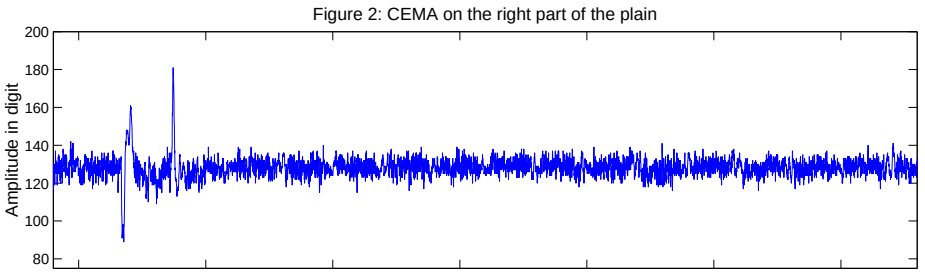
Sommaire

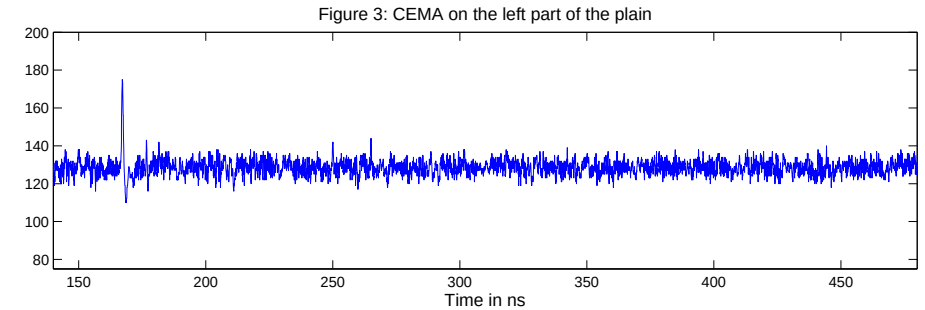
Hypothèse sur le schéma de Feistel



Identification du schéma par SCA







SCA pour deviner la sortie à un tour de la fonction de Feistel

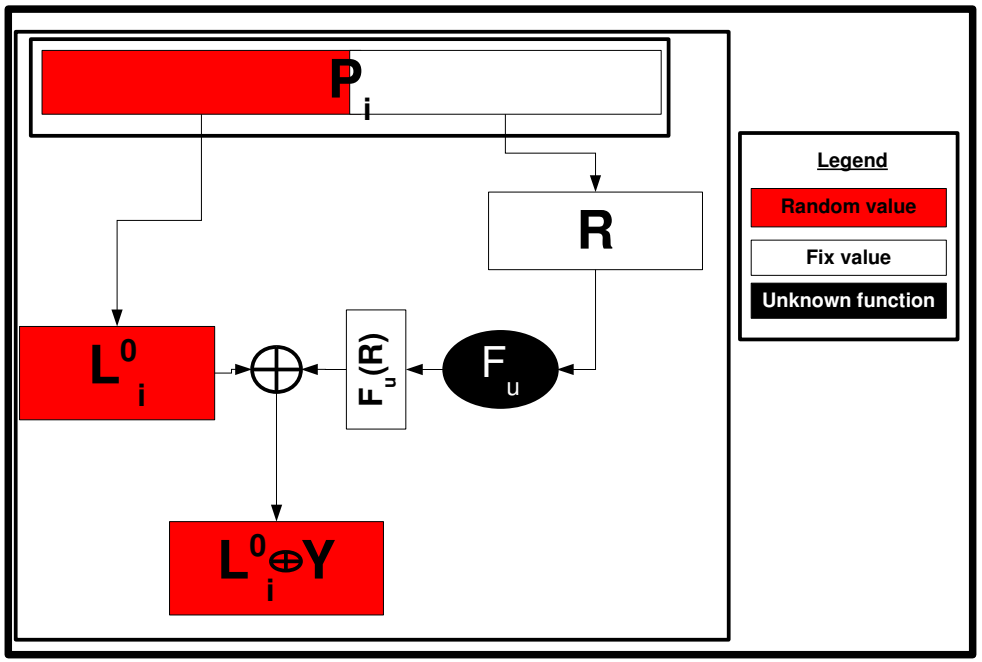
attaque par SCA à messages choisis

- N opérations de chiffrement.
- F_u la fonction Feistel.
- Les messages clairs $P_i = L_i||R$ for $i < N$.
- Soit $Y = F_u(R)$.
- La sortie droite du 1^{er} tour : $R_i^1 = L_i \oplus Y$.

attaque par SCA à messages choisis

- R_i^1 écrase R.
- Le nombre de changement de bits mini pour $R_i^1 = R$.
- Le nombre de changement de bits mini pour $L_i = R \oplus Y$.

SCA pour deviner la sortie à un tour de la fonction de Feistel



SCA pour deviner la sortie à un tour de la fonction de Feistel

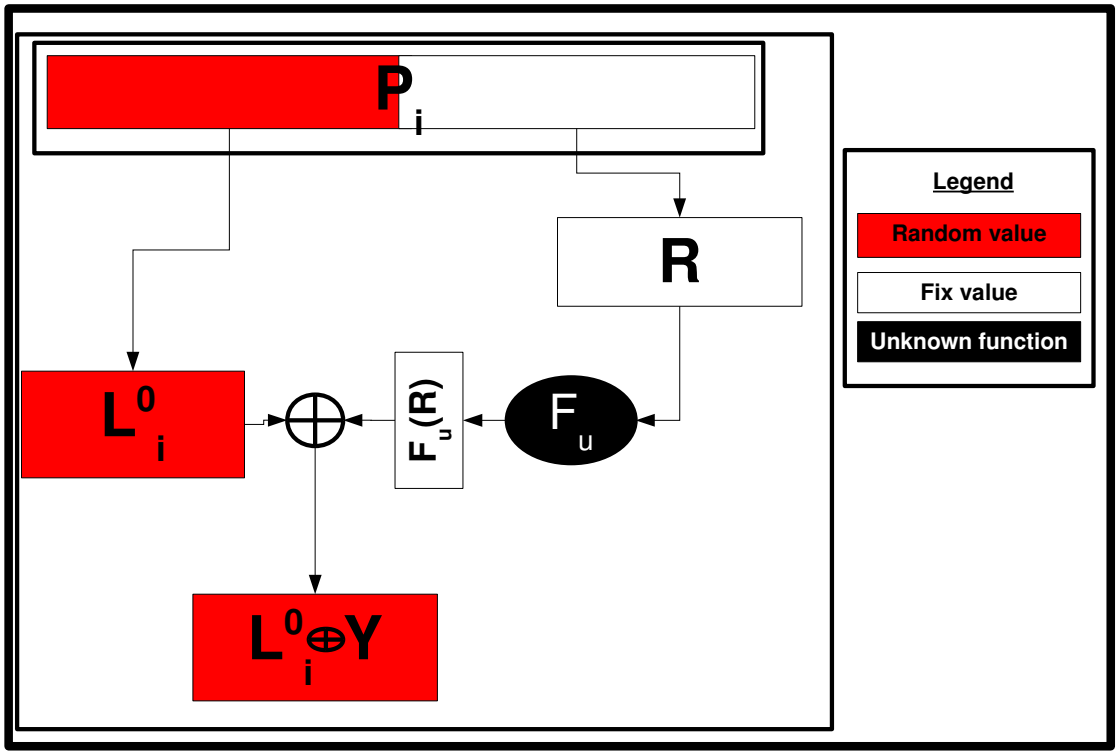
Le nombre de changement de bits est minimal pour $L_i = R \oplus Y$

- Relation sur 32 pour un DES.
- Problème est réduit à 4 bits de contrainte.

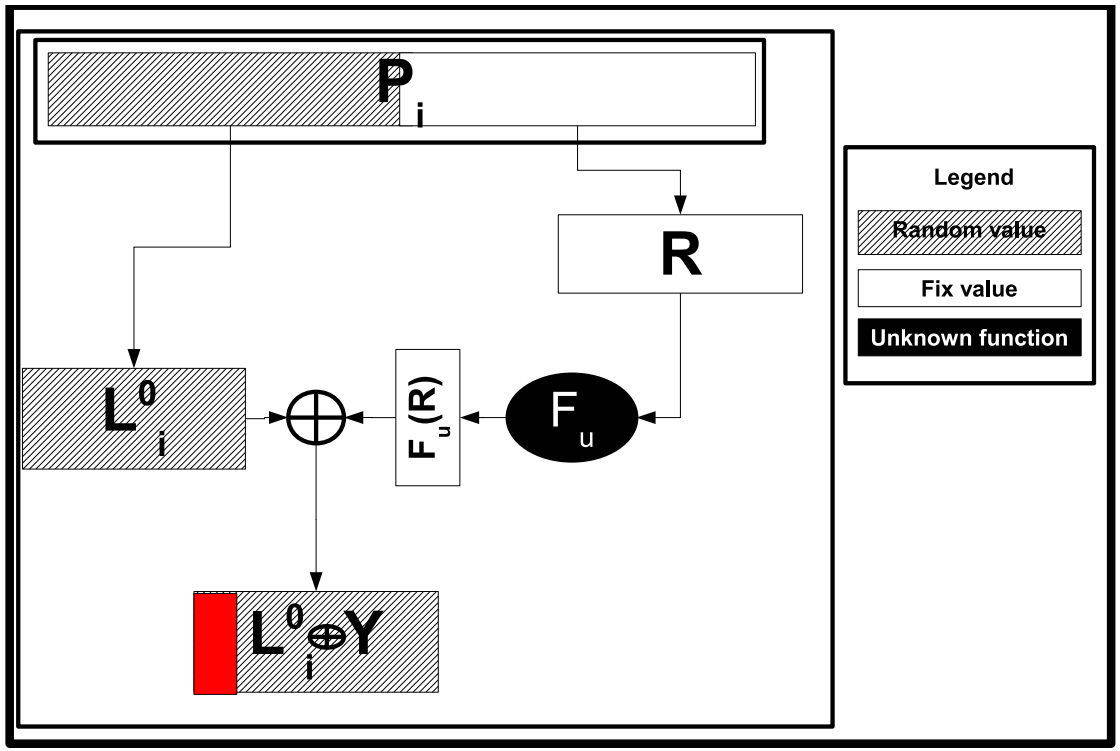
La strategie SCA

- Prendre un pool de clairs P_i comme défini avant.
- Faire une hypothèse sur $Y_{0..3}$.
- Faire une CPA $(L_i \oplus Y \oplus R)_{0..3}$.
- Comparer les 16 traces EM moyenne.

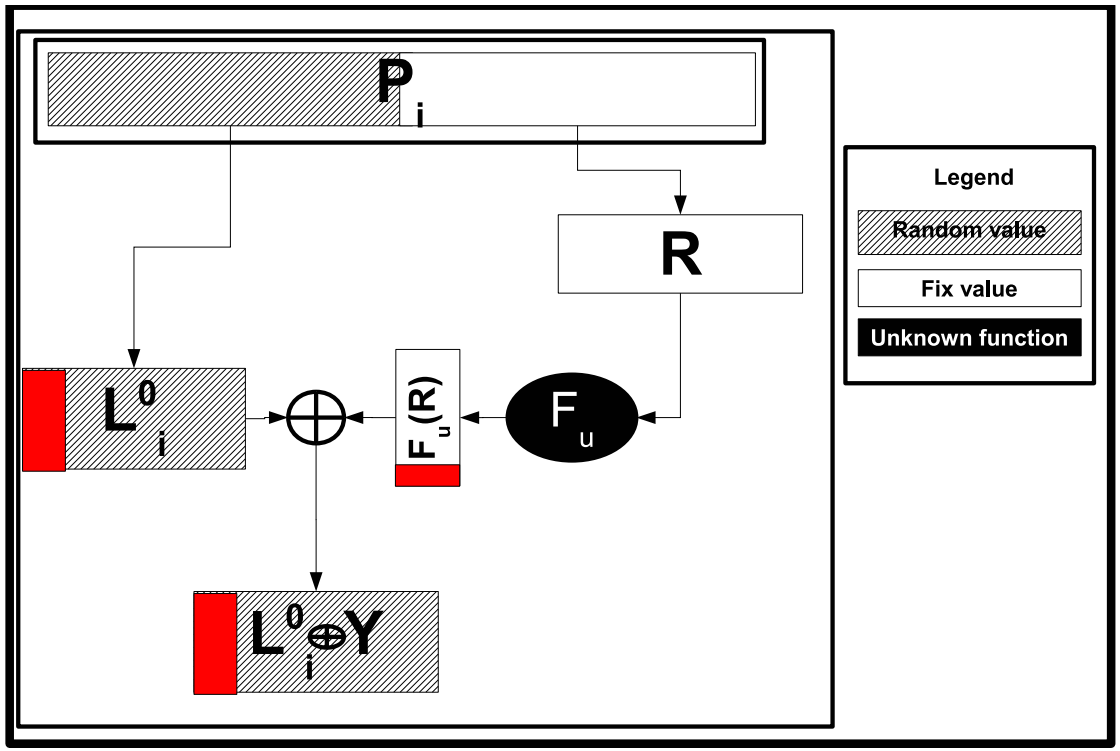
SCA pour deviner la sortie à un tour de la fonction de Feistel



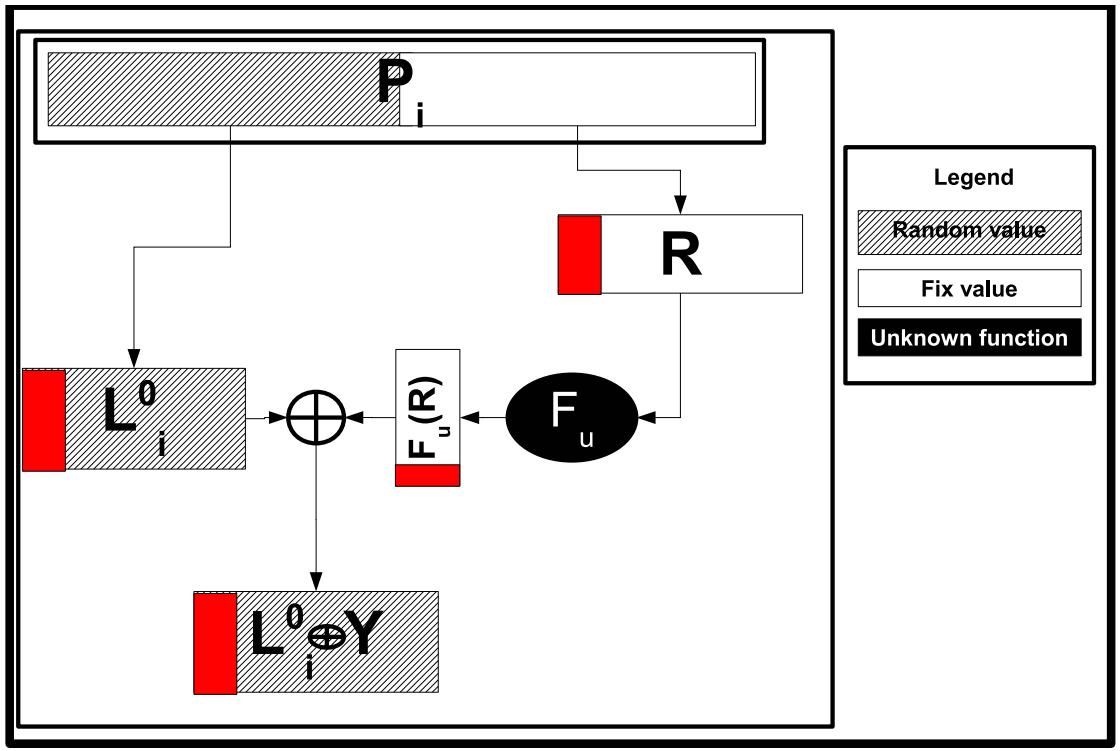
SCA pour deviner la sortie à un tour de la fonction de Feistel



SCA pour deviner la sortie à un tour de la fonction de Feistel



SCA pour deviner la sortie à un tour de la fonction de Feistel



SCA pour deviner la sortie à un tour de la fonction de Feistel

Figure 1: EM radiation during a Feistel scheme encryption

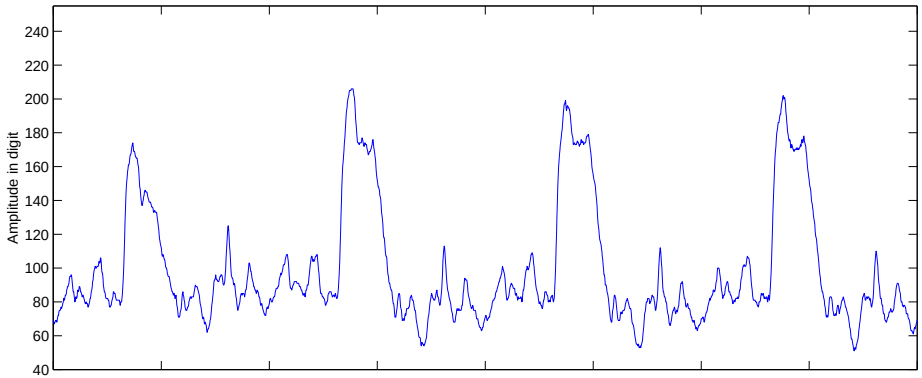
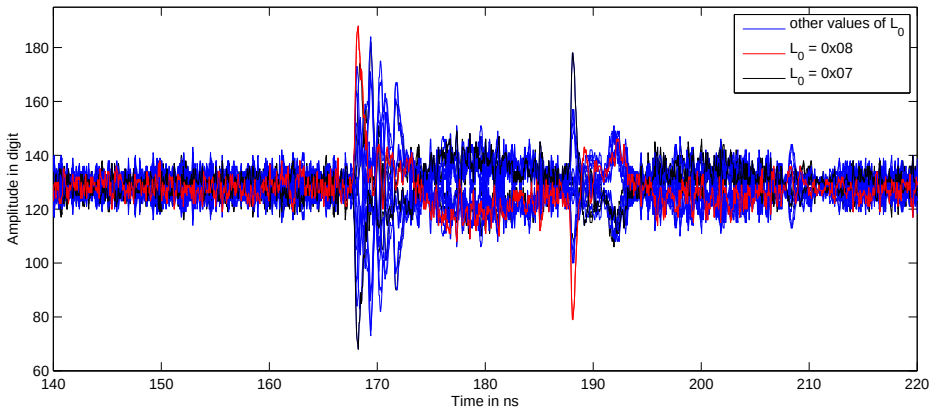


Figure 2: 16 CEMAs for the 16 possible values of L_0



MINISTÈRE DE LA DÉFENSE
DGA

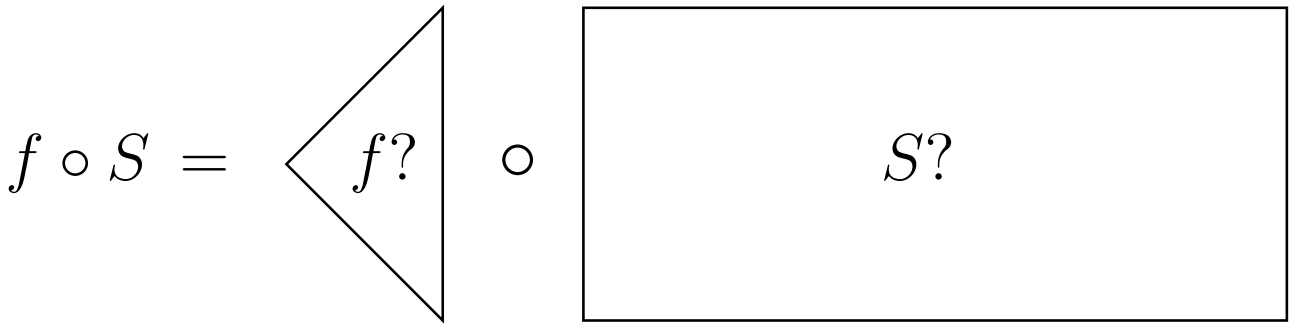
Sommaire

Attaque par Interpolation

$$F_u(R) = Y$$

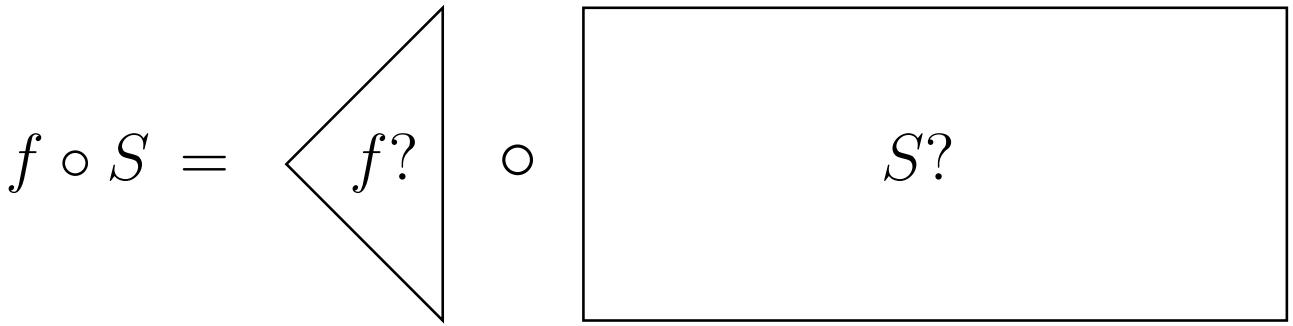
- Attaque par Interpolation.
- Directement dérivée de l'attaque par Interpolation sur les chiffrements blocs de Jakobsen et Knudsen.

Attaque sur des schémas généralement utilisés



Pour chaque permutation ϕ des lignes de S, $f \circ \phi^{-1}$ et $\phi \circ S$ sont une solution alternative.

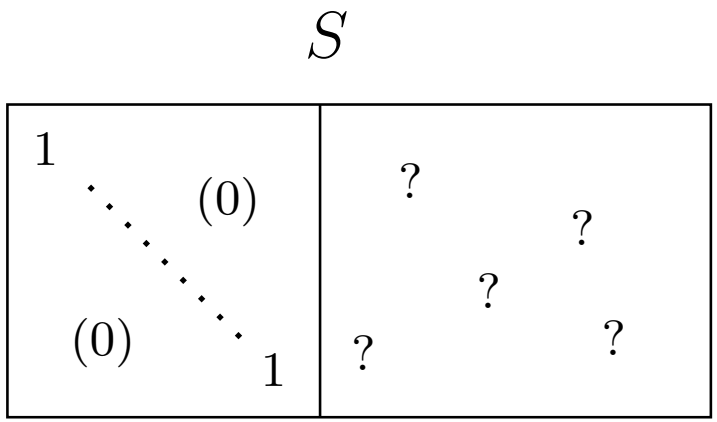
Attaque sur des schémas généralement utilisés



Pour chaque permutation ϕ des lignes de S, $f \circ \phi^{-1}$ et $\phi \circ S$ sont une solution alternative.

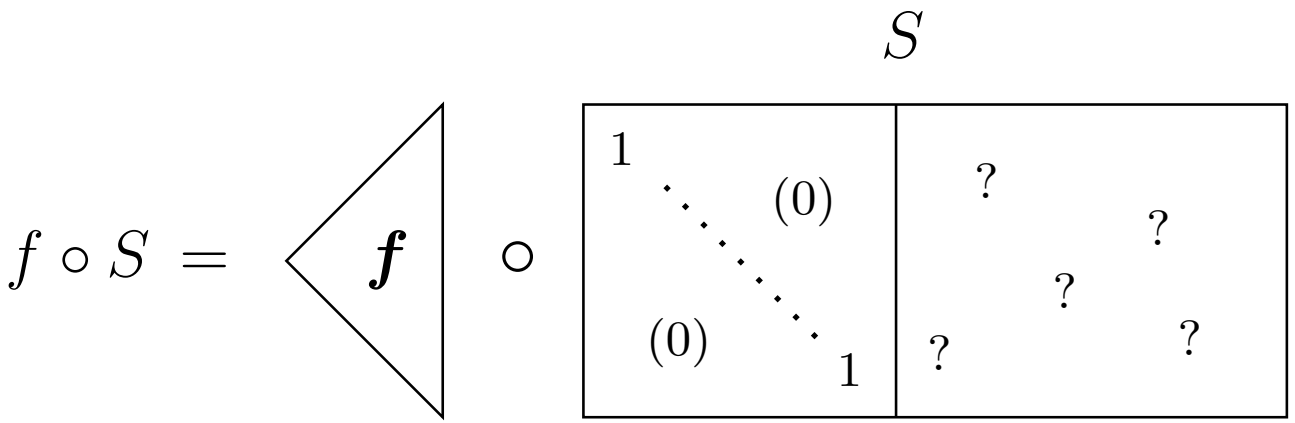
Attaque sur des schémas généralement utilisés

$$f \circ S = \boldsymbol{f} \circ$$



$2^d + (n-d)d$ entrées-sorties choisies et $2^{3d} + (n-d)2^d$ opérations. Pour $n = 64$ et $d = 8$, $2^{9.5}$ chiffrement et 2^{24} opérations.

Attaque sur des schémas généralement utilisés



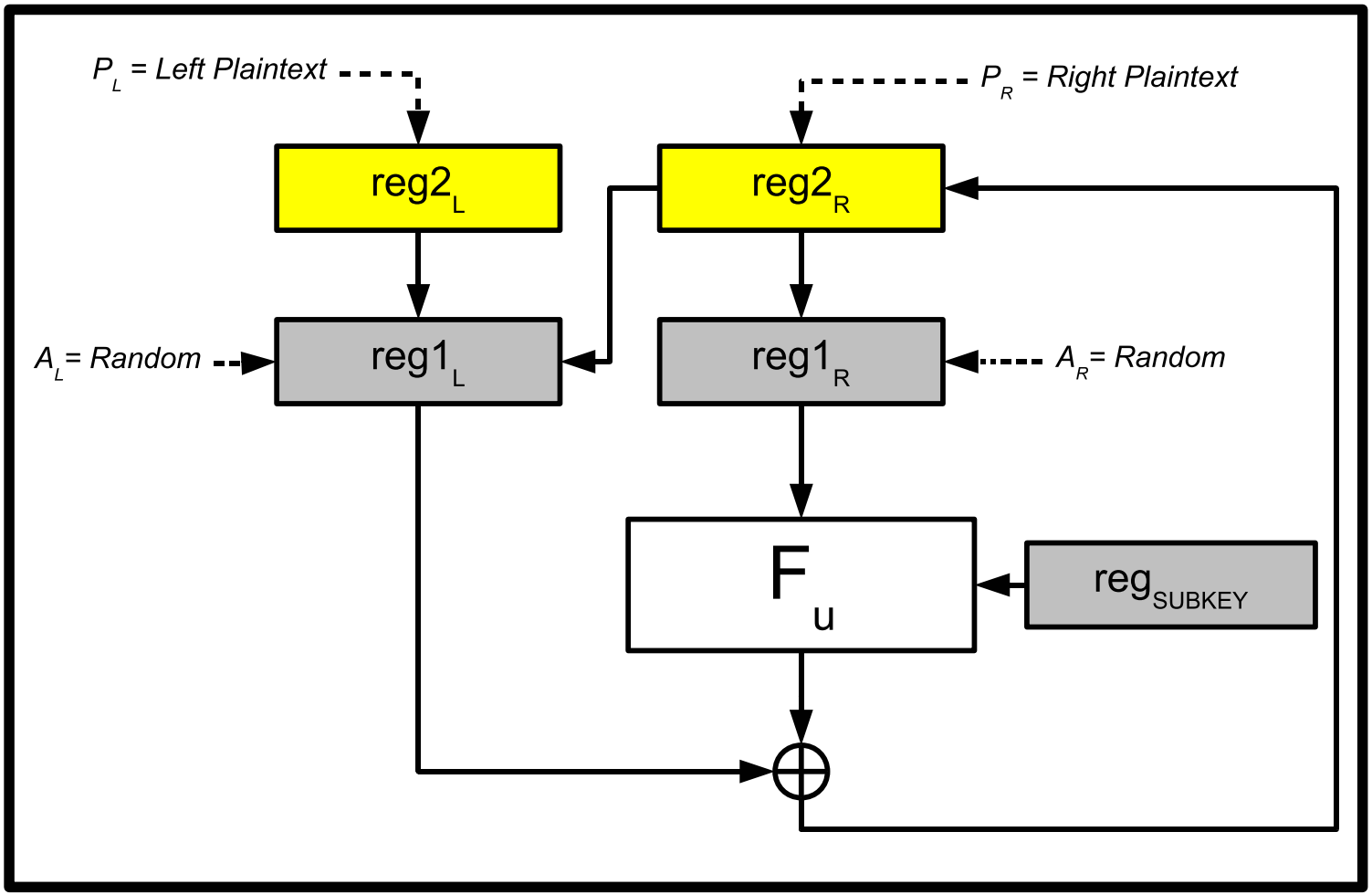
$2^d + (n-d)d$ entrées-sorties choisies et $2^{3d} + (n-d)2^d$ opérations. Pour $n = 64$ et $d = 8$, $2^{9.5}$ chiffrement et 2^{24} opérations.

Sommaire

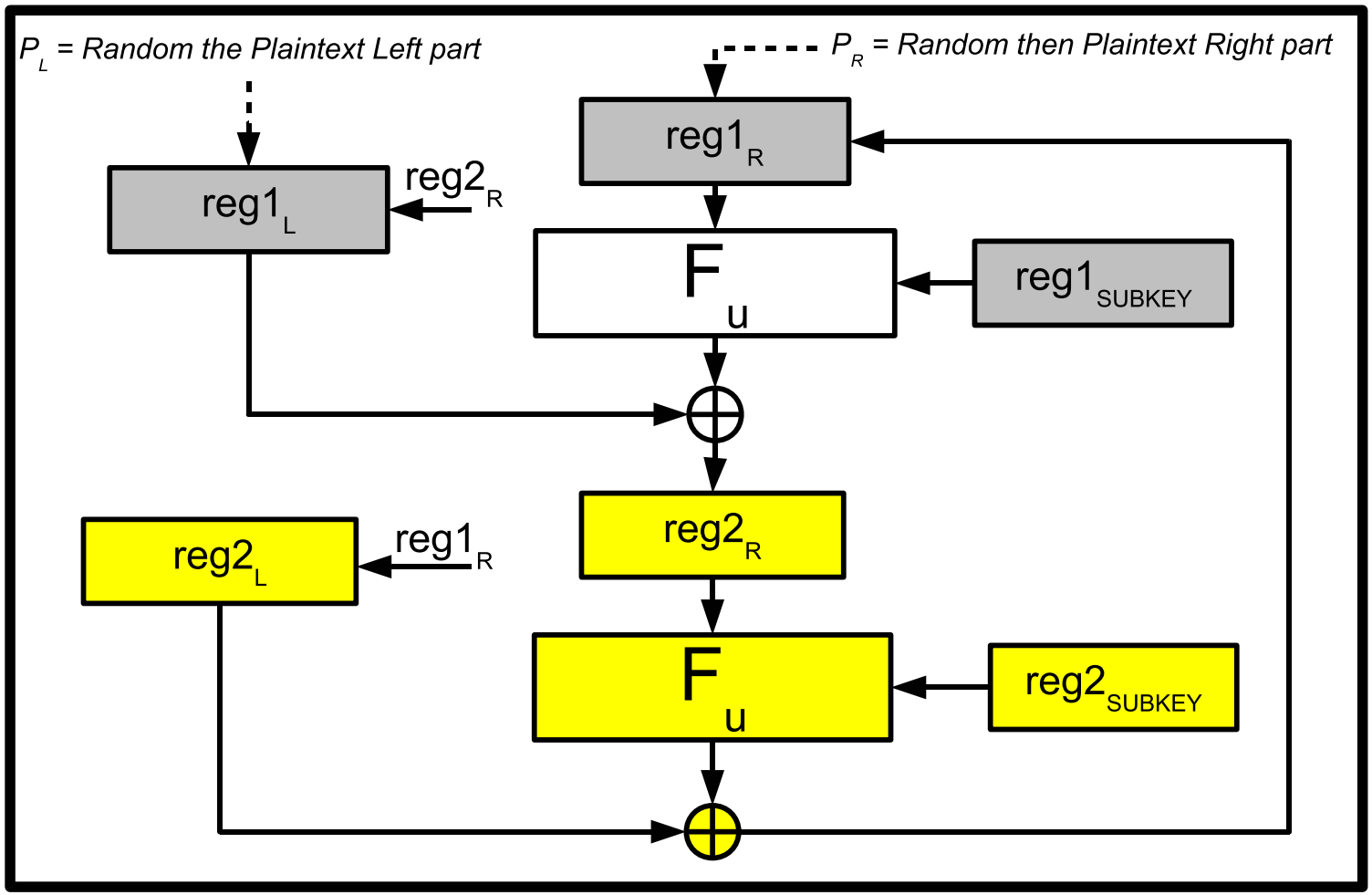
Principle du modèle du rail d'alimentation

- Le courant consommait durant un changement d'état est supérieur à la dissipation statique.
- SCA est basée sur la connaissance de la première valeur du registre R.
- Pré charger R avec un aléa avant d'écrire une valeur dépendant du secret.

Contre-mesure avec le modèle du rail d'alimentation



Contre-mesure avec le modèle du rail d'alimentation



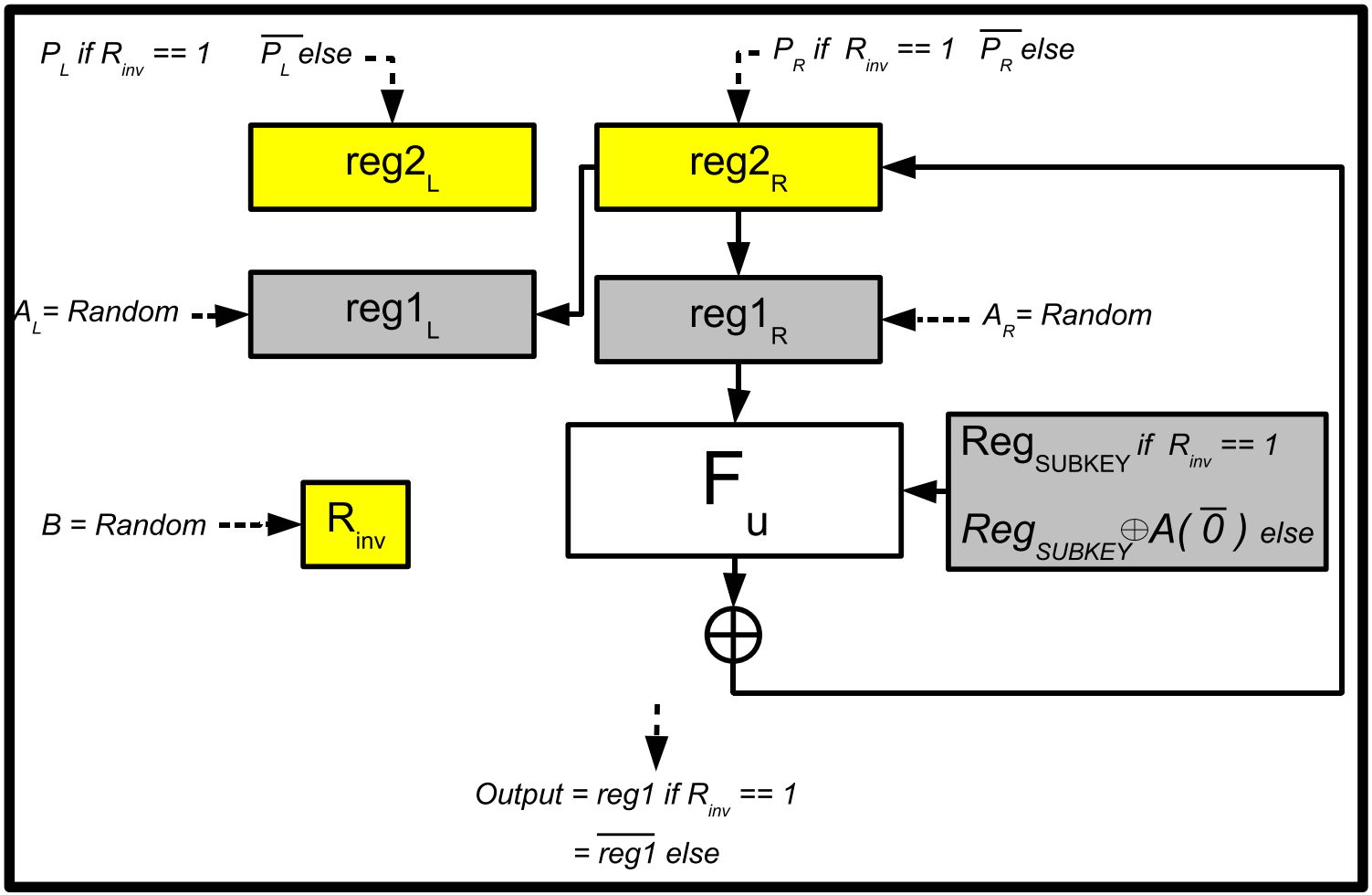
MINISTÈRE DE LA DÉFENSE
DGA

Contre-mesure améliorée dans le cas du modèle DFF

Principe du modèle DFF

- Les fronts montant et descendant d'une transition sont différents.
- SCA est toujours possible au niveau du bit :$0 -> 1 => 1$.

Contre-mesure améliorée dans le cas du modèle DFF



Sommaire

Conclusion

Attaque SCARE

- Schéma de FEISTEL.
- Implémentation Hardware.

Contre-mesures

- Différents modèles de rayonnement.
- Bas coût.

Conclusion

Attaque SCARE

- Schéma de FEISTEL.
- Implémentation Hardware.

Contre-mesures

- Différents modèles de rayonnement.
- Bas coût.

Conclusion

Attaque SCARE

- Attaques très opérationnelles.
- Toujours exploitables même en cas d'algorithmes secrets.

Travaux Futurs

- SPN.
- Injection de fautes.

Conclusion

Attaque SCARE

- Attaques très opérationnelles.
- Toujours exploitables même en cas d'algorithmes secrets.

Travaux Futurs

- SPN.
- Injection de fautes.

denis.real@dga.defense.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE LA DÉFENSE
DGA