BALoo: Première Contre-Mesure Efficace contre les Attaques par Fautes Persistantes

Pierre-Antoine TISSOT – Lilian BOSSUET – Vincent GROSSO
Université Jean Monnet Saint-Etienne, CNRS, Institut d Optique Graduate School
Laboratoire Hubert Curien UMR 5516, F-42023, SAINT-ETIENNE, France

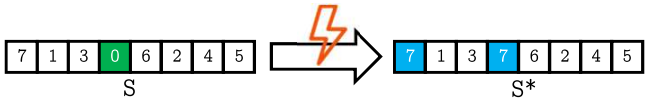
Contexte

Fautes persistantes

- Injectées en mémoire non volatile
- Immunité contre la redondance temporelle
- Analyse non différentielle

Analyse des fautes

- Injection de fautes sur un octet de la S-box

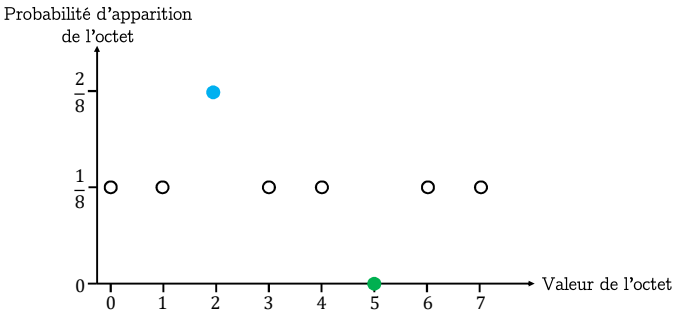


- Persistent Fault Analysis [1] : Analyse de la distribution de probabilités d'apparition des octets dans le message de sortie

Contremesure proposée [2]

- Détection de l'injection
- Utilisation des propriétés de permutation

Analyse des Fautes Persistantes



Distribution des octets dans la sortie $(S_i \oplus k)$

Informations sur la clé k données par cette distribution :

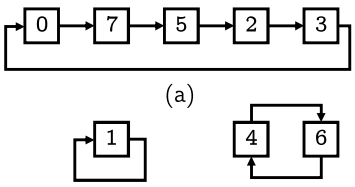
- Probabilité minimale $\rightarrow 5 = 0 \oplus k \Rightarrow k = 5$
- Probabilité maximale $\rightarrow 2 = 7 \oplus k \Rightarrow k = 5$
- Probabilité quelconque $\rightarrow$
  $3 \neq 0 \oplus k \Rightarrow k \neq 3$ and $3 \neq 7 \oplus k \Rightarrow k \neq 4$

Résultat : $k = 5$

Solution – Représentation de la S-box sous forme de cycles

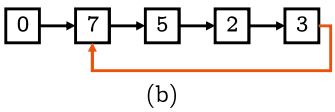
Création des cycles

- Cycle contenant la valeur 0
  $S_0 = 7 \rightarrow S_7 = 5 \rightarrow \cdots \rightarrow S_3 = 0$
- Création de tous les cycles et stockage de leur longueur
- (a) longueur 5 (partant du 0)



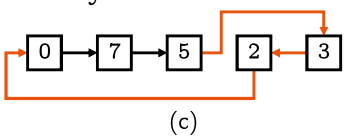
Détection des fautes

- Calcul des longueurs des cycles
- Comparaison avec la longueur stockée
- (b) longueur infinie (partant du 0)



Fautes non détectées

- Minimum de 3 fautes injectées
  $\rightarrow$ *bitset* et *bitreset*
- Distribution des probabilités d'apparition non modifiée
  $\rightarrow$ Injection inutilisable sur cette analyse



Couverture des fautes exploitables : 100%

Application sur AES : AES utilisant 16 S-boxes en parallèle (chiffrement en 11 coups d'horloge)

- PFA efficace avec environ 1600 chiffrés
- Ajout d'une 17e S-box
  - Une S-box est vérifiée quand les 16 autres chiffrent
  - Toutes les S-boxes sont vérifiées au bout de 4352 cycles d'horloge, soit moins de 400 chiffrements

Coûts d'implémentation (Cyclone V)

	Logique (ALM)	Registres	Mémoire (Bits)	F_{max} (MHz)
AES	339	13	32 768	94
AES sécurisé	608	34	34 816	58

Références

[1] F. Zhang, X. Lou, X. Zhao, S. Bhasin, W. He, R. Ding, S. Qureshi, and K. Ren, "Persistent fault analysis on block ciphers," IACR Trans. Cryptogr. Hardw. Embed. Syst., vol. 2018, no. 3, pp. 150–172, 2018
[2] P-A. Tissot, L. Bossuet, V. Grosso, "BALoo: First and Efficient Countermeasure dedicated to Persistent Fault Attacks", *The 29th IEEE International Symposium on On-Line Testing and Robust System Design* (IOLTS 2023).

Travaux réalisés dans le cadre du Projet ANR PROFY ANR-22-CE39-000