Utilisation de ressources cryptographiques pour le test des circuits sécurisés

Marion DOULCIER, Marie-Lise FLOTTES, Bruno ROUZEYRE

{doulcier, flottes, rouzeyre}@lirmm.fr

Contexte

Fonctions

Gestion de mémoires sécurisées

CPU

Contrôleur d'accès

Capacité cryptographique

Co-Processeur crypto (DES, AES...)

Applications

Carte Bancaire

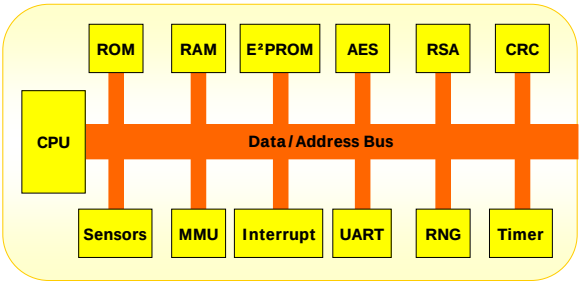
Passeport Électronique

GSM

TV à péage

carte Vitale

...



Architecture de smartcard

Sécurité

Attaques :

invasive : sondes, modifications structurelles...

non invasive : DFA, DPA...

Test

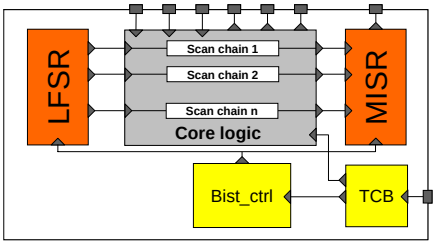
⇒ Sécurité ↗

⇒ DFT ⇒ contrôlabilité ↗ observabilité ↗ ⇒ Sécurité ↘

⇒ **BIST :**

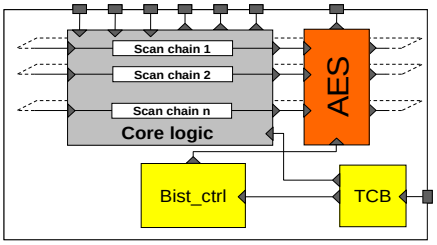
efficacité, coût, ... ?

AES : ressource de TEST



BIST traditionnel

⇒ **Utilisation du crypto-core AES comme générateur de vecteurs de test et analyseur de signature**



Crypto-BIST

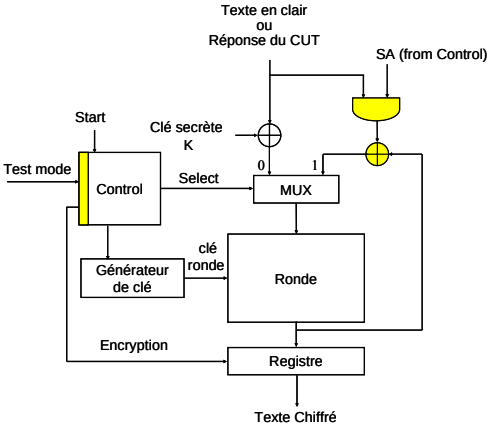
AES

(Advanced Encryption Standard)

- Sélectionné en 2001 par le NIST pour succéder au DES (TDES), conçu par Joan Daemen et Vincent Rijmen
- Paramètres

– taille clé secrète	128	192	256
– taille entrée/sortie	128	128	128
– nombre de rondes	10	12	14
– taille clé de ronde	128	128	128

- Structure SPN et non Feistel



AES TPG/SA implantation

Modes :

Encryptions : SA = 0, select = 0 pour un cycle puis 1 (10 rondes)

Génération : SA = 0, select = 1 (ou 0 puis 1) (1 vecteur/ronde ≈ 1 vecteur/cycle d'horloge)

Analyseur de signature : SA = 1, select = 1 (1 réponse/ronde ≈ 1 vecteur/cycle d'horloge)

AES vs LFSR TPG/SA

Génération de vecteurs de test

Propriétés de séquences aléatoires

- NIST Special Publication 800-22
15 tests statistiques développés pour évaluer les propriétés aléatoires d'une séquence de bits
- Comparaison de 128 séquences générées par un LFSR et par un AES

	LFSR	AES
	P en %	P en %
Freq	21,09	99,22
BlkFreq	100	97,66
CuSum	21,09	100
Runs	100	80,47
LongRuns	100	99,22
Rank	96,88	99,22
DFFT	100	99,22
Univ	97,66	99,22
Apen	100	94,53
Serial1	100	97,66
Serial2	100	99,22
LinComp	0	99,22
non over	99,18	98,64
overl	100	96,88
Random	95,16	99,17

Proportion de flots de bits validant un test statistique du NIST

Simulation de fautes

- Séquences générées par l'AES et par un LFSR
- 3 circuits benchmark ISCAS'89 (s9234, s13207 et s38584)
- 3 configurations différentes (1, 16 et 128 chaînes de scan)

Circuit	Patterns	Nombre de chaînes de scan	LFSR	AES
			TC (%)	TC (%)
s9234	21483	1	95.77	95.96
		16	95.54	95.96
		128	95.52	95.84
s13207	15000	1	99.37	95.83
		16	94.62	96.02
		128	86.48	95.42
s38584	84898	1	91.26	91.93
		16	90.82	92.25
		128	91	91.53

Expérimentation BIST traditionnel et crypto-BIST

Compaction de réponses

Analyseur de signature

- Compacter les réponses du CUT en une seule signature qui sera comparée à celle attendue
- Signatures différentes → au moins une réponse incorrecte → le circuit est fautif
- Signatures égales,
  - Circuit sain ?
  - Masquage ?

$$P(\text{Masquage AES}) = \frac{1}{2^m} - \left(\frac{1}{2^m}\right)^n \approx \frac{1}{2^m}$$

m = 128 et n = nombre de réponses

Conclusion

- Alternative à l'implantation des ressources traditionnelles du BIST
  ⇒ Réduction du coût d'implantation
- 2 modes de fonctionnement supplémentaires /crypto-core AES
  - Générateur de vecteurs de test
  - Analyseur de signatures