Résistance comparée des automates linéaires à la SPA

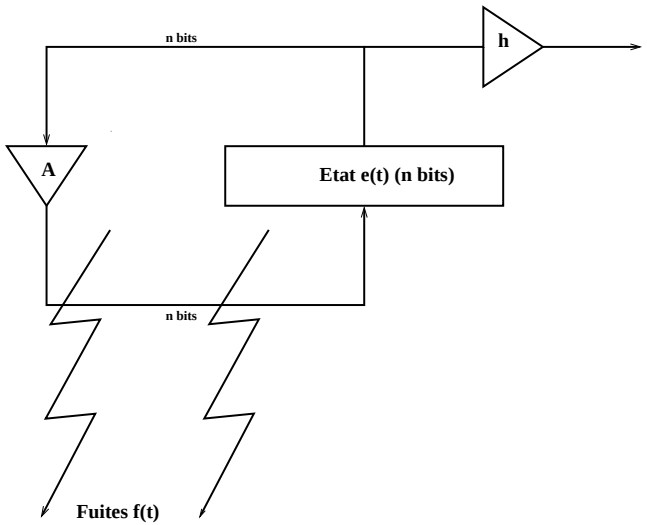
L. Albanese

Nagra France
Université Paris 8

4 avril 2011

Position du problème

On étudie le comportement d'un automate linéaire lorsqu'il est soumis à une SPA.



Objectif : trouver des matrices A telles que l'observation des fuites ne permettent pas de discriminer l'état initial.

Modélisation des fuites

Le modèle choisi est celui de la **distance de Hamming**.

$$f_t = w_H(e_{t+1} \oplus e_t)$$

Propriétés :

- repose sur des lois physiques,
- néglige le bruit de mesure,
- se ramène au modèle du **poids de Hamming** par linéarité

$$f_t = w_H((A - I)e_t).$$

Equations des fuites observées :

$$f_t = w_H(A^t y_0)$$

où

$$y_t = e_{t+1} \oplus e_t$$

Remarque : il n'y a qu'un nombre fini de fuites.

Supposition et considérations

On supposera l'**inversibilité** de A.
On considèrera :

- La périodicité du cycle $(A^t y_0)_{t \geq 0}$.
- La complexité de l'automate.

Insolubilité inconditionnelle

Insolubilité : le système

$$(f_t = w_H(A^t y))_{t \geq 0}$$

admet d'autres solutions que y_0. On distingue :

- les systèmes *résolubles* (ex : registre à décalage rebouclé en période maximale),
- les systèmes *insolubles*, parmi eux :
  - les systèmes *optimaux* qui minimisent l'information fournie à l'adversaire,
  - les systèmes non optimaux qui bornent l'information H communiquée à une valeur insuffisante (ex $n - H \geq 80$ bits),
  - les autres...

Remarque : l'adversaire récupère toujours au moins $w_H(y_0)$.

Matrices aléatoires

Etude de la robustesse d'un automate quelconque soumis à la SPA.
Soit A inversible choisie aléatoirement.
Heuristiquement on constate :

1. A est résoluble,
2. moins de $\frac{2n}{\ln(n)}$ observations suffisent.

Automates optimaux

Ils minimisent l'information délivrée par les fuites.
Les trois propositions sont équivalentes :

- A est optimale
- A conserve le poids de Hamming
- A est une matrice de permutation

Soit p la période du cycle maximal, alors

$$\ln(p) \sim \sqrt{n \ln(n)}$$

Exemple : si on souhaite $p = 2^{128}$ alors $n \geq 1100$.

Réduction modulo 2

On ne garde que le bit de poids faible des observations.
Le système se simplifie et devient **linéaire**.
Un automate est optimal pour ce système ssi le poids de Hamming des colonnes de A est **impair**.
Période maximale d'un cycle : $2^{n-1} - 1$.
Remarque : en pratique la parité est difficile à observer en raison du bruit de mesure.

Réduction modulo 2 : registre à décalage

Cas d'un registre linéaire à décalage en période maximale (P_A primitif) :

- résoluble,
- n observations suffisent.

Réduction au i$^{\text{ème}}$ bit du poids de Hamming

i varie entre 1 et $1 + [\log_2(n)]$.
Généralise le cas précédent ($i = 1$).
On obtient un système d'équations booléennes de degré 2^{i-1},

$$(f_t = \sigma_{2^{i-1}}(A^t y))_{t \geq 0}$$

où σ_k est le polynôme symétrique élémentaire à n variables et de degré k.

Optimalité vis à vis du i$^{\text{ème}}$ bit du poids de Hamming

A est optimale ssi

$$\sigma_{2^{i-1}} \circ A = \sigma_{2^{i-1}}$$

Critère équivalent :

1. le poids de Hamming de toute somme de 2^{i-1} colonnes distinctes de A est congru à $r \geq 2^{i-1} \bmod 2^i$
2. le poids de Hamming de toute somme de *moins* de 2^{i-1} colonnes distinctes de A est congru à $r < 2^{i-1} \bmod 2^i$

Conclusion et perspectives

Il est possible de construire des automates linéaires résistants inconditionnellement à la SPA.
Les registres à décalage usuellement utilisés en cryptographie ne résistent pas.
Pour la suite :

- Taille maximum des cycles d'un automate optimal vis à vis du système réduit selon le $i^{\text{ème}}$ bit du poids de Hamming.
- Construction efficace de ces automates.
- DPA.
- Automates non linéaires.
- ...