

Th de l'info

ILFSP longueur L période $N \leq 2^L - 1$

A. Critères statistiques de Golomb

On veut qu'une suite $(S_i)_{i=0}^{\infty}$ soit indistinguable d'une suite aléatoire.

Golomb: trois critères pour une suite périodique de période N : $(S_0, \dots, S_{N-1})$.

1) Dans chaque période, le nombre de 0 est approximativement égal au nombre de 1.
$$\left| \sum_{i=0}^{N-1} (-1)^{S_i} \right| = \left| \sum_{i=0}^{N-1} \psi(S_i) \right| \leq 1$$

Remarque: $\psi: \mathbb{F}_2 \rightarrow \{+1, -1\}$
 $S \mapsto (-1)^S$

est un homomorphisme (iso) de groupes, qu'on appelle un caractère (de groupe $(\mathbb{F}_2, +)$)

2) Def: Une série (de 0 ou de 1) est une ss-suite finie de bits successifs.

Dans une période on note S l'ensemble de séries maximales (suites)

Ex: soit 1100101 une période, alors

$$S = (11, 00, 1, 0, 1), |S| = 5$$

Soit l , $2^l \leq |S| \leq 2^{l+1}$

$\forall k \leq l$, on trouve au moins $\frac{|S|}{2^k}$ séries maximales de longueur k . En particulier on a $\frac{|S|}{2}$ séries de longueur 1, etc.

$$\frac{|S|}{2} = 2, 5 \leq 3 \quad \frac{|S|}{4} = 1, 25 \leq 2$$

Motivation:

Règle: dans chaque série, la proba de l'un ou l'autre bit est $\frac{1}{2}$.

De plus, le nb de séries k-maximales de 0 et de 1 sont approximativement égaux (à un près).

3) auto correlation

La fct d'auto correlation: $C: \mathbb{Z}/N\mathbb{Z} \rightarrow \mathbb{Z}$

$$C(j) = \sum_{i=0}^{N-1} \psi(s_i + s_{i+j})$$

ne prend que deux valeurs:

$$C(j) = \begin{cases} N & \text{si } j=0 \\ K & \text{sinon} \end{cases}$$

Pour un LFSR la valeur de K est -1

Ex: 1 1 0 0 1 0 1

$j=1$ 1 1 1 0 0 1 0
0 0 1 0 1 1 1

$$C(1) = 3 - 4 = -1$$

$j=2$ 0 1 1 1 0 0 1
1 0 1 1 1 0 0

$$C(2) = 3 - 4 = -1$$

$j=3$ 1 0 1 1 1 0 0
0 1 1 1 0 0 1

$$C(3) = 3 - 4 = -1$$

Comportement d'une suite d'un LFSR

Prop: Dans une suite provenant d'un LFSR de période max $2^L - 1$, toute suite $(s_i, \dots, s_{i+L-1}) \in \mathbb{F}_2^L \setminus (0, \dots, 0)$ apparaît une et une seule fois.

(3)

Th de Vito

Preuve: Le registre $(s_1, \dots, s_{L-1})$
(= état du système en temps i)ne peut ~~pas~~ apparaître qu'une seule fois par période. Or il y a
 $2^L - 1$ telles ss. suites possibles (dans $\mathbb{F}_2^L \setminus \{(0, \dots, 0)\}$)Donc $|\{S_i\}| = 2^L - 1 = |\mathbb{F}_2^L \setminus \{0\}| \quad \square$.Propriété statistique d'une suite maximale ^{periode $2^L - 1$} produite par un LFSR.

Cor 1: Le premier critère de Golomb est satisfait.

Def: On dit que la suite est équilibrée (balanced).

$$\text{Preuve: } \frac{\sum_{i=0}^{N-1} \left(\sum_{j=i}^{L-1} \psi(s_{i+j}) \right)}{L \cdot \psi(s_i) \text{ (Def)}} = \frac{\sum_{i=0}^{N-1} \psi(s_i)}{\sum_{s \in \mathbb{F}_2^L \setminus \{0\}} \psi(s)}$$

mais si $a = (1, 1, \dots, 1)$ on a $\psi(s_{i+1}) + \psi(s_i) = 0$, par conséquent $\sum_{s \in \mathbb{F}_2^L} \psi(s) = 0$ et

$$\sum_{s \in \mathbb{F}_2^L \setminus \{0\}} \psi(s) = -\psi(0, \dots, 0) = -L$$

$$\text{alors } \sum_{i=0}^{N-1} \psi(s_i) = -1 \quad \square$$

Cor 2: Le 2^e critère de Golomb est satisfait.Preuve: Comptons le nb de fois où une suite d'écartement
k apparaît. $Z = (0, \dots, 0) \rightarrow (a_1, \dots, a_k)$

$$S_0 = (s_0, s_1, \dots, s_{L-1}) \rightarrow (s_0, \dots, s_k)$$

$$S_1 = (s_1, s_2, \dots) \rightarrow$$

⋮

$$S_{N-1}(\dots) \rightarrow (s_{N-1}, \dots, s_{N-2+k})$$

$$\mathbb{F}_2^L \rightarrow \mathbb{F}_2^k$$

④

Il y a exactement 2^{L+L-1} préimages de $(c, \dots, 0)$, dont 2^{L+L-1}

Cor 3: Le troisième critère de Golomb est satisfait.

Rappel: $C(j) = -1$ si $j \neq 0$, où $C(j) = \sum_{i=0}^{N-1} \varphi(S_i + S_{i+j})$

Les suites (s_i) et (S_{i+j}) sont définies par la même récurrence. Étant linéaire, la suite $(S_i') = (S_i + S_{i+j})$ l'est également et il n'est pas 0. Alors (S_i') est aussi une suite maximale provenant d'un LFSR. Par Cor 1, on a $\sum_i \varphi(S_i + S_{i+j}) = \sum_i \varphi(S_i') = -1 \quad \square$

Remarque: On note que $(S_i') = (S_{i+j})$ une valeur de i $0 \leq i < N$

3 L'algo de Berlekamp-Massey

permet de déter une suite récurrente (linéairement) à partir de $2L$ bits consécutifs. Donc il n'est pas cryptographiquement sûr.

Lemme: Soit (S_i) une suite provenant d'un LFSR de période maximale $(2^L - 1)$. Si on connaît $2L$ termes consécutifs on peut calculer la récurrence en inversant un système linéaire de taille $L \times L$ (ou en calculant le noyau d'un système de taille $L \times (L+1)$)

Preuve: On a la relation linéaire:

$$\begin{bmatrix} S_i & \dots & S_{i+L-1} \\ \vdots & & \vdots \\ S_{i+L-1} & \dots & S_{i+2L-1} \end{bmatrix} \begin{bmatrix} c_0 \\ \vdots \\ c_{L-1} \end{bmatrix} = \begin{bmatrix} S_{i+L} \\ \vdots \\ S_{i+2L} \end{bmatrix}$$

①

Il suffit de dire que A est inversible

Une dépendance entre colonnes est équivalente à une réécriture linéaire de la période.
 Il suffit donc d'inverser A pour trouver $\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = A^{-1} \begin{bmatrix} s_{i,1} \\ s_{i,2} \\ \vdots \\ s_{i,n-1} \end{bmatrix}$
 ou dit le $R(A) \begin{bmatrix} s_{i,1} \\ s_{i,2} \\ \vdots \\ s_{i,n-1} \end{bmatrix}$

Rem: L'algorithme de B-M est un algo de type $O(L^2)$ au lieu de $O(L^3)$ pour un système générique de $\square$

Conclusion

- A (Golomb): Les suites LFSR ont de bonnes prop pour la crypto
 B (B-M): la linéarité de LFSR est une faiblesse et donc ces suites ne sont pas adaptées à la crypto.

II Fonctions booléennes:

$$f: \mathbb{F}_2^n \rightarrow \mathbb{F}_2$$

Sont importantes en crypto

1) f est monotone de suite $(f_1, \dots, f_m): \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$

2) f est pour diminuer la linéarité
 $S_i = (S_1, \dots, S_{i+m-1}) \rightarrow f(S_i)$
 $(m \leq L)$

d'un LFSR

3) f est de combinaison de plusieurs LFSR
 $(LFSR_j(S_{ij}))_{1 \leq j \leq m} = (S_1^{(1)}, \dots, S_i^{(m)}) = T_i \rightarrow f(T_i)$

$$\left. \begin{array}{l} LFSR_1 \dots S_1^{(1)} S_0^{(1)} \\ \vdots \\ LFSR_m \dots S_1^{(m)} S_0^{(m)} \end{array} \right\} \rightarrow f(T_1) \cdot f(T_0)$$