Attaques exploitant les représentations équivalentes des LFSRs filtrés

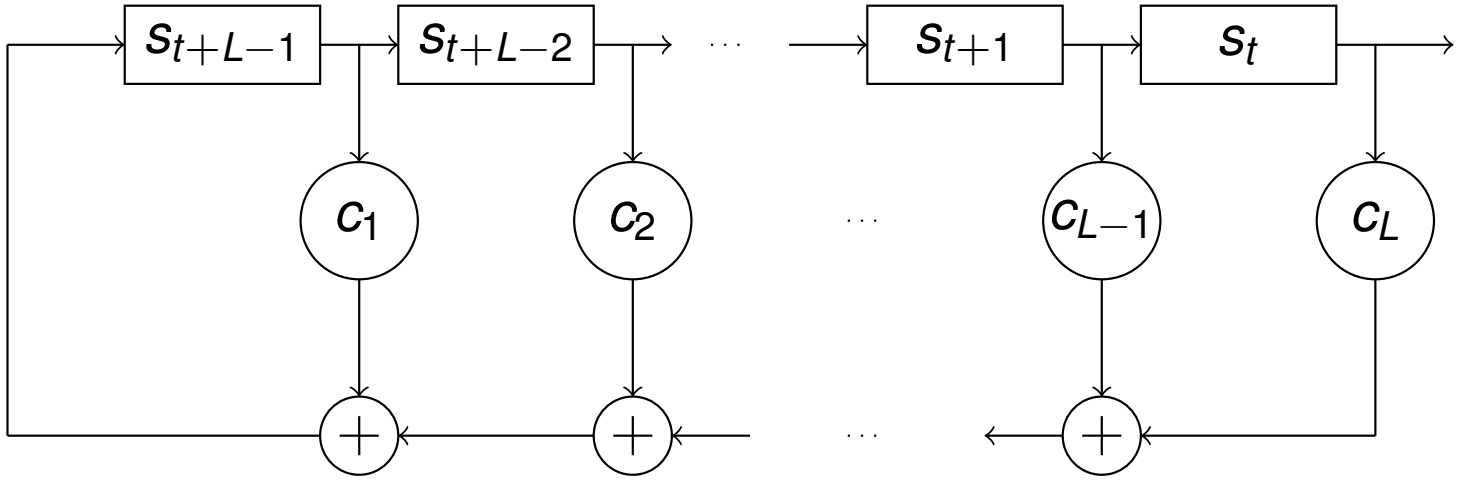
Anne Canteaut & Yann Rotella

Journées Codage et Cryptographie 2015
INRIA équipe SECRET

7 octobre 2015

Registres à décalage à rétroaction linéaire (LFSR)

$$\forall t \geq 0,\ s_{t+L} = \sum_{i=1}^{L} c_i s_{t+L-i} \text{ et } P(X) = 1 + \sum_{i=1}^{L} c_i X^i$$



Intérêt

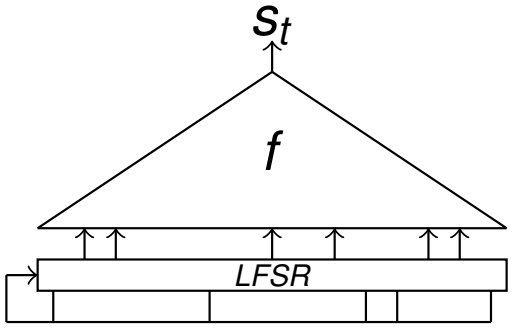
Les suites générées ont de bonnes propriétés statistiques.

Problème

Ce système seul est trop simple (linéaire).

Registres filtrés

Une solution classique est de filtrer le LFSR par une fonction booléenne non-linéaire.



Définition (Forme algébrique normale)

$$f(x) = \sum_{I \in P(N)} a_I x^I$$

où $P(N)$ *désigne l'ensemble des parties de* $\{1, \ldots, N\}$, $a_i \in \mathbb{F}_2$

Cryptanalyses classiques

Attaques algébriques [Shannon 49, Courtois-Meier 03]

- Complexité $O(D^3)$ avec $D = \sum_{k=0}^{\deg(f)} \binom{L}{k}$
- Il faut donc des fonctions booléennes de degré élevé et une immunité algébrique (AI) élevée où

$$\mathrm{AI}(f) = \min(\{\deg(g) : g \neq 0, fg = 0\} \cup \{\deg(h), h \neq 0, (1+f)h = 0\})$$

Cryptanalyses classiques

Attaques algébriques [Shannon 49, Courtois-Meier 03]

- Complexité $O(D^3)$ avec $D = \sum_{k=0}^{\deg(f)} \binom{L}{k}$
- Il faut donc des fonctions booléennes de degré élevé et une immunité algébrique (AI) élevée où

$$\mathrm{AI}(f) = \min(\{\deg(g) : g \neq 0, fg = 0\} \cup \{\deg(h), h \neq 0, (1+f)h = 0\})$$

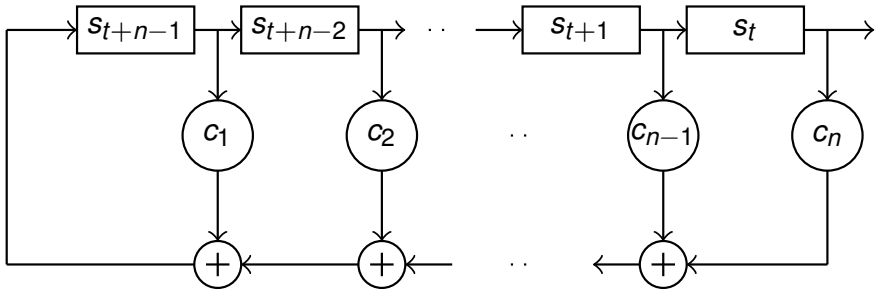
Attaques par corrélation rapides [Meier-Staffelbach 98]

On exploite une bonne approximation de f par une fonction affine.

$$\mathrm{NL}(f) = \min_{\text{h affine}} d(f, h)$$

Pour résister aux attaques par corrélation, la non-linéarité doit être élevée i.e. il n'existe pas de bonne approximation affine de f.

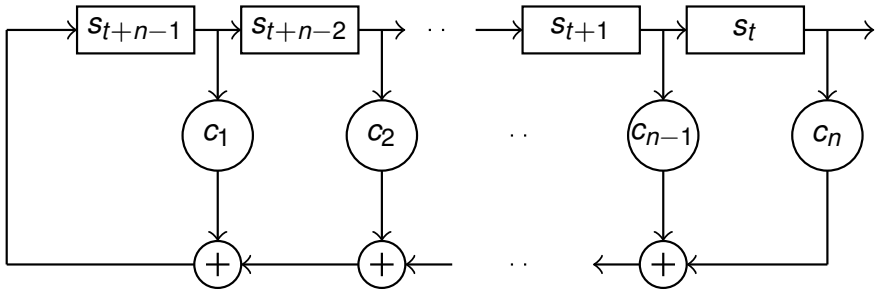
Corps finis



Proposition

Soit $P^\star$ un polynôme irréductible dans $\mathbb{F}_2[X]$ de degré n. Soit $\alpha \in \mathbb{F}_{2^n}$ une racine de $P^\star$ et $\beta_0, \ldots, \beta_{n-1}$ la base duale de $1, \alpha, \ldots, \alpha^{n-1}$. Alors l'état du LFSR de polynôme caractéristique $P^\star$ à l'instant $(t+1)$ est l'état du LFSR à l'instant t multiplié par α, où l'on identifie les vecteurs de $\mathbb{F}_2$ aux éléments de $\mathbb{F}_{2^n}$ en les décomposant dans la base duale $\beta_0, \ldots, \beta_{n-1}$.

Corps finis



Proposition

Soit $P^\star$ un polynôme irréductible dans $\mathbb{F}_2[X]$ de degré n. Soit $\alpha \in \mathbb{F}_{2^n}$ une racine de $P^\star$ et $\beta_0, \ldots, \beta_{n-1}$ la base duale de $1, \alpha, \ldots, \alpha^{n-1}$. Alors l'état du LFSR de polynôme caractéristique $P^\star$ à l'instant $(t+1)$ est l'état du LFSR à l'instant t multiplié par α, où l'on identifie les vecteurs de $\mathbb{F}_2$ aux éléments de $\mathbb{F}_{2^n}$ en les décomposant dans la base duale $\beta_0, \ldots, \beta_{n-1}$.

Pour tout t, $X_t = X_0 \alpha^t$

Fonctions booléennes

Proposition (Représentation univariée des fonctions booléennes)

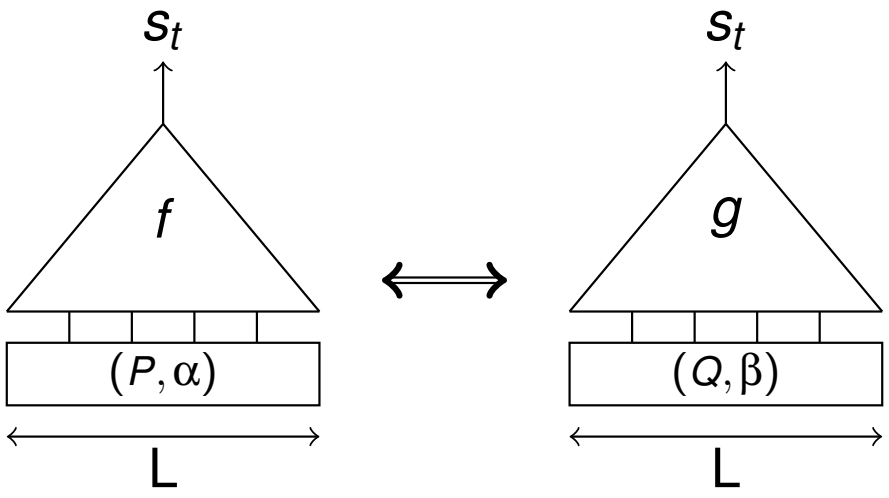
Il existe une unique représentation univariée de f de la forme :

$$f(x) = \sum_{j \in \Gamma_n} \mathrm{Tr}^{C_j}(a_j x^j) + \varepsilon(1 + x^{2^n - 1})$$

avec :

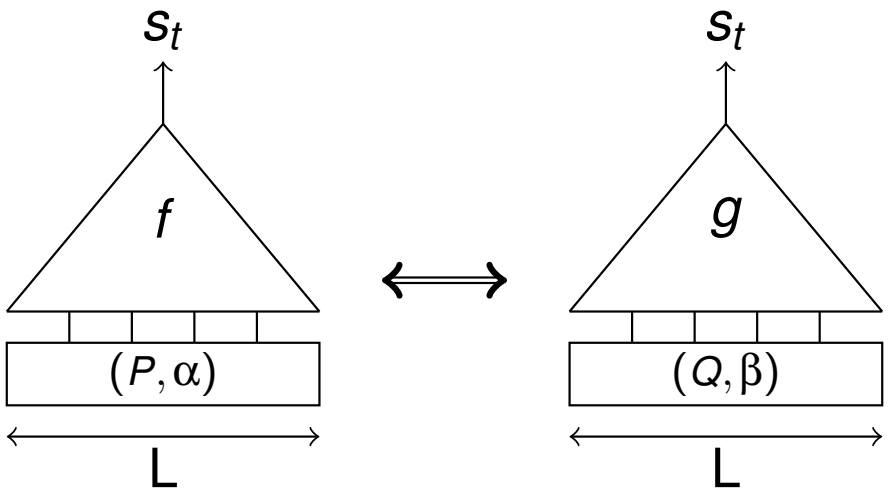
1. Γ_n *est l'ensemble des représentants de chaque classe cyclotomique modulo* $2^n - 1$.
2. C_j *est la taille de la classe cyclotomique contenant* j.
3. $a_j \in \mathbb{F}_{2^{C_j}}$
4. $\varepsilon = \mathrm{w}_H(f) \mod 2$
5. *où* $\mathrm{Tr}_r^k(x) = \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}} = x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{k-r}}$

Equivalence proposée par Rønjom & Cid [2010] (1)



$\beta = \alpha^k$, $Y_0 = X_0^k$ et $g(x) = f(x^r)$ et $rk \equiv 1 \mod (2^n - 1)$

Equivalence proposée par Rønjom & Cid [2010] (1)



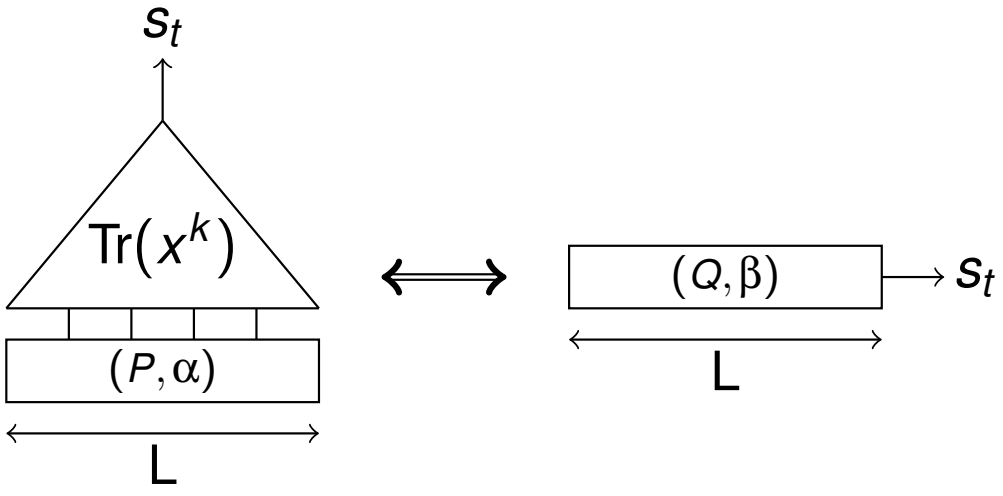
$\beta = \alpha^k$, $Y_0 = X_0^k$ et $g(x) = f(x^r)$ et $rk \equiv 1 \mod (2^n - 1)$

Implication

Le niveau de sécurité d'un LFSR filtré est le niveau de sécurité minimal pour un générateur de sa classe d'équivalence.

Equivalence proposée par Rønjom & Cid [2010] (2)

Cas particulier ($f(x) = \mathrm{Tr}(x^r)$, $\mathrm{pgcd}(r, 2^n - 1) = 1$) :
Soit k tel que $rk \equiv 1 \mod (2^n - 1)$ et $\beta = \alpha^k$.



$\Longrightarrow$ Le LFSR filtré est équivalent à un LFSR non-filtré de même taille.

Généralisation à d'autres fonctions creuses (1)

Si $f(x) = \mathrm{Tr}(Ax^k)$, $\mathrm{pgcd}(k, 2^n - 1) > 1$ alors on retrouve X_0^k.

Lemme

La connaissance de X_0^k nous donne $\log_2 \tau_k$ bits d'informations sur X_0 où $\tau_k = \mathrm{ord}(\alpha^k)$.

$$X_0 = \alpha^i,\ X_0^k = \alpha^{rk} \text{ où } r = i \mod \tau_k$$

- Le nombre d'états internes possibles est τ_k.
- La taille du LFSR équivalent est l'ordre de 2 modulo τ_k, c'est C_k la taille de la classe cyclotomique de k.

Généralisation à d'autres fonctions creuses (2)

Si $f(x) = \mathrm{Tr}(A_1 x^{k_1}) + \mathrm{Tr}(A_2 x^{k_2})$, avec $\mathrm{pgcd}(k_1, 2^n - 1) = 1$ alors on peut rendre le degré de f' au moins inférieur à $\left\lceil \frac{n}{2} \right\rceil$.

Généralisation à d'autres fonctions creuses (2)

Si $f(x) = \mathrm{Tr}(A_1 x^{k_1}) + \mathrm{Tr}(A_2 x^{k_2})$, avec $\mathrm{pgcd}(k_1, 2^n - 1) = 1$ alors on peut rendre le degré de f' au moins inférieur à $\left\lceil \frac{n}{2} \right\rceil$.

Proposition

Pour tout entier $k \in [0, 2^n - 2]$ *alors*

$$\min_{0<r<2^n-1, \mathrm{pgcd}(r,2^n-1)=1} [\max(\mathrm{w}_H(r), \mathrm{w}_H(kr))] \leq \left\lceil \frac{n}{2} \right\rceil$$

et cette borne est atteinte si $\mathrm{w}_H(k) = n - 1$

Complexité linéaire

La complexité linéaire Λ d'une suite est la taille du plus petit LFSR qui la génèrerait. On la calcule avec l'algorithme de Berlekamp Massey.

Complexité linéaire

La complexité linéaire Λ d'une suite est la taille du plus petit LFSR qui la génèrerait. On la calcule avec l'algorithme de Berlekamp Massey.

Proposition

Soit un LFSR de taille n filtré par une fonction booléenne f :

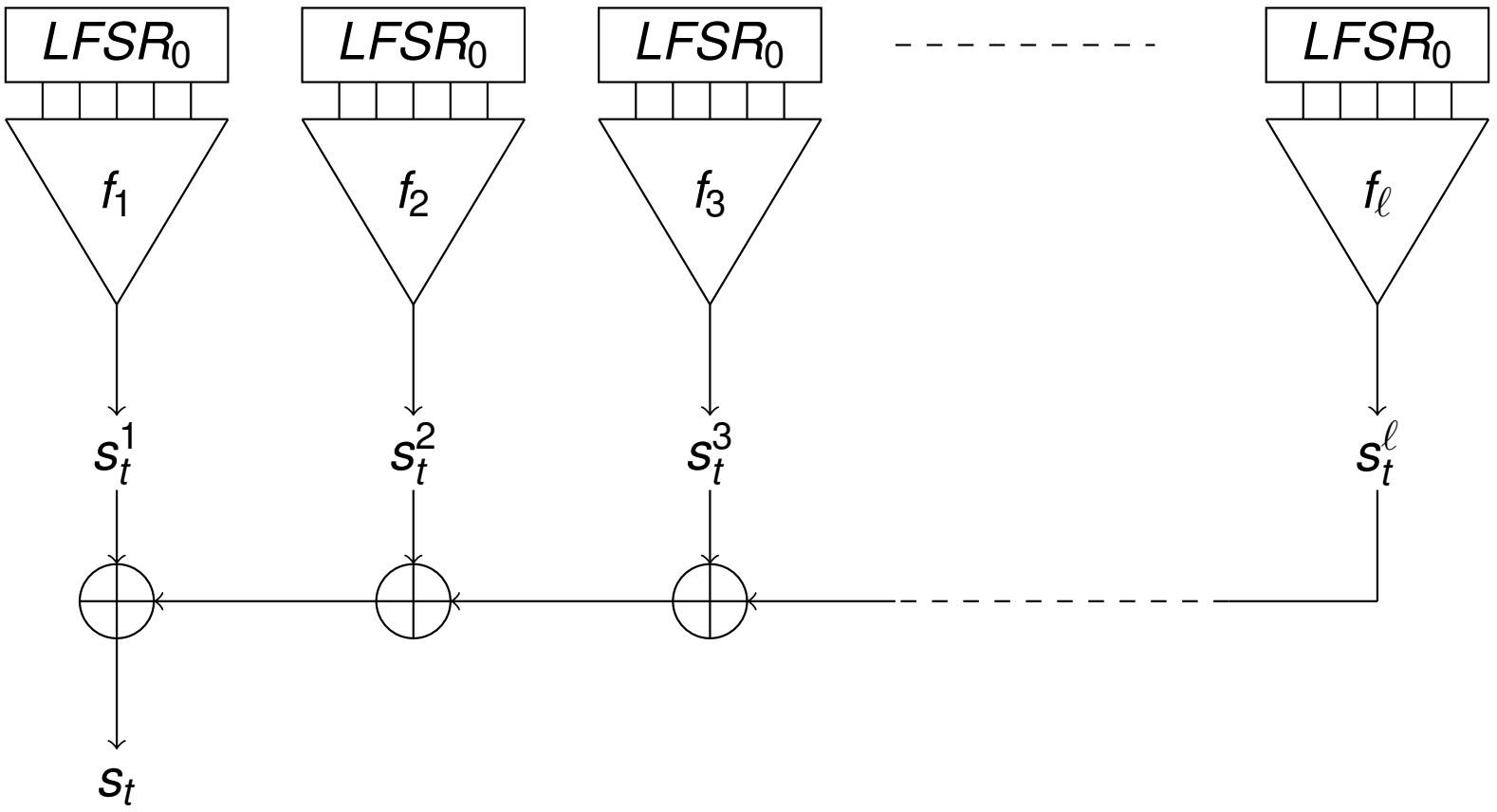
$$f(x) = \sum_{k \in \Gamma_n} \mathrm{Tr}^{C_k}(A_k x^k)$$

Alors

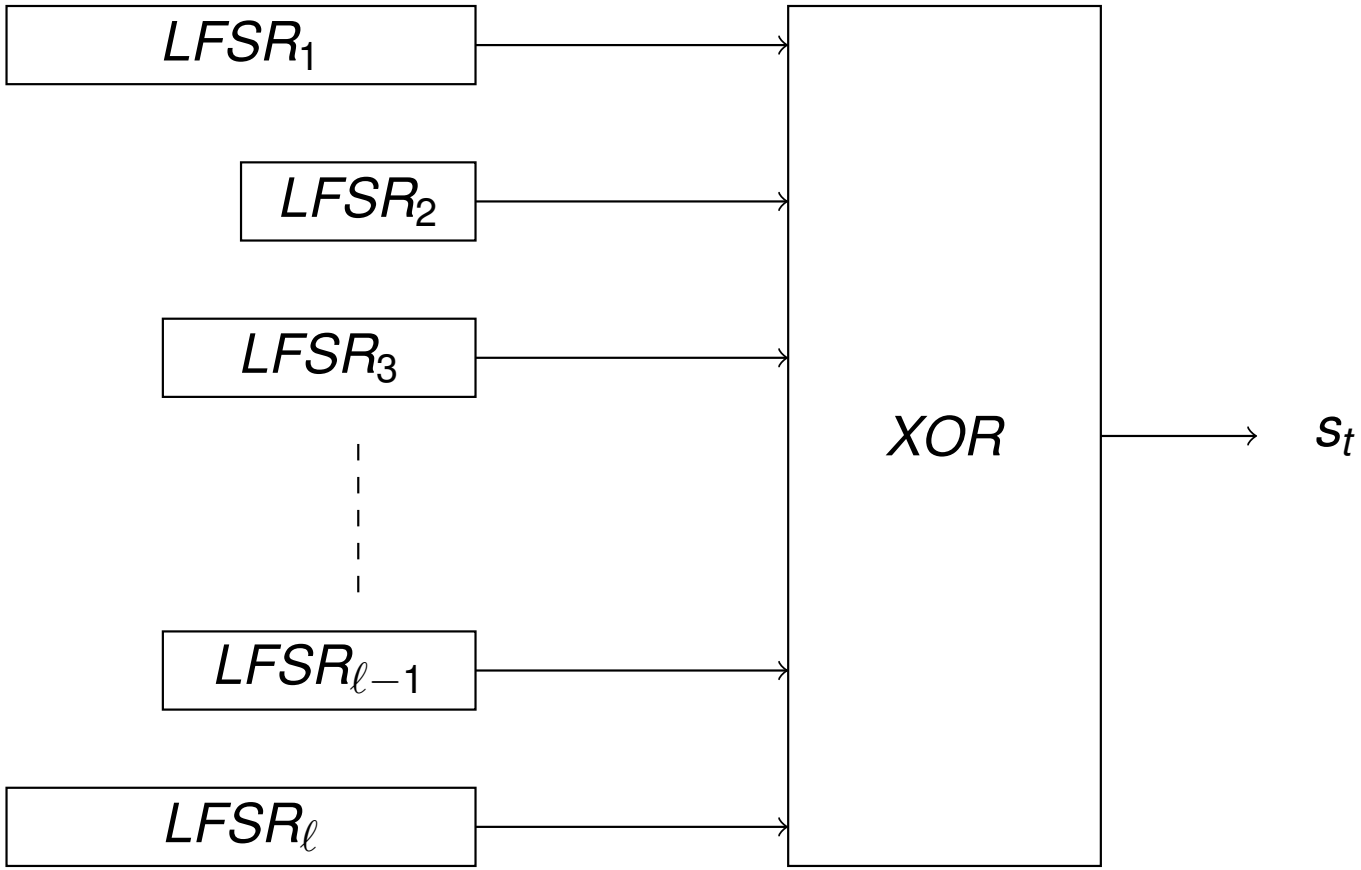
$$\Lambda(s) = \sum_{k \in \Gamma_n, A_k \neq 0} C_k$$

Le résultat est déjà mentionné sans preuve en 2011 par Gong, et al, nous en avons donné une ici.

Complexité linéaire

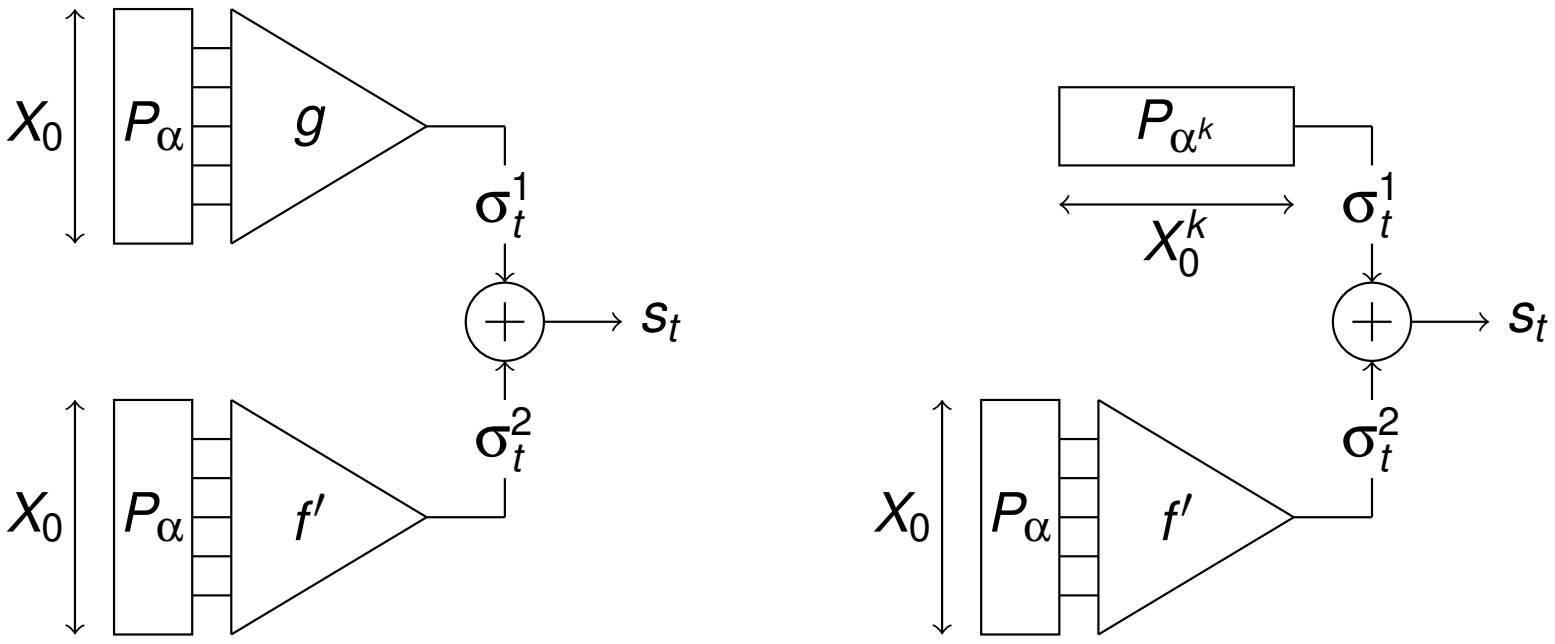


Complexité linéaire



Attaque par corrélation généralisée

Pour $g = \mathrm{Tr}(Ax^x)$



Non-linéarité généralisée [Gong & Youssef 01]

Définition (Transformée de Walsh étendue)

Soit f une fonction booléenne, alors

$$\widehat{f}(\lambda, k) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}(\lambda x^k)}$$

où $\lambda \in \mathbb{F}_{2^n}$, $\mathrm{pgcd}(k, 2^n - 1) = 1$ et $\widehat{f}(\lambda, k)$ est la transformée étendue de Walsh-Hadamard de la fonction f.

Non-linéarité généralisée [Gong & Youssef 01]

Définition (Transformée de Walsh étendue)

Soit f une fonction booléenne, alors

$$\widehat{f}(\lambda, k) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}(\lambda x^k)}$$

où $\lambda \in \mathbb{F}_{2^n}$, $\mathrm{pgcd}(k, 2^n - 1) = 1$ et $\widehat{f}(\lambda, k)$ est la transformée étendue de Walsh-Hadamard de la fonction f.

Non-linéarité généralisée

$$\mathrm{NLG}(f) = 2^{n-1} - \frac{1}{2} \max_{\substack{\lambda \in \mathbb{F}_{2^n} \\ k:\mathrm{pgcd}(k,2^n-1)=1}} \left|\widehat{f}(\lambda, k)\right|$$

Fonctions de haute non-linéarité généralisée

Ce critère a été énoncé une première fois en 2001 par Amr M. Youssef et Guang Gong mais sans être motivé par l'existence d'une attaque concrète.

Définition

$$\mathrm{NLG}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$$

avec égalité pour les fonctions hypercourbes.
De plus, f est hypercourbe si et seulement si $f(x^k)$ *est courbe pour tout* k *tel que* $\mathrm{pgcd}(k, 2^n - 1) = 1$.

Complexité linéaire et fonctions hypercourbes

Théorème (Nechaev et al 2006)

Si f est hypercourbe, alors

$$f(x) = \sum_{k \in M(\lambda)} \mathrm{Tr}(A_k x^k)$$

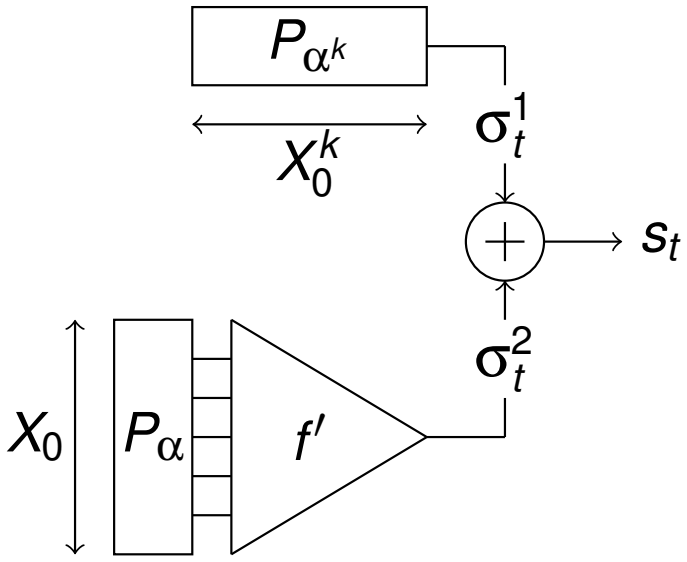
avec

$$M(\lambda) = \{k : \forall r : \mathrm{pgcd}(r, 2^n - 1) = 1, \mathrm{w}_H(rk) = \frac{n}{2}\}$$

Questions

- Quelle est la plus haute NLG possible pour une fonction équilibrée ?
- Combien de termes peut-il y avoir dans la représentation trace ?

Généralisation avec $\mathrm{pgcd}(k, 2^n - 1) > 1$



$\tau_k = \mathrm{ord}(\alpha^k)$ et $L =$ ordre de 2 modulo τ_k.
Complexité en temps de l'attaque :

- $\mathrm{T} = \frac{\tau_k \log(\tau_k)}{\varepsilon^2}$
- Si $L < n$, $\mathrm{T} = 2^{\frac{L}{\omega-1}} \left(\frac{1}{2\varepsilon}\right)^{\frac{2\omega(\omega-2)}{\omega-1}}$ où $\omega \in \{2,3,4,5\}$

où ε le biais : $\Pr[s_t \neq \sigma_t] = \frac{1}{2}(1-\varepsilon)$, i.e. $\varepsilon = 1 - \frac{\mathrm{d}(f,g)}{2^{n-1}}$ avec $g = \mathrm{Tr}(Ax^k)$ ou $h(x^k)$.

Combinaison d'attaques

Conclusion

On obtient $\log(\tau_k)$ bits d'information sur X_0 où $\tau_k = \mathrm{ord}(\alpha^k)$.

Combinaison d'attaques

Conclusion

On obtient $\log(\tau_k)$ bits d'information sur X_0 où $\tau_k = \mathrm{ord}(\alpha^k)$.

Propriété

Si on réalise deux attaques distinctes avec k_1 et k_2, alors on obtient $\log_2(\mathrm{ppcm}(\tau_{k_1}, \tau_{k_2}))$ bits d'information.

Combinaison d'attaques

Conclusion

On obtient $\log(\tau_k)$ bits d'information sur X_0 où $\tau_k = \text{ord}(\alpha^k)$.

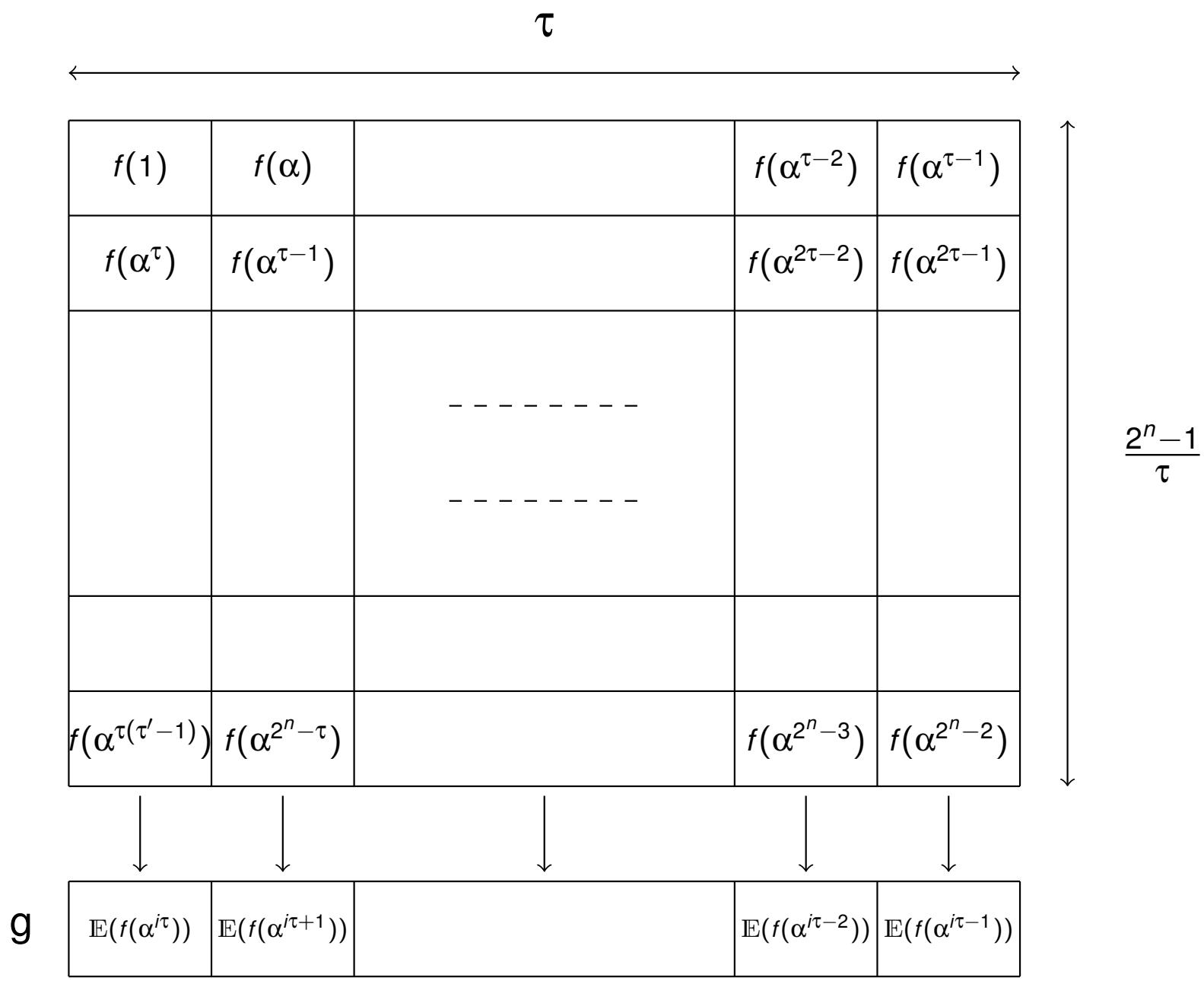
Propriété

Si on réalise deux attaques distinctes avec k_1 et k_2, alors on obtient $\log_2(\text{ppcm}(\tau_{k_1}, \tau_{k_2}))$ bits d'information.

Conséquence

Si $2^n - 1 = p_1 p_2 \ldots p_\ell$ alors on peut retrouver l'état initial en

$$\frac{p_1 \log(p_1)}{\varepsilon_1^2} + \frac{p_2 \log(p_2)}{\varepsilon_2^2} + \ldots + \frac{p_{\ell-1} \log(p_{\ell-1})}{\varepsilon_{\ell-1}^2} + p_\ell$$


τ
$f(1)$ $f(\alpha)$ $f(\alpha^{\tau-2})$ $f(\alpha^{\tau-1})$
$f(\alpha^{\tau})$ $f(\alpha^{\tau-1})$ $f(\alpha^{2\tau-2})$ $f(\alpha^{2\tau-1})$
$f(\alpha^{\tau(\tau'-1)})$ $f(\alpha^{2^n-\tau})$ $f(\alpha^{2^n-3})$ $f(\alpha^{2^n-2})$
$\frac{2^n-1}{\tau}$
g
$\mathbb{E}(f(\alpha^{i\tau}))$ $\mathbb{E}(f(\alpha^{i\tau+1}))$ $\mathbb{E}(f(\alpha^{i\tau-2}))$ $\mathbb{E}(f(\alpha^{i\tau-1}))$

- Si $\tau_{k_1} = 2^l - 1$, et que g est linéaire, alors on peut améliorer en faisant une attaque par corrélation rapide.
- On aura toujours un biais ε supérieur à $\frac{\tau}{2^n}$.
- On peut changer $\frac{\tau \log(\tau)}{\varepsilon^2}$ en $\tau \log(\tau)$ si on fait une transformée de Fourier rapide [Canteaut-Naya Plasencia 2012].
- On aura toujours besoin de $\frac{\log(\tau)}{\varepsilon^2}$ bits de la suite chiffrante.

Conclusions

- Nombre de termes dans la représentation trace élevé
- Critère de non-linéarité généralisée à prendre en compte
- Généralisation de ce critère à toutes les fonctions monomiales

Problèmes ouverts

- Calcul de la représentation trace d'une fonction booléenne
- Amélioration de la complexité de l'attaque
- Faut-il $2^n - 1$ premier ?

Merci pour votre attention !