

(multivariables sur des corps finis)

Université Paris 6, SIS Université de Toulon.
courtois@univ-tln.fr

27-ème École de Printemps de Codage et Cryptographie
Batz-sur-Mer, 1er juin 1999.

Plan

1. Résoudre des équations quadratiques est NP-complet.
2. Et pourtant ... la relinéarisation [Kipnis].
3. Représentation univariante et multivariante.
4. Des fonctions trappe à représentation obscure, HFE.
5. Attaque de Shamir-Kipnis.
6. Des attaques équationnelles [Patarin-Courtois].

Slide 2



MQ_K u K

$$f : \begin{cases} b_k = \sum_{i=0}^n \sum_{j=i}^n \lambda_{ijk} a_i a_j \\ \text{avec } k = 1..u, \quad a_0 = 1 \end{cases}$$

$$n = u = 1$$

$$K = N$$

N

$$K = q$$

d

MQ_K est NP-complet pour tout corps K

[Garey,Johnson, Patarin, Goubin].

2

\mapsto

$$\begin{cases} 0 = x \vee y \vee z \\ 1 = \neg t \end{cases} \quad \begin{cases} 0 = xyz + xy + yz + xz + x + y + z \\ 1 = 1 + t \end{cases}$$

- $y_{ij} = x_i x_j$
- $0 = y_{ij} - x_i x_j$

MQ_K

- $u \ll n$

$$u = n$$

- $u \approx \frac{n^2}{2}$



- $y_{ij} = x_i x_j$

- u

$$u = \varepsilon \frac{n^2}{2} \geq n \qquad \frac{n^2}{2}$$



K -anneau, [Kipnis, Shamir, Crypto 99]

1. Exprimer chaque y_{ij} (ou x_i) comme une expression linéaire de $M = \frac{n^2}{2} - u = (1 - \varepsilon) \frac{n^2}{2}$ variables z_i .
2. Ajouter les équations triviales en les y_{ij} et x_i de degré $c > 1$, p.ex. $y_{12}y_{34} = y_{13}y_{24}$. Elles sont indépendantes en tant que polynômes multivariés de degré $\geq c$.
3. Remplacer les y_{ij} et x_i par les z_i :
4. soit par la simple linéarisation si le nombre d'équations dépasse le nombre de termes qui y apparaissent, soit réitérer l'attaque.



Les arrangements possibles de $2c$ indexes en c groupes:

$$k_c = (2c - 1) * (2c - 3) * (2c - 5) * \dots = \frac{(2c)!}{2^c c!}$$

Donne $k_c - 1$ équations triviales de degré c en les y_{ij} et x_i .

En négligeant des termes de degré $< c$ des groupes de $k_c - 1$ équations correspondent à des groupes de k_c termes. Si $c \ll n$.

$(k_c - 1) * \frac{n^{2c}}{(2c)!}$ équations

- $(k_c) * \frac{n^{2c}}{(2c)!}$ termes.
- $(1 - \varepsilon)^c * (k_c) * \frac{n^{2c}}{(2c)!}$ termes.



Pour tout ε il existe un c tq. nb. d'équations $>$ nb. termes:

$$(k_c - 1) * \frac{n^{2c}}{(2c)!} > (1 - \varepsilon)^c * (k_c) * \frac{n^{2c}}{(2c)!}$$

- $\varepsilon > 0.5$ donne $c = 1$, simple linéarisation en $\mathcal{O}(n^6)$.
- $\varepsilon > 0.1$ donne $c = 2$, algorithme en $\mathcal{O}(n^{12})$.
- $\varepsilon > 0.01$ donne $c = 3$, algorithme en $\mathcal{O}(n^{18})$.

La recherche exhaustive est mieux pour $n \leq 110$ (!).

Même si $u = n$ la technique s'applique avec $\varepsilon = \frac{2}{n}$. (!!!)

Elle est censé marcher dans le cas moyen, pb. si la substitution génère des équations non-indépendantes.



Elle marche beaucoup moins bien que prévu, voir l'article de Courtois, Patarin, Klimov, Shamir de Eurocrypt'2000 pour la version améliorée appelée XL.

K $K = \mathbb{F}_q$
 \exists $q^n = K[X]/P(X)$
 P n K
 q^n n K K^n
 n $K[X]$ P



$$f : K^n \rightarrow K^n$$

◇

◇ n K

$$b = f(a) = a^{q^s} \quad b_i = f_i(a_1, \dots, a_n) \quad K$$

$$f(a) = \sum a^{q^s + q^t} \quad f_i$$

2

$$b = f(a) = a + a^3 + a^5 =$$

$$(a_2X^2 + a_1X + a_0) + (a_2X^2 + a_1X + a_0)^3 + (a_2X^2 + a_1X + a_0)^5 \text{ mod } X^3 + X^2 + 1 =$$

$$(a_2 + a_2a_1 + a_2a_0 + a_1)X^2 + (a_2a_1 + a_1a_0 + a_2)X + (a_0 + a_2 + a_1a_0 + a_2a_0)$$

$$\begin{cases} b_2 = a_2 + a_2a_1 + a_2a_0 + a_1 \\ b_1 = a_2a_1 + a_1a_0 + a_2 \\ b_0 = a_0 + a_2 + a_1a_0 + a_2a_0 \end{cases}$$

$$f(a) = \sum_{q^s + q^t < d} \gamma_{st} a^{q^s + q^t}$$

-
- $g = T \circ f \circ S \quad 2 \quad S \quad T$

n

g

$T \quad S \quad f$

$\leq d$

f
 $g^{-1} = S^{-1} \circ f^{-1} \circ T^{-1}$
 f^{-1}

$\exists \quad 2 * 500$

$S \quad T$

$f \quad \exists \quad q^{n/2}$

$f \quad 99\% \quad d \ll q^n - 1$

$g \quad f$

G

$$g(x) = \sum_{i=0}^{n-1} \sum_{j=0}^{n-1} G_{ij} x^{q^i + q^j}$$

$G \quad n \quad F \quad r = \log d$

$T^{-1} \circ g \stackrel{?}{=} f \circ S$

$f \circ S$

$G' = WGW^t$

$$T^{-1} \circ g = \sum_{k=0}^{n-1} t_k G^{*k}$$

G^{*k}

G'

$\diamond \quad n(n-r) \quad r(n-r)$

$\diamond \quad K^n \quad \varepsilon \approx \frac{2}{r^2}$

$\diamond \quad (r+1) \quad (r+1) \quad G'$

$n^{\mathcal{O}(\log d)} \quad 2^{120}$
1
80



- D^*
-
-

-
-
- D^*

C^* $[C]$
 C^{*-}

g

◇

x $g(x)$

◇

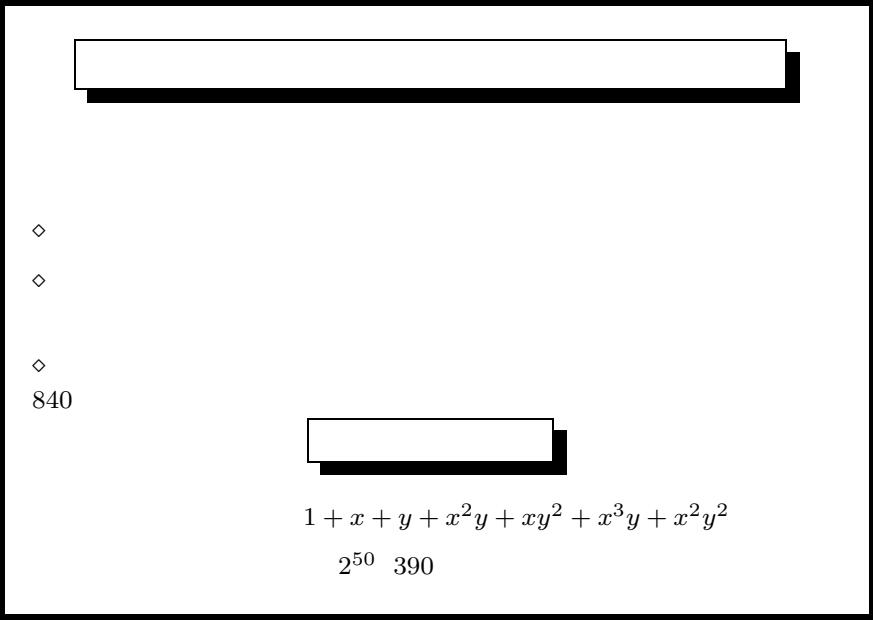
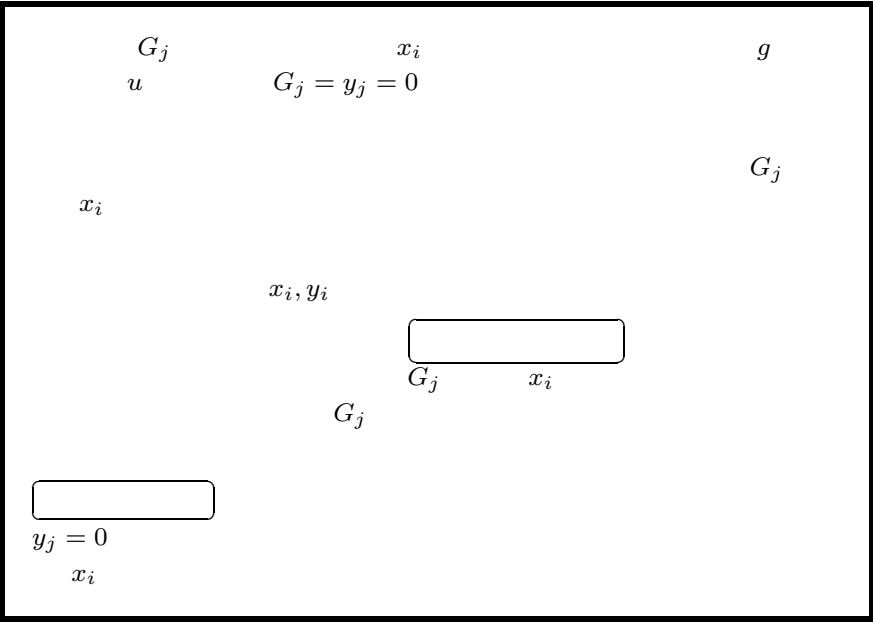
$(x, g(x))$

x_i

$x_i = 0$ 1

x_i





[Redacted]

◇

$$n \geq 128 \quad d > 96$$

◇

$e^{\log^2 n}$
$e^{n^{\frac{1}{3}}}$

◇

◇

—

Pour ou contre.