(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.

Slide 2

Plan

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

$\mathbf{MQ_K}$ **u**

n 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}

$\mapsto$

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

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

MQ_K

- $u << n$

  $u = n$

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

- $y_{ij} = x_i x_j$

- u u

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

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 multivariables 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:

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

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 $c << n$.

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

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

- $\varepsilon > 0.5$ 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 appellée XL.

K $K =$ $_q$

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

P n K

$_{q^n}$ n K K^n

n $K[X]$ P

$f : K^n \to K^n$

$\diamond$

$\diamond$ n K

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

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

2

$b = f(a) = a + a^3 + a^5 =$
$(a_2X^2 + a_1X + a_0) + (a_2X^2 + a_1X + a_0)^3 + (a_2X^2 + a_1X +$
$a_0)^5$ *mod* $X^3 + X^2 + 1 =$
$(a_2+a_2a_1+a_2a_0+a_1)X^2+(a_2a_1+a_1a_0+a_2)X+(a_0+a_2+a_1a_0+a_2a_0)$

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

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

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

n g

T S f $\leq d$

f f^{-1}

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

$\exists$ $2 * 500$

$S \quad T$

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

f 99% $d << q^n - 1$

$g \quad f$

G

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

G n F $r = \log d$

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

$f \circ S$

$G' = WGW^t$ r

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

g^{p^k}

G'

◇ $n(n-r)$ $r(n-r)$

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

◇ $(r+1)$ $(r+1)$ G'

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

- D^*
-
-

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

g

◇ x $g(x)$

◇

$(x, g(x))$

x_i

$x_i = 0$ 1

x_i

G_j x_i g
u $G_j = y_j = 0$

G_j

x_i

x_i, y_i

G_j x_i

G_j

$y_j = 0$
x_i

◇

◇

◇

840

$1 + x + y + x^2y + xy^2 + x^3y + x^2y^2$

2^{50} 390

◇

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

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

◇

◇

–

Pour ou contre.