Cryptanalyse algébrique de McEliece

J.-C. Faugère, L. Perret, A. Otmani, J.-P. Tillich

Frédéric de Portzamparc

Journées C2 2012, Dinard

08 octobre 2012

Sommaire

Cryptosystème de McEliece

-  R.J. McEliece.
  A public-key cryptosystem based-on algebraic coding theory, 1978.

-  N. Courtois, M. Finiasz, N. Sendrier.
  How to achieve a McEliece-based digital signature scheme.
  ASIACRYPT 2001

Cryptosystème de McEliece

-  R.J. McEliece.
  A public-key cryptosystem based-on algebraic coding theory, 1978.

-  N. Courtois, M. Finiasz, N. Sendrier.
  How to achieve a McEliece-based digital signature scheme.
  ASIACRYPT 2001

- G_{Gop} : matrice d'un code de Goppa $[n, k, t]_q$
  $(S, P) \in GL_k(\mathbb{F}) \times P_n$: clé privée

$$G_{pub} = \mathbf{S} G_{Gop} \mathbf{P}.$$

Cryptosystème de McEliece

-  R.J. McEliece.
  A public-key cryptosystem based-on algebraic coding theory, 1978.

-  N. Courtois, M. Finiasz, N. Sendrier.
  How to achieve a McEliece-based digital signature scheme.
  ASIACRYPT 2001

- G_{Gop} : matrice d'un code de Goppa $[n, k, t]_q$
  $(S, P) \in GL_k(\mathbb{F}) \times P_n$: clé privée

$$G_{pub} = \mathbf{S} G_{Gop} \mathbf{P}.$$

- Sécurité : problème NP-dur de décodage d'un code

Sécurité de McEliece

ISD (Information Set Decoding) :

-  A. Canteaut, N. Sendrier
  Cryptanalysis of the Original McEliece Cryptosystem, 1998
  McEliece 1978 : $[1024, 524, 50]_2$ $\mathbf{2^{64}}$ op.

$\vdots$

-  D. J. Bernstein, T. Lange, C. Peters
  Attacking and defending the McEliece cryptosystem,
  Post-Quantum Cryptography, 2008

$\vdots$

-  Anja Becker, Antoine Joux, Alexander May, Alexander Meurer
  Decoding Random Binary Linear Codes in 2 n/20 : How 1 + 1 = 0 Improves Information Set Decoding
  EUROCRYPT 2012

Sécurité du McEliece

Attaque structurelle : Recherche exhaustive sur un des éléments privés.

-  N. Sendrier
  Finding the permutation between linear codes : The support splitting algorithm.
  IEEE, 2000

 P. Loidreau, N. Sendrier
Weak keys in the McEliece public-key cryptosystem.
IEEE, 2001

Sécurité du McEliece

Attaque structurelle : Recherche exhaustive sur un des éléments privés.

-  N. Sendrier
  Finding the permutation between linear codes : The support splitting algorithm.
  IEEE, 2000

   P. Loidreau, N. Sendrier
  Weak keys in the McEliece public-key cryptosystem.
  IEEE, 2001

- Bilan : attaques exponentielles en la taille des paramètres

Variantes compactes du cryptosystème de McEliece

Tailles de clé importantes (80-bits de sécurité : $\mathbf{460,000}$ bits)

Variantes compactes du cryptosystème de McEliece

Tailles de clé importantes (80-bits de sécurité : $\mathbf{460,000}$ bits)

$$C_i = \begin{pmatrix} a_0 & a_1 & \cdots & a_{\ell-1} \\ a_{\ell-1} & a_0 & \cdots & a_{\ell-2} \\ \vdots & \ddots & \ddots & \vdots \\ a_1 & a_{\ell-1} & \cdots & a_0 \end{pmatrix}$$

bloc cyclique

T. Berger, P.-L. Cayrel, Ph. Gaborit, A. Otmani.
Reducing Key Length of the McEliece Cryptosystem.
AFRICACRYPT 2009

Variantes compactes du cryptosystème de McEliece

Tailles de clé importantes (80-bits de sécurité : **460, 000** bits)

$$C_i = \begin{pmatrix} a_0 & a_1 & \cdots & a_{\ell-1} \\ a_{\ell-1} & a_0 & \cdots & a_{\ell-2} \\ \vdots & \ddots & \ddots & \vdots \\ a_1 & a_{\ell-1} & \cdots & a_0 \end{pmatrix}$$

bloc cyclique

$$\Delta_i = \left(\begin{array}{cc|cc} a_0 & a_1 & a_2 & a_3 \\ a_1 & a_0 & a_3 & a_2 \\ \hline a_2 & a_3 & a_0 & a_1 \\ a_3 & a_2 & a_1 & a_0 \end{array}\right)$$

bloc dyadique

T. Berger, P.-L. Cayrel, Ph. Gaborit, A. Otmani.
Reducing Key Length of the McEliece Cryptosystem.
AFRICACRYPT 2009

R. Misoczki, P. S. L. M. Barreto.
Compact McEliece Keys from Goppa Codes.
SAC 2009

1 Cryptosystème de McEliece

2 **Attaque algébrique de Faugère-Otmani-Perret-Tillich (FOPT)**

3 Étude approfondie de l'attaque

Attaque algébrique de Faugère-Otmani-Perret-Tillich :*Algebraic Cryptanalysis of McEliece Variants with Compact Keys, Eurocrypt 2010*

Attaque algébrique de Faugère-Otmani-Perret-Tillich : *Algebraic Cryptanalysis of McEliece Variants with Compact Keys, Eurocrypt 2010*

Théorème

Les codes de Goppa sont des codes alternants.

Attaque algébrique de Faugère-Otmani-Perret-Tillich : *Algebraic Cryptanalysis of McEliece Variants with Compact Keys, Eurocrypt 2010*

Théorème

Les codes de Goppa sont des codes alternants.

Définition(Codes alternants)

Soient $\mathbf{x} = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_{q^m}^n$,avec $x_i \neq x_j$ et $\mathbf{y} = (y_0, \ldots, y_{n-1}) \in \mathbb{F}_{q^m}^n$, tq $y_i \neq 0$, et une matrice de parité de la forme

$$A_t(\mathbf{x}, \mathbf{y}) = \begin{pmatrix} y_0 & y_1 & \cdots & y_{n-1} \\ y_0 x_0 & y_1 x_1 & \cdots & y_{n-1} x_{n-1} \\ \vdots & & \ddots & \vdots \\ y_0 x_0^{t-1} & & \cdots & y_{n-1} x_{n-1}^{t-1} \end{pmatrix}$$

$\mathcal{C}_{alt} = \{\mathbf{c} \in \mathbb{F}_q^n | A_t(\mathbf{x}, \mathbf{y})^t \mathbf{c} = 0\}$ de paramètres $[n, k \geq n - mt, \geq t]_q$

- $\mathbf{x}, \mathbf{y}$ connus $\Longrightarrow$ décodage polynomial de $\frac{t}{2}$ erreurs

Attaque algébrique de Faugère-Otmani-Perret-Tillich

But de l'attaque : retrouver x et y

Attaque algébrique de Faugère-Otmani-Perret-Tillich

But de l'attaque : retrouver $\mathbf{x}$ et $\mathbf{y}$

- $A_t(\mathbf{x}, \mathbf{y})$ matrice de parité $\iff {}^tG_{pub}A_t(\mathbf{x}, \mathbf{y}) = 0$

$$\left\{ \sum_{l=0}^{n-1} g_{i,l} y_l x_l^p = 0 \mid 0 \leq i < k, 0 \leq p \leq t-1 \right\}.$$

Attaque algébrique de Faugère-Otmani-Perret-Tillich

But de l'attaque : retrouver $\mathbf{x}$ et $\mathbf{y}$

- $A_t(\mathbf{x}, \mathbf{y})$ matrice de parité $\iff {}^tG_{pub}A_t(\mathbf{x}, \mathbf{y}) = 0$

$$\left\{ \sum_{l=0}^{n-1} g_{i,l} y_l x_l^p = 0 \mid 0 \leq i < k, 0 \leq p \leq t-1 \right\}.$$

- Système algébrique : résolution par bases de Gröbner (F4,F5)
  - Système très structuré

Attaque algébrique de Faugère-Otmani-Perret-Tillich

But de l'attaque : retrouver $\mathbf{x}$ et $\mathbf{y}$

- $A_t(\mathbf{x}, \mathbf{y})$ matrice de parité $\iff {}^tG_{pub}A_t(\mathbf{x}, \mathbf{y}) = 0$

$$\left\{ \sum_{l=0}^{n-1} g_{i,l} y_l x_l^p = 0 \mid 0 \leq i < k, 0 \leq p \leq t-1 \right\}.$$

- Système algébrique : résolution par bases de Gröbner (F4,F5)
  - Système très structuré
- Complexité polynomiale ou exponentielle ?

Attaque algébrique de Faugère-Otmani-Perret-Tillich

T. Berger, P.-L. Cayrel, Ph. Gaborit, A. Otmani.

Reducing Key Length of the McEliece Cryptosystem, AFRICACRYPT 2009.

R. Misoczki, P. S. L. M. Barreto.

Compact McEliece Keys from Goppa Codes, SAC 2009.

q	n_0	t	FGb(F5)
2^8	9	51	0.06 s
2^8	10	51	0.03 s
2^8	12	51	0.05 s
2^8	15	51	0.02 s
2^{10}	6	75	0.05s
2^{10}	6	93	0.05s
2^{10}	8	93	0.02s
2^8	15	255	0.08s

Table: Paramètres quasi-cycliques $[n = n_0 t, k, t]_q$

.

Attaque algébrique de Faugère-Otmani-Perret-Tillich

T. Berger, P.-L. Cayrel, Ph. Gaborit, A. Otmani.

Reducing Key Length of the McEliece Cryptosystem, AFRICACRYPT 2009.

R. Misoczki, P. S. L. M. Barreto.

Compact McEliece Keys from Goppa Codes, SAC 2009.

q	n_0	t	FGb(F5)
2^8	9	51	0.06 s
2^8	10	51	0.03 s
2^8	12	51	0.05 s
2^8	15	51	0.02 s
2^{10}	6	75	0.05s
2^{10}	6	93	0.05s
2^{10}	8	93	0.02s
2^8	15	255	0.08s

Table: Paramètres quasi-cycliques $[n = n_0 t, k, t]_q$

q	n_0	t	Fgb(F5)
2^8	5	256	0.03 s
2^8	5	128	0.02 s
2^8	6	128	0.05 s
2^8	12	64	0.03 s
2^4	32	64	0.50 s
2^2	56	64	1776 s
2	40	64	NA
2	80	128	NA

Table: Paramètres quasi-dyadiques $[n = n_0 t, k, t]_q$

1. Cryptosystème de McEliece

2. Attaque algébrique de Faugère-Otmani-Perret-Tillich (FOPT)

3. **Étude approfondie de l'attaque**

Étude approfondie de l'attaque

- Mieux comprendre le rôle des différents paramètres.
  - Compter précisément variables et équations dans le cas quasi-dyadique

Étude approfondie de l'attaque

- Mieux comprendre le rôle des différents paramètres.
  - Compter précisément variables et équations dans le cas quasi-dyadique

- Étendre l'attaque à $\mathbb{F}_2$
  - **Possible** en exploitant une propriété des Goppa binaires (dyadique ou quelconque)

Étude approfondie de l'attaque

- Mieux comprendre le rôle des différents paramètres.
  - Compter précisément variables et équations dans le cas quasi-dyadique
- Étendre l'attaque à $\mathbb{F}_2$
  - **Possible** en exploitant une propriété des Goppa binaires (dyadique ou quelconque)
- Automatiser l'attaque de FOPT
  - Implantation Magma de **TweakedF4**
- En cours : adapter des résultats théoriques sur les systèmes bilinéaires

Système FOPT : comptage des équations

$$\left\{ \mathbf{P}_{i,p} = \sum_{0 \leq l < n} g_{i,k} y_l x_l^p = 0 \mid 0 \leq i \leq k, 0 \leq p \leq t-1 \right\}$$
$$g_{i,j} \in \mathbb{F}_q, Y_l, X_l \in \mathbb{F}_{q^m}, q = 2^u.$$

Système FOPT : comptage des équations

$$\left\{ \mathbf{P}_{i,p} = \sum_{0 \le l < n} g_{i,k} y_l x_l^p = 0 \mid 0 \le i \le k, 0 \le p \le t-1 \right\}$$
$$g_{i,j} \in \mathbb{F}_q, Y_l, X_l \in \mathbb{F}_{q^m}, q = 2^u.$$

- G de la forme $\left(\begin{array}{c|c} I_k & A \end{array} \right) \Longrightarrow y_i + \sum_{l=0}^{n-k-1} g_{i,k+l} y_{k+l} = 0, 0 \le i < k.$

Système FOPT : comptage des équations

$$\left\{ \mathbf{P}_{i,p} = \sum_{0 \le l < n} g_{i,k} y_l x_l^p = 0 \mid 0 \le i \le k, 0 \le p \le t-1 \right\}$$
$$g_{i,j} \in \mathbb{F}_q, Y_l, X_l \in \mathbb{F}_{q^m}, q = 2^u.$$

- G de la forme $\left(\begin{array}{c|c} I_k & A \end{array} \right) \implies y_i + \sum_{l=0}^{n-k-1} g_{i,k+l} y_{k+l} = 0, 0 \le i < k.$
- $(\mathbf{x}, \mathbf{y})$ solution $\implies$ $(a\mathbf{x} + b, c\mathbf{y})$ solution : on peut fixer des variables.

Système FOPT : comptage des équations

$$\left\{ \mathbf{P}_{i,p} = \sum_{0 \le l < n} g_{i,k} \mathbf{y}_l \mathbf{x}_l^p = 0 \mid 0 \le i \le k, 0 \le p \le t-1 \right\}$$
$$g_{i,j} \in \mathbb{F}_q, Y_l, X_l \in \mathbb{F}_{q^m}, q = 2^u.$$

- G de la forme $\left(\begin{array}{c|c} I_k & A \end{array} \right) \implies y_i + \sum_{l=0}^{n-k-1} g_{i,k+l} y_{k+l} = 0, 0 \le i < k.$
- $(\mathbf{x}, \mathbf{y})$ solution $\implies$ $(a\mathbf{x} + b, c\mathbf{y})$ solution : on peut fixer des variables.
- G_{pub} **quasi-dyadique** : relations supplémentaires
  1. $\mathbf{y_{rt+i}} = \mathbf{y_{rt}}$
  2. $\mathbf{x_{rt+i}} = \mathbf{x_{rt}} + \sum_{i=0}^{\lambda-1} i_k (\mathbf{x_0} + \mathbf{x_{2^k}})$ avec $0 \le r < n_0, 0 \le i < t, i = \sum_{k=0}^{s-1} i_k 2^k$

Système FOPT : comptage des équations

$$\left\{ \mathbf{P}_{i,p} = \sum_{0 \le l < n} g_{i,k} \mathbf{y}_l \mathbf{x}_l^p = 0 \mid 0 \le i \le k, 0 \le p \le t-1 \right\}$$
$$g_{i,j} \in \mathbb{F}_q, Y_l, X_l \in \mathbb{F}_{q^m}, q = 2^u.$$

- G de la forme $\left(\begin{array}{c|c} I_k & A \end{array} \right) \implies y_i + \sum_{l=0}^{n-k-1} g_{i,k+l} y_{k+l} = 0, 0 \le i < k.$
- $(\mathbf{x}, \mathbf{y})$ solution $\implies$ $(a\mathbf{x} + b, c\mathbf{y})$ solution : on peut fixer des variables.
- G_{pub} **quasi-dyadique** : relations supplémentaires
  1. $\mathbf{y_{rt+i}} = \mathbf{y_{rt}}$
  2. $\mathbf{x_{rt+i}} = \mathbf{x_{rt}} + \sum_{i=0}^{\lambda-1} i_k(\mathbf{x_0} + \mathbf{x_{2^k}})$ avec $0 \le r < n_0, 0 \le i < t, i = \sum_{k=0}^{s-1} i_k 2^k$

McEliece général	McEliece QD
$n-2$ inconnues X	$n_0 + \lambda - 2$ inconnues X
$mt-1$ inconnues Y	$m-1$ inconnues Y
$t(n-mt)$ équations	$t(n-mt)$ équations
$\lambda(n-mt)$ eq. $(1, 2^s)$	$\lambda(n-mt)$ eq. $(1, 2^s)$

$\lambda = \log_2(t)$.

Codes de Goppa quasi-dyadiques : nouvelles relations

- Structure quasi-dyadique = dyadique par blocs :

$$G_{pub} = \left(\begin{array}{cc|cc|c} g_0 & g_1 & g_2 & g_3 & \\ g_1 & g_0 & g_3 & g_2 & \cdots \\ \hline \vdots & \vdots & \vdots & \vdots & \end{array}\right)$$

$$g_{i,j}^{(k)} = g_{0,j\oplus i}^{(k)} \text{ avec } i,j < t.$$

Codes de Goppa quasi-dyadiques : nouvelles relations

- Structure quasi-dyadique = dyadique par blocs :

$$G_{pub} = \left(\begin{array}{cccc|c} g_0 & g_1 & g_2 & g_3 & \\ g_1 & g_0 & g_3 & g_2 & \cdots \\ \hline \vdots & \vdots & \vdots & \vdots & \end{array}\right)$$

$$g_{i,j}^{(k)} = g_{0,j\oplus i}^{(k)} \text{ avec } i,j < t.$$

$$\begin{aligned}
\mathbf{P}_{0,2^s} + \mathbf{P}_{1,2^s} &= \sum_{k=0}^{n-1} g_{0,k} y_k x_k^{2^s} + \sum_{k=0}^{n-1} \underbrace{g_{1,k}}_{=g_{0,k\oplus 1}} y_k x_k^{2^s} \\
&= \sum_{k=0}^{n-1} g_{0,k} y_k x_k^{2^s} + \sum_{k=0}^{n-1} g_{0,k} \underbrace{y_{k\oplus 1}}_{=y_k} x_{k\oplus 1}^{2^s} \\
&= \sum_{k=0}^{n-1} g_{0,k} y_k (x_k + x_{k\oplus 1})^{2^s} \\
&= \left(\sum_{k=0}^{n-1} g_{0,k} y_k\right)(x_0 + x_1)^{2^s} \\
&= 0.
\end{aligned}$$

Codes de Goppa quasi-dyadiques : description du système

$$(S_{QD}) : \left\{ \sum_{0 \le p < n_0} Y_p \sum_{0 \le i < t} g_{kt,pt+i} X_{pt+i}^{2^s} = 0 \right\}_{0 \le k < (n_0 - m), 0 \le s \le \lambda - 1}$$

Théorème

(S_{QD}) contient exactement :
- $n_0 + \lambda - 2$ variables X_i
- $m - 1$ variables Y_j
- $\lambda(\cancel{n - mt}) \rightarrow \lambda(n_0 - m)$ eq. $(1, 2^s)$

Codes de Goppa quasi-dyadiques : description du système

$$(S_{QD}) : \left\{ \sum_{\substack{0 \le k < (n_0 - m), 0 \le s \le \lambda - 1}} Y_p \sum_{0 \le i < t} g_{kt, pt+i} X_{pt+i}^{2^s} = 0 \right\}_{0 \le p < n_0}$$

Théorème

(S_{QD}) contient exactement : $\begin{cases} n_0 + \lambda - 2 \text{ variables } X_i \\ m - 1 \text{ variables } Y_j \\ \lambda(\cancel{n - mt}) \to \lambda(n_0 - m) \text{ eq. } (1, 2^s) \end{cases}$

-  JC Faugère, M. Safey El Din, PJ Spaenlehauer.
  Gröbner Bases of Bihomogeneous Ideals generated by Polynomials of Bidegree (1,1) : Algorithms and Complexity.
- $\left\{ \sum_{i,j} \alpha_{i,j}^{(k)} Y_i X_j = 0, k \le n_X + n_Y \right\}$:min(n_X, n_Y) constant, la résolution est polynomiale en $n_X + n_Y$.

Système pour un code sur $\mathbb{F}_2$

- McEliece standard : code de Goppa binaire

Difficultés rencontrées :

1. Problème dans l'implantation FOPT : peu d'équations
2. Système ${}^t G A_t(\mathbf{x}, \mathbf{y}) = 0$ avec $g_{i,j} \in \mathbb{F}_2$: pas 0-dimensionnel

Système pour un code sur $\mathbb{F}_2$

- McEliece standard : code de Goppa binaire

Difficultés rencontrées :

1. Problème dans l'implantation FOPT : peu d'équations
2. Système ${}^t G A_t(\mathbf{x}, \mathbf{y}) = 0$ avec $g_{i,j} \in \mathbb{F}_2$: pas 0-dimensionnel

F.J. MacWilliams and N.J.A. Sloane

The Theory of Error-Correcting Codes, Elsevier/NorthHolland, 1977

Propriété (Codes de Goppa binaires)

$$ {}^t G_{pub} A_t(\mathbf{x}, \mathbf{y}) = 0 \implies {}^t G_{pub} A_{2t}(\mathbf{x}, \mathbf{y}^2) = 0. $$

Système pour un code sur $\mathbb{F}_2$

- McEliece standard : code de Goppa binaire

Difficultés rencontrées :

1. Problème dans l'implantation FOPT : peu d'équations
2. Système ${}^tGA_t(\mathbf{x}, \mathbf{y}) = 0$ avec $g_{i,j} \in \mathbb{F}_2$: pas 0-dimensionnel

F.J. MacWilliams and N.J.A. Sloane

The Theory of Error-Correcting Codes, Elsevier/NorthHolland, 1977

Propriété (Codes de Goppa binaires)

$$ {}^tG_{pub}A_t(\mathbf{x}, \mathbf{y}) = 0 \implies {}^tG_{pub}A_{2t}(\mathbf{x}, \mathbf{y}^2) = 0. $$

- Nouvelles équations qui complètent (S_{QD}) :

$$ \sum_{l=0}^{n-1} g_{it,l} y_l^2 x_l = 0, 0 \leq i < n_0 $$

- Avec ces équations, le cas binaire n'est pas à part *i.e.* même stratégie de résolution

Stratégie de résolution

- F4 $\Longrightarrow$ calcul directe de base de Gröbner : complexité élevée

Stratégie de résolution

- F4 $\Longrightarrow$ calcul directe de base de Gröbner : complexité élevée
- $(y_0, \ldots, y_{d-1})$ connus

$$\left\{ \sum_{k=0}^{n-1} g_{i,k} y_k X_k^{2^s} = 0 \right\} \Longrightarrow \left\{ \sum_{k=0}^{n-1} g_{i,k}^{q^m - 2^s} y_k^{q^m - 2^s} X_k = 0 \right\} \text{ linéaire}$$

Stratégie de résolution

- F4 $\Longrightarrow$ calcul directe de base de Gröbner : complexité élevée
- $(y_0, \ldots, y_{d-1})$ connus

$$\left\{ \sum_{k=0}^{n-1} g_{i,k} y_k X_k^{2^s} = 0 \right\} \Longrightarrow \left\{ \sum_{k=0}^{n-1} g_{i,k}^{q^m - 2^s} y_k^{q^m - 2^s} X_k = 0 \right\} \text{ linéaire}$$

Calcul de bases de Gröbner : TweakedF4

1: **repeat**
2: G_d :=GröbnerBasis$<_{ord}$(S,d) pour $<_{ord}$ bien choisi

Stratégie de résolution

- F4 $\Longrightarrow$ calcul directe de base de Gröbner : complexité élevée
- $(y_0, \ldots, y_{d-1})$ connus

$$\left\{ \sum_{k=0}^{n-1} g_{i,k} y_k X_k^{2^s} = 0 \right\} \Longrightarrow \left\{ \sum_{k=0}^{n-1} g_{i,k}^{q^m - 2^s} y_k^{q^m - 2^s} X_k = 0 \right\} \text{ linéaire}$$

Calcul de bases de Gröbner : TweakedF4

1: **repeat**
2: G_d :=GröbnerBasis$<_{ord}$(S,d) pour $<_{ord}$ bien choisi
3: $f_1(\mathbf{Y}), \ldots, f_i(\mathbf{Y}) := G_d \cap \mathbb{F}_{q^m}[\mathbf{Y}]$

Stratégie de résolution

- F4 $\Longrightarrow$ calcul directe de base de Gröbner : complexité élevée
- $(y_0, \ldots, y_{d-1})$ connus

$$\left\{ \sum_{k=0}^{n-1} g_{i,k} y_k X_k^{2^s} = 0 \right\} \Longrightarrow \left\{ \sum_{k=0}^{n-1} g_{i,k}^{q^m - 2^s} y_k^{q^m - 2^s} X_k = 0 \right\} \text{ linéaire}$$

Calcul de bases de Gröbner : TweakedF4

1: **repeat**
2: G_d :=GröbnerBasis$<_{ord}$(S,d) pour $<_{ord}$ bien choisi
3: $f_1(\mathbf{Y}), \ldots, f_i(\mathbf{Y}) := G_d \cap \mathbb{F}_{q^m}[\mathbf{Y}]$
4: **until** $S_Y = \{f_1(\mathbf{Y}) = 0, \ldots, f_i(\mathbf{Y}) = 0\}$ a un nombre fini de sols
5: **return** $(y_0, \ldots, y_{d-1})$

Stratégie de résolution

- F4 $\Longrightarrow$ calcul directe de base de Gröbner : complexité élevée
- $(y_0, \ldots, y_{d-1})$ connus

$$\left\{ \sum_{k=0}^{n-1} g_{i,k} y_k X_k^{2^s} = 0 \right\} \Longrightarrow \left\{ \sum_{k=0}^{n-1} g_{i,k}^{q^m - 2^s} y_k^{q^m - 2^s} X_k = 0 \right\} \text{ linéaire}$$

Calcul de bases de Gröbner : TweakedF4

1: **repeat**
2: G_d :=GröbnerBasis$<_{ord}$(S,d) pour $<_{ord}$ bien choisi
3: $f_1(\mathbf{Y}), \ldots, f_i(\mathbf{Y}) := G_d \cap \mathbb{F}_{q^m}[\mathbf{Y}]$
4: **until** $S_Y = \{f_1(\mathbf{Y}) = 0, \ldots, f_i(\mathbf{Y}) = 0\}$ a un nombre fini de sols
5: **return** $(y_0, \ldots, y_{d-1})$

- Choix de $<_{ord}$: "favoriser" les **Y**

grevlex$[X, Y]$	$25s$	elim$[X, Y]$	$5s$
grevlex$_{\mathbf{W}}[X, Y]$	$20s$	elim$_{\mathbf{W}}[X, Y]$	$3s$

Temps de résolution pour $n_0 = 32, m = 2, t = 128$

Nouvelle implantation en Magma

Challenges quasi-dyadiques : $\mathbf{x}, \mathbf{y} \in \mathbf{F}_{2^{16}}$

q	n_0	t	n_Y	n_X	Fgb(F5)	Magma TweakedF4
2^8	5	256	1	11	0.03s	30s
2^8	5	128	1	10	0.02s	12s
2^8	6	128	1	11	0.05s	8.5s
2^8	12	64	1	12	0.03s	0.2s

Paramètres : $\mathbf{x}, \mathbf{y} \in \mathbf{F}_{2^{12}}$

2^4	32	64	2	36		688s

En contournant **artificiellement** la recherche des $\mathbf{Y}$:

2^4	32	64	1	36	0.50 s	0.45s
2^2	56	64	1	60	1776 s	1.7s
2	40	64	1	44	NA	0.8s

Table: Cryptanalyse de codes QD$[n = n_0 t, k, t]$ sur $\mathbb{F}_q$.

Travaux en cours

- **TweakedF4** : Affiner le choix de $<_{ord}$, borner le degré à atteindre
- Approfondir le lien avec les systèmes bi-homogènes $(1,1)$ ou $(1,D)$
- Exploiter la surdétermination

Merci de votre attention !