Une Attaque Polynomiale de McEliece basé sur des codes de Goppa sauvages sur des extensions quadratiques (ou Comment domestiquer les codes de Goppa sauvages?)

Alain Couvreur, Ayoub Otmani, Jean-Pierre Tillich

INRIA/École Polytechnique, Université de Rouen, INRIA

Journées C2 2014

Plan

Principe du schéma de McEliece

C'est un schéma **à clé publique.**

On se donne une famille de triplets $(\mathscr{C}, t, \mathcal{A})$, où

- $\mathscr{C}$ est un code $[n,k]_q$ de matrice génératrice $\boldsymbol{G}$;
- $t \in \mathbb{N}^*$;
- $\mathcal{A}$ est algorithme "rapide" corrigeant jusqu'à t erreurs

Principe du schéma de McEliece

Fonctionnement :

Principe du schéma de McEliece

Fonctionnement :

- **Clé publique :** $(\boldsymbol{G}, t)$;

Principe du schéma de McEliece

Fonctionnement :

- **Clé publique :** $(\boldsymbol{G}, t)$;
- **Clé secrète :** $\mathcal{A}$.

Principe du schéma de McEliece

Fonctionnement :

- **Clé publique :** $(\boldsymbol{G}, t)$;
- **Clé secrète :** $\mathcal{A}$.
- **Chiffrement :** $m \in \mathbb{F}_q^k$
  - $c = m\boldsymbol{G} \in \mathscr{C}$

Principe du schéma de McEliece

Fonctionnement :

- **Clé publique :** $(\boldsymbol{G}, t)$;
- **Clé secrète :** $\mathcal{A}$.
- **Chiffrement :** $m \in \mathbb{F}_q^k$
  - $c = m\boldsymbol{G} \in \mathscr{C}$
  - On génère $e \in \mathbb{F}_q^n$ aléatoire tel que $w_H(e) \leqslant t$;

Principe du schéma de McEliece

Fonctionnement :

- **Clé publique :** $(\boldsymbol{G}, t)$;
- **Clé secrète :** $\mathcal{A}$.
- **Chiffrement :** $m \in \mathbb{F}_q^k$
  - $c = m\boldsymbol{G} \in \mathscr{C}$
  - On génère $e \in \mathbb{F}_q^n$ aléatoire tel que $w_H(e) \leqslant t$;
  - message chiffré :

$$m_{chiffr} \stackrel{\text{def}}{=} c + e$$

Principe du schéma de McEliece

Fonctionnement :

- **Clé publique :** $(\boldsymbol{G}, t)$;
- **Clé secrète :** $\mathcal{A}$.
- **Chiffrement :** $m \in \mathbb{F}_q^k$
  - $c = m\boldsymbol{G} \in \mathscr{C}$
  - On génère $e \in \mathbb{F}_q^n$ aléatoire tel que $w_H(e) \leqslant t$;
  - message chiffré :

$$m_{chiffr} \stackrel{\text{def}}{=} c + e$$

- **Déchiffrement :** On applique $\mathcal{A}$ et on retrouve c puis m.

Familles proposées

Codes de Goppa Binaires [McEliece, 1977]

Paramètres	Clé	Sécurité
$[1024, 524, 101]_2$	67ko	2^{62}
$[2048, 1608, 48]_2$	412ko	2^{96}

Familles proposées

Codes de Goppa Binaires [McEliece, 1977]

Paramètres	Clé	Sécurité
$[1024, 524, 101]_2$	67ko	2^{62}
$[2048, 1608, 48]_2$	412ko	2^{96}

Pas d'attaque structurelle connue à ce jour

Familles proposées

Codes de Reed–Solomon Généralisés (GRS)

[Niederreiter, 1986]

Paramètres	Clé	Sécurité
$[256, 128, 129]_{256}$	67ko	2^{95}

Familles proposées

Codes de Reed–Solomon Généralisés (GRS)

[Niederreiter, 1986]

Paramètres	Clé	Sécurité
$[256, 128, 129]_{256}$	67ko	2^{95}

[Sidelnikov Shestakov, 1992]
Attaque en $O(n^3)$

Familles proposées

Codes de Reed–Muller Binaires [Sidelnikov, 1994]

Paramètres	Clé	Sécurité
$[1024, 176, 128]_2$	22.5ko	2^{72}
$[2048, 232, 256]_2$	59.4ko	2^{93}

Familles proposées

Codes de Reed–Muller Binaires [Sidelnikov, 1994]

Paramètres	Clé	Sécurité
$[1024, 176, 128]_2$	22.5ko	2^{72}
$[2048, 232, 256]_2$	59.4ko	2^{93}

[Minder Shokrollahi, 2007]
Attaque sous-exponentielle.

Familles proposées

Codes géométriques [Janwa Moreno, 1996]

Paramètres	Clé	Sécurité
$[171, 109, 61]_{128}$	16ko	2^{66}

Familles proposées

Codes géométriques [Janwa Moreno, 1996]

Paramètres	Clé	Sécurité
$[171, 109, 61]_{128}$	16ko	2^{66}

Attaques Polynomiales
[Faure Minder, 2008], genre $\leqslant 2$
[C-, Márquez–Corbella, Pellikaan, 2014], genre quelconque

Familles proposées

Variantes avec clés compactes

- [Gaborit, 2005], codes BCH ;
  ($\sim$ 1.5 ko, Sécurité : $\geqslant 2^{80}$)
- [Berger, Cayrel, Gaborit, Otmani, 2009], codes alternants quasi-cycliques ;
  ($\sim$ 750 o, Sécurité : $\geqslant 2^{80}$)
- [Misoczki, Baretto, 2009], codes alternants quasi-diadiques.
  ($\sim$ 2.5 ko, Sécurité : $\geqslant 2^{80}$)

Familles proposées

Variantes avec clés compactes

- [Gaborit, 2005], codes BCH ;
  ($\sim$ 1.5 ko, Sécurité : $\geqslant 2^{80}$)
- [Berger, Cayrel, Gaborit, Otmani, 2009], codes alternants quasi-cycliques ;
  ($\sim$ 750 o, Sécurité : $\geqslant 2^{80}$)
- [Misoczki, Baretto, 2009], codes alternants quasi-diadiques.
  ($\sim$ 2.5 ko, Sécurité : $\geqslant 2^{80}$)

[Otmani, Tillich, Dallot, 2008]
[Faugère, Otmani, Perret, Tillich, 2010]
+ cf Exposé F. De Portzamparc

Familles proposées

Codes de Goppa Sauvages [Bernstein, Lange, Peters, 2010]

Des clés de 78 à 200ko d'une sécurité $> 2^{128}$.

Familles proposées

Codes de Goppa Sauvages [Bernstein, Lange, Peters, 2010]

Des clés de 78 à 200ko d'une sécurité $> 2^{128}$.

Non cassé,

Familles proposées

Codes de Goppa Sauvages [Bernstein, Lange, Peters, 2010]

Des clés de 78 à 200ko d'une sécurité $> 2^{128}$.

Non cassé, mais...

Codes de Reed Solomon généralisés

Définition

Soient

- $\boldsymbol{x} = (x_0, \ldots, x_{n-1})$ un n-uplet d'éléments de $\mathbb{F}_q$ deux à deux distincts.

Codes de Reed Solomon généralisés

Définition

Soient

- $\boldsymbol{x} = (x_0, \ldots, x_{n-1})$ un n-uplet d'éléments de $\mathbb{F}_q$ deux à deux distincts.
- $\boldsymbol{y} = (y_0, \ldots, y_{n-1})$ un n uplet d'éléments non nuls dans $\mathbb{F}_q$.

Codes de Reed Solomon généralisés

Définition

Soient

- $\boldsymbol{x} = (x_0, \ldots, x_{n-1})$ un n-uplet d'éléments de $\mathbb{F}_q$ deux à deux distincts.
- $\boldsymbol{y} = (y_0, \ldots, y_{n-1})$ un n uplet d'éléments non nuls dans $\mathbb{F}_q$.
- un entier $k < n$.

Codes de Reed Solomon généralisés

Définition

Soient

- $\boldsymbol{x} = (x_0, \ldots, x_{n-1})$ un n-uplet d'éléments de $\mathbb{F}_q$ deux à deux distincts.
- $\boldsymbol{y} = (y_0, \ldots, y_{n-1})$ un n uplet d'éléments non nuls dans $\mathbb{F}_q$.
- un entier $k < n$.

Le code $\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$ est défini par

$$\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y}) = \left\{ (y_0 f(x_0), \ldots, y_{n-1} f(x_{n-1})) \mid f \in \mathbb{F}_q[z]_{<k} \right\}.$$

Codes de Reed Solomon généralisés

Définition

Soient

- $\boldsymbol{x} = (x_0, \ldots, x_{n-1})$ un n-uplet d'éléments de $\mathbb{F}_q$ deux à deux distincts.
- $\boldsymbol{y} = (y_0, \ldots, y_{n-1})$ un n uplet d'éléments non nuls dans $\mathbb{F}_q$.
- un entier $k < n$.

Le code $\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$ est défini par

$$\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y}) = \left\{(y_0 f(x_0), \ldots, y_{n-1} f(x_{n-1})) \mid f \in \mathbb{F}_q[z]_{<k}\right\}.$$

Le vecteur $\boldsymbol{x}$ est appelé le *support* et le vecteur $\boldsymbol{y}$ le *multiplicateur*.

Codes de Reed Solomon généralisés

Theorème

Les paramètres de $\mathbf{GRS}_k(x, y)$ *sont*

- $\dim \mathbf{GRS}_k(x, y) = k$
- $d_{min}\mathbf{GRS}_k(x, y) = n - k + 1$

Codes Alternants

Définition

Soit $\mathscr{C} \subseteq \mathbb{F}_{q^m}^n$ un code sur $\mathbb{F}_{q^m}$, on définit son sous-code sur un sous-corps par

$$\mathscr{C} \cap \mathbb{F}_q^n.$$

Codes Alternants

Définition

Soit $\mathscr{C} \subseteq \mathbb{F}_{q^m}^n$ un code sur $\mathbb{F}_{q^m}$, on définit son sous-code sur un sous-corps par

$$\mathscr{C} \cap \mathbb{F}_q^n.$$

Proposition

Si $\mathscr{C} \subseteq \mathbb{F}_{q^m}^n$ a pour paramètres $[n, n-c, d]_{q^m}$, alors

$$\begin{aligned} \dim \mathscr{C} \cap \mathbb{F}_q^n &\geqslant n - mc \\ d_{min} \mathscr{C} \cap \mathbb{F}_q^n &\geqslant d. \end{aligned}$$

Codes Alternants

Définition

Soient $\boldsymbol{x} \in \mathbb{F}_{q^m}^n, \boldsymbol{y} \in \mathbb{F}_{q^m}^n$ comme dans la définition des GRS Le code $\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y})$ est défini par

$$\mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y}) \stackrel{\text{def}}{=} \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{\perp} \cap \mathbb{F}_q^n$$

Codes Alternants

Définition

Soient $x \in \mathbb{F}_{q^m}^n, y \in \mathbb{F}_{q^m}^n$ comme dans la définition des GRS Le code $\mathscr{A}_r(x, y)$ est défini par

$$\mathscr{A}_r(x, y) \stackrel{\text{def}}{=} \mathbf{GRS}_r(x, y)^{\perp} \cap \mathbb{F}_q^n$$

Proposition

$$\begin{aligned} \dim \mathscr{A}_r(x, y) &\geqslant n - mr \\ d_{min}\mathscr{A}_r(x, y) &\geqslant r + 1 \end{aligned}$$

Codes de Goppa

Définition

Soit $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ un support et $\Gamma \in \mathbb{F}_{q^m}[z]$ tel que $\forall i, \Gamma(x_i) \neq 0$, alors le code de Goppa $\mathscr{G}(\boldsymbol{x}, \Gamma)$ est défini par

$$\mathscr{G}(\boldsymbol{x}, \Gamma) = \mathscr{A}_{\deg \Gamma}(\boldsymbol{x}, \boldsymbol{y}),$$

avec $y_i = \frac{1}{\Gamma(x_i)}$.

Codes de Goppa

Définition

Soit $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ un support et $\Gamma \in \mathbb{F}_{q^m}[z]$ tel que $\forall i, \Gamma(x_i) \neq 0$, alors le code de Goppa $\mathscr{G}(\boldsymbol{x}, \Gamma)$ est défini par

$$\mathscr{G}(\boldsymbol{x}, \Gamma) = \mathscr{A}_{\deg \Gamma}(\boldsymbol{x}, \boldsymbol{y}),$$

avec $y_i = \frac{1}{\Gamma(x_i)}$.

Proposition

Les paramètres de code sont

$$\begin{aligned} \dim \mathscr{G}(\boldsymbol{x}, \Gamma) &\geqslant n - m \deg \Gamma \\ d_{min} \mathscr{G}(\boldsymbol{x}, \Gamma) &\geqslant \deg \Gamma + 1 \end{aligned}$$

Codes de Goppa sauvages

Theorème (Sugyiama et al. 1978)

Soit $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ *un support et* $\gamma \in \mathbb{F}_{q^m}[z]$ *irréductible, alors*

$$\mathscr{G}\left(\boldsymbol{x}, \gamma^{q-1}\right) = \mathscr{G}\left(\boldsymbol{x}, \gamma^{q}\right)$$

Codes de Goppa sauvages

Theorème (Sugyiama et al. 1978)

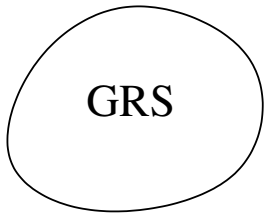
Soit $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ *un support et* $\gamma \in \mathbb{F}_{q^m}[z]$ *irréductible, alors*

$$\mathscr{G}\left(\boldsymbol{x}, \gamma^{q-1}\right) = \mathscr{G}\left(\boldsymbol{x}, \gamma^{q}\right)$$

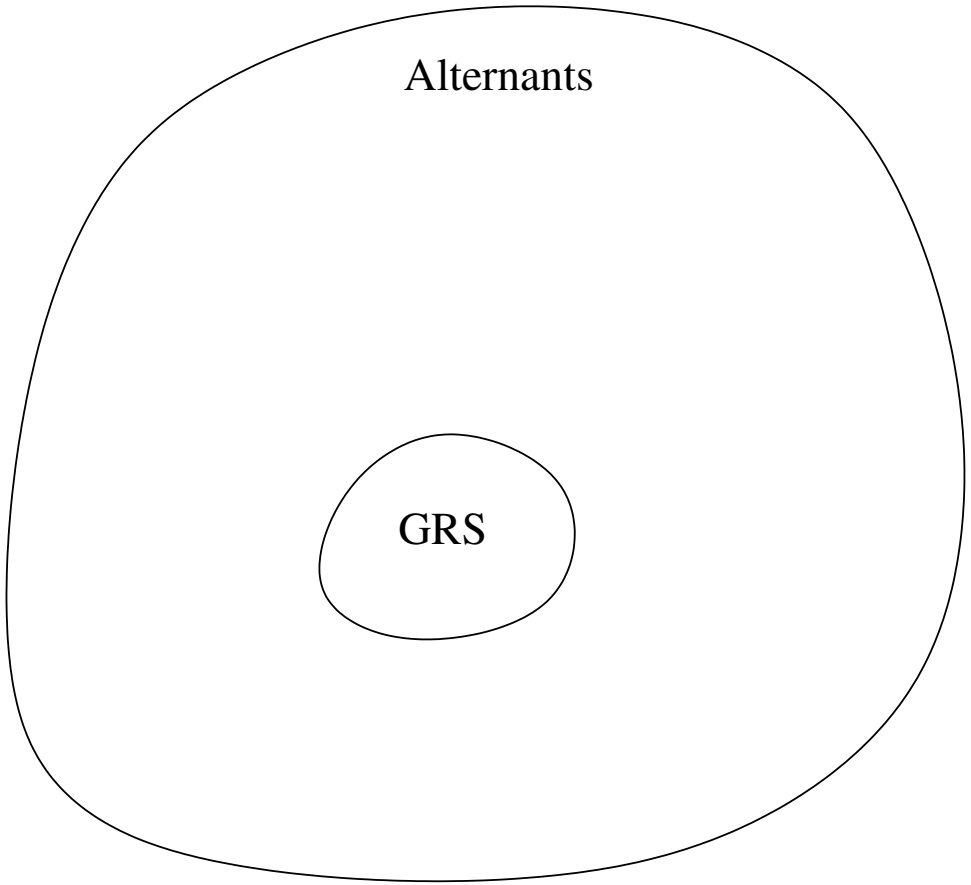
Un tel code est dit sauvage. *De plus ses paramètres sont de la forme*

$$\begin{aligned} \dim \mathscr{G}\left(\boldsymbol{x}, \gamma^{q}\right) &\geqslant n - m(q-1)\deg\gamma \\ d_{min}\mathscr{G}\left(\boldsymbol{x}, \gamma^{q}\right) &\geqslant q\deg\gamma + 1. \end{aligned}$$

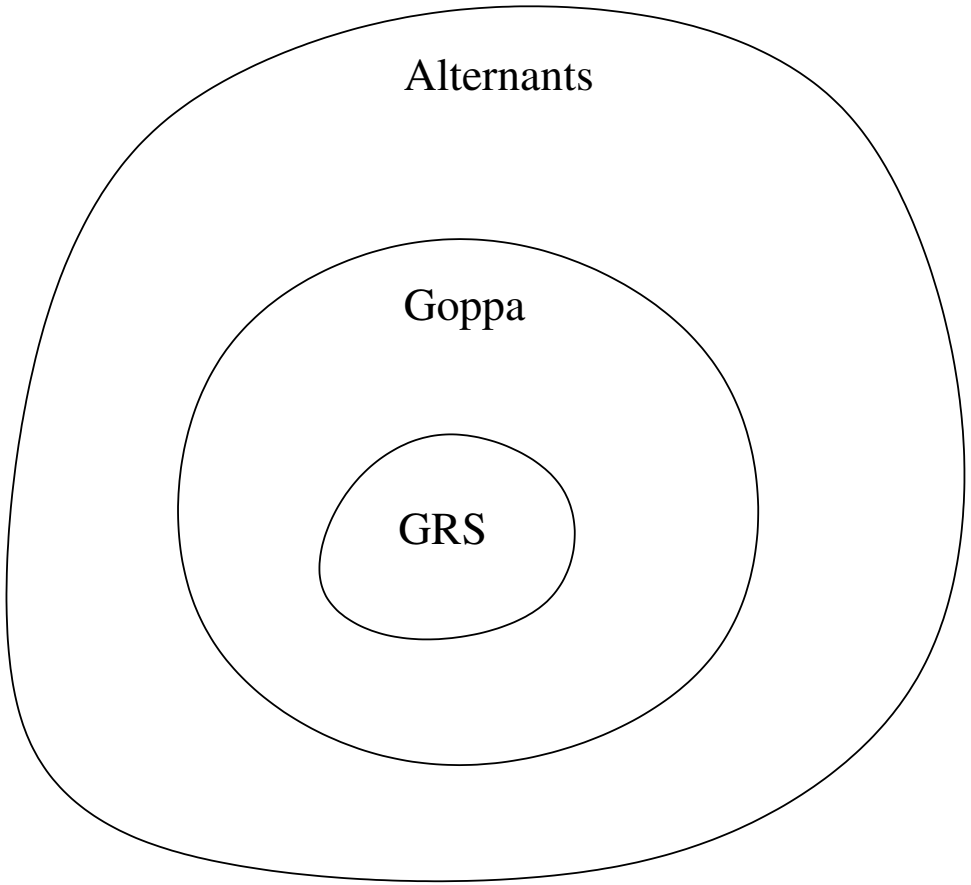
Un dessin



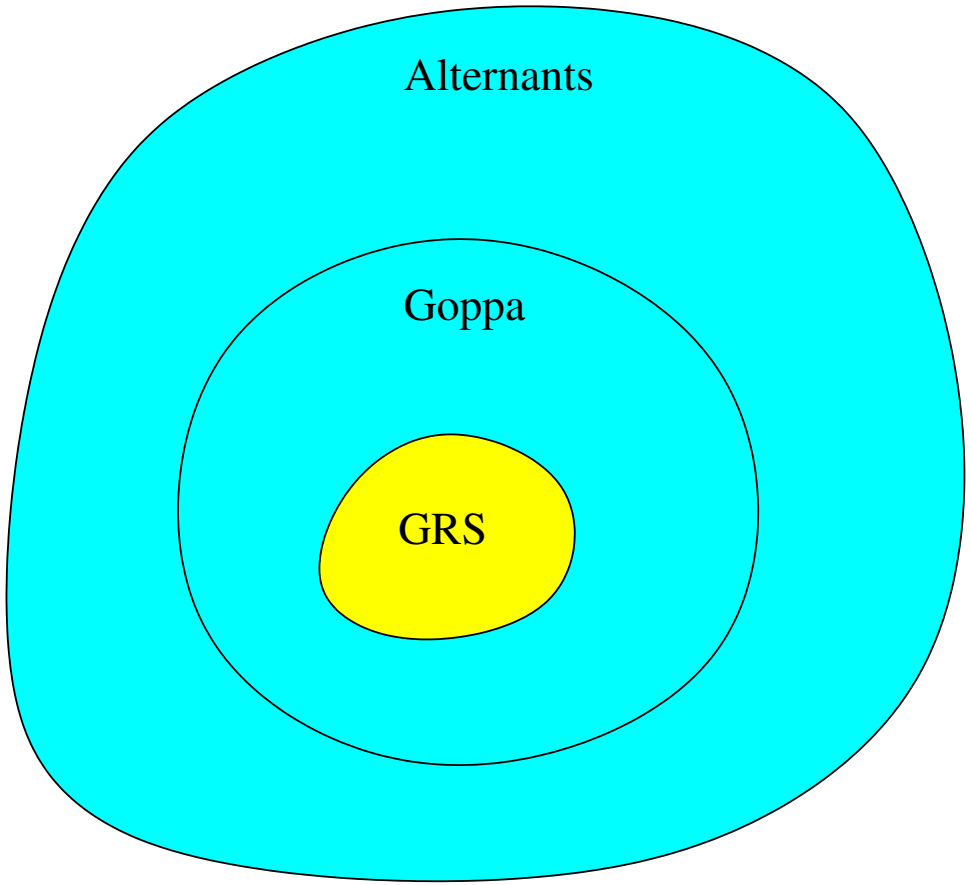
Un dessin



Un dessin

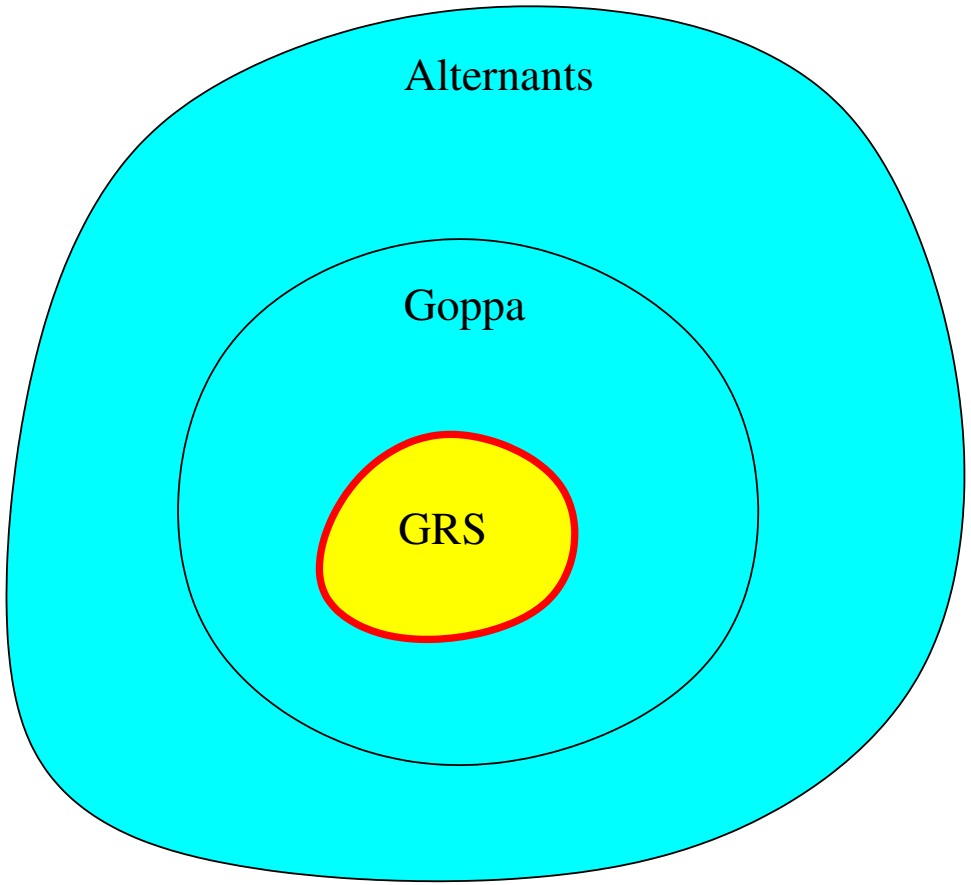


Un dessin



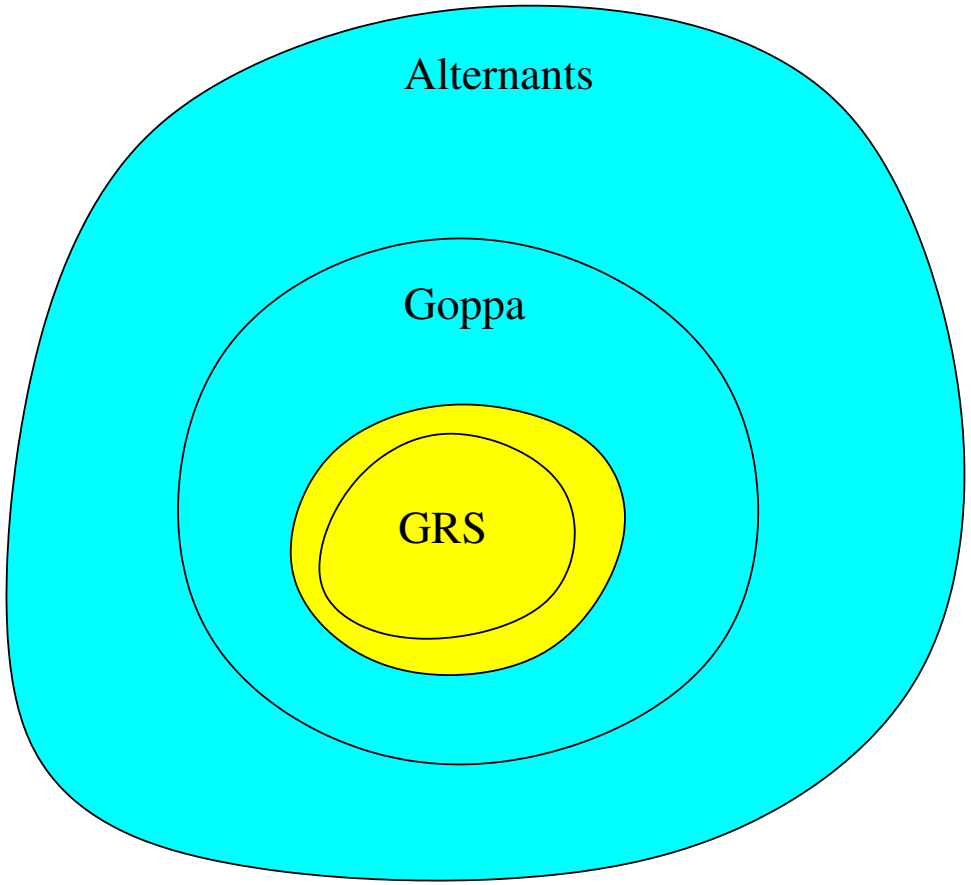
Avant : Cassé Non cassé

Un dessin



Avant : Cassé Non cassé

Notre contribution



Après : Cassé Non cassé

Produit $\star$ et codes carrés

Dans ce qui suit, on munit $\mathbb{F}_q^n$ du *produit de Schur* $\star$

$$c \star d \stackrel{\text{def}}{=} (c_0 d_0, \ldots, c_{n-1} d_{n-1}).$$

Définition

Soient $\mathscr{A}, \mathscr{B} \subseteq \mathbb{F}_q^n$, on définit

$$\mathscr{A} \star \mathscr{B} \stackrel{\text{def}}{=} \mathrm{Span}_{\mathbb{F}_q} \{ \boldsymbol{a} \star \boldsymbol{b} \mid \boldsymbol{a} \in \mathscr{A},\ \boldsymbol{b} \in \mathscr{B} \}.$$

Si $\mathscr{A} = \mathscr{B}$, on note $\mathscr{A}^{\star 2} \stackrel{\text{def}}{=} \mathscr{A} \star \mathscr{A}$.

Propriétés

Proposition

$$\dim \mathscr{A}^{\star 2} \leqslant \min \left\{ n, \binom{\dim \mathscr{A} + 1}{2} \right\}$$

Distingueur

Theorème (Faugère, Gautier-Umaña, Otmani, Perret, Tillich, 2013)

Soit $\mathscr{A}$ un code aléatoire de dimension k telle que $k = \circ(\sqrt{n})$,

$$\textbf{Prob}\left(\dim \mathscr{A}^2 < \binom{\dim \mathscr{A} + 1}{2}\right) \underset{n\to+\infty}{\longrightarrow} 0.$$

Distingueur

Theorème (Faugère, Gautier-Umaña, Otmani, Perret, Tillich, 2013)

Soit $\mathscr{A}$ un code aléatoire de dimension k telle que $k = \circ(\sqrt{n})$,

$$\textbf{Prob}\left(\dim \mathscr{A}^2 < \binom{\dim \mathscr{A} + 1}{2}\right) \underset{n\to+\infty}{\longrightarrow} 0.$$

De cette propriété on dispose d'une méthode pour distinguer certains codes algébriques de codes aléatoires.

Distingueur sur les GRS

Theorème

Soient $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$ *un support et un multiplicateur et* $k < n/2$. *Alors* $\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})^{\star 2} = \mathbf{GRS}_{2k-1}(\boldsymbol{x}, \boldsymbol{y}^{\star 2})$ *et donc :*

$$\dim \mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})^{\star 2} = 2k - 1.$$

Distingueur sur les GRS

Theorème

Soient $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}_q^n$ *un support et un multiplicateur et* $k < n/2$. *Alors* $\mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})^{\star 2} = \mathbf{GRS}_{2k-1}(\boldsymbol{x}, \boldsymbol{y}^{\star 2})$ *et donc :*

$$\dim \mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})^{\star 2} = 2k - 1.$$

Idée de Preuve.

$$(y_1 f(x_1), \ldots, y_n f(x_n)) \star (y_1 g(x_1), \ldots, y_n g(x_n)) = (y_1^2 h(x_1), \ldots, y_n^2 h(x_n))$$

où $h = fg$ est de degré $\leqslant 2k - 2$. □

Filtrations

À partir d'un distingueur on peut calculer une filtration du code :

$$\mathscr{C} \supseteq \mathscr{C}_1 \supseteq \mathscr{C}_2 \supseteq \cdots \supseteq \mathscr{C}_s \supseteq \cdots$$

Filtrations

À partir d'un distingueur on peut calculer une filtration du code :

$$\mathscr{C} \supseteq \mathscr{C}_1 \supseteq \mathscr{C}_2 \supseteq \cdots \supseteq \mathscr{C}_s \supseteq \cdots$$

Mots et polynômes

Important : À tout mot correspond un unique polynôme

$$\boldsymbol{c} \in \mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y}) \quad \longleftrightarrow \quad \begin{cases} p_{\boldsymbol{c}} \in \mathbb{F}_{q^2}[z], \\ \deg(p_{\boldsymbol{c}}) < k \end{cases}$$

$$\boldsymbol{c} \in \mathscr{G}(\boldsymbol{x}, \Gamma) \quad \longrightarrow \quad \begin{cases} p_{\boldsymbol{c}} \in \mathbb{F}_{q^2}[z], \\ \deg(p_{\boldsymbol{c}}) < n - \deg(\Gamma) \end{cases}$$

Un exemple pédagogique sur les GRS

Clé publique : $\mathscr{C} = \mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$ avec $k < n/2$

Un exemple pédagogique sur les GRS

Clé publique : $\mathscr{C} = \mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$ avec $k < n/2$

Hypothèse farfelue : On connait aussi $\mathbf{GRS}_{k-1}(\boldsymbol{x}, \boldsymbol{y})$.

Un exemple pédagogique sur les GRS

Clé publique : $\mathscr{C} = \mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$ avec $k < n/2$

Hypothèse farfelue : On connait aussi $\mathbf{GRS}_{k-1}(\boldsymbol{x}, \boldsymbol{y})$.

Point de vue polynômes, on connait : $\mathbb{F}_q[z]_{\leqslant k-1}$ et $\mathbb{F}_q[z]_{\leqslant k-2}$ Alors :

Proposition

$\mathbf{GRS}_{k-2}(\boldsymbol{x}, \boldsymbol{y})$ *est l'ensemble des solutions du problème*

$$\begin{cases} c \in \mathbf{GRS}_{k-1}(\boldsymbol{x}, \boldsymbol{y}) \\ c \star \mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y}) \subseteq \mathbf{GRS}_{k-1}(\boldsymbol{x}, \boldsymbol{y})^{\star 2} \end{cases}$$

Un exemple pédagogique sur les GRS

Clé publique : $\mathscr{C} = \mathbf{GRS}_k(x, y)$ avec $k < n/2$

Hypothèse farfelue : On connait aussi $\mathbf{GRS}_{k-1}(x, y)$.

Point de vue polynômes, on connait : $\mathbb{F}_q[z]_{\leqslant k-1}$ et $\mathbb{F}_q[z]_{\leqslant k-2}$ Alors :

Proposition

$\mathbf{GRS}_{k-2}(x, y)$ *est l'ensemble des solutions du problème*

$$\begin{cases} c \in \mathbf{GRS}_{k-1}(x, y) \\ c \star \mathbf{GRS}_k(x, y) \subseteq \mathbf{GRS}_{k-1}(x, y)^{\star 2} \end{cases}$$

Idée de preuve.

$$p \in \mathbb{F}_q[z]_{\leqslant k-3} \iff p \cdot \underbrace{\mathbb{F}_q[z]_{\leqslant k-1}}_{\boldsymbol{GRS}_k} \subseteq \underbrace{\mathbb{F}_q[z]_{\leqslant 2k-4}}_{\boldsymbol{GRS}_{k-1}^{\star 2}}$$

Attaque par filtration

Par cette manière, on calcule de manière itérée

$$\boldsymbol{GRS}_k \supseteq \boldsymbol{GRS}_{k-1} \supseteq \ldots \supseteq \boldsymbol{GRS}_1$$

et

$$\begin{aligned} \boldsymbol{GRS}_1 &= \left\{ (y_1 f(x_1), \ldots, y_n f(x_n)) \mid \deg f = 0 \right\} \\ &= \mathrm{Span}\{\boldsymbol{y}\}. \end{aligned}$$

On en déduit ainsi le multiplicateur $\boldsymbol{y}$.

Attaque par filtration

Par cette manière, on calcule de manière itérée

$$\boldsymbol{GRS}_k \supseteq \boldsymbol{GRS}_{k-1} \supseteq \ldots \supseteq \boldsymbol{GRS}_1$$

et

$$\begin{aligned} \boldsymbol{GRS}_1 &= \left\{ (y_1 f(x_1), \ldots, y_n f(x_n)) \mid \deg f = 0 \right\} \\ &= \mathrm{Span}\{\boldsymbol{y}\}. \end{aligned}$$

On en déduit ainsi le multiplicateur $\boldsymbol{y}$.

Remarque

Du point de vue des polynômes la filtration ci-dessus n'est autre que

$$\mathbb{F}_q[z]_{\leqslant k-1} \supseteq \mathbb{F}_q[z]_{\leqslant k-2} \supseteq \cdots \supseteq \mathbb{F}_q[z]_{\leqslant 0}$$

Quelle filtration choisir ?

On n'a pas de raison de connaître à la fois $\boldsymbol{GRS}_k$ et $\boldsymbol{GRS}_{k-1}$. Par contre, on peut considérer la filtration correspondant à

$$\mathbb{F}_q[z]_{\leqslant k-1} \supseteq z\mathbb{F}_q[z]_{\leqslant k-2} \supseteq \cdots \supseteq z^{\ell-1}\mathbb{F}_q[z]_{\leqslant k-\ell} \supseteq \cdots$$

Les deux premiers termes de la filtration sont connus.

- Le premier $\mathscr{C} = \mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$
- Le second : son raccourci en la première position (on peut supposer w.l.o.g. que $x_1 = 0$).

Quelle filtration choisir ?

On n'a pas de raison de connaître à la fois $\boldsymbol{GRS}_k$ et $\boldsymbol{GRS}_{k-1}$. Par contre, on peut considérer la filtration correspondant à

$$\mathbb{F}_q[z]_{\leqslant k-1} \supseteq z\mathbb{F}_q[z]_{\leqslant k-2} \supseteq \cdots \supseteq z^{\ell-1}\mathbb{F}_q[z]_{\leqslant k-\ell} \supseteq \cdots$$

Les deux premiers termes de la filtration sont connus.

- Le premier $\mathscr{C} = \mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$
- Le second : son raccourci en la première position (on peut supposer w.l.o.g. que $x_1 = 0$).

$$\begin{pmatrix} 1 & * & \cdots & * \\ 0 & a'_{11} & \cdots & a'_{1,n-1} \\ \vdots & \vdots & & \vdots \\ 0 & a'_{n-1,1} & \cdots & a'_{n-1,n-1} \end{pmatrix}$$

Quelle filtration choisir ?

On n'a pas de raison de connaître à la fois $\boldsymbol{GRS}_k$ et $\boldsymbol{GRS}_{k-1}$. Par contre, on peut considérer la filtration correspondant à

$$\mathbb{F}_q[z]_{\leqslant k-1} \supseteq z\mathbb{F}_q[z]_{\leqslant k-2} \supseteq \cdots \supseteq z^{\ell-1}\mathbb{F}_q[z]_{\leqslant k-\ell} \supseteq \cdots$$

Les deux premiers termes de la filtration sont connus.

- Le premier $\mathscr{C} = \mathbf{GRS}_k(\boldsymbol{x}, \boldsymbol{y})$
- Le second : son raccourci en la première position (on peut supposer w.l.o.g. que $x_1 = 0$).

$$\begin{pmatrix} 1 & * & \cdots & * \\ 0 & a'_{11} & \cdots & a'_{1,n-1} \\ \vdots & \vdots & & \vdots \\ 0 & a'_{n-1,1} & \cdots & a'_{n-1,n-1} \end{pmatrix}$$

Pour des Alternants

On a

$$\begin{aligned} \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y}) &= \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{\perp} \cap \mathbb{F}_q^n \\ &= \mathbf{GRS}_{n-r}(\boldsymbol{x}, \boldsymbol{y}') \cap \mathbb{F}_q^n \end{aligned}$$

et

$$\dim \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y}) \geqslant n - mr.$$

Pour des Alternants

On a

$$\begin{aligned} \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y}) &= \mathbf{GRS}_r(\boldsymbol{x}, \boldsymbol{y})^{\perp} \cap \mathbb{F}_q^n \\ &= \mathbf{GRS}_{n-r}(\boldsymbol{x}, \boldsymbol{y}') \cap \mathbb{F}_q^n \end{aligned}$$

et

$$\dim \mathscr{A}_r(\boldsymbol{x}, \boldsymbol{y}) \geqslant n - mr.$$

Fait

Pour distinguer, il faudrait

$$n - r < n/2 \quad \Longrightarrow \quad r > n/2,$$

mais

$$m > 1 \quad \Longrightarrow n - mr < 0.$$

Distingueur par raccourcissement

Theorème (C-, Otmani, Tillich 2013)

Si $m = 2$ *et* $\gamma \in \mathbb{F}_{q^2}[z]$ *un polynôme irréductible de degré* r

(i) $\mathscr{G}\left(\boldsymbol{x}, \gamma^{q-1}\right) = \mathscr{G}\left(\boldsymbol{x}, \gamma^{q+1}\right)$;

(ii) $\dim \mathscr{G}\left(\boldsymbol{x}, \gamma^{q}\right) \geqslant n - \underbrace{m}_{=2} r(q-1)$

Distingueur par raccourcissement

Theorème (C-, Otmani, Tillich 2013)

Si $m = 2$ *et* $\gamma \in \mathbb{F}_{q^2}[z]$ *un polynôme irréductible de degré* r

(i) $\mathscr{G}\left(\boldsymbol{x}, \gamma^{q-1}\right) = \mathscr{G}\left(\boldsymbol{x}, \gamma^{q+1}\right)$;

(ii) $\dim \mathscr{G}\left(\boldsymbol{x}, \gamma^{q}\right) \geqslant n - \underbrace{m}_{=2} r(q-1) + r(r-2)$

Distingueur par raccourcissement

Theorème (C-, Otmani, Tillich 2013)

Si $m = 2$ *et* $\gamma \in \mathbb{F}_{q^2}[z]$ *un polynôme irréductible de degré* r

(i) $\mathscr{G}\left(\boldsymbol{x}, \gamma^{q-1}\right) = \mathscr{G}\left(\boldsymbol{x}, \gamma^{q+1}\right)$;

(ii) $\dim \mathscr{G}\left(\boldsymbol{x}, \gamma^{q}\right) \geqslant n - \underbrace{m}_{=2} r(q-1) + r(r-2)$

Theorème (C-, Otmani, Tillich 2014)

Les raccourcis de ces codes en a *positions sont distinguables pour* $a \in \{a^-, \ldots, a^+\}$ *et*

$$
\begin{aligned}
a^- &= n - 2r(q+1) - 1 \\
a^+ &= \max\left\{ a \geqslant 0 \;\middle|\; \begin{array}{c} 3(n-a) - 4r(q+1) - 2 \leqslant \\ \min\left\{ n-a, \binom{n-a-2r(q-1)+r(r-2)}{2} \right\} \end{array} \right\}
\end{aligned}
$$

Goppa sauvages distinguables (pour $m = 2$)

Table : Plus grande valeur de q pour laquelle on peut espérer distinguer $\mathscr{G}\left(\boldsymbol{x}, \gamma^{q-1}\right)$ avec γ irreductible de degré r.

r	2	3	4	5
q	9	19	37	64

Notre attaque

La clé publique $\mathscr{C}$ est le code $\mathscr{G}\left(\boldsymbol{x}, \gamma^{q-1}\right)$, avec $m = 2$.

Notre attaque

La clé publique $\mathscr{C}$ est le code $\mathscr{G}\left(\boldsymbol{x}, \gamma^{q-1}\right)$, avec $m = 2$.

Fait

Sans perte de généralité on peut supposer

$$x_0 = 0 \quad et \quad x_1 = 1.$$

Notre attaque

Étape 1 : calcul de filtrations. On calcule en utilisant le distingueur les filtrations associées à

$$\mathbb{F}_{q^2}[z]_{\leqslant s} \supseteq z\mathbb{F}_{q^2}[z]_{\leqslant s-1} \supseteq \cdots \supseteq z^{q+1}\mathbb{F}_{q^2}[z]_{\leqslant s-(q+1)}$$

où $s = n - r(q+1) - 1$.

Notre attaque

Étape 1 : calcul de filtrations. On calcule en utilisant le distingueur les filtrations associées à

$$\mathbb{F}_{q^2}[z]_{\leqslant s} \supseteq z\mathbb{F}_{q^2}[z]_{\leqslant s-1} \supseteq \cdots \supseteq z^{q+1}\mathbb{F}_{q^2}[z]_{\leqslant s-(q+1)}$$

où $s = n - r(q+1) - 1$.

Les deux premiers termes de cette filtration s'obtiennent en raccourcissant le code en la première position.

Notre attaque

Étape 2 : calcul de $x^{\star(q+1)}$

On note $\mathscr{C}_{q+1}$ le code associé à $z^{q+1}\mathbb{F}_{q^2}[z]_{\leqslant s-(q+1)}$.

Lemme

$$x^{\star(-(q+1))} \star \mathscr{C}_{q+1} \subseteq \mathscr{C}.$$

Notre attaque

Étape 2 : calcul de $x^{\star(q+1)}$

On note $\mathscr{C}_{q+1}$ le code associé à $z^{q+1}\mathbb{F}_{q^2}[z]_{\leqslant s-(q+1)}$.

Lemme

$$x^{\star(-(q+1))} \star \mathscr{C}_{q+1} \subseteq \mathscr{C}.$$

Idée de preuve.

Soient $c \in \mathscr{C}_{q+1}$ et p_c le polynôme correspondant. p_c est de la forme

$$p_c(z) = z^{q+1} f(z), \qquad \deg q_c \leqslant s - (q+1).$$

Notre attaque

Étape 2 : calcul de $x^{\star(q+1)}$

On note $\mathscr{C}_{q+1}$ le code associé à $z^{q+1}\mathbb{F}_{q^2}[z]_{\leqslant s-(q+1)}$.

Lemme

$$\boldsymbol{x}^{\star(-(q+1))} \star \mathscr{C}_{q+1} \subseteq \mathscr{C}.$$

Idée de preuve.

Soient $\boldsymbol{c} \in \mathscr{C}_{q+1}$ et $p_{\boldsymbol{c}}$ le polynôme correspondant. $p_{\boldsymbol{c}}$ est de la forme

$$p_{\boldsymbol{c}}(z) = z^{q+1} f(z), \qquad \deg q_{\boldsymbol{c}} \leqslant s-(q+1).$$

Pour tout $x \in \mathbb{F}_{q^2}$, $x^{q+1} \in \mathbb{F}_q$ (c'est $\mathrm{N}_{\mathbb{F}_{q^2}/Fq}(x)$).

Si $x_i^{q+1} q(x_i) \in \mathbb{F}_q$ pour tout i, alors $q(x_i) \in \mathbb{F}_q$ et donc à q correspond le mot $\boldsymbol{x}^{\star-(q+1)} \star \boldsymbol{c} \in \mathscr{C}$ □

Notre attaque

Étape 2 : calcul de $\boldsymbol{x}^{\star(q+1)}$

$\boldsymbol{x}^{\star(q+1)}$ est solution du problème d'inconnue $\boldsymbol{t}$:

$$\mathscr{C}_{q+1} \subseteq \boldsymbol{t} \star \mathscr{C}.$$

Notre attaque

Étape 2 : calcul de $x^{\star(q+1)}$

$x^{\star(q+1)}$ est solution du problème d'inconnue t :

$$\mathscr{C}_{q+1} \subseteq t \star \mathscr{C}.$$

Remarque

On montre que ce calcul revient à résoudre un système de taille $\leqslant n^2 \times n$ (coût $O(n^4)$) puis à faire une recherche exhaustive dans un code de dimension 4 (coût $O(q^3) = O(n\sqrt{n})$).

Notre Attaque

On dispose de x^{q+1} et après ?...

Notre Attaque

On dispose de $\boldsymbol{x}^{q+1}$ et après ?... On peut calculer $(\boldsymbol{x}-\mathbf{1})^{\star(q+1)}$ par la même méthode !

Notre Attaque

On dispose de $\boldsymbol{x}^{q+1}$ et après ?... On peut calculer $(\boldsymbol{x}-\mathbf{1})^{\star(q+1)}$ par la même méthode !

Lemme

Soit $x \in \mathbb{F}_{q^2}$, si on connaît $N(x)$ et $N(x-1)$ alors on connaît le polynôme minimal de x

Démonstration.

Notre Attaque

On dispose de x^{q+1} et après ?... On peut calculer $(x-1)^{\star(q+1)}$ par la même méthode !

Lemme

Soit $x \in \mathbb{F}_{q^2}$, si on connaît $N(x)$ et $N(x-1)$ alors on connaît le polynôme minimal de x

Démonstration.

$$\begin{aligned}(x-1)^{q+1} &= (x-1)(x-1)^q = (x-1)(x^q-1) \\ &= \underbrace{x^{q+1}}_{\text{Connu}} - \underbrace{(x^q+x)}_{=\mathrm{Tr}_{\mathbb{F}_{q^2}/Fq}(x)} +1.\end{aligned}$$

Notre Attaque

On dispose de x^{q+1} et après ?... On peut calculer $(x-1)^{\star(q+1)}$ par la même méthode !

Lemme

Soit $x \in \mathbb{F}_{q^2}$, si on connaît $N(x)$ et $N(x-1)$ alors on connaît le polynôme minimal de x

Démonstration.

$$\begin{aligned}(x-1)^{q+1} &= (x-1)(x-1)^q = (x-1)(x^q-1)\\ &= \underbrace{x^{q+1}}_{\text{Connu}} - \underbrace{(x^q+x)}_{=\mathrm{Tr}_{\mathbb{F}_{q^2}/Fq}(x)} +1.\end{aligned}$$

Or le polynôme minimal de x est

$$z^2 - \mathrm{Tr}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x)z + \mathrm{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x).$$

Notre Attaque

On dispose donc de la connaissance du support $\boldsymbol{x}$ à action Galoisienne près. Le calcul de $\boldsymbol{x}$ et $\boldsymbol{y}$ tel que $\mathscr{C} = \mathscr{A}_{r(q+1)}(\boldsymbol{x}, \boldsymbol{y})$ se ramène à de l'algèbre linéaire (un peu technique).

Notre Attaque

On dispose donc de la connaissance du support $\boldsymbol{x}$ à action Galoisienne près. Le calcul de $\boldsymbol{x}$ et $\boldsymbol{y}$ tel que $\mathscr{C} = \mathscr{A}_{r(q+1)}(\boldsymbol{x}, \boldsymbol{y})$ se ramène à de l'algèbre linéaire (un peu technique).

Complexité et temps de calcul

La complexité de l'attaque est en $O(n^5)$
(plus précisément $O(n^4\sqrt{n} + n^4(q^2 - n))$).

Table : Temps de calcul obtenus avec un processeur Intel® Xeon 2.27GHz

$[q, n, k, r]$	[29,781, 516,5]	[29, 791, 575, 4]	[29,794,529,5]
Average time	16min	19.5min	15.5min

(q, n, k, r)	[31, 795, 563, 4]	[31,813, 581,4]	[31, 851, 619, 4]
Average time	31.5min	31.5min	27.2min

(q, n, k, r)	[32,841,601,4]
Average time	49.5min

Conclusion

- Première attaque polyomiale sur des codes de Goppa classiques.

Conclusion

- Première attaque polyomiale sur des codes de Goppa classiques.
- Première attaque polynomiale sur des codes *sans aucune structure apparente*

Conclusion

- Première attaque polyomiale sur des codes de Goppa classiques.
- Première attaque polynomiale sur des codes *sans aucune structure apparente*
- Et après ?

Conclusion

- Première attaque polyomiale sur des codes de Goppa classiques.
- Première attaque polynomiale sur des codes *sans aucune structure apparente*
- Et après ? D'autres distingueurs ?

Conclusion

- Première attaque polyomiale sur des codes de Goppa classiques.
- Première attaque polynomiale sur des codes *sans aucune structure apparente*
- Et après ? D'autres distingueurs ? Peut-on transformer tout distingueur en un attaque ?

Merci de votre attention