# Signature sur les codes correcteurs en métrique rang

P.Gaborit, O.Ruatta, **Julien Schrek** et G.Zémor

Université de Limoges,XLIM-DMI

25 mars 2014

# Plan

# Notations

- $GF(q)$ un corps fini avec $q$ une puissance de premier.
- $GF(q^m)$ une extention de degré $m$ de $GF(q)$.
- $B = (b_1, ..., b_m)$ une base de $GF(q^m)$ sur $GF(q)$.

**$GF(q^m)$ peut être vu comme un espace vectoriel sur $GF(q)$.**

- $\mathcal{C}$ un code linéaire sur $GF(q^m)$ de dimension $k$ et de taille $n$.
- $G$ une matrice génératrice $k \times n$ du code $\mathcal{C}$.
- $H$ une matrice de parité $(n-k) \times n$ de $\mathcal{C}$, $G.H^t = 0$.

# Métrique rang

## Métrique rang

Introduite en 1985 par Gabidulin pour les codes correcteurs.

Soit

$$v = (v_1, \ldots, v_n)$$

avec $v_i \in GF(q^m)$.
Pour chaque coordonnée $v_i = \sum_{j=1}^{m} v_{ij} b_j$ avec $v_{ij} \in GF(q)$.

$$V = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{pmatrix}$$

# Définitions

## Définition (Rang d'un mot)

*$Rang(v) = r$ ssi le rang de $V = (v_{ij})$ est $r$.*

**Le rang de $v$ ne dépend pas de la base.**

## Définition (Distance rang)

*Soit $x, y \in GF(q^m)^n$, la distance rang entre $x$ et $y$ est définie par $d_R(x, y) = Rang(x - y)$.*

# Propriétés

## Proposition

Soit $e \in GF(q^m)^n$ de rang $r$, alors $e = \beta U$ avec :

- $\beta$ dans $GF(q^m)^r$ (coefficients linéairements indépendants sur $GF(q)$)
- $U$ une matrice $r \times n$ à coefficients dans $GF(q)$.

## Définition (Support)

*Soit $e$ un mot de $GF(q^m)$. On appelle support de $e$ ($Supp(e)$) l'espace vectoriel sur $GF(q)$ engendré par les coordonnées de $e$.*

## Remarque

Dans la décomposition (non-unique) $e = \beta U$, le support de $e$ est associé au vecteur $\beta$.

# Problème de décodage par syndrome

## Problème de décodage par syndrome

Soit $H$ la matrice de parité d'un code $\mathcal{C}$ de taille $(n-k) \times n$.
Soit $s$ un syndrome de taille $n-k$.
Existe-t-il un mot $e$ de rang $r$ tel que $He^T = s$ ?

En métrique rang :

- *A priori* post-quantique
- Pas prouvé NP-Complet
- Proche de pb NP-Complet : SD Hamming, MinRank
- La complexité des attaque donne des clés plus petite en général

# Meilleures attaques

Il y a deux types d'attaques sur le problème de décodage en métrique rang.

- Les attaques combinatoires
- Les attaques algébriques

**Pas de meilleure attaque.**
**L'efficacité de l'attaque dépend des paramètres.**

# Attaques sur le décodage par syndrome

**Historique des attaques :**

- Première attaque par Chabaud-Stern en 1996 : énumération des bases
- Amélioration de A.Ourivski et T.Johannson en 2002
  - Enumération de base : $\leq (k+r)^3 q^{(r-1)(m-r)+2}$
  - Enumération des coordonnées : $\leq (k+r)^3 r^3 q^{(r-1)(k+1)}$
- Amélioration de P.Gaborit,O.Ruatta et J.Schrek en 2012 :
  - Attaque sur le support : $\mathcal{O}(q^{(r-1)\frac{\lfloor (k+1)m \rfloor}{n}})$
  - Attaque algébrique utilisant des bases de Gröbner

# Nouvelle signatures en métrique rang

**Différentes approches :**

- Signatures par inversion
  - Inverse unique : RSA,CFS
  - Plusieurs inverses : NTRUSign, GGH, GPV
- Signatures par preuve de connaissance
  - Par construction : Schnorr, DSA, Lyubashevsky (lattices 2013)
  - Générique : transformation de Fiat-Shamir
- Signatures one-time : KKS 1997, Lyubashevsky 2008

# Nouvelle approche pour la métrique rang

Deux approches pour inverser le calcul de syndrome :

- CFS : **sous GV** et recherche d'une solution inversible.
- GPV, NTRUSign, GGH : **au delà de Gauss** (approximation du syndrome).
  $\rightarrow$ meilleurs paramètres
  $\rightarrow$ fuites d'information potentielles

La nouvelle approche utilise cette deuxième approche en métrique rang.

# Nouvelle Idée

## Idée

Trouver un mot de petit poids au delà de GV pour être sûr qu'il existe une solution.

## Mise en place

On se restreint à chercher une solution parmi les mots ayant le même support.

## Solution

On utilise les codes LRPC car leur décodage permet de fixer un support aléatoire en entrée.

# Code LRPC

## Low Rank Parity Code

$\rightarrow$ Matrice de parité avec coeff dans un e.v. de dimension $d$.

## Construction

- Choisir un ensemble de vecteurs linéairements indépendants dans $GF(q^m) : F = \{F_1, \ldots, F_d\}$.
- Génèrer chaque coefficient de la matrice de parité du code à l'aide d'une combinaison aléatoire de $\{F_1, \ldots, F_d\}$.

# Décodage LRPC

**Entrée** $T =< T_1, \cdots, T_t >$, $H$ une matrice LRPC, un syndrome $s$
**Sortie** : $e$ de rang $r$ avec $T \subset Supp(e)$.

1. **Transformation du syndrome**
   a) Calcul de $B = \{F_1 T_1, \cdots, F_d T_t\}$ de l'espace produit $< F.T >$.
   b) Calcul du sous-espace $S =< B \cup \{s_1, \cdots, s_{n-k}\} >$.

2. **Reformer le support $E$ de l'erreur**
   Définir $S_i = F_i^{-1} S$, calculer $E = S_1 \cap S_2 \cap \cdots \cap S_d$, et en déduire une base $\{E_1, E_2, \cdots, E_r\}$ de $E$.

3. **Reformer le vecteur $e$**
   Ecrire $e_i = \sum_{i=1}^{n} e_{ij} E_j$, et résoudre le système linéaire.

# Schéma

## Clé privée

A : inversible dans $GF(q^m)^{(n-k)\times(n-k)}$
P : inversible dans $GF(q)^{(n+t)\times(n+t)}$
H : matrice de parité d'un code LRPC augmenté

## Clé publique

H' = AHP

## Signature de $m$

1. $i \leftarrow 0$
2. Décodage de $h(m|i)$ avec le code LRPC augmenté et un support aléatoire $T$.
3. Si ce n'est pas possible, $i \leftarrow i+1$ et retour au point 2.

# Fuite d'information

Le principal problème pour ce type de signature est la fuite d'information

**Idée de la preuve**

Algorithme de signature $\rightarrow$ signature valide aléatoire uniforme
Donc pas de fuite avec une probabilité de $1 - 1/q$.

**La fuite d'information est évaluée et les paramètres sont choisis pour contrer cette faille théorique.**

# Paramètres

| n | n-k | m | q | d | GVR | Singleton | clé pub. (bits) | sign. (bits) | sécurité |
|---|---|---|---|---|---|---|---|---|---|
| 16 | 8 | 18 | $2^{40}$ | 2 | 5 | 8 | 57600 | 8640 | 130 |
| 16 | 8 | 18 | $2^{8}$ | 2 | 5 | 8 | 11520 | 1728 | 80 |
| 16 | 8 | 18 | $2^{16}$ | 2 | 5 | 8 | 23040 | 3456 | 120 |
| 20 | 10 | 24 | $2^{8}$ | 2 | 6 | 10 | 24960 | 3008 | 104 |
| 27 | 9 | 20 | $2^{6}$ | 3 | 4 | 7 | 23328 | 1470 | 120 |
| 48 | 12 | 40 | $2^{4}$ | 4 | 6 | 10 | 78720 | 2976 | 114 |
| 50 | 10 | 42 | $2^{4}$ | 5 | 5 | 9 | 70560 | 2800 | 104 |

# Conclusion sur la signature

- *A priori* post-quantique
- Clée de 11 520 bits / Signature de 1728 bits
- Evaluation et prise en compte de la fuite d'information
- Densité proche de 1 et probabilité d'échec de $1/q$

# MERCI