Codes en métriques rang et applications en cryptographie *†

par Olivier Ruatta

XLIM UMR 7252 Université de Limoges - CNRS

*. Travaux communs avec : Gaëtan Murat, Julien Schrek, Nicolas Aragon, Adrien Hauteville, Philippe Gaborit, Gilles Zemor, Victor Dysern, Alain Couvreur, ...

†. Ce document a été rédigé avec GNU TEXMACS ; voir `www.texmacs.org`.

Soit $q = p^s$ avec p premier, on note $\mathbb{F}_q$ un corps a q éléments.

Soit E et F deux $\mathbb{F}_q$-espaces vectoriels, on note $\mathcal{L}(E, F)$ le $\mathbb{F}_q$-espace vectoriel des applications $\mathbb{F}_q$-linéaire de E dans F.

Proposition 1. *L'application* $\mathrm{rk}: \begin{cases} \mathcal{L}(E,F) \times \mathcal{L}(E,F) \longrightarrow \mathbb{N} \\ (\mathcal{U}, \mathcal{V}) \longmapsto \mathrm{rk}(\mathcal{U} - \mathcal{V}) \end{cases}$ *est une distance sur* $\mathcal{L}(E, F)$.

Définition 2. *Un code en métrique rang est un sous-espace vectoriel de* $\mathcal{L}(E, F)$.

Premier exemple : codes matriciels (Delsartes 78)

Exemple 3. Soit $\mathcal{M}_{n\times n}(\mathbb{F}_q)$ l'e.v. des matrices $n\times n$ à coefficients dans $\mathbb{F}_q$ et V un s.e.v. de $\mathcal{M}_{n\times n}(\mathbb{F}_q)$. Alors V est un code en métrique rang.

Exemple 4. Soient m et $n\in\mathbb{N}$, on note $\mathbb{F}_{q^m}$ une extension de $\mathbb{F}_q$ de degré m engendré ar $\beta_1,\cdots,\beta_m$ et soit V un $\mathbb{F}_{q^m}$-s.e.v. de $(\mathbb{F}_{q^m})^n$. Pour tout $\boldsymbol{v}=(v_1,\cdots,v_n)\in(\mathbb{F}_{q^m})^n$, et pour tout $i\in\{1,\cdots,n\}$, on a $v_i=\sum_{j=1}^{m} v_{j,i}\cdot\beta_j$, on associe alors à $\boldsymbol{v}$:

$$M_{\boldsymbol{v}}=\begin{pmatrix} v_{1,1} & v_{1,2} & \cdots & v_{1,n}\\ \vdots & \vdots & & \vdots\\ v_{m,1} & v_{m,2} & \cdots & v_{m,n}\end{pmatrix}. \tag{1}$$

Dès lors V est muni d'une structure de code en métrique rang en posant $d_r(\boldsymbol{v},\boldsymbol{w})=\mathrm{rang}(M_{\boldsymbol{v}}-M_{\boldsymbol{w}})$.

Exemple plus concret

On s'intéresse aux matrices de $\mathcal{M}_{2\times 3}(\mathbb{F}_2)$ de la forme $(C_1|C_2|C_3)$ avec $C_i \in \mathbb{F}_2^2$ et $C_3 = C_1 + C_2$.

$$\mathcal{C} = \Bigg\{ \underset{(1,0,0,0)}{\begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}}, \underset{(0,1,0,0)}{\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}}, \underset{(1,1,0,0)}{\begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}}, \underset{(0,0,1,0)}{\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}}, \underset{(0,0,0,1)}{\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}}, ,$$

$$\underset{(0,0,1,1)}{\begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}}, \underset{(1,0,1,0)}{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}}, \underset{(1,0,0,1)}{\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}}, \underset{(0,1,0,1)}{\begin{pmatrix} 0 & 0 & 0 \\ 1 & 1 & 0 \end{pmatrix}}, \underset{(0,1,1,0)}{\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}}, \underset{(1,1,1,1)}{\begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix}},$$

$$\underset{(1,1,1,0)}{\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}}, \underset{(1,1,0,1)}{\begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}}, \underset{(1,0,1,1)}{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}}, \underset{(0,1,1,1)}{\begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}}, \underset{(0,0,0,0)}{\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}} \Bigg\} \tag{2}$$

Soit $q = p^s$ une puissance d'un premier. On note $\mathbb{F}_q$ le corps a q-éléments, $\mathbb{F}_{q^m}$ une extension de degré m de $\mathbb{F}_q$, $\mathbb{F}_{q^m}[X]$ l'anneau des polynômes à coefficients dans $\mathbb{F}_{q^m}$ de la variable X et on définit :

$$R = \mathbb{F}_{q^m}\langle X^q \rangle := \left\{ \sum_{i=0}^{d} a_i \cdot X^{q^i} \mid a_i \in \mathbb{F}_{q^m}, \forall i \in \{0, \cdots, d\} \right\}. \tag{3}$$

L'anneau R muni de l'addition des polynômes et de la composition est un anneau dont le produit est « tordu » :

$$(a \cdot X^{q^i}) \circ (b \cdot X^{q^j}) = a \cdot b^{q^i} \cdot X^{q^{i+j}}; (b \cdot X^{q^j}) \circ (a \cdot X^{q^i}) = b \cdot a^{q^j} \cdot X^{q^{i+j}}. \tag{4}$$

Définition 5. *Soit* $F(X) = \sum_{i=0}^{d} f_i \cdot X^{q^i} \in R$ *tel que* $f_d \neq 0$, *l'entier* d *est appelé* q*-degré de* F *et on note* $d = \deg_q(F)$.

Proposition 6. *Soit* F *et* $G \in R$ *tels que* $\deg_q(F) \geqslant \deg_q(G)$ *alors il existe* $(Q, R) \in R^2$ *tels que* $\deg_q(R) < \deg_q(G)$ *(le* q*-degré est un sthasme) et* $F = Q \circ G + R$, *on dit que* Q *est le quotient la division à droite de* F *par* G *et que* R *en est le reste à droite.*

$$
\begin{array}{r|l}
f_d \cdot X^{q^d} + \cdots + f_0 \cdot X & g_e \cdot X^{q^e} + \cdots + g_0 \cdot X \\
\cline{2-2}
-f_d \cdot X^{q^d} - f_d \cdot g_e^{q^{e-d}} \cdot g_{e-1}^{q^{d-e}} \cdot X^{q^{d-1}} + \cdots + \alpha \cdot X & f_d \cdot g_e^{q^{e-d}} \cdot X^{d-e} \\
\cline{1-1}
\left(f_{d-1} - f_d \cdot g_e^{q^{e-d}} \cdot g_{e-1}^{q^{d-e}}\right) \cdot X^{q^{d-1}} + \cdots + \beta \cdot X &
\end{array}
$$

Théorème 7. *Muni de la division à droite, l'anneau R est un euclidien (à droite).*

On a donc des notions de PGCD (à droite) et de PPCM (à gauche).

Proposition 8. *Soient F et $G \in R$ alors il existe un unique polynôme unitaire de plus grand q-degré, noté $F \wedge_r G$, tel que $F \wedge_r G$ divise à la fois F et G. On l'appelle le plus grand diviseur commun à droite de F et G. Il se calcule comme le dernier reste non nul de l'algorithme d'euclide à droite étendu.*

Proposition 9. *Soient F et $G \in R$ alors il existe un unique polynôme unitaire de plus petit q-degré, noté $F \vee_l G$, divisible à droite à la fois par F et G. On l'appelle le plus petit commun multiple à gauche de F et G. Il se calcule comme coeffcient de la dernière relation de Bézout non triviale dans l'algorithme d'euclide à droite étendu.*

Proposition 10. *Soit $\zeta \in \mathbb{F}_{q^m}$ alors pour tout $P(X) \in R$, on a $P(X) = Q(X) \circ (X^q - \zeta^{q-1} \cdot X) + P(\zeta) \cdot X$.*

Proposition 11. *Soit $P(X) \in \mathbb{F}_{q^m}\langle X^q \rangle$, alors l'application $M_P \colon \zeta \in \mathbb{F}_{q^m} \mapsto P(\zeta) \in \mathbb{F}_{q^m}$ est $\mathbb{F}_q$-linéaire.*

Théorème 12. $\mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^m}) = \mathbb{F}_{q^m}\langle X^q \rangle / (X^{q^m} - X)$

Proposition 13. $P(X) \wedge_r (X^{q^m} - X) = X \Leftrightarrow M_P$ *inversible.*

Définition 14. *Soit $P \in R$, on définit $\mathcal{Z}_{\mathbb{F}_{q^m}}(P) = \{\zeta \in \mathbb{F}_{q^m} \mid P(\zeta) = 0\}$, qui est le noyau de l'endomorphisme associé.*

Lemme 15. *Soit $\zeta \in \mathbb{F}_{q^m}$, alors si $F(X) = (X^q - \zeta^{q-1} \cdot X)$, on a $F(\zeta) = 0$, de plus si $P \in R$ et tel que $P(\zeta) = 0$ alors F divise P à droite.*

Proposition 16. *Soit V un $\mathbb{F}_q$-sous-espace vectoriel de $\mathbb{F}_{q^m}$ alors il existe un unique polynôme unitaire $P_V \in R$ tel que $V = \mathcal{Z}_{\mathbb{F}_{q^m}}(P)$, de plus $\deg_q(P_V) = \dim_{\mathbb{F}_q}(V)$.*

Existence : Soit $\{e_1, \cdots, e_l\}$ une base de V, on considère alors $P_V(X) = (X^q - e_1^{q-1}X) \vee_l \cdots \vee_l (X^q - e_l^{q-1}X)$ qui est polynôme de q-degré l exactement.

Unicité : Si P est que que $\mathcal{Z}_{\mathbb{F}_{q^m}}(P) \supset V$ alors P_V divise à droite P.

Proposition 17. *Soient V et W deux $\mathbb{F}_q$-sous-espaces vectoriels de $\mathbb{F}_{q^m}$, alors on a :*

1. $P_{V\cap W} = P_V \wedge_r P_W$
2. $P_{V+W} = P_V \vee_l P_W$.

C'est une simple conséquence du fait que l'inclusion d'espaces vectoriels correspond à la divisibilité des polynômes linéarisés associés.

Proposition 18. *Si A et B sont de q-degré respectivement a et b alors* $\deg_q(A \vee_l B) + \deg_q(A \wedge_r B) = a + b$.

Notation 19. *Soit* $e \in \mathbb{N}$, *on note* $R_e = \{P \in R | \deg_q(P) < e\}$.

Définition 20. *Soient* $A(X) = \sum_{i=0}^{d} a_i \cdot X^{q^i}$ *et* $B(X) = \sum_{i=0}^{e} b_i \cdot X^{q^i} \in \mathbb{F}_{q^m}\langle X^q \rangle \in R$ *de* q*-degré respectivement* d *et* e, *on définit l'application linéaire suivante :*

$$\mathcal{S}_{e,d} : \begin{cases} R_e \times R_d & \longrightarrow & R_{d+e-1} \\ (U(X), V(X)) & \longmapsto & U(X) \circ A(X) + V(X) \circ B(X) \end{cases}.$$

Proposition 21. $\det(\mathcal{S}_{e,d}) \neq 0$ *si et seulement si* $A \wedge_r B = X$.

Résultant de deux polynômes linéarisés (2)

La matrice de $\mathcal{S}_{e,d}$ dans la base des « monomes » $X, X^q, \cdots$ est :

$$\mathrm{Syl}_{d,d} = \begin{pmatrix} a_0 & & & b_0 & & \\ \vdots & \ddots & & \vdots & \ddots & \\ a_d & & a_0^{q^{d-1}} & b_d & & b_0^{q^{d-1}} \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_d^{q^{d-1}} & & & b_d^{q^{d-1}} \end{pmatrix}.$$

Il y a une autre formulation intéressante du résultant.

Matrice de multiplication

Soit $P \in R$ un polynôme linéarisé de q-degré d. On note alors :

$$\Pi_P : \begin{cases} R \longrightarrow R/(P) \\ U(X) \longmapsto \Pi_P(U)(X) \end{cases}$$

avec $\Pi_P(U)$ qui dénote le reste de la division à droite de U par P.

Définition 22. *Soit $A \in R/(P) \cong R_d$, on définit alors l'opérateur de multiplication à droite par A :*

$$\mathcal{M}_A : \begin{cases} R/(P) & \longrightarrow & R/(P) \\ B & \longmapsto & \Pi_P(B \circ A). \end{cases} \tag{5}$$

Proposition 23. *Soit $P(X)$ et $A(X) \in R$, on note $\mathcal{M}_A$ la matrice de multiplication par A à droite dans $R/(P)$, alors $\det(\mathcal{M}_A) = 0$ si et seulement si $P(X) \wedge_r A(X) \neq X$, en d'autres termes, il existe $\alpha \in \mathbb{F}_{q^m}^{\times}$ tel que $\det(\mathcal{M}_A) = \alpha \cdot \mathrm{Res}(P(X), A(X))$.*

Si $P \wedge_r A \neq X$ alors on note P_1 le reste de la division à droite par A de $P \vee_l A$. On a alors $\mathcal{M}_A(P_1) = 0$.

Soit $B \in R/(P)$ tel que $\mathcal{M}_A(B) = 0$. On sait alors que $B \circ A$ est un multiple de P et donc de $P \vee_l A$. Comme A et $B \neq 0$, alors $P \vee_l A \neq 0$ et par suite $A \wedge_r P \neq X$.

Corollaire 24. *Soit $A(X), B(X)$ et $C(X) \in R$ on a alors $\mathrm{Res}(A(X), B(X) \circ C(X)) = \mathrm{Res}(A(X), B(X)) \cdot \mathrm{Res}(A(X), C(X))$.*

Définition 25. *Soient* $\zeta_1, \cdots, \zeta_d \in \mathbb{F}_{q^m}$ *et* $k \in \mathbb{N}$ *on définit alors ma matrice de* q*-Vandermonde associée :*

$$V_{k,\zeta} = \begin{pmatrix} \zeta_1 & \zeta_1^q & \cdots & \zeta_1^{q^{k-1}} \\ \vdots & \vdots & & \vdots \\ \zeta_d & \zeta_d^q & \cdots & \zeta_d^{q^{k-1}} \end{pmatrix} \tag{6}$$

et dans le cas où $k = d$*, on note* $v_\zeta = \det(V_\zeta)$ *le déterminant de* q*-Vandermonde.*

Proposition 26. *Soient* $\zeta_1, \cdots, \zeta_d \in \mathbb{F}_{q^m}$*, alors* $\zeta_1, \cdots, \zeta_d$ *sont* $\mathbb{F}_q$*-libres si et seulement si* $v_\zeta \neq 0$*.*

Définition 27. *Soient* $\zeta_1, \cdots, \zeta_d \in \mathbb{F}_{q^m}$, *et* $i \in \{1, \cdots, d\}$, *on définit alors le* $i^{ème}$ *polynôme de Lagrange linéarisé :*

$$L_{i,\zeta} = \begin{vmatrix} \zeta_1 & \zeta_1^q & \cdots & \zeta_1^{q^{d-1}} \\ \vdots & \vdots & & \vdots \\ \zeta_{i-1} & \zeta_{i-1}^q & \cdots & \zeta_{i-1}^{q^{d-1}} \\ X & X^q & \cdots & X^{q^{d-1}} \\ \zeta_{i+1} & \zeta_{i+1}^q & \cdots & \zeta_{i+1}^{q^{d-1}} \\ \vdots & \vdots & & \vdots \\ \zeta_d & \zeta_d^q & \cdots & \zeta_d^{q^{d-1}} \end{vmatrix} / v_\zeta \tag{7}$$

Définition 28. *Soient $\zeta_1, \cdots, \zeta_d \in \mathbb{F}_{q^m}$ des points $\mathbb{F}_q$-libres, on définit alors :*

$$Z(X) = \bigvee_{i=1}^{d}{}_{l}(X^q - \zeta_i^{q-1}) \cdot X \tag{8}$$

et $\mathcal{A}_\zeta = R/(Z)$.

Proposition 29. *La famille $\{L_{1,\boldsymbol{\zeta}}(X), \cdots, L_{d,\boldsymbol{\zeta}}(X)\}$ est une base de $\mathcal{A}_{\boldsymbol{\zeta}}$ comme $\mathbb{F}_{q^m}$-espace vectoriel.*

Lemme 30. *La valeur ζ_i^q est une valeur propre associé au vecteur propre $\begin{pmatrix} \zeta_i \\ \zeta_i^q \\ \vdots \\ \zeta_i^{q^{d-1}} \end{pmatrix}$ de $\mathcal{M}_{X^q}$.*

Proposition 31. *Soient* $\zeta_1, \cdots, \zeta_d \in \mathbb{F}_{q^m}$ *des points* $\mathbb{F}_q$*-libres et soit* $v_1, \cdots, v_d \in \mathbb{F}_{q^m}$ *alors l'unique polynôme* $F \in R_d$ *tel que* $F(\zeta_i) = v_i$ *pour tout* $i \in \{1, \cdots, d\}$ *est donné par :*

$$F(X) = \sum_{i=1}^{d} v_i \cdot L_{i,\zeta}(X). \tag{9}$$

Lemme 32. *Soit* $\boldsymbol{\zeta} = \{\zeta_1, \cdots, \zeta_d\} \subset \mathbb{F}_{q^m}$, $Z(X) = \bigvee_{i=1}^{d}{}_g (X^q - \zeta_i \cdot X)$ *et soit* $B(X) \in \mathbb{F}_{q^m}\langle X^q \rangle$ *alors le reste de la division de* $B(X)$ *par* $Z(X)$ *à droite est donné par* $\sum_{i=1}^{d} B(\zeta_i) \cdot L_{i,\boldsymbol{\zeta}}(X)$.

Corollaire 33. *Soit* $\boldsymbol{\zeta} = \{\zeta_1, \cdots, \zeta_d\} \subset \mathbb{F}_{q^m}$, $Z(X) = \bigvee_{i=1}^{d}{}_g (X^q - \zeta_i \cdot X)$ *et soit* $B(X) \in \mathbb{F}_{q^m}\langle X^q \rangle$ *alors* $\mathrm{Res}(Z(X), B(X)) = \prod_{i=0}^{d} B(\zeta_i)$.

Proposition 34. *Soit* $A(X)$ *et* $B(X) \in \mathbb{F}_{q^m}\langle X \rangle$ *sans facteur carré de* q*-degré respectivement* d *et* e *et soit* $\mathbb{K} = \mathbb{F}_{q^l}$ *le corps de décomposition de* $A(X) \vee_l B(X)$ *et soit* $\{\zeta_1, \cdots, \zeta_d\} = \mathcal{Z}(A(X))$ *et* $\{\xi_1, \cdots, \xi_e\} = \mathcal{Z}(B(X))$ *alors :* .

$$\mathrm{Res}(A(X), B(X)) = \prod_{i=1}^{d} B(\zeta_i) = \prod_{j=1}^{e} A(\xi_j) \in \mathbb{F}_{q^m}. \tag{10}$$

Soient $\zeta_1, \cdots, \zeta_n \in \mathbb{F}_{q^m}$ des valeurs $\mathbb{F}_q$-libres et $\mathcal{Z} = \{\zeta_1, \cdots, \zeta_n\}$. On note R_d l'ensemble des polynômes linéarisés de q-degré inférieur (strict) à $d\,(<n)$.

On note $\mathrm{ev}_{\mathcal{Z}}$: $\begin{cases} R_d \longrightarrow (\mathbb{F}_{q^m})^n \\ P(X) \longmapsto (P(\zeta_1), \cdots, P(\zeta_n)) \end{cases}$.

Définition 35. $\mathcal{G}_{d,n} = \mathrm{Im}(\mathrm{ev}_{\mathcal{Z}})$.

Matrice génératrice :

$$G_{d,n} = \begin{pmatrix} \zeta_1 & \cdots & \zeta_n \\ \zeta_1^q & & \zeta_n^q \\ \vdots & \cdots & \vdots \\ \zeta_1^{q^{d-1}} & \cdots & \zeta_n^{q^{d-1}} \end{pmatrix}$$

Proposition 36. *Les codes de Gabidulin sont* MRD, *i.e.* $w_R(\boldsymbol{x}, \boldsymbol{y}) \geqslant \left\lfloor \frac{n-d}{2} \right\rfloor$.

Matrice de parité

Définition 37. *Soit $\mathcal{C} \subset \mathbb{F}_q^n$ un code de longueur n et de dimension k. Une matrice génératrice de $\mathcal{C}$ est une matrice G de $\mathcal{M}_{n\times k}(\mathbb{F}_q)$ telle que $\mathrm{Im}(G) = \mathcal{C}$.*

Définition 38. *Soit $\mathcal{C} \subset \mathbb{F}_q^n$ un code de longueur n et de dimension k, une matrice de parité de $\mathcal{C}$ est une matrice H de $\mathcal{M}_{n-k\times n}(\mathbb{F}_q)$ de rang $n-k$ telle que $H \cdot G = 0$.*

Si $\boldsymbol{x} = G \cdot \boldsymbol{m}$ est un mot de code et qu'on reçoit $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$ où $\boldsymbol{e}$ est une « erreur » et si H est une matrice de parité associée à G, alors $H \cdot \boldsymbol{y} = H \cdot \boldsymbol{x} + H \cdot \boldsymbol{e} = H \cdot \boldsymbol{e}$. Retrouver $\boldsymbol{e}$ consiste en résoudre $H \cdot \boldsymbol{e} = \boldsymbol{y}$. Une fois déterminé $\boldsymbol{e} \to \boldsymbol{x} = \boldsymbol{y} - \boldsymbol{e}$. Le mot $\boldsymbol{y}$ est appelé un syndrome.

Définition 39. *Soit* $\boldsymbol{v} = (v_1, \cdots, v_l) \in (\mathbb{F}_{q^m})^l$, $M = (m_{i,j}) \in (\mathbb{F}_{q^m})^n$ *et* $P(x) = \sum_{i=0}^{d} a_i \cdot x^i$ *on définit le support de* $\boldsymbol{v}$ *comme* $\mathrm{supp}(\boldsymbol{v}) = \langle v_1, \cdots, v_l \rangle \subset \mathbb{F}_{q^m}$, *celui de* M *comme* $\mathrm{supp}(M) = \langle m_{i,j} \rangle_{i,j} \subset \mathbb{F}_{q^m}$ *et* $\mathrm{supp}(P) = \mathrm{supp}(a_0, \cdots, a_d) = \langle a_0, \cdots, a_d \rangle$.

Définition 40. *[Gaborit,Murat,R.; Zémor] Les codes « Low Rank Parity Check-matrices » sont ceux qui admettent une matrice de partité dont le support est de petite dimension (c'est le rang de la matrice engendré par les coefficients pas celle de la matrice de parité).*

Codes LRPC (2)

On procède en deux étapes : on cherche d'abord une base du $\mathbb{F}_q$-sous-espace vectoriel de $\mathbb{F}_{q^m}$ engendré par les coefficients de $\boldsymbol{e}$ connaissant une base de ceux engéndrés par les coefficients de $\boldsymbol{y}$ et H.

Puis c'est de l'algèbre linéaire de déterminer les coordonnées des coefficients de $\boldsymbol{e}$ dans cette base.

Problème 1. Soit A et C deux $\mathbb{F}_q$-sous-espaces vectoriels de $\mathbb{F}_{q^m}$, touver B tel que $C = A \cdot B$ où $A \cdot B = \sum a_i \cdot b_i$ avec $a_i \in A$ et $b_i \in B$.

Théorème 41. *[Gaborit,Murat,R.; Zémor] Soit H la matrice de parité $(n-k) \times n$ d'un code LRPC dont les coefficients engendrent un $\mathbb{F}_q$-espace vectoriel de petite dimension $d \geqslant 2$ dans $\mathbb{F}_{q^m}$, alors il existe un algorithme décodant une erreur aléatoire de rang k telle que $r \cdot d \leqslant n-k$ avec une probabilité d'échec en $q^{-(n-k+1-r\cdot d)}$ et une complexité dans $\mathcal{O}(r^2 \cdot (4 \cdot d^2 \cdot m + n^2))$.*

Soient f_1 et $f_2 \in R$ de q-degré respectivement d_1 et d_2, $\forall g \in R$, on note $\pi_i(g)$ son reste par la division à droite par f_i. Pour tout $g \in R$, on note $\pi_3(g)$ le reste de la division à droite de g par $f_1 \vee_l f_2$.

Proposition 42. *On suppose que f_1 et f_2 vérifient une relation de Bézout $S_1 \circ f_1 + S_2 \circ f_2 = X$ avec $q\text{-}deg(S_1) < d_2$ et $q\text{-}deg(S_2) < d_1$. Soit $g \in R$ de q-degré strictement inférieur à $d_1 + d_2$ alors $g = \pi_3(\pi_2(g) \circ S_1 \circ f_1 + \pi_1(g) \circ S_2 \circ f_2)$.*

$\Pi = \pi_1 \times \pi_2 : R_k \longrightarrow R/(f_1)_l \times R/(f_2)_l$ et soit $A \in R$, on note $\mathcal{M}_A : P \in R \longmapsto P \circ A \in R$ et a le q-degré de A et on définit $\Psi_A = \Pi \circ \mathcal{M}_A : \begin{cases} R \longrightarrow R/(f_1)_l \times R/(f_2)_l \\ g \longmapsto (\pi_1(g \circ A), \pi_2(g \circ A)) \end{cases}$.
Soit $d < d_1 + d_2 - a$ et on suppose maintenant que f_1 et f_2 sont à coefficients dans $\mathbb{F}_q$.

Définition 43. *Le code qCRT associé à d, A et $F = (f_1, f_2)$ est $\mathcal{C}_{F,d} = \Psi_A(R_d)$.*

Décodage des qCRT

On reçoit $\boldsymbol{y} = \boldsymbol{x} + \boldsymbol{e}$ où $\boldsymbol{x} = \Psi_A(\boldsymbol{c})$, on calcule $\Psi_A^{-1}(\boldsymbol{y}) = \boldsymbol{c} \circ A + E$ où $E = \underline{E} + \overline{E} \circ X^{q^d}$ avec $\underline{E}$ de q-degré $\leqslant d$ et $\overline{E}$ de degré $d_1 + d_2 - a - d$.

On a alors $\mathrm{supp}(\overline{E}) = \mathrm{supp}(E) = \mathrm{supp}(\boldsymbol{e})$ avec une probabilité de l'ordre de $1 - q^{d-(d_1+d_2-a)}$ (sous de bonnes hypothèses).

Le reste du décodage, comme pour les LRPC consiste à résoudre des systèmes linéaires.

Problème 2. Si f_1 et f_2 sont à support dans $\mathbb{F}_q$ il y a des mots de poids 1 dans le dual.

Dual d'un qCRT

$H\,v = 0$ avec Hv correspond à $u \circ A = f_2$ et $w \circ A = f_1$ pour que $H \cdot G = 0$ et donc $u \circ A \circ f_1 - w \circ A \circ f_2 = 0 \rightarrow u' \circ f_1 + w' \circ f_2 = 0$ (syzygy).

Donc si $\mathrm{supp}(f_1, f_2) = \mathbb{F}_q$ alors on a des u' et w' à coefficient dans $\mathbb{F}_q$.

Si $\mathrm{supp}(f_1, f_2) = V \underset{\neq}{\supset} \mathbb{F}_q$ alors on a bien $\Psi_A^{-1}(\boldsymbol{y}) = \boldsymbol{c} \circ A + E$ où $E = \underline{E} + \overline{E} \circ X^{q^d}$ avec $\underline{E}$ de q-degré $\leqslant d$ et $\overline{E}$ de degré $d_1 + d_2 - a - d$. Mais $\mathrm{supp}(\overline{E}) \subset \mathrm{supp}(\boldsymbol{e}) \cdot V$.

Nous sommes ramener, de nouveau à une étape de décodage type LRPC, mais la matrice de parité ne contient plus de mots de poids 1 (en fait le poids du dual dépend de $\dim_{\mathbb{F}_q}(V)$).

Clé privé : $G \in \mathbb{F}_{q^m}^{k \times n}$ matrice génératrice d'un code de capacité de décodage d, $U \in \mathrm{Gl}(\mathbb{F}_{q^m}^k)$, $V \in \mathrm{Gl}(\mathbb{F}_q^n)$

Clé public : $G' = U \cdot G \cdot V$

Chiffrement : Pour envoyer $\boldsymbol{x} \in \mathbb{F}_{q^m}^k$ on engendre $\boldsymbol{e} \in \mathbb{F}_{q^m}^n$ tel que $w_R(\boldsymbol{e}) \leqslant d$, on calcule $\boldsymbol{y} = \boldsymbol{x} \cdot G' + \boldsymbol{e}$

Déchiffrement : On calcule $\boldsymbol{y} \cdot V^{-1} = \boldsymbol{x}' \cdot G + \boldsymbol{e} \cdot V^{-1}$ avec $\boldsymbol{x}' = \boldsymbol{x} \cdot U$ et $w_R(V^{-1} \cdot \boldsymbol{e}) \leqslant d$. On décode pour trouver $\boldsymbol{x}'$ puis on calcule $\boldsymbol{x}' \cdot U^{-1} = \boldsymbol{x}$.

Problème difficile : Décoder un code aléatoire en métrique rang [Gaborit, Zémor, 13].

Hypothèse de sécurité : Il est difficile de distinger G' d'une matrice génératrice d'un code aléatoire.

[Gaborit, R., Schrek, Zémor, 14]

Définition 44. *Soient E et F deux $\mathbb{F}_q$-s.e.v. de $\mathbb{F}_{q^m}$ de dimension respective r et d, on définit $E \cdot F = \langle \{e \cdot f \,|\, e \in E \text{ et } f \in F\} \rangle$.*

Généralement : si $E = \langle e_1, \cdots, e_r \rangle$ et $F = \langle f_1, \cdots, f_d \rangle$ alors $E \cdot F = \langle e_i \cdot f_j \,|\, i \in \{1, \cdots, r\} \text{ et } j \in \{1, \cdots, d\} \rangle$ (GMRZ08)

Soit $H \in \mathbb{F}_{q^m}^{2 \cdot n \times n}$ telle que $\mathrm{supp}(H) = F$ et $\boldsymbol{e} \in \mathbb{F}_{q^m}^{2 \cdot n}$ tel que $\mathrm{supp}(\boldsymbol{e}) = E$ et soit $\mathcal{C}$ le code LRPC associé à H. On note $\boldsymbol{s}^T = H \cdot \boldsymbol{e}^T$ et $S = \mathrm{supp}(\boldsymbol{s})$. On a S s.e.v. de $E \cdot F$.

Pour tout $i \in \{1, \cdots, d\}$, on note $S_i = f_i^{-1} \cdot S$.

Objectif : Connaissant S et F, retrouver E (quand c'est possible).

Algorithme 1

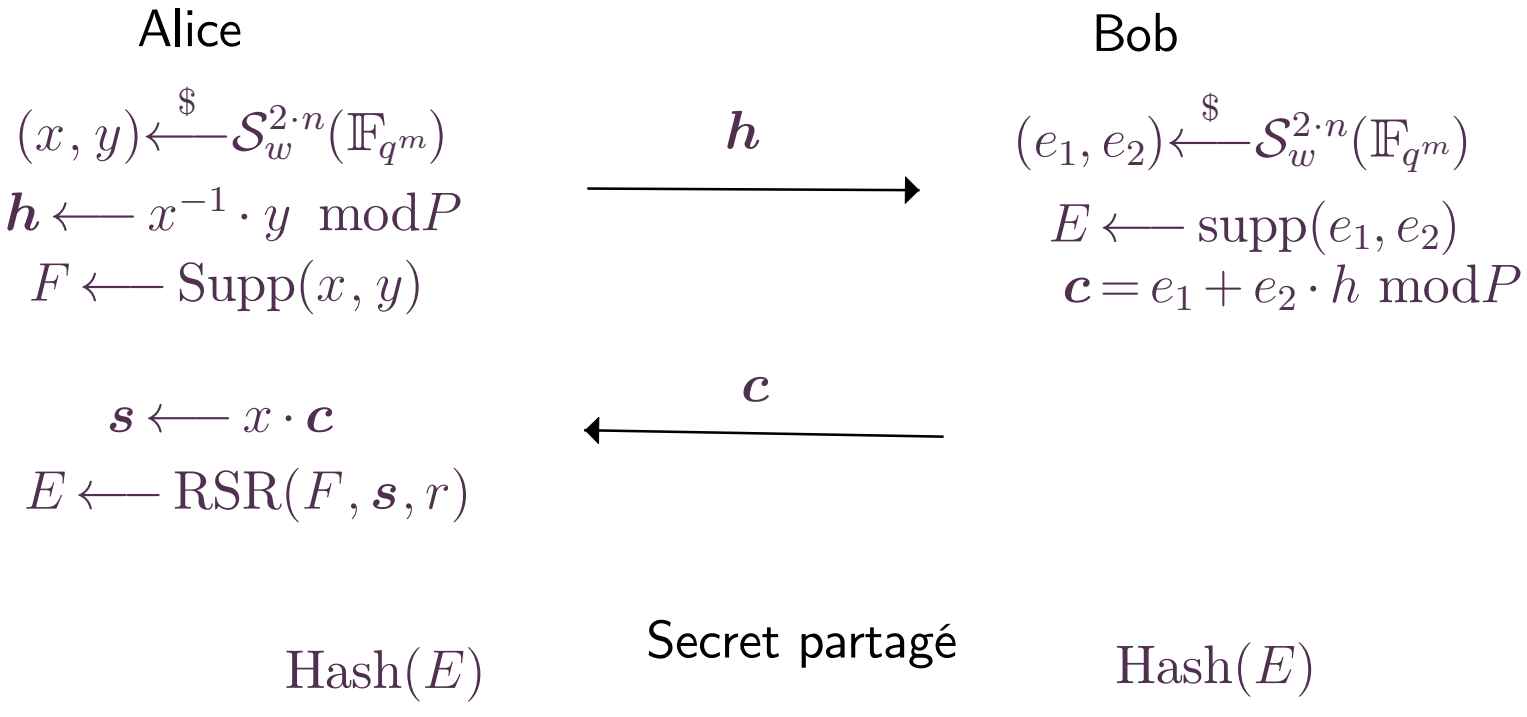
Données : $F = \langle f_1, \cdots, f_d \rangle$ et $\boldsymbol{s} = (s_1, \cdots, s_{2 \cdot n})$ tel que $\boldsymbol{s}^T = H \cdot \boldsymbol{e}$.

Sortie : Un candidat pour $E = \mathrm{supp}(\boldsymbol{e})$.

1. Calculer $S = \mathrm{supp}(\boldsymbol{s})$
2. $E \leftarrow \bigcap_{i=1}^{d} f_i^{-1} \cdot S$
3. retourner E

Proposition 45. *Probabilité d'échec :* $q^{-(n-r\cdot d+1)} + q^{-(d-1)\cdot(m-r\cdot d-r)}$.

Rollo I est un algorithme d'encapsulation de clés. $\mathcal{S}_w^n(\mathbb{F}_{q^m}) = \{\boldsymbol{v} \in \mathbb{F}_{q^m}^n \,|\, w_r(v) = w\}$ et $P(X)$ irréductible dans $\mathbb{F}_q[X]$.



Conclusion

La métrique rang voit de nouveaux codes et surtout de nouveaux problèmes calculatoires !

Problème 3. Soit A et C deux $\mathbb{F}_q$-sous-espaces vectoriels de $\mathbb{F}_{q^m}$, touver B tel que $C = A \cdot B$ où $A \cdot B = \sum a_i \cdot b_i$ avec $a_i \in A$ et $b_i \in B$.