Codes Fonctionnels Construits sur des Variétés Quadriques

Frédéric A. B. EDOUKOU
e.mail: edoukou@iml.univ-mrs.fr
Institut de Mathématiques de Luminy
Marseille, France

Journées C2 (Codage et Cryptographie) 2008
Carcans (Gironde)
Jeudi 20 Mars 2008

Plan de travail

I-Notations

II- Construction du code $C_h(X)$

III-Bornes supérieurs pour l'intersection de deux quadriques

IV-Etude de $C_2(X)$ pour X une surface quadrique non-dégénérée dans $\mathbb{P}^3(\mathbb{F}_q)$

V-Etude de $C_2(X)$ pour X une variété quadrique dans $\mathbb{P}^4(\mathbb{F}_q)$

VI-Etude de $C_2(X)$ pour X une variété quadrique non-dégénérée dans $\mathbb{P}^n(\mathbb{F}_q)$

VII-Questions Ouvertes: une conjecture à résoudre

I-Notations

- $\mathbb{F}_q$: finite field with q elements, where $q = p^a$.

- $V = \mathbb{A}^{m+1}$ the affine space of dimension $m+1$ on $\mathbb{F}_q$.
  $\mathbb{P}^m(\mathbb{F}_q)$:the corresponding projective space of dimension m.

- $\#\mathbb{P}^m(\mathbb{F}_q) = \pi_m = q^m + q^{m-1} + ... + q + 1$

- $\mathcal{F}_h(V, \mathbb{F}_q)$: vector space of forms of degree h on V with coefficients in $\mathbb{F}_q$.

- Si $f \in \mathcal{F}_h(V, \mathbb{F}_q)$,
  $Z(f)$: the set of zeros of f in $\mathbb{P}^m(\mathbb{F}_q)$.

- Let $X \subset \mathbb{P}^m(\mathbb{F}_q)$ a variety in $\mathbb{P}^m(\mathbb{F}_q)$, $X \cap Z(f)$: the section of degree h of X, and $X_{Z(f)}(\mathbb{F}_q)$: the set of rational points on $\mathbb{F}_q$ of the algebraic set $X \cap Z(f)$.

II- Construction du code $C_h(X)$

- Soit $X \subset \mathbb{P}^m(\overline{\mathbb{F}}_q)$ et $N = \#X(\mathbb{F}_q)$

$$c : \mathcal{F}_h(V, \mathbb{F}_q) \longrightarrow \mathbb{F}_q^N$$

$$f \longmapsto c(f) = (f(P_1), \ldots, f(P_N))$$

$\boxed{C_h(X) = \mathrm{Im} c}$

- **définition** Soit $c(f)$ un mot de code.

$$cw(f) = \#\{P \in X \quad | \quad f(P) = 0\}$$

$$w(c(f)) = \#X(\mathbb{F}_q) - cw(f)$$

$$\mathrm{dist} C_h(X) = \#X(\mathbb{F}_q) - \max_{\mathrm{f} \in \mathcal{F}_h} cw(f)$$

- **Proposition** Les paramètres du code $C_h(X)$: longueur $C_h(X) = \#X(\mathbb{F}_q)$,

$$\dim C_h(X) = \dim \mathcal{F}_h - \dim \ker c,$$

$$\mathrm{dist} C_h(X) = \#X(\mathbb{F}_q) - \max_{\mathrm{f} \in \mathcal{F}_h} \#X_{Z(f)}(\mathbb{F}_q)$$

c injective $\Rightarrow \dim C_h(X) = \binom{m+h}{h}$

III-Intersection of two quadrics in $\mathbb{P}^n(\mathbb{F}_q)$.

- In 1991, Y. Aubry, A.G.C.T-3

$$\boxed{|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq 2(4q^{n-2} + \pi_{n-3} + \frac{1}{q-1})}$$

- In 1999, D. B. Leep et L. M. Schueller

Suppose: $w(\mathcal{Q}_1, \mathcal{Q}_2) = n + 1$

If $n + 1 \geq 4$ and even, then:

$$\boxed{|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq 2q^{n-2} + \pi_{n-3} + 2q^{\frac{n-1}{2}} - 3q^{\frac{n-3}{2}}}$$

If $n + 1 \geq 5$ and odd, then

$$\boxed{|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq 2q^{n-2} + \pi_{n-3} + q^{\frac{n}{2}}}$$

- In 2006, **Lemma**

Let $1 \leq l \leq n - 1$ and $w(\mathcal{Q}_1, \mathcal{Q}_2) = n - l + 1$.

If $|\mathcal{Q}_1 \cap \mathcal{Q}_2 \cap E| \leq m$ where $E \simeq \mathbb{P}^{n-l}(\mathbb{F}_q)$,

then $\boxed{|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq mq^l + \pi_{l-1}}$

This bound is the best possible as soon as m is optimal for E.

IV-Etude de $C_2(X)$ pour X une surface quadrique non-dégénérée dans $\mathbb{P}^3(\mathbb{F}_q)$

$X : F(x_0, x_1, x_2, x_3) = 0$

Table 1: Quadriques dans PG(3,q).

r($\mathcal{Q}$)	Description	$\lvert\mathcal{Q}\rvert$	g($\mathcal{Q}$)
1	repeated plane $\Pi_2\mathcal{P}_0$	π_2	2
2	pair of distinct planes $\Pi_2\mathcal{H}_1$	$2q^2 + \pi_1$	2
2	the line $\Pi_1\mathcal{E}_1$	π_1	1
3	the (quadric) cone $\Pi_0\mathcal{P}_2$	π_2	1
4	hyperbolic quadric $\mathcal{H}_3(\mathcal{R}, \mathcal{R}')$	$\pi_2 + q$	1
4	elliptic quadric $\mathcal{E}_3$	$\pi_2 - q$	0

Quelques valeurs de $\#X_{Z(f)}(\mathbb{F}_q)$

$$H(q) = 4q,\ H_2(q) = 3q + 1,\ H_3(q) = 3q$$
$$E(q) = 2(q + 1),\ E_2(q) = 2q + 1,\ E_3(q) = 2q$$

Distribution des poids de $C_2(\mathcal{H}_3)$

- $\boxed{w_1 = q^2 - 2q + 1}$
  The codewords $<< w_1 >>$:
  –Union of 2 tan planes and l bisecante
  –hyperbolic quadric containning $\|$ and $=$ lines of X.

- $\boxed{w_2 = q^2 - q}$
  Les mots atteignant le deuxième poids:
  –hyperpolic quadric containning contenant exactement deux droites dans des regulus distinct et les q autre doites d'un regulus sont des bisecantes de X.
  –réunion de deux plans tangents à X et la droite d'intersection des deux plans est contenue dans X.
  –réunion de deux plans l'un est tangent et le second non-tangent à X et la droite d'intersection des deux plans intersectant X en un seul point.

- $\boxed{w_3 = q^2 - q + 1}$

Weight Distribution of $C_2(\mathcal{E}_3)$

- $\boxed{w_1 = q^2 - 2q - 1}$
  Les mots atteignant le premier poids:
  –Union de 2 plans non-tan et l disjointe de X.
  –Quadriques hyperboliques dont les toutes les droites d'un regulus sont des bisecantes.
  –Quadriques dégénérées de rank 3 (i.e. $q+1$ droites) dont le sommet n'est pas contenu dans X et toutes les $q+1$ droites sont des bisecantes.

- $\boxed{w_2 = q^2 - 2q}$
  Les mots atteignant le deuxième poids sont donnés par des quadriques qui sont réunion de deux plans non-tangents à X et la droite d'intersection des deux plans intersectant X en un seul point.

- $\boxed{w_3 = q^2 - 2q + 1}$

V-Etude de $C_2(X)$ pour une variété quadrique non-dégénérée dans $\mathbb{P}^4(\mathbb{F}_q)$

Table 2: Quadrics in $\mathbb{P}^4(\mathbb{F}_q)$.

r($\mathcal{Q}$)	Description	$\|\mathcal{Q}\|$	g($\mathcal{Q}$)
1	repeated hyperplane $\Pi_3\mathcal{P}_0$	π_3	3
2	pair of hyperplanes $\Pi_2\mathcal{H}_1$	$2q^3+\pi_2$	3
2	the plane $\Pi_2\mathcal{E}_1$	π_2	2
3	the cone $\Pi_1\mathcal{P}_2$	π_3	2
4	the cone $\Pi_0\mathcal{H}_3(\mathcal{R},\mathcal{R}')$	π_3+q^2	2
4	the cone $\Pi_0\mathcal{E}_3$	π_3-q^2	1
5	parabolic quadric $\mathcal{P}_4$	π_3	1

Section plane de X: g($\mathcal{Q}$)=2

Table 3: Plane quadric curves

r($\mathcal{Q}'$)	Description	$\|\mathcal{Q}'\|$	g($\mathcal{Q}'$)
1	repeated line $\Pi_1\mathcal{P}_0$	$q+1$	1
2	pair of lines $\Pi_0\mathcal{H}_1$	$2q+1$	1
2	point $\Pi_0\mathcal{E}_1$	1	0
3	parabolic $\mathcal{P}_2$	$q+1$	0

$$\boxed{\#X_{Z(f)}(\mathbb{F}_q) \leq 2q^2+3q+1}$$

Section hyperplane de X: g($\mathcal{Q}$)=3

a. $\mathcal{Q}$ est un hyperplan répété

Théorème [Primrose, 1951]
Soit $H \subset \mathbb{P}^4(\mathbb{F}_q)$ un hyperplan

$$\#\mathcal{X}_H(\mathbb{F}_q) = \begin{cases} \pi_2+q, \pi_2-q & \text{si H non-tangent à} \\ \pi_2 & \text{si H est tangent à} \end{cases}$$

b. $\mathcal{Q}$ est une paire d' hyperplans: $\mathcal{Q} = H_1 \cup H_2$

$\hat{\mathcal{X}}_1 = H_1 \cap \mathcal{X}$, $\hat{\mathcal{X}}_2 = H_2 \cap \mathcal{X}$ et $\mathcal{P} = H_1 \cap H_2$

$$|\mathcal{Q} \cap \mathcal{X}| = |H_1 \cap \mathcal{X}| + |H_2 \cap \mathcal{X}| - |\mathcal{P} \cap \mathcal{X}|. \quad (1)$$

$$\mathcal{P} \cap \mathcal{X} = \mathcal{P} \cap \hat{\mathcal{X}}_1 = \mathcal{P} \cap \hat{\mathcal{X}}_2. \quad (2)$$

Théorème [Swinnerton-Dyer, 1964] Let $\tilde{\mathcal{X}}$ be a degenerate quadric variety of rank $r < n+1$ in $\mathbb{P}^n(\mathbb{F}_q)$ and Π_{r-1} a linear projective space of dimension $r-1$ disjoint from the singular space Π_{n-r} of $\tilde{\mathcal{X}}$. Then $\Pi_{r-1} \cap \tilde{\mathcal{X}}$ is a non-degenerate quadric variety in Π_{r-1}.

Théorème [Wolfmann, 1975] Let $\tilde{\mathcal{X}} \subset \mathbb{P}^n(\mathbb{F}_q)$ be a non-degenerate quadric variety. A tangent hyperplane meets $\tilde{\mathcal{X}}$ at a denegerate quadric of the same type as $\tilde{\mathcal{X}}$.

b.1 Deux hyperplans tangents à $\mathcal{Q}$

b.2 tangent et l'autre non-tangent à $\mathcal{Q}$

b.3 Deux hyperplans non-tangents à $\mathcal{Q}$

Proposition Si $\mathcal{Q}$ est une paire d'hyperplans dans $\mathbb{P}^4(\mathbb{F}_q)$ et $\mathcal{X}$ la variété quadrique non-dégénerée dans $\mathbb{P}^4(\mathbb{F}_q)$, alors

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2q^2 + 3q + 1,\ 2q^2 + 2q + 1$$

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2q^2 + q + 1,\ 2q^2 + 1,$$

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2q^2 - q + 1$$

Section rectiligne de $\mathcal{X}$: g($\mathcal{Q}$)=1

a. $\mathcal{X} \cap \mathcal{Q}$ ne contient pas de droites

$$\boxed{\# X_{Z(f)}(\mathbb{F}_q) \leq 2(q^2+1)}$$

b. $\mathcal{X} \cap \mathcal{Q}$ contient une droite

b.1. $\mathcal{Q}$ est dégénérée

$$\boxed{\# X_{Z(f)}(\mathbb{F}_q) \leq 2q^2+2q+1}$$

b.2. $\mathcal{Q}$ est non-dégénérée

Table 4: Intersection of $\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i$ in $\mathbb{P}^3(\mathbb{F}_q)$

Type	$\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i$
1	(hyperbolic quadric) $\cap$ (quadric cone)
2	(quadric cone) $\cap$ (quadric cone)
3	(hyperbolic quadric) $\cap$ (hyperbolic quadric)

Table 5: Number of points and lines in $\hat{\mathcal{Q}}_i \cap \hat{\mathcal{X}}_i$

Types	4 lines	2 lines	1 line
1		$3q$	$2q+1$
2	4q+1	$3q$	$2q+1$
3	$4q$	$3q+1$	$2(q+1)$

A) $\mathcal{X} \cap \mathcal{Q}$ contient exactement une droite

$\boxed{\#X_{Z(f)}(\mathbb{F}_q) \leq q^2 + 3q + 2}$

B) $\mathcal{X} \cap \mathcal{Q}$ contient au moins deux droites:
B-1) $\mathcal{X} \cap \mathcal{Q}$ contient que des droites disjointes

$\boxed{\#X_{Z(f)}(\mathbb{F}_q) \leq q^2 + 3q + 2}$

B-2) $\mathcal{X} \cap \mathcal{Q}$ contient au moins deux droites secantes:
($\star$)Il existe H_1 et H_2 tel que $\hat{\mathcal{X}}_i = \hat{\mathcal{Q}}_i$

$\boxed{\#X_{Z(f)}(\mathbb{F}_q) \leq 2q^2 + 2q + 1}$

($\star\star$) Il existe H_1 tel que $\hat{\mathcal{X}}_1 = \hat{\mathcal{Q}}_1$

$\boxed{\#X_{Z(f)}(\mathbb{F}_q) \leq q^2 + 6q + 2}$

($\star\star\star$) Pour $i = 1, ..., q+1$ $\hat{\mathcal{X}}_i \neq \hat{\mathcal{Q}}_i$

$\boxed{\#X_{Z(f)}(\mathbb{F}_q) \leq 2q^2 + 3q + 1}$

Quelques valeurs de $\#X_{Z(f)}(\mathbb{F}_q)$

Théorème Si $\mathcal{X}$ est une quadrique non-dégénérée dans $\mathbb{P}^4(\mathbb{F}_q)$ et $\mathcal{Q}$ une quadrique de $\mathbb{P}^4(\mathbb{F}_q)$ telle que $\mathcal{X} \neq \lambda\mathcal{Q}$, alors

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2q^2 + 3q + 1,\ 2q^2 + 2q + 1$$

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2q^2 + q + 1,\ 2q^2 + 1,$$

$$\#\mathcal{X}_{Z(\mathcal{Q})}(\mathbb{F}_q) = 2q^2 - q + 1$$

Table 6: Les 5 premiers poids de $C_2(X)$.

Poids	$\mathcal{Q}$	$\mathcal{P} \cap \mathcal{X}$	w_i
1	2 n-tan $\mathcal{H}$	n-sin. conic	$q^3 - q^2 - 2q$
2	2 n-tan	sin. cve (r=2)	$q^3 - q^2 - q$
3	1t+1n-tan	$\Pi_0\mathcal{H}_1$	$q^3 - q^2$
4	1t+1n-tan	sin. cve (r=2)	$q^3 - q^2 + q$
	2tan	$\Pi_0\mathcal{H}_1$	
5	2 n-tan $\mathcal{E}$	n-sin. conic	$q^3 - q^2 + 2q$

Tuesday 02/27/2007 (Seminar of GRIM, Toulon)

Théorème [Ax, 1964]

Let r polynomials $f_i(x_1, ..., x_n)$ and deg $(f_i) = d_i$ on $\mathbb{F}_q$ then: if $n > b\sum_{i=1}^{r} d_i \Rightarrow q^b | \#Z(f_1, ..., f_n)$.

VI-Etude de $C_2(X)$ pour X une variété quadrique non-dégénérée dans $\mathbb{P}^n(\mathbb{F}_q)$

$X : f(x_0, x_1, x_2, x_3, ..., x_n) = 0$

• 6.1 X est une quadrique non-dégénérée de $\mathbb{P}^{2l+1}(\mathbb{F}_q)$

Distribution des poids de $C_2(\mathcal{H}_{2l+1})$

dist$C_h(X)$: D. Leep, en 1999, FFA (7).

$$\text{dist}C_h(X) \geq q^{2l} - q^{2l-1} - q^l + q^{l-1}$$

Table 6: Les 6 premiers poids de $C_2(X)$.

Poids	$\mathcal{Q}$	$\Pi_{2l-1} \cap \mathcal{X}$	w_i
1	2 tan.	$\mathcal{H}_{2l-1}$	$q^{2l} - q^{2l-1} - q^l + q^{l-1}$
2	1t+1n-tan	$\Pi_0\mathcal{P}_{2l-2}$	$q^{2l} - q^{2l-1}$
	2tan	$\Pi_1\mathcal{H}_{2l-3}$	
3	1t+1n-tan	$\mathcal{H}_{2l-1}$	$q^{2l} - q^{2l-1} + q^{l-1}$
4	2 n-tan.	$\mathcal{E}_{2l-1}$	$q^{2l} - q^{2l-1} + q^l - q^{l-1}$
5	2 n-tan	$\Pi_0\mathcal{P}_{2l-2}$	$q^{2l} - q^{2l-1} + q^l$
6	2 n-tan	$\mathcal{H}_{2l-1}$	$q^{2l} - q^{2l-1} + q^l + q^{l-1}$

Distribution des poids de $C_2(\mathcal{E}_{2l+1})$

dist$C_h(X)$: D. Leep, en 1999, FFA (7).

$$\text{dist}C_h(X) \geq q^{2l} - q^{2l-1} - 3q^l + 3q^{l-1}$$

Table 7: Les 7 premiers poids de $C_2(\mathcal{E}_{2l+1})$.

Poids	$\mathcal{Q}$	$\Pi_{2l-1} \cap \mathcal{X}$	w_i
1	2 n-tan.	$\mathcal{E}_{2l-1}$	$q^{2l} - q^{2l-1} - q^l - q^{l-1}$
2	2 n-tan	$\Pi_0\mathcal{P}_{2l-2}$	$q^{2l} - q^{2l-1} - q^l$
3	1t+1n-tan	$\mathcal{H}_{2l-1}$	$q^{2l} - q^{2l-1} - q^l + q^{l-1}$
4	2 n-tan.	$\mathcal{E}_{2l-1}$	$q^{2l} - q^{2l-1} - q^{l-1}$
5	1t+1n-tan	$\Pi_0\mathcal{P}_{2l-2}$	$q^{2l} - q^{2l-1}$
	2tan	$\Pi_1\mathcal{E}_{2l-3}$	
6	2 tan	$\mathcal{E}_{2l-1}$	$q^{2l} - q^{2l-1} + q^l - q^{l-1}$
7	2 tan	$\Pi_0\mathcal{P}_{2l-2}$	$q^{2l} - q^{2l-1} + q^l$

Théorème [Edoukou, Dec. 2007]
Soit $\mathcal{X}$ une quadrique non-dégénérée dans $\mathbb{P}^{2l+1}(\mathbb{F}_q)$ avec $l \in \mathbb{N}^\star$.
Alors tous les poids du code $C_2(X)$ défini sur X sont divisibles par q^{l-1}.

• 6.2 X quadrique non-dégénérée de $\mathbb{P}^{2l+2}(\mathbb{F}_q)$

dist$C_h(X)$: D. Leep, en 1999, FFA (7).

$$\text{dist}C_h(X) \geq q^{2l+1} - q^{2l} - q^{l+1}$$

Table 8: Les 5 premiers poids de $C_2(\mathcal{P}_{2l+2})$.

Poids	$\mathcal{Q}$	$\Pi_{2l} \cap \mathcal{X}$	w_i
1	2 n-tan. $\mathcal{H}$	$\mathcal{P}_{2l}$	$q^{2l+1} - q^{2l} - 2q^l$
2	2 n-tan	$\Pi_0\mathcal{H}_{2l-1}$	$q^{2l+1} - q^{2l} - q^l$
	1tan+1n-tan	$\mathcal{P}_{2l}$	
	2 tan	$\Pi_0\mathcal{E}_{2l-1}$	
3	2 n-tan	$\mathcal{P}_{2l}$	$q^{2l+1} - q^{2l}$
	1tan+1n-tan	$\Pi_0\mathcal{H}_{2l-1}$	
	1tan+1n-tan.	$\Pi_0\mathcal{E}_{2l-1}$	
	2 tan	$\Pi_1\mathcal{P}_{2l-2}$	
4	2 n-tan. $\mathcal{H}$	$\Pi_0\mathcal{E}_{2l-1}$	$q^{2l+1} - q^{2l} + q^l$
	1tan+1n-tan	$\mathcal{P}_{2l}$	
	2 tan	$\Pi_0\mathcal{H}_{2l-1}$	
5	2 n-tan $\mathcal{E}$	$\mathcal{P}_{2l}$	$q^{2l+1} - q^{2l} + 2q^l$

Théorème [Nicholas Katz, 1971]

Théorème[Edoukou, Dec. 2008]
Soit $\mathcal{X}$ une quadrique non-dégénérée dans $\mathbb{P}^{2l+2}(\mathbb{F}_q)$ avec $l \in \mathbb{N}^\star$.
Alors tous les poids du code $C_2(X)$ défini sur X sont divisibles par q^l.

VII-Questions ouvertes: une conjecture à résoudre

En 2007, **Conjecture:**

Soient $\mathcal{Q}_1$ et $\mathcal{Q}_2$ deux quadriques dans $\mathbb{P}^n(\mathbb{F}_q)$ n'ayant pas d'hyperplan commun.
Alors:

$$\boxed{|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq 4q^{n-2} + \pi_{n-3}}$$

Remarque:
$\boxed{n = 2, 3, 4} \Rightarrow \boxed{\text{conjecture vraie}}$.

- En Juillet 2007,

$$\boxed{|\mathcal{Q}_1 \cap \mathcal{Q}_2| \leq 4q^{n-2} + \pi_{n-3} + 2q^{n-3}}$$