Attaques basées sur les produits de codes

A.Michel, Y.Zirri et J.Doz

Master CSI, Université de Bordeaux, France

17 mars 2015

Plan

Codes de Reed-Solomon généralisés

- Soit $x = \{x_1, x_2, \ldots, x_n\}$ une partie à n éléments distincts de $\mathbb{F}_q, n < q$ et y un n-uplet d'éléments non nuls de $\mathbb{F}_q^n$.
  Un code de Reed-Solomon généralisé est l'ensemble des vecteurs de $\mathbb{F}_q$ qui s'écrivent sous la forme :

$$GRS_k(x,y) = \{\ (y_1.P(x_1), y_2.P(x_2), \ldots, y_n.P(x_n)),\ P(X) \in F_q[X]_{<k}\ \}$$

Codes de Reed-Solomon généralisés

- Soit $x = \{x_1, x_2, \ldots, x_n\}$ une partie à n éléments distincts de $\mathbb{F}_q, n < q$ et y un n-uplet d'éléments non nuls de $\mathbb{F}_q^n$.
  Un code de Reed-Solomon généralisé est l'ensemble des vecteurs de $\mathbb{F}_q$ qui s'écrivent sous la forme :

$$GRS_k(x,y) = \{\ (y_1.P(x_1), y_2.P(x_2), \ldots, y_n.P(x_n)),\ P(X) \in F_q[X]_{<k}\ \}$$

- "Singleton Bound" : Pour tout code $[n,k,d], d \leq n-k+1$.
  Si c'est un code de Reed-Solomon généralisé, alors nous avons $d = n-k+1$.

Produits de code

- Soit $a = (a_1, \ldots, a_n)$ et $b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$.
  On note $a \star b$ le produit par composante $a \star b = (a_1.b_1, \ldots, a_n.b_n)$.

Produits de code

- Soit $a = (a_1, \ldots, a_n)$ et $b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$.
  On note $a \star b$ le produit par composante $a \star b = (a_1.b_1, \ldots, a_n.b_n)$.

- Soit A et B deux codes de longueur n.
  $A \star B$ est l'espace vectoriel engendré par tous les produits $a \star b$ où $a \in A$ et $b \in B$.

Produits de code

- Soit $a = (a_1, \ldots, a_n)$ et $b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$.
  On note $a \star b$ le produit par composante $a \star b = (a_1.b_1, \ldots, a_n.b_n)$.

- Soit A et B deux codes de longueur n.
  $A \star B$ est l'espace vectoriel engendré par tous les produits $a \star b$ où $a \in A$ et $b \in B$.

- Pour $k \leq \frac{n+1}{2}$, $GRS_k(x, y)^2 = GRS_{2k-1}(x, y \star y)$.

Cryptosystème de McEliece

Le cryptosystème Le cryptosystème de McEliece est le premier cryptosystème asymétrique basé sur la théorie des codes correcteurs. Sa sécurité se base sur le problème NP-complet du décodage.
Génération de Clef Le cryptosystème de McEliece est le premier cryptosystème asymétrique basé sur la théorie des codes correcteurs. Sa sécurité se base sur le problème NP-complet du décodage.

Questions ?

Codage/Décodage