Introduction

Notations

- $f \in L(\mathbb{F}^k, \mathbb{F}^n)$ avec k < n
- $G = Mat(f)$ matrice génératrice $n \times k$
- $Ker(H) = Im(f)$ matrice de parité $k \times n$
- $S_y : y \in \mathbb{F}^n \rightarrow Hy \in \mathbb{F}^k$ syndrome
- $\omega : y \in \mathbb{F}^n \rightarrow Card(i/y_i \neq 0)$ poids de Hamming
- d la distance minimale du code

Définition

- g polynôme de $\mathbb{F}_{2^m}[X]$ irréductible
- $L = (\alpha_1, .., \alpha_n) \in \mathbb{F}_{2^m}^n$ le support

On définit un code de Goppa par son syndrome

$$\mathbf{S}_y(x) = \sum_{i=1}^{n} \frac{y_i}{x - \alpha_i} \ mod \ g(x)$$

En pratique on prendra $n = 2^m$

Matrice de parité

$$\frac{1}{x-\alpha_i} = \frac{1}{g(\alpha_i)} \sum_{k=0}^{t-1} x^k \sum_{j=k+1}^{t} g_j \alpha_i^{j-1-k}$$

De là on déduit une expression d'une matrice de parité.

$$\begin{pmatrix} \frac{1}{g(\alpha_1)} & \frac{1}{g(\alpha_2)} & \cdots & \frac{1}{g(\alpha_n)} \\ \frac{1}{g(\alpha_1)} g_t \alpha_1 & \frac{1}{g(\alpha_2)} g_t \alpha_2 & \cdots & \frac{1}{g(\alpha_n)} g_t \alpha_n \\ \vdots & \vdots & \vdots & \vdots \\ \frac{1}{g(\alpha_1)} g_t \alpha_1^{t-1} & \frac{1}{g(\alpha_2)} g_t \alpha_2^{t-1} & \cdots & \frac{1}{g(\alpha_n)} g_t \alpha_n^{t-1} \end{pmatrix}$$

Décodage

Soit le polynôme localisateur d'erreurs σ

$$\sigma_y(x) = \prod \epsilon_i(x - \alpha_i)$$

Il faut résoudre l'équation clef suivante :

$$\omega_y(x) = S_y(x)\sigma_y(x) \ mod \ g$$

On montre son unicité. On explicite une solution avec l'algorithme d'Euclide étendu.

Clefs

Clef privée

- G matrice génératrice, ainsi que L et g
- P matrice de permutation $n \times n$
- Q $\in GL_k(\mathbb{F})$

Clef publique

- G' = PGQ
- capacité de correction

Principe

- $x \in \mathbb{F}^k$ le message a envoyer
- $G'x + \epsilon = PGQx + \epsilon$ message envoyé
- $GQ + P^{-1}\epsilon$ peut être corrigé
- Connaissant Q on déduit x le message initial

Sécurité par 2 problèmes de théorie des codes :

- Indistinguabilité d'un code de Goppa
- Décodage par syndrome NP-complet

Programmation Orientée objet

Rédaction de classes :

- Corps de galois $\mathbb{F}_{p^m}$
- Optimisation en binaire pour p=2
- Matrices
- Polynomes
- Clefs publiques et clefs privées

Algorithme de Berlekamp-Hensel

Teste l'irréductibilité de $g \in \mathbb{F}_{2^m}[X]$

$\exists P / 1 < deg(P) < deg(g)$ *et* $P^{2^m} - P = 0$ *mod* $g \Leftrightarrow g$ *reductible*

Par le morphisme de Frobenius, on regarde le noyau de l'application linéaire :

$$P \leftarrow P^{2^m} - P$$