MII - Codes correcteurs d'erreurs

Janvier 2007 - tous documents manuscrits autorisés

Les parties I,II et III sont indépendantes

I Applications du cours

1) Expliquer en quelques lignes le principe de l'algorithme de Viterbi et pourquoi il est si utilisé.

2) Soit le code convolutif ayant pour générateurs $g_1 = (1101)$ et $g_2 = (1011)$.

a) Quels sont les paramètres (n, k, m) de ce code.

b) Donner le schéma de ce code.

c) Calculer l'image du mot (10111) par ce code.

II Réduction des clés pour le schéma de McEliece

Dans cette partie on se propose de réduire la taille des clés utilisées dans le système de McEliece.

1) Rappeler le principe du cryptosystème de McEliece. Et présenter ses intérêts par rapport aux systèmes classiques basés sur la théorie des nombres.

Un code C est dit quasi-cyclique d'ordre s si toute permutation circulaire σ de s positions vers la droite associe un mot du code à un autre mot du code. En d'autres termes si le code est stable sous l'action de σ. En particulier un code cyclique est un code quasi-cyclique d'ordre 1.

2) Montrer que tout code cyclique de longueur $n = rs$ est quasi-cyclique d'ordre s.

3) Montrer que le groupe d'automorphisme d'un code est le même que celui de son dual. Caractériser la notion de quasi-cyclicité d'ordre s en terme d'élément du groupe d'automorphisme. En déduire que le dual d'un code quasi-cyclique d'ordre s est aussi quasi-cyclique d'ordre s.

4) Soit C un code $[n, k]$ quasi-cyclique d'ordre s avec $n = rs$ montrer qu'il existe nécessairement une matrice $k' \times n$ M_C (avec $k' \geq k$), qui engendre C de la forme:

$$M_C = \begin{pmatrix} A_1 & A_2 & A_3 & \cdots & A_r \\ A_r & A_1 & A_2 & \cdots & A_{r-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ A_2 & A_3 & A_4 & \cdots & A_1 \end{pmatrix}.$$

où les A_i sont des matrices $\frac{k'}{r} \times s$.

Décrire (simplement) un algorithme qui permet de construire une matrice M_C associée à tout code C quasi-cyclique d'ordre s.

(chaque 1 k pour un seul mot)

Un mot nou[illegible] donne une ma[illegible] A_i et une ma[illegible] A_i nou[illegible] donne une [illegible] M_C par l[illegible]

pour obtenir un sous-code quasi cyclique, on considère
... cyclique, après on lui enlève un mot et les mots
s-shiftés

5) Pourquoi n'a-t-on pas en général $k' = k$? Construire un exemple de code quasi-cyclique $[n, k]$ d'ordre 5 en longueur 15 (simplement à partir d'un ensemble de définition d'un code cyclique de longueur 15) tel que $k' > k$. La matrice M_C est-elle en général ce qu'on appelle une matrice génératrice de C ?

On souhaite maintenant construire des sous-codes quasi-cycliques d'ordre s à partir d'un code quasi-cyclique $C[n, k]$ d'ordre s.

6) Montrer qu'en partant d'un mot aléatoire x de $\mathbb{F}_2^n$, on peut construire un sous-code quasi-cyclique d'ordre s de C de dimension au moins $k - \frac{n}{s}$ en ajoutant un certain nombre de mots bien choisis (liés à x) à une matrice de parité de C → les mots qu'on choisit c'est un mot aléatoire + tous les s-shiftés

7) En déduire alors qu'on peut par cette méthode construire au moins $2^{k-[illegible]}$ sous-codes quasi-cycliques d'ordre s de C.

On souhaite maintenant proposer un schéma qui diminue la taille de la clé publique. Soit M_C une matrice associée à C comme au 4). Il est clair que la donnée des A_i de la première ligne par blocs de M_C permet de reconstruire M_C.

8) Proposer un ensemble Π très simple de permutations par blocs tel que l'action de tout élément P de Π sur M_C conserve la quasi-cyclicité d'ordre s. Montrer qu'alors la donnée de la première ligne par blocs de $M_C.P$ (l'action de P sur M_C) permet de reconstruire tout $M_C.P$. Quel est alors le gain approximatif pour décrire la matrice permutée par rapport au schéma de McEliece classique?

9) Les éléments de Π permettent alors de cacher la structure originelle de la matrice M_C et on se propose de les utiliser comme permutation secrète plutot qu'une permutation de taille n comme dans le schéma original de McEliece. Quel est le nombre d'éléments de Π ? En déduire une contrainte sur n pour que l'ensemble des clés secrètes soit assez important.

10) Supposons que la clé publique du schéma soit donnée directement par une matrice de type $M_C.P$ décrite au 9). Montrer qu'alors une telle matrice ne peut être utilisée directement dans le schéma de McEliece. Montrer qu'il faut nécessairement en extraire une matrice génératrice du code permuté $C.P$. Décrire (simplement) le principe d'un tel algorithme.

On admettra qu'il est important que l'ensemble des codes possibles pour le schéma de McEliece soit important.

11) Donner un exemple d'une famille infinie de codes quasi-cycliques avec de bons paramètres et très facilement décodable.

12) Décrire à partir des idées précédentes une variation sur le schéma de McEliece avec une taille de clé publique beaucoup plus petite.

13) On suppose qu'on prend le cas pour la famille de code du 11) des longueurs $n = 1023$ et $n = 2047$. Quels ordres s peut-on proposer alors ? En supposant qu'on parte de codes de taux 1/2, comparer approximativement la taille des clés par le schéma originel de McEliece et par le schéma du 12).

III Principe d'équilibre

Soit C un code auto-dual $[n, \frac{n}{2}]$. Soit P_{n_1} un ensemble de n_1 coordonnées et soit P_{n_2} l'ensemble des $n_2 = n - n_1$ coordonnées complémentaires. On appelle C_1 le code engendré par les mots de C dont le support est contenu dans P_1 (cela correspond aussi aux mots qui sont nuls sur P_2). De même C_2 est le code engendré par les mots de C dont le support est dans P_{n_2}.

1) Montrer que C_1 et C_2 sont des sous-codes linéaires de C.

2) Montrer qu'en réordonnant par permutation les coordonnées de P_{n_1} comme les colonnes les plus à gauche, respectivement les plus à droite pour P_{n_2}, que C a pour matrice génératrice à permutation près:

$$G = \begin{pmatrix} A & 0 \\ 0 & B \\ D & E \end{pmatrix}$$

avec C_1 engendré par $[A\ 0]$ et C_2 engendré par $[0\ B]$. Avec A, B, D, E des matrices et 0 la matrice nulle (de taille adaptée).

3) Montrer que si $k_i = \dim(C_i)$ (i=1,2) alors les matrices D et E ont chacune rang $\frac{n}{2} - k_1 - k_2$.

4) Soit C_A le code engendré par la matrice A et soit C_{AD} le code engendré par les rangées de A et D. Montrer qu'alors $C_{AD} = C_A^{\perp}$. De même pour $C_{BE} = C_B^{\perp}$.

5) En utilisant l'auto-dualité de C, montrer qu'un calcul sur les dimensions de C_A et de son orthogonal implique que que $k_1 + (\frac{n}{2} - k_2) \leq n_1$. En déduire une formule similaire à partir de C_B.

6) Déduire de la question précédente, le principe d'équilibre:

$$dim\, C_1 - \frac{n_1}{2} = dim\, C_2 - \frac{n_2}{2}.$$

7) On s'intéresse maintenant à l'existence potentielle d'un code $[10, 5, 4]$ auto-dual (distance extrémale d'après les bornes vues en cours). Supposons qu'un tel code existe, alors, appliquer le principe d'équilibre en prenant pour A un code très simple de dimension 1. En déduire l'existence d'un certain code auto-orthogonal $[6, 2, 4]$. Montrer qu'un tel code ne peut exister et conclure sur l'existence d'un $[10, 5, 4]$ auto-dual.

8) Montrer d'une manière similaire qu'un code $[18, 9, 6]$ auto-dual ne peut exister.