IFT6170 Devoir 4

à rendre au début du cours le mercredi 3 décembre 1997

Partage de secret [6 points]

Soit un code Reed-Solomon sur $\mathcal{F}_q$ ayant des paramètres $[N = q-1, K, N-K+1]$. On suppose que ses mots de code sont définis de façon standard

$$c = (c_0\ c_1\ \ldots\ c_{N-1}) = \big(F(1), F(\alpha), ..., F(\alpha^{N-1})\big)$$

pour les polynômes F sur $\mathcal{F}_q$ de degré $< K$. Supposons qu'Alice dispose d'un secret $s \in \mathcal{F}_q$. Elle peut choisir un polynôme aléatoire

$$F(x) = s + f_1 x + f_2 x^2 + \cdots + f_{K-1}x^{K-1}$$

tel que $F(0) = s$, où chaque f_i est sélectionné au hasard dans $\mathcal{F}_q$. Soit $P_0, P_1, ..., P_{N-1}$ des personnes distinctes à qui Alice va distribuer des "ombres" de son secret: Alice donne c_i à P_i. Soit $\Phi \subseteq \{0, 1, ..., N-1\}$.

- Montrez que si $|\Phi| < K$ alors $\mathbf{I}(s; \{(i, c_i) : i \in \Phi\}) = 0$. C'est à dire que tout ensemble de personnes de taille inférieure à K n'a aucune information sur s.
- Montrez que si $|\Phi| \geq K$ alors $\mathbf{H}(s \mid \{(i, c_i) : i \in \Phi\}) = 0$. C'est à dire que tout ensemble de personnes de taille au moins K peut déterminer s.
- Supposons que toutes les personnes se rencontrent et échangent leurs c_i. Considérons qu'un certain nombre t d'entre eux soit menteur et révèlent au contraire $\tilde{c}_i \neq c_i$. Donnez une relation entre N, K et t qui donne les situations où l'on sera capable d'identifier les menteurs et de récupérer quand même le secret s. Comment peut-on identifier les menteurs efficacement?

Justesen généralisés [6 points]

Considérez sur $\mathcal{F}_2$ les codes $C_{\alpha,\beta} = \{[u, \alpha u, \beta u] : u \in \mathcal{F}_{2^m}\}$ pour $\alpha, \beta \in \mathcal{F}_{2^m} - \mathbf{0}$.

- Montrez qu'il existe parmis les codes $C_{\alpha,\beta}$ des codes de paramètres $[3m, m, 3\gamma m]$ pour $\gamma \geq h^{-1}\left(\frac{2}{3}\right) \approx 0.1739523$.
- Montrez qu'une construction semblable à celle de Justesen nous permet de construire à partir des codes $C_{\alpha,\beta}$ des codes sur $\mathcal{F}_2$ ayant des paramètres $[N, RN, \delta N]$ pour $N = 3m2^m$, $0 \leq R \leq \frac{1}{3}$ et $\delta \geq (1 - 3R)h^{-1}\left(\frac{2}{3}\right)$.
- Montrez qu'une construction semblable à la précédente nous permet de construire pour chaque entier a des codes sur $\mathcal{F}_2$ ayant des paramètres $[N, RN, \delta N]$ pour $N = am2^m$, $0 \leq R \leq \frac{1}{a}$ et $\delta \geq (1 - aR)h^{-1}\left(\frac{a-1}{a}\right)$.
- Tracez ces droites sur un graphique et montrez qu'elles forment un ensemble de tangentes à la courbe de Zyablov.

Codes réversibles [4 points]

Un code $C \subseteq \mathcal{F}_q$ est *réversible* si $c_0 c_1 \ldots c_{n-1} \in C$ implique $c_{n-1}c_{n-2}\ldots c_0 \in C$ également. Montrez qu'un code cyclique $C = \langle g \rangle$ est réversible si et seulement si $g(\alpha) = 0$ implique toujours $g(\alpha^{-1}) = 0$. Montrez qu'un code cyclique C est réversible si et seulement si -1 est une puissance de q modulo n.