Master CSI 2 2013-2014

Crypto avancée : feuille de TD 5

– Exercice 1. Problème du millionnaire. Alice et Bob sont des millionnaires possédant entre 1 et 10 millions, et qui souhaitent savoir qui est le plus riche, sans dévoiler leur fortune. On considère le protocole suivant, présenté ainsi par Yao (1982) :

- Alice donne à Bob sa clé publique RSA $(n, e = 3)$.
- Bob choisit un entier modulo n aléatoire x, calcule $y = x^3 \mod n$, puis communique à Alice l'entier $Z = y - j + 1$ où j est le nombre de millions qu'il possède.
- Alice calcule les entiers modulo n

  $$Z_1 = Z^{1/3}, Z_2 = (Z+1)^{1/3}, \ldots, Z_{10} = (Z+9)^{1/3}$$

  choisit un nombre premier π d'ordre de grandeur $\sqrt{n}$, calcule les réductions $z_i = Z_i \mod \pi$, $i = 1 \ldots 10$, puis communique à Bob l'entier π, ainsi que la suite d'entiers,

  $$z_1, z_2, \ldots, z_i, z_{i+1} + 1, \ldots, z_{10} + 1$$

  où i est le nombre de millions qu'elle possède.
- calcule $x \mod \pi$ est le compare à z_j. Si $x = z_j \mod \pi$, alors il en conclut que $i \geqslant j$ et que $i < j$ sinon.
- Bob communique à Alice le résultat.

Commenter la complétude et la validité du protocole en faisant des hypothèses raisonnables. Comment peut-on généraliser le protocole et étudier plus précisément sa validité grâce à une fonction de hachage.

– Exercice 2. On souhaite construire des matrices $H = [\mathbf{h}_1, \mathbf{h}_2, \ldots, \mathbf{h}_n]$ de $\mathbb{F}_2^{r \times n}$ avec la propriété :

$$\forall I \subset \{0,1\}^n, \text{ une des deux sous-matrices } H_I \textit{ ou } H_{\overline{I}} \text{ est de rang } r.$$

a) Montrer que la matrice de parité d'un code de Hamming

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

a cette propriété, mais pas celle du code de Hamming étendu

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

b) Montrer que la matrice H a la propriété voulue si et seulement si le code linéaire engendré par les lignes de H a la propriété d'intersection, c'est-à-dire que deux mots non nuls quelconques du code ont des supports qui s'intersectent.

– Exercice 3.

a) On suppose qu'Alice veut envoyer un message secret $s \in \mathbb{F}_2^r$ à Bob en présence d'un espion qui écoute la communication à travers un un canal à effacements de probabilité d'effacement p (problème du wiretap). Soit H une matrice aléatoire de $\mathbb{F}_2^{r\times n}$. Alice communique à Bob un vecteur $\mathbf{x} \in \mathbb{F}_2^n$ sur le canal «wiretap», ainsi que la quantité $s+H\,{}^t\mathbf{x}$ sur un canal totalement public. Montrer pourquoi l'espion n'a aucune information sur s. On pourra invoquer le résultat suivant : une matrice aléatoire uniforme de $\mathbb{F}_2^{r\times r+\ell}$ a rang r avec probabilité au moins $1 - 1/2^\ell$.

b) On suppose maintenant qu'Alice et Bob partagent à canal à effacement de probabilité p, ainsi qu'un canal non-bruité. On souhaite réaliser un protocole de transfert inconscient d'un secret parmi les deux $\{s_1, s_2\}$ d'Alice vers Bob. On commence par traiter le cas $p = 1/2$. Comment réaliser un tel protocole, en commençant ainsi : Alice envoie à Bob un vecteur x aléatoire de n bits sur le canal à effacements, où $n = 4r$, r étant la longueur en bits de chacun des secrets s_1, s_2.