TD2 - MPC II

Responsable : M. Bombar

1 Transferts Inconscients et Transferts Inconscients Aléatoires

On rappelle qu'un protocole de transfert inconscient vise à calculer la fonctionnalité idéale suivante où les messages m_0, m_1 sont fixés.

Objectif :

- Bob apprend m_σ.
- Alice n'apprend rien sur σ.
- Bob n'apprend rien sur $m_{1-\sigma}$.

Cependant, dans le modèle du précalcul, on obtient des OT aléatoires, où les messages m_0, m_1 sont remplacés par des bits uniformément aléatoires r_0, r_1, de même pour $b \leftarrow \{0,1\}$.

(Q1) On suppose qu'Alice et Bob partage un OT aléatoire, c'est à dire qu'alice possède (r_0, r_1) uniformément aléatoires, Bob possède (s, r_s) où s est aléatoire. Construire alors un protocole sécurisé extrêmement efficace pour réaliser un véritable Transfert Inconscient entre Alice et Bob (sur des véritables messages m_0, m_1 chosis par Alice.

2 Protocole d'Extension d'OT : IKNP

On a vu dans le cours que les protocoles de transferts inconscients nécessitaient de la cryptographie à clé publique, qui est souvent assez coûteuse. Or, nous avons besoin de deux OT par multiplication, ce rend les protocoles beaucoup moins attractifs. Dans cet exercice, on propose de regarder un protocole dû à Ishai, Kilian, Nissim et Petrank [**IKNP03**] qui explique comment construire un nombre m arbitraire (par exemple $m = 10^9$) d'OT à

partir d'un petit nombre initial (par exemple $n = 128$). Ce protocole reste aujourd'hui une référence pour la construction d'OT.

Mise en place : Alice possède m paires $(x_1^{(0)}, x_1^{(1)}), \ldots, (x_m^{(0)}, x_m^{(1)})$ qui correspondent à ses entrées du protocole d'OT général, et Bob possède un vecteur binaire de sélection $\sigma \stackrel{\text{def}}{=} \sigma_1, \ldots, \sigma_m$. Le protocole se joue alors en 2 phases.

Phase I : Alice et Bob vont réaliser un petit nombre n d'OT, mais attention, ils inversent leurs rôles : Alice devient le récepteur et Bob devient l'envoyeur.

- Plus précisément, Bob génère aléatoirement $T_1, \ldots, T_n$ où $T_j \leftarrow \mathbb{F}_2^m$. Il prépare alors les n paires $(T_j, T_j \oplus \sigma)$ qui seront ses entrées du protocole d'OT interne.
- De son côté, Alice génère aléatoirement $s \stackrel{\text{def}}{=} (s_1, \ldots, s_n) \leftarrow \mathbb{F}_2^n$ qui seront ses bits de sélection pour le protocole interne.
- À la fin du protocole, Alice reçoit des vecteurs $Q_1, \ldots, Q_n \in \mathbb{F}_2^m$ qu'elle écrit en colonne dans une matrice $Q \in \mathbb{F}_2^{m \times n}$.
- Bob construit de même la matrice $T \in \mathbb{F}_2^{m \times n}$ correspondant à ses vecteur T_i comme colonnes.

Phase II : Il s'agit du véritable transfert inconscient entre Alice et Bob. Pour $1 \leq i \leq m$, on note $Q(i)$ (respectivement $T(i)$) la i-ème ligne de Q (respectivement T). Ce sont des vecteurs de longueur n. Alice définit

$$y_i^{(0)} \stackrel{\text{def}}{=} H(i, Q(i)) \oplus x_i^{(0)}, \qquad y_i^{(1)} \stackrel{\text{def}}{=} H(i, Q(i) \oplus s) \oplus x_i^{(1)}.$$

qu'elle envoie à Bob, où $H : \mathbb{N} \times \mathbb{F}_2^n$ est une fonction de hachage.

(Q2) Que doit calculer Bob pour obtenir $x_i^{(\sigma_i)}$?

(Q3) On modélise H par un oracle aléatoire. Montrer que le protocole est alors sécurisé.

3 Multiplication Sécurisée à n joueurs

(Q4) Expliquer comment réaliser un protocole de multiplication sécurisée à n joueurs, où les joueurs possèdent un (n, n)-partage de deux entrées x et y.

4 Comportement Malicieux et Évaluation de Circuit

On considère un protocole à 3 joueurs d'évaluation de circuit arithmétique avec sécurité passive (*i.e.*, contre des adversaires semi-honnêtes). Par exemple, BGW ou GMW comme vus dans le cours.

On suppose que les trois joueurs P_1, P_2, P_3 cherchent à calculer $f(x_1, x_2, x_3) \stackrel{\text{def}}{=} x_1 x_2 x_3$.

(Q5) Dérouler le protocole BGW sur le calcul de f sur $\mathbb{F}_5$.

(Q6) Montrer que si P_1 joue un adversaire **actif** (c'est-à-dire que s'il ne respecte pas le protocole entièrement) il peut apprendre x_3.

(Q7) En déduire que BGW à 3 joueurs ne peut pas être sécurisé contre des adversaires malicieux.