Université de Sherbrooke - Département d'informatique
IFT814 – Cryptographie
Martin Fiset, chargé de cours

**Devoir 5**
**Date de remise : Vendredi 28 novembre à 23h59**

Effectuez ce devoir en équipe d'au plus 4 personnes. Utilisez MOODLE, le système de soumission de travaux du Département d'informatique, pour soumettre votre travail. Soumettez un seul fichier PDF par équipe (n'oubliez pas d'y mettre tous les noms), contenant le pseudo-code source nécessaire comme texte dans le corps de votre devoir. Ce devoir compte pour 12% de la note finale.

Pour ce devoir, veuillez choisir 3 questions à faire parmi les 6 questions suivantes :
1, 2, 3.(a), 3.(b), 4, et 5.

Elles concernent :

- Le calcul sécuritaire multipartie,
- Deux saveurs de transfert à l'aveugle (oblivious transfer, OT), soit 1 parmi 2 OT (1/2 - OT) et Rabin OT (R - OT),
- La mise en gage (bit commitment, BC),
- Le lancement de pièce de monnaie fort (strong coin tossing/flipping, S-CT).

Vous pouvez utiliser comme vrai les résultats des autres questions si ça peut vous être utile. Vous pouvez également utiliser plus d'une instance de la primitive donnée (e.g. plusieurs OT pour obtenir un BC), vous pouvez supposer que vous avez accès à ces primitives où les rôles de Alice et Bob sont interchangés, et finalement, une sécurité imparfaite mais avec probabilité d'échec négligeable est suffisante.

## 1. OT à partir du calcul sécuritaire multipartie

Montrez comment ½ - OT peut être vu comme étant une instance dans le scénario du calcul sécuritaire multipartie. Combien y a-t-il de participants ? Quelles sont leurs entrées ? Leurs fonctions de sortie ?

Argumentez pourquoi les propriétés désirées sont satisfaites.

## 2. BC à partir de OT

En supposant l'existence d'une procédure pour implémenter ½ - OT, montrez comment vous en servir d'une façon ''boîte noire'' (c'est-à-dire sans avoir à considérer les détails d'implémentation) pour implémenter un BC.

Argumentez pourquoi les propriétés désirées sont satisfaites.

## 3. Deux saveurs de OT

### (a) ½ - OT à partir de R-OT

En supposant l'existence d'une procédure pour implémenter R - OT, montrez comment vous en servir d'une façon ''boîte noire'' (c'est-à-dire sans avoir à considérer les détails d'implémentation) pour implémenter ½ - OT.

Argumentez pourquoi les propriétés désirées sont satisfaites.

### (b) R-OT à partir de ½ - OT

En supposant l'existence d'une procédure pour implémenter ½ - OT, montrez comment vous en servir d'une façon ''boîte noire'' (c'est-à-dire sans avoir à considérer les détails d'implémentation) pour implémenter R- OT.

Argumentez pourquoi les propriétés désirées sont satisfaites.

## 4. CT à partir de BC

En supposant l'existence d'une procédure pour implémenter BC, montrez comment vous en servir d'une façon ''boîte noire'' (c'est-à-dire sans avoir à considérer les détails d'implémentation) pour implémenter S-CT.

Argumentez pourquoi les propriétés désirées sont satisfaites.

## 5. Partage de secret inefficace

Nous avons vu une manière d'implémenter le partage de secret où le seuil est égal au nombre de participants. Utilisez l'idée vue dans ce cas pour montrer une manière d'implémenter un partage de secret à 4 participants avec seuil de 3 parts.

---

## Question Bonus : TFHE et applications en santé

Le chiffrement totalement homomorphe sur le tore (TFHE - Fully Homomorphic Encryption over the Torus) est un schéma cryptographique permettant d'effectuer des calculs arbitraires sur des données chiffrées sans jamais les déchiffrer.

Décrivez une application concrète du TFHE dans le domaine de la santé. Votre réponse doit inclure :

- Une description claire du cas d'utilisation (quel problème est résolu ?)
- Les acteurs impliqués (patient, hôpital, serveur cloud, etc.)
- Un diagramme de flux simple montrant comment les données circulent entre les acteurs, en indiquant clairement quelles données sont chiffrées et où les calculs homomorphes sont effectués
- Une explication des avantages du TFHE pour cette application spécifique par rapport à d'autres approches cryptographiques

*Note : Le diagramme peut être dessiné à la main et numérisé, ou créé avec un outil de votre choix. Il doit être simple mais clair, montrant le flux : données en clair → chiffrement → traitement homomorphe → résultats (chiffrés ou déchiffrés).*

---

**Suggestions :**

Bibliographie :
L'utilisation de Zotero (extension dans votre navigateur) afin de créer un catalogue des liens de vos consultations sur le Net. À la fin, cela donne une bibliographie que vous pouvez insérer à la fin de votre PDF. C'est gratuit comme outil et très pratique pour la correction de vos travaux par les auxiliaires d'enseignement.
https://zotero.org

Pseudo-code :
Il existe plusieurs approches et façon de s'y prendre. En voici une utilisée au Collège de Lionel-Groulx, gracieuseté de Vincent Échelard (Coordonnateur académique UdS- programmes d'informatique au Pavillon de Longueuil):
Règles du bon pseudocode