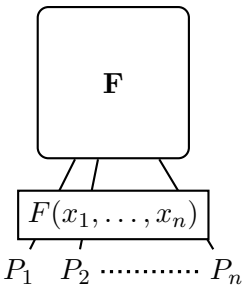
TD1 - Introduction au MPC

Responsable : M. Bombar

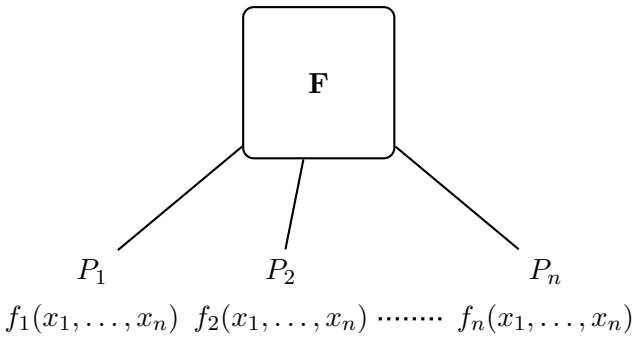
1 MPC avec Sorties Indépendantes

Considérons un protocole de MPC à n joueurs souhaitant calculer une certaine fonction : $f : G_1 \times \cdots \times G_n \to E$ où les G_i et E sont des groupes finis. Si ça vous rassure, pensez les comme étant un espace vectoriel de la forme $\mathbb{F}_q^\ell$.

Sorties identiques C'est le scénario vu dans ce cours. Ici, **tous les participants** obtiennent à la fin le **même** résultat $f(x_1, \ldots, x_n)$.



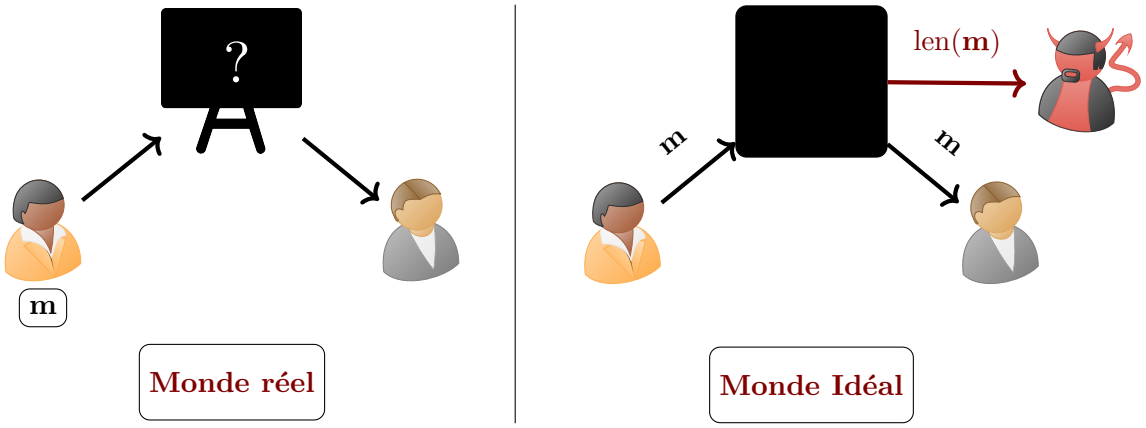
Sortie indépendantes Cette fois-ci les participants reçoivent chacun un **résultat spécifique** : le joueur P_i reçoit un résultat de la forme $f_i(x_1, \ldots, x_n)$, potentiellement différent des autres, et n'**apprend rien** sur $f_j(x_1, \ldots, x_n)$ pour $j \neq i$.



(Q1) Expliquez comment le second scénario peut-être utilisé pour représenter une situation où certains participants au protocole ne reçoivent pas de résultat.

(Q2) Montrez qu'une solution générale au MPC classique (scénario I) pour toute fonction f fournit une solution générale au MPC dans le second scénario.

2 Technique du Simulateur

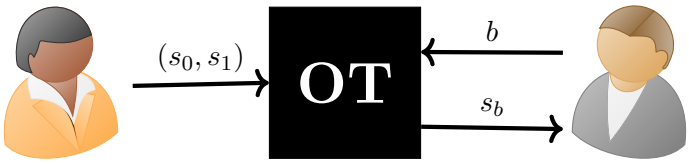


On considère un protocole de calcul sécurisé où Alice souhaite transmettre à Bob un message $\mathbf{m}$. On considère le modèle de communication de type « tableau noir » dans lequel un attaquant potentiel peut observer tous les messages qui sont échangés entre Alice et Bob. L'objectif est de construire un protocole permettant de réaliser cette fonctionnalité de manière à ce que l'attaquant ne puisse apprendre rien d'autre que la longueur du message.

(Q3) À l'aide d'une technique de Simulateur, montrez qu'un chiffrement IND-CPA réalise exactement ce protocole sécurisé.

3 Vers le Cours 02 : Transferts Inconscients et Protocoles de Multiplication

On définit la fonctionnalité de transfert inconscient (*Oblivious Transfer*) de la manière suivante



En d'autres termes, Alice possède deux bits s_0, s_1. Bob reçoit alors un des deux bits de son choix, et ne doit rien apprendre sur l'autre bit. Pendant ce temps, Alice ne doit pas savoir quel bit elle a transmis à Bob.

3.1 Protocoles de Multiplication Sécurisés

On suppose qu'il existe un protocole d'OT (on verra comment en construire un plus tard). L'objectif de cet exercice est de montrer comment réaliser un protocole de multiplication sécurisé sur des parts additives.

(Q4) À l'aide d'un protocole d'OT, construire un protocole permettant de calculer une part additive de la multiplication de deux bits tel que représenté dans la Figure 1.
Indication : Réaliser un protocole d'OT entre Alice et Bob de sorte que le bit de sélection de Bob soit son entrée x_2.

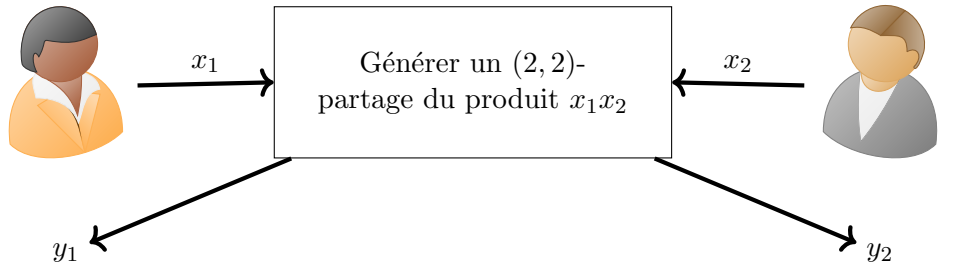


FIGURE 1 – Fonctionalité idéale pour la multiplication de 2 bits

(Q5) En déduire que l'on peut réaliser un protocole de multiplication sécurisé à deux joueurs en établissant 2 protocoles d'OT.

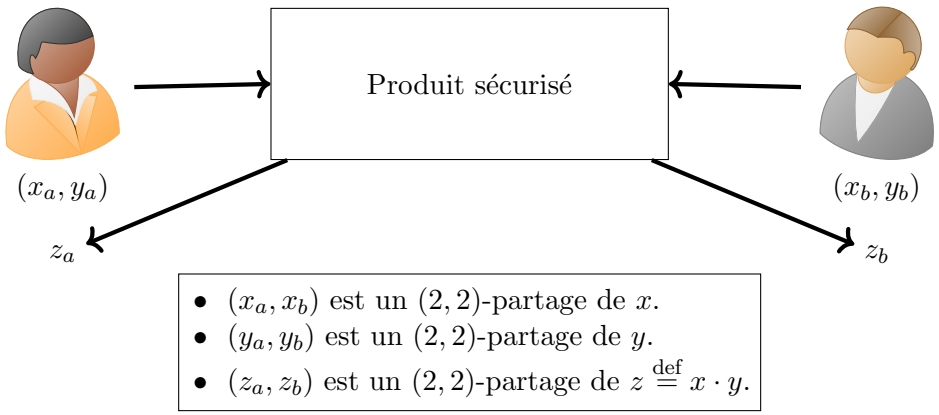


FIGURE 2 – Fonctionalité idéale pour la multiplication de 2 parts.