École normale supérieure **2022-2023**
Département d'informatique

Introduction à la cryptologie
TD n° 4 : Calcul multipartite.

Dans tous les protocoles qui suivent, on suppose que les participants sont honnêtes.

Exercice 1 (Calcul de produit à n joueurs)**.** Soit $\mathbb{G} = \langle g \rangle$ un groupe fini d'ordre p. On considère n joueurs $P_1, \ldots, P_n$, disposant respectivement d'une donnée $x_1, \ldots, x_n \in \mathbb{G}$. Leur but est de calculer le produit $x_1 \cdots x_n$ sans révéler d'information sur leurs valeurs respectives.

1. Montrer que le chiffrement d'El Gamal est multiplicativement homomorphe, autrement dit, montrer qu'étant donné deux chiffrés c_x, c_y de x et de y respectivement, on peut calculer un chiffré de $x \cdot y$.
2. En utilisant de la cryptographie distribuée, en déduire un protocole pour résoudre le problème.

Exercice 2 (« Five-card trick »)**.** Alice et Bob sont en couple depuis de nombreuses années et se posent la question du mariage... Cependant, aucun des deux n'ose faire sa demande de peur de subir l'affront d'un refus de son partenaire. Ils voudraient donc effectuer un calcul distribué entre eux deux dont le résultat est « oui » si et seulement les deux veulent se marier, et où les participants n'apprennent rien d'autre que ce résultat. Cependant, à cause du confinement, tout ce qu'ils ont sous la main est un jeu de cartes...
Voilà comment ils procèdent. Ils utilisent 5 cartes : 3 cartes ♣, deux cartes ♡. On suppose que les cartes face cachée sont indistinguables. Alice et Bob prennent chacun une carte ♣ et une carte ♡.

— Si Alice veut se marier, elle place les cartes dans l'ordre ♡♣ face cachée sur la table. Sinon elle place ♣♡.
— Si Bob veut se marier, il place les cartes dans l'ordre ♣♡ face cachée à droite de celles d'Alice. Sinon il place ♡♣.
— Enfin, on place la carte ♣ restante face cachée entre les cartes d'Alice et celles de Bob. L'ordre est donc : 2 cartes d'Alice, ♣, 2 cartes de Bob.
— Alice effectue une permutation circulaire aléatoire des cartes (toujours face cachée), sans que Bob regarde. Bob fait de même, sans qu'Alice regarde.
— Finalement, les cartes sont retournées et tout le monde peut les voir.

1. Comment savoir si Alice et Bob veulent tous deux se marier en regardant la disposition finale des cartes ?
2. Montrer que si Alice ou Bob ne veut pas se marier, Alice et Bob n'apprennent rien d'autre que ce résultat. (Plus exactement, chacun d'eux n'apprend rien d'autre que ce qu'il peut inévitablement déduire du résultat et de son propre souhait.)
3. Ce protocole permet de calculer un « et » logique sécurisé entre les entrées d'Alice et de Bob. Proposer un protocole qui calculerait de même un « ou exclusif »(XOR).

Exercice 3 (Calcul privé d'intersection)**.** Deux pays frontaliers souhaitent déterminer la liste des gens considérés comme suspects simultanément par les douanes des deux pays. Pour des raisons de droit international, ils ne souhaitent pas révéler à l'autre pays les noms de suspects qu'il ne connaîtrait pas déjà. Autrement dit, le pays Alice a une liste de suspects A, et le pays Bob a une liste de suspects B. Ils veulent calculer conjointement $A \cap B$, sans révéler $A \setminus B$ ni $B \setminus A$.
Solution #1. Alice et Bob se mettent d'accord sur une fonction de hachage H, qu'on suppose sans collision. Alice envoie $\{H(x) : x \in A\}$. Bob envoie $\{H(x) : x \in B\}$. Les collisions entre ces deux ensembles révèlent les suspects communs.

1. Que pensez-vous de cette solution ?

Solution #2. Alice et Bob se mettent d'accord sur une fonction de hachage H, qu'on suppose sans collision. L'image de H est dans un groupe $\mathbb{G}$ cyclique d'ordre premier p où Diffie-Hellman décisionnel est difficile. Alice tire $a \leftarrow \mathbb{Z}_p$ et envoie $\{H(x)^a : x \in A\}$. Bob tire $b \leftarrow \mathbb{Z}_p$ et envoie $\{H(x)^b : x \in B\}$. Enfin, Alice et Bob publient respectivement $\{H(x)^{ab} : x \in B\}$ et $\{H(x)^{ab} : x \in A\}$.

2. Comment retrouver l'intersection commune ?
3. En supposant que $B \setminus A$ contient un seul élément, comment argumenter (sans preuve formelle) qu'Alice n'apprend rien sur cet élément au terme de l'échange ?

Solution #3. Alice choisit un chiffrement additivement homomorphique E (i.e. $E(a)+E(b) = E(a+b)$). Pour cela, pour chiffrer v, elle peut utiliser le chiffrement ElGamal de g^v, comme on avait fait pour le vote (le chiffré de v est donc $(g^r, g^v h^r)$ pour r aléatoire, générateur g, clef publique $h = g^x$). Alice calcule un polynôme $P = \prod_{a \in A}(X - a) = \sum \alpha_i X^i$, et envoie les $E(\alpha_i)$ à Bob, ainsi que la clef publique de E. Bob renvoie $E(P(b) \cdot r_b + b)$ pour chaque $b \in B$, avec r_b uniformément aléatoire.

4. Comment Bob peut-il effectuer son calcul ?
5. Comment Alice retrouve-elle le résultat ?
6. Comment argumenter qu'Alice n'apprend rien sur les valeurs dans $B \setminus A$?

Exercice 4 (Dîner de cryptologues)**.** N cryptologues sont invités à un dîner à la Tour d'Argent. À la fin du repas, le serveur annonce que l'addition est déjà payée. Les cryptologues voudraient savoir si c'est l'un d'entre eux qui a payé, ou si c'est une entité extérieure (comme la NSA). Mais si c'est l'un d'entre eux, soucieux de vie privée, ils ne veulent pas que cette personne ait à se révéler.
Voilà comment ils procèdent : si le cryptologue $i \in [\![1, N]\!]$ a payé le repas, on pose $p_i = 1$, sinon $p_i = 0$. Chaque paire (i, j) de cryptologues se met d'accord sur une valeur secrète uniformément aléatoire $x_{i,j} \in \{0, 1\}$ (en tirant secrètement à pile ou face par exemple [1]). Finalement, chaque cryptologue i publie

$$p_i + \sum_{j \neq i} x_{i,j} \bmod 2.$$

1. À partir des valeurs publiées, comment savoir si un des cryptologues a payé le repas ?
2. Un sous-ensemble K de cryptologues sont dans la poche du KGB, et voudraient savoir qui a payé le repas parmi les convives (si ce n'est pas la NSA). Ils mettent donc en commun toutes leurs valeurs secrètes $x_{i,j}$, et essaient de déduire un maximum d'information sur l'identité du payeur. Montrer qu'ils n'apprenent rien de plus ce faisant que ce qu'ils peuvent déduire purement du résultat du protocole (autrement dit, les autres valeurs qu'ils apprennent via le protocole ne révèlent rien de plus).
3. Au lieu d'échanger une valeur secrète avec tous les autres cryptologues, les cryptologues se mettent en cercle et échangent un secret commun $x_{i,j}$ seulement avec leur deux voisins immédiats. En fin de compte le cryptologue i publie donc $x_{i,i-1}+x_{i,i+1}+p_i \bmod 2$. La propriété de la question précédente est-elle vérifiée ? (Si on représente les cryptologues comme les sommets d'un graphe, avec une arête ssi ils communiquent, on utilise donc un graphe cyclique au lieu d'un graphe complet.)
4. Plus généralement, est-il possible d'inventer une protocole où cette propriété est vérifiée, mais où le graphe n'est pas complet ?

1. Alternativement, voir TD précédent pour un protocole qui permet de le faire à distance !