École normale supérieure **2018-2019**
Département d'informatique

Introduction à la cryptologie
TD n° 8 : Chaîne de blocs.

Exercice 1 (Hachage pour preuve de travail)**.** On dit (informellement) qu'une fonction de hachage $H : \{0,1\}^* \to \{0,1\}^n$ est sûre pour les preuves de travail avec niveau de difficulté d ssi pour $x \in \{0,1\}^a$ uniforme, trouver $y \in \{0,1\}^*$ tel que $H(x \parallel y)$ commence par d zéros coûte un temps de calcul équivalent à 2^d appels à H. Ici $a > n > d$, et $\parallel$ dénote la concaténation de chaînes de caractères.

1. Soit $H : \{0,1\}^* \to \{0,1\}^n$ une fonction de hachage résistante aux collisions. Modifier H pour construire une fonction $H' : \{0,1\}^* \to \{0,1\}^{n+m}$ (m de votre choix) non sûre pour les preuves de travail avec niveau de difficulté d, mais aussi résistante aux collisions que H, au sens où toute collision sur H' implique une collision sur H.
2. Suite à la question précédente, on peut dire en un sens qu'une fonction de hachage qui résiste aux collisions n'est pas nécessairement sûre pour les preuves de travail. Qu'en est-t-il de la réciproque ? Pouvez-vous construire une fonction de hachage sûre pour les preuves de travail, mais non résistante aux collisions ?
3. Même question en remplaçant la résistance aux collisions par la résistance aux préimages.

Exercice 2 (Signatures de Lamport, Merkle et Goldreich)**.** Soit $H : \{0,1\}^\lambda \to \{0,1\}^\lambda$ une fonction à sens unique, c'est-à-dire : pour x uniforme dans $\{0,1\}^\lambda$, étant donné $H(x)$, trouver x est difficile (*i.e.* pas d'algorithme polynomial qui réussit avec probabilité non-négligeable). Protocole de signature à usage unique : Alice tire x_0, x_1 uniformément. Sa clef secrète est x_0, x_1, et sa clef publique est $pk_0 = H(x_0)$, $pk_1 = H(x_1)$. Pour signer un bit b, Alice publie x_b. Pour vérifier une signature, il suffit de vérifier $H(x_b) = pk_b$.

1. Supposons qu'il existe un adversaire $\mathcal{A}$ qui étant donné uniquement une clef publique du schéma ci-dessus, parvient à produire une signature en temps polynomial. Montrer que H n'est pas à sens unique.
2. Comment peut-on adapter le schéma ci-dessus pour signer un message quelconque (sans savoir à l'avance la longueur du message) ?
3. Alice souhaite pouvoir signer ℓ messages, et non juste un message. Elle peut utiliser ℓ instances du schéma ci-dessus, mais cela implique une taille de clef publique qui croît linéairement avec ℓ. Montrer comment utiliser un arbre de Merkle pour réduire la taille de la clef publique. Quelle est la taille d'une signature, en fonction de λ et de ℓ ?
4. Au lieu d'utiliser un arbre de Merkle binaire, on considère un arbre de Merkle k-aire, où chaque nœud interne a k enfants. Si l'on souhaite minimiser la taille d'une signature, quel choix de k est optimal ?
5. Dans le schéma précédent, quel est le temps nécessaire au calcul de la clef publique ? Peut-on signer un nombre exponentiel de messages ?
6. On considère maintenant un arbre binaire dont chaque nœud contient une instance de signature à usage unique comme ci-dessus. Chaque nœud interne est utilisé pour signer le haché des clefs publiques de ses deux enfants. Les feuilles sont utilisées pour signer des messages. Déduire de ce schéma général un schéma de signature permettant de signer un nombre exponentiel de messages. Quelle est la taille de la clef publique ? Quelle est la taille d'une signature ?

Exercice 3 (Mineurs égoïstes)**.** Supposons qu'un groupe E de mineurs égoïstes de bitcoin soient capables de faire la chose suivante : si un mineur hors du groupe réussit à publier un nouveau bloc dans la blockchain en même temps que le groupe publie un nouveau bloc (il y a donc un branchement), c'est le bloc appartenant au groupe E qui va l'emporter (l'autre branche sera abandonnée). Le groupe E se comporte de la manière suivante. Quand le groupe réussit à miner une nouveau bloc dans la blockchain, au lieu de le publier, il le garde pour lui et continue à miner sur cette branche de manière privée, sans rien publier. Si quelqu'un hors du groupe publie un nouveau bloc, le groupe E publie en même temps le bloc correspondant de sa chaîne privée (tant qu'elle est de longueur non nulle).
On suppose que le groupe E réussit à miner un bloc avant quelqu'un hors du groupe avec probabilité $\alpha < 1/2$. Autrement dit, à tout instant donné, le prochain bloc qui va être découvert sera trouvé par un mineur du groupe E avec probabilité α. Soit p_i^t la probabilité qu'à l'instant t, la chaîne privée du groupe E ait i blocs d'avance sur la chaîne publique. Au départ, $p_0^0 = 1$ et $p_i^0 = 0$ pour $i > 0$: le groupe E n'a aucun bloc d'avance. Chaque instant t discret correspond à l'apparition d'un nouveau bloc.

1. On admet que la distribtion de probabilité (p_i^t) tend vers un point fixe. Calculer ce point fixe. On suppose dans la suite qu'on a atteint ce point fixe.
2. On compte un gain de 1 pour le groupe E quand le nouveau bloc de la blockchain publique appartient à E. Donner l'espérance de ce gain.
3. Le groupe E augmente-t-il son rendement en étant égoïste ? Qu'en est-t-il du rendement des mineurs hors de E ? Ont-ils intérêt à se joindre à E ?