École normale supérieure **2019-2020**
Département d'informatique

Introduction à la cryptologie
TD n° 10 : Cryptographie post-quantique

Exercice 1 (Hachage et synchronisation)**.** Supposons qu'Alice partage avec un serveur distant (aussi connu sous le nom de « nuage ») un ensemble de n fichiers. De temps en temps elle souhaite pouvoir vérifier que ses fichiers locaux (chez elle) et distants (dans le nuage) sont bien synchronisés, i.e. égaux. Pour ça, au lieu de comparer tous les fichiers à chaque fois, son système de fichier maintient de part et d'autre un haché de la concaténation des fichiers. Pour tester l'égalité il suffit de vérifier l'égalité des hachés (comme chacun sait, une fonction de hachage est « injective »). On suppose que les fichiers sont de taille $O(1)$, et que le calcul d'un haché coûte un temps linéaire en la taille de l'entrée. Noter que dans cette solution, si Alice modifie un fichier, recalculer le haché global coûte un temps $O(n)$.

1. Donner une solution en $O(\log n)$ (au prix d'un surcoût négligeable en stockage).
   Indication : contrairement aux apparences, ça a un rapport avec le cours.

Exercice 2 (Signatures de Lamport)**.** On rappelle le schéma de signature de Lamport. 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 ?

Exercice 3 (Signatures de Winternitz)**.** On généralise le schéma de Lamport comme suit. $H : \{0,1\}^\lambda \to \{0,1\}^\lambda$ est toujours une fonction à sens unique. Pour simplifier l'analyse, supposons de plus que H est une permutation. Cette fois, nous allons signer un « message » $v \in \{0,\dots,a-1\}$ pour un certain $a \geq 2$, et non plus un seul but. Protocole : Alice tire x_0, x_1 uniformément. Sa clef secrète est x_0, x_1, et sa clef publique est $pk_0 = H^{a-1}(x_0)$, $pk_1 = H^{a-1}(x_1)$. Pour signer un message $v \in \{0,\dots,a-1\}$, Alice publie $H^v(x_0)$ et $H^{a-1-v}(x_1)$.

1. Comment peut-on vérifier une signature ?
2. Supposons qu'on modifie le schéma : au lieu de signer en publiant $H^v(x_0)$ et $H^{a-1-v}(x_1)$, Alice signe en publiant $H^v(x_0)$ et $H^v(x_1)$. Donner une attaque sur cette variante. Ici, une attaque signifie qu'étant donné la signature d'un message quelconque $v < a-1$, l'attaquant parvient à créer la signature d'un autre message.

3. Montrer que si le schéma de l'énoncé peut être attaqué étant donné la signature d'un message arbitraire, alors H n'est pas à sens unique.
4. Donner une idée pour réduire la taille de la clef privée à λ bits.
5. Supposons que l'on veuille signer un message $v \in \{0, a-1\}^k$ pour $k > 1$. Donner une solution avec : clef privée de λ bits, clef publique et signature de $2k\lambda$ bits. (Au maximum, si vous trouvez plus petit c'est encore mieux.)
6. Même question, avec clef publique et signature de $(k+1)\lambda$ bits.
Indication : clef privée $x_1, \ldots, x_k, x'$ uniformes, clef publique $H^{a-1}(x_0), \ldots, H^{a-1}(x_k), H^{ka-1}(x')$.

Exercice 4 (Huile et vinaigre)**.** On considère le schéma de signature « huile et vinaigre ». La clef publique est une fonction quadratique $F : \{0,1\}^{2k} \to \{0,1\}^k$ (qu'on va supposer homogène). La signature d'un message $Y \in \{0,1\}^k$ est un X tel que $F(X) = Y$. La fonction F est choisie de telle sorte que le i-ième bit de $F(X)$ s'exprime matriciellement $X^T F_i X = X^T S^T M_i S X$ pour des matrices $M_1, \ldots, M_k$ dont le quadrant inférieur droit est nul, et une matrice inversible S. La clef secrète est la décomposition de F en les M_i et S : la connaissance d'une telle décomposition permet de signer.
On rappelle que deux matrices A et B sont similaires ssi il existe C inversible telle que $A = C^{-1}BC$, et que deux matrices similaires ont le même polynôme caractéristique.

1. Montrer les matrices de la forme $S^{-1}KS$ où K a un quadrant supérieur droit entièrement nul forment une algèbre $\mathcal{A}$ (clôture par addition, multiplication interne et externe).
2. Montrer que pour tout $i \neq j$, $F_{i,j} = F_i^{-1} F_j$ appartient à $\mathcal{A}$.
3. Soit Z l'ensemble des vecteurs de $\{0,1\}^{2k}$ dont les k premières coordonnées sont nulles. Soit H (pour « huile ») défini par $H = S^{-1}Z$. Montrer que H est un espace propre des $F_{i,j}$.
4. Soit $M \in \mathcal{A}$. On admet qu'avec une probabilité « suffisamment élevée », la polynôme caractéristique de M est produit de deux polynômes irréductibles P_1 et P_2 de degré k (correspondant au polynôme caractéristique des deux quadrants diagonaux), et que dans ce cas, les seuls espaces propres non-triviaux de M sont les noyaux de $P_1(M)$ et $P_2(M)$. Montrer qu'un attaquant peut retrouver une décomposition de F de la même forme que la clef privée en temps polynomial, en utilisant seulement la clef publique.