ISEC - TME Projet
2019

Énoncé

Une *signature de Lamport* (ou *signature jetable*) est une méthode pour construire un protocole de signature numérique dont la sécurité repose sur une fonction à sens-unique $f : X \longrightarrow Y$. Ces signatures ont été proposées par L. Lamport en 1979.

Protocole de signature de Lamport

Génération des clés : étant donnée une fonction à sens unique $f : X \longrightarrow Y$ et un espace de message $\mathcal{M} = \{0,1\}^k$, le signataire tire uniformément aléatoirement $2k$ valeurs

$$(x_1^{(0)}, x_1^{(1)}, x_2^{(0)}, x_2^{(1)}, \ldots, x_k^{(0)}, x_k^{(1)}) \in X^{2k}$$

et calcule, pour $i \in \{1, \ldots, k\}$ et $j \in \{0,1\}$, $y_i^{(j)} = f(x_i^{(j)})$.
La clé publique est le vecteur $(y_1^{(0)}, y_1^{(1)}, y_2^{(0)}, y_2^{(1)}, \ldots, y_k^{(0)}, y_k^{(1)}) \in Y^{2k}$ et la clé secrète est le vecteur $(x_1^{(0)}, x_1^{(1)}, x_2^{(0)}, x_2^{(1)}, \ldots, x_k^{(0)}, x_k^{(1)}) \in X^{2k}$.

Signature : Pour signer un message $m = (m_1, \ldots, m_k) \in \mathcal{M}$ où $m_i \in \{0,1\}$ pour $i \in \{1, \ldots, k\}$, le signataire révèle $\sigma = (x_1^{(m_1)}, \ldots, x_k^{(m_k)}) \in X^k$.

Vérification : Le k-uplet $\sigma = (\sigma_1, \ldots, \sigma_k) \in X^k$ est une signature valide de $m = (m_1, \ldots, m_k) \in \mathcal{M}$ où $m_i \in \{0,1\}$ pour $i \in \{1, \ldots, k\}$ pour la clé publique

$$(y_1^{(0)}, y_1^{(1)}, y_2^{(0)}, y_2^{(1)}, \ldots, y_k^{(0)}, y_k^{(1)}) \in Y^{2k},$$

si et seulement si $f(\sigma_i) = y_i^{(m_i)}$ pour tout $i \in \{1, \ldots, k\}$.

Nous avons vu en cours plusieurs variantes des signatures de Lamport et l'objectif de ce projet est de les implanter et de comparer leur efficacité.

Le projet est à réaliser en binôme (un seul monôme est autorisé si le nombre d'étudiants est impair). Il devra comporter un programme (en langage C ou Python) et un rapport d'au plus 8 pages expliquant les choix effectués et comment utiliser le programme.

Le projet est à rendre pour le 13 mai 2019 (par courrier électronique à l'adresse damien.vergnaud@lip6.fr). En cas de problème personnel d'un étudiant, si le projet ne peut être rendu pour cette date butoir, il pourra être rendu au plus tard le 17 mai 2019 sans justificatif (mais aucun autre report ne sera autorisé). Le projet devra ensuite être présenté lors d'une soutenance de 20 minutes (10 minutes de présentation et 10 minutes de questions) la semaine du 20 mai 2019.

Exercice 1 :

1.a] Proposer un choix de fonction f pour que le schéma de signature de Lamport tel que décrit ci-dessus assure un niveau de sécurité de 128 bits (*i.e.* telle que la meilleure attaque en contrefaçon contre le schéma demande de l'ordre de 2^{128} opérations élémentaires).

1.b] Avec ce choix de fonction f, proposer une implantation du schéma de signature de Lamport (*i.e.* des trois algorithmes de génération de clés, de signature et de vérification) tel que présenté dans le cadre ci-dessus.

1.c] Donner les tailles en bits des clés publiques, des clés secrètes et des signatures pour un niveau de sécurité de 128 bits (pour un signer un message de 256 bits).

1.d] Implanter les variantes vues en cours du schéma de signature de Lamport qui permettent

1. de signer un message de taille arbitraire ;
2. d'avoir une clé secrète plus courte ;
3. d'avoir une clé publique plus courte ;

Donner les tailles en bits des clés publiques, des clés secrètes et des signatures pour un niveau de sécurité de 128 bits et comparer l'efficacité des algorithmes de signature et de vérification dans ces différents cas.

1.e] Considérons une variante de la signature de Lamport où le signataire ne révèle dans les signatures que les valeurs $x_i^{m_i}$ pour lesquelles $m_i = 1$ (et la vérification consiste simplement à vérifier que $f(\sigma_i) = y_i^{(m_i)}$ pour tous les $i \in \{1, \ldots, k\}$ tels que $m_i = 1$). Montrer que cette variante n'est pas résistante à la contrefaçon existentielle sous une attaque à un message choisi.

Justifier que si le signataire utilise en plus de cette variante, le schéma de Lamport classique (avec des clés indépendantes) pour signer le nombre de 1 qui apparaît dans m, alors cette variante est sûre et produit des signatures formées de $k + 2\lceil \log_2(k) \rceil$ éléments de X (au lieu de $2k$ éléments de X).

Indication. On pourra reprendre l'idée vue dans le TD5 pour signer des messages de taille quelconque inférieure ou égale à k en modifiant le schéma de Lamport.

Implanter cette variante et comparer l'efficacité du schéma de Lamport et de cette variante pour signer des messages de 64 bits, de 128 bits, de 192 bits et de taille arbitraire.

1.f] Nous supposons désormais que $X = Y$ et $f : X \longrightarrow X$. Considérons la variante suivante où $T \geq 1$ est un paramètre entier et pour tout entier $i \geq 0$, f^i désigne la fonction identité si $i = 0$ et $f \circ f^{i-1}$ si $i \geq 1$ (*i.e.* f^i consiste à composer i fois la fonction f).

Variante du protocole de signature de Lamport

Génération des clés : étant donnée une fonction à sens unique $f : X \longrightarrow Y$ et un espace de message $\mathcal{M} = \{0, 1, \ldots, T\}^k$, le signataire tire uniformément aléatoirement $2k$ valeurs

$$(x_1^{(0)}, x_1^{(1)}, x_2^{(0)}, x_2^{(1)}, \ldots, x_k^{(0)}, x_k^{(1)}) \in X^{2k}$$

et calcule, pour $i \in \{1, \ldots, k\}$ et $j \in \{0, 1\}$, $y_i^{(j)} = f^T(x_i^{(j)})$.
La clé publique est le vecteur $(y_1^{(0)}, y_1^{(1)}, y_2^{(0)}, y_2^{(1)}, \ldots, y_k^{(0)}, y_k^{(1)}) \in Y^{2k}$ et la clé secrète est le vecteur $(x_1^{(0)}, x_1^{(1)}, x_2^{(0)}, x_2^{(1)}, \ldots, x_k^{(0)}, x_k^{(1)}) \in X^{2k}$.

Signature : Pour signer un message $m = (m_1, \ldots, m_k) \in \mathcal{M}$ où $m_i \in \{0, 1, \ldots, T\}$ pour $i \in \{1, \ldots, k\}$, le signataire révèle $\sigma \in X^{2k}$ avec

$$\sigma = (f^{m_1}(x_1^{(0)}), f^{T-m_1}(x_1^{(1)}), f^{m_2}(x_2^{(0)}), f^{T-m_2}(x_2^{(1)}, \ldots, f^{m_k}(x_k^{(0)}), f^{T-m_k}(x_k^{(1)})).$$

Vérification : Le $2k$-uplet $\sigma = (\sigma_1^{(0)}, \sigma_1^{(1),} \ldots, \sigma_k^{(0)}, \sigma_k^{(1)}) \in X^{2k}$ est une signature valide de $m = (m_1, \ldots, m_k) \in \mathcal{M}$ où $m_i \in \{0, 1, \ldots, T\}$ pour $i \in \{1, \ldots, k\}$ pour la clé publique

$$(y_1^{(0)}, y_1^{(1)}, y_2^{(0)}, y_2^{(1)}, \ldots, y_k^{(0)}, y_k^{(1)}) \in Y^{2k},$$

si et seulement si $f^{T-m_i}(\sigma_i^{(0)}) = y_i^{(0)}$ et $f^{m_i}(\sigma_i^{(1)}) = y_i^{(1)}$ pour tout $i \in \{1, \ldots, k\}$.

1.g] Comparer cette variante avec le schéma de Lamport lorsque $T = 1$. Justifier rapidement la sécurité de ce schéma pour T quelconque.

1.h] Implanter ce schéma de signature.

1.i] En remarquant que avec les paramètres $T = 4$ et $k = 128$, ce schéma permet de signer des messages de 256 bits, comparer l'efficacité des algorithmes de signature et de vérification et les tailles des clés publiques, clés secrètes et signatures avec le schéma de Lamport de la question **1.c**.

1.j] Expliquer quelles modifications de la question **1.d** peuvent s'appliquer à cette variante du schéma de Lamport.

1.k] Proposer différentes valeurs de T et de k et comparer l'efficacité du schéma de Lamport et de cette variante pour signer des messages de 64 bits, de 128 bits, de 192 bits et de taille arbitraire.

1.l] **(Bonus)** Rechercher d'autres variantes du protocole de Lamport sur Internet et implanter les pour comparer l'efficacité du schéma de Lamport et de ces variantes pour signer des messages de 64 bits, de 128 bits, de 192 bits et de taille arbitraire.