Université Paris 8 Année 2021–2022

M1 Mathématiques et applications, parcours ACC et CSSD

Cryptographie à clef publique – Devoir semaine 6

devoir du 18/03/2022
à rendre jusqu'au 25/03/2022

Exercice 1. Signature de cercle.

Une signature de cercle (*ring signature*) est une primitive cryptographique qui permet à chaque membre d'un « cercle » (= groupe d'utilisateur) de signe anonymement un message m au nom du cercle.

Voici quelques propriétés désirées dans une signature de cercle :

1. N'importe quel vérificateur extérieur doit pouvoir vérifier (et être convaincu) qu'une signature s d'un message m est émise au nom du cercle.
2. Par ailleurs, il doit être impossible de déterminer quel membre du cercle a émis la signature.
3. Enfin, le signataire ne doit pas avoir besoin de l'aide d'autres membres du groupe pour poubvoir signer un message.

Dans cet exercice, on présente une signature de cercle basée sur la signature RSA-FDH. La fonction de hachage utilisée est notée H, à valeur dans $\{0,1\}^t$. On suppose également que toutes les clefs publiques des membres du cercle sont authentifiées.

Pour commencer l'exercice, on considère un cercle composé de deux membres seulement : Alice et Bob. Leurs clefs publiques sont respectivement (n_A, e_A) et (n_B, e_B). On suppose que les modules n_A et n_B sont de taille $t+1$ bits, et on assimile tout élément de $\{0,1\}^t$ avec un entier inférieur à 2^t. La signature d'un message $\boldsymbol{m}$ par Alice est donc $H(\boldsymbol{m})^{d_A} \mod n_A$ où d_A est la clé privée associée à (n_A, e_A).

On note enfin $\oplus$ l'opération de `xor` (addition modulo 2) bit-à-bit pour des entiers vus comme des chaînes de bits de longueur t.

L'Algorithme 1 décrit les opérations à effectuer par Alice pour émettre une signature de cercle. Notons qu'une description similaire est possible pour Bob, en remplaçant simplement les données propres à Alice par celles propres à Bob, et réciproquement. L'Algorithme 2 décrit la vérification de la signature effectuée par une personne potentiellement extérieure au cercle.

Question 1.– Vérifier que l'Algorithme 2 est valide, c'est-à-dire qu'il accepte toute signature effectuée honnêtement par Alice (ou Bob).

Question 2.– Expliquer en quoi la signature est anonyme pour un signataire quelconque du cercle. C'est-à-dire, argumenter sur le fait que le vérificateur ne peut pas savoir qui, parmi Alice et Bob, a produit la signature $s = (s_A, s_B)$.

Algorithme 1 : Algorithme de signature de cercle (opéré par Alice)

Entrée : un message $\boldsymbol{m}$, les clés publiques $(n_A, e_A), (n_B, e_B)$, la clé privée d_A d'Alice
Sortie : une signature de cercle s

1 Hacher le message $\boldsymbol{m}$ en $h = H(\boldsymbol{m})$.
2 Tirer aléatoirement $s_B \leftarrow (\mathbb{Z}/n_B\mathbb{Z})^\times$.
3 Calculer $z_B = s_B^{e_B} \mod n_B$.
4 Calculer $s_A = (z_B \oplus h)^{d_A} \mod n_A$.
5 Retourner $s = (s_A, s_B)$.

Algorithme 2 : Algorithme de vérification de signature de cercle

Entrée : un message $\boldsymbol{m}$, les clés publiques $(n_A, e_A), (n_B, e_B)$, une signature $s = (s_A, s_B)$
Sortie : accepte/refuse

1 Calculer $x = (s_A^{e_A} \mod n_A) \oplus (s_B^{e_B} \mod n_B)$.
2 Vérifier que $x = H(\boldsymbol{m})$.

On dit qu'une fonction de hachage est résistante au calcul de préimage si, étant donné un haché h, il est impossible calculatoirement de trouver un message $\boldsymbol{m}$ tel que $H(\boldsymbol{m}) = h$.

Question 3.– Supposons que la fonction de hachage H ne soit pas résistante au calcul de préimage. Donner une attaque sur le schéma de signature de cercle. On précisera le type d'attaque et les moyens donnés à l'attaquant.

Question 4.– Dans un contexte où l'on souhaite avoir une sécurité à long terme, quelle serait la taille de la signature de cercle ?

Une méthode pour falsifier une signature de $\boldsymbol{m}$ consiste à créer deux tableaux de valeurs de la forme $v_A := u_A^{e_A} \mod n_A$ et $v_B := u_B^{e_B} \mod n_B$ (où les u_A et u_B sont tirées aléatoirement), et de chercher une « collision » entre les tableaux de la forme $v_A \oplus H(\boldsymbol{m}) = v_B$. Un fois cette collision trouvée, on soumet la signature (u_A, v_A) associéau message $\boldsymbol{m}$

Question 5.– Supposons ici que $t = 256$.

1. Préciser si cette attaque induit une falsification existentielle ou universelle. Justifier clairement.
2. Quelle est la taille approximative des tableaux nécessaires pour avoir une falsification avec probabilité proche de 0.5 ?

Question 6.– Généraliser le schéma de signature de cercle à K utilisateurs au lieu de 2 (Alice et Bob). On présentera l'algorithme de signature de l'un de ces K utilisateurs, ainsi que l'algorithme de vérification à effectuer.