Sécurité prouvable
TD Schéma de signatures

Exercice I

Une façon d'authentifier un message (ou une personne) est d'utiliser un schéma d'authentification de message (Message Authentication). Une autre façon est d'utiliser un schéma de signatures.

1. Comment un schéma de signatures fonctionne-t-il ?
2. Reprenez la syntaxe des schémas de MAC. Pouvez-vous définir la syntaxe d'un schéma de signatures ?
3. Quelle est la fonctionnalité (correctness) d'un schéma de signatures ?
4. Reprenez la notion de EUF-CMA pour les schémas de MA.
    a. Pouvez-vous définir une version du jeu EUF-CMA pour les signatures ?
    b. Pouvez-vous définir ce qui veut dire qu'un schéma est EUF-CMA secure ?

Exercice II

On peut définir un schéma de signatures basée sur une version standard de RSA, pour laquelle on a une clé publique d et une clé publique e tel que $d \cdot e = 1\ (mod\ \Phi(N))$, pour un produit de grands nombres premiers $N = p \cdot q$.

1. Quelle pourrait être une signature d'un message m ?
2. Pouvez-vous instancier la syntaxe de l'exercice I par votre schéma ?
3. Est-ce que ce schéma est sécurisé ?
    a. Rappelez comment marche le chiffrement RSA (oui, c'est important)
    b. Trouvez une attaque qui consiste à trouver un tuple (m, s) tel que s vérifie comme signature pour m
    c. Un attaquant est en possession de deux signatures, une pour un message m_1 et l'autre pour un message m_2. Montrez comment il peut trouver une signature pour un troisième message.
    d. Pouvez-vous formaliser cette attaque ? (la décrire en utilisant le jeu EUF-CMA)

Exercice III

Un moyen assez efficace de rendre une signature RSA sécurisée c'est de rajouter une étape de hachage intermédiaire. Soit une fonction de hachage $H: \{0,1\}^* \to \{0,1\}^{|N|}$ pour un modulus RSA $N = p \cdot q$. Le protocole marche comme dans l'exercice II, sauf que, au lieu de signer un message m, on signe $H(m)$. Dans cet exercice nous allons montrer que cette construction – qui s'appelle aussi RSA-FDH (RSA-Full Domain Hash) – est sécurisée dans le modèle de l'oracle aléatoire, à condition que le problème RSA soit difficile.

1. Informellement, dans le problème RSA, on choisit deux nombres premiers « safe » p et q, on calcule $N = p \cdot q$ et $\Phi(N) \coloneqq (p-1) \cdot (q-1)$ et on choisit e et d tel que $e \cdot d = 1 \; mod \; \Phi(N)$. Étant donné ensuite N, y et e, pour un y aléatoire, il faut qu'il soit difficile qu'on retrouve $y^d \; mod \; N$.
   Transformez ce problème dans un jeu de sécurité.

2. Instanciez la syntaxe du schéma de signatures, tel que vous l'avez décrit pour l'exercice I, avec le schéma RSA-FDH.

3. Nous sommes dans le modèle de l'oracle aléatoire. Quelles conséquences cela peut avoir sur le jeu de sécurité EUF-CMA que vous avez décrit pour l'exercice I ?

4. Maintenant, la preuve … en quelques étapes.

   a. La phrase « le schéma RSA-FDH est sécurisé dans le modèle de l'oracle aléatoire à condition que le problème RSA soit difficile » veut dire quoi, en termes de réductions ?

   b. Essayez premièrement, avec un raisonnement informel, de voir comment une telle preuve pourrait marcher (indice : pensez à ce qu'il faut trouver pour la réduction)

   c. Essayez de décrire, plus formellement la réduction : quelles requêtes on fait, comment on simule l'environnement de notre adversaire, etc.

   d. Finalisez la preuve (c'est-à-dire, argumentez la dépendance entre la probabilité de gagner de l'adversaire et de la réduction et tirez des conclusions sur la fin de la preuve).