Crypto Symétrique
TD L'authentification de messages

Contexte

Pendant ce TD, nous allons explorer la notion de EUF-CMA, vue en cours.

Pour certains exercices, ceci veut dire trouver une attaque qu'on peut décrire en détail en utilisant la syntaxe du jeu (quelles requêtes faut-il faire à l'oracle oTag et quelle est la sortie finale (m,t) qui gagne le jeu ?). Pour les autres exercices, l'idée serait de finalement pouvoir donner une preuve de sécurité pour la construction envisagée, en utilisant la technique de game-hopping.

Exercice I

Soit une famille de fonctions de hachage $H: K \times \{0,1\}^* \to \{0,1\}^{512}$ et soit $x \in K$ tel que H_x est un représentant de cette famille, pour une clé x connue.

Un algorithme de MAC est défini tel que, pour une clé $k_{\mathrm{MAC}} \leftarrow \mathrm{KGen}(1^\lambda)$, l'algorithme MAC est défini par : $\mathrm{MAC}(k_{MAC}; m) = H_x(k_{MAC} \mid m)$.

Pouvez-vous trouver une attaque EUF-CMA contre ce schéma, même si on remplace H par un RO ?

Exercice II

Maintenant nous allons changer de schéma. On prend la même fonction de hachage que la dernière fois, mais cette fois-ci $MAC(k_{MAC}; m) = H_x(k_{MAC}) \oplus H_x(k_{MAC} \oplus m)$. Ce schéma, est-il mieux sécurisé si on suppose que H se comporte comme un oracle aléatoire ?

Exercice III

Reprenons le jeu d'indistinguabilité entre l'utilisation d'une fonction de hachage et un oracle aléatoire vu en CM.

1. Qu'est-ce qui se passe si $|X| = 1$? Et si $|X| = 2$? Et si la taille de X est polynomiale (en tant que fonction de la taille du paramètre de sécurité) ?
2. Quelle doit être la taille de l'ensemble de sortie d'un vrai oracle aléatoire ?
3. Nous avons un attaquant qui peut trouver des collisions dans un fonction de hachage (le jeu pour $s = 2$) avec une probabilité de 10%. Pouvez-vous montrer comment on peut utiliser cet attaquant pour obtenir un adversaire qui peut distinguer entre la fonction de hachage et le RO avec un avantage non-négligeable ?

Exercice IV

Pour un message m de taille n bits, nous allons noter par $m_{\left[0\ldots\left\lfloor\frac{n}{2}\right\rfloor\right]}$ la moitié la plus significative de m et par $m_{\left[n-\left\lfloor\frac{n}{2}\right\rfloor\ldots n\right]}$, la moitié la moins significative de m. Pour une fonction de hachage H tel que définie dans les exercices précédents, nous allons définir un algorithme de MAC par :

$$MAC(k_{MAC}; m) = H_x\left(H_x\left(k_{MAC} \mid m_{\left[0\ldots\left\lfloor\frac{n}{2}\right\rfloor\right]}\right) \oplus H_x\left(k_{MAC} \mid m_{\left[n-\left\lfloor\frac{n}{2}\right\rfloor\ldots n\right]}\right)\right)$$

1. Pouvez-vous trouver une attaque contre ce schéma d'authentification de messages, même si H est un oracle aléatoire ?
2. Nous allons remplacer le XOR de la relation ci-dessus par une concaténation.
    a. Ce schéma, est-elle sécurisée ?
    b. Pouvez vous prouver la sécurité du nouveau schéma, ou, au contraire, trouver une attaque qui s'encadre dans le jeu EUF-CMA ?