HAI709I - TD 11

Rocco Mora

8 Décembre, 2025

Exercice 1 :

Montrez comment un attaquant peut falsifier une signature pour le schéma de signature RSA sur un message arbitraire à l'aide d'une seule requête de signature à l'oracle (**hint:** pensez à la malleabilité).

Exercice 2 :

Considérez une variante de la transformation Fiat-Shamir dans laquelle la signature est (I, s) au lieu de (r, s) et la vérification est modifiée de manière naturelle. Montrez que si le schéma d'identification sous-jacent est sûr, alors le schéma de signature qui en résulte est également sûr.

Exercice 3 :

Considérons une variante de DSA dans laquelle l'espace de message est Z_q et H est omis, c'est-à-dire que le deuxième composant de la signature est désormais $s := k^{-1} \cdot (m + xr) \mod q$. Montrez que cette variante n'est pas sûre.

Exercice 4 :

Écrivez formellement le schéma de signature de Schnorr et vérifiez la propriété de correction.

Considérons ensuite l'exemple où le groupe est $\mathbb{Z}_{23}^*$, le générateur est $g = 2$ (trouvez l'ordre du sous-groupe) et la clé secrète $x = 4$. Déterminez la clé publique y. Calculez le message initial I en utilisant la valeur $k = 6$. Étant donné le message $m = 19$, produisez le défi r à partir de la fonction simplifiée $H(I, m) = I + m \mod q$. Calculez s et vérifiez la correction.

Exercice 5 :

Écrivez formellement le protocole d'identification dont sont dérivés DSA/ECDSA et vérifiez la propriété de correction.