

Introduction à la cryptologie
TD n° 12 : Chaîne de blocs.

Exercice 1 (Ring signature). Dans une signature de cercle, le signataire peut choisir un ensemble quelconque de clefs publiques incluant sa propre clef publique, et signer son message sans révéler quelle clef publique parmi cet ensemble a été utilisée. Essayons de construire une signature de ce type.

On part d'un schéma de signature à clef publique, mettons RSA. Notons sa fonction de chiffrement $E_{pk}(m)$ pour la clef publique pk , et sa fonction de déchiffrement $D_{sk}(c)$. Dans le schéma de signature de cercle que nous construisons, une signature pour un « cercle » de clefs publiques (pk_1, \dots, pk_n) est une solution d'une certaine équation qui dépend du haché du message $H(m)$ et des clefs publiques :

$$\text{Eq}(H(m), E_{pk_1}(x_1), \dots, E_{pk_n}(x_n)).$$

La signature de m est $(pk_1, \dots, pk_n, x_1, \dots, x_n)$. Vérifier une signature, c'est vérifier Eq.

1. Essayons :

$$\text{Eq}(h, y_1, \dots, y_n) : y_1 \oplus \dots \oplus y_n = h.$$

- (a) Comment le signataire peut-il calculer une signature ?
- (b) Décrire une attaque contre ce schéma, qui permet à un adversaire de calculer efficacement la signature d'un message quelconque pour un ensemble quelconque (suffisamment grand) de clefs publiques, en résolvant un système linéaire. Le schéma de signature est-il résistant aux forges existentielles avec messages choisis ?

2. On suppose qu'on utilise RSA avec un exposant public $e = 3$, c'est-à-dire que la fonction de chiffrement est $m \mapsto m^3 \pmod N$ (attention, ceci n'est pas un vrai chiffrement à clef publique, mais ce n'est pas grave pour notre utilisation). On suppose que tous les modules RSA ont le même nombre de bits b . Deuxième tentative :

$$\text{Eq}(h, y_1, \dots, y_n) : y_1 + \dots + y_n = h \quad \text{dans } \mathbb{Z}_{2^b}.$$

Décrire une attaque contre ce schéma, du même type que dans la question précédente.

Indication non-triviale : tout nombre entier $x \in \mathbb{N}$ peut se décomposer efficacement en une somme $\sum x_i^3$ de 9 cubes avec $x_i \in \mathbb{N}$.

3. Soit S_k la fonction de chiffrement d'un chiffrement symétrique pour la clef k . On suppose que tous les y_i vivent dans le même espace, qui est aussi l'entrée/sortie de S . Dernière tentative :

$$\text{Eq}(h, y_1, \dots, y_n) : S_h(y_1 \oplus S_h(y_2 \oplus \dots S_h(y_n))) = 0.$$

- (a) Expliquer comment un signataire légitime (donc connaissant la clef privée d'un des pk_i du cercle) peut signer un message.
- (b) Montrer que pour $s \leq n$ et $h, y_1, \dots, y_{s-1}, y_{s+1}, \dots, y_n$ fixés quelconques, la solution y_s à l'équation $\text{Eq}(h, y_1, \dots, y_n)$ est unique.
- (c) Montrer que la distribution de probabilité générée en tirant $y_1, \dots, y_{s-1}, y_{s+1}, \dots, y_n$ de manière indépendante et uniforme, et en calculant le y_s approprié, ne dépend pas de s .
- (d) En déduire une manière de signer qui garantit que la signature ne révèle *rien* sur quel membre du cercle a signé.
- (e) Comment la taille d'une signature croît-elle avec le nombre n de personnes dans le cercle ?

Exercice 4 (Wifi Protected Setup, ou comment ne pas utiliser des commitments, exercice de détente). En 2006, la Wifi Alliance, qui gouverne les normes Wifi, a créé le Wifi Protected Setup (WPS), qui permet entre autres à un ordinateur de s'authentifier auprès d'une box wifi à l'aide d'un code PIN de 8 chiffres. Les 8 chiffres c_1, \dots, c_8 vérifient $c_1 + 3c_2 + c_3 + 3c_4 + c_5 + 3c_6 + c_7 + 3c_8 = 0 \pmod{10}$. Le code est à vie pour l'appareil et ne peut pas être changé.

Le protocole utilisé est le suivant. Soit A l'ordinateur d'Alice et B la box internet en wifi. On utilise un schéma de commitment C comme décrit dans l'exercice précédent. *S'engager* sur une valeur $m \in \mathcal{X}$ signifie tirer $a \in \mathcal{A}$ uniformément, et publier $e = C(m, a)$. *Dévoiler* l'engagement signifie publier a . *Vérifier* l'engagement est simplement vérifier $e = C(m, a)$ une fois a dévoilé. Le code PIN est composé de deux moitiés de 4 chiffres $m_1 \parallel m_2$ (où \parallel dénote la concaténation). A et B commencent par faire un échange de clef Diffie-Hellman pour chiffrer les communications avec un secret commun, puis continuent comme suit.

- a) La box s'engage sur m_1 et sur m_2 .
- b) Alice publie m_1 et s'engage sur m_2 .
- c) La box vérifie l'engagement d'Alice sur m_1 , et dévoile son engagement sur m_1 .
- d) Alice vérifie l'engagement de la box sur m_1 , et dévoile le sien sur m_2 .
- e) La box vérifie l'engagement d'Alice sur m_2 , et dévoile le sien sur m_2 .
- f) Alice vérifie l'engagement de la box sur m_2 .

Si une étape de vérification échoue, le protocole est arrêté.

1. Si un adversaire se fait passer pour la box auprès d'Alice, combien d'essais sont nécessaires pour apprendre le code PIN ?
2. Même question si l'adversaire se fait passer pour Alice auprès de la box.