École normale supérieure **2019-2020**
Département d'informatique

Introduction à la cryptologie
TD n° 11 : real protocols.

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 $(pk_1, \ldots, pk_n)$ est une solution d'une certaine équation qui dépend du haché du message $H(m)$ et des clefs publiques :

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

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

1. Essayons :
$$\mathsf{Eq}(h, y_1, \ldots, y_n) : y_1 \oplus \cdots \oplus y_n = h.$$
   (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 $m \mapsto m^3 \bmod N$ (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 :
$$\mathsf{Eq}(h, y_1, \ldots, y_n) : y_1 + \cdots + y_n = h \quad \text{dans } \mathbb{Z}_{2^b}.$$
   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 symmétrique 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 :
$$\mathsf{Eq}(h, y_1, \ldots, y_n) : S_h(y_1 \oplus S_h(y_2 \oplus \ldots S_h(y_n))) = 0.$$
   (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 $h, y_1, \ldots, y_{s-1}, y_{s+1}, \ldots, y_n$ fixés quelconques, la solution y_s à l'équation $\mathsf{Eq}(h, y_1, \ldots, y_n)$ est unique.
   (c) Montrer que la distribution de probabilité générée en tirant $y_1, \ldots, y_{s-1}, y_{s+1}, \ldots, y_n$ 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 2 (More Ring Signatures.)**.** Dans les TDs auparavant, nous avons apris des techniques pour créer des signature basées sur des preuves zero-knowledge. Nous revisitons ces techniques pour créer des signature de cercle.

1. Rappeler le protocol du TD 10, exercise 1. Soit $\mathsf{pk}_1, \ldots, \mathsf{pk}_n$ un cercle des clés publiques du protocol, ou le clé secret sk_s pour pk_s est connu. Alors, $\mathsf{pk}_i = \mathsf{H}(\vec{x}_i)$, et $\mathsf{sk}_s = \vec{x}_i$.
   Adapter le circuit (i.e., la fonction calculé par le protocol MPC) pour créer une signature de cercle.
2. Même question, mais la signature pour un cercle de taille n a une taille $\mathcal{O}(\log n)$.
   Hint : Un arbre Merkle sera utile.
3. Rappeler le protocol du TD 3, exercise 3. Les clées publiques sont $\mathsf{pk}_i = g^{x_i}$ et le clé secret x_s de pk_s est connu. Créer une signature de cercle à la base des signatures Schnorr en utilisant la technique de partage de secret.

Exercice 3 (Authentification avec LPN)**.** On introduit la notation pour cette exercise. $x \leftarrow_\$ S$ signifie que x est tiré uniformément dans l'ensemble S. $\mathsf{Ham}(\cdot)$ désigne le poids de Hamming (nombre de coordonnées non nulles). Soit $\eta \in]0, 1/2[$, et soit $B(\eta)$ la distribution sur $\mathbb{Z}_2$ caractérisée par $\Pr[x = 1 : x \leftarrow B(\eta)] = \eta$. Pour $s \in \mathbb{Z}_2^n$, on définit la distribution $\mathsf{LPN}_s(m, n, \eta)$ comme $(A, As + e)$ où $A \leftarrow_\$ \mathbb{Z}_2^{m \times n}$, $e \leftarrow B(\eta)^m$. Soit $\mathsf{U}(m, n)$ la distribution uniforme (A, b) où $A \leftarrow_\$ \mathbb{Z}_2^{m \times n}$, $b \leftarrow_\$ \mathbb{Z}_2^m$. L'hypothèse LPN décisionnelle stipule que pour $s \leftarrow_\$ \mathbb{Z}_2^n$, aucun algorithme efficace ne peut distinguer des échantillons $\mathsf{LPN}_s(m, n, \eta)$ d'échantillons $\mathsf{U}(m, n)$.

La société ACME conçoit un système d'authentification comportant une carte et un capteur sans contact reconnaissant la carte. Ce système peut être ciblé par différents types d'adversaires. Un adversaire *passif* enregistre discrètement les communications entre la carte et le capteur lors de son utilisation légitime. Cet adversaire peut observer autant d'utilisations de la carte qu'il le souhaite. Un adversaire *actif* a de plus volé la carte et peut interagir avec elle arbitrairement. Un adversaire *au milieu* a volé la carte et le capteur et peut interagir librement avec le deux, y compris en relayant des messages (éventuellement modifiés) de l'un à l'autre. Dans tous les cas, le but de l'attaquant est de retrouver la clef secrète interne à la carte.

Comme la carte ne peut effectuer que des calculs très simples, les ingénieurs ACME s'intéressent à LPN. On suppose que la carte et le capteur connaissent tous deux une clef secrète LPN s, que la carte utilise pour s'authentifier. Les ingénieurs d'ACME considèrent d'abord le protocole suivant.

(a) Le capteur envoie à la carte $A \leftarrow_\$ \mathbb{Z}_2^{m \times n}$.
(b) La carte tire $e \leftarrow B(\eta)^m$ et renvoie $b = As + e$.
(c) Le capteur accepte (LED verte s'allume) ssi $\mathsf{Ham}(b - As) \leq \eta' m$ pour un certain $\eta' > \eta$.

1. Montrer que ce protocole est sûr contre un adversaire passif.
2. Décrire une attaque contre le système par un adversaire actif.
3. Proposer une légère modification du protocole permettant d'assurer la sécurité contre un adversaire actif, en utilisant une fonction de hachage (modélisée comme une fonction uniformément aléatoire). Montrer que le protocol est sûr.

Comme la carte est très limitée en calculs, les ingénieurs d'ACME souhaitent éviter l'utilisation d'une fonction de hachage. Ils proposent le protocole suivant. Cette fois, le secret partagé est un couple (s_1, s_2) avec $s_i \in \mathbb{Z}_2^n$.

(a) La carte envoie au capteur $A_1 \leftarrow_\$ \mathbb{Z}_2^{m \times n}$.
(b) Le capteur répond avec $A_2 \leftarrow_\$ \mathbb{Z}_2^{m \times n}$.
(c) La carte tire $e \leftarrow B(\eta)^m$ et renvoie $b = A_1 s_1 + A_2 s_2 + e$.
(d) Le capteur accepte ssi $\mathsf{Ham}(b - A_1 s_1 - A_2 s_2) \leq \eta' m$ pour un certain $\eta' > \eta$.

4. Montrer que ce protocole est sûr contre un adversaire actif.
5. Décrire une attaque par un adversaire au milieu.

6. Si l'on ne se préoccupe pas des limites de la carte et qu'on s'autorise tous les outils cryptographiques que l'on souhaite, proposer un protocole d'authentification qui résiste à un adversaire au milieu (pas de justification demandée). Dans ce contexte plus général, le but de l'adversaire est de « dupliquer » la carte, c'est-à-dire créer une nouvelle carte qui passe aussi le test d'authentification.