Split VR
Flow

M2 - Mécanismes Cryptographiques

7 février 2013 - 2h - deux feuilles manuscrites autorisées

Questions de cours:

a. Qu'est-ce qu'un certificat, rappeller son utilisation.

b. Qu'est-ce qu'une chaine de certificats ? Dans quel cas l'utilise-t-on ?

c. Qu'est-ce qu'un tiers de confiance, donner des exemples de telles entités.

d. Est-ce que le chiffrement permet de faire: de la signature ? de l'échange de clés ? de l'authentification ? Si oui comment ?

e. Que permettent de faire les schémas de Retrait d'Information Privé (RIP en français ou PIR en anglais). Expliquer le principe general. Donner des exemples d'utilisation concrète de ce type de protocole.

f. Qu'est-ce qu'un chiffrement homomorphe ? Donner un exemple d'un tel protocole, et donner un exemple d'application.

Exercice 1 (Authentification):

On considère le protocole de Schnorr. Soit p et q deux entiers (grands) tels que q divise $p-1$, et soit g un entier d'ordre q modulo p. Le secret détenu par Alice est un entier $a \in [0, q-1]$ et la donnée de $A = g^{-a} \ mod \ p$ est rendue publique. Le protocole est alors le suivant: (1) Alice fournit un engagement aléatoire k dans l'intervalle $[0, q-1]$ et calcule $K = g^k \ mod \ p$. Elle transmet K à Bob. (2) Bob choisit un défi r au hasard dans $[0, q-1]$ et le transmet à Alice. (3) Alice calcule la réponse $y = (k + ar) \ mod \ q$ et la transmet à Bob. Bob vérifie que $g^y A^r = K \ mod \ p$.

a. Faire un schéma de ce protocole

b. Montrer que le protocole est juste

c. Montrer que la probabilité de tricher pour s'authentifier est au maximum $1/q$

d. Quel est l'intérêt de ce protocole par rapport au protocole de Fiat-Shamir (en terme de nombre de passes).

e. Ce protocole vérifie-t-il la propriété de zero-knowledge ? (i.e. un pirate qui suit les messages échangés ne peut rien déduire sur clé secrète).

f. Montrer que pour un schéma de type Fiat-Shamir ou on fixerait les engagements à l'avance, on peut le transformer en algorithme de signature (paradigme de Fiat-Shamir).

Exercice 2 (Signatures)

Signature aveugle On rappelle qu'un schéma de signature aveugle est un schéma où un Blinder B peut obtenir d'un signataire S, une signature d'un message sans que S sache ce qu'il a signé.

a. Donner un exemple d'application dans lequel une telle propriété pour la signature a vraiment un sens.

On considère une bi-clé de type RSA,clé publique (n, e), clé privée: (d, p, q) avec les notations habituelles.

Examen : deux feuilles Recto/Verso autorisées

b. Soit m un message que l'on souhaite faire signer, sans que le signataire connaisse le contenu. Montrer qu'on peut facilement adapter le schéma de signature RSA pour obtenir cette propriété (*indice: il faut multiplier m par quelque chose*)

c. Pourquoi un tel schéma est-il sur et ne laisse-t-il pas passer d'information.

d. La signature aveugle est un type de protocole utilisé pour garantir des propriétés de type anonymat, connaissez-vous d'autres types de protocoles aussi utilisable dans un contexte d'anonymat ?

Délégation de signature On suppose qu'Alice et Bob ont chacun une clé privée et un clé publique permettant de faire de la signature. Alice souhaite faire une délégation de signature à Bob pendant ses vacances, c'est à dire que Bob doit pouvoir signer au nom d'Alice pendant une période de temps fixée, et ce bien sur sans qu'Alice soit obligée de donner sa clé privée. Comment peut-on faire cela ?

Exercice 3 (Partage de secret) :

Coca-cola On rappelle qu'un schéma de partage de secret permet à plusieurs personnes qui ont en commun un (ou des) bout de secret de retrouver un secret donné.

a. Quel est la différence entre le partage de secret et l'échange de clé ? Donner un exemple d'application du partage de secret.

b. Rappeler le schéma de partage de secret de Shamir. On se place dans un cas ou le secret est la valeur du polynome en 0.

c. On suppose que la formule de Coca Cola a été partagée entre trois personnes. De telle sorte que 2 personnes parmi les 3 puissent la retrouver. On se place dans $Z/43Z$ et on recupere les parts données à chacune des trois personnes (une part est constituée de x et de P(x), le secret est la valeur de P en 0).

Part 1: (2,8), Part 2: (5,12), Part 3: (10,23).

Quel est le degré du polynome recherché. Quel est le secret partagé X (la formule de Coca Cola), on écrira le secret sous la forme d'un entier compris entre 1 et 43.

La bombe

(a) On suppose maintenant qu'on veut mettre en place en place un système qui permet à certains type de combinaisons de militaires de retrouver le secret du code nucléaire. On veut que les combinaisons suivantes puissent retrouver le secret: 3 généraux, 4 colonels + 1 général, 3 colonels + 5 capitaines ou encore 20 capitaines. Comment faire ?

(b) Le problème de la solution précédente est qu'il est possible qu'un groupe formé uniquement de capitaines puisse retrouver le secret, ce qui pose problème. On souhaite donc mettre en place un système où pour retrouver le secret il faille **au moins**: 1 général, 2 colonels et 4 capitaines qui collaborent. Cela signifie donc qu'un groupe formé simplement de capitaines ou de colonels (par exemple) **ne pourra pas** retrouver le secret. Comment faire ? (toujours en utilisant un schéma basé sur le schéma de Shamir ou une variation).

Exercice 4 (Courbes elliptiques)

a. Quel est l'intérêt des courbes elliptiques en cryptographie ? Rappeler par un schéma le fonctionnement de l'addition et du doublement pour le groupe des points de la courbe.
On consière la courbe définie sur le corps à 5 éléments $K = Z/5Z$ par $y^2 = x^3 + x + 3$.
b. Combien y a-t-il de points sur la courbe et quels sont-ils ?
c. Pour tous les points P différents du point à l'infini, calculer 2P et 4P.
d. Donner un générateur du groupe (un point P, tel que 0P,P,2P,etc.. engendre le groupe). En déduire la structure du groupe de la courbe.

N.B. On rappelle que dans ce cas, si la courbe a pour équation $y^2 = x^3+ax+b$, le doublement de $P(x_1, x_2)$ est $2P(x_3, y_3)$ avec:

$x_3 = \left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1$ et $y_3 = \left(\frac{3x_1^2+a}{2y_1}\right)(x_1 - x_3) - y_1$.