Master CSI 2 2013-2014

Crypto avancée : feuille de TD 7

– Exercice 1. Monnaie numérique 1. Système de Chaum.

Le protocole suivant est destiné à permettre à un utilisateur U d'acquérir une unité de monnaie numérique auprès d'une banque B. La banque possède une clé publique RSA (n, e). On utilisera une fonction de hachage publique H. On procède ainsi :
– l'utilisateur U choisit deux entiers aléatoires r et x et se manifeste auprès de la banque et lui communique $y = r^e H(x) \bmod n$.
– La banque déchiffre Y et donne le résultat $Y^d \bmod n$ à l'utilisateur.
– l'utilisateur calcule $X = Y^d r^{-1} \bmod n$.

a) Vérifier que le couple (X, x) satisfait une équation aisément vérifiable, et qu'il est difficile d'obtenir un tel couple sans l'aide de la banque. C'est une unité de monnaie numérique.

b) L'anonymat de l'utilisateur est-il garanti ?

c) Une telle unité de monnaie est-elle copiable ? Réutilisable ?

d) Pour assurer l'utilisation *off-line* du moyen de paiement, on souhaite que deux utilisations de la monnaie auprès d'un marchand révèle l'identité de l'utilisateur. Comment peut-on réaliser un tel procédé
– en supposant l'utilisateur honnête,
– avec une probabilité de démasquer la double utilisation égale à 1/2.

e) Comment rendre le procédé résistant à un utilisateur malhonnête ?

f) Comment rendre la probabilité de démasquer une double utilisation arbitrairement proche de 1 ?

– Exercice 2. Monnaie numérique 2. Système de Brands.

Tous les calculs se font dans $\mathbb{Z}/p\mathbb{Z}$. On fixe g, g_1, g_2 trois générateurs d'un sous-groupe multiplicatif d'ordre q de $\mathbb{Z}/p\mathbb{Z}$. On utilisera deux fonctions de hachage H et H_1 publiques.

La banque a un secret x modulo q, et sa clé publique associée est le triplet

$$(h, h_1, h_2) = (g^x, g_1^x, g_2^x).$$

L'utilisateur U a un secret $u \bmod q$ et une identité publique $I = g_1^u$. La banque, au cours de l'enregistrement de U, lui donne la quantité $z' = (Ig_2)^x$.

Création de la monnaie. La banque choisit un entier aléatoire w, calcule

$$g_w = g^w \quad \beta = (Ig_2)^w$$

et les communique à U. L'utilisateur choisit le quintuplet secret :

$$(s, x_1, x_2, \alpha_1, \alpha_2)$$

puis il calcule

$$A = (Ig_2)^s, \;\; B = g_1^{x_1} g_2^{x_2}, \;\; z = z'^s, \;\; a = g_w^{\alpha_1} g^{\alpha_2}, \;\; b = \beta^{s\alpha_1} A^{\alpha_2}.$$

L'utilisateur calcule ensuite

$$c = \alpha_1^{-1} H(A, B, z, a, b) \bmod q$$

et le donne à la banque. La banque calcule $c_1 = cx + w \bmod q$ et le donne à U. Enfin, U calcule

$$r = \alpha_1 c_1 + \alpha_2 \bmod q.$$

L'unité de monnaie est le 6-uple :

$$(A, B, z, a, b, r).$$

Paiment auprès du marchand.

a) le commerçant (vendeur) qui réceptionne la monnaie vérifie :

$$g^r = ah^{H(A,B,z,a,b)} \;\text{ et }\; A^r = z^{H(A,B,z,a,b)} b.$$

De quoi est-il convaincu ?

b) Le commerçant est identifié auprès de la banque par un entier M. Il calcule

$$d = H_0(A, B, M, t)$$

où t est la date et l'heure de la transaction. Le nombre d est communiqué à l'utilisateur U qui calcule et donne au marchand

$$r_1 = dus + x_1, \quad r_2 = ds + x_2.$$

Le commerçant vérifie

$$g_1^{r_1} g_2^{r_2} = A^d B.$$

La banque reçoit la monnaie (A, B, z, a, b, r) et le triplet (r_1, r_2, d) et vérifie que le sextuple n'a pas été utilisé. Montrer que si la monnaie est utilisée deux fois avec deux triplets (r_1, r_2, d) et (r'_1, r'_2, d') alors l'identité de l'utilisateur est exposée.

c) A quoi sert la fonction H_0 ?