Master CSI 2 2013-2014

Crypto avancée : feuille de TD 4

– Exercice 1. Soient donnés p un grand nombre premier, q un diviseur de $p-1$, et g un élément d'ordre q dans $(\mathbb{Z}/p\mathbb{Z})^*$. Soit $P = g^s \bmod p$ une quantité publique. On considère le protocole suivant, destiné à démontrer la connaissance de s.

- Le prouveur P choisit un entier aléatoire r modulo q, puis calcule $x_1 = g^r \bmod p$ et $x_2 = g^{s-r} \bmod p$. Il communique x_1 et x_2 au vérificateur V.
- V choisit au hasard $i = 1$ ou $i = 2$ et demande à P un entier y_i tel que $g^{y_i} = x_i \bmod p$.
- P s'exécute.
- V vérifie que $x_1 x_2 = P$ et que $g^{y_i} = x_i \bmod p$.

Expliquer pour quoi ce protocole démontre la connaissance de s par P, et montrer qu'il est sans divulgation.

– Exercice 2. Soit L le langage constitué des quadruplets (n, p, x, y) tels que $2^n = 1 \bmod p$ et tels qu'il existe s vérifiant simultanément

$$\begin{aligned} s^2 &= x \bmod n \\ 2^s &= y \bmod p \end{aligned}$$

On considère le protocole suivant destiné à prouver l'appartenance à L.

- P communique à V deux entiers a, b modulo n,
- V communique à P un bit aléatoire ε,
- P communique à V un entier z.
- V vérifie que :
  - si $\epsilon = 0$, alors $z^2 = a \bmod n$ et $y^z = b \bmod p$,
  - si $\epsilon = 1$, alors $z^2 = ax \bmod n$ et $2^z = b \bmod p$.

Montrer que ce protocole est complet, valide, et sans divulgation.

– Exercice 3. On souhaite réaliser un protocole sans divulgation de ce que l'entier y n'est *pas* un carré modulo l'entier n.

a) On considère un premier protocole :
- Le vérificateur V choisit un entier modulo n aléatoire r ainsi qu'un bit $\varepsilon \in \{0, 1\}$. Il calcule $x = r^2 y^\varepsilon$ et le communique au prouveur P.

- Le prouveur révèle un bit $b \in \{0,1\}$. Si $b = \varepsilon$ le vérificateur accepte, sinon il rejette.

Montrer que ce protocole est bien complet et valide, mais qu'il n'est pas sans divulgation.

b) Soit f une fonction à sens unique sur les entiers modulo n, par exemple $f : z \mapsto g^z \bmod n$ pour un certain g. On fait l'hypothèse cryptographique que la donnée de $f(z)$ ne révèle aucun bit d'information sur z à un vérificateur ne disposant que d'une capacité de calcul en temps polynomial (sauf peut-être sur une infime proportion d'entiers z). On considère maintenant le protocole suivant :

- Le vérificateur V choisit un entier modulo n aléatoire r ainsi qu'un bit $\varepsilon \in \{0,1\}$. Il calcule $x = r^2 y^\varepsilon$ et le communique au prouveur P.
- Le prouveur choisit un bit $b \in \{0,1\}$. Puis il choisit aléatoirement un entier $z \in \{0,1,\ldots,n-1\}$ où z est pair si $b = 0$ et impair si $b = 1$. Il calcule $e = f(z)$ et le donne à V.
- Le vérificateur V révèle à P les quantités r et ε.
- Le prouveur P vérifie que $x = r^2 y^\varepsilon$: si ce n'est pas le cas il arrête le protocole. Si c'est le cas il révèle z à V.
- Le vérificateur calcule $f(z)$ et vérifie que cette quantité est bien égale à e. Il vérifie également que z est pair si $\varepsilon = 0$ et impair si $\varepsilon = 1$. Si l'une de ces vérifications échoue il rejette la réponse, sinon il accepte.

Montrer que ce protocole est complet et valide, et qu'il est sans divulgation au sens calculatoire.