

# TD 8 de Cryptologie

## Protocoles

Lundi 5 décembre 2005

### 1 Fiat-Shamir

On décrit le protocole d'identification *zero-knowledge* de Fiat-Shamir :

1. Le serveur de clef  $T$  publie un module RSA  $n = pq$  et garde  $p$  et  $q$  secrets.
2. Alice choisit un entier secret  $s$  tel que  $1 \leq s \leq n - 1$  et  $s$  est premier avec  $n$ , et publie  $v = s^2 \bmod n$  comme sa clef publique.
3. Pour s'identifier auprès de Bob, Alice choisit un gage  $r$  tel que  $1 \leq r \leq n - 1$  et envoie à Bob le message  $x = r^2 \bmod n$ .
4. Bob choisit un bit de défi au hasard  $e \in \{0, 1\}$  et l'envoie à Alice.
5. Alice renvoie à Bob la réponse  $y = rs^e$ .
6. Bob vérifie que  $y^2 = x \cdot v^e$  et refuse l'authentification sinon.

1. Montrer comment un imposteur peut répondre à l'un des deux défis possibles sans connaître le secret.
2. En déduire la probabilité de réussite d'un imposteur, et proposer une méthode pour renforcer le protocole.
3. Montrer que le protocole est effectivement *zero-knowledge* en discutant l'information que Bob a appris sur la clef d'Alice dans le cas  $e = 0$  et le cas  $e = 1$ .
4. Sur quel problème supposé difficile la sécurité du protocole repose-t-elle ?
5. Que se passe-t-il lorsque Alice choisit par hasard deux fois la même valeur de  $r$  ? Cela pose-t-il un problème en pratique pour les tailles de clefs recommandées ?
6. Rappeler pourquoi savoir calculer des racines carrées modulo  $n$  est équivalent à savoir factoriser  $n$ .

### 2 Partage de secret

Dans la suite on se place dans un corps fini  $\mathbb{F}_p$  (donc  $p$  premier) mais le résultat de l'interpolation de Lagrange reste valide dans un corps quelconque.

Pour  $x_1, x_2, \dots, x_n$ ,  $n$  points distincts de  $\mathbb{F}_p$  fixés l'application  $\varphi : \begin{cases} \mathbb{F}_p[X]_{n-1} & \longrightarrow (\mathbb{F}_p)^n \\ P & \longmapsto (P(x_1), P(x_2), \dots, P(x_n)) \end{cases}$  est un isomorphisme de  $\mathbb{F}_p$ -espaces vectoriels.

7. Montrer que  $\varphi$  est effectivement un isomorphisme, et montrer comment calculer  $\varphi^{-1}$ .
8. Application: calculer  $P(X)$  de degré au plus 3 dans  $\mathbb{F}_{17}$  tel que
  - $P(0) = 3$
  - $P(3) = 6$
  - $P(12) = 13$
  - $P(1) = 7$

Alice souhaite partager un secret de taille environ  $n \cdot \log_2 p$  bits qu'elle découpe en  $n$  morceaux  $a_0, a_1, \dots, a_{n-1}$  tel que  $0 \leq a_i \leq p-1$  pour tout  $i$ . Elle définit  $P(X) = \sum_{i=0}^{n-1} a_i X^i$  et distribue ensuite les  $n$  secrets partagés  $P(x_1), \dots, P(x_n)$ .

9. Montrer que la connaissance des  $n$  secrets partagés  $(P(x_i))_{1 \leq i \leq n}$  permet de retrouver le secret initial.
10. Que se passe-t-il si l'un des  $x_i$  est 0 ?
11. Quelle "quantité d'information" est contenue dans un des secrets partagés, c'est-à-dire, combien de secrets sont encore théoriquement possibles lorsqu'on connaît un seul des secrets partagés ?
12. Même question lorsqu'on connaît de 2 à  $n-1$  des secrets partagés.

Alice décide de changer de stratégie. Son secret  $s$  n'est plus que de taille  $\log_2 p$  bits, elle fixe  $a_0 = s$  et choisit les autres coefficients de  $P$  au hasard. Elle distribue comme avant  $P(x_1), P(x_2), \dots, P(x_n)$ .

13. Reprendre les questions 10 à 12 dans ce cas.
14. Comment adapter le protocole de partage de secret pour en faire un protocole "à seuil", où  $k$  parmi  $n$  secrets partagés suffisent pour retrouver le secret originel ?