Chapitre XI. Quelques protocoles cryptographiques

Le but de ce chapitre est de présenter quelques protocoles non liés au chiffrement ou à la signature.

1) Le partage de secret (secret sharing)

Plutôt que de confier un secret à une seule personne, il est souvent plus prudent de confier à plusieurs personnes des informations qui leur permettent de reconstituer ce secret. Formalisons un peu. Soit $n \geqslant 2$ un entier et soit k un entier vérifiant $2 \leq k \leq n$. Soit s un secret. On confie à la i-ème personne P_i une information s_i (pour tout $1 \leq i \leq n$) de telle sorte que k personnes parmi les n soient en mesure de retrouver s à partir des informations dont elles disposent, mais pas $k-1$ personnes. On parle de <u>schéma à seuil</u>.

■ <u>Exemple 1</u> : $k = n$, $s \in \{0,1\}^\ell$ où $\ell \geqslant 1$. À la i-ème personne P_i on confie $s_i \in \{0,1\}^\ell$ et $s = \bigoplus_{i=1}^{n} s_i$.

Le problème ici est que l'on a besoin des n personnes pour retrouver s. L'une d'entre elles peut décéder et emporter son information s_i dans la tombe. Donnons deux exemples plus généraux.

■ <u>Exemple 2 (Mignotte).</u>

Soient n entiers m_i vérifiant $0 < m_1 < m_2 \cdots < m_n$ et tels que $M = m_1 m_2 \cdots m_k > m_n m_{n-1} \cdots m_{n-k+2} = N$ (le produit des k premiers est strictement supérieur au produit des $k-1$ derniers).

Supposons en outre que les m_i sont premiers entre eux deux à deux. Le secret est un entier s vérifiant $N \leqslant s < M$.

À la i-ème personne P_i on confie $s_i := (s \bmod m_i, m_i)$.

- Prenons k personnes, les P_i où $i \in I$ et $|I| = k$.

Elles peuvent calculer $s \bmod \prod_{i \in I} m_i$ à l'aide du théorème chinois. où $\prod_{i \in I} m_i \geq m_1 \dots m_k = M$.

Or $s < M$. Elles connaissent donc s.

- Prenons $k-1$ personnes, les P_i où $i \in J$ et $|J| = k-1$

Elles peuvent calculer $s \bmod \prod_{i \in J} m_i = s'$ à l'aide du théorème chinois mais cette fois, $\prod_{i \in J} m_i \leq N < M$. et les $k-1$ personnes ont plusieurs candidats pour s à savoir :

$s' + l \prod_{i \in J} m_i$, $s' + (l+1) \prod_{i \in J} m_i$, $\dots$, $s' + k \prod_{i \in J} m_i$ où l et k sont définis par $l = \min \{ j \,/\, s' + j \prod_{i \in J} m_i \geq N \}$ et $k = \max \{ j \,/\, s' + j \prod_{i \in J} m_i < M \}$. On voit que le nombre de candidats est $> \frac{M-N}{N} - 1$, qui peut être très grand si les m_i sont bien choisis.

■ Exemple 3 (Shamir)

Soit p un premier $> n$. Le secret $s \in \mathbb{F}_p$. et p est public.

On tire au hasard un polynôme $Q(X) = s + a_1 X + \dots + a_{k-1} X^{k-1} \in \mathbb{F}_p[X]$ de degré strictement inférieur à k et de terme constant s.

À la i-ème personne P_i on confie $s_i = (Q(\ell_i), \ell_i)$ où les ℓ_i sont n éléments deux à deux distincts de $\mathbb{F}_p^\times$. (on évite 0 sinon une des personnes détient s, même si elle l'ignore).

- Prenons k personnes, les P_i où $i \in I$ et $|I| = k$.

Elles peuvent procéder de différentes façons pour retrouver s.

Par exemple pour tous les $i \in I$, elles peuvent déterminer les polynômes d'interpolation $Q_i(X) = \prod_{\substack{j \in I \\ j \neq i}} \frac{X - \ell_j}{\ell_i - \ell_j}$ qui sont de degré $k-1$ et vérifient $Q_i(\ell_i) = 1$ et $Q_j(\ell_j) = 0$ pour $j \neq i$.

Alors $P(X) = \sum_{i \in I} Q(l_i)\, Q_i(X)$ est de degré $\leq k-1$ et vérifie

$P(l_i) = Q(l_i)$ pour tout $i \in I$.

$P(X)$ et $Q(X)$ qui sont de degré $\leq k-1$ et qui prennent les mêmes valeurs en k éléments distincts sont forcément égaux.

On a donc $P(X) = Q(X)$ et les k personnes connaissent s le terme constant de $P(X)$, $\sum_{i \in I} Q(l_i) \prod_{\substack{j \in I \\ j \neq i}} \frac{-l_j}{l_i - l_j} = s$

Une autre façon de procéder est de résoudre le système $\{ s + a_1 l_i \cdots + a_{k-1} l_i^{k-1} = Q(l_i) \ , i \in I \}$ dont la matrice est une matrice de Vandermonde inversible (les l_i sont deux à deux distincts)

- Prenons maintenant $k-1$ personnes, les P_i où $i \in I$ et $|I| = k-1$. Comme $0 \notin \{ l_i ; i \in I \}$, la construction précédente montre que quel que soit $a \in \mathbb{F}_p$, il existe un (unique) polynôme $P(X)$ de degré $\leq k-1$ tel que $P(0) = a$ et $P(l_i) = Q(l_i)$ $\forall i \in I$. Ainsi les $k-1$ personnes ne peuvent pas retrouver s. Pire, toutes les valeurs de s sont possibles (contrairement à ce qui se passait dans l'exemple 2).

2) Pile ou face par téléphone

Blum présente ce nouveau problème de façon imagée. Alice et Bob qui viennent de divorcer, habitent deux villes différentes et décident de se partager les biens du foyer au téléphone. Alice propose à Bob de jouer cela à pile ou face. Imaginons.

A : " Bon, qui va hériter du paillasson ? Pile ou face ? "

B : " Pile ".

A : " Je lance la pièce. C'est pile, tu as gagné. Passons maintenant à la Ferrari. Que dis-tu ?

B : " Face ".

A : " Je lance la pièce. Ah c'est encore pile. Tu as perdu. "

On peut bien sûr soupçonner Alice de tricherie.

Le problème est donc le suivant : A et B qui communiquent à distance ont besoin de se mettre d'accord sur un tirage aléatoire. Comment procéder ?

- Voici la solution apportée par Blum (1982).

  Soit f une fonction à sens unique connue de A et B.

  $f : E \longrightarrow F$ avec $E = E_0 \cup E_1$, $|E_0| = |E_1|$ et $E_0 \cap E_1 = \emptyset$

  Le protocole est le suivant :

  1. Alice choisit $x \in E$, calcule $y = f(x)$ et communique y à Bob.
  2. Bob choisit $a \in \{0,1\}$ (pile ou face) et l'annonce à Alice.
  3. Alice déclare que Bob a gagné si $x \in E_a$ et que Bob a perdu si $x \notin E_a$, puis révèle x.
  4. Bob vérifie que $y = f(x)$. (et que ~~x~~ appartient ou non à E_a).

  Remarques :

  - On suppose donc qu'il est facile pour A et B de décider si $x \in E_0$ ou E_1 (exemple : pair ou impair)
  - Si f est bien choisie, Bob ne peut pas deviner x, ce qui protège Alice.
  - Il faut même que f soit à sens unique dans un sens très fort : y ne donne ni x, ni la moindre information sur le fait que $x \in E_0$ ou E_1.
  - Alice ne peut pas changer son choix, ce qui protège Bob, mais elle peut tricher et révéler $x' \neq x$ avec $x \in E_a$ et $x' \in E_b$ à condition que $y = f(x')$. Pour éviter cela, il faut prendre f injective.

- Etudions une variante plus concrète. Le protocole est le suivant :

  1. Bob choisit 2 grands premiers distincts p, q vérifiant

p et $q \equiv 3 \bmod 4$. Il donne $n = pq$ à Alice et garde secrets p et q.

2. Alice choisit x premier avec n au hasard et envoie $y = x^2 \bmod n$ à Bob. Elle garde x secret.

3. Bob sait que y est un carré modulo n et il peut calculer les 4 racines carrées de y : $\pm a$ et $\pm b$. Parmi ces racines il y a x mais Bob ne sait pas laquelle. Il en choisit une au hasard, disons a, et la communique à Alice (pile ou face).

4. Si $x = \pm a$, Alice dit à Bob qu'il a gagné.
   si $x = \pm b$, Alice dit à Bob qu'il a perdu.

Comment être sûr qu'Alice ne ment pas ? Si $x = \pm b$, Alice connaît a et b et peut donc factoriser n, et c'est la condition pour qu'elle y parvienne. Si elle annonce à Bob qu'il a perdu, Bob demande à Alice la factorisation de n.

On a donc :

5. Si Alice dit à Bob qu'il a perdu, elle lui donne la factorisation de n.

Remarques.

- Si Bob envoie n'importe quoi z à Alice (pour qu'elle ne puisse pas factoriser n), Alice peut vérifier que $y \neq z^2$.
- Si Bob propose un n erroné, à la fin du protocole, quelle qu'en soit l'issue, Alice peut demander à Bob la factorisation de n et vérifier qu'elle est correcte.
- Si le x choisi par Alice n'est pas premier avec n, elle peut factoriser n, envoie $y = x'^2$ avec x' premier avec n, ce qui lui permettra de gruger Bob. Mais ceci n'arrivera qu'avec une probabilité $\frac{n - \varphi(n) - 1}{n-1} \approx \frac{p+q}{pq}$ très faible. On a d'ailleurs le même problème avec RSA !

3) Preuve sans transfert de connaissance (Zero Knowledge Proof)

Utiliser un mot de passe à distance n'est pas sans danger. Il peut être intercepté et réutilisé. L'idéal serait que chaque utilisateur ait un secret s qui l'identifie et qu'à chaque connexion par exemple, il puisse convaincre le serveur qu'il détient s sans rien en révéler. C'est cette idée qui est à la base de la notion de preuve sans transfert de connaissance (ou preuve à divulgation nulle de connaissance).

Pour une introduction pédagogique, la page wikipédia donne deux schémas simples : "la caverne d'Ali Baba" et "l'aveugle et les billes colorées". Donnons des exemples plus élaborés.

La situation est donc la suivante : Peggy (P pour prouveur) détient un secret s et veut convaincre Victor (V pour vérificateur) qu'elle détient s sans rien en révéler à Victor.

Exemple 1

Soit p un grand premier et soit α une racine primitive modulo p. p et α sont publics.

Le secret de Peggy est un entier s défini modulo $p-1$ et bien choisi (il est difficile de trouver s connaissant $I = \alpha^s \bmod p$). Elle veut convaincre Victor qu'elle détient s.

Voici le protocole.

1. P s'identifie auprès de V par I.
2. P choisit r modulo $p-1$ aléatoire et calcule $t = \alpha^r \bmod p$ qu'elle donne à V
3. V choisit $\varepsilon = 0$ ou 1 aléatoirement et le communique à P.
4. $\left.\begin{array}{l}\text{Si } \varepsilon = 0, \text{ P donne } r \bmod p-1 \\ \text{Si } \varepsilon = 1, \text{ P donne } r+s \bmod p-1\end{array}\right\}$ noté x.
5. V vérifie que $\alpha^x = t \bmod p$ si $\varepsilon = 0$ et $\alpha^x = It \bmod p$ si $\varepsilon = 1$.

Remarques. • Supposons que P' connaisse I mais pas s et veuille se faire passer pour P auprès de V. Il suit le protocole et envoie $t = \alpha^r \bmod p$. Si $\varepsilon = 0$, il envoie r et V sera satisfait, mais si $\varepsilon = 1$, il ne sait pas quoi envoyer. Il peut aussi envoyer $t' = \alpha^r I^{-1} \bmod p$ à la place de t. Si $\varepsilon = 1$, il envoie r et V est satisfait, mais si $\varepsilon = 0$, il ne sait pas quoi envoyer. Quoi que fasse P', il ne peut pas envoyer à la fois $\log_\alpha t$ et $\log_\alpha It$ car il ignore $s = \log_\alpha I$.

La probabilité de réussite de l'imposture est au mieux de $\frac{1}{2}$ et au bout de k applications du protocole, V est convaincu avec une probabilité de $1 - \frac{1}{2^k}$ que P connaît bien s.

• L'information révélée à V n'est qu'une suite d'entiers modulo p aléatoires, à condition bien sûr de changer de r à chaque fois (sinon V peut en déduire s). Ainsi P n'a rien révélé sur s.

Exemple 2. Soient p, q 2 grands premiers distincts tenus secrets et $n = pq$ public. Le secret de P est un entier s défini modulo p et que l'on peut supposer premier avec n. Voici le protocole.

1. P s'identifie auprès de V par $y = s^2 \bmod n$
2. P choisit r_1 au hasard tel que $\mathrm{pgcd}(r_1, n) = 1$. Soit $r_2 = s r_1^{-1} \bmod n$. P calcule $x_1 = r_1^2 \bmod n$, $x_2 = r_2^2 \bmod n$ et envoie x_1 et x_2 à V.
3. V vérifie que $x_1 x_2 = y \bmod n$, choisit x_1 ou x_2 et demande à P une racine carrée du x_i choisi.
4. P lui répond et V vérifie que c'est bien le cas.

Les commentaires sont plus ou moins les mêmes que précédemment.