Cryptographie Civile

Robert Rolland

C.N.R.S., Institut de Mathématiques de Luminy
F13288 Marseille CEDEX 9
e-mail: rolland@iml.univ-mrs.fr

Transmission de l'Information

- Représentation de l'information, codage, compression.
- Intégrité des données, détection et correction des erreurs.
- Confidentialité, cryptographie, chiffrement, cryptanalyse.

Principaux outils utilisés

- Complexité des algorithmes.
- Probabilités, entropie.
- Arithmétique.
- Corps finis, géométrie affine et projective sur les corps finis, géométrie combinatoire.
- Algèbre commutative.
- Géométrie algébrique sur les corps finis.

Les problèmes de la cryptographie

- Chiffrement.
- Authentification.
- Signature.
- Gestion des clés.
- Mise en place de protocoles.

Le Chiffrement

- Clé secrète (une seule clé partagée):
  - ▷ One-time-pad (masque jetable), utilise un masque aléatoire de la longueur du texte clair.
  - ▷ DES (Data Encryption Standard). Clé de 56 bits, entrée de 64 bits, sortie 64 bits.
  - ▷ IDEA (International Data Encryption Algorithm). Clé 128 bits, entrée 64 bits, sortie 64 bits.

Le Chiffrement

Principe du masque jetable

$Masque$	:	0	1	1	0	1	0	1	0	0	0	$\cdots$
$clair1$	:	1	1	1	0							
$crypt1$	:	1	0	0	0							
$clair2$	:					0	1	0	0	1		
$crypt2$	:					1	1	1	0	1		
$\vdots$	:										$\vdots$	$\cdots$

Pour le masque: Utilisation de générateurs de bits aléatoires (par exemple Blum Blum Shub).

Le Chiffrement

- Clé publique:

  ▷ RSA (Rivest-Shamir-Adleman). Basé sur la difficulté de décomposer un nombre en facteurs premiers.

  ▷ ElGamal (Chiffrement). Basé sur la difficulté du calcul des logarithmes discrets dans certains groupes.

  ▷ McEliece. Basé sur la difficulté du décodage d'un code linéaire général.

La signature

Pour signer un document on en construit une empreinte (Hachage) et on signe l'empreinte.

- Hachage: SHA (Secure Hash Algorithm).
- Signature:
  - ▷ DSS (Digital Signature Standard) utilise DSA (Digital Signature Algorithm).
  - ▷ RSA (Rivest-Shamir-Adleman)

Authentification

Utilise

- La signature et ses outils liés au hachage, aux certificats.
- L'authentification:
  - ▷ Schéma d'authentification de Feige-Fiat-Shamir. Utilise la dificulté du calcul de la racine carrée dans $\mathbb{Z}/n\mathbb{Z}$ si la décomposition de n en facteurs premiers n'est pas connue.

Gestion des clés

Le chiffrement rapide utilise les systèmes à clé secrète (par exemple PGP (pretty good privacy) utilise IDEA). Mais la gestion des clés se pose:

- Échanges de clés de Diffie et Hellman (logarithme discret).
- Chiffrement à clé publique.
- signature.

Gestion des clés

L'utilisateur d'un système à clé publique doit avoir confiance à la clé publiée: utilisation de certificats (signature par des autorités)

L'Échange de clé de Diffie et Hellman

Basé sur le problème du logarithme discret.

On donne (public) un groupe G et un $\alpha \in G$.

$$
\begin{array}{ccc}
\text{Alice} & \longleftrightarrow & \text{Bob} \\
m \text{ secret} & & n \text{ secret} \\
g^m & \longrightarrow & \\
 & \longleftarrow & g^n \\
g^{nm} & & g^{mn}
\end{array}
$$

L'Échange de clé de Diffie et Hellman

On choisit pour groupe un groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^*$ où p premier de l'ordre de 10^{50} ou encore un corps fini et pour α un élément primitif.

On peut aussi prendre pour G une courbe elliptique ou la Jacobienne d'une courbe hyperelliptique.

Le système RSA

Basé sur le problème de la factorisation d'un produit de deux grands nombres premiers.

Alice engendre deux nombres premiers p et q grands (100 chiffres),

puis calcule $n = pq$ et $\phi(n) = (p-1)(q-1)$.

Alice choisit b aléatoire $1 < b < \phi(n)$ tel que $pgcd(b, \phi(n)) = 1$,

puis calcule $a = b^{-1} \quad mod\ \phi(n)$ (Algo. d'Euclide).

Le système RSA

Alice publie n et b dans un répertoire (clé publique) et garde a secret (clé privée).

Si on veut transmettre x à Alice $1 < x < n$ on envoie $y = e_K(x) = x^b \;\; mod \; n$.

Alice calcule alors $d_K(y) = y^a \;\; mod \; n = x$

Le système RSA

En effet

$$y^a \mod n = x^{(ab)} \mod n =$$

$$x^{(1+k\phi(n))} \mod n.$$

Remarque: On peut montrer que pour tout $0 \leq x < n$ (pas nécessairement premier avec n) on a $x^{(1+k\phi(n))} \mod n = x$.

Chiffrement d'ElGamal

Basé sur le problème du logarithme discret.

Alice choisit p premier puis g et $x < p$.

Elle calcule $y = g^x \ \ mod\ p$. La clé publique est (y, g, p) (g, p pouvant être partagés).

La clé privée est x.

Chiffrement d'ElGamal

Si Bob veut communiquer le texte clair m ($m < q$) à Alice:

il choisit k premier avec $p - 1$ puis calcule

$$a = g^k \mod p,$$

$$b = y^k m \mod p.$$

Le texte chiffré est (a, b).

Chiffrement d'ElGamal

Pour déchiffrer Alice calcule

$$ba^{-x} \mod p.$$

En effet:

$$a^x = g^{kx} \mod p,$$

$$ba^{-x} \mod p = y^k m g^{-kx} \mod p =$$

$$g^{kx} m g^{-kx} \mod p = m.$$

La signature DSA

Basée sur le problème du logarithme discret.

On construit $512 \leq L \leq 1024$, L multiple de 64.

p premier $2^{L-1} < p < 2^L$ (p a L bits).

q diviseur premier de $p-1$ avec $2^{159} < q < 2^{160}$ (q a 160 bits).

h primitif dans $\mathbb{Z}/p\mathbb{Z}$ et $g = h^{(p-1)/q}$. Donc g est d'ordre q dans $\mathbb{Z}/p\mathbb{Z}$.

La signature DSA

Sont publics et communs p, q, g.

Chaque utilisateur choisit un x tel que $0 < x < q$ (clé privée) et calcule $y = g^x \mod p$ (sa clé publique).

Pour signer une empreinte M d'un texte m l'utilisateur choisit $0 < k < q$ (un nouveau k à chaque signature) et calcule

$$r = (g^k \mod p) \mod q,$$

$$s = k^{-1}(M + rx) \mod q.$$

La signature DSA

(r, s) est la signature envoyée avec le texte m.

Celui qui reçoit le message doit vérifier la signature de la manière suivante: à partir du texte m il calcule l'empreinte M puis calcule

$$w = s^{-1} \ \ mod\ q, \quad u_1 = Mw \ \ mod\ q,$$

$$u_2 = rw \ \ mod\ q, \quad v = (g^{u_1} y^{u_2} \ \ mod\ p) \ \ mod\ q.$$

Il vérifie que $v = r$.

Canal subliminal dans la signature DSA

Si Alice envoie un message signé à Bob, et si Bob (en accord avec Alice) dispose de la clé privée d'Alice x. Alors à partir de (r, s) Bob peut calculer $rx, M + rx$ et donc
$k = (M + rx)s^{-1}$.

Alice et Bob ont donc échangé k à l'insu de tout observateur.

Un exemple sur les courbes hyperellyptiques

Basé sur le problème du logarithme discret.

Cette étude s'appuie sur l'étude de la courbe algébrique

$$y^2 + h(x)y = f(x)$$

où $deg(f) = 2g + 1$ et $deg(h) \leq g$.

Un exemple sur les courbes hyperellyptiques

Les points de la jacobiennes peuvent être représentés par les couples de polynômes (a, b) où

- a unitaire de degré $deg(a) \leq g$.
- $deg(b) < deg(a)$.
- a divise $f - hb - b^2$.

La loi de groupe est définie par

$$(a', b') = (a_1, b_1) * (a_2, b_2)$$

avec

$$d = pgcd(a_1, a_2, b_1 + b_2 + h) =$$

$$s_1 a_1 + s_2 a_2 + s_3(b_1 + b_2 + h),$$

$$a = a_1 a_2 / d^2,$$

$$b = (s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f))/d \quad mod\ a,$$

puis

$$a' = (f - hb - b^2)/a$$

$$b' = (-h - b) \ \ mod \ a'.$$

Et on réitère les calculs des deux dernières lignes (à partir de a' et b') jusqu'à ce que les résultats obtenus vérifient les conditions de degré imposées pour la représentation d'un point de la jacobienne.

Schéma d'identification Feige - Fiat - Shamir

Basé sur la difficulté d'extraire une racine carrée dans $\mathbb{Z}/n\mathbb{Z}$ pour $n = pq$ (p, q premiers).

Un arbitre choisit $n = pq$ et engendre les clés publiques et privées des utilisateurs. s clé privée, $s^2 = \mu$, $\nu = \mu^{-1} \;\; mod \; n$. ν est la clé publique.

Alice choisit $r < n$ et envoie $x = r^2 \mod n$ à Victor. Victor envoie un bit b à Alice.

Si $b = 0$ Alice renvoie r à Victor qui vérifie que $r^2 = x$.

Si $b = 1$ Alice renvoie $y = (rs) \mod n$ à Victor qui vérifie que $x = y^2\nu \mod n$.

Si Alice veut tricher elle a une chance sur deux de se tromper. Au bout de t tests, Victor est convaincu.

Générateur aléatoire de Blum - Blum - Shub

On calcule deux grands nombres premiers $p, q \equiv 3 \mod 4$. On pose $n = pq$. On choisit x aléatoire premier avec n et on pose $x_0 = x^2 \mod n$.

Le i^{e} bit pseudo aléatoire est le bit le moins significatif de

$$x_i = x_{i-1}^2 \mod n.$$

Références

M. Demazure, Cours d'Algèbre, Cassini

Groupe de travail sur la liaison Lycées-Universités, Cours et activités en arithmétique pour les classes terminales, IREM de Marseille

D. Kahn, La Guerre des Codes Secrets, InterEditions

N. Koblitz, Algebraic Aspects of Cryptography, Springer

Références

R. Kumanduri, C. Romero, Number theory with computer applications

B. Schneier, Cryptographie Appliquée, Thomson Publishing

J. Stern, La Science du Secret, Editions Odile Jacob

D. Stinson, Cryptographie Théorique et Pratique, Thomson Publishing