RSA ET LES EQUATIONS DIOPHANTIENNES

Abderrahmane Nitaj

02 Novembre 2006

nitaj@math.unicaen.fr

http://www.math.unicaen.fr/~nitaj

Contenu

- L'équation RSA
- Les fractions continues
- L'attaque de Wiener
- L'algorithme LLL
- Le théorème de Coppersmith (1)
- L'attaque de Boneh et Durfee
- L'attaque de Blömer et May
- Les clés contraintes
- L'équation $eY - p(q-u)X = Z$
- L'équation $eY^m - (p+1)(q-1)X^m = Z$
- Les courbes elliptiques
- L'équation $eX + (p-1)(q-1)Y = NZ$

L'équation RSA (1977)

- Le module :
  - On choisit p et q nombres premiers.
  - On calcule $N = pq$.
  - On calcule $\phi(N) = (p-1)(q-1)$: l'indicateur d'Euler.
- Les clés :
  - On prend $e \in \{0, 1, \cdots, \phi(N) - 1\}$, $\gcd(e, \phi(N)) = 1$.
  - On calcule $d \equiv e^{-1} \pmod{\phi(N)}$
    $\Longrightarrow \exists k, \quad ed - k\phi(N) = 1.$
- L'équation RSA : $\boxed{ed - k\phi(N) = 1}$.

Les fractions continues

- Données :
  - $\theta \in \mathbb{R}^+$.
- On cherche :
  - $a, b \in \mathbb{N}$ tels que $\frac{a}{b} \approx \theta$.
- Algorithme des fractions continues.
  - Calcule $\theta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_s + \cfrac{1}{\cdots}}}} = [a_0, a_1, \cdots]$.
    - $r_0 = \theta$, $a_0 = [r_0]$.
    - $n \geq 1, \quad r_n = \frac{1}{r_{n-1} - a_{n-1}}, \quad a_n = [r_n]$,
  - $[a_0, a_1, \cdots, a_s] = \frac{a}{b}$.
  - $\frac{a}{b}$ est une convergente.

Le théorème de Legendre

- Données :
  - $\theta \in \mathbb{R}$.
  - $a, b \in \mathbb{N}$, $\gcd(a, b) = 1$.
- Problème :
  - $\frac{a}{b}$ est-il une convergente de θ?
- Le Théorème de Legendre.
  - Si $\left|\frac{a}{b} - \theta\right| < \frac{1}{2b^2}$, alors $\frac{a}{b}$ est une convergente de θ.

L'attaque de Wiener

(Les fractions continues)

- Données :
  - $N \in \mathbb{N}$.
  - $e \in \mathbb{N}, \qquad e < \phi(N)$.
  - Equation $ed - k\phi(N) = 1 \Longrightarrow \frac{k}{d} \approx \frac{e}{\phi(N)}$.
- Wiener (1990):
  - $\phi(N) \approx N$.
  - $\frac{k}{d} \approx \frac{e}{N}$.
  - Si $d < N^{\frac{1}{4}}$, alors $\frac{k}{d}$ est une réduite de $\frac{e}{N}$.

L'algorithme LLL

- Données :
  - $v_1, v_2, \cdots v_m \in \mathbb{R}^m$, linéairement indépendants.
  - $L = \mathbb{Z}.v_1 \oplus \mathbb{Z}.v_2 \oplus \cdots \oplus \mathbb{Z}.v_m$.
- Caractéristiques
  - $\dim(L) = m$.
  - $\det(L) = \prod_{i=1}^{m} ||v_i^*||$ (via Gram-Schmidt).
- Problème : Déterminer un vecteur v
  - $v \in L$.
  - $||v||$ est assez petite.
- L'algorithme LLL (Lenstra-Lenstra-Lovasz, 1982) :
  - Produit un vecteur v, $||v|| \leq 2^{\frac{m-1}{4}} \det(L)^{\frac{1}{m}}$.
  - En temps polynomial en m.

Le théorème de Coppersmith (1)

Deux variables

- Données :
  - $f(x,y) \in \mathbb{Z}[x,y]$ contenant ω termes.
  - m, $M \in \mathbb{N}$.
- Problème :
  - Déterminer x_0 et y_0, $\quad f(x_0,y_0) \equiv 0 \pmod{M^m}$.
- Le théorème de Coppersmith (à la Howgrave-Graham):
  - Produire $h(x,y) \in \mathbb{Z}[x,y]$ à partir de $f(x,y)$.
    - Si $h(x_0,y_0) \equiv 0 \pmod{M^m}$ avec $|x_0| < X$, $|y_0| < Y$.
    - Si $||h(xX,yY)|| < \frac{M^m}{\sqrt{\omega}}$, (norme euclidienne).
  - Alors $h(x_0,y_0) = 0$ dans $\mathbb{Z}^2$.

L'attaque de Boneh et Durfee

(Les techniques de Coppersmith)

- Données :
  - $e, N \in \mathbb{N}, \qquad e < \phi(N)$.
  - Equation $ed - k\phi(N) = 1$
    $\Longrightarrow -k(N+1-(p+q)) \equiv 1 \pmod{e}$.
- Boneh et Durfee (2000):
  - $f(x,y) = x(N+1-y) - 1$ + Coppersmith.
  - $f(x_0, y_0) \equiv 0 \pmod{e}$, $|x_0| < X = e^{\delta}$, $|y_0| < Y = e^{\frac{1}{2}}$
  - Si $d < N^{0.292}$, alors détermination de d et k par Coppremith.

Le théorème de Coppersmith (2)

Une variable

- Données :
  - $f(x) \in \mathbb{Z}[x]$ de degré δ.
  - m, $M \in \mathbb{N}$.
- Problème :
  - Déterminer x_0, $\quad f(x_0) \equiv 0 \pmod{M^m}$.
- Le théorème de Coppersmith (à la Howgrave-Graham):
  - Produire $h(x) \in \mathbb{Z}[x]$ à partir de $f(x)$.
    - Si $h(x_0) \equiv 0 \pmod{M^m}$ avec $|x_0| < X$.
    - Si $||h(xX)|| < \frac{M^m}{\sqrt{\delta+1}}$, (norme euclidienne).
  - Alors $h(x_0) = 0$ dans $\mathbb{Z}$.

Le théorème de Coppersmith (3)

Une variable

- Données :
  - $N = pq$, $q < p$.
  - $\tilde{P}$, tel que $|kp - \tilde{P}| \leq N^{\frac{1}{4}}$.
  - $k \not\equiv 0 \pmod{q}$.
- Problème :
  - Déterminer p.
- Le théorème de Coppersmith (à la May):
  - Calculer kp par le théorème de Coppersmith.
  - $p = \gcd(kp, N)$.
  - En temps polynomial en $\log(N)$.

L'attaque de Blömer et May

(Les fractions continues + Coppersmith)

- Données :
  - $e, N \in \mathbb{N}, \qquad e < \phi(N)$.
  - Equation $ex - k\phi(N) = y. \Longrightarrow \frac{k}{x} \approx \frac{e}{\phi(N)}$.
- Blömer et May (2004):
  - $\phi(N) \approx N$, $\frac{k}{x} \approx \frac{e}{N}$.
  - Si $x < N^{\frac{1}{4}}$, alors $\frac{k}{x}$ est une réduite de $\frac{e}{N}$.
  - Si $|y| < N^{-\frac{3}{4}}ex$, alors $\left|p + q - \left(N + 1 - \frac{ex}{k}\right)\right| < N^{\frac{1}{4}}$.

Clés faibles, clés contraintes

- Données :
  - $e, N \in \mathbb{N},\ e < \phi(N)$.
- Définition (clés faibles) :
  - A partir de e, on peut factoriser N en temps polynomial.
  - $\#\{e,\ e \text{ est faible}\} = N^{\alpha},\ \alpha > 0$.
- Définition (clés contraintes) :
  - e est en relation avec une expression $F(p, q)$.
  - $F(p, q) \approx N$.
  - A partir de $F(p, q)$ on peut calculer p ou q.

Clés faibles, clés contraintes : exemples

- Données :
  - $e, N \in \mathbb{N}, \qquad e < \phi(N)$.
- Clés (Wiener) (Boneh-Durfee):
  - Equation : $ed - k\phi(N) = 1$.
  - $\#\{e,\ e \text{ est faible}\} = \mathcal{O}\left(N^{\frac{1}{4}-\varepsilon}\right) \qquad (= \mathcal{O}\left(N^{0.292-\varepsilon}\right))$.
  - Contraintes avec $F(p,q) = \phi(N) = N + 1 - p - q$.
- Clés (Blömer-May) :
  - Equation : $ex - k\phi(N) = -y$.
  - $\#\{e,\ e \text{ est faible}\} = \mathcal{O}\left(N^{\frac{3}{4}-\varepsilon}\right)$.
  - Contraintes avec $F(p) = \phi(N) = N + 1 - p - q$.

L'équation $eY - p(q-u)X = Z$ (1)

(Les fractions continues + Coppersmith)

- Données :
  - $N = pq$, $e < \phi(N)$.
  - Equation $eY - p(q-u)X = Z$.
- But : Trouver X, Y, Z, p, q.
- L'idée : Si X et Y sont "petits":
  - $\frac{X}{Y} \approx \frac{e}{p(q-u)} \approx \frac{e}{N} \Longrightarrow \frac{X}{Y}$ est une réduite de $\frac{e}{N}$.
  - $p(q-u) = N - pu \approx \frac{eX}{Y} \Longrightarrow pu \approx N - \frac{eX}{Y}$.
  - Calcul de pu par Coppersmith.
  - $p = \gcd(N, pu)$.

L'équation $eX - p(q-u)Y = Z$ (2)

- Données :
  - $N = pq$, $e < \phi(N)$.
  - Equation $eX - p(q-u)Y = Z$.
- Particularités :
  - Contraintes avec $F(p,q) = p(q-u)$.
  - $\#\{e,\ eX - p(q-u)Y = Z,\ X, Y$ "sont petits"$\} = \mathcal{O}\left(N^{\frac{3}{4}-\varepsilon}\right)$.
- Variantes
  - $F(p,q) = p + a - qu$.
  - $F(p,q) = (p-u)\left(q - \frac{a}{u}\right) \Longrightarrow \phi(N) = (p-1)(q-1)$.
  - Echanger p et q dans F.

L'équation $eX^m - (p+1)(q-1)Y^m = Z$ (1)

(Les fractions continues + Coppersmith)

- Données :
  - Equation $eX^m - (p+1)(q-1)Y^m = Z$.
- But : Trouver X, Y, Z, m, p, q.
- L'idée : Si X et Y sont "petits" et $1 \leq m \leq \log N$:
  - $\frac{X}{Y} \approx \left(\frac{e}{(p+1)(q-1)}\right)^{1/m} \approx \left(\frac{e}{N}\right)^{1/m} \Longrightarrow \frac{X}{Y}$ réduite de $\left(\frac{e}{N}\right)^{1/m}$.
  - $(p+1)(q-1) = N - 1 - (p-q) \approx \frac{eX^m}{Y^m}$ $\Longrightarrow p - q \approx N - 1 - \frac{eX^m}{Y^m}$.
  - Calcul de p par Coppersmith.

L'équation $eX^m - (p+1)(q-1)Y^m = Z$ (2)

- Données :
  - $N = pq$, $e < \phi(N)$.
  - Equation $eX^m - (p+1)(q-1)Y^m = Z$.
- Particularités :
  - Contraintes avec $F(p,q) = (p+1)(q-1)$.
  - $\#\{e,\ eX^m - (p+1)(q-1)Y^m = Z,\ X, Y \text{ sont "petits"}\} = \mathcal{O}\left(mN^{\frac{1}{2}-\varepsilon}\right)$.
- Variantes
  - $F(p,q) = (p-1)(q-1) = \phi(N)$.
  - $F(p,q) = (p+1)(q+1)$.
  - Echanger p et q dans F.

Les courbes elliptiques

- Données :
  - $p > 3$, premier.
  - $a, b \in \mathbb{F}_p$ avec $4a^3 + 27b^2 \neq 0$.
  - Equation E : $y^2 = x^3 + ax + b$. item $E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p,$ solutions de$E\} \cup \mathcal{O}$ est un groupe additif.
- Addition :
  - $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ avec $x_P \neq x_Q$,
  - $\lambda = \frac{y_P - y_Q}{x_P - x_Q}$, $\mu = \frac{3x_P^2 + a}{2y_P}$,
  - $x_{P+Q} = \lambda^2 - x_P - x_Q$, $x_{2P} = \mu^2 - 2x_P$.
  - $y_{P+Q} = \lambda(x_P - x_{P+Q}) - y_Q$, $y_{2P} = \mu(x_P - x_{2P}) - y_P$.

ECM (1)

(Les courbes elliptiques)

- Données :
  - $M = pM'$, p premier, $p < 10^{40}$.
- But : Trouver p.
- ECM (H.W. Lenstra, 1985) : Si p est "petit" :
  - Choisir $P_0 = (x_0 : y_0 : z_0) \in (\mathbb{Z}/M\mathbb{Z})^3$ et $a \in \mathbb{Z}/M\mathbb{Z}$.
  - Définir $b \in \mathbb{Z}/M\mathbb{Z}$ avec $y_0^2 z_0 = x_0^3 + a x_0 z_0^2 + b z_0^3 \pmod{M}$ et $4a^3 + 27b^2 \not\equiv 0 \pmod{M}$.
  - Définir $E : y^2 z = x^3 + axz^2 + bz^3$ sur $\mathbb{Z}/M\mathbb{Z}$.

ECM (2)

- Choisir $B_1, B_2 \in \mathbb{N}$.
- Phase 1: Calculer $Q = kP_0$ avec

$$k = \prod_{g \leq B_1, \text{premier}} g^{e_g}, \qquad e_g = [\log B_1 / \log g] .$$

- Phase 2: Pour chaque premier g, $B_1 < g < B_2$, calculer $gQ = (x_{gQ} : y_{gQ} : z_{gQ})$.
  - Si $\gcd(z_{gQ}, M) > 1$, c'est un facteur de M.
- Complexité : $\mathcal{O}\left(\exp\left(\left(\sqrt{2} + o(1)\right)\sqrt{\log p \log\log p}\right)\right)$.

ECM (3)

- Records :
  - ECMNET project (INRIA) : $p|M = 10^{381} + 1$ avec $p \approx 10^{67}$ (B. Dodson, 2006).
  - Dario Alpern : $p|M$ avec $p \approx 10^{48}$ (A. Griffiths, 2004).
- Facteurs inférieurs à 10^{40}: (GMP-ECM, Zimmermann)
  - $B_1 = 3 \times 10^6$,
  - $B_2 = 5 \times 10^9$,
  - Nombre de courbes ≈ 2240.

L'équation $eX + (p-1)(q-1)Y = NZ$

(Les fractions continues + ECM)

- Données :
  - $N = pq$, $e < \phi(N)$.
  - Equation $eX + (p-1)(q-1)Y = NZ$
- But : Trouver X, Y, Z, p, q.
- L'idée : Si X et Y sont "petits" et Y est 10^{40}-lisse :
  - Ecrire $eX - N(Z-Y) = (p+q-1)Y$.
  - $\frac{X}{Z-Y} \approx \frac{e}{N}$. $\Longrightarrow$ $\frac{X}{Z-Y}$ réduite de $\frac{e}{N}$.
  - $M = |eX - N(Z-Y)| \Longrightarrow (p+q-1)|Y| = M$.
  - Déterminer $|Y|$ par ECM.
  - Déterminer $p+q-1$ et p.

L'équation $eX + (p-1)(q-1)Y = NZ$

- Données : $M = eX - N(Y - Z)$.
- Equation: $(p + q - 1)|Y| = M$.
- But : Trouver Y, p, q.
- L'idée : Si $|Y|$ est 10^{40}-lisse :
  - $q < p < 2q \Longrightarrow 2\sqrt{N} < p + q < \frac{3\sqrt{2}}{2}\sqrt{N}$.
  - Calculer $D_1 = \frac{M}{\frac{3\sqrt{2}}{2}\sqrt{N}}$, $D_2 = \frac{M}{2\sqrt{N}}$.
  - Appliquer ECM avec M
    $\Longrightarrow M = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s} M'$, $p_i < 10^{40}$.
  - Puisque $M = |Y|(p + q - 1)$,, alors
    $|Y| = {p_1}^{x_1} {p_2}^{x_2} \cdots {p_s}^{x_s}$.

L'équation $eX + (p-1)(q-1)Y = NZ$

- Déterminer les diviseurs $D = {p_1}^{x_1} {p_2}^{x_2} \cdots {p_s}^{x_s} \in [D_1, D_2]$.
  - Résoudre
    $\log D_1 < x_1 \log p_1 + x_2 \log p_2 + \cdots + x_s \log p_s < \log D_2$
    - LLL (de Weger, 1987).
    - PSLQ (Ferguson et Bailey, 1992)
- En moyenne, il y a $\log M < \log N$ solutions.
- Pour chaque diviseur D de M, tester si $p + q = \frac{M}{D} + 1$.
- Complexité :
  $\mathcal{O}\left((\log N)^2 \exp\left(\left(\sqrt{2} + o(1)\right)\sqrt{\log p \log\log p}\right)\right)$, p plus grand facteur premier de Y.
- Nombre de clés : $\mathcal{O}\left(N^{\frac{1}{2}-\varepsilon}\right)$.