Préparation à l'agrégation de Mathématiques 2009 ENS Cachan Ker Lann
Epreuve de modélisation, option C : algèbre et calcul formel

richard.leroy@univ-rennes1.fr
http://perso.univr-rennes1.fr/richard.leroy/

Cryptosystème de Chebychev

Résumé : On présente dans ce texte un cryptosystème basé sur les polynômes de Chebychev, ainsi qu'une attaque contre celui-ci.

Mots-clés : Cryptosystème, polynômes de Chebychev, algorithme d'Euclide étendu.

Il est rappelé que le jury n'exige pas une compréhension exhaustive du texte. Vous êtes laissé(e) libre d'organiser votre discussion comme vous l'entendez. Des suggestions de développement vous sont proposées en fin de texte. Vous n'êtes pas tenu(e) de les suivre. Il est conseillé de mettre en lumière vos connaissances à partir du fil conducteur constitué par le texte. Le jury demande que la discussion soit accompagnée d'exemples traités sur ordinateur.

1 Polynômes de Chebychev

On introduit dans ce paragraphe les polynômes de Chebychev, qui seront à la base du cryptosystème étudié dans ce texte.

Définition : *Les polynômes de Chebychev sont les polynômes satisfaisant la récurrence suivante :*

$$T_0 = 1,\ T_1 = X$$
$$\forall n \geq 2,\ T_n = 2XT_{n-1} - T_{n-2}.$$

On peut également caractériser les polynômes de Chebychev de la manière suivante :

Proposition : *Pour tout* $x \in [-1,1]$*, on a* $T_n(x) = \cos(n \arccos(x))$.

Une des propriétés fondamentales des polynômes de Chebychev est leur propriété de semi-groupe, affirmant que :

$$\forall x \in [-1,1],\ T_r(T_s(x)) \ = \ T_{rs}(x).$$

On en déduit immédiatement que les polynômes de Chebychev commutent, dans le sens où :

$$\forall x \in [-1,1],\ T_r(T_s(x)) \ = \ T_s(T_r(x)).$$

2 Le cryptosystème

Il s'agit d'un cryptosystème à clef publique. Celle-ci est générée de la manière suivante :

1. *Générer un grand entier* s.
2. *Prendre un nombre* $x \in [-1,1]$ *au hasard, et calculer* $T_s(x)$.
3. *La clef publique est alors le couple* $(x, T_s(x))$*, la clef secrète étant l'entier* s.

Le chiffrement d'un message $M \in [-1,1]$ *est alors effectué en utilisant le clef publique :*

1. *Générer un grand entier* r.
2. *Calculer* $T_r(x),\ T_{rs}(x) \ = \ T_r(T_s(x))$ *et* $N = MT_{rs}(x)$.
3. *Le message chiffré est alors le couple* $(T_r(x), N)$.

Le déchiffrement d'un message (t,n) *se fait à l'aide de la clef privée :*

1. *Calculer* $T_s(t)$.

2. *Calculer* $n/T_s(t)$.

La correction du cryptosystème est dûe à la propriété de commutation des polynômes de Chebychev.

La génération de la clef publique, le chiffrement et le déchiffrement utilisent tous les trois des évaluations de polynômes de Chebyshev. Utiliser leur définition récursive pour calculer $T_n(x)$ *conduit à un complexité linéaire en* n*. Cependant, on peut obtenir une complexité logarithmique en remarquant que :*

$$T_{2n}(x) = T_2(T_n(x)) = 2T_n(x)^2 - 1 \quad et \quad T_{2n+1}(x) = 2T_{n+1}(x)T_n(x) - x.$$

3 Attaque du cryptosystème

On montre dans cette section que, malgré la ressemblance avec le système ElGamal, le cryptosystème ici présenté n'est pas sûr. Le défaut majeur est que plusieurs polynômes de Chebychev peuvent passer par le même point.

3.1 Présentation de l'attaque

Soit $(x, T_s(x))$ *la clef publique d'Alice. Afin de lui envoyer un message* M*, Bob choisit un grand entier* r *et calcule :*

$$T_r(x),\ T_{rs}(x) \text{ et } N = MT_{rs}(x).$$

Il envoie alors le message chiffré $C = (T_r(x), N)$ *à Alice.*

Un attaquant , connaissant la clef publique d'Alice et le message chiffré C*, procède de la manière suivante :*

1. *Il calcule un entier* r' *tel que* $T_{r'}(x) = T_r(x)$.
2. *Puis il calcule* $T_{r's}(x) = T_{r'}(T_s(x))$.

3. Enfin, il retrouve le message $M = N/T_{r's}(x)$.

On montre dans le prochain paragraphe comment l'entier r' *peut être obtenu.*

3.2 Calcul de r'

On considère l'ensemble $\wp = \left\{ \frac{\pm \arccos(T_r(x)) + 2k\pi}{\arccos(x)} \mid k \in \mathbb{Z} \right\}$. *Le résultat suivant montre que* $\wp$ *contient tous les entiers* r' *vérifiant* $T_{r'}(x) = T_r(x)$ *possibles :*

Proposition : *Pour chaque couple* $(x, T_r(x))$ *fixé, l'entier* r' *vérifie* $T_{r'}(x) = T_r(x)$ *si et seulement si* $r' \in \wp \cap \mathbb{N}$.

On pose

$$a = \frac{\arccos(T_r(x))}{\arccos(x)} \text{ et } b = \frac{2\pi}{\arccos(x)}.$$

L'attaquant doit donc trouver un entier $k \in \mathbb{Z}$ *et un entier* $n > 1$ *solutions de l'une des deux équations suivantes :*

$$a + kb = u \qquad ou \qquad -a + kb = u.$$

Notons $(a \bmod 1)$ *et* $(b \bmod 1)$ *les parties fractionnaires de* a *et* b. *Le problème revient alors à résoudre*

$$(a \bmod 1) + k(b \bmod 1) = z \qquad ou \qquad -(a \bmod 1) + k(b \bmod 1) = z.$$

Supposons que l'on travaille en précision finie, en base $B \geq 2$, *et que* L *soit le nombre maximal de décimales de* $(a \bmod 1)$ *et* $(b \bmod 1)$. *En multipliant par* B^L, *on obtient les équations suivantes :*

$$\begin{gathered}(a \bmod 1)B^L + k(b \bmod 1)B^L = zB^L \\ ou \\ -(a \bmod 1)B^L + k(b \bmod 1)B^L = zB^L.\end{gathered}$$

On pose $a' = (a \bmod 1)B^L$ *et* $b' = (b \bmod 1)B^L$.

L'attaquant a alors à résoudre :

$$a' + kb' \equiv 0 \ mod \ B^L \qquad ou \qquad -a' + kb' \equiv 0 \ mod \ B^L.$$

Les solutions de la première équation s'obtiennent facilement à partir des solutions de la deuxième. Il suffit donc de savoir résoudre les équations du type :

$$kb' \equiv a' \ mod \ B^L.$$

Une telle équation admet une solution si et seulement si d divise a', où d désigne le pgcd de b' et de B^L divise a'. Les solutions s'obtiennent alors grâce à l'algorithme d'Euclide étendu.

4 Suggestions pour le développement

Soulignons qu'il s'agit d'un menu à la carte et que vous pouvez choisir d'étudier certains points, pas tous, pas nécesairement dans l'ordre, et de façon plus fouillée. Vous pouvez aussi vous poser d'autres questions que celles indiquées. Il est demandé que vos investigations comportent une partie ordinateur.

➢ *Plusieurs propriétés des polynômes de Chebychev sont affirmées sans démonstration. Le candidat est invité à les expliciter.*

➢ *Le candidat pourra détailler le calcul de r' présenté dans le texte, notamment l'utilisation de l'algorithme d'Euclide étendu.*

➢ *En ce qui concerne le passage sur machine, le candidat est invité à programmer le cryptosystème de Chebychev, ainsi que l'attaque présentée.*

➢ *Le candidat pourra étudier la complexité (dans le cas le pire) des algorithmes présentés.*