Mise en place d'un cryptosystème d'EL Gamal sur les courbes elliptiques et étude comparative de sa sécurité.

Liste des membres du groupe

— DENEUX Rafael (snif il s'en va....)
— COMMUNAL Hugo

Positionnements thématiques

— Mathématiques (Algèbre, Théorie des groupes, Coubres elliptiques)
— Informatique (informatique théorique, Python)

Mots-clés (en français)

- Cryptographie
- Groupes cycliques
- Courbes elliptiques
- Logarithme discret
- Complexité algorithmique
- Calcul numérique

Mots-clés (en français)

- Cryptography
- Cyclic groups
- Elliptic curves
- Discrete logarithm
- Algorithmic complexity
- Numerical computation

Bibliographie commentée

De pars l'essort des flux d'informations sensibles qu'a apporté l'ère numérique, la cryptographe s'est révélée être un domaine essentiel à la sécurité des communications. De plus ces encrytions et décryption se doivent d'être rapides et peu coûteuse à mettre en place.

Un de ces systèmes, introduit en 1984 par Taher Elgamal, le cryptosystème d'ElGamal est un protocole de cryptographie asymétrique largement utilisé et construit sur le problème du logarithme discret. Cet algorithme permet à deux parties d'échanger un message de manière sécurisée en utilisant une paire de clés : une clé publique et une clé privée qui servent, respectivement à encrypter le message et à le décrypter.

En effet les meilleurs algorithmes connus pour résoudre le problème du logarithme discret sur les corps de nombres tels que le crible généralisé ont une complexité sous-exponentielle, tandis que les meilleurs algorithmes connus pour les courbes elliptiques, comme l'algorithme de rho de

Pollard, ont une complexité exponentielle.

C'est pourquoi en 2005 la National Security Agency (NSA) des États-Unis a recommandé l'utilisation de courbes elliptiques pour les systèmes de cryptographie à clé publique, soulignant leur efficacité et leur sécurité accrues par rapport aux méthodes traditionnelles [1].

Le principe de l'encryptage par la méthode d'ElGamal repose donc sur le logarithme discret : il est nettement plus facile de calculer le reste de la division euclidienne que la réciproque de cette opération quand on opère sur un groupe cyclique. Dans le cadre des courbes elliptiques ce groupe utilisé est construit à partir de l'ensemble des points d'une courbe elliptique dans le plan projectif sur lesquels on applique un logarithme et auquels on ajoute un point à l'infini qui va servir de neutre pour la loie de groupe.

Une première approche pour casser cette encryption serait d'essayer toutes les valeurs possibles de la clé privée jusqu'à trouver la bonne, d'opérer en force brute. Cependant, la taille des clés utilisées dans les systèmes modernes rend cette approche impraticable car le nombre de possibilités serait astronomique. Pour des clés de 256 bits, il y aurait 2^{256} possibilités, ce qui est bien au-delà de la capacité de calcul de n'importe quel ordinateur.

Pour réduire les temps de calculs au maximum, nous allons nous intéresser l'algorithme dit du "rho de Pollard" qui est un algorithme probabiliste qui repose sur le paradoxe des anniversaires et de la reconnaissance de cycle dans l'apparition des valeurs. Il est nettement plus efficace pour résoudre le problème du logarithme discret, il permet de trouver la clé privée en un temps approximativement proportionnel à la racine carrée de l'ordre du groupe.

Pour conclure, les courbes elliptiques offrent une sécurité supplémentaire comparé aux groupes cycliques usuels utilisés dans le cryptosystème d'El Gamal. Leur structure mathématique complexe et leur mise en place relativement aisée offre une solution de cryptographie robuste et efficace, adaptée à l'échange de clés de sécurité dans des contextes de confidentialité très variés.

Problématique retenue

En quoi les courbes elliptiques permettent-elles de renforcer la sécurité du cryptosystème d'El Gamal par rapport aux autres groupes cycliques usuels ?

Objectifs du TIPE

- construction de groupes cycliques sur les courbes elliptiques
- mise en place du cryptosystème d'El Gamal sur les courbes elliptiques
- comparaison de différents algorithmes de résolution du problème du logarithme discret
- étude comparative de la sécurité du cryptosystème d'El Gamal sur les courbes elliptiques et sur d'autres groupes cycliques usuels

Références

[1] National Security Agency (NSA). (2005). *The Case for Elliptic Curve Cryptography*. Suite B Cryptography.