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

Liste des membres du groupe

— COMMUNAL Hugo

Positionnements thématiques

— Informatique (Python, informatique théorique, complexité algorithmique)
— Mathématiques (Algèbre, Théorie des groupes, Courbes elliptiques)

Mots-clés (en français)

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

Mots-clés (en anglais)

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

Bibliographie commentée

De par l'essor des échanges d'information sensible qu'a apporté l'ère numérique, la cryptographie s'est révélée être un domaine essentiel à la sécurité des communications. De plus ces chiffrement et déchiffrement se doivent d'être rapides et peu coûteuses à mettre en place.

Un de ces systèmes, introduit en 1984 par Taher Elgamal [1] , le cryptosystème d'ElGamal est un protocole de cryptographie asymétrique largement utilisé et construit sur le problème du logarithme discret [2]. 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.

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 [3] par rapport à la longueur des clés, tandis que les meilleurs algorithmes connus pour les groupes construits sur les courbes elliptiques [4] , comme l'algorithme de rho de Pollard [5] , 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 [6].

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

Une première approche pour casser ce codage 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 calcul au maximum, nous allons nous intéresser à l'algorithme dit du "rho de Pollard" qui est un algorithme probabiliste qui repose sur le paradoxe des anniversaires [7] et de la reconnaissance de cycles dans une suite récurrente. 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 du nombre de bits de l'ordre du groupe, il offre donc une complexité réelle exponentielle. Nous allons donc étudier la sécurité de ce cryptosystème en jouant le rôle d'un attaquant qui cherche à retrouver le message encrypté, nous allons donc comparer le temps que nous mettons à résoudre ce problème mathématique avec plusieurs algorithmes.

Cependant, il est important de noter que la sécurité de ce cryptosystème sera compromis quand des ordinateurs quantiques suffisamment puissants seront développés, car ils pourraient résoudre le problème du logarithme discret en temps polynomial grâce à l'algorithme de Shor.

Pour conclure, les courbes elliptiques offrent une sécurité supplémentaire comparée aux groupes cycliques usuels utilisés dans le cryptosystème origniel d'El Gamal. Leurs structures mathématiques complexes et leur mise en place relativement aisée offrent 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 sont des objets mathématiques indispensables à la cryptographie moderne ?

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] ElGamal, T. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In : Blakley, G.R., Chaum, D. (eds) Advances in Cryptology. CRYPTO 1984. Lecture Notes in Computer Science, vol 196. Springer, Berlin, Heidelberg.DOI

[2] Aude LE GLUHER encadrée par Guénaël RENAULT 22 août 2015Problème du logarithme discret appliqué à la cryptanalyse sur courbes elliptiques : algorithme MOV

[3] Fabrice Boudot, Pierrick Gaudry, Aurore Guillevic, Nadia Heninger, Emmanuel Thomé, et al.. Nouveaux records de factorisation et de calcul de logarithme discret. Techniques de l'Ingénieur, 2021, pp.17. ff10.51257/a-v2-in131ff. ffhal-03045666f URL

[4] Elliptic Curves in cryptography, London Mathematical Society Lecture Notes Series 265, Cambridge university press URL

[5] Handbook of Applied Cryptography, by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996. URL

[6] National Security Agency (NSA). (2005). *The Case for Elliptic Curve Cryptography.* Suite B Cryptography. URL(web archive)

[7] wikipedia Paradoxe des anniversaires