Génération de courbes elliptiques

Motivation:

La sécurité des communications entre systèmes informatiques est de nos jours un enjeu crucial. En cela, la génération de courbes elliptiques présente un intérêt en cherchant à apporter une solution à ce problème en permettant la génération de courbes fiables et sécurisées.

Ancrage:

La cryptographie est avant tout un moyen de communiquer entre individus et systèmes, en cela ce sujet est en lien avec la partie 'interaction' du thème de l'année. Les systèmes cryptographiques utilisés peuvent présenter des failles et vulnérabilités, empêchant ainsi leur bon fonctionnement, ce que l'on relie au mot clé de rupture.

Positionnement thématique (phase 2)

MATHEMATIQUES (Algèbre), INFORMATIQUE (Informatique pratique).

Mots-clés (phase 2)

Mots-Clés (en français)	**Mots-Clés** (en anglais)
Cryptographie	*Cryptography*
Courbes elliptiques	*Elliptic curves*
Algorithmes	*Algorithms*
Sécurité	*Security*
Génération	*Generation*

Bibliographie commentée

La cryptographie est la science de transmettre des messages sans qu'une tierce partie puisse ni les comprendre ni en envoyer, et les méthodes pour atteindre ce résultat n'ont cessées d'évoluer depuis sa création dans l'Antiquité. En particulier la récente invention de la cryptographie asymétrique [1] a permis de développer des systèmes cryptographiques basés sur l'opération d'un groupe cyclique fini G. Ceux-ci fonctionnent de la manière suivante: les deux partis s'accordent d'abord sur le groupe fini G à utiliser, et un générateur g de ce groupe. Ensuite, chacun choisit un nombre aléatoire secret, appelé clé privée, α et β. Ils calculent g^α et g^β, qui sont leur clé publique, et se les échangent. Ils peuvent finalement calculer $g^{(\alpha\beta)}$ chacun de leur côté, qui pourra leur servir de clé de chiffrement secrète pour communiquer de manière sécurisée par la suite.

La sécurité d'un tel système dépend de la difficulté de la résolution du problème du logarithme discret: étant donné un générateur g du groupe et un élément quelconque g^k de G, déterminer k. En particulier, les travaux sur les courbes elliptiques [2] ont montrés que la structure de groupe qu'on peut leur imposer est adaptée à leur utilisation en cryptographie asymétrique, le problème du logarithme discret y étant particulièrement difficile, grâce notamment à leur absence de structure

supplémentaire. Leur utilisation pratique requiert un accord préalable des utilisateurs sur le groupe précis utilisé, qui dépend des paramètres de l'équation de la courbe et de son corps de définition. Ainsi plusieurs standards ont été définis, cherchant chacun à obtenir un niveau de sécurité adapté à leur utilisation. Ces standards ont été créés par des organismes gouvernementaux, et dans d'autres cas par des cryptographes indépendants [3].

La sélection de ces paramètres est toutefois sujette à caution: un choix particulier de paramètres peut donner à celui qui les choisit le moyen de compromettre le système cryptographique, en obtenant par exemple la clé privée des utilisateurs, leur permettant de décrypter leurs transmissions. Ces considérations ont motivé la recherche dans la sélection de ces paramètres, et ce par deux méthodes majeures: la méthode classique dans laquelle on compte les points sur la courbe dont on a déterminé les paramètres, et la seconde dite de "multiplication complexe" [4, 5]. La première méthode est plus adaptée à la génération de courbes que l'on souhaite réutiliser car l'opération de comptage de points, réalisée par l'algorithme de Schoof ou dérivés, prend un temps non négligeable [5]. La seconde méthode consiste à générer des courbes dont on connait le nombre de points par avance, permettant un gain de temps considérable. Ainsi cette dernière méthode est adaptée à la génération de courbes à usage unique: à chaque transmission sécurisée, une nouvelle courbe est générée, utilisée puis oubliée. Ces courbes éphémères ont donc l'avantage d'éliminer le besoin de faire confiance à un organisme de standard, en plus de ne pas être vulnérables aux attaques connues. Cette technique a toutefois un désavantage, celui de restreindre les paramètres de l'équation des courbes générées.

Problématique retenue

Les paramètres d'une courbe elliptique la déterminent entièrement, nous nous attacherons donc à la détermination algorithmique de tels paramètres permettant d'obtenir une courbe sécurisée et fiable.

Objectifs du TIPE

L'objectif de ce TIPE est de créer ou d'améliorer une méthode algorthmique pour générer de nouvelles courbes elliptiques sécurisées et utilisables dans des cas concrets, ceci passant par la compréhension de la théorie des courbes elliptiques et des méthodes utilisées actuellement pour les générer.

Abstract

We first present the basic mathematical framework of elliptic curves and elliptic curve cryptography, and in particular Schoof's point counting algorithm. We then investigate algorithms to generate new elliptic curves suitable for use in cryptographic applications, first through point counting, then through the complex multiplication method. We provide an optimized implementation and comparison of these approaches and in the process, we implement the elements necessary for working with elliptic curves along with tools to ensure their security, based on state-of-the-art requirements.

Références bibliographiques (phase 2)

[1] W. Diffie, M. Hellman : New Directions in Cryptography : *https://www-*

ee.stanford.edu/~hellman/publications/24.pdf, 1976

[2] J. H. Silverman : The Arithmetic of Elliptic Curves : *Springer, ISBN 978-0-387-09494-6, 1986*

[3] D. J. Bernstein : Curve25519: new Diffie-Hellman speed records :
https://cr.yp.to/ecdh/curve25519-20060209.pdf, 2006

[4] H. Baier, J. Buchmann : Generation Methods of Elliptic Curves :
https://www.ipa.go.jp/security/enc/CRYPTREC/fy15/doc/1030_Buchmann.evaluation.pdf, 2002

[5] A. Miele, A. K. Lenstra : Efficient Ephemeral Elliptic Curve Cryptographic Keys :
https://eprint.iacr.org/2015/647.pdf, 2015

DOT

[1] *Compréhension et implémentation des opérations sur les courbes elliptiques*

[2] *Implémentation de l'algorithme d'échange de clés Diffie-Hellman*

[3] *Implémentation d'attaques du problème du logarithme discret*

[4] *Compréhension et implémentation de l'algorithme de Schoof*

[5] *Utilisation de l'algorithme de Schoof pour générer des courbes elliptiques sécurisées*

[6] *Implémentation de la méthode de multiplication complexe*

[7] *Optimisation et comparaison des algorithmes implémentés.*