Vulnérabilités et attaques en cryptographie sur les courbes elliptiques

Dans la société entièrement axée sur le numérique qui se dessine, la sécurisation des transmission informatiques est un enjeu majeur qui passe par l'utilisation de systèmes cryptographiques. La cryptographie sur les courbes elliptiques, notamment utilisée par les cryptomonnaies Bitcoin et Ethereum, est aujourd'hui celle qui prime.

Ces objets mathématiques étant particuliers, cette cryptographie n'a pas les mêmes propriétés que les systèmes l'ayant précédé : cela a capté ma curiosité. On s'attachera à expliquer les vulnérabilités que présentent certaines courbes et à proposer des attaques les exploitant.

Professeurs encadrants du candidat :

Philippe Châteaux

Positionnement thématique (phase 2)

INFORMATIQUE (Informatique Théorique), MATHÉMATIQUES (Algèbre)

Mots-clés (phase 2)

Mots-clés (en français) :	**Mots-clés** (en anglais) :
Cryptographie sur les courbes elliptiques	*Cryptography on elliptic curves*
Cryptanalyse	*Cryptanalysis*
Logarithme discret	*Discrete logarithm*
Courbes elliptiques	*Elliptic curves*
Factorisation d'entiers	*Integer factorization*

Bibliographie commentée

Depuis l'invention de la cryptographie à clef publique en 1976 par Whitfield Diffie et Martin Hellman, de nombreux systèmes cryptographiques à clef publique ont été proposés. Tous ces systèmes se fondent sur la difficulté à inverser une certaine fonction mathématique. Au cours des années, la plupart de ces systèmes ont été cassés ou bien se sont révélés irréalisables. Aujourd'hui trois types de systèmes sont considérés comme à la fois sécurisés et efficaces.

Ces systèmes et les problèmes sur lesquels ils s'appuient sont entre autres : le chiffrement RSA qui repose sur le problème de la factorisation d'entiers (IFP), le chiffrement ElGamal, le *Digital Signature Algorithm* (DSA) ou bien le protocole d'échange de clefs Diffie-Hellman qui sont fondés sur la difficulté du problème du logarithme discret (DLP) [2]. Enfin vient une troisième catégorie de systèmes qui s'appuient eux sur le problème du logarithme discret pour les courbes elliptiques (ECDLP) et qui sont en fait la transposition aux courbes elliptiques de systèmes comme le chiffrement ElGamal, DSA ou le protocole Diffie-Hellman [1].

Il convient de faire remarquer qu'aucun de ces problèmes n'a été prouvé comme étant insoluble. On peut plutôt parler d'un consensus sur le fait qu'ils sont insolubles puisque de nombreuses années de travail intense de mathématiciens et d'informaticiens de renom n'ont pas réussi à produire d'algorithme efficace pour les résoudre [2]. Certains chercheurs expriment des craintes que l'ECDLP n'ait pas été suffisamment approfondi en détail comme par exemple l'IFP, cependant tous ces systèmes, fondés sur la difficulté perçue du problème mathématique auxquels ils sont reliés, vivent dans la crainte d'une percée majeure dans ce domaine [1].

L'étude des courbes elliptiques par les algébristes et les spécialistes de la théorie des nombres remonte au milieu du 19^{e} siècle. En 1984, Hendrik Lenstra décrit un algorithme de factorisation d'entiers reposant sur les propriétés des courbes elliptiques. Cette découverte poussa les chercheurs à explorer d'autres applications en cryptographie et en théorie algorithmique des nombres. La cryptographie sur les courbes elliptiques (ECC) fut découverte en 1985 par Neal Koblitz et Victor Miller [3].

La cryptographie sur les courbes elliptiques est rapidement devenue le système leader dans l'industrie, et a supplanté d'autres cryptosystèmes tels que RSA et DSA, et ce grâce à plusieurs avantages. D'une part, son utilisation permet une augmentation de la vitesse pendant la mise en œuvre, une utilisation de mémoire moindre, un temps de calcul bien inférieur pour la génération des clefs et des tailles de clefs bien plus petites à niveau de sécurité égal [3] [4]. Ce dernier point est d'ailleurs d'autant plus important que la différence de taille augmente drastiquement avec la sécurité demandée [2].

Un autre avantage notable concerne le ECDLP : contrairement à l'IFP, pour lequel un algorithme sous-exponentiel a été trouvé, les meilleurs algorithmes généraux résolvant l'ECDLP sont en temps exponentiel [3]. Cependant, même si l'ECDLP est considéré comme un problème insoluble, cela n'a pas stoppé la recherche d'attaques contre les cryptosystèmes l'utilisant. De nombreuses attaques ont été conçues et testées par des mathématiciens de premier plan au cours des années, dans le but de trouver des vulnérabilités dans ces systèmes. Certaines tentatives furent partiellement réussies, d'autres non [4]. Puisque les meilleurs algorithmes généraux s'attaquant à l'ECDLP sont en temps exponentiel, les attaques ont dû être spécifiques à certaines courbes [5].

Problématique retenue

Il s'agit d'étudier les vulnérabilités des systèmes cryptographiques reposant sur les corps finis et les courbes elliptiques, ainsi que de les exploiter grâce à des attaques idoines.

Objectifs du TIPE du candidat

1. Reproduire et analyser différents algorithmes généraux de test de primalité et de factorisation.
2. Étudier le problème du logarithme discret, coder des algorithmes généraux et tester leurs limites.
3. Implémenter l'algorithme de Schoof pour compter les points d'une courbe elliptique.
4. Établir un système cryptographique simple, repérer des courbes elliptiques vulnérables, et les attaquer avec des algorithmes spécifiques.

Références

[1] F. Blake, Gadiel Seroussi, and Nigel P. Smart. *Elliptic Curves in Cryptography*. Cambridge University Press, 1999.

[2] Certicom Corp. The elliptic curve cryptosystem. `https://citeseer.ist.psu.edu/viewdoc/download?doi=10.1.1.109.6966&rep=rep1&type=pdf`, 1997.

[3] Darrel Hankerson, Alfred Menezes, and Scott Vanstone. *Guide to elliptic curve cryptography*. Springer, 2004.

[4] Santoshi Pote1 and Jayashree Katti. Attacks on Elliptic Curve Cryptography Discrete Logarithm Problem (EC-DLP). `https://ijireeice.com/upload/2015/april-15/IJIREEICE28.pdf`, 2015.

[5] Vanessa Vitse. Attacks on the curve-based discrete logarithm problem. `https://www-fourier.ujf-grenoble.fr/~viva/research/talks/summerschool-vitse.pdf`, 2011.