Mathieu Gestin
Pierrick Heyman
Automne 2020

Rapport TX - Cryptographie à base de courbes elliptiques

Sommaire

Partie 1

Introduction

Les réseaux permettent aux ordinateurs de communiquer entre eux. Néanmoins, aucune sécurité n'est à priori mise en place pour rendre ces échanges confidentiel. Il faut donc définir des méthodes pour permettre à différentes entités de communiquer de façon sûre, sans que ces échanges ne puissent être interceptés par une tierce personne. En effet, il est généralement considéré que toute communication sur un réseau ouvert peut être écouté par une tierce personne, potentiellement mal intentionnée. Pour résoudre ce problème, les différentes applications doivent utiliser des primitives cryptographiques, permetant notamment :

— Le chiffrement ;
— L'authentification ; et
— La signature.

Plusieurs méthodes existent, tels que la primitive RSA, ou AES. Ces primitives sont soit symétriques (les clés pour chiffrer et déchiffrer sont identiques), soit asymétiques (les clés de chiffrement et de déchiffrement sont différentes). Parmis ces méthodes, il existe des systémes reposant sur un objet mathématique spécifique, appelé courbe elliptique, qui, de par ses propriétés, permet de répondre aux contraintes de sécurité posées ci-avant, et ce en limitant la taille des objets manipulés, par rapport à d'autres systèmes.

Partie 2

Préliminaires

Nous allons ici nous référer à des diminutifs pour parler des acteurs de toute transaction réalisée grace à un système cryptographique. Par exemple si deux ordinateurs communiquent sur le réseau, nous allons appelé le premier Alice, et le second Bob. Un potentiel attaquant sera quand à lui nommé Eve.

Partie 3

Hypothèse

Nous allons ici principalement utiliser l'hypothèse du logarithme discret ; Elle stipule que dans un groupe muni d'une loi multiplicative, il est difficile de trouver le logarithme d'un élément. Par exemple, il est facile pour Alice de calculer :

$$y = g^x mod\ n \tag{3.1}$$

Mais la réciproque, soit trouver $x' = x$ tel que :

$$x' = log_g(y) mod\ n \tag{3.2}$$

Est considérée difficile à calculer en un temps polynomial pour tout ordinateur.

L'exemple exposé ci dessus est l'exemple courant, dans des groupes multiplicatifs. Mais nous allons, nous, travailler dans des groupes additifs. Le problème du log discret se transpose alors ainsi : Soit un groupe G d'ordre premier n. Pour $x \in G$ et $k \in_n^*$ connu, il est facile de calculer $y = k * x\ mod\ n$, mais pour x et y connu, il est dur de retrouver k.

La difficulté du problème dépend de la taille de n. Cet élément doit donc être choisi suffisamment grand, pour que les ordinateurs modernes ne puissent casser le chiffrement.

Partie 4

Généralitées sur les courbes elliptiques

Une courbe elliptique (E) est une courbe que l'on peut présenter sous la forme de Weierstrass dite non réduite :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, avec(a, b) \in R^2 \tag{4.1}$$

Sous certaines conditions, on peut simplifier cette équation et la présenter sous la forme :

$$y^2 = x^3 + Ax + B \tag{4.2}$$

Pour pouvoir utiliser une courbe elliptique dans un système cryptographique, il faut pouvoir définir une tangente en tout point de cette courbe, c'est à dire qu'elle soit lisse. Une condition à vérifier pour s'assurer que la courbe soit lisse est que ses deux dérivées partielles soient non nulles. Condition qu'on peut ramener à :

$$4A^3 + 27B^2 \neq 0 \tag{4.3}$$

Où A et B correspondent aux coefficients de l'équation 4.2

L'ensemble des points P de la courbe est l'ensemble sur lequel nous allons travailler. A cet ensemble, nous rajoutons un point, qui va nous servir d'élément neutre, que nous nomerons ∞, et que nous définirons plus tard.

Nous avons donc un nombre fini ou infini de point, défini par une coordonnée en x, et en y, noté (x,y)

Nous ajoutons à cet ensemble une loi de groupe, que nous écrirons +, mais qui diffère d'une addition classique.

4.1 L'addition expliquée graphiquement

Voici les étapes permettant d'additionner deux points P_1 et P_2 :

1. Trouver la droite passant par les deux points P_1 et P_2
2. Trouver le point P' , différent de P_1 et P_2, coupant la courbe E (les cas particulier seront étudier plus tard)
3. Le résultat de la somme est le symétrique de P' par rapport à l'axe des abscisses.

Tout d'abord, cette loi permet d'additionner tous les éléments du groupe entre eux, et de retomber sur un élément du corps, c'est donc une loi de composition interne. Ensuite, la courbe est symétrique par rapport à l'axe des abscisses. La troisième étape nous ramène donc forcément sur un point de la courbe.

Pour ce qui est des cas particuliers, pour faire la somme de deux point identiques, $P_1 + P_1$, on prend la tangente de la courbe en ce point, et puis on réalise les mêmes opérations que précédemment. C'est à dire, on prend le point P', intersection entre la courbe et la tangeante, tel que $P_1 \neq P'$. Le résultat est le symétrique de P' par rapport à l'axe des abscisses.

4.2 L'addition expliquée algébriquement

Voyons comment se passe l'addition de deux points $P(x_p, y_p)$ et $Q(x_q, y_q)$ tels que P + Q = R. Comme précédemment, deux cas sont à prendre en compte ici :

a. Premier cas : $P \neq Q$

P et Q sont deux points distincts de la courbe elliptique. On commence par calculer λ :

$\lambda = \frac{y_q - y_p}{x_q - x_p}$

On peut ensuite calculer les coordonnées du point $R(x_r, y_r)$:

$x_r = \lambda^2 - x_p - x_q$
$y_r = \lambda(x_p - x_r) - y_p$

b. Second cas : $P = Q$

P et Q réprésentent le même point. Comme précédemment, on calcule λ :

$\lambda = \frac{3{x_p}^2 + A}{2y_p}$

Ce qui nous permet ensuite de calculer les coordonnées du point $R(x_r, y_r)$:

$x_r = \lambda^2 - 2x_p$
$y_r = \lambda(x_p - x_r) - y_p$

c. ∞ : L'élément neutre

Un élément est à définir pour pouvoir avoir à faire à un groupe, c'est l'élément neutre de ce groupe, selon la loi de groupe. Nous appelons cette élément, dans le cas des courbes elliptiques, ∞.

Ce point peut se trouver graphiquement comme la somme d'un point de la courbe et de son symétrique par rapport à l'axe des abscisses. En effet, c'est l'un des deux cas ou la courbe passant par deux points de la courbe ne la recoupe pas en un troisième point. On a en effet une droite de type $x = cte$. Cet élément neutre est donc le point que croise cette courbe à l'infini, que ce soit du coté positif, ou négatif. En effet, les deux éléments que l'on voudrait noter $+\infty$ et $-\infty$ sont considérés comme un seul et même point.

Une autre méthode permet d'obtenir l'élément neutre comme résultat de la loi de groupe entre deux points, c'est d'aditionner deux fois le même point, si celui-ci se trouve sur l'axe des abscisses

4.3 Taille d'un groupe

La taille, ou l'ordre, d'un groupe défini ci dessus n'est pas trivial, comme avec RSA, ou le modulo est l'ordre du groupe additif. Ici, il faut compter le nombre de points appartenant à la courbe. Ce nombre peut se calculer avec un algorithme nommé algorithme de schoof.

Il est important de connaitre l'ordre du groupe dans lequel on travail, car la sécurité des courbes utilisées dépend de cet ordre. Il faut, en effet, que l'ordre du groupe soit un grand premier, ou divisible par un grand premier, pour que les algorithmes cryptographiques implémentés soient considérés sécurisés.

Pour ce qui l'ordre d'un point du groupe, ce dernier dépend de l'ordre du groupe. LE théorème de lagrange dit que l'ordre d'un sous groupe divise l'ordre du groupe. Donc, si l'ordre du groupe est premier, tous les points du groupe sont de l'ordre du groupe, à l'exception du point à l'infini (ils sont tous générateurs du groupe). Dans nimporte quel autre cas, il est nécessaire de découposer l'ordre du groupe en facteur premier, et l'ordre du point P est le plus petit facteur premier a pour lequel $aP = 0$.

Partie 5

Utilisation des courbes elliptiques en cryptographie

5.1 Protocole Elliptic Curve Diffie-Hellman (ECDH)

Le but de cette partie est d'expliquer comment deux utilisateurs Alice et Bob vont pouvoir se mettre d'accord sur un secret partagé noté s en utilisant l'algorithme ECDH qui repose sur les courbes elliptiques sans qu'il soit possible pour un attaquant Eve d'intercepter ce secret.

Alice et Bob vont d'abord se mettre d'accord sur différents paramètres qui seront utilisés pour générer ce secret :

— A, B et P qui définiront la courbe $(C) : y^2 = x^3 + Ax + B \mod P$ utilisée

— Un point $G(g_x; g_y)$ de la courbe (C)

5.2 Importance du choix des paramètres

Les paramètres cités précédemment de doivent pas être choisis au hasard. Certaines configurations de courbes elliptiques ne sont pas considérées commes sûres. En effet, la sécurité de la cryptographie en courbes elliptiques repose sur la difficulté de résoudre le problème du logaithme discret. Le choix de certains paramètres peut rendre ce problème plus "facile" et ainsi mettre en péril la sécurité d'une communication. Les attaques possibles ne seront pas détaillées ici.

Différentes organisations telles que le National Institute of Standards and Technology (NIST, USA) ou l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSII, France) mettent à disposition du public des configurations de courbes elliptiques considérées comme sûres.

5.3 Calcul du secret partagé

Ces paramètres sont publics, Eve peut les intercepter sans que cela n'ait d'importance pour la sécurité de la communication.

Ayant connaissance de ces paramètres, Alice et Bob vont respectivement choisir un nombre aléatoire k_{alice} et k_{bob} tels que $k_{alice} < P-1$ et $k_{bob} < P-1$. Ces deux nombres constitueront leurs clés privées respectives. Ces clés sont la garantie de la sécurité de la communication à venir, elles doivent rester secrètes.

Alice et Bob vont ensuite générer leurs clés publiques respectives en utilisant leurs clés privées respectives de la manière suivante :

— $pub_{alice} = k_{alice} * G$

— $pub_{bob} = k_{bob} * G$

Comme nous l'avons vu précédemment, ce calcul est dit "facile", cependant retrouver k_{alice} et k_{bob} à partir de G et pub_{alice} pub_{bob} est difficile (problème du logarithme discret). Ces clés publiques sont comme leur nom l'indique publiques. Alice et Bob vont se les échanger sur un canal non sécurisé. On peut imaginer qu'Eve parvienne à intercepter cet échange de clés et a donc connaissance de pub_{alice} et pub_{bob}.

Après cet échange, Alice et Bob vont respectivement calculer s de la manière suivante :

— $s_{alice} = k_{alice} * pub_{bob}$

— $s_{bob} = k_{bob} * pub_{alice}$

En décomposant s_{alice} et s_{bob}, on obtient :

— $s_{alice} = k_{alice} * pub_{bob} = k_{alice} * k_{bob} * G$

— $s_{bob} = k_{bob} * pub_{alice} = k_{bob} * k_{alice} * G$

Comme vu précédemment, la multiplication est commutative sur l'ensemble utilisé, on a donc $s_{alice} = s_{bob} = s$. Alice et Bob ont donc chacun en leur possession un secret partagé s. s étant un point de la courbe, le secret partagé est son abscisse.

5.4 Interception des messages

Eve qui a intercepté leur communication ne connait que pub_{alice}, pub_{bob} et les paramètres de la communication détaillés en 5.1. Pour connaître s, il faudrait qu'Eve connaisse k_{alice} et k_{bob}. Le seul moyen d'y arriver à partir des informations qu'elle a interceptées est de résoudre le problème du logarithme discret sur pub_{alice} et pub_{bob} ce qui est excessivement long si les paramètres de la communication ont été bien choisis.

Partie 6

Robustesse et longueur de clé

L'algorithme de chiffrement asymétrique majoritairement utilisé à l'heure actuelle est l'algorithme RSA. Il est utilisé dans de nombreux domaines tels que la sécurisation des communications web, les cartes bancaires ou l'échange de clés de chiffrement symétriques.

La sûreté d'une clé de chiffrement repose en partie sur sa taille (exprimée en bits), plus la taille est importante, plus la sûreté offerte est élevée. En fonction de l'utilisation, une clé RSA peut être considérée comme sûre. A l'heure actuelle c'est le cas si elle fait 2048 bits ce qui pose des problèmes fonctionnels. En effet, plus une clé est grande, plus la puissance de calcul nécessaire pour effectuer le chiffrement/déchiffrement d'une information en un temps donné est importante. Cette puissance supplémentaire est certes peu perceptible sur des machines telles que nos ordinateurs aujourd'hui mais est problématique dans des supports avec très peu de ressources embarquées tels que les cartes bancaires. De plus, une grande clé demande un plus grand espace de stockage. Une autre contrainte est le calcul. En effet, tous les processeurs ne sont pas capables de manipuler d'aussi grands nombres et il faut également composer avec la taille des registres.

La cryptographie en courbes elliptiques résout ces problème en proposant une sécurité équivalente pour une taille de clé inférieure. En effet d'après le NIST une taille de clé de 2048 bits utilisant RSA offre une sécurité équivalente à une clé de 224 bits en utilisant les courbes elliptiques.

Il faut tout de même rappeler qu'en terme de nombre d'opérations, seule une analyse poussée des algorithmes utilisés peut mesurer l'efficacité réelle. Et étant donné que les algorithmes utilisés sur des corps discrets, et sur des courbes elliptiques sont différents, la comparaison n'est jamais triviale.

On compare souvent le niveau de sécurité apporté par une primitive cryptographique à son équivalent en cryptographie symétrique, notamment par rapport aux tailles de clés de l'algorithme AES. Nous proposons ici une comparaison

RSA-ECC-AES :

Security level (AES key size)	RSA key size	ECC key size
80	1024	160
128	3072	256
192	7680	384
256	15360	512

TABLE 6.1: Comparaison du niveau de sécurité en fonction de la taille de la clé de chiffrement

Partie 7

Conclusion

Ce projet nous a permis de mieux comprendre l'utilité et l'utilisation de la théorie des courbes elliptiques dans le domaine de la cryptographie. Les propriétés mathématiques de ces courbes en font d'excellents outils cryptographiques, les atouts principaux étant la robustesse en comparaison à la taille de clé de chiffrement et la possibilité de partager une clé symétrique de chiffrement via un canal non sûr. L'utilisation de ces outils est appelée à se démocratiser au vue des standards de sécurité qui sont en constante augmentation.