Cryptographie à clé publique

Abdelhakim CHILLALI

Une des notions les plus couramment utilisées dans les crypto systèmes à clé publique est celle de logarithme discret(LD).

La cryptographie est aujourd'hui au cœur du développement des nouvelles technologies de l'information et de la communication.

En effet, le besoin d'assurer la confidentialité, l'authentification, l'intégrité des données, l'efficacité et la non-répudiation, se fait sentir dans un très grand nombre d'applications : commerce électronique, réseaux mobiles. . .

Le principe de ces crypto systèmes est de rendre possible la publication de la clef de chiffrement, tout en gardant secrète la clef de déchirement. Un système cryptographique est la donnée d'un 5-uplet (P, C, K, E, D) vérifiant :

1) P est un ensemble fini de blocs de texte clairs possibles.

2) C est un ensemble fini de blocs de texte chiffrés possibles.

3) K que l'on appelle espace des clefs est un ensemble fini de clefs possibles.

4) $\forall k \in K$, il existe une fonction de chiffrement e_k et une fonction de déchiffrement d_k avec :

$$e_k : P \to C$$
$$m \mapsto c = e_k(m)$$

$$d_k : C \to P$$
$$c \mapsto m = d_k(c)\ '$$

et $d_k \circ e_k(m) = m$; $\forall\, m$ texte clair de P.

L'échange de clé de Diffie-Hellman a été développé par ces deux auteurs en 1976 et publié dans l'article : W. Diffie and M. E .Hellman, New directions in cryptography, IEEE Transactions on Information Theory 22 (1976), 644-654. La méthode d'échange de clé de Diffie-Hellman repose sur la difficulté du problème du logarithme discret (PLD). Un groupe cyclique public G est fixé ainsi qu'un générateur public g de ce groupe. Ali et Omar vont construire une clé commune k, pour cela Ali choisit un entier n plus petit que l'ordre de G, de même Omar choisit un entier m plus petit que l'ordre de G. Ali calcule g^n et le transmet à Omar qui calcule g^m et le transmet à Ali. En fin, Ali et Omar calculent leur clé secrète $k = g^{nm}$. On remarque que si on savait résoudre facilement le (PLD), ce système n'aurait aucune sécurité.

Dans un contexte cryptographique, nous nous intéressons à des courbes définies sur un corps fini $\mathbb{F}_p$ et le groupe associé à la courbe est sa jacobienne. La sucées des courbes elliptiques dans les systèmes cryptographiques à clés publiques a donc crée un nouvel intérêt dans l'´étude de l'arithmétique d'objets géométriques. Le groupe des points d'une courbe elliptique est un groupe intéressant en cryptographie dans la mesure où on ne connait aucun algorithme sous-exponentiel pour son (PLD). En général, le PLD est difficile, mais pas autant que dans un groupe générique. On

connait des algorithmes sous-exponentiel pour le résoudre, ceci a des conséquences sur la taille du groupe à utiliser de manière à ce que le PLD soit infaisable. Le nombre premier p doit avoir au minimum 1024 bits, ce qui assure à peu près la même sécurité qu'un groupe générique d'ordre ayant 160 bits.

Ce cours est une introduction à l 'arithmétique des courbes elliptiques appliquée à la cryptographie, il est composé de trois chapitres.

1. **Le chapitre(1): Rappel sur les corps finis**
    a. **Caractéristique**
    b. **Construction des corps finis**
    c. **Le groupe multiplicatif**
    d. **Nombre de polynômes irréductibles sur $\mathbb{F}_p$**
    e. **Représentation des éléments d'un corps fini**

2. **Le chapitre(2): Introduction sur les courbes elliptiques**
    a. **Le plan projectif**
    b. **Définition D'une Courbe Elliptique sur un corps K**
    c. **Loi de groupe explicite**
    d. **Exemples**

3. **Le chapitre(3): Crypto système à clé publique**
    a. **Fonction à sens unique**
    b. **Exemples**
    c. **Cryptographie**
        i. **Principe de Diffie-Hellman**
        ii. **Algorithmes pour résoudre le problème du Logarithme discret**
            1. **Algorithme Naïf**
            2. **Algorithme Pas de bébé, Pas de géant**