PIER – Recherches bibliographiques sur les courbes elliptiques

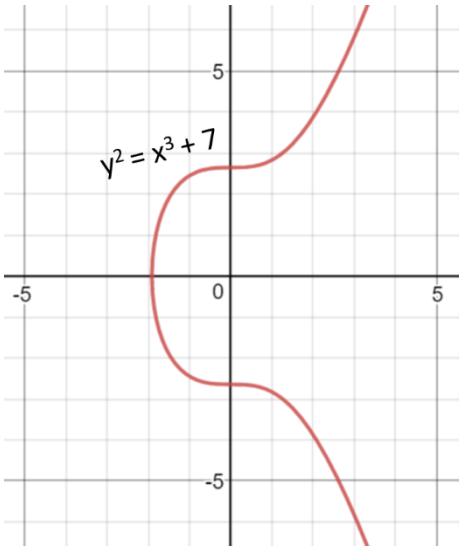
Laurent Signac – CC-BY-SA – 13-10-21 2312 a650a3568db98eda9ce6

Il existe essentiellement deux familles d'algorithmes cryptographiques : les méthodes de chiffrement symétriques, et les méthodes de chiffrement asymétriques. Ces dernières, inventées dans les années 70, permettent à deux correspondants de chiffrer des messages sans avoir à échanger de clé de chiffrement. Elles sont aussi utilisées en signatures numériques. Employées dans de très nombreux contextes (chiffrement du protocole http, paiement par cartes bancaires, blockchain, pass sanitaires…), les deux méthodes asymétriques les plus employées sont RSA et les méthodes à base de courbes elliptiques.

L'objectif de ce travail, essentiellement bibliographique (avec un peu de programmation éventuellement), est d'exposer le mode de fonctionnement de la cryptographie à base de courbes elliptiques, de donner des informations factuelles et techniques sur les bonnes pratiques (types de courbes les plus utilisées, taille conseillée des nombres etc.) et enfin de lister les pièges à éviter dans les implémentations (mauvaise génération de nombres aléatoires…)

Ce travail devra aborder à la fois les problèmes de chiffrement (ECC) et de signature (ECDSA) et comporter des exemples reproductibles (manuellement ou avec un programme informatique).

Il est envisageable d'appuyer le travail sur l'analyse de la signature électronique utilisée dans le pass sanitaire européen, ou encore dans les transactions bitcoin.



Pour avoir plus d'informations sur ce sujet, merci de prendre contact avec Laurent Signac.