D34: Méthodes de calcul efficaces et sécurisées

Introduction

Nicolas Méloni

Master 2: 1er semestre
(2014/2015)

Introduction

Objectifs du cours

- Se familiariser avec l'arithmétique multiprécision
- Implanter efficacement les primitives cryptographiques
- Savoir Se protéger des attaques classiques (Y. Téglia)

El Gamal sur les courbes elliptiques

Le cryptosystème

Soit $\mathbb{K}$ un corps ($\mathbb{K} = \mathbb{F}_p$ ou $\mathbb{F}_{2^n}$). Soient $E(\mathbb{K}$ une courbe elliptique, P un point d'ordre n, $Q \in < P >$ et k un entier et $Q = [k]P$. On définit:

$$\begin{aligned} \mathcal{P} &= E(\mathbb{K}) \\ \mathcal{C} &= E(\mathbb{K}) \times E(\mathbb{K}) \\ K_{pub} &= (E(\mathbb{K}), P, Q) \\ K_{sec} &= k \end{aligned}$$

El Gamal sur les courbes elliptiques

Chiffrement

So it $M \in E(\mathbb{K})$,

$$E(K_{pub}, M) = (P_1, P_2)$$

où $P_1 = [r]P, P_2 = M + [r]Q$ et r est un entier généré aléatoirement.

Déchiffrement

Le chiffré est $C = (P_1, P_2)$,

$$D(K_{sec}, C) = P_2 - [k]P1.$$

Besoin en arithmétique

Opération principale

Calcul de $[a]T$ où $a \in \mathbb{N}$ et $T \in E(\mathbb{K})$

Besoins

- Algorithme d'exponentiation/multiplication de points: $[k]P = P + P + \cdots + P$
- Arithmétique de la courbe: $P + Q$
- Arithmétique de corps finis: $\lambda = \frac{y_1 - y_2}{x_1 - x_2} \mod p$
- Addition/multiplication/division multiprécision

Plan du cours

Représentation multiprécision

- Mutiplication classique
- Algorithme de Karatsuba
- Algorithme de Toom-Cook
- Algorithme de Schonhage et Strassen

Plan du cours

Arithmétique dans $\mathbb{F}_p$

- Réduction modulaire
- Multiplication modulaire de Montgomery
- Nombre de Mersennes généralisés
- Residue Number System

Plan du cours

Arithmétique dans $\mathbb{F}_{2^n}$

- Addition/multiplication classiques
- Produit matrice-vecteur
- Bases normales

Plan du cours

Exponentiation modulaire

- Square-and-multiply
- Algorithme de Brauer
- Non-Adjacent-Form
- Sliding Windows
- Multi-exponentiation

Plan du cours

Arithmétique des courbes elliptiques

- Loi de groupe sur $\mathbb{F}_p/\mathbb{F}_{2^n}$
- Choix des coordonnées
- Courbes de Montgomery
- Courbes de Koblitz
- Half-and-add