

Introduction to ECC

Nigel Smart

nigel@cs.bris.ac.uk

January 27, 2009

Why the need for Elliptic Curves?

Basics on Elliptic Curves

The Group Law

Why the need for Elliptic Curves?

Discrete logarithm problem example

Let $p =$

10535462803950169753046165829339587319488718149259
 13489342608734258717883575185867300386287737705577
 93738292587376245199045043066135085968269741025626
 82711472830348975632143002371663691740666159071764
 72549470083113107138189921280884003892629359

NB: $p = 158(2^{800} + 25) + 1$ and has 807 bits.**Problem:**Find $\lambda \in \mathbb{Z}$ such that

$$2 \equiv 3^\lambda \pmod{p}.$$

Discrete logarithm problem

Let p and L be large primes such that $L|(p-1)$.The multiplicative group of integers modulo p contains an element g of order L .**The discrete logarithm problem:**Suppose $h \in \mathbb{Z}_p^*$ also has order L .Find $\lambda \in \mathbb{Z}$ such that

$$h \equiv g^\lambda \pmod{p}.$$

One-way function:Fast to compute g^λ but difficult to compute λ .

Generalisation of DLOGs

Can take any (finite) group.

Bad Choices:

- ▶ Additive group \mathbb{Z} or \mathbb{F}_q .
- ▶ Multiplicative group of or \mathbb{C} .

Apparently Good Choices:

- ▶ Finite fields \mathbb{F}_q^* .
- ▶ Elliptic curves over finite fields.
- ▶ Ideal class groups of number fields.
- ▶ Jacobian varieties of curves over finite fields.

Subexponential Algorithms

For factoring and the discrete logarithm problem in finite fields \mathbb{F}_q^* there are **index calculus** algorithms.

These have subexponential complexity

$$O(\exp(c(\ln N)^{1/3}(\ln \ln N)^{2/3})).$$

For solving the discrete logarithm problem in class groups and Jacobians of curves of sufficiently high genus there are index calculus algorithms of subexponential complexity

$$O(\exp(c(\ln N)^{1/2}(\ln \ln N)^{1/2})).$$

Basics on Elliptic Curves

Elliptic Curves

An elliptic curve over a field K is non-singular curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_1, a_2, a_3, a_4, a_6 \in K$.

From these constants we define

$$\begin{aligned} b_2 &= a_1^2 + 4a_6, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

Elliptic Curves

A curve is called non-singular if it has no singularities.

- Essentially the "curve" does not cross or intersect itself.

This is easy to detect since the "discriminant" Δ will be zero if the curve is singular

$$\Delta = -b_2^2 b_6 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6.$$

Think of this as related to the discriminant of a polynomial, which is zero when the polynomial has repeated roots.

The curve is considered to be the set of solutions to the equations, plus

- An additional special point at infinity \mathcal{O}_E .

This is considered to lie infinitely far up the y -axis.

Elliptic Curves

Two curves E and E' are isomorphic over K if there is a bi-rational map between them which preserves the point at infinity.

Two curves with variables X, Y and X', Y' are isomorphic over K if there are constants $r, s, t \in K$ and $u \in K^*$, such that the change of variables

$$X = u^2 X' + r, \quad Y = u^3 Y' + su^2 X' + t \quad (1)$$

transforms E into E' .

Two most used cases are

- Characteristic p : $K = \mathbb{F}_p$, p a large prime
- Characteristic 2: $K = \mathbb{F}_{2^m}$.

Elliptic Curves: Char p

In char p all curves are isomorphic to one of the form

$$E_{A,B}: Y^2 = X^3 + AX + B,$$

in which case we have

$$\Delta = -64A^3 - 432B^2.$$

Two curves in this form $E_{A,B}$ and $E_{A',B'}$ are isomorphic over K if

$$A' = u^4 A \text{ and } B' = u^6 B \text{ for } u \in K^*.$$

Elliptic Curves: Char p

If $-3/A$ is a fourth root in K^* then we can replace $E_{A,B}$ by the curve

$$E_{-3,B'}: Y^2 = X^3 - 3X + B',$$

which will provide a lot of efficiency gains later.

- In practice it is rare to choose $A \neq -3$ for cryptography.

The value $-3/A$ will be a fourth root

- 25 percent of the time when $p \equiv 1 \pmod{4}$.
- 50 percent of the time when $p \equiv 3 \pmod{4}$.

Elliptic Curves: Char 2

In char 2 all curves are isomorphic to one of the form

$$E_{A,B}: Y^2 + XY = X^3 + AX^2 + B,$$

where $A \in \{0, \gamma\}$ where γ is a fixed element in B of trace one.

In which case we have

$$\Delta = B.$$

Note for later, the number of elements in $E_{A,B}(K)$ is divisible by 4 if the trace of A is zero, and divisible by 2 otherwise.

Since we want curves with small cofactor and we usually choose fields of odd exponent, e.g. $K = \mathbb{F}_{2^m}$ where p is prime it is common to select

$$A = 1,$$

since this aids efficiency.

Elliptic Curves As Groups

$$E(K) = \{\text{points } (x, y) \in K^2\} \cup \{\mathcal{O}_E\}.$$

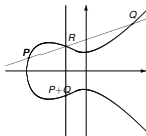
Point Addition

There is a process which, given two points (x_1, y_1) and (x_2, y_2) , gives a third point (x_3, y_3) .

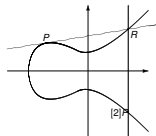
This addition process makes the set $E(K)$ an Abelian group with identity \mathcal{O}_E .

- An Abelian group is what you need for a lot of crypto protocols.

Adding two points on an elliptic curve



Doubling a point on an elliptic curve



Addition Formulae

We can write down formulae for the addition law

- ▶ Hence, can compute with the addition law

This can be done with the general equation in any characteristic.

We shall give the simplifications in the two main cases.

Addition Formulae: Char p

Suppose we are in characteristic p

$$E: Y^2 = X^3 + AX + B$$

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E .

Negation in group law is given by

- ▶ $-P_1 = (x_1, -y_1)$.

Addition Formulae: Char p

Suppose

$$P_3 = (x_3, y_3) = P_1 + P_2$$

then

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2, \\ y_3 &= (x_1 - x_2)\lambda - y_1. \end{aligned}$$

where when $x_1 \neq x_2$ we set

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},$$

and when $x_1 = x_2$ and $y_1 \neq 0$ we set

$$\lambda = \frac{3x_1^2 + A}{2y_1}.$$

Addition Formulae: Char 2

Suppose we are in characteristic 2

$$E: Y^2 + XY = X^3 + AX^2 + B$$

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on E .

Negation in group law is given by

- ▶ $-P_1 = (x_1, y_1 + x_1)$.

Addition Formulae: Char 2

Suppose

$$P_3 = (x_3, y_3) = P_1 + P_2$$

then

$$\begin{aligned} x_3 &= \lambda^2 + \lambda + A + x_1 + x_2, \\ y_3 &= (x_1 + x_2)\lambda + x_3 + y_1. \end{aligned}$$

where when $x_1 \neq x_2$ we set

$$\lambda = \frac{y_2 + y_1}{x_2 + x_1},$$

and when $x_1 = x_2 \neq 0$ we set

$$\lambda = \frac{x_1^2 + y_1}{x_1}.$$

Cost of Addition Formulae: Char p

Point Addition:

- ▶ 6 Field Additions (Trivial)
- ▶ 3 General Field Multiplications
- ▶ 1 Field Inversion

Point Doubling:

- ▶ 5 Field Additions (Trivial)
- ▶ 2 Scalar/Field Multiplications (Trivial)
- ▶ 4 General Field Multiplications
- ▶ 1 Field Inversion

Cost of Addition Formulae: Char 2

Point Addition:

- ▶ 9 Field Additions (Trivial)
- ▶ 1 Field squaring (Trivial in Char 2)
- ▶ 2 General Field Multiplications
- ▶ 1 Field Inversion

Point Doubling:

- ▶ 8 Field Additions (Trivial)
- ▶ 2 Field squaring (Trivial in Char 2)
- ▶ 2 General Field Multiplications
- ▶ 1 Field Inversion

Note point doubling requires fewer multiplications than in the char p case.

The ECDLP

Given $P = (x, y)$ and an integer n we can efficiently compute

$$nP = \underbrace{(x, y) + (x, y) + \dots + (x, y)}_{n \text{ times}}$$

using the **double-and-add** method.

The **Order** of the point P is the smallest number $L > 0$ such that

$$LP = \mathcal{O}_E.$$

Assume that L is a 'large' prime.

ECDLP

Suppose that $Q = (x', y')$ is some other point of order L .

Then there is some number λ such that

$$Q = \lambda P.$$

The **ECDLP** is to find this number λ .

- ▶ This problem is believed to be **hard**.
- ▶ This gives a **one way function**.

It is believed in general that the best algorithm to solve this problem takes time

$$\mathcal{O}(\sqrt{L}).$$

i.e. fully exponential complexity.

It is common to design ECC systems according to the following software stack.

- ▶ This also helps in understanding the relatively places of different design decisions
- ▶ However, in choices made in one layer can effect another.

Cryptographic Protocols

Point Multiplication

Point Addition

Finite Field Arithmetic