
ELLIPTIC CRYPTOGRAPHY

CIS 400/628 — Spring 2005
Introduction to Cryptography

This is based on Chapter 15 of Trappe and Washington and Chapter IV of “A Course in Number Theory and Cryptography,” by Neal Koblitz, Springer 1987.

GROUP RECAP

A group G :

▶ Set of elements (finite or infinite)

▶ Binary operation $*$

▶ Four properties ($\forall A, B, C \in G$):

Closure: $A * B \in G$.

Associativity: $(A * B) * C = A * (B * C)$

Identity: $\exists I \ni I * A = A * I = A$ for **every** element $A \in G$.

Inverse: $\exists A^{-1} \ni A * A^{-1} = A^{-1} * A = I$

▶ Is the set of integers a group?

▶ Is the set of integers mod a prime a group?

▶ Is the set of integers mod 26 a group?

▶ An **Abelian** group has $A * B = B * A \quad \forall A, B \in G$

FIELD RECAP

Take an Abelian Group under both Addition and Multiplication:

$$a + b = b + a$$

$$ab = ba$$

$$(a + b) + c = a + (b + c)$$

$$(ab)c = a(bc)$$

$$a + 0 = a = 0 + a$$

$$a * 1 = a = 1 * a$$

$$a + (-a) = 0 = (-a) + a$$

$$aa^{-1} = 1 = a^{-1}a \text{ if } a \neq 0$$

And add Distributivity:

$$(b + c) = ab + ac$$

$$(a + b)c = ac + bc$$

This is now a field.

CHARACTERISTIC OF A FIELD

The **Characteristic** of a field F , sometimes written $\text{ch}(F)$, is defined as follows:

▶ Call the multiplicative identity 1 .

▶ Consider the numbers:

$$2 = 1 + 1$$

$$3 = 1 + 1 + 1$$

...

▶ If these are all different, then $\text{ch}(F) = 0$.

▶ If two of them are the same, then for some number p ,

$$\underbrace{1 + 1 + \cdots + 1}_{p \text{ times}} = 0.$$

▶ The smallest p fulfilling this condition is $\text{ch}(F)$ (and is prime).

ELLIPTIC CURVES

Definition

An **elliptic curve** E over a field F is a curve given by an equation of the form:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

where $a_1, \dots, a_6 \in F$.

If $\text{ch}(F) \neq 2, 3$, then this can be simplified to:

$$Y^2 = X^3 + aX + b$$

where $a, b \in F$.

See pictures on the board

WHY ARE ELLIPTIC CURVES COOL?

- ▶ There are abelian groups hiding in these curves that are very similar to $\mathbb{Z}_{p^k}^*$.
- ▶ There are a “**lot more**” elliptic curves than $\mathbb{Z}_{p^k}^*$ ’s.
- ▶ You can build cryptosystems based on E.C.’s that require much smaller key length (e.g., **4096 bits vs. 313 bits**) for similar security.
- ▶ They played a key role in Wiles’ proof of Fermat’s Last Theorem.

ELLIPTIC CURVES: ADDITION RULES

- ▶ The curves always include a point at ∞ , where $\infty = -\infty$.
∴ The curves are really on a torus/doughnut.
- ▶ The curves are symmetric around the x-axis.
- ▶ $P_1 + P_2 = P_3$.
 1. Draw a line through P_1 and P_2 . (If $P_1 = P_2$, use the tangent line.)
 2. The line hits the curve at a unique third point Q .
 3. Let P_3 be the point symmetric to Q on the other side of the x-axis.
- ▶ **Note:** $P_1 + \infty = P_1$. (∴ ∞ acts like 0.)
- ▶ **Fact:** $P + Q + R = \infty$ iff P , Q , and R are co-linear.

See the pictures on the board.

ELLIPTIC CURVES: ADDITION RULES, CONTINUED

Addition Rules (Algebraic)

Suppose

$$E : Y^2 = X^3 + aX + b$$

$$P_1 = (x_1, y_1)$$

$$P_2 = (x_2, y_2)$$

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

$$x_3 = m^2 - x_1 - x_2$$

$$y_3 = m \cdot (x_1 - x_3) - y_1$$

$$m = \begin{cases} (y_2 - y_1)/(x_2 - x_1), & \text{if } P_1 \neq P_2 \\ (3x_1^2 + a)/(2y_1) & \text{if } P_1 = P_2 \end{cases}$$

(If $m = \infty$, then $P_3 = \infty$.)

Facts: $(P + Q) + R = P + (Q + R)$ and $P + Q = Q + P$.

ELLIPTIC CURVES MOD N

Consider

$$E : y^2 = x^3 + 2x + 3 \pmod{5}.$$

$$\begin{aligned} E &= \{ (x, y) \in (\mathbb{Z}_5 \times \mathbb{Z}_5) \cup \{ (\infty, \infty) \} \mid y^2 \equiv x^3 + 2x + 3 \pmod{5} \} \\ &= \{ (1, 1), (1, 4), (2, 0), (3, 1), (3, 4), (4, 0), (\infty, \infty) \} \end{aligned}$$

Point Arithmetic: $(1, 4) + (3, 1) = ?$.

Since $(1, 4) \neq (3, 1)$,

$$m = \frac{y_2 - y_1}{x_2 - x_1} \equiv \frac{1 - 4}{3 - 1} \equiv 2 \cdot 2^{-1} \equiv 1 \pmod{5}.$$

$$x_3 \equiv m^2 - x_1 - x_2 \equiv 1^2 - 1 - 3 \equiv 2 \pmod{5}.$$

$$y_3 \equiv m \cdot (x_1 - x_3) - y_1 \equiv 1 \cdot (1 - 2) - 4 \equiv 0 \pmod{5}.$$

$\therefore (1, 4) + (3, 1) = (2, 0)$.

ELLIPTIC CURVES MOD N, CONTINUED

How many points are there on an curve mod m ?

Hasse's Theorem

Let \mathbb{F}_q be a finite field with q elements. (E.g., $\mathbb{F}_p = \mathbb{Z}_p$.)

Suppose E over \mathbb{F}_q has N points. Then:

$$|N - q - 1| < 2\sqrt{q}$$

which means

$$(q + 1) - 2\sqrt{q} < N < (q + 1) + 2\sqrt{q}$$

which in turn means there are **enough to make trouble**.

Schoof's Algorithm

Given E.C. E over \mathbb{F}_q , one can find $|E|$ in $O((\log_2 q)^8)$ time.
(There are faster algs for special cases.)

ELLIPTIC CURVES MOD N, CONTINUED

The Classical Discrete Log Problem

Given β , α , and $p \ni \beta \equiv \alpha^k \pmod{p}$. Find k .

The Discrete log problem for Elliptic Curves mod m

Suppose A & B are points on $E \pmod{n} \ni$

$$B = k \cdot A \stackrel{\text{def}}{=} \underbrace{A + \cdots + A}_{k \text{ many}} \text{ in } \mathbb{F}_q.$$

Find k . (For E.C.'s $+$ is analogous to $\times \pmod{p}$.)

Innuendo

The known algorithms for solving the E.C.-discrete log problem are **even worse** than the ones for the classical problem.

(Good news for Crypto.)

Factoring and Primality Testing with E.C.s

See text.

RECALL: QUADRATIC RESIDUES

We want to solve equations like:

$$x^2 \equiv b \pmod{n}$$

There may not be a solution. E.g., $x^2 \equiv 3 \pmod{5}$, since

$$1^2 = 1 \equiv 1 \pmod{5}$$

$$2^2 = 4 \equiv 4 \pmod{5}$$

$$3^2 = 9 \equiv 4 \pmod{5}$$

$$4^2 = 16 \equiv 1 \pmod{5}$$

DEFINITION Suppose $a \in \mathbb{Z}_p^*$, where p is a prime.

We say that a is a **quadratic residue mod p** when

$$x^2 \equiv a \pmod{p}$$

has a solution, otherwise we say that a is a **nonresidue**.

FACT: $|\{x \in \mathbb{Z}_p^* \mid x \text{ is a quad. res.}\}| = (p - 1)/2.$

RECALL: EULER'S CRITERION

THEOREM

Suppose $a \in \mathbb{Z}_p^*$ where p is prime.

a is a quadratic residue mod p iff $a^{(p-1)/2} \equiv 1 \pmod{p}$.

PROPOSITION

Suppose p is a prime and $p \equiv 3 \pmod{4}$.

Let $y \in \mathbb{Z}_p^*$ and $x = y^{(p+1)/4} \pmod{p}$.

Then either

- ▶ y is a quadratic residue with roots $\pm x$ or
- ▶ $-y$ is a quadratic residue with roots $\pm x$.

REPRESENTING PLAINTEXT ON E.C.'S

Finding points on a given E.C.

There is no known deterministic poly-time algorithm for this.

However, there are reasonably fast probabilistic methods
(that have a certain probability of failure).

Koblitz's Method All of the following will be public

- ▶ Suppose p is a prime with $p \equiv 3 \pmod{4}$ (Why?)
and that $E : y^2 = x^3 + ax + b$ is the E.C. in question.
- ▶ Pick K so that $1/2^K$ (the failure bound) is tolerably small.
- ▶ Messages will be from $\{ m \in \mathbb{Z}_p \mid m < \frac{p-K}{K} \}$. Let m be a message.
- ▶ For $j = 0, \dots, K - 1$:
Set $x_j = m \cdot K + j$ & $w_j = x_j^3 + ax_j + b$ & $z_j = w_j^{\frac{p+1}{4}} \pmod{p}$.
If $z_j^2 = w_j$, then (x_j, z_j) is the point on E that will encode m .
Else we have $z_j^2 = -w_j$ (Why?) and we keep on.
If no j works, report **failure**. Prob. of failure $\leq 2^{-K}$. (Why?)
- ▶ If (x, y) on E encodes a message m , then $m = \lfloor x/K \rfloor$.

THE EL GAMAL CRYPTOSYSTEM FOR E.C.'S

“Classical”

Bob Chooses

p , prime public
 $\alpha \in \mathbb{Z}_p^*$, prim. elm. public
 $a \in \mathbb{Z}$ private
 $\beta = \alpha^a \pmod{p}$ public

Alice with message x

Chooses $k \stackrel{\text{ran}}{\in} \mathbb{Z}_{p-1}$
Computes $y_1 \equiv \alpha^k \pmod{p}$
Computes $y_2 \equiv x\beta^k \pmod{p}$
Sends (y_1, y_2)

Bob

Computes
 $x \equiv y_2 \cdot y_1^{-a} \pmod{p}$.

Elliptic Curve

Bob Chooses

$E \pmod{p}$, p prime public
 $e = |E|$, public
 $\alpha \in E$ public
 $a \in \mathbb{Z}$ private
 $\beta = a \cdot \alpha$ public

Alice with message m

$m \mapsto P$, a point on E
Chooses $k \stackrel{\text{ran}}{\in} \mathbb{Z}_{e-1}^*$
Computes $y_1 = k \cdot \alpha$
Computes $y_2 = P + k \cdot \beta$
Sends (y_1, y_2)

Bob

Computes $P = y_2 - a \cdot y_1$
Extracts m from P

DIFFIE-HELLMAN ON ELLIPTIC CURVES

Setup

$E : y^2 \equiv x^3 + ax + b \pmod{p}$ with e points
 G , a point on E

Public
Public

Alice

Chooses $n_a \stackrel{\text{ran}}{\in} \mathbb{Z}_{e-1}^*$.
Sends $n_a \cdot G$ to Bob.

Private

Bob

Chooses $n_b \stackrel{\text{ran}}{\in} \mathbb{Z}_{e-1}^*$.
Sends $n_b \cdot G$ to Alice.

Private

Alice

Computes $K_{ab} = n_a \cdot (n_b \cdot G) = n_a \cdot n_b G$.

Bob

Computes $K_{ab} = n_b \cdot (n_a \cdot G) = n_a \cdot n_b G$.

EL GAMAL SIGNATURES ON E.C.'S

Alice's Setup

Chooses an E.C. $E \pmod{p}$, where p is a prime.

public

Chooses A , a point on E .

public

Computes n , the number of points on E .

public

Assume $n >$ any message.

Chooses $a \in \mathbb{N}$.

private

Computes $B = a \cdot A$

public

Alice: signs m

Chooses $k \stackrel{\text{ran}}{\in} \mathbb{Z}_n^*$

Computes $R = k \cdot A = (x \cdot y)$.

Computes $S \equiv k^{-1}(m + ax) \pmod{n}$

Sends (m, R, s) .

EL GAMAL SIGNATURES ON E.C.'S, CONTINUED

Bob Wants to verify (m, R, s)

Obtains p, E, n, A , and B .

Computes $V_1 = x \cdot B + s \cdot R$

Computes $V_2 = m \cdot A$

Checks if $V_1 = V_2$

$$B = a \cdot A$$

$$R = k \cdot A = (x, y)$$

$$s = k^{-1}(m - ax) \pmod{n}$$

Why does this work?

$$\begin{aligned} V_1 &= x \cdot B + s \cdot R \\ &= x \cdot a \cdot A + k^{-1} \cdot (m - a \cdot x) \cdot (k \cdot A) \\ &= x \cdot a \cdot A + (m - a \cdot x) \cdot A \\ &= x \cdot a \cdot A + m \cdot A - a \cdot x \cdot A \\ &= m \cdot A \\ &= V_2. \end{aligned}$$