An introduction to Elliptic Curve Cryptography

Craig Costello

Information Security Institute
Queensland University of Technology

INN652 - Advanced Cryptology, October 2009
Outline

1. Groups
2. Elliptic Curves
In modern cryptography, we need “stuff” to work with

By “stuff”, I mean well defined collections of objects that allow us to do certain “things”

By “things”, I mean

1. Work quickly with these objects
2. Bury knowledge beneath “hard problems” that we construct using these objects

By “hard problems”, I mean impossibly hard (Big factorizations, discrete logarithms...)

The most simple definition of such a collection of objects we use in cryptography is called a GROUP!!!
A group is a collection of objects (or set of elements) accompanied by an operation with the following 4 properties:

1. **Closure**: Performing the operation on any two objects in the group will give you another object in the group.
2. **Associativity**: When operating between any three (or more) objects, it doesn’t matter which ones you choose to operate on first.
3. **Identity**: There’s some object in the group (called the identity) that has no effect on the rest of them (under the operation).
4. **Inverse**: Each object in the group has a “partner” (an inverse). The result of performing the operation between these partners will be the identity.

The following collections of objects are examples of groups (under addition): $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_n$. Which ones are still groups under multiplication?
A group of 6 elements...

A set \( G \)

- \( G \)
- \( Q \)
- \( 0 \)
- \( R \)
- \( P \)
- \( S \)
- \( T \)

A binary operation on \( G \)

- \( Q + R = T \)
- \( S + P = R \)
- \( 0 + S = S \) (identity)
- \( 0 + 0 = 0 \)
- \( P + T = 0 \) (inverse)
A group is a pair \((G, +)\) consisting of a nonempty set \(G\) and a binary operation \(+\), (closed) on \(G\), such that \((\forall P, Q, R \in G)\):

- Binary operation is associative; \((P + Q) + R = P + (Q + R)\),
- A unique identity exists; \(0 + P = P + 0 = P\),
- Every element has a unique inverse; \(P + Q = Q + P = 0\).

Furthermore, \((G, +)\) is abelian if \(P + Q = Q + P\ \ \forall P, Q \in G\).
A slang definition of a subgroup

- Just a group contained inside a bigger group...
- A smaller group inside the bigger group, but nonetheless a group on its own merits...
A slightly more formal definition of a subgroup

**Definition**

A subset $H$ of a group $G$ which is

- **closed** under the binary operation of $G$,

- a **group** itself,

is called a **subgroup** of $G$. ($H \subseteq G$)
A subgroup example...

$H$ is a subset of $G$

$G = \mathbb{Z} \mod 9$

$H \subset G$

Check

- Closed
- Identity
- Inverses
- Associativity

$$
\begin{array}{c|ccc}
+ & 0 & 3 & 6 \\
\hline
0 & 0 & 3 & 6 \\
3 & 3 & 6 & 0 \\
6 & 6 & 0 & 3 \\
\end{array}
$$
Groups are **cyclic** if the whole group can be generated by successively operating on one element only...

We call any element that can achieve this a “**generator**”...

Every element in a group will generate some sort of subgroup (if not the whole group) all by itself...
A slightly more formal definition of cyclic (sub)groups and generators

**Definition**
Let $P \in G$, then

$$H = \{nP = P + P + \ldots + P \mid n \in \mathbb{Z}\}$$

is the cyclic subgroup of $G$ generated by $P$. ($H = \langle P \rangle$)

**Remark**
- If an element $P \in G$ generates $G$, then $P$ is a generator for $G$. ($G = \langle P \rangle$)
Cyclic (Sub)group, Generator

Consider integers modulo 8.

$G = \langle 5 \rangle$

6 is not a generator for $G$.

5 is a generator for $G$. 

Groups

Elliptic Curves
The order of an element

The number of elements in $\langle P \rangle$ is called the order of $P$ and is denoted by $|\langle P \rangle|$.

Remarks

$G = \langle P \rangle$ and $|\langle P \rangle| = n$.

- Let $Q \in G$ and $Q = sP$ for some $s \in \mathbb{Z}$. Then $Q$ generates a cyclic subgroup $H$ of $G$ containing $n/d$ elements where $d = \text{GCD}(n, s)$.

- Other generators are of the form $rP$ with $r \in \mathbb{Z}$, where $\text{GCD}(r, n) = 1$. 
Some examples

$G = \mathbb{Z}_7^+$: The integers modulo 7

Proper subgroups: none. Generators of $G$: $\{1, 2, 3, 4, 5, 6\}$.

$G = \mathbb{Z}_9^+$: The integers modulo 9

Proper subgroups: $H_3 = \{0, 3, 6\}$. Generators of $G$: $\{1, 2, 4, 5, 7, 8\}$.

$G = \mathbb{Z}_{12}^+$: The integers modulo 12

Proper subgroups: $H_2 = \{0, 6\}$, $H_3 = \{0, 4, 8\}$, $H_4 = \{0, 3, 6, 9\}$, $H_6 = \{0, 2, 4, 6, 8, 10\}$. Generators of $G$: $\{1, 5, 7, 11\}$.

$G = \mathbb{Z}_{30}^+$: The integers modulo 30

... see the tutorial questions....
Find the linear factor that relates two objects of a group
Two elements $P$ and $Q$ in a group. What is $s \in \mathbb{Z}$ such that $Q = sP$?
This is the discrete logarithm problem (DLP) to base $P$
The formal Discrete Logarithm Problem definition

- Let \((G, +)\) be a cyclic group of order \(n\) and let \(P\) be a generator of \(G\). Consider the map

\[
\varphi : \mathbb{Z}/n\mathbb{Z} \rightarrow G
\]

\[
k \mapsto kP = P + P + \ldots + P
\]

\(k\)-times

- \(\varphi\) is an isomorphism between \((G, +)\) and \((\mathbb{Z}/n\mathbb{Z}, +)\).
- Computing the inverse map is called the **Discrete Logarithm Problem (DLP)** to base \(P\).
Discrete Logarithm Problem

- i.e. given $Q \in G$ and a generator $P$ find the unique $k$ such that $0 \leq k \leq n - 1$ and $Q = kP$.

**Remarks:**

- $k$ exists since $P$ is a generator.
- $k$ may not exist if $P$ is not a generator.
- $k$ exists if $Q \in \langle P \rangle$.
- The complexity of finding $k$ depends on the selection of the group $G$ and its binary operation $\_\_\_$. 
Discrete Logarithm Problem... recall $G = \mathbb{Z}^+_{12}$

$G = \mathbb{Z}^+_{12}$: The integers modulo 12

Proper subgroups: $H_2 = \{0, 6\}$, $H_3 = \{0, 4, 8\}$, $H_4 = \{0, 3, 6, 9\}$, $H_6 = \{0, 2, 4, 6, 8, 10\}$. Generators of $G$: $\{1, 5, 7, 11\}$.

- Can we find $s \in \mathbb{Z}$ such that $8 = s2$?
- Can we find $s \in \mathbb{Z}$ such that $2 = s8$?
- Can we find $s \in \mathbb{Z}$ such that $3 = s9$?
- Can we find $s \in \mathbb{Z}$ such that $3 = s5$?
- For all $Q \in G$, can we find $s \in \mathbb{Z}$ such that $Q = s5$?
- For all $Q \in G$, can we find $s \in \mathbb{Z}$ such that $Q = sP$, where $P$ is any generator of $G$?
Discrete Logarithm Problem

\[ G = \mathbb{Z}_{11}^+ : \text{The integers modulo 11} \]

No proper subgroups... every element of \( G \) (except 0) is a generator of \( G \).

- For all \( Q \in G \) and \( P \in G/\{0\} \), **WE CAN** find \( s \in \mathbb{Z} \) such that \( Q = sP \).
- Now lets up the anti a “little”... change the definition of the operation \( + \) to be multiplication modulo....
$p = 1797693134862315907729305190789024733617976$

$9789423065727343008115773267580550096313270847$

$7322407536021120113879871393357658789768814416$

$6224928474306394741243777678934248654852763022$

$1960124609411945308295208500576883815068234246$

$2881473913110540827237163350510684586298239947$

$245938479716304835356329624224137859$

$p$ is a 1024-bit prime
Suppose we have two random elements $P$ and $Q$ in $\mathbb{Z}_p^*$. The DLP would be to find $s$ such that $Q = sP$.

Confusingly, the binary operation $+$ is (in this case) multiplication so that (under the notation we’re used to) we are trying to find $s \in \mathbb{Z}$ such that $Q = P^s$.

\[
Q = \left\{ sP = \underbrace{P + P + \ldots + P}_{\text{$s$ times}} \mid s \in \mathbb{Z} \right\}
\]

\[
Q = \left\{ sP = \underbrace{P \times P \times \ldots \times P}_{\text{$s$ times}} \mid s \in \mathbb{Z} \right\}
\]

\[
Q = P^s
\]
Basic ElGamal Encryption/Decryption

- Let $G = \langle P \rangle$ be a cyclic group and $Q = kP$.
- Encryption is $C_1 = (M + rQ)$, $C_0 = (rP)$.
- Decryption is $M = (C_1 - kC_0)$
- So, decryption corresponds to

\[
\begin{align*}
(M + rQ) - k(rP) &= \\
M + rQ - r(kP) &= \\
M + rQ - rQ &= M
\end{align*}
\]
The search for “better” groups

- We have discussed groups in settings that we are (relatively) familiar with
- In what follows we will search for a more abstract group (called Elliptic curves)
- We will see that this group can be much more beneficial in certain protocols
Some rough motivation on where to start

- We want a setting where combining (operating on) two objects gives another object.
- Very very roughly: a polynomial of degree $n$ has $n$ roots over $\mathbb{C}$.
- Therefore, a polynomial of degree 3 has 3 roots.
- If we have two of the roots, this implies (allows us to determine) the third root.
- None of this is very helpful yet and we’re nowhere near a group... but it’s a start.
A step closer...

Theorem (Bezout)
Two projective curves of degree $m$ and $n$ having no component in common intersect in $mn$ points.

- Let's generalise (in a sense) the statement about roots of polynomials on the previous slide
- The statement on the previous slide: take $x$-axis as a curve of degree 1... then $n$ degree polynomial intersects $x$-axis in $n$ places, i.e. has $n$ roots.
- ... forget the $x$-axis from now on
A step closer...

- There will be 3 intersections of a line (curve of degree 1) and a cubic (curve of degree 3).
- Specifying two of them allows us to find the third, but how can we form a “big” cryptographically useful group out of the intersection of a line and a cubic (three points)?
- Behold the magic of the group definition on elliptic curves....
Elliptic Curve

- We are interested in cubic equations
  \[ ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0 \]
- Any cubic with a rational point can be transformed into
  \[ y'^2 + px'y' + qy' = x'^3 + rx'^2 + sx' + t \]

**Definition**

An elliptic curve over \( \mathbb{Q} \) is the set of points \( (x_i, y_i) \in \mathbb{Q} \times \mathbb{Q} \) satisfying the equation

\[ y^2 = x^3 + Ax + B \]

for some \( A, B \in \mathbb{Q} \) where \( 4A^3 + 27B^2 \neq 0 \) together with the point at infinity \( \mathcal{O} \).
The Group Law

- We have a set of points (i.e. what an elliptic curve is!).
- Our goal is to form a group (Remember ElGamal!).
- All we need is a binary operation (Remember groups!).
The Group Law

- We have a set of points.
- Our goal is to form a group.
- And the binary operation is:
The Group Law

- With this binary operation......
- We select $O$ as the identity element.
- The inverse of a point $(x, y)$ is $(x, -y)$.

\[ y^2 = x^3 + Ax + B \]

\[ y = \pm \sqrt{x^3 + Ax + B} \]

- The only axiom to check is the associativity, i.e.

\[(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3).\]
The Group Law
The Group Law

Elliptic Curves
The Group Law

\[ P + P \]

\[ (P + P) + P \]

\[ P + P \]

\[ (P + P) \oplus P \]

\[ P + P \]

\[ (P + P) + P \]

\[ P + P \]

\[ (P + P) \oplus P \]
Point Addition Formulae ($P_1 \neq P_2$)

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on an elliptic curve $C$. The point $P_3 = (x_3, y_3)$ is the sum $P_1 + P_2$.

The line $L$ through $P_1$ and $P_2$ intersects $C$ at a third point $P_3$. The coordinates of $P_3$ are given by:

$$x_3 = \frac{(x_1 + x_2)^2 - x_1 - x_2}{m^2 - x_1 - x_2}$$
$$y_3 = \frac{(x_1 + x_2)(m(x_1 + x_2) - 2(y_1 - y_2))}{m^2 - x_1 - x_2}$$

where $m$ is the slope of the line $L$.
### Point Addition Formulae \((P_1 \neq P_2)\)

**L**: \(y = \lambda x + \beta\)

where

\[
\lambda = \frac{y_2 - y_1}{x_2 - x_1}
\]

**C**: \(y^2 = x^3 + Ax + B \quad \longrightarrow \quad (x^3 + Ax + B - y^2) = (x - x_1)(x - x_2)(x - x')\)

\[
x^3 + Ax + B - (\lambda x + \beta)^2 = x^3 - (x_1 + x_2 + x')x^2 + (x_1x_2 + x_2x' + x'x_1)x - (x_1x_2x')
\]

\[
x^3 - \lambda^2x^2 + (A - 2\lambda \beta)x + (B - \beta^2) = x^3 - (x_1 + x_2 + x')x^2 + (x_1x_2 + x_2x' + x'x_1)x - (x_1x_2x')
\]
**Point Addition Formulae** \((P_1 \neq P_2)\)

\[
\lambda^2 = x_1 + x_2 + x'
\]

\[
x' = \lambda^2 - x_1 - x_2
\]

\[
x_3 = x' = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2
\]

**L** : \(y = \lambda x + \beta\)

\[
y_3 = -y' = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1
\]
Point Addition Formulae \((P_1 = P_2)\)

\[
x_3 = \left(\frac{3x_1^2 + A}{2y_1}\right)^2 - 2x_1
\]

\[
y_3 = \left(\frac{3x_1^2 + A}{2y_1}\right)(x_1 - x_3) - y_1
\]
Point Addition \((P + \mathcal{O} = P)\) \((P = -P)\)
Point Addition \((P + O = P) (P = -P)\)
**E :** \(y^2 = x^3 - x + 1\) over \(\mathbb{Q}\)

- \(A = -1\) and \(B = 1\).

- \(\Delta = -4A^3 - 27B^2 = -23 \neq 0\), \(E\) is an elliptic curve.

- The point \(P = (1, 1)\) is a rational point on \(E\).

- \(Q = P + P = (1, 1) + (1, 1) = (-1, 1)\)

- \(R = Q + P = (1, -1) + (1, 1) = (0, -1)\)
Point Addition

\[ E : y^2 = x^3 - x + 1 \text{ over } \mathbb{Q} \]

- \( S = R + P = (0, -1) + (1, 1) = (3, -5) \)
- \( T = S + P = (3, -5) + (1, 1) = (5, 11) \)
- \( U = T + P = (5, 11) + (1, 1) = (1/4, 7/8) \)
- \( V = U + P = (1/4, 7/8) + (1, 1) = (-11/9, -17/27) \)
- \( Y = V + P = (-11/9, -17/27) + (1, 1) = (19/25, -103/125) \)
Everything is starting to take shape, but the points are growing in size... we need to control this and have some consistency.

Instead of defining elliptic curves over the rationals, let's use finite fields.

In this class, we will only consider (at least for this week) prime fields \( \mathbb{F}_p \).

For our purposes, operating over these fields is the same as working over \( \mathbb{Z}_p \)... so everything is done modulo \( p \).
Point Addition

Same curve as before $E : y^2 = x^3 - x + 1$ over $\mathbb{F}_{13}$

- $\Delta = -4A^3 - 27B^2 = -23 \equiv 3 \mod 13 \neq 0$, $E$ is an elliptic curve.
- 19 Points: $(0, 1), (0, 12), (1, 1), (1, 12), (3, 5), (3, 8), (4, 3), (4, 10), (5, 2), (5, 11), (6, 4), (6, 9), (7, 5), (7, 8), (10, 4), (10, 9), (12, 1), (12, 12)$....., oh, and don’t forget $O$.
- Let $P = (1, 12)$ and $Q = (4, 10)$ on $E$.
- $P + Q = (1, 12) + (4, 10) = (7, 5)$.
- $2P = P + P = (1, 12) + (1, 12) = (12, 12)$
- $3P = 2P + P = (12, 12) + (1, 12) = (0, 1)$
- $4P = 3P + P = (0, 1) + (1, 12) = (3, 5)$ .........
Point Addition

Same curve as before $E : y^2 = x^3 - x + 1$ over $\mathbb{F}_{13}$

- $10 \times P = P + P + \ldots + P = (4, 10) = Q$

- Given $P$ and $Q$, the discrete log problem to base $P$ involves finding $s$ such that $sP = Q$ and in this case $s = 10$.

- It is simple to find the discrete logarithm (using brute force attack) when curve is defined over such a small field...

- But again, what if we “up the anti” and increase the field size like we did before...
A cryptographically suitable curve

Same curve as before $E : y^2 = x^3 - x + 1$ over $\mathbb{F}_p$

- $p = 1461501637330902918203684832716283019655932542983$
- $\#E = 1461501637330902918203686004385807989344528195053$
- $P = (1321554781015706068290537639827905592412509913620, 1136877326354697828904160020005825111410953389610)$
- $r = 115641388596795456695979756324256781634201930388$
- $Q = rP = (715875109644815085946717311816604681845099700277, 1450877329524262790654657764775612031321288027789)$
A cryptographically suitable curve

- It was easy for me (my computer) to multiply $P$ by $r$ to get $Q$ (milliseconds)...
- ... but to get $r$ from $Q$ and $P$...
- A lazy brute force loop...
  
  $T = P$
  
  while $T \neq Q$
  do
  $T = T + P$
  
  end while

- Loop will have to do $r \approx p$ additions before terminating (impossible)
- So $r$ is buried inside the elliptic curve discrete logarithm problem (ECDLP)
- Attacks are much better than brute force (as always), but in this context they are much slower than what we may be used to
Elliptic curves in cryptography

- To put it simply, elliptic curves just provide an alternative discrete logarithm problem (the ECDLP).
- Arithmetic in the forward direction, i.e. multiplying a point by an integer (finding $rP$ from $r$ and $P$) is very fast (double-and-add techniques).
- Finding $r$ from $P$ and $rP$ is computationally “hard”.
- In fact, for identical field sizes, the ECDLP is much harder than the DLP (more about this in the tutorial).
- This is the beauty of elliptic curves - we can use much much smaller fields (shorter keys) for ElGamal (discrete log) based cryptosystems.
Elliptic curves in cryptography

There is one more reason we need elliptic curves (pairings)... but this is next week’s lecture...