Introduction to Cryptology

Lecture 23
Announcements

• HW8 up on course webpage. Due Tuesday, 5/2.
• Reminder: Extra Credit due Tuesday, 5/9
Agenda

• Last time:
  – Cyclic Groups, prime order groups
  – Hard problems

• This time:
  – More hard problems
  – Elliptic Curve Groups
  – Diffie-Hellman Key Exchange (K/L 10.3)
  – El Gamal Public Key Encryption (K/L 11.4)
The Discrete Logarithm Problem

The discrete-log experiment \( DLog_{A,G}(n) \)

1. Run \( G(1^n) \) to obtain \((G, q, g)\) where \( G \) is a cyclic group of order \( q \) (with \( \|q\| = n \)) and \( g \) is a generator of \( G \).
2. Choose a uniform \( h \in G \)
3. \( A \) is given \( G, q, g, h \) and outputs \( x \in Z_q \)
4. The output of the experiment is defined to be 1 if \( g^x = h \) and 0 otherwise.

Definition: We say that the DL problem is hard relative to \( G \) if for all ppt algorithms \( A \) there exists a negligible function \( neg \) such that

\[
\Pr[DLog_{A,G}(n) = 1] \leq neg(n).
\]
The Diffie-Hellman Problems
The CDH Problem

Given \((G, q, g)\) and uniform \(h_1 = g^{x_1}, h_2 = g^{x_2}\), compute \(g^{x_1 \cdot x_2}\).
The DDH Problem

We say that the DDH problem is hard relative to $G$ if for all ppt algorithms $A$, there exists a negligible function $neg$ such that

$$|\Pr[A(G, q, g, g^x, g^y, g^z) = 1] - \Pr[A(G, q, g, g^x, g^y, g^{xy}) = 1]| \leq neg(n).$$
Relative Hardness of the Assumptions

Breaking DLog → Breaking CDH → Breaking DDH

DDH Assumption → CDH Assumption → DLog Assumption
Elliptic Curves over Finite Fields

Why use them?

• No known sub-exponential time algorithm for solving DL in appropriate Curves.
• Implementation will be more efficient.
Elliptic Curves over Finite Fields

- $\mathbb{Z}_p$ is a finite field for prime $p$.
- Let $p \geq 5$ be a prime
- Consider equation $E$ in variables $x, y$ of the form:
  \[ y^2 := x^3 + Ax + B \mod p \]
  Where $A, B$ are constants such that $4A^3 + 27B^2 \neq 0$.
  (this ensures that $x^3 + Ax + B \mod p$ has no repeated roots).

Let $E(\mathbb{Z}_p)$ denote the set of pairs $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ satisfying the above equation as well as a special value $O$.

\[ E(\mathbb{Z}_p) := \{(x, y) | x, y \in \mathbb{Z}_p \text{ and } y^2 = x^3 + Ax + B \mod p\} \cup \{O\} \]

The elements $E(\mathbb{Z}_p)$ are called the points on the Elliptic Curve $E$ and $O$ is called the point at infinity.
Elliptic Curves over Finite Fields

Example:
Quadratic Residues over $\mathbb{Z}_7$.

$0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 9 = 2, 4^2 = 16 = 2, 5^2 = 25 = 4, 6^2 = 36 = 1$.

$f(x) := x^3 + 3x + 3$ and curve $E: y^2 = f(x) \mod 7$.

• Each value of $x$ for which $f(x)$ is a non-zero quadratic residue mod 7 yields 2 points on the curve.
• Values of $x$ for which $f(x)$ is a non-quadratic residue are not on the curve.
• Values of $x$ for which $f(x) \equiv 0 \mod 7$ give one point on the curve.
Elliptic Curves over Finite Fields

<table>
<thead>
<tr>
<th>$f(0) \equiv 3 \mod 7$</th>
<th>a quadratic non-residue mod 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f(1) \equiv 0 \mod 7$</td>
<td>so we obtain the point $(1,0) \in E(Z_7)$</td>
</tr>
<tr>
<td>$f(2) \equiv 3 \mod 7$</td>
<td>a quadratic non-residue mod 7</td>
</tr>
<tr>
<td>$f(3) \equiv 4 \mod 7$</td>
<td>a quadratic residue with roots 2,5. so we obtain the points $(3,2), (3,5) \in E(Z_7)$</td>
</tr>
<tr>
<td>$f(4) \equiv 2 \mod 7$</td>
<td>a quadratic residue with roots 3,4. so we obtain the points $(4,3), (4,4) \in E(Z_7)$</td>
</tr>
<tr>
<td>$f(5) \equiv 3 \mod 7$</td>
<td>a quadratic non-residue mod 7</td>
</tr>
<tr>
<td>$f(6) \equiv 6 \mod 7$</td>
<td>a quadratic non-residue mod 7</td>
</tr>
</tbody>
</table>
Elliptic Curves over Finite Fields

Point at infinity: $O$ sits at the top of the $y$-axis and lies on every vertical line.

Every line intersecting $E(Z_p)$ intersects it in exactly 3 points:

1. A point $P$ is counted 2 times if line is tangent to the curve at $P$.
2. The point at infinity is also counted when the line is vertical.
Addition over Elliptic Curves

Binary operation “addition” denoted by $+$ on points of $E(Z_p)$.

• The point $O$ is defined to be an additive identity for all $P \in E(Z_p)$ we define $P + O = O + P = P$.

• For 2 points $P_1, P_2 \neq O$ on $E$, we evaluate their sum $P_1 + P_2$ by drawing the line through $P_1, P_2$ (If $P_1 = P_2$, draw the line tangent to the curve at $P_1$) and finding the 3rd point of intersection $P_3$ of this line with $E(Z_p)$.

• The 3rd point may be $P_3 = O$ if the line is vertical.

• If $P_3 = (x, y) \neq O$ then we define $P_1 + P_2 = (x, -y)$.

• If $P_3 = O$ then we define $P_1 + P_2 = O$. 
Additive Inverse over Elliptic Curves

• If \( P = (x, y) \neq O \) is a point of \( E(\mathbb{Z}_p) \) then 
  \( -P = (x, -y) \) which is clearly also a point on 
  \( E(\mathbb{Z}_p) \).

• The line through \( (x, y), (x, -y) \) is vertical and 
  so addition implies that \( P + (-P) = O \).

• Additionally, \( -O = O \).
Groups over Elliptic Curves

Proposition: Let \( p \geq 5 \) be prime and let \( E \) be the elliptic curve given by \( y^2 = x^3 + Ax + B \mod p \) where \( 4A^3 + 27B^2 \neq 0 \mod p \).

Let \( P_1, P_2 \neq O \) be points on \( E \) with \( P_1 = (x_1, y_1) \) and \( P_2 = (x_2, y_2) \).

1. If \( x_1 \neq x_2 \) then \( P_1 + P_2 = (x_3, y_3) \) with 
   \[
   x_3 = [m^2 - x_1 - x_2 \mod p], \quad y_3 = [m - (x_1 - x_3) - y_1 \mod p]
   \]
   Where \( m = \left[ \frac{y_2 - y_1}{x_2 - x_1} \mod p \right] \).

2. If \( x_1 = x_2 \) but \( y_1 \neq y_2 \) then \( P_1 = -P_2 \) and so \( P_1 + P_2 = O \).

3. If \( P_1 = P_2 \) and \( y_1 = 0 \) then \( P_1 + P_2 = 2P_1 = O \).

4. If \( P_1 = P_2 \) and \( y_1 \neq 0 \) then \( P_1 + P_2 = 2P_1 = (x_3, y_3) \) with 
   \[
   x_3 = [m^2 - 2x_1 \mod p], \quad y_3 = [m - (x_1 - x_3) - y_1 \mod p]
   \]
   Where \( m = \left[ \frac{3x_1^2 + A}{2y_1} \mod p \right] \).

The set \( E(Z_p) \) along with the addition rule form an abelian group.

The elliptic curve group of \( E \).

**Difficult property to verify is associativity. Can check through tedious calculation.**
DDH over Elliptic Curves

DDH: Distinguish \((aP, bP, abP)\) from \((aP, bP, cP)\).
Size of Elliptic Curve Groups?

How large are EC groups \( mod \ p \)?

Heuristic: \( y^2 = f(x) \) has 2 solutions whenever \( f(x) \) is a quadratic residue and 1 solution when \( f(x) = 0 \).

Since half the elements of \( Z_p^* \) are quadratic residues, expect \( \frac{2(p-1)}{2} + 1 = p \) points on curve. Including \( O \), this gives \( p + 1 \) points.

Theorem (Hasse bound): Let \( p \) be prime, and let \( E \) be an elliptic curve over \( Z_p \). Then
\[
p + 1 - 2\sqrt{p} \leq |E(Z_p)| \leq p + 1 + 2\sqrt{p}.
\]