Introduction to Cryptology

Lecture 21

Announcements

- HW10 due on Thursday, 4/30
- HW 9 grades up on Canvas
- HW 7,8 solutions up on Canvas
- Dr. Feng-Hao Liu will be subbing next class

Agenda

- Last time:
  - Number theory background (8.2)
- This time:
  - Number theory background
    - Hard problems in Cyclic Groups (8.3)
    - Elliptic Curve Groups (8.3)
  - Key Exchange definition and Diffie-Hellman KE (10.3)

Recall: Cyclic Groups

For a finite group G of order m and $g \in G$, consider:

$$\langle g \rangle = \{g^0, g^1, \ldots, g^{m-1}\}$$

$\langle g \rangle$ always forms a cyclic subgroup of G.

However, it is possible that there are repeats in the above list.

Thus $\langle g \rangle$ may be a subgroup of order smaller than m.

If $\langle g \rangle = G$, then we say that G is a cyclic group and that g is a generator of G.

The Discrete Logarithm Problem

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

1. Run $\boldsymbol{G}(1^n)$ 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 $\boldsymbol{G}$ if for all ppt algorithms A there exists a negligible function neg such that

$$\Pr\left[DLog_{A,\boldsymbol{G}}(n) = 1\right] \leq neg(n).$$

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 $\boldsymbol{G}$ 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 $\rightarrow$ Breaking CDH $\rightarrow$ Breaking DDH

DDH Assumption $\rightarrow$ CDH Assumption $\rightarrow$ 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

- 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 $E\left(Z_p\right)$ denote the set of pairs $(x, y) \in Z_p \times Z_p$ satisfying the above equation as well as a special value O.

$$E\left(Z_p\right) := \left\{(x, y) | x, y \in Z_p \; and \; y^2 = x^3 + Ax + B \; mod \; p\right\} \cup \{O\}$$

The elements $E\left(Z_p\right)$ 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 Z_7.

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

$f(x) \coloneqq x^3 + 3x + 3$ 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

$f(0) \equiv 3 \, mod \, 7$	a quadratic non-residue mod 7
$f(1) \equiv 0 \, mod \, 7$	so we obtain the point $(1,0) \in E(Z_7)$
$f(2) \equiv 3 \, mod \, 7$	a quadratic non-residue mod 7
$f(3) \equiv 4 \, mod \, 7$	a quadratic residue with roots $2,5$. so we obtain the points $(3,2), (3,5) \in E(Z_7)$
$f(4) \equiv 2 \, mod \, 7$	a quadratic residue with roots $3,4$. so we obtain the points $(4,3), (4,4) \in E(Z_7)$
$f(5) \equiv 3 \, mod \, 7$	a quadratic non-residue mod 7
$f(6) \equiv 6 \, mod \, 7$	a quadratic non-residue mod 7

Elliptic Curves over Finite Fields

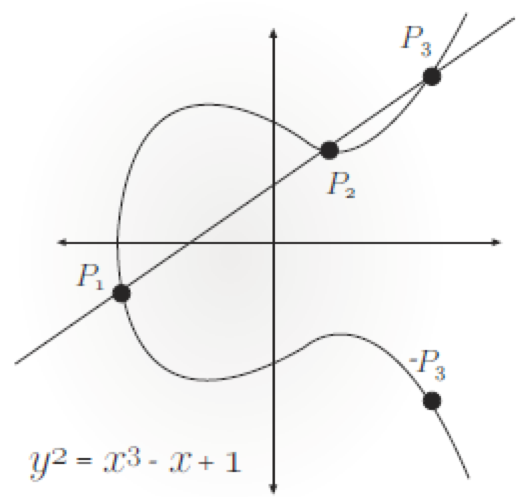

FIGURE 8.2: An elliptic curve over the reals.

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 $E\left(Z_p\right)$ then $-P = (x, -y)$ which is clearly also a point on $E\left(Z_p\right)$.
- 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

$$x_3 = [m^2 - x_1 - x_2 \ mod \ p], y_3 = [m - (x_1 - x_3) - y_1 \ mod \ p]$$

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

$$x_3 = [m^2 - 2x_1 \ mod \ p], y_3 = [m - (x_1 - x_3) - y_1 \ mod \ p]$$

Where $m = \left[\frac{3{x_1}^2 + A}{2y_1} \ mod \ p\right]$.

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

$$p + 1 - 2\sqrt{p} \leq \left|E\left(Z_p\right)\right| \leq p + 1 + 2\sqrt{p}.$$

Applications

Key Agreement

The key-exchange experiment ${KE^{eav}}_{A,\Pi}(n)$:

1. Two parties holding 1^n execute protocol Π. This results in a transcript $trans$ containing all the messages sent by the parties, and a key k output by each of the parties.
2. A uniform bit $b \in \{0,1\}$ is chosen. If $b = 0$ set $\hat{k} \coloneqq k$, and if $b = 1$ then choose $\hat{k} \in \{0,1\}^n$ uniformly at random.
3. A is given $trans$ and $\hat{k}$, and outputs a bit b'.
4. The output of the experiment is defined to be 1 if $b' = b$ and 0 otherwise.

Definition: A key-exchange protocol Π is secure in the presence of an eavesdropper if for all ppt adversaries A there is a negligible function neg such that

$$\Pr\left[{KE^{eav}}_{A,\Pi}(n) = 1\right] \le \frac{1}{2} + neg(n).$$

Discussion of Definition

- Why is this the “right” definition?
- Why does the adversary get to see $\widehat{k}$?