Cryptography

Lecture 22

Announcements

- No Instructor Office Hours on Friday
- HW8 due on Monday, 4/29

Agenda

- Last time:
  - Cyclic groups
  - Hard problems (Discrete log, Diffie-Hellman Problems—CDH, DDH)
  - Elliptic Curve Groups
- This time:
  - Elliptic Curve Groups
  - Key Exchange, Diffie-Hellman Key Exchange
  - Public Key Encryption, ElGamal Encryption

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

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

The elements $E(Z_p)$ are called the points on the Elliptic Curve E and O is called the point at infinity.

Elliptic Curves over Finite Fields

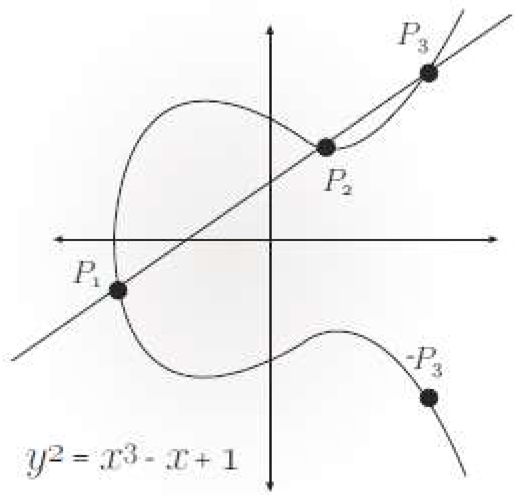

FIGURE 8.2: An elliptic curve over the reals.

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

Every line intersecting $E(Z_p)$ in 2 points, 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 $E(Z_p)$ then $-P = (x, -y)$ which is clearly also a point on $E(Z_p)$.
- 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
$$x_3 = [m^2 - x_1 - x_2 \; mod \; p], y_3 = [m - (x_1 - x_3) - y_1 \; mod \; p]$$
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

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

Public Key Cryptography

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

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

Discussion of Definition

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

Diffie-Hellman Key Exchange

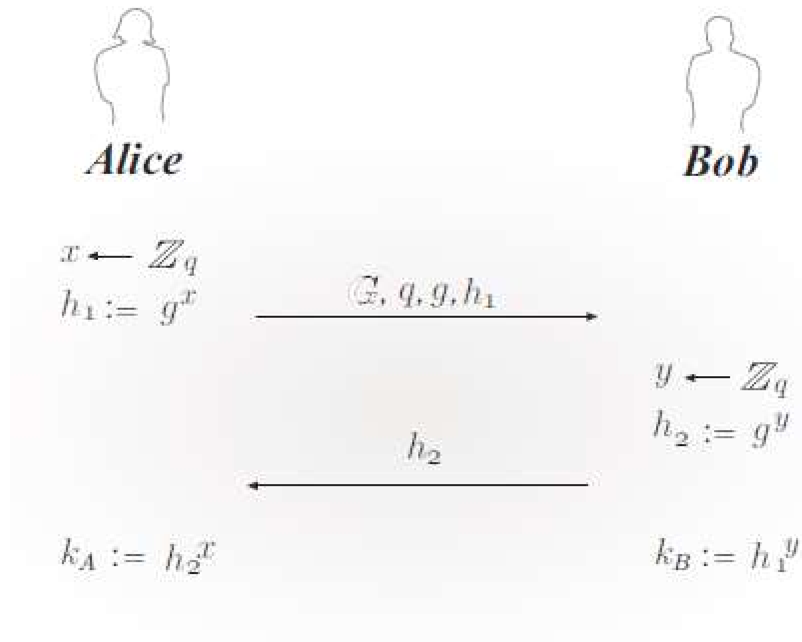

FIGURE 10.2: The Diffie-Hellman key-exchange protocol.

Recall 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

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

Security Analysis

Theorem: If the DDH problem is hard relative to $\boldsymbol{G}$, then the Diffie-Hellman key-exchange protocol Π is secure in the presence of an eavesdropper.

Public Key Encryption

Definition: A public key encryption scheme is a triple of ppt algorithms (Gen, Enc, Dec) such that:

1. The key generation algorithm Gen takes as input the security parameter 1^n and outputs a pair of keys (pk, sk). We refer to the first of these as the public key and the second as the private key. We assume for convenience that pk and sk each has length at least n, and that n can be determined from pk, sk.
2. The encryption algorithm Enc takes as input a public key pk and a message m from some message space. It outputs a ciphertext c, and we write this as $c \leftarrow Enc_{pk}(m)$.
3. The deterministic decryption algorithm Dec takes as input a private key sk and a ciphertext c, and outputs a message m or a special symbol $\perp$ denoting failure. We write this as $m \coloneqq Dec_{sk}(c)$.

Correctness: It is required that, except possibly with negligible probability over (pk, sk) output by $Gen(1^n)$, we have $Dec_{sk}\left(Enc_{pk}(m)\right) = m$ for any legal message m.

CPA-Security

The CPA experiment ${PubK^{cpa}}_{A,\Pi}(n)$:

1. $Gen(1^n)$ is run to obtain keys (pk, sk).
2. Adversary A is given pk, and outputs a pair of equal-length messages m_0, m_1 in the message space.
3. A uniform bit $b \in \{0,1\}$ is chosen, and then a challenge ciphertext $c \leftarrow Enc_{pk}(m_b)$ is computed and given to A.
4. A outputs a bit b'. The output of the experiment is 1 if $b' = b$, and 0 otherwise.

Definition: A public-key encryption scheme $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ is CPA-secure if for all ppt adversaries A there is a negligible function neg such that

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

Discussion

- Discuss how in the public key setting security in the presence of an eavesdropper and CPA security are equivalent (since anyone can encrypt using the public key).
- Discuss how CPA-secure encryption cannot be deterministic!!
  - Why not?

El Gamal Encryption

--Show how we can derive El Gamal PKE from Diffie-Hellman Key Exchange

Important Property

Lemma: Let G be a finite group, and let $m \in G$ be arbirary. Then choosing uniform $k \in G$ and setting $k' := k \cdot m$ gives the same distribution for k' as choosing uniform $k' \in G$. Put differently, for any $\hat{g} \in G$ we have

$$\Pr[k \cdot m = \hat{g}] = 1/|G|\,.$$

El Gamal Encryption Scheme

CONSTRUCTION 11.16

Let $\mathcal{G}$ be as in the text. Define a public-key encryption scheme as follows:

- Gen: on input 1^n run $\mathcal{G}(1^n)$ to obtain $(\mathbb{G}, q, g)$. Then choose a uniform $x \leftarrow \mathbb{Z}_q$ and compute $h := g^x$. The public key is $\langle \mathbb{G}, q, g, h \rangle$ and the private key is $\langle \mathbb{G}, q, g, x \rangle$. The message space is $\mathbb{G}$.
- Enc: on input a public key $pk = \langle \mathbb{G}, q, g, h \rangle$ and a message $m \in \mathbb{G}$, choose a uniform $y \leftarrow \mathbb{Z}_q$ and output the ciphertext
$$\langle g^y,\ h^y \cdot m \rangle.$$
- Dec: on input a private key $sk = \langle \mathbb{G}, q, g, x \rangle$ and a ciphertext $\langle c_1, c_2 \rangle$, output
$$\hat{m} := c_2 / c_1^x.$$

The El Gamal encryption scheme.