6.857 Rivest
3/11/09 L11.1

**Admin:**

**Outline:** Diffie-Hellman key exchange; bilinear groups, El Gamal

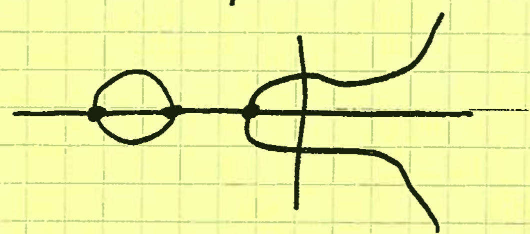
- ☐ Elliptic curve groups
- ☐ review PK setup based on DLP
- ☐ Diffie-Hellman key exchange
- ☐ Gap groups & bilinear maps
- ☐ Boneh/Lynn/Shacham signature scheme
- ☐ El Gamal PK encryption

## Elliptic curve groups:

Let $p$ be a prime

Let $a, b \in \mathbb{Z}_p$ $\quad [4a^3 + 27b^2 \neq 0 \bmod p]$

Consider eqn $E$: $y^2 = x^3 + ax + b \pmod p$



roots $r_1, r_2, r_3$

$$((r_1 - r_2)(r_1 - r_3)(r_2 - r_3))^2 = -(4a^3 + 27b^2)$$

So roots are distinct

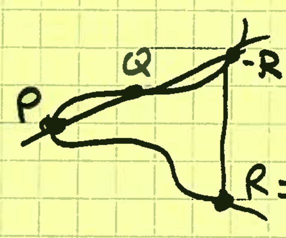
**Def:** points on curve $E = E(\mathbb{F}_p)$ $\qquad F_p = GF(p)$

$$= \{(x,y) : y^2 = x^3 + ax + b\} \cup \{\infty\}$$

$|E(\mathbb{F}_p)| = p + 1 + t$ where $|t| \leq 2\sqrt{p}$ $\quad$ [can ~~do~~ find "efficiently"]

Can define group law on $E(F_p)$: (written additively)

- $\infty$ is the identity $\qquad P + \infty = \infty + P = P$
- $P + Q = R$




$P = (x_1, y_1)$

$Q = (x_2, y_2)$

If $x_1 \neq x_2$: $\begin{cases} x_3 = m^2 - x_1 - x_2 \\ y_3 = m(x_1 - x_3) - y_1 \end{cases}$ $\qquad m = \frac{y_2 - y_1}{x_2 - x_1}$

If $x_1 = x_2$ & $y_1 \neq y_2$: $P + Q = \infty$

If $P = Q$ & $y_1 = 0$: $P + Q = \infty$

If $P = Q$ & $y_1 \neq 0$: $\begin{cases} x_3 = m^2 - 2x_1 \\ y_3 = m(x_1 - x_3) - y_1 \end{cases}$ $\qquad m = \frac{3x_1^2 + A}{2y_1}$ $\quad a$

associative!

$P = (x, y) \Rightarrow -P = (x, -y)$ inverses

may or may not be cyclic.

## DLP:

Let $G$ be a group, $g \in G$ (perhaps a generator)
Suppose $y = g^x$ $\quad 0 \le x < \text{ord}(g)$
then $x$ is the discrete log of $y$, base $g$, in $G$.

Often assumed that DLP (computing discrete logs) is hard/infeasible.

(DLP easy if ord($g$) has only small prime factors...)

DLP in $Z_p^*$ essentially as hard as factoring an $n$ of same size as $p$. (heuristic)

---

E.g. typical public key setup

$p = 2r+1$ large "safe" prime ($r$ prime)

$g$ generator of $Z_p^*$ $\quad \text{ord}(g) = p-1 = |Z_p^*|$

$p, g$ public system parameters

- Alice picks secret key $x$, $1 \le x \le p-1$
- Alice publishes her public key $y = g^x \pmod p$
- Her secret key is protected from disclosure by DLP.

6.857 Rivest
3/11/09 L11.4

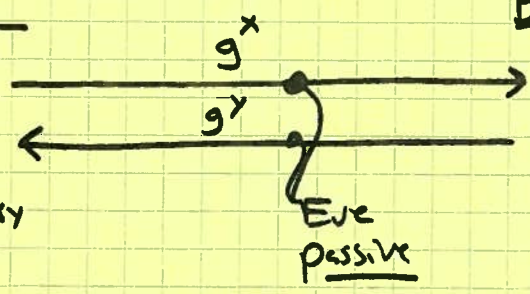
## Diffie Hellman key exchange

p, g public parameters

**Alice:** secret key $x$, public key $g^x$ (permanent or transient)

**Bob:** secret key $y$, public key $g^y$ ( " " " )

Alice Bob




$K = (g^y)^x = g^{xy}$ $K = (g^x)^y = g^{xy}$

requires DLP to be hard, but not known to be sufficient

**CDH:** given $g^x$ & $g^y$, to compute $g^{xy}$ (is hard)
(Computational Diffie Hellman assumption.)

CDH ⇒ DH key exchange is secure (against passive eavesdropper) (Duh!)
(for secrecy key)

Related problem:

**DDH:** Given $(g^a, g^b, g^c)$ a, b, c random
or $(g^a, g^b, g^{ab})$ a, b random
— to be able to distinguish the two cases... (is hard)
"Decision diffie hellman"

DDH ⇒ CDH (i.e. ¬CDH ⇒ ¬DDH)

Is DDH easier than CDH??
in some groups???
recognizing right answer $g^{ab}$ might be
easier than computing it...??

Gap groups (DDH easy, CDH hard)

Bilinear groups:

Let $G_1$ be group of prime order $q$ (multiplicative) gen $g$
Let $G_2$ be group of prime order $q$ ( " ) gen $h$

Suppose we also have (bilinear) map

$$e : G_1 \times G_1 \to G_2$$

s.t.

$$(\forall a,b)\ e(g^a, g^b) = h^{ab} \qquad (!!)$$

Then:

DDH is easy in $G_1$:

given $g^a, g^b, g^c$

$$c = ab \pmod q \iff e(g^a, g^b) = e(g, g^c)$$

$$h^{ab} \stackrel{?}{=} h^c$$

$$ab = c \mod q$$

Doesn't make CDH easy, though; we have gap between DDH & CDH

How: $G_1$ is elliptic curve (supersingular: $y^2 = x^3 + ax + b \pmod p$)

$$|E(\mathbb{F}_p)| = p + 1 \qquad (p \geq 5)$$

$p \equiv 2 \pmod 3$, $b \in Z_p^*$, $a = 0$ — supersingular $y^2 = x^3 + b$

or $p \equiv 3 \pmod 4$, $a = 1$, $b = 0$ — $y^2 = x^3 + x$

$G_2$ is $\mathbb{F}_{p^k}$ some small $k$.

$e$: is "Weil pairing" or "Tate pairing" ...

## Boneh, Lynn, Shacham (2001) BLS Signature scheme

$G_1, G_2, e, g$     $H$ maps msgs $\rightarrow G_1$

secret key $x$ for signer

public key $g^x$

Sign $m$:    $\sigma = H(m)^x$

Verify:    $e(g, \sigma) = e(g^x, H(m))$

$$= e(g, H(m))^x$$

## El Gamal encryption (Taher El Gamal, 1984)

- Public key encryption scheme
  - Keygen$(1^\lambda) \longrightarrow (PK, SK)$ $\lambda$ = "security parameter"
  - $E(PK, m) \longrightarrow c$ [may be randomized $E(PK, m, r)$
  - $D(SK, c) \longrightarrow m$ deterministic

- Let $G = \langle g \rangle$ be a cyclic group
- We suppose $m \in G$, via suitable encoding

- Keygen: pick $SK = x$ $\quad 0 \le x < |G|$
  let $PK = g^x$ } Alice's PK

- Encryption: (randomized) let $PK = y$ of recipient Alice $(y = g^x)$
  pick $k$ at random $\quad 0 \le k < |G|$
  let $c = (g^k, m \cdot y^k)$

- Decryption: let $c = (a, b)$ received ciphertext
  then $m = b / a^x$ $\quad (SK = x)$
  [Note: $a^x = g^{kx} = y^k$]

- Relation to DH Key exchange

Alice $\xrightarrow{\quad y = g^x \text{ (via PKI?)} \quad}$ Bob

$\xleftarrow{\quad a = g^k \quad}$

$\xleftarrow{\quad b = m \cdot \text{key} \quad}$

DH key $= (g^k)^x = g^{xk} = a^x$

DH key $= (g^x)^k = y^k = g^{xk}$