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 \left[ y^3 + 27b^2 \neq 0 \pmod{p} \right]

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

roots $r_1, r_2, r_3$

\[ \left( (r_1 - r_2)(r_1 - r_3)(r_2 - r_3) \right)^2 = -\left( y^3 + 27b^2 \right) \]

so roots are distinct

$E = \mathbb{F}_p$ (finite field)

Def: points on curve $E = E(\mathbb{F}_p) = \{ (x,y) : y^2 = x^3 + ax + b \} \cup \{ \infty \}$

$|E(\mathbb{F}_p)| = \# \mathbb{F}_p + 1 + t$ where $|t| \leq 2\sqrt{p}$ \quad \left[ \text{can do \, \emph{elliptic curve} \, \text{arith.}} \right]

Can define group law on $E(\mathbb{F}_p)$: (written additive)

- $\infty$ is the identity
- $P + Q = R$
- $P = (x_1,y_1)$
  $Q = (x_2,y_2)$

- If $x_1 \neq x_2$, \[ \begin{cases} x_3 = m^2 - x_1 - x_2 & m = y_2 - y_1 \frac{x_2 - x_1}{x_2 - x_1} \\ y_3 = m(x_1 - x_3) - y_1 \end{cases} \]

- If $x = x_2 \land y_1 \neq y_2$, $P + Q = \infty$

- If $P = Q \land y_1 = 0$, $P + Q = \infty$

- If $P = Q \land y_1 \neq 0$, \[ \begin{cases} x_3 = m^2 - 2x_1 & m = 3x_1^2 + A \frac{2y_1}{2y_1} \\ y_3 = m(x_1 - x_3) - y_1 \end{cases} \]

associative!

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

may or may not be cyclic.
DLP:
\[
\text{Let } G \text{ be a group, } g \in G \text{ (perhaps a generator)}.
\]
\[
\text{Suppose } y^x = g^x \quad 0 \leq x < \text{ord}(g)
\]
\[
\text{then } x \text{ is the discrete log of } y \text{, base } g, \text{ in } G.
\]

Often assumed that DLP (computing discrete logs) is hard/ infeasible.
(DLP can if ord(g) has only small prime factors...)

\[\text{Almost as hard as factoring an } n \text{ as same size as } p.\]

---

**Example**

**Typical public key setup**

\[
\begin{align*}
p &= 2r + 1 \quad \text{large "safe" prime (or prime)} \\ g &\text{ generator of } \mathbb{Z}_p^* \quad \text{ord}(g) = p - 1 = 127_{\text{mod } 127^{\ast}} \\
p, g &\text{ public system parameters}
\end{align*}
\]

- **Alice picks secret key** \( x \), \( 1 \leq x \leq p - 1 \)
- **Alice publishes her public key** \( y = g^x \mod p \)
- **Her secret key is protected from disclosure by DLP.**
Diffie Hellman key exchange

\( p, g \) public params

Alice: secret key \( x \), public key \( g^x \) (permanent or transient)
Bob: secret key \( y \), public key \( g^y \)

\[
\begin{align*}
\text{Alice} & \quad g^x \\
\text{Bob} & \quad g^y
\end{align*}
\]

\( k = (g^y)^x = g^{xy} \)

\( k = (g^x)^y = g^{xy} \)

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

\( \text{CDH: given } g^x \text{ and } g^y, \text{ to compute } g^{xy} \text{ is hard} \)
(Computational Diffie Hellman assumption.)

\( \text{CDH} \Rightarrow \text{DH key exchange is secure (under passive eavesdropper)} \) (Dub.)

(For secure key)

Related problem:

\( \text{DDH: given } (g^a, g^b, g^c) \text{ a, b, c random} \)

\( \text{or } (g^a, g^b, g^{ab}) \text{ a, b random} \)

\( \text{to be able to distinguish the two cases... is hard} \)

"Decision Diffie Hellman"

\( \text{DDH} \Rightarrow \text{CDH} \) (i.e. \( \neg \text{CDH} \Rightarrow \neg \text{DDH} \))

Is DDH easier than CDH??

in some groups ???

recognizably right answer \( g^{ab} \) might be
closer 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 $q$ (additive) gen $h$

Support we also have (bilinear) map
$e: G_1 \times G_1 \rightarrow G_2$

s.t.
$e(g^a, g^b) = h^{ab}$ (1)

Then:
DDH is easy in $G_1$:
given $g^a, g^b, g^c$
$c = ab \iff e(g^a, g^b) = e(g^c, g^c)$
(mod $q$)
$h^{ab} = h^c$
$ab = c \mod q$

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

How: $G_1$ is elliptic curve (supersingular: $y^2 = x^3 + ax + b$ (mod $p$))
$|E(F_p)| = p + 1$ $(p \geq 5)$
$\rho \equiv 2 \mod 3$
$b \in \mathbb{F}_p^*$
$a = 0$
$\rho \equiv 3 \mod 4$
$y^2 = x^3 + x$
$b = 0$

$G_2$ is $\mathbb{F}_p^*$ some small $k$.

C: a "Weil point" or "Tate point"...
Boneh, Lynn, Shacham (2001) BLS Signature scheme

$G_1, G_2, e, g^g$  
$H$ maps msg $\rightarrow G_1$

[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 Gamel encryption (Taher El Gamal, 1984)

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

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

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

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

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

- Relation to DH key exchange
  Alice $\quad y = g^x \quad \text{(via PK?)} \quad \rightarrow \quad$ Bob
  $\quad \text{DH key} = (g^k)^x \quad \leftrightarrow \quad a = g^k$
  $\quad b = m \cdot \text{key}$ $\quad \text{DH key} = (g^x)^k = y^k = g^{xk}$