Today:

- Gap groups & bilinear maps
- BLS (Boneh-Lynn-Shacham) signatures
- Three-way key agreement (Joux)
- Identity-based encryption (Boneh-Franklin)

**Gap Groups**

A gap group is a group where:

- **Decisional Diffie-Hellman**
  - DDH is easy

\[(\text{Recall DDH: } (g, g^a, g^b, g^c) \not\approx (g, g^a, g^b, g^{a+b}))\]

- **Com. Diffie-Hellman**
  - CDH is easy

\[(\text{Recall CDH: } (g, g^a, g^b) \xrightarrow{\text{HARD}} g^{ab})\]

Note: CDH is easy \implies DDH is easy

This difference between DDH ("easy") and CDH ("hard") forms a "gap".
Q1: How can we construct "gap groups"?
Q2: What good would that be?

Bilinear maps

Suppose: $G_1$, group of prime order $g$, w. generator $g$
$G_2$, group of prime order $h$

[We use mult. notation for both groups].

& there exists a bilinear map $E : G_1 \times G_1 \rightarrow G_2$

s.t.

$\forall a,b \in G_1 \quad e(g^a, g^b) = e(g, g)^{a \cdot b}$
$e(g, g) = h.$

$\Rightarrow e(g^a, g^b) = e(g^{a+b}, g) = e(g^b, g^a) = e(g, g^{ab}) = \ldots$

Bilinear maps are also called pairing functions

They have numerous applications
Thm: If there exists a bilinear map
\[ e : G_1 \times G_1 \rightarrow G_2 \]
between two groups of prime order
then DDH is easy in \( G_1 \)

\textbf{Pf:} Given \((g, g^{a}, g^{b}, g^{c})\)

Check if \( e(g^{a}, g^{b}) = e(g, g^{c}) \)
if so output "c = ab"
o.w. ""c is random."

\textbf{Note:} Even though DDH is easy in \( G_1 \),
CDH may still be hard.
I.e., we may have a gap group.

\textbf{How to construct a gap group w. bilinear map?}

This is not simple!

\( G_1 \) is an elliptic curve (w. certain properties)
\( e \) (bilinear map) is a "Well pairing" or a
"Tate pairing"
Application 4: Digital Signatures
(Boneh-Lynn-Shacham 2001)

Signatures are short (eg. 160 bits)!

Public Params:
- Groups $G_1, G_2$ of prime order $q$
- Pairing function $e : G_1 \times G_1 \rightarrow G_2$
- $g = \text{generator of } G_1$
- $H = \text{hash function (coll. resistant)} \text{ from msgs to } G_1$

KeyGen:

$SK = x \leftarrow \mathbb{Z}_q$

$PK = y = g^x \text{ (in } G_1)$

Sign$(m)$:

$\sigma = (H(m))^x \text{ (in } G_1)$

Verify$(PK, m, \sigma)$:

Check $e(g, \sigma) = e(y, H(m))$

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

Thm: BLS sig scheme is existentially unforgeable
against chosen msg attacks in ROH, assuming CDH is hard in $G_1$.

**Application 2: 3-Way Key Agreement**

[Joux, generalizing DH]

Recall DH: $A \to B : g^a$
$B \to A : g^b$
key = $g^{ab}$

Joux: Let $G_1, G_2$ be groups w. bilinear map $e : G_1 \times G_1 \to G_2$ & let $g$ be generator of $G_1$

$A \to B, C : g^a$
$B \to A, C : g^b$
$C \to A, B : g^c$

A computes $e(g^b, g^c)^a = e(g, g)^{abc}$
B $\quad e(g^a, g^c)^b = \quad$ "
C $\quad e(g^a, g^b)^c = \quad$ "

L15.5
key = \( e(g,g)^{abc} \)

Secure assuming Bilinear Diffie-Hellman (BDH) problem is hard:

Given \( g, g^a, g^b, g^c, e \)

hard to compute \( e(g,g)^{abc} \)

4-way key-agreement? Open!

(Multi-linear maps)

Application 3: Identity-based Encryption (IBE)

[Boneh-Franklin 01]

TTP (trusted third party) publishes

\( G, G_2, e \) (bilinear map), \( g \) (generator for \( G_1 \)), \( y \)

where \( y = g^a \), \( a \) is TTP's master secret.

Let \( H_1 \) be RO mapping names (e.g., "alice@mit.edu")

to elements in \( G_1 \)

Let \( H_2 \) be RO mapping \( G_2 \) to msg space.
Goal: Enable anyone to encrypt msg for Alice, knowing only TTP public parameters & Alice's name.

\[ \text{Encrypt} (y, \text{name}, m) : \]

\[ r \in \mathbb{Z}_g^* \quad (q = 1G_1 = 1G_2 \text{ is prime}) \]

Let \( g_A = e(H_1(\text{name}), y) \)

Output \( (g^r, m \oplus H_2(g_A^{-})) \)

Decrypt ciphertext \( c = (u, v) : \)

- Alice obtains \( d_A = (H_1(\text{name}))^a \) from TTP.
  
  Alice’s secret key!
  Needs to obtain this only once.
  Note: TTP also knows it.

- Compute: \( u \oplus H_2(e(d_A, u)) \)
  
  \[ = u \oplus H_2(e(H_1(\text{name})^a, g^r)) \]
  
  \[ = u \oplus H_2(e(H_1(\text{name}), g)^{a \cdot r}) \]
  
  \[ = u \oplus H_2(e(H_1(\text{name}), g^a)^r) \]
\[ = y \oplus H_2 \left( e \left( H_i(name), y \right) \right) \]
\[ = y \oplus H_2 \left( g_A \right) \]
\[ = m \]

**Security**: Semantically secure in ROM assuming BDH (Bilinear Diffie-Hellman Assumption)

\[
\begin{align*}
\text{(Given } g_0, g_5, & \text{ } q, \text{ } q^* \text{ hard} \Rightarrow e(q, g)^{q^*} \\
& \text{ y } \text{ } \text{ } \text{ } \text{ } \text{ } \text{ } \text{ } \text{ } \text{ } \text{ } \text{ } \text{ } \text{ } \text{ } \text{ } \text{ } H_i(name)\text{)}
\end{align*}
\]