4/5/17

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

(Recall DDH: $(g, g^a, g^b, g^c) \cong (g, g^a, g^b, g^{a \cdot b})$

comp. indistinguishable)

Comp. Diffie-Hellman

- CDH is easy

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

Note: CDH is easy $\Longrightarrow$ 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 q, w. generator g.
G_2 group of prime " " " " h.

[We use mult. notation for both groups].

& there exists a bilinear map
$$e : G_1 \times G_1 \longrightarrow G_2$$
s.t.
$$\forall a,b \in G_1 \qquad e(g^a, g^b) = e(g,g)^{a \cdot b}$$
$$e(g,g) = h.$$

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

Bilinear maps are also called pairing functions

They have enumerous applications

<u>Thm</u>: If there exists a bilinear map

$$e : G_1 \times G_1 \longrightarrow G_2$$

between two groups of prime order

then DDH is easy in G_1

<u>Pf</u>: 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"

$\blacksquare$

<u>Note</u>: Even though DDH is easy in G_1, CDH may still be hard.

I.e., we may have a gap group.

<u>How to construct a gap group w. bilinear map?</u>

This is <u>not simple</u>!

G_1 is an elliptic curve (w. certain properties)

e (bilinear map) is a "Weil pairing" or a "Tate pairing".

Application 1: 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 $e: G_1 \times G_1 \to G_2$
- g = generator of G_1
- H = hash function (coll. resistant) from msgs to G_1

KeyGen: $SK = x \leftarrow \{1, \ldots, q-1\}$

$PK = y = g^x$ (in G_1)

Sign(m): $\sigma = (H(m))^x$ (in G_1)

Verify($\underset{\text{"}y\text{"}}{PK}$, m, σ):

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 ROM, assuming CDH is hard in G_1.

Application 2: 3-Way Key Agreement

[Joux, generalizing DH]

Recall DH: $A \to B : g^a$

$B \to A : g^b$

$\text{key} = g^{ab}$

Joux: Let G_1, G_2 be $\overbrace{\text{groups}}^{\text{prime order}}$ 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 " $e(g^a, g^c)^b =$ "

C " $e(g^a, g^b)^c =$ "

$$\text{Key} = e(g,g)^{abc}$$

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
$G_1\, G_2$, 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 (eg. "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.

Encrypt $(\overset{pp}{\downarrow}\atop y$, name, $m)$:

$r \leftarrow \mathbb{Z}_q^*$ $\quad$ ($q = |G_1| = |G_2|$ is prime).

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

Output $\left(g^r,\ m \oplus H_2(g_A^r)\right)$

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

- Alice obtains $d_A = \left(H_1(\text{name})\right)^a$ from TTP.

Alice's secret key!
Needs to obtain this only once.
Note: TTP also knows it.

- Compute: $v \oplus H_2\left(e(d_A, u)\right)$

$$= v \oplus H_2\left(e\left(H_1(\text{name})^a, g^r\right)\right)$$

$$= v \oplus H_2\left(e\left(H_1(\text{name}), g\right)^{a \cdot r}\right)$$

$$= v \oplus H_2\left(e\left(H_1(\text{name}), g^a\right)^r\right)$$

$$= v \oplus H_2\left(e(H_1(\text{name}), y)^r\right)$$
$$= v \oplus H_2(g_A^r)$$
$$= m$$

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

$$\left(\text{Given } \underset{y}{g^a}, g^r, \underset{H_1(\text{name})}{Q} \xrightarrow{\text{HARD}} e(Q,g)^{ar}\right)$$