Today: Groups with bilinear maps, and applications

1. Signature scheme [Boneh-Lynn-Shacham2001]
2. 3-way key agreement [Joux2000]
3. Identity-based encryption [Boneh-Fanklin2001]

Definition:

A finite cyclic multiplicative group G is said to have a bilinear map if there exists a group G' (often called the target group) and there exists a map $e: G \times G \longrightarrow G'$ such that: Let g be a generator of G

1. For every $a,b \in |G|$ $\quad e(g^a, g^b) = e(g,g)^{ab}$
2. $e(g,g) \neq 1$ (degenerate condition)

Claim: For every finite cyclic group G with generator g and bilinear map $e: G \times G \longrightarrow G'$, it holds that for every $a, b \in |G|$:

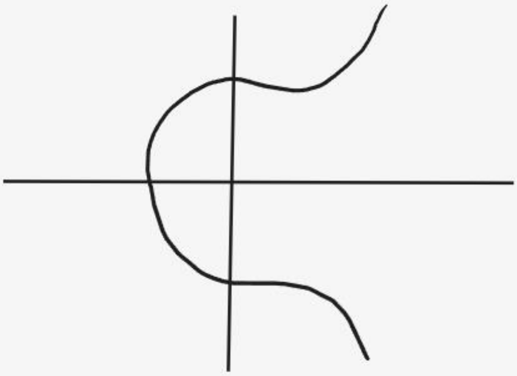
$$e(g^a, g^b) = e(g^{ab}, g) = e(g, g^{ab}) = e(g^b, g^a) = e(g,g)^{ab}$$

Which groups have bilinear maps?? Elliptic curves

Groups which consist of all pairs (x,y) that satisfy the following equation over a finite field F, where $a,b \in F$:

$y^2 = x^3 + ax + b$, and a special point ∞

where this equation has distinct roots.



There is a way of defining multiplication and inverse.

(Often the operation over elliptic curve is described using Additive notation, but we will use multiplicative notation.)

These groups are attractive for several reasons:

1. We don't know how to break discrete log in sub-exp time over these groups.
2. These groups have a bilinear map, sometimes called a (Weil) pairing.

Claim: Let G be a group with bilinear map $e: G \times G \to G'$.

Then DDH assumption is false in G.

Proof: Given g^a, g^b, g^c output 1 if and only if

$e(g^a, g^b) = e(g^c, g)$.

We believe that CDH is true for these groups.

Moreover we believe that the following assumption is true:

(Decisional) Bilinear Diffie Hellman Assumption:

For random a,b,c,d in $\{1, \ldots, |G|\}$

$$g^a, g^b, g^c, g^{abc} \cong g^a, g^b, g^c, g^d$$

Application 1: 3-Way key agreement

This is a generalization of Diffie-Hellman key agreement

Recall:

The Diffie-Hellman key agreement protocol allows 2 parties to agree on a secret key in a secure way against a passive adversary.

We will see how to extend this to 3 parties using a group G with a bilinear map.

Let G be a group of order q with a bilinear map $e: G \times G \longrightarrow G'$

Consider 3 parties: Alice, Bob, and Carol.

Alice chooses a random a in $\{1, \ldots, q\}$ and sends g^a

Bob chooses a random b in $\{1, \ldots, q\}$ and sends g^b

Carol chooses a random c in $\{1, \ldots, q\}$ and sends g^c

The secret key is $e(g,g)^{abc} = e(g^a g^b)^c = e(g^b, g^c)^a$

Secure under the Bilinear Diffie-Hellman (BDH) assumption

Note: If we use this group for a 2-party DH key exchange protocol the secret does not look random, since DDH is false. However, since we believe CDH is true, we can use $H(g^{ab})$ as the key.

Open problem: Extend to more than 3 players (called multilinear map)

Can be done if we allow interaction.

Any function can be computed securely in the interactive setting!

(More about this in 6.875)

Application 2: Short digital signatures

Public parameters: Cyclic group G of order q, a generator g,

and a bilinear map $e: G \times G \longrightarrow G'$,

and a hash function $H: \underset{\substack{\uparrow \\ \text{msg space}}}{\mathcal{M}} \rightarrow G$ modelled as a RO.

Key Gen: Choose a random x in $\{1,\dots,q\}$, let $sk=x$ and $pk=g^{x}$

$\text{Sign}(sk,m) = H(m)^{sk}$

$\text{Ver}(pk,m,\sigma)=1$ if and only if

$$\begin{tikzcd}[column sep=tiny] e(g,\sigma) \arrow[dr, phantom, "\shortparallel"] & = & e(pk,H(m)) \arrow[dl, phantom, "\shortparallel"] \\ & e(g,H(m))^{sk} & \end{tikzcd}$$

Theorem: This signature scheme is secure (against adaptive chosen message attacks) assuming CDH and assuming that H is a RO.

Proof idea:

First note that this scheme is secure if the adv is givem no signatures, since o.w., the adv given a random r in G can compute r^{sk} given only $pk=g^{sk}$ then this adv breaks the CDH assumption.

It remains to note that seeing a signature for a chosen message m is not helpful since the adv can simulate it on its own: he will generate r, r^{sk} by choosing (g^u, pk^u), and setting $H(m) = g^r$, and $\sigma = pk^r$.

Note that $e(g, \sigma) = e(g,g)^{sk \cdot r} = e(pk, H(m))$.

Note: This signature is extremely small since it consists of a single group element, which consists of only 256 bits (since we don't have non-trivial attacks on Discrete Log in elliptic curves we can groups of small order, such as order 256)

Application 3: Identity Based Encryption (IBE)

In public key cryptography we assume that each user has a pk.

How do I know the other user's pk?

We will talk about this more next lecture...

But this question gave rise to the idea of identity based encryption, where the goal is to use "natural" pk's. For example, to use our email address as our pk.

The the question is: How do I generate a sk corresponding to my "name" (say, my email address)? This is precisely what IBE does!

IBE assumes a trusted third party (TTP):

TTP:

1. Choose group G of prime order q, a generator g, and pairing function $e: G \times G \longrightarrow G'$.

2. Choose 2 hash functions: H_1: names $\longrightarrow G$ and $H_2: G' \rightarrow$ msg space, both modelled as ROs.

3. Choose a random secret s in $\{1, \ldots, q\}$.

4. Publish G, G', g, e, H_1, H_2 as public parameters (which we think of as fixed), along with the master public key $MPK = y = g^s$,

Goal:

Allow anyone to encrypt a msg to Alice knowing only PP and Alice's "name".

Alice

Enc((pp, y), name, m):

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

Choose a random r in $\{1,\ldots,q\}$, and output

$(g^r, m \oplus H_2(g_A^r))$.

a la El Gamal

To decrypt this message Alice needs a secret key, which she obtains from the TTP.

$sk_A = H_1(\text{"Alice"})^s$

Dec((pp, sk_A), (u,v)):

Compute: $m = v \oplus H_2(e(sk_A, u))$

Correctness:

To prove correctness we need to argue that

$$\begin{tikzcd}
g_A^r \arrow[d, equal] & = & e(sk_A, u) \arrow[dll, equal] \\
e(H_1(\text{"Alice"}), g)^{sr} & &
\end{tikzcd}$$

Security:

To prove security, by relying on the ROM, we need to argue that given pp, g^s, h, g^r it is hard to compute $e(h,g)^{r \cdot s}$

follows from the BDH assumption.