Pairing Based Crypto

Thursday, November 21, 2019 11:42 AM

Bilinear Groups.

Let G_1, G_2, G_T be cyclic groups

$g_1, g_2,$ ~~g_T~~ are generators.

$$|G_1| = |G_2| = |G_T| = p$$

Defn: a <u>bilinear</u> map or pairing, is a function

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

$$g_T = e(g_1, g_2)$$

Satisfying:

1) $\forall R \in G_1,\ S \in G_2,\ a, b \in \mathbb{Z}_p$

$$e(R^a, S^b) = e(R, S)^{ab} \quad \text{(bilinearity)}$$

2) $e(g_1, g_2) \neq 1$ (id in G_T) (non-degenerate)

Consequences:

- If $\underline{G}_1 = \underline{G}_2$ then

$$e(\underline{R}, \underline{S}) = e(\underline{S}, \underline{R})$$

$R = g^r$ for some r

$S = g^s$ for some s

$$e(R, S) = e(g^r, g^s) = e(g, g)^{\underline{rs}} = e(g^s, g^r)$$

- Can problems involving bilinear groups be hard?

- Suppose DLOG is solvable in G_T. Then can it be hard in $\underline{G}_1$?

Suppose $\mathcal{A}$ solves DLOG in G_T.

$[\, X \xleftarrow{\$} G_T \quad x\ x \,]$ [illegible]

$\Pr[x \leftarrow \mathcal{A}(\underset{\in G_T}{X}) : g_T^x = X] =$ high prob.

$\underline{\mathcal{A}'}(X_1 \in G_1)$:

goal: x sugh that $g_1^x = X_1$

$$x_t \leftarrow \mathcal{A}(e(X_1, g_2))$$

$$g_T^{x_t} = e(X_1, g_2)$$

$$e(g_1, g_2)^{x_t} = e(X_1, g_2)$$

$$\shortparallel$$

$$e(g_1^{x_t}, g_2) = e(X_1, g_2)$$

$$g_1^{x_t} = X_1$$

So output x_t

- Can $\underline{DDH}$ be hard in G? (assume $\underline{G_1} = \underline{G_2} = \underline{G}$)

$\underline{NO}$

$\underline{\mathcal{A}}(\underset{\in G}{A}, \underset{\in G}{B}, \underset{\in G}{X})$ check if $X \overset{?}{=} A^{\log B}$

A is g^a for some a

B is g^b for some b

$$e(g, g) \overset{?}{=} g_T$$

$$e(A, B) \overset{?}{=} e(X, g)$$

$$(a \quad b) \overset{?}{} \quad (x \quad ,)$$

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

$$e(g,g)^{\underline{ab}} \overset{?}{=} e(g,g)^{\underline{X}}$$

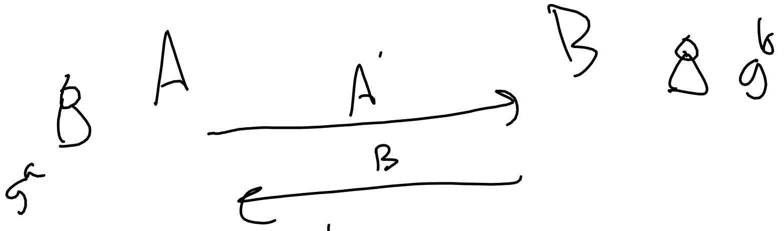
$$ab \overset{?}{=} X$$

Gap-DH

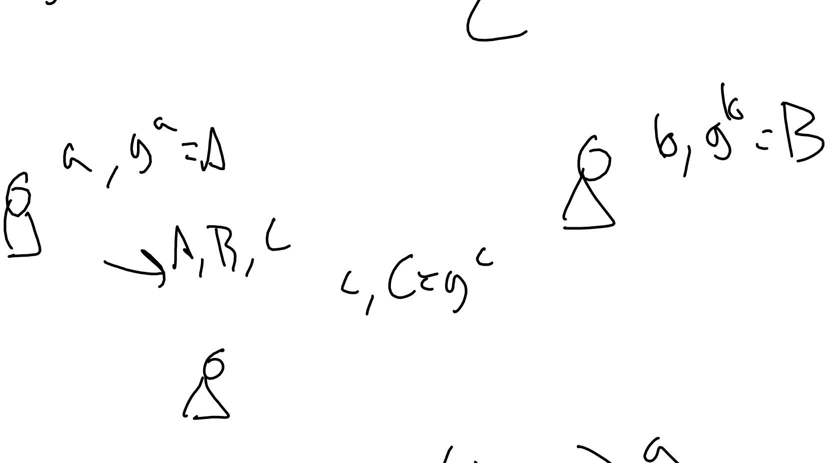
means – Comp. DH is hard

(~~tha~~ we have a pairing so Decisional DH is easy

1st.



$g^{ab} = B^a = A^b$



Alice computes $e(B, C)^a$

Bob $e(A, C)^b$

$e(A, B)^c = e(g,g)^{abc}$

Joux's 3party keyexchange

↑ shared secret

$\longrightarrow A, B, C$

$\rightsquigarrow B^a, C^a$

$, C^b$

A^c Bob $(A^c)^b$

BLS short signatures.

Recall Schnorr signatures

$sk = x, \; X = g^x = pk$

Sign(m):

$k \xleftarrow{\$} \mathbb{Z}_p$

$H(g^k \| m) \in \mathbb{Z}_p$

$s = k - cx$

$\sigma = (K, s)$

$\in G_1 \times \mathbb{Z}_p$

BLS

BLS

$sk = x, \; X = g^x = pk \in G_1$

Sign(m):

$h = \mathcal{H}(X \| m)$ Hash-into-group $\in G_1$

$\sigma = h^x$

Verification (σ, m, X):

$$e(\sigma, g) \overset{?}{=} e(h, X)$$

Sanity check:

$$e(h^x, g) = e(h, g^x) = e(h, g)^x$$