Let G_1, G_2, G_T be cyclic groups of order p (prime)

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

1) Bilinearity:

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

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

$e(x,y) \in G_T$

$g^a, g^b \rightarrow g^{ab}$

2) Non degeneracy: $e(g_1, g_2) \neq \mathbb{1}_T$

$G_1 = \langle g_1 \rangle,\ G_2 = \langle g_2 \rangle$

3) $e(R,S) = \mathbb{1}_T$

$e(R^a, S^b) = \mathbb{1}_T^{ab}$

- Bilinearity (alternate)
  - $\forall R, S \in G_1,\ T \in G_2,\quad e(RS, T) = e(R,T) \cdot e(S,T)$
  - $\forall R \in G_1,\ S, T \in G_2,\quad e(R, ST) = e(R,S) \cdot e(R,T)$

$e(RS, T) = e(g^{r+s}, g^t) = e(g,g)^{(r+s)\cdot t}$
$= e(g,g)^{rt} \cdot e(g,g)^{st}$
$= e(g,T)^{r} \cdot e(g,T)^{s}$
$= e(R,T) \cdot e(S,T)$

- Another Consequence

$e(\mathbb{1}_1, \mathbb{1}_2) \stackrel{?}{=} \mathbb{1}_T$

$e(\mathbb{1}_1^a, \mathbb{1}_2^b) = e(\mathbb{1}_1, \mathbb{1}_2)^{ab} = e(\mathbb{1}_1, \mathbb{1}_2)$

$X_T^{ab} = X_T$

$e(R^0, S^0) = e(R,S)^0$

- Typically: $G_1 = G_2$

$e: G \times G \longrightarrow G_T$

- If discrete log is solvable in G_T, then it is also solvable in G.

Let $(g, X) \in G$, ($X = g^x$ for some x)

$X_T = e(g, X) \in G_T \quad g_T = e(g,g)$

(g, X) such $g^x = X_T$

$e(g, X) = e(g, g^x) = e(g, g)^x = X_T$

- DDH cannot be hard in G,

distinguish $\{g, g^a, g^b, X = g^{ab}\}$

from $\{g, g^a, g^b, X = g^r\}$

Compute $e(g^a, g^b) \stackrel{?}{=} e(g, X)$ if $X = g^{ab}$

$e(g,g)^{ab} \stackrel{?}{=} e(g,g)^{ab}$

- Computational DH can be still be hard

g^a, g^b, find g^{ab}?

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

Defn:
- Gap-DH if DDH is easy, but CDH is hard

Pairings arise in elliptic curves

- Weil pairings
- Tate pairings

Ways of constructing a pairing operation over certain kinds of elliptic curves

Taxonomy of Pairing-Friendly Elliptic Curves,

"Family" (many curves even over same $\mathbb{F}$)
- Sparse
  - MNT
  - GMV
- Complete

"Non-Families" (curve only depends on $\mathbb{F}$)
- Supersingular ($G_1 = G_2$)
- CP-
- DEM

Libraries: PBC, Relic, miracl, Charm

python bindings

$G = \langle g \rangle$

Joux's 3-party key exchange $|G| = p$ prime
$|G_T| = |G|$

Alice	Bob	Carol
$a \xleftarrow{\$} \mathbb{Z}_p$	$b \xleftarrow{\$} \mathbb{Z}_p$	$c \xleftarrow{\$} \mathbb{Z}_p$
$A = g^a$	$B = g^b$	$C = g^c$

Broadcast A, B, C

$e(B,C)^a \qquad e(A,C)^b \qquad e(A,B)^c$

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

Short Signature (BLS)

Recall Schnorr

$$x \xleftarrow{\$} \mathbb{Z}_p, \quad X = g^x \qquad c \in \mathbb{Z}_p \setminus \{0\}$$

$$k \xleftarrow{\$} \mathbb{Z}_p, \quad K = g^k, \quad c = \mathcal{H}(K, m, X)$$

$$s = k - cx, \qquad \sigma = (K, s)$$

$$K \in G, \quad s \in \mathbb{Z}_p$$

$(\mathcal{H} : \{0,1\}^* \to G)$

BLS

gen(1^λ): $x \xleftarrow{\$} \mathbb{Z}_p \quad X = g^x$

sig(m):

$$h = \mathcal{H}(X, m) \in G$$

$$\sigma := h^x \in G$$

Verification(X, m, σ):

$$h = \mathcal{H}(X, m)$$

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

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

Aggregatable Signatures using BLS

(m_i, σ_i) party i signs message m_i $\quad \sigma_i \leftarrow \mathcal{H}(X_i, m_i)^{x_i}$ $\quad$ x_i is party i's secret

(assume all m_i are distinct)

Aggregate $\sigma = \prod_i \sigma_i$ $\qquad$ where $h_i = \mathcal{H}(X_i, m_i)$

To verify: check $e(\sigma, g) \stackrel{?}{=} \prod_i e(h_i, X_i)$

$$e(\sigma, g) = e(h_i^{x_i} \cdot h_{i+1}^{x_{i+1}} \cdots)$$

$g^{\bar{h}_1} = h_1$

$$\rightarrow e(g^{\bar{h}_1 \cdot x_1 + \bar{h}_2 x_2 \cdots}, g)$$

$$= e(g,g)^{\bar{h}_1 \cdot x_1 \cdots}$$

$$= e(g,g)^{(\bar{h}_1 x_1)} e(g,g)^{\bar{h}_2 x_2} \cdots$$

$$= e(g^{\bar{h}_1}, X_1)$$

- New Hard problems:
  - Decisional Bilinear DH

    Distinguish $(g, g^a, g^b, g^c, e(g,g)^{abc})$

    from $(g, g^a, g^b, g^c, e(g,g)^r)$