Contents

0.1 Self-pairing implies failure of DDH

Let $h = e(g_0, g_1)$

$e(a \cdot g_0, b \cdot g_1) = h^{ab}$

$e(\sqrt{y} \cdot g_0, \sqrt{y} \cdot g_1) = h^{\sqrt{y}^2} = h^y$

Check that: $h^y = h^{ab}$

0.2 BLS Signatures are complete

Properties of a bilinear map (elliptic pairing e):

$e(a \cdot x, y) = a \cdot e(x, y) = e(x, a \cdot y)$

$e(x_1, y_1) + e(x_2, y_2) = e(x_1 + x_2, y_1 + y_2)$

Call the signature $\sigma = a * H(m)$, And $H(m)$ is in G_1, so it can also be represented as $H(m) = \phi \cdot g_1$

Starting from

$e(g_0, \sigma) = e(pk, H(m))$

expand inner terms

$e(g0, a \cdot \phi \cdot g_1) = e(a \cdot g_0, \phi \cdot g_1)$

take terms out of e and you see they are equal, so the check is sufficient to prove a correct signature will match a pk with hash of m.

$(a \cdot \phi) \cdot e(g_0, g_1) = (a \cdot \phi) \cdot e(g_0, g_1)$

0.3 BLS signature aggregation

First we show that $e(g_0, \sigma_0 + \sigma_1) = e(g_0, \sigma_0) + e(g_0, \sigma_1)$

By expanding

$e(g_0, (a_0\phi_0 + a_1\phi_1) \cdot g_1)$

Take out the inner term

$(a_0\phi_0 + a_1\phi_1) \cdot e(g_0, g_1)$

Distribute

$(a_0\phi_0) \cdot e(g_0, g_1) + (a_1\phi_1) \cdot e(g_0, g_1)$

Reintroduce terms

$e(g_0, (a_0\phi_0) \cdot g_1) + e(g_0, (a_1\phi_1) \cdot g_1)$

$= e(g_0, \sigma_0 g_1) + e(g_0, \sigma_1 g_1)$

We've shown that an aggregate σ is the same as computing each σ independently. Now we just need to show that $e(g_0, \sigma) = e(pk, H(m))$ (completeness of BLS signatures), which was just proved in 2.