1 PS optimization

1.1 Setup

$$pp \leftarrow (p, \mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, e) \tag{1}$$
$$g \leftarrow \mathbb{G}_1 \tag{2}$$
$$(x, y) \leftarrow \mathbb{Z}_p^2, \tilde{g} \leftarrow \mathbb{G}_2 : (\tilde{X}, \tilde{Y}) \leftarrow (\tilde{g}^x, \tilde{g}^y) \tag{3}$$
$$sk = (x, y), pk = (\tilde{g}, \tilde{X}, \tilde{Y})) \tag{4}$$

g $\leftarrow \mathbb{G}_2$
$(x, y) \leftarrow \mathbb{Z}_p^2, \tilde{g} \leftarrow \mathbb{G}_1 : (\tilde{X}, \tilde{Y}) \leftarrow (\tilde{g}^x, \tilde{g}^y)$

1.2 Join

$$sk_i \leftarrow \mathbb{Z}_p : (\tau, \tilde{\tau}) \leftarrow (g^{sk_i}, \tilde{Y}^{sk_i})) \tag{5}$$
$$u \leftarrow \mathbb{Z}_p : \sigma \leftarrow (\sigma_1, \sigma_2) \leftarrow (g^u, (g^x \tau^y)^u)) \tag{6}$$
$$gsk_i = (sk_i, \sigma, e(\sigma_1, \tilde{Y}), pk = (\tilde{g}, \tilde{X}, \tilde{Y})) \tag{7}$$

1.3 Sign

$$t \leftarrow \mathbb{Z}_p \tag{8}$$
$$(\sigma_1', \sigma_2') \leftarrow (\sigma_1^t, \sigma_2^t) \tag{9}$$
$$k \leftarrow \mathbb{Z}_p : e(\sigma_1', \tilde{Y})^k \leftarrow e(\sigma_1, \tilde{Y})^{kt} \tag{10}$$
$$c \leftarrow H(\sigma_1', \sigma_2', e(\sigma_1', \tilde{Y})^k, m) \tag{11}$$
$$s \leftarrow k + c \cdot sk_i \tag{12}$$
$$\mu(m) = (\sigma_1', \sigma_2', c, s) \in (\mathbb{G}_1^2 \times \mathbb{Z}_p^2) \tag{13}$$

Here we add the G1 element $\tilde{Y}^{-k}$ to the signature to be able to verify it with pairing check
$\mu(m) = (\sigma_1', \sigma_2', \tilde{Y}^{-k}, c, s) \in (\mathbb{G}_1^3 \times \mathbb{Z}_p^2)$

1.4 Verify

$$R \leftarrow (e(\sigma_1^{-1}, \tilde{X}) \cdot e(\sigma_2, \tilde{g}))^{-c} \cdot e(\sigma_1^s, \tilde{Y}) \tag{14}$$
$$c \stackrel{?}{=} H(\sigma_1, \sigma_2, R, m) \tag{15}$$

Correctness comes from :

$$e(\sigma_1, \tilde{X} \cdot \tilde{Y}^m) = e(\sigma_2, \tilde{g}) \tag{16}$$

From 14, we want to check:

$$e(\sigma_1, \tilde{Y})^k \stackrel{?}{=} (e(\sigma_1^{-1}, \tilde{X}) \cdot e(\sigma_2, \tilde{g}))^{-c} \cdot e(\sigma_1^s, \tilde{Y}) \tag{17}$$

Exchanging the groups for signatures and public keys we have:

$$e(\tilde{Y}, \sigma_1)^k \stackrel{?}{=} (e(\tilde{X}, \sigma_1^{-1}) \cdot e(\tilde{g}, \sigma_2))^{-c} \cdot e(\tilde{Y}, \sigma_1^s) \tag{18}$$

$$e(\tilde{X}, \sigma_1)^{-c} \cdot e(\tilde{Y}, \sigma_1)^k \cdot e(\tilde{Y}, \sigma_1^s)^{-1} \stackrel{?}{=} e(\tilde{g}, \sigma_2)^{-c} \tag{19}$$

$$e(\tilde{X}^{-c}\tilde{Y}^{k-s}, \sigma_1) \stackrel{?}{=} e(\tilde{g}, \sigma_2)^{-c} \tag{20}$$

$$e(\tilde{X}^c\tilde{Y}^{s-k}, \sigma_1) \stackrel{?}{=} e(\tilde{g}^c, \sigma_2) \tag{21}$$

Finally the verification takes one pairing check and one hash check.

$$e(\tilde{X}^c\tilde{Y}^{s-k}, \sigma_1) \stackrel{?}{=} e(\tilde{g}^c, \sigma_2) \tag{22}$$

$$c \stackrel{?}{=} H(\sigma_1, \sigma_2, \tilde{Y}^{-k}, m) \tag{23}$$

1.4.1 Completeness

$$e(\tilde{X}^c\tilde{Y}^{s-k}, \sigma_1) \stackrel{?}{=} e(\tilde{g}^c, \sigma_2) \tag{24}$$

$$e(\tilde{X}^c\tilde{Y}^{c \cdot sk_i}, \sigma_1) \stackrel{?}{=} e(\tilde{g}^c, \sigma_2) \tag{25}$$

$$e(\tilde{X}\tilde{Y}^{sk_i}, \sigma_1)^c \stackrel{?}{=} e(\tilde{g}, \sigma_2)^c \tag{26}$$

$$e(\tilde{X}\tilde{Y}^{sk_i}, \sigma_1) \stackrel{?}{=} e(\tilde{g}, \sigma_2) \tag{27}$$

Which is a valid signature on sk_i.

1.4.2 Cost

The on-chain verification is constrained on:

- efficiency in terms of gas
- operations with only pairing check possible, no pairing operation

It needs 3 exponentiations (scalar multiplications for ECC) and 2 multiplications (point additions for ECC), along with the hash check operation.

1.5 Open

$$\forall (i, \tau_i, \tilde{\tau}_i) : e(\sigma_2, \tilde{g}) \cdot e(\sigma_1, \tilde{X})^{-1} \stackrel{?}{=} e(\sigma_1, \tilde{\tau}_i) \tag{28}$$

$$\forall (i, \tau_i, \tilde{\tau}_i) : e(\tilde{g}, \sigma_2) \cdot e(\tilde{X}, \sigma_1)^{-1} \stackrel{?}{=} e(\tilde{\tau}_i, \sigma_1) \tag{29}$$