RING SCHNORR SIGNATURE

RSign(m, x_j, Y)

for each $i \in \{1, \dots, n\}$ $i \neq j$

$a_i \leftarrow_R \mathbb{Z}_q$

$r_i \leftarrow g^{a_i}$

$h_i \leftarrow \mathcal{H}(m, r_i)$

$a_j \leftarrow_R \mathbb{Z}_q$

$r_j \leftarrow g^{a_j} \prod_{i \neq j} y_i^{-h_i}$

$h_j \leftarrow \mathcal{H}(m, r_j)$

$s \leftarrow a_j + x_j h_j + \sum_{i \neq j} a_i = \sum_i a_i + x_j h_j$

$R = \{r_1, \dots, r_n\}$

ret $\sigma = (R, s)$

RVerify

for each $i \in \{1, \dots, n\}$

$h_i = \mathcal{H}(m, r_i)$

if $g^s = \prod_i r_i y_i^{h_i}$

true

else

false

KeyGen(G)

$\cancel{\{(x_i, g^{x_i})\}}$ $\{(x_i, g^{x_i} = X_i)\}_i$

$X = \{x_1, \dots, x_n\} : x_i \leftarrow \mathbb{Z}_q^*$

$Y = \{g^{x_1}, \dots, g^{x_n}\}$

The scheme is correct if $\Pr\left[\begin{array}{l} G \leftarrow \mathrm{Str}(\xi), Y = \{y_i : (x_i, y_i) \leftarrow \mathrm{KeyGen}(G)\}, \sigma \leftarrow \mathrm{RSign} \\ (m, x_j, Y) : \mathrm{RVerify}(m, \sigma, Y) = 1 \end{array}\right] = 1$

Proof: 1

$\cancel{g^s = g^{\sum a_i + x_j h_j} = \prod_i g^{a_i} \cdot g^{x_j h_j} = \prod_i r_i \cdot (g^{x_j})^{h_j} = \prod_i r_i y_i^{h_i} = R}$

the scheme is unforgeable if $\Pr\left[\begin{array}{l} G \leftarrow \mathrm{Str}(\xi), Y = \{y_i : (x_i, y_i) \leftarrow \mathrm{KeyGen}(G)\}, m \in \{m_i\} \\ \{(m_i, \sigma_i)\}_i \leftarrow \mathcal{A}^{O_{\mathrm{sign}}(\cdot)}(Y) : \mathrm{RVerify}(m^*, \sigma^*, Y) \to 1 \end{array}\right]$

$\leq A$ negl.

$\{(m^*, \sigma^*) \leftarrow \mathcal{A}(Y), \ \{(m_i, \sigma_i)\} = V, \ (m^*, \sigma^*) \notin V$

$O_{\mathcal{H}}()$

$\cancel{\prod_i r_i y_i}$

$\cancel{\left(\prod_i r_i\right) \cdot y_j^{h_j}}$

Proof

Simulation

Sim(Y, m)

for each $i \in \{1, \dots, n\}$ $i \neq j$

$a_i \leftarrow_R \mathbb{Z}_q$

$r_i \leftarrow g^{a_i}$

for each $i \in \{1, \dots, n\}$ with j

$h_i \leftarrow_R \mathbb{Z}_q$

$s \leftarrow_R \mathbb{Z}_q$

$r_j = (g^s / g^{\sum_{i \neq j} a_i}) \cdot \prod_i y_i^{-h_i}$

$R = \{r_i\}_i$

return $\sigma(R, s)$

m, r_1	h_1
$\vdots$	$\vdots$
m, r_i	h_i
$\vdots$	$\vdots$
m, r_n	h_n

By the power of forking lemma
$\mathcal{A}$ has $(m, r_1 \dots r_n, h_1 \dots h_n, s)$ such that $h_j \neq h_j'$
$(m, r_1 \dots r_n, h_1' \dots h_n', s')$ (one pair)

$$g^s = r_1 \cdot \dots \cdot r_n \cdot y_1^{h_1} \cdot \dots \cdot y_j^{h_j} \cdot \dots \cdot y_n^{h_n}$$
$$g^{s'} = r_1 \cdot \dots \cdot r_n \cdot y_1^{h_1} \cdot \dots \cdot y_j^{h_j'} \cdot \dots \cdot y_n^{h_n}$$
$$g^{s-s'} = y_i^{h_j - h_j'} \Rightarrow y_i = \left(g^{s-s'}\right)^{\frac{1}{h_j - h_j'}} = g^{\frac{s-s'}{h_j - h_j'}}$$
$$y_i = g^{x_j} \quad x_j = \frac{s-s'}{h_j - h_j'}$$ what breaks DLP

3. Anonimity
$Pr[\sigma \leftarrow RSign(m, Y, x_i) \quad D(Y, \sigma) \to \hat{i} \quad \hat{i} = i] < \cancel{\text{negligible}} + \frac{1}{n}$
Scheme is anonymous if with non-negligible probability distinguisher is not able to tell which signer signed a message

?

Proof of anonim.: Let $SIG = (m, r_1 \dots r_n, h_1, \dots h_n, s)$ is a valid signature of a message m. Let U_j be a member of ring. Now, we find the probability that U_j computes exactly the SIG. The probability that U_j computes pairwise different r_i and $r_i \neq 1$ where $i \neq j$ is $\frac{1}{q-1} \cdot \frac{1}{q-2} \cdots \frac{1}{q-n+1} = P_1$
Then the prob. that U_j computes $a_j \leftarrow \mathbb{Z}_q$ that leads to r_j such that $r_j \neq r_i$ for all $i \in \{1 \dots n\}$ $i \neq j$ is $\frac{1}{q-n} = P_2$
Summing $P_1 \cdot P_2 = \frac{1}{q-1} \cdots \frac{1}{q-n}$ and this prob. doesn't depend on so it is the same for all member of ring

(1) $1 \dots n$

$i \neq j$: a_i, $r_i = g^{a_i}$

a_j, $r_j = g^{a_j} \prod_{i \neq j} y_i^{-h_i}$

$$g^s = g^{x_j h_j + \sum_{i=1}^{n} a_i} =$$

$$= y_j^{h_j} \cdot g^{a_j} \cdot \prod_{\substack{i=1 \\ i \neq j}}^{n} g^{a_i} =$$

$$= y_j^{h_j} \cdot \left(r_j \cdot \prod_{i \neq j} y_i^{+h_i} \right) \cdot \prod_{i \neq j} g^{a_i} =$$

$$= \left(y_j^{h_j} \cdot r_j \right) \cdot \prod_{i \neq j} y_i^{h_i} g^{a_i} =$$

$$= \prod_{i=1}^{n} r_i y_i^{h_i}$$