→ Authentication: Ft

* Users provide SP with t_k and proves in ZK that $t_0 \dots t_{k-1}$ don't belong in blacklist
* On successful authentication, user generates t_{k+1} & drops t_k from g

→ Ticket $t_k \in \Pi_{l_t=166}$ → set of primes with almost 166 bits

$|\Pi_{166}| \approx 2^{160}$

Ticket domain $T = [-2^{l_T}+1, 2^{l_T}-1]$, where $l_T = 330$

→ Ticket Acc

→ Keygen: On input security param$_{acc} = l_N$,

- Choose $N = pq$, where N is an l_N-bit safe prime.
- Pick $g \in_R QR_N$
- $sk_{acc} = \phi(N)$ $pk_{acc} = (l_n, N, g)$ $l_N = 1024$

→ Accumulating tickets ~~$t \in T$~~.

- Accumulate $(V, t) \to V' = V^t \bmod N$
- $acc_0 = g$
- $\therefore acc_{\{t_1,\dots,t_k\}} = g^{t_1 t_2 \dots t_k} \pmod N$ → S_T

→ Non-membership witness

If $V = acc_{S_T}$ for $S_T \subset T$ & $t \in T \setminus S_T$, then

$\exists\ w = (a, d) \in \mathbb{Z}_{[2^{l_t}]} \times QR_N$ for t w.r.t. V s.t. t is non-member of V if $V^a \equiv d^t g$

→ witness update

Given w, t s.t. $1 = \text{Isnonmember}(t, V, w)$, for $V' = V^{t'}$, anyone can compute w' s.t. $1 = \text{Isnonmember}(t, V', w')$

→ ZKPoK of non membership

- $PK\{(Q[\cdot], w) : 1 = \text{Isnonmember}(Q[\cdot], V, w)\}$
- Proof in Li paper

→ Proving integrity of the queue (QueueSig)

→ KeyGen $(l_N, l_s, l_0, l_T, l, \delta_n)$

- Choose l_N bit safe prime product $N = pk$ & $b, c, g_0, \dots, g_k \in_R QR_N$
- $sk_{sig} = \phi(N)$ $pk_{sig} = (\text{Commit}_{sig}, N, b, c, g_0, \dots, g_k)$

→ Signature Request

- $Q = (t_i)_{i=0}^{k}$
- Alice picks $r \in_R \Delta(l_N, \delta_n)$ and computes commitment
  $\text{Commit}(Q, r) \to C = c^r \prod_{i=0}^{k} g_i^{t_i} \bmod N$
  and sends C to SP
- Proof of correctness: $PK\{(Q, r): C = \text{Commit}(Q, r) \wedge Q \in \mathcal{Q} \wedge r \in \mathbb{R}\}$

→ Signing

- $\text{Sign}(C, sk_{sig}) \to \bar{\sigma} = (r', e, v)$ where $r' \in_R \Lambda_{l_s}$, $e \in_R \Pi_{l_e}$ & $v = (b c^{r'} C)^{1/e \bmod \phi(N)} \pmod N$

→ Finalizing

- $\text{Finalize}(\bar{\sigma}, r) \to \sigma = (r + r', e, v)$

→ Verification

$\text{Verify}(Q, \sigma) = \begin{cases} 1 & \text{if } v^e = b c^s \prod_{i=0}^{k} g_i^{t_i} \wedge e > 2^{l_e - 1} \\ 0 & \text{otherwise} \end{cases}$

→ ZKPOK for verification

- $PK\{(Q, \sigma): 1 = \text{Verify}(Q, \sigma) \wedge Q \in \mathcal{Q}\}$
- Proof standard for CL signatures.

→ ZKPOK of relation b/w two queues