Setup(n)

1 : Choose prime-order group $\mathbb{G} = \langle g \rangle$ of order q.
2 : Select domain-separated hashes H_{agg}, $H_{\text{musig-non}}$, H_{chal}, $H_{\text{frost-non}}$.
3 : Return $(\mathbb{G}, g, q, H_{\text{agg}}, H_{\text{musig-non}}, H_{\text{chal}}, H_{\text{frost-non}})$.

KeyAgg(L) **// MuSig2 key aggregation**

1 : $L := (X_1, \ldots, X_n)$ is ordered; let $[n] = \{1, \ldots, n\}$.
2 : For $i \in [n]$: $a_i \leftarrow H_{\text{agg}}(L, X_i)$.
3 : $\widetilde{X} \leftarrow \prod_{i=1}^{n} X_i^{a_i}$.
4 : Return $\widetilde{X}$.

Indexing (session-scoped)

1 : Predicate $f : [n] \to \{0, 1\}$; $F := \{\, i \in [n] : f(i) = 1 \,\}$ (FROST-backed).
2 : For each $i \in F$: fix $Q_i = \{1, \ldots, q_i\}$, threshold t_i, and choose $S_i \subseteq Q_i$ with $|S_i| \geq t_i$.
3 : Dependent set $K := \{\, (i, \alpha) : i \in F,\ \alpha \in S_i \,\}$.

PreRoundFROST(i, α) $(i, \alpha) \in K$

1 : $d_{i,\alpha} \xleftarrow{\$} \mathbb{Z}_q$; $e_{i,\alpha} \xleftarrow{\$} \mathbb{Z}_q$.
2 : $D_{i,\alpha} \leftarrow g^{d_{i,\alpha}}$; $E_{i,\alpha} \leftarrow g^{e_{i,\alpha}}$.
3 : $\text{state}_{i,\alpha} \leftarrow (d_{i,\alpha}, e_{i,\alpha})$.
4 : Return $(\text{state}_{i,\alpha}, (D_{i,\alpha}, E_{i,\alpha}))$.

PreAggFROST$(i, \{(D_{i,\alpha}, E_{i,\alpha})\}_{\alpha \in S_i})$ $i \in F$

1 : $D_i \leftarrow \prod_{\alpha \in S_i} D_{i,\alpha}$; $E_i' \leftarrow \prod_{\alpha \in S_i} E_{i,\alpha}$.
2 : $b_i' \leftarrow H_{\text{frost-non}}(X_i, S_i, \rho_i, m)$
3 : $E_i \leftarrow (E_i')^{\,b_i'}$.
4 : Return (D_i, E_i).

Lagrange(S_i, α)

1 : $\Lambda_{i,\alpha} \leftarrow \prod_{\beta \in S_i \setminus \{\alpha\}} \beta/(\beta - \alpha)$
2 : Return $\Lambda_{i,\alpha}$.

PreRoundATOM(i) $i \in A := [n] \setminus F$

1 : $d_i \xleftarrow{\$} \mathbb{Z}_q$; $e_i \xleftarrow{\$} \mathbb{Z}_q$.
2 : $D_i \leftarrow g^{d_i}$; $E_i \leftarrow g^{e_i}$.
3 : $\text{state}_i \leftarrow (d_i, e_i)$.
4 : Return $(\text{state}_i, (D_i, E_i))$.

PreAggMUSIG$\big(m, L, \{(D_i, E_i)\}_{i=1}^{n}\big)$

1 : $D \leftarrow \prod_{i=1}^{n} D_i$; $E \leftarrow \prod_{i=1}^{n} E_i$.
2 : $b \leftarrow H_{\text{musig-non}}(\widetilde{X}, L, (D, E), m)$.
3 : $R \leftarrow D \cdot E^{\,b}$.
4 : $c \leftarrow H_{\text{chal}}(\widetilde{X}, R, m)$.
5 : Return (b, R, c).

SignRoundFROST$(i, \alpha, \text{state}_{i,\alpha}, b_i', b, c, x_{i,\alpha}, S_i, a_i)$

1 : $(d_{i,\alpha}, e_{i,\alpha}) \leftarrow \text{state}_{i,\alpha}$.
2 : $\Lambda_{i,\alpha} \leftarrow \text{Lagrange}(S_i, \alpha)$.
3 : $z_{i,\alpha} \leftarrow d_{i,\alpha} + e_{i,\alpha}\, b_i'\, b + a_i\, \Lambda_{i,\alpha}\, x_{i,\alpha}\, c$.
4 : Return $z_{i,\alpha}$.

SignAggFROST$(i, \{z_{i,\alpha}\}_{\alpha \in S_i})$ $i \in F$

1 : $z_i \leftarrow \sum_{\alpha \in S_i} z_{i,\alpha}$
2 : Return z_i.

SignRoundATOM$(i, \text{state}_i, b, c, x_i, a_i)$ $i \in A$

1 : $(d_i, e_i) \leftarrow \text{state}_i$.
2 : $z_i \leftarrow d_i + e_i b + a_i x_i c$.
3 : Return z_i.

SignAgg_MUSIG$\big(\{z_i\}_{i=1}^{n}, R\big)$

1 : $s \leftarrow \sum_{i=1}^{n} z_i$; $\sigma \leftarrow (R, s)$.
2 : Return σ.

Verify$(L, \widetilde{X}, m, \sigma)$

1 : $(R, s) \leftarrow \sigma$; $c \leftarrow H_{\text{chal}}(\widetilde{X}, R, m)$.
2 : Return $\big(g^{\,s} \stackrel{?}{=} R \cdot \widetilde{X}^{\,c}\big)$.

Figure 1: Nested FROST3 inside MuSig2. Inner clusters use one FROST3 nonce coefficient b_i' per cluster; outer layer uses MuSig2 nonce coefficient b.