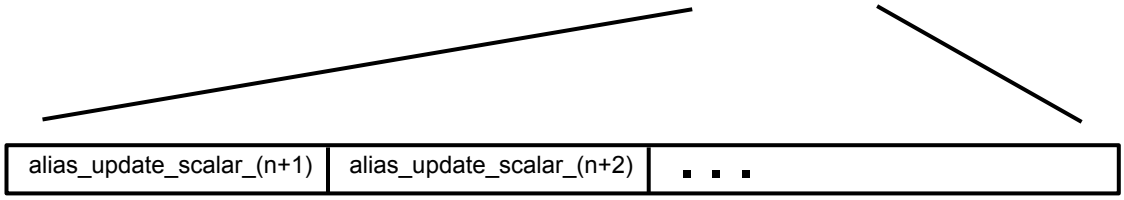
Alice shares: *timing_secret, ID_secret*

Phase 1) Bob computes:

period_start = current_time - (PERIOD_LENGTH % current_time)

Generate alias_update_scalars:

SHA-256(timing_secret, period_start, n) = timing digest



Generate alias_update_times:

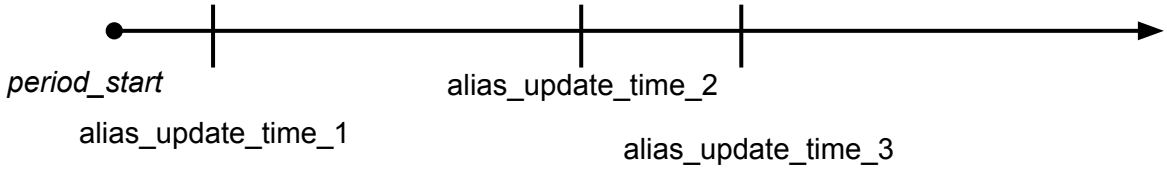
alias_update_time_1 = period_start + MIN_UPDATE +

(alias_update_scalar_1 / max_alias_update_scalar) (MAX_UPDATE - MIN_UPDATE),

alias_update_time_n = alias_update_time_(n-1) + MIN_UPDATE +

(alias_update_scalar_n / max_alias_update_scalar) (MAX_UPDATE - MIN_UPDATE),

If current_time < alias_update_time_1,
recompute using previous period.



last_update_time is the largest alias_update_time that does not exceed current_time.

Phase 2) Bob computes:

current_pseudonym = SHA-256(timing_secret, period_start)