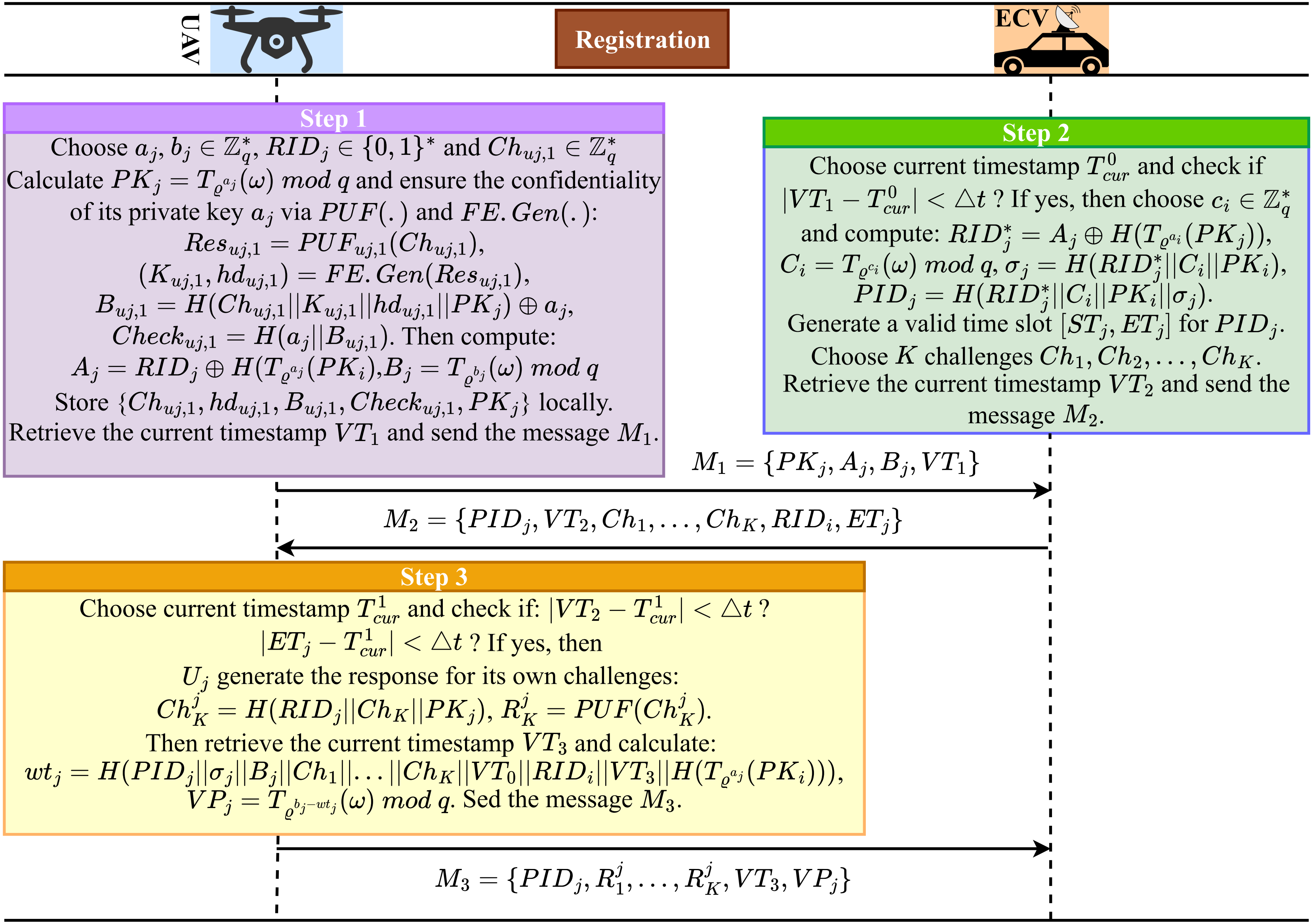

Step 1

Choose $a_j, b_j \in \mathbb{Z}_q^*$, $RID_j \in \{0,1\}^*$ and $Ch_{uj,1} \in \mathbb{Z}_q^*$
Calculate $PK_j = T_{\varrho^{a_j}}(\omega)\ mod\ q$ and ensure the confidentiality of its private key a_j via $PUF(.)$ and $FE.Gen(.)$:

$Res_{uj,1} = PUF_{uj,1}(Ch_{uj,1})$,
$(K_{uj,1}, hd_{uj,1}) = FE.Gen(Res_{uj,1})$,
$B_{uj,1} = H(Ch_{uj,1}||K_{uj,1}||hd_{uj,1}||PK_j) \oplus a_j$,
$Check_{uj,1} = H(a_j||B_{uj,1})$. Then compute:
$A_j = RID_j \oplus H(T_{\varrho^{a_j}}(PK_i)$,$B_j = T_{\varrho^{b_j}}(\omega)\ mod\ q$
Store $\{Ch_{uj,1}, hd_{uj,1}, B_{uj,1}, Check_{uj,1}, PK_j\}$ locally.
Retrieve the current timestamp VT_1 and send the message M_1.

Step 2

Choose current timestamp T_{cur}^0 and check if $|VT_1 - T_{cur}^0| < \triangle t$? If yes, then choose $c_i \in \mathbb{Z}_q^*$ and compute: $RID_j^* = A_j \oplus H(T_{\varrho^{a_i}}(PK_j))$,
$C_i = T_{\varrho^{c_i}}(\omega)\ mod\ q$, $\sigma_j = H(RID_j^*||C_i||PK_i)$,
$PID_j = H(RID_j^*||C_i||PK_i||\sigma_j)$.
Generate a valid time slot $[ST_j, ET_j]$ for PID_j.
Choose K challenges $Ch_1, Ch_2, \ldots, Ch_K$.
Retrieve the current timestamp VT_2 and send the message M_2.

$M_1 = \{PK_j, A_j, B_j, VT_1\}$

$M_2 = \{PID_j, VT_2, Ch_1, \ldots, Ch_K, RID_i, ET_j\}$

Step 3

Choose current timestamp T_{cur}^1 and check if: $|VT_2 - T_{cur}^1| < \triangle t$?
$|ET_j - T_{cur}^1| < \triangle t$? If yes, then
U_j generate the response for its own challenges:
$Ch_K^j = H(RID_j||Ch_K||PK_j)$, $R_K^j = PUF(Ch_K^j)$.
Then retrieve the current timestamp VT_3 and calculate:
$wt_j = H(PID_j||\sigma_j||B_j||Ch_1||\ldots||Ch_K||VT_0||RID_i||VT_3||H(T_{\varrho^{a_j}}(PK_i)))$,
$VP_j = T_{\varrho^{b_j - wt_j}}(\omega)\ mod\ q$. Sed the message M_3.

$M_3 = \{PID_j, R_1^j, \ldots, R_K^j, VT_3, VP_j\}$