In this algorithm, $Ppub$ is the master public key, the identity of the vehicle $V$is represented as ID_v, the public key is represented as $PK_v = (X_v, R_v)$, and the private key is represented as $SK_v = (x_v, y_v)$. Similarly, the identity of the RSU_i is represented as ID_i, the public key is represented as $PK_i = (X_i, R_i)$, and the private key is represented as $SK_i = (x_i, y_i)$. The output T is the temporary key, the σ is the signature of the vehicle V, and A is set to the array $\{a_0, a_1, \cdots, a_{n-1}\}$.

Algorithm 1 Message Generation Algorithm

Input: X_V, R_v, X_i, R_i, x_v, y_v, ID_i, ID_v, P_{pub}
Output: T, σ, A
1: $t = \text{rand}()$;
2: $T = tP$;
3: $h_1 = Hash(ID_i, X_i, R_i, P_{pub})$;
4: $Q_i = (x_v + y_v + t) * (X_v + R_v + h_1 Ppub)$
5: $\gamma_i = Hash2(Q_i)$
6: k=rand();
7: $f(x) = \prod_{i=1}^{n}(x - \gamma_i) + k \pmod q = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$; //set A to $\{a_0, a_1, \cdots, a_{n-1}\}$
8: $h_3 = Hash3(ID_v, T, k, A)$;
9: $h_4 = Hash4(ID_v, T, k, A)$;
10: $h_5 = Hash5(ID_v, T, k, A)$;
11: $\sigma = h_3 * (t + k) + h_4 * x_v + h_5 * y_v$;
12: Return T, σ, A.

In this algorithm, the input has the same meaning as in **Algorithm 1**, T_i in the output is the temporary key of the RSU_i, and σ_i is the signature of the RSU_i.

Algorithm 2 RSU_i Authentication Algorithm

Input: T, σ, A,X_V, R_v, X_i, R_i,P_{pub},x_i, y_i
Output: T_i, σ_i
1: $h_v = Hash(ID_v, X_v, R_v, P_{pub})$;
2: $Q_i' = (x_i + y_i) * (X_v + R_v + h_v P_p ub + T)$
3: $\gamma_i' = Hash2(Q_i')$;
4: $k' = f(\gamma_i') = \gamma_i^{'n} + a_(n-1)\gamma_i^{'n-1} + ... + a_1\gamma_i' + a_0$;
5: $h_3' = Hash3(ID_v, T, k', A)$;
6: $h_4' = Hash4(ID_v, T, k', A)$;
7: $h_5' = Hash5(ID_v, T, k', A)$;
8: $\sigma' * P = h_3' * (T + k'P) + h_4' * X_v + h_5' * (R_v + h_v * P_{pub})$;
9: **if** $\sigma P == \sigma' P$ **then**
10: RSU_i authenticates the identity of Vehicle V as legitimate;
11: **else**
12: break;
13: **end if**
14: $t_i = \text{rand}()$;
15: $T_i = t_i * P$
16: $h_6 = Hash6(ID_i, T_i, k')$;
17: $h_7 = Hash7(ID_i, T_i, k')$;
18: $h_8 = Hash8(ID_i, T_i, k')$;
19: $\sigma_i = h_6 * (t_i + k') + h_7 * x_i + h_8 * y_i$;
20: Return T_i, σ_i.

The meaning of the input parameters in this algorithm is the same as in **algorithm 2**, and the legitimate in the output indicates whether the vehicle V is valid to verify the RSU_i identity.

Algorithm 3 Vehicle Authentication Algorithm

Input: T_i, σ_i, ID_i, X_i, R_i
Output: legitimate
1: $h'_6 = Hash6(ID_i, T_i, k)$;
2: $h'_7 = Hash7(ID_i, T_i, k)$;
3: $h'_8 = Hash8(ID_i, T_i, k)$;
4: $\sigma'_i P = h'_6(T_i + kP) + h'_7 X_i + h'_8(R_i + h_1 P_{pub})$;
5: **if** $\sigma_i P == \sigma'_i P$ **then**
6: Vehicle V authenticates the identity of RSU_i as legitimate;
7: legitimate=1
8: **else**
9: legitimate=0;
10: **end if**
11: Return legitimate.