V_i: i^{th} vehicle
LTC_V_i: Long Term Certificate of ith vehicle
$L_1C\_V_i$: Linkage Certificate provided by LA_1 for the ith vehicle
$L_2C\_V_i$: Linkage Certificate provided by LA_2 for the ith vehicle
SK_V_i : Private key generated by LA_1 for the ith vehicle
PK_V_i : Public key generated by LA_1 for the ith vehicle
PLV   : Pre-Linkage Value
LV   : Linkage Value
$E\{x\}_y$:   Encryption of x using the public key of y

PCA

$LV_{i1} = PLV1_{i1} \oplus PLV2_{i1}$
$PC \leftarrow LV_{i1}$

6) $E\{PLV1_{i1}\}_{PCA}$; $E\{PLV2_{i1}\}_{PCA}$

8) $E\{PC\}_{Vi}$

LA$_1$

5) $E\{PLV_{i1}\}_{PCA}$

4) $E\{LA_1C\_V_i\}_{LA1}$

V_i:
PK_V_i, SK_V_i
Random: m_{i0}, r_{i0}
$H_i(m_{i0}, r_{i0})$
$m_{i1}, r_{i1} \mid m_{i2}, r_{i2} \mid m_{i3}, r_{i3} \mid \ldots$
$PLV1_{i1} = m_{i1} \oplus r_{i1}$

1) $V_i \rightarrow$ RA:
$E\{LA_1C\_V_i\}_{LA1}$, $E\{LA_2C\_V_i\}_{LA2}$, $E\{LTC\_V_i\}_{LTCA}$

Vehicle (V_i)

RA

9) $E\{PC\}_{Vi}$

LTC_V_i
$LA_1C\_V_i$
$LA_2C\_V_i$

4') $E\{LA_2C\_V_i\}_{LA2}$

5') $E\{PLV_{i2}\}_{PCA}$

2) Valid?

3) Yes /No

LTCA

LA$_2$

V_i:
PK'_V_i, SK'_V_i
Random: m'_{i0}, r'_{i0}
$H_i(m'_{i0}, r'_{i0})$
$m'_{i1}, r'_{i1} \mid m'_{i2}, r'_{i2} \mid m'_{i3}, r'_{i3} \mid \ldots$
$PLV2_{i1} = m'_{i1} \oplus r'_{i1}$

Butterfly keys scheme

ITSS-V | RA | PCA

$$\begin{cases} B_\iota = A + f1(ck, \iota) * \mathcal{G} \ (signing\ keys), \\ Q_\iota = P + f2(ek, \iota) * \mathcal{G} \ (encryption\ keys) \end{cases}$$

$$\begin{cases} b_\iota = a + f1(ck, \iota) \ (signing\ keys) \\ q_\iota = p + f2(ek, \iota) \ (encryption\ keys) \end{cases}$$

Generate AES Keys ck and ek

Generate $(a, A = a.G)$
$(p, P = p.G)$

Send(ck, ek, A, P)

For each ι
Generate (B_ι, Q_ι)
Send (B_ι, Q_ι)

For each (B_ι, Q_ι)
Generate $(c, C = c.G)$
$B_\iota + C$
Encrypt Response using Q_ι
Encrypt $(Q_\iota, ((B_\iota + C), c))$

Relay Encryption $(Q_\iota, ((B_\iota + C), c))$

Send Encryption $(Q_\iota, ((B_\iota + C), c))$

Compute q_ι
Decipher response using q_ι
Compute b_ι
Compute private key $b_\iota + c$
Verify compliance priv/Pub