$\boldsymbol{GlobalSetup}(k)$
$GP = \{p, G_1, G_2, G_T, e, g, \tilde{g}, H, H'\}$
$e: G_1 \times G_2 \to G_T, g \in G_1, \tilde{g} \in G_2, H: \{0,1\}^* \to Z_p^*, H': G_T \to G_1$

$\boldsymbol{KeyGen_{Ser}}(GP)$
$pk_s = \left(X, \tilde{V}\right), X = g^x, x \in Z_p^*, \tilde{V} \in G_2^*$
$sk_s = x$

$\boldsymbol{KeyGen_R}(GP)$
$pk_i = Y_i = \tilde{g}^{y_i}$
$sk_i = y_i \in Z_p^*$

$\boldsymbol{PECK1}(GP, pk_s, pk_i, W)$
$C_i = (C_{i,1}, C_{i,2}, C_{i,3}, B_\varphi, 0 \le \varphi \le n+1,)$
$W = (w_1, w_2, \cdots, w_n, \tau \in Z_p^*)$
$f(x) = \left(x - H(w_1)\right)\left(x - H(w_2)\right)\cdots\left(x - H(w_n)\right)(x - \tau) + 1$
$= \eta_{n+1}x^{n+1} + \eta_n x^n + \cdots + \eta_1 x + \eta_0 + 1$
$= 1$

在方程$f(x)$中,η_{n+1}是x^{n+1}的系数，η_{n+1}是加密的内容

$$t = e(X, \tilde{V})^s, C_{i,1} = g^s, C_{i,2} = t \cdot e(X, Y_i)^r, C_{i,3} = \tilde{g}^r, B_\varphi = C_{i,3}^{\eta_\varphi}, 0 \le \varphi \le (n+1)$$

s, r都是随机整数

$\boldsymbol{Trapdoor1}(GP, pk_s, sk_i, Q)$
$T_{i,Q} = \left(T_{i,-1}, T_{i,-2}, T_{i,\varphi}\right), 0 \le \varphi \le (n+1)$
$Q = (q_1, q_2, \cdots, q_m),, m \le l$

$T_{i,-1}, \zeta$是随机整数

$$T_{i,-2} = g^\zeta, T_{i,\varphi} = g^{m^{-1}\cdot T_{i,-1}\cdot \sum_{\mu=1}^{m} H(q_\mu)^\varphi} \cdot X^\zeta, 0 \le \varphi \le (n+1)$$

$\boldsymbol{Test1}(GP, pk_s, sk_s, T_{i,Q}, C_i)$
先计算$t = e(C_{i,1}, \tilde{V})^x$

再测试等式是否相等$t^{T_{i,-1}} \cdot \prod_{\varphi=0}^{n+1} e(T_{i,\varphi}/T_{i,-2}^x, B_\varphi)^x = C_{i,2}^{T_{i,-1}}$

$\boldsymbol{ReKeyGen}(GP, pk_s, sk_j, Q)$
$s_j \in Z_p^*, K_j \in G_T, j = 1, \cdots l_i$
$rk_{j-1\to j} = (rk_{j-1\to j}^1, rk_{j-1\to j}^2, rk_{j-1\to j}^3)$
$rk_{j-1\to j}^1 = g^{s_j},$
$rk_{j-1\to j}^2 = H'(K_1 \cdot K_2 \cdots K_j),$
$rk_{j-1\to j}^3 = \begin{cases} K_j \cdot e(X, \tilde{V})^{s_j}, j = 1 \\ K_j \cdot e(X, \tilde{V})^{s_j - s_{j-1}}, j > 1 \end{cases}$
举个实例说明$rk_{j-1\to j}^3$

$j=1, rk_{j-1\to j}^{3}=rk_{0\to 1}^{3}=K_1\cdot e(X,\tilde{V})^{s_1}$
$j=2, rk_{j-1\to j}^{3}=rk_{1\to 2}^{3}=K_2\cdot e(X,\tilde{V})^{s_2-s_1}$

$\boldsymbol{RePECK}$
$C_j=\left(C_{j,1},C_{j,2},C_{j,3},C_{j,4},C_{j,5},C_{j,6},B_\varphi\right), 0\le\varphi\le(n+1)$
$C_{j,1}=C_{i,1}, C_{j,2}=C_{i,2}, C_{j,3}=C_{i,3}$
$C_{j,4}=rk_{j-1\to j}^{1}, C_{j,5}=e(rk_{j-1\to j}^{2},C_{j,3}), C_{j,6}=\begin{cases} rk_{j-1\to j}^{3}, j=1 \\ C_{j-1,6}\cdot rk_{j-1\to j}^{3}, j>1\end{cases}, B_\varphi=C_{i,3}^{\eta_\varphi},$
举个实例说明$C_{j,6}$
$j=1, C_{1,6}=rk_{0\to 1}^{3}=K_1\cdot e(X,\tilde{V})^{s_1}$
$j=2, C_{2,6}=C_{1,6}\cdot rk_{1\to 2}^{3}=K_1\cdot e(X,\tilde{V})^{s_1}\cdot K_2\cdot e(X,\tilde{V})^{s_2-s_1}$

$\boldsymbol{Trapdoor2}(GP,pk_s,sk_j,Q)$
$T_{j,Q}=\left(T_{j,-1},T_{j,-2},T_{j,\varphi}\right), 0\le\varphi\le(n+1)$
$Q=(q_1,q_2,\cdots,q_m), m\le l$
$T_{j,-1},\xi$是随机整数
$T_{j,-2}=g^{\xi}, T_{j,\varphi}=g^{m^{-1}\cdot T_{j,-1}\cdot y_j\cdot\sum_{\mu=1}^{m}H(q_\mu)^{\varphi}}\cdot X^{\xi}, 0\le\varphi\le(n+1)$

$\boldsymbol{Test2}(GP,pk_s,sk_s,T_{j,Q},C_j)$
先计算$t=e(C_{j,1},\tilde{V})^{x}, K=\frac{C_{j,6}}{e(C_{j,4},\tilde{V})^{x}}$
再测试等式是否相等$[t\cdot C_{j,5}]^{T_{i,-1}}\cdot\prod_{\varphi=0}^{n+1}e(T_{j,\varphi}/T_{j,-2}^{x},B_\varphi)^{x}=[C_{j,2}\cdot e(H'(K),C_{j,3})]^{T_{j,-1}}$