$\boldsymbol{Setup}(1^{\lambda})$

$PK = (G_1, G_T, e, p, g, g_1, g_2, H, EK, pk_{cs}, pk_{ts})$

$e: G_1 \times G_1 \to G_T, g_1 = g^{b_1}, g_2 = g^{b_2}, H: \{0,1\}^* \to G_1, EK = g^{\frac{f(x_t)}{b_1}}, pk_{cs} = g^{sk_{cs}},$

$pk_{ts} = g^{sk_{ts}}, f(x) = b_1 + a_1 x$

$MSK = (b_1, b_2, a_1, x_t, k_1, k_2)$

$\boldsymbol{KeyGen}$

$SK_i = (D_i, E_i, F_i, G_i),\ PK_i = g^{y_i}$

$D_i = g_2^{f(x_{t_i}) \cdot \frac{-x_t}{x_{t_i} - x_t}}, E_i = g_2^{b_1 \cdot \frac{-x_{t_i}}{x_t - x_{t_i}}}, G_i = y_i$

x_{t_i}, y_i都是随机整数

$\boldsymbol{Ciphertext}$

$C_W = (C_{1,\varphi}, 0 \le \varphi \le l, C_2, C_3, C_4)$

$W = (w_1, w_2, \cdots, w_l)$

$N(x) = \big(x - H(w_1)\big)\big(x - H(w_2)\big) \cdots \big(x - H(w_l)\big) + 1$

$= \pi_l x^l + \pi_{l-1} x^{l-1} + \cdots + \pi_1 x + \pi_0 + 1$

$= 1$

在方程$N(x)$中,π_l是x^l的系数，π_l是加密的内容

$$C_{1,\varphi} = g_1^{r \cdot \pi_\varphi}, 0 \le \varphi \le l; C_2 = EK^r, C_3 = g^r$$

r是随机整数

$\boldsymbol{Trapdoor}$

$T_Q = (T_1, T_2, T_3)$

$Q = (\overline{w}_1, \overline{w}_2, \cdots, \overline{w}_m), m \le l$

$$T_{1,\varphi} = g_2^{s \cdot m^{-1} \cdot \sum_{\mu=1}^{m} H(\overline{w}_\mu)^\varphi} \cdot pk_{cs}^{\tau}, 0 \le \varphi \le l, T_2 = E_i^S, T_3 = D_i^S, T_4 = g^{\tau}$$

$\boldsymbol{Match}$

$$\prod_{\varphi=0}^{l} e(C_\varphi, T_{1,\varphi} / T_4^{sk_{cs}}) = e(C_2, T_2) \cdot e(C_3, T_3)$$