TBEKS

$\boldsymbol{Setup}(\mathbf{1}^{\lambda}) \rightarrow (\boldsymbol{PK}, \boldsymbol{MSK})$

$e: G_1 \times G_1 \rightarrow G_T, H_0: \{0,1\}^* \rightarrow Z_p$

$MSK = (r = 5, d = 4, s, v = 6)$ 都是随机整数

$PK = (h, u = s/d, \varpi_1 = g^{r/d}, \varpi_2 = g^{ru}, \theta = e(g,g)^v, h_1, h_2, h_3, h_4)$, 其中$h, h_1, h_2, h_3, h_4 \in G_1$

$\boldsymbol{KeyGen}(\boldsymbol{n} = \mathbf{4}, \boldsymbol{t} = \mathbf{3})$

$f_0(x) = 5 + 2x + 3x^2$

$f_1(x) = 4 + x + 2x^2$

$f_2(x) = 6 + 3x + 4x^2$

$sk_1 = (r_1 = f_0(1) = 10, d_1 = f_1(1) = 7, g^{-a}, h_1^a g^v, h_2^a, h_3^a, h_4^a)$

$sk_2 = (r_2 = f_0(2) = 21, d_2 = f_1(2) = 14, g^{-b}, h_1^b, h_2^b g^v, h_3^b, h_4^b)$

$sk_3 = (r_3 = f_0(3) = 38, d_3 = f_1(3) = 25, g^{-c}, h_1^c, h_2^c, h_3^c g^v, h_4^c)$

$sk_4 = (r_4 = f_0(4) = 61, d_4 = f_1(4) = 40, g^{-d}, h_1^d, h_2^d, h_3^d, h_4^d g^v)$

$\boldsymbol{Enc}$

$I_0' = h^{-\alpha}, I_1' = \varpi_1^{\alpha}, I_1 = \varpi_2^{\alpha H_0(w_1)}, I_2 = \varpi_2^{\alpha H_0(w_2)}, I_3 = \varpi_2^{\alpha H_0(w_3)}$

$\boldsymbol{Trap}$

$A = g^{\beta}, B = h^{u[H_0(w_1)+H_0(w_2)+H_0(w_3)]+\beta}$

$\lambda_1 = A^{r_1 \times 3} = A^{10 \times 3}, \mu_1 = B^{d_1 \times 3} = B^{7 \times 3}$

$\lambda_2 = A^{r_2 \times (-3)} = A^{21 \times (-3)}, \mu_1 = B^{d_2 \times (-3)} = B^{14 \times (-3)}$

$\lambda_3 = A^{r_3 \times 3} = A^{38 \times 1}, \mu_3 = B^{d_3 \times 1} = B^{25}$

$T_1 = \lambda_1 \times \lambda_2 \times \lambda_3 = A^{30-63+38} = A^5$

$T_2 = \mu_1 \times \mu_2 \times \mu_3 = B^{21-42+25} = B^4$

$\boldsymbol{Search}$

$e(I_0', T_1) \cdot e(I_1', T_2) = e(I_1 I_2 I_3, h)$