4.2 Construction

在不损失一般性的情况下，我们在一个固定的字母表$\Sigma \in Z_q^*$上观察最大长度为 n 的向量，其他字母表可以映射到这样一个子集上。系统不要求关键字具有相同的长度，但是我们将用 0 填充不同长度的关键字直到均匀的长度n，这种填充将在计算中被安全地忽略【填充后面有举例说明】。完整的系统构造由如下四个算法$(Setup, Enc, KeyGen, Dec)$构成。

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

System Public Key $PK = (G_1, G_T, e, p, g, g_1, EK = g^{\frac{f(x_t)}{b_1}}, h, pk_c, pk_a)$

Master Secret Key $MSK = (b_1, b_2, a_1, x_t, v)$

(2) $\boldsymbol{User\ Key\ Generation}$

The user public key is set as $PK_i = (N_i = g^r, F_i = g^{r \cdot b_2}, h_{i,\psi} = g^{s_{i,\psi}} \cdot h^{v_{i,\psi}})$

The user secret key is $SK_i = (M_i = r, D_i = g^{b_2 \cdot f(x_{t_i}) \cdot \frac{-x_t}{x_{t_i} - x_t}}, E_i = g^{b_2 \cdot \frac{-x_{t_i}}{x_t - x_{t_i}}}, s_{i,\psi}, v_{i,\psi})$.

(3) $\boldsymbol{Enc}(\boldsymbol{mpk}, \boldsymbol{W}) \rightarrow \boldsymbol{ct}$:加密算法以主公钥$mpk$和关键字$W$作为输入，输出密文$ct$。让$W = (w_1, \ldots, w_n) \in \Sigma^n$，其中$n$为关键字的长度，$w_i$为$W$的第$i$位。首先，数据提供者需要将表示关键字的向量的维数从一维扩展到二维。随机选取$r_1, \cdots, r_n \overset{R}{\leftarrow} Z_N$，构造向量$X = (x_1, \ldots, x_{2n})$，如下所示:

$$x_{2\psi-1} \coloneqq M_i \cdot r_\psi \cdot w_\psi = r \cdot r_\psi \cdot w_\psi \quad x_{2\psi} \coloneqq -M_i \cdot r_\psi = -r \cdot r_\psi$$

其中所有乘法都是模q运算。然后计算$C_1 = F_i = g^{r \cdot b_2}, C_2 = EK^{M_i} = EK^r, C_3 = N_i = g^r$，对于每个$i \in [2n]$, 计算 $E_\psi = g_1^{M_i \cdot x_\psi}$。它将此关键字$W$的密文输出为$ct = (C_1, C_2, C_3, (E_1, \ldots, E_{2n}))$.

(4) $\boldsymbol{KeyGen}(\boldsymbol{msk}, \overline{\boldsymbol{W}}) \rightarrow \boldsymbol{sk}_{\overline{\boldsymbol{W}}}$:密钥生成算法以主密钥$msk$和包含要查询的通配符的关键字$\overline{W}$作为输入，输出一个功能密钥$sk_{\overline{W}}$。让$\overline{W} = (\overline{w}_1, \cdots, \overline{w}_n) \in \Sigma_*^n$，其中包含通配符或“不在乎”符号。同样的数据用户需要将关键字$\overline{W}$扩展到向量$Y = (y_1, \cdots, y_{2n})$，从一维扩展到二维，如下所示:

if $\overline{w}_\psi = \star$, $y_{2\psi-1} = y_{2\psi} = 0$;

if $\overline{w}_\psi \neq \star$, $y_{2\psi-1} = 1$, $y_{2\psi} = \overline{w}_\psi$.

选择一个随机数$s, m \overset{R}{\leftarrow} Z_q$并计算

$$\{K_\psi = g_2^{m \cdot y_\psi}, P_\psi = h_\psi^s\}_{\psi=1}^{2n},$$

$$T_1 = g_1^s, T_2 = E_j^s = g^{s \cdot b_2 \cdot \frac{-x_{t_j}}{x_t - x_{t_j}}}, T_3 = D_j^s = g^{s \cdot b_2 \cdot f(x_{t_j}) \cdot \frac{-x_t}{x_{t_j} - x_t}},$$

$$T_4 = g^{m \cdot \sum_{\psi=1}^{2n} s_{j,\psi} \cdot y_\psi}, T_5 = g^{m \cdot \sum_{\psi=1}^{2n} v_{j,\psi} \cdot y_\psi}$$

然后输出搜索陷门，如$T_{\overline{W}} = (T_1, T_2, T_3, T_4, T_5, (K_1, \ldots, K_{2n}), (P_1, \ldots, P_{2n}))$.

(5) $\boldsymbol{Dec}(\boldsymbol{ct}, \boldsymbol{sk}_{\overline{\boldsymbol{W}}}) \rightarrow \boldsymbol{z}$: 云服务器运行的解密算法以主公钥$mpk$、密文$ct$和功能秘钥$sk_{\overline{W}}$作为输入，输出一个组元素$z \in G_T$，以下等式成立则$ct$和$sk_{\overline{W}}$匹配

$$e(C_1, T_1) \cdot \frac{\prod_{i=1}^{2n} e(E_i, K_i)}{e(g, T_4) \cdot e(h, T_5)} \overset{?}{\Leftrightarrow} e(C_2, T_2) \cdot e(C_3, T_3)$$