1 SchemeVLPSICA

1.1 Setup$(m, n, d) \rightarrow (\boldsymbol{mpk}, \boldsymbol{msk})$

$g_1 \leftarrow 1_{\mathbb{G}_1}$
$g_2 \leftarrow 1_{\mathbb{G}_2}$
generate $s \in \mathbb{Z}_p^*$ randomly
$\vec{S} \leftarrow (S_0, S_1, \cdots, S_{m+d}) = (g_2^{s_0}, g_2^{s_1}, \cdots, g_2^{s^{m+d}})$
$S' \leftarrow g_1^s \in \mathbb{G}_1$
$H : \mathbb{G}_T \rightarrow \{0,1\}^\lambda$
$mpk \leftarrow (g_1, S', H)$
$msk \leftarrow (g_2, \vec{S})$
return (mpk, msk)

1.2 Sender$(\vec{v}, \vec{Y}) \rightarrow (\vec{T}||\vec{T}', \vec{U}||\vec{U}')$

generate $k \in \mathbb{N} * \cap [0, n)$ randomly
$\pi : x \rightarrow (x + k)\%n$
generate $\vec{t} \leftarrow (t_1, t_2, \cdots, t_n) \in \mathbb{Z}_r^n$ randomly
$\vec{T} \leftarrow (T_1, T_2, \cdots, T_n) = (g_1^{t_1}, g_1^{t_2}, \cdots, g_1^{t_n})$
$\vec{U} \leftarrow (U_1, U_2, \cdots, U_n) = (S' \cdot (g_1^{-y_{\pi(1)}}), S' \cdot (g_1^{-y_{\pi(2)}}), \cdots, S' \cdot (g_1^{-y_{\pi(n)}}))$
generate $\vec{t'} = (t'_1, t'_2, \cdots, t'_d) \in \mathbb{Z}_r^d$ randomly
$\vec{T}' \leftarrow (T'_1, T'_2, \cdots, T'_d) = (g_1^{t'_1}, g_1^{t'_2}, \cdots, g_1^{t'_d})$
$\vec{U}' \leftarrow (U'_1, U'_2, \cdots, U'_d) = (S' \cdot (g_1^{-v_1})^{t'_1}, S' \cdot (g_1^{-v_2})^{t'_2}, \cdots, S' \cdot (g_1^{-v_d})^{t'_d})$
return $(\vec{T}||\vec{T}', \vec{U}||\vec{U}')$

1.3 Receiver$(\vec{v}, \vec{X}) \rightarrow (R, \vec{R}')$

$\vec{X}' \leftarrow (\vec{X}||\vec{v}) \in \mathbb{Z}_r^{m+d}$
generate $r \in \mathbb{Z}_r$ randomly
$$R \leftarrow \left(\prod_{j=0}^{m+d} S_j^{p(X',j)} \right)^r$$
$$R_{-i} \leftarrow \left(\prod_{j=0}^{m+d-1} S_j^{p(X'_{-i},j)} \right)^r, \forall i \in 1, 2, \cdots, m+d$$
return $(R, \vec{R}')$

1.4 Cloud1$((\vec{T}, \vec{T}'), R) \rightarrow \vec{W}$

$W_j \leftarrow H(e((\vec{T}||\vec{T}')_j, R)), \forall j \in 1, 2, \cdots, n+d$
generate $k_1 \in \mathbb{N} * \cap [0, n+d)$ randomly
$\pi_1 : x \rightarrow (x + k_1)\%(n+d)$
$\vec{W} \leftarrow \{\vec{W}_{\pi_1(j)}\}_j$
return $\vec{W}$

1.5 Cloud2$(\vec{U}, R') \rightarrow \vec{K}$

$\vec{K}_{i(n+d)+j} \leftarrow H(e((\vec{U}||\vec{U'})_j, R'_i)), \forall i \in 1, 2, \cdots, m+d, \forall j \in 1, 2, \cdots, n+d$
generate $k_2 \in \mathbb{N} * \cap [0, (m+d)(n+d))$ randomly
$\pi_2 : i, j \rightarrow (i(n+d) + j + k_2)\%(m+d)(n+d)$
$\vec{K} \leftarrow \{\vec{K}_{\pi_2(i,j)}\}_{i,j}$
return $\vec{K}$

1.6 Verify$(\vec{K}, \vec{W}) \rightarrow$ ***result***

if $\vec{W} \subseteq \vec{K}$ **then**
  result $\leftarrow |\vec{K} \cap \vec{W}| - d = |\vec{W}| - d = n + d - d = n$
else
  result $\leftarrow \perp$
end if
return *result*