Project 6

基于 DDH 的私有交集求和协议

设参与方为 P_1 和 P_2：

输入

1. 双方共有：
   a. 一个素数阶乘法循环群 G
   b. 识符空间 U
   c. 哈希函数 $H : U \to G$（建模为随机预言机），将任意标识符映射到群 G 中的随机元素
2. P_1：持有集合 $V = \{v_i\}_{i=1}^{m_1}$，其中每个 $v_i \in U$
3. P_2：持有成对集合 $W = \{(w_j, t_j)\}_{j=1}^{m_2}$，其中 $w_j \in U$，且 $t_j \in \mathbb{Z}^+$

初始化阶段

1. 每一方 P_i 独立地在群 G 中选择一个随机私钥指数 $k_i \xleftarrow{\$} \mathbb{Z}_q^*$（$q$ 是群 G 的阶）
2. P_2 为某个加法同态加密方案生成新的密钥对 $(pk, sk) \leftarrow \mathrm{AGen}(\lambda)$，并将公钥 pk 发送给 P_1

第 1 轮（由 P_1 执行）

对于集合 V 中的每个元素 v_i：

1. 计算 $c_i = H(v_i)^{k_1}$
2. 将所有计算出的值组成多集 $\{c_i\}_{i=1}^{m_1}$，并以随机顺序发送给 P_2

第 2 轮（由 P_2 执行）

收到来自 P_1 的所有 c_i 后，执行以下操作：

1. 对每个收到的 $c_i = H(v_i)^{k_1}$，使用自己的私钥 k_2 进行指数运算，得到 $d_i = c_i^{k_2} = H(v_i)^{k_1 k_2}$，构成集合 $Z = \{d_i\}_{i=1}^{m_1}$
2. 对于本地输入中的每一项 $(w_j, t_j) \in W$：
   a. 计算 $e_j^{(1)} = H(w_j)^{k_2}$
   b. 使用公钥 pk 对数值 t_j 进行加法同态加密，得到密文 $\sigma_j = AEnc_{pk}(t_j)$
   c. 构造元组 $(e_j^{(1)}, \sigma_j)$
3. 将整个集合 $\{(e_j^{(1)}, \sigma_j)\}_{j=1}^{m_2}$ 以随机顺序发送给 P_1

4. 同时，将之前计算出的集合 $\mathbb{Z}$ 以随机顺序发送给 P_1

第 3 轮（由 P_1 执行）

收到来自 P_2 的消息后，执行以下步骤：

1. 对每个接收到的元组 $(e_j^{(1)}, \sigma_j)$，用自身的私钥 k_1 对第一部分再次进行指数运算，得到 $e_j^{(2)} = (e_j^{(1)})^{k_1} = H(w_j)^{k_1 k_2}$
2. 根据这些变换后的值确定交集索引集：$J = \left\{ j \mid e_j^{(2)} \in \mathbb{Z} \right\}$（$\mathbb{Z}$ 是从 P_2 接收到的集合）
3. 对所有属于交集 J 的项对应的密文 $\{\sigma_j\}_{j \in J}$ 执行同态加法聚合：

$$\Sigma_{\text{enc}} = ASum\left(\{\sigma_j\}_{j \in J}\right) = AEnc_{pk}\left(\sum_{j \in J} t_j\right)$$

   记作 $AEnc_{pk}(S_J)$，其中 $S_J = \sum_{j \in J} t_j$

4. 应用随机化算法 $ARfresh$ 对最终得到的密文进行处理，然后将结果发送给 P_2

输出阶段

P_2 使用秘密密钥 sk 解密收到的密文，恢复出交集元素的总和：$S_J = \text{Decrypt}_{sk}(\Sigma_{\text{enc}})$

结果展示

根据上述协议构造的代码输出结果如下：

```
初始化完成:
 - P1私钥指数k₁=109651649774350050156223351534710402727
 - P2私钥指数k₂=144946634995669775460800363739078528644
 - HE公钥pk=
  (69949435355456013324709831288893248168702785058359908076721739910916367608822290424064958466491271119124754803106983604572464452524028000325585902187602388115571577777684553615079751367599744939614113031157422883223448293136976696906986603655881190149738835483397154636752310905275169299340785768090655568869,
  69949435355456013324709831288893248168702785058359908076721739910916367608822290424064958466491271119124754803106983604572464452524028000325585902187602388115571577777684553615079751367599744939614113031157422883223448293136976696906986603655881190149738835483397154636752310905275169299340785768090655568870)

第1轮传输: 4个c_i值已发送至P2

第2轮传输:
 - Z集合大小=4
 - 元组数量=4

第3轮结果:
 - 交集索引J=[0]
 - 聚合密文Σ_enc已随机化处理

最终输出: 交集元素的总和 S_J = 10
验证通过！协议执行成功。
```