1. 问题描述

有n个用户，每个用户拥有集合$S_i (1 \le i \le n)$, 集合大小为k, 在不暴露用户自身集合元素的前提下，计算出$S_1 \cap S_2 \cap \cdots \cap S_n$.

2. 攻击模型

1. 诚实但好奇（Honest But Curious）：若n个用户均严格按照协议执行，则在交互过程中，除了最终结果，每个用户（或几个用户联合）不会获得其他额外知识。
2. 恶意（Malicious）：恶意用户或几个恶意用户联合不能获得额外知识。

3. 背景知识

3.1. 同态加密

我们需要的加密方案需要满足下面两个性质：

1. 加法同态：$Enc_{pk}(a+b) = Enc_{pk}(a) +_h Enc_{pk}(b)$
2. 数乘同态：$Enc_{pk}(c \times a) = c \times_h Enc_{pk}(a)$

注意上述的加法和乘法不一定是现实意义的加法乘法，只是代表两种抽象运算，需要根据具体的加密算法来定。

3.2. Paillier加密算法

Paillier算法具有同态性质，我们可以使用该算法。

3.2.1. Paillier加密算法流程

1. 密钥生成算法$Gen(1^n)$：随机选取两个等长大素数p, q, 令$N = pq$. 则输出公钥为N, 私钥为$(N, \phi(N))$. $\phi(N)$为欧拉函数，表示比N小与N互质的数，如果$N = pq$，那么$\phi(N) = (p-1)(q-1)$.
2. 加密算法$Enc(m, N)$：输入公钥$N, m \in \mathbb{Z}_N$, 随机选取$r \leftarrow \mathbb{Z}_p^*$, 输出

   $c = (1+N)^m \cdot r^N \ mod \ N^2$.
3. 解密算法$Enc_{pk}(c, (N, \phi(N)))$：输入私钥$(N, \phi(N))$以及密文$c$, 计算

   $m = \frac{c^{\phi(N)} \ mod \ N^2 - 1}{N} \cdot \phi^{-1}(N) \ mod \ N$.

3.2.2. 算法的准正确性

首先注意到$\phi(N^2) = \phi(p^2q^2) = \phi(p^2)\phi(q^2) = p(p-1)q(q-1) = N\phi(N)$. 所以对于任意的$x \in Z_{N^2}^*$有$x^{N\phi(N)} \ mod \ N^2 = x^{\phi(N^2)} \ mod \ N^2 = 1$.

所以将密文代入解密算法中我们有

$\frac{c^{\phi(N)} \ mod \ N^2 - 1}{N} \cdot \phi^{-1}(N) \ mod \ N$

$= \frac{((1+N)^m \cdot r^N)^{\phi(N)} \ mod \ N^2 - 1}{N} \cdot \phi^{-1}(N) \ mod \ N$

$= \frac{((1+N)^{m\phi(N)} \cdot r^{N\phi(N)}) \ mod \ N^2 - 1}{N} \cdot \phi^{-1}(N) \ mod \ N$

$= \frac{((1+N)^{m\phi(N)}) \ mod \ N^2 - 1}{N} \cdot \phi^{-1}(N) \ mod \ N$

$= \frac{(1 + C^1_{m\phi(N)} \cdot N + C^2_{m\phi(N)} \cdot N^2 + \cdots + C^{m\phi(N)}_{m\phi(N)} \cdot N^{\phi(m\phi(N))}) \ mod \ N^2 - 1}{N} \cdot \phi^{-1}(N) \ mod \ N$

$= \frac{(1 + C^1_{m\phi(N)} \cdot N) \ mod \ N^2 - 1}{N} \cdot \phi^{-1}(N) \ mod \ N$

$= \frac{1 + m\phi(N) \cdot N - 1}{N} \cdot \phi^{-1}(N) \ mod \ N$

$= m$

3.2.3. 算法的同态性

1. $Enc_{pk}(a) \cdot Enc_{pk}(b)$
   $= (1+N)^a \cdot r_1^N \ mod \ N^2 \cdot (1+N)^b \cdot r_2^N \ mod \ N^2$
   $= (1+N)^{a+b} \cdot (r_1 r_2)^N \ mod \ N^2$
   $= Enc_{pk}(a+b)$
2. $[Enc_{pk}(a)]^c = [(1+N)^a \cdot r^N \ mod \ N^2]^c$
   $= (1+N)^{ac} \cdot (rc)^N \ mod \ N^2$
   $= Enc_{pk}(a \cdot c)$
   注意到在使用Paillier算法的前提下，论文中的 $+_h$ 代表实际的乘法，$\times_h$ 代表实际的乘方。

3.3. 多项式环

3.3.1. 符号说明

$R[x]$: 多项式环，系数在集合R上的所有多项式构成的集合（在Paillier中，$R = \mathbb{Z}_n$）。

$deg(f)$: 多项式f的次数。

$f[i]$: 多项式f中x^i前的系数，则$R[x]$中任意多项式可写为$f(x) = \sum_{i=0}^{deg(f)} f[i]x^i$,可用数组来表示多项式
$f(x) = (f[0], f[1], \cdots f[deg(f)])$

3.3.2. 加密多项式上的运算（用Paillier的前提下）