多方隐私集合交集及秘密信誉值比较协议

李功丽[a,b],范云[a],马婧雯[a]

(河南师范大学 a.计算机与信息工程学院;b.河南省教育人工智能与个性化学习重点实验室,河南 新乡 453007)

摘 要:多方隐私集合交集(multiparty private set intersection,MPSI)作为安全计算领域一种保护数据安全的计算技术,支持在不泄露任何参与方隐私的前提下,计算多个参与方数据集的交集,可通过同态加密、不经意传输等技术手段实现.但现有基于同态加密的 MPSI 协议存在计算效率低、交互轮数多等问题,且通过交互无法实现交集用户保密数据的计算.为此,首先基于布隆过滤器和 ElGamal 算法提出了 n 方交集用户的秘密信誉值比较协议.进一步针对查询交集失败的问题,基于信誉值过滤器和多密钥加解密,提出用户交集基数协议并完成多方秘密信誉值评估.实验结果表明,研究提出的 2 种协议满足半诚实安全,可抵抗 $n-1$ 个参与方的合谋且执行时间优于其他方案.

关键词:多方隐私集合交集;秘密信誉值比较;信誉阈值比较;多方秘密信誉值比较;多方交集基数

中图分类号:TP309 **文献标志码**:A **文章编号**:1000-2367(2025)05-0121-10

隐私集合交集(private set intersection,PSI)允许两个或多个参与方秘密地计算交集而不泄露交集以外的其他信息,为用户提供服务的同时最大程度地保护隐私[1].以银行征信查询为例:银行借贷业务需查询用户在本地和其他银行的信誉状况,判断用户是否信誉良好且具有还贷能力,从而降低信贷风险.在这个过程中用户在不同机构的数据作为隐私信息无法在多家银行直接共享[2],而现实中又需要对借贷用户进行信誉评估.因此,在保护各方隐私的前提下,安全查询借贷用户在其他银行中的信誉状况是一个值得研究的问题.

两个参与方场景下的 PSI(简称两方 PSI)大多基于不经意传输或公钥加密等技术手段实现,已有多种高效且安全的实现方案.随着 PSI 应用场景的不断扩大,研究愈发深入,PSI 协议也从两方扩展到多方.而多方隐私集合交集(multiparty private set intersection,MPSI)致力于在不泄露任何参与方信息的前提下,计算多个参与方数据集的交集.当两方 PSI 扩展到多方时,随着参与方的数量增多,使用同态方案造成的计算负荷不可忽视,且各参与方数据集规模差异大,导致隐私保护难度加大,易出现隐私泄露.

针对两方 PSI 协议扩展到多方时存在交集计算易失败以及用户在多个机构中的查询结果不一致、无法准确评估信誉等问题,本研究利用 ElGamal 算法和多密钥加解密,提出多方用户交集和用户交集基数的秘密信誉值比较协议.该协议在保护查询方和被查询方隐私的同时,通过布隆过滤器(bloom filter,BF)和 ElGamal 加密计算交集用户并完成秘密信誉值比较.此外,考虑到实际应用中用户在所有机构中均创建账户的概率较低,提出隐私集合多方交集基数的概念和求解方法,利用信誉过滤器值和多密钥加解密构建更为实用的信誉评估方案.最后证明了协议在半诚实模型下的安全,在不同数量级集合输入的情况下分别测试 2 种协议各阶段的在线计算时间和查询方解密时间,与其他多方隐私集合计算协议进行了对比.

收稿日期:2024-04-13;**修回日期**:2025-05-10.

基金项目:国家自然科学基金(62372157);河南省科技攻关项目(232102211057).

作者简介(通信作者):李功丽(1981—),女,河南信阳人,河南师范大学副教授,博士,研究方向为信息安全、隐私保护,E-mail:ligl522@163.com.

引用本文:李功丽,范云,马婧雯.多方隐私集合交集及秘密信誉值比较协议[J].河南师范大学学报(自然科学版),2025,53(5):121-130.(Li Gongli,Fan Yun,Ma Jingwen.Multiparty privacy set intersection and secret reputation value comparison protocols[J].Journal of Henan Normal University(Natural Science Edition),2025,53(5):121-130.DOI:10.16366/j.cnki.1000-2367.2024.04.13.0001.)

1 相关工作

多方隐私集合交集是两方 PSI 向两个以上参与方的自然延伸,研究最初,并未像两方 PSI 那样受关注,随着应用需求的扩展,MPSI 已经成为了新的研究热点.FREEDMAN 等[3]提出基于同态加密和多项式的 MPSI 协议,将集合元素表示为多项式的根,为多方协议构造提供了思路.之后,KISSNER 等[4]使用加性同态加密和私钥秘密共享实现的 MPSI 协议计算和通信开销是集合大小和参与者数量的两倍,无法满足实际应用要求.此后降低同态密码技术的 MPSI 协议的计算开销和通信开销已成为一个重要的目标.2022 年,BAY 等[5]将文献[6]两方 PSI 拓展到多方,但协议运行时间较长、效率不高.RUAN 等[7]提出基于 BF 和 Shamir 阈值秘密共享方案的 MPSI 协议,虽在效率上有所提高,但交互轮数多.在现有的 MPSI 研究中,通信成本和协议轮数是影响性能的主要因素,随着参与方数量增多,导致协议产生高昂的计算和通信开销,影响其在现实场景的可行性.

秘密数据比较本质是在不泄露参与方输入信息的情况下比较出两数值大小,YAO[8]最早提出的"百万富翁问题"形象描述了此问题.匿名投票作为秘密数据比较协议的应用场景之一,借助密码学技术剥离对可信第三方的依赖.2021 年张静等[9]提出一种采用 0-1 编码的数据比较协议,通过改进保密数据编码规则和 ElGamal 同态加密解决安全两方计算问题,保证协议半诚实安全但需要 3 轮通信.2022 年李顺东等[10]提出结合 ElGamal 乘法同态性质和保密洗牌的零知识证明设计了抵抗恶意安全的保密比较协议,协议中对 m 个数据的加密,需要 $24m+4$ 次模幂运算,计算复杂度与数据范围成正比且在大数比较时效率较低.

2 预备知识

2.1 布隆过滤器

布隆过滤器(BF)[11]是一个拥有 k 个哈希函数$\{h_1,h_2,\cdots,h_k\}$长度为 m 的比特数组,$BF=\{BF[1],BF[2],\cdots,BF[m]\}$.当插入数据集 $X=\{x_1,\cdots,x_n\}$ 的元素 x_i 到 BF 中时,将元素 x_i 使用k 个哈希函数映射到$\{h_1(x_i),\cdots,h_k(x_i)\}$ 的位置设置为 1,如附录图 S1 所示.

BF 中的相应位置均被设置为 1,即 $BF[h_u(y)]=1$.此时,假阳性发生的概率与布隆过滤器长度 m、哈希函数个数 k 和元素 n 直接相关[12],其概率为 $p=1-(1-\frac{1}{m})^{kn}$,且该概率上界关于 k 的可忽略值为 $\varepsilon=p^k\cdot(1+O(\frac{k}{p}\sqrt{\frac{\ln m-k\ln p}{m}}))$,当 ε 可忽略不计时,对上式进行约束后 k,m 分别取值 $k=-\frac{\ln e}{\ln 2}$ 和 $m=k\cdot\frac{d}{\ln 2}$.

2.2 混淆布隆过滤器

DONG 等[12]提出混淆布隆过滤器(garbled bloom filter,GBF)的概念:哈希函数映射位置不再存放单个比特,而是 λ 比特的字符串.比如当插入元素 x_l 到 GBF 中时,哈希函数映射位置不再是 1,而是一个随机数,且映射到所有位置的值异或后的结果为 x_l,即 $x_l=\bigoplus_{u=1}^{k}GBF[h_u(x_l)]$,其余空位置填充随机值.当插入 x_l 元素到 GBF 时构造如附录图 S2 所示.

GBF 插入第 n 个元素到某一映射位置被占据的概率为 $p=1-(1-\frac{1}{m})^{kn}$,而所有 k 个位置被占据的概率为 $Pr=p^k\times(1+O(\frac{k}{p}\sqrt{\frac{\ln m-2k\ln p}{m}}))$,此时 GBF 创建失败.

2.3 ElGamal 加密算法

ElGamal[13]是一种满足乘法同态的公钥加密算法,其安全性基于离散对数困难问题,它包含了一个生成元 g、模素数 p、私钥 α 和公钥 h.ElGamal 算法可分为 3 个主要部分:密钥生成 *KenGen*、加密 *Enc* 和解密 *Dec*.

KenGen:产生一个大素数 p 和一个循环群 Z_p^*,$g(g<p)$ 是循环群 Z_p^* 的生成元.随机选取一个私钥 $\alpha\in Z_p^*$,计算 $h=g^\alpha \bmod p$ 作为公钥.

Enc:设明文消息 $M\in Z_p^*$,随机选择 $r\in Z_p^*$,$2\le r\le p-2$,则加密密文 $Enc(M)=(c_1,c_2)=(g^r \bmod$

$p, Mh^r \bmod p$).

Dec：对密文 $Enc(M)=(c_1,c_2)$，则解密明文 $M=Dec(c_1,c_2)=c_2(c_1^{\alpha})^{-1} \bmod p$.

ElGamal 具有乘法同态性质：$Enc(m_1 \cdot m_2)=Enc(m_1) \cdot Enc(m_2)$；

同时满足标量乘法运算：$c \cdot Enc(M)=Enc(c \cdot M)$.

3　协议设计

针对银行跨机构安全查询用户信誉问题，设计 2 种多方交集及秘密信誉值比较协议，查询方获得用户在不同机构中的信誉比较结果，协议功能如附录图 S3 所示.协议涉及的角色分别为：持有集合 $X=\{(x_1,v_1),\cdots,(x_{m_R},v_{m_R})\}$ 的查询方 R，x_i 和 v_i 分别表示用户的身份信息和信誉值.n 个被查询方 $S_1,\cdots,S_n$ 分别持有大小为 $m_1,\cdots,m_n$ 的集合 $Y_1=\{(y_1^1,v_1^1),\cdots,(y_{m_1}^1,v_{m_1}^1)\},\cdots,Y_n=\{(y_1^n,v_1^n),\cdots,(y_{m_n}^n,v_{m_n}^n)\}$.$k$ 个哈希函数 $h_1,\cdots,h_k:\{0,1\}^* \to \{0,1\}^{\kappa}$ 是抗碰撞哈希函数，κ 表示其输出长度，对任意输入 $x \in \{0,1\}^*$ 使用哈希函数计算后获得结果 $h_n(x) \in \{0,1\}^{\kappa}$.

3.1　构造 VBF

在整个交互中，被查询方利用混淆布隆过滤器构造隐藏输入集.对元素 x 使用 k 个哈希函数映射的位置将填充信誉值的随机份额，其余空位置不再填充随机值而是“1”值，该结构称为信誉过滤器(value bloom filter，VBF).这样构造的 VBF 既满足 $v=\bigoplus_{u=1}^{k} VBF_i[h_u(x_l)]$，又适用于 ElGamal 乘法同态，避免了对“0”的加密.当 n 个被查询方 $S_1,\cdots,S_n$ 对用户集合 $Y_1,\cdots,Y_n$ 构造 VBF_i 时，具体算法如下.

算法 1　$VBF()$

输入：集合 $Y_i=\{(y_1^i,v_1^i),\cdots,(y_{m_i}^i,v_{m_i}^i)\}$.

输出：构造 VBF_i.

```
1. VBF = NULL
2.for j=1 to m_i do
3.   value=v_j^i
4.   for u=1 to k do
5.     index=h_u(y_j^i)
6.     if VBF[index]==NULL then
7.      if emptyBin==-1 then
8.        emptyBin=index
9.        else
10.          VBF[index]←{0,1}^κ
11.          lastShare←lastShare⊕VBF[index]
12.       end if
13.       else
14.       lastShare←lastShare⊕VBF[index]
15.     end if
16.   end for
17.     VBF[emptyBin]←lastShare
18.   end for
19.   for j=1 to m do
20.     if VBF[i]=NULL then
21.      VBF[j]←1
22.     end if
23.   end for
24.   return VBF_i
```

3.2　多方隐私集合交集

多方交集秘密信誉值比较协议利用 BF 和 VBF 隐藏被查询方的用户信息，并由被查询方将操作转移到离线阶段以提升协议计算效率.VBF 经对应映射位置异或可获得信誉值，而 BF 需将映射后的值经 ElGamal 加密发给查询方 R.考虑 ElGamal 算法无法对“0”值进行加密，被查询方 S_i 要在位数组 BF 未设置为 1 处填充随机数 r 后加密.当查询方 R 用 ElGamal 公钥对 n 个被查询方 S_i 发来的 BF_i 进行运算时，由于乘法同态性，相同映射为“1”的位置经密文下乘法运算后保留明文上的“1”值，R 计算后获得隐藏交集用户身份信息的 BF.

在协议 1 中，查询方 R 生成并公开密钥对 (pk,sk).随后 n 个被查询方 $S_1,\cdots,S_n$ 对用户信息中的 $\{y_i\}$ 生成 BF_i 后，利用 pk 加密获得 $EBF_i=Enc(BF_i)$ 并发送给查询方 R.R 计算 $EBF=\prod_{i=1}^{n} EBF_i$ 后将该结果乘以信誉阈值密文返回被查询各方，EBF 中隐藏交集用户信息.查询方 R 可通过私钥解密得到包含所有交集用户的 BF，经设置的信誉阈值密文计算 $w=EBF \cdot Enc(v^{-1})$ 后返回各方.最后被查询方 S_i 利用离线阶段生成的 VBF_i 与密文 w 进行标量乘并发送，查询方 R 获得 n 方交集用户的信誉值比较结果. 协议 1 具体执行步骤如下.

协议 1 多方交集秘密信誉值比较协议

输入:查询方 R 的数据集 X,被查询方 $S_1,\cdots,S_n$ 的数据集 $Y_1,\cdots,Y_n$,$i\in[1,n]$,R 和 S_i 的集合大小分别为 $m_R,m_1,\cdots,m_n$,$j\in[1,m_i]$. 输出:交集用户 $\{w\}$,秘密信誉值比较结果 $|V|$.

步骤 1 初始化

(1)查询方 R 生成 ElGamal 密钥对 $(pk,sk)\leftarrow KenGen()$,并随机选择 k 个哈希函数 $h_1,\cdots,h_k$,$u\in[1,k]$,将 $(pk,h_1,\cdots,k_k)$ 公开.

步骤 2 预处理阶段

(1)查询方 R 对待查询用户 $X=\{(x_l,v_l)\}$,$l\in[1,m_R]$,计算信誉阈值密文 $Enc(v^{-1})$;

(2)被查询方对持有集合 $Y_i=\{(y_1^i,v_1^i),\cdots,(y_{m_i}^i,v_{m_i}^i)\}$ 中用户身份信息构造 VBF_i 和 BF_i.对 S_i 中每个用户的身份信息 y_j^i 和信誉值 v_j^i 生成 VBF_i,使得 VBF_i 中相应哈希映射位置异或结果满足 $\bigoplus_{u=1}^{k}VBF_i[h_u(y_j^i)]=v_j^i$.对用户身份信息 $\{y_1^i,\cdots,y_{m_i}^i\}$ 构造 BF_i 使用公钥 pk 加密获得 $EBF_i=Enc(BF_i)$,各方将生成的 EBF_i 发送给任意一个 S_i,$j\in[1,n]$,$j\neq i$.

(3) S_j 将对集合生成的 EBF_j 计算 $EBF_i\cdot EBF_j$ 发送给查询方 R.

步骤 3 在线阶段.查询方 R 接收到 $EBF=(EBF_1,\cdots,EBF_n)$,准备计算:

(1)查询方 R 计算 $EBF=\prod_{i=1}^{n}EBF_i$,并将结果 $value=EBF\cdot Enc(v^{-1})$ 返回给 n 个被查询方 $S_1,\cdots,S_n$.

(2)被查询方 S_i 收到消息 $value$ 后,计算 $w_i=value\cdot VBF_i$,并发送给查询方 R.

步骤 4 离线阶段

(1)查询方 R 收到 $(w_1,\cdots,w_n)$ 后,对用户 x_i 使用 k 个哈希函数 $h_1,\cdots,h_k$ 计算 $h_u(x)$ 获得 $w_i[h_u(x_l)]$.若用户 x_l 是查询方 R 同 n 个被查询方的交集用户,则获得秘密信誉值 $\bigoplus_{u=1}^{k}w_i[h_u(x_l)]=Enc(\frac{v_j^i}{v})$.$R$ 可从解密结果 $w=Dec(Enc(\frac{v_j^i}{v}))=\frac{v_j^i}{v}$ 判断信誉状况,若 $w<1$,说明该交集用户在其中一家机构信誉不良,记 $|V|=|\{x_l\}\cup V|$,最后输出 $|V|$.

正确性分析 查询方 R 获得 n 个被查询方的 BF_i 经 ElGamal 公钥 pk 加密的结果 $EBF_i=Enc(BF_i)$ 计算获得 $EBF=\prod_{i=1}^{n}EBF_i$.当查询的用户 x_l 是交集用户时,由于 ElGamal 的乘法同态性 EBF 中交集元素对应位置保持“1”值,R 输入信誉阈值 $Enc(v^{-1})$ 计算后返回.推导如下:

$$\begin{aligned}EBF=\prod_{i=1}^{n}EBF_i=Enc(pk_1,BF_1)\times\cdots\times Enc(pk_n,EB_n)=(g^{r_1}\bmod p,BF_1\cdot pk^{r_1}\bmod p)\times\cdots\times\\(g^{r_n}\bmod p,BF_n\cdot pk^{r_n}\bmod p)=(g^{r_1+\cdots+r_n}\bmod p,BF_1\times\cdots\times\\BF_n\cdot pk^{r_1+\cdots+r_n}\bmod p)=Enc(BF_1\times\cdots\times BF_n).\end{aligned}\tag{1}$$

被查询方 S_i 对查询方 R 提供的信誉阈值 $Enc(v^{-1})$ 输入信誉值明文进行计算,利用 ElGamal 标量乘法性质即可获得交集用户的秘密信誉值比较结果:

$$\begin{aligned}w_i=value\cdot VBF_i=EBF\cdot Enc(v^{-1})\cdot VBF_i=Enc(BF_1\times\cdots\times BF_n)\cdot Enc(v^{-1})\cdot\\\bigoplus_{u=1}^{k}VBF_i[h_n(x_l)]=Enc(BF_1\times\cdots\times BF_n)\cdot Enc(v^{-1})\cdot v_j^i=1\cdot Enc(\frac{v_j^i}{v}).\end{aligned}\tag{2}$$

因此,当查询 x_l 是交集用户时,协议 1 可正确输出其在所有机构不良信誉.

3.3 多方隐私集合交集基数

协议 1 计算了查询方 R 同 n 个被查询方的交集用户,但当待查询用户未在所有机构创建账户,或仅部分银行留有该用户信誉信息时,查询方 R 执行协议 1 无法找到用户在其他机构的信誉,导致比较失败,从而无法准确评估信誉.现实中用户在 n 个机构均创建账户的概率较低,更多的是在部分机构设有账户和信誉信息,此时只需评估用户在这些机构中的信誉情况即可.传统的交集基数是指所有方都出现的交集元素个数,例如文献[14]所求交集基数.而本场景需确定用户在多少个机构中存在,现有交集基数求解方法无法满足.

因此本节设计了多方交集基数及秘密信誉值比较协议,使查询方获得待查询用户在 n 家机构中出现的基数 $|w|$ 和不良信誉次数 $|V|$.

在协议 2 中,n 个被查询方 $S_1,\cdots,S_n$ 分别生成密钥对 (pk_i,sk_i),并将公钥 pk_i 发送给查询方 R,由 R 计算公共公钥 $pk=\prod_{i=1}^{n}pk_i$,在之后的执行步骤中用此公钥加密参数.被查询方 S_i 对输入元素 $\{(y_j^i,v_j^i)\}$ 生成 VBF_i 并加密.对新用户来说,若在本机构中没有信誉记录,则设定信誉值为安全临界值.当查询方 R 对集合 $\{(x_l,v_l)\}$ 中元素 x_l 映射到 VBF_i 相应位置获得份额 $VBF_i[h_u(x_l)]$,只有输入 x_l 也是被查询方 S_i 的用户时,才能通过异或份额计算出正确的秘密信誉值份额 $c_{l,j}=\bigoplus_{u=1}^{k}VBF_i[h_u(x_l)]$,但无法解密.查询方 R 查询用户 x_l 在 n 家机构的情况,获得 n 个密文结果 $c_{l,1},\cdots,c_{l,n}$,并对用户的信誉值 v_l 计算 $Enc(v_l^{-1})$,利用 ElGamal 算法乘同态特性计算 $c_{l,i}\cdot Enc(v_l^{-1})$,并将结果发送给 n 个被查询方 S_i.由 S_i 使用私钥 sk_i 提供解密份额后返回,查询方 R 完成聚合解密后获得交集基数 $|w|$ 和信誉不良个数 $|V|$. 协议 2 具体执行步骤如下.

协议 2　多方交集基数及秘密信誉比较协议

输入:查询方 R 的数据集 X,被查询方 S_i 的数据集 Y_i,$i\in[1,n]$,集合大小为分别为 $m_R,m_1,\cdots,m_n$,$j\in[1,m_i]$.

输出:交集基数 $|w|$,信誉不良基数 $|V|$,$\dfrac{|V|}{|w|}$.

步骤 1　初始化

(1)被查询方 S_i 生成 ElGamal 密钥对 (pk_i,sk_i),将公钥 pk_i 发送给查询方 R,$i\in[1,n]$.

(2)查询方 R 计算 $pk=\prod_{i=1}^{n}pk_i=g^{\sum_{i=1}^{n}sk_i}$ 并选择 k 个哈希函数,公开参数 $(pk,h_1,\cdots,h_k)$.

步骤 2　预处理阶段

(1)查询方 R 对每个用户 x_l 相应的信誉值 v_l,使用公钥 pk 计算 $Enc(v_l^{-1})$,$l\in[1,m_R]$.

(2)被查询方 S_i 对自己的集合 $Y_i=\{(y_1^i,v_1^i),\cdots,(y_{m_i}^i,v_{m_i}^i)\}$,$j\in[1,m_i]$,生成哈希映射后的 VBF_i,并使用公钥 pk 加密发送给查询方 R.这样被查询方 S_i 生成的 VBF_i 整体由密文构成,元素映射后异或结果为 $Enc(v_j^i)$,其余位置为密文 $Enc(1)$.

步骤 3　在线阶段.查询方 R 接收到 $VBF_i=(VBF_1,\cdots,VBF_n)$,准备计算:

(1)查询方 R 对元素 $X=\{(x_l,v_l)\}$ 使用 k 个哈希函数计算 $c_{l,i}^u=VBF_i(h_u(x_l))$ 对 k 个 $c_{l,i}^u$ 联合计算 $c_{l,i}=\bigoplus_{u=1}^{k}VBF_i[h_u(x_l)]$,其中 $i\in[1,n]$,$l\in[1,m_R]$,$u\in[1,k]$.

(2)对查询方 R 在预处理阶段计算的信誉值密文 $Enc(v_l^{-1})$,计算 $C_{l,i}=c_{l,i}\cdot Enc(v_l^{-1})$,并将 $(C_{l,1},\cdots,C_{l,n})$ 发送给每一个被查询方 $S_1,\cdots,S_n$.

(3)被查询方 S_i 使用各自持有的私钥 sk_i,对 $(C_{l,1},\cdots,C_{l,n})$ 计算解密份额 $share_{l,i}=((C_{l,1})^{sk_i}\bmod p,\cdots,(C_{l,n})^{sk_i}\bmod p)$,$i\in[1,n]$,将 $share_{l,i}$ 发送给查询方.

步骤 4　离线阶段

(1)查询方 R 收到 n 方发送的密文份额后 $(share_{l,1},\cdots,share_{l,n})$ 后,计算 $Cipher_{l,i}=\prod_{i=1}^{n}share_i^{sk_i}\bmod p$,解密计算获得明文 $Dec(Cipher_{l,i})$,$i\in[1,n]$,$l\in[1,m_R]$.

(2)若成功解密 $w_{l,i}=Dec(Cipher_{l,i})$,则有 $|w|=|\{x_l\}\cup w|$,说明用户在其中一家机构中存在账户.查询方 R 继续计算 $Cipher_{l,i}$,从解密结果 $w_{l,i}=\dfrac{v_j^i}{v_l}$ 判断信誉状况,若 $w_{l,i}<1$,则有 $|V|=|\{x_l\}\cup V|$,说明用户在一家机构中信誉状况不佳.最终输出 $\dfrac{|V|}{|w|}$.

正确性分析　n 个被查询方 $S_1,\cdots,S_n$ 对集合 Y_i 生成的 VBF_i 使用公钥 pk 加密后隐藏信誉值明文.查询方 R 在获得 S_i 发送的 VBF_i 后,计算待查询用户 x_l 在各方 VBF_i 中映射到的值 $c_{l,i}^u=(c_{l,i}^1,\cdots,c_{l,i}^k)=(VBF_i[h_1(x_l)],\cdots,VBF_i[h_k(x_l)])$,$l\in[1,m_R]$,异或后结果为 $c_{l,i}=\bigoplus_{u=1}^{k}VBF_i[h_u(x_l)]$.对 $i\in[1,n]$,

查询方对 c_l^i 与用户 x_l 对应秘密信誉值进行运算并返回 $C_{l,i}=c_{l,i}\cdot Enc(v_l^{-1})=(c_{l,1}\cdot Enc(v_l^{-1}),\cdots,c_{l,n}\cdot Enc(v_l^{-1}))$.被查询方 S_i 提供解密份额 $share_l^{sk_i}=(share_l^{i,1},\cdots,share_l^{i,n})=(C_{l,i}^{sk_1} \bmod p,\cdots,C_{l,i}^{sk_n} \bmod p)$,查询方 R 计算 $\prod_{i'=1}^{n} share_l^{sk_i}$.

当查询方 R 最终解密 $Cipher_{l,i}=\prod_{i'=1}^{n} share_l^{sk_i} \bmod p$ 时:

$$w_l^i=Dec(Cipher_{l,i})=Dec(\prod_{i=1}^{n} share_l^{sk_i} \bmod p)=Dec(C_{l,i}^{\sum_{i=1}^{n} sk_i} \bmod p)=$$

$$Dec(\bigoplus_{u=1}^{k} VBF_i[h_u(x_l)]\cdot Enc(pk,v_l^{-1}) \bmod p)=Dec(Enc(pk,v_j^i)\cdot Enc(pk,v_l^{-1}) \bmod p)=\frac{v_j^i}{v_l}. \quad (3)$$

3.4 多密钥解密

在 3.3 节中协议 2 要求公钥由 n 个被查询方 $S_1,\cdots,S_n$ 的公钥 pk_i 聚合而成,所有参数基于该公钥加密,其中 S_i 保留私钥.查询方 R 只有获得足够多的私钥份额,才能成功解密输出消息 $\frac{|V|}{|w|}$ 或 $\perp$.若查询方 R 有交集用户 $\{(x_l,v_l)\}$,被查询方 S_i 在 VBF_i 中输入对应用户可获得 $Enc(v_i)$.利用 ElGamal 算法的乘法同态性实现,就能实现 v_i 和 v_l 的大小比较($v_l>v_i$ 或 $v_l\leq v_i$),具体协议描述如下.

协议 3 秘密信誉值比较协议

输入:查询方 R 的秘密信誉值 v_l,被查询方 S_i 的秘密信誉值 v_i.

输出:v_l 和 v_i 秘密信誉值比较结果.

步骤 1 被查询方 S 生成 ElGamal 加密公钥对 (pk_i,sk_i),将公钥 pk_i 发送给查询方 R,R 计算公钥 $\prod_{i=1}^{n} pk_i=pk$,公开 pk,任一被查询方 S_i 持有私钥 $sk_i=\alpha$.

步骤 2 查询方 R 查询用户 x_l 在被查询方 S_i 的 VBF_i 中对应秘密信誉值 $Enc(v_i)$.

步骤 3 查询方 R 使用公钥 pk 加密 v_l^{-1} 得到 $Enc(v_l^{-1})=(c_1,c_2)=(g^{r_1} \bmod p,v_l^{-1}h^{r_1} \bmod p)$,计算 $(c_1',c_2')=Enc(v_l^{-1})\cdot Enc(v_i)$ 并结果发送给被查询方 S_i.

步骤 4 被查询方 S_i 收到 (c_1',c_2') 后,使用私钥 α_i 解密计算 $C_{l,i}=((c_1')^{\alpha_i},c_2')$ 并发给查询方 R.

步骤 5 查询方 R 将收到的 n 个 $C_{l,i}$ 联合计算 $\prod_{i=1}^{n} C_{l,i}=\prod_{i=1}^{n}(c_1^i)^{sk_i}=c_1^{i\sum_{i=1}^{n} sk_i}$,输出 $\frac{|V|}{|w|}$.

正确性分析 参与解密的被查询方 S_i 各自持有 ElGamal 密钥对 (pk_i,sk_i),由查询方 R 计算总公钥 $pk=\prod_{i=1}^{n} pk_i$,又 $pk_i=g^{sk_i} \bmod p$,则公钥 pk 满足

$$pk=\prod_{i=1}^{n} pk_i \bmod p=\prod_{i=1}^{n} g^{sk_i} \bmod p=g^{\sum_{i=1}^{n} sk_i} \bmod p. \quad (4)$$

当被查询方 S_i 对明文消息 M 选择随机数 $r\in Z_p^*$ 进行加密时,则有:

$$Enc(M)=(c_1',c_2')=(g^r \bmod p,M\cdot pk^r \bmod p). \quad (5)$$

查询方 R 解密时计算 $Dec(M)=\frac{c_2}{c_1^{sk}} \bmod p$,但总私钥 sk 未知,需要 S_i 返回后 $(c_1')^{sk_i}=g^{r\cdot sk_i} \bmod p$ 联合计算 $\prod_{i=1}^{n}(c_1')^{sk_i}=g^{r\sum_{i=1}^{n} sk_i}$ 解密,结果如下:

$$\frac{c_2}{\prod_{i=1}^{n}(c_1')^{sk_i}} \bmod p=\frac{M\cdot pk^r \bmod p}{\prod_{i=1}^{n} g^{r\cdot sk_i} \bmod p}=\frac{M\cdot(\prod_{i=1}^{n} g^{sk_i})^r \bmod p}{\prod_{i=1}^{n} g^{r\cdot sk_i}}=\frac{M\cdot g^{r\cdot\sum_{i=1}^{n} sk_i} \bmod p}{g^{r\cdot\sum_{i=1}^{n} sk_i} \bmod p}=M. \quad (6)$$

M 对应 $\frac{v_i}{v_l}$,根据解密出 M 与“1”的大小关系,判定用户在被查询方 S_i 的信誉值状况,可确定查询的用户在被查询方 S_i 中存在交集.若 $M<1$ 则说明用户在被查询方 S_i 中信誉不良.

4 安全性证明

采用被广泛接受的模拟范式[15]来证明协议 1、2、3 的安全性.

定理 1　协议 1 在半诚实模型下安全地计算多方集合交集及信誉状况.

证明　假设存在多项式时间模拟器 Sim_R 和模拟器 Sim_S，使得 Sim_R 和 $View_R^{\pi}$ 以及 Sim_S 和 $View_S^{\pi}$ 在计算上无法区分，即：

$$Sim_R\{X, |V|\} \overset{c}{\equiv} View_R^{\pi}, \tag{7}$$

$$Sim_S\{Y_i, \perp\} \overset{c}{\equiv} View_S^{\pi}. \tag{8}$$

当式(7)、(8)成立时多方交集计算协议 π 在半诚实敌手存在时是安全的.

首先，假设查询方 R 是腐败方的情况，构造模拟器 Sim_R 模拟 R 的视图.模拟器 Sim_R 收到 R 的集合输入 X 和输出结果 $|V|$，腐败方 R 执行协议时的真实视图为 $View_R^{\pi}$，即 $View_R^{\pi}=\{X,(pk,sk),w,(v_1,\cdots,v_n),|V|\}$.对于随机生成的 $\{Y_1',\cdots,Y_n'\}$，模拟器 Sim_R 经 ElGamal 公钥 pk 加密后产生的 $\{EBF_1',\cdots,EBF_n'\}$ 和真实世界执行协议产生 $\{EBF_1,\cdots,EBF_n\}$ 的不可区分，因此 $w' \overset{c}{\equiv} w$.而腐败方 R 无法区分根据 $\{VBF_1',\cdots,VBF_n'\}$ 和 w' 计算后得到的 $\{value_1',\cdots,value_n'\}$ 和协议执行过程中获得的 $\{value_1,\cdots,value_n\}$.模拟器 $Sim_R\{X,|V|\}=\{X,(pk,sk),w',(v_1',\cdots,v_n'),|V|\}$，因此式(7) 成立.同理，腐败方 S_i 执行协议时的真实视图 $View_S^{\pi}=\{Y_i,w,\perp\}$ 和模拟器 Sim_S 模拟 S_i 的视图 $Sim_R\{Y_i,\perp\}$ 无法区分，即式(8)成立.协议 1 达到半诚实安全.

定理 2　协议 2 在半诚实模型下安全地输出查询用户在 n 方的交集基数以及不良信誉情况，且协议能够抵抗 $n-1$ 个敌手合谋.

证明　从 2 种情况考虑协议 2 中可能发生的不诚实行为：一种是敌手控制的腐败方包括查询方 R，另一种是不包括查询方 R.本节针对此分析协议 2 安全性.

情况 1　存在 t 个被查询方 S_i 是腐败方且查询方 R 不受敌手控制.

假定 t 个腐败方 $S_1,\cdots,S_t$ 被敌手控制，敌手可获得腐败方输入及协议执行过程产生的参数.构建模拟器 Sim_{S_t} 模拟 t 个腐败方 $S_1,\cdots,S_t$ 的视图，模拟器 Sim_{S_t} 收到数据集 $\{Y_1,\cdots,Y_t\}$、公钥对 (pk_i,sk_i) 和信誉过滤器 $\{VBF_1,\cdots,VBF_t\}$，为查询方 R 提供私钥 sk_i 解密的份额 $share_{l,i}$，$i\in[1,t]$，记腐败方 $S_1,\cdots,S_t$ 执行协议时的真实视图为 $View_{S_i}^{\pi}=\{(Y_1,\cdots,Y_t),(pk_1,\cdots,pk_i),(VBF_1,\cdots,VBF_t),(share_{l,1},\cdots,share_{l,t})\}$.

由于模拟器 Sim_{S_i} 控制 t 个被查询方，它只能获得 t 个被查询方的密钥份额，且在 ElGamal 多密钥加密中，交集用户信誉值的解密需要全部 n 个被查询方的联合计算，所以模拟器 Sim_{S_i} 无法从 t 个腐败方的联合计算中获得最终的解密结果.

t 个被查询方 $S_1,\cdots,S_t$ 在协议真实交互过程中的视图表示为 $View_{S_i}^{\pi}$，而模拟器 Sim_{S_i} 的视图为 $Sim_t\{(Y_1,\cdots,Y_t),\perp\}$.对于随机生成的元素 $(Y_1,\cdots,Y_t)$ 和 $(pk_1,\cdots,pk_i)$，由于 ElGamal 算法的安全性和随机性，模拟器 Sim_t 生成的 $(VBF_1',\cdots,VBF_t')$ 和真实协议中的 $(VBF_1,\cdots,VBF_t)$ 在计算上是不可区分的.对不同被查询方 $S_1,\cdots,S_t,S_{t+1},\cdots,S_n$ 使用私钥对密文 $C_{l,i}'$ 计算生成的 $(share_{l,1}',\cdots,share_{l,t}')$ 和 $(share_{l,1},\cdots,share_{l,t})$ 在计算上是不可区分的.因此：$Sim_{S_t}\{(Y_1,\cdots,Y_t),\perp\} \overset{c}{\equiv} View_{S_t}^{\pi}$.

情况 2　存在 t 个被查询方 S_i 是腐败方且查询方 R 也是腐败的.

与以上情况相同，构建模拟器 Sim_{R,S_t} 模拟腐败方 R 和 $S_1,\cdots,S_t$ 的视图.模拟器 Sim_{R,S_t} 收到的输入集为 $\{X,Y_1,\cdots,Y_t\}$，从 $S_1,\cdots,S_t$ 获取 $\{VBF_1,\cdots,VBF_t\}$ 以及计算的中间结果 $(C_{l,1},\cdots,C_{l,t})$ 和 $(share_{l,1},\cdots,share_{l,t})$，最后输出结果为 $\frac{|V|}{|w|}$，记腐败方 R 和 $S_1,\cdots,S_t$ 执行协议时的真实视图为：

$$View_{R,S_t}^{\pi}=\{(X,Y_1,\cdots,Y_t),(pk,pk_1,\cdots,pk_t),(VBF_1,\cdots,VBF_t),(C_{l,1},\cdots,C_{l,t}),(share_{l,1},\cdots,share_{l,t}),\frac{|V|}{|w|}\}. \tag{9}$$

模拟器 Sim_{R,S_t} 拥有 $\{pk,(pk_1,sk_1),\cdots,(pk_t,sk_t)\}$，但解密 $C'^{\sum_{i=1}^{t}sk_i+\sum_{t+1}^{n}sk_i'}$ 需要 $S_{t+1},\cdots,S_n$ 的私钥 $\{sk_{t+1},\cdots,sk_n\}$，由于 ElGamal 加密算法是基于离散对数困难问题的，仅通过 pk 和 $(pk_1,sk_1),\cdots,(pk_t,sk_t)$ 无法分解解密出 $C_{l,i}'$ 对应的明文，而模拟器 Sim_{R,S_t} 生成的 $\{share_{l,1},\cdots,share_{l,t},share_{l,t+1}',\cdots,share_{l,n}'\}$ 和

真实协议执行过程中产生的($share_{l,1},\cdots,share_{l,t},share'_{l,t+1},\cdots,share'_{l,n}$)在密文下无法区分,敌手也无法从中获取解密结果以及用户信息.因此,$Sim_{R,S_t}\{(X,Y_1,\cdots,Y_t),\frac{|V|}{|w|}\}\overset{c}{\equiv}View^{\pi}_{S_t}$.

情况 3 仅查询方 R 是腐败方.

假设查询方 R 是腐败方,意图获取被查询方 S_i 的用户信誉值,在整个过程中,敌手可以获得输入和最终的输出结果.腐败方 R 的真实视图为 $View^{\pi}_{R}$,输入集为 X,最终输出为$\frac{|V|}{|w|}$.此处不再详细证明,腐败方无法获得诚实被查询方的隐私信息,模拟视图与真实视图是不可区分,因此,$Sim_R\{X,\perp\}\overset{c}{\equiv}View^{\pi}_{R}$.

从以上 3 种情况可以看出,面对半诚实敌手时,敌手无法推断出诚实方的输入集,也无法从中间的消息推断出最终结果.至此,协议 2 半诚实安全的.

定理 3 在半诚实模型下,协议 3 保密地计算了秘密信誉值比较结果.

证明 对任意半诚实敌手构造模拟器 Sim_R 和 Sim_S 模拟功能 $f_1(v_l,v_i)=f_2(v_l,v_i)=\frac{|V|}{|w|}$.模拟器 Sim_r 模拟查询方 R 的行为:由 ElGamal 算法是语义安全的,$output_S(v_l,v_i)$ 与 $f_2(v_l,v_i)$ 是计算不可区分的.构造模拟器 Sim_S 模拟被查询方 S 的行为,$output_1(v_l,v_i)$ 和 $f_1(v_l,v_i)$ 是计算不可区分的.

$$\{Sim_R(v_l,f_1(v_l,v_i),f_2(v_l,v_i))\}\overset{c}{\equiv}\{view_1(v_l,v_i),output_2(v_l,v_i)\},\tag{10}$$

$$\{f_1(v_l,v_i),Sim_S(v_2,f_2(v_l,v_i))\}\overset{c}{\equiv}\{output_1(v_l,v_i),view_2(v_l,v_i)\}.\tag{11}$$

至此,定理 3 证毕.

5 性能分析与比较

5.1 性能分析

该实验依赖 GMP 库和 NTL 库完成 ElGamal 加密,实验中选择 1 024 bit 大素数、随机生成 32 bit 元素进行操作,进行多次重复实验并取平均值作为最终结果.

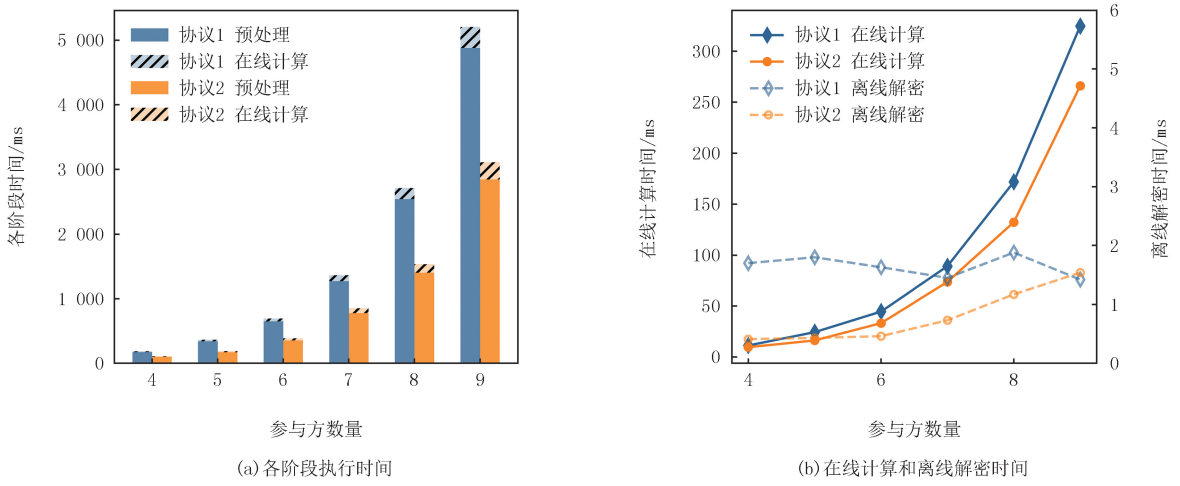
当设置查询方 R 集合为 2^8、被查询方集合大小为 2^{10},被查询方 n 个数分别设置为$\{2^4,2^5,2^6,2^7,2^8,2^9\}$时,协议 1 和协议 2 运行时间如表 1 所示.结果显示协议 1 预处理耗时,因涉及加密布隆过滤器和生成 VBF 操作,且参与方数量增多时,查询方需要执行解密操作时间不受影响,在线计算时间成倍增加.在协议 2 中,查询方需要获取 n 个参与方提供的解密份额,随着被查询方数量增多,解密耗时增长.由于仅需对生成的 VBF 执行加密操作,协议 2 的整体耗时优于协议 1,但 2 种协议总耗时均在执行预处理阶段.

表 1 不同参与方下协议各阶段运行时间

Tab. 1 Running time of phases of the agreement under different participants ms

被查询方个数	协议	预处理	在线计算	离线解密	总时间	被查询方个数	协议	预处理	在线计算	离线解密	总时间
2^4	协议 1	176.32	11.30	1.70	189.65	2^7	协议 1	1 273.78	89.10	1.45	1 364.96
	协议 2	102.04	9.62	0.41	112.70		协议 2	778.00	73.68	0.73	852.73
2^5	协议 1	342.45	24.37	1.80	368.92	2^8	协议 1	2 541.47	171.85	1.88	2 715.57
	协议 2	174.52	16.24	0.43	191.80		协议 2	1 402.73	132.30	1.17	1 536.15
2^6	协议 1	650.12	44.58	1.63	696.70	2^9	协议 1	4 878.82	324.81	1.42	5 205.45
	协议 2	354.75	33.22	0.46	388.43		协议 2	2 844.82	266.16	1.54	3 112.53

接着对比协议 1 和协议 2 各阶段运行时间以及在线计算与离线解密时间.如图 1(a)所示,协议 2 整体各项执行时间均优于协议 1,其中预处理时间占比显著,导致总耗时增长,原因在于多个被查询方在该阶段对持有的大集合用户数据进行处理.从图 1(b)所示的 2 种协议的在线时间和离线解密时间,协议 2 虽一开始优于协议 1,但随着被查询方数量增多,查询方 R 离线解密的时间增加,逐渐超过协议 1,因此协议 2 更适合参与方数量有限的查询.



(a) 各阶段执行时间　　(b) 在线计算和离线解密时间

图1　2种协议各项执行时间对比

Fig. 1　Comparison of implementation time for each of the two agreements

5.2　方案比较

为了与文献[5]和[7]方案性能对比，设置大集合方为服务器，小集合方为客户端.当参与方数量为 2^5 时，小集合大小设为 2^8、大集合分别设为$\{2^{10},2^{11},2^{12},2^{13},2^{14}\}$时，各方执行时间如表 2 所示.实验显示，被查询方数据量小时，协议 1 与现有方案效率相近，协议 2 更优.当被查询方数据量较大时，客户端执行效率均优于文献[5]和[7].协议 1 中大集合方的服务器端执行时间虽高于文献[7]，但在后续工作中可通过并行执行编码优化.

表 2　与其他方案的实验时间对比

Tab. 2　The time of experimental comparison with other schemes　　s

方案来源	参与方	2^{10}	2^{11}	2^{12}	2^{13}	2^{14}	方案来源	参与方	2^{10}	2^{11}	2^{12}	2^{13}	2^{14}
文献[5]	Client	9.52	18.90	37.60	76.49	154.54	本文协议 1	Client	8.85	16.01	19.29	21.30	22.10
	Server	22.96	43.63	87.13	166.92	345.27		Server	11.33	19.63	31.84	65.12	119.53
文献[7]	Client	1.49	3.00	5.90	13.32	28.39	本文协议 2	Client	0.34	0.62	1.31	2.59	5.02
	Server	3.10	6.08	13.61	27.99	56.98		Server	5.05	10.12	20.23	40.65	77.12

6　结　论

本文基于 VBF 构造和多密钥加解密原理提出 2 种多方隐私集合交集及秘密数据比较协议，在隐藏查询方查询意图的前提下，保护了被查询方的用户身份和隐私数据.协议执行结束后，查询方获得信誉查询结果，而被查询方对查询结果无从得知，最终实现机构中用户信息隐私安全，同时在 t 个腐败方($t<n$)联合的情况下，证明协议达到半诚实敌手的安全.

附录见电子版(DOI:10.16366/j.cnki.1000-2367.2024.04.13.0001).

参　考　文　献

[1]　高莹，王玮.多方隐私集合交集计算技术综述[J].电子与信息学报，2023，45(5)：1859-1872.
GAO Y，WANG W.A survey of multi-party private set intersection[J].Journal of Electronics & Information Technology，2023，45(5)：1859-1872.

[2]　张萍，蒋琳.隐私保护的网络实名制体系研究[J].河南师范大学学报(自然科学版)，2021，49(6)：91-98.
ZHANG P，JIANG L.Research on privacy-preserving Internet real-Name system[J].Journal of Henan Normal University(Natural Science Edition)，2021，49(6)：91-98.

[3]　FREEDMAN M J，NISSIM K，PINKAS B.Efficient private matching and set intersection[C]//Advances in Cryptology-EUROCRYPT

2004.Berlin:Springer Berlin Heidelberg,2004:1-19.
[4] KISSNER L,SONG D.Privacy-preserving set operations[C]//Advances in Cryptology-CRYPTO 2005.Berlin:Springer Berlin Heidelberg,2005:241-257.
[5] BAY A,ERKIN Z,HOEPMAN J H,et al.Practical multi-party private set intersection protocols[J].IEEE Transactions on Information Forensics and Security,2022,17:1-15.
[6] DAVIDSON A,CID C.An efficient toolkit for computing private SetOperations[C]//Information Security and Privacy.Cham:Springer International Publishing,2017:261-278.
[7] RUAN O,YAN C W,ZHOU J,et al.A practical multiparty private set intersection protocol based on bloom filters for unbalanced scenarios[J].Applied Sciences,2023,13(24):13215.
[8] YAO A C.Protocols for secure computations[C]//23rd Annual Symposium on Foundations of Computer Science(sfcs 1982).November 3-5,1982.Chicago:IEEE,1982:160-164.
[9] 张静,何铮,葛炳辉,等.一种高效的百万富翁问题协议及其应用[J].计算机工程,2021,47(2):168-175.
ZHANG J,HE Z,GE B H,et al.An efficient protocol for millionaires'problem and its application[J].Computer Engineering,2021,47(2):168-175.
[10] 李顺东,王文丽,陈明艳,等.抗主动攻击的保密比较协议[J].软件学报,2022,33(12):4771-4783.
LI S D,WANG W L,CHEN M Y,et al.Comparing protocol against active attacks[J].Journal of Software,2022,33(12):4771-4783.
[11] BLOOM B H.Space/time trade-offs in hash coding with allowable errors[J].Communications of the ACM,1970,13(7):422-426.
[12] DONG C Y,CHEN L Q,WEN Z K.When private set intersection meets big data:an efficient and scalable protocol[C]//Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security-CCS'13.November 4-8,2013.Berlin:ACM,2013:789-800.
[13] ELGAMAL T.A public key cryptosystem and a signature scheme based on discrete logarithms[C]//Advances in Cryptology.Berlin:Springer Berlin Heidelberg,1985:10-18.
[14] YANG X Y,ZHAO Y Q,ZHOU S F,et al.A lightweight delegated private set intersection cardinality protocol[J].Computer Standards & Interfaces,2024,87:103760.
[15] LINDELL Y.How to simulate it-a tutorial on the simulation proof technique[M].Tutorials on the Foundations of Cryptography:Dedicated to Oded Goldreich,[S.l.]:Springer,2017.

Multiparty privacy set intersection and secret reputation value comparison protocols

Li Gongli[a,b], Fan Yun[a], Ma Jingwen[a]

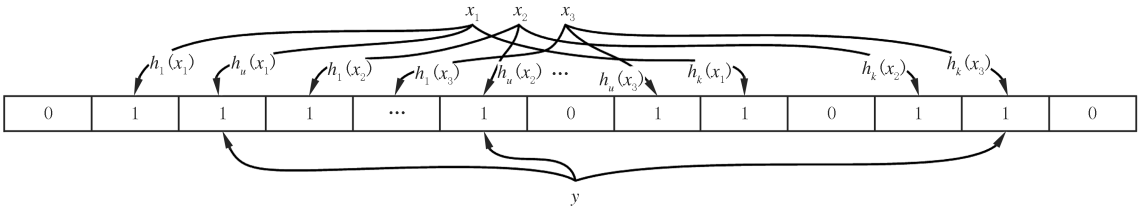
(a. College of Computer and Information Engineering; b. Key Laboratory of Artificial Intelligence and Personalized Learning in Education of Henan Province, Henan Normal University, Xinxiang 453007, China)

Abstract: Multiparty private set intersection(MPSI), as a data security protection computation technology in the field of secure computation, supports the computation of the intersection of multiple participant datasets without revealing any participant's privacy, which can be achieved by using homomorphic encryption, oblivious transfer, and other technical means. However, the existing MPSI protocols based on homomorphic encryption have problems such as low computational efficiency and many rounds of interaction, and cannot compute the intersection of users' confidential data through interaction. Therefore, this article first proposes an n-party intersection user's secret reputation value comparison protocol, based on bloom filters and the ElGamal algorithm. Furthermore, aiming at the problem of failed query intersection, a user intersection cardinality protocol is proposed based on reputation value filters and multi-key encryption and decryption, and the evaluation of multi-party secret reputation values is completed. Experimental results show that the two protocols proposed in the study satisfy semi-honest security, can resist coalitions of $n-1$ participants, and have better execution time than other schemes.

Keywords: multi-party private set intersection; secret reputation comparison; reputation threshold comparison; multiple secret reputation value comparison; multiparty intersection cardinality

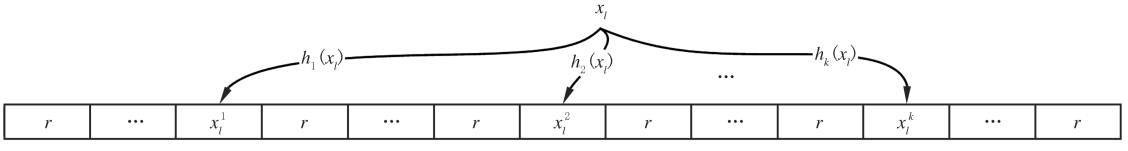
[责任编校 赵晓华 刘洋]

附　录



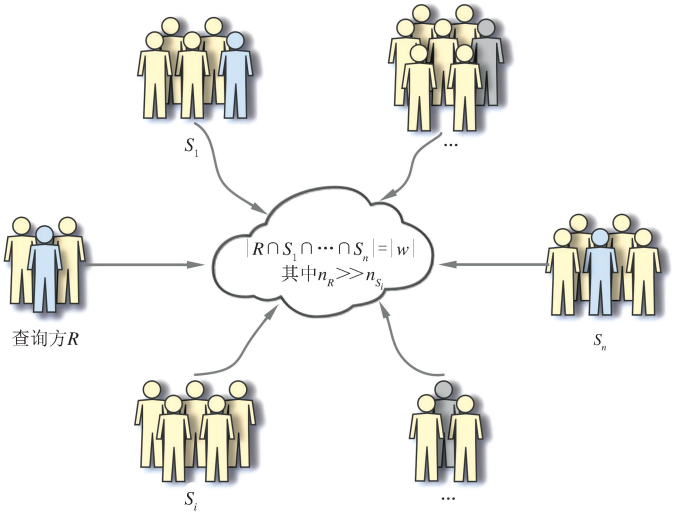
图S1　插入元素$\{x_1, x_2, x_3\}$到BF

Fig. S1　Insert element $\{x_1, x_2, x_3\}$ into BF



图S2　插入元素x_l到GBF

Fig. S2　Insert element x_l into GBF



图S3　多方隐私集合交集的理想功能

Fig. S3　Multi-party private set intersection ideal functions