Computer Science and Application 计算机科学与应用, 2021, 11(8), 2080-2087
Published Online August 2021 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2021.118213

Hans汉斯

有理数域上集合成员关系的保密判定协议

李亚伟

长安大学理学院，陕西 西安
Email: 943890247@qq.com

收稿日期：2021年7月5日；录用日期：2021年8月3日；发布日期：2021年8月11日

摘　要

本文通过将有理数按位编码为矩阵，并结合ElGamal同态加密算法，设计了有理数域上集合成员关系的保密判定协议，其中点集成员关系的保密判定协议可适用于$n(n \geq 2)$维有理点。其次，应用模拟范例的方法严格证明了协议的安全性，同时协议能够保护集合的势。最后，比较分析表明当参与者的有理数满足一定条件时，本文设计的协议是高效的。

关键词

集合成员关系，安全多方计算，有理数，ElGamal同态加密算法

Privacy Preserving Protocol of Rational Set Membership's Judge

Yawei Li

School of Science, Chang'an University, Xi'an Shaanxi
Email: 943890247@qq.com

Received: Jul. 5th, 2021; accepted: Aug. 3rd, 2021; published: Aug. 11th, 2021

Abstract

By encoding the rational numbers into a matrix, combined with the ElGamal homomorphic encryption algorithm, this paper designs secure protocol for the rational set membership's judge, in which the protocol for the point set membership can be applied to $n(n \geq 2)$ dimensional rational points. Secondly, using the well accepted simulation paradigm proves that the proposed protocols are secure, and at the same time, the protocol can protect the number of elements in the partici-

文章引用: 李亚伟. 有理数域上集合成员关系的保密判定协议[J]. 计算机科学与应用, 2021, 11(8): 2080-2087.
DOI: 10.12677/csa.2021.118213

pant set. Finally, the comparison and analysis show that the efficiency of the proposed protocol when the rational numbers meet certain conditions.

Keywords

Set Membership, Secure Multi-Party Computation, Rational Number, ElGamal Homomorphic Encryption Algorithm

1. 引言

隐私集合计算是安全多方计算[1] [2]领域中的一类重要问题，集合成员关系的保密判定问题是其中的一个基本问题，要求判定一个元素是否属于一个集合，而不泄露该元素和集合的具体信息。集合成员关系的保密判定问题在可搜索加密[3]、访问控制[4]、可撤销访问结构[5]等问题中有重要的应用。

集合成员关系保密判定可通过数据相等比较[1] [6] [7]、两方集合交集或交集的势[8] [9] [10] [11] [12]、集合包含关系[13] [14] [15] [16]的保密计算协议间接地来实现。上述方法或者需要将元素与集合中元素进行一一比较、或者不需要协议的全部计算功能，会使协议的效率欠佳或导致参与方拥有的信息泄露。文献[17]利用可交换加密方案提出了数集成员关系保密判定协议。文献[18]利用全同态加密，结合范德蒙行列式的性质，设计了集合成员判定关系的相关协议。上述协议均仅适用于整数集上的集合成员关系判定。文献[19]首次设计了有理数域上集合成员关系保密判定协议，并在数集成员关系保密判定协议的基础上，利用哥德尔编码将有理点编码为有理数，设计了点集成员关系的保密判定协议，但该协议只适用于 2 维有理点。

由于信息技术的快速发展，与坐标定位相关的应用软件得到了广泛应用，使用户的位置信息的私密性成为需要关注的问题。因此，设计有理点的相关保密计算协议有重要的实用价值。本文借助文献[20]中提出的按位编码思想，结合 ElGamal 同态加密算法，针对有理数集合成员关系和有理点集成员关系的判定问题设计了保密计算协议。

2. 预备知识

2.1. 安全多方计算模型

安全多方计算中通常使用半诚实模型和恶意模型。半诚实模型下的参与者会忠实地执行协议，但同时他们会保留执行协议中收到的中间信息，并试图推断其它参与者的输入。恶意模型下的参与者不按要求执行协议，可能有拒绝参加协议、提供错误的输入或者中间计算结果以及随时终止协议等行为。本文考虑半诚实模型下协议的安全性。

2.2. 半诚实模型下的安全性定义

设 $P_i(i=1,2)$ 拥有私密信息 X_i，利用协议 π 合作计算函数 $f(X_1,X_2)=(f_1(X_1,X_2),f_2(X_1,X_2))$，其中 $f_i(X_1,X_2)(i=1,2)$ 是 P_i 收到的输出。将参与者 $P_i(i=1,2)$ 收到的信息序列记为 $VIEW_i^{\pi}(X_1,X_2)=(X_i,r_i,m_1^i,m_2^i,\cdots,m_l^i,f_i(X))$，其中 X_i 是 P_i 的输入，r_i 是 P_i 产生的随机数，$m_t^i(t=1,2,\cdots,l)$

表示 P_i 收到的第 t 个消息。

定义 1 [21] (半诚实模型下协议的安全性)对于 $f(X_1,X_2)=(f_1(X_1,X_2),f_2(X_1,X_2))$，若存在概率多项式时间模拟器 $S_i(i=1,2)$ 满足下式：

$$\{S_i(X_i,f(X_1,X_2))\}_{X_1,X_2} \overset{c}{\equiv} \{VIEW_i^{\pi}(X_1,X_2)\}_{X_1,X_2} \tag{1}$$

则称 π 保密地计算了 $f(X_1,X_2)$，其中符号 $\overset{c}{\equiv}$ 表示计算上不可区分。

可通过构造满足式(1)的概率多项式时间模拟器 $S_i(i=1,2)$ 来证明协议的安全性，此方法称为模拟范例[21]。本文将用此方法证明协议的安全性。

2.3. ElGamal 同态加密算法

同态加密的概念最早由 RIVEST [22]提出，可以通过对密文的操作实现对相应明文的计算。ElGamal 加密算法[23]是基于有限域上计算离散对数问题的困难性和 Diffie-Hellman 假设设计的，算法描述如下：

1) 密钥生成算法

对给定安全参数 k，系统生成一个 k 比特的大素数 p 和循环群 Z_p^* 的一个生成元 g。若选取随机数 x 作为私钥，对应公钥为 $h=g^x \bmod p$。

2) 加密算法 E

对明文 $M(M\in Z_p^*)$，选取的随机数 r，加密得密文：$E(M)=(c_1,c_2)=(g^r \bmod p, Mh^r \bmod p)$。

3) 解密算法 D

对于密文 $E(M)$，其明文为：$M=c_2\cdot c_1^{-x} \bmod p$。

ElGamal 同态加密算法具有乘法同态性。对于明文消息 $M_1,M_2(M_1+M_2<p)$，其密文 $E(M_1),E(M_2)$ 满足 $E(M_1)\times E(M_2)=E(M_1\times M_2)$。

3. 有理数域上集合成员关系保密判定

3.1. 编码方法

李顺东[20]等人为了解决多个有理数相等保密判定问题，提出了按位编码的方法，将一个有理数编码为一个矩阵，具体过程如下：

首先，对于参与者 P_i 持有的有理数 $x_i=a_i/b_i=a_i^1a_i^2\cdots a_i^{s_i}/b_i^1b_i^2\cdots b_i^{s_i}$，其中 $\gcd(a_i,b_i)=1$，$a_i^k,b_i^l\in\{0,1,\cdots,9\},1\le k\le s_i,1\le l\le q_i$，统一其分子和分母位数分别为 s,q，位数不够的情况按下式转换数据，

$$x_i\to\frac{0\cdots0a_i^1a_i^2\cdots a_i^{s_i}}{0\cdots0b_i^1b_i^2\cdots b_i^{q_i}}\to e_i^1\cdots e_i^j\cdots e_i^{s+q} \tag{2}$$

即通过在分子分母之前补 0 将其拥有的有理数的分子分母位数统一，并将其分子分母连接起来，其中 $1\le j\le s+q$。其次，根据式(2)将有理数 x_i 按位编码为矩阵：

$$U_{(s+q)\times10}=\begin{bmatrix} u_1^1 & u_2^1 & \cdots & u_{10}^1 \\ u_1^2 & u_2^2 & \cdots & u_{10}^2 \\ \vdots & \vdots & & \vdots \\ u_1^{s+q} & u_2^{s+q} & \cdots & u_{10}^{s+q} \end{bmatrix} \tag{3}$$

对于每一行 $u^j=\begin{bmatrix} u_1^j & u_2^j & \cdots & u_{10}^j \end{bmatrix}(1\le j\le s+q)$，有：

$$u_k^j=\begin{cases}0, & e_i^j=k-1\\ r_k^j, & e_i^j\neq k-1\end{cases} \tag{4}$$

其中 $r_k^j\in Z_p^*$ 且是非零的随机数。现将上述编码方法中的式(4)改为：

$$u_k^j=\begin{cases}1, & e_i^j=k-1\\ r_k^j, & e_i^j\neq k-1\end{cases} \tag{5}$$

其中 $r_k^j\in Z_p^*$ 且是大于 1 的随机数。下文将利用改动后的方法设计有理数域上集合成员关系的保密判定协议。

3.2. 有理数域上数集成员关系的保密判定

问题描述 Alice 拥有有理数 v_0，Bob 拥有有理数集合 $V=\{v_1,v_2,\cdots,v_m\}$。双方希望在不泄露 v_o，V 中元素及 V 的势的前提下合作计算函数 $P(v_0,V)$：若 $v_0\in V$，$P(v_0,V)=1$；否则，$P(v_0,V)=0$。

计算原理 Alice 和 Bob 依据式(2)将有理数 $v_i\ (i=0,1,\cdots,m)$ 作如下转换：

$$v_i\to e_i^1\cdots e_i^j\cdots e_i^{s+q} \tag{6}$$

其中 $1\le j\le s+q$。Alice 依据式(5)将有理数 v_0 编码为矩阵 U，并将 U 发送给 Bob。Bob 对于其拥有的有理数 v_i，依据式(6)中的 $e_i^j\ (1\le j\le s+q)$ 从 u^1 至 u^{s+q} 中依次取出对应位置编码 $u^1_{e_i^1+1},u^2_{e_i^2+1},\cdots,u^{s+q}_{e_i^{s+q}+1}$，计算 $U_i=u^1_{e_i^1+1}u^2_{e_i^2+1}\cdots u^{s+q}_{e_i^{s+q}+1}$，容易得到以下命题是正确的。

命题 1 $P(v_0,V)=1$ 当且仅当对于每一个 $i=1,2,\cdots,m$ 存在 $U_i=1$。

协议 1 有理数域上数集成员关系的保密判定协议

输入：Alice 输入 v_0，Bob 输入 $V=\{v_1,v_2,\cdots,v_m\}$。

输出：$P(v_0,V)$

准备：Alice 和 Bob 依据式(2)对有理数 $v_0,v_i\ (i=1,2,\cdots,m)$ 进行转换得到式(6)。

1. Alice 执行以下操作：

1) 产生 ElGamal 同态算法的密钥对 (sk,pk)；

2) 根据(5)式将 v_0 按位编码为矩阵 U；

3) 利用公钥 pk 加密矩阵 U 中 $u_k^j=1$ 的分量，得加密矩阵：

$$E(U)=\begin{bmatrix}u_1^1 & u_2^1 & \cdots & u_{10}^1\\ u_1^2 & u_2^2 & \cdots & u_{10}^2\\ \vdots & \vdots & & \vdots\\ u_1^{s+q} & u_2^{s+q} & \cdots & u_{10}^{s+q}\end{bmatrix}=\begin{bmatrix}(c_{11}^1,c_{12}^1) & (c_{21}^1,c_{22}^1) & \cdots & (c_{(10)1}^1,c_{(10)2}^1)\\ (c_{11}^2,c_{12}^2) & (c_{21}^2,c_{22}^2) & \cdots & (c_{(10)1}^2,c_{(10)2}^2)\\ \vdots & \vdots & & \vdots\\ (c_{11}^{s+q},c_{12}^{s+q}) & (c_{21}^{s+q},c_{22}^{s+q}) & \cdots & (c_{(10)1}^{s+q},c_{(10)2}^{s+q})\end{bmatrix} \tag{7}$$

其中 $\left(c^j_{\left(e_0^j+1\right)1},c^j_{\left(e_0^j+1\right)2}\right)=E(1)$，$\left(c^j_{\left(\neq e_0^j+1\right)1},c^j_{\left(\neq e_0^j+1\right)2}\right)\in Z_p^*\times Z_p^*$ 为随机数对。Alice 将矩阵 $E(U)$ 及公钥 pk 发送给 Bob。

2. 对于每个 $i=1,2,\cdots,m$，Bob 执行以下操作：

1) 根据式(6)中的 $e_i^j\ (1\le j\le s+q)$ 从 $E(U)$ 中按位取出密文 $E\left(u^1_{e_i^1+1}\right),E\left(u^2_{e_i^2+1}\right),\cdots,E\left(u^{s+q}_{e_i^{s+q}+1}\right)$，并计算：

$$E(U_i)=E\left(u^1_{e_i^1+1}\right)E\left(u^2_{e_i^2+1}\right)\cdots E\left(u^{s+q}_{e_i^{s+q}+1}\right) \tag{8}$$

2) 选取正整数 l，满足 $l>m$。从 Z_p^* 中选取 $l-m$ 个大于 1 的随机数 $r_1,r_2,\cdots,r_{l-m}$，并计算其密文

$E(r_1),E(r_2),\cdots,E(r_{l-m})$；

3) 对密文 $E(U_i),E(r_1),E(r_2),\cdots,E(r_{l-m})(i=1,2,\cdots,m)$ 的顺序进行随机置换，并按置换后的顺序发送给 Alice。

3. Alice 解密收到的密文，记解密结果为 $d_k\ (1\le k\le l)$。若存在 $d_k=1$，Alice 输出 $P(v_0,V)=1$；否则，输出 $P(v_0,V)=0$。

正确性分析 命题 1 的正确性及本文采用的 ElGamal 加密算法的同态性保证了协议 1 的正确性。

安全性分析 Alice 将加密矩阵 $E(U)$ 发送给 Bob，由于 Bob 没有私钥，因此无法获得有理数 v_0 的任何信息。Bob 将随机置换后的 l 个密文 $E(U_i),E(r_1),E(r_2),\cdots,E(r_{l-m})(i=1,2,\cdots,m)$ 发送给 Alice，由于 Alice 不知道具体置换，因此无法推得集合 V 中任何元素的信息；同时，由于随机数 $r_1,r_2,\cdots,r_{l-m}$ 均大于 1，则发送密文 $E(r_1),E(r_2),\cdots,E(r_{l-m})$ 给 Alice 的操作不影响协议的正确性且隐藏了集合 V 的势。

定理 1 协议 1 在半诚实模型下是安全的。

证明：利用模拟范例证明协议 1 的安全性。在协议 1 中，$f_1(v_0,V)=f_2(v_0,V)=P(v_0,V)$。首先构造模拟器 S_1，S_1 接受输入 $(v_0,P(v_0,V))$，按照如下方式运行：

1) 随机选取有理数集 $V'=\{v_1',v_2',\cdots,v_m'\}$ 使得 $P(v_0,V)=P(v_0,V')$，将 $v_0,v_i'(i=1,2,\cdots,m)$ 进行转换：

$$\begin{aligned} v_0&\to e_0^1\cdots e_0^j\cdots e_0^{s+q}\\ v_i'&\to e_i^{1\prime}\cdots e_i^{j\prime}\cdots e_i^{s+q\prime}\end{aligned}\tag{9}$$

2) S_1 将 v_0 编码为矩阵 U，并加密得矩阵 $E(U)$，如式(7)所示。

3) 计算 $E(U_i')=E\left(u_{e_i^{1\prime}+1}^1\right)E\left(u_{e_i^{2\prime}+1}^2\right)\cdots E\left(u_{e_i^{s+q\prime}+1}^{s+q}\right)$，$(i=1,2,\cdots,m)$，生成 $l-m$ 个大于 1 的随机数 $r_1',r_2',\cdots,r_{l-m}'$，计算其密文 $E(r_1'),E(r_2'),\cdots,E(r_{l-m}')$。

4) 解密 $E(U_i'),E(r_1'),E(r_2'),\cdots,E(r_{l-m}')(i=1,2,\cdots,m)$，记解密结果为 $d_k'\ (1\le k\le l)$，根据 d_k' 可得 $P(v_0,V')$。

令 $S_1(v_0,P(v_0,V))=\{v_0,E(U_i'),r_u',E(r_u'),P(v_0,V')\}$，其中 $i=1,2,\cdots,m$，$u=1,2,\cdots,l-m$。而协议执行中，$VIEW_1(v_0,V)=\{v_0,E(U_i),r_u,E(r_u),P(v_0,V)\}$。由于 Bob 没有私钥，根据 ElGamal 加密算法的语义安全性，对 Bob 来说，$E(U_i)\overset{c}{\equiv}E(U_i')$ 以及 $E(r_u)\overset{c}{\equiv}E(r_u')$，其中 $i=1,2,\cdots,m$，$u=1,2,\cdots,l-m$。由于随机数计算上不可区分，则 $r_u\overset{c}{\equiv}r_u'$。又因为 $P(v_0,V)=P(v_0,V')$，因此 $\{S_1(v_0,P(v_0,V))\}=\{VIEW_1(v_0,V)\}$。

S_2 可用类似方法构造，此处省略。定理 1 得证。

3.3. 有理数域上点集成员关系的保密判定

以 n 维有理点为例设计点集成员关系的保密判定协议。

问题描述 Alice 拥有 n 维有理点 $X=(x_1,x_2,\cdots,x_n)$，Bob 拥有 n 维有理点集合 $Y=\{Y_1,Y_2,\cdots,Y_m\}$，其中 $Y_t=(y_1^t,y_2^t,\cdots,y_n^t)(t=1,2,\cdots,m)$。双方希望在不泄露 X、Y 中元素及 Y 的势的前提下合作计算函数 $P(X,Y)$：若 $X\in Y$，$P(X,Y)=1$；否则 $P(X,Y)=0$。

计算原理 Alice 和 Bob 依据式(2)将有理点 $X=(x_1,x_2,\cdots,x_n),Y_t=(y_1^t,y_2^t,\cdots,y_n^t)(t=1,2,\cdots,m)$ 的坐标作如下转换：

$$\begin{aligned} x_i&\to e_i^1\cdots e_i^j\cdots e_i^{s+q}\\ y_i^t&\to e_i^{t1}\cdots e_i^{tj}\cdots e_i^{t(s+q)}\end{aligned}\tag{10}$$

其中 $i=1,2,\cdots,n$， $1\le j\le s+q$。对于每一个 $i=1,2,\cdots,k$，Alice 依据下式：

$$ {}_{(i)}u_k^j=\begin{cases}1, & e_i^j=k-1\\ r_k^j, & e_i^j\ne k-1\end{cases} \tag{11}$$

将 x_i 编码为矩阵 ${}_{(i)}U$，并发送给 Bob。对于每一个有理点 $Y_t\left(t=1,2,\cdots,m\right)$ 的坐标 $y_i^t\left(i=1,2,\cdots,n\right)$，Bob 依据式(10)中的 e_i^{tj}，从 ${}_{(i)}u^1$ 至 ${}_{(i)}u^{s+q}$ 中依次取出对应位置编码 ${}_{(i)}u^1_{e_i^{t1}+1}$, ${}_{(i)}u^2_{e_i^{t2}+1}$,$\cdots$, ${}_{(i)}u^{s+q}_{e_i^{t(s+q)}+1}$，并计算：$U_i^t={}_{(i)}u^1_{e_i^{t1}+1}\cdot{}_{(i)}u^2_{e_i^{t2}+1}\cdots\cdots{}_{(i)}u^{s+q}_{e_i^{t(s+q)}+1}$。容易得到以下命题是正确的。

命题 2 $P\left(X,Y\right)=1$ 当且仅当对于每个 $t=1,2,\cdots,m$ 存在 $\prod_{i=1}^n U_i^t=1$。

协议 2 有理数域上点集成员关系保密判定协议

输入：Alice 输入有理点 $X=\left(x_1,x_2,\cdots,x_n\right)$，Bob 输入有理数集合 $Y=\left\{Y_1,Y_2,\cdots,Y_m\right\}$，其中 $Y_t=\left(y_1^t,y_2^t,\cdots,y_n^t\right)\left(t=1,2,\cdots,m\right)$。

输出：$P\left(X,Y\right)$。

准备：Alice 和 Bob 据式(2)对有理点 $X=\left(x_1,x_2,\cdots,x_n\right),Y_t=\left(y_1^t,y_2^t,\cdots,y_n^t\right)\left(t=1,2,\cdots,m\right)$ 的坐标转换得到式(10)。

1. Alice 执行以下操作：

1) 产生 ElGamal 加密算法的密钥对 $\left(sk,pk\right)$；

2) 根据(11)式将 $x_i\left(i=1,2,\cdots,n\right)$ 按位编码为矩阵 ${}_{(i)}U$；

3) 利用公钥 pk 加密矩阵 ${}_{(i)}U\left(i=1,2,\cdots,n\right)$ 中 ${}_{(i)}u_k^j=1$ 的分量，得加密矩阵：

$$ E\left({}_{(i)}U\right)=\begin{bmatrix}E\left({}_{(i)}u_1^1\right) & E\left({}_{(i)}u_1^1\right) & \cdots & E\left({}_{(i)}u_{10}^1\right)\\ E\left({}_{(i)}u_1^2\right) & E\left({}_{(i)}u_1^2\right) & \cdots & E\left({}_{(i)}u_{10}^2\right)\\ \vdots & \vdots & & \vdots\\ E\left({}_{(i)}u_1^{s+q}\right) & E\left({}_{(i)}u_1^{s+q}\right) & \cdots & E\left({}_{(i)}u_{10}^{s+q}\right)\end{bmatrix}=\begin{bmatrix}{}_{(i)}\left(c_{11}^1,c_{12}^1\right) & {}_{(i)}\left(c_{21}^1,c_{22}^1\right) & \cdots & {}_{(i)}\left(c_{(10)1}^1,c_{(10)2}^1\right)\\ {}_{(i)}\left(c_{11}^2,c_{12}^2\right) & {}_{(i)}\left(c_{21}^2,c_{22}^2\right) & \cdots & {}_{(i)}\left(c_{(10)1}^2,c_{(10)2}^2\right)\\ \vdots & \vdots & & \vdots\\ {}_{(i)}\left(c_{11}^{s+q},c_{12}^{s+q}\right) & {}_{(i)}\left(c_{21}^{s+q},c_{22}^{s+q}\right) & \cdots & {}_{(i)}\left(c_{(10)1}^{s+q},c_{(10)2}^{s+q}\right)\end{bmatrix} \tag{12}$$

其中 ${}_{(i)}\left(c^j_{\left(e_i^j+1\right)1},c^j_{\left(e_i^j+1\right)2}\right)=E\left(1\right)$，${}_{(i)}\left(c^j_{\left(\ne e_i^j+1\right)1},c^j_{\left(\ne e_i^j+1\right)2}\right)\in Z_p^*\times Z_p^*$ 为随机数对。Alice 将矩阵 ${}_{(i)}E\left(U\right)$ 及公钥 pk 发送给 Bob。

2. 对于每一个 $t=1,2,\cdots,m$ 和 $i=1,2,\cdots,n$，Bob 执行以下操作：

1) 根据 y_i^t 从 $E\left(U\right)$ 中按位取出密文 $E\left({}_{(i)}u^1_{e_i^{t1}+1}\right),E\left({}_{(i)}u^2_{e_i^{t2}+1}\right),\cdots,E\left({}_{(i)}u^{s+q}_{e_i^{t(s+q)}+1}\right)$，计算：

$$ U_i^t=E\left({}_{(i)}u^1_{e_i^{t1}+1}\right)E\left({}_{(i)}u^2_{e_i^{t2}+1}\right)\cdots E\left({}_{(i)}u^{s+q}_{e_i^{t(s+q)}+1}\right) \tag{13}$$

进一步计算 $U_t=\prod_{i=1}^n U_i^t$。

2) 选取正整数 l，满足 $l>m$。从 Z_p^* 中选取 $l-m$ 个大于 1 的随机数 $r_1,r_2,\cdots,r_{l-m}$，并计算其密文 $E\left(r_1\right),E\left(r_2\right),\cdots,E\left(r_{l-m}\right)$；

3) 对密文 $E\left(U_i\right),E\left(r_1\right),E\left(r_2\right),\cdots,E\left(r_{l-m}\right)\left(i=1,2,\cdots,m\right)$ 的顺序进行随机置换，并按置换后的顺序发送给 Alice。

3. Alice 解密收到的密文，记解密结果为 $d_k\left(1\le k\le l\right)$。若存在 $d_k=1$，Alice 输出 $P\left(X,Y\right)=1$；否则，

输出 $P(X,Y)=0$。

正确性分析 命题 2 的正确性以及本文采用的 ElGamal 加密系统的同态性保证了协议 2 的正确性。

安全性分析 X、Y 中元素及 Y 的势的隐私性可类似于协议 1 中 v_o、V 中元素及 V 的势的隐私性进行分析。

定理 2 协议 2 在半诚实模型下是安全的。

定理 2 的证明类似于定理 1 的证明，故省略。

4. 协议分析与比较

本文中设计的协议用到了 ElGamal 同态加密算法，计算复杂性分析只考虑费时的模指数运算。用通信次数衡量协议的通信复杂性，一方发送给另一方算一次。

计算复杂性分析 每进行一次 ElGamal 加密(解密)操作需要 2 次(1 次)模指数运算。协议 1 中 Alice 需加密 $s+q$ 次，解密 l 次；Bob 需加密 $l-m$ 次。因此，协议 1 共需 $3l+2(s+q)-2m$ 次模指数运算。类似地进行分析可知协议 2 共需 $3l+2n(s+q)-2m$ 次模指数运算。

通信复杂性分析 协议 1 和协议 2 的通信次数均为 2 次。

将本文设计的协议与文献[19]中的协议进行比较，结果如表 1 所示。

Table 1. The comparison of protocols
表 1. 协议的比较

文献	计算功能	计算复杂性	通信复杂性	适用范围
协议 1	数集成员关系	$3l+2(s+q)-2m$	2	有理数
协议 2	点集成员关系	$3l+2n(s+q)-2m$	2	$n(n\geq 2)$ 维有理点
文献[19]	数集成员关系	$3l+8$	4	有理数
	点集成员关系	$3l+8$	4	2 维有理点

注解：其中 l 均是参与方为隐藏集合的势选取的正整数。

相比文献[19]，当参与计算的有理数按(2)式统一转换后，当 $s+q<m$ 时，协议 1 计算复杂性低；当 $n=2$ 且 $s+q<m/2$ 时，协议 2 计算复杂性低。本文协议的通信效率高于文献[19]中的协议。此外，协议 2 可用于 $n(n\geq 2)$ 维有理点。

5. 结束语

针对有理数域上集合成员关系的保密判定问题，本文借助文献[20]中按位编码的方法，提出了有理数集成员关系和有理点集成员关系的保密判定协议，且点集成员关系的保密判定协议适用于 $n(n\geq 2)$ 维有理点。比较分析表明本文设计的协议通信效率高于相关协议，当参与计算的有理数满足一定条件时，本文协议的计算复杂度更低。因此，未来将进一步研究高效的集合成员关系的保密判定协议。

参考文献

[1] Yao, A.C. (1982) Protocols for Secure Computations. *The 23rd Annual IEEE Symposium on Foundations of Computer Science*, Chicago, 3-5 November 1982, 160-164. https://doi.org/10.1109/SFCS.1982.38

[2] Benor, M., Goldwasser, S., Widerson, A., *et al.* (1988) Completeness Theorems for Non-Crypto-Graphic Fault-Tolerant Distributed Computation. *The Twentieth Annual ACM Symposium on Theory of Computing*, Chicago, 2-4 May 1988, 1-10. https://doi.org/10.1145/62212.62213

[3] Dan, B., Giovanni, D.C., Rafail, O., *et al.* (2004) Public Key Encryption with Keyword Search. *International Conference on the Theory and Applications of Cryptographic Techniques*, Interlaken, 2-6 May 2004, 506-522.

[4] Sandhu, R.S., Coyne, E.J., Feinstein, H.L., *et al*. (1996) Role-Based Access Control Models. *Computer*, **29**, 38-47. https://doi.org/10.1109/2.485845

[5] Ruj, S., Stojmenovic, M., Nayak, A. (2014) Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds. *IEEE Transactions on Parallel and Distributed Systems*, **25**, 384-394. https://doi.org/10.1109/TPDS.2013.38

[6] 秦静, 张振峰, 冯登国, 李宝. 一个特殊的安全双方计算协议[J]. 通信学报, 2004(11): 35-42.

[7] 秦静, 张振峰, 冯登国, 李宝. 无信息泄漏的比较协议[J]. 软件学报, 2004(3): 421-427.

[8] Pinka, B., Schneider, T., Weinert, C. and Wieder, U. (2018) Efficient Circuit-Based PSI via Cuckoo Hashing. In: Nielsen, J.B. and Rijmen, V., Eds., *Advances in Cryptology—EUROCRYPT* 2018, LNCS, Vol. 10822, Springer, Berlin, 125-157. https://doi.org/10.1007/978-3-319-78372-7_5

[9] 窦家维, 刘旭红, 周素芳, 等. 高效的集合安全多方计算协议及应用[J]. 计算机学报, 2018, 41(8): 1844-1860.

[10] 周素芳, 李顺东, 郭奕旻, 窦家维, 陈振华. 保密集合相交问题的高效计算[J]. 计算机学报, 2018, 41(2): 464-480.

[11] 陈振华, 李顺东, 黄琼, 丁勇, 刘娅茹. 非加密方法安全计算两种集合关系[J]. 软件学报, 2018, 29(2): 473-482.

[12] 唐春明, 林旭慧. 隐私保护集合交集计算协议[J]. 信息网络安全, 2020, 20(1): 9-15.

[13] 李荣花, 武传坤, 张玉清. 判断集合包含关系的安全计算协议[J]. 计算机学报, 2009, 32(7): 1337-1345.

[14] Dou, J.W., Gong, L.M., Li, S.D., *et al*. (2016) Efficient Private Subset Computation. *Security and Communication Networks*, **9**, 5965-5976. https://doi.org/10.1002/sec.1749

[15] Zhou, S.F., Li, S.D., Dou, J.W., *et al*. (2017) Efficient Secure Multiparty Subset Computation. *Security and Communication Networks*, **2017**, Article ID: 9717580. https://doi.org/10.1155/2017/9717580

[16] 程楠, 赵运磊. 一种高效的关于两方集合并/交集基数的隐私计算方法[J]. 密码学报, 2021, 8(2): 352-364.

[17] Li, S.D., Wang, D.S. and Dai, Y.Q. (2009) Symmetric Cryptographic Protocols for Extended Millionaires' Problem. *Science China Information Sciences*, **52**, 974-982. https://doi.org/10.1007/s11432-009-0109-6

[18] 张茜, 苏烨, 秦静. 集合成员关系判定的安全多方计算协议[J]. 山东大学学报(理学版), 2020, 55(4): 118-126.

[19] 窦家维, 刘旭红, 王文丽. 有理数域上两方集合的高效保密计算[J]. 计算机学报, 2020, 43(8): 1397-1413.

[20] 李顺东, 杜润萌, 杨颜璟, 魏琼. 有理数相等的保密判定[J]. 电子学报, 2020, 48(10): 1933-1937.

[21] Goldreich, O. (2004) Foundation of Cryptography: Volume 2, Basic Applications. Cambridge University Press, London, 599-764. https://doi.org/10.1017/CBO9780511721656

[22] Rivest, R.L., Adleman, L.M. and Dertouzos, M.L. (1978) On Data Banks and Privacy Homeomorphisms. In: *Foundations of Secure Computation*, Academia Pres, Cambridge, 169-177.

[23] Gamal, T. (1984) A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, **31**, 469-472. https://doi.org/10.1109/TIT.1985.1057074