集合成员关系的安全多方计算及其应用

陈振华[1],李顺东[2],王道顺[3],黄 琼[4],张卫国[1]
(1. 西安科技大学计算机科学与技术学院,陕西西安 710054;2. 陕西师范大学计算机科学学院,陕西西安 710062;
3. 清华大学计算机科学与技术系,北京 100084;4. 华南农业大学数学与信息学院,广东广州 510642)

摘 要: 集合成员关系的安全多方计算在保密数据挖掘和保密数据查询等方面有着重要的应用价值.针对以往方案在集合规模较大时的低效问题,本文将原问题转化成多项式一次性求值问题,在此基础上共设计了四个协议.利用同态加密设计了平凡协议1;利用离散对数设计了高效协议2,此协议非常简洁.最后,针对不同的应用场景又分别设计了云计算环境下外包用户计算的协议3和抗抵赖环境下可公开保密判定的协议4.通过分析和比较显示,我们的方案除了集合的势,其余任何信息都没有泄露,并且在集合规模较大时,相比以往方案高效而简洁.

关键词: 集合成员;安全多方计算;同态加密;离散对数;云计算;抗抵赖
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2017)05-1109-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.05.013

Secure Multiparty Computation of Set Membership and Its Applications

CHEN Zhen-hua[1], LI Shun-dong[2], WANG Dao-shun[3], HUANG Qiong[4], ZHANG Wei-guo[1]
(1. *School of Computer Science and Technology, Xi'an University of Science and Technology, Xi'an, Shaanxi* 710054, *China*;
2. *School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*;
3. *Department of Computer Science and Technology, Tsinghua University, Beijing* 100084, *China*;
4. *College of Mathematics and Informatics, South China Agricultural University, Guangzhou, Guangdong* 510642, *China*)

Abstract: Secure multiparty computation of set membership is significant to privacy-preserving data mining, data query, etc. In this paper, we first transform the original problem into the one-time evaluation problem for polynomial, and then construct four protocols. We design the trivial protocol 1 using homomorphic encryption and construct the efficient protocol 2 using discrete logarithm instead of encryption, which is very concise. Lastly, according to the different application scenarios, we also propose protocol 3 and protocol 4: the former can be used to outsource computation in cloud computing environment; the latter can be used for public secure computation against repudiation. The analysis and comparison show that our protocols are more efficient and concise than previously known.

Key words: set membership; secure multi-party computation; homomorphic encryption; discrete logarithm; cloud computing; against repudiation

1 引言

安全多方计算最早由Yao[1]提出,是指在不泄漏各方的输入数据(隐私性)的条件下,能正确完成输入数据的函数计算(正确性).安全多方计算的特点使得人们能够最大限度的利用私有数据完成所需的计算任务而不破坏数据的隐私性.因此它在科学计算[2]、保密数据挖掘[3,4]、保密数据查询[5,6]、云计算[7]等方面有着广泛的应用.

Goldwasser[8]曾预言安全多方计算所处的地位就如同公钥密码学10年前所处的地位一样重要,它是计算科学一个极其重要的工具,而实际应用才刚起步.因此丰富其理论将使它成为计算科学和现实应用中一个必不可少的工具.接着,Goldreich等人[9,10]给出了安全多方计算问题的通用解决方案,从理论上证明了一般的多方保密计算问题是可解的,并引入了安全多方计算的安全性形式化定义与模拟范例.但同时他们指出,由于效率问题,利用通用的解决方案解决安全多方计算

收稿日期:2015-11-02;修回日期:2016-05-12;责任编辑:马兰英
基金项目:西安科技大学博士启动基金(No.2015QDJ008);信息安全国家重点实验室开放课题基金(No.2016-MS-19)

问题虽在理论上可行,而在实际中并不可行,应该具体问题研究具体的解决方案. Goldwasser 的预言和 Goldreich 等人的工作使得针对特定领域构造安全多方计算的高效解决方案,成为了现代密码学的研究热点之一.

本文也正是针对这一点,就具体问题进行了具体的研究.

Du 等人[11]在前人的基础上,进一步研究了一些具体的安全多方计算问题及其应用,包括科学计算、几何计算、统计分析等问题. 集合问题的保密计算也是安全多方计算中一个很重要的组成部分. 针对此,Freedman 等人[12]研究了集合相交、交集的势等问题. Kissner[13]等人研究了集合相交、包含等问题. 而集合成员关系的安全计算是集合问题中的一个分支,它要求保密地判断一方所拥有的元素是否在另一方的集合中. 比如以下的场景:

由于目前航空事件频发,为了乘客的安全,航空安检部门需要检查准备登机的乘客中是否有人出现在安全局所持有的"黑名单"里. 一方面航空公司的安检部门有责任对正常乘客的个人信息进行保密;但是,另一方面安全局的"黑名单"属于机密文件,不能轻易泄密. 因此这两个部门如何在不泄露各自隐私的前提下检查是否有乘客出现在"黑名单"中呢?

以上场景属于保密数据查询问题,转化成数学模型就是典型的集合成员关系的安全计算问题,但是目前这方面的研究文献并不多. 由于现实中很多问题都可以归结为此问题. 因此研究其理论意义对现实问题有着重要的应用价值.

1.1 相关工作

针对集合成员关系安全计算问题,以往的学者们提出了一些解决方案. 文献[14]利用可交换加密,将集合成员关系安全计算问题转化成元素比较匹配问题. 但是若集合很大的话,这个方案需要多次可交换加密和多次逐一查找和匹配,效率较低. 2010 年,马敏耀等人[15]先将集合中元素编码,再利用 Goldwasser-Micali 的异或同态加密算法解决了此问题. 由于此方法同样用到了公钥加密算法,并且只能进行自然数组成集合的成员判定问题,具有很大局限性. 2013 年,豆永丽等人[16]利用混沌加密算法也将原问题转化成多次比较匹配问题,因此存在和文献[14]方案中同样的问题.

由于以上的方案大多是把原问题转化成匹配查找问题,利用加解密算法,进行逐一比对. 当集合的规模较大时,方案并不高效.

1.2 本文贡献

(1) 将集合成员关系问题转化成一次性多项式求值问题,避免了前人方案中的多次匹配查找,从而提高了效率.

(2) 在将原问题转化成其他问题的基础上,设计了 4 个协议:

(i) 利用同态加密算法设计了平凡协议 1.

(ii) 利用离散对数而非加密的方法,设计了高效协议 2,此协议非常简洁.

(iii) 首次针对云外包计算场景,利用 2-DFN(Disjunctive Normal Form,DNF)的同态加密算法设计了应用型协议 3;首次针对抗抵赖环境,利用离散对数和双线性对设计了可公开保密计算的协议 4.

2 预备知识

2.1 问题的描述及集合的多项式表示

(1) 集合成员关系的安全多方计算

Alice 拥有元素 a,Bob 拥有集合 $X=(x_1,x_2,\cdots,x_n)$. Alice 和 Bob 都想知道元素 a 是否为集合 X 中的成员,除了集合 X 的势,而不泄露 a 与 X 中的任何信息.

(2) 集合的多项式表示

$X=(x_1,x_2,\cdots,x_n)$ 为一个集合,则此集合可表示为一个 n 次的多项式

$$f(x)=(x-x_1)(x-x_2)\cdots(x-x_n)$$

$$=a_0+a_1x+\cdots+a_nx^n=\sum_{i=0}^{n}a_ix^i$$

定理 1 若 $a\in X\Leftrightarrow f(a)=0$.

从这个定理可以看出,要判断一个元素是否属于一个集合,只要判断这个元素是否是这个集合转化的多项式的根即可.

2.2 安全多方计算的安全性定义

(1)半诚实参与者

安全多方计算的协议运行环境分为半诚实参与者模型和恶意攻击者模型[9,10],半诚实参与者指协议方将诚实地执行协议,不会篡改输入和输出信息,但可能会保留计算的中间结果,试图推导出协议之外的信息或者他人的信息.

(2)半诚实模型下的安全性定义

Goldreich[9,10]利用比特承诺和零知识证明理论设计了一个编译器,这个编译器可以将在半诚实参与者条件下保密计算函数 f 的协议 π 自动生成在恶意参与者条件下也能保密计算 f 的协议 π'. 新的协议 π' 可以迫使恶意参与者以半诚实方式参与协议的执行,否则就会被发现. 因此大多数情况下,我们只设计半诚实模型下的协议. 当我们设计出所需要的半诚实模型下的安全多方协议时,只要按照 Goldreich[9,10]的通用转化方法就可以将原协议转化为恶意模型下的新协议. 基于这一结论,本文也只给出半诚实模型下的协议和相应的安全性模拟范例.

设 $f(x,y)$ 为概率多项式函数,π 是计算 f 的协议,

设 Alice 拥有 x,Bob 拥有 y,他们要在不暴露 x,y 的前提下,合作计算函数 $f(x,y)=(f_1(x,y),f_2(x,y))$. 计算的目的是为了让 Alice 和 Bob 分别得到函数 f 的两个分量 $f_1(x,y),f_2(x,y)$. Alice 在执行协议 π 的过程中所得到的视图记为 $\text{view}_1(x,y)$,输出记作 $\text{output}_1(x,y)$;同理,Bob 的视图记为 $\text{view}_2(x,y)$,输出记作 $\text{output}_2(x,y)$. Goldreich 在文献[10]中给出计算不可区分性的半诚实参与者的安全两方计算的定义,表述如下:

定义 1　我们说协议 π 保密地计算了 $f(x,y)$,如果存在概率多项式时间模拟器 S_1 与 S_2 使得以下两式同时成立:

$$\{(S_1(x,f_1(x,y)),f_2(x,y))\} \tag{1}$$
$$\underline{c}\{(\text{view}_1(x,y),\text{output}_2(x,y))\}$$
$$\{(S_2(y,f_2(x,y)),f_1(x,y))\} \tag{2}$$
$$\underline{c}\{(\text{view}_2(x,y),\text{output}_1(x,y))\}$$

其中 $\underline{c}$ 表示计算不可区分.

此定义说明了任何一方参与者视图中的信息只能从自己输入和所获得的输出中得到,即说明任何一方参与者视图中不包含额外的信息,这样就保证了在协议执行过程中,任何一方得不到其他方的私有信息. 因此要证明一个两方计算协议是保密的,就必须构造使得式(1)和式(2)成立的模拟器 S_1 与 S_2.

2.3　Paillier 的同态加密算法[17]

设 E 是一个加密算法,$C_1=E(m_1,r_1)$ 是对 m_1 的加密,$C_2=E(m_2,r_2)$ 是对 m_2 的加密,若有 $C_1C_2=E(m_1+m_2,r)$,其中 r_1,r_2,r 是随机数. 则称 E 是一个加法同态加密算法.

Paillier 在文献[17]中提出了一种加密方案如下:

系统建立　系统选取 $N=pq$,其中 p,q 为两个素数,$\lambda=lcm(p-1,q-1)$,$g\in B$,其中 $B=\bigcup_{\alpha=1}^{\lambda}B_\alpha$,$B_\alpha\subset Z_{N^2}^*$,每个集合 B_α 中元素的阶分别为 $N\alpha$. 系统公钥(N,g),私钥 λ.

加密过程　明文 $m<N$,任取随机数 $r\in Z_N$,密文 $c=g^m r^N \bmod N^2$.

解密过程　密文 $c<N^2$,$L(u)=\dfrac{u-1}{N}$,$u<N^2$,明文

$$m=\frac{L(c^\lambda \bmod N^2)}{L(g^\lambda \bmod N^2)} \bmod N.$$

在以上方案中,令 $r_1r_2=r$,则有:

$$\begin{aligned}c_1c_2&=(g^{m_1}r_1^N \bmod N^2)(g^{m_2}r_2^N \bmod N^2)\\&=g^{m_1+m_2}(r_1r_2)^N \bmod N^2\\&=g^{m_1+m_2}r^N \bmod N^2\end{aligned}$$

即有:

$$E(m_1)E(m_2)=E(m_1+m_2)$$

因此,Paillier 加密方案具有同态加法性质.

2.4　Boneh 的 2-DNF 同态加密算法[18]

设 E 是一个加密算法,$C_1=E(m_1,r_1)$ 是对 m_1 的加密,$C_2=E(m_2,r_2)$ 是对 m_2 的加密,若有 $C_1C_2=E(m_1m_2,r)$,其中 r_1,r_2,r 是随机数. 则称 E 是一个乘法同态加密算法.

Boneh 在文献[18]中提出了一种加密方案如下:

系统建立　解密者选取 $N=pq$,其中 p,q 为两个素数,双线对 $e:G_1\to G$,G_1 和 G 同为阶数为 N 的群,g,h 为 G_1 的两个随机生成元,且 $h=g^p$. 私钥为 q,公钥为(G_1,G,e,g,h,N).

加密过程　明文 $m\in\{0,1\}$,任取随机数 $r\in Z_N$,密文为 $c=g^m h^r$.

解密过程　密文 $c<N$,明文 $m'=c^q$,若 $m'=1$,说明加密的明文 $m=0$;若 $m'\neq 1$,说明加密的明文 $m=1$.

在以上方案中,令 $m_2r_1+m_1r_2+r_1r_2=r'$,$r_1r_2=r$,$e(g,g)=g_1$,$e(g,h)=h_1$,则有:

(1)
$$\begin{aligned}c_1c_2&=g^{m_1}h^{r_1}\cdot g^{m_2}h^{r_2}\\&=g^{m_1+m_2}h^{r_1+r_2}\\&=g^{m_1+m_2}h^{r}\end{aligned}$$

(2)
$$\begin{aligned}e(c_1,c_2)&=e(g^{m_1}h^{r_1},g^{m_2}h^{r_2})\\&=e(g,g)^{m_1m_2}e(g,h)^{m_2r_1+m_1r_2+r_1r_2}\\&=g_1^{m_1m_2}h_1^{r'}\end{aligned}$$

即:

(3)　$E(m_1)E(m_2)=E(m_1+m_2)$

(4)　$e(E(m_1),E(m_2))=E(m_1m_2)$

备注 1　对于式(2)中的乘法同态,由于 $g_1^{m_1m_2}h_1^{r'} \bmod N\in G$,但 $\notin G_1$,不能再进行双线性对运算,即只能进行一次同态乘法运算. 因此,Boneh 加密方案具有多次同态加法和一次同态乘法性质.

3　两个具体的方案

基于不同技巧,本节给出安全计算集合成员关系的两个具体协议. 两种协议都假设所有的参与者都是在半诚实模型下,网络之间传输都是公开信道.

3.1　平凡协议

基于加法同态加密,我们设计了安全计算集合成员关系的平凡协议 1.

协议 1　安全计算集合成员关系

输入　Alice 保密输入 a,Bob 保密输入 $X=(x_1,x_2,\cdots,x_n)$.

输出　Alice 和 Bob 都知道 $a\in X$ 或者 $a\notin X$.

(1) Alice 选择 Paillier 加密方案,公布公钥(n,g),保密私钥 λ. 利用 Paillier 加密算法得到:$b_0=E(1)$,$b_1=E(a)$,$\cdots$,$b_n=E(a^n)$,发送给 Bob.

(2) Bob 将集合 X 表示为 n 次多项式 $f(x)$,$f(x)$ 的

系数分别为 $a_0,a_1,\cdots,a_n$. 选取随机数 $r(r\neq0,1)$,利用 Paillier 加密算法的同态性质,得到:

$$c_0=b_0^{ra_0},c_1=b_1^{ra_1},\cdots,c_n=b_n^{ra_n}$$

并计算密文 c 发送给 Alice.

$$\begin{aligned}c&=c_0c_1\cdots c_n\\&=E(ra_0+ra_1a+\cdots+ra_na^n)\\&=E(rf(a))\end{aligned}$$

(3) Alice 收到密文 c 后解密,若 $rf(a)=0$,则 $f(a)=0$,即 $a\in X$;若为一个随机数,则 $a\notin X$.

(4) Alice 将结果告诉 Bob.

分析 在协议 1 中,利用加密算法保护了 Alice 持有的元素 a 的隐私性. 利用加密算法的同态性保护了 Bob 持有的多项式 $f(x)$ 的系数 $a_0,a_1,\cdots,a_n$ 的隐私性,从而保护了集合 X 的隐私性. 而 Alice 若想从解密的结果 $rf(a)$ 中推出 $f(x)$ 的系数 $a_0,a_1,\cdots,a_n$,也不可能. 由于在表达式 $ra_0+ra_1a+\cdots+ra_na^n$ 中,即使 Bob 的集合中只包含一个元素,但这个表达式由于随机数 r 的存在,也有两个未知数,是个不定表达式,因此无法获得集合 X 的隐私.

3.2 高效协议

由于协议 1 使用了公钥加密方法,计算复杂性较高. 为了提高计算效率,我们利用离散对数,设计了更简洁的协议 2.

协议 2 安全计算集合成员关系

输入 Alice 保密输入 a,Bob 保密输入 $X=(x_1,x_2,\cdots,x_n)$.

输出 Alice 和 Bob 都知道 $a\in X$ 或者 $a\notin X$.

(1) Alice 选取较大随机数 $r(r\neq0,1)$,计算持有的元素 a 的承诺 $g^r,g^{ra},\cdots,g^{ra^n}$,发送给 Bob.

(2) Bob 将集合表示为 n 次多项式 $f(x)$,$f(x)$ 的系数分别为 $a_0,a_1,\cdots,a_n$. 计算 $(g^r)^{a_0},(g^{ra})^{a_1},\cdots,(g^{ra^n})^{a_n}$,并计算乘积:

$$\begin{aligned}&(g^r)^{a_0}(g^{ra})^{a_1}\cdots(g^{ra^n})^{a_n}\\&=g^{ra_0+ra_1a+\cdots+ra_na^n}\\&=g^{rf(a)}\end{aligned}$$

若计算的结果 $g^{rf(a)}=1$,则 $rf(a)=0$,即 $f(a)=0$,因此 $a\in X$;否则 $a\notin X$.

(3) Bob 将结果告诉 Alice.

分析 在协议 2 中,根据 Mitsunari 等人在文献[19]中给出的 q-DHI(q-Diffie-Hellman inversion)数学困难问题假设:对于给定的 $g,g^a,g^{a^2}\cdots,g^{a^n}$,求 $g^{1/a}$ 是困难的. 因此,从公开的信息 $g^r,g^{ra},g^{ra^2},\cdots,g^{ra^q}$ 中不能得到关于 a 的任何信息,否则 q-DHI 问题将被攻破. 而这里加入的随机数 r 又进一步阻止了 Bob 获得 Alice 持有的元素 a 的可能性. 如果没有随机数 r,且 $g^{f(a)}$ 的次数较低,使得离散对数可解,那么 Bob 就可能得到 $f(a)$,进一步通过反解多项式得到 a. 而这里的较大随机数 $r(r\neq0,1)$,使得破解离散对数困难,因此 Bob 无法获得 $rf(a)$,即无法获得 a 的隐私.

4 不同应用场景下的方案

4.1 云外包计算中安全计算集合成员关系

在协议 1 中,Alice 需要模幂运算和模乘运算,尤其当 a 很大时,进行这些运算会造成 Alice 的计算成本很大. 云计算是一个很好的利用工具,可将用户的计算任务外包给云,从而减少用户的计算成本. 但代之而来的问题是:云服务器是不可信的,可能会将数据自己保留或者泄漏给恶意的敌手. 因此在云计算里,数据隐私性是首要保证的问题. 为了利用云计算能力的同时保护好数据的隐私性,需要将 Bob 和 Alice 的数据加密后外包给云. 而多项式的计算中既有乘法运算又有加法运算,而 Paillier 的加密算法只具有加法同态,不能进行乘法同态操作,因此协议 1 在这个场景下已经失效. 这就需要我们重新设计适合此场景的协议 3.

以下协议假设云服务器和两方都是在半诚实模型下,网络之间都是公开信道,允许云服务器和任何一方合谋.

协议 3 云外包计算中安全计算集合成员关系

输入 Alice 保密输入 a,Bob 保密输入 $X=(x_1,x_2,\cdots,x_n)$.

输出 Alice 和 Bob 都知道 $a\in X$ 或者 $a\notin X$.

(1) Alice 选择 Boneh 加密方案,公布公钥 $(e,G_1,G,n=pq,g,h)$,保密私钥 (p,q). 计算以下密文发给云服务器.

$$c_0=E(1),c_1=E(a),\cdots,c_n=E(a^n)$$

(2) Bob 将集合表示为 n 次多项式 $f(x)$,$f(x)$ 的系数分别为 $a_0,a_1,\cdots,a_n$. 选择随机数 $r(r\neq0)$,并利用 Alice 的公钥,用同样的 Boneh 加密方案计算 $b_0=E(a_0+r),b_1=E(a_1+r),\cdots b_n=E(a_n+r)$ 发给云服务器.

(3) 云服务器收到 Alice 和 Bob 发来的密文后,利用同样的 Boneh 加密方案计算 2-DNF 的多项式,得到下式:

$$\begin{aligned}c&=e(b_0,c_0)e(b_1,c_1)\cdots e(b_n,c_n)\\&=e(E(a_0+r),E(1))e(E(a_1+r),E(a))\\&\quad\cdots e(E(a_n+r),E(a^n))\\&=E((a_0+r)+(a_1+r)a+\cdots+(a_n+r)a^n)\\&=E(f(a)+r(1+a+\cdots+a^n))\end{aligned}$$

云服务器将 c 发送给 Bob.

(4) Bob 收到密文 c 后,要求 Alice 发送 $E(1+a+\cdots+a^n)$,并利用同样的 Boneh 加密方案计算

$$c'=E(r(1+a+\cdots+a^n))$$

$$=e(E(r),E(1+a+\cdots+a^n))$$

然后计算$\frac{c}{c'}=E(f(a))$,并将此结果返回给 Alice.

(5) Alice 解密,若解密结果为 1,根据 Boneh 方案的结论,那么加密的明文$f(a)=0$,则$a\in X$;否则$a\notin X$.

(6) Alice 将结果告诉 Bob.

分析　在协议 3 中,利用加密算法保护了 Alice 持有的 a 的隐私性. 利用同样的加密算法保护了 Bob 持有的多项式$f(x)$系数 $a_0,a_1,\cdots,a_n$ 的隐私性. 但由于云服务器可以和任何一方合谋,而 Alice 具有解密密钥,云服务器收到 Bob 发来的密文 c 后可以和 Alice 合谋解密,这样 Bob 的隐私性就得到了破坏. 因此为了抵抗合谋,在 Bob 的明文中加入随机数 r,使得云服务器收到的密文即使交给 Alice 解密,也有 $n+2$ 个未知数,却只有 $n+1$ 个方程,仍然可以保护 Bob 的隐私. 即使选择攻击方法通过构造$(a_0+r)+(a_1+r)x+\cdots+(a_n+r)x^n=0$,想求出使得多项式$f(x)=a_0+a_1x+\cdots+a_nx^n=0$ 的所有解,从而获得 Bob 集合中元素,也不可能. 因为从$(a_0+r)+(a_1+r)x+\cdots+(a_n+r)x^n=0$ 只能得到$f(x)=-r(1+x+\cdots+x^n)$,仍为一个随机多项式,因此保护了 Bob 的隐私.

此外,在该协议中,由于大多数的计算任务交付给了云服务器,而两个用户只进行了加密运算和唯一的一个对运算和模乘运算,因此极大的节省了用户计算成本.

4.2　抗抵赖场景下安全计算集合成员关系

在协议 1,协议 2,协议 3 中,最后一步输出结果时,如果一方给另一方的结果为真,但对方却声称自己收到的不为真,这样会导致两方争执不下. 因此当出现抵赖时,为了仲裁,除了 X 的势,在不暴露 a 与 X 中任何元素的情况下,必须公开判断 a 到底是否属于集合 X,从而使得任何第三方都知道真正的结果. 在这个场景中,既要保护双方的隐私,又要能公开计算. 协议 1、协议 2、协议 3 虽然都可以保护双方的隐私,但是都不能公开计算,其中的一方仍然可以抵赖. 为了解决这个问题,我们需要重新设计适合此场景的协议 4.

以下协议假设两方和任何第三方验证者都是半诚实模型下,网络之间都是公开信道,允许第三方验证者和任何一方合谋.

协议 4　抗抵赖场景下安全计算集合成员关系

输入　Alice 保密输入 a,Bob 保密输入 $X=(x_1,x_2,\cdots,x_n)$.

输出　任何一人都知道 $a\in X$ 或者 $a\notin X$.

(1) Bob 将集合表示为 n 次多项式$f(x)$,$f(x)$ 的系数分别为 $a_0,a_1,\cdots,a_n$. 选取较大随机数 $r(r\neq0,1)$,并公布$f(x)$系数的承诺 $g^{ra_0},g^{ra_1},\cdots,g^{ra_n}$.

(2) Alice 计算 $g^a,g^{a^2},\cdots,g^{a^n}$,并公布这些结果.

(3) 任何第三方(包括 Alice,Bob)计算:

$$e(g^{ra_0},g)=e(g,g)^{ra_0}$$
$$e(g^{ra_1},g^a)=e(g,g)^{ra_1a}$$
$$\vdots$$
$$e(g^{ra_n},g^{a^n})=e(g,g)^{ra_na^n}$$

并计算乘积:

$$e(g,g)^{ra_0}e(g,g)^{ra_1a}\cdots e(g,g)^{ra_na^n}$$
$$=e(g,g)^{ra_0+ra_1a+\cdots+ra_na^n}$$
$$=e(g,g)^{rf(a)}$$

若计算的结果$e(g,g)^{rf(a)}=1$,则$rf(a)=0$,即$f(a)=0$,因此$a\in X$;否则$a\notin X$.

分析　在协议 4 中,类似于 Feldman 的 VSS(Verifiable Secret Sharing)方案的承诺方法[20],使用了离散对数来保护 Bob 所持有的多项式$f(x)$的系数 $a_0,a_1,\cdots,a_n$ 的隐私性,从而保护了集合 X 的隐私性. 但两者并不相同:Feldman 的 VSS 方案中的多项式系数是随机选取,而且破解离散对数困难;而我们这里的多项式系数是定值. 因此为了保护 Bob 的多项式$f(x)$系数的隐私性,要加入随机数 r. 并且为了无法破解离散对数,随机数 r 要在一个较大数域中选择. 这样选择的随机数 r 很好的保护了 Bob 的多项式系数 $a_0,a_1,\cdots,a_n$ 的隐私性,但却并不影响$f(a)$的结果. 而对于 Alice 所持有 a 的隐私性,根据 Mitsunari 等人在文献[19]给出的 q-DHI(q-Diffie-Hellman inversion)数学困难问题假设:对于给定的 $g,g^{a^2},\cdots,g^{a^q},$,求 $g^{1/a}$ 是困难的. 因而从公开的信息 $g,g^a,g^{a^2},\cdots,g^{a^n}$ 中不能得到关于 a 的任何信息,否则 q-DHI 问题将被攻破.

备注 2　协议 2,协议 4 中的承诺都是以离散对数形式给出. 也可以利用椭圆曲线加法群上的离散对数形式. 即把有限域乘法群上的离散对数形式平移到椭圆曲线加法群上的离散对数. 有关椭圆曲线上的协议这里不再累述.

备注 3　以上的协议 1,协议 2,协议 3,协议 4,唯一泄露的就是 Bob 集合的势,但这不是协议本身的缺陷,因为用多项式表示集合的时候,多项式的系数确定了集合的势. 即使泄露了集合的势,但这并不影响集合成员的保密判定. 关于这一点,Du 等人[21]在“A Practical approach to solve secure multi-party computati-on problems”一文中专门有论证在设计协议时,如果在降低完美安全性的程度上,允许泄露的信息并不影响方案的有效执行,那么这就是可接受性安全. 而可接受性安全要根据具体问题,具体设定. 因此,在 2.1 节原问题给出时,我们已经设定集合的势并不需要保密.

5　安全性分析

在本节我们应用 2.2 节的安全性模拟范例给出本

文4个协议的安全性证明,证明过程相似的,为了节省篇幅,我们只给出结论即可.

定理1 协议1保密的判定了集合成员关系.

证明 通过构造满足(1)和(2)的模拟器 S_1,S_2 来证明本定理. 在本协议中

$$f_1(a,X)=f_2(a,X)=a\in X$$

或者 $$f_1(a,X)=f_2(a,X)=a\notin X.$$

假设 $f_1(a,X)=f_2(a,X)=a\in X$ 来构造模拟器 S_2. S_2 接受 $(X,f_2(a,X))$ 作为输入,按如下方式工作:

第一步 S_2 接受输入 $(X,a\in X)$ 后,首先随机的选取一个元素 a',使得 $f_2(a,X)=f_2(a',X)$,然后用 (a',X) 来模拟. 按照协议,根据 a' 得到数据 $a',(a')^2,\cdots,(a')^n$,加密这些数据得到

$$b'_0=E(1),b'_1=E(a'),$$

$$b'_2=E((a')^2),\cdots,b'_n=E((a')^n)$$

记做 $E(A')$.

第二步 S_2 将集合 X 表示为多项式 $f(x)$,得到 $f(x)$ 的系数 $a_0,a_1,\cdots,a_n$. 并选取较大随机数 $r'(r'\neq 0,1)$,计算 $c'_0=(b'_0)^{r'a_0},c'_1=(b'_1)^{r'a_1},\cdots,c'_n=(b'_n)^{r'a_n}$,记做 $E(B')$. 并计算乘积 $c'=c'_0c'_1\cdots c'_n$,记做 $E(C')$.

第三步 解密得到 C'.

第四步 得到结果 $a'\in X$.

在本协议中:

$$\text{view}_2(a,X)=\{X,r,E(A),E(B),E(C),a\in X\}$$

$$S_2(X,a\in X)=\{X,r',E(A'),E(B'),E(C'),a'\in X\}$$

r,r' 都是随机变量,而 $E(A),E(B),E(C)$ 和 $E(A'),E(B'),E(C')$ 都是概率性加密的结果,因此为随机变量,因而这些量在计算上不可区分. 由于 $f_2(a,X)=(a\in X),(a'\in X)=f_2(a',X)$,而 $f_2(a,X)=f_2(a,X')$,因此,$(a\in X)\underline{c}(a'\in X)$. 又因为 $\text{output}_1(a,X)=f_1(a,X)=(a\in X)$. 所以

$$\{(S_2(y,f_2(x,y)),f_1(x,y))\}$$

$$\underline{c}\{(\text{view}_2(x,y),\text{output}_1(x,y))\}$$

同理,用类似的方法可构造模拟器 S_1 使得:

$$\{(S_1(x,f_1(x,y)),f_2(x,y))\}$$

$$\underline{c}\{(\text{view}_1(x,y),\text{output}_2(x,y))\}$$

定理2 协议2保密的判定了集合成员关系.

证明 通过构造满足(1)和(2)的模拟器 S_1,S_2 来证明本定理. 在本协议中

$$f_1(a,X)=f_2(a,X)=a\in X$$

或者 $$f_1(a,X)=f_2(a,X)=a\notin X$$

假设 $f_1(a,X)=f_2(a,X)=a\in X$ 来构造模拟器 S_2. S_2 接受 $(X,f_2(a,X))$ 作为输入,按如下方式工作:

第一步 S_2 接受输入 $(X,a\in X)$ 后,首先随机的选取一个元素 a',使得 $f_2(a,X)=f_2(a',X)$,然后用 (a',X) 来模拟. 按照协议,根据 a' 得到数据 $a',(a')^2,\cdots,(a')^n$,选取较大随机数 $r'(r'\neq 0,1)$,并计算 $b'_0=g^{r'}$,$b'_1=g^{r'a},b'_2=g^{r'(a')^2},,\cdots,b'_n=g^{r'(a')^n}$,记做 $E(A')$.

第二步 S_2 将集合 X 表示为多项式 $f(x)$,得到 $f(x)$ 的系数 $a_0,a_1,\cdots,a_n$. 计算 $c'_0=(b'_0)^{a_0},c'_1=(b'_1)^{a_1},\cdots,c'_n=(b'_n)^{a_n}$,记做 $E(B')$. 并计算乘积 $c'=c'_0c'_1\cdots c'_n$,记做 $E(C')$.

第三步 得到结果 $a'\in X$.

在本协议中

$$\text{View}_2(a,X)=\{X,E(A),E(B),E(C),a\in X\}$$

$$S_2(X,a\in X)=\{X,E(A'),E(B'),E(C'),a'\in X\}$$

$E(A),E(B),E(C)$ 和 $E(A'),E(B'),E(C')$ 都是通过随机数得来的结果,仍为随机变量,因而这些量在计算上不可区分. 又由于 $(a\in X)=f_2(a,X),(a'\in X)=f_2(a',X)$,而 $f_2(a,X)=f_2(a,X')$,因此,$(a\in X)\underline{c}(a'\in X)$. 又因为 $\text{output}_1(a,X)=f_1(a,X)=(a\in X)$. 所以

$$\{(S_2(y,f_2(x,y)),f_1(x,y))\}$$

$$\underline{c}\{(\text{view}_2(x,y),\text{output}_1(x,y))\}$$

同理,用类似的方法可构造模拟器 S_1 使得:

$$\{(S_1(x,f_1(x,y)),f_2(x,y))\}$$

$$\underline{c}\{(\text{view}_1(x,y),\text{output}_2(x,y))\}$$

定理3 在云外包计算中,协议3保密的判定了集合成员关系.

定理4 在抗抵赖环境下,协议4保密的判定了集合成员关系.

用类似的方法可以证明定理3和定理4,这里不再一一赘述.

6 效率分析与比较

本节给出我们的四个协议和引言中的相关文献[14~16]在计算复杂性、查找匹配次数、通信复杂性以及性能方面的分析和比较.

计算复杂度 为了便于比较,统一各个协议中集合的势为 n. 由于这些方案使用的都是公钥加密算法,而公钥加密算法的计算复杂性较高,因此以加密算法的加解密次数作为衡量计算复杂性的指标. 文献[14]中两方各需要 $n+1$ 次加密,文献[15]需要 $n+1$ 次加密和1次解密,文献[16]需要 $n+1$ 次加密. 而我们的四个协议,其中协议1需要 $n+1$ 次加密和1次解密;协议3需要 $2(n+1)+2$ 次加密和1次解密;而协议2和协议4并没有使用加解密算法.

通信复杂度 衡量通信复杂度的指标用协议交换信息的比特数,或者用通信轮数,在多方保密计算研究中通常用轮数.

性能 在本文中以各个协议是否适合云计算环境

和抗抵赖环境作为衡量性能的指标. 这样得到各个协议的具体比较如表 1.

表 1　本文协议与现有方案的比较

方案	计算复杂性	查找匹配次数	通信复杂性	云计算环境	抗抵赖环境
文献[14]	$2n+2$	1 到 n 次	3	No	No
文献[15]	$n+2$	0	3	No	No
文献[16]	$n+1$	1 到 n 次	2	No	No
协议 1	$n+2$	0	3	No	No
协议 2	0	0	2	No	No
协议 3	$2n+5$	0	4	Yes	No
协议 4	0	0	2	Yes	Yes

从表 1 可以看出,匹配查找的方法在集合很大时,最坏情况下需要查找 n 次,比较低效. 而我们的四个协议并没有使用查找匹配的方法. 在具有相同性能的协议中,我们的协议要不就没有使用加解密的方法. 即使使用,加解密次数也较少,通信复杂度也较低. 因此我们的方案效率较高. 此外,我们提供的协议 3,协议 4,在并没有提高较多计算复杂性和通信复杂性的同时,是针对不同的应用场景非常实用的协议.

7　总结和开放问题

集合成员关系安全计算问题是安全多方计算中很重要的组成部分,现实中很多问题都能归结于此. 而已存在的方案大多利用了多次匹配查找和公钥加解密算法,这在集合规模很大时,要进行逐一比对,效率比较低下. 本文首先将原问题转化成多项式一次性求值问题,然后基于密码学中不同的知识解决了此问题. 我们设计的四个协议,都没有使用匹配查找的方法,有的甚至也没有使用加解密公钥算法,有的即使使用公钥加密算法,加解密次数也很少,因此本文效率较高. 此外,我们提供的其中两个协议,赋予了集合成员保密判定新的意义和新的应用场景.

在本文所有协议中,利用的一个潜在数学工具就是多项式的零根,充分利用该性质并进一步推广,并结合不同的密码学知识,可以解决很多新的安全多方计算问题和与此相关的问题. 例如,利用多个零根或者零根和原值的关系,可以解决集合包含、集合相交等问题,将这些推广又可以设计出带有集合属性关系的加密方案. 这些工作,我们都已经在陆续研究和整理中.

参考文献

[1] Yao A C. Protocols for secure computations[A]. Proceedings of 23rd IEEE Symposium on Foundations of Computer Science[C]. Chicago, USA, 1982. 160 – 164.

[2] Du W L, Atallah M J. Privacy-preserving cooperative scientific computations[A]. Proceedings of 14th IEEE Computer Security Foundations Workshop Lecture[C]. Cape Breton, Canada, 2001. 273 – 282.

[3] Agrawal R, Srikant R. Privacy-preserving data mining[A]. Proceedings of ACM International Conference on Management of Data and Symposium on Principles of Database Systems[C]. Dallas, USA, 2000. 439 – 450.

[4] 杨高明,杨静,张健沛. 聚类的(A,k)-匿名数据发布[J]. 电子学报,2011,39(8):1941 – 1946.
Yang G M, Yang J, Zhang J P. Achieving (A,k)-anonymity via clustering in data publishing[J]. Acta Electronica Sinica, 2011, 39(8): 1941 – 1946. (in Chinese)

[5] Goldberg I. Improving the robustness of private information retrieval[A]. Proceedings of IEEE Symposium on Security and Privacy[C]. Berkeley, CA, 2007. 131 – 148.

[6] Samanthula, B K, Elmehdwi, Y, Howser, Gerry, et al. A secure data sharing and query processing framework via federation of cloud computing[J]. Information Systems, 2015, 48: 196 – 212.

[7] Loftus J, Smart N P. Secure outsourced computation[A]. Progress in Cryptology-AfricaCrypt 2011[C]. Dakar, Senegal, 2011. LNCS 6737: 1 – 20.

[8] Goldwasser. Multi-party computations: Past and present[A]. Proceedings of the 16th Annual ACM Symposium on Principles of Distributed Computing[C]. Santa Barbara, USA, 1997. 1 – 6.

[9] Goldreich O, Micali S, Wigderson, A. How to play ANY mental game[A]. Proceedings of the 19th^Annual ACM Conference on Theory of Computing[C]. Pittsburgh, USA, 1987. 218 – 229.

[10] Goldreich O. Foundations of cryptography: Basic applications[M]. London: Cambridge University Press, 2004. 599 – 729.

[11] Du W L, Atallah M J. Secure multi-party computation problems and their applications: A review and open problems[A]. Proceedings of New Security Paradigms Workshop 2001[C]. Cloudcroft, USA, 2001. 11 – 20.

[12] Freedman M J, Nissim K, Pinkas B. Efficient private matching and set intersection[A]. Advances in Cryptology-EuroCrypt 2004[C]. Interlaken, Switzerland, 2004. LNCS 3027: 1 – 19.

[13] Kissner L, Song D. Privacy-preserving set operations[A]. Advances in Cryptology-Crypt 2005[C]. Santa Barbara, USA, 2005. LNCS 3621: 241 – 257.

[14] 李顺东,王道顺. 现代密码学:理论. 方法与研究前沿[M]. 北京:科学出版社,2009. 193 – 232.

[15] 马敏耀. 安全多方计算及其扩展问题的研究[M]. 北京:北京邮电大学,2010.

[16] 豆永丽,等. 集合成员判定问题的安全多方计算解决方案[J]. 计算机应用,2013,33(12):3527 – 3530.
Dou yongli,et al. Secure multiparty computation solutions of collection member decision[J]. Journal of Computer Applications,2013,33(12):3527 – 3530. (in Chinese)
[17] Paillier P. Public-key cryptosystems based on composite degree residue classes[A]. Advances in Cryptology-EuroCrypt 1999, Prague, Czech[C]. Republic. 1999, LNCS 1592:223 – 238.
[18] Boneh, EJGD, Nissim K. Evaluating 2-DNF Formulas on Ciphertexts[A]. TCC 2005[C]. Cambridge, USA, 2005. LNCS 3378:325 – 341.
[19] Mitsunari S, Sakai R, Kasahara M. A new traitor tracing [J]. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 2002, E85 – A (2):181 – 484.
[20] Feldman,P A practical scheme for non-interactive verifiable secret sharing[A]. Proceedings of the IEEE 28th Annual Symposium on Foundations of Computer Science [C]. Los Angeles, USA, 1987. 427 – 438.
[21] Du W, Zhan Z. A practical approach to solve secure multi-party computation problems[A]. Proceedings of the ACM 2002 workshop on New security paradigms[C]. Virginia Beach, USA, 2002. 127 – 135.

作者简介

陈振华(通信作者) 女,1976 年生于陕西宝鸡,博士,研究方向为秘密共享和安全多方计算.
E-mail:czh333330@163.com

李顺东 男,1963 年生于河南,博士生导师,研究方向为安全多方计算.

王道顺 男,1967 年生于四川,硕士生导师,研究方向为分组密码的设计与分析.

黄 琼 男,1981 年生于江西,硕士生导师,研究方向为数字水印,防伪技术.

张卫国 男,1963 年生于陕西,硕士生导师,研究方向为信息安全.