最小值问题的安全多方计算及其应用

窦家维[1],马 丽[1],李顺东[2]
(1. 陕西师范大学数学与信息科学学院,陕西西安 710062;2. 陕西师范大学计算机科学学院,陕西西安 710062)

摘 要: 安全多方计算是国际密码学界近年来的研究热点.本文主要研究科学计算中最小值问题的安全多方计算,目前尚没有见到关于这个问题的解决方案.本文设计了一种新的编码方法,应用该编码方法和ElGamal乘法同态加密算法,并结合秘密分享以及门限密码体制,在半诚实模型下设计了三个能够抵抗合谋攻击的最小值安全多方计算方案,并应用模拟范例证明了方案的安全性.以最小值解决方案为基础还可以解决最大值安全计算以及并集的安全计算等科学计算问题.效率分析表明所设计的安全计算方案是高效的方案.

关键词: 密码学;安全多方计算;最小值;同态加密;秘密分享;门限密码体制
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112 (2017)07-1715-07
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.07.023

Secure Multi-Party Computation for Minimum and Its Applications

DOU Jia-wei[1], MA Li[1], LI Shun-dong[2]
(1. *School of Mathematics and Information Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*;
2. *School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*)

Abstract: Secure multi-party computation is a focus in the international cryptographic community. This paper studies how to privately compute the minimum of some private numbers. We have not read about any a solution to this problem. In this study, we introduce a new encoding scheme, and then, based on this new encoding scheme and ElGamal multiplicatively homomorphic encryption scheme, using secret sharing and threshold decryption, devise protocols for this problem. By using the simulation paradigm, we prove that these protocols are secure in the semi-honest model. These protocols can resist collision attack. Based on the computing methods for minimum problem, secure multi-party computation for maximum and union of sets can also be solved. Efficiency analysis shows that these schemes are efficient.

Key words: cryptography; secure multi-party computation; minimum; homomorphic encryption; secret sharing; threshold decryption

1 引言

网络的迅速发展为多个参与者利用各自的保密数据联合进行数据挖掘、知识发现、信息搜索以及寻求数据之间的各种统计规律、合作进行科学研究等提供了巨大的机会,同时也给参与者的信息安全带来了巨大的挑战.在互不信任的网络环境中,参与者需要保护各自所拥有数据的隐私性.在联合计算过程中稍有不慎就可能导致数据的机密性丧失,这使得安全多方计算越来越受到人们的关注.

安全多方计算是指两个或更多参与者利用各自的保密数据(作为计算的输入),联合进行保密计算.计算结束后,没有参与方能够获得多于规定输出的信息.Yao[1]和Goldreich等人[2,3]首先提出了安全多方计算问题并对其进行了深入的研究,从理论上证明了任意的安全多方计算问题都是可解的,并给出了通用的解决方案.

利用通用的解决方案解决具体的计算问题是不实际的,从效率方面考虑,对具体问题应该研究具体的解决方案.近年来,人们研究了各类安全多方计算问题,如保密的科学计算[1,4~9],保密的计算几何[10~12],保密的统计分析[13],保密的数据挖掘[14,15],安全多方计算应用[16~18]等.在保密的科学计算方面,人们研究了比较两个数的大小[1,8,9],保密的信息比较[4,5],保密计算集合

收稿日期:2015-08-28;修回日期:2016-09-20;责任编辑:孙瑶
基金项目:国家自然科学基金(No. 61272435)

的交集[6],保密计算多重集的并集[7],保密的多项式计算[19]等.保密计算多个数据的最小(大)值是保密的科学计算中一个非常重要的问题,就我们所知,目前还没有见到关于这个问题的解决方案.

安全多方计算一般采用加密电路、不经意传输、秘密分享、同态加密等技术作为基本模块设计针对具体问题的解决方案.文献[20]全面地总结了实现安全多方计算的各种技术.本文通过巧妙设计编码方法,并结合这些基本技术,将最大最小值保密计算以及集合并集问题归约到相应数组的保密乘积而得到高效的解决方案.本文的贡献如下:

(1)提出了一种新的编码方法,使每个参与者的保密数据隐藏在一个特殊数组中.这种编码方法可以为解决其他安全多方计算问题提供一种新的途径.

(2)利用所设计的新编码方法、ElGamal 同态加密算法、秘密分享和门限密码体制的方法设计了三个保密计算最小值问题的解决方案.这些方案对半诚实参与者是安全的,可以抵抗合谋攻击的程度不同,其中第三个方案可以抵抗任意数量的合谋攻击.

(3)以保密计算最小值方案为基础,可以进一步解决最大值和多个集合并集问题的保密计算,设计获得高效安全的解决方案.

2 预备知识

2.1 理想模型

假设有一个可信的第三者(Trusted Third Party,TTP),他在任何情况下都不会泄露不该泄露的信息.参与者 $P_1,\cdots,P_m$ 分别将各自的秘密消息 $x_1,\cdots,x_m$ 告诉 TTP,TTP 自己单独计算函数 f:

$$f(x_1,\cdots,x_m)=(f_1(x_1,\cdots,x_m),\cdots,f_m(x_1,\cdots,x_m)),$$

参与者 P_i 除了从协议得到 TTP 发送给自己的计算结果 $f_i(x_1,\cdots,x_m)$ 外得不到任何其他信息.上面借助于 TTP 保密计算函数 $f(x_1,\cdots,x_m)$ 的协议称为理想的安全多方计算协议(简称理想协议).理想协议是最简单、安全性最高的保密计算协议,任何计算 $f(x_1,\cdots,x_m)$ 的实际保密计算协议的安全性都不可能超过理想协议,实际保密计算协议可以通过和理想协议进行比较来了解其安全性.

2.2 半诚实模型

本文假设所有的参与者都是半诚实的参与者[3].所谓半诚实参与者是指那些在协议的执行过程中按照协议要求忠实地履行协议的参与者,但他们可能会记录下协议执行中收集到的信息,在协议执行后试图根据记录的信息推算出其他参与者的输入.

设参与者 $P_1,\cdots,P_m$,分别具有保密数据 $x_1,\cdots,x_m$,他们利用协议 Π 保密地计算 $f(x_1,\cdots,x_m)$.令 $X=(x_1,\cdots,x_m)$.在协议执行过程中,P_i 得到的信息序列记为

$$\text{view}_i^{\Pi}(X)=(x_i,r_i,M_i^1,\cdots,M_i^t),$$

其中 $M_i^j(j=1,\cdots,t)$ 表示 P_i 收到的第 j 个信息.对于部分参与者构成的子集 $I=\{P_{i_1},\cdots,P_{i_s}\}\subseteq\{P_1,\cdots,P_m\}$,记

$$\text{view}_I^{\Pi}(X)=(I,\text{view}_{i_1}^{\Pi}(X),\cdots,\text{view}_{i_s}^{\Pi}(X)).$$

定义 1(半诚实参与者协议的安全性[3]) 在参与者都是半诚实的情况下,如果存在概率多项式时间算法 S,使得对于任意的 $I=\{P_{i_1},\cdots,P_{i_s}\}\subseteq\{P_1,\cdots,P_m\}$,均有式(1)成立:

$$\{S(I,(x_{i_1},\cdots,x_{i_s}),f_I(X))\}_{X\in(\{0,1\}^*)^m}\overset{c}{\equiv}\{\text{view}_I^{\Pi}(X)\}_{X\in(\{0,1\}^*)^m} \tag{1}$$

其中,$\overset{c}{\equiv}$ 表示计算上不可区分,则称协议 Π 保密地计算了函数 f.

本文的解决方案是对于半诚实参与者安全的方案.

2.3 同态加密算法

同态性是某些公钥加密方案所具有的重要性质.ElGamal 加密算法是一种具有乘法同态性的加密算法.具体如下:

KeyGen.给定安全参数 k,产生一个位数为 k 的大素数 p 以及 Z_p^* 的一个生成元 g,随机选取私钥 $x\in Z_p^*$,计算其对应的公钥 $h=g^x \bmod p$.

Encrypt.为加密消息 $M(M\in Z_p^*)$,选择一个随机数 r,密文为:

$$E(M)=(c_1,c_2)=(g^r \bmod p, Mh^r \bmod p).$$

Decrypt.对于密文 $E(M)=(c_1,c_2)$,解密得到明文:

$$M=c_2\cdot c_1^{-x} \bmod p.$$

Evaluate.

$$\begin{aligned}&E(M_1)\times E(M_2)\bmod p\\&\equiv(g^{r_1},M_1h^{r_1})\times(g^{r_2},M_2h^{r_2})\bmod p\\&\equiv(g^{r_1+r_2},(M_1\times M_2)h^{r_1+r_2})\bmod p\\&\equiv E(M_1\times M_2)\bmod p.\end{aligned}$$

所以 ElGamal 加密算法是一种具有乘法同态性的加密算法.

3 基于 ElGamal 算法的最小值保密计算

3.1 协议的基本原理

参与者 $P_1,\cdots,P_m$ 分别拥有数据 $x_1,\cdots,x_m$,假设 $1\leqslant x_i\leqslant n(i=1,\cdots,m)$.他们要保密地计算 $y=\min\{x_1,\cdots,x_m\}$.

参与者 $P_i(i=1,\cdots,m)$ 首先按照下面的方法构造数组:

$$X_i=(x_{i1},\cdots,x_{in}) \tag{2}$$

其中,当 $j<x_i$ 时,$x_{ij}=1$;当 $j\geqslant x_i$ 时,$x_{ij}=r_{ij}$,而 $r_{ij}\in Z_p^*$

为不等于 1 的随机数. 这样,P_i 具有的秘密数据 x_i 与式(2)形式的数组 X_i 相对应. 对于 m 个数组 $X_1,\cdots,X_m$ 作乘积,即将这些数组的对应元素相乘,得到一个新的数组:

$$Y=(y_1,\cdots,y_n)=\left(\prod_{i=1}^{m}x_{i1},\cdots,\prod_{i=1}^{m}x_{in}\right). \tag{3}$$

由数组 X_i 的构造式以及 Y 的表达式,容易证明下面结论:

命题 1　对于每一个 $x_i(i=1,\cdots,m)$,按照式(2)构造数组 X_i,并按式(3)计算 Y,则可知:

$$\begin{aligned}\min\{x_1,\cdots,x_m\}&=\min\{j\mid y_j\neq 1\}\\&=\min\left\{j\mid\left(\prod_{i=1}^{m}x_{ij}\right)\neq 1\right\}.\end{aligned}$$

上面提出的编码方式和命题 1 是计算多个数据中最小值的基本原理. 若直接这样做显然没有秘密可言,需要利用同态加密算法对数组中的 1 加密,使得加密后的 1 和随机数计算上不可区分,从而可保密计算使 y_j 不等于 1 的 j. 本文中几个数组相乘均指这些数组的对应元素相乘,而对一个数组加密,是指对其每一个元素分别加密.

3.2　基本最小值保密计算方案

首先应用具有乘法同态性的 ElGamal 公钥加密算法给出一种基本最小值保密计算方案,具体如协议 1.

协议 1　基本的最小值保密计算

输入:$P_1,\cdots,P_m$ 各自的秘密数据 $x_1,\cdots,x_m$.

输出:$y=\min\{x_1,\cdots,x_m\}$.

(i)P_1 应用 ElGamal 公钥系统生成私钥 sk 和公钥 pk,并公布公钥 pk.

(ii)每个参与者 $P_i(i=1,\cdots,m)$ 以方式(2)将自己的数据转化为数组 X_i,并用公钥 pk 将数组 X_i 加密为:

$$(c_{i1},\cdots,c_{in})=(E(x_{i1}),\cdots,E(x_{in})).$$

(iii) 令 $c=(c_1,\cdots,c_n)=(1,\cdots,1)$,参与者计算如下:

For $i=1$ to $m-1$

P_i computes

$(c_1,\cdots,c_n)\leftarrow(c_1c_{i1}\bmod p,\cdots,c_nc_{in}\bmod p)$

sends to P_{i+1}

End

P_m computes

$(c_1,\cdots,c_n)\leftarrow(c_1c_{m1}\bmod p,\cdots,c_nc_{mn}\bmod p)$

(iv) 参与者 P_m,P_1 计算如下:

For $j=1$ to n

P_m sends c_j to P_1

P_1 computes $y_j=\mathrm{Dec}(c_j)$

If $y_j\neq 1$, then $y\leftarrow j$ and breaks

End

(v) P_1 输出 y,并公布.

关于效率方面的改进　由数组(2)的构造过程可知,每个数组后半部分若干个元素本身即为随机数,而随机数的密文仍为随机数,因此在协议 1 的第(ii)步可以不对随机数进行加密,直接用 $x_{ij}=r_{ij}$ 代替 $E(x_{ij})$,根据协议的基本原理,这样做不影响协议的正确性及安全性,但可以提高协议效率.

上述方案的正确性由命题 1 得到保证. 由于只有 P_1 有私钥可以解密,所以可以抵抗没有 P_1 参与的任何合谋攻击. 但不能抵抗有 P_1 参与时的合谋攻击,比如,如果参与者 P_1,P_{i-1},P_{i+1} 合谋,可以恢复 P_i 的数组 $X_i=(x_{i1},\cdots,x_{in})$. 为了抵抗这类合谋攻击还需要考虑一些新的策略,下面分别应用秘密分享与门限密码体制设计抵抗任意合谋的保密计算方案.

4　基于秘密分享的最小值保密计算

4.1　基本原理与协议

这个协议的原理与协议 1 基本相同,只是在协议的执行过程中,每个参与者要将自己的数组加密后的密文分成 k 份(具体的分割方法参见 4.3 小节),并随机发送给 m 个参与者中的 k 个. 然后每个参与者把收到的所有份额相乘之后交给 P_1,P_1 最后要做的工作与协议 1 基本相同.

协议 2　基于秘密分享的最小值保密计算

输入:$P_1,\cdots,P_m$ 各自的秘密数据 $x_1,\cdots,x_m$.

输出:$y=\min\{x_1,\cdots,x_m\}$.

(i) P_1 应用 ElGamal 公钥系统生成私钥 sk 和公钥 pk,并公布公钥 pk.

(ii) 参与者 $P_i(i=1,\cdots,m)$ 计算如下:

① P_i 以方式(2)将数据 x_i 转化为数组 X_i.

②P_i 用公钥 pk 加密数组 X_i,得到 $E(X_i)=(E(x_{i1}),\cdots,E(x_{in}))$. P_i 将密文 $E(X_i)$ 分成 k 份,即 $(E(x_{i1})_1,\cdots,E(x_{in})_1),\cdots,(E(x_{i1})_k,\cdots,E(x_{in})_k)$,使得对于所有的 $j(j=1,\cdots,n)$,有 $\prod_{t=1}^{k}E(x_{ij})_t\equiv E(x_{ij})\bmod p$.

③ P_i 将 k 个密文份额分别发送给 m 个参与者中的 k 个.

④ P_i 把自己收到的所有密文份额相乘得到新的密文数组 $E(X_i')=(E(x_{i1}')),\cdots,E(x_{in}'))=(c_{i1},\cdots,c_{in})$.

(iii) $P_i(i=2,\cdots,m)$ 与 P_1 计算如下:

For $j=1$ to n

P_i sends c_{ij} to P_1

P_1 computes $y_j=\mathrm{Dec}\left(\prod_{i=1}^{m}c_{ij}\right)$

If $y_j\neq 1$, then $y\leftarrow j$ and breaks

End

(iv) P_1输出 y,并公布.

4.2 方案分析

参与者 P_i 将 $E(X_i)$ 分割成 k 份进行随机分发,分发完成后,每个参与者要将其收到的所有密文相乘,每个 $P_i(i=1,\cdots,m)$ 所得到的乘积密文为 $E(X_i')=(E(x_{i1}'),\cdots,E(x_{in}'))$. 由 ElGamal 算法的同态性,容易证明下面的命题.

命题 2 在协议 2 中,对于所有的 $j(j=1,\cdots,n)$,有

$$\prod_{i=1}^{m}E(x_{ij}')\equiv E\Big(\prod_{i=1}^{m}x_{ij}\Big)\bmod p.$$

正确性分析 类似于协议 1,由命题 1,乘积数组中第一个不为 1 的元素下标就是所求的最小值. 为了防止合谋攻击虽然进行了一系列的保密信息分割,但由命题 2,下面等式成立:

$$E(x_{1j}')\cdot E(x_{2j}')\cdots E(x_{mj}')\equiv E(x_{1j}\cdot x_{2j}\cdots x_{mj})\bmod p,$$

因此有 $\min\{x_1,\cdots,x_m\}=\min\{j\mid y_j\neq 1\}$.

安全性分析 关于协议 2 的安全性,有下面的定理.

定理 1 基于秘密分享的最小值保密计算的协议 2(简记为 Π)是安全的.

证明 下面应用形式化证明方法证明协议的安全性,分三种情形证明.

情形 1 P_1 不参与合谋,子集 $I=\{P_{i_1},\cdots,P_{i_s}\}$ ($I\subseteq\{P_2,\cdots,P_m\}$)中的参与者合谋想得到参与者 $P_i\notin I$ 的数组 X_i 的元素. 如果 ElGamal 加密算法是安全的,没有 P_1 的私钥,任何参与者的合谋都不能通过解密得到相应的元素;实际上 ElGamal 加密算法是语义安全的,这也排除了通过选择明文攻击得到相应元素的可能性.

在协议 2 中,每个参与者除了自己的输入之外,收到的所有信息都是用语义安全的加密算法进行加密的,这些密文本身以及对它们做任意运算后得到的结果都是计算不可区分的,所以存在概率多项式时间算法 S,使得下式成立:

$$\begin{aligned}&\{S(I,(x_{i_1},\cdots,x_{i_s}),f_I(X))\}_{X\in(\{0,1\}^*)^m}\\&\overset{c}{\equiv}\{\text{view}_I^{\Pi}(X)\}_{X\in(\{0,1\}^*)^n}\end{aligned}\tag{4}$$

S 可按下面方式构造:S 在 $\{1,2,\cdots,n\}$ 内任意选择参与者 $\{P_1,\cdots,P_m\}\setminus I$ 的输入,但要保证 $y=\min\{x_1,\cdots,x_m\}$,然后模拟协议的实际执行过程并得到一个 view;将 S 在模拟过程中的 view 作为 $S(I,(x_{i_1},\cdots,x_{i_s}),f_I(X))$,则容易证明式(4)成立,因此可知协议是安全的.

情形 2 P_1 参与合谋. 即假设 $P_1\in I=\{P_{i_1},\cdots,P_{i_s}\}\subseteq\{P_1,\cdots,P_m\}$,$I$ 中的参与者合谋想获得 $P_i\notin I$ 的数据 x_i. 因为 P_i 已将自己的数据转换成数组 X_i,对数组元素分别加密得到加密数组 $E(X_i)$,然后分成 k 份发送给任意 k 个参与者,具体发送给了哪些参与者,其他参与者没有信息. I 中的合谋者不知道所收到的 $E(x_{ij})$ 的份额是否为全部份额,所以合谋者不能根据其收到的份额确定 P_i 的任何数组元素 x_{ij}.

在协议执行后,除 P_i 外的所有参与者合作可以获得 x_{ij} 的具体值,又由于在协议的解密阶段,参与者 $P_i(i=2,\cdots,m)$ 是将其密文数组元素 c_{ij} 逐项发送给 P_1 的,即要求 P_1 一旦获得所需要的最小值,协议应立刻停止,这样就避免了后面数据信息的泄露,因此执行该协议和借助于可信第三者的理想协议所获得的安全性基本相同,仅有的区别是当其他 $m-1$ 个参与者的数据包含该最小值时,他们合谋可以判断 x_i 是否为该最小值,而在理想协议中关于这点也是保密的.

同样,存在概率多项式时间算法 S 使得式(1)成立. 模拟器 S 的构造类似于情形 1,因此在此情形下协议 2 是安全的.

情形 3 P_1 参与合谋. $P_1\in I\subseteq\{P_1,\cdots,P_m\}$,$I$ 中成员合谋想获得 $\bar{I}=\{P_1,\cdots,P_m\}\setminus I$ 中参与者的数据. 显然,当$\bar{I}$中只有一个元素时,属于上面的情形 2. 当$\bar{I}$包含两个或更多元素时,其分析方法和结论类似于情形 2 的讨论,$\bar{I}$中参与者数据的安全性与理想协议基本相同. 只是当合谋者的数据中有所求最小值时,合谋者能够判断未参与合谋者是否也有该最小值,其他信息则无法获知. 在此情形下,完全类似于上面两种情形证明,存在概率多项式时间算法 S 使得式(1)成立.

综上所述,在任何情形下都存在使式(1)成立的概率多项式时间算法 S,所以协议 2 是安全的.

4.3 分割加密技巧

在协议 2 中,参与者 P_i 需要将每一个密文数组元素 $E(x_{ij})$ 分割成 $k\leqslant m$ 份,下面是具体的分割加密方法.

利用 ElGamal 算法的乘法同态性,为了使分割后的密文能够合成正确的密文,分成的 k 份密文份额$E(x_{ij})_s$ $(s=1,\cdots,k)$要满足 $E(x_{ij})=\prod_{s=1}^{k}E(x_{ij})_s\bmod p$. 根据模运算的性质,选择 k 个随机数 $r_1,r_2,\cdots,r_k$,使 $r_1r_2\cdots r_k\equiv 1\bmod p$. 然后将 $E(x_{ij})\cdot r_1$ 作为第一个份额,将 $r_2,\cdots,r_k$ 分别作为第 $2,\cdots,$第 k 个份额发送给 k 个不同的参与者. 如此,这 k 个参与者的份额相乘仍然等于原来的密文,即 $E(x_{ij})r_1r_2\cdots r_k\equiv E(x_{ij})\bmod p$. 如果在构造数组时,$x_{ij}$本身为随机数 r_{ij},则类似于上节最后关于效率改进方面的讨论,不需要对随机数加密,直接用随机数代替密文,用上面的方法进行分割即可.

5 基于门限密码体制的最小值保密计算

门限密码体制是安全多方计算中对抗合谋攻击的

一个重要工具. 本节需要的是一种朴素的门限密码体制,即(m,m)门限密码体制,它是抵抗合谋攻击的一种有效方法. 在协议设计中利用 ElGamal 密码系统具体构造.

5.1　协议构造

该方案的基本原理仍由命题 1 给出,协议构造如下.

协议 3　基于门限密码体制的最小值保密计算

输入:$P_1,\cdots,P_m$ 各自的秘密数据 $x_1,\cdots,x_m$.

输出:$y=\min\{x_1,\cdots,x_m\}$.

(i) $P_1,\cdots,P_m$ 首先选取 ElGamal 公钥系统的公开参数 g,p. 每个参与者 P_i 选择私钥 k_i,联合生成公钥:

$$h\equiv\prod_{i=1}^{m}g^{k_i}\bmod p\equiv g^{\sum_{i=1}^{m}k_i}\bmod p.$$

(ii) 参与者 $P_i(i=1,\cdots,m)$用方式(2)将 x_i 转化为数组 X_i,并用公钥加密自己的数组 X_i,得到

$$(u_{i1},v_{i1}),(u_{i2},v_{i2}),\cdots,(u_{in},v_{in}),$$

其中$(u_{ij},v_{ij})=(g^{s_{ij}}\bmod p,x_{ij}h^{s_{ij}}\bmod p)$,并发送给 P_m.

(iii) P_m 计算并公布$(u_1,v_1),(u_2,v_2),\cdots,(u_n,v_n)$,其中对$j=1,\cdots,n$

$$(u_j,v_j)=\left(\prod_{i=1}^{m}u_{ij}\bmod p,\prod_{i=1}^{m}v_{ij}\bmod p\right).$$

(iv) 计算最小值的过程如下:

For $j=1$ to n

$P_i(i=1,\cdots,m)$ computes and

sends $t_{ij}=u_j^{k_i}\bmod p$ to P_m

P_m computes $y_j\equiv\dfrac{v_j}{\prod_{i=1}^{m}t_{ij}}\bmod p$

If $y_j\neq1$, then $y\leftarrow j$ and breaks

End

Outputs y

5.2　方案分析

正确性分析　根据 ElGamal 密码系统的乘法同态性,有

$$\begin{aligned}(u_j,v_j)&\equiv\left(\prod_{i=1}^{m}u_{ij}\bmod p,\prod_{i=1}^{m}v_{ij}\bmod p\right)\\&\equiv\left(g^{\sum_{i=1}^{m}s_{ij}}\bmod p,\prod_{i=1}^{m}x_{ij}h^{\sum_{i=1}^{m}s_{ij}}\bmod p\right)\\&\equiv\left(g^{\sum_{i=1}^{m}s_{ij}}\bmod p,(g^{\sum_{i=1}^{m}k_i})^{\sum_{i=1}^{m}s_{ij}}\prod_{i=1}^{m}x_{ij}\bmod p\right),\end{aligned}$$

$$\begin{aligned}\prod_{i=1}^{m}t_{ij}\bmod p&\equiv\prod_{i=1}^{m}u_j^{k_i}\bmod p\equiv\left(\prod_{i=1}^{m}u_{ij}\right)^{\sum_{i=1}^{m}k_i}\bmod p\\&\equiv\left(\prod_{i=1}^{m}g^{s_{ij}}\right)^{\sum_{i=1}^{m}k_i}\bmod p\equiv(g^{\sum_{i=1}^{m}s_{ij}})^{\sum_{i=1}^{m}k_i}\bmod p,\end{aligned}$$

因此

$$y_j\equiv\prod_{i=1}^{m}x_{ij}\bmod p\equiv\frac{v_j}{\prod_{i=1}^{m}t_{ij}}\bmod p.$$

根据命题 1,使得 $y_j\neq1$ 的最小下标 j 即为 $y=\min\{x_1,\cdots,x_m\}$. 因此,协议 3 是正确的.

安全性分析　协议的安全性是基于 ElGamal 加密算法的安全性. 由于门限 ElGamal 公钥系统的公钥是由所有参与者共同产生的,即 $h=g^{k_1+\cdots+k_m}\bmod p$,其中 k_i 是参与者 P_i 所持有的私钥碎片,解密必须有所有参与者的私钥碎片,所以只有所有参与者合作才能对加密信息进行解密,因而可以抵抗合谋攻击.

在计算过程中,每个参与者 P_i 对外仅公布了加密信息$(g^{s_{ij}}\bmod p,x_{ij}h^{s_{ij}}\bmod p)$,在解密过程中对外也仅公布了信息 $h^{k_i}\bmod p$,由 ElGamal 公钥密码系统的安全性可知,在协议执行过程中如果没有 P_i 的参与,无法解密得到 x_{ij},因此在协议执行过程中,P_i 的数据 x_{ij}是完全保密的. 我们给出下面的定理,仅给出证明思路,详细的证明过程省略.

定理 2　基于门限密码体制的最小值保密计算的协议 3 是安全的.

证明思路　证明协议的安全性需要构造满足式(1)的模拟器 S. 根据语义安全的同态加密算法的性质,如果没有私钥,应用公钥加密的任何信息都是计算不可区分的,因此只要有一个参与者不合谋,对其他合谋者来说,他们实际执行协议时获得的 view 和用满足最小值不变的任意一组输入进行模拟所得到的信息序列是计算不可区分的,所以只要在式(1)中令 $S(I,(x_{i_1},\cdots,x_{i_s}),f_I(X))$为模拟过程中的 view,即可使式(1)满足.

6　效率分析

计算效率分析　首先分析上面三个协议的计算复杂性,分析中忽略各协议执行中需要的乘法运算,只考虑模指数运算,应用 ElGamal 公钥密码系统加密(或解密)一次需要进行两次模指数运算. 假设有 m 个参与者,并且每个参与者的数据不超过 n,在三个协议中,每个参与者首先要将自己的数据转化成一个 n 维数组.

在协议 1 中,每个参与者对自己数组中取值为 1 的元素都要进行 ElGamal 加密,m 个参与者最多需要 $2mn$ 次模指数运算;其次,每个参与者对前一个参与者传送过来的密文数组和自己的密文数组做乘法运算;最后,参与者 P_1 对 m 个参与者构成的乘积密文数组解密,如果最小值为 y,需要进行 $2y$ 次模指数运算. 所以协议 1 最多共需要 $2(mn+y)$次模指数运算.

在协议 2 中,每个参与者首先对自己数组中取值为 1 的元素进行一次 ElGamal 加密,m 个参与者最多需要计算 $2mn$ 次模指数运算;在信息分割阶段,如果应用

4.3 小节给出的分割加密技巧对密文进行分割,那么只需要做乘法运算即可;在最后的解密阶段,如果最小值为 y,需要解密 y 次,因此需要 $2y$ 次模指数运算. 所以执行协议 2 最多需要 $2(mn+y)$ 次模指数运算.

在协议 3 中,参与者各方首先合作产生公钥 $h=g^{k_1+\cdots+k_n} \bmod p$,共需要 m 次模指数运算;加密过程所有参与者最多共需要 $2mn$ 次模指数运算;最小值为 y 时,解密过程也需要 my 次模指数运算,所以执行协议 3 最多需要 $m(y+2n+1)$ 次模指数运算.

通信效率分析 协议 1 中,每个参与者将数组加密后的密文发送给下一个参与者,P_m 最后得到所有参与者的加密数组乘积,这期间参与者之间需要 $m-1$ 次通信. 在解密过程中,如果最小值为 y,则 P_m 还需要向 P_1 发送 y 次数据. 因此协议 1 总共需要 $m+y-1$ 次通信.

协议 2 中,每个参与者将自己的密文分成 k 份,并随机地发送给 m 个参与者中的 k 个,m 个参与者之间需要 mk 次通信;在解密过程中,如果最小值为 y,则除 P_1 外的其他参与者要把自己得到的所有密文份额乘积发送给 P_1,这个过程共需要 $(m-1)y$ 次通信,因此执行协议 2 共需要 $mk+(m-1)y$ 次通信.

协议 3 中所有参与者构造公钥与加密过程各需要 $m-1$ 次通信;如果最小值为 y,解密过程需要 $(m-1)y$ 次通信,共需要 $(m-1)(y+2)$ 次通信.

协议 1,协议 2 与协议 3 执行效率的具体比较如表 1 所示. 其中计算复杂性表示使用 ElGamal 公钥加密算法时的模指数运算次数,通信复杂性指通信次数.

表 1 三个协议的性能比较

	计算复杂性	通信复杂性	是否抗合谋
协议 1	$2(mn+y)$	$m+y-1$	部分抵抗
协议 2	$2(mn+y)$	$mk+(m-1)y$	较强抵抗
协议 3	$m(y+2n+1)$	$(m-1)(y+2)$	完全抵抗

7 保密计算方案的推广应用

前面所述的保密求解最小值问题,均假定各参与者的数据属于集合 $\{1,2,\cdots,n\}$. 只要数据的个数有限,总可以将 n 取得充分大使问题得到解决. 但随着 n 的增大,协议的计算效率将线性降低,当参与者的数据分布比较分散时这个问题尤显突出. 本节对前面的方案加以推广,将能更好地解决上面所提出的问题.

一般的最小值保密求解问题 一般地,假设 m 个参与者的数据集合 $\{x_1,x_2,\cdots,x_m\}\subseteq\{z_1,z_2,\cdots,z_n\}$,其中 $z_1<z_2<\cdots<z_n$. 现在,每个 P_i 按照下述方式应用自己的数据 x_i 构造对应的数组 $V_i=(x_{i1},\cdots,x_{in})$,其中当 $z_j<x_i$ 时,$x_{ij}=1$;当 $z_j\geqslant x_i$ 时,$x_{ij}=r_{ij}$,这里 r_{ij} 为不等于 1 的随机数. 为了利用协议 1~3 保密求解 $x_1,x_2,\cdots,x_m$ 的最小值,以数组 V_i 代替协议 1~3 中的数组 X_i,并需要对协议的最后一段作相应的修改,以协议 2 为例,最后一段应修改为:

For $j=1$ to n

P_i sends c_{ij} to P_1

P_1 computes $y_j=\mathrm{Dec}\left(\prod_{i=1}^{m}c_{ij}\right)$

If $y_j\neq 1$, then $y\leftarrow z_j$ and breaks

End

Outputs y

这样通过对数组构造方法的推广,对协议 1~3 稍加修改便可解决更一般的最小值求解问题. 对上述协议稍加修改也可应用于保密求解若干个数值的最大值以及保密计算若干个集合的并集. 限于篇幅,我们仅对这两个问题的求解思想进行简单说明.

最大值保密求解问题 假设参与者 $P_1,\cdots,P_m$ 分别有保密数据 $x_1,\cdots,x_m$,他们需要合作保密计算这些数据的最大值. 这里假设对于所有的 $i=1,\cdots,m$,x_i 满足 $1\leqslant x_i<n$.

我们可以对参与者 P_i 所持有的数据 x_i 按下面方法进行预处理. 在所有数据满足 $1\leqslant x_i<n$ 的条件下,如果令 $x_i'=n-x_i$,则一定有 $1\leqslant x_i'<n$. 在执行协议 1~3 的过程中,每个参与者 P_i 将自己的保密数据 x_i 用 x_i' 代替,那么协议执行结果求出的将是 $y=\min\{n-x_1,\cdots,n-x_m\}$,又因为

$$\begin{aligned}z&=\max\{x_1,\cdots,x_m\}\\&=n-\min\{n-x_1,\cdots,n-x_m\}\\&=n-y,\end{aligned}$$

因此利用此法可求得 $z=\max\{x_1,\cdots,x_m\}$.

集合并集保密计算问题 假设参与者 $P_i(i=1,\cdots,m)$ 各有一个秘密集合 $A_i=\{a_{i1},\cdots,a_{is_i}\}$,他们希望保密计算这 m 个集合的并集 B. 这里假设所有 m 个集合均满足 $A_i\subseteq\{1,2,\cdots,n\}$. 为了解决这个问题,每一个参与者 P_i 首先根据自己的集合构造一个 n 维数组 $U_i=(x_{i1},\cdots,x_{in})$,其中,如果 $j\in A_i$,则取 x_{ij} 为不等于 1 的随机数 r_{ij},如果 $j\notin A_i$,则取 $x_{ij}=1$. 如果将所有数组相乘,得到的乘积数组记为 $Y=(y_1,\cdots,y_n)$,则容易证明数据 j 属于并集 B 的充要条件是 $y_j\neq 1$. 以此为基础,即可把集合的并集问题转化为数组的乘积问题,通过对协议 1~3 进行相应修改即可保密计算并集 B.

8 结论

本文设计了一种新的编码方法,以新的编码方法与 ElGamal 同态加密算法为基础,分别利用秘密分享和门限密码体制构造了最小值问题的三个安全多方计算协议. 这些协议稍作修改就可以用于最大值的保密计

算以及多个集合并集的保密计算. 还可以将协议加以推广改进以适用于不同数值范围的相应保密计算问题,而且方案是高效的.

参考文献

[1] YAO A C. Protocols for secure computations[A]. Proceedings of the 23th IEEE Symposiumon Foundations of Computer Science [C]. Piscataway: IEEE Press, 1982. 160 – 164.

[2] GOLDREICH O, MICALI S, WIGDERSON A. How to play any mental game[A]. Proceedings of the Nineteenth Annual ACM Conference on Theory of Computing[C]. Piscataway:IEEE Press,1987. 218 – 229.

[3] GOLDREICH O. The Fundamental of Cryptography: Basic Applications[M]. London:Cambridge University Press,2004.

[4] FAGIN R, NAOR M, WINKLERY P. Comparing information without leaking it[J]. Communications of the ACM, 1996,39(5):77 – 85.

[5] 刘文,王永滨. 安全多方信息比较相等协议及其应用[J]. 电子学报,2012,40(5):871 – 876.
LIU W, WANG Y B. Secure multi-party comparing protocol and its applications[J]. Acta Electronica Sinica, 2012, 40(5):871 – 876. (in Chinese)

[6] FREEDMAN M J, NISSIM K, PINKAS B. Efficient private matching and set intersection[A]. Advances in Cryptology-EUROCRYPT[C]. Berlin Heidelberg:Springer,2004. 1 – 19.

[7] KISSNER L, SONG D. Privacy-preserving set operations [A]. Advances in Cryptology-CRYPTO[C]. Berlin Heidelberg:Springer,2005. 241 – 257.

[8] 李顺东,王道顺. 基于同态加密的高效安全多方计算[J]. 电子学报,2013,41(4):798 – 803.
LI S D, WANG D S. Efficient secure multiparty computation based on homomorphic encryption[J]. Acta Electronica Sinica,2013,41(4):798 – 803. (in Chinese)

[9] LIN H Y, TZENG W G. An efficient solution to the millionaires' problem based on homomorphic encryption[A]. Applied Cryptography and Network Security [C]. Berlin Heidelberg:Springer,2005. 456 – 466.

[10] ATALLAH M J, DU W. Secure multi-party computational geometry[A]. Algorithms and Data Structures[C]. Berlin Heidelberg:Springer,2001. 165 – 179.

[11] LI S D, WU C Y, WANG D S, et al. Secure multiparty computation of solid geometric problems and their applications[J]. Information Sciences,2014,282:401 – 413.

[12] QIN J, DUAN H, ZHAO H, et al. A new Lagrange solution to the privacy-preserving general geometric intersection problem[J]. Journal of Network and Computer Applications,2014,46:94 – 99.

[13] DU W L, ATALLAH M J. Privacy-preserving cooperative statistical analysis[A]. Proceedings of the 17th Annual Conference of Computer Security Applications[C]. Piscataway:IEEE Press,2001. 102 – 110.

[14] 王波,杨静. 一种基于逆聚类的个性化隐私匿名方法[J]. 电子学报,2012,40(5):883 – 890.
WANG B, YANG J. A personalized privacy anonymous method based on inverse clustering[J]. Acta Electronica Sinica,2012,40(5):883 – 890. (in Chinese)

[15] AGGARWAL C C. Privacy-preserving data mining[A]. Data Mining[C]. Berlin Heidelberg:Springer,2015. 663 – 693.

[16] DU W L, ATALLAH M J. Protocols for secure remote database access with approximate matching[A]. Advance of E-Commerce and Privacy[C]. New York:Springer,2001. 87 – 111.

[17] CACHIN C. Efficient private bidding and auctions with a noblivious third party[A]. Proceedings of the 6th ACM Conferenceon Computer and Communications Security [C]. New York:ACM,1999. 120 – 127.

[18] 石润华,仲红,崔杰,等. 具有统计特性的不经意传输协议[J]. 电子学报,2014,42(11):2273 – 2279.
SHI R H, ZHONG H, CUI J, et al. A novel oblivious transfer protocol with statistical analysis[J]. Acta Electronica Sinica,2014,42(11):2273 – 2279. (in Chinese)

[19] NAOR M, PINKAS B. Oblivious transfer and polynomial evaluation[A]. Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing [C]. New York:ACM,1999. 245 – 254.

[20] 刘木兰,张志芳. 密钥共享体制和安全多方计算[M]. 北京:电子工业出版社,2008.
LIU M L, ZHANG Z F. Secret Sharing Schemes and Secure Multiparty Computation [M]. Beijing: Publishing House of Electronics Industry,2008. (in Chinese)

作者简介

窦家维　女,1963 年 3 月生于西安. 副教授,硕士生导师. 研究方向为密码学、信息安全. E-mail:jiawei@ snnu. edu. cn

马　丽　女,1983 年 6 月生于陕西渭南. 陕西师范大学数学与信息科学学院硕士研究生. 研究方向为密码学及其应用. E-mail:mary@ snnu. edu. cn