安全多方信息比较相等协议及其应用

刘 文,王永滨
(1.中国传媒大学计算机学院,北京 100024; 2.中国传媒大学广播电视信息安全与安全播出研究所,北京 100024)

摘 要: 安全多方信息比较协议是一个由两方向多方进行推广的问题,可以在不泄漏各个参与方信息的情况下比较出多方信息是否全部相等以及得到具有相等信息的参与方的数目.该问题的研究目前尚没有见到报道.本文在半诚实模型下利用设计的F函数和具有语义安全性的加法同态加密体制设计了一个安全多方信息比较协议;分析了该协议的正确性,安全性和效率.该方案在安全多方计算研究中有广泛应用.

关键词: 安全多方计算; 安全多方比较相等问题; 加法同态加密体制
中图分类号: TN309 **文献标识码:** A **文章编号:** 0372-2112 (2012) 05-0871-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2012.05.002

Secure Multi-Party Comparing Protocol and Its Applications

LIU Wen, WANG Yong-bin
(1. *School of Computer, Communication University of China, Beijing* 100024, *China*;
2. *Institute of Information Security and Secure Broadcasting in Broadcast and Television, Communication University of China, Beijing* 100024, *China*)

Abstract: The secure multi-party comparing problem is generalized from the millionaires' problem, which is used to get whether the multi-party's secret inputs are all equal and if not, the number of users whose inputs are same as an indicated user's. Based on the F function and semantic addition homomorphic encryption, a protocol of secure multi-party comparing is proposed. The correctness, security and efficiency of the protocol are analyzed. This protocol can be used in many aspects of secure multi-party computation.

Key words: secure multi-party computation; secure multi-party comparing problem; addition homomorphic encryption

1 引言

多方安全计算要解决的问题是:n 个参与方 $P_1, P_2, \cdots, P_n$ 各自有一个秘密输入 $x_1, x_2, \cdots, x_n$,他们要计算这些秘密输入的一个函数 $f(x_1, x_2, \cdots, x_n) = (y_1, y_2, \cdots, y_n)$,参与方 P_i 得到输出 y_i.其中安全的含义是指对于任何一个参与方 P_i,除了 y_i 和 x_i 所隐含的信息,P_i 不能得到任何其它信息.实际上,一个解决多方安全计算问题的协议是一种分布式算法,每个成员运行一个算法,成员之间经过若干次交互完成计算任务,得到相应的输出.

在安全多方计算领域中有关信息比较的问题有:安全两方比较大小问题[1](即百万富翁问题),安全两方比较相等问题[2~7](即社会主义百万富翁问题),安全两方比较问题的扩展问题——安全多方多数据排序问题[8~10].Goldreich O等人指出将安全两方计算推广为安全多方计算是一个重要的研究方向[11].美国普渡大学的Du博士在其博士论文[12]中特别指出把安全两方计算推广到安全多方计算不是一个容易的工作.

本文致力于研究安全两方比较相等问题的扩展问题——安全多方信息比较相等问题.该问题的描述为:假设有 n 方 $P_1, P_2, \cdots, P_n$ 分别有一个保密数值,用 N_i 表示 P_i 拥有的参与比较的保密数值,$i = 1, 2, \cdots, n$. n 方希望在不泄漏各自的保密信息的前提下,得到所有的保密数值是否全部相等的结论.如果这些保密数值不全部相等,则 P_i 方希望得到 $n-1$ 方的保密数值集合中与 P_i 拥有的保密数值 N_i 相等的保密数值的数目 NE_i.为了更好的理解这个问题,请看下面的例子:假设 P_1, P_2, P_3, P_4 分别拥有一个保密数值 3,4,6,3.通过安全多方信息比较协议,P_1, P_2, P_3, P_4 得到他们四方拥有的保密数值不全部相等;如得到 $NE_1 = 1$,则 P_1 知道 P_2, P_3, P_4 拥有的数据中只有一个与它拥有的数据相等.安全多方信息比较相等协议在安全多方计算中有广泛的应用.

1.1 相关工作

在文献[13,14]中提出了通用的安全多方计算协议可以用于解决任何的安全多方计算问题.该方法自然

收稿日期:2010-03-09;修回日期:2012-02-21
基金项目:国家高技术研究发展计划863项(No.2011AA01A107);2009年北京市文化创意产业发展专项资金

可以用于解决安全多方信息比较相等问题.但是这种通用的方法效率很不理想.

为了提高效率必须设计专门的解决安全多方信息比较相等问题的协议.目前还没有专门用于解决安全多方信息比较相等问题的协议,研究者着力于解决安全两方信息比较相等问题.在文献[2]中,Fagin R 等人总结了利用随机置换,特殊设备等方法解决该引申问题的多种方案;在文献[3]中,Jakobsson M 等人给出了一个计算复杂度为 $O(k)$次模指数运算的无信息泄漏的两方比较相等协议;在文献[4]中,Boudot F 给出了一个基于 DHH 假设的社会主义百万富翁协议,该协议只需要常数次模指数运算,且具有公平性;在文献[5]中,秦静老师等人将 Cachin C 的百万富翁协议[6]推广为基于 Φ-隐藏假设和同态加密体制语义安全性假设的无信息泄漏的两方比较相等协议;在文献[7]中,作者等人给出了一种利用滑动窗口函数和交换加密函数解决社会主义百万富翁问题的新方案.

所有这些协议都只发生在两方之间,可以设计一个平凡的方案,通过反复利用已有的安全两方信息比较相等协议来完成安全多方信息相等的比较.假设 P_i 与 P_j(i 为某固定值,$j=1,2,\cdots,n$ 且 $i\neq j$)使用安全两方信息比较相等协议比较它们拥有的保密数值 N_i 与 N_j 是否相等.经过 $n-1$ 次比较后,P_i 可以得到它拥有的保密数值 N_i 是否与其它 $n-1$ 方拥有的保密数值全部相等.如果这 n 个保密数值不是全部相等,则 P_i 得到拥有与保密数值 N_i 相等的保密数值的参与方的数目 NE_i.该方案存在一个弱点,P_i 在每次进行两方比较时都能得到它与 P_i($j=1,2,\cdots,n$ 且 $i\neq j$)的保密信息是否相等这样一个额外信息.所以本文希望能设计出一种不泄漏任何额外信息的安全多方信息比较相等协议.

1.2 本文的贡献

首先针对安全两方信息比较相等问题的扩展问题——安全多方信息比较相等问题,提出了一个不泄漏任何额外信息的安全多方信息比较相等协议.该协议使用具有语义安全性的门限同态加密体制做为基础工具进行设计.然后利用模拟器法证明该协议的安全性.最后将该协议应用于安全多集合比较相等问题和安全多向量比较相等问题中.

2 预备知识

2.1 具有语义安全性的门限加法同态加密体制

门限同态加密体制是一类具有特殊性质的加密体制,它具有如下性质:

(1)在加密体制中,n 方 $P_1,P_2,\cdots,P_n$ 知道一个公钥 pk,并且分别拥有与该公钥相对应的私钥 sk 的一部分 sk_1, sk_2, …, sk_n;本文采用 $E_{pk}(\cdot)$ 表示加密,$D_{sk_1,sk_2,\cdots,sk_n}(\cdot)$表示解密.

(2)对于给定密文 $E_{pk}(m_1)$,$E_{pk}(m_2)$:如果该门限同态加密体制是具有加法同态性的,通过计算 $E_{pk}(m_1)\oplus E_{pk}(m_2)=E_{pk}(m_1+m_2)$,可以得到 m_1+m_2 的密文;其中 + 表示加法运算,$\oplus$表示总和操作.

(3)该门限同态加密方案具有语义安全性,即密文不泄漏明文的任何信息.这可以通过一个攻击游戏说明:假定有一个敌手,选择了两个等长的明文 m_0,m_1,敌手把两个消息发送给用户;用户随机地选取一个比特 $b\in\{0,1\}$,并对 m_b 进行加密得到密文 $c=E(m_b)$,把 c 发送给敌手;则敌手正确猜测 b 的概率为 $1/2+\varepsilon(k)$,这里 $\varepsilon(k)$是可忽略函数.

2.2 协议的安全性定义

定义 1(可以忽略的函数) 如果对于每一个多项式 p 和所有足够大的 n,函数 $\mu:N\to[0,1]$使得 $\mu(n)<1/p(n)$成立,则称函数 μ 是可忽略函数.

定义 2(计算不可区分性) 假设 $S\subseteq\{0,1\}^*$.如果对于每一个的多项式大小的电路族$\{D_n\}_{n\in N}$,两个集合 $X\overset{def}{=}\{X_w\}_{w\in S}$、$Y\overset{def}{=}\{Y_w\}_{w\in S}$,存在一个可以忽略的函数 $\mu:N\to[0,1]$,满足:

$$\left|\Pr[D_n(w,X_w)=1]-\Pr[D_n(w,Y_w)=1]\right|<\mu(|w|)$$

则称 $X\overset{def}{=}\{X_w\}_{w\in S}$与 $Y\overset{def}{=}\{Y_w\}_{w\in S}$是计算不可区分的,记为 $X\overset{c}{\equiv}Y$.

假设参与计算的 n 方为 $P_1,P_2,\cdots,P_n$.设 f 表示一个 n 变量的概率多项式时间函数,f_i 表示 f 的第 i 个计算结果,π 表示计算该函数的协议.设 $I=\{i_1,\cdots,i_t\}\subset\{1,\cdots,n\}$为半诚实参与方序号集合,$f_I(x_1,\cdots,x_n)$表示序列 $f_{i_1}(x_1,\cdots,x_n),\cdots,f_{i_t}(x_1,\cdots,x_n)$,$View_I^{\pi}(x_1,\cdots,x_n)$表示序列 $View_{i_1}^{\pi}(x_1,\cdots,x_n),\cdots,View_{i_t}^{\pi}(x_1,\cdots,x_n)$,$View_{i_k}^{\pi}(x_1,\cdots,x_n)$表示$(x_{i_k},r^{i_k},m_1^{i_k},\cdots,m_k^{i_k})$,其中 r^{i_k}表示 P_{i_k}独立掷币结果,$m_i^{i_k}$ 表示 P_{i_k}第 i 次收到的信息;执行协议以后,$P_1,P_2,\cdots,P_n$ 的输出表示为 $out_1^{\pi}(x_1,\cdots,x_n),\cdots,out_n^{\pi}(x_1,\cdots,x_n)$.

定义 3(半诚实模型的安全性) 对于一个函数 f,如果存在概率多项式时间模拟器 S 使得$\{S(I,x_{i_1},\cdots,x_{i_t},f_I(x_1,\cdots,x_n)\}_{x_i\in\{0,1\}^*}\overset{c}{\equiv}\{View_I^{\pi}(x_1,\cdots,x_n)\}_{x_i\in\{0,1\}^*}$成立,则认为 π 安全地计算 f.

3 安全多方信息比较相等协议

本文假设参与比较的各方都是“半诚实的”,即参与各方能严格执行协议的规程,不会中途强行退出或

恶意掺入虚假数据.但在协议执行过程中他们可能会保留所有能搜集到的关于其它参与方的信息,以期望在协议结束后推断出其它参与方的输入信息.

3.1 安全多方多信息比较问题的描述

假设有 n 方 $P_1,P_2,\cdots,P_n$ 分别有一个保密数值,用 N_i 表示 P_i 拥有的参与比较的保密数值,$i=1,2,\cdots,n$.n 方希望在不泄漏各自的保密信息的前提下,得到所有的保密数值是否全部相等的结论.如果这些保密数值不全部相等,则 P_i 方希望得到 $n-1$ 方的保密数值集合中与 P_i 拥有的保密数值 N_i 相等的保密数值的数目 NE_i.

3.2 函数 F

构造一个函数 $F:\{1,2,\cdots,N\}\to\{0,1\}^N$,该函数使得定义域在 $\{1,2,\cdots,N\}$ 内的某个数值 x 映射为一个满足一定规则的长度为 N 的二进制数组 s.该函数可以帮助进行安全多方多信息比较.

该函数映射到的长度为 N 的二进制数组 s 需要满足规则为:如果 $x=i\in\{1,2,\cdots,N\}$,则 $s[i]=1$,而 $s[k]=0(k=1,\cdots,i-1,i+1,\cdots,N)$.例如 $x=3\in\{1,2,3\}$,则 $F(x)=s[1]s[2]s[3]=001$;$x=2\in\{1,2,3,4,5\}$,则 $F(x)=s[1]s[2]s[3]s[4]s[5]=01000$.

3.3 安全多方多信息比较协议

假设 $P_1,P_2,\cdots,P_n$ 知道一个具有语义安全性门限加法同态加密体制的公钥 pk,并且分别拥有与该公钥相对应的私钥 sk 的一部分 $sk_1,sk_2,\cdots,sk_n$;P_1 拥有保密数值 N_1,P_2 拥有保密数值 N_2,$\cdots$,P_n 拥有保密数值 N_n,其中 $N_1,N_2,\cdots,N_n\in\{1,2,\cdots,N\}$.$P_1,P_2,\cdots,P_n$ 分别利用 F 函数计算

$F(N_1),F(N_2),\cdots,F(N_n)$,

$F(N_1)=s_1[1]s_1[2]\cdots s_1[N_1-1]s_1[N_1]s_1[N_1+1]\cdots s_1[N]=00\cdots010\cdots0$,

$F(N_2)=s_2[1]s_2[2]\cdots s_2[N_2-1]s_2[N_2]s_2[N_2+1]\cdots s_2[N]=00\cdots010\cdots0$

$\cdots$

$F(N_n)=s_n[1]s_n[2]\cdots s_n[N_n-1]s_n[N_n]s_n[N_n+1]\cdots s_n[N]=00\cdots010\cdots0$.

$P_1,P_2,\cdots,P_n$ 共同选择一个 $j\in\{1,2,\cdots,n\}$,然后执行下面的步骤:

(1)对于 $i=1,\cdots,j-1,j+1,\cdots,n$:$P_i$ 利用具有语义安全性门限加法同态加密体制分别加密二进制数组 $s_i[1]s_i[2]\cdots s_i[N_i-1]s_i[N_i]s_i[N_i+1]\cdots s_i[N]$ 中的各个分量得到加密数列:$E_{pk}(s_i[1])E_{pk}(s_i[2])\cdots E_{pk}(s_i[N_i-1])E_{pk}(s_i[N_i])E_{pk}(s_i[N_i+1])\cdots E_{pk}(s_i[N])$;$P_i$ 将得到的加密序列发送给参与方 P_j.

(2)P_j 从得到的 $n-1$ 个加密序列中分别取出第 N_j 个加密数据 $E_{pk}(s_i[N_j])$,计算

$$E_{pk}(NE_j)=\bigoplus_{i=1,i\neq j}^{n}E_{pk}(s_i[N_j])=E_{pk}\Big(\sum_{i=1,i\neq j}^{n-1}s_i[N_j]\Big).$$

(3)$P_1,P_2,\cdots,P_n$ 利用自己的子私钥联合进行解密,得到结果 NE_j.如果 $NE_j=n-1$,则 $N_1=N_2=\cdots=N_n$;否则 $N_1,N_2,\cdots,N_n$ 不全部相等,P_j 知道 $N_1,N_2,\cdots,N_{j-1},N_{j+1},\cdots N_n$ 中有 NE_j 个数值等于 N_j.

为了便于理解,现举例说明上述协议的执行过程:

假设有 P_1,P_2,P_3,P_4 四方,分别拥有保密数值 $N_1=2,N_2=2,N_3=4,N_4=2$ 其中 $N_1,N_2,N_3,N_4\in\{1,2,3,4\}$.$P_1,P_2,P_3,P_4$ 共同选择一个 $j=2$.P_1,P_2,P_3,P_4 分别利用 F 函数计算

$F(N_1),F(N_2),F(N_3),F(N_4)$:

$F(N_1)=s_1[1]s_1[2]s_1[3]s_1[4]=0100$;

$F(N_2)=s_2[1]s_2[2]s_2[3]s_2[4]=0100$;

$F(N_3)=s_3[1]s_3[2]s_3[3]s_3[4]=0001$;

$F(N_4)=s_4[1]s_4[2]s_4[3]s_4[4]=0100$.

(1)P_1 计算 $E_{pk}(s_1[1])E_{pk}(s_1[2])E_{pk}(s_1[3])E_{pk}(s_1[4])=E_{pk}(0)E_{pk}(1)E_{pk}(0)E_{pk}(0)$,并将结果发送给 P_2;

P_3 计算 $E_{pk}(s_3[1])E_{pk}(s_3[2])E_{pk}(s_3[3])E_{pk}(s_3[4])=E_{pk}(0)E_{pk}(0)E_{pk}(0)E_{pk}(1)$,并将结果发送给 P_2;

P_4 计算 $E_{pk}(s_4[1])E_{pk}(s_4[2])E_{pk}(s_4[3])E_{pk}(s_4[4])=E_{pk}(0)E_{pk}(1)E_{pk}(0)E_{pk}(0)$,并将结果发送给 P_2.

(2)P_2 从得到的 3 个加密数组中分别取出第二个数据 $E_{pk}(s_1[2]),E_{pk}(s_3[2]),E_{pk}(s_4[2])$,计算 $E_{pk}(NE)=E_{pk}(s_1[2])\oplus E_{pk}(s_3[2])\oplus E_{pk}(s_4[2])=E_{pk}(2)$.

(3)$P_1,P_2,\cdots,P_n$ 利用自己的子私钥联合进行解密,得到结果 $NE=2$.P_2 知道四方分别拥有的保密数值 N_1,N_2,N_3,N_4 不全部相等并且 N_1,N_3,N_4 中有 2 个数值与 N_2 相等.

3.4 安全多方信息比较协议的安全性和效率分析

3.4.1 安全性分析

定理 1　在半诚实模型下,在门限加法同态加密体制具有语义安全性假设下,设计的安全多方信息比较相等协议是安全的.

证明　正确性:容易看出来协议执行完步骤(1),(2)P_j 将得到的每一个加密数组作为矩阵的一行,可以得到如下形式的矩阵:

$$\begin{bmatrix} E_{pk}(s_1[1]) & \cdots & E_{pk}(s_1[N_i]) & \cdots & \cdots & E_{pk}(s_1[N]) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ E_{pk}(s_{j-1}[1]) & \cdots & \cdots & E_{pk}(s_{j-1}[N_{j-1}]) & \cdots & E_{pk}(s_{j-1}[N]) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ E_{pk}(s_n[1]) & \cdots & E_{pk}(s_n[N_n]) & E_{pk}(s_n[N_n+1]) & \cdots & E_{pk}(s_n[N]) \end{bmatrix}$$

$\cdot E_{pk}(NE_j)=\bigoplus_{i=1,i\neq j}^{n}E_{pk}(s_i[N_j])=E_{pk}\left(\sum_{i=1,i\neq j}^{n-1}s_i[N_j]\right)$

等于矩阵第 N_j 列的所有加密数据的$\oplus$运算.

由 F 函数运算的规则我们可以知道,如果 $N_k=N_j(k=1,2,\cdots,j-1,j+1,\cdots,N,k\neq j)$,则 $F(N_k)=F(N_j)$,即 $s_k[N_k]=s_j[N_j]=1$. $E_{pk}(NE_j)$实际上就是 $N_1,N_2,\cdots,N_{j-1},N_{j+1},\cdots N_n$ 中等于 N_j 的数目的加密结果.最后 $P_1,P_2,\cdots,P_n$ 联合解密得 NE_j.

需要指出的是在无异常出现的情况下,该协议的正确率是 100%,不会产生错误的判断.

安全性 在半诚实模型下安全多方信息比较相等协议是安全的,指的是各个参与方 P_i 除了知道自己的保密数据是否与其它参与方全部相等之外或者自己的保密数值与其它参与方保密数值相等的数目之外,均不能从自己的输入、输出以及在计算过程中搜集到的中间结果中得到关于其它参与方输入的任何信息.

采用反证法进行证明.假设我们所设计的协议是不安全的,即存在一个概率多项式时间的敌手 D,该敌手可以从协议计算过程中获得关于其它参与方的输入信息 N_i.假设欺骗方为 $P_1,P_2,\cdots,P_n$ 中的一个或几个,不妨假设为 $\Omega\subset\{P_1,P_2,\cdots,P_n\}$.敌手 D 可以控制 Ω,通过 Ω 知道一些信息.按照 Ω 中是否包含参与方 P_j 两种情况对 Ω 中知道的信息进行讨论:

(1)$\Omega=\{P_{k_1},\cdots,P_{k_i}\}$,$P_j\notin\Omega$,敌手 D 可以控制 Ω,通过 Ω 知道信息包括 $P_{k_1},\cdots,P_{k_i}$ 拥有的保密数值,F 函数值,F 函数数组各个分量的加密结果.这些信息不包含任何不属于 Ω 的参与方的信息,所以敌手 D 仍然不知道关于任何不属于 Ω 的参与方的信息.

(2)$\Omega=\{P_{k_1},\cdots,P_{k_i}\}$,$P_j\in\Omega$,敌手 D 可以控制 Ω,通过 Ω 知道信息包括 $P_{k_1},\cdots,P_{k_i}$ 拥有的保密数值 $N_{k_1},\cdots,N_{k_i}$,F 函数值,F 函数数组各个分量的加密结果以及所有其它参与方法 $P_t\notin\Omega$ 送给 P_j 的 F 函数数组各个分量的加密结果,即矩阵

$$\begin{bmatrix} E_{pk}(s_1[1]) & \cdots & E_{pk}(s_1[N_i]) & \cdots & \cdots & E_{pk}(s_1[N]) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ E_{pk}(s_{j-1}[1]) & \cdots & \cdots & E_{pk}(s_{j-1}[N_{j-1}]) & \cdots & E_{pk}(s_{j-1}[N]) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ E_{pk}(s_n[1]) & \cdots & E_{pk}(s_n[N_n]) & E_{pk}(s_n[N_n+1]) & \cdots & E_{pk}(s_n[N]) \end{bmatrix}$$

敌手 D 可以通过 $P_t\notin\Omega$ 向 $P_j\in\Omega$ 发送的信息获得关于参与方 $P_t(P_t\notin\Omega)$的保密信息 N_t.因为敌手 D 从 $P_i\in\Omega$ 自己计算得到的信息 F 函数值,F 函数数组各个分量的加密结果.这些信息不包含任何不属于 Ω 的参与方的信息,所以敌手 D 只能从其它参与方 $P_t\notin\Omega$ 发送给 P_j 的 F 函数数组各个分量的加密结果来推测其它参与方 $P_t(P_t\notin\Omega)$的保密数值.假设此时参与方 $P_t(P_t\notin\Omega)$的输入为 N_t.如果敌手 D 知道 $P_t(P_t\notin\Omega)$的输入 N_t,它可以得到 $P_t(P_t\notin\Omega)$的 F 函数数组,并且知道 $P_t(P_t\notin\Omega)$发送来的数组加密序列是 $P_t(P_t\notin\Omega)$的 F 函数数组各个分量利用门限加法同态密码体制加密后得到的密文序列数组.显然这与门限加法同态密码体制的语义安全性假设是相矛盾.

定理 1 得证.

3.4.2 效率分析

在协议的第(1)步中,$P_1,P_2,\cdots,P_nn$ 方利用门限加法同态密码体制一共加密 nN 次;在第(2)中 P_j 方进行一些中间计算,需要进行 $n-2$ 次乘法;在第(3)步中,n 方共同解密 1 个密文.假设门限加法同态密码体制的安全参数为 k,本文设计的安全多方信息比较相等协议的计算复杂度为 nN 次加密运算和一次解密运算,通信复杂度为 knN 比特.

4 安全多方信息比较相等协议的应用

安全多方信息比较相等协议在现实中有许多用途,举例如下:

假设 $P_1,P_2,\cdots,P_n$ 分别拥有保密集合 $D_{P_1}=\{m_1^1,m_2^1,\cdots,m_{k_1}^1\}$,$D_{P_2}=\{m_1^2,m_2^2,\cdots,m_{k_2}^2\}$,$\cdots$,$D_{P_n}=\{m_1^n,m_2^n,\cdots,m_{k_n}^n\}$,$D_{P_1},D_{P_2},\cdots,D_{P_n}\subset\{1,2,\cdots,N\}$. $P_1,P_2,\cdots,P_n$ 希望保密判断出他们拥有的多个集合是否全部相等;如果不是全部相等则希望保密得到集合交集的势$|D_{P_1}\cap D_{P_2}\cap\cdots\cap D_{P_n}|$.该问题称为安全多集合比较相等问题.

为了解决上面的问题,$P_1,P_2,\cdots,P_n$ 首先分别对集合中的数值采用改造的函数 $F:\{D_{P_1},D_{P_2},\cdots,D_{P_n}\}\to\{0,1\}^N$,该函数使得集合 $D_{P_k}\subset\{1,2,\cdots,N\}$映射为一个满足一定规则的长度为 N 的二进制数组 s.

该函数映射到的长度为 N 的二进制数组 s 需要满足规则为:如果对于 $i=1,2,\cdots,N$,如果 $i\in D_{P_k}$,则$s[i]=1$,否则 $s[i]=0$. 例如 $D_{P_k}=\{1,3\}\subset\{1,2,3\}$,则 $F(D_{P_k})=s[1]s[2]s[3]=101$; $D_{P_k}=\{1,3\}\subset\{1,2,3,4,5\}$,则 $F(D_{P_k})=s[1]s[2]s[3]s[4]s[5]=10100$.

$P_1,P_2,\cdots,P_n$ 利用改造的 F 函数计算得 $F(D_{P_1})$,$F(D_{P_2})$,$\cdots$,$F(D_{P_n})$后,对于每一个 $j=1,2,\cdots,n$,执行下面的步骤:

(1)对于 $i=1,\cdots,j-1,j+1,\cdots,n$:$P_i$ 利用门限加法同态加密体制分别加密二进制数组 $F(D_{P_1})$,$F(D_{P_2})$,$\cdots$,$F(D_{P_n})$ 中的各个分量,得到加密数列:$E_{pk}(F(D_{P_1}))$,$E_{pk}(F(D_{P_2}))$,$\cdots$,$E_{pk}(F(D_{P_n}))$;P_i 将得到的加密序列发送给参与方 P_j.

(2)P_j 从得到的 $n-1$ 个加密序列中分别取出第

$m_1^j, m_2^j, \cdots, m_{k_j}^j$ 个加密数据进行 $\oplus$ 计算 $E_{pk}(NE_k^i) = \bigoplus_{i=1, i\neq j}^{n} E_{pk}(s_i[m_k^j]) = E_{pk}\left(\sum_{i=1, i\neq j}^{n-1} s_i[m_k^j]\right)(k = 1, 2, \cdots, k_j)$.

(3) $P_1, P_2, \cdots, P_n$ 利用自己的子私钥联合进行解密,得到结果 $NE_1^j, \cdots, NE_{k_j}^j$. 如果对于每一个 $j = 1, 2, \cdots, n$ 都有 $NE_1^j = \cdots = NE_{k_j}^j = n - 1$,则 $D_{P_1} = D_{P_2} = \cdots = D_{P_n}$.

需要指出的是在文献[16]中,李顺东老师等人也提出了一个安全两集合比较相等协议.对该协议进行一些改造就可以解决安全多集合比较相等问题,并且在效率上比本文提出的协议要好很多.但是他的协议有可能出现单边错误,对于正确性要求高的场合采用我们提出的协议会合适一些.另外李顺东老师提出的协议只能得出两个集合是否相等结论.而利用我们的协议除了能得出这些集合是否全部相等结论外,当结果是集合不全部相等时,还得到这些集合交集的势 $|D_{P_1} \bigcap D_{P_2} \bigcap \cdots \bigcap D_{P_n}|$,即 $NE_1^j, \cdots, NE_{k_j}^j$ 中值等于 $n - 1$ 的数目.

另外安全多向量比较相等问题和安全多元组比较相等问题都可以转换为安全多集合比较相等问题,采用相同的方案解决.

5　结论

安全多方信息比较相等问题目前还没有见到研究报道,虽然用多次使用安全两方信息比较相等协议可以解决该问题甚至可能取得更好的效率,但是该方案在保密性上存在弱点.而本文利用新设计的 F 函数和门限加法同态加密体制设计的安全多方信息比较相等协议可以克服平凡解决方案中存在的安全隐患.

最后需要指出的是本文提出解决方案的计算复杂度和通信复杂度较高,希望在以后的研究中可以研究出更加高效的解决安全多方信息比较相等问题的方案.

参考文献

[1] Yao A. Protocols for secure computation[A]. Proceeding of the 23th IEEE Symposium on Foundations of Computer Science [C]. Los Alamitos, CA: IEEE Computer Society Press, 1982. 160 – 164.

[2] Cachin C. Efficient private bidding and auctions with an oblivious third party[A]. Proceedings of the 6th ACM Conference on Computer and Communications Security[C]. New York: ACM Press, 1999. 120 – 127.

[3] Lin H Y, Tzeng W G. An efficient solution to the millionaires problem based on homomorphic Encryption[A]. Proceedings of the 4th International Conference on Applied Cryptography and Networks Security[C]. New York: 2005. 456 – 466.

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

[5] 李顺东,戴一奇,游启友.姚氏百万富翁问题的高效解决方案[J].电子学报,2005,33(5):769 – 773.
Li Shun-dong, Dai Yi-qi, You Qi-you. An efficient solution to yao's millionaires' problem[J]. Acta Electronica Sinica, 2005, 33(5): 769 – 773. (in Chinese)

[6] 秦波,秦慧,周克复,王晓峰,王育民.常数复杂性的百万富翁协议[J].西安理工大学学报,2005,21(2):149 – 152.
Qin Bo, Qin Hui, Zhou Ke-fu, Wang Xiao-feng, Wang Yu-ming. Millionaires' protocol with constant complexity[J]. Journal of Xi'an University of Technology, 2005, 21(2): 149 – 152. (in Chinese)

[7] Ioannidis I, Grama A. An efficient protocol for Yao's millionaires' problem[A]. In Proceedings of the 36th Annual Hawaii International Conference on System Sciences [C]. Hawaii: 2003.

[8] Li S D, Wang D S, Dai Y Q, Luo P. Symmetric cryptographic solution to Yao's Millionaires' problem and an evaluation of secure multiparty computations[J]. Information Sciences. 2008, 178: 244 – 255.

[9] Goldreich O, Micali S, Wigderson A. How to play any mental game[A]. In Proceedings of the 19th Annual ACM Conference on Theory of Computing[C]. New York: ACM, 1987. 218 – 229.

[10] Du W L. A Study of several specific secure two-party computation problems, Ph. D. Thesis[D]. Purdue University. Available From: http://www. cis. edu/ ~ wedu/ Research/publication. html. 2000.

[11] 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,2004,15(3):421 – 427.
Qing Jing, Zhang Zhen-feng, Feng Deng-guo, Li Bao. A protocol of comparing information without leaking[J]. Journal of Software, 2004, 15(3): 421 – 427. (in Chinese)

[12] 肖倩,罗守山,陈萍,吴波.半诚实模型下安全多方排序问题的研究[J].电子学报,2008,36(4):709 – 714.
Xiao Qian, Luo Shou-shan, Chen Ping, Wu Bo. Research on the problem of secure multi-party ranking under semi-honest model[J]. Acta Electronica Sinica, 2008, 36(4): 709 – 714. (in Chinese)

[13] 刘文,罗守山,陈萍.基于 El Gamal 密码体制解决安全多方多数据排序问题[J].通信学报,2007,28(10):1 – 5.
Liu Wen, Luo Shou-shan, Chen Ping. Solution for secure multi-party multi-data ranking problem based on El Gamal encryption[J]. Journal on Communications, 2007, 28(10): 1 – 5. (in Chinese)

[14] 邱梅,罗守山,刘文,陈萍.利用 RSA 密码体制解决安全多方多数据排序问题[J].电子学报,2009,37(5):1119 –

1123.
Qiu Mei, Luo Shou-shan, Chen Ping. A solution of secure multi-party multi-data ranking problem based on RSA encryption scheme. Acta Electronica Sinica, 2009, 37(5): 1119 – 1123. (in Chinese)
[15] Cormen T H, Leiserson C E el al. Introduction to Algorithms [M]. Second Edition. Massachusetts: The MIT Press, 2001.
[16] 李顺东,王顺道,戴一奇,罗平. 两集合相等的多方保密计算[J]. 中国科学 F 辑:信息科学,2009,39(3):305 – 310.
Li Shun-dong, Wang Shun-dao, Dai Yi-qi, Luo Ping. Multi-party secure computation for comparing two sets[J]. Science in China Series F: Information Sciences, 2009, 39(3): 305 – 310. (in Chinese)

作者简介

刘 文 女,1982 年生于湖南湘潭,2009 年在北京邮电大学获工学博士学位,现为中国传媒大学讲师. 主要研究方向为信息安全,安全多方计算,数字版权管理.
E-mail: lw8206@gmail.com

王永滨 男,1985 年、1988 年 6 月和 2003 年分别在北京理工大、北京理工大学和河北工业大学获理学学士、理学硕士学位和工学博士学位. 2006 年 12 月解放军信息工程大学信息与通信工程专业(国家数字交换系统工程技术研究中心)博士后流动站出站. 现为中国传媒大学教授,博士生导师,计算机学院院长,主要从事网络新媒体技术、广播电视与新媒体信息安全、智能信息处理等方面的研究工作.