# 安全两方向量优势统计协议及其应用

刘 文[1,2],罗守山[3,4,5],王永滨[1,2]

(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;
3.北京邮电大学网络与交换技术国家重点实验室信息安全中心,北京 100876;4.北京邮电大学网络与信息攻防技术教育部重点实验室,北京 100876;5.灾备技术国家工程实验室,北京 100876)

**摘 要:** 安全两方向量优势统计问题是百万富翁问题的推广问题,用于两方在不泄漏自己保密向量信息的前提下统计出满足大于关系的分量的数目.本文在半诚实模型下利用加同态加密体制解决了安全两方向量优势统计问题,分析了该解决方案的正确性,安全性和复杂性;利用该优势统计协议设计了一个安全两方向量分量和排序协议,并且将设计的安全两方向量分量和排序协议应用于安全生成最小树图形算法中.

**关键词:** 安全两方计算; 安全两方向量优势统计问题; 安全两方向量分量和排序协议; 安全生成最小树

**中图分类号:** TN309 **文献标识码:** A **文章编号:** 0372-2112 (2010) 11-2573-05

# Secure Two-Party Vector Dominance Statistic Protocol and Its Applications

LIU Wen[1,2], LUO Shou-shan[3,4,5], WANG Yong-bin[1,2]

(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*;
3. *Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*; 4. *Key Laboratory of Network and Information Attack & Defense Technology of MOE, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*; 5. *National Engineering Laboratory for Disaster Backup and Recovery, Beijing* 100876, *China*)

**Abstract:** Secure two-party vector dominance statistic problem is a problem generalized from the millionaires' problem, which can be used by two party to get the number of $a_i > b_i$ without leaking further information. A secure two-party vector dominance statistic protocol in semi-honest model is presented based on the additive homomorphic encryption. The correctness, security and complexity of the protocol are analyzed. A secure components sum of two vectors ranking protocol is proposed based on the dominance statistic protocol and the ranking protocol is also applied in the secure minimum spanning trees algorithm.

**Key words:** secure two-party computation; secure two-party vector dominance statistic problem; secure components sum of two vectors ranking protocol; secure minimum spanning trees algorithm

## 1 引言

在文献[1]中,华裔计算机科学家、图灵奖获得者姚启智教授提出了这样一个问题:两个百万富翁 Alice 和 Bob 想知道他们两个人谁更加富有,但他们都不想让对方知道自己财富的任何信息,这就是百万富翁问题.百万富翁问题是安全多方计算中一个基本问题.近年来人们针对该问题设计出了各种能够提高效率的协议[2,8],并且将该问题引申为一系列的特殊的安全多方计算问题.在文献[9]中,Goldreich, Micali 和 Wigderson 将安全两方计算问题扩展为安全多方计算问题;在文献[10]中,Du 将问题引申为安全两方向量统治问题;在文献[11]中,秦静等人将问题引申为安全两方比较协议;在文献[12]中,肖倩等人将问题引申为安全多方排序问题;在文献[13]中,作者等人将问题扩展为安全多方多数据排序问题;在文献[14]中,邱梅等人在文献[13]的基础上提出了一种新的解决方案.

本文将百万富翁问题引申为这样一个问题:假设 Alice 拥有一个保密的 $l$ 维向量 $\boldsymbol{V}_A=(a_1,a_2,\cdots,a_l)$,Bob 拥有一个保密的 $l$ 维向量 $\boldsymbol{V}_B=(b_1,b_2,\cdots,b_l)$,其中 $a_i$, $b_i(i=1,2,\cdots,l)$均为正整数.两方希望在不泄漏自己保密向量信息的基础上统计出 $a_i>b_i(i=1,2,\cdots,l)$的数目,我们将这个问题称为安全两方向量优势统计问题.

安全两方向量优势统计协议可以应用到图形算法的安全计算中,比如安全最小生成树算法以及安全求解最短路径算法.

收稿日期:2009-07-30;修回日期:2010-04-19
基金项目:2009 年北京市文化创意产业发展专项资金;国家"211 工程"项目;校级工科规划项目(No.XNG0925)

## 2 预备知识

**定义 1**(半诚实模型) 参与的两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一参与方可能会保留所有能搜集到的关于另一参与方的信息,以期望在协议结束后推断出另一参与方的输入信息.本文假设参与协议的两个参与方都是"半诚实的".

**定义 2**(基于语义安全的加同态加密体制) 设加密算法为 $E(\cdot)$,相应的解密算法为 $D(\cdot)$,其中加密密钥公开,解密密钥保密.明文空间 $M\subseteq Z$,$E(\cdot)$满足下述两个性质:

(1)语义安全性:对任意两个消息 $m_1, m_2\in M$,不存在任何多项式时间算法区分 $E(m_1), E(m_2)$.

(2)加法同态性:对任意消息 $m_1, m_2\in M$,任意 $k\in Z$,若 $m_1+m_2\in M$ 且 $km_1\in M$,则 $D(E(m_1)E(m_2))=m_1+m_2$ 且 $D(E(m_1)^k)=km_1$.

## 3 安全两方向量优势统计协议

### 3.1 协议的描述

假设 Alice 和 Bob 分别拥有一个保密的 $l$ 维向量 $\boldsymbol{V}_A=(a_1,a_2,\cdots,a_l)$和 $\boldsymbol{V}_B=(b_1,b_2,\cdots,b_l)$(以下只考虑 $a_1,a_2,\cdots,a_l,b_1,b_2,\cdots,b_l$ 为正整数的情况),两方希望在不泄漏自己保密向量信息的基础上统计出 $a_i>b_i(i=1,2,\cdots,l)$的数目 $N_>$.

在该协议的执行过程中,Alice 和 Bob 在茫然第三方 Calvin 的帮助下,利用具有加法同态性质的加密体制分别对 $\boldsymbol{V}_A,\boldsymbol{V}_B$ 的分量 $a_i,b_i$ 进行两次"伪装",经过"伪装"之后可以很方便地判断出 $\boldsymbol{V}_A,\boldsymbol{V}_B$ 各个分量 $a_i,b_i$ 之间的 $>$、$<$、$=$ 关系.利用判断出来的关系信息对向量 $\boldsymbol{V}=(v_1,v_2,\cdots,v_n)$中的分量 $v_i$ 进行赋值,其中如果 $a_i>b_i$,则 $v_i=1$;否则 $v_i=0$;而向量 $\boldsymbol{V}$ 的各个分量相加就统计出了 $a_i>b_i(i=1,2,\cdots,l)$的数目 $N_>$.

**协议 3.1** 安全两方向量优势统计协议

输入:Alice 和 Bob 分别拥有一个保密的 $l$ 维向量 $\boldsymbol{V}_A=(a_1,a_2,\cdots,a_l)$和 $\boldsymbol{V}_B=(b_1,b_2,\cdots,b_l)$(其中 $a_1,a_2,\cdots,a_l,b_1,b_2,\cdots,b_l$ 都为正整数),加、解密算法 $E(\cdot)$,$D(\cdot)$满足基于语义安全的加同态性,由 Alice 产生该算法的公私钥对;

输出:$a_i>b_i(i=1,2,\cdots,l)$的个数 $N_>$;

中间变量:$v^1\in\{0,1\}$,$v^2\in\{0,1\}$,$\boldsymbol{V}=(v_1,\cdots,v_l)$ $(v_{i'}\in\{0,1\},i'=1,2,\cdots,l)$;

初始化:$v^1=0,v^2=0,V=(0,\cdots,0)$;

茫然第三方:Calvin.

协议执行过程如下:

(1)对于 $i=1,2,\cdots,l$,Alice 用自己的公钥计算:$c_i=E(a_i)$.Alice 将序列$(c_1,\cdots,c_l)$发送给 Bob.

(2)对于 $i=1,2,\cdots,l$:

(2.1)Bob 首先随机选择两组整数:$u_i^1,v_i^1,w_i^1$ 和 $u_i^2,v_i^2,w_i^2$,这些数据满足如下条件:$u_i^1>0,u_i^2>0,|v_i^1-w_i^1|<u_i^1,|v_i^2-w_i^2|<u_i^2$,且$(v_i^2-w_i^2)(v_i^1-w_i^1)<0$;

(2.2)利用 Alice 的公钥计算:$(x_i^1,y_i^1)=(c_i^{u_i^1}E(v_i^1),E(u_i^1b_i+w_i^1))$,$(x_i^2,y_i^2)=(c_i^{u_i^2}E(v_i^2),E(u_i^2b_i+w_i^2))$.

(3)Bob 将计算所得的数据组成一个序列:$(e_1,\cdots,e_l)=(((x_1^1,y_1^1),(x_1^2,y_1^2)),\cdots,((x_l^1,y_l^1),(x_l^2,y_l^2)))$,发送给 Calvin.Calvin 对该序列进行置换运算 $\pi$ 仅打乱序列中数据的次序(该置换运算对 Alice 和 Bob 是保密的),并将置换后得到的新序列 $\pi((e_1,\cdots,e_l))=(e_1^\pi,\cdots,e_l^\pi)=\{((x_i^{1\pi},y_i^{1\pi}),(x_i^{2\pi},y_i^{2\pi}))\mid i'=1,2,\cdots,l\}$ 发送给 Alice.

(4)对于 $i'=1,2,\cdots,l$:

(4.1)Alice 计算:

$(D(x_{i'}^{1\pi}),D(y_{i'}^{1\pi}))=(u_{i'}^{1\pi}a_{i'}^\pi+v_{i'}^{1\pi},u_{i'}^{1\pi}b_{i'}^\pi+w_{i'}^{1\pi})$,

$(D(x_{i'}^{2\pi}),D(y_{i'}^{2\pi}))=(u_{i'}^{2\pi}a_{i'}^\pi+v_{i'}^{2\pi},u_{i'}^{2\pi}b_{i'}^\pi+w_{i'}^{2\pi})$.

(4.2)Alice 比较 $D(x_{i'}^{1\pi}),D(y_{i'}^{1\pi})$的大小关系和 $D(x_{i'}^{2\pi}),D(y_{i'}^{2\pi})$的大小关系:

如果 $D(x_{i'}^{j\pi})>D(y_{i'}^{j\pi})$,则 $v^j=1$;

如果 $D(x_{i'}^{j\pi})<D(y_{i'}^{j\pi})$,则 $v^j=0$;其中 $j=1,2$.

(4.3)Alice 计算 $v_{i'}=\min\{v^1,v^2\}$.

(5)Alice 将向量 $V=(v_{1'},\cdots,v_{l'})$ $(v_{i'}\in\{0,1\},i'=1,2,\cdots,l)$发送给 Bob;此时 $N_>=\sum_{i'=1}^{l}v_{i'}$.

### 3.2 协议的性能分析

本节分析安全两方向量优势统计协议正确性、安全性和效率.

#### 3.2.1 正确性分析

**定理 3.2.1** 在半诚实模型下,安全两方向量优势统计协议是正确的,即 $a_{i'}^\pi>b_{i'}^\pi(i'=1,2,\cdots,l)$当且仅当 $v^1=1,v^2=1$.

**证明** 我们逐一考虑 $v^1,v^2$ 取值的情况:

当 $v^1=1,v^2=0$ 时,$D(x_{i'}^{1\pi})>D(y_{i'}^{1\pi})$,$D(x_{i'}^{2\pi})<D(y_{i'}^{2\pi})$,则 $u_{i'}^{1\pi}(a_{i'}^\pi-b_{i'}^\pi)+(v_{i'}^{1\pi}-w_{i'}^{1\pi})>0$,$u_{i'}^{2\pi}(a_{i'}^\pi-b_{i'}^\pi)+(v_{i'}^{2\pi}-w_{i'}^{2\pi})<0$.由 $|v_{i'}^{1\pi}-w_{i'}^{1\pi}|<u_{i'}^{1\pi}$,$|v_{i'}^{2\pi}-w_{i'}^{2\pi}|<u_{i'}^{2\pi}$,$(v_{i'}^{2\pi}-w_{i'}^{2\pi})(v_{i'}^{1\pi}-w_{i'}^{1\pi})<0$,可知 $a_{i'}^\pi=b_{i'}^\pi$.同理可证当 $v^1=0,v^2=1$ 时,$a_{i'}^\pi=b_{i'}^\pi$;当 $v^1=1,v^2=1$ 时,$a_{i'}^\pi>b_{i'}^\pi$;当 $v^1=0,v^2=0$ 时,$a_{i'}^\pi<b_{i'}^\pi$.综上所述,协议可以正确比较出各分量的 $>$、$<$、$=$,将所有满足 $>$ 关系的向量数目相加就是我们所希望得到的结果.

#### 3.2.2 安全性分析

**定理 3.2.2**　在半诚实模型下,基于加同态密码体制的语义安全性,安全两方向量优势统计协议是安全的.

**证明**

(1)Bob 接收到序列$(c_1,\cdots,c_l)$后,因为 $E(\cdot)$是语义安全的,所以 Bob 无法从中获得任何有关 $l$ 维向量 $\boldsymbol{V}_A=(a_1,a_2,\cdots,a_l)$的信息.

(2)Calvin 接收到序列$(e_1,\cdots,e_l)=(((x_1^1,y_1^1),(x_1^2,y_1^2)),\cdots,((x_l^1,y_l^1),(x_l^2,y_l^2)))$,因为 $E(\cdot)$是语义安全的,所以 Calvin 无法从中获得任何有关 $l$ 维向量 $\boldsymbol{V}_A=(a_1,a_2,\cdots,a_l)$和 $\boldsymbol{V}_B=(b_1,b_2,\cdots,b_l)$($a_1,a_2,\cdots,a_l,b_1,b_2,\cdots,b_l$ 为正整数的情况)的信息.

(3)Alice 接收并解密$(D(x_{i'}^{1\pi}),D(y_{i'}^{1\pi}))=(u_{i'}^{1\pi}a_{i'}^{\pi}+v_{i'}^{1\pi},u_{i'}^{1\pi}b_{i'}^{\pi}+w_{i'}^{1\pi})$后,$D(x_{i'}^{1\pi})-D(y_{i'}^{1\pi})=u_{i'}^{1\pi}(a_{i'}^{\pi}-b_{i'}^{\pi})+(v_{i'}^{1\pi}-w_{i'}^{1\pi})$,由 $u_{i'}^{1\pi},(v_{i'}^{1\pi}-w_{i'}^{1\pi})$对于 Alice 来说未知,她无法从 $D(x_{i'}^{1\pi})-D(y_{i'}^{1\pi})$中解出 $a_{i'}^{\pi}-b_{i'}^{\pi}$,进而 Alice 不知道 $b_{i'}^{\pi}$的取值,即使$(v_{i'}^{1\pi}-w_{i'}^{1\pi})=0$,由于 $D(x_{i'}^{1\pi})-D(y_{i'}^{1\pi})=u_{i'}^{1\pi}\times(a_{i'}^{\pi}-b_{i'}^{\pi})$.要求出$(a_{i'}^{\pi}-b_{i'}^{\pi})$相当于对大整数 $D(x_{i'}^{1\pi})-D(y_{i'}^{1\pi})$进行分解,因此它是计算上安全的.Alice 接收并解密$(D(x_{i'}^{2\pi}),D(y_{i'}^{2\pi}))=(u_{i'}^{2\pi}a_{i'}^{\pi}+v_{i'}^{2\pi},u_{i'}^{2\pi}b_{i'}^{\pi}+w_{i'}^{2\pi})$后同理也不知道 $b_{i'}^{\pi}$的取值为多少.如果 Alice 将两次得到的信息联立起来,有 6 个未知数,只有 4 个已知条件,所以她无法从中解出 $b_{i'}^{\pi}$的值.

(4)Alice 接收的序列 $\pi((e_1,\cdots,e_l))=(e_{1'}^{\pi},\cdots,e_{l'}^{\pi})=\{((x_{i'}^{1\pi},y_{i'}^{1\pi}),(x_{i'}^{2\pi},y_{i'}^{2\pi}))\mid i'=1,2,\cdots,l\}$是变换过顺序的,协议结束之后所以 Alice 仅知道 $a_i>b_i(i=1,2,\cdots,l)$的个数 $N_>$,而无法知道具体的哪一些位置上的 $a_i>b_i(i=1,2,\cdots,l)$.

### 3.2.3　效率分析

**定理 3.2.3**　在半诚实模型下,基于加同态密码体制的安全两方向量优势统计协议的计算复杂度为 $9nkl+\sum_{i=1}^{l}(u_i^1+u_i^2+4)$模乘运算,通信复杂度为$(5nkl+l)$bits.

**证明**　设加密算法的安全参数为 $k$,各个向量具有 $l$ 个分量,各个分量的长度为 $n$bits.

(计算复杂度):在第一步中 Alice 使用公钥进行了 $l$ 次加密;在第二步中 Bob 使用公钥进行了 $4l$ 次加密、$\sum_{i=1}^{l}(u_i^1+u_i^2+2)$次乘法运算;第四步中 Alice 使用私钥进行了 $4l$ 次解密.所以本协议的计算复杂度为 $8nkl+\sum_{i=1}^{l}(u_i^1+u_i^2+2)$模乘运算.

(通信复杂度):在第一步中 Alice 将$(c_1,\cdots,c_l)$发送给 Bob;在第三步中 Bob 将$(e_1,\cdots,e_l)=(((x_1^1,y_1^1),(x_1^2,y_1^2)),\cdots,((x_l^1,y_l^1),(x_l^2,y_l^2)))$发送给 Calvin;Calvin 将 $\pi((e_1,\cdots,e_l))$发送给 Alice;在第三步中 Alice 将 $V$ 发送给 Bob.所以本协议的通信复杂度为$(9nkl+l)$bits.

## 4　安全两方向量分量和排序问题

本节我们首先提出了安全两方向量分量和排序问题,然后利用安全两方向量优势统计协议解决提出的问题.

### 4.1　问题描述

假设 Alice 和 Bob 分别拥有一个保密的 $l$ 维向量 $\boldsymbol{V}_A=(a_1,a_2,\cdots,a_l)$和 $\boldsymbol{V}_B=(b_1,b_2,\cdots,b_l)$,两方希望在不泄漏自己保密向量信息的基础上确定各分量和$(a_i+b_i)(i=1,\cdots,l)$在其和向量 $\boldsymbol{V}_A+\boldsymbol{V}_B=((a_1+b_1),\cdots,(a_l+b_l))$中个分量按从小到大排序后得到序列中的位置.

### 4.2　安全两方向量分量和排序协议

协议执行过程如下:

对于每一个 $i=1,2,\cdots,l$:

(1)Alice 计算向量:$\boldsymbol{V}_a=(a_i-a_1,\cdots,a_i-a_i,\cdots,a_i-a_l)$;

Bob 计算向量:$\boldsymbol{V}_b=(b_1-b_i,\cdots,b_i-b_i,\cdots,b_l-b_i)$;

(2)Alice 和 Bob 使用安全两方向量优势统计协议计算得 $N_>$,计算$(a_i+b_i)$的排序位置为 $r_i=N_>+1$.

协议的正确性分析:我们的协议需要计算$(a_i+b_i)$在序$(a_1+b_1),(a_2+b_2),\cdots,(a_l+b_l)$中按从小到大顺序排成的序列中的位置,即需要计算出序列中比$(a_i+b_i)$小的数.如果$(a_i+b_i)>(a_k+b_k)(k=1,\cdots,i-1,i+1,\cdots,l)$则$(a_i-a_k)>(b_k-b_i)$,$(a_i-a_k)$由 Alice 拥有,$(b_k-b_i)$由 Bob 拥有,即可以将问题转换为安全统计两方向量 $\boldsymbol{V}_a=(a_i-a_1,\cdots,\cdots,a_i-a_i,\cdots,a_i-a_l)$,$\boldsymbol{V}_b=(b_1-b_i,b_i-b_i,\cdots,b_l-b_i)$优势的问题从而确定$(a_i+b_i)$在从小到大顺序排成的序列中的位置 $r_i$.

该协议的安全性依赖与安全两方向量优势统计协议的安全性.

该协议的计算复杂度为 $8nkl+\sum_{i=1}^{l}(u_i^1+u_i^2+2)l$模乘运算;通信复杂度为$(9nkl+l)l$bits.

## 5　安全生成最小树算法

本节我们首先提出了安全生成最小树问题,然后通过对 Kursal 算法[15]加入安全两方向量分量和排序协议提出了一个安全生成最小树算法.

### 5.1　问题描述

假设 Alice 拥有无向赋权连通图 $G_1=(V_1,E_1,w_1)$,Bob 拥有无向赋权连通图 $G_2=(V_2,E_2,w_2)$,其中 $V_1=V_2=V,E_1=E_2=E,w_1(e_i)$和 $w_2(e_i)$为 $G_1$ 和 $G_2$ 的权重函数.两个子图可以合成为一个无向赋权连通图 $G,G=(V,E,w)$,其中 $w(e_i)=w_1(e_i)+w_2(e_i)$为 $G$ 的权重函数.Alice 和 Bob 两人想在不泄漏自己的子图信息的

情况下得到合成图 $G$ 的最小生成树.

### 5.2 安全生成最小树算法

最小生成树问题是找出可使整个图连通的权值和最小的边的子集.Kursal 算法能够产生一个图的最小生成树,我们设计的协议利用 Kursal 算法安全生成最小生成树.该算法的执行过程如下:

初始化:$A=\varnothing$;对于 $G$ 中每一个点 $v_i\in V$ 生成一个集合 $Set_{vi}=\{v_i\}$;

(1)对 $|E|$ 维向量 $(w_1(e_1),\cdots,w_1(e_i),\cdots,w_1(e_{|E|}))$ 和 $(w_2(e_1),\cdots,w_2(e_i),\cdots,w_2(e_{|E|}))$ 使用安全两方向量分量和排序协议确定 $w(e_i)=w_1(e_i)+w_2(e_i)(i=1,\cdots,|E|)$ 在 $w(e_1),\cdots,w(e_{|E|})$ 中按从小到大顺序排序后得到序列中的位置 $r_i$;

(2)按照图中所有边 $e_1,e_2,\cdots,e_{|E|}$ 的排序位置 $r_i=1,2,\cdots,|E|$ 顺序取出边 $(v_i,v_j)\in E$:如果 $Set_{vi}\neq Set_{vj}$,则 $A=A\cup\{(v_i,v_j)\}$,$UNION(v_i,v_j)$;

(3)完成以上步骤后 $A$ 为该无向赋权连通图 $G$ 的一棵最小生成树.

该算法的正确性和安全性依赖与安全两方向量分量和排序协议的正确性和安全性.

该算法的计算复杂度为 $8nkl+\sum_{i=1}^{l}(u_i^1+u_i^2+2)|E|$ 模乘运算;通信复杂度 $(9nkl+l)|E|$ bits.

## 6 结论

本文设计了一个半诚实模型下的基于加法同态公钥加密体制的安全两方向量优势统计协议,并且详细地分析了统计协议的安全性和复杂性;利用安全两方向量优势统计协议设计了一个安全两方向量分量和排序协议;最后利用设计的排序协议帮助半诚实两方对他们的无向赋权连通子图的合成图安全地生成最小树.

需要指出的是我们所设计的安全两方向量优势统计协议是通过多次执行一个一次就能将两个向量的正整数分量之间的"相等"关系单独区分出来的协议来实现的.并且通过引入茫然第三方进行置换运算使得在协议结束之后参与协议的两方都仅知道两个向量各个分量中满足 $a_i>b_i(i=1,2,\cdots,l)$ 的个数 $N_>$,而无法知道具体的哪一些位置上的 $a_i>b_i(i=1,2,\cdots,l)$,使得协议具有公平性.

在以后的工作中,我们希望能够利用文献[8]中提出的基于对称加密体制的安全两方比较协议的实现执行一次协议将两个正整数之间的"相等"关系单独区分出来的功能,进一步提高协议的效率.将该协议推广到恶意模型下或者将其应用于其他的图形算法的安全计算中也是一个值得研究的方向.

**参考文献:**


[1] A Yao. 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] C Cachin. 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] H Y Lin, W G Tzeng. 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: Springer-Verlag, 2005. 456 – 466.

[4] R Fagin, M Naor, P Winkler. 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] I Ioannidis, A Grama. An efficient protocol for Yao's millionaires' problem[A]. In Proceedings of the 36th Annual Hawaii International Conference on System Sciences[C]. Los Alamitos: IEEE Computer Society Press, 2003. 205.

[8] Shundong Li, Daoshun Wang, Yiqi Dai, Ping Luo. Symmetric cryptographic solution to yao's millionaires' problem and an evaluation of secure multiparty computations[J]. Information Sciences. 2008, 178(1): 244 – 255.

[9] O Goldreich, S Micali, A Wigderson. 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] W L Du. A Study of Several Specific Secure Two-party Computation Problems, Ph. D. Thesis[D]. Purdue University, 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. Re- search 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 of China Institute of 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[J]. Acta Electronica Sinica,2009,37(5):1119 – 1123.(in Chinese)
[15] T H Cormen,C E Leiserson el al. Introduction to Algorithms[M]. Second Edition. Massachusetts: The MIT Press,2001.

**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@gamil.com

**罗守山**　男,1962 年生于北京市.1985 年、1994 年和 2001 年分别在北京师范大学、北京邮电大学和北京邮电大学获理学学士、理学硕士学位和工学博士学位.现为北京邮电大学教授,博士生导师,主要从事信息安全、密码学等方面的研究工作.

**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.