基于编码和同态加密的高效SMP方案

唐 璇 仲 红 石润华 崔 杰

(安徽大学计算机科学与技术学院 合肥 230601)

摘 要 社会主义百万富翁问题(SMP)即是保密地比较数据是否相等的问题,其解决方案可以作为很多应用系统的基础协议。首先,提出一种对保密数据进行编码的新方案。然后,基于该编码方案和ElGamal同态加密算法,设计一个新的方案来解决社会主义百万富翁问题,并分析方案的正确性、安全性和效率。最后,将本方案与其它协议进行了比较,结果表明所提出的方案具有更高的效率。

关键词 安全多方计算,社会主义百万富翁问题,编码,同态加密

中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.1.041

Efficient Solution to SMP Based on Coding and Homomorphic Encryption

TANG Xuan ZHONG Hong SHI Run-hua CUI Jie

(School of Computer Science and Technology, Anhui University, Hefei 230601, China)

Abstract Socialist millionaires' problem(SMP) is the problem of two millionaires wanting to know whether they are equally rich, whose solutions can be used to build the basic protocol in many application systems. Firstly, we presented a new encoding scheme to encode private data. And then based on this encoding scheme and the ElGamal homomorphic encryption algorithm, we designed a creative scheme for socialist millionaires' problem. The validity, security and efficiency were analyzed. Finally, the comparison of protocols indicates that our scheme has high efficiency.

Keywords Secure multi-party computation, Socialist millionaires' problem(SMP), Encoding, Homomorphic encryption

1 引言

随着网络及分布式计算的飞速发展,用户之间的合作越来越多。为保护用户各自的数据安全,安全多方计算应运而生。目前安全多方计算主要研究的关于数据比较的问题有:百万富翁问题[1-9]、社会主义百万富翁问题[10-17]、安全多方排序问题等。其中,社会主义百万富翁问题简称SMP(Socialist Millionaires' Problem)[10],即保密地比较数据是否相等问题,它是百万富翁问题的变形问题。该类问题的解决方案可以作为网上拍卖、电子选举、身份认证等应用系统的基本协议,具有广阔的应用背景。

1.1 相关工作

图灵奖得主Andrew C. Yao较早开始研究安全多方计算,1982年他在文献[1]中提出了姚氏百万富翁问题,即两个富翁如何在不暴露各自财富的情况下比较谁更富有。目前对百万富翁问题的研究主要借助于同态加密体制、不经意传输协议、不可信第三方等方法来解决。特别是在文献[6]中,Lin等人设计了一种特殊编码,通过对保密输入进行0-编码和1-编码,并且基于ElGamal乘法同态加密算法,将百万富翁问题转化为判断集合是否相交问题,是一个非常新颖的百万富翁协议。本文也是采用编码和同态加密算法,从而将要解决的问题进行了转化。但解决的问题和采用的编码方案都不同。文献[6]解决的是百万富翁问题,本文解决的是保密地比较数据是否相等问题,即社会主义百万富翁问题。本文设计了一种新的编码方案(二叉树编码),通过对保密输入进行编码,并基于ElGamal乘法同态加密算法,将保密地比较数据是否相等转化为二进制位置的一种特殊对应问题,是一个新颖的社会主义百万富翁问题解决方案。

社会主义百万富翁问题是百万富翁问题的变形。目前对社会主义百万富翁问题的研究方法不一,主要基于零知识证明、加法同态加密及设计的特殊函数,或者借助于第三方等。目前还没有采用乘法同态加密体制的社会主义百万富翁协议。但在实际中,乘法同态加密方案比加法同态加密方案更高效,会节省计算时间和通信带宽[6]。本文的方案就是基于乘法同态加密方案的。在文献[10]中,Fagin R等人对利用随机置换、特殊设备等方法解决该变形问题的多种方案进行了总结;在文献[11]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[12]中,Boudot F等人给出了基于离散对数DL-DH-DDH假设和零知识证明的社会主义百万富翁协议,该协议

到稿日期:2014-12-30 返修日期:2015-03-27 本文受国家自然科学基金项目(61173188,61173187),教育部博士点基金项目(20133401110004),安徽省科技计划(科技强警)项目(1401b042015),安徽省高校自然科学研究重点项目(KJ2013A017)资助。

唐 璇 女,硕士生,主要研究方向为网络与信息安全;仲 红 女,教授,博士生导师,主要研究方向为分布式计算、网络与信息安全,E-mail:zhongh@mail.ustc.edu.cn;石润华 男,教授,主要研究方向为保护隐私的多方协作计算、量子密码,E-mail:hfsrh@sina.com;崔 杰 男,讲师,主要研究方向为网络与信息安全、WSN,E-mail:cvjxabcd@126.com。

需要O(k)次模指数运算，且具有公平性；在文献[13]中，秦静等人给出了基于 ϕ-隐藏假设和同态加密体制语义安全性假设的两方比较相等协议，协议借助茫然第三方；在文献[14]中，刘文等人给出了一种基于滑动窗口和交换加密函数解决SMP的新方案；在文献[15]中，肖倩等人将文献[8]中的一个常数复杂性的百万富翁协议推广，完成两方保密数据的比较；在文献[16]中，刘文等人将安全多方信息比较协议由两方推广到多方，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多方信息比较相等协议，但协议计算复杂度和通信复杂度较高。

1.2 本文贡献

本文在半诚实模型下提出一个新的解决社会主义百万富翁问题的方案。首先，提出了一种对保密数据进行编码的新方案，利用该编码方案对保密输入进行特殊编码(二叉树编码)。然后利用该编码方案和ElGamal同态加密算法，设计了一个新颖的SMP方案，并且分析了方案的正确性、安全性和复杂度。最后，与文献[15,16]中的方案进行比较，结果表明本文方案具有更高的效率。

2 预备知识

2.1 半诚实参与者

半诚实参与者在执行协议的过程中会完全按照协议规则和步骤来完成协议，但可能会通过更多的计算获得额外的信息，甚至将自己的输入和得到的输出结果泄露给攻击者。

但是，Goldreich[17]利用比特承诺和零知识证明理论设计的编译器，使得即使是恶意参与者也必须以半诚实方式参与协议的执行，否则就会被发现。

所以，本文仅研究在半诚实参与者条件下的安全多方保密计算协议是具有实际意义的。

2.2 计算不可区分性

SMP是一个安全两方计算问题，参与者 Alice 和 Bob 共同执行协议保密计算函数 f，函数 $f(x,y)=1$ 当且仅当 $x=y$，其中，x 是 Alice 的保密输入，y 是 Bob 的保密输入。协议应满足下列要求：

(1)参与方 Alice 和 Bob 都是概率多项式时间的图灵机并通过安全信道交互，这里假定 Alice 和 Bob 都是半诚实参与者；

(2)正确性：协议执行后，Alice 返回 1 当且仅当 $x=y$；

(3)(计算不可区分性)对于函数 f，我们说保密地计算 $f(x,y)$，要求存在概率多项式时间算法 S_1 和 S_2，使得：

$$\{(S_1(x,f_1(x,y)),f_2(x,y))\}_{x,y}\overset{c}{\equiv}\{(view_1^{\Pi}(x,y),output_2^{\Pi}(x,y))\}_{x,y} \tag{1}$$

$$\{(f_1(x,y),S_2(y,f_2(x,y)))\}_{x,y}\overset{c}{\equiv}\{(output_1^{\Pi}(x,y),view_2^{\Pi}(x,y))\}_{x,y} \tag{2}$$

两个等式成立。其中，$\overset{c}{\equiv}$表示计算上不可区分，$f=(f_1,f_2)$：$\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^*\times\{0,1\}^*$ 是一个概率多项式函数，S_1，S_2 称为模拟器。

2.3 ElGamal同态加密算法

2.3.1 同态加密

同态加密的特殊性质使得我们可以对密文进行某些运算，且与对明文进行同样运算得到的结果相同。

乘法同态的加密方案满足：

$E(m_1)\otimes E(m_2)=E(m_1\times m_2)$

加法同态的加密方案满足：

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

向量化的加密方案满足 $c=E(km)$ 可以随机映射到密文 $E(m^k)$ 或 $c'=E(km)$，k 为随机数。

2.3.2 ElGamal同态加密算法

ElGamal加密方案是具有向量属性的乘法同态加密方案。令 $p=2q+1$，p、q 为素数，使 G_q 是 QR_p 的子集，g 是 G_q 的生成元。公钥为 $h=g^{-a}$，$a\in Z_q$，私钥为 a。ElGamal同态加密算法如图1所示。

加密　对明文 $m\in G_q$，加密 $E(m)=(a,b)=(g^r,mh^r)$，其中 $r\in Z_q$。

解密　对密文 $c=(a,b)$，解密 $D(c)=b\times a^a=m$。

向量化　计算 $c'=E(m^k)=(a^k,b^k)$，$k\in Z_q$，向量化操作使得 c' 从随机对中无法区分。

图1　ElGamal同态加密算法

ElGamal同态加密算法是乘法同态的，其安全性基于DDH假设，即要区分如下是计算不可行的。

$D=(g^a,g^b,g^{ab})$，$a\in Z_q$，$b\in Z_q$

$R=(g^a,g^b,g^c)$，$a\in Z_q$，$b\in Z_q$，$c\in Z_q$

另外，如果仅需要加密的随机数，无需先选择随机数再对其进行加密，否则将产生大量加密开销。可以选择随机对 $c=(a,b)\in G_q^2$，其为对随机数的加密[6]。此方法可以节省加密开销，提高协议的效率。

3 编码与解决方案

3.1 社会主义百万富翁问题

A、B双方各有一个消息，如何在不暴露各自消息的前提下比较出二者的消息是否一致，称为社会主义百万富翁问题。可将该问题数学化表示为：A有数值 a，B有数值 b，能否安全地比较 $a=b$，即保密地比较数据是否相等。这里，安全的含义是指除最后结果($a\neq b$ 或 $a=b$)以外，不泄漏各自的任何信息。

3.2 二叉树编码

本文方案的主要思想就是将保密地比较数据相等问题转化为二进制位置的某种特殊对应问题。这里首先定义对保密数据进行编码的方式，即二叉树编码(因为编码过程符合二叉树的构造及遍历，得此命名)。下面通过二叉树来解释说明。

定义1　将长度为 n 位的二进制串 t 扩充编码得到长度为 $2n+1$ 位的二进制串 T，称为二叉树编码，即将 $t=t_nt_{n-1}\cdots t_1\in\{0,1\}_n$ 进行二叉树编码得到 $T=T_{2n+1}T_{2n}\cdots T_1$。其中，对于 $T_i(1\leqslant i\leqslant 2n+1)$：

$$T_i=\begin{cases}t_j, & 1\leqslant j\leqslant n\\ \triangle, & \triangle\text{为要填充的数}\end{cases}$$

二叉树构造：对 t 的每一位 $t_i(1\leqslant i\leqslant n)$，从 t_n 开始扩展节点直到 t_1，完成二叉树构造。

令 t_n 为二叉树根节点。首先扩展 t_n，若 $t_{n-1}=1$，则 t_{n-1} 扩展为 t_n 的左节点，且令 t_n 的右节点为△；反之，若 $t_{n-1}=0$，则 t_{n-1} 扩展为 t_n 的右节点，且令 t_n 的左节点为填充的△(填充的△将在之后的具体协议中给出值的定义)。

依此类推，扩展每一个节点 t_i，若 $t_{i-1}=1$，则 t_{i-1} 扩展为 t_i 的左节点，且令 t_i 的右节点为△；反之，若 $t_{i-1}=0$，则 t_{i-1} 扩

展为 t_i 的右节点，且令 t_i 的左节点为填充的△。

也就是说，每次扩展某个节点时，采取遇 1 向左、遇 0 向右的方式扩展为此节点的左(右)节点，并填充一个△在右(左)节点。对于最后一位 t_1，则直接令其左、右节点均是填充的△，因此整个二叉树构造完成时将填充 $n+1$ 个△。

编码结果：遍历二叉树即得到二叉树编码的结果。方便起见，按照先序的方式进行遍历，得 $2n+1$ 位二进制串(包括原有的 n 位，及 $n+1$ 个填充的△)，得二叉树编码的结果。

例 1　假设 $x=53=110101_2$，对 x 构造二叉树，如图 2 所示。

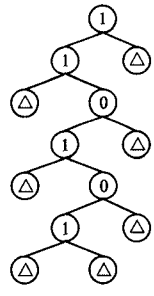

图 2　对 $x=53$ 构造二叉树

例 2　假设 $y=55=110111_2$，对 y 构造二叉树，如图 3 所示。

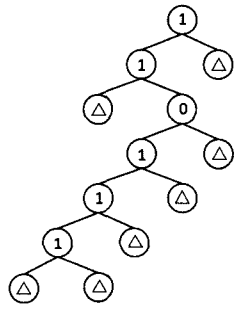

图 3　对 $y=55$ 构造二叉树

先序遍历 x 的二叉树，得二叉树编码 X：11△01△01△△△△△。

先序遍历 y 的二叉树，得二叉树编码 Y：11△0111△△△△△△。

观察 x 及 y，二者前 4 位二进制位对应相等，第 5 位开始不同；再观察 X 及 Y，发现 11△01 之后的二进制位顺序也开始不对应。本文的二叉树编码使得 x 及 y 对应二进制位的不等也体现在其二进制编码位置的不对应。

3.3　社会主义百万富翁问题的协议

3.3.1　协议描述

假设 Alice，Bob 分别拥有秘密输入 x,y，并分别用二进制表示为 $x=x_nx_{n-1}\cdots x_1$，$y=y_ny_{n-1}\cdots y_1$。他们希望在不泄露各自的秘密输入情况下比较出 x,y 是否相等。本文基于设计的二叉树编码及 ElGamal 同态加密设计了如下的协议，从而保密地比较二者数据是否相等。该协议更为新颖、高效和简洁。

输入：Alice 的保密输入 $x=x_nx_{n-1}\cdots x_1$，Bob 的保密输入 $y=y_ny_{n-1}\cdots y_1$

输出：x=y or x≠y

1. Alice 选择公私钥对(pk，sk)；

对于 x 的二叉树编码 $X=X_{2n+1}X_{2n}\cdots X_1$，若 $X_i=0$ 或 $1(1\leqslant i\leqslant 2n+1)$，令 $X_i=E(1)$，否则 $X_i=E(r_i)$，$r_i\in G_q$，共有 n+1 个 $E(r_i)$；然后将 X 发给 Bob。

2. 对于 y 的二叉树编码 $Y=Y_{2n+1}Y_{2n}\cdots Y_1$，执行：

for(j=1;j<=2n+1;j++){if(Y_j==0 ‖ Y_j==1) c=c * X_j;}

将 c 发给 Alice。

3. Alice 解密，D(c)=m，当且仅当 m=1 时，判断 x=y，否则 x≠y。Alice 将比较结果告诉 Bob。

3.3.2　协议分析

(1)安全性分析

(正确性)协议的正确性很容易证明。根据 3.2 节的定义及二叉树构造过程，若 $x=y$，则对应的二叉树编码 X 与 Y 的 $E(1)$ 与 $E(r_i)$ 位置完全对应，而 Bob 的计算是根据 Alice 相应的各 $E(1)$ 的位置来计算 Y 的，则必定会得到 c，对其解密后 $D(c)=1$；若 $x\neq y$，则必存在某 i 位使得 $x_i\neq y_i$，因而对应的二叉树编码的位置便从 i 位开始完全不对应，或者不完全对应，则对应的二叉树编码 X 与 Y 的 $E(1)$ 与 $E(r_i)$ 位置不是完全对应的，而 Bob 的计算是根据 Alice 相应的各 $E(1)$ 的位置来计算 Y 的，则必定会得到一个 c，解密后 $D(c)\neq 1$。

(安全性)目前，在安全多方计算领域，Goldreich 提出的安全性定义被广泛接受和使用。该定义可理解为，如果对于任意一个半诚实参与者，都可以直接从执行时自己的输入与协议的输出，通过单独模拟协议的执行过程而得到在执行协议过程中他所能得到的任何信息，那么协议就是安全的，即能够保证输入的隐私性[18]。也就是说，参与者所得到的所有信息都隐含在自己的输入与输出中，不会泄露额外的信息。

常用模拟器范例来证明上述过程，即如果一个多方计算协议能够这样进行模拟，参与者就不能从协议的执行中得到任何额外的信息，这样的多方计算过程就是安全的。文献[6-8]等均是应用模拟器范例证明协议的安全性，在研究 SMP 问题的文献[14-16]中，也是应用模拟器范例证明协议的安全性。下面应用模拟器范例来证明本文协议的安全性。

证明：构造满足式(1)和式(2)的模拟器 S_A，S_B 来证明。

对于 Bob 的保密性，构造模拟器 S_A，其工作过程如下：

①S_A 的输入为 $(x,f_1(x,y))$，x 为 Alice 的保密输入，比较的结果为 $f_1(x,y)=0$ 或 1。通过随机选择一个 y' 作为 Bob 的输入使得 $f_1(x,y')=f_1(x,y)$ 来模拟协议。首先按照协议计算 x 的二叉树编码 X。

②计算得到 y' 的二叉树编码 $Y_{y'}$，再根据 X 及 $Y_{y'}$ 计算得到 c'。

③解密 $D(c')$ 得到 m'。

在本协议中，$view_A(x,y)=\{x,X,c,m\}$，$(m=f_1(x,y))$。而 $S_A(x,f_1(x,y))=\{x,X,c',m'\}$，$(m'=f_1(x,y'))$。由于 $f_1(x,y)=f_1(x,y')$，则 $m=m'$，由 c 的计算方式可知 $c\overset{c}{\equiv}c'$，所以 $\{(S_A(x,f_1(x,y)),f_2(x,y))\}_{x,y}\overset{c}{\equiv}\{(view_A^{\Pi}(x,y),output_B^{\Pi}(x,y))\}_{x,y}$ 成立，则保证了 Bob 的保密性。Alice 除了知道 x 与 Bob 的保密输入 y 的大小关系外，无法计算 Bob 的保密输入 y 的值。

对于 Alice 的保密性，构造模拟器 S_B，y 为 Bob 的输入，通过随机选择 x' 作为 Alice 的输入来模拟协议。则在本协议中，$S_B(y,f_2(x,y))=\{y,X_{x'}\}$，$view_B(x,y)=\{y,X_x\}$。由于 ElGamal 加密的安全性，$X_x$ 与 $X_{x'}$ 在计算上不可区分，因此 $\{(f_1(x,y),S_B(y,f_2(x,y)))\}_{x,y}\overset{c}{\equiv}\{(output_A^{\Pi}(x,y),view_B^{\Pi}(x,y))\}_{x,y}$ 成立，则保证了 Alice 的保密性。

(2)复杂度分析

本文中,基本的加密方案是 ElGamal 加密方案,令 p 为模数,n 为保密输入的长度。考虑计算复杂度时,本文忽略选择随机数的开销,同时也忽略 Alice 选择公钥对的开销,因为其可以在初始化阶段完成。若将所有操作转换成模乘运算来度量,则对于 ElGamal 方案,每次加密需要 $2\log p$ 次模乘运算,每次解密需要 $\log p$ 次模乘运算。

计算复杂度:在步骤 1 中,Alice 加密 n 个二进制位;在步骤 2 中,Bob 计算 c,至多需要密文相乘 $n-1$ 次;在步骤 3 中,Alice 解密密文 c。因此,Alice 需要 $(2n+1)\log p$ 次模乘(加密 n 次,解密 1 次),Bob 需要 $n-1$ 次模乘。总计算开销为 $(2n+1)\log p+(n-1)=n\times 2\log p+n-1+\log p$ 次模乘,计算复杂度为 $O(n)$。

通信复杂度:若以协议交换信息的比特数衡量,Alice 与 Bob 间交换的消息量为 X 的大小及 c,故通信复杂度为 $(2n+1+1)2\log p=(2n+2)2\log p$。若以通信轮数衡量,通信复杂度为 3。

3.3.3 比较

将本文方案与文献[15]中对常数复杂性的百万富翁协议推广的两方排序协议(记作 Xiao'),及文献[16]的利用设计的 F 函数和具有语义安全性的加法同态加密体制的多方信息比较相等协议(记作 Liu')做比较,如表 1 所列。

表 1 计算复杂度与通信复杂度(以轮数为基准)比较

	本文方案	Xiao'[15]	Liu'[16]
加密次数	n	5	2N
解密次数	1	4	1
中间计算次数	n-1(模乘)	2(模指数)	n-2(模乘)
通信复杂度	3	5	3

本文方案在步骤 1 利用 ElGamal 乘法同态加密体制加密 n 次(n 为 Alice 保密输入的二进制长度);步骤 2 进行中间计算,需要进行 $n-1$ 次乘法;步骤 3 解密 1 次。故总计算开销为 $n+1$ 次模指数运算和 $n-1$ 次模乘运算。协议 1 需 3 轮通信。

Xiao'方案也基于同态加密算法(且为加法同态),基本运算是模指数运算,协议需加密 5 次(Alice 加密 1 次,Bob 在 STEP2 和 STEP4 分别加密 2 次),解密 4 次(Alice 在 STEP3 和 STEP5 分别解密 2 次),还包括 2 次模指数运算(在 STEP2 和 STEP4 各 1 次)。总的模指数运算次数为 11,但与 n 无关。但 Xiao'需 5 轮通信。

Liu'方案是多方的信息比较相等协议,本文所提出的是两方的保密比较协议(但完全可以由两方推广到多方)。因此与 Liu'方案比较时,不妨考虑 Liu'方案为两方时的情况。Liu'在步骤 1 中利用门限同态加密体制加密 $2N$(N 为数据的数值大小,因此当比较的数值稍大时复杂度将非常高)次;在步骤 2 中进行中间计算,需要 1 次乘法;在步骤 3 中,两方共同完成一次解密运算。Liu'需 3 轮通信。

因此,与 Xiao'方案相比,本文方案通信复杂度为 3,Xiao'方案通信复杂度为 5,故本文方案的通信复杂度优于 Xiao'方案。在计算复杂度上(为比较方便,仅考虑复杂度高的模指数运算),本文方案需 $n+1$ 次模指数运算,n 为保密数值二进制长度,而 Xiao'方案总的模指数运算次数为 11,故在大多数的电子拍卖系统的标价或者比较参与者的年龄等情况下,n 值取不太大时,两个方案的计算复杂度相当,否则本文的计算复杂度更高一些。但本文采用乘法同态加密,Xiao'方案采用加法同态加密。在实际中,乘法同态加密比加法同态加密更高效,因此会节省计算时间和通信带宽[6]。考虑到现代设备的计算性能很强,方案的应用场景为网上拍卖、电子选举、身份认证等,通信复杂度相对于计算复杂度对方案效率的影响更大。

与 Liu'方案相比,通信复杂度均为 3 轮通信。在计算复杂度上,本文方案加密 n 次,n 为保密数值二进制长度;Liu'方案加密 $2N$ 次,N 为保密数值的大小。通过计算很容易发现,$n\leqslant N(N\geqslant 1)$,且保密数值 N 越大,n 与 N 差距就越明显,满足 $n\approx\log 2N$,例如 $N=1024$ 时,$n=10$,N 是 n 的约 100 倍,加密次数则是约 200 倍。因此本文方案的计算复杂度优于 Liu'。

结束语 社会主义百万富翁问题(SMP)是百万富翁问题的变形问题。该类问题的解决方案可以作为网上拍卖、电子选举、身份认证等应用系统的基本协议。

本文提出一个对保密输入进行二叉树编码和 ElGamal 同态加密的新的 SMP 方案,并对协议的正确性、安全性和效率进行了分析。最后的分析、比较结果表明,本文方案具有更高的效率。下一步将考虑设计具体的应用。

参 考 文 献

[1] Yao A C. Protocol for Secure Computations [C]// 2013 IEEE 54th Annual Symposium on Foundations of Computer Science. Los Alamitos: IEEE, 1982: 160-164

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

[3] Qin Jing, Zhang Zhen-feng, Feng Deng-guo, et al. A protocol of specific secure two-party computation[J]. Journal of China Institute of Communications, 2004, 25(11): 35-42(in Chinese)
秦静,张振峰,冯登国,等. 一个特殊的安全多方计算协议[J]. 通信学报,2004,25(11):35-42

[4] Ioannidis I, Grama A. An efficient protocol for Yao's millionaires problem[C]// Proceedings of the 36th Annual Hawaii International Conference on System Sciences. Hawaii: IEEE, 2003: 205a

[5] 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)
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

[6] Lin H Y, Tzeng W G. An efficient solution to the millionaires problem based on homomorphic encryption[C]// Proceedings of the Third international conference on Applied Cryptography and Network Security. NewYork: Springer Berlin Heidelberg, 2005: 456-466

[7] Qin Bo, Qin Hui, Zhou Ke-fu, et al. Millionaires' protocol with constant complexity[J]. Journal of Xi'an University of Technology, 2005, 21(2): 149-152(in Chinese)
秦波,秦慧,周克复,等. 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

[8] Li Shun-dong, Wang Dao-shun. Efficient Secure Multiparty Computation Based on Homomorphic Encryption[J]. Acta Electronica Sinica, 2013, 41(4): 798-803(in Chinese)

李顺东,王道顺. 基于同态加密的高效多方保密计算[J]. 电子学报,2013,41(4):798-803

[9] Schoenmakers B, Tuyls P. Practical two-party computation based on the conditional gate[M]// Advances in Cryptology-ASIACRYPT 2004. Springer Berlin Heidelberg, 2004:119-136

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

[11] Jakobsson M, Yung M. Proving Without Knowing : On Oblivious, Agnostic and Blindfolded Provers[C]// Proceedings of Advances in Cryptology-CRYPTO'96. Springer-Verlag, 1996: 186-200

[12] Boudot F, Schoenmakers B, Traoré J. A Fair and Efficient Solution to the Socialist Millionaires' Problem [J]. Discrete Applied Mathematics, 2001, 111(1):23-36

[13] Qin Jing, Zhang Zhen-feng, Feng Deng-guo, et al. A protocol of comparing information without leaking [J]. Journal of Software, 2004, 15(3):421-427(in Chinese)
秦静,张振峰,冯登国,等. 无信息泄露的比较协议[J]. 软件学报,2004,15(3):421-427

[14] Liu Wen, Luo Shou-shan, Chen Ping. Solution to SMP Based on Sliding Window and Commutation Encryption Function [J]. Computer Engineering, 2007, 33(22):163-171(in Chinese)
刘文,罗守山,陈萍. 基于滑动窗口和交换加密函数解决 SMP 的新方案[J]. 计算机工程,2007,33(22):163-171

[15] Xiao Qian, Luo Shou-shan, Chen Ping, et al. Research on the Problem of Secure Multi-party Ranking Under Semi-honest Model[J]. Acta Electronica Sinica, 2008, 36(4):709-714(in Chinese)
肖倩,罗守山,陈萍,等. 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

[16] Liu Wen, Wang Yong-bin. Secure multi-party comparing protocol and its applications[J]. Acta Electronica Sinica, 2012, 40(5): 871-876(in Chinese)
刘文,王永滨. 安全多方比较相等协议及其应用[J]. 电子学报,2012,40(5):871-876

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

[18] Goldreich O. Secure multi-party computation(Manuscript. Preliminary version)[Z]. 1998

(上接第 171 页)

[3] Ni Q, Bertino E, Lobo J, et al. Privacy-aware role-based access control[J]. ACM Transactions on Information and System Security (TISSEC), 2010, 13(3):24

[4] Ardagna C A, Cremonini M, De Capitani di Vimercati S, et al. A privacy-aware access control system[J]. Journal of Computer Security, 2008, 16(4):369-397

[5] Ardagna C A, Damiani E, di Vimercati S D C, et al. Towards privacy-enhanced authorization policies and languages[M]// Data and Applications Security XIX. Springer Berlin Heidelberg, 2005:16-27

[6] Kolter J, Schillinger R, Pernul G. A privacy-enhanced attribute-based access control system[C]// Proc. of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security. Edondo Beach, CA, USA, July 2007

[7] Ferraiolo D F, Sandhu R, Gavrila S, et al. Proposed NIST standard for role-based access control[J]. ACM Transactions on Information and System Security (TISSEC), 2001, 4(3):224-274

[8] Ferraiolo D, Cugini J, Kuhn D R. Role-based access control (RBAC): Features and motivations[C]// Proceedings of 11th Annual Computer Security Application Conference. 1995:241-248

[9] Anderson A. A comparison of two privacy policy languages: EPAL and XACML[C]// Proceedings of the 3rd ACM Workshop on Secure Web Service. 2005

[10] Ardagna C A, Cremonini M, De Capitani di Vimercati S, et al. A privacy-aware access control system[J]. Journal of Computer Security, 2008, 16(4):369-397

[11] Ke Chang-bo, Huang Zhi-qiu, Tang Mei. Supporting negotiation mechanism privacy authority method in cloud computing[J]. Knowledge-Based Syst., 2013, 51:48-59

[12] Lv Fu-jun. Web Services Reputation Evaluation Model Based on QoS and User Recommendation[D]. Qinghuangdao: Yanshan University, 2010(in Chinese)
吕福军. 一种基于 QoS 与用户推荐的 Web 服务信誉度评价模型[D]. 秦皇岛:燕山大学,2010

[13] Liu Lin-yuan. Research on Privacy Analysis and Verification of Web Service Composition [D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2011(in Chinese)
刘林源. Web 服务组合隐私分析与验证研究[D]. 南京:南京航空航天大学,2011

[14] Smari W W, Clemente P, Lalande J F. An extended attribute based access control model with trust and privacy: Application to a collaborative crisis management system[J]. Future Generation Computer Systems, 2014, 31:147-168

[15] Liu Yi-min, Wang Zhi-hui, Wang Wei. Research and Implementation of purpose-Based Privacy Access Control Policy in XML Data Mode[J]. Computer Applications and Software, 2013, 30(2):148-151(in Chinese)
刘逸敏,王智慧,汪卫. XML 数据模式下基于 purpose 的隐私访问控制策略研究与实现[J]. 计算机应用与软件,2013,30(2):148-151

[16] Nabeel M, Bertino E, Kantarcioglu M, et al. Towards privacy preserving access control in the cloud[C]// 2011 7th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom). IEEE, 2011:172-180

[17] Ruj S, Stojmenovic M, Nayak A. Privacy preserving access control with authentication for securing data in clouds[C]// 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid). IEEE, 2012:556-563

[18] Takabi H. Privacy aware access control for data sharing in cloud computing environments[C]// Proceedings of the 2nd International Workshop on Security in Cloud Computing. ACM, 2014: 27-34

[19] Nabeel M, Bertino E. Privacy preserving delegated access control in the storage as a service model[C]// 2012 IEEE 13th International Conference on Information Reuse and Integration (IRI). IEEE, 2012:645-652

[20] Kim Y, Song E. Privacy-aware role based access control model: Revisited for multi-policy conflict detection[C]// 2010 International Conference on Information Science and Applications (ICISA). IEEE, 2010:1-7