具有隐私保护的分布式协作统计计算方案

马 飞[1,2]，蒋建国[1]

（1. 合肥工业大学 计算机与信息学院，安徽 合肥 230009；
2. 北方民族大学 计算机科学与工程学院，宁夏 银川 750021）

摘 要：由于针对分布式环境下具有隐私保护的统计计算技术的研究较少，利用 Paillier 加密算法的加法同态性，提出一种在互不信任的分布式环境下具有隐私保护的协作统计计算方案。充分利用分布式环境的计算能力，由用户客户端与统计服务器协作对数据进行相关系数、算术平均、方差与线性回归等统计分析，整个分析过程对用户敏感数据进行有效的隐私保护。论证该方案在 SHM 模式下的安全性，对其进行性能测试。

关键词：分布式环境；隐私保护；加同态；统计分析；SHM 模式
中图法分类号：TP309.7 **文献标识号**：A **文章编号**：1000-7024（2015）09-2383-05
doi：10.16208/j.issn1000-7024.2015.09.013

Privacy preserving distributed collaborative statistical calculation scheme

MA Fei[1,2], JIANG Jian-guo[1]

(1. School of Computer and Information, Hefei University of Technology, Hefei 230009, China;
2. School of Computer Science and Engineering, Beifang University of Nationalities, Yinchuan 750021, China)

Abstract: The research on privacy preserving statistical calculation in mistrustful distributed environment is relatively less. Using the additive homomorphism of Paillier encryption algorithm, a collaborative statistical calculation scheme with privacy preserving in mistrustful distributed environment was introduced. The calculating ability of distributed environment was used, and clients and the statistical server collaboratively calculated arithmetic mean, correlation coefficient, variance and linear regression, etc. Users' privacy data were protected during the period of calculation. The security of scheme under semi-honest mode was demonstrated, and the performance of the scheme was tested.

Key words: distributed environment; privacy preserving; additive homomorphism; statistics analysis; SHM

0 引 言

随着 Internet 的快速发展，参与统计分析的数据往往来自于多个数据源，而目前多数据源的隐私保护统计计算方案主要是基于加密技术的方案[1-4]和 SMC（secure multi-party computation）[5-8]方案。由于基于加密的方案涉及过多的加解密过程，较为低效，而 SMC 由于涉及过多繁琐的协议交互过程，不适用于相对计算简单的统计分析问题。如何在互不信任的多数据源环境下对数据进行统计计算且不破坏敏感数据的隐私性是一个具有重要理论意义与实际应用价值的研究课题。

本文利用 Paillier 加密算法[9-11]的加法同态性质[12,13]设计了一种在互不信任的分布式环境下具有隐私保护的协作统计分析方案。该方案不但使用户的隐私数据在整个统计计算过程中都处于被保护状态，而且充分利用了分布式环境下的高计算与存储能力，由用户端与服务器端协作完成整个统计计算过程。

1 Paillier 公钥加密算法及其加法同态性

（1）密钥生成：选择两个素数 p 和 q，计算 $N=pq$，$\lambda=lcm(p-1,q-1)$，然后选择一个随机数 $g\in Z_{N^2}^*$，需满足 $\gcd(L(g^\lambda \bmod N^2),N)=1$，此处 $L(x)=(x-1)/N$。Paillier 的公钥和私钥分别为 $<N,g>$ 和 λ。

（2）加密操作：令 $m\in Z_N$ 为明文，$r\in Z_N$ 为一随机数，用 $E(\cdot)$ 表示加密操作

$$E(m \bmod N, r \bmod N)=g^m r^N \bmod N^2 \quad (1)$$

收稿日期：2014-10-11；修订日期：2014-12-28
基金项目：北方民族大学科研基金项目（2013XYZ029）
作者简介：马飞（1976-），男，陕西榆林人，博士，副教授，CCF 会员，研究方向为网络安全、隐私保护、社交网络分析；蒋建国（1955-），男，安徽广德人，教授，博士生导师，研究方向为分布式计算、图形图像处理。E-mail：feixiangflying33@nxu.edu.cn

(3) 解密操作：给定密文 $c \in Z_{N^2}$，$D(\cdot)$ 表示用私钥 λ 进行解密，计算公式如下

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

为保证 Paillier 算法语义安全，必须 N 与 g 足够大。$\forall m_1, m_2, r_1, r_2 \in Z_N$，都有下式成立

$$E(m_1, r_1)E(m_2, r_2) = E(m_1 + m_2, r_1 r_2) \bmod N^2 \tag{3}$$

$$E^{m_2}(m_1, r_1) = E(m_1 m_2, r_1^{m_2}) \bmod N^2 \tag{4}$$

式 (3) 与式 (4) 表明：在密文域上做“乘”运算，其运算结果等于明文域上先做“加”运算，然后对结果进行加密之后的输出，这是 Paillier 算法的加法同态性。

2 几种典型统计计算公式变换与同态计算

2.1 统计计算公式变换

为了能够应用 Paillier 算法的加法同态性到统计计算中，需对统计计算公式做等价变换：

(1) 算术平均：假设样本空间为 $\{x_1, \cdots x_n\}$，算术平均可表示为

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{5}$$

(2) 方差：方差表征变量 X 取值的散度，其变换后的计算公式如下

$$var(X) = \frac{1}{n}\sum_{i=1}^{n} x_i^2 - (\frac{1}{n}\sum_{i=1}^{n} x_i)^2 \tag{6}$$

(3) 线性回归：设有数据集：$\{(x_1, y_1), \cdots, (x_i, y_i) \cdots (x_n, y_n)\}$，一元线性回归的目的是找到线性方程 $y = a + bx$ 去拟合这个数据集，最常采用最小二乘法来确定参数 a 与 b，等价变换后的计算公式如下

$$a = \frac{1}{n}\sum_{i=1}^{n} y_i - b\frac{1}{n}\sum_{i=1}^{n} x_i \tag{7}$$

$$b = \frac{n\sum_{i=1}^{n} x_i y_i - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i}{n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2} \tag{8}$$

(4) 相关系数：变量 X 与 Y 的相关系数是用来衡量两者之间线性关系的强度与方向，其变换后的计算公式如下

$$corr(X,Y) = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}}$$

$$= \frac{n\sum_{i=1}^{n} x_i y_i - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i}{\sqrt{n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2}\sqrt{n\sum_{i=1}^{n} y_i^2 - \left(\sum_{i=1}^{n} y_i\right)^2}} \tag{9}$$

2.2 加法同态性与统计计算

符号定义：① K_{pk}：Paillier 加密算法的公钥，由统计服务器提供给参与统计计算的各个客户端。② $E_{pk}(\ \ )$：Paillier 加密操作。参与统计计算的客户端用 K_{pk} 加密其隐私数据。

令中间统计结果：$w_x = \sum_{i=1}^{n} x_i^2$，$u_x = \sum_{i=1}^{n} x_i$，$w_y = \sum_{i=1}^{n} y_i^2$，$u_y = \sum_{i=1}^{n} y_i$，$z_{xy} = \sum_{i=1}^{n} x_i y_i$。用 K_{pk} 分别加密 x_i、x_i^2、y_i、y_i^2、$x_i y_i$ 与 1，即：$E_{pk}(x_i)$、$E_{pk}(x_i^2)$、$E_{pk}(y_i)$、$E_{pk}(y_i^2)$、$E_{pk}(x_i y_i)$ 与 $E_{pk}(1)$。根据 Paillier 算法的加法同态性，有以下等式成立

$$E_{pk}(w_x) = \prod_{i=1}^{n} E_{pk}(x_i^2), E_{pk}(u_x) = \prod_{i=1}^{n} E_{pk}(x_i) \tag{10}$$

$$E_{pk}(w_y) = \prod_{i=1}^{n} E_{pk}(y_i^2), E_{pk}(u_y) = \prod_{i=1}^{n} E_{pk}(y_i) \tag{11}$$

$$E_{pk}(z_{xy}) = \prod_{i=1}^{n} E_{pk}(x_i y_i), E_{pk}(n) = \prod_{i=1}^{n} E_{pk}(1) \tag{12}$$

3 方案拓扑结构及计算步骤

3.1 拓扑结构与组成

如图 1 所示，方案采用环形拓扑结构，参与统计计算的用户数据采用单向传递。结构中有 3 种不同类型的结点：CClient，KClient，SServer。

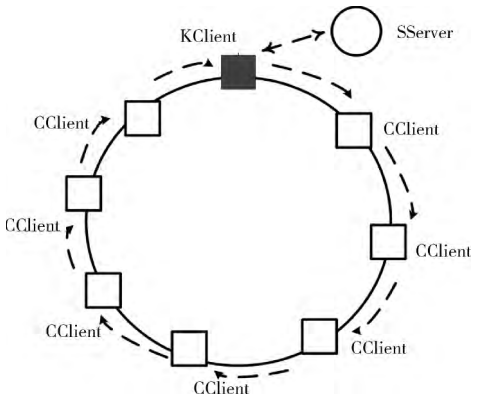

图 1 方案拓扑结构

(1) SServer：统计计算服务器：①完成最终的统计计算并输出统计结果。②给参与统计计算的客户端提供 Paillier 算法的公钥。

(2) CClient：参与统计计算的用户客户端：①提供加密统计数据：用 SServer 提供的公钥加密统计数据以保证隐私性。②参与统计计算：利用 Paillier 算法的加法同态性来参与隐私统计计算。

(3) KClient：把各 CClient 经过同态计算得到的中间统计结果最终交于 SServer。若其也有数据需参加统计计算，则也完成 CClient 的两种操作。

3.2 方案执行步骤

(1) 计算步骤

1) SServer 利用 Paillier 算法生成一对密钥，把公钥广播给参与统计计算的 CClient。各 CClient 用 Paillier 算法公

钥加密各自的隐私数据与整数“1”，若无隐私数据参与统计计算，则加密“0”。

2）加密隐私数据在环中进行单向传递，参与统计计算的 CClient 用其前趋传递过来的加密数据与自己的加密数据做同态计算，把结果传递给其后继。

3）经过计算与传递，加密中间统计结果最终到达 KClient，由其交于 SServer 后由 SServer 用 Paillier 加密算法私钥解密，并将解密结果带入到相应的统计计算公式中，得到最终的统计结果并输出。

说明：每个有数据需要参与统计计算的客户端都加密“1”，并让其也参与计算和传递，最后参与计算的客户端数 n 将以加密形式交于统计计算服务器。若客户端无数据参与统计计算，则为了满足协议的一致性要求，也必须加密“0”，即：$E_{PK}(0)$。该 $E_{PK}(0)$ 需要参与以下两个运算，其结果并不影响最终的统计值

$$E_{pk}(x) = E_{pk}(x+0) = E_{pk}(0)E_{pk}(x) \tag{13}$$

$$E_{pk}(n) = E_{pk}(n+0) = E_{pk}(0)E_{pk}(n) \tag{14}$$

（2）分布式隐私保护计算“算术平均”实例

输入：每个 CClient 都具有隐私数据 $x_i, i \in N, N$ 为 CClient 的个数。$X = \{x_1, \ldots, x_i, \ldots, x_N\}$。

输出：$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i$。

目标：由各 CClient 与 SServer 协作计算统计量 X 的“算术平均”，且不破坏 x_i 的隐私性。

设 CClientX、CClientY、CClientZ 为单向逻辑环中的客户端，x_a、x_b、x_c 分别为它们的隐私数据。CClientX 与 CC-lientZ分别为 CClientY 的前趋与后继。

步骤 1 设 CClientX、CClientY 与 CClientZ 的隐私数据经加密后分别为：$E_{pk}(x_a)$、$E_{pk}(x_b)$、$E_{pk}(x_c)$，并且每个 CClient 都有一个 $E_{pk}(1)$。

步骤 2 CClientX 把 $E_{pk}(1)$ 与 $E_{pk}(x_a)$ 传递给其后继 CClientY 后，CClientY 进行如下计算

$$E_{pk}(x_a + x_b) = E_{pk}(x_a)E_{pk}(x_b) \tag{15}$$

$$E_{pk}(1+1) = E_{pk}(1)E_{pk}(1) \tag{16}$$

CClientY 把 $E_{pk}(x_a + x_b)$ 与 $E_{pk}(1+1)$ 传递给其后继 CClientZ，CClientZ 做如下计算

$$E_{pk}(x_a + x_b + x_c) = E_{pk}(x_c)E_{pk}(x_a + x_b) \tag{17}$$

$$E_{pk}(1+1+1) = E_{pk}(1+1)E_{pk}(1) \tag{18}$$

CClientZ 把 $E_{pk}(x_a + x_b + x_c)$ 与 $E_{pk}(1+1+1)$ 向其后继传递，其它 CClient 进行类似处理过程。

步骤 3 KClient 将收到如下加密中间统计结果

$$E_{pk}(u_x) = \prod_{i=1}^{n} E_{pk}(x_i), E_{pk}(n) = \prod_{i=1}^{n} E_{pk}(1) \tag{19}$$

KClient 把 $E_{pk}(u_x)$ 与 $E_{pk}(n)$ 交于 SServer，并被 SServer 解密得到 u_x 与 n，代入式（5），$\bar{x}$ 即为所求“算术平均”。在统计计算的整个过程中，若 CClient 无统计数据参与统计计算，则执行 $E_{pk}(0)$ 操作，并按式（13）与式（14）参与计算，然后按协议要求进行数据传递。

方差、线性回归、相关系数的计算过程除所用公式不同以外，其它皆与上述计算步骤一致。

4 方案安全性分析与性能测试

4.1 方案安全性分析

SHM 模式（semi-honest mode）[14]：参与统计计算的 CClient、KClient 和 SServer 都遵循统计计算的步骤，但希望在计算的过程中能够获得除了最终统计计算结果以外的其它额外信息。

（1）攻击模型：

CASE1：全部 CClient 可信，SServer 不可信；

攻击目的：所有 CClient 遵循方案要求的统计计算步骤，但非可信 SServer 想获得各 CClient 的隐私数据。

CASE2：部分 CClient 共谋，SServer 可信；

攻击目的：SServer 可信，部分共谋 CClient 希望推出非共谋 CClient 的隐私数据或中间计算结果。

CASE3：部分 CClient 共谋，SServer 不可信；

攻击目的：部分 CClient 与 SServer 共谋，希望获得非共谋 CClient 的隐私数据。

（2）安全性分析：

对于第 1 种攻击，方案中，加密数据经过计算与单向传递后，SServer 最终获得的是加密后的中间结果，所以即使 SServer 对其进行解密，也无法推出 CClient 各自的原始隐私数据。

对于第 2 种攻击，由于所有 CClient 的隐私信息及中间计算结果都被可信的 SServer 的公钥所加密，而在 SServer 私钥安全的情况下，共谋 CClient 是无法对其解密，故非共谋 CClient 的隐私信息在计算的任何阶段都不会被泄露。

对于第 3 种攻击，设 n 为 CClient 的总数，m 为共谋 CClient 的个数。①当 $m = n-1$ 时，即只有一个 CClient 是非共谋，其它 $n-1$ 个 CClient 都与 SServer 共谋，当非共谋 CClient 把隐私统计数据用 SServer 的公钥加密后交于其后继结点，后继结点与其它共谋 CClient 仍然按照协议要求的步骤执行，但都只用加密后的“0”与非共谋的 CClient 的加密隐私数据做同态计算并把结果按环拓扑结构单向传递。最终 SServer 收到的数据其实就是非共谋 CClient 的加密隐私数据，SServer 对其解密即可获得非共谋 CClient 的隐私数据。②当 $m < n-1$ 时，即非共谋的 CClient 个数 $\geqslant 2$ 时，按照协议的计算步骤，SServer 收到的一定是非共谋 CC-lient隐私数据做加法之后的中间结果的加密形式，所以 SServer 即使对其解密，也无法从隐私数据“和”中反推出非共谋 CClient 各自的隐私数据。故对于本方案，只要满足 $m < n-1$ 条件，则共谋的 CClient 与 SServer 不能推出非共谋 CClient 的隐私数据。

4.2 方案性能测试

测试所实现方案在计算“方差”、“回归系数”和“相关系数”时的时间代价。

由于方案采用分布式计算统计量，计算的时间代价主要集中在两方面：①单个客户端对数据进行 Paillier 算法加密，及进行加性同态计算时所用时间。②统计服务器对中间统计结果进行解密及计算最终统计结果所用时间。

方案实现环境参数：CClient、KClient、SServer 都采用性能一致的 Acer 笔记本电脑，共设置了 7 台电脑，其中具有 CClient 身份的电脑共 5 台，KClient 和 SServer 各一台。设备通过 IEEE 802.11g 网络进行互联。具体参数见表 1。

表 1 方案实现环境参数

OS	Windows 7 32-bit professional
CPU	1.70 GHz，2.86 GB RAM
Software	VC++ Crypto++库

为了保证 Paillier 加密算法有足够的语义安全[15]，设置参数：N：1024 bit g：160 bit。公钥 $<N,g>$：1184 bit，密文为 2048-bit。基于以上参数，Paillier 加密过程实质是做两次 1024-bit 的幂运算，一次 2048-bit 的乘法运算，而解密过程是做一次 2048-bit 的幂运算。私钥与公钥利用生成算法在模型运行前按要求位数已生成。方案的客户端模块（CClient）和服务器端模块（SServer）都处于工作状态。共进行了 30 次测试。

符号定义：

$tE(\cdot)$ 表示单次 Paillier 加密操作所用时间；

$tD(\cdot)$ 表示单次 Paillier 解密操作所用时间；

$tH(\cdot)$ 表示单次同态操作所用时间；

$Tout$：指 SServer 对收到的中间结果进行解密所用时间与计算最终统计结果的时间之和。

计算“方差”时间代价见表 2。

表 2 计算“方差”时间代价

	Max/ms	Min/ms	Mean/ms
$tE(\cdot)$	40.0	35.1	37.53
$tH(\cdot)$	78.2	69.3	24.82
$tD(\cdot)$	41.0	36.0	37.66
$Tout$	41.9	36.8	38.20

计算“回归系数”时间代价见表 3。

表 3 计算“回归系数”时间代价

	Max/ms	Min/ms	Mean/ms
$tE(\cdot)$	40.1	35.6	37.89
$tH(\cdot)$	77.0	69.6	25.12
$tD(\cdot)$	41.6	36.4	37.95
$Tout$	42.2	36.3	38.41

计算“相关系数”时间代价见表 4。

表 4 计算“相关系数”时间代价

	Max/ms	Min/ms	Mean/ms
$tE(\cdot)$	41.2	35.3	37.73
$tH(\cdot)$	77.2	68.9	25.17
$tD(\cdot)$	41.3	36.6	38.06
$Tout$	42.4	37.1	38.74

$tE(\cdot)$ 和 $tH(\cdot)$ 是在 5 台 CClient 上分别进行测试得到相应的数值，$tD(\cdot)$ 与 $Tout$ 是在 SServer 上测试得到。单个 CClient 做加密及同态运算所花费时间与方案规模（参与统计计算的用户端数）无关。SServer 最后对中间结果解密及计算最终统计结果所用时间也与规模无关。

4.3 方案特点与应用展望

（1）方案特点：①隐私数据由客户端独立进行存储，方便用户对数据施加灵活的访问控制。统计计算由客户端与服务器共同完成，从而降低了传统服务器由于集中进行统计计算与存储而带来的安全隐患及计算复杂性过高的问题，适用于大数据量计算。②数据的传递过程也是统计计算的过程，不必事先合并数据。除了中间统计结果及最终的统计结果以外，用户个体隐私数据在整个统计计算过程中都处于保密状态。③加密只在客户端提供原始统计数据时出现，而解密操作也仅在统计服务器对中间统计结果进行解密时发生，所以方案只涉及很少的加解密过程。

（2）方案不足：对于部分 CClient 与 SServer 进行共谋的攻击，必须满足非共谋 CClient 的个数大于 1 时方案才能正确执行，这将是以后需要对方案改进的地方。

（3）方案应用展望：医疗系统中监测患者体征的可穿戴设备、智能电网中的智能电表等都需要采集设备环境或用户的体征数据，而这些数据都具有很强的隐私性，对这类数据进行统计分析时，则可采用本文提出的方案。本文只实现了 Windows 环境下的方案，下一步可对方案进行 Android 环境下的实现。

5 结束语

统计分析是数据挖掘领域重要的工具之一，但在分布式环境下对具有隐私保护的统计计算技术的研究还比较少。针对该问题，利用 Paillier 加密算法的加法同态性，提出了一种在互不信任的分布式环境下具有隐私保护的协作统计计算方案。该方案充分利用分布式环境的计算能力，由用户客户端与统计服务器协作对数据进行相关系数、算术平均、方差与线性回归等统计分析，整个分析过程对用户隐私数据都进行了有效的保护。最后论证了方案在 SHM 模式下的安全性，并对方案进行了性能测试。

参考文献：

[1] LI Chaoling，CHEN Yue. Fragmentation and encryption-based pri-

vacy-preserving mechanism for cloud database [J]. Journal of Information Engineering University, 2012, 13 (3): 376-384 (in Chinese). [李超零，陈越. 基于分解与加密的云数据库隐私保护机制研究 [J]. 信息工程大学学报，2012，13 (3)：376-384.]

[2] QIAN Ping, WU Meng. Survey of privacy preserving data mining methods based on homomorphic encryption [J]. Application Research of Computers, 2011, 28 (5): 45-50 (in Chinese). [钱萍，吴蒙. 同态加密隐私保护数据挖掘方法综述 [J]. 计算机应用研究，2011，28 (5)：45-50.]

[3] ZHANG Bin. Research on efficient secure basic protocols of multiparty computation and their application [D]. Jinan: Shandong University, 2012: 77-81 (in Chinese). [张斌. 高效安全的多方计算基础协议及应用研究 [D]. 济南：山东大学，2012：77-81.]

[4] SONG Maohua. Research on secure mulit-party computation and its application [D]. Beijing: Beijing University of Posts and Telecommunications, 2013: 37-39 (in Chinese). [孙茂华. 安全多方计算及其应用研究 [D]. 北京：北京邮电大学，2013：37-39.]

[5] WEI Zhiqiang, KANG Mijun. Research on privacy-protection policy for pervasive computing [J]. Chinese Journal of Computers, 2010, 33 (1): 128-138 (in Chinese). [魏志强，康密军. 普适计算隐私保护策略研究 [J]. 计算机学报，2010，33 (1)：128-138.]

[6] Ziba Eslami, Saideh Kabiri Rad. A new verifiable multi-secret sharing scheme based on bilinear maps [J]. Wireless Personal Communications, 2012, 63 (2): 459-467.

[7] PANG Lei, SUN Maohua. Full privacy preserving electronic voting scheme [J]. The Journal of China Universities of Posts and Telecommunications, 2012, 19 (4): 45-48.

[8] YE Yun. Research on protecting and utilizing private data in cooperative computation [D]. Hefei: University of Science and Technology of China, 2012: 90-93 (in Chinese). [叶云. 保护私有数据合作计算问题及其应用研究 [D]. 合肥：中国科学技术大学，2012：90-93.]

[9] BAI Jian, YANG Yatao, LI Zichen. The homomorphism and efficiency and analysis of Paillier cryptosystem [J]. Journal of Beijing Electronic Science and Technology Institute, 2012, 25 (4): 77-81 (in Chinese). [白健，杨亚涛，李子臣. Paillier 公钥密码体制同态特性及效率分析 [J]. 北京电子科技学院学报，2012，25 (4)：77-81.]

[10] ZHOU Qinqting. Research on scalar product protocol based on Paillier cryptosystem [D]. Kunming: Yunnan University, 2012: 57-60 (in Chinese). [周青婷. 基于 Paillier 密码体制的点积协议研究 [D]. 昆明：云南大学，2012：57-60.]

[11] LI Meiyun, LI Jian, HUANG Chao. A credible cloud storage platform based on homomorphic encryption [J]. Netinfo Security, 2012, 12 (9): 35-40 (in Chinese). [李美云，李剑，黄超. 基于同态加密的可信云存储平台 [J]. 信息网络安全，2012，12 (9)：35-40.]

[12] Gentry C. Fully homomorphic encryption using ideal lattices [C] //Proc of the ACM Int'l Symp on Theory of Computing, 2009: 13-17.

[13] REN Fule, ZHU Zhixiang. A cloud computing security solution based on fully homomorphic encryption [J]. Journal of Xi'an University of Posts and Telecommunications, 2013, 25 (5): 56-58 (in Chinese). [任福乐，朱志祥. 基于全同态加密的云计算数据安全方案 [J]. 西安邮电大学学报，2013，25 (5)：56-58.]

[14] ZHENG Qiang. Study on several secure multi-party computation problem in different models [D]. Beijing: Beijing University of Posts and Telecommunications, 2011: 12-15 (in Chinese). [郑强. 不同模型下若干安全多方计算问题的研究 [D]. 北京：北京邮电大学，2011：12-15.]

[15] Dong W, Wang V. Secure friend discovery in mobile social network [C] //INFOCOM, 2011: 46-48.