(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 103441836 A
(43)申请公布日 2013.12.11

(21)申请号 201310397321.5

(22)申请日 2013.09.04

(71)申请人 安徽大学
地址 230601 安徽省合肥市经济技术开发区九龙路 111 号

(72)发明人 石润华 仲红 崔杰 许艳

(74)专利代理机构 安徽省合肥新安专利代理有限责任公司 34101
代理人 何梅生

(51)Int.Cl.
H04L 9/00(2006.01)
H04H 60/23(2008.01)

权利要求书2页 说明书6页

(54)发明名称

一种广播加密及其解密方法

(57)摘要

本发明公开了一种广播加密及其解密方法，其特征是在分布式网络环境中，存在一个广播中心节点和 n 个代理用户节点，所述广播中心节点向所述代理用户节点广播密文；所述代理用户节点接收所述密文进行解密。本发明以点积运算代替模幂运算，能够降低加密和解密计算的复杂度，节约计算资源，从而高效、快速地实现广播加密；其安全性基于推广的子集和问题的困难性，因而获得了比现有主流广播加密方法更高的安全性。

CN 103441836 A

1. 一种广播加密及其解密方法，其特征是，在分布式网络环境中，存在一个广播中心节点和 n 个代理用户节点，所述广播中心节点向所述代理用户节点广播密文；所述代理用户节点接收所述密文并进行解密；所述广播加密及其解密方法按如下步骤进行：

步骤 1：所述广播中心节点按如下步骤生成大素数 p、加密密钥以及解密密钥：

1.1) 建立一个大素数 p，并通过广播的方式向所述代理用户节点公开所述大素数 p；

1.2) 随机生成一个 1×n 维的矩阵 A(1<n)，所述矩阵 A 中的元素为小于所述大素数 p 的非负整数；

1.3) 随机生成一个 n 维列向量$\vec{x}_0$，利用式 (1) 获得向量$\vec{y}$：

$$\vec{y} = A\vec{x}_0 \bmod p \qquad (1)$$

式 (1) 中，矩阵 A 和向量$\vec{y}$均为广播中心节点的加密密钥；

1.4) 利用加密密钥 A 和$\vec{y}$，建立方程组$A\vec{x} \bmod p = \vec{y}$；

1.5) 求解方程组$A\vec{x} \bmod p = \vec{y}$获得 n 个不同的解向量$\vec{x}_i$ ($1 \leqslant i \leqslant n$)；所述解向量$\vec{x}_i$为第 i 个代理用户节点的解密密钥；

步骤 2：所述广播中心节点按如下步骤获得密文：

2.1) 随机生成一个 l 维的行向量$\vec{k} = (k_1, k_2, ..., k_l)$，$1 \leqslant k_i \leqslant p-2 (1 \leqslant i \leqslant l)$；

2.2) 假设广播中心节点所需要发送的明文为 m，$m \in \{0, 1, 2, .., p-1\}$，根据所述加密密钥利用式 (2) 和式 (3) 获得密文$\{\vec{c}_1, c_2\}$：

$$\vec{c}_1 = \vec{k}A \bmod p \qquad (2)$$

式 (2) 中，$\vec{c}_1$为 n 维行向量；

$$c_2 = m(\vec{k}^T \cdot \vec{y}) \bmod p \qquad (3)$$

式 (3) 中，$\vec{k}^T$表示行向量$\vec{k}$转置后所对应的列向量，$\vec{k}^T \cdot \vec{y}$表示列向量$\vec{k}^T$与$\vec{y}$的点积运算；

步骤 3：所述代理用户节点根据所述大素数 p 和解密密钥进行解密：

第 i 个代理用户节点根据所接收的密文$\{\vec{c}_1, c_2\}$利用式 (4) 和式 (5) 获得明文 m：

$$c_1 = \vec{c}_1^{\,T} \cdot \vec{x}_i \bmod p \qquad (4)$$

式 (4) 中，$\vec{x}_i$为第 i 个代理用户节点的解密密钥；$\vec{c}_1^{\,T}$表示行向量$\vec{c}_1$转置后所对应的列向量，$\vec{c}_1^{\,T} \cdot \vec{x}_i$表示列向量$\vec{c}_1^{\,T}$与$\vec{x}_i$的点积运算；

$m = c_2 / c_1 \bmod p$　　(5)。

2. 根据权利要求 1 所述的广播加密及其解密方法，其特征是，所述大素数 p 按如下步骤生成：

a) 确定大素数 p 的位长 d；

b) 随机生成一个位长为 d 比特的首位和末位均为 1 的奇数 q；

c) 采用素数检测方法判断 q 是否是素数，若是则令 p=q，否则重新执行步骤 b。

3. 根据权利要求 1 所述的广播加密及其解密方法，其特征是，利用所述解密密钥按如下步骤进行身份认证：

1) 所述广播中心节点随机生成一个 n 维的列向量$\vec{r}$并发送给所述第 i 个代理用户节点；

2) 所述第 i 个代理用户节点收到所述列向量$\vec{r}$后计算$s=h(\vec{r}\cdot\vec{x}_i)$,并把 s 返回给所述广播中心节点,h(•) 表示哈希函数 ;

3) 所述广播中心节点根据生成的列向量$\vec{r}$及所述第 i 个代理用户节点的解密密钥$\vec{x}_i$,计算$t=h(\vec{r}\cdot\vec{x}_i)$;

4) 所述广播中心节点判断 s 是否等于 t,若相等,则身份认证成功,否则,身份认证失败。

4. 根据权利要求 1 所述的广播加密及其解密方法,其特征是,利用所述解密密钥按如下步骤解密来自广播中心节点单播的加密信息 :

1) 所述广播中心节点随机生成一个 n 维的列向量$\vec{r}$,使得$\vec{r}\cdot\vec{x}_i=m$;

2) 所述广播中心节点将所述列向量$\vec{r}$发送给第 i 个代理用户节点 ;

3) 所述第 i 个代理用户节点收到所述列向量$\vec{r}$后,计算$m=\vec{r}\cdot\vec{x}_i$;获得明文 m。

一种广播加密及其解密方法

技术领域

[0001] 本发明属于数据加密领域，具体地说是一种广播加密及其解密方法。

背景技术

[0002] 21世纪是信息时代，随着科技发展，信息越来越重要。基于通信和网络的信息系统已在政治、经济、军事等部门广泛应用。但随之而来的是安全问题。信息系统的安全一旦受到破坏，不仅会导致社会混乱，还会带来巨大的政治、经济和军事损失。众所周知，密码技术是信息安全的理论基础及核心技术。例如各种加解密、实体认证、消息鉴别等技术。它能够安全、有效地保证数据或服务的机密性、完整性、不可抵赖性等。传统的密码体制，根据加密密钥与解密密钥是否相同，可以分为两大类：对称密码和非对称密码（即公钥密码）。前者加密密钥与解密密钥相同，而后者则不同。

[0003] 不管是对称密码还是非对称密码主要涉及两方：一方加密（发送），另一方解密（接收）。但随着通信和计算技术的快速发展，出现了许多面向多方的应用环境。在这些新的环境中，因为牵涉到多方，若依旧采用传统的涉及两方的密码算法，需要的密钥数量将大大增加，而存储和管理这些密钥会带来过重的负担，也是安全上的最大隐患。由此产生了一些面向多方应用环境的新型密码或密钥管理算法，例如各种群组密码、广播加密等。其中广播加密的概念最早由Fiat等于1993年提出，它是一种在不安全信道上给一组用户传输加密信息的密码体制，它可使发送者选取特定用户集合进行广播加密，只有授权用户才能够用各自隐私的密钥解密密文。广播加密在付费电视、数字版权保护、在线游戏等方面有着重要的应用。因而它一经提出立即成为研究的焦点，各种广播加密方案相继被提出。

[0004] 与公钥密码算法相似，已有的诸多广播加密方案的安全性也是基于某个数学难题，主流的有：整数因子分解问题、离散对数问题、椭圆曲线离散对数问题等。在这些主流方法中，由于底层难题涉及很多大整数的模幂运算，因而需要花费很多的计算资源。这对于一些计算资源受限的设备或环境来说很难实现。

发明内容

[0005] 本发明为了避免现有广播加密方法所存在的不足之处，在不降低安全性的前提下，提出一种广播加密及其解密方法，能够降低加密和解密计算的复杂度，节约计算资源，从而高效、快速地实现广播加密。

[0006] 本发明为解决技术问题所采用如下的技术方案是：

[0007] 本发明一种广播加密及其解密方法的特点是，在分布式网络环境中，存在一个广播中心节点和n个代理用户节点，所述广播中心节点向所述代理用户节点广播密文；所述代理用户节点接收所述密文并进行解密；所述广播加密及其解密方法按如下步骤进行：

[0008] 步骤1：所述广播中心节点按如下步骤生成大素数p、加密密钥以及解密密钥：

[0009] 1.1）建立一个大素数p，并通过广播的方式向所述代理用户节点公开所述大素数p；

[0010] 1.2) 随机生成一个 1×n 维的矩阵 A(1<n),所述矩阵 A 中的元素为小于所述大素数 p 的非负整数;

[0011] 1.3) 随机生成一个 n 维列向量$\vec{x}_0$,利用式 (1) 获得向量$\vec{y}$:

[0012] $$\vec{y} = A\vec{x}_0 \bmod p \qquad (1)$$

[0013] 式 (1) 中,矩阵 A 和向量$\vec{y}$均为广播中心节点的加密密钥;

[0014] 1.4) 利用加密密钥 A 和$\vec{y}$,建立方程组$A\vec{x} \bmod p = \vec{y}$;

[0015] 1.5) 求解方程组$A\vec{x} \bmod p = \vec{y}$获得 n 个不同的解向量$\vec{x}_i\ (1 \le i \le n)$;所述解向量$\vec{x}_i$为第 i 个代理用户节点的解密密钥;

[0016] 步骤 2:所述广播中心节点按如下步骤获得密文:

[0017] 2.1) 随机生成一个 1 维的行向量$\vec{k} = (k_1, k_2, ..., k_l)$,$1 \leqslant k_i \leqslant p-2\ (1 \leqslant i \leqslant 1)$;

[0018] 2.2) 假设广播中心节点所需要发送的明文为 m,$m \in \{0,1,2,..,p-1\}$,根据所述加密密钥利用式 (2) 和式 (3) 获得密文$\{\vec{c}_1, c_2\}$:

[0019] $$\vec{c}_1 = \vec{k}A \bmod p \qquad (2)$$

[0020] 式 (2) 中,$\vec{c}_1$为 n 维行向量;

[0021] $$c_2 = m(\vec{k}^T \cdot \vec{y}) \bmod p \qquad (3)$$

[0022] 式 (3) 中,$\vec{k}^T$表示行向量$\vec{k}$转置后所对应的列向量,$\vec{k}^T \cdot \vec{y}$表示列向量$\vec{k}^T$与$\vec{y}$的点积运算;

[0023] 步骤 3:所述代理用户节点根据所述大素数 p 和解密密钥进行解密:

[0024] 第 i 个代理用户节点根据所接收的密文$\{\vec{c}_1, c_2\}$利用式 (4) 和式 (5) 获得明文 m:

[0025] $$c_1 = \vec{c}_1^{\,T} \cdot \vec{x}_i \bmod p \qquad (4)$$

[0026] 式 (4) 中,$\vec{x}_i$为第 i 个代理用户节点的解密密钥;$\vec{c}_1^{\,T}$表示行向量$\vec{c}_1$转置后所对应的列向量,$\vec{c}_1^{\,T} \cdot \vec{x}_i$表示列向量$\vec{c}_1^{\,T}$与$\vec{x}_i$的点积运算;

[0027] $m = c_2 / c_1 \bmod p$ (5)。

[0028] 本发明广播加密及其解密方法的特点也在于,

[0029] 所述大素数 p 按如下步骤生成:

[0030] a) 确定大素数 p 的位长 d;

[0031] b) 随机生成一个位长为 d 比特的首位和末位均为 1 的奇数 q;

[0032] c) 采用素数检测方法判断 q 是否是素数,若是则令 p=q,否则重新执行步骤 b。

[0033] 利用所述解密密钥按如下步骤进行身份认证:

[0034] 1) 所述广播中心节点随机生成一个 n 维的列向量$\vec{r}$并发送给所述第 i 个代理用户节点;

[0035] 2) 所述第 i 个代理用户节点收到所述列向量$\vec{r}$后计算$s = h(\vec{r} \cdot \vec{x}_i)$,并把 s 返回给所述广播中心节点,h(•) 表示哈希函数;

[0036] 3) 所述广播中心节点根据生成的列向量$\vec{r}$及所述第 i 个代理用户节点的解密密钥$\vec{x}_i$,计算$t = h(\vec{r} \cdot \vec{x}_i)$;

[0037] 4) 所述广播中心节点判断 s 是否等于 t,若相等,则身份认证成功,否则,身份认证失败。

[0038] 利用所述解密密钥按如下步骤解密来自广播中心节点单播的加密信息：

[0039] 1) 所述广播中心节点随机生成一个 n 维的列向量$\vec{r}$，使得$\vec{r}\cdot\vec{x}_i = m$；

[0040] 2) 所述广播中心节点将所述列向量$\vec{r}$发送给第 i 个代理用户节点；

[0041] 3) 所述第 i 个代理用户节点收到所述列向量$\vec{r}$后，计算$m = \vec{r}\cdot\vec{x}_i$；获得明文 m。

[0042] 与已有技术相比，本发明的有益效果体现在：

[0043] 1、本发明通过点积运算来代替模幂运算，大大降低了计算的复杂度，从而提高了运算速度。

[0044] 2、本发明的安全性基于推广的子集和问题(the subset sum problem)的困难性，因而比现有的基于因子分解、离散对数、椭圆曲线离散对数等问题的主流方法更安全。

[0045] 3、本发明的加密过程中的参数$\vec{k}$为随机生成，因此是一种概率加密方法，从而能够抵抗重放攻击。

[0046] 4、本发明因设置矩阵 A 的列数与向量$\vec{x}_i$的列数均为 n，即等于用户的总个数，从而能够抵抗用户的串谋攻击。

[0047] 5、本发明因代理用户节点的解密密钥互相不同，从而还具有身份认证和单播解密的功能。

具体实施方式

[0048] 本发明一种广播加密及其解密方法是在分布式网络环境中，存在一个广播中心节点和 n 个代理用户节点，广播中心节点向代理用户节点广播密文；代理用户节点接收密文并进行解密；广播加密及其解密方法按如下步骤进行：

[0049] 步骤 1：广播中心节点按如下步骤生成大素数 p、加密密钥以及解密密钥：

[0050] 1.1) 建立一个大素数 p，并通过广播的方式向代理用户节点发送大素数 p；

[0051] 大素数 p 采用如下方式生成：

[0052] a) 确定大素数 p 的位长 d，例如根据具体的安全需求，可以将位长 d 设定为 256、512 或 1024 等；

[0053] b) 随机生成一个位长为 d 的首位和末位均为 1 的奇数 q；

[0054] c) 采用素数检测方法判断 q 是否是素数，若是则令 p=q，否则重新执行 b；

[0055] 大素数 p 是广播中心节点一次生成多次利用。

[0056] 1.2) 随机生成一个 1×n 维的矩阵 A(1<n)，矩阵 A 中的元素为小于大素数 p 的非负整数；

[0057] 1.3) 随机生成一个 n 维列向量$\vec{x}_0$，利用式 (1) 获得向量$\vec{y}$：

[0058] $$\vec{y} = A\vec{x}_0 \bmod p \qquad (1)$$

[0059] 式 (1) 中，矩阵 A 和$\vec{y}$为广播中心节点的加密密钥；矩阵 A 是 1×n 维的，向量$\vec{x}_0$是 n 维的列向量，因而$\vec{y}$是一个 1 维的列向量；

[0060] 1.4) 利用加密密钥 A 和$\vec{y}$，建立方程组$A\vec{x} \bmod p = \vec{y}$；

[0061] 1.5) 求解方程组$A\vec{x} \bmod p = \vec{y}$获得 n 个不同的解向量$\vec{x}_i\ (1 \le i \le n)$；解向量$\vec{x}_i$为第 i 个代理用户节点的解密密钥；广播中心节点通过秘密信道或当面分发的方式给各代理用户节点分配解密密钥；加密密钥和解密密钥也是一次生成多次利用。

[0062] 不同代理用户节点采用不同的解密密钥的原因是：不同解密密钥可以用于身份认

证或用于解密来自广播中心节点单播的加密信息；

[0063] 身份认证的过程如下：

[0064] a) 广播中心节点随机生成一个 n 维的列向量$\vec{r}$并发送给第 i 个代理用户节点；

[0065] b) 第 i 个代理用户节点收到列向量$\vec{r}$后计算$s=h(\vec{r}\cdot\vec{x}_i)$，并把 s 返回给广播中心节点；h(•) 表示哈希函数；

[0066] c) 广播中心节点根据生成的列向量$\vec{r}$及第 i 个代理用户节点的解密密钥$\vec{x}_i$，计算$t=h(\vec{r}\cdot\vec{x}_i)$；

[0067] d) 广播中心节点验证 s 是否等于 t，若相等，则身份认证成功，否则，身份认证失败。

[0068] 指定第 i 个代理用户节点解密广播中心节点单播的加密信息的过程如下：

[0069] a) 广播中心节点随机生成一个 n 维的列向量$\vec{r}$，使得$\vec{r}\cdot\vec{x}_i=m$；

[0070] b) 广播中心节点将列向量$\vec{r}$发送给第 i 个代理用户节点；

[0071] c) 第 i 个代理用户节点收到列向量$\vec{r}$后，计算$m=\vec{r}\cdot\vec{x}_i$；从而获得明文 m；

[0072] 上述身份认证或单播解密过程只有广播中心节点指定的代理用户节点才能通过认证或正确解密。

[0073] 由式 (1) 可知$\vec{y}=A\vec{x}_0$，因而方程组$A\vec{x}=\vec{y}$有解，即$r(A)=r(\overline{A})$；$r(\cdot)$表示矩阵的秩函数，$\overline{A}$为矩阵 A 的增广矩阵；又因为 1 < n，因而 r(A) < n，所以方程组$A\vec{x}=\vec{y}$有无数解；因而可以为每个代理用户节点生成一个唯一（即互相不同）的解向量$\vec{x}_i$作为其隐私的解密密钥；

[0074] 此外，为了抵抗代理用户节点的串谋攻击，规定矩阵 A 的列数与向量$\vec{x}_i$的列数均为 n，即等于用户的总个数，理由如下：

[0075] 假定所有 n 个用户串谋，想计算中心的加密密钥 A 和$\vec{y}$，故此他们堆积所有的隐私解密密钥形成如下方程组：

[0076]
$$\begin{cases} A\vec{x}_1=\vec{y} \\ A\vec{x}_2=\vec{y} \\ \quad\vdots \\ A\vec{x}_n=\vec{y} \end{cases}$$

[0077] 上述方程组里，未知变量总数为 1×n+1 个（即矩阵 A 和向量$\vec{y}$的元素个数），而方程的总个数为 1×n 个；此时方程个数小于未知量个数，因而即使所有 n 个用户串谋也不能够计算出 A 和$\vec{y}$；但若有 n+1 个用户参与，则方程的总个数为 1×(n+1)，大于未知变量总数 1×n+1，进而通过求解方程组能够计算出 A 和$\vec{y}$；

[0078] 步骤 2：广播中心节点按如下步骤获得密文：

[0079] 2.1) 随机生成一个 1 维的行向量$\vec{k}=(k_1,k_2,...,k_l)$，$1\leqslant k_i\leqslant p-2(1\leqslant i\leqslant 1)$；

[0080] 行向量$\vec{k}$随机生成，这样即使是相同的明文，所对应的密文也不同，即是一种概率加密方法，因而能够抵抗重放攻击；

[0081] 2.2) 假设广播中心节点所需要发送的明文为 m，m ∈ {0,1,2,...,p-1}，利用式 (2) 和式 (3) 获得密文$\{\vec{c}_1,c_2\}$：

[0082] $$\vec{c}_1=\vec{k}A \bmod p \qquad (2)$$

[0083] 式 (2) 中，$\vec{c}_1$为 n 维行向量；

[0084] $$c_2 = m(\vec{k}^T \cdot \vec{y}) \bmod p \qquad (3)$$

[0085] 式 (3) 中，$\vec{k}^T$表示行向量$\vec{k}$转置后所对应的列向量，$\vec{k}^T \cdot \vec{y}$表示列向量$\vec{k}^T$与$\vec{y}$的点积运算，即$\vec{k}^T \cdot \vec{y} = \sum_{i=1}^{l} k_i y_i$；

[0086] 步骤 3：代理用户节点根据大素数 p 和解密密钥进行解密：

[0087] 第 i 个代理用户节点根据所接收的密文$\{\vec{c}_1, c_2\}$利用式 (4) 和式 (5) 获得明文 m：

[0088] $$c_1 = \vec{c}_1^{\,T} \cdot \vec{x}_i \bmod p \qquad (4)$$

[0089] 式 (4) 中，$\vec{x}_i$为第 i 个代理用户节点的解密密钥；$\vec{c}_1^{\,T}$表示行向量$\vec{c}_1$转置后所对应的列向量，$\vec{c}_1^{\,T} \cdot \vec{x}_i$表示列向量$\vec{c}_1^{\,T}$与$\vec{x}_i$的点积运算；

[0090] $m = c_2 / c_1 \bmod p \qquad (5)$

[0091] 上述广播加密及其解密方法的最大优势是不需要模幂运算，只需若干次模乘运算；尤其是代理用户节点解密过程非常简单，只需一次点积和一次模除运算，其正确性证明如下：

[0092] 令$\vec{k} = (k_1, k_2, ..., k_l)$，$\vec{y}^T = (y_1, y_2, ..., y_l)$，则

[0093] $$\vec{k}^T \cdot \vec{y} = \begin{pmatrix} k_1 \\ k_2 \\ \vdots \\ k_{n^*} \end{pmatrix} \cdot \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{n^*} \end{pmatrix} = (k_1 y_1 + k_2 y_2 + ... + k_l y_l) \bmod p \qquad (6)$$

[0094] 令矩阵$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{l,1} & a_{l,2} & \cdots & a_{l,n} \end{bmatrix}$，向量$\vec{x}_i = \begin{pmatrix} x_{i_1} \\ x_{i_2} \\ \vdots \\ x_{i_n} \end{pmatrix}$；因为 $\vec{x}_i$ 是线性方程组 $A\vec{x} \bmod p = \vec{y}$ 的一个解向量，故有$A\vec{x}_i \bmod p = \vec{y}$，即

[0095] $$\begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{l,1} & a_{l,2} & \cdots & a_{l,n} \end{bmatrix} \begin{pmatrix} x_{i_1} \\ x_{i_2} \\ \vdots \\ x_{i_n} \end{pmatrix} \bmod p = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_l \end{pmatrix} \qquad (7)$$

[0096] $$\begin{cases} (a_{1,1} x_{i_1} + a_{1,2} x_{i_2} + ... + a_{1,n} x_{i_n}) \bmod p = y_1 \\ (a_{2,1} x_{i_1} + a_{2,2} x_{i_2} + ... + a_{2,n} x_{i_n}) \bmod p = y_2 \\ \vdots \\ (a_{l,1} x_{i_1} + a_{l,2} x_{i_2} + ... + a_{l,n} x_{i_n}) \bmod p = y_l \end{cases} \qquad (8)$$

[0097] 把$\vec{c}_1 = \vec{k}A \bmod p$代入$c_1 = \vec{c}_1^{\,T} \cdot \vec{x}_i \bmod p$得：

[0098] $$c_1=(\vec{k}A)^T\cdot\vec{x}_i=[(k_1,k_2,...,k_l)\begin{bmatrix}a_{1,1}&a_{1,2}&\cdots&a_{1,n}\\a_{2,1}&a_{2,2}&\cdots&a_{2,n}\\\vdots&\vdots&\vdots&\vdots\\a_{l,1}&a_{l,2}&\cdots&a_{l,n}\end{bmatrix}]^T\cdot\begin{pmatrix}x_{i_1}\\x_{i_2}\\\vdots\\x_{i_n}\end{pmatrix}$$

[0099] $$=\begin{pmatrix}k_1a_{1,1}+k_2a_{2,1}+...+k_la_{l,1}\\k_1a_{1,2}+k_2a_{2,2}+...+k_la_{l,2}\\\vdots\\k_1a_{1,n}+k_2a_{2,n}+...+k_la_{l,n}\end{pmatrix}\cdot\begin{pmatrix}x_{i_1}\\x_{i_2}\\\vdots\\x_{i_n}\end{pmatrix}$$

[0100] $$=(k_1a_{1,1}+k_2a_{2,1}+...+k_la_{l,1})x_{i_1}+(k_1a_{1,2}+k_2a_{2,2}+...+k_la_{l,2})x_{i_2}+...$$

[0101] $$+(k_1a_{1,n}+k_2a_{2,n}+...+k_la_{l,n})x_{i_n}$$

[0102] $$=k_1(a_{1,1}x_{i_1}+a_{1,2}x_{i_2}+...+a_{1,n}x_{i_n})+k_2(a_{2,1}x_{i_1}+a_{2,2}x_{i_2}+...+a_{2,n}x_{i_n})+...$$

[0103] $$+k_l(a_{l,1}x_{i_1}+a_{l,2}x_{i_2}+...+a_{l,n}x_{i_n})$$

[0104] $$=(k_1y_1+k_2y_2+...+k_ly_l)\bmod p$$（根据式（8））　　(9)

[0105] 根据式（6）和（9），必有$c_1=\vec{k}^T\cdot\vec{y}$且

[0106] $$m=\frac{c_2}{c_1}\bmod p$$

[0107] $$=\frac{m(\vec{k}^T\cdot\vec{y})}{c_1}\bmod p$$

[0108] $$=\frac{m(k_1y_1+k_2y_2+...+k_ly_l)}{(k_1y_1+k_2y_2+...+k_ly_l)}\bmod p$$

[0109] $$=m$$

[0110] 本发明广播加密及其解密方法的安全性基于推广的子集和问题（the subset sum problem）的困难性。推广的子集和问题定义及说明如下：

[0111] 假定随机向量$\vec{a}\in Z_p^n$及$\vec{s}\in\{0,1\}^n$，$t=\vec{a}\cdot\vec{s}\bmod p$，所述子集和问题为：已知$\vec{a}$和t，求$\vec{s}$。这里我们把子集和问题推广到更一般的情形。假定随机向量$\vec{a}\in Z_p^n$及$\vec{s}\in Z_p^n$，$t=\vec{a}\cdot\vec{s}\bmod p$，则更一般的子集和问题或推广的子集和问题为：已知$\vec{a}$和t，求$\vec{s}$。尽管已有快速的量子算法求解因子分解问题、离散对数问题及椭圆曲线离散对数问题，但还没有快速求解子集和问题的量子算法。推广的子集和问题被认为是比上述困难问题还要难的困难性问题。因此，本发明比现有的基于因子分解、离散对数、椭圆曲线离散对数等问题的主流方法更安全。