(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 9 月 3 日 (03.09.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/173062 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01)

(21) 国际申请号: PCT/CN2019/102934

(22) 国际申请日: 2019 年 8 月 28 日 (28.08.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910140289.X 2019年2月26日 (26.02.2019) CN

(71) 申请人: 清华大学(TSINGHUA UNIVERSITY) [CN/CN]; 中国北京市海淀区清华园清华大学, Beijing 100084 (CN)。

(72) 发明人: 王小云 (WANG, Xiaoyun); 中国北京市海淀区清华园清华大学, Beijing 100084 (CN)。王安宇 (WANG, Anyu); 中国北京市海淀区清华园清华大学, Beijing 100084 (CN)。孙悦 (SUN, Yue); 中国北京市海淀区清华园清华大学, Beijing 100084 (CN)。

(74) 代理人: 北京竹辰知识产权代理事务所（普通合伙）(BEIJING ZHUCHEN IP FIRM); 中国北京市北清路68号用友产业园北区16A四层聂鹏, Beijing 100094 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,

(54) **Title:** ERROR COORDINATION METHOD FOR LWE PUBLIC KEY CRYPTOGRAPHY

(54) 发明名称: 一种用于LWE公钥密码的错误协调方法

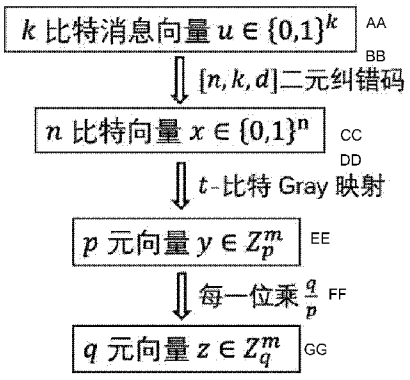

图 1

A k-bit message vector u ∈ $\{0,1\}^k$
BB [n,k,d] binary error correction code
CC n-bit vector x ∈ $\{0,1\}^n$
DD t-bit Gray mapping
EE p-nary vector y ∈ Z_p^m
FF Each bit is multiplied by q/p
GG q-nary vector z ∈ Z_p^m

(57) Abstract: Disclosed is an error coordination method for LWE public key cryptography. The method comprises an encoding algorithm and a decoding algorithm, wherein the input of the encoding algorithm is a binary message vector u $\in \{0,1\}^k$ with the length being k, and the output thereof is a q-nary vector z $\in Z_q^m$ with the length being m, where $Z_q = \{-q/2,\ldots,q/2-1\}$; and the input of the decoding algorithm is a q-nary vector w $= z+e \in Z_q^m$ that includes an error and has the length of m, and the output thereof is a binary vector u $\in \{0,1\}^k$ corresponding to z. According to the error coordination method for LWE public key cryptography provided in the present invention, a binary linear code is combined with a Gray code to realize an error coordination scheme in LWE public key cryptography. The error coordination method includes an encoding algorithm and a decoding algorithm, which can be used for solving an error coordination problem in LWE public key cryptography. The solution of the present invention realizes a good fault-tolerance performance and can obviously improve the transmission rate of encrypted information.

(57) 摘要: 本发明公开了一种用于LWE公钥密码的错误协调方法，该方法包括编码算法和译码算法；其中，编码算法的输入为一个长度为k的二元消息向量u∈$\{0,1\}^k$，输出为一个长度为m的q元向量z∈Z_q^m，这里$Z_q=\{-q/2,\cdots,q/2-1\}$；译码算法的输入为一个包含错误的长度为m的q元向量w＝z+e∈Z_q^m，输出为z对应的二元向量u∈$\{0,1\}^k$；本发明提供的用于LWE公钥密码的错误协调方法通过将二元线性码与格雷码结合用以实现LWE公钥密码中的错误协调方案。该错误协调方法包含编码算法和译码算法，可用于解决LWE公钥密码中的错误协调问题。本发明的方案容错性能好，能够显著提高加密信息的传输速率。

WO 2020/173062 A1

[见续页]

GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) **指定国**(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

一种用于LWE公钥密码的错误协调方法

本申请要求于2019年2月26日提交中国专利局、申请号为201910140289.X，发明名称为“一种用于 LWE 公钥密码的错误协调方法”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本发明涉及密码学技术领域，尤其涉及一种用于LWE公钥密码的错误协调方法。

背景技术

近年来，随着量子计算理论的发展，现有公钥密码体制在量子计算模型下的安全性受到了极大的挑战。例如目前广泛使用的 RSA 公钥密码体制或椭圆曲线公钥密码体制，其依赖的困难数学问题——大整数分解或椭圆曲线群上的离散对数问题，在量子计算模型下均存在多项式时间的高效求解算法。这促使研究人员开始设计能够抵抗量子计算机攻击的密码，即“后量子密码”。目前,后量子密码的研究已成为一个极重要和活跃的新兴密码学方向,许多发达国家已着力加强后量子密码的研究,并设立了各类重大研究支持计划。美国国家安全局(NSA)已于2015年8月宣布了抗量子密码算法的迁移计划。同年,美国国家标准与技术研究院(NIST)开启了后量子密码算法的征集与评估。根据底层困难数学问题的不同,后量子密码主要可以分为:基于编码的密码,基于格的密码,基于哈希的密码,以及基于多变量的密码。LWE公钥密码是一类重要的基于格的后量子公钥密码。

基于LWE问题设计公钥密码算法的一个关键是错误协调问题。例如 Alice 将消息 u 通过 LWE 公钥密码加密为密文 v，并将 v 发送给接收方 Bob，Bob 在解密密文 v 时通过计算只能得到 w＝u+e，这里 e 为高斯错误。错误协调问题即从向量 w＝u+e 中消除错误 e 得到消息 u 的问题。一方面，方案中引入的错误在安全性上是必须的，错误对于 LWE 问题在量子计算模型下的困难性有关键作用,没有错误则此方案可被攻击者轻易破解；另一方面,合法的接收方 Bob 又需要能够有效的消除错误，否则错误的存在会使接收方只能得到信息的近似值，从而导致通信无法正常进行。现有的错误协调方案是将消息的每个比特信息直接分散到整数区间{-q/2,…,q/2-1}中，再传输分散之后的信息。如目前常用的 Peikert 错误协调方案中，Alice 首先将消息 u 的每一比特按照规则 0->0；1->-q/2 进行映射，得到向量 u′ 然后加密并传输给 Bob。Bob 在解密时通过计算得到 w=u′+e，然后对向量 w 按照规则 {-q/4, … ,q/4-1}->0；{-q/2,…,-q/4-1}U{q/4,…,q/2-1}->1 进行映射并得到消息 u。

在现有的错误协调方案中，消息接收方解码成功的关键是错误 e 不能超出既定的范围。如 Peikert 错误协调方案中，要求错误 e 的每一位都必须处在整数区间

{-q/4,…,q/4-1}中，否则无法成功解码。而在 LWE 公钥密码算法的设计中，错误 e 是一个满足高斯分布的向量，其范围需按照算法的安全级别预先确定。因此在设计错误协调方案时，为确保解密成功，一种方法是选取较大的 q，这将导致密文较大；另一种方法是降低每次传输的明文比特数，这两种方法都将导致传输速率的损失。

发明内容

针对上述现有技术中存在的不足之处，本发明提供一种用于 LWE 公钥密码的错误协调方法，通过将二元线性码与格雷码结合用以实现 LWE 公钥密码中的错误协调方案。

该用于 LWE 公钥密码的错误协调方法包括编码算法和译码算法；其中，所述编码算法的输入为一个长度为 k 的二元消息向量 $u\in\{0,1\}^k$，输出为一个长度为 m 的 q 元向量 $z\in Z_q^m$，这里 $Z_q=\{-q/2,\cdots,q/2-1\}$；所述译码算法的输入为一个包含错误向量 e 的长度为 m 的 q 元向量 $w=z+e\in Z_q^m$，输出为 z 对应的二元向量 $u\in\{0,1\}^k$；

所述编码算法包括以下步骤：

步骤一、使用一个[n,k,d]二元线性码的编码器，将二元向量 u 映射为一个长度为 n 的二元向量 $x\in\{0,1\}^n$；

步骤二、使用一个 t-比特格雷码，将二元向量 x 的每 t 个比特映射为一个 Z_p 上的整数，从而得到一个长度为 m 的 p 元向量 $y\in Z_p^m$；这里参数需满足关系：$n=t\times m$，$p=2^t$，p 整除 q;

步骤三、将向量 y 每一位乘以 q/p，得到一个长度为 m 的 q 元向量 $z\in Z_q^m$；

所述译码算法包括以下步骤：

步骤一、将向量 w 的每一位除以 q/p，然后根据预设取整方式取整，得到一个长度为 m 的 p 元向量 $y'\in Z_p^m$；

步骤二、使用 t-比特格雷码，将向量 $y'\in Z_p^m$ 的每一位拆分为 t 个比特，从而得到一个长度为 n 的二元向量 $x'\in\{0,1\}^n$；

步骤三、使用[n,k,d]二元线性码的译码器，从二元向量 $x'\in\{0,1\}^n$ 中恢复出消息向量 u。

可选地，所述预设取整方式为四舍五入取整方式。

进一步地，所述编码算法中的输入消息的长度 k 和输出消息的模数 q 由 LWE 公钥密码算法的安全级别事先确定；此外，错误向量 e 的范围也由 LWE 公钥密码算法的安全级别确定。

进一步地，参数[n,k,d]二元线性码和 t-比特格雷码，以及由[n,k,d]二元线性码和 t-比特格雷码确定的参数 $p=2^t$，$m=n/t$ 的选取步骤包括：

步骤一、任取一个 t-比特格雷码，使得 t>1 且 $p=2^t$ 整除 q；

步骤二、根据所述译码算法中的步骤一、步骤二和错误向量 e 的范围计算所对应的二元信道的容量；

步骤三、根据二元信道容量选取相应的[n,k,d]二元线性码，使得译码错误概率满足 LWE 公钥密码算法的安全级别要求；

步骤四、计算参数 m=n/t，并判断对应的密文大小是否满足 LWE 公钥密码算法的通信效率要求；如不满足则选取新的 t-比特格雷码并重复上述步骤。

本发明提供的用于 LWE 公钥密码的错误协调方法，通过将二元线性码与格雷码结合用以实现 LWE 公钥密码中的错误协调方案。该错误协调方法包含编码算法和译码算法，可用于解决 LWE 公钥密码中的错误协调问题。本发明的方案容错性能好，能够显著提高加密信息的传输速率。

附图说明

图 1 为本发明实施例提供的用于 LWE 公钥密码的错误协调方法中的编码算法流程图；

图 2 为本发明实施例提供的用于 LWE 公钥密码的错误协调方法中的译码算法流程图；

图 3 为本发明实施例提供的用于 LWE 公钥密码的错误协调方法中的参数选取步骤流程图。

具体实施方式

为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明的一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都属于本发明保护的范围。

请参阅图 1 和图 2，本实施例提供一种用于 LWE 公钥密码的错误协调方法，其包含编码算法(如图 1 所示)和译码算法(如图 2 所示)两个部分。其中编码算法的输入为一个长度为 k 的二元消息向量 $u\in\{0,1\}^k$，输出为一个长度为 m 的 q 元向量 $z\in Z_q^m$，这里 $Z_q=\{-q/2,\cdots,q/2-1\}$。译码算法的输入为一个包含错误向量 e 的长度为 m 的 q 元向量 $w=z+e\in Z_q^m$，输出为 z 对应的二元向量 $u\in\{0,1\}^k$。具体地，编码算法和译码算法的步骤分别如下：

编码算法：

步骤一、使用一个[n,k,d]二元线性码的编码器，将二元向量 u 映射为一个长度为 n 的二元向量 $x\in\{0,1\}^n$ 。

步骤二、使用一个 t-比特格雷码(Gray code)，将二元向量 x 的每 t 个比特映射为一个 Z_p 上的整数，从而得到一个长度为 m 的 p 元向量 $y\in Z_p^m$ 。这里参数需满足关系 $n=t\times m$，$p=2^t$ ，p 整除 q。

步骤三、将向量 y 每一位乘以 q/p，得到一个长度为 m 的 q 元向量 $z\in Z_q^m$ 。

译码算法：

步骤一、将向量 w 的每一位除以 q/p，然后取整，得到一个长度为 m 的 p 元向量 $y'\in Z_p^m$ 。这里取整指四舍五入取整(即 Round 取整)，例如 2.4 取整得 2，-3.6 取整得-4。

步骤二、使用 t-比特格雷码(Gray code)，将向量 $y'\in Z_p^m$ 的每一位拆分为 t 个比特，从而得到一个长度为 n 的二元向量 $x'\in\{0,1\}^n$ 。

步骤三、使用[n,k,d]二元线性码的译码器，从二元向量 $x'\in\{0,1\}^n$ 中恢复出消息向量 u。

参数选取：

错误协调方案中输入消息的长度 k 和输出消息的模数 q 已由 LWE 公钥密码算法的安全级别事先确定，此外错误向量 e 的范围也由安全级别确定。因此需要在错误协调方案中确定的参数包括一个[n,k,d]二元线性码和一个 t-比特格雷码，以及由这些参数确定的 $p=2^t$ ，$m=n/t$。参数选取的步骤如图 3 所示，其包括以下步骤：

步骤一、任取一个 t-比特格雷码，使得 $t>1$ 且 $p=2^t$ 整除 q。

步骤二、根据译码算法的步骤一、步骤二和错误向量 e 的范围计算所对应的二元信道的容量。

步骤三、根据二元信道容量选取相应的[n,k,d]二元线性码，使得译码错误概率满足 LWE 公钥密码算法的安全级别要求。

步骤四、计算参数 $m=n/t$，并判断对应的密文大小是否满足 LWE 公钥密码算法的通信效率要求。如不满足则选取新的 t-比特格雷码并重复上述步骤。

值得一提的是，本实施例的上述方案采用的二元线性码与格雷码结合可替换为 q 元线性码(或非线性码)与 q 元格雷码结合，该替代方案同样可实现 LWE 公钥密码中的错误协调，其原理与本实施例的上述方案的原理相同。

本实施例提供的用于 LWE 公钥密码的错误协调方法，通过将二元线性码与格雷码结合用以实现 LWE 公钥密码中的错误协调方案。该错误协调方法包含编码算法和译码算法，可用于解决 LWE 公钥密码中的错误协调问题。本发明的方案容错性能好，

能够显著提高加密信息的传输速率。

此外，需要说明的是，本发明实施例中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者终端设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者终端设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者终端设备中还存在另外的相同要素。

以上仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域技术人员来说，本发明可有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

权 利 要 求 书

1.一种用于LWE公钥密码的错误协调方法，其特征在于，所述错误协调方法包括编码算法和译码算法；其中，所述编码算法的输入为一个长度为k的二元消息向量$u\in\{0,1\}^k$，输出为一个长度为m的q元向量$z\in Z_q^m$，这里$Z_q=\{-q/2,\cdots,q/2-1\}$；所述译码算法的输入为一个包含错误向量e的长度为m的q元向量$w=z+e\in Z_q^m$，输出为z对应的二元向量$u\in\{0,1\}^k$；

所述编码算法包括以下步骤：

步骤一、使用一个[n,k,d]二元线性码的编码器，将二元向量u映射为一个长度为n的二元向量$x\in\{0,1\}^n$；

步骤二、使用一个t-比特格雷码，将二元向量x的每t个比特映射为一个Z_p上的整数，从而得到一个长度为m的p元向量$y\in Z_p^m$；这里参数需满足关系：$n=t\times m$，$p=2^t$，p整除q；

步骤三、将向量y每一位乘以q/p，得到一个长度为m的q元向量$z\in Z_q^m$；

所述译码算法包括以下步骤：

步骤一、将向量w的每一位除以q/p，然后根据预设取整方式取整，得到一个长度为m的p元向量$y'\in Z_p^m$；

步骤二、使用t-比特格雷码，将向量$y'\in Z_p^m$的每一位拆分为t个比特，从而得到一个长度为n的二元向量$x'\in\{0,1\}^n$；

步骤三、使用[n,k,d]二元线性码的译码器，从二元向量$x'\in\{0,1\}^n$中恢复出消息向量u。

2.如权利要求1所述的用于LWE公钥密码的错误协调方法，其特征在于，所述预设取整方式为四舍五入取整方式。

3.如权利要求1所述的用于LWE公钥密码的错误协调方法，其特征在于，所述编码算法中的输入消息的长度k和输出消息的模数q由LWE公钥密码算法的安全级别事先确定；此外，错误向量e的范围也由LWE公钥密码算法的安全级别确定。

4.如权利要求1所述的用于LWE公钥密码的错误协调方法，其特征在于，参数[n,k,d]二元线性码和t-比特格雷码，以及由[n,k,d]二元线性码和t-比特格雷码确定的参数$p=2^t$，$m=n/t$的选取步骤包括：

步骤一、任取一个t-比特格雷码，使得$t>1$且$p=2t$整除q；

步骤二、根据所述译码算法中的步骤一、步骤二和错误向量e的范围计算所对应的二元信道的容量；

步骤三、根据二元信道容量选取相应的[n,k,d]二元线性码，使得译码错误概率满足

LWE 公钥密码算法的安全级别要求；

步骤四、计算参数 m＝n/t，并判断对应的密文大小是否满足 LWE 公钥密码算法的通信效率要求；如不满足则选取新的 t-比特格雷码并重复上述步骤。

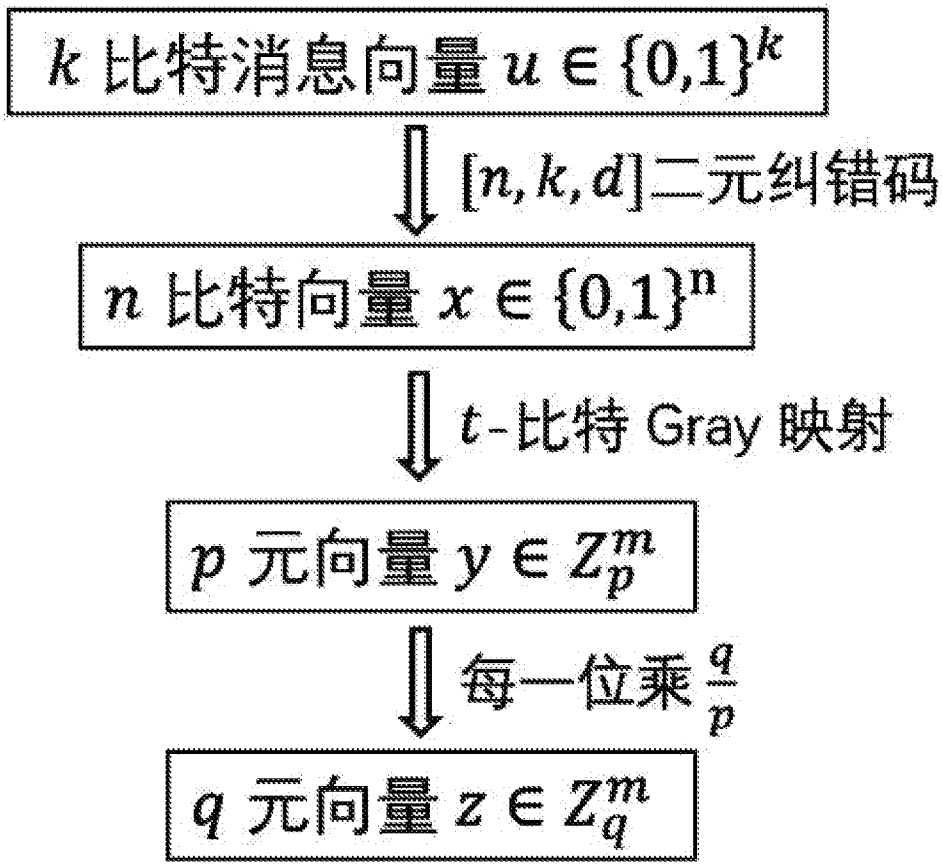
k 比特消息向量 $u \in \{0,1\}^k$
$[n,k,d]$二元纠错码
n 比特向量 $x \in \{0,1\}^n$
t-比特 Gray 映射
p 元向量 $y \in Z_p^m$
每一位乘 $\frac{q}{p}$
q 元向量 $z \in Z_q^m$

图 1

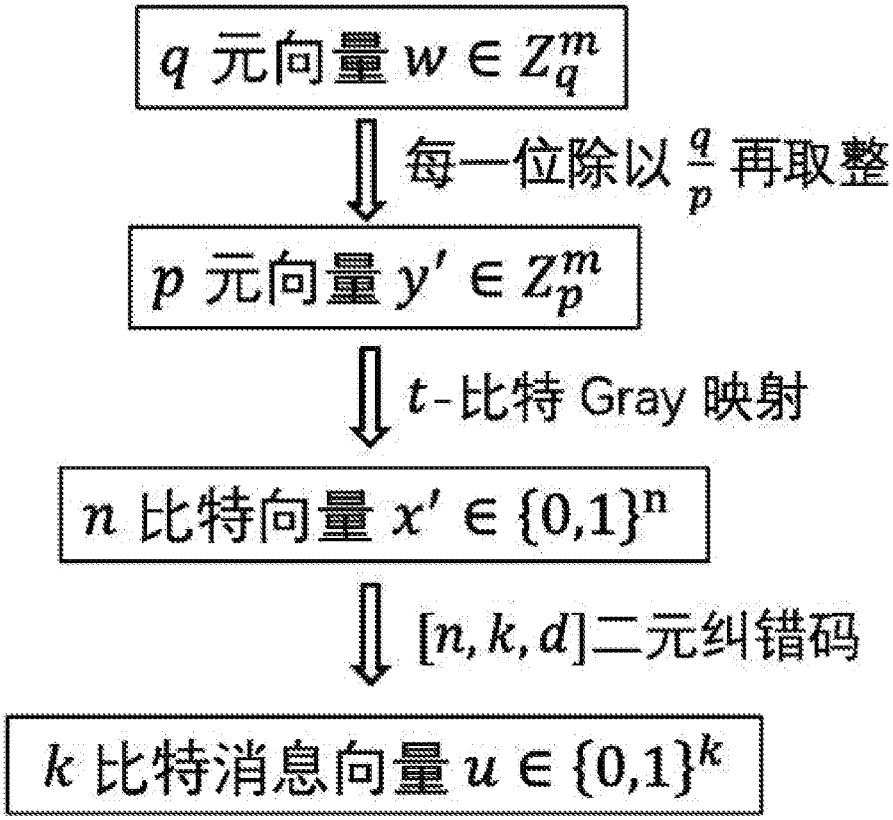
q 元向量 $w \in Z_q^m$
每一位除以 $\frac{q}{p}$ 再取整
p 元向量 $y' \in Z_p^m$
t-比特 Gray 映射
n 比特向量 $x' \in \{0,1\}^n$
$[n,k,d]$二元纠错码
k 比特消息向量 $u \in \{0,1\}^k$

图 2

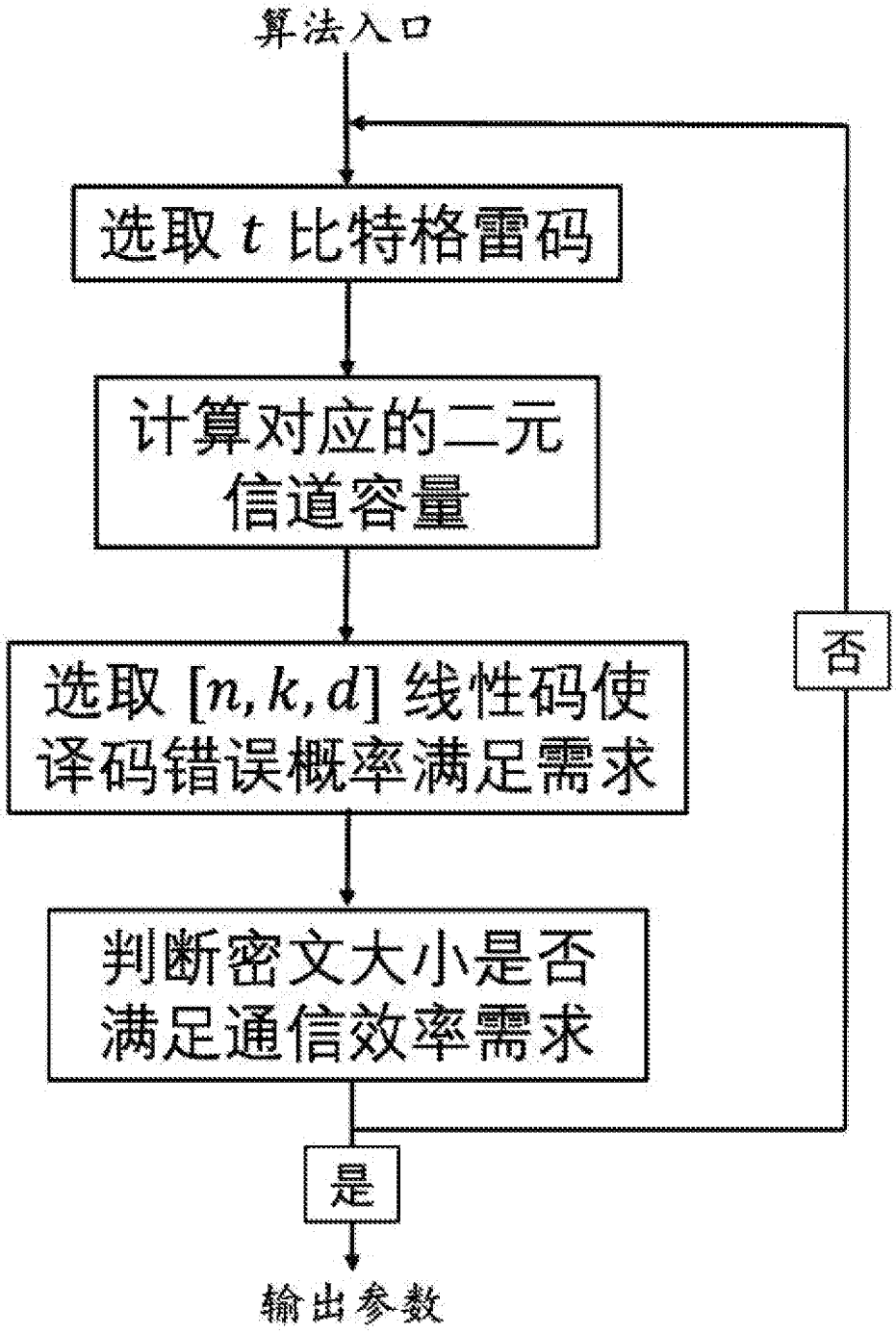
算法入口
选取 t 比特格雷码
计算对应的二元信道容量
选取 $[n,k,d]$ 线性码使译码错误概率满足需求
判断密文大小是否满足通信效率需求
否
是
输出参数

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/102934

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNKI, CNPAT: 公钥, 密码, 错误, 编码, 译码, 格雷, 比特, 映射, 向量, key, error, decode, mapping, vector, encode

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109861821 A (TSINGHUA UNIVERSITY) 07 June 2019 (2019-06-07) description, paragraphs [0005]-[0021], and claims 1-4	1-4
A	CN 101321058 A (GUAN, Haiming et al.) 10 December 2008 (2008-12-10) description, page 11, line 6 to page 12, line 1	1-4
A	CN 106341208 A (UNIVERSITY OF CHINESE ACADEMY OF SCIENCES) 18 January 2017 (2017-01-18) entire document	1-4
A	CN 104396184 A (DING, Jintai) 04 March 2015 (2015-03-04) entire document	1-4
A	US 2014074719 A1 (FORTRESS GB LTD.) 13 March 2014 (2014-03-13) entire document	1-4

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 October 2019	**31 October 2019**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/102934

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109861821 A	07 June 2019	None	
CN 101321058 A	10 December 2008	WO 2008148275 A1	11 December 2008
CN 106341208 A	18 January 2017	None	
CN 104396184 A	04 March 2015	WO 2013152725 A1	17 October 2013
		US 2015067336 A1	05 March 2015
		KR 20150032928 A	31 March 2015
		TW 201404106 A	16 January 2014
		EP 2837128 A1	18 February 2015
US 2014074719 A1	13 March 2014	CN 103608829 A	26 February 2014
		GB 201314465 D0	25 September 2013
		WO 2012098543 A2	26 July 2012

国际检索报告

国际申请号
PCT/CN2019/102934

A. 主题的分类

H04L 9/32(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

WPI,EPODOC,CNKI,CNPAT:公钥，密码，错误，编码，译码，格雷，比特，映射，向量，key，error，decode，mapping，vector，encode

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 109861821 A (清华大学) 2019年 6月 7日 (2019-06-07) 说明书第[0005]-[0021]段，权利要求1-4项	1-4
A	CN 101321058 A (管海明等) 2008年 12月 10日 (2008-12-10) 说明书第11页第6行-第12页第1行	1-4
A	CN 106341208 A (中国科学院大学) 2017年 1月 18日 (2017-01-18) 全文	1-4
A	CN 104396184 A (丁津泰) 2015年 3月 4日 (2015-03-04) 全文	1-4
A	US 2014074719 A1 (FORTRESS GB LTD.) 2014年 3月 13日 (2014-03-13) 全文	1-4

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2019年 10月 14日	2019年 10月 31日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 吕源 电话号码 86-(10)-53961640

表 PCT/ISA/210 (第2页) (2015年1月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/102934

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	109861821	A	2019年 6月 7日		无		
CN	101321058	A	2008年 12月 10日	WO	2008148275	A1	2008年 12月 11日
CN	106341208	A	2017年 1月 18日		无		
CN	104396184	A	2015年 3月 4日	WO	2013152725	A1	2013年 10月 17日
				US	2015067336	A1	2015年 3月 5日
				KR	20150032928	A	2015年 3月 31日
				TW	201404106	A	2014年 1月 16日
				EP	2837128	A1	2015年 2月 18日
US	2014074719	A1	2014年 3月 13日	CN	103608829	A	2014年 2月 26日
				GB	201314465	D0	2013年 9月 25日
				WO	2012098543	A2	2012年 7月 26日