密码学进展—CHINACRYPT'94

第三届中国密码学学术会议论文集

肖国镇　戴宗铎　王育民 编

科学出版社

密码学进展——CHINACRYPT'94

第三届中国密码学学术会议论文集

肖国镇　戴宗铎　王育民 编

科学出版社

1994

（京）新登字 092 号

内 容 简 介

本书为第三届中国密码学学术会议论文集，收录论文 43 篇及特邀报告 2 篇，内容涉及密码学的各个领域，其中包括与密码学有关的数学和计算机科学，以及密码学在信息安全方面的应用.

主要内容有：密码分析，密码体制，认证码，自动机密码，序列与线性复杂性，线性阵列，与密码学有关的数论、统计、组合和逻辑问题，复杂性理论，密码学的实际应用等.

本书可供从事密码、信息安全、数学、计算机通信专业的科技人员和高等院校相关专业的师生参考.

新华书店北京发行所发行　各地新华书店经售

*

1994 年 10 月第　一　版　　开本：787×1092 1/16

1994 年 10 月第一次印刷　　印张：19 1/8

印数：1－1 000　　字数：440 000

ISBN 7-03-004363-4/TP・398

定价：25.00 元

前　言

第三届中国密码学学术会议(1994 年 11 月 11～15 日在西安举行)上提出的论文涉及密码学的各个领域,其中包括与密码学有关的数学、通信和计算机科学,以及密码学在信息安全方面的应用等内容.

本书收录的 43 篇论文和 2 篇特邀报告对上述各个方面进行较为深入的论述.本届会议共收到论文 69 篇,每篇论文均由程序委员会指定两名专家评审.1994 年 3 月 20 日在北京召开了程序委员会会议,对各篇文章进行了分析,并作出了最后选择.

我们衷心感谢所有投稿者对会议的关心和支持!衷心感谢程序委员会的同行和所有的论文评审者的辛勤工作.感谢任南衡、陶仁骐、裴定一等教授提出的宝贵意见和建议.最后,还要感谢信息安全国家重点实验室的同志们,特别是西安电子科技大学信息保密研究所的同志们在会议的安排和组织方面所付出的辛勤劳动.

第三届密码学学术会议程序委员会

主　席　肖国镇　西安电子科技大学

副主席　王育民　西安电子科技大学

戴宗铎　中国科学院研究生院

委　员　（以姓氏笔划为序）

王蓉芳　北京大学

王新梅　西安电子科技大学

冯克勤　中国科学技术大学

卢开澄　清华大学

刘木兰　中国科学院系统科学研究所

朱　洪　复旦大学

沈世镒　南开大学

杨义先　北京邮电学院

周锦君　郑州信息工程学院

龚奇敏　机电部30所

黄民强　中国科学院系统科学研究所

曹祖良　中国科学院软件研究所

曹珍富　哈尔滨工业大学

卿斯汉　中国科学院计算中心

目　　录

密码分析

单钥密码体制

双钥密码体制

认证码

自动机密码

序列、线性复杂度和阵列

数论、代数与统计

布尔函数

复杂性理论

密码的实际应用

关于广义码公钥密码体制的密码分析[1)]

李大兴　王小云

（山东大学数学系，济南　250100）

（信息安全国家重点实验室，北京　100039）

摘要　在许多种公钥密码被破译的今天，人们对基于编码理论的公钥密码体制逐渐加以重视．但至今所提出的各种与编码有关的体制几乎都是McEliece体制[1]的变形．史晓明同志利用推广的线性码译码的困难性设计了一种颇有新意的公钥密码体制[2]（本文简称之为广义码体制）．我们对该体制进行了初步分析，结果表明该体制可以被彻底攻破．在对该体制的分析过程中，我们主要利用了欧几里德算法与"逐步求精"法来解出该体制的一对等价解密密钥，从而破译了该密码体制．或许这种攻击思想能对读者分析其它体制有所帮助，因此特写成此文供读者参考．

关键词　密码分析　公钥密码　广义线性码

一. 广义码公钥体制简介

取适当的自然数 m,n 使 n 为偶数且有 $\frac{n}{2}<m<n$.

任取两个正整数 n_1,n_2，使 $\mathrm{GCD}(n_1,n_2)=1$．由孙子定理求出 a_1,a_2 满足 $1\leqslant a_1,a_2<n_1n_2$，且下列两个同余方程组成立：

$$\begin{cases} a_1 \equiv 1 \pmod{n_1} \\ a_1 \equiv 0 \pmod{n_2} \end{cases} \tag{1}$$

$$\begin{cases} a_2 \equiv 0 \pmod{n_1} \\ a_2 \equiv 1 \pmod{n_2} \end{cases} \tag{2}$$

取两个 $\frac{n}{2}$ 阶非负整数随机方阵 B_1 和 B_2，做 $n\times m$ 阶矩阵 A_0：

---

1)　本课题为国家教委博士点基金资助的课题．

$$A_0=\begin{pmatrix} a_1 I_{\frac{n}{2}}+a_2 n_2 B_1, & 0 \\ a_2 I_{\frac{n}{2}}+a_1 n_1 B_2, & 0 \end{pmatrix}=\begin{pmatrix} A_1 \\ A_2 \end{pmatrix}$$

任取两个 m 阶正整数可逆方阵 E_1 和 E_2，令

$$A=\begin{pmatrix} A_1 E_1 \\ A_2 E_2 \end{pmatrix}$$

取 $l\leqslant\min\{n_1,n_2\}-1$ 及 $k<n$，将 l,k,A 公开，作为加密密钥. $n_1,n_2,a_1,a_2,B_1,B_2,E_1,E_2$ 保密，其中 $n_1,n_2,D_1=E_1^{-1},D_2=E_2^{-1}$ 作为解密密钥.

加密过程如下：

(1)将要加密的明文 M 看作大于 0 且$\leqslant l$ 的数据序列，将这个序列的每 k 个元素编为一组，得明文组

$$m=(m_1,m_2,\cdots,m_i,\cdots,m_k)\qquad 0<m\leqslant l,i=1,2,\cdots,k$$

(2)用户自选长为 n 的 0,1 向量 $x'=(x'_1,x'_2,\cdots,x'_n)$ 使 x' 中为 1 的元素有 k 个，亦即 x' 的 Hamming 重量 $w(x')=k$. 对 $i=1,2,\cdots,n$，令

$$x_i=\begin{cases} m_j, & x'_i \text{ 是 } x' \text{ 的第 } j \text{ 个非零元素} \\ 0, & x'_i=0 \end{cases}$$

这一作法实际上是在 k 个分量的明文组 m 中随机地插入 $n-k$ 个 0 分量使其扩充为 n 个分量的向量 $x=(x_1,x_2,\cdots,x_n)$.

(3)用 A 加密 x 得密文 $C=xA$.

解密过程如下：

(1)因 $C=xA=x\begin{pmatrix} A_1E_1 \\ A_2E_2 \end{pmatrix}$，我们计算

$$\begin{aligned} CD_1&=x\begin{pmatrix} A_1 \\ A_2E_2D_1 \end{pmatrix}\equiv x\begin{pmatrix} I_{\frac{n}{2}} & 0 \\ 0 & 0 \end{pmatrix} \qquad (\mathrm{mod}\ n_1)\\ &=(x_1,x_2,\cdots,x_{\frac{n}{2}},0,0,\cdots,0)) \\ CD_2&=x\begin{pmatrix} A_1E_1D_2 \\ A_2 \end{pmatrix}\equiv x\begin{pmatrix} 0 & 0 \\ I_{\frac{n}{2}} & 0 \end{pmatrix} \qquad (\mathrm{mod}\ n_2)\\ &=(x_{\frac{n}{2}+1},x_{\frac{n}{2}+2},\cdots,x_n,0,\cdots,0) \end{aligned}$$

由此得到 $x=(x_1,x_2,\cdots,x_i,\cdots,x_n),0\leqslant x_i\leqslant l,\quad i=1,2,\cdots,n.$

(2)去掉 x 中的 0 分量就得到明文 m.

在介绍完这种新体制之后，我们首先对该体制作一附加说明.

在体制的构造过程中，需产生两个 m 阶正整数的可逆方阵 E_1 和 E_2，在解密过程中使用了它们的逆矩阵 $D_1=E_1^{-1}$ 和 $D_2=E_2^{-1}$. 必须明确的是，E_1 和 E_2 不仅是有理域 Q 上的可逆阵，还必须分别是 Z_{n_1} 和 Z_{n_2} 上的可逆阵，亦即存在正整数矩阵 D_1 和 D_2 使 $D_1E_1\equiv E_1D_1\equiv I_m(\mathrm{mod}\ \ n_1)$ 及 $D_2E_2\equiv E_2D_2\equiv I_m(\mathrm{mod}\ \ n_2)$. 否则 D_1 和 D_2 中便有分数元素，这样在解密过程中 $A_2E_2D_1(\mathrm{mod}\ \ n_1)$ 及 $A_1E_1D_2(\mathrm{mod}\ \ n_2)$ 就可能无意义.

二. 破译广义码体制

为本节密码分析的需要，我们首先给出环 Z_m 上矩阵的两个引理及广义码体制的一些基本性质.

引理 1 设 $M_n(Z_m)$ 为环 Z_m 上 n 阶方阵全体，对 $A\in M_n(Z_m)$，A 在 Z_m 上可逆当且仅当 $\mathrm{GCD}(\det(A),m)=1$.

引理 2 $A\in M_n(Z_m)$，A 在 Z_m 上可逆. 若 $m'\mid m$，则 A 在 $Z_{m'}$ 上亦可逆，显然当 $m'=1$ 时，A 为 Z 上可逆阵.

从上一节的同余方程组(1)、(2)可直接得知：

性质 1

(a) $\quad n_2\mid a_1, n_1\mid a_2$

(b) $\quad \mathrm{GCD}(n_1,a_1)=1, \mathrm{GCD}(n_2,a_2)=1$

由 A_1, A_2 的结构及上述性质又可看出：

性质 2

(a) $\quad n_2\mid A_1$，亦即 n_2 整除 A_1 的每一元素，从而 $n_2\mid A_1E_1$.

(b) $\quad n_1\mid A_2$，从而 $n_1\mid A_2E_2$.

令 $\overline{A}_1=A_1E_1, \overline{A}_2=A_2E_2$，因 $A=\begin{pmatrix}\overline{A}_1\\ \overline{A}_2\end{pmatrix}$ 公开，从而 $\overline{A}_1, \overline{A}_2$ 公开. 记 $\overline{A}_1=(a_{ij}^{(1)})_{\frac{n}{2}\times m}$，$\overline{A}_2=(a_{ij}^{(2)})_{\frac{n}{2}\times m}$；令 $d_2=\underset{\substack{i=1,2,\cdots,\frac{n}{2}\\ j=1,2,\cdots,m}}{\mathrm{GCD}}(a_{ij}^{(1)})$，$d_1=\underset{\substack{i=1,2,\cdots,\frac{n}{2}\\ j=1,2,\cdots,m}}{\mathrm{GCD}}(a_{ij}^{(2)})$，亦即 d_1 和 d_2 分别为 $\overline{A}_2, \overline{A}_1$ 中各元素的最大公因子. 由性质 2 得：

性质 3 $\quad n_1\mid d_1, n_2\mid d_2$.

性质 4 $\quad \overline{A}_1E_1^{-1}\bmod n_1=(I_{\frac{n}{2}},0)$，$\overline{A}_2E_2^{-1}\bmod n_2=(I_{\frac{n}{2}},0)$.

如下事实是本文进行密码分析的最基本依据，不妨称之为分析原理.

分析原理：若已找到一对正整数 n'_1, n'_2 满足下列条件：

(1) $n_1\mid n'_1, n_2\mid n'_2$.

(2) 已找到 Z'_{n_1} 上 m 阶可逆阵 $\overline{E}_1$ 和 Z'_{n_2} 上 m 阶可逆阵 $\overline{E}_2$ 满足：

$\overline{A}_1\overline{E}_1=(\overline{A}''_1,0)(\mathrm{mod}\ n'_1)$，$\overline{A}_2\overline{E}_2=(\overline{A}''_2,0)(\mathrm{mod}\ n'_2)$，其中 $\overline{A}''_1$ 与 $\overline{A}''_2$ 分别为 Z'_{n_1} 和 Z'_{n_2} 上 $\frac{n}{2}$ 阶可逆阵.

(3) $n'_2\mid\overline{A}_1, n'_1\mid\overline{A}_2$；即 $\overline{A}_1(\mathrm{mod}\ n'_2)=0$，$\overline{A}_2(\mathrm{mod}\ n'_1)=0$.

这样，广义码体制可以被破译.

证明： 由于密文

$$C=xA=x\begin{pmatrix}\overline{A}_1\\ \overline{A}_2\end{pmatrix}$$

则

$$C\overline{E}_1=xA\overline{E}_1=x\begin{pmatrix}\overline{A}_1\overline{E}_1\\ \overline{A}_2\overline{E}_2\end{pmatrix}=x\begin{pmatrix}\overline{A}_1'', & 0\\ 0, & 0\end{pmatrix}\qquad(\mathrm{mod}\ n_1')$$

令 $y_1=C\overline{E}_1$，则

$$((x_1,x_2,\cdots,x_{\frac{n}{2}})\cdot\overline{A}''_1,0,\cdots,0)=y_1\qquad(\mathrm{mod}\ n'_1)$$

因此，

$$(x_1,x_2,\cdots,x_{\frac{n}{2}},0,\cdots,0)=y_1(\overline{A}''_1)^{-1}\qquad(\mathrm{mod}\ n'_1)$$

由 $n_1|n'_1$ 可知，$(x_1,x_2,\cdots,x_{\frac{n}{2}})$已经求出．

同样，令 $y_2=C\overline{E}_2(\mathrm{mod}\quad n'_2)$，则可求出$(x_{\frac{n}{2}+1},x_{\frac{n}{2}+2},\cdots,x_n)$满足

$$(0,0,\cdots,0,x_{\frac{n}{2}+1},x_{\frac{n}{2}+2},\cdots,x_n)=y_2(\overline{A}''_2)^{-1}\qquad(\mathrm{mod}\ n'_2)$$

从而明文 $x=(x_1,x_2,\cdots,x_{\frac{n}{2}},x_{\frac{n}{2}+1},\cdots,x_n)$被求出，因此广义码体制被彻底破译．

若 n_1,n_2 已知(或者比较小容易猜到)，因 n_1,n_2 本身就满足 n'_1,n'_2 的条件，则该体制立即可破．以下在假设 n_1,n_2 未知情况下，我们将通几个结论来说明如何在多项式时间内找出满足分析原理的 n'_1,n'_2 及 $\overline{E}_1,\overline{E}_2$.

结论 1 对任何正整数 N，设 A 是 Z_N 上任一 $m\times k$ 阶矩阵，$A=(a_{ij})_{m\times k}$. 对任何给定的 $i,j,j',1\leqslant i\leqslant m,1\leqslant j,j'\leqslant k,j\neq j'$，设 $d=\mathrm{GCD}(a_{ij},a_{ij'})$(将 Z_N 中元素视为 Z 中元素)，则可在多项式时间内找到 Z_N 上的 k 阶可逆阵 E'，使

$$AE'=A'=(a'_{st})_{m\times k}$$

其中 $a'_{ij}=d,a'_{ij'}=0$.

证明：设 $d=(a_{ij},a_{ij'})$，根据 Euclid 算法对 A 中位置(i,j)和(i,j')上两个元素作辗转相除(同时 j 列和 j' 列其它元素陪伴着作相同的操作)，就可求出 d，这相当于做若干次 A 的 j 列减去 j' 列的倍数或 j' 列减去 j 列的倍数这类的初等变换，且当 d 出现在(i,j')位置时再进行一次 j 列和 j' 列互换的初等变换．由此不难看出此结论为真．

结论 2 对于广义码体制中的矩阵 $\overline{A}_1,\overline{A}_2$，可在多项式时间内求得 Z_{d_1}和 Z_{d_2}上的 m 阶可逆阵 $\overline{E}_1,\overline{E}_2$ 使

$$\overline{A}_1\overline{E}_1=\begin{pmatrix}r_{11} & 0\cdots\cdots0 & 0\cdots\cdots0\\ r_{21} & r_{22}\cdots\cdots 0 & 0\cdots\cdots0\\ \cdots\cdots & \cdots\cdots & \cdots\cdots\\ r_{\frac{n}{2},1} & r_{\frac{n}{2},2}\cdots r_{\frac{n}{2},\frac{n}{2}} & 0\cdots\cdots0\end{pmatrix}\qquad(\mathrm{mod}\ d_1)$$

$$\triangleq(R_1,0)$$

$$\overline{A}_2\overline{E}_2=\begin{pmatrix}r'_{11} & 0\cdots\cdots0 & 0\cdots\cdots0\\ r'_{21} & r'_{22}\cdots\cdots 0 & 0\cdots\cdots0\\ \cdots\cdots & \cdots\cdots & \cdots\cdots\\ r'_{\frac{n}{2},1} & r'_{\frac{n}{2},2}\cdots r'_{\frac{n}{2},\frac{n}{2}} & 0\cdots\cdots0\end{pmatrix}\qquad(\mathrm{mod}\ d_2)$$

$$\triangleq(R_2,0)$$

证明：通过结论 1 的方法对 $\overline{A}_1,\overline{A}_2$，各行实施消元法即可．

由性质 4 不难看出结论 2 中的 R_1 和 R_2 具有如下性质：

性质 5 $R_1(\mathrm{mod}\ n_1)$和 $R_2(\mathrm{mod}\ n_2)$分别为 Zn_1,Zn_2 上可逆阵，亦即 $\mathrm{GCD}(\det(R_1),n_1)=1,\mathrm{GCD}(\det(R_2),n_2)=1$.

由结论 2 可以看出，d_1,d_2 满足分析原理中的(1)，(3)两条，且对任意的 n'_1,n'_2，若

$$n_1|n'_1|d_1,n_2|n'_2|d_2(\mathrm{s})$$

则 n'_1,n'_2 必满足(1)，(3)两条．下面我们将说明如何找出在满足(s)的条件下还满足(2)的 n'_1,n'_2，从而 n'_1,n'_2 满足分析原理．

显然，n'_1,n'_2 满足(s)时还满足(2)，当且仅当 $R_1(\mathrm{mod}\ n'_1),R_2(\mathrm{mod}\ n'_2)$为 Zn'_1,Zn'_2 上可逆矩阵，亦即 $\mathrm{GCD}(\det(R_1),n'_1)=\mathrm{GCD}(\det(R_2),n'_2)=1$．我们下面来构造 n'_1，而 n'_2 的构造完全相同．

若 $\mathrm{GCD}(\det(R_1),d_1)=1$，则 d_1 满足 n_1'的要求，令 $n'_1=d_1$ 即可．若 $\mathrm{GCD}(\det(R_1),d_1)=G_1>1$，则必有 $\mathrm{GCD}(n_1,G_1)=1$．若不然，令 $g_1=\mathrm{GCD}(n_1,G_1)>1$，因 $g_1|G_1|\det(R_1)$，从而 $\det(R_1)(\mathrm{mod}\ g_1)=0$；又因 $g_1|n_1$，由性质 5 与引理 2 知 $R_1(\mathrm{mod}\ g_1)$可逆，亦即 $\mathrm{GCD}(\det(R_1),g_1)=1$，从而两者矛盾，因此，$\mathrm{GCD}(n_1,G_1)=1$．令 $d'_1=d_1/G_1$，则 $n_1|d'_1|d_1$，且 d'_1 为 d 的真因子．若 d'_1 仍不满足要求，则可找出 d'_1 的真因子 d''_1，使 $n_1|d''_1|d'_1|d_1$；如此进行下去，在不超过 $\log_2 d_1$ 次过程中，必可找到 $\overline{d}_1,n_1|\overline{d}_1|d_1$ 且 $\mathrm{GCD}(\det(R_1),\overline{d}_1)=1$，令 $n'_1=\overline{d}_1$ 即可．

如上过程可以形式化为如下算法：

(1)$D_1\leftarrow d_1$

(2)$G_1\leftarrow\mathrm{GCD}(\det(R_1),D_1)$

(3)IF $G_1=1$,THEN

$n'_1\leftarrow D_1$,HALT!

(4)$D_1\leftarrow D_1/G_1$,GO TO (2)

由以上分析可见，我们已彻底破译了广义码体制．

本文的结论及攻击方法对攻击文献[3]的体制是有用的．

参 考 文 献

[1] McEliece,R. J.,A Public-Key Cryptosystem Based on Algebraic Coding Theory, DSN Progress Report, Jet Propulsion Laboratory, California Institute of Technology, 42－44,1978.

[2] 史晓明，一个新的公钥密码体制及其应用，全国计算机安全交流会论文集，常州，123－128,1988.

[3] 邵祖华，矩阵共轭变换掩护下的公钥密码系统和数字签名，电子学报，Vol. 16,No. 6,76－81,1988.

Cryptanalysis of Extended Linear Code Public-Key Cryptosystem

Li Daxing Wang xiaoyun

(*Dept. of Math., Shandong Uni., Jinan* 250100, *PRC*)

(*State Key Lab. of Inform. Security, Beijing* 100039, *PRC*)

Abstract Today, as many public-key cryptosystems have been broken, the public-key cryptosystems based on coding theory are being attended, but almost all of them are variations of McEliece cryptosystem[1]. Shi Xiaoming[2] proposed a new public-key cryptosystem based on the difficulty of decoding exetnded linear code. In this paper, by computing a pair of equivalent decryption keys with Euclid algorithm, we completely break this cryptosystem.

Key words Cryptanalysis Public-key cryptosystem Extended linear code

子集和组的求解与真分式背包体制的攻破

邵祖华

（杭州金融管理干部学院，杭州　310023）

摘要　本文采用概率的方法，计算了子集和组中短向量的期望个数，得到了与文献[2]中相符的结论，并证明了该文献的猜测．本文修改了计算格归约基的 L^3 算法，以用于解一般的子集和组问题．本文进一步分析了真分式背包体制[6]的性能，介绍了使用修改的 L^3 算法攻击它的方法．本文认为将一个子集和问题分拆为子集和组问题的结果将适得其反．

关键词　概率　子集和　格归约基算法

一. 前　言

子集和问题是一个 NP 难题，并且被用来设计背包公钥密码体制[1]．不幸的是 Shamir 首先利用陷门中的超递增数列攻破了基本 Merkle-Hellman 体制，尔后 Odlyzko 等人攻破了低密度的背包公钥密码体制，其中包括乘法背包体制和 Shamir 的快速背包签名方案[2,3]．他们的基本工具是由 Lenstra，Lenstra 和 Lovasz 发明的 L^3 格归约基算法[4]．因此人们寻找各种抵御 L^3 算法的方法．刘锐同志在通信学报[5]发表的“真分式背包体制”就是这样的一个尝试，其安全依据是子集和组的难解性．

二. 子集和组的求解

1. 子集和问题：

已知 n 个正整数 $a_1,a_2,\cdots,a_n$ 和正整数 S，求 $x_1,x_2,\cdots,x_n\in\{0,1\}$，使得 $\sum_{i=1}^{n}a_ix_i=S$.

这是一个 NP 难题．

Lagarias 等人提出了攻击低密度子集和的方法．他们构造 $n+1$ 维整数格 $L(a,s)=zV_1\oplus zV_2\oplus\cdots\oplus ZV_{n+1}$，其中

$$V_1=(1,0,\cdots,0,a_1)$$
$$V_2=(0,1,\cdots,0,a_2)$$
$$\cdots\cdots\cdots\cdots$$
$$V_n=(0,0,\cdots,1,a_n)$$

$$V_{n+1}=(0,0,\cdots,0,-s)$$

$$S=\sum_{i=1}^{n}a_ie_i,\qquad e_1,e_2,\cdots,e_n\in\{0,1\},\qquad \sum_{i=1}^{n}e_i^2\leqslant\frac{n}{2}$$

他们使用算法 L^3 寻找格 L 中的归约基．他们定义向量 $a=(a_1,a_1,\cdots,a_n)$ 的密度 $d(a)=\frac{n}{\log_2(\max a_i)}$，证明了在几乎全部密度 $d(a)<0.645$ 的格中，固定向量 $e=(e_1,e_2,\cdots,e_n)$ 是最短向量．当 $d(a)<(2-\varepsilon)(\log\frac{4}{3})^{-1}n^{-1}$，$L^3$ 算法几乎全部求出背包的解．他们还猜测，当 $d(a)>0.645$，格中就有 $2^{(d(a)-0.645)n}$ 个短向量．

2. 设 R^m 是 m 维实向量空间，定义向量的长度为

$$\|x\|^2=\sum_{i=1}^{n}x_i^2,\text{其中 }x=(x_1,x_2,\cdots,x_n)$$

设 $b_1,b_2,\cdots,b_n$ 是 R^m 中一组线性无关的向量组，$n\leqslant m$．定义整数格 $L_n=Zb_1\oplus Zb_2\oplus\cdots\oplus Zb_n$ 是 R^m 中一个加法子群．

使用 Gram-Schmidt 正交处理法，定义向量组 $b_1^*,b_2^*,\cdots,b_n^*\in R^m$ 如下：

$$b_i^*=b_i-\sum_{j=1}^{i-1}u_{ij}b_j^*,u_{ij}=(b_i,b_j^*)/(b_j^*,b_j^*)\qquad 1\leqslant j<i\leqslant n$$

（ ， ）表示 R^m 中的欧氏内积．

定义 1 线性无关向量组 $b_1,b_2,\cdots,b_n$ 构成格 L_n 的归约基，如果

$$|u_{ij}|\leqslant\frac{1}{2},1\leqslant j<i\leqslant n,\ \|b_i^*+u_{ii-1}b_{i-1}^*\|^2\geqslant\frac{3}{4}\|b_{i-1}^*\|^2,1<i\leqslant n$$

将文献[4]中论证的内容稍作修改，我们便有：

引理 1 设$[b_1,b_2,\cdots,b_n]$是整数格 L_n 的归约基，则

$$\|b_1\|^2\leqslant 2^{n-1}\min_{x\in L,x\neq 0}\|x\|^2$$

引理 2 设 $L_n\subset R^m$ 是具有归约基 $b_1,b_2,\cdots,b_n$ 的整数格．如果 $x_1,x_2,\cdots,x_t\in L_n$ 是线性无关的向量组，则

$$\|b_j\|^2\leqslant 2^{n-1}\max\{\|x_1\|^2,\|x_2\|^2,\cdots,\|x_t\|^2\}\qquad j=1,2,\cdots,t$$

我们只要对 L^3 算法[4]稍作修改，把空间的维数从 n 提高到 m，就可以运用到整数格 L_n 上，计算格 L_n 的归约基．计算的复杂性为：

引理 3 设 $L_n\subset Z^m$ 是具有基底 $b_1,b_2,\cdots,b_n$ 的整数格，$n\leqslant m$，$\|b_i\|^2\leqslant B,1\leqslant i\leqslant Bn$，那么修改后的 L^3 算法寻找 L_n 的归约基最多要求 $O(mn^3\log B)$ 次算术运算，并且运算操作的整数的二进制长度为 $O(m\log B)$．

3. 子集和组问题：

已知 $l\times n$ 矩阵

$$A=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\ \cdots\cdots\cdots\cdots\\ a_{l1}&a_{l2}&\cdots&a_{ln}\end{pmatrix}$$

$a_{ij}\in z$，以及 l 个整数 $s_1,s_2,\cdots,s_l$，求 $x_1,x_2,\cdots,x_n\in\{0,1\}$

使 $\sum_{i=1}^{n}a_{ji}x_i=s_j\quad j=1,2,\cdots,l.$

为了方便起见，我们假设 A 的行向量线性无关．我们可以构造整数格 L_n 如下：

$$L(A_1,S_1,S_2,\cdots S_l)=ZV_1\oplus ZV_2\oplus\cdots\oplus ZV_{n+1}$$

其中

$$V_1=(1,0,\cdots,0,\quad a_{11},a_{21},\cdots,a_{l1})$$
$$V_2=(0,1,\cdots,0,\quad a_{12},a_{22},\cdots,a_{l2})$$
$$\cdots\cdots$$
$$V_n=(0,0,\cdots,1,\quad a_{1n},a_{2n},\cdots,a_{ln})$$
$$V_{n+1}=(0,0,\cdots,0,-S_1,-S_2,\cdots,S_l)$$

固定向量 $e_1,e_2,\cdots,e_n\in\{0,1\}$，$\sum_{i=1}^{n}e_i^2\leqslant\frac{n}{2}$，$S_j=\sum_{i=1}^{n}a_{ji}e_i$

显然 $L(A,S_1,S_2,\cdots,S_l)\subset R^m$，并且 $V_1,V_2,\cdots,V_{n+1}$ 线性无关，这里 $m=n+l$.

4. L^3 算法的成功与否取决于整数格中短向量的个数．Lagaris 等[2]是通过研究含有向量 $\|W\|^2\leqslant\frac{n}{2}$ 的整数格的个数来解决这个问题．但我们认为，背包类公钥体制若要投入使用，其元数至少大于 200，甚至大于 500，因而我们可以借助于概率论中的一些成果来研究这个问题．

我们先研究概率

$$P\{\sum_{i=1}^{n}a_ix_i=k\sum_{i=1}^{n}a_ie_i\mid(x_1,x_2,\cdots,x_n)\neq k(e_1,e_2,\cdots,e_n),\sum_{i=1}^{n}e_i^2\leqslant R,\sum_{i=1}^{n}x_i^2\leqslant R\}$$

我们假设 a_i 均匀分布于$[1,B]$，设 $b_i=\mathrm{sign}(x_i-Ke_i)a_i$，sign( )是符号函数，于是 b_i 均匀分布于$[-B,B]$.

数学期望

$$E(b_i)=0$$

方差

$$D(b_i)=\frac{2}{2B}(1^2+2^2+\cdots+B^2)=\frac{2B^2+3B+1}{6}\approx\frac{B^2}{3}$$

再计算

$$\sum_{i=1}^{n}(x_i-ke_i)^2=\sum x_i^2-2K\sum x_ie_i+k^2\sum e_i^2$$
$$\leqslant\sum x_i^2+2|k|\sqrt{\sum x_i^2}\cdot\sqrt{\sum e_i^2}+k^2\sum e_i^2$$
$$=(\sqrt{\sum x_i^2}+|k|\sqrt{\sum e_i^2})^2$$
$$\leqslant(1+|k|)^2R$$

设随机变量 $\eta=\sum_{i=1}^{n}(x_i-ke_i)a_i$，则有

$$E(\eta)=0\quad D(\eta)=\sum_{i=1}^{n}(x_i-ke_i)^2D(b_i)\leqslant\frac{(1+|k|)^2B^2R}{3}$$

当 $n>100$，由中心极限定理，我们可以假设 η 近似地服从正态分布 $N(0,(1+|K|^2B^2R/3)$ 于是

$$P\{\sum_{i=1}^{n}a_ix_i=\eta\sum_{i=1}^{n}a_ie_i\}=P\{\sum_{i=1}^{n}a_i(x_i-ke_i)=0\}$$

$$=P\{-\frac{1}{2}\leqslant k<\frac{1}{2}\}=P\{-\alpha\leqslant\frac{\sqrt{3}\eta}{(1+|k|)BR^{1/2}}<\alpha\}$$

$$=\int_{-\alpha}^{\alpha}\frac{1}{\sqrt{2\pi}}e^{-t^2}dt\approx\frac{\sqrt{3}}{\sqrt{2\pi}(1+|k|)BR^{1/2}}\ e^{-\theta^2}$$

$$\approx\frac{1}{\sqrt{2}\,(1+|k|)BR^{1/2}}$$

其中

$$-\alpha\leqslant\theta<\alpha\quad\alpha=\frac{\sqrt{3}}{2(1+|k|)BR^{1/2}}$$

推导中使用了定积分中值定理.

如果我们假设在矩阵 $A=(a_{ji})$ 中,a_{ji} 均匀分布于整数区间$[1,B_j]$,$j=1,2,\cdots,l$,则有

$$P\Big\{\sum_{i=1}^{n}a_{ji}x_i=k\sum_{i=1}^{n}a_{ji}e_i,j=1,2,\cdots,l\,|\,(x_1,x_2,\cdots,x_n)$$

$$\neq k(e_1,e_2,\cdots,e_n),\sum_{i=1}^{n}e_i^2\leqslant R,\sum_{i=1}^{n}x_i^2\leqslant R\Big\}=\left(\frac{1}{\sqrt{2}\,(1+|k|)R^{1/2}}\right)^{l}\frac{1}{B_1B_2\cdots B_l}$$

我们研究$|k|$的上界

$$\min|\sum_{i=1}^{n}a_ie_i|=B$$

$$\max|\sum_{i=1}^{n}a_ix_i|=RB$$

因此$|k|\leqslant R$.

这样整数格 $L(A,S_1,S_2,\cdots,S_l)$ 中存在短向量

$$(x_1,x_2,\cdots,x_n,0,\cdots,0)\neq k(e_1,e_2,\cdots,e_n,0,\cdots,0)$$

的概率

$$Pr=\frac{1}{2^{l/2}R^{l/2}B_1B_2\cdots B_l}(1+\frac{2}{2^l}+\frac{2}{3^l}+\cdots+\frac{2}{(R+L)^l})$$

$$\approx\frac{1}{B_1B_2\cdots B_l}$$

类似地,我们还可以得到

$$P_0=P\{\sum_{i=1}^{n}a_{li}x_i=0,\cdots\sum_{i=1}^{n}a_{li}x_i=0\,|\,\sum_{i=1}^{n}x_i^2\leqslant R\}$$

$$\approx\frac{1}{B_1B_2\cdots B_lR^{l/2}2^{l/2}}$$

5. 我们采用文献[2]中的表示方法,$S_n(R)$表示不等式$\sum_{i=1}^{n}x_i^2\leqslant R$ 的整数解的个数. 我们有文献[2]的成果:

当 $R=\frac{n}{2}$

$$S_n(\frac{n}{2})\approx2^{1.54725n}$$

一般地

$$S_n(R)\leqslant3^nR^{n/2}$$