理想格上格基的快速三角化算法研究

张 洋*①② 刘仁章③ 林东岱①
①(中国科学院信息工程研究所信息安全国家重点实验室 北京 100093)
②(中国科学院大学网络空间安全学院 北京 100049)
③(卫士通摩石实验室 北京 100166)

摘 要：为了提高理想格上格基的三角化算法的效率，该文通过研究理想格上的多项式结构提出了一个理想格上格基的快速三角化算法，其时间复杂度为$O(n^3\log_2 B)$，其中n是格基的维数，B是格基的无穷范数。基于该算法，可以得到一个计算理想格上格基Smith标准型的确定算法，且其时间复杂度也比现有的算法要快。更进一步，对于密码学中经常所使用的一类特殊的理想格，可以用更快的算法将三角化矩阵转化为格基的Hermite标准型。

关键词：理想格；Hermite标准型；Smith标准型；三角化
中图分类号：TP309.7; O157.4 **文献标识码**：A **文章编号**：1009-5896(2020)01-0098-07
DOI: 10.11999/JEIT190725

Fast Triangularization of Ideal Latttice Basis

ZHANG Yang①② LIU Renzhang③ LIN Dongdai①
①(*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*)
②(*School of Cyber Security,University of Chinese Academy of Sciences, Beijing* 100049, *China*)
③(*Westone Cryptologic Research Center, Beijing* 100166, *China*)

Abstract: To improve the efficiency of the triangularization of ideal lattice basis, a fast algorithm for triangularizing an ideal lattice basis is proposed by studying the polynomial structure, which runs in time $O(n^3\log_2 B)$, where n is the dimension of the lattice, B is the infinity norm of lattice basis. Based on the algorithm, a deterministic algorithm for computing the Smith Normal Form (SNF) of ideal lattice is given, which has the same time complexity and thus is faster than any previously known algorithms. Moreover, for a special class of ideal lattices, a method to transform such triangular bases into Hermite Normal Form (HNF) faster than previous algorithms will be present.

Key words: Ideal lattice; Hermite Normal Form (HNF); Smith Normal Form (SNF); Triangularization

1 引言

Hermite标准型和Smith标准型是两种定义在整数矩阵上的重要标准型，它们在很多方面都有应用，比如，Hermite标准型可以用于解丢番图方程[1]，整数规划[2]和格上的计算问题[3]，Smith标准型可以用来确定有限生成阿贝尔群的基础理论中的不变常量[4]。而计算Hermite标准型和Smith标准型通常来说需要将格基三角化以后才能进行。所以为了提高计算Hermite标准型和Smith标准型的算法的效率，提高矩阵三角化算法的效率有很重要的意义。

从另一个角度来看，格是数论中很重要的概念，而基于格的密码学由于其高效、多功能和潜在抗量子攻击等性质吸引了众多密码学家的注意。对于同一个格而言，由于所有的格基都有相同的Hermite标准型，所以一般在基于格的公钥密码体制中将Hermite标准型作为公钥[5]。

为了提高基于格的密码算法的效率，密码学家提出了理想格的概念。理想格相比于一般的格拥有更多的代数结构，可以加速运算并减少空间存储。目前已经有一些算法在理想格上运行比在一般格上要快，比如Lyubashevsky等人[6]在理想格上给出了更快的Gram-Schmit正交化和高斯采样算法(循环格)。但是目前还没有理想格上对三角化的加速算法。

目前最快的格基三角化算法是Hafner和McCurley[7]在1991年提出的。对于一个$n\times n$的整数矩

收稿日期：2019-09-19；改回日期：2019-11-15；网络出版：2020-01-01
*通信作者： 张洋 zhangyang9091@iie.ac.cn

阵$\boldsymbol{A}$，其每个元素的上界为B，那么计算$\boldsymbol{A}$的三角化矩阵可以在$O\left(n^{1+\omega}\log_2 B\right)$时间复杂度内完成，其中$O\left(n^{\omega}\right)$是两个$n\times n$维矩阵相乘所需要的乘法次数，目前最快的算法中$\omega$可以降低到2.372[8]。该算法使用快速矩阵乘法来实现三角化，但是并没有结果说明如何在相同的时间内得到矩阵的Hermite标准型。直到1996年，Storjohann等人[9]利用快速矩阵乘法技术将计算Hermite标准型的时间复杂度降低到$O\left(n^{1+\omega}\log_2 B\right)$。

至于Smith标准型的计算，确定性算法步骤基本是先计算出Hermite标准型然后再通过初等变换来计算。所以目前计算Smith标准型最快的时间复杂度和计算Hermite标准型是一样的。

本文利用理想格上的特殊结构来降低对理想格上格基三角化的复杂度，该算法的时间复杂度可以降低到$O\left(n^3\log_2 B\right)$。同时，基于在文献[10]和文献[11]中提出的理想格性质，本文可以确定地得到理想格上格基的Smith标准型，其时间复杂度也低于目前最快的算法。虽然和文献[7]中类似，本文还不能在$O\left(n^3\log_2 B\right)$时间复杂度内得到任意理想格上格基的Hermite标准型，但是针对格密码学中经常使用的一类理想格，本文可以得到一个在$O\left(n^3\log_2 B\right)$时间内计算格基的Hermite标准型的算法。

本文的结构安排如下：第2部分介绍预备知识和现有的结果；第3部分提出新的理想格上格基三角化算法；第4部分说明对一类特殊的理想格可以在$O\left(n^3\log_2 B\right)$时间内计算格基的Hermite标准型。

2　预备知识

2.1　符号约定

本文用斜体粗体大写字母来表示矩阵，用粗体小写字母来表示行向量。对于矩阵$\boldsymbol{A}\in\mathbb{Z}^{n\times m}$，在第$i$行、第$j$列的元素表示为$a_{ij}$，矩阵$\boldsymbol{A}$的$i$行表示为$\boldsymbol{A_i}$。一个整数矩阵的三角化矩阵用$\boldsymbol{T}$来表示，且用$\boldsymbol{H}$和$\boldsymbol{S}$分别表示该矩阵的Hermite标准型和Smith标准型。

对于一个多项式$f(x)$，其首项系数用$\mathrm{lc}(f)$来表示，最高次数用$\deg(f)$来表示。零多项式的次数定义为$-\infty$。

2.2　多项式的最大公因式及扩展欧几里得算法

给定某个唯一分解整环上两个多项式$f(x)$和$g(x)$，判定它们的最大公因子的最高次数是否≥ 1是一个经典问题。为此，下面介绍两个多项式的结式，其定义如下。

定义 1(结式)　令$f(x)=f_nx^n+f_{n-1}x^{n-1}+\cdots+f_1x+f_0$，$g(x)=g_mx^m+g_{m-1}x^{m-1}+\cdots+g_1x+g_0$为次数分别为$n$和$m$的两个多项式。定义$f(x)$和$g(x)$的Sylvester矩阵：

$$\mathbf{Sylv}(f(x),g(x))=\begin{bmatrix}x^{m-1}f(x)\\x^{m-2}f(x)\\\vdots\\f(x)\\x^{n-1}g(x)\\x^{n-2}g(x)\\\vdots\\g(x)\end{bmatrix}=\begin{bmatrix}f_n & f_{n-1} & \cdots & f_0 & & & & \\ & f_n & f_{n-1} & \cdots & f_0 & & & \\ & & \ddots & & & \ddots & & \\ & & & f_n & f_{n-1} & \cdots & f_1 & f_0\\ g_m & g_{m-1} & \cdots & g_1 & g_0 & & & \\ & g_m & g_{m-1} & \cdots & g_1 & g_0 & & \\ & & \ddots & & & \ddots & & \\ & & & g_m & g_{m-1} & \cdots & g_1 & g_0\end{bmatrix}_{(m+n)\times(m+n)}$$

则$f(x)$和$g(x)$的结式定义为$\mathbf{Sylv}(f(x),g(x))$的行列式，用$\mathrm{Res}(f(x),g(x))$来表示。

结式的概念可用来判定$f(x)$和$g(x)$是否存在次数大于1的最大公因式，而为了计算$f(x)$和$g(x)$的最大公因式，需要多项式上扩展欧几里得算法来计算。下列等式给出了计算$f(x)$和$g(x)$的最大公因式的过程：

$$\left.\begin{array}{ll}\alpha_1 f(x) & =q_1(x)g(x)+r_1(x)\\ \alpha_2 r_1(x) & =q_2(x)r_1(x)+r_2(x)\\ \vdots & \vdots\\ \alpha_l r_{l-2}(x) & =q_l(x)r_{l-1}(x)+r_l(x)\\ \alpha_{l+1}r_{l-1}(x) & =q_{l+1}(x)r_l(x)\end{array}\right\}\quad(1)$$

这里$\deg(g)>\deg(r_1)>\deg(r_2)>\cdots>\deg(r_{l-1})>\deg(r_l)=0$。

如果上述计算是在一个域中进行(比如$\mathbb{Q}$)，那么所有的α_i都可以取为1，则$r_l(x)$就为$f(x)$和$g(x)$在域中拥有最大次数的公因式。

从上述过程中,可以用$f(x)$和$g(x)$来表示所有的余式$r_i(x)$，即$s_i(x)f(x)+t_i(x)g(x)$，其中$i=1,2,\cdots,l-1,l$，那么有如下性质。

引理 1　令$f(x)$, $g(x)$为次数分别为n和m的两个多项式，这里$n>m$。令$r_1(x),r_2(x),\cdots,r_l(x)$为式(1)中定义的余式。若$\deg(r_1)=n_i$，且$r_i(x)=s_i(x)f(x)+t_i(x)g(x)$，则$\deg(s_i)=m-n_{i-1}<m$, $\deg(t_i)=n-n_{i-1}<n$并且满足$s_i(x)=\alpha_i s_{i-2}(x)-q_i(x)s_{i-1}(x)$, $t_i(x)=\alpha_i t_{i-2}(x)-q_i(x)t_{i-1}(x)$。

欧几里得算法是最古老的算法之一，其应用非常广泛。本文给出文献[12]中关于$\mathbb{Z}$上多项式的扩

展欧几里得算法的相关结论。引理2对于证明本文算法的正确性和分析复杂度有重要作用。

引理 2 令$\mathcal{F}$为一个域，$f(x), g(x), s(x), t(x) \in \mathcal{F}[x]$，且$\deg(f(x))=n$, $r(x)=s(x)f(x)+t(x)g(x)$, $t(x)\neq 0$，并假设$\deg(r)+\deg(t)<n=\deg(f)$。令$r_i(x)=s_i(x)f(x)+t_i(x)g(x)$为通过式(1)得到的余式，其中$0\le i\le l+1$。定义整数$j$满足条件$\deg(r_j)\le \deg(r) <\deg(r_{j-1})$。那么存在一个非零元素$\alpha(x)\in\mathcal{F}[x]$使得

$$\begin{aligned} r(x) =&\alpha(x)r_j(x), s(x)=\alpha(x)s_j(x),\\ t(x) =&\alpha(x)t_j(x) \end{aligned} \tag{2}$$

引理 3 对于$f(x), g(x)\in\mathbb{Z}[x]$，且满足$\deg(f)=n>\deg(g)=m\ge 1$。令$0\le k\le m<n$，那么$k$不会出现在式(1)中余式序列的次数中当且仅当存在$s(x)$和$t(x)$满足

$$\begin{aligned} &t(x)\neq 0, \deg(s)<m-k,\\ &\deg(t)<n-k, \deg(sf+tg)<k \end{aligned} \tag{3}$$

引理 4 对于$f(x), g(x)\in\mathbb{Z}[x]$，且满足$\deg(f)=n>\deg(g)=m\ge 1$。那么存在快速的扩展欧几里得算法可以$O\left(n^3\log_2 B\right)$时间内计算出$\mathbb{Q}[x]$上的$r_i(x)$, $s_i(x)$, $t_i(x)$，这里B是$f(x)$和$g(x)$的系数上界。

2.3 格

定义 2(格) 给定m个线性无关的向量，$\boldsymbol{b_1}, \boldsymbol{b_2}, \cdots, \boldsymbol{b_m}$，其中$\boldsymbol{b_i}\in\mathbb{R}^n$。$\boldsymbol{B}\in\mathbb{R}^{m\times n}$定义为$\boldsymbol{B_i}=\boldsymbol{b_i}$。则由$\boldsymbol{B}$生成的格$\mathcal{L}(\boldsymbol{B})$定义为

$$\mathcal{L}(\boldsymbol{B})=\left\{\sum_{i=1}^{m} x_i\boldsymbol{b_i}, x_i\in\mathbb{Z}\right\}=\{\boldsymbol{xB}:\boldsymbol{x}\in\mathbb{Z}^n\} \tag{4}$$

则称$\boldsymbol{B}$是格$\mathcal{L}(\boldsymbol{B})$的一组基，其中$m$和$n$分别称为格$\mathcal{L}(\boldsymbol{B})$的秩和维数。当$m=n$时，称格$\mathcal{L}(\boldsymbol{B})$是满秩的。

定义 3(行列式) 给定格$\mathcal{L}(\boldsymbol{B})$，其行列式定义为$\det(\mathcal{L}(\boldsymbol{B}))=\sqrt{\det(\boldsymbol{B}^{\mathrm{T}}\boldsymbol{B})}$。

当$\mathcal{L}(\boldsymbol{B})$是满秩的时候，$\boldsymbol{B}$是一个非奇异的方阵，此时$\det(\mathcal{L}(\boldsymbol{B}))=|\det(\boldsymbol{B})|$。

注意到，当从给定格$\mathcal{L}$中选取任意格向量时，并不是每一组选取的格向量集合都可以扩展为格$\mathcal{L}$的一组基。下面的引理给出了判定一组选取的格向量集合是否能扩展为一组格基的方法[13]。

引理 5 给定满秩格$\mathcal{L}(\boldsymbol{b_1}, \boldsymbol{b_2}, \cdots, \boldsymbol{b_n})$中$r$个线性无关的向量$\boldsymbol{v_1}, \boldsymbol{v_2}, \cdots, \boldsymbol{v_r}$，且满足

$$\begin{pmatrix} \boldsymbol{v_1}\\ \boldsymbol{v_2}\\ \vdots\\ \boldsymbol{v_r} \end{pmatrix} = \boldsymbol{A}_{r\times n}\cdot \begin{pmatrix} \boldsymbol{b_1}\\ \boldsymbol{b_2}\\ \vdots\\ \boldsymbol{b_r} \end{pmatrix} \tag{5}$$

则下列的条件是等价的：

(1) 存在格向量$\boldsymbol{u_{r+1}}, \boldsymbol{u_{r+2}}, \cdots, \boldsymbol{u_n}$使得$\boldsymbol{v_1}, \boldsymbol{v_2}, \cdots, \boldsymbol{v_r}, \boldsymbol{u_{r+1}}, \boldsymbol{u_{r+2}}, \cdots, \boldsymbol{u_n}$是$\mathcal{L}$的一组基；

(2) $\boldsymbol{A}$的所有$r\times r$阶子式的最大公因子为1；

(3) $\boldsymbol{v_1}, \boldsymbol{v_2}, \cdots, \boldsymbol{v_r}$是$\mathcal{L}\cap\mathrm{span}(\boldsymbol{v_1}, \boldsymbol{v_2}, \cdots, \boldsymbol{v_r})$的一组基；

(4) 存在一个矩阵$\boldsymbol{P}\in\mathbb{Z}^{n\times n}$使得$\boldsymbol{A}\cdot\boldsymbol{P}=\begin{bmatrix}\boldsymbol{I_r} & \boldsymbol{O}_{r\times(n-r)}\end{bmatrix}_{r\times n}$；

(5) 存在一个矩阵$\boldsymbol{B}\in\mathbb{Z}^{(n-r)\times n}$使得$\begin{bmatrix}\boldsymbol{A}\\ \boldsymbol{B}\end{bmatrix}_{n\times n}$是一个幺模矩阵。

引理 6 令$\boldsymbol{A}\in\mathbb{Z}^{m\times n}$，其中$n>m$。假设$\boldsymbol{A}$可以通过添加$(n-m)$个合适的行成为幺模矩阵。如果$\boldsymbol{A}$的每一行都是一个格$\mathcal{L}$的格向量，那么$\boldsymbol{A}$可以扩充为$\mathcal{L}$的一组基。

由引理5可知，因为$\boldsymbol{A}$可以扩充为一个幺模矩阵，则存在$\boldsymbol{P}\in\mathbb{Z}^{n\times n}$使得$\boldsymbol{A}\cdots\boldsymbol{P}=(\boldsymbol{I}_m, 0, \cdots, 0)_n$，其中等式右边有$(n-m)$个0。假设$\mathcal{L}$的一组基是$\boldsymbol{B}\in\mathbb{Z}^{n'\times n}$，其中$m\le n'\le n$。

因为$\boldsymbol{A}\in\mathcal{L}$，所以存在矩阵$\boldsymbol{U}\in\mathbb{Z}^{m\times n'}$使得$\boldsymbol{A}=\boldsymbol{U}\cdot\boldsymbol{B}$。所以$\boldsymbol{A}\cdot\boldsymbol{P}=\boldsymbol{U}\cdot\boldsymbol{B}\cdot\boldsymbol{P}=\boldsymbol{I}_m, 0, \cdots, 0_n$。记$\boldsymbol{P'}=\boldsymbol{B}\cdot\boldsymbol{P}$然后将$\boldsymbol{P'}$分为两个部分，$\boldsymbol{P_1}'\in\mathbb{Z}^{n'\times n'}$和$\boldsymbol{P_2}'\in\mathbb{Z}^{n'\times(n-n')}$，即$\boldsymbol{P}'=[\boldsymbol{P_1}'\mid\boldsymbol{P_2}']$。于是有

$$\begin{aligned} \boldsymbol{U}\cdot[\boldsymbol{P_1}'\mid\boldsymbol{P_2}'] =&[\boldsymbol{U}\cdot\boldsymbol{P_1}'\mid\boldsymbol{U}\cdot\boldsymbol{P_2}']\\ =&(\boldsymbol{I}_m, 0, \cdots, 0)_n \end{aligned} \tag{6}$$

因为$\boldsymbol{U}\cdot\boldsymbol{P_1}'=\mathbb{Z}^{m\times n'}$，$m\le n'$，所以$\boldsymbol{U}\cdot\boldsymbol{P_1}'=(\boldsymbol{I}_m, 0, \cdots, 0)_{n'}$。则$\boldsymbol{U}$可扩充为一个幺模矩阵。假设$\boldsymbol{U'}=\left[\boldsymbol{U}^{\mathrm{T}}\mid\bar{\boldsymbol{U}}^{\mathrm{T}}\right]^{\mathrm{T}}$是一个幺模矩阵，$\boldsymbol{U'}\cdot\boldsymbol{B}=\left[\boldsymbol{A}^{\mathrm{T}}\mid\bar{\boldsymbol{A}}^{\mathrm{T}}\right]^{\mathrm{T}}$是$\mathcal{L}$的一组基。所以$\boldsymbol{A}$可以扩充为$\mathcal{L}$的一组基。

2.4 理想格

理想格是定义在多项式环上的一类特殊的格，同时具有加法和乘法封闭的性质。一般来说，考虑环$R=\mathbb{Z}[x]/\langle f(x)\rangle$，这里$f(x)\in\mathbb{Z}[x]$是一个次数为$n$的首一多项式，$\langle f(x)\rangle$表示$f(x)$在多项式环$\mathbb{Z}[x]$中生成的理想。然后考虑式(7)的嵌入

$$\left.\begin{aligned} \sigma: R\to\ & \mathbb{Z}^n\\ \sum_{i=0}^{n-1} a_i x^i\mapsto\ & (a_{n-1}, a_{n-2}, \cdots, a_0) \end{aligned}\right\} \tag{7}$$

对于任何一个多项式$v(x)\in R$，用$\boldsymbol{v}$来表示$v(x)$在嵌入σ下的像，并且将$\boldsymbol{v}$和$v(x)$考虑为等价的表达式。

令$g(x)\in R$为一个次数小于n的多项式且$v(x)\in\langle g(x)\rangle$，则存在一个次数小于$n$的多项式$w(x)\in\mathbb{Z}[x]$使得$v(x)=w(x)g(x)\bmod f(x)$。如果将$w(x)$表示为$w(x)=w_{n-1}x^{n-1}+w_{n-2}x^{n-2}+\cdots+w_0$，那么$v(x)=\sum_{i=0}^{n-1} w_i x^i g(x)\bmod f(x)$。于是每

一个$\langle g(x)\rangle$中的元素都可以由$g(x)\bmod f(x)$, $xg(x)\bmod f(x)$, $\cdots$, $x^{n-1}g(x)\bmod f(x)$整系数线性表示的。所以$\langle g(x)\rangle$在嵌入σ下构成一个格。于是有：

定义 4(理想格) 给定$g(x)\in R=\mathbb{Z}[\mathrm{x}]/\langle f(x)\rangle$，这里$f(x)\in\mathbb{Z}[x]$是一个次数为$n$的首一多项式，那么由$g(x)$在嵌入$\sigma$下构成一个格$\mathcal{L}$，称$\mathcal{L}$为由$g(x)$生成的理想格。

更进一步，如果$g(x)$和$f(x)$在$\mathbb{Z}$上互素，则$g(x)\bmod f(x)$, $xg(x)\bmod f(x)$, $\cdots$, $x^{n-1}g(x)\bmod f(x)$是线性无关的。否则存在不全为零的整系数a_0, a_1, $\cdots, a_{n-1}$使得$\sum_{i=0}^{n-1}a_ix^ig(x)\bmod f(x)=0$，即$\left(\sum_{i=0}^{n-1}a_ix^i\right)g(x)=0\bmod f(x)$，而这说明$g(x)$和$f(x)$并不是互素的，矛盾。所以此时由$g(x)$生成的理想格是满秩的。

定义 5(本原格向量) 一个格向量$\boldsymbol{v}\in\mathcal{L}$如果是格$\mathcal{L}$中的一个本原格向量当且仅当对任意的整数$k>1$，$\boldsymbol{v}/k\notin\mathcal{L}$。

定义 6(本原向量) 对于一个向量$\boldsymbol{v}=(v_1,v_2,\cdots,v_n)\in\mathcal{L}$，如果$\gcd(v_1,v_2,\cdots,v_n)=1$，则称$\boldsymbol{v}$是一个本原向量。

定义 7(本原多项式) 一个多项式$a(x)\in\mathbb{Z}[x]$称为本原多项式当且仅当对任意整数满足$k>1$都有$a(x)/k\notin\mathbb{Z}[x]$。

定义 8(容度) 给定一个多项式$a(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\in\mathbb{Z}[x]$，其容度定义为$a(x)$的各系数的最大公因子，即$\gcd(a_n,a_{n-1},\cdots,a_0)$，并将容度表示为$\mathrm{cont}(a(x))$。

很明显，对于任意的多项式$a(x)\in\mathbb{Z}[x]$，$a(x)/\mathrm{cont}(a(x))$是一个本原的多项式，称之为$a(x)$的本原部分。

一个格向量$\boldsymbol{v}=\boldsymbol{x}\boldsymbol{B}\in\mathcal{L}(\boldsymbol{B})$是一个本原的格向量当且仅当$\boldsymbol{x}$是一个本原向量。和在一般格中类似，在由$g(x)\in R=\mathbb{Z}[x]/\langle f(x)\rangle$生成的理想格中，一个格向量$v(x)=t(x)g(x)\bmod f(x)$是本原的当且仅当$t(x)$是一个本原多项式。

2.5 Hermite标准型

对于整数矩阵而言，Hermite标准型是一个非常重要的概念，其定义如下：

定义 8(Hermite标准型) 一个非奇异的方阵$\boldsymbol{H}\in\mathbb{Z}^{n\times n}$是Hermite标准型，如果满足如下条件：

(1) $h_{ii}>0, 1\le i\le n$;

(2) $h_{ij}>0, 1\le j<i\le n$;

(3) $0\le h_{ji}<h_{ii}, 1\le j<i\le n$。

需要注意的是，这里只给出了Hermite标准型的一种定义，是作行变换得到一个上三角矩阵。根据是行列变换以及最后是上三角矩阵还是下三角矩阵，Hermite标准型会有不同的定义。

对于高维随机生成的矩阵，其Hermite标准型的对角元素是非常不平衡的：大多数都很小(实际上大多数都为1)，而且经常最后一个元素非常大，该类Hermite标准型通常会有密码学意义。由此定义如下一个非常特别的Hermite标准型：

定义 8(简单Hermite标准型) 一个非奇异的方阵$\boldsymbol{H}\in\mathbb{Z}^{n\times n}$是简单Hermite标准型当且仅当其是Hermite标准型且满足$h_{ii}=1$，其中$1\le i\le n-1$。

通常在格密码中选择具有简单Hermite标准型的格，可以使得计算更简单、密钥尺寸更小。

2.6 Smith标准型

对于整数矩阵而言，另一个重要的标准型是Smith标准型。其定义如下：

定义 8(Smith标准型) 一个方阵$\boldsymbol{S}\in\mathbb{Z}^{n\times n}$是Hermite标准型，如果满足如下条件：

(1) $s_{ii}|s_{jj}, i<j$;

(2) $s_{ij}>0, i\ne j$。

文献[10,11]说明在理想格中，格基的Hermite标准型具有非常特殊的形式。

引理 7 令$\mathcal{L}$为由$g(x)\in R=\mathbb{Z}[x]/\langle f(x)\rangle$生成的理想格，这里$f(x)$是$\mathbb{Z}[x]$中一个次数为$n$的首一多项式，$g(x)$的次数为$m$，且$n>m$。假设$g(x)$与$f(x)$互素，那么$\mathcal{L}$的Hermite标准型由式(8)表示

$$\boldsymbol{H}=\begin{bmatrix} h_{11} & h_{12} & \cdots & h_{1n} \\ & h_{22} & \cdots & h_{2n} \\ & & \ddots & \vdots \\ & & & h_{nn} \end{bmatrix} \tag{8}$$

满足$h_{ii}|h_{1j}$，对于$1\le i\le l\le j\le n$。

由上所述，对于一个理想格而言，其格基的Hermite标准型的对角线构成了其Smith标准型。

3 理想格上格基三角化的快速算法

这节给出对于理想格$\mathcal{L}$上格基快速三角化的算法，该算法可以在$O\left(n^3\log_2 B\right)$时间内完成，这里$\mathcal{L}$是由$g(x)\in R=\mathbb{Z}[x]/\langle f(x)\rangle$生成的理想格，$f(x)$是$\mathbb{Z}[x]$上一个首一$n$次的不可约多项式，$B$是$f(x)$和$g(x)$的系数上界(在本文中，不作特殊说明外，考虑$g(x)$为一个本原多项式)。本文算法包括两个步骤，首先利用扩展欧几里得算法计算出一系列次数递减的本原格向量，然后从这些格向量中构造出$\mathcal{L}$的一个三角化格基。

为了简单表达，先给出一些符号：对于由$f(x)$和$g(x)$得到的余式序列表示为$r_1(x)$, $r_2(x)$, $\cdots$, $r_l(x)$。将$f(x)$和$g(x)$分别表示为$r_{-1}(x)$和$r_0(x)$,余

式的次数分别用n_i来表示，即$n_i=\deg(r_i)$，且用δ_i来表示相邻次数之差，即$\delta_i=n_i-n_{i-1}$，对于$i=-1,0,\cdots,l-1$。

3.1 计算本原格向量序列

这节给出计算本原格向量序列的算法，该算法源于理想格上三角化和使用欧几里得算法来计算多项式的余式时情况很类似。表1给出了计算本原格向量序列的过程。

表 1 本原格向量序列

输入：$\mathbb{Z}[x]$中$f(x)$和$g(x)$，次数分别为n和m，且$n>m$；

(1) 利用扩展欧几里得算法计算$\mathbb{Q}[x]$上$r_i'(x)$, $s_i'(x)$, $t_i'(x)$，使得$r_i'(x)=r_{i-2}'(x)+q_i'(x)r_{i-1}'(x)$和$r_i'(x)=s_i'(x)f(x)+t_i'(x)g(x)$成立，这里$i=1,2,\cdots,l$；

(2) 计算每一个$t_i'(x)$系数分母的最小公倍数C_i，$i=1,2,\cdots,l$；

(3) 令$r_i(x)=r_i'(x)\cdot C_i$为余式序列中第i个余式，$i=1,2,\cdots,l$；

输出：$r_1(x), r_2(x), \cdots, r_l(x)$

引理 8 令$f(x)$和(x)为$\mathbb{Z}[x]$中次数分别为n和m两个多项式，$f(x)$是首一不可约多项式且次数满足$n>m$。定义$\mathcal{L}$是由$g(x)\in R=\mathbb{Z}[x]/\langle f(x)\rangle$生成的理想格。令$B$为$f(x)$和$g(x)$所有系数的上界，那么表1算法可以在$O\left(n^3\log_2 B\right)$内输出$\mathcal{L}$中次数递减的本原格向量。

首先，可以看到$t_i(x)=t_i'(x)\cdot C_i$是本原多项式。注意到$C_i r_i'(x)=C_i s_i'(x)f(x)+C_i t_i'(x)g(x)$，由于$f(x)$是首一的，那么从理想格的角度来看，$t_i(x)$对应于格基的整系数表示，所以可以得到$C_i s_i'(x)$和$C_i t_i'(x)$都是整系数多项式。因此，算法1中输出的余式$r_i(x)$为格$\mathcal{L}$中的本原格向量，$i=1,2,\cdots,l$。

至于表1算法的时间复杂度，根据引理4，在$O\left(n^3\log_2 B\right)$时间内计算出$\mathbb{Q}[x]$上所有的$r_i'(x)$, $s_i'(x)$, $t_i'(x)$，这意味着输出长度最大为$O\left(n^3\log_2 B\right)$。另一方面，在表1算法中计算$t_i'(x)$所有系数分母的最小公倍数，其最大为所有分母的乘积，于是可以得到$t_i'(x)$的系数大小是由行列式$O(n\log_2 B)$唯一决定的。所以算法1的输出尺寸最大为$O\left(n^3\log_2 B\right)$，当考虑快速整数乘法时，步骤(2)中时间复杂度也最大为$O\left(n^3\log_2 B\right)$。所以表1算法可以在$O\left(n^3\log_2 B\right)$时间内输出次数递减的本原格向量序列。

表1算法是将域上面多项式的扩展欧几里得算法延伸到了整数多项式环上，因为在由$g(x)\in R=\mathbb{Z}[x]/\langle f(x)\rangle$生成的理想格$\mathcal{L}$中有$r(x)=s(x)f(x)+t(x)g(x)$，所以当$t(x)$的系数为整数时，相当于$x(x)$在格$\mathcal{L}$中是由格基的整系数线性表示的，可以得到$r(x)$的系数也必然为整数。

3.2 理想格上格基的三角化

这节说明怎么利用次数递减的本原格向量序列来对格基进行三角化。为了便于表述，将集合$\{1,2,\cdots,n\}$划分为l个子集合：$\{n-n_{i-1}+1, n-n_{i-1}+2\cdots, n-n_i\}=\bigcup_{i=1}^{l} I_i$。具体算法如表2所示。

表 2 理想格上格基的三角化

输入：本原格向量序列，$r_0(x), r_1(x), \cdots, r_l(x)$(向量形式为$\boldsymbol{r_0}, \boldsymbol{r_1}, \cdots, \boldsymbol{r_l}$)

(1) 令$\boldsymbol{T}\leftarrow 0^{n\times n}$

(2) 如果$k\in I_l, \boldsymbol{T}_k(x)=r_l(x)x^{n-k}, i\leftarrow l-1$

(3) 如果$k\in I_i$，

(a) 计算ϕ和ψ使得 $\phi\mathrm{lc}(r_i)+\psi\mathrm{lc}\left(\boldsymbol{T}_{n-n_{i+1}}\right)=\gcd\left(\mathrm{lc}\left(\boldsymbol{T}_{n-n_{i+1}}\right), \mathrm{lc}(r_i)\right)$

(b) 令$\boldsymbol{T}_{n-n_i}(\boldsymbol{x})=\phi r_i(x)+\psi\boldsymbol{T}_{n-n_{i+1}}(x)x^{\delta_i}$

(c) 如果$\mathrm{lc}\left(\boldsymbol{T}_{n-n_i}\right)=1$，则令 $\boldsymbol{T}_j(x)=\boldsymbol{T}_{n-n_i}(x)x^{n-n_i-j}$, $j=1,2,\cdots,n-n_i$，并结束循环

(d) 否则$\boldsymbol{T}_k(x)=\boldsymbol{T}_{n-n_i}(x)x^{n-n_i-k}$, $i\leftarrow i-1$

(e) 如果$i>0$，到(3)开始循环，否则结束循环

输出：$\boldsymbol{T}$

引理 9 令$f(x)$和$g(x)$为$\mathbb{Z}[x]$中次数分别为n和m两个多项式，$f(x)$是首一不可约多项式且次数满足$n>m$。定义$\mathcal{L}$是由$g(x)\in R=\mathbb{Z}[\mathrm{x}]/\langle f(x)\rangle$生成的理想格。那么存在一个确定性算法，输入表1算法中得到的本原格向量序列，输出$\mathcal{L}$的一个三角化格基，运行时间为$O\left(n^3\log_2 B\right)$，其中$B$为$f(x)$和$g(x)$所有系数的上界。

现在来分析表2算法的时间复杂度。根据Hadmard界，$r_i(x)$的各系数的上界为$\left(\sqrt{n+m}B\right)^{n+m}$，所以$r_i(x)$的系数由$\left(\sqrt{n+m}B\right)^{n+m}$界定。每一次迭代需要$n_i+n_{i+1}+2$次$O(n\log_2 B)$比特数字的乘法，所以总的时间复杂度为$\sum_{i=0}^{l-1}\left((n_i+n_{i+1}+2)O(n\log_2 B)\right)=O\left(n^3\log_2 B\right)$。

由于t_{nn}为格$\mathcal{L}$中的常数，且$t_{nn}x^i\in\mathcal{L}$，其中$i=0,1,\cdots,n-1$。所以在进行表2算法时，实际可以在计算中通过模t_{nn}来降低计算量，这种操作并不会增加总的时间复杂度。

定理 1 令$f(x)$和$g(x)$为$\mathbb{Z}[x]$中次数分别为n和m两个多项式，$f(x)$是首一不可约多项式且次数满足$n>m$, B为$f(x)$和$g(x)$所有系数的上界。定义$\mathcal{L}$是由$g(x)\in R=\mathbb{Z}[x]/\langle f(x)\rangle$生成的理想格。那么存在一个确定的算法输入$f(x)$和$g(x)$，在

$O\left(n^3\log_2 B\right)$时间内输出$\mathcal{L}$的一个三角化格基$\boldsymbol{T}$。特别地，$\boldsymbol{T}$的对角线为$\mathcal{L}$上格基的Smith标准型。

证明　根据算法1和算法2，定理的第1部分是正确的。

对于定理的第2部分，利用引理7来证明。根据$\boldsymbol{T}$的结构，可知$\boldsymbol{T_i}=\boldsymbol{H_i}+\sum_{k=i+1}^{n}\boldsymbol{H}_k$。由引理7，$t_{ii}=h_{ii}|h_{jk}$，其中$i\le j\le k\le n$,所以$t_{ii}|\boldsymbol{T_i}$。然后利用矩阵的初等列变换可知$\boldsymbol{T}$的对角线正好构成$\mathcal{L}$上格基的Smith标准型。　　证毕

3.3 例子

根据本文的算法，给出一个例子来形象地表示算法过程。假设$f(x)=x^8+x^6-3x^4-3x^3+8x^2+2x-5$，$g(x)=3x^6+5x^4-4x^2-9x+21$。利用算法1，得到本原格向量如式(9)

$$\left.\begin{aligned} r_0(x)&=3x^6+5x^4-4x^2-9x+21\\ r_1(x)&=-5x^4+x^2-3\\ r_2(x)&=13x^2+25x-49\\ r_3(x)&=-9326x+12300\\ r_4(x)&=130354 \end{aligned}\right\} \tag{9}$$

这里$n_1=4$, $n_2=2$, $n_3=1$, $n_4=0$。然后利用算法2，得到

$$\left.\begin{aligned} \boldsymbol{T}_2(x)&=x^6+30596x^5+591x^4+2x^2-9x+21\\ \boldsymbol{T}_4(x)&=x^4+115056x^3-293x^2-3\\ \boldsymbol{T}_6(x)&=x^2+84353x-49\\ \boldsymbol{T}_7(x)&=2x+72848\\ \boldsymbol{T}_8(x)&=130354 \end{aligned}\right\} \tag{10}$$

于是一个三角化矩阵为

$$\boldsymbol{T}=\begin{bmatrix} 1 & 84353 & -49 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 84353 & -49 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 84353 & -49 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 84353 & -49 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 84353 & -49 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 84353 & -49\\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 72848\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 130354 \end{bmatrix} \tag{11}$$

并且Smith标准型为

$$\boldsymbol{S}=\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 2 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 130354 \end{bmatrix} \tag{12}$$

4　快速计算Hermite标准型

这一节说明怎么在$O\left(n^3\log_2 B\right)$时间内计算一类特殊的理想格的Hermite标准型。事实上，这一类特殊的理想格的Hermite标准型是具有简单形式的。

同样，计算是基于文献[11]中发现的理想格的性质。对于具有简单Hermite标准型的理想格，其Hermite标准型可以隐式地由两个整数(d,r)来表示，其中d为理想格的行列式，$r=-h_{(n-1)n}$。而唯一非平凡的列是最后一列，且$h_{in}=r^{n-i}\bmod d$，对于$i=1,2,\cdots,n-1$。所以最后一列可以在$O\left(n^3\log_2 B\right)$时间内平凡地计算出来。但是目前还不清楚对于Hermite标准型为一般形式的理想格怎么来加速计算过程，这也将是下一步的研究内容。

5　结论

本文通过利用理想格本身特殊的多项式结构，提出了一个新的算法可以在$O\left(n^3\log_2 B\right)$时间内对理想格格基进行三角化，并且利用理想格上Hermite标准型的特殊性质，同样可以在$O\left(n^3\log_2 B\right)$内计算出Smith标准型。最后，针对某一类应用于密码学的理想格，可以在$O\left(n^3\log_2 B\right)$时间内计算出Hermite标准型。

参 考 文 献

[1] FRUMKIN M A. Complexity questions in number theory[J]. *Journal of Soviet Mathematics*, 1985, 29(4): 1502–1517. doi: 10.1007/bf02104748.

[2] HUNG M S and ROM W O. An application of the Hermite normal form in integer programming[J]. *Linear Algebra and its Applications*, 1990, 140: 163–179. doi: 10.1016/0024-3795(90)90228-5.

[3] HAFNER J L and MCCURLEY K S. A rigorous subexponential algorithm for computation of class groups[J]. *Journal of the American Mathematical Society*, 1989, 2(4): 837–850. doi: 10.1090/S0894-0347-1989-1002631-0.

[4] HARTLEY B and HAWKES T O. Rings, Modules and Linear Algebra[M]. London: Chapman and Hall, 1970: 73.

[5] MICCIANCIO D. Improving lattice based cryptosystems using the Hermite normal form[C]. International Conference on Cryptography and Lattices, Providence, 2001: 126–145. doi: 10.1007/3-540-44670-2_1.

[6] LYUBASHEVSKY V and PREST T. Quadratic time, linear

space algorithms for Gram-Schmidt orthogonalization and Gaussian sampling in structured lattices[C]. The 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, 2015: 789–815. doi: 10.1007/978-3-662-46800-5_30.

[7] HAFNER J L and MCCURLEY K S. Asymptotically fast triangulation of matrices over rings[C]. The 1st Annual ACM-SIAM Symposium on Discrete Algorithm, San Francisco, 1990: 197–200.

[8] LE GALL F. Powers of tensors and fast matrix multiplication[C]. The 39th International Symposium on Symbolic and Algebraic Computation, Kobe, 2014: 296–303. doi: 10.1145/2608628.2608664.

[9] STORJOHANN A and LABAHN G. Asymptotically fast computation of Hermite normal forms of integer matrices[C]. 1996 International Symposium on Symbolic and Algebraic Computation, Zurich, 1996: 259–266.

[10] DING Jintai and LINDNER R. Identifying ideal lattices[EB/OL]. http://eprint.iacr.org/2007/322, 2007.

[11] ZHANG Yang, LIU Renzhang, and LIN Dongdai. Improved key generation algorithm for Gentry's fully homomorphic encryption scheme[C]. The 20th International Conference on Information Security and Cryptology, Seoul, 2018: 93–111. doi: 10.1007/978-3-319-78556-1_6.

[12] VON ZUR GATHEN J and GARHARD J. Modern Computer Algebra[M]. 3rd ed. Cambridge: Cambridge University Press, 2013: 313–332.

[13] 刘仁章. 格算法及其密码学应用[D]. [博士论文], 中国科学院大学数学与系统科学研究院, 2016.

张 洋：男，1991年生，博士生，研究方向为基于理想格算法的密码算法分析.

刘仁章：男，1989年生，博士，研究方向为格算法及格密码算法分析.

林东岱：男，1964年生，研究员，研究方向为密码学与安全协议、网络与系统安全、分布式密码计算.