一类高维随机矩阵置乱变换的周期*

王泽辉
（中山大学科学计算与计算机应用系，广东 广州 510275）

摘 要：为了适合多媒体信息量庞大、存在数据冗余的特点，实施可证明安全、高效率的加密解密，使用了数论、近世代数、矩阵变换、算法分析等工具，对高维随机矩阵置乱变换的精确周期进行了研究。将实数域上线性代数的若干结果，推广到模素数有限域上，得到一类整数矩阵及其相关同余方程组之解的若干新性质；在此基础上将用于置乱的矩阵由 2 维扩展到任意高维，给出广泛一类高维随机整数矩阵 A 决定的置乱变换，在任意素数幂 $N=p^r$ 模数下，其周期 $T(A, N)$ 的精确表达式，给出求精确周期算法的时间复杂度。结论可用于 建立新型数字多媒体密码体制和信息隐藏体制，扩大其密钥空间，增加其安全性 。

关键词：随机矩阵置乱变换；周期性；模素数有限域；数字多媒体加密；快速算法
中图分类号：TN918 **文献标志码**：A **文章编号**：0529－6579（2010）04－0038－05

On Periods of Higher Dimensional Random Matrix Scrambling Permutations

WANG Zehui
(Department of Scientific Computation and Computer Applications,
Sun Yat-sen University, Guangzhou 510275, China)

Abstract: For efficiently implementing the encryption/decryption for digital multimedia, which is often with huge amount of data and much redundancy, the accurate period of high dimension random matrix scrambling permutation is studied with the help of number theory and algebraic theory. Some new properties of a class of integer matrices and the solutions of its correlative congruent equations are obtained by generalizing some results for linear algebra in real fields to the finite fields over modulo prime numbers. Based on these properties, random scrambling permutation can be extended to any high dimension matrix A and the period T (A, N) with an arbitrary prime power modulo $N=p^r$ can be accurately expressed. The complexity of the computation of T (A, N) is presented. The results can be used to construct new cryptosystems for digital multimedia and information hiding systems with bigger key spaces to improve their security levels.

Key words: random matrices scrambling transformations; periodicity; finite fields over modulo prime numbers; digital multimedia encipher; fast algorithm

随机矩阵置乱变换技术是在以 Arnold 变换为代表的简单矩阵置乱变换技术基础上发展而来的（对置乱技术矩阵都默认为整数矩阵），在数字图像加密和信息隐藏中有重要的作用[1]。文［2］给出 2 维随机整数矩阵 A 决定的置乱变换在任意模 N 下，其周期 $T(A,N)$ 的精确表达式及上界估计，并提出确定性算法 T_{2D}：随机输入 2 维整数矩阵的元素值及随机的模数 N，输出精确周期 $T(A,N)$，证

* 收稿日期：2009－11－20
基金项目：广东省自然科学基金资助项目（7003624）
作者简介：王泽辉（1963 年生），男，副教授；E-mail：mcswzh@mail.sysu.edu.cn

明算法的时间复杂度仅 96 $|\log_2 N|^2$次模 N 乘法，属于多项式时间算法。文［2］证明了把一般整数 N 分解为一系列素数幂 p^r 之积后，求 $T(A,N)$ 转化为求所有的 $T(A,p^r)$。文［3］在文［2］基础上建立了语义安全的数字多媒体密码体制。在该体制中确定随机矩阵置乱变换的周期至为重要，该周期可类比于 RSA 加密的 mod n 周期 $\varphi(n)$，ECC 加密中循环群的阶，确定周期（阶）才能构造私钥，继而才能加密、解密，这是最基础的工作。为增加密码体制的密钥空间，需将置乱矩阵由 2 维推广到任意维。这方面文献已有些初步结果，较有代表性是，文［4］给出 3 维 Arnold 变换周期的一些结果. 文［5］给出 n 维 Arnold 变换周期的等价条件，其置乱矩阵元素由 1 到 n 有规律排列即属于简单置乱。文［6］给出三维随机矩阵置乱变换的周期 。本文将随机矩阵由 3 维扩展到任意维，把 模数限制为素数幂 p^r，研究广泛一类高维随机整数矩阵 A，所决定的置乱变换精确周期 $T(A,p^r)$ 的表达式，并探讨其应用价值。

1　有限域上线性代数若干结果

下文中 $\mathbb{Z}$，$\mathbb{N}$，$\mathbb{R}$ 分别为整数集，自然数集与实数集，gcd、lcm 分别为最大公约数与最小公倍数记号，$|A|$ 为方矩阵 A 的行列式。

设 p 为素数，$(\mathbb{Z}_p)_{m\times m}$为有限域 $\mathbb{Z}_p=\{0,1,\cdots,p-1\}$ 上所有 $m\times m$ 矩阵集合，其中 $O\in(\mathbb{Z}_p)_{m\times m}$为零矩阵，$\mathrm{diag}(c_1,c_2,\cdots,c_m)$ 表示对角线为 $c_1,c_2,\cdots,c_m$ 其余位置为 0 的矩阵，I_m 为 m 维单位矩阵，简记为 I。$(\mathbb{Z}_p)_m$ 为有限域 $\mathbb{Z}_p$ 上所有 m 维列向量集合，其中 $\theta\in(\mathbb{Z}_p)_m$ 为零向量，c 的模 p 逆元简记为 c^{-1}。

任意两个 $n\times m$ 矩阵（特殊为向量）$E=(e_{ij})_{n\times m}$，$F=(f_{ij})_{n\times m}$，当任意 i,j 成立 $e_{ij}\equiv f_{ij}\pmod p$ 时记 $E\equiv F(\bmod p)$，简记 $E\equiv F$，否则记 $E\not\equiv F(\bmod p)$，简记 $E\not\equiv F$。类似于实数域可建立线性同余方程组 $Bz\equiv b$ 及齐次同余方程组 $Bz\equiv\theta$，未知量用 z 表示。

定义 1　(i)对于 $B\in(\mathbb{Z}_p)_{m\times m}$，如存在 $D\in(\mathbb{Z}_p)_{m\times m}$，使 $BD\equiv BD\equiv I$ 成立，则称 B 模 p 可逆，记 $D=B^{-1}$。如找不到这样的 D 则称 B 模 p 不可逆。

(ii) 设 $\alpha_1,\alpha_2,\cdots\alpha_k\in(\mathbb{Z}_p)_m$，如存在模 p 不同时为 0 的 k 个数 $c_1,c_2,\cdots,c_k$，使 $c_1\alpha_1+\cdots+c_k\alpha_k\equiv\theta$ 成立，则称 $\alpha_1,\alpha_2,\cdots\alpha_k$ 模 p 线性相关，如找不到这样的一组数，则称 $\alpha_1,\alpha_2,\cdots\alpha_k$ 模 p 线性无关。

任意 $B\in(\mathbb{Z}_p)_{m\times m}$，类似于 $R_{m\times m}$可以对 B 作第 1、2 类初等变换，得到：

命题 1　任意 $B\in(\mathbb{Z}_p)_{m\times m}$，$B\not\equiv O$，则存在第 1、第 2 类初等矩阵 P_1，P_2，$\cdots P_l$，Q_1，Q_2，$\cdots Q_r$，使

$$P_1P_2\cdots P_lBQ_r\cdots Q_2Q_1\equiv \mathrm{diag}(a_{11},\cdots,a_{kk},0,\cdots 0)\tag{1}$$

其中 $\gcd(a_{jj},p)=1$，$j=1,\cdots,k$，$1\leqslant k\leqslant m$.

推论 1　在命题 1 的条件下有：

(i) $|B|\not\equiv 0(\bmod p)\Leftrightarrow k=m\Leftrightarrow|B|\equiv a_{11}a_{22}\cdots a_{mm}\not\equiv 0\Leftrightarrow B$ 模 p 可逆且逆矩阵可表示为

$B^{-1}\equiv Q_r\cdots Q_2Q_1\ \mathrm{diag}((a_{11})^{-1}\cdots,(a_{mm})^{-1})P_1P_2\cdots P_l$。

(ii) $|B|\equiv 0(\bmod p)\Leftrightarrow k<n\Leftrightarrow Bz\equiv\theta$ 有非零解 $z_0\not\equiv\theta\Leftrightarrow B$ 模 p 不可逆。

推论 2　(i) 设 $B\in(\mathbb{Z}_p)_{m\times m}$，则 B 模 p 可逆等价于 $Bz\equiv\theta$ 仅有零解 $z_0\equiv\theta$。

(ii) 设 $B\in(\mathbb{Z}_p)_{m\times m}$，$B\not\equiv O$，则存在 $z_0\not\equiv\theta$ 使 $Bz_0\not\equiv\theta$。

(iii) 如 $\alpha_1,\alpha_2,\cdots\alpha_m\in(\mathbb{Z}_p)_m$ 模 p 线性无关，将其合并为 $W=(\alpha_1,\alpha_2,\cdots\alpha_m)\in(\mathbb{Z}_p)_{m\times m}$，则 W 模 p 可逆。

模仿实数域上线性代数的有关证明方法，容易证明推论 1、2，因篇幅限制，不赘述。

命题 2　设 $A\in(\mathbb{Z}_p)_{m\times m}$，$I$ 为单位矩阵，如有 $\lambda_i\in\mathbb{Z}$ 使 $|\lambda_iI-A|\equiv 0(\bmod p)$，记 $B_i=\lambda_iI-A$，则同余方程组 $B_iz\equiv\theta$ 必有非零解 $z_i\not\equiv\theta$。

证明　由推论 1(ii) 可得。

2　一类高维随机置乱变换的周期

设整数 $m\geqslant 3$，r 为正整数，p 为素数，^ 表示幂运算，$a\hat{}b=a^b$，$N=p\hat{}r$ 为素数幂，$\mathbb{Z}_N=\{0,1,\cdots,N-1\}$，$(\bmod N)$ 表示代数运算及矩阵运算结果都在 $\mathbb{Z}_N$ 取值。$\mathrm{ord}_p(b)$ 表示 b 模 p 之阶，即满足 $b^t\equiv 1(\bmod p)$ 之最小正整数。有限环 $\mathbb{Z}_p[x]$ 中元素由于参与运算经常表现为 $\mathbb{Z}[x]$ 中元素。

定义 1　定义 m 维随机整数矩阵 A 在任意模 $N=p\hat{}r$ 下的置乱变换如下

$$w'=Aw\ (\bmod N)\tag{2}$$

其中 $A\in(\mathbb{Z}_p)_{m\times m}$，$w'$，$w\in(\mathbb{Z}_p)_m$；变换(2) 式的周期 $T(A,N)$ 即是使(3) 式成立的最小正整数。

$$A^t\equiv I(\bmod N)\tag{3}$$

定义 2　(i) 设 $f_1(x)$，$f_2(x)\in\mathbb{Z}[x]$，$f_1(x)=x^k+b_1x^{k-1}+\cdots+b_k$，$f_2(x)=x^k+c_1x^{k-1}+\cdots+c_k$，如 $b_i\equiv c_i(\bmod p)$，$i=1,2,\cdots,k$，则记 f_1

$(x) \equiv f_2(x) \pmod p$，简记为$f_1(x) \equiv f_2(x)$。

(ii) 对$h(x)$，$f(x) \in \mathbb{Z}[x]$，如存在$g(x) \in \mathbb{Z}[x]$使$h(x) \equiv g(x) f(x) \pmod p$成立，则称“在$\mathbb{Z}_p[x]$中$f(x)$整除$h(x)$”，简记为$f(x) \mid h(x)$。

下面的引理1-3分别由文[2]的引理1、定理1及定理2的证明部分得到。

引理1 变换(1)存在周期$T(A,N)$当且仅当

$$\gcd(|A|,N) = 1 \tag{4}$$

引理2 设$N = p^r$，$\gcd(|A|, N) = 1$，则变换(2)式的周期

$$T(A, N) = \min\{(p\hat{}y)\ l \mid 0 \leqslant y \leqslant r-1,\ y \in \mathbb{Z};\ A\hat{}(Ql) \equiv I_m \pmod N,\ l = T(A, p),\ Q = (p\hat{}y)\} \tag{5}$$

引理3 对任意素数p，记$d = \mathrm{ord}_p(e)$，则存在$h(x) \in \mathbb{Z}_p[x]$使得$(x-e) \mid (x^d - 1)$或

$$x^d - 1 \equiv h(x)(x-e) \pmod p \tag{6}$$

以下研究广泛一类高维随机矩阵$A \in (\mathbb{Z}_p)_{m\times m}$，$\gcd(|A|, p) = 1$，$A$使$m$次同余方程

$$f(\lambda) \equiv 0 \pmod p \tag{7}$$

在$\mathbb{Z}_p$存在m个解，其中$f(\lambda) = |\lambda I - A|$，显然$f(\lambda)$为$\lambda$的$m$次多项式。故$f(0) = |-A| = (-1)^m |A|$，$\gcd(|A|, p) = 1$隐含了$|A| \not\equiv 0 \pmod p$，(7)式在$\mathbb{Z}_p$没有零根。且(7)式所有$m$个解模$p$不同余仅发生于$p \geqslant m+1$时，$p < m+1$必导致模$p$重根的存在。

定理1 如(7)式在$\mathbb{Z}_p$中有k个模p互相不同余之根$\lambda_1, \lambda_2, \cdots \lambda_k$，$B_i = \lambda_i I - A$，$B_i z \equiv \theta$的非零解为$z_i \not\equiv \theta$，$i = 1, \cdots, k$；则$z_1, z_2, \cdots z_k$模$p$线性无关；特别是$k = m$时，合并其为$W = (z_1, z_2, \cdots z_m) \in (\mathbb{Z}_p)_{m\times m}$，则$W$模$p$可逆。

证明 $B_i z_i \equiv \theta \Leftrightarrow A z_i \equiv \lambda_i z_i$. 前部分用归纳法证明之。当$k = 1$时结论显然，设$k = t$时成立，$z_1, z_2, \cdots z_t$模$p$线性无关，则$k = t+1$时，如存在$t+1$个数$c_1, c_2, \cdots, c_{t+1}$，使$c_1 z_1 + \cdots + c_{t+1} z_{t+1} \equiv \theta$成立，两边同左乘于$A$以及同乘于$\lambda_{t+1}$并相减推出矛盾，即$z_1, z_2, \cdots z_{t+1}$模$p$线性无关，归纳法得证。后部分由推论2(iii)得证。

定理2 如$p \geqslant m+1$，(7)式在$\mathbb{Z}_p$中有m个模p互相不同余之根$\lambda_1, \lambda_2, \cdots \lambda_m$，则

$$T(A, p) = \mathrm{lcm}(\mathrm{ord}_p(\lambda_1), \mathrm{ord}_p(\lambda_2), \cdots, \mathrm{ord}_p(\lambda_m)) \tag{8}$$

证明 记$d = \mathrm{lcm}(\mathrm{ord}_p(\lambda_1), \mathrm{ord}_p(\lambda_2), \cdots, \mathrm{ord}_p(\lambda_m))$，$t = T(A, p)$，由假定$f(\lambda) \equiv (\lambda - \lambda_1)(\lambda - \lambda_2) \cdots (\lambda - \lambda_m)$。记$B_i = \lambda_i I - A$，$B_i z \equiv \theta$的非零解为$z_i$，$i = 1, \cdots, m$；则由定理1，$W = (z_1, z_2, \cdots z_m)$模$p$可逆。

$B_i z_i \equiv \theta$等价于$A z_i \equiv \lambda_i z_i$，故$A(z_1, z_2, \cdots z_m) \equiv (z_1, z_2, \cdots z_m) \Lambda$，其中$\Lambda = \mathrm{diag}(\lambda_1, \lambda_2, \cdots \lambda_m)$，$A \equiv W \Lambda W^{-1}$，推出$A^t \equiv W \mathrm{diag}((\lambda_1)^t, (\lambda_2)^t, \cdots, (\lambda_m)^t) W^{-1}$，由定义$A^t \equiv I$，即$(\lambda_i)^t \equiv 1 \pmod p$，$\mathrm{ord}_p(\lambda_i) \mid t$，$i = 1, \cdots, m$；所以$d \mid t$。

由引理3，$(\lambda - \lambda_i) \mid (\lambda\hat{}\ \mathrm{ord}_p(\lambda_i) - 1)$，故$(\lambda - \lambda_i) \mid (\lambda^d - 1)$，$i = 1, \cdots m$；$\lambda_1, \lambda_2, \cdots \lambda_m$模$p$互不同余，推出$(\lambda - \lambda_1)(\lambda - \lambda_2) \cdots (\lambda - \lambda_m) \mid (\lambda^d - 1)$，即存在$h(\lambda)$使得$\lambda^d - 1 \equiv h(\lambda) f(\lambda)$. 由凯莱定理$f(A) = O$，所以$A^d - I \equiv h(A) f(A) \equiv O$，$A^d \equiv I$，依周期最小性，$t \mid d$。已证$d \mid t$，故$d = t$即(8)式成立。

易知$\gcd(d, p) = 1$，由引理2可得

定理3 如$p \geqslant m+1$，(7)式在$\mathbb{Z}_p$中有m个模p互相不同余之根$\lambda_1, \lambda_2, \cdots \lambda_m$，$d = \mathrm{lcm}(\mathrm{ord}_p(\lambda_1), \mathrm{ord}_p(\lambda_2), \cdots, \mathrm{ord}_p(\lambda_m))$，则变换(2)式的周期 $T(A, p^r) = d \times \min\{p^y \mid 0 \leqslant y \leqslant r-1,\ A\hat{}(p^y d) \equiv I_m \pmod{p^r}\}$，

计算机程序只需作r个循环便可确定$T(A, p^r)$之值。

命题3 设m阶矩阵$\mathbb{U}$为

$$\mathbb{U} = \begin{pmatrix} e & 0 & 0 & \cdots & 0 & 0 \\ 1 & e & 0 & \cdots & 0 & 0 \\ 0 & 1 & e & \cdots & 0 & 0 \\ \cdots\cdots & & & & & \\ 0 & 0 & 0 & \cdots & 1 & e \end{pmatrix} \tag{9}$$

则任意整数e与正整数t，当$t < m$时

$$\mathbb{U}^m = \begin{pmatrix} e^t & 0 & 0 & \cdots & 0 & 0 \\ C_t^1 e^{t-1} & e^t & 0 & \cdots & 0 & 0 \\ \cdots\cdots & & & & & \\ C_t^{t-1} e & C_t^{t-2} e^2 & C_t^{t-3} e^3 & \cdots & 0 & 0 \\ 1 & C_t^{t-1} e & C_t^{t-2} e^2 & \cdots & 0 & 0 \\ \cdots\cdots & & & & & \\ 0 & 0 & 0 & \cdots & C_t^1 e^{t-1} & e^t \end{pmatrix} \tag{10}$$

(10)式的第$t+1 \leqslant m$条下斜对角线值全为1.

当$t \geqslant m$时下式成立

$$\mathbb{U}^m = \begin{pmatrix} e^t & 0 & 0 & \cdots & 0 & 0 \\ C_t^1 e^{t-1} & e^t & 0 & \cdots & 0 & 0 \\ C_t^2 e^{t-2} & C_t^1 e^{t-1} & e^t & \cdots & 0 & 0 \\ \cdots\cdots & & & & & \\ C_t^{m-1} e^{t-m+1} & C_t^{m-2} e^{t-m+2} & C_t^{m-3} e^{t-m+3} & \cdots & C_t^1 e^{t-1} & e^t \end{pmatrix} \tag{11}$$

证明　把 U 写成 $eI+J$，J 为 m 阶若当矩阵，$U^t=(eI+J)^t=e^tI+C_t^1e^{t-1}J\cdots+C_t^{t-1}eJ+J^t$，当 $t<m$ 时一一代入(10)式成立。利用若当矩阵幂的性质有 $t\geqslant m$ 时 $J^t=O$，这时 $U^t=(eI+J)^t=e^tI+C_t^1e^{t-1}J\cdots+C_t^{m-1}e^{t-m-1}J^{m-1}$，一一代入(11)式得证。

命题4　如(7)式在 $\mathbb{Z}_p$ 中有 m 个模 p 同余的重根 e，即 $f(\lambda)\equiv(\lambda-e)^m$，且 $(A-eI)^{m-1}\not\equiv O$，则存在模 p 可逆矩阵 V 及形如(9)式矩阵 U 使下式成立

$$A\equiv VUV^{-1}$$

证明　$(A-eI)^{m-1}\not\equiv O$，由推论2(ii)，$\exists v_1\not\equiv\theta$，使 $(A-eI)^{m-1}v_1\not\equiv\theta$，故 k，$1\leqslant k\leqslant m-2$，$(A-eI)^kv_1\not\equiv\theta$，否则矛盾。令 $v_{j+1}=(A-eI)v_j$，$j=1,2,\cdots,m-1$，$v_{j+1}=(A-eI)^jv_1\not\equiv\theta$，故 $Av_j=ev_j+v_{j+1}$，$j=1,2,\cdots,m-1$；由凯莱定理 $f(A)=O\equiv(eI-A)^m\equiv(-1)^m(A-eI)^m$，$(A-eI)v_m=(A-eI)^mv_1\equiv\theta$，写成矩阵等式 $A(v_1,v_2,\cdots,v_m)=(v_1,v_2,\cdots,v_m)U$，$U$ 如(9)式所定义。

类似定理1证明易证 $v_1,v_2,\cdots,v_m$ 模 p 线性无关。由推论2(iii)，合并 $V=(v_1,v_2,\cdots,v_m)$，则 V 模 p 可逆，故 $AV\equiv VU$，$A\equiv VUV^{-1}$。

定理4　如(7)式在 $\mathbb{Z}_p$ 中有 m 个模 p 同余的重根 e，即 $f(\lambda)\equiv(\lambda-e)^m$，且 $(A-eI)^{m-1}\not\equiv O$，设 L 满足 $p^{L-1}<m\leqslant p^L$，则

$$T(A,p)=\mathrm{ord}_p(e)\times\min\{p^j;A\hat{}(p^j\,\mathrm{ord}_p(e))\equiv I,\ 1\leqslant j\leqslant L\}\quad(12)$$

特别是 $m\leqslant p$ 时 $T(A,p)=\mathrm{ord}_p(e)\times p$。

证明　由命题4(11)式成立，令 $t=T(A,p)$，则 $A^t\equiv(VUV^{-1})^t\equiv VU^tV^{-1}\equiv I$，$U^t\equiv I$，由命题3当 $t<m$ 时 U^t 非对角线位置有非0元，只能 $t\geqslant m$，U^t 形式如(11)所示。$U^t\equiv I$，$e\not\equiv 0$ 故 $e^t\equiv 1\pmod p$，$C_t^{t-i}e^i\equiv 0\pmod p$，$\therefore C_t^{t-i}\equiv 0\pmod p$ 对 $i=1,2,\ldots,m-1$ 均成立，只能 $p\mid t$，又 $\mathrm{ord}_p(e)\mid t$，$\gcd(p,\mathrm{ord}_p(e))=1$，

所以，$p\times\mathrm{ord}_p(e)\mid T(A,p)$。

另由引理3，$(\lambda-e)\mid(\lambda\hat{}\,\mathrm{ord}_p(e)-1)$，当 p 为奇素数或2均有 $(\lambda-e)^p\mid\lambda\hat{}(p\mathrm{ord}_p(e))-1$，反复作 L 次有 $(\lambda-e)\hat{}(p^L)\mid\lambda\hat{}(p^L\mathrm{ord}_p(e))-1$，存在 $g(\lambda)$ 使 $\lambda\hat{}(p^L\mathrm{ord}_p(e))-1\equiv g(\lambda)(\lambda-e)\hat{}(p^L)\equiv g_1(\lambda)(x-e)^m\equiv g_1(\lambda)f(\lambda)$，由 $f(A)=O$，所以，$A\hat{}(p^L\mathrm{ord}_p(e))-I\equiv g_1(A)f(A)\equiv O$，$A\hat{}(p^L\mathrm{ord}_p(e))\equiv I$，由周期的最小性，$T(A,p)\mid p^L\mathrm{ord}_p(e)$，结合前已证的 $p\times\mathrm{ord}_p(e)\mid T(A,p)$，$T(A,p)$ 只能取(12)的形式。当 $m\leqslant p$ 时 $L=1$，$T(A,p)=\mathrm{ord}_p(e)\times p$。

定理5　如(7)式在 $\mathbb{Z}_p$ 中有 m 个根 $\lambda_1,\lambda_2,\cdots\lambda_m$，$\lambda_1,\lambda_2,\cdots\lambda_k$ 彼此模 p 同余，$k>1$，$\lambda_k,\lambda_{k+1},\cdots\lambda_m$ 彼此模 p 不同余，$(A-\lambda_1I)^{k-1}\not\equiv O$，设 L 满足 $p^{L-1}<k\leqslant p^L$，则

$$T(A,p)=l\times\min\{p^j;A\hat{}(p^jl)\equiv I,\ 1\leqslant j\leqslant L\}\quad(13)$$

其中 $l=\mathrm{lcm}(\mathrm{ord}_p(\lambda_k),\mathrm{ord}_p(\lambda_{k+1}),\cdots,\mathrm{ord}_p(\lambda_m))$ 特别是 $k\leqslant p$ 时 $T(A,p)=l\times p$。

定理6　如(7)式在 $\mathbb{Z}_p$ 中有 m 个根其中含有模 p 同余的重根，任意一个重根 λ_i，记重数为 K_i，满足 $(A-\lambda_iI)\hat{}K_i\not\equiv O$，设最大的重数为 k，L 满足 $p^{L-1}<k\leqslant p^L$，m 个根中彼此模 p 不同余的设为 $\lambda_1,\lambda_2,\cdots\lambda_t$，$l=\mathrm{lcm}(\mathrm{ord}_p(\lambda_1),\mathrm{ord}_p(\lambda_2),\cdots,\mathrm{ord}_p(\lambda_t))$，则

$$T(A,p)=l\times\min\{p^j;A\hat{}(p^jl)\equiv I,\ 1\leqslant j\leqslant L\}\quad(14)$$

特别是 $k\leqslant p$ 时 $T(A,p)=l\times p$。而变换(2)的周期 $T(A,p^r)=l\times\min\{p^{y+j}\mid 0\leqslant y\leqslant r-1,\ 1\leqslant j\leqslant L,\ A\hat{}(p^{y+j}l)\equiv I_m(\mathrm{mod}\,p^r)\}$，

计算机程序只需作 r 个循环便可确定 $T(A,p^r)$ 之值。

定理5、定理6证明与定理4类似，略。

故对广泛一类随机整数矩阵 A，当(7)式在 $\mathbb{Z}_p$ 中有与没有重根时，其精确周期分别由定理6与定理3给出。类似于文[2]中时间复杂性证明有：

定理7　设 $N=p^r$ 为素数幂，对广泛一类高维随机矩阵 $A\in(\mathbb{Z}_p)_{m\times m}$，$\gcd(|A|,p)=1$，$A$ 使 m 次同余方程(7)在 $\mathbb{Z}_p$ 存在 m 个解，则存在快速算法，只需 $O((\log_2N)^2)$ 次模 N 乘法，便可得到精确周期 $T(A,N)$。

3　数值例子及应用范例

例1　$m=5$，$p=59$，$r=1$，$N=p$，

$$A=\begin{pmatrix}16&0&0&0&0\\32&16&0&0&0\\24&32&16&0&0\\8&24&32&16&0\\1&8&24&32&16\end{pmatrix}$$

(7)式在 $\mathbb{Z}_p$ 有模 p 的 m 重根 $e=2$，$\mathrm{ord}_p(e)=58$，$p>m$，$l=T(A,p)=\mathrm{ord}_p(e)\times p=3\,422$，验算知 $T(A,59)=3\,422$ 正确.

$r=2$，$N=p^2$，$\min\{(p\hat{}y)\ l\mid 0\leqslant y\leqslant r-1,\ y$

$\in \mathbb{Z}$; $A^{\wedge}(Ql) \equiv I_m(\bmod N)$, $l = T(A, p)$, $Q = (p^{\wedge} y)\} = 201\,898$, 验算知 $T(A, 59^2) = 201\,898$ 正确。

$r = 3$, $N = p^3$, $\min\{(p^{\wedge}y)\ l \mid 0 \leqslant y \leqslant r-1$, $y \in \mathbb{Z}$; $A^{\wedge}(Ql) \equiv I_m(\bmod N)$, $l = T(A, p)$, $Q = (p^{\wedge} y)\} = 11\,911\,982$, 验算知 $T(A, 59^3) = 11\,911\,982$ 正确。

数字多媒体的信息加密及信息隐藏，是当前信息安全领域的研究热点之一，本文结果可构造基于任意 n 维随机置乱技术的密码体制与信息隐藏体制，可有更大的密钥空间、更广的适用面，其思想方法可见于文 [8-11]，下列出应用范例。

例2 数字图像的加密解密（见下图 1-3）。明文图像经过 10 轮 4 维随机矩阵置乱得到密文图像，解密后得到译文图像同明文图像完全一致。

图1 明文图像
Fig. 1 Plain image

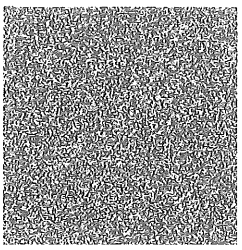

图2 密文图像
Fig. 2 Cipher image

图3 译文图像
Fig. 3 Decryption image

5 结 语

本文给出广泛一类高维随机矩阵置乱变换的周期精确表达式，数学结论与仿真实验相吻合，其结果对于数字多媒体的安全高效加密、信息隐藏，有重要的理论价值和应用价值。进一步工作是开拓其他领域的应用研究。

参考文献：

[1] 齐东旭，邹建成，韩效宥. 一类新的置乱变换及其在图像信息隐蔽中的应用[J]. 中国科学：E 辑，2000，30(5)：440-447.

[2] 王泽辉. 二维随机矩阵置乱变换的周期及在图像信息隐藏中的应用[J]. 计算机学报，2006，29(12)：2218-2225.

[3] 王泽辉，张治国. 语义安全的数字多媒体密码体制[J]. 通信学报. 2008，29(3)：87-92.

[4] 洪春勇，邹玮刚. 基于三维 Arnold 变换的数字图像置乱技术及其周期性[J]. 南昌大学学报：理科版，2005，29(6)：619-621.

[5] 赵慧. n 维 Arnold 变换及其周期性[J]. 北方工业大学学报. 2002，14(1)：21-25.

[6] 王泽辉. 三维随机矩阵置乱变换的周期及其应用[J]. 中山大学学报：自然科学版，2008，47(2)：21-25.

[7] 潘承洞，潘承彪. 初等数论[M]. 2 版. 北京：北京大学出版社，2003.

[8] LI S, LI C, LO K T, et al. Cryptanalysis of an image encryption scheme[J]. Journal of Electronic Imaging, 2006, 15(4): 043012, 1-13.

[9] GAO H J, ZHANG Y S, L IANG S Y, et al. A new chaotic algorithm for image encryption[J]. Chaos, Solutions and Fractals, 2006, 29(2): 393-399.

[10] 熊昌镇，邹建成，齐东旭. 一种基于混沌映射的数字图像加密新算法[J]. 中山大学学报：自然科学版，2004，43(S2)：29-33.

[11] 顾国生，战荫伟，侯文邦. 图像 Contourlet 域快速置乱算法[J]. 计算机工程与应用，2010，46(4)：15-21.