三维随机矩阵置乱变换的周期及其应用*

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： 为了适合数字多媒体特性，实施多媒体加密与信息隐藏，生成充分大的密钥空间，使用了数论、近世代数、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。给出三维随机整数矩阵 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，构造了求周期的快速算法，仅耗费 $O(\log_2 N)^2$ 次模 N 乘法便可得到 $T(A, N)$。大量的算例和应用范例与理论结果相吻合。结论可用于建立数字多媒体的新型密码体制，实施高效率的加密。

关键词： 数字多媒体；随机矩阵置乱变换；周期性；多项式时间复杂性；安全性
中图分类号： TN918 **文献标识码：** A **文章编号：** 0529-6579（2008）01-0021-05

矩阵置乱变换是实施数字图像加密和信息隐藏的一种高效技术，与其他适用技术如混沌技术有本质不同[1]，其研究经历了两个阶段，第一阶段是以 Arnold 变换为代表的规则矩阵置乱变换技术，由于未解决精确周期特别是缺乏快速算法，技术主要用于数字水印的预处理[2]。第二阶段是随机矩阵置乱变换技术，由文[3]首次提出，整数矩阵元素可以充分随机、模数 N 维数 k 可以任意，并给出求精确周期快速算法的一般框架，针对2维随机矩阵置乱变换给出变换周期 $T(A,N)$ 的精确表达式及上界估计，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 $T(A, N)$，证明算法的时间复杂度仅 $O((\log 2N)^2)$，属于多项式时间算法。文[4]在文[3]基础上建立抗选择明文攻击的数字图像密码体制，故此随机矩阵置乱可独立发挥作用，并可推广用于其他多媒体。为增加密码体制的密钥空间，探讨随机置乱变换技术在更广泛领域的应用，本文将求出3维随机整数矩阵 A 决定的置乱变换在任意模 N 下的精确周期 $T(A,N)$，并构造快速算法。

1 基本引理

下文中 $\mathbb{Z},\mathbb{Z}^+$ 分别为整数集与自然数集，gcd、lcm 分别为最大公约数与最小公倍数记号，整数 $N \in \mathbb{Z}^+ = \{0,1,\cdots,N-1\}$，mod N 表示标量及矩阵运算结果在 $\mathbb{Z}_N$ 取值. ^表示幂运算，$a\hat{}b = a^b$，ord$q(b)$ 表示 b 模 q 之阶，即满足 $b^l \equiv 1(\mathrm{mod}_q)$ 之最小正整数。$\det(A)$ 为矩阵 A 的行列式，I_m 为 m 维单位矩阵。

定义1 定义 m 维随机整数矩阵 A 在任意模 N 下的置乱变换如下

$$x' \equiv AX(\mathrm{mod}N) \tag{1}$$

其中 $A \in Z_N^{m\times m}, X, X' \in Z_N^m$；变换（1）的周期 $T(A, N)$ 即是使（2）成立的最小正整数。

$$A^t \equiv I_m(\mathrm{mod}N) \tag{2}$$

在不引起混淆时 $T(A,N)$ 简记为 $T(N)$。设 p 为 N 的任一素数因子，$F_p = \mathbb{Z}/(p) = \{0,1,\cdots p-1\}$ 表示元素个数为 p 的有限域，$F_p[x]$ 为系数在 F_p 的多项式环。$\forall f(x) \in F_p[x] \subset \mathbb{Z}[x]$，由于运算或因式分解，$f(x)$ 系数可能表现为整数，相当于 $f(x) \in \mathbb{Z}[x]$.

定义2 （1）$f_1(x), f_2(x) \in \mathbb{Z}[x]$，设 $f_1(x) = x^k + b_1x^{k-1} + \cdots + b_k$，$f_2(x) = x_k + c_1x^{k-1} + \cdots + c_k$，如 $b_i \equiv c_i(\mathrm{mod}\ p)$，$i = 1, 2, \cdots, k$，则记 $f_1(x) \equiv f_2(x)(\mathrm{mod}\ p)$，简记为 $f_1(x) \equiv f_2(x)$，并称“在 $F_p[x]$ 中 $f_1(x) = f_2(x)$”。

（2）对 $h(x), f(x) \in F_p[x]$ 如存在 $g(x) \in F_p[x]$ 使 $h_1(x) \equiv g(x)f(x)$ 成立，则称“在 $F_p[x]$ 中 $f(x)$ 整除 $h(x)$”，简记为 $f(x)|h(x)$。

下列引理1-5由文[3]直接得到：

引理1 变换（1）存在周期 $T(A,N)$ 当且仅当

$$\gcd(\det(A), N) = 1 \tag{3}$$

引理2 设 N 有标准因子分解式

$$N = (p_1)\hat{}(r_1)(p_2)\hat{}(r_2)\cdots(p_s)\hat{}(r_s) \tag{4}$$

* **收稿日期：** 2007-05-22
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

其中 p_1，p_2，…，p_s 为互不相同的素数，r_1，r_2，…，r_s 为自然数，$\gcd(\det(A),N)=1$，则变换（1）的周期

$$T(A,N)=\min\{(p_1\hat{}y_1)(p_2\hat{}y_2)\cdots(p_s\hat{}y_s)l \mid 0\leqslant y_i\leqslant r_{i-1},\ y_i\in\mathbf{Z},i=1,\cdots,s;\ A\hat{}(Ql)\equiv I_m(\mathrm{mod}\ N),\ l=1\mathrm{cm}(T(p_1),\cdots,T(p_s),\ Q=(p_1\hat{}y_1)(p_2\hat{}y_2)\cdots(p_s\hat{}y_s)\} \tag{5}$$

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

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

引理4 对于2维矩阵 A，存在求 $A^L(\mathrm{mod}\ N)$ 的快速算法，至多只需 $2\times2^3\times\lfloor\log_2L\rfloor$ 次模 N 乘法。

引理5 对于2维矩阵 A，设 n 代表模数 N 或任一奇素数，正整数 f 有标准分解

$$f=(q_1)\hat{}(v_1)(q_2)\hat{}(v_2)\cdots(q_w)\hat{}(v_w)$$

其中 q_1，q_2，…，q_w 为互不相同的素数，v_1，v_2，…，v_w 为自然数。

（i）如果 f 有上界估计：$f\leqq F_1$，则求 $h_1=\min\{d:A^d\equiv I(\mathrm{mod}\ n),\ d\mid f\}$ 相当于求

$$h_1=\min\{(q_1\hat{}y_1)(q_2\hat{}y_2)\cdots(q_w\hat{}y_w)\mid A\hat{}Q\equiv I(\mathrm{mod}\ n),Q=(q_1\hat{}y_1)(q_2\hat{}y_2)\cdots(q_w\hat{}y_w)\ 0\leqslant y_i\leqslant v_i,\ i=1,\cdots w\}$$

只需不超过 $4\times2^3\times\log_2F_1\times\lfloor\log_2n\rfloor$ 次模 n 乘法，便得 h_1。

（ii）如存在正整数 l 使 f 有上界估计：$fl\leqq F_2$，则求

$$h_2=\min\{(q_1\hat{}y_1)\cdots(q_w\hat{}y_w)l\mid A\hat{}(Ql)\equiv I(\mathrm{mod}\ n),\ Q=(q_1y_1)\cdots(q_1\hat{}y_1)\cdots(q_w\hat{}y_w),0\leqslant y_i\leqslant v_i-1,\ i=1,\cdots w\}$$

只需不超过 $2\times2^3\times\log_2F_2\times\lfloor\log_2n\rfloor$ 次模 n 乘法。

考虑3次同余方程式

$$f(x)=x^3+b_1x^2+b_2x+b_3\equiv0(\mathrm{mod}\ p) \tag{7}$$

假定 $b_3\not\equiv0(\mathrm{mod}\ p)$ 及 p 为奇素数。文[5]研究了式（7）解的分布、$f(x)$ 在 $F_p[x]$ 中分解，及当式（7）在 F_p 有唯一解时如何求唯一解，文[6]研究了当式（7）在 F_p 有解时如何求出全部 F_p 中之解，[5，6]与本文相关的主要结论是引理6-8：

引理6 方程式（7）的解及 $f(x)$ 在 $F_p[x]$ 中的因式分解能且只能下列4种情况：

（i）（7）在 F_p 中有3个不同余的解，$f(x)$ 在 $F_p[x]$ 可分解为1次多项式的乘积且无重因式。

（ii）（7）在 F_p 中有3个解且至少有两个同余，$f(x)$ 在 $F_p[x]$ 可分解为1次多项式的乘积且有重因式。

（iii）（7）在 F_p 中有唯一解，$f(x)$ 在 $F_p[x]$ 可分解为1次多项式与一个2次不可约多项式 $g_2(x)$ 的乘积且无重因式。

（iv）（7）在 F_p 中没有解，$f(x)$ 是 $F_p[x]$ 中的3次不可约多项式。

引理7 存在快速算法，可以在 $O((\log_2\{p\})^3)$ 比特时间内，判断任意3次同余方程（7）解的结构，即对（7）与 $f(x)$ 发生了引理6中（i）-（iv）四种情况的哪一种；存在快速算法可以在情况（iii）发生时，耗费 $O((\log_2\{p\})^3)$ 比特时间求出（7）在 F_p 中的唯一解。

引理8 存在快速算法，当情况（i）、（ii）、（iii）发生时，耗费 $O((\log_2\{p\})^3)$ 比特可求出式（7）在 F_p 中的全部解。

当 p 非奇素数即 $p=2$ 时，$f(x)$ 在 $F_2[x]$ 有更简单的内部结构，下节再讨论。将引理4的矩阵 A 扩展到一般 m 维矩阵，参考文[3]中对引理4、引理5的证明，可得

推论1 对于 m 维矩阵 A，存在求 $A^L(\mathrm{mod}\ N)$ 的快速算法，至多只需 $2\times m^3\times\lfloor\log_2L\rfloor$ 次模 N 乘法。

推论2 对于 m 维矩阵 A，设 n 代表模数 N 或任一奇素数 p，正整数 f 有标准分解

$$f=(q_1)\hat{}(v_1)(q_2)\hat{}(v_2)\cdots(q_w)\hat{}(v_w)$$

其中 q_1，q_2，…，q_w 为互不相同的素数，v_1，v_2，…，v_w 为自然数。

（i）如果 f 有上界估计：$f\leqq F_1$，则存在快速算法求 $h_1=\min\{d:A^d\equiv I(\mathrm{mod}\ n),\ d\mid f\}$ 只需不超过 $4\times m^3\times\log_2F_1\times\lfloor\log_2n\rfloor$ 次模 n 乘法。

（ii）如存在正整数 l 使 f 有上界估计：$fl\leqq F_2$，则求

$$h_2=\min\{(q_1\hat{}y_1)\cdots(q_w\hat{}y_w)\ l\mid A\hat{}(Ql)\equiv I(\mathrm{mod}\ n),\ Q=(q_1\hat{}y_1)\cdots(q_w\hat{}y_w),\ 0\leqslant y_i\leqslant v_i-1,\ i=1,\cdots w\}$$

只需不超过 $2\times m^3\times\log_2F_2\times\lfloor\log_2n\rfloor$ 次模 n 乘法。

2 三维随机置乱变换的周期

以下均假定 $m=3$ 且式（3）成立即 $\gcd(\det(A),N)=1$，N 有标准分解式（4），p 为 N 的任一素因子，令

$$f_3(x)=\det(xI_3-A)=x_3+c_1x^2+c_2x+c_3,$$

则 $f_3(0)=c_3=-\det(A)$，式（3）成立等价于任意 p 满足 $\gcd(c_3,p)=1$。考虑下列同余方程之解：

$$f_3(x) \equiv 0(\bmod p) \tag{8}$$

式（3）成立等价于式（8）在 F_p 中无零解。

下先设 $p>2$ 为奇素数。将引理 6 的情况（ii）再细分为 3 个解均同余及仅两个同余，易知上述判定与求解的快速算法时间复杂性不变。

命题 1　对任意素数 p，如果 $g_k(x)=x^k+e_1x^{k-1}+\cdots+e_k$ 是 $F_p[x]$ 中的不可约多项式，记 $v_0=(-1)^k e_k, v=(p^k-1)/(p-1)\times \mathrm{ord}_p(v_0)$，则存在 $h_k(x)\in F_p[x]$ 使得 $g_k(x)\mid(x^v-1)$

$$x^v-1\equiv h_k(x)g_k(x)(\bmod p) \tag{9}$$

证明　利用文[7]中代数扩域性质及韦达定理可证（9）成立。

定理 1　对任意奇素数 p，$f_3(x)$ 在 $F_p[x]$ 的标准因式分解只有（i）-（v）五种情况，可耗费 $O((\log_2\{p\})^3)$ 比特时间加以判定，对应 $T(p)$ 如下：

（i）$f_3(x)\equiv(x-x_1)(x-x_2)(x-x_3)(\bmod p)$，其中 x_1, x_2, x_3 模 p 互不同余，则

$$T(p)=\min\{d;A^d\equiv I(\bmod p), d\mid \mathrm{lcm}(\mathrm{ord}_p(x_1),\mathrm{ord}_p(x_2),\mathrm{ord}_p(x_3))\}. \tag{10}$$

（ii）$f_3(x)\equiv(x-x_1)^2(x-x_2)(\bmod p)$，其中 x_1, x_2 模 p 互不同余，则

$$T(p)=\min\{d;A^d\equiv I(\bmod p), d\mid \mathrm{lcm}(p\times \mathrm{ord}p(x_1), \mathrm{ord}p(x_2))\}. \tag{11}$$

（iii）$f_3(x)\equiv(x-x_1)^3(\bmod p)$，则

$$T(p)=\min\{d;A^d\equiv I(\bmod p), d\mid p\times \mathrm{ord}_p(x_1)\}. \tag{12}$$

（iv）$f_3(x)\equiv(x-x_1)g_2(x)$，其中 $g_2(x)$ 为 $F_p[x]$ 上的 2 次不可约多项式，则

$$T(p)=\min\{d;A^d\equiv I(\bmod p), d\mid (p+1)\times \mathrm{ord}_p(\det(A)\times(x_1)^{-1})\}. \tag{13}$$

（v）$f_3(x)\equiv g_3(x)$，其中 $g_3(x)$ 为 $F_p[x]$ 上的 3 次不可约多项式，则

$$T(p)=\min\{d;A^d\equiv I(\bmod p), d\mid (1+p+p^2)\times \mathrm{ord}_p(\det(A))\}. \tag{14}$$

证明　代入验证易知

$$f_3(A)\equiv O(\bmod p). \tag{15}$$

（i）由引理 3，令 $d_i=\mathrm{ord}_p(x_1)$，存在 $h_i(x)\in F_p[x]$ 使 $x\hat{}d_i-1\equiv h_i(x)(x-x_1)$，$\therefore (x-x_i)\mid(x^d-1)$，$i=1, 2, 3$. $(x-x_1)(x-x_2)(x-x_3)\mid(x_d-1)$，$d=1\mathrm{cm}(d_1, d_2, d_3)$。即存在 $h_4(x)\in F_p[x]$，使 $(x^d-1)=h_4(x)f(x)$，由式（15）知

$$A^d-I=h_4(A)f(A)\equiv O,\therefore A^d\equiv I,\mathrm{T}(p)\mid d,$$

由周期定义，式（10）成立。

（ii）利用二项式展开及奇素数性质，类似于（i）可证，同理可证明（iii）。

（iv）易知 $g_2(x)\equiv x^2+c_4x+\det(A)\times(x_1)^{-1}$，由命题 1，对 $k=2$，$v=(p+1)ord_p(\det(A)\times(x_1)^{-1})$，$g_2(x)\mid(x^v-1)$，$g_2(x)\mid(x^d-1)$，$d=1\mathrm{cm}(v, d_1)$. 由引理 3，$(x-x_1)\mid(x^d-1)$，类似有 $(x-x_1)g_2(x)\mid(x_d-1)$，$A^d\equiv I$，$T(p)\mid d$，式（13）成立.

（v）直接应用命题 1 类似上面证明得式（14）。

推论 3　对任意奇素数 p 存在 $T'(p)$ 使 $T(p)\mid T'(p)$，$T(p)\leqq T'(p)\leqq p^3$，$2\mid T'(p)$。

类似于文[3]，其证明主要利用定理 1、素数及 1cm 性质，略。

当 $p=2$ 时，函数有更简洁表示，容易得到：

定理 2　当 $p=2$ 且 $\gcd(\det(A), 2)=1$ 时，$f_3(x)$ 在 $F_p[x]$ 的标准因式分解只有（ⅰ）-（ⅲ）三种情况，只须用 $O(1)$ 时间加以判定，对应 $T(p)$ 如下：

（ⅰ）$f_3(x)\equiv(x-1)^3(\bmod 2)$，则 $T(p)\in\{1, 2, 4\}$。

（ⅱ）$f_3(x)\equiv(x-1)(x^2+x+1)(\bmod 2)$，则 $T(p)=3$。

（ⅲ）$f_3(x)$ 是 $F_2[x]$ 上 3 次不可约多项式，则 $T(p)=7$。

推论 4　当 $p=2$ 且 $\gcd(\det(A), 2)=1$ 时，求变换（1）的周期 $T(A, p)$ 仅需 $O(1)$ 时间，对应于定理 2 的（ⅰ）、（ⅱ）、（ⅲ），分别存在 $T'(p)=4,3,7$ 使 $T(p)\mid T'(p), T(p)\leqq T'(p)\leqq p^3$。

3　求精确周期快速算法及其时间复杂性分析

定理 1、定理 2 与引理 2 构成了对 3 维随机置乱变换一般周期 $T(A, N)$ 的精确表达式。

故可以构造确定型算法 T_{3D}，先求出 $T(p_1)$，…，$T(p_s)$，再利用式（5）借助一个循环语句，至多作有限 $r_1+r_2+\cdots+r_s$ 次判断（每次需作 1 次矩阵幂快速运算），便可得到周期 $T(A, N)$。

定理 3　对于所有形如式（1）的变换（$m=3$），当条件式（3）成立时其周期有如下估计

$$T(A,N)\leqslant N^3 \tag{16}$$

证明　由定理 1 及式（5），$l=1\mathrm{cm}(T(p_1),\cdots, T(p_s),$

$$T(A,N)\leqslant(P_1\hat{}(r_1-1))(p_2(r_2-1))\cdots(p_s\hat{}$$

$(r_s-1))\times l$，由式（4），$T(A,N)\leqslant N/(p_1p_2\cdots p_s)l$，再由推论3与4，$l\leqslant T(p_1)T(p_2)\cdots T(p_s)\leqslant p_1^3p_2^3\cdots p_s^3$

$$T(A,N)\leqslant N/(p_1p_2)\cdots T(p_s)\times p_1^3p_2^3\cdots p_s^3$$
$$=Np_1^2p_2^2\cdots p_2^2\cdots p_s^2\leqslant N^3$$

推论5 对任意奇素数p，存在快速算法求$T(p)$至多要作$324\times\log_2p\times\lfloor\log_2p\rfloor$次模$p$乘法。

证明 由定理1，求$T(p)$均需作运算求

$h_1=\min\{d:\ A^d\equiv I\ (\mathrm{mod}n),\ d\mid f\}$，由推论3均有$f\leqslant p^3$，将$m=3$代入推论2（i），知存在快速算法求$T(p)$至多要作$3\times4\times3^3\times\log_2p\times\lfloor\log_2p\rfloor=324\times\log_2p\times\lfloor\log_2p_i\rfloor$次模$p$乘法。

定理4 对于形如式（1）的3维随机矩阵A在任意模数N下的置乱变换，存在一个确定的算法T_{3D}，只需$486\lceil\log_2p_N\rceil^2$次模$N$乘法便可确定变换（1）的精确周期$T(A,N)$.

证明 由推论5，对所有的$i=1,2,\cdots,s$，求$T(p_i)$至多要作$324\times\log_2p_i\times\lfloor\log_2p_i\rfloor$次模$p_i$乘法（$p_i=2$仅$O(1)$时间），不超过$324\times\log_2p_i\times[\log_2N]$次模$N$乘法，全部$s$个共需要的模$N$乘法次数不高于$324(\log_2p_i+\cdots+\log_2p_s)\lfloor\log_2p_N\rfloor\leqslant324\log_2N[\log_2N]\leqslant324\lceil\log_2p_N\rceil^2$，便可得到$l=\mathrm{lcm}(T(p_1),T(p_2),\cdots T(p_s))$，由定理3及推论2之（ii），令$F_2=N^3$，$m=3$代入，求（5）的$T(A,N)$需要的模$N$乘法次数不超过$2\times3^3\times\log_2N^3\times[\log_2N]\leqslant162\lceil\log_2p_N\rceil^2$，$324+162=486$，故精确求$T(A,N)$只需不超过$486\lceil\log_2p_N\rceil^2$次模$N$乘法。

4 算例及应用范例

例子1 随机选择$a_{11}=23$，$a_{12}=76$，$a_{13}=42$，$a_{21}=55$，$a_{22}=39$，$a_{23}=81$，$a_{31}=17$，$a_{32}=37$，$a_{33}=27$，$\det(A)=4704\neq1$. 调用算法T_{3D}求得：$T(13^3)=371124$；$T(13^4)=4824612$；$T(13^5)=62719956$；$T(19^3)=412623$；$T(19^4)=7839834$；$T(19^5)=148956903$；$T(23^3)=11638$；$T(23^4)=267674$；$T(23^5)=6156502$；$T(29^3)=353220$；$T(29^4)=10243380$；$T(29^5)=297058020$；均验证了定理1。

数字多媒体的加密以及信息隐藏，是当前信息安全领域的研究热点之一，国内外不断出现新的成果[8-11]，随机矩阵置乱变换技术由于兼顾了安全性和高效性，在该领域有广泛应用前景，其思想方法可见于文献[3-4]，而3维随机矩阵置乱的密钥空间比2维随机置乱更多，适用面更广，限于篇幅，仅列出一些应用范例。

例子2 数字图像的加密解密（见图1-3）。明文图像经过10轮三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。

例子3 数字音频的加密解密。将录得的石块掉进铁滚筒声音为明文音频，8轮三维随机矩阵置乱得到密文音频，解密后得到译文音频同明文音频完全一致（图4-6）。

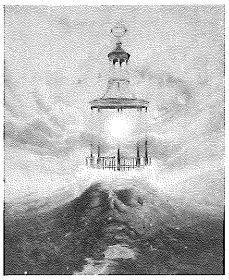

图1 明文图像
Fig.1 Plain Image

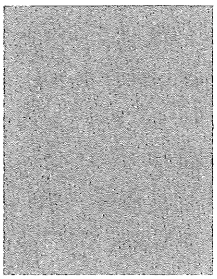

图2 密文图像
Fig.2 Cipher Image

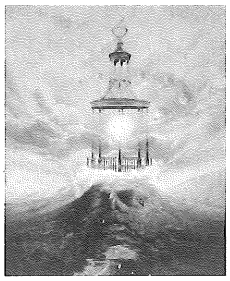

图3 译文图像
Fig.3 Decryption Image

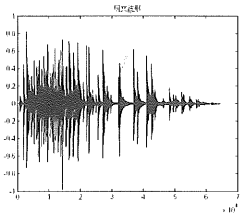

图4 明文波形
Fig.4 Plain Wave-form

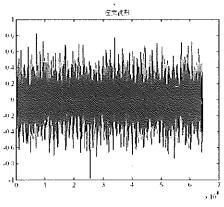

图5 密文波形
Fig.5 Cipher Wave-form

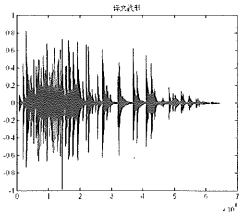

图6 译文波形
Fig.6 Decryption Wave-form

结语 利用快速算法T_{3D}可求出3维随机置乱变换的精确周期，构造数字多媒体密码体制比2维置乱变换可以有更大的密钥空间，有更高的安全性，在多媒体信息网络远程保密传输和信息隐藏，有重大的实用价值。

参考文献：

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

[2] 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.
QI Dongxu, ZOU Jiancheng, HANG Xiaoyou. A new scrambling transformation and its applications in image information hiding[J]. Science in China(Series E),2000, 30(5):440 - 447.

[3] 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.
WANG Zehui. On the period of 2 - D random matrix mcrambling transformation and its applications in image information hiding[J]. Chinese Journal of Computers, 2006,29(12):2218 - 2225.

[4] 王泽辉. 抗选择明文攻击的数字图像密码体制[J]. 哈尔滨工业大学学报, 2006,38(Sup):715 - 719.
WANG Zehui. A against chosen plaintext attack cryptosystem in digital images[J]. Journal of Haerbin Institute of Technology. 2006,38(Sup): 715 - 719.

[5] 王泽辉,方小洵. 增加多媒体隐藏信息量的高效算法[J]. 哈尔滨工业大学学报,2006,38(Sup):710 - 714.
WANG Zehui, FANG Xiaoxun. An efficient algorithm for increasing the amount of hidden information in multimedia [J]. Journal of Haerbin Institute of Technology. 2006,38 (Sup):710 - 714.

[6] 王泽辉. 基于 3 次同余方程的概率公钥密码体制[J]. 通信学报,2006,27(12A):61 - 65.
WANG Zehui, FANG Xiaoxun. Probabilistic public key cryptosystems based on congruence of 3rd degree[J]. Journal of Communications. 2006,27(12A):61 - 65.

[7] 胡冠章. 应用近世代数(M). 北京:清华大学出版社, 1999.

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

[9] CHEN L, ZHAO D. Reply to comment on optical image encryption with hartley trans forms[J]. Opt Lett,2007, 32:767 - 768. http://www. opticsinfobase. org/abstract. cfm? URI = ol - 32 - 7 - 767

[10] 林代茂,胡岚,郭云彪,等. 广义信息隐藏技术的安全问题[J]. 中山大学学报:自然科学版,2004,43(s2): 14 - 16.
LIN Daimao , HU Lan , GUO Yunbiao , et al. The security of genera - lized information hiding[J]. Acta Scientiarum Naturalium Universitatis Sunyatseni. 2004, 43(s2):14 - 16.

[11] 张卫明,刘九芬,李世取. LSB 隐写术的密钥恢复方法[J]. 中山大学学报:自然科学版,2005,44(3):29 - 33.
ZHANG Weiming ,LIU Jiufen1 ,LI Shiqu1. Approaches for recovering key of LSB steganography[J]. Acta Scientiarum Naturalium Universitatis Sunyatseni. 2005, 44 (3):29 - 33.

The Period of 3 - D Random Matrix Scrambling Transformation and Its Applications

WANG Ze-hui

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

Abstract: For implementing the encryption/decryption and information hiding for digital multimedia, and aiming to generate enough large cipher key space, the accurate period of high dimension random matrix scrambling transformation is studied with the help of number theory and algebraic theory. An accurate expression and an upper bound estimation for the period T (A, N) of a 3 - D random integer matrix scrambling transformation under any modular N is presented. The efficient algorithm for computing the period is constructed. It is proved that the algorithm needs only $O(\log_2 N)^2$ times multiplications modulo N for determining the period T (A, N). Many practical demonstration examples verified the results. This approach can be used to construct new efficient cryptosystems for digital multimedia encryption/decryption.

Key words: digital multimedia; random matrix scrambling transformation; periodicity; polynomial time complexity; security