基于矩阵张量积的数据加密方案*)

A Kind of Data Encryption Scheme Based on the Tensor Product of Matrices

谭国律

(上饶师范学院数学计算机系　上饶334001)

Abstract Using the theory of tensor product of matrices, this paper puts forward a kind of data encryption scheme, analyzes its feasibility and advance, and gives a practical application model. Furthermore, it points out the possibility for regarding this scheme as a common-code encryption scheme.

Keywords Data encrypt, Matrix, Tensor product

1 引言

在当今信息社会中，计算机技术的应用日趋深化，大量的数据交换越来越频繁，由此引起的数据安全也更加突出。作为保障数据安全的一种非常重要方法，数据加密技术已越来越受重视，对它的研究也就有着非常重要的现实意义。

文[2,3]研究了基于最大秩距离码的密码系统，文[4]对此密码系统进行了进一步的讨论。1929年，美国的希尔(Hill)提出了一种代数加密体制，其思想是用代数编码方式来进行加密和解密，采用解方程的方法把明文变成密文。本文利用矩阵的张量积理论，提出一种代数加密方案。

2 加密思路简述

取定两个正整数 n 和 P，且 $n\geqslant 3$，让 $m=2^p$。引入如下一些记号：序列集合 $\Gamma(s_1,s_2,\cdots,s_t)=\{a\mid a=(a(1),a(2),\cdots,a(t)),1\leqslant a(i)\leqslant s_i,i=1,2,\cdots,t\}$ 它共有 $\prod_{i=1}^{t}s_i$ 个元素，且按字典序排列。为了简便记号，当 $s_1=s_2=\cdots=s_t=s$ 时，用 $\Gamma_{(t,s)}$ 表示 $\Gamma(s_1,s_2,\cdots,s_t)$；对于序列 $a\in\Gamma_{(2,n)}$，$\hat{a}^i$ 表示这样一个序列，$\hat{a}^i$ 与 a 除第 i 个分量不同外，其余分量与 a 完全一样，而 $\hat{a}^i$ 的第 i 分量是这样的，当 $a(i)=1$ 时 $\hat{a}^i(i)=2$，当 $a(i)=2$ 时 $\hat{a}^i(i)=1$；记集合 $E=\{i;0\leqslant i\leqslant m-1\}$。没有特别声明，本文的算术运算均是按模 m 进行的。

按以下步骤构作加密矩阵 A：

1)取 n 个 E 上的2阶可逆矩阵 $A_1,A_2,\cdots,A_n$，其中 $A_i=(a_{ij}^i)_{2\times 2}$，作张量积 $\tilde{A}=\bigotimes_{i=1}^{n}A_i$，它为 2^n 阶的方阵，其中 $(\tilde{A})_{\alpha\beta}=\prod_{i=1}^{n}a^i_{\alpha(i)\beta(i)}$，$\alpha,\beta\in\Gamma_{(2,n)}$。

2)在整数子集$\{1,2,3,\cdots,2^n\}$中随机取出 $2n$ 个互不相同的整数，作成 n 对整数对 $(i_{11},i_{12}),(i_{21},i_{22}),\cdots(i_{n1},i_{n2})$，且把它们看成是 n 个对换，对 $\tilde{A}$ 施行这样的 n 次行对换，记结果矩阵为 A(由于当 $n\geqslant 3$时，$2^n>2n$，故取法可行)。

利用加密矩阵 A，对于明文组 $X=(x_1,x_2,\cdots,x_{2^n})$，$AX$ 作为它的密文。

设 $A=P\tilde{A}$，其中 P 是由 n 次行对换形成的 2^n 阶的置换矩阵，则解密算法为：

$X=A^{-1}Y=\tilde{A}^{-1}P^{-1}Y=\tilde{A}^{-1}PY$

为叙述方便，按以上思路形成的加密方案简记为 $TGL(n,p)$。

3 相关数学原理及可行性

由以上可知，要利用矩阵 A 进行加密，首先必须解决的问题就是矩阵 A 的可逆性及其逆矩阵的求解。

定理1[5]　设有 n 个方阵 $A_1,A_2,\cdots,A_n$，其张量积为 $A=\bigotimes_{i=1}^{n}A_i$，则 A 可逆的充分必要条件是每个 A_i 均可逆，且当 A 可逆时，$A^{-1}=\bigotimes_{i=1}^{n}A_i^{-1}$。

由定理1知，要得知 A 的可逆性，可由诸 A_i 的可逆性来判断，而且其逆矩阵也可由诸 A_i 的逆矩阵来获得。

对于集合 E，在按模 m 的加法和乘法下构成一个有单位元的交换环。

定理2[6]　设 A 是 E 上的一个方阵，则 A 在 E 上可逆的充分必要条件是，A 的行列式 $|A|$ 在 E 中有逆元。

定理3　设 a 是环 E 中的一个元素，则 a 在 E 中有逆元的充分必要条件是 a 为奇数。

证明　设 $a\in E$ 为奇数，由于 m 的任何非1因子必被2整除，故 a 与 m 互素，所以存在整数 k_1,k_2，使得：$k_1a+k_2m=1$。

又由整数中的带余除法知，存在整数 $k,b,0\leqslant b<m$，使得 $k_1=mk+b$，所以

$ab+(k_2+ka)m=1$，即 $ab\equiv 1 \bmod(m)$

这说明 a 在 E 中有逆元。

反之，对任何 $a\in E$，若 a 为偶数，则它可写成：$a=2^st$，t 为奇数或零，$0<s<p$。取 $b=2^{p-s}$，则 $ab\equiv 0 \bmod(m)$，所以 a 不可能有逆元。　证毕

利用定理3，对于 E 上的2阶方阵 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$，要判断它是否可逆，只须验证 $ad-cb$ 是否为奇数即可。进一步，若 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ 可逆，则它的逆矩阵可按如下方法求得：

由于 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}d & -b\\ -c & a\end{pmatrix}=\begin{pmatrix}ad-cb & 0\\ 0 & ad-cb\end{pmatrix}=(ad-cb)\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$，记 $ad-cb$ 在 E 中的逆元为 e，则 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}^{-1}=e\begin{pmatrix}d & -b\\ -c & a\end{pmatrix}$。

引理4　设 P 为 2^n 阶的置换矩阵，若 P 是 E 上的某 n 个2阶方阵的张量积，则必存在 n 个2阶置换矩阵，使得 P 是这些

*)上饶师范学院科研基金资助课题。谭国律　硕士，副教授，主要研究方向为计算机安全和计算机应用。

2阶置换矩阵的张量积。

证明　设 $P=\overset{n}{\underset{i=1}{\otimes}}A_i$，其中诸 A_i 均为2阶方阵。由于 P 可逆，所以每个 A_i 均可逆。下面证明每个 A_i 的任一行不能有2个非零元素。

设某个 $A_i=\begin{pmatrix} a & b \\ * & * \end{pmatrix}$，$a,b\in E$。取 $\alpha\in\Gamma_{(2,n)}$，使得 $\alpha(i)=1$。由于 P 的第 α 行必有一个值为1的元素，故存在 $\beta\in\Gamma_{(2,n)}$，使得 $(P)_{\alpha\beta}=1$，而且对任何 $\beta\neq\gamma\in\Gamma_{(2,n)}$，必有 $(P)_{\alpha\gamma}=0$（因为 P 的第 α 行只有一个非零元）。由于 $(P)_{\alpha\beta}=\overset{n}{\underset{q=1}{\prod}}(A_q)_{\alpha(q)\beta(q)}$，取 $e=\overset{n}{\underset{q=1,q\neq i}{\prod}}(A_q)_{\alpha(q)\beta(q)}$，则 $e\in E$，且 $(P)_{\alpha\beta}=ea=1$（这里不妨设 $\beta(i)=1$），这说明 e 在 E 中有逆元。另一方面，由于 $\beta\neq\beta'\in\Gamma_{(2,n)}$，从而 $(P)_{\alpha\beta'}=eb=0$，这就导致 b 为零。

同理可证 A_i 的第二行不能有二个非零元素。

这样，再加上每个 A_i 可逆，从而每个 A_i 具有形式

$\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix},\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$，$a,b\in E$ 且均在 E 中有逆元。

若有某个 $A_i=\begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix}$，取 $\alpha\in\Gamma_{(2,n)}$，使得 $\alpha(i)=1$，这时存在 $\beta\in\Gamma_{(2,n)}$，使得 $(P)_{\alpha\beta}=1$。同上，存在 $e\in E$，使得 $ea=1$，其中 $e=\overset{n}{\underset{q=1,q\neq i}{\prod}}(A_q)_{\alpha(q)\beta(q)}$（这里必有 $\beta(i)=2$）。由于 $(P)_{\alpha'\beta'}=eb\neq0$，所以 $eb=1$（P 的非零元只能为1）。所以 $b=a$。

同理，若某个 A_i 具有形式 $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$，则也必须有 $b=a$。

以上已经证明，$A_i=a_iP_i$，$a\in E$，P_i 为2阶置换矩阵，$i=1,2,\cdots,n$，所以 $P=(\overset{n}{\underset{i=1}{\prod}}a_i)(\overset{n}{\underset{i=1}{\otimes}}P_i)$。很明显，$\overset{n}{\underset{i=1}{\prod}}a_i=1$，从而 $P=\overset{n}{\underset{i=1}{\otimes}}P_i$。　证毕

定理5　设 P 为 2^n 阶的置换矩阵，且其主对角线上既有值为0的元素也有值为1的元素，则 P 不可能是 E 上的某 n 个2阶方阵的张量积。

证明　若 P 是 E 上的某 n 个2阶方阵的张量积，则由引理4知，必存在 E 上的某 n 个2阶置换矩阵，使得 P 是它们的张量积。设 $P=\overset{n}{\underset{q=1}{\otimes}}E^q_{i_qi'_q}$，其中每个 $E^q_{i_qi'_q}$ 为2阶置换矩阵，且当 $s_q=t_q$ 时，$E^q_{i_qi'_q}=I_2$（2阶单位矩阵），当 $s_q\neq t_q$ 时，$E^q_{i_qi'_q}$ 的 (s_q,t_q) 和 (t_q,s_q) 位置上元素均为1，其余二个位置上元素均为0（下面的 $E_{\alpha(q)\beta(q)}$ 与 $E^q_{i_qi'_q}$ 具有类似的意义）。

因为 P 的主对角线至少有一个0元素，故它的主对角线以外必有值为1的元素，所以必存在 $\alpha,\beta\in\Gamma_{(2,n)}$ 且 $\alpha\neq\beta$，使得 $(P)_{\alpha\beta}=1$。而 $(P)_{\alpha\beta}=\overset{n}{\underset{q=1}{\prod}}(E^q_{i_qi'_q})_{\alpha(q)\beta(q)}$，由于每个 $(E^q_{i_qi'_q})_{\alpha(q)\beta(q)}$ 要么为0，要么为1，故每个 $(E^q_{i_qi'_q})_{\alpha(q)\beta(q)}=1$，所以

$E^q_{i_qi'_q}=E_{\alpha(q)\beta(q)}$，$q=1,2,\cdots,n$。

另一方面，由假设，存在 $\gamma\in\Gamma_{(2,n)}$，使得 $(P)_{\gamma\gamma}=1$。于是可同理推得

$E^q_{i_qi'_q}=E_{\gamma(q)\gamma(q)}$，$q=1,2,\cdots,n$

所以，$E_{\alpha(q)\beta(q)}=E_{\gamma(q)\gamma(q)}$，$q=1,2,\cdots,n$。这就导致 $\alpha(q)=\gamma(q)=\beta(q)$，$q=1,2,\cdots,n$，从而 $\alpha=\beta$，矛盾。　证毕

定理6　设 $\tilde{A}$ 是 E 上的某 n 个2阶可逆方阵的张量积，又设 P 为 2^n 阶的置换矩阵，它不是 E 上的某 n 个2阶置换矩阵的张量积，则 $P\tilde{A}$ 不可能是 E 上的某 n 个2阶可逆方阵的张量积。

证明　假设存在2阶可逆方阵 $A_1,A_2,\cdots,A_n$，使得 $P\tilde{A}=\overset{n}{\underset{i=1}{\otimes}}A_i$，由于 $\tilde{A}$ 是 E 上的某 n 个2阶可逆方阵的张量积，即存在2阶可逆方阵 $B_1,B_2,\cdots,B_n$ 使得 $\tilde{A}=\overset{n}{\underset{i=1}{\otimes}}B_i$，则 $P=(\overset{n}{\underset{i=1}{\otimes}}A_i)\tilde{A}^{-1}=(\overset{n}{\underset{i=1}{\otimes}}A_i)(\overset{n}{\underset{i=1}{\otimes}}B_i^{-1})=\overset{n}{\underset{i=1}{\otimes}}(A_iB_i^{-1})$，从而 P 是 E 上的某 n 个2阶可逆矩阵的张量积，由引理4知，P 是 E 上的某个2阶置换矩阵的张量积，矛盾。　证毕

在加密思路简述中，1）是为了方便寻求加密矩阵以及求其逆矩阵。事实上，若要直接计算一个 2^n 阶矩阵的逆矩阵是很不现实的，若事先知道它间接地是某 n 个2阶可逆矩阵的张量积，则利用定理1，2，3来求它的逆矩阵将是容易实现的。

由于当 $n\geqslant3$ 时，$2^n>2n$，故加密思路简述2）中的 P 满足定理5，所以由定理6可知，2）中的 $P\tilde{A}$ 不可能是某 n 个2阶矩阵的张量积，即那里的加密矩阵 A 不可能是某 n 个2阶矩阵的张量积，这对于不知道这些2阶矩阵 A_i 以及置换矩阵 P 的人来说，要想从 A 来获得 A^{-1} 将是不太可能的。

4　TGL(8,8)的分析

本节讨论 TGL(8,8)方案，这时 $n=p=8$，$m=256$，加密矩阵 A 是256阶的，而 $E=\{0,1,2,\cdots,255\}$。

4.1　TGL(8,8)加、解密算法描述

加密过程如下：

1）对于明文 M，可纯粹地把它看成是字节流（普通 ASCII 码字符为一个字节，其 ASCII 值在0到127之间，而汉字是二个字节，且每个字节的 ASCII 码值在128到255之间），把 M 按每256个字节为一组进行分组，若分到最后不足256，则采用填充的技术补足到256个，记分组为 $M_1,M_2,\cdots,M_t$。

2）由 $N_i=AM_i$ 得密文系列 $N_1,N_2,\cdots,N_t$

解密的过程为：

1）利用 n 个2阶可逆方阵，求得 $\tilde{A}^{-1}=\overset{n}{\underset{i=1}{\otimes}}A_i^{-1}$，再由 2^n 阶的置换矩阵 P 求得加密矩阵 A 的逆矩阵 $A^{-1}=\tilde{A}^{-1}P$。

2）由 $M_i=A^{-1}N_i$ 还原为明文系列 $M_1,M_2,\cdots,M_t$。

4.2　TGL(8,8)方案分析

利用定理2和定理3，经简单编程计算，在 TGL(8,8)方案下，E 上总共有1610612736个2阶可逆矩阵，没有任何零元素的2阶可逆矩阵也有1593868288个，从而利用加密思路简述中的1），可至少构作出 1593868288^8 个 E 上的256阶可逆矩阵。若全球有100亿人口，则平均每人拥有的加密矩阵至少有 $4.165*10^{63}$ 个。可见，用作加密的矩阵其数量是庞大的。

下面分析，即使是知道加密矩阵 A，而不知道置换矩阵 P 以及 n 个2阶可逆矩阵 $A_1,A_2,\cdots,A_n$，计算它的逆矩阵所要付出的代价。

假设采用穷举的方法，把乘法、除法、加法和比较均作为一次基本运算。对于给定的矩阵 A，要验证是否有矩阵 B，使得 $AB=I$ 所需的基本运算有如下估计：由于验证 AB 中的一个元素，需要的基本运算是256次乘法、255次加法、1次模 m 运算和1次比较运算，共计 $256\times2+1$ 次基本运算。加之 AB 有256个元素，故所需的基本运算次数是 $256\times(256\times2+1)$。又由于 B 的取法至少有 1593868288^8（1593868288^8 约为 2^{244}）种可能，所以，对于矩阵 A，用枚举验证的方法来求出它的逆矩阵，平均所需的基本运算次数至少为 $2^{244}\times256\times(256\times2+1)$

（下转第125页）

tems, Pittsburg, May 1993. 410～419
9 Kopetz H, Grunsteidle G. TTP-A: Time-Triggered Protocol for Fault Tolerant Real-Time Systems. In: Proc. IEEE CS FTCS-23, Toulose, France, June 1993. 524～533
10 Kim K, Subbaraman C. A Supervisor-Based Semi-Centralized Network Survillance Scheme and the Fault Detection Latency Bound. In: Proc. 16th Symp. on Reliable Dist. Systems, Oct. 1997. 146～155
11 Kim K. Group Communication in Real-Time Computing Systems: Issues and Directions. In: Proc. FTDCS'99 (7th IEEE Workshop on Future Trends of Distributed Computing Systems), Cape Town, South Africa, Dec. 1999. 252～258
12 Kim K. Issues Insufficiently Resolved in Century 20 in the Fault-Tolerance Distributed Computing Field. In: Proc. SRD2000(IEEE CS 19th Symp. On Reliable Distributed Systems), Nuremberg, Germany, Oct. 2000. 106～115
13 Barcellos Marinho P, Ezhilchelvan Paul D. A End-to-End Reliable Multicast Protocol Using Polling for Scalability: [Tech. Rept. 609]. Dept. of Computing Science, Univ. of Newcastle upon Tyne, 1997
14 Birman K , Schiper A, Stephenson P. Lightweight Causal and Atomic Group Multicast. ACM Trans. On Computer Systems, 1991, 9(3): 272～314
15 Chang J M, Maxemchunk N. Reliable Broadcast Protocols. ACM Trans. On Computer Systems, 1984, 2(3): 251～273
16 Christian F, Aghili H , Strong R, Dolev D. Atomic Broadcast: From simple message diffusion to Byzantine Agreement. In: Proc. FTCS 15, Ann Arbor, Michigan, 1985. 200～206
17 Cheriton D R, Skeen D. Understanding the Limitations of Causally and Totally Ordered Communication. In: 14th ACM Symposium on Operating Systems Principles, pp. 44～57
18 Shokri E, et al. An Approach for Adaptive Fault Tolerance in Object-Oriented Open Distributed Systems. International Journal of Software Engineering and Knowledge Engineering, 1998, 8(3)
19 Hurley P , Dussault J L. The Development and Assessment of An Adaptive Fault Resistant System(AFRS). In: Proc. of Second International Command & Control Research & Technology Symposium, Warwickshire, UK, Sept. 1996. 256～267
20 Shokri E, Hecht M. Adaptive Fault-Tolerance for Autonomous Spacecraft. NASA SBIR Phase 1, Final Report, SoHaR Inc., Beverly Hills, CA, June 1996
21 Gupta, et al. Adaptive Fault Resistant System(AFRS)", Rome Laboratory USAF: [Technical Report RL-TR-95-3]
22 Goldberg J. Adaptive Fault Resistant System", SRI International: [Technical Report SRI-CSL-95-02]
23 Bihari B, Schman K. Dynamic Adaptation of Real-Time Software. ACM Transactions on Computer Systems, 1991, 9: 143～174
24 Kim K. Action-level fault tolerance, in Advances in Real-Time Systems. S. H. Sang ed., Prentice Hall, 1994. 415～434
25 Bondavalli A, Stankovic J, Strigini L. Adaptive Fault Tolerance for Real-Time Systems, in Responsive Computer Systems: Steps toward Fault-Tolerant Real-Time System. D. S. Fussell and M. Malek ed., Kluwer, 1995. 187～208
26 Sabnis C, Cukier M, Ren J, et al. Proteus: A Flexible Infrastructure to Implement Adaptive Fault-Tolerance in AquA. In: Proc. of the 7th IFIP IWC in DCCA, 1999. 137～156
27 Kalbarczyk Z, et al. Chameleon: a Software infrastructure for Adaptive Fault Tolerance. IEEE Transactions on Parallel and Distributed Systems, 1999, 10(6): 560～579
28 李琪林，陈宇，周明天. 基于CORBA的分布式系统自适应容错模型的研究. 计算机科学，2002，29(3)：119～121

(上接第120页)

÷2次，它大致为$2^{244}\times 2^{16}=2^{260}$。若计算机每秒能做千亿次($10^{11}$)基本运算，由于$2^{10}$约为$10^3$，而$2^{260}=(2^{10})^{26}\approx 10^{3\cdot 26}=10^{78}$，故所需的时间是$10^{78}\div 10^{11}=10^{67}$秒，这相当于$3.17\times 10^{59}$年(一年365天，一天24小时)。

5 需进一步讨论的问题

从以上分析来看，有理由相信，能把$TGL(8,8)$方案作为公钥体制下的一种加密方法，加密矩阵A公开，而置换矩阵P和n个2阶可逆矩阵作为解密密钥。进一步，为加大这种可能性，在$TGL(n,p)$中可取大些的n和p，这样，至少在理论上可以把$TGL(n,p)$方案作为公钥体制下的一种加密方法。限于篇幅，本文不再讨论。

小结 本文利用矩阵张量积理论，讨论了$TGL(n,p)$方案作为私钥体制下的一种数据加密方法的可行性及先进性，并详细分析了它的一种具体实用模型$TGL(8,8)$。进一步指出了把$TGL(n,p)$方案作为公钥体制下的一种数据加密方法的可能性。对于实用模型$TGL(8,8)$，在笔者近年来进行的软件研制开发工作中得到了具体的应用，取得了很好的效果。

参 考 文 献

1 Meyer C H, Matyas S M. Cryptograhy: A New Dimension in Computer Data Security—A Guide for the design and Implementation of Secure Systems. John Wiley & Sons, Inc, 1982
2 Gabidulin E M, Paramonov A V, Tretjakov. Ideals over a non-commutative ringand their application in cryptology. In: Lecture Notes in Computer Science 547, Springer-verlag, 1991. 482～489
3 Gibson J K. Severely denting the Gabidulin version of the McEliece public key cryptosystem. Designs, Codes and Cryptography, 1995, 6: 37～45
4 杜伟章，王新梅. 基于最大秩距离码的私钥加密方案. 计算机学报，2001，24(6)：650～653
5 王伯英. 多重线性代数基础. 北京：北京师范大学出版社，1985，5
6 McCoy N H. 著，刘绍谋译. 环与理想. 1983，5
7 郑雪雪. 数据安全与软件加密技术. 北京：人民邮电出版社，1995，6
8 李新晖，陈梅兰. 信息安全技术的研究发展与应用. 计算机与现代化，2000(4)：28～33