DOI：10.13718/j.cnki.xdzk.2018.11.006

$GF(2^8)$上高矩阵为密钥矩阵的 Hill 加密衍生算法①

刘海峰[1,2]，　卢开毅[1]，　梁星亮[2]

1. 陕西科技大学 电气与信息工程学院，西安 710021；2. 陕西科技大学 文理学院，西安 710021

摘要：针对传统的 Hill 加密算法仅是利用有限域 $GF(p)$ 上可逆的数字方阵作为密钥矩阵与明文向量做模 P 乘法进行加密运算，提出了一种新的在有限域 $GF(2^8)$ 上以多项式高矩阵作为密钥矩阵的 Hill 加密衍生算法. 在 Hill 加密衍生算法中，明文向量为明文字符对应的多项式构成的多项式向量，随机选取密钥矩阵的一列作为加密时的平移增量，在 $GF(2^8)$ 上进行密钥矩阵与明文向量的模 8 次不可约多项式 $p(x)$ 的乘法和加法，然后获得元素为多项式的密文向量，从而实现明文信息加密. 由于在不知道有限域的 8 次不可约多项式、密钥矩阵以及随机抽取的平移向量的情况下由密文破解得到明文的难度更大，从而提高了有限域 $GF(2^8)$ 上 Hill 加密衍生算法的抗攻击能力.

关　键　词：有限域 $GF(2^8)$；Hill 加密；多项式高矩阵；不可约多项式

中图分类号：O151.21　　**文献标志码：A**　　**文章编号：**1673－9868(2018)11－0041－07

传统的 Hill 加密算法将英文字母、数字以及常见的符号构成编码字符集. 编码字符集的基数为 p，以一定的编码规则进行编码，并对应 0 到 $p-1$ 之间的整数，但是如果编码字符集的基数 p 不为素数[1]，还必须使得加密矩阵行列式的值在模 p 下有乘法逆元；文献[2－3]给出了在模 26 情况下的数字方阵作为密钥矩阵需要满足的要求，并给出了在模 26 意义下选取密钥矩阵以及 MATLAB 求解逆矩阵的方法；文献[4]针对密钥矩阵在模 26 意义下的逆矩阵可能是分数的问题提出了行列变换的改进，当 p 为素数时，可以得到一个具有 p 个元素的有限域 $GF(p)$，但其上的 Hill 加密的密钥矩阵易受到暴力攻击.

有限域 $GF(2^8)$ 是一种特殊的有限域[5]，其具有 2^8 个元素，而不是像有限域 $GF(p)$ 上必须有 p 个元素（p 为素数）. 有限域 $GF(2^8)$ 上每个元素都可以表示为 8 位的二进制数，并可以将元素唯一地映射为一个系数为 0，1 的 8 次以下的一元多项式，其有限域上的多项式的加法和乘法等运算具有封闭性，在密码学、信息编码等领域都是很重要的数学工具[6]. 有限域 $GF(2^8)$ 的算术运算具有一定的复杂性和特殊性（表中的 space 表示空格符）.

本文论述有限域 $GF(2^8)$ 上的 Hill 加密是对传统 Hill 加密的衍生，把有限域 $GF(2^8)$ 上互为伪逆的一对矩阵作为加密和解密密钥，能满足安全密码系统的基本条件. 本文选取空格和 255 个互异的可见字符进行字符编码，如表 1 所示，并按照 0 ～ 255 的顺序对表格中的字符按照行优先进行编码.

① 收稿日期：2017－12－13
基金项目：陕西省自然科学基础研究计划青年项目(2017JQ1026)；陕西省教育厅专项科学研究计划项目(17JK0102).
作者简介：刘海峰(1964－)，男，副教授，硕士，主要从事计算机网络与信息安全及代数编码与密码学的研究.

表1 字符编码表

space	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
r	s	t	u	v	w	x	y	z	A	B	C	D	E	F	G	H	I
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0
1	2	3	4	5	6	7	8	9	!	@	#	$	%	^	&	*	(
)	—	_	=	+	~	`	[	]	\	;	,	.	/	{	}	:	"
’	<	>	?	α	β	γ	δ	ε	ζ	η	θ	ι	κ	λ	μ	ν	ξ
ο	π	ρ	σ	τ	υ	φ	χ	ψ	ω	Α	Β	Γ	Δ	Ε	Ζ	Η	Θ
Ι	Κ	Λ	Μ	Ν	Ξ	Ο	∏	Ρ	∑	Τ	Υ	Φ	Χ	Ψ	Ω	℃	℉
Ⅰ	Ⅱ	Ⅲ	Ⅳ	Ⅴ	Ⅵ	Ⅶ	Ⅷ	Ⅸ	Ⅹ	Ⅺ	Ⅻ	ⅰ	ⅱ	ⅲ	ⅳ	ⅴ	ⅵ
ⅶ	ⅷ	ⅸ	×	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю
Я	★	☆	▲	△	◆	◇	■	□	⊙	○	▽	〖	〗	〖	〗	《	》
〔	〕	「	」	【	】	£	¢	¥	←	↑	→	↓	↖	↗	↘	↙	∈
√	∞	∽	≈	∵	∷	※	≌	∫	≦	≧	≮	≯	≡	≠	×	÷	±
•	≤	≥	§														

1 有限域 $GF(2)[x]/(p(x))$ 的定义

定义1 有限域 $GF(2)[x]$ 指二元域 $GF(2)$ 上的一元多项式的全体的集合.

设 $p(x)$ 是 $GF(2)$ 上的一个8次不可约多项式，$GF(2)[x]/(p(x))=\langle S,+,*,p(x)\rangle$ 是一个代数结构，满足

$$S=\{a(x)\mid a(x)\in GF(2)[x],\deg(a(x))<8\}$$

且 $GF(2)[x]/(p(x))$ 关于域上的加法"+"构成阿贝尔群，其单位元为零多项式，$GF(2)[x]/(p(x))-\{0\}$ 关于有限域上的乘法"*"构成阿贝尔群，且"*"对"+"满足分配律，也即对 $\forall a(x),b(x),c(x)\in S$，记

$$a(x)=\sum_{i=0}^{7}a_ix^i \qquad b(x)=\sum_{i=0}^{7}b_ix^i \qquad c(x)=\sum_{i=0}^{7}c_ix^i$$

其中 $a_i,b_i,c_i\in\{0,1\}$，满足左右分配律

$$(a(x)+b(x))*c(x)=a(x)*c(x)+b(x)*c(x)$$

$$c(x)*(a(x)+b(x))=c(x)*a(x)+c(x)*b(x)$$

成立. 考虑到 $GF(2^8)$ 与 $GF(2)[x]/(p(x))$ 上的元素及其元素间相应的运算具有一一对应的性质，所以下文重点讨论 $GF(2)[x]/(p(x))$ 上的Hill加密衍生算法. 有限域 $GF(2)[x]/(p(x))$ 上相应运算定义如下：

1) $a(x)+b(x)=\sum_{i=0}^{7}((a_i+b_i)\bmod 2)x^i$

2) $a(x)-b(x)=a(x)+b(x)$

3) $a(x)*b(x)=(\sum_{i=0}^{7}\sum_{j=0}^{7}((a_i\times b_j)\bmod 2)x^{i+j})\bmod p(x)$

4) $a(x)^{-1}$：当且仅当 $a(x)*a(x)^{-1}=1$

5) $a(x)/b(x)=a(x)*b(x)^{-1}$

2　有限域 $GF(2)[x]/(p(x))$ 上多项式和多项式矩阵的求逆

2.1　有限域 $GF(2)[x]/(p(x))$ 的多项式求逆[7]

对 $\forall a(x) \in GF(2)[x]/(p(x))$，$a(x) \neq 0$，因为 $p(x)$ 为不可约多项式，显然有

$$\gcd(a(x),\ p(x)) = 1$$

根据代数性质，必然存在有限域上的唯一多项式 $b(x)$ 使得 $b(x) = a(x)^{-1}$ 为 $a(x)$ 的乘法逆元，可用如下方法求多项式 $a(x)$ 的逆多项式.

1）令 $a(x) = a_k x^k + \cdots + a_2 x^2 + a_1 x + a_0$，其中 $a_i \in \{0, 1\}$，$k \leqslant 7$.

2）设 $b(x)$ 是 $a(x)$ 在模 $p(x)$ 下的逆多项式，令 $b(x) = b_7 x^7 + \cdots + b_2 x^2 + b_1 x + b_0$，其中 $b_i \in \{0, 1\}$.

3）由多项式的乘法可得

$$c(x) = a(x) * b(x) = a_k b_7 x^{k+7} + (a_{k-1} b_7 + a_k b_6) x^{k+6} + \cdots + a_0 b_0$$

也即有

$$c(x) = (x^{k+7},\ x^{k+6},\ \cdots,\ x^7,\ \cdots,\ x^2,\ x,\ 1) \begin{pmatrix} a_k & 0 & 0 & \cdots & 0 & \cdots & 0 & 0 \\ a_{k-1} & a_k & 0 & \cdots & 0 & \cdots & 0 & 0 \\ a_{k-2} & a_{k-1} & a_k & \cdots & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_k & \cdots & 0 & 0 \\ a_0 & a_1 & a_2 & \cdots & a_{k-1} & \cdots & 0 & 0 \\ 0 & a_0 & a_1 & \cdots & a_{k-2} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & \cdots & a_0 & a_1 \\ 0 & 0 & 0 & \cdots & 0 & \cdots & 0 & a_0 \end{pmatrix} \begin{pmatrix} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{pmatrix}$$

其中的二维矩阵是一个$(k+8) \times 8$的矩阵，可以把 $c(x)$ 中方次大于 7 的项 $x^m (m > 7)$ 用模 $p(x)$ 的余式替换掉，也即在有限域 $GF(2)[x]/(p(x))$ 用 $x^m \bmod p(x)$ 得到的结果替换掉 x^m，从而消去 x 的方次大于 7 的项，替换后合并同类项得到降幂的多项式

$$c(x) = c_7 x^7 + \cdots + c_2 x^2 + c_1 x + c_0$$

其中 c_i 包含未知数 $b_7, b_6, \cdots, b_1, b_0$.

4）由于设 $b(x)$ 是 $a(x)$ 在模 $p(x)$ 下的逆多项式，所以

$$c(x) = a(x) * b(x) = 1 \bmod p(x)$$

也即可以得到

$$c(x) = c_7 x^7 + \cdots + c_2 x^2 + c_1 x + c_0 = 1 \bmod p(x)$$

又因为

$$c(x) \in GF(2)[x]/(p(x))$$

所以可以得

$$c(x) = c_7 x^7 + \cdots + c_2 x^2 + c_1 x + c_0 = 1$$

因此有下面的方程组成立

$$\begin{cases} c_7(b_7,\ b_6,\ \cdots,\ b_2,\ b_1,\ b_0) = 0 \\ \qquad\qquad \vdots \\ c_1(b_7,\ b_6,\ \cdots,\ b_2,\ b_1,\ b_0) = 0 \\ c_0(b_7,\ b_6,\ \cdots,\ b_2,\ b_1,\ b_0) = 1 \end{cases}$$

可以用模 2 意义下的高斯消元法解此方程组，最后即可得 $b(x)$ 中各项的系数，得到 $a(x)$ 的逆多项式 $b(x)$.

2.2 有限域 $GF(2)[x]/(p(x))$ 的 n 阶方阵求逆

有限域上的 n 阶多项式方阵

$$\boldsymbol{Key}(x)=\begin{bmatrix} a_{11}(x) & a_{12}(x) & \cdots & a_{1n}(x) \\ a_{21}(x) & a_{22}(x) & \cdots & a_{2n}(x) \\ \vdots & \vdots & & \vdots \\ a_{n1}(x) & a_{n2}(x) & \cdots & a_{nn}(x) \end{bmatrix}$$

$$a_{ij}(x)\in GF(2)[x]/(p(x))$$

根据代数学方法求 $\boldsymbol{Key}(x)$ 在有限域 $GF(2)[x]/(p(x))$ 上的行列式

$$\det(\boldsymbol{Key}(x))=|\boldsymbol{Key}(x)| \bmod p(x)$$

$|\boldsymbol{Key}(x)|$ 为矩阵 $\boldsymbol{Key}(x)$ 的普通 n 阶行列式. 定义伴随矩阵

$$\boldsymbol{Key}(x)^{*}=\begin{bmatrix} A_{11}(x) & A_{21}(x) & \cdots & A_{n1}(x) \\ A_{12}(x) & A_{22}(x) & \cdots & A_{n2}(x) \\ \vdots & \vdots & & \vdots \\ A_{1n}(x) & A_{2n}(x) & \cdots & A_{nn}(x) \end{bmatrix}$$

其伴随矩阵中的 $A_{ij}(x)$ 为多项式方阵 $\boldsymbol{Key}(x)$ 中元素 $a_{ij}(x)$ 在模 $p(x)$ 意义下的代数余子式. 如果有 $\det(\boldsymbol{Key}(x))\neq 0$, 则根据上节有限域 $GF(2)[x]/(p(x))$ 上多项式求逆的方法可以求得多项式 $\det(\boldsymbol{Key}(x))$ 的逆多项式 $|\boldsymbol{Key}(x)|^{-1}$, 最后可得逆矩阵

$$\boldsymbol{Key}(x)^{-1}=(|\boldsymbol{Key}(x)|^{-1}\cdot\boldsymbol{Key}(x)^{*}) \bmod p(x)$$

2.3 有限域 $GF(2)[x]/(p(x))$ 的多项式高矩阵左伪逆求解

高矩阵是指列线性无关的矩阵[8]. 可逆方阵为高矩阵的一种特例.

有限域 $GF(2)[x]/(p(x))$ 上的多项式高矩阵: $GF(2)[x]/(p(x))$ 上的高矩阵指列满秩的多项式矩阵, 其中多项式矩阵的元素属于 $GF(2)[x]/(p(x))$, $p(x)$ 是 $GF(2)$ 上的一个 8 次不可约多项式.

根据一般数字高矩阵 $\boldsymbol{A}$ 求左伪逆的公式 $pinv(\boldsymbol{A})=(\boldsymbol{A}'*\boldsymbol{A})^{-1}*\boldsymbol{A}'$[9](其中 $\boldsymbol{A}$ 为列满秩的数字矩阵), 可得有限域 $GF(2)[x]/(p(x))$ 上高矩阵求左伪逆的方法, 设高矩阵

$$\boldsymbol{A}(x)=\begin{bmatrix} a_{11}(x) & a_{12}(x) & \cdots & a_{1l}(x) \\ a_{21}(x) & a_{22}(x) & \cdots & a_{2l}(x) \\ \vdots & \vdots & & \vdots \\ a_{k1}(x) & a_{k2}(x) & \cdots & a_{kl}(x) \end{bmatrix}$$

是列满秩的矩阵, 且满足 $k\geq l$, 则有

$$(\boldsymbol{A}(x)'*\boldsymbol{A}(x))_{ij}=(\sum_{t=1}^{k}a_{ti}(x)a_{tj}(x)) \bmod p(x) \qquad i,j=1,2,\cdots,l$$

然后利用上节有限域 $GF(2)[x]/(p(x))$ 上多项式方阵求逆的方法可求得 $\boldsymbol{A}'(x)*\boldsymbol{A}(x)$ 在模 $p(x)$ 意义下的逆多项式矩阵 $(\boldsymbol{A}'(x)*\boldsymbol{A}(x))^{-1}$, 最后用求得的 $(\boldsymbol{A}'(x)*\boldsymbol{A}(x))^{-1}$ 与 $\boldsymbol{A}'(x)$ 做模 $p(x)$ 的多项式矩阵的乘法, 即可求得高矩阵 $\boldsymbol{A}(x)$ 的左伪逆矩阵 $pinv(\boldsymbol{A}(x))$.

3 有限域 $GF(2)[x]/(p(x))$ 上的 Hill 加密衍生算法及其解密算法

文献[10-12]提出了有限域上有关衍生的 Hill 加密以及分组加密的思想, 其中包括利用有限域上圆锥曲线密码体制等结合 Hill 分组加密来保证数据的安全, 本文对一般的 Hill 加密算法做了如下衍生.

3.1 有限域 $GF(2)[x]/(p(x))$ 上的 Hill 加密衍生算法

假设由字符编码集中的字符构成明文字符串 $M=M_1M_2\cdots M_m$, 现需要对明文进行加密发送, 首先选取有限域上合适的列满秩的加密矩阵

$$\boldsymbol{G}(x)=\begin{bmatrix} a_{11}(x) & a_{12}(x) & \cdots & a_{1l}(x) \\ a_{21}(x) & a_{22}(x) & \cdots & a_{2l}(x) \\ \vdots & \vdots & & \vdots \\ a_{k1}(x) & a_{k2}(x) & \cdots & a_{kl}(x) \end{bmatrix}$$

(其中 $k>l$) 和一个 8 次不可约多项式 $p(x)$，若明文字符串的长度 m 不满足 $l \mid m$，则根据文献[13]处理哑元的方法，添加 i 个空格字符作为哑元构成新的明文字符串 $M=M_1M_2\cdots M_k\cdots M_m\cdots M_{m+i}$，使 $l \mid (m+i)$，其中 $i<l$，加密时对字符串 M 按 l 个字符为一组进行分组，然后对每一组进行 Hill 加密，对加密后的字符串不做更改.

不妨取分组中的第一组字符进行加密，取 M 的前 l 个字符 $M_1M_2\cdots M_l$，对其中的每个字符 $M_j(1\leqslant j\leqslant l)$ 在字符编码表 1 中查询其对应位置的索引值 $Index_j$，并将索引值 $Index_j$ 转换成对应的二进制的表达式，也即有

$$Index_j=m_{j_7}*2^7+m_{j_6}*2^6+\cdots+m_{j_1}*2+m_{j_0}$$

把式中的 2 替换为 x 得到多项式

$$f_j(x)\in GF(2)[x]/(p(x))$$

最后可以得到一个明文字符串 $M_1M_2\cdots M_l$ 所对应的一个多项式向量

$$\boldsymbol{f}(x)=[f_1(x)\quad f_2(x)\quad\cdots\quad f_l(x)]^{\mathrm{T}}$$

在有限域上左乘加密矩阵 $\boldsymbol{G}(x)$，并选取密钥矩阵的第 l 列(也可以随机选取密钥矩阵的其他列) 作为平移增量，利用加密矩阵进行 Hill 加密后的密文向量 $e(x)$，其中

$$\boldsymbol{e}(x)=[e_1(x)\quad e_2(x)\quad\cdots\quad e_k(x)]^{\mathrm{T}}$$

向量的分量满足

$$e_j(x)=((\sum_{i=1}^{l}a_{ji}(x)*f_i(x))+a_{jl}(x))\bmod p(x)\qquad j=1,2,\cdots,k$$

用矩阵的形式来表示即

$$\boldsymbol{e}(x)=(\boldsymbol{G}(x)*\boldsymbol{f}(x)+\boldsymbol{a}._l(x))\bmod p(x)$$

其中 $a._l(x)$ 表示抽取矩阵 $\boldsymbol{G}(x)$ 中的第 l 列. 将密文多项式向量中每个多项式中的 x 用 2 替换，并求多项式的值，也即得到加密后密文字符在字符编码表中所对应的索引值，通过查表转换即可得到密文字符串 $C_1C_2\cdots C_l\cdots C_k$.

3.2　有限域 $GF(2)[x]/(p(x))$ 上的 Hill 加密衍生算法的解密

先根据上节的方法求加密矩阵 $\boldsymbol{G}(x)$ 在有限域 $GF(2)[x]/(p(x))$ 的左伪逆矩阵，并记左伪逆矩阵为 $\boldsymbol{G}_L(x)$，作为解密矩阵.

$$\boldsymbol{G}_L(x)=\begin{bmatrix} b_{11}(x) & b_{12}(x) & \cdots & b_{1k}(x) \\ b_{21}(x) & b_{22}(x) & \cdots & b_{2k}(x) \\ \vdots & \vdots & & \vdots \\ b_{l1}(x) & b_{l2}(x) & \cdots & b_{lk}(x) \end{bmatrix}$$

其中，由于加密时已经对相应的哑元进行了替换处理，因此加密后的密文字符串的长度必然为 $k(m+i)/l$，且有 $l \mid (m+i)$，因此可以直接对密文字符串 $C=C_1C_2\cdots C_k\cdots C_m\cdots C_{k(m+i)/l}$ 以 k 个字符为一组进行分组，再对每一组进行解密运算.

现在对分组中的其中一组密文字符讨论解密算法，不妨取 C 的第 1 组的 k 个字符 $C_1C_2\cdots C_k$，对其中的每个字符 $C_j(1\leqslant j\leqslant k)$ 在字符编码表中查询其对应位置的索引值 $Index_j$，并将索引值 $Index_j$ 转换成对应的二进制的表达式，也即有

$$Index_j=c_{j_7}*2^7+c_{j_6}*2^6+\cdots+c_{j_1}*2+c_{j_0}$$

把式中的 2 替换为 x 得到多项式

$$g_j(x)\in GF(2)[x]/(p(x))$$

最后可以得到一个密文字符串 $C_1C_2\cdots C_k$ 所对应的一个多项式向量

$$\boldsymbol{g}(x)=[g_1(x)\quad g_2(x)\quad\cdots\quad g_k(x)]^{\mathrm{T}}$$

在有限域上先减去平移增量(即密钥矩阵的第 l 列),再用得到的结果右乘解密矩阵 $\boldsymbol{G}_{\boldsymbol{L}}(x)$,然后可以得明文向量 $d(x)$,其中

$$\boldsymbol{d}(x)=[d_1(x)\quad d_2(x)\quad\cdots\quad d_l(x)]^{\mathrm{T}}$$

向量的分量满足

$$d_j(x)=(\sum_{i=1}^{k}b_{ji}(x)*(g_i(x)-a_{il}(x)))\bmod p(x)\qquad j=1,2,\cdots,l$$

用矩阵形式来表示即 $d(x)=(\boldsymbol{G}_{\boldsymbol{L}}(x)*(g(x)-a._l(x)))\bmod p(x)$,其中 $a._l(x)$ 表示抽取矩阵 $\boldsymbol{G}(x)$ 中的第 l 列. 将明文多项式向量中每个多项式中的 x 用2替换,并求多项式的值,即得到解密后明文字符在字符编码表中所对应的索引值,通过查表转换即可得到明文字符串 $M_1M_2\cdots M_l$.

4 多项式环 $GF(2)[x]$ 中的8次不可约多项式

$GF(2)[x]$ 中的8次不可约多项式是指系数只能为0,1的8次不可约的一元多项式,即8次不可约多项式 $p(x)=x^8+a_7x^7+\cdots+a_1x+a_0$(其中 a_7,…,a_1,$a_0\in\{0,1\}$),满足不能分解成 $GF(2)[x]$ 上7次及以下的多项式的乘积. 为了求解 $GF(2)[x]$ 上的8次不可约多项式的集合 A,可以先通过遍历相乘的方法求出多项式环 $GF(2)[x]$ 上的8次可约多项式的集合 B;通过分析,$GF(2)[x]$ 上的8次可约多项式的集合可以表示为 $B=B_1\cup B_2\cup B_3\cup B_4$,其中 B_1 为任意1次和任意7次多项式乘积的集合,B_2 为任意2次和任意6次多项式乘积的集合,B_3 为任意3次和任意5次多项式乘积的集合,B_4 为任意两个4次多项式乘积的集合. 然后利用 $GF(2)$ 上的8次多项式的全集 S 对 B 作差集运算,即可得相应的8次不可约多项式的集合 $A=S-B$.

通过Python程序实现以上思想,即可求得多项式环 $GF(2)[x]$ 上的所有8次不可约多项式,其降幂排列时对应的系数向量如表2所示.

表2 多项式环 $GF(2)[x]$ 上所有8次不可约多项式的系数向量

[1, 0, 0, 0, 1, 1, 0, 1, 1],	[1, 0, 0, 0, 1, 1, 1, 0, 1],	[1, 0, 0, 1, 0, 1, 0, 1, 1]
[1, 0, 0, 1, 0, 1, 1, 0, 1],	[1, 0, 0, 1, 1, 1, 0, 0, 1],	[1, 0, 0, 1, 1, 1, 1, 1, 1]
[1, 0, 1, 0, 0, 1, 1, 0, 1],	[1, 0, 1, 0, 1, 1, 1, 1, 1],	[1, 0, 1, 1, 0, 0, 0, 1, 1]
[1, 0, 1, 1, 0, 0, 1, 0, 1],	[1, 0, 1, 1, 0, 1, 0, 0, 1],	[1, 0, 1, 1, 1, 0, 0, 0, 1]
[1, 0, 1, 1, 1, 0, 1, 1, 1],	[1, 0, 1, 1, 1, 1, 0, 1, 1],	[1, 1, 0, 0, 0, 0, 1, 1, 1]
[1, 1, 0, 0, 0, 1, 0, 1, 1],	[1, 1, 0, 0, 0, 1, 1, 0, 1],	[1, 1, 0, 0, 1, 1, 1, 1, 1]
[1, 1, 0, 1, 0, 0, 0, 1, 1],	[1, 1, 0, 1, 0, 1, 0, 0, 1],	[1, 1, 0, 1, 1, 0, 0, 0, 1]
[1, 1, 0, 1, 1, 1, 1, 0, 1],	[1, 1, 1, 0, 0, 0, 0, 1, 1],	[1, 1, 1, 0, 0, 1, 1, 1, 1]
[1, 1, 1, 0, 1, 0, 1, 1, 1],	[1, 1, 1, 0, 1, 1, 1, 0, 1],	[1, 1, 1, 1, 0, 0, 1, 1, 1]
[1, 1, 1, 1, 1, 0, 0, 1, 1],	[1, 1, 1, 1, 1, 0, 1, 0, 1],	[1, 1, 1, 1, 1, 1, 0, 0, 1]

5 结束语

本文提出了一种新的有限域 $GF(2)[x]/(p(x))$ 上的Hill加密衍生算法,其中 $p(x)$ 是多项式环 $GF(2)[x]$ 上随机选取的一个8次不可约多项式,密钥矩阵为有限域 $GF(2)[x]/(p(x))$ 上随机选取的多项式高矩阵,并将随机选取密钥矩阵的其中一列作为加解密时的平移增量,在不知道 $p(x)$、密钥矩阵以及随机抽取的平移向量的情况下求多项式高矩阵左伪逆比单纯的数字矩阵求左伪逆更困难,因此很难求得相应解密矩阵,密文破解得到明文的难度更大,从而提高了有限域 $GF(2)[x]/(p(x))$ 上Hill加密的抗攻击能力. 本文采用的是 3×2 的高矩阵作为加密的密钥矩阵,在实际应用中可以采用更高阶的密钥矩阵,当密钥矩阵是 $k\times l$ 的规模时,其对应的 $k\times l$ 的多项式矩阵多达 $256^{k\times l}$ 种($k>l$),从而可选的密钥矩阵的数目

也越多，并且加密后密文的长度和明文的长度并不一致，从而使得暴力破解密钥矩阵更难，因此其上的 Hill 加密具有更高的安全性，适合大量数据的分组加密.

参考文献：

[1] 万福永，戴浩晖. Hill 2 密码体系加密过程中的哑元问题 [J]. 数学的实践与认识，2007，37(8)：87－90.

[2] 杨淑菊. Hill 密码的加密解密矩阵的求法 [J]. 价值工程，2016，35(26)：285－287.

[3] 徐小华，黎民英. Hill 密码加密解密时矩阵的求法 [J]. 电脑与信息技术，2010(02)：31－33.

[4] 王　容，廖群英，王云莹，等. Hill 加密算法的改进 [J]. 四川师范大学学报(自然科学版)，2015，38(1)：8－14.

[5] 付卫平，陈继业. 有限域 GF(2～n)的一种除法运算算法 [J]. 邵阳学院学报(自然科学版)，2015，12(2)：3－10.

[6] 蒲保兴，王伟平. 线性网络编码运算代价的估算与分析 [J]. 通信学报，2011，32(5)：47－55.

[7] 焦占亚，曾永莹，刘海峰. 一次一密的密码算法研究 [J]. 西安科技大学学报，2005，25(4)：477－480.

[8] 谢邦杰. 线性代数 [M]. 北京：人民教育出版社，1978.

[9] 王松桂，杨振海. 广义逆矩阵及其应用 [M]. 北京：北京工业大学出版社，1996.

[10] 张玉安，冯登国. 一种实用的仿一次一密分组加密方案 [J]. 北京邮电大学学报，2005，28(2)：101－104.

[11] 刘海峰，吴　鹏，马令坤. 基于有限域上圆锥曲线的分组加密算法及实现 [J]. 吉林大学学报(理学版)，2012，50(1)：54－58.

[12] 卢开澄. 计算机密码学：计算机网络中的数据保密与安全 [M]. 3 版. 北京：清华大学出版社，2003.

[13] 刘海峰，何立勇，郭改慧，等. Hill 密码体系中的加密矩阵与哑元 [J]. 西南大学学报(自然科学版)，2014，36(11)：138－142.

Hill Encryption Derivative Algorithm in Finite Field $GF(2^8)$ with High-Matrix as Key Matrix

LIU Hai-feng[1,2]，　LU Kai-yi[1]，　LIANG Xing-liang[2]

1. *College of Electrical and Information Engineering*, *Shannxi University of Science and Technology*, *Xi'an 710021*, *China*;
2. *College of Arts and Sciences*, *Shannxi University of Science and Technology*, *Xi'an 710021*, *China*

Abstract: In traditional Hill encryption algorithm, the modulo P multiplication of the invertible matrix and plaintext vector in finite field $GF(P)$ are used to calculate ciphertext vector. This paper proposes a new Hill encryption derivative algorithm in finite field $GF(2^8)$, which takes polynomial high-matrix as the key matrix. In this new Hill encryption derivative algorithm, plaintext vector is composed of the polynomial derived from the corresponding plaintext, a column of key matrix is selected as translation increment randomly modulo eighth degree irreducible polynomial $p(x)$ multiplication of the polynomial high-matrix and plaintext vector in finite field $GF(2^8)$ is done. Then modulo eighth degree irreducible polynomial $p(x)$ addition of the product and translation increment in finite field $GF(2^8)$ is carried out, thus the polynomial ciphertext vector is obtained, and the purpose of encrypting the plaintext messages is achieved. Because it is more difficult to get plaintext from ciphertext under the condition that eighth degree irreducible polynomial, key matrix and random selected translation vector are unknown, the new Hill encryption derivative algorithm in finite field $GF(2^8)$ improves the capability for anti-attack.

Key words: finite field $GF(2^8)$; Hill encryption; polynomial high-matrix; irreducible polynomial

责任编辑　张　枸