第 7 卷第 7 期
1996 年 7 月

软 件 学 报
JOURNAL OF SOFTWARE

Vol. 7, No. 7
Jul. 1996

$GF(q)$上置换多项式与函数的相关免疫性*

隆永红

(中国科学院软件研究所 北京 100080)

摘要 本文提出了$GF(q)$上(n,k)置换多项式的概念,建立了它与函数相关免疫性之间的联系,并研究了它们的性质.得到了$GF(q)$($q>2$)上一些特殊类型的函数是m阶和所有二次多项式是最大阶相关免疫的充分必要条件.证明了在$GF(q)$($q>4$)上存在非线性的具有最大阶相关免疫阶的函数,也给出了一种由低次数具有特定相关免疫阶的函数构造非线性次数高的同阶相关免疫函数的有效方法.

关键词 置换多项式,相关免疫,流密码,组合序列,滚动密钥生成器.

如图 1 所示的组合序列生成器在流密码设计中占有十分重要的地位.为了分析这种流密钥生成器 RKG(running key generator)抵抗相关性攻击[1]的能力,Siegenthaler[2]提出了组合序列的相关免疫性概念.就$GF(2)$的情形,人们对相关免疫函数的判定和构造进行了较为充分的研究[3~7],得到了一系列有价值的结果,如著名的 Xiao—Massey 引理和 Xiao—Massey 定理.[4]$GF(2)$上函数的相关免疫阶与函数的非线性次数之间存在十分强的制约关系.而高的相关免疫阶与高的线性复杂度又都是设计好的组合序列的重要指标.Rueppel[5]提出的有记忆的组合函数模型,如图 2 所示,虽然可以同时达到最大相关免疫阶和最高可能的线性复杂度,避免了不得以的折衷,但有时当$s_{j+1}=f_s(x_1,\cdots,x_n,s_j)$达到最大非线性阶时,比如,当$f_s(x_1,\cdots,x_n,s_j)=x_1,\cdots,x_ns_j$时,由$f_0(x_1,\cdots,x_n,s_j)=x_1+\cdots+x_n+s_j$组合出的序列与由$f'_0(x_1,\cdots,x_n)=x_1+\cdots+x_n$组合出的序列至多在$1/2^n$(期望值)的位置上值不同.事实上,此时的 Hamming 重量$w(f_0+\sum_i x_i)$远远小于2^{n-1},线性逼近攻击[6,7]可以对它构成威胁.研究多元流密码和在流密码中使用多元组合序列也许是解决上述矛盾的最有效的途径之一.因此,近几年,多元流密码得到了重视,如陶仁骐[8~10]提出的拉丁阵+m序列体制和 Anderson[11]提出的现代转轮密码都属于多元流密码的例子.同时,$GF(q)$上函数或任意多值逻辑函数的相关免疫性也得到了研究.[12,13]文献[14]研究了$GF(q^m)$上的m序列与$GF(q)$上m序列的关系,指出$GF(q^m)$上的m序列比$GF(q)$上m序列具有更好的自相关性.

过去,研究$GF(2)$上布尔函数相关免疫性的主要方法是 Walsh 谱方法和重量分析

* 本文研究得到国家自然科学基金资助.作者隆永红,1964 年生,副教授,主要研究领域为计算机软件,分布式数据库与密码学.

本文通讯联系人:隆永红,北京 100080,中国科学院软件研究所

本文 1995—04—03 收到修改稿

法.[3~7]文献[12,13]研究$GF(q)$上函数或任意多值逻辑函数的相关免疫性,使用的方法也是谱方法和重量分析法,显示了谱方法在理论上的有效性.但有些情况下,谱值的有效计算本身就是一个值得研究的问题,因此有必要寻找更为直接和显式的相关免疫性判别和相关免疫函数的构造方法.

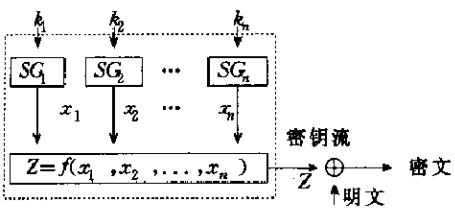

图1 无记忆组合流密钥生成器(RKG)的一般模型

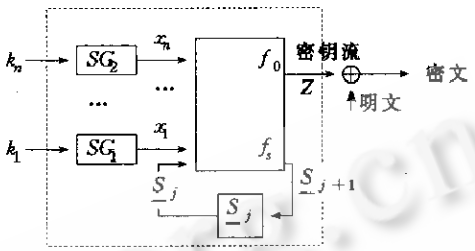

图2 有记忆组合流密钥生成器(RKG)的一般模型

为此,本文提出$GF(q)$上(n,k)置换多项式的概念,并研究了它与$GF(q)$上平衡函数(即置换多项式)相关免疫性之间的关系,将n元m阶相关免疫函数的判定转化为对(n,m)置换多项式的判定,期望为相关免疫函数的判定和构造开拓更多一条途径.特别地,我们研究了具有最大相关免疫阶的$GF(q)$上函数及其性质,得到了一些既区别于$GF(2)$情形,也不能直接从$GF(2)$上推广的结果.比如,在$GF(2)$上,具有最大相关免疫阶的函数必是线性函数,而在$GF(q)(q>2)$上则不然.本文结果也将表明,相关免疫阶与多项式非线性次数之间的制约关系在$GF(q)(q>2)$上也将以与$GF(2)$上截然不同的形式出现.此外,本文给出了一种方法可以方便地由低非线性次数函数构造具有同阶相关免疫性的高非线性次数函数,也给出了一些特殊类型的和所有二次n元多项式具有最大相关免疫阶的充要条件.

1　(n,k)置换多项式与组合序列的相关免疫性

用$GF(q)$表示q元有限域,$q=p^l$, p为素数,l为正整数.称系数取自$GF(q)$的含n个不定元的多项式$f(x_1,\cdots,x_n)$为$GF(q)$上n元多项式.用$GF^n(q)$表示n个$GF(q)$的笛卡儿积.

定义 1.1. $GF(q)$上n元多项式$f(x_1,\cdots,x_n)$称为一个n元置换多项式(PP),如果对任意$a\in GF(q)$,方程$f(x_1,\cdots,x_n)=a$在$GF^n(q)$中恰有q^{n-1}个解.[15]

有关置换多项式的理论和结果可查阅 Lidl 和 Niederreiter.[15]

首先我们引入(n,k)置换多项式的概念并讨论其有关性质,然后讨论它与组合序列的相关免疫性之间的关系.

定义 1.2. $GF(q)$上n元多项式$f(x_1,\cdots,x_n)$称为一个(n,k)置换多项式,如果对任意$i_1,\cdots,i_k$, $1\leqslant i_1<i_2<\cdots<i_k\leqslant n$和任意$a_1,\cdots,a_k\in GF(q)$,有$g(x_1,\cdots,x_{i_{1-1}},x_{i_{1+1}},\cdots,x_{i_{k-1}},x_{i_{k+1}},\cdots,x_n)=f(x_1,\cdots,x_{i_{1-1}},a_1,x_{i_{1+1}},\cdots,x_{i_{k-1}},a_k,x_{i_{k+1}},\cdots,x_n)$是$GF(q)$上$n-k$元置换多项式.

易证,$GF(q)$上(n,k)置换多项式具有下列性质.

定理 1.1. $GF(q)$上n元多项式$f(x_1,\cdots,x_n)$是一个(n,k)置换多项式当且仅当任给$i_1,\cdots,i_k$, $1\leqslant i_1<i_2<\cdots<i_k\leqslant n$和任意$a_1,\cdots,a_k$, $a\in GF(q)$,方程$f(x_1,\cdots,x_{i_{1-1}},a_1,x_{i_{1+1}},\cdots,x_{i_{k-1}},a_k,x_{i_{k+1}},\cdots,x_n)=a$在$GF^n(q)$中恰有$q^{n-k-1}$组解.

定理 1.2. 若$GF(q)$上n元多项式$f(x_1,\cdots,x_n)$是一个(n,k)置换多项式,则必有$0\leqslant k$

$<n$. 且当 $0<k<n$ 时，$f(x_1,\cdots,x_n)$也是一个$(n,k-1)$置换多项式.

下面讨论(n,k)置换多项式与组合序列的相关免疫性之间的关系.

总假定所考虑的组合序列生成器具有图1所示的结构.其中 SG_i, $i=1,\cdots,n$,为 n 个分支生成器.$f(x_1,\cdots,x_n)$为 $GF(q)$上 n 元多项式(这一假定不失一般性,因为 $GF(q)$上任意 n 元函数均可唯一地表示为一个具有简化次数的多项式).$+$为 $GF(q)$上加法运算.也总是假定图1中 n 个分支生成器所产生的序列是彼此独立且等概分布的 q 元序列.

与 $GF(2)$上情形类似,$GF(q)$上函数的相关免疫性概念可以叙述为

定义 1.3. 设 $z=f(x_1,\cdots,x_n)$为 $GF(q)$上 n 元随机变量函数.其中 $x_1,\cdots,x_n$ 为 $GF(q)$上 n 个彼此独立且等概分布的随机变量.称 f 是 m 阶相关免疫的当且仅当任给 $i_1,\cdots,i_m$, $1\leqslant i_1<i_2<\cdots<i_m\leqslant n$,$z$ 与 m 个随机变量 $x_{i_1},\cdots,x_{i_m}$统计独立,或者,当且仅当互信息 $I(z;x_{i_1},\cdots,x_{i_m})=0$.[2]

下面的定理建立了 m 阶相关免疫函数与(n,m)置换多项式之间的对应关系.虽然图1中的组合函数不一定是平衡的(即置换多项式),但在密码应用中,我们往往希望组合出的序列仍具有良好的伪随机性,其中包括 $GF(q)$中元素在序列中的等概分布性质.在本文的假设下,有且只有平衡的或置换函数具有这一性质.因此,仅讨论置换多项式的相关免疫性就足够了.

定理 1.3. 设 $f(x_1,\cdots,x_n)$是 $GF(q)$上 n 元置换多项式,m 是正整数,$1\leqslant m<n$,则 $f(x_1,\cdots,x_n)$是 m 阶相关免疫的当且仅当 $f(x_1,\cdots,x_n)$是一个(n,m)置换多项式.

证明:必要性.设 $f(x_1,\cdots,x_n)$是 $GF(q)$上 n 元置换多项式,且是 m 阶相关免疫的.由定义1.3,任意 $i_1,\cdots,i_m$, $1\leqslant i_1<i_2<\cdots<i_m\leqslant n$,互信息 $I(z;x_{i_1},\cdots,x_{i_m})=0$.即对任何 $a_1,\cdots,a_m\in GF(q)$, 有

$$prob\{f(x_1,\cdots,x_n)=a\mid x_{i_1}=a_1,\cdots,x_{i_m}=a_m\}=prob\{f(x_1,\cdots,x_n)=a\} \tag{1.1}$$

对任意 $a\in GF(q)$都成立.任给 $a\in GF(q)$, 用 $N(x_1,\cdots,x_n)$ 记 $f(x_1,\cdots,x_n)=a$ 在 $GF^n(q)$中的解的个数.(1.1)式等价于

$$N(x_1,\cdots,x_{i_1-1},a_1,x_{i_1+1},\cdots,x_{i_m-1},a_m,x_{i_m+1},\cdots,x_n)/q^{n-m}=q^{n-1}/q^n \tag{1.2}$$

或者

$$N(x_1,\cdots,x_{i_1-1},a_1,x_{i_1+1},\cdots,x_{i_m-1},a_m,x_{i_m+1},\cdots,x_n)=q^{n-m-1} \tag{1.3}$$

从而 $f(x_1,\cdots,x_{i_1-1},a_1,x_{i_1+1},\cdots,x_{i_m-1},a_m,x_{i_m+1},\cdots,x_n)=a$ 在 $GF^n(q)$中恰有 q^{n-m-1}组解.由定理1.1,$f(x_1,\cdots,x_{i_1-1},a_1,x_{i_1+1},\cdots,x_{i_m-1},a_m,x_{i_m+1},\cdots,x_n)$是 $GF(q)$上(n,m)置换多项式.

充分性.设 $f(x_1,\cdots,x_n)$是一个(n,m)置换多项式,$1\leqslant m<n$.注意到充分证明中各步均是可逆的,不难得出 $f(x_1,\cdots,x_n)$是 m 阶相关免疫的.

推论 1.1. $GF(q)$上 n 元置换多项式 $f(x_1,\cdots,x_n)$具有最大相关免疫阶 $n-1$ 的充分必要条件是 $f(x_1,\cdots,x_n)$是$(n,n-1)$置换多项式.

在 $GF(2)$上,$(n,n-1)$置换多项式仅 $f(x_1,\cdots,x_n)=a+x_1+x_2+\cdots+x_n$,$a=0$ 或 1 这2个,这与 Xiao−Massey[4]中的结论是一致的.但我们将看到,当 $q>4$ 时,存在非线性的$(n,n-1)$置换多项式.

2 $GF(q)$上(n,k)置换多项式和函数相关免疫性判定的一些结果

引理 2.1. 若 $f(x_1,\cdots,x_n)$是一个 $GF(q)$上 n 元多项式,且形如

$$f(x_1,\cdots,x_n)=g(x_1,\cdots,x_m)+h(x_{m+1},\cdots,x_n)$$

$1\leqslant m<n$, 则当 g 和 h 中至少有一个是置换多项式时,$f(x_1,\cdots,x_n)$必是 $GF(q)$上置换多项式.[15]

称 $GF(q)$上 n 元多项式 $f(x_1,\cdots,x_n)$是 x_i 的置换,如果任意固定 $x_1,\cdots,x_{i-1},x_{i+1},\cdots,x_n$ 为 $GF(q)$中值分别为 $\alpha_1,\cdots,\alpha_{i-1},\alpha_{i+1},\cdots,\alpha_n\in GF(q)$, $f(\alpha_1,\cdots,\alpha_{i-1},x_i,\alpha_{i+1},\cdots,\alpha_n)$看作 x_i 的函数构成 $GF(q)$到自身的一一映射. 容易证明,

引理 2.2. 若 $f(x_1,\cdots,x_n)$是一个 $GF(q)$上 n 元多项式,且形如

$$f(x_1,\cdots,x_n)=g(x_1,\cdots,x_m)+h(x_{m+1},\cdots,x_n)$$

$1\leqslant m<n$, 则 $f(x_1,\cdots,x_n)$是 x_i 的置换,且 $m<i<n+1$, 当且仅当 $h(x_{m+1},\cdots,x_n)$是 x_i 的置换;$f(x_1,\cdots,x_n)$是 x_i 的置换,且 $0<i<m+1$, 当且仅当 $g(x_1,\cdots,x_m)$是 x_i 的置换.

定理 2.1. 设 $f_1(x),\cdots,f_n(x)$是 $GF(q)$上置换多项式,$a_1,\cdots,a_n,a\in GF(q)$. 那么

$$f(x_1,\cdots,x_n)=a+\sum_{i=1}^{n}a_if_i(x_i)$$

为(n,k)置换多项式的充分必要条件是存在 $i_1,\cdots,i_{k+1}$, $1\leqslant i_1<\cdots<i_{k+1}\leqslant n$,使得 $a_{i1}\cdots a_{ik+1}$非零.

证明:充分性. 由引理 2.1 是显然的.

必要性. 用反证法. 若 $a_1,\cdots,a_n$ 中非零元素个数小于 $k+1$,不妨设非零元均在$\{a_1,\cdots,a_k\}$中,则有

$$f(x_1,\cdots,x_n)=a+\sum_{i=1}^{k}a_if_i(x_i)$$

此时若固定 $x_1,\cdots,x_k$ 为 $a_1,\cdots,a_k\in GF(q)$, 则

$$f(a_1,\cdots,a_k,x_{k+1},\cdots,x_n)=a+\sum_{i=1}^{n}a_if_i(a_i)$$

为常数,而非置换多项式. 与 $f(x_1,\cdots,x_n)$是(n,k)置换多项式相矛盾. 故 $a_1,\cdots,a_n$ 中非零元素个数必大于或等于 $k+1$. 定理即证.

推论 2.1. 设 $f_i(x)$同上,$a_1,\cdots,a_n,a\in GF(q)$,$a+\sum_{i=1}^{n}a_if_i(x_i)$是 $GF(q)$上$(n,n-1)$ 置换多项式的充分必要条件是所有 a_i,$1\leqslant i\leqslant n$, 非零.

定理 2.2. 若 q 为奇数且 $n\geqslant 2$, 则 $GF(q)$上任何次数不超过 2 的 $f(x_1,\cdots,x_n)$为$(n,n-1)$ 置换多项式的充分必要条件是 $f(x_1,\cdots,x_n)=c_0+c_1x_1+c_2x_2+\cdots+c_nx_n,c_i\in GF(q)\backslash\{0\}$, $i=0,1,2,\cdots,n$.

证明:充分性. 显然. 下证必要性. 先证若 $f(x_1,\cdots,x_n)$是 x_1 的置换,则必有 $f(x_1,\cdots,x_n)=c_1x_1+f_0(x_2,\cdots,x_n)$,$c_1\in GF(q)$非零. 因为 $f(x_1,\cdots,x_n)$次数不超过 2,所以 $f(x_1,\cdots,x_n)$可写成如下形式

$$f(x_1,\cdots,x_n)=bx_1^2+c_1x_1+c'_2x_1x_2+\cdots+c'_nx_1x_n+f_0(x_2,\cdots,x_n)$$

其中 $c_1,c'_2,\cdots,c'_n\in GF(q)$，$f_0(x_2,\cdots,x_n)$是 $GF(q)$上次数不超过 2 的关于变元 $x_2,\cdots,x_n$ 的多项式. 由假设，$f(x_1,\cdots,x_n)$是 x_1 的置换，则 $h(x_1)=f(x_1,0,\cdots,0)=bx_1^2+c_1x_1+\tau,\tau\in GF(q)$，是 $GF(q)$上置换. 若 $b\neq 0$，则对 $c_1=0$ 有 $h(x_1)=h(-x_1)$，而 $c_1\neq 0$ 时有 $h(0)=h(-c_1/b)$. 因此 b 必为 0. 又因 $f(x_1,0,\cdots,0)$是 $GF(q)$上置换，故必有 $c_1\neq 0$. 若 $c'_2,\cdots,c'_n$ 中某个 $c'_i\neq 0$，则可选取 $\alpha_2,\cdots,\alpha_n\in GF(q)$满足 $c'_2\alpha_2+\cdots+c'_n\alpha_n=-c_1$，使得 $f(x_1,\alpha_2,\cdots,\alpha_n)=f_0(\alpha_2,\cdots,\alpha_n)$是常数，而非置换. 因此 $c'_2,\cdots,c'_n$ 必全为零. 故若 $f(x_1,\cdots,x_n)$是 x_1 的置换，则必有 $f(x_1,\cdots,x_n)=c_1x_1+f_0(x_2,\cdots,x_n)$，$c_1\in GF(q)$，非零.

又由引理 2.2，$f(x_1,\cdots,x_n)=c_1x_1+f_0(x_2,\cdots,x_n)$是 x_2 的置换当且仅当 $f_0(x_2,\cdots,x_n)$是 x_2 的置换，从而存在 $c_2\neq 0,c_2\in GF(q)$使得 $f_0(x_2,\cdots,x_n)=c_2x_2+f_1(x_3,\cdots,x_n)$，且 $f_1(x_3,\cdots,x_n)$ 次数不超过 2. 依次类推，即可证得：若 $f(x_1,\cdots,x_n)$是 $(n,n-1)$置换多项式，则必有

$$f(x_1,\cdots,x_n)=c_0+c_1x_1+c_2x_2+\cdots+c_nx_n,\ c_i\in GF(q)\backslash\{0\},i=0,1,2,\cdots,n.$$

定理即证.

定理 2.3. 若 q 为偶数且 $n\geqslant 2$，则次数不超过 2 的 n 元多项式 $f(x_1,\cdots,x_n)$为 $(n,n-1)$置换多项式的充分必要条件是

$$f(x_1,\cdots,x_n)=c_0+\sum_{i=1}^{n}c_ix_i^{d_i},c_0,c_i\in GF(q)\backslash\{0\},d_i\in\{1,2\},\ i=1,2,\cdots,n.$$

证明：与定理 2.3 类似，不赘述.

引理 2.3. 若 $f(x_1,\cdots,x_n)$是 $GF(q)$上置换多项式，k 是正整数，且 $gcd(k,q-1)=1$，则 f^k 也是 $GF(q)$上置换多项式.[15]

定理 2.4. 若 $f(x_1,\cdots,x_n)$是 $GF(q)$上 (n,m)置换多项式，k 是正整数，且 $gcd(k,q-1)=1$，则 f^k 也是 $GF(q)$上 (n,m)置换多项式.

与定理 2.1～2.4 相对应，有

定理 2.1′. 设 $f_i(x)$同定理 2.1，$1\leqslant i\leqslant n$，则对任何 $a,a_1,\cdots,a_n\in GF(q)$，

$$f(x_1,\cdots,x_n)=a+\sum_{i=1}^{n}a_if_i(x_i)$$

为 k 阶相关免疫函数的充分必要条件是存在 $i_1,\cdots,i_{k+1},1\leqslant i_1<\cdots<i_{k+1}\leqslant n$，使得 $a_{i_1},\cdots,a_{i_{k+1}}$非零.

定理 2.2′. 若 q 为奇数且 $n\geqslant 2$，则 $GF(q)$上任何次数不超过 2 的置换多项式 $f(x_1,\cdots,x_n)$ 具有最大相关免疫阶 $n-1$ 的充分必要条件是

$$f(x_1,\cdots,x_n)=c_0+c_1x_1+c_2x_2+\cdots+c_nx_n,c_i\in GF(q)\backslash\{0\},i=0,1,2,\cdots,n.$$

定理 2.3′. 若 q 为偶数且 $n\geqslant 2$，则次数不超过 2 的 $GF(q)$上 n 元置换多项式 $f(x_1,\cdots,x_n)$ 具有最大相关免疫阶 $n-1$ 的充分必要条件是

$$f(x_1,\cdots,x_n)=c_0+\sum_{i=1}^{n}c_ix_i^{d_i},c_0,c_i\in GF(q)\backslash\{0\},d_i\in\{1,2\},i=1,2,\cdots,n.$$

定理 2.4′. 设 $f(x_1,\cdots,x_n)$是 $GF(q)$上 n 元置换多项式，k 是正整数，且 $gcd(k,q-1)=1$，则如果 $f(x_1,\cdots,x_n)$是 m 阶相关免疫的，那么 f^k 也是 m 阶相关免疫的.

此定理一方面表明，可以由低次数具有特定相关免疫阶的函数构造非线性次数高的同

阶相关免疫函数;另一方面也表明,在$GF(q)$上,相关免疫阶与函数的非线性次数不再受形如$k+m<n$的关系的制约,其中k,m和n分别代表函数的非线性次数、相关免疫阶和变元的个数.

3 讨　论

考虑到置换多项式的判定和构造已有相当广泛且比较成熟的研究结果,本文提出(n,k)置换多项式的概念,并建立它与相关免疫性概念之间的联系,期望为一般有限域上相关免疫函数的判定和构造寻求更多一条途径.从本文的讨论可以看出,一般有限域上的相关免疫性的结果比$GF(2)$上要丰富得多.在此,我们得到了$GF(q)(q>2)$上一些特殊类型的函数是m阶和所有二次多项式是最大阶相关免疫的充分必要条件,证明了在$GF(q)(q>4)$上存在非线性的具有最大阶相关免疫的函数,也给出了一种由低次数具有特定相关免疫阶的函数构造非线性次数高的同阶相关免疫函数的有效方法.利用有关置换多项式的已知结果,还可以得到一些有意义的结论.但是,仍然有许多问题尚未解决,如更一般类型的(n,k)置换多项式的显式判别和计数问题,相关免疫阶与函数非线性次数之间的具体制约关系(或相关免疫阶的可达性问题)等等,都是有待解决的.

致谢　作者非常感谢陶仁骐教授和陈世华教授的悉心指导.

参考文献

1 Siegenthaler T. Decrypting a class of stream ciphers using ciphertext only. IEEE Trans. Computer, C-34, 1985, (4):81~85.

2 Siegenthaler T. Correlation immunity of nonlinear combining functions for cryptographic applications. IEEE Trans. Inform. Theory, IT-30, 1984, (10):776~780.

3 肖国镇.非线性生成器相关分析研究的频谱方法.电子学报,1986,14(4):78~84.

4 Xiao G Z, Massey J L. A spectral characterization of correlation-immune combining functions. IEEE Trans. Inform. Theory, IT-34, 1988, (3):569~571.

5 Ruepple R A. Analysis and design of stream ciphers. Berlin: Springer-Verlag, 1986.

6 杨义先,林须端.编码密码学.北京:人民邮电出版社,1992.

7 王育明,何大可.保密学-基础与应用.西安:西安电子科技大学出版社,1990.

8 陶仁骐,陈世华.关于无误差传播密码体制.第3次全国密码学会议会议录,1988.

9 陶仁骐.(4,4)-拉丁阵在密码设计上的一种应用.计算机学报,1991,(6):423~431.

10 Tao R. On finite automata one-key cryptosystems. Cambridge Security Workshop, 9~11 Dec. 1993. LNCS no. 809, 135~148.

11 Anderson R. Modern rotormachine (extended abstract). Cambridge Security Workshop, 9~11 Dec. 1993. 47~50.

12 罗群.$GF(q)$上多项式函数的相关免疫性.密码与信息,1993,(2):23~31.

13 李世取,曾本胜.多值逻辑函数相关免疫性的充分必要条件.密码学进展-CHIANCRIPT'94.北京:科学出版社,1994.

14 Park W J JR., Komo J J. Relationships between m sequences over $GF(q)$ and $GF(q^m)$. IEEE Trans. Inform. Theory, IT-34, 1989, (1):183~186.

15 Lidl R, Niederreiter H. Finite fields, encyclopedia of mathematics and applications. Reading, MA: Addison

—Wesley, 1983.

16 曾肯成,吕述望,杨君辉. 相关免疫缺陷与复合序列的攻击. 密码学进展—CHIANCRIPT'92. 北京:科学出版社, 1992.

17 隆永红. 拉丁阵与置换多项式及其在双无序列密码中的应用[博士论文]. 中国科学院软件研究所,1996.

PERMUTATION POLYNOMIALS AND CORRELATION IMMUNITY OF FUNCTIONS OVER $GF(q)$

Long Yonghong

(*Institute of Software The Chinese Academy of Sciences Beijing* 100080)

Abstract The concept of (n,k) permutation polynomial over $GF(q)$ is first introduced. The properties of (n,k) permutation polynomials and the relation to k^{th} order correlation immune functions have been studied. Sufficient and necessary conditions are proved for some special n—ary functions to be $m^{th}(m<n)$ order correlation immune and all functions with degree no greater than 2 to be $(n-1)^{th}$ order correlation immune. The results show that over $GF(q)(q>4)$ are there nonlinear functions of highest possible correlation immunity order. An efficient method is put forward to construct functions of high nonlinearity from those of lower nonlinearity with the same correlation immunity order.

Key words Permutation polynomial, correlation immunity, stream cipher, combination sequence, RKG(running key generator).