一类 k 阶拟 Bent 函数密码性质的矩阵特征

滕吉红 张文英 李世取 黄晓英

(解放军信息工程大学信息工程学院信息研究系 郑州 450002)

摘 要 由于非线性组合函数的密码性质通常可以由函数的 Walsh 谱和自相关函数来刻划,因而对函数的密码性质的分析通常要计算大量的 Walsh 循环谱值和自相关函数值来验证. 该文利用一类 k 阶拟 Bent 函数的特殊性质,把对这类函数的密码性质的研究转化为对矩阵性质的研究,如平衡性、相关免疫性、扩散性、最高代数次数等. 这种转化避开了大量的计算,同时为构造密码性质好的 k 阶拟 Bent 函数提供了一种更为简洁且易于实现的方法.

关键词 部分 Bent 函数;k 阶拟 Bent 函数;特征矩阵;相关免疫性;代数次数

中图法分类号 TN918

The Matrix Characteristics of the Cryptographic Properties of a Special Kind of k-Order Quasi-Bent Functions

TENG Ji-Hong ZHANG Wen-Ying LI Shi-Qu HUANG Xiao-Ying

(*Department of Information Research, The PLA Information Engineering University, Zhengzhou* 450002)

Abstract In this paper, the cryptographic properties of a special kind of k-order quasi-Bent functions are studied by a new kind of method, which is denoted by the matrix method. The cryptographic properties of the k-order quasi-Bent functions, such as balancedness, correlation immunity, propagation criterion and the highest algebraic degree can all be easily decided only by the distributions of 0 and 1 in the character matrix, which is different from the spectrum method and the auto-correlation method. The method proposed here can also be used to construct the k-order quasi-Bent functions with good cryptographic properties, which is more effective and much simpler than the spectrum method and can be carried out easily.

Keywords partially-Bent function; k-order quasi-Bent functions; characteristic matrix; correlation immunity; algebraic degree

1 引 言

通信保密的实现方法之一是对需要发送的明文进行加密,其安全性在很大程度上取决于生成密钥流序列的非线性组合器的安全性. 目前根据不同的攻击方法,判定非线性组合器的安全性有一系列标准,如非线性组合函数必须有高的代数次数、高的非线性度,有一定阶的相关免疫性和一定次数的扩散性等等.

依据上面的准则,密码设计者设计了大量的非线性组合函数,但由于这些准则之间存在着一定的制约关系[1~3],因此要设计出兼顾各种性质的非线性组合函数有一定难度. 其中,Bent 函数[4]是一类

收稿日期:2003-04-17;修改稿收到日期:2003-07-15.**滕吉红**,女,1974 年生,博士,讲师,主要研究方向为概率统计在密码学中的应用. E-mail: tengjihong@263.net. **张文英**,女,1970 年生,博士研究生,讲师,主要研究方向为概率统计在密码学中的应用. **李世取**,男,1945 年生,教授,博士生导师,主要研究方向为密码学. **黄晓英**,女,1962 年生,博士,副教授,主要研究方向为密码学.

特殊的非线性组合函数,它的非线性度达到最大,稳定性强,因此无论是在密码设计还是通信领域中都有广泛的应用. 但这类函数不具有平衡性和相关免疫性,为了弥补 Bent 函数的这一不足,1992 年,Carlet 提出了部分 Bent 函数[5]的概念,这类函数可以具有平衡性、相关免疫性和一定次数的扩散性,但所有非仿射的部分 Bent 函数都可以通过 Bent 函数来构造[6],因此,它的某些性质也受到了限制. 后来,李世取教授等提出了 k 阶拟 Bent 函数的概念[7],它是包含 Bent 函数和部分 Bent 函数的更大的函数类. 它可以具有 Bent 函数所不具有的密码学性质:如平衡性、相关免疫性等. 我们发现澳大利亚学者给出的可变长 Hash 算法——HAVAL 标准算法[8]中所选择的密码函数无一例外都是 7 元 1 阶拟 Bent 函数,因此这类函数具有理论意义和应用价值,所以有必要对这类函数的密码性质进行深入的研究,如平衡性、相关免疫性、扩散性等. 由于密码函数的平衡性、相关免疫性和非线性度都可以通过它的 Walsh 谱来刻划[1,2],而密码函数的扩散性与它的自相关函数有关[1,3],因此目前判定一个密码函数是否满足前面所提出的密码准则主要是通过计算大量的 Walsh 循环谱值和自相关函数值来验证的. 本文用不同的方法对一类特殊的 k 阶拟 Bent 函数的密码性质进行了分析. 我们的研究结果表明,对这类 k 阶拟 Bent 函数的密码学性质的研究几乎完全可以转化为对 $GF(2)$ 上的一类矩阵的研究,如相关免疫性、扩散性、代数次数等,这种转化从另外的角度给出了一种密码函数的设计方法,当变元个数较少时,易于通过计算机编程实现.

2 基本定义和结论

文献[1,3]用 Walsh 循环谱和自相关函数给出了函数具有 m 阶相关免疫性和满足 l 次扩散准则的定义.

定义 1[1]. 称 $f(x),x\in GF^n(2)$具有 m 阶相关免疫性,如果对任意的 $w\in GF^n(2)$,且 $1\leq W(w)\leq m$,都有

$$S_{(f)}(w)=\frac{1}{2^n}\sum_{w\in GF^n(2)}(-1)^{f(x)+w\cdot x}=0.$$

定义 2[3]. 称 $f(x),x\in GF^n(2)$满足 l 次扩散准则,如果对任意的 $s\in GF^n(2)$, $1\leq W(s)\leq l$, $f(x)$的自相关函数

$$r_f(s)=\frac{1}{2^n}\sum_{x\in GF^n(2)}(-1)^{f(x+s)+f(x)}=0.$$

特别地,当 $l=1$ 时,称 $f(x)$满足严格雪崩准则.

称$GF^n(2)$中使得 $f(x)$取值为 1 的点的个数为 $f(x)$的重量.

李世取教授等在文献[7]中给出了 k 阶拟 Bent 函数的定义如下.

定义 3[7]. 称 $f(x),x\in GF^n(2)$为 k 阶拟 Bent 函数,如果对任意 $w\in GF^n(2)$, $f(x)$的 Walsh 循环谱满足 $S^2_{(f)}(w)=0$ 或 $\frac{1}{2^{n-k}}$.

特别地,当 $k=0$ 时,n 元 k 阶拟 Bent 函数即为 Rothaus 提出的 Bent 函数;当 $k=1$ 时,n 元 k 阶拟 Bent 函数即为胡磊提出的半 Bent 函数[9].

定理 1. 设 $f(x),x\in GF^n(2)$为 k 阶拟 Bent 函数,则 $f(x)$的代数次数不超过$\frac{n-k}{2}+1$.

证明. 设 $f(x)$的代数标准形如下:

$$f(x)=a_0+\sum_{r=1}^{n}\sum_{1\leq i_1<\cdots<i_r<n}a_{i_1i_2\cdots i_r}x_{i_1}x_{i_2}\cdots x_{i_r},$$

记

$$S_{i_1\cdots i_r}=\{x=(x_1,x_2,\cdots,x_n):x_j=0,j\neq i_1,\cdots,i_r\},$$
$$\overline{S}_{i_1\cdots i_r}=\{x=(x_1,x_2,\cdots,x_n):x_j=0,j=i_1,\cdots,i_r\}.$$

而

$$\begin{aligned}a_{i_1\cdots i_r}&=\sum_{x\in S_{i_1\cdots i_r}}f(x)(\mathrm{mod}2)\\&=\sum_{x\in S_{i_1\cdots i_r}}\sum_{w\in GF^n(2)}S_f(w)(-1)^{w\cdot x}(\mathrm{mod}2),\end{aligned}$$

再由 Walsh 循环谱和线性谱的关系知:

$$\begin{aligned}a_{i_1\cdots i_r}&=(2^{r-1}-2^{r-1}\sum_{w\in\overline{S}_{i_1\cdots i_r}}S_{(f)}(w))(\mathrm{mod}2)\\&=-2^{r-1}\sum_{w\in\overline{S}_{i_1\cdots i_r}}S_{(f)}(w)(\mathrm{mod}2).\end{aligned}$$

由上式和 k 阶拟 Bent 函数的谱特征易知,当 $r>\frac{n-k}{2}+1$ 时,$a_{i_1\cdots i_r}=0$,所以 $f(x)$的代数次数不超过$\frac{n-k}{2}+1$. 证毕.

文献[7]还给出了一类 k 阶拟 Bent 函数的构造方法.

引理 1[7]. 设$f(x,y),x\in GF^r(2),y\in GF^{r+k}(2)$为 $2r+k$ 元布尔函数,$f(x,y)$定义如下:

$$f(x,y)=\pi(x)\cdot y+g(x) \tag{1}$$

其中$\pi(x)=(\phi_1(x),\cdots,\phi_{r+k}(x))$,$\phi_i(x)(1\le i\le r+k)$为 r 元布尔函数,$g(x)$也是 r 元布尔函数,则 $f(x,y)$为 k 阶拟 Bent 函数的充分必要条件是 $\pi(x)$为 $GF^r(2)$到$GF^{r+k}(2)$的单射.

引理 1 所给出的 k 阶拟 Bent 函数具有如下的谱特征和自相关特征:

引理 2[7]. 设 $f(x,y)$是如式(1)所定义的 k 阶拟 Bent 函数,则对任意的 $w\in GF^r(2)$,$v\in GF^{r+k}(2)$,都有

$$S_{(f)}(w,v)=\begin{cases}0, & \text{若 } v\notin\{\pi(x):x\in GF^r(2)\}\\ \frac{1}{2^r}(-1)^{g(x_0)+w\cdot x_0}, & \text{若存在唯一 } x_0,\text{使得 } \pi(x_0)=v\end{cases}.$$

定理 2. 设 $f(x,y)$是如式(1)所定义的 k 阶拟 Bent 函数,则对任意 $s_1\in GF^r(2)$,$s_2\in GF^{r+k}(2)$,都有

$$r_f(s_1,s_2)=\begin{cases}0, & s_1\neq 0\\ \frac{1}{2^r}\sum\limits_{x\in GF^r(2)}(-1)^{\pi(x)\cdot s_2}, & s_1=0\end{cases}.$$

证明. 对任意的 $s_1\in GF^r(2)$,$s_2\in GF^{r+k}(2)$,有

$$\begin{aligned}r_f(s_1,s_2)&=\frac{1}{2^{2r+k}}\sum_{x\in GF^r(2),y\in GF^{r+k}(2)}(-1)^{\pi(x+s_1)\cdot(y+s_2)+g(x+s_1)+\pi(x)\cdot y+g(x)}\\&=\frac{1}{2^{2r+k}}\sum_{x\in GF^r(2)}(-1)^{\pi(x+s_1)s_2+g(x+s_1)+g(x)}\sum_{y\in GF^{r+k}(2)}(-1)^{(\pi(x+s_1)+\pi(x))\cdot y}\\&\overset{\text{正交性}}{=}\begin{cases}0, & s_1\neq 0\\ \frac{1}{2^r}\sum\limits_{x\in GF^r(2)}(-1)^{\pi(x)\cdot s_2}, & s_1=0\end{cases}.\end{aligned}$$

证毕.

3 k 阶拟 Bent 函数密码性质的矩阵特征

为了方便,我们分别以引理 1 中 $\pi(x)=(\phi_1(x),\cdots,\phi_{r+k}(x))$的所有项为行向量作矩阵

$$\boldsymbol{E}=\begin{pmatrix}\phi_1(x^{(0)}) & \phi_2(x^{(0)}) & \cdots & \phi_{r+k}(x^{(0)})\\ \phi_1(x^{(1)}) & \phi_2(x^{(1)}) & \cdots & \phi_{r+k}(x^{(1)})\\ \vdots & \vdots & & \vdots\\ \phi_1(x^{(2^r-1)}) & \phi_2(x^{(2^r-1)}) & \cdots & \phi_{r+k}(x^{(2^r-1)})\end{pmatrix}$$

称 $\boldsymbol{E}$ 为 $\pi(x)$的特征矩阵,其中 $x^{(i)}$,$0\le i\le 2^r-1$ 为 i 的二进制表示. $\boldsymbol{E}$ 的各列恰好是映射 $\pi(x)$相应分量函数的真值表.

定理 3. 设 $f(x,y)$是形如式(1)的布尔函数,则 $f(x,y)$是 k 阶拟 Bent 函数的充分必要条件是 $\pi(x)$的特征矩阵 $\boldsymbol{E}$ 中没有相同的行向量.

证明. 由引理 1 知,$f(x,y)$是 k 阶拟 Bent 函数当且仅当 $\pi(x)$是$GF^r(2)$到$GF^{r+k}(2)$的单射,当且仅当 $\pi(x)$的特征矩阵 $\boldsymbol{E}$ 中没有相同的行向量.

证毕.

下面如无特别说明,$\pi(x)$的特征矩阵 $\boldsymbol{E}$ 中都没有相同的行向量,即 $f(x,y)$都是形如式(1)的 k 阶拟 Bent 函数.

我们的研究结果表明,形如式(1)的 k 阶拟 Bent 函数的密码性质在一定程度上是由 $\pi(x)$的特征矩阵所决定的,如平衡性、相关免疫性,扩散性,以及代数次数等.

定理 4. 设 $f(x,y)$,$x\in GF^r(2)$,$y\in GF^{r+k}(2)$是形如式(1)的 k 阶拟 Bent 函数,则 $f(x,y)$平衡的充要条件是 $\pi(x)$的特征矩阵 $\boldsymbol{E}$ 中不存在全 0 的行向量.

证明. $f(x,y)$平衡的充要条件是对任意的 $\overline{0}\in GF^r(2)$,$\overline{0}'\in GF^{r+k}(2)$,$S_{(f)}(\overline{0},\overline{0}')=0$,再由引理 2知 $S_{(f)}(\overline{0},\overline{0}')=0$ 当且仅当$\overline{0}'\notin\{\pi(x):x\in GF^{r+k}(2)\}$,当且仅当 $\pi(x)$的特征矩阵 $\boldsymbol{E}$ 中不存在全 0 的行向量.

证毕.

定理 5. 设 $f(x,y)$,$x\in GF^r(2)$,$y\in GF^{r+k}(2)$是形如式(1)的 k 阶拟 Bent 函数,则 $f(x,y)$具有 l 阶相关免疫性的充要条件是 $\pi(x)$的特征矩阵 $\boldsymbol{E}$ 中任意行向量中 1 的个数要大于 l.

证明. 由定义 1 知,$f(x,y)$具有 l 阶相关免疫性的充要条件是对任意的 $w\in GF^r(2)$以及 $v\in GF^{r+k}(2)$,且 $1\le W(w,v)\le l$,有 $S_{(f)}(w,v)=0$,而由引理 2 知 $S_{(f)}(w,v)=0$ 的充分必要条件是 $v\notin\{\pi(x):x\in GF^r(2)\}$,即 v 不在 $\boldsymbol{E}$ 的行向量中.

证毕.

定理 6. 设 $f(x,y)$,$x\in GF^r(2)$,$y\in GF^{r+k}(2)$是形如式(1)的 k 阶拟 Bent 函数,则 $f(x,y)$满足 l 次扩散准则的充要条件是 $\pi(x)$的特征矩阵 $\boldsymbol{E}$ 中任意 $s(1\le s\le l)$列的和所得到的列向量中 0,1 的个数

相等.

证明. 由定义 2 知,$f(x,y)$满足 l 次扩散准则的充要条件是对任意的 $s_1 \in GF^r(2), s_2 \in GF^{r+k}(2)$,且 $1 \leq W(s_1,s_2) \leq l, r_f(s_1,s_2)=0$,而由定理 2 可知,$r_f(0,s_2)=0$ 的充要条件是 $\pi(x)$的特征矩阵 $\boldsymbol{E}$ 中任意 $s(1 \leq s \leq l)$列的和所得到的列向量中 0,1 的个数相等. 证毕.

定理 7. 设 $f(x,y), x \in GF^r(2), y \in GF^{r+k}(2)$是形如式(1)的 k 阶拟 Bent 函数,则 $f(x,y)$能达到最高代数次数的充要条件是 $\pi(x)$的特征矩阵 $\boldsymbol{E}$ 中存在某个列向量,其中 1 的个数为奇数.

证明. 因为 $\boldsymbol{E}$ 中的每一列都是映射 $\pi(x)$相应分量函数 $\phi_i(x)(1 \leq i \leq r+k)$的真值表,则由定理 1 和 $f(x,y)$的形式知,$f(x,y)$能达到最高代数次数 $\frac{n-k}{2}+1$(此处 $n=2r+k$)的充要条件是存在某个函数 $\phi_i(x)$,其代数次数为 $\frac{n-k}{2}=r$,即 $\phi_i(x)$达到 r 元函数所能达到的最高代数次数,而 r 元函数达到最高代数次数的充要条件是 $\phi_i(x)$的重量为奇数,即其真值表中 1 的个数为奇数,因此 $\boldsymbol{E}$ 中存在某个列向量,其中 1 的个数为奇数. 证毕.

定理 8. 设 $f(x,y), x \in GF^r(2), y \in GF^{r+k}(2)$是形如式(1)的 k 阶拟 Bent 函数,则 $f(x,y)$的代数标准型中具有最高次数的项数至多为 $r+k$ 项,此时 $\pi(x)$的特征矩阵 $\boldsymbol{E}$ 中任意的列向量中 1 的个数为奇数,而且 $f(x,y)$的最高次项中都含有乘积 $x_1 x_2 \cdots x_r$.

证明. 当 $\pi(x)$的特征矩阵 $\boldsymbol{E}$ 中任意列向量中 1 的个数为奇数时,对任意的 $1 \leq i \leq r+k$,$\phi_i(x)$都能达到最高代数次数 r 次,即 $\phi_i(x)(1 \leq i \leq r+k)$的代数标准型中都有单项式 $x_1 x_2 \cdots x_r$,此时 $f(x,y)$的最高次项的次数为 $r+1$ 次,且它们分别为 $x_1 x_2 \cdots x_r y_i (1 \leq i \leq r+k)$,总共有 $r+k$ 项. 证毕.

推论 1. 设 $f(x,y), x \in GF^r(2), y \in GF^{r+k}(2)$是形如式(1)的 k 阶拟 Bent 函数,且 $r \geq 2$,若 $f(x,y)$满足严格雪崩准则,则 $f(x,y)$的代数次数不超过 r 次,即不存在形如式(1)的代数次数为 $r+1$ 的满足严格雪崩准则的函数.

证明. 由定理 6 知 $f(x,y)$满足严格雪崩准则的充要条件是 $\pi(x)$的特征矩阵 $\boldsymbol{E}$ 中任意列向量中 0,1 的个数相等,即 $\pi(x)$的特征矩阵 $\boldsymbol{E}$ 中任意列向量中 1 的个数为偶数,再由定理 7 知 $f(x,y)$不可能达到最高代数次数. 证毕.

4 结束语

我们将一类 k 阶拟 Bent 函数的密码学性质的研究问题转化为对矩阵性质的研究,根据矩阵的性质可以判定函数是否具有某些密码学性质,如平衡性、相关免疫性、扩散性以及最高代数次数等. 同时也提供了一种构造具有某些特殊密码性质的布尔函数的方法. 而当函数的变元比较少时,利用矩阵构造函数可以通过编程实现.

参 考 文 献

1 Ding Cun-Sheng, Xiao Guo-Zhen. Stream Cipher and Its Application. Beijing: Military Industry Press, 1994(in Chinese)
(丁存生, 肖国镇. 流密码学及其应用. 北京:国防工业出版社, 1994)

2 Feng Deng-Guo. Spectrum theory and its application in the technology of communications secret[Ph. D. dissertation]. Xi'an: Xidian University, 1995(in Chinese)
(冯登国. 频谱理论及其在通信保密技术中的应用[博士学位论文]. 西安: 西安电子科技大学, 1995)

3 Feng Deng-Guo, Pei Ding-Yi. The Introduction of Cryptology. Beijing: Science Press, 1999(in Chinese)
(冯登国, 裴定一. 密码学导引. 北京:科学出版社,1999)

4 Rothaus O. S.. On Bent functions. Journal of Combinatorial Theory(Series A), 1976, 20: 300～305

5 Carlet C.. Partially-Bent functions. Advances in Cryptology-CRYPTO'92. New York: Springer-Verlag, 1993, 280～291

6 Li Shi-Qu, Zhao Ya-Qun,. The relation between partially-Bent and Bent functions. In: Proceedings of CCICS'99, Beijing, 1999, 196～201(in Chinese)
(李世取, 赵亚群. 部分 Bent 函数和 Bent 函数的关系. 见:信息和通信安全——CCICS'99,北京,1999,196～201)

7 Li Shi-Qu, Liu Wen-Fen, Teng Ji-Hong. The properties and constructions of k-order quasi-Bent functions. In: Proceedings of the 7th Session of Communications for the National Youth, Nanjing, 2001, 939～943(in Chinese)
(李世取,刘文芬,滕吉红. k 阶拟 Bent 函数的性质及其应用. 见:第 7 届全国青年通信学术会议,南京,2001, 939～943)

8 Zheng Yu-Liang, Josef Pieprzyk, Jennifer Seberry. HAVAL——A one-way hash algorithm with variable length of output. In: Proceedings of Advances in Cryptology-AUSCRYPTO'92, Lecture Notes in Computer, Springer-Verlag, 1993, 718: 280～291

9　Hu Lei, Pei Ding-Yi, Feng Deng-Guo. Construction of Bent functions. In: Proceedings of CCICS'2001, Shanghai, 2001, 249～253(in Chinese)

(胡　磊,裴定一,冯登国. Bent 函数的构造. 见:信息和通信安全——CCICS'2001,上海,2001,249～253)

TENG Ji-Hong, born in 1974, Ph. D., lecturer. Her current interests include application of probability and statistics in the field of cryptology.

ZHANG Wen-Ying, born in 1970, Ph. D. candidate. Her current interests include application of probability and statistics in the field of cryptology.

LI Shi-Qu, born in 1945, professor and Ph. D. supervisor. His current research interests focus on the cryptology.

HUANG Xiao-Ying, born in 1962, Ph. D., associate professor. Her current research interests focus on the cryptology.

Background

The thesis is part of the authors dissertation, which is titled by "The Cryptographic Criteria of the Cryptographic Functions". The aim of the dissertation is to study the relationship of the cryptographic criteria of cryptographic functions, and hence to investigate some new functions that can be widely used on the nonlinear combined generator to generate the key stream in the secure communications. Parts of the material on tl1is direction have been presented at various conferences and in journals.

• Liu Wen-Fen, Li Shi-Qu, Ten Ji-Hong. The properties and constructions of k-order quasi-Bent functions. In: Proceedings of the 7th Session of Communications for the National Youth. Nanjing, 200l,939～943(in Chinese)

• Teng Ji-Hong, Tan Hui-Yi, Li Shi-Qu. Extended bent functions. Chinese Journal of Engineering Mathematics, 2003, 20(2): 92～98(in Chinese)

• Teng Ji-Hong, Li Shi-Qu, Liu Wen-Fen. The application of k-order quasi-Bent functions in cryptology and communications. The Journal of China Institute of Communications, 24(12): 58～66(in Chinese)

As one part of the dissertation, the authors explore a class of Boolean functions with three-valued walsh spectrum that includes Bent functions and partially-Bent functions as its proper subsets. Although Bent functions and partially-Bent functions play an important role in cryptology, they do not possess the correlation immunity and balancedness, which deprive them of the possibility to resist the correlation attack and statistic attack. In this way the k-order quasi-Bent functions are better than Bent functions and partially-Bent functions, and in order to show the application of these functions, we need to show the good properties and effective constructions of them. The method here is proposed just to fulfill this task.