不重复齐次函数的性质及其应用

张串绒[1]，朱红儒[2]，肖国镇[2]
(1. 空军工程大学 电讯工程学院，陕西 西安 710077；2. 西安电子科技大学 信息保密所，陕西 西安 710071)

摘　要：不重复齐次函数是一类特殊的布尔函数，它在构造密码安全非线性组合函数中有着重要的应用，因此，文中研究了这类函数的密码性质，作为结果，得知不重复齐次一次函数有良好的平衡性和相关免疫性，不重复齐次二次函数是一类Bent函数，有着最高的非线性度和最高的扩散次数等。并以此为基础，深入研究了不重复齐次函数在构造非线性组合函数中的应用，从而得到了具有高非线性度且平衡相关免疫的函数和具有较高非线性度且代数次数达到最高的函数的结构。

关键词：不重复齐次函数；非线性准则；非线性组合函数
中图分类号：TN918.1　　**文献标识码**：A　　**文章编号**：1009-3516(2001)05-0042-03

文献[1]提出了一类特殊布尔函数：不重复齐次k次型(又称不重复齐次k次函数或不重复函数)，本文对这类函数的密码性质进行了研究，给出了不重复齐次k次型所满足的非线性准则；并以此为基础，研究了这类函数在构造密码安全非线性组合函数中的应用，给出了同时满足几个非线性准则的函数的结构。

1　不重复齐次k次型及其密码性质

定义1：$f(x)=a_0+\sum_{r=1}^{n}\sum_{1\le i_1\le\cdots\le i_r\le n}a_{i_1\cdots i_r}x_{i_1}\cdots x_{i_r}$称为$f(x)$的代数标准型，$f$的代数次数记为：$\deg f$。若$\deg f=k$，称$f$为$k$次布尔函数，$k\ge 2$时，称$f$为非线性布尔函数。

定义2[1]：设f为布尔函数，如果其代数标准型中每个乘积项的阶数为k，并且每个变量在代数标准型中出现且出现一次，则称f为不重复齐次k次型。如果f的阶数为k，并且每个变量在代数标准型中出现且出现一次，称f为不重复k次型(简称不重复布尔函数)。

不重复齐次布尔函数当然是不重复布尔函数，因此文献[2]中的结果，对不重复齐次布尔函数也适用。从而我们有如下定理：

定理1：若f为不重复齐次k次型，那么有

1)f是平衡的当且仅当f的代数标准型中有一次单项式。

2)f是不平衡的，则f不具有相关免疫性，$U_f=\{0\}$。

3)f的代数标准型中有l个一次单项式，则f是$l-1$阶相关免疫的，且$|U_f|=2^l$。

4)f是严格雪崩的当且仅当f是不重复齐次二次型。

由**定理1**我们还可以得到以下结论。

结论1：n元不重复齐次一次型，即线性函数：$f(x)=x_1+x_2+\cdots+x_n$，它是对称的、平衡的、$n-1$阶相关免疫函数。且：$\deg f=1$，$N_f=0$，$|U_f|=2^n$。

结论2：不重复齐次二次型，即$f(x_1,\cdots,x_n,y_1,\cdots y_n)=\sum_{i=1}^{n}x_iy_i$，它是Bent函数，满足严格雪崩准则，是$n$次扩散的，$U_f=\{0\}$。且$\deg f=2$，不平衡，不具有相关免疫性。

对$k\ge 3$的不重复齐次k次函数，分析可知，尽管它的一些密码性能并不好，但是它有类似于Bent函数

收稿日期：2001-01-08
基金项目：国家自然科学基金资助项目(60073051)
作者简介：张串绒(1965-)，女，陕西眉县人，讲师，硕士，主要从事数学教学和密码学方面的研究.

的渐近谱特征,另外利用它可以提高函数的代数次数。

定理 2[1]:设 $f_n(x_1,x_2,\cdots,x_n)$ 是不重复齐次 k 次型,$k\geqslant 3$,则对任意 $\omega\in GF^n(2)$,$\lim\limits_{n\to\infty}S_{(f_n)}(\omega)=0$。

上面已经看到不重复齐次 k 次型有许多优越的地方,比如不重复齐次一次型是平衡的且具有最高相关免疫阶;不重复齐次二次型非线性度达到最高,线性结构最少等等。尽管如此,我们也清楚地认识到无论如何象不重复齐次 K 次型这样一个性能达到最好而其它性能皆为最差的函数在密码学上是不安全的,不能直接被用作非线性组合函数。然而如果将它们和其它函数进行组合,采取优势互补原则,便可以得到适于实际安全需要的非线性组合函数。

2　不重复齐次一次型在非线性组合函数构造中的应用

引理 1:设 $f(x_1,\cdots,x_{n_1},x_{n_1+1},\cdots,x_n)=f_1(x_1,\cdots,x_{n_1})+f_2(x_{n_1+1},\cdots,x_n)$,记 $n_2=n-n_1$,则 $(a)f$ 平衡的充分必要条件是 f_1 或 f_2 是平衡的;$(b)N_f=2^{n_2}N_{f_1}+2^{n_1}N_{f_2}-2N_{f_1}N_{f_2}$。

证明:

1)由 f 的构造知:$w(f)=2^{n_2}w(f_1)+2^{n_1}w(f_2)-2w(f_1)w(f_2)$,

故 $w(f)-2^{n_1+n_2-1}=2[w(f_1)-2^{n_1-1}][2^{n_2-1}-w(f_2)]$ 而 f 平衡,即 $w(f)=2^{n_1+n_2-1}$,由上式当且仅当 $w(f_1)=2^{n_1-1}$ 或 $w(f_2)=2^{n_2-1}$,亦即 f_1 或 f_2 是平衡的。

2)由非线性度的定义和 $w(f)=2^{n_2}w(f_1)+2^{n_1}w(f_2)-2w(f_1)w(f_2)$ 易得 (b) 的结果。

引理 2[3]:设 $f=f(x_1,\cdots,x_n)$ 是平衡 m 阶相关免疫函数,令 $g(x_1,\cdots,x_{n+1})=f(x_1,\cdots,x_n)+x_{n+1}$,则 g 是平衡 $m+1$ 阶相关免疫函数。

依据引理 1 和引理 2 可推得如下引理 3 和引理 4。

引理 3:设 f 是 $2k$ 元的 Bent 函数,令 $g(x_1,\cdots,x_{2k},x_{2k+1})=f(x_1,\cdots,x_{2k})+x_{2k+1}$,则 $2k+1$ 元函数 g 是平衡的,且 $N_g=2N_f$。

引理 4:设 f 是 $2k$ 元的 Bent 函数,令 $g(x_1,\cdots,x_{2k+2})=f(x_1,\cdots,x_{2k})+x_{2k+1}+x_{2k+2}$,则 $2k+2$ 元函数 g 是平衡的 1 阶相关免疫函数,且 $N_g=4N_f$。

定理 3:设 f 是 $2k$ 元的 Bent 函数,令 $g(x_1,\cdots,x_{2k+j})=f(x_1,\cdots,x_{2k})+x_{2k+1}+\cdots x_{2k+j}$,则 $2k+j$ 元函数 g 是平衡的 $j-1$ 阶相关免疫函数,且 $N_g=2^jN_f$,$|U_f|=2^j$。

证明:1)由引理 1 的 (a) 和引理 3 可知 g 是平衡的。

2)由引理 2,3,4 可知 g 是 $j-1$ 阶相关免疫函数。

3)令 $f_1=f$,$f_2=x_{2k+1}+\cdots+x_{2k+j}$,由引理 1$(b)$ 可得 $N_g=2^jN_f$。

4)因为 f 是 Bent 函数,它是不平衡的,而 $x_{2k+1}+\cdots+x_{2k+j}$ 作为不重复齐次一次型,由定理 1 的 2)、3)和结论 1 可知 $|U_f|=2^j$。

定理 3 给出了一类平衡的且具有可控相关免疫阶和较高非线性度的非线性组合函数,显然,其平衡性和相关免疫性是得益于不重复齐次一次型,而不重复齐次一次型的缺陷(非线性度为零)在这里得到非线性度最高的 Bent 函数的弥补。因此只要 j,k 选择恰当,由定理可得到满足一定密码安全需要的布尔函数(要注意 N_g 并不是 j 的增函数)。

3　不重复齐次二次型在非线性组合函数构造中的应用

不重复齐次二次型的优势是非线性度最高,缺陷是不平衡不具有相关免疫性,同样采取取长补短的原则,可构造出具有较好非线性度的函数。

定理 4[4]:设 $f(x,y)=\sum\limits_{i=1}^{n}x_iy_i+g(y_1,\cdots,y_n)$,其中,$x=(x_1,x_2,\cdots,x_n)$,$y=(y_1,y_2,\cdots,y_n)$,则 f 是 $2n$ 元的 Bent 函数。

此定理给出了许多的 Bent 函数,而我们知道 Bent 函数在好几个方面密码性能都是很好的,如果还要 f 具有其它一些密码特性,只要恰当的选择 g 即可。比如,还要 f 具有平衡相关免疫性,那末,让 g 取为线性函数即可。这样得到的函数,虽然它的非线性度不如 Bent 函数那样高,但还是能够满足一定实际需要的;若还

想提高 f 的代数次数,只要选 g 是有相应代数次数的函数。对函数 $f(x,y)=\sum_{i=1}^{n}x_iy_i+x,\cdots x_k$,$k$ 取不同的值得到一系列互不等价的 Bent 函数,其中代数次数最高的 $2n$ 元 Bent 函数是 n 次的,即 $f(x,y)=\sum_{i=1}^{n}x_iy_i+x_1x_2,\cdots x_n$,以它作为非线性组合函数,生成的密钥流序列一方面具有较强的抗线性逼近攻击能力,另一方面具有高的线性复杂度,无疑,该函数这两方面的密码性能同时达到了较理想。另外,这里的 $g=x_1x_2\cdots\cdots x_k$,又是一类不重复齐次 k 次函数,所以,由此我们不仅体会到了不重复二次函数的作用,也看到了高次不重复齐次函数在非线性组合函数构造中的一个应用。

4 结束语

文中利用不重复齐次函数,构造出了具有较高非线性度的平衡相关免疫布尔函数和具有最高非线性度或代数次数达到最高的性能良好的密码函数,然而和其它布尔函数一样,用本文给出的方法得到的函数,同样地,一个性能指标的提高可能要以其它性能指标的降低为代价,正如在有高非线性度平衡相关免疫布尔函数的结构中看到的,平衡相关免疫性的实现要以降低非线性度为代价。因此,在实际选择非线性组合函数时,必须考虑各种性能指标的折衷。

参考文献:

[1] 张木想,肖国镇. 流密码中非线性组合函数的分析和设计[J]. 电子学报,1996,24(1):48-52.
[2] 吴文玲. 关于一类布尔函数[J]. 通信保密,1997,(1):58-60.
[3] 扬义先,林须端. 编码密码学[M]. 北京:人民邮电出版社,1992.
[4] 丁存生,肖国镇. 流密码学及其应用[M]. 北京:国防工业出版社,1994.

Properties and Applications of Non-repeated Homogeneous Functions

ZHANG Chuan-rong[1], ZHU Hong-ru[2], XIAO Guo-zhen[2]
(1. The Telecommunications Engineering Institute, Air Force Engineering University, Xi'an 710077, China;
2. The Institute of Information Security, Xidian University, Xi'an, 710071, China)

Abstract: Non-repeated homogeneous functions are a class of special Boolean functions. They are very important in constructing cryptographic security nonlinear combining functions. So, their cryptographic properties are studied in this paper. As a result, we know that non-repeated homogeneous functions of one degree are possessed of good equilibrium and correlation-immunity, and those of two degrees are one class of Bent functions with the highest non-linearity, the largest order number of diffusion, etc. On the basis of the above, the applications of non-repeated homogeneous functions to constructing non-linear combining functions are studied in detail. Therefore, the constructions of balanced correlation-immune functions with higher non-linearity as well as of functions with the highest non-linearity and the highest algebra degree are obtained.

Key words: non-repeated homogeneous functions; nonlinear criteria; nonlinear combining functions

通 知

依据空军工程大学学术工作管理暂行规定([2000]科技字第 21 号通知),在《空军工程大学学报》自然科学版发表文章按国家核心期刊发表同等对待。