满足SAC(k)及其它几个密码准则的函数

张串绒[1],刘卫江[1],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:对k阶严格雪崩性及满足k阶严格雪崩性的函数进行了研究。首先,对已有重要结果进行了深入分析;其次,给出了满足一定阶严格雪崩性布尔函数的结构;最后,得到了满足k阶严格雪崩且同时具有较高非线性度和最高代数次数的平衡函数。

关键词:密码学;k阶严格雪崩准则;平衡;非线性度;代数次数
中图分类号:TN918.1　　**文献标识码**:A　　**文章编号**:1009-3516(2002)02-0047-03

1985年Webster和S. Tavares在研究S-盒的设计时,将"完全性"和"雪崩特性"这两个概念进行组合定义了一个新的概念——严格雪崩准则(strict avalanche criterion 简记SAC)。从此,SAC成为衡量布尔函数密码性能好坏的重要指标,如何构造满足SAC(k)及同时又满足其它密码特性的函数成为密码学界的一个重要问题。本文在分析和研究SAC和SAC(k)有关的重要结果基础上,给出了满足SAC(k)及同时又满足其它良好密码性质的的函数。

1 基本概念

设$f(x)$是n元布尔函数,简记为f;对于任意的$\alpha\in F_2^n$,$W(\alpha)$表示α的汉明重量。

定义1　对n元布尔函数$f(x)$,如果$W(f)=2^{n-1}$,称$f(x)$是平衡的。

定义2　如果对任意的$\alpha\in F_2^n$,$W(\alpha)=1$,恒有$f(x)\oplus f(x\oplus\alpha)$是平衡的,称$f(x)$满足严格雪崩准则,简称$f(x)$满足SAC。

定义3　如果固定$f(x)$的任意k个变元所得到的所有$n-k$元函数都满足SAC,称$f(x)$是k阶严格雪崩的,简称$f(x)$满足SAC(k)。

定义4　$f(x)$与所有线性函数的最短距离称为$f(x)$的非线性度,记为N_f,即$N_f=\min_{l\in L_n} d(f,l)$,其中$L_n$表示全体线性函数。

定义5　$f(x)=a_0+\sum_{r=1}^{n}\sum_{1\le i_1\le\cdots\le i_r\le n} a_{i_1\cdots i_r}x_{i_1}\cdots x_{i_r}$称为$f(x)$的代数标准型。$f$的代数次数是指$f$的代数标准型中非零系数项的最高次数,记为:deg$f$。

2 关于SAC及满足SAC(k)函数结构的一些重要结论

首先要说明的是,以下出现的"$\sum$"和"$+$"均表示二进制和,对出现的n均要求$n\neq 1$。

文献[1]对SAC(k)及满足SAC(k)的函数进行了研究,从中可以得出以下重要结论。

结论1　不存在满足SAC($n-1$)的n元布尔函数。

结论1说明n元布尔函数所能达到的最高严格雪崩阶数是$n-1$,或者说不存在n阶严格雪崩的n元布

收稿日期:2001-05-18
基金项目:国家重点基础研究发展规划项目资助(G1999035804)
作者简介:张串绒(1965-),女,陕西眉县人,讲师,硕士,主要从事信息安全与保密方面的研究.

尔函数。

结论 2 若 n 元布尔函数 $f(x)$ 满足 SAC($n-2$),则 $\deg f=2$ 若 $f(x)$ 满足 SAC(k)、$0\leqslant k\leqslant n-3$,则 $\deg f\leqslant n-k-1$。

由结论 2 可知,满足 SAC($n-2$)的 n 元布尔函数一定是二次函数,满足低于 $n-2$ 阶严格雪崩的函数,其代数次数不超过 $n-k-1$。该结论反应出严格雪崩阶数与代数次数之间的相互制约关系。

结论 3 假设 $f(x)$ 是二次函数,$f(x)$ 满足 SAC(k)、$0\leqslant k\leqslant n-2$,当且仅当每个变元 x_i 至少在 $f(x)$ 的代数标准型中 $n-1$ 个二次项中出现。

这是一个非常有用的结论,比如对函数 $f(x_1,\cdots,x_n)=\sum_{1\leqslant i\leqslant j\leqslant n}x_ix_j$,由于每个 x_i 在 $f(x)$ 的 $n-1$ 个项中出现,因此立即可得以下结论。

结论 4 $f(x_1,\cdots,x_n)=\sum_{1\leqslant i\leqslant j\leqslant n}x_ix_j$ 是满足 SAC($n-2$)的。

结论 5 设 n 元布尔函数 $f(x)$ 满足 SAC($n-2$),如果它不含线性部分,该这函数一定有 $f(x_1,\cdots,x_n)=\sum_{1\leqslant i\leqslant j\leqslant n}x_ix_j$。

结论 6 如果 n 元的布尔函数 $f(x)$ 满足 SAC(k)、$0\leqslant k\leqslant n-2$,则 $f\oplus g$ 也满足 $SAC(k)$。其中 g 是任意 n 元仿射函数。

由结论 5 和结论 6 可知,满足 SAC(k)的布尔函数具有形式 $\sum_{1\leqslant i\leqslant j\leqslant n}x_ix_j\oplus g$,其中 g 是任意 n 元仿射函数。

可见,若 n 元布尔函数满足 SAC(k),则它所能达到的最大值是 $n-2$,满足 SAC($n-2$)的函数全体是 $\sum_{1\leqslant i\leqslant j\leqslant n}x_ix_j\oplus g$($g$ 是任意 n 元仿射函数)。然而,仅仅严格雪崩特性好是不能满足密码安全的实际需要的,密码体制还要求函数具备平衡性、有较高的代数次数、高的非线性度等等。所以,研究满足 SAC(k)同时还满足其它密码特性的函数,是密码学的一个重要课题。

3 满足 SAC(k)的平衡高非线性度函数

引理 1[2] 当 n 是奇数时,函数 $\sum_{1\leqslant i\leqslant j\leqslant n}x_ix_j$ 是平衡的;当 n 是偶数时,函数 $\sum_{1\leqslant i\leqslant j\leqslant n}x_ix_j$ 是不平衡的。

由结论 4 和引理 1 可得

定理 1 当 n 是奇数时,n 元布尔函数 $\sum_{1\leqslant i\leqslant j\leqslant n}x_ix_j$ 是满足 SAC($n-2$)的平衡函数。

由引理 1 和定理 1,当 n 是偶数时,不存在平衡且满足 SAC($n-2$)的函数。

定理 2[3] 设 $f(x_1,\cdots,x_{2k})$ 是 $2k$ 元的 Bent 函数,$k\geqslant 2$,$x=(x_1,\cdots,x_{2k})$,$h(x)$ 是 $2k$ 元非常数仿射函数,令

$$g(u,x_1,\cdots,x_{2k})=f(x_1,\cdots,x_{2k})+uh(x_1,\cdots,x_{2k})$$

则 g 是平衡函数,$N_g\geqslant 2^{2k}-2^k$,且满足严格雪崩准则。

定理 3[3] 设 $f(x_1,\cdots,x_{2k-2})$ 是 $2k-2$ 元的 Bent 函数,$k\geqslant 2$,$x=(x_1,\cdots,x_{2k})$,$h_j(x)$、$(j=1,2,3)$ 是 $2k-2$ 元的非常数的仿射函数,令

$$g(u,v,x_1,\cdots,x_{2k-2})=f(x)+uh_1(x)+uh_2(x)+uvh_1(x)+h_2(x)+h_3(x)$$

则 g 是平衡函数,$N_g\geqslant 2^{2k}-2^k$ 且满足严格雪崩准则。

显然,定理 2 和定理 3 给出的函数密码性能是比较好的,它们不仅满足严格雪崩准则,而且是具有较高非线性度的平衡函数。

4 满足 SAC(k)且代数次数达到最高的平衡函数

引理 2[2] 设 $f(x_1,\cdots,x_n)=(x_1+\cdots+x_{n-k-1})(x_{n-k}+\cdots+x_n)+g(x_1,\cdots,x_{n-k-1})$

g 是任意 $n-k-1$ 元函数,则 f 满足 SAC(k)、$k\leqslant\frac{n}{2}-1$。

由引理 2 可以看出,对 f_1+f_2,如果 f_1 和 f_2 之一满足 SAC(k),则 f_1+f_2 就满足 $SAC(k)$。利用结论 3,只要每个 x_i 在函数的代数标准型中至少 $k+1$ 个二次项中出现,函数就满足 SAC(k)。因此要想得到同时满足

其它密码性质的函数,在引理 2 中只要让 g 满足这些密码性质即可。由此结合文献[4]我们可以得到一些满足 $SAC(k)$同时还满足其它某些性质的布尔函数。

推论 1　对函数 $f(x_1,\cdots,x_n)=(x_1+\cdots+x_{n-k-1})(x_{n-k}+\cdots+x_n)+g(x_1,\cdots,x_{n-k-1})$,令 $g(x_1,\cdots,x_{n-k-1})=x_1\cdots x_{n-k-1}$,则,$\deg f=n-k-1$,且 f 满足 SAC(k)、$0\leqslant k\leqslant\frac{n}{2}-1$。

推论 1 指出了代数次数达到最高且满足 SAC(k)的函数($0\leqslant k\leqslant\frac{n}{2}-1$)。

推论 2　对函数 $f(x_1,\cdots,x_n)=(x_1+\cdots+x_{n-k-1})(x_{n-k}+\cdots+x_n)+g(x_1,\cdots,x_{n-k-1})$

令　$g=a_1x_1+\cdots+a_{n-k-1}x_{n-k-1}+x_1\cdots x_{n-k-1}$

当 $0\leqslant k\leqslant\frac{n}{2}-1$、$n-k-1$ 是奇数时,$\deg f=n-k-1$,f 平衡且满足 SAC(k)。其中,$[a_1,\cdots,a_{n-k-1}]\neq[0,\cdots,0],[1,\cdots,1]$。

推论 3　对函数 $f(x_1,\cdots,x_n)=(x_1+\cdots+x_{n-k-1})(x_{n-k}+\cdots+x_n)+g(x_1,\cdots,x_{n-k-1})$

令　$g=a_1x_1+\cdots+a_{n-k-1}x_{n-k-1}+x_1\cdots x_{n-k-2}+x_2\cdots\cdots x_{n-k-1}$,

当 $0\leqslant k\leqslant\frac{n}{2}-1$、$n-k-1$ 是偶数时,$\deg f=n-k-1$,f 平衡且满足 SAC(k)。其中,$[a_1,\cdots,a_{n-k-1}]\neq[0,\cdots,0],[1,\cdots,1]$。

参考文献:

[1] Thomas W C. Boolean functions satisfying a higher order strict avalanche criterion [A]. EUROCRYPT'93 [C]. 1994,103 - 117.

[2] Kaoru Kurosawa, Takashi Satoh. Design of SAC/PC(1) of order k Boolean functions and three other cryptographic criteria [A]. EUROCRYPT'97[C]. 1998, 435 - 449.

[3] Jennifer Seberry, Zhang Xian - mo. Highly nonlinear 0 - 1 balanced Boolean functions satisfying strict avalanche criterion [A]. EUROCRYPT '92[C]. 1993, 145 - 155.

[4] 张串绒,朱红儒,肖国镇. 不重复齐次数的性质及其应用[J]. 空军工程大学学报(自然科学版),2001,2(5):42 - 44.

(编辑:门向生)

Functions Satisfying SAC(k) and Some Other Cryptographic Criteria

ZHANG Chuan - rong[1],　LIU Wei - jiang[1],　XIAO Guo - zhen[2]

(1. The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an 710077, China; 2. Institute of Information Security, Xidian University, Xi'an 710071, China)

Abstract: SAC(k) and the functions satisfying SAC(k) are studied in this paper. First, some important results about SAC of order k are deeply analyzed; then the construction Boolean functions satisfying SAC(k) of a certain order are given, and finally the balanced SAC(k) functions with higher nonlinearity and highest algebra degree are obtained.

Keywords: cryptography; strict avalanche criterion of order k; balance; nonlinearity; algebra degree