Journal of Computer Applications
计算机应用,2014,34(2):442-443,460
ISSN 1001-9081
CODEN JYIIDU
2014-02-10
http://www.joca.cn

文章编号:1001-9081(2014)02-0442-02
doi:10.11772/j.issn.1001-9081.2014.02.0442

对称布尔函数的算术相关函数

赵庆兰[1,2*],郑　东[1,2],董晓丽[1,2]
(1.西安邮电大学 通信与信息工程学院,西安 710121;　2.无线网络安全技术国家工程实验室,西安 710121)
(*通信作者电子邮箱 qlz@snnu.edu.cn)

摘　要:算术相关函数是最近提出的一种研究布尔函数密码学性质的方法,该方法通过定义多元2-adic数上的加法和乘法运算,构建一种新的环结构,实现对经典相关函数的带进位计算的模拟。首先介绍了算术相关函数的定义,并针对具有良好密码学性质的对称布尔函数讨论了其算术相关函数的性质和取值,最后利用对称布尔函数的实值对称性证明了对称布尔函数的算术自相关函数也是一个与向量的重量有关的实值对称函数,至多是 $n+1$ 值的。

关键词:密码学;布尔函数;2-adic数;算术相关函数;对称布尔函数
中图分类号:TN918.1　　**文献标志码**:A

Arithmetic correlations of symmetric Boolean function

ZHAO Qinglan[1,2*], ZHENG Dong[1,2], DONG Xiaoli[1,2]
(1. *School of Telecommunication and Information Engineering, Xi'an University of Posts and Telecommunications, Xi'an Shaanxi* 710121, *China*;
2. *National Engineering Laboratory for Wireless Security, Xi'an Shaanxi* 710121, *China*)

Abstract: The arithmetic correlation function is a new method for studying the cryptographic properties of Boolean functions. Based on the basic definitions of addition and multiplication of multi-2-adic integer, the study constructed a new algebraic ring and realized the arithmetic or "with-carry" analogs of classic correlation functions. In this paper the definition of arithmetic autocorrelation function was introduced. The arithmetic correlation value of symmetric Boolean functions was studied. The results show that the arithmetic autocorrelation function of symmetric Boolean functions is a real symmetric function with at most $n+1$ values.

Key words: cryptology; Boolean function; 2-adic number; arithmetic correlation function; symmetric boolean function

0　引言

布尔函数在密码学包括流密码和分组密码的设计和分析中有着重要的作用[1],但是这些函数必须满足一定的条件才能应用到具体的密码系统中。非线性、平衡性、相关免疫性和扩散性是衡量密码函数密码学性质优劣的重要指标[2],函数的自相关性能有效地刻画密码函数的扩散性质,函数的平方自相关值越低,那么它的扩散性就越好。所以研究布尔函数的相关函数有十分重要的意义,对相关函数的研究已有很多成果[1,3]。Klapper[4-5]提出了一种新的研究布尔函数性质的工具——算术Walsh变换和算术相关函数,通过借鉴2-adic整数环上的运算构建一个新的环结构,是对经典Walsh变换和相关函数的一种带进位运算的模拟。算术相关函数定义在序列的算术自相关的基础之上,而序列的算术自相关在进位反馈寄存器(Feedback with Carry Shift Registers,FCSR)中有着重要的作用。文献[5]证明了布尔函数算术自相关函数的计算定理,并计算了线性函数、仿射函数的算术自相关函数。文献[6]对二次型函数的算术Walsh变换系数进行了分析计算,进一步讨论了对布尔函数的性质进行进位模拟的意义。目前尚无文献对对称布尔函数的相关函数进行研究。本文首先介绍了一些基础知识,引出了布尔函数算术相关函数的定义,并针对称布尔函数这一具有良好密码学性质的布尔函数的子类进行了初步的讨论,在文献[5]给出的定理的基础上证明了 n 元对称布尔函数的算术自相关函数具有实值对称性,在某个向量上的算术自相关函数与向量的重量有关。

1　预备知识

定义1　令 n 为正整数,n 元布尔函数的定义为 $f:V_n=\mathbf{F}_2^n\to\mathbf{F}_2$,其中 $\mathbf{F}_2=\{0,1\}$。记 B_n 为全体 n 元布尔函数的集合,$1_f=\{\boldsymbol{x}\mid\boldsymbol{x}\in\mathbf{F}_2^n,f(\boldsymbol{x})=1\}$,$0_f=\{\boldsymbol{x}\mid\boldsymbol{x}\in\mathbf{F}_2^n,f(\boldsymbol{x})=0\}$,$f$ 的汉明重量为 $wt(f)=|1_f|$。

定义2　令 $\mathbf{N}=\{0,1,2,\cdots\}$,布尔函数 f 的扩展函数 $F:\mathbf{N}^n\to\mathbf{F}_2$,$F(a_1,a_2,\cdots,a_n)=f(a_1\bmod 2,\cdots,a_n\bmod 2)$,这样的扩展集合定义为 $P_n=\{F:\mathbf{N}^n\to\mathbf{F}_2:F(\boldsymbol{a}+2\boldsymbol{b})=F(\boldsymbol{a})\}$,$P_n$ 是 R_n 的子集,其中 $R_n=\{F:\mathbf{N}^n\to\mathbf{F}_2\}$。

R_1 实际上就是2-adic整数[7-8],对于任意一个函数 $F\in R_1$ 都可以唯一地用一个2-adic数 $\sum_{a=0}^{\infty}f(a)2^a$ 来表示。为了唯一地表示 $F\in R_n$ 的任意一个具有多个变量的函数,需要对2-adic数进行多项式的模拟,定义一个带有多个"2"的multi-2-adic数,为了和普通的整数2区别,用 $t_1,t_2,\cdots,t_n$ 来表示,因此multi-2-adic数的正规表达是:$\sum_{\boldsymbol{a}=(a_1,\cdots,a_n)\in\mathbf{N}^n}f_{\boldsymbol{a}}(t_1^{a_1},\cdots,t_n^{a_n})$。

收稿日期:2013-08-02;**修回日期**:2013-10-28。　**基金项目**:国家自然科学基金资助项目(61272037,61070249);陕西省自然科学基础研究计划重点项目(2013JZ020);陕西省教育厅科学研究计划项目(12JK0551);西安邮电大学校青年基金资助项目(ZL2013-12,ZL2013-02)。

作者简介:赵庆兰(1981-),女,山东曹县人,讲师,博士研究生,主要研究方向:密码学、信息安全;　郑东(1964-),男,山西翼城人,教授,博士生导师,博士,主要研究方向:云计算安全、密码学;　董晓丽(1980-),女,山西阳曲人,讲师,博士,主要研究方向:密码算法。

为了方便,对 $\boldsymbol{a} \in \mathbf{N}^n$,用 $\boldsymbol{t}^{\boldsymbol{a}}$ 表示 $t_1^{a_1}\cdots t_n^{a_n}$,$1^n = (1,1,\cdots,1) \in \mathbf{N}^n$,且 $\mathbf{0}^n = (0,0,\cdots,0) \in \mathbf{N}^n$。在算术运算下,当每一项系数为 2 时向"每一个变量的下一个位置"产生一个进位,"每一个变量的下一个位置"指的是每一个 t_i 的指数都加 1。

定义 3　如果存在满足当且仅当 $\boldsymbol{a}$ 中有一个分量为 0 时 $d_{\boldsymbol{a}} = 0$ 的整数 $\{d_{\boldsymbol{a}}:\boldsymbol{a} \in \mathbf{N}^n\}$;并且对于所有的 $\boldsymbol{a} \in \mathbf{N}^n$,有 $f_{\boldsymbol{a}} + g_{\boldsymbol{a}} + d_{\boldsymbol{a}} = h_{\boldsymbol{a}} + 2d_{\boldsymbol{a}+1^n}$。

定义下面的加法运算:

$$\sum_{\boldsymbol{a}\in\mathbf{N}^n} f_{\boldsymbol{a}}\boldsymbol{t}^{\boldsymbol{a}} + \sum_{\boldsymbol{a}\in\mathbf{N}^n} g_{\boldsymbol{a}}\boldsymbol{t}^{\boldsymbol{a}} = \sum_{\boldsymbol{a}\in\mathbf{N}^n} h_{\boldsymbol{a}}\boldsymbol{t}^{\boldsymbol{a}}$$

定义 4　如果存在满足当且仅当 $\boldsymbol{a}$ 中有一个分量为 0 时 $d_{\boldsymbol{a}} = 0$ 的整数 $\{d_{\boldsymbol{a}}:\boldsymbol{a} \in \mathbf{N}^n\}$;并且对于所有的 $\boldsymbol{a} \in \mathbf{N}^n$,有 $\sum_{\boldsymbol{b}+\boldsymbol{c}=\boldsymbol{a}} f_{\boldsymbol{b}}g_{\boldsymbol{c}} + d_{\boldsymbol{a}} = h_{\boldsymbol{a}} + 2d_{\boldsymbol{a}+1^n}$。

定义如下乘法:

$$\sum_{\boldsymbol{a}\in\mathbf{N}^n} f_{\boldsymbol{a}}\boldsymbol{t}^{\boldsymbol{a}} \cdot \sum_{\boldsymbol{a}\in\mathbf{N}^n} g_{\boldsymbol{a}}\boldsymbol{t}^{\boldsymbol{a}} = \sum_{\boldsymbol{a}\in\mathbf{N}^n} h_{\boldsymbol{a}}\boldsymbol{t}^{\boldsymbol{a}}$$

在上面定义的加法和乘法下,R_n 是一个环。

定理 1[5]　环 R_n 和 S_n 是同构,其中

$$S_n = \mathbf{Z}[[t_1,\cdots,t_n]]/(t_1t_2\cdots t_n - 2)$$

$$\mathbf{Z}[[t_1,\cdots,t_n]] = \left\{ \sum_{\substack{\boldsymbol{a}=(a_1,a_2,\cdots,a_n)\\ a_j\in\mathbf{N}}} c_{\boldsymbol{a}}t_1^{a_1}\cdots t_n^{a_n} : c_{\boldsymbol{a}} \in \mathbf{Z} \right\}$$

上面所定义的加法是沿着对角线 $D_{\boldsymbol{a}} = \{\boldsymbol{a} + \boldsymbol{c}(1,1,\cdots,1):\boldsymbol{c} \in \mathbf{N}\}$ 定义的,对于一个固定的位于某条对角线上的 $\boldsymbol{a} \in \mathbf{N}^n$,沿着对角线 $D_{\boldsymbol{a}}$ 上的所有项的和在同构的意义下定义了一个 2-adic 数

$$\bar{f}(\boldsymbol{a}) = \sum_{i=0}^{\infty} F(\boldsymbol{a} + i(1,\cdots,1))(t_1,\cdots,t_n)^i = \sum_{i=0}^{\infty} F(\boldsymbol{a} + i(1,\cdots,1))2^i \tag{1}$$

2　算术相关函数

定义 5　对于任意 $F \in R_n$,如果存在一个整数 k 满足对于任意 $\boldsymbol{a} = (a_1,\cdots,a_n) \in \mathbf{N}^n, a_i \geqslant k(i = 1,2,\cdots,n)$,使得对于任意 $\boldsymbol{b} \in \mathbf{N}^n$ 有 $F(\boldsymbol{a} + p\boldsymbol{b}) = F(\boldsymbol{a})$ 成立,则 F 是最终 p-周期的。如果任意 $\boldsymbol{a} = (a_1,\cdots,a_n) \in \mathbf{N}^n, a_i \geqslant k(i = 1,2,\cdots,n)$,$F$ 在集合 $\{\boldsymbol{a} + \boldsymbol{b}:\boldsymbol{b} = (b_1,\cdots,b_2), 0 \leqslant b_i < p, i = 1,2,\cdots,n\}$ 的值称为 F 的一个完整的周期[5]。

假设 $F \in R_n$,是严格 2-周期的函数,则在式(1)中得

$$\bar{f}(\boldsymbol{a}) = \sum_{i=0}^{\infty} F(\boldsymbol{a} + i\cdot 1^n)2^n = f(\boldsymbol{a}) + f(\boldsymbol{a}+1^n)2 + f(\boldsymbol{a})2^2 + f(\boldsymbol{a}+1^n)2^3 + \cdots = -\frac{f(\boldsymbol{a}) + 2f(\boldsymbol{a}+1^n)}{3} \tag{2}$$

定义 6[5]　对于任意 $F \in R_n$ 是最终 p-周期的,F 不平衡度为 $Z(F)$:

$$Z(F) = \sum_{\boldsymbol{a}\in V_n} (-1)^{F(\boldsymbol{a})}$$

定义 7　任意最终 p-周期的函数 $F \in R_n$ 和 $G \in R_n$,它们的算术互相关函数是实值函数 $C_{F,G}^{\boldsymbol{a}} \in \mathbf{R}$,定义为 $C_{F,G}^{\boldsymbol{a}}(\boldsymbol{b}) = Z(F - G_{\boldsymbol{b}})$,其中 $G_{\boldsymbol{b}} = G(\boldsymbol{a} + \boldsymbol{b})$。布尔函数 $f,g \in B_n$ 的算术互相关函数的定义为:$C_{f,g}^{\boldsymbol{a}}(\boldsymbol{b}) = C_{F,G_{\boldsymbol{b}}}^{\boldsymbol{a}}$,其中 F、$G_{\boldsymbol{b}}$ 是 f 和 $g_{\boldsymbol{b}}$ 的扩展。f 的算术自相关函数定义为

$$A_f^{\boldsymbol{a}}(\boldsymbol{b}) = C_{f,f}^{\boldsymbol{a}}(\boldsymbol{b})$$

布尔函数 f 的扩展函数 F 是最终 2-周期函数,令 $U_n = \{\boldsymbol{a} = (a_1,a_2,\cdots,a_n):a_i \in \{0,1\} \text{ and } a_1 = 0\}$,则函数 $F \in R^n$ 在每条对角线 $D_{\boldsymbol{a}}$ 上的不平衡度就是 2-adic 数 $\bar{f}(\boldsymbol{a})$ 的不平衡度。因此 $Z(f) = \sum_{\boldsymbol{a}\in V_n} Z(\bar{f}(\boldsymbol{a}))$,利用此式和式(2)文献[5]证明了下面的定理。

定理 2[5]　$f:V_n \to \mathbf{F}_2$ 是布尔函数,$\boldsymbol{b} \in V_n, A_f^{\boldsymbol{a}}(\boldsymbol{b}) = |\{\boldsymbol{a} \in V_n: f(\boldsymbol{a}) = f(\boldsymbol{a} + \boldsymbol{b}), \text{ and } f(\boldsymbol{a} + 1^n) = f(\boldsymbol{a} + \boldsymbol{b} + 1^n)\}|$。本文得出了以下推论。

推论 1　n 元布尔函数 $f(\boldsymbol{x}) \in B_n$ 为对称布尔函数,满足 $f(\boldsymbol{a}) = f(\boldsymbol{a} + 1^n)$,则 $A_f^{\boldsymbol{a}}(\boldsymbol{b}) = |\{\boldsymbol{a} \in V_n:f(\boldsymbol{a}) = f(\boldsymbol{a} + \boldsymbol{b})\}|$,并且 $A_f^{\boldsymbol{a}}(\boldsymbol{b}) = A_f^{\boldsymbol{a}}(\bar{\boldsymbol{b}})$。

3　对称布尔函数的算术相关函数

对称布尔函数作为布尔函数的一个子类:一方面,在函数的存储上占用较少的内存空间;另一方面,实际应用中需要的逻辑门个数与变元个数呈线性关系。因此,研究具有良好密码学性质的对称布尔函数有着十分重要的意义[9-12]。

定义 8　称 n 元布尔函数 $f(\boldsymbol{x}) \in B_n$ 为对称布尔函数,如果对任意 $n \times n$ 阶置换矩阵 $\boldsymbol{P}$ 恒有 $f(\boldsymbol{x}) = f(\boldsymbol{x}\boldsymbol{P})$。

换言之,如果对于任意两个具有相同汉明重量的输入向量 $\boldsymbol{x},\boldsymbol{y} \in V_n$,都有 $f(\boldsymbol{x}) = f(\boldsymbol{y})$,则 f 是对称布尔函数。

根据定义 8 每个 n 元对称布尔函数 $f(\boldsymbol{x}) \in B_n$ 可以由一个 $n+1$ 元向量

$$\boldsymbol{v}_f = (v_f(0),v_f(1),\cdots,v_f(n)) \in \mathbf{F}_2^{n+1}$$

来表示。其中分量 $v_f(i)$ 表示重量为 i 的输入向量的函数值。记 $f'(\boldsymbol{x}) = f(\boldsymbol{x} + 1^n)$,易知 $f'(\boldsymbol{x})$ 和 $f(\boldsymbol{x})$ 等价,并且 $v_f(i) = v_f(n-i)$。因为条件 $f'(\boldsymbol{a}) = f'(\boldsymbol{a} + \boldsymbol{b})$,and $f'(\boldsymbol{a} + 1^n) = f'(\boldsymbol{a} + \boldsymbol{b} + 1^n)$ 和 $f(\boldsymbol{a}) = f(\boldsymbol{a} + \boldsymbol{b})$,and $f(\boldsymbol{a} + 1^n) = f(\boldsymbol{a} + \boldsymbol{b} + 1^n)$ 是等价的,所以根据定理 2 可推出以下推论。

推论 2　n 元布尔函数 $f(\boldsymbol{x}) \in B_n$ 是对称布尔函数,记 $f'(\boldsymbol{x}) = f(\boldsymbol{x} + 1^n)$,则 $A_f^{\boldsymbol{a}}(\boldsymbol{b}) = A_f^{\boldsymbol{a}}(\boldsymbol{b})$。

定理 3　对称布尔函数 $f(\boldsymbol{x})$ 的算术自相关函数是实值对称函数。

证明　因为 f 是对称布尔函数,所以对任意的 $n \times n$ 阶置换 $\boldsymbol{P}$,$f(\boldsymbol{a}) = f(\boldsymbol{a}\boldsymbol{P})(a \in V_n)$ 成立。

$$\begin{aligned} A_f^{\boldsymbol{a}}(\boldsymbol{b}) = |\{&\boldsymbol{a} \in V_n:f(\boldsymbol{a}) = f(\boldsymbol{a} + \boldsymbol{b}) \text{ and } f(\boldsymbol{a} + 1^n) = f(\boldsymbol{a} + \boldsymbol{b} + 1^n)\}| = |\{\boldsymbol{a} \in V_n: f(\boldsymbol{a}\boldsymbol{P}) = \\ &f((\boldsymbol{a} + \boldsymbol{b})\boldsymbol{P}) \text{ and } f((\boldsymbol{a} + 1^n)\boldsymbol{P}) = \\ &f((\boldsymbol{a} + \boldsymbol{b} + 1^n)\boldsymbol{P})\}| = |\{\boldsymbol{a} \in V_n: f(\boldsymbol{a}\boldsymbol{P}) = \\ &f(\boldsymbol{a}\boldsymbol{P} + \boldsymbol{b}\boldsymbol{P}) \text{ and } f(\boldsymbol{a}\boldsymbol{P} + 1^n) = \\ &f(\boldsymbol{a}\boldsymbol{P} + \boldsymbol{b}\boldsymbol{P} + 1^n)\}| = |\{\boldsymbol{a} \in V_n: f(\boldsymbol{a}) = \\ &f(\boldsymbol{a} + \boldsymbol{b}\boldsymbol{P}) \text{ and } f(\boldsymbol{a} + 1^n) = f(\boldsymbol{a} + \boldsymbol{b}\boldsymbol{P} + 1^n)\}| \end{aligned}$$

最后一个等号成立的原因是 $\boldsymbol{P}$ 置换,当 $\boldsymbol{a}$ 遍历 V_n 时 $\boldsymbol{a}\boldsymbol{P}$ 也遍历 V_n,所以 $A_f^{\boldsymbol{a}}(\boldsymbol{b}) = A_f^{\boldsymbol{a}}(\boldsymbol{b}\boldsymbol{P})$ 成立,因此对称布尔函数 $f(\boldsymbol{x})$ 的算术自相关函数也具有实值对称性。

进一步说明,f 是对称布尔函数,对于任意的 $\boldsymbol{b} \in V_n, \boldsymbol{c} \in V_n$,满足 $wt(\boldsymbol{b}) = wt(\boldsymbol{c})$,则 $A_f^{\boldsymbol{a}}(\boldsymbol{b}) = A_f^{\boldsymbol{a}}(\boldsymbol{c})$,因此 f 的算术自相关函数至多是 $n+1$ 值的。

(下转第 460 页)

足大多数有源 RFID 标签系统的应用需求。

参考文献：

[1] SARMA S E, WEIS S A, ENGELS D W. RFID systems and security and privacy implications[C]// Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer-Verlag, 2003: 454 - 469.

[2] OHKUBO M, SUZUKI K, KINOSHITA S. Hash-chain based forward-secure privacy protection scheme for low-cost RFID[C]// SCIS 2004: Proceedings of the 2004 Symposium on Cryptography and Information Security. Berlin: Springer-Verlag, 2004: 719 - 724.

[3] ZHANG H, WANG B. RFID security protocol based on symmetric cryptosystem[J]. Modern Electronics Technique, 2013, 36(5): 106 - 108. (张淏湜, 王斌. 基于对称密码体制的 RFID 安全协议[J]. 现代电子技术, 2013, 36(5): 106 - 108.)

[4] TTYYLG P, BATINA L. RFID tags for anti-counterfeiting[C]// Proceedings of the Cryptographer's Track at the RSA Conference. Berlin: Springer-Verlag, 2006: 115 - 131.

[5] LEE Y K, BATINA L, VERBAUWHEDE I. EC-RAC (ECDLP based randomized access control): provably secure RFID authentication protocol [C]// Proceedings of the 2008 IEEE International Conference on RFID. Piscataway: IEEE, 2008: 97 - 104.

[6] GURA N, PATEL A, WANDER A, *et al.* Comparing elliptic curve cryptography and RSA on 8-bit CPUs[C]// Proceedings of 6th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer-Verlag, 2004: 119 - 132.

[7] PAN Z, ZHU L. Application of ECC and AES algorithm to security of CPU card[J]. Computer Systems & Applications, 2012, 21(9): 162 - 165. (潘峥嵘, 朱丽丽. ECC 与 AES 混合加密算法在射频 CPU 卡安全机制中的应用[J]. 计算机系统应用, 2012, 21(9): 162 - 165.)

[8] LI C, ZHANG W. Research on signcryption algorithm based on ECC in RFID[J]. Commputer and Modernization, 2010, 8(1): 191 - 193. (李春华, 张伟. 一种 ECC 签密算法在 RFID 中的应用研究[J]. 计算机与现代化, 2010, 8(1): 191 - 193.)

[9] WANG M, WANG J. Efficient RFID mutual authentication protocol [J]. Journal of Computer Applications, 2011, 31(10): 2694 - 2696. (王明辉, 王建东. 高效的 RFID 双向认证协议[J]. 计算机应用, 2011, 31(10): 2694 - 2696.)

[10] KOBLITZ N. ELLIPTIC curve cryptosystem [J]. Mathematics of Computation, 1987, 48(177): 203 - 309.

[11] NIST. Advanced encryption standard, FIPS PUB 197 [S/OL]. [2012-10-10]. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[12] SHENG F. The statistics analysis on the security of SHA algorithms [D]. Zhengzhou: PLA Information Engineering University, 2011. (申飞. SHA 系列算法安全性的统计分析 [D]. 郑州: 信息工程大学, 2011.)

[13] YU J, WANG J, YANG C. The realization of encryption system based on ECC and AES[J]. Information Technology, 2006, 1(2): 44 - 46. (俞经善, 王晶, 杨川龙. 基于 ECC 和 AES 相结合的加密系统的实现[J]. 信息技术, 2006, 1(2): 44 - 46.)

(上接第 443 页)

4 结语

本文初步讨论了对称布尔函数的算术自相关函数，证明了对称布尔函数的算术自相关函数跟向量的重量有关，至多是 $n+1$ 值的。而对于算术相关函数的其他性质，比如特殊布尔函数中的对称布尔函数、bent 函数的算术相关函数值的分布，上界或者下界，以及与布尔函数其他密码学性质之间的关系都是有待研究的问题。

全局雪崩准则(Global Avalanche Criterion, GAC)和 k 阶扩散准则是研究布尔函数在抵抗密码攻击方面的密码学性质的重要指标，布尔函数的相关函数则是这些概念定义的基础。文献[5]在定义算术相关函数的基础上也定义了算术雪崩准则(Arithmetic Avalanche Criterion, AAC)和 k 阶扩散准则(Arithmetic Propagation Criterion of degree k, APC(k))，对于怎样构造满足 AAC 或者 APC(k)的布尔函数并没有进一步的讨论，这也是以后的一个研究方向。

参考文献：

[1] CARLET C. Boolean functions for cryptography and error correcting codes[EB/OL]. [2013-08-20]. http://www1.spms.ntu.edu.sg/~kkhoongm/chap-fcts-Bool.pdf.

[2] WEN Q, NIU X, YANG Y. Boolean functions of modern cryptography[M]. Beijing: Science Press, 2008. (温巧燕, 钮心忻, 杨义先. 现代密码学中的布尔函数 [M]. 北京: 科学出版社, 2000.)

[3] CUSICK T, STANICA P. Cryptographic boolean functions and applications[M]. San Diego: Academic Press, 2009.

[4] KLAPPER A, GORESKY M. A with-carry Walsh transform (extended abstract)[C]// Proceedings of the 6th International Conference on Sequences and Their Applications. Berlin: Springer-Verlag, 2010: 217 - 228.

[5] KLAPPER A, GORESKY M. Arithmetic correlations and Walsh transforms[J]. IEEE Transactions on Information Theory, 2012, 58(1): 479 - 492.

[6] KLAPPER A. Arithmetic Walsh transform of quadratic boolean functions[C]// Proceedings of the 8th International Conference on Sequences and Their Applications. Berlin: Springer-Verlag, 2012: 65 - 76.

[7] KOBLITZ N. p-Adic numbers, p-Adic analysis, and Zeta functions [M]. Berlin: Springer, 1984.

[8] KLAPPER A, GORESKY M. Feedback shift registers, combiners with memory, and 2-Adic span[J]. Journal of Cryptology, 1997, 10(2): 111 - 147.

[9] CANTEAUT A, VIDEANU M. Symmetric Boolean functions[J]. IEEE Transactions on Information Theory, 2005, 51(8): 2791 - 2811.

[10] BRAEKEN A, PRENEEEL B. On the algebraic immunity of symmetric boolean functions[C]// Proceedings of the 6th International Conference on Cryptology. Heidelberg: Springer, 2005: 35 - 48.

[11] DALAI D K, MAITRA S, SKAKAR S. Basic theory in construction of boolean functions with maximum possible annihilator immunity [J]. Design, Codes and Cryptography, 2006, 40(1): 41 - 58.

[12] OU Z, ZHAO Y. On one class of symmetric Boolean functions[J]. Journal on Communications, 2013, 34(1): 89 - 104. (欧智慧, 赵亚群. 一类对称布尔函数的研究[J]. 通信学报, 2013, 34(1): 89 - 104.)