胡凤. 密码学中指数和公式及其应用[J].湖南科技大学学报(自然科学版),2019,34(3):119-124. doi:10.13582/j.cnki.1672-9102.2019.03.017

Hu F. Exponential Sum Formula in Cryptology and Its Applications [J]. Journal of Hunan University of Science and Technology (Natural Science Edition), 2019,34(3):119-124. doi:10.13582/j.cnki.1672-9102.2019.03.017

密码学中指数和公式及其应用

胡凤*

(河南大学 国际教育学院,河南 开封 475000)

摘　要:对密码学的研究始终伴随着对布尔函数的研究. 指数和公式是研究布尔函数的平衡性、非线性度和相关免疫度等密码学指标的一个重要工具,具有很多重要的应用. 指数和公式的成立有许多不同的证明方法:能量守恒的方法、组合的方法、线性代数的方法、抽象代数的方法.文章最后给出了指数和公式的应用.

关键词:指数和公式;布尔函数;Bent 函数;Semi-Bent 函数

中图分类号:TN911.1　　**文献标志码**:A　　**文章编号**:1672-9102(2019)03-0119-06

Exponential Sum Formula in Cryptology and Its Applications

Hu Feng

(International Education College, Henan University, Kaifeng 475000, China)

Abstract: The study of cryptology is always in line with the study of Boolean functions. Exponential sum formula is an important tool to study the balancedness, nonlinearity, correlation immunity and other cryptographic properties of Boolean functions. The exponential sum formula was proven by using some method, such as the energy conservation method, the combination method, the linear algebra method, and the abstract algebra method respectively. Finally, an application of the exponential sum formula was given.

Keywords: exponential sum formula; Boolean function; Bent function; semi-Bent function

密码学是研究密码理论和密码技术的科学. 20 世纪初期,密码学相关知识主要应用在军事、政治、外交等领域,随着现代科技的迅猛发展,密码学的应用已经渗透到生产、生活的各个领域. 现代密码学由两部分组成,即密码分析学(cryptoanalytics)和密码编码学(cryptography)[1-3]. 根据密钥的使用方式的不同,密码体制可以分为私钥密码和公钥密码. 根据加密形式的差异,密码体制可以分为流密码[4-5]和分组密码[6-7]. 相对于分组密码来说,流密码出错概率较小,更容易在硬件中实现,因此在通信领域内的应用也更为广泛. 目前对流密码的研究主要分为 2 部分,即驱动部分和非线性组合部分. 关于驱动部分的研究目前已经比较成熟,而非线性部分的研究是当前研究的重点、难点和热点. 对非线性组合部分的研究就是对布尔函数的研究. 布尔函数是实现密码体制的不可缺少的一个重要工具. 对流密码的研究始终伴随着对布尔函数的研究. 而研究布尔函数的密码学性质:平衡性、非线性度、相关免疫度,构造密码学性质良好的布尔函数是研究流密码问题的中心问题.

收稿日期:2019-03-18

* **通信作者**,E-mail: hedahufeng@126.com

1 基本知识

$\boldsymbol{F}^2$ 表示只含有 2 个元素的有限域,即 $\boldsymbol{F}^2=\{0,1\}$. $\boldsymbol{F}_2^n$ 表示 $\boldsymbol{F}^2$ 上的所有 n 元向量构成的向量空间. n 元布尔函数 f 是从向量空间 $\boldsymbol{F}_2^n$ 到有限域 F^2 上的一个映射.

设向量 $\boldsymbol{\alpha}=(a_1,a_2,\cdots,a_n)\in\boldsymbol{F}_2^n,\boldsymbol{\beta}=(b_1,b_2,\cdots b_n)\in\boldsymbol{F}_2^n$. 本文中记 $\boldsymbol{0}_n=(0,0,\cdots,0)\in\boldsymbol{F}_2^n,\boldsymbol{1}_n=(1,1,\cdots,1)\in\boldsymbol{F}_2^n$. 向量 $\boldsymbol{\alpha}$ 的支撑集记为 $\mathrm{supp}(\boldsymbol{\alpha})=\{0\leqslant i\leqslant n-1\mid a_i=1\}$. 向量 $\boldsymbol{\alpha}$ 的 Hamming 重量为它的分量中 1 的个数,记为 $wt(\boldsymbol{\alpha})$. 显然,$\mathrm{wt}(\boldsymbol{\alpha})=|\mathrm{supp}(\boldsymbol{\alpha})|$. 向量 $\boldsymbol{\alpha}$ 和向量 $\boldsymbol{\beta}$ 的模 2 加定义为 $\boldsymbol{\alpha}\oplus\boldsymbol{\beta}=(a_1\oplus b_1,a_2\oplus b_2,\cdots,a_n\oplus b_n)$;向量 $\boldsymbol{\alpha}$ 和向量 $\boldsymbol{\beta}$ 的模 2 内积定义为 $\boldsymbol{\alpha}\cdot\boldsymbol{\beta}=a_1b_1\oplus a_2b_2\oplus\cdots\oplus a_nb_n$.

布尔函数的 Walsh 变换是研究布尔函数的密码学指标的一个非常重要的工具,多个关于布尔函数的密码学指标的刻画都可以借助于它的 Walsh 变换的谱值来完成.

定义 1 n 元布尔函数 f 的 Walsh 变换定义为

$$W_f(\boldsymbol{w})=\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^n}(-1)^{f(\boldsymbol{x})\oplus\boldsymbol{x}\cdot\boldsymbol{w}},\boldsymbol{w}\in\boldsymbol{F}_2^n. \tag{1}$$

为了保证密码体制能够抵抗几种常见的密码攻击,符合安全性的需求,流密码中所使用的布尔函数必须满足若干密码学原则,也就是说布尔函数要满足如下的基本性质:

1) 平衡性:布尔函数 f 的平衡性[8-9]指的是对于它的 2^n 个不同的输入来说,输出 0 和 1 的个数相等. 即 $|\{\boldsymbol{x}:f(\boldsymbol{x})=0,\boldsymbol{x}\in\boldsymbol{F}_2^n\}|=|\{\boldsymbol{x}:f(\boldsymbol{x})=1,\boldsymbol{x}\in\boldsymbol{F}_2^n\}|=2^{n-1}$.通过简单的计算可以知道一个布尔函数 f 是平衡的当且仅当

$W_f(\boldsymbol{0}_n)=0,\boldsymbol{0}_n\in\boldsymbol{F}_2^n$.

平衡性是流密码中使用布尔函数的基本要求之一. 如果布尔函数的平衡性得不到满足,使用该布尔函数的密码体制将会受到基于统计分析攻击.

2)高非线性度:非线性度[10-11]是一个布尔函数 f 与全体代数次数不超过 1 的布尔函数(即仿射函数)的 Hamming 距离的最小值. 非线性度可以用 Walsh 变换来定义:

$$nl_f=2^{n-1}-\frac{1}{2}\max_{\boldsymbol{w}\in\boldsymbol{F}_2^n}|W_f(\boldsymbol{w})|.$$

若布尔函数的非线性度足够高,也就是布尔函数和全体仿射函数的 Hamming 距离足够大,则就可以抵抗最佳仿射逼近[12]和快速相关攻击[13].

3)合适的相关免疫度:相关免疫度刻画的是布尔函数 f 抵抗相关攻击的能力. 一个布尔函数 f 的相关免疫度 d 定义为[14-15]

$W_f(\boldsymbol{w})=0,\boldsymbol{w}\in\boldsymbol{F}_2^n,1\leqslant\boldsymbol{w}t(\boldsymbol{w})\leqslant d$.

相关攻击的原理是利用密钥流发生器的输出序列与 LFSR 的输出序列之间的相关性还原 LFSR 的初始状态[16].

定义 2 若 n 元布尔函数 f 的 Walsh 谱值满足

$W_f(\boldsymbol{\alpha})=\pm 2^{\frac{n}{2}},\boldsymbol{\alpha}\in\boldsymbol{F}_2^n$.

那么称函数 f 为 Bent 函数.

定义 3 若 n 元布尔函数 f 的 Walsh 谱值满足

$W_f(\boldsymbol{\alpha})=\pm 2^{\left|\frac{n+1}{2}\right|},\boldsymbol{\alpha}\in\boldsymbol{F}_2^n$.

那么称函数 f 为 semi-Bent 函数.

Bent 函数[17-21]和 semi-Bent 函数[22-24]是非线性度特别好的布尔函数,在序列设计、分组密码等领域有着广泛的应用,是最近 40 多年的一个热门研究问题.

下面介绍在本文中非常重要的 2 个数学公式.

引理 1 任给向量 $\boldsymbol{\alpha}\in\boldsymbol{F}_2^n$ 和 n 元布尔函数 f,等式 $\sum_{\boldsymbol{\alpha}\in\boldsymbol{F}_2^n}(W_f(\boldsymbol{\alpha}))^2=2^{2n}$ 成立.

引理 1 中的这一等式称为 Parseval' 等式[25],即能量守恒公式.

引理 2　任给正整数 n, 等式 $\sum_{k=0}^{\left|\frac{n-1}{2}\right|}\binom{n}{2k}=2^{n-1}$ 成立. 这里 $\left|\frac{n-1}{2}\right|$ 表示 $\frac{n-1}{2}$ 取上整.

证明　根据二项式定理可知

$$\begin{cases}(1+1)^n=\sum_{i=0}^{n}\binom{n}{i}=2^n;\\(1-1)^n=\sum_{i=0}^{n}(-1)^i\binom{n}{i}=0.\end{cases}$$

故

$$\sum_{k=0}^{\left|\frac{n-1}{2}\right|}\binom{n}{2k}=\frac{\sum_{i=1}^{n}\binom{n}{i}+\sum_{i=1}^{n}(-1)^i\binom{n}{i}}{2}=2^{n-1}.$$

2　指数和公式的几种证明方法

指数和公式在布尔函数的平衡性、非线性度、相关免疫度等性质中有着广泛的应用. 本节用 4 种不同的方法证明指数和公式:能量守恒的方法、线性代数的方法、组合的方法、抽象代数的方法.

定理 1　若向量 $\boldsymbol{w}\in\boldsymbol{F}_2^n$,则指数和公式

$$\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^n}(-1)^{\boldsymbol{x}\cdot\boldsymbol{w}}=\begin{cases}2^n,\ \boldsymbol{w}=\boldsymbol{0}_n\in\boldsymbol{F}_2^n;\\0,\ \boldsymbol{w}\neq\boldsymbol{0}_n\in\boldsymbol{F}_2^n.\end{cases}$$

成立. 这里 $\boldsymbol{x}=(x_1,\cdots,x_{n-1})$.

证明　若 $\boldsymbol{w}=\boldsymbol{0}_n$, 显然, $\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^n}(-1)^{\boldsymbol{x}\cdot\boldsymbol{w}}=2^n$. 下面仅证 $\boldsymbol{w}\neq\boldsymbol{0}_n$ 的情形.

【证法一】　能量守恒的方法

能量守恒的方法密码学中关于布尔函数一个最基本的方法. 能量守恒定律也就是引理 1 可以用来证明指数和公式.

令式(1)中的$f(\boldsymbol{x})=0$, 由引理 1 得 $\sum_{\boldsymbol{w}\in\boldsymbol{F}_2^n}\left(\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^n}(-1)^{\boldsymbol{x}\cdot\boldsymbol{w}}\right)^2=2^{2n}$. 当 $\boldsymbol{w}=\boldsymbol{0}_n$ 时, $\left(\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^n}(-1)^{\boldsymbol{x}\cdot\boldsymbol{w}}\right)^2=2^{2n}$. 而 $\sum_{\boldsymbol{w}\neq\boldsymbol{0}_n}\left(\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^n}(-1)^{\boldsymbol{x}\cdot\boldsymbol{w}}\right)^2=2^{2n}$, 故当 $\boldsymbol{w}\neq\boldsymbol{0}_n$ 时, $\left(\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^n}(-1)^{\boldsymbol{x}\cdot\boldsymbol{w}}\right)^2$ 只能为 0. 因此, 当向量 $\boldsymbol{w}\neq\boldsymbol{0}_n$ 时, $\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^n}(-1)^{\boldsymbol{x}\cdot\boldsymbol{w}}=0$.

【证法二】　线性代数的方法

线性代数中线性方程组的相关理论也可以用来证明指数和公式.线性方程组的相关理论即 n 元齐次线性方程组的系数矩阵的秩为 r, 则基础解系含 $n-r$ 个解向量.

若 $\boldsymbol{w}\neq\boldsymbol{0}_n$, 设

$$\boldsymbol{A}=\{\boldsymbol{x}\in\boldsymbol{F}_2^n\mid\boldsymbol{x}\cdot\boldsymbol{w}=0\}. \tag{2}$$

式中:$\boldsymbol{A}$ 为与向量 $\boldsymbol{w}$ 正交的所有向量构成的集合,也是 $\boldsymbol{F}_2^n$ 的一个子空间.此时,对任意的 $\boldsymbol{x}\in\boldsymbol{F}_2^n\backslash\boldsymbol{A}$ 有 $\boldsymbol{w}\cdot\boldsymbol{x}=1$. 于是

$$\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^n}(-1)^{\boldsymbol{x}\cdot\boldsymbol{w}}=\sum_{\boldsymbol{x}\in\boldsymbol{A}}(-1)^{\boldsymbol{x}\cdot\boldsymbol{w}}+\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^n\backslash\boldsymbol{A}}(-1)^{\boldsymbol{x}\cdot\boldsymbol{w}}=\sum_{\boldsymbol{x}\in\boldsymbol{A}}(-1)^0+\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^n\backslash\boldsymbol{A}}(-1)^1=|\boldsymbol{A}|-|\boldsymbol{F}_2^n\backslash\boldsymbol{A}|=$$

$$2|\boldsymbol{A}|-2^n. \tag{3}$$

问题可以转化为求齐次方程组 $\boldsymbol{x}\cdot\boldsymbol{w}=0$ 解的个数. 事实上,此线性方程组系数矩阵的秩为 1,基础解系含 $n-1$ 个解向量, 于是 $|\boldsymbol{A}|=2^{n-1}$. 故 $\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^n}(-1)^{\boldsymbol{x}\cdot\boldsymbol{w}}=0$.

【证法三】　组合的方法

组合的相关理论也就是引理 2 可以用来证明指数和公式.

(2)式中的 $\boldsymbol{A}$ 还可以写成如下形式.于是式(3)中 $|\boldsymbol{A}| = \sum_{k=0}^{\left|\frac{\mathrm{wt}(\boldsymbol{w})-1}{2}\right|} \binom{\mathrm{wt}(\boldsymbol{w})}{2k} \cdot 2^{n-\mathrm{wt}(\boldsymbol{w})}$. 又根据引理 1 可得 $|\boldsymbol{A}| = 2^{\mathrm{wt}(\boldsymbol{w})-1} \cdot 2^{n-\mathrm{wt}(\boldsymbol{w})} = 2^{n-1}$.

从而 $\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^n} (-1)^{\boldsymbol{x}\cdot\boldsymbol{w}} = 0$.

【证法四】 抽象代数的方法

密码学是和抽象代数紧密结合的,抽象代数中的陪集可以用来证明指数和公式.

若 $\boldsymbol{w} \neq \boldsymbol{0}_n$,定义 $\boldsymbol{F}_2^n$ 到 $\boldsymbol{F}_2$ 的映射 $\varphi: \boldsymbol{x} \to \boldsymbol{w}\cdot\boldsymbol{x}$.可以验证,这是一个群同态,且 $\ker(\varphi) = \boldsymbol{A}$. 其中 $\boldsymbol{A}$ 在式(2)中给出. 由于 φ 为满同态,由同态基本定理得集 $\boldsymbol{F}_2^n/(\ker\varphi) \simeq \boldsymbol{F}_2$. 由于 $|\boldsymbol{F}_2| = 2$,于是 $\boldsymbol{F}_2^n$ 分成了 2 个陪集,一个陪集的映射为 0,另一个为 1. 这 2 个陪集的大小是相等的,都等于 $2^n/2 = 2^{n-1}$. 因此 $\boldsymbol{w}\cdot\boldsymbol{x}$ 有 2^{n-1} 种情况下等于 0,有 2^{n-1} 种情况下等于 1. 从而 $\sum_{\boldsymbol{x}\in\boldsymbol{F}_2^n} (-1)^{\boldsymbol{x}\cdot\boldsymbol{w}} = 0$.

3 指数和公式的一个应用

关于布尔函数的 Walsh 变换的计算工作是研究布尔函数的各项指标的重要组成部分,有的时候计算难度非常大.在本节中,通过具体的例子展示,指数和公式在计算布尔函数的 Walsh 谱值的时候能够提供快速、便捷的辅助效果.

Bent 函数是一种特殊的布尔函数. 它在密码学、编码理论、组合数学等领域有着广泛的应用. Bent 函数的主要优点是它具有最优的非线性度,能够有效地抵抗线性攻击、最佳仿射逼近攻击和差分分析攻击等. 但是 Bent 函数也有缺陷,比如不满足平衡性, n 不能为奇数等.semi-Bent 函数可以在一定程度上弥补这种不足.

例 1 任给一个 n 元布尔函数

$f(x_1, x_2\cdots, x_n) = x_1x_{m+1} \oplus x_2x_{m+2} \oplus \cdots \oplus x_mx_{2m}$.

这里 $n \geqslant 2m$,则对任意的 $\boldsymbol{w} \in \boldsymbol{F}_2^n$,有

$$W_f(\boldsymbol{w}) = \begin{cases} (-1)^{w_1w_{m+1}\oplus w_2w_{m+2}\oplus\cdots\oplus w_mw_{2m}} 2^{n-m}, & (w_{2m+1}, w_{2m+2}, \cdots, w_n) = \boldsymbol{0}_{n-2m} \\ 0, & (w_{2m+1}, w_{2m+2}, \cdots, w_n) \neq \boldsymbol{0}_{n-2m} \end{cases}.$$

证明 任给 $\boldsymbol{w} \in \boldsymbol{F}_2^n$,由式(1)可知

$$W_f(\boldsymbol{w}) = \sum_{\boldsymbol{x}\in\boldsymbol{F}_2^n} (-1)^{f(\boldsymbol{x})\oplus\boldsymbol{w}\cdot\boldsymbol{x}} = \sum_{(x_1,x_2\cdots,x_n)\in\boldsymbol{F}_2^n} (-1)^{x_1x_{m+1}\oplus x_2x_{m+2}\oplus\cdots\oplus x_mx_{2m}\oplus x_1w_1\oplus x_2w_2\oplus\cdots\oplus x_nw_n} =$$

$$\sum_{(x_{m+1},x_{m+2},\cdots,x_{2m})\in\boldsymbol{F}_2^m} (-1)^{x_{m+1}w_{m+1}\oplus\cdots\oplus x_{2m}w_{2m}} \sum_{(x_1,x_2\cdots,x_m)\in\boldsymbol{F}_2^m} (-1)^{x_1(x_{m+1}\oplus w_1)\oplus\cdots\oplus x_m(x_{2m}\oplus w_m)} =$$

$$\sum_{(x_{2m+1},x_{2m+2},\cdots,x_n)\in\boldsymbol{F}_2^{n-2m}} (-1)^{x_{2m+1}w_{2m+1}\oplus\cdots\oplus x_nw_n}$$

下面分 2 种情形分别讨论:

1)若 $(w_{2m+1}, \cdots, w_n) \neq \boldsymbol{0}_{n-2m}$, 应用定理 1,则:

$$\sum_{(x_{2m+1},x_{2m+2},\cdots,x_n)\in\boldsymbol{F}_2^{n-2m}} (-1)^{x_{2m+1}w_{2m+1}\oplus\cdots\oplus x_nw_n} = 0.$$

所以, $W_f(\boldsymbol{w}) = 0$.

2)若 $(w_{2m+1}, \cdots, w_n) = \boldsymbol{0}_{n-2m}$,应用定理 1,则

$$\sum_{(x_{2m+1},\cdots,x_n)\in\boldsymbol{F}_2^{n-2m}} (-1)^{x_{2m+1}w_{2m+1}\oplus\cdots\oplus x_nw_n} = 2^{n-2m}.$$

应用定理 1,可得

$$W_f(\boldsymbol{w}) = \sum_{(x_{m+1},x_{m+2},\cdots,x_{2m})\in\boldsymbol{F}_2^{2m}} (-1)^{x_{m+1}w_{m+1}\oplus\cdots\oplus x_{2m}w_{2m}} \sum_{(x_1,x_2\cdots,x_m)\in\boldsymbol{F}_2^m} (-1)^{x_1(x_{m+1}\oplus w_1)\oplus\cdots\oplus x_m(x_{2m}\oplus w_m)} 2^{n-2m} =$$

$$\sum_{(x_{m+1},x_{m+2},\cdots,x_{2m})\in\boldsymbol{F}_2^m} (-1)^{x_{m+1}w_{m+1}\oplus\cdots\oplus x_{2m}w_{2m}} 2^{n-m} = (-1)^{w_1w_{m+1}\oplus w_2w_{m+2}\oplus\cdots\oplus w_mw_{2m}} 2^{n-m}.$$

综上所述,可得

$$W_f(w)=\begin{cases}(-1)^{w_1w_{m+1}\oplus w_2w_{m+2}\oplus\cdots\oplus w_mw_{2m}}2^{n-m}, & (w_{2m+1},w_{2m+2},\cdots,w_n)=\mathbf{0}_{n-2m};\\ 0, & (w_{2m+1},w_{2m+2},\cdots,w_n)\neq\mathbf{0}_{n-2m}.\end{cases}$$

说明:

分析例 1 中的结论可知当 n 与 m 的取值满足某些特殊的关系的时候,就可以得到相应的 Bent 函数以及 semi-Bent 函数.具体来说,有下面 3 种情形:

1)当 $n=2m$ 时,

$W_f(\boldsymbol{w})=(-1)^{w_1w_{m+1}\oplus w_2w_{m+2}\oplus\cdots\oplus w_mw_{2m}}2^m$.

此时 $f(x_1,x_2\cdots,x_n)$ 是个 Bent 函数,这也就是众所周知的 Rothaus Bent 函数[26-27].

2)当 $n=2m+1$ 时,

$$W_f(\boldsymbol{w})=\begin{cases}(-1)^{w_1w_{m+1}\oplus w_2w_{m+2}\oplus\cdots\oplus w_mw_{2m}}2^{m+1}, & w_{2m+1}=0;\\ 0, & w_{2m+1}\neq 0.\end{cases}$$

此时 $f(x_1,x_2\cdots,x_n)$ 是奇数个变元的 semi-Bent 函数.

3)当 $n=2m+2$ 时,

$$W_f(\boldsymbol{w})=\begin{cases}(-1)^{w_1w_{m+1}\oplus w_2w_{m+2}\oplus\cdots\oplus w_mw_{2m}}2^{m+2}, & (w_{2m+1},w_{2m+2})=(0,0);\\ 0, & (w_{2m+1},w_{2m+2})\neq(0,0).\end{cases}$$

此时 $f(x_1,x_2\cdots,x_n)$ 是偶数个变元的 semi-Bent 函数.

4)当 $n=2m+3,\cdots$ 时,不再是 Bent 函数或者 semi-Bent 函数.

对例 1 的 n 元布尔函数进行修改,加上任意的一次项,得到一个新的 n 元布尔函数 $f(x_1,x_2,\cdots,x_n)=x_1x_{m+1}\oplus x_2x_{m+2}\oplus\cdots\oplus x_mx_{2m}\oplus a_1x_1\oplus\cdots\oplus a_nx_n$,对于这个新的布尔函数,可以得到和例 1 同样的结论.下面的例 2 是对这个布尔函数的证明.

例 2 设 n 元布尔函数

$f(x_1,x_2\cdots,x_n)=x_1x_{m+1}\oplus x_2x_{m+2}\oplus\cdots\oplus x_mx_{2m}\oplus a_1x_1\oplus a_2x_2\oplus\cdots\oplus a_nx_n$,

这里 $n\geqslant 2m$,$a_i\in F_2$,则对任意的 $\boldsymbol{w}\in\boldsymbol{F}_2^n$,有

$$W_f(\boldsymbol{w})=\begin{cases}(-1)^{(w_1\oplus a_1)\,w_{m+1}\oplus\cdots\oplus(w_m\oplus a_m)\,w_{2m}}2^{n-m}, & (w_{2m+1}\oplus a_{2m+1},\cdots,w_n\oplus a_n)=\mathbf{0}_{n-2m};\\ 0, & (w_{2m+1}\oplus a_{2m+1},\cdots,w_n\oplus a_n)\neq\mathbf{0}_{n-2m}.\end{cases}$$

证明　任给 $\boldsymbol{w}\in\boldsymbol{F}_2^n$,由式(1)可知

$$W_f(\boldsymbol{w})=\sum_{x\in\boldsymbol{F}_2^n}(-1)^{f(\boldsymbol{x})\oplus\boldsymbol{w}\cdot\boldsymbol{x}}=\sum_{(x_1,x_2,\cdots,x_n)\in\boldsymbol{F}_2^n}(-1)^{x_1x_{m+1}\oplus x_2x_{m+2}\oplus\cdots\oplus x_mx_{2m}\oplus a_1x_1\oplus\cdots\oplus a_nx_n\oplus x_1w_1\oplus x_2w_2\oplus\cdots\oplus x_nw_n}=$$

$$\sum_{(x_{m+1},x_{m+2},\cdots,x_{2m})\in\boldsymbol{F}_2^m}(-1)^{x_{m+1}(w_{m+1}\oplus a_{m+1})\oplus\cdots\oplus x_{2m}(w_{2m}\oplus a_{2m})}=\sum_{(x_1,x_2,\cdots,x_m)\in\boldsymbol{F}_2^m}(-1)^{x_1(x_{m+1}\oplus w_1\oplus a_1)\oplus\cdots\oplus x_m(x_{2m}\oplus w_m\oplus a_n)}=$$

$$\sum_{(x_{2m+1},x_{2m+2},\cdots,x_n)\in\boldsymbol{F}_2^{n-2m}}(-1)^{x_{2m+1}(w_{2m+1}\oplus a_{2m+1})\oplus\cdots\oplus x_n(w_n\oplus a_n)}.$$

接着和例 1 的讨论形式一样,可以得到例 2 的结果.

说明:

1)和例 1 一样,例 2 的 n 元布尔函数当 $n=2m$ 时,是 Bent 函数;当 $n=2m+1$ 或 $2m+2$ 时,是 semi-Bent 函数.

2)例 1、例 2 中的 n 元布尔函数 $f(x_1,x_2,\cdots,x_n)$ 还可以有其他的形式,例如:$f(x_1,x_2,\cdots,x_n)=x_1x_2\oplus x_3x_4\oplus\cdots\oplus x_{2m-1}x_{2m}$ 等.这里不再一一赘述.

4　结论

1)利用 4 种数学理论证明了在编码密码中有着重要应用的指数和公式. 依据不同的证明过程,可以更清晰的明白指数和公式所蕴含的数学逻辑及其数学本质,从而可以更好地发挥它在编码密码中的实际

应用功能.

2)利用指数和公式快速地给出了 2 类 Walsh 谱值几乎最优的布尔函数的构造.如何利用指数和公式构造更有实际应用价值的旋转对称 Bent 函数以及 k -旋转对称 Bent 函数将在接下来的研究工作中进行.

参考文献:

[1] Denning D E R. Cryptography and data security 2[J]. Journal of Clinical Computing, 1982, 15(1): 11-14.

[2] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[J]. Asiacrypt, 2003, 2894(2): 452-473.

[3] Regev O . On lattices,learning with errors,random linear codes,and cryptography[C]// Proc. 37th ACM Symposium on Theory of Computing,2005. ACM,2005: 84-93.

[4] 武传坤,王新梅. Bent 函数在流密码中的应用[J]. 通信学报, 1993(4):23-27.

[5] 潘森杉,夏文涛,王良民. 流密码快速相关攻击综述[J]. 江苏大学学报(自然科学版),2017(38): 570.

[6] Dalai D K ,Maitra S . Reducing the number of Homogeneous linear equations in finding annihilators[C]// International Conference on Sequences & Their Applications. Springer-Verlag,2006: 376-390.

[7] 赵新杰, 王韬, 郭世泽,等. 分组密码 Cache 攻击技术研究[J]. 计算机研究与发展, 2012, 49(3): 453-468.

[8] Clark J A . Results on rotation symmetric bent and correlation immune Boolean functions[J]. Lecture Notes in Computer Science, 2004, 3017: 161-177.

[9] Chen Q. Research on Boolean functions of balance and strict avalanche[J]. Journal of University of Electronic Science & Technology of China,2001,32(1): 26-28.

[10] Zeng X,Carlet C,Shan J,et al. More balanced Boolean functions with optimal algebraic immunity and good nonlinearity and resistance to fast algebraic attacks[J]. Information Theory,IEEE Transactions on. 2011,57(9): 6310-6320.

[11] Li J, Carlet C, Zeng X ,et al. Two constructions of balanced Boolean functions with optimal algebraic immunity, high nonlinearity and good behavior against fast algebraic attacks[J]. Designs,Codes and Cryptography,2015,76(2): 279-305.

[12] Golić J D. Linear cryptanalysis of stream ciphers[C]//International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 1994: 154-169.

[13] Meier W, Staffelbach O. Fast correlation attacks on certain stream ciphers[J]. Journal of Cryptology, 1989, 1(3): 159-176.

[14] Courtois N . Fast algebraic attacks on stream ciphers with linear feedback[J]. Proc of Eurocrypt,2003,2656(5): 345-359.

[15] Su W, Zeng X, Hu L. Construction of 1-resilient Boolean functions with optimum algebraic immunity[J]. International Journal of Computer Mathematics,2010,88(2): 1-17.

[16] Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications[J]. Information Theory, IEEE Transactions on, 1984,30(5): 776-780.

[17] Mesnager S. A new class of bent and hyper-bent Boolean functions in polynomial forms[J]. Designs Codes & Cryptography, 2011, 59(1/3):265-279.

[18] 李春雷,张焕国,曾祥勇,等. 一类 Bent 函数的二阶非线性度下界[J]. 计算机学报,2012,35(8): 1588-1593.

[19] Su S, Tang X. Systematic constructions of rotation symmetric bent functions, 2-rotation symmetric bent functions, and bent idempotent functions[J]. IEEE Transactions on Information Theory, 2016, 63(7): 4658-4667.

[20] 黄冬梅,唐春明. 向量值 Bent 函数的一个注记[J]. 密码学报,2017(2): 9-15.

[21] Xu G,Cao X,Xu S. Several classes of quadratic ternary bent,near-bent and 2-plateaued functions[J]. International Journal of Foundations of Computer Science,2017,28(1): 1-18.

[22] Carlet C ,Gao G ,Liu W . Results on constructions of rotation symmetric bent and semi-bent functions[C]// International Conference on Sequences and Their Applications. Springer International Publishing,2014: 21-23.

[23] 肖艳, 陈媛. 奇变元 Semibent-negabent 函数的构造[J]. 数学的实践与认识, 2016, 46(11): 149-156.

[24] Dong D , Qu L , Fu S , et al. New constructions of semi-bent functions in polynomial forms[J]. Mathematical & Computer Modelling An International Journal, 2013, 57(5/6): 1139-1147.

[25] Massey J L. The theory of error-correcting codes[J]. Proceedings of the IEEE, 1980, 68(1): 185-186.

[26] Meidl W. Generalized Rothaus construction and non-weakly regular bent functions[J]. Journal of Combinatorial Theory, Series A, 2016, 141: 78-89.

[27] Zhang F ,Pasalic E ,Wei Y ,et al. Constructing bent functions outside the maiorana-mcFarland class using a general form of rothaus[J]. IEEE Transactions on Information Theory,2017,63(8): 5336-5349.