逐重量完美平衡布尔函数的构造

赵庆兰，王富佳，秦宝东
（西安邮电大学网络空间安全学院，陕西 西安 710121）

摘　要：在FLIP等同态友好流密码的背景下，逐重量完美平衡布尔函数成为密码学中研究的热点问题，但已有的研究结果构造的逐重量完美平衡布尔函数的k−重量非线性度离其上界仍有距离，基于此，提出一种新的逐重量完美平衡布尔函数的构造方法。首先，对于$m\geq4$的正整数，给出了一类2^m元的八次基础布尔函数，并利用代数正规型确定其k−重量分布。随后，通过修改此类基础函数的支撑集，构造出了一类2^m元逐重量完美平衡布尔函数，从理论上证明了其在每个非平凡等重量子集上都是平衡的。此外，分析了所提构造方法与同类构造方法之间的区别，证明了逐重量完美平衡布尔函数的代数次数。最后，与目前已有的同类函数进行比较，结果表明，新构造的8元函数在k=3和k=4时分别超过现有的k−重量非线性度，达到18和26，新构造的16元函数在k=13时的k−重量非线性度从目前最高值152提高到了160。

关键词：FLIP；逐重量完美平衡布尔函数；代数次数；重量非线性度
中图分类号：TN92
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025030

Construction of weightwise perfectly balanced Boolean functions

ZHAO Qinglan, WANG Fujia, QIN Baodong
School of Cyberspace Security, Xi’an University of Posts and Telecommunications, Xi’an 710121, China

Abstract: In the context of homomorphic-friendly stream ciphers such as FLIP, weightwise perfectly balanced Boolean functions have become a hot topic in cryptography in recent years. The k-weight nonlinearity of weightwise perfectly balanced Boolean functions constructed by existing research is still far from its upper bound. Based on this, a new construction of weightwise perfectly balanced Boolean functions was introduced. Initially, for positive integers $m\geq4$, a class of 2^m-variable Boolean functions with algebraic degree 8 was given, and their k-weight distribution was determined using algebraic normal forms. Subsequently, by modifying the support set of these basic functions, a class of 2^m-variable weightwise perfectly balanced Boolean functions was constructed. It was theoretically proven that they were balanced on every nontrivial subset with the same weight vector. Additionally, the difference between the construction methods presented and those of similar constructions was analyzed. The algebraic degree of the weightwise perfectly balanced Boolean functions is proven. Compared with existing constructions, the new 8-variable WPB function outperforms the existing k-weight nonlinearity at values of 3 and 4, reaching 18 and 26, respectively, and the new 16-variable WPB function shows enhanced k-weight nonlinearity at k=13, achieving 160, surpassing the highest value of 152 for the existing constructions.

Keywords: FLIP, weightwise perfectly balanced Boolean function, algebraic degree, weightwise nonlinearity

收稿日期：2024–10–23；**修回日期：**2025–02–10
通信作者：赵庆兰，zhaoqinglan@foxmail.com
基金项目：国家自然科学基金资助项目（No.62372370, No.61902314, No.62072371）
Foundation Items：The National Natural Science Foundation of China (No.62372370, No.61902314, No.62072371)

0 引言

全同态加密（FHE，fully homomorphic encryption）[1]技术允许用户在不解密数据密文的情况下对给定数据的密文执行计算操作，无须了解数据或计算结果的明文内容，为外包计算中的隐私保护问题提供了理论上的解决方案。然而，现有的FHE方案在每次执行同态操作时都会使噪声增加，导致明显的密文膨胀、实现效率低，这成为其实际应用的主要障碍。为此，近年来密码学界提出多种解决方案，其中之一就是混合同态加密（HHE，hybrid homomorphic encryption）方案[2]。HHE方案将对称密码（包括流密码和分组密码）与FHE相结合，客户端使用对称加密算法将明文数据加密成对称密文，并使用同态算法将对称密文进行同态加密，然后将明文的对称密文和密钥的同态密文传输至服务器端。服务器端对接收到的对称密文执行同态操作，并执行对称密码的解密电路得到明文的同态密文，然后进行后续计算任务。相较于直接使用FHE对明文数据进行同态加密，HHE的客户端仅对对称密钥进行同态加密，减轻了客户端的计算负担，有效降低了带宽需求。HHE既能保证用户的隐私，又能将昂贵的同态操作转移到云端，从而提高了同态系统的效率。

起初，研究人员尝试在混合同态系统中使用经典的对称算法，如高级数据加密标准（AES，advanced encryption standard），尽管这些算法在硬件和软件实现上比较高效，然而为了避免处理密文时出现过度膨胀，同态加密要求对称算法的电路具有较低的乘法深度和复杂度，这种需求与经典对称密码算法的设计约束不匹配，因此研究者们转向设计新型分组或流密码算法。这些新型算法具有较低的乘法深度和复杂度，能够有效提升同态加密的效率，被称为同态友好分组/流密码算法。

在2016年的欧洲密码学会议上，Méaux等[3]提出一种同态友好流密码滤波置换器族（FLIP，family of filter permutator）。FLIP密码的核心组件是滤波置换器，它由密钥寄存器、置换生成器和滤波函数3个主要部分构成。密钥寄存器用于存储密钥。置换生成器利用伪随机数生成器（PRNG，pseudo random number generator）生成新的置换P，用于重新排列密钥信息。滤波函数（为布尔函数）F则负责对置换后的密钥进行滤波。滤波置换器的结构如图1所示。与传统设计不同，所有经过置换生成器处理的密钥序列都具有相同的汉明重量，这意味着布尔函数F的输入实际上被限定在$\mathbb{F}_2^n$中具有相同汉明重量的等重量子集内。与经典流密码中布尔函数需要满足全局密码性质不同，这里的布尔函数需要在子集上满足平衡性、非线性度和代数免疫度（AI，algebraic immunity）等密码性质[4]。首先考虑平衡性，如果布尔函数在每个非平凡等重量子集上均能保持输出的平衡性，这个布尔函数就是逐重量完美平衡（WPB，weightwise perfectly balanced）函数。近年来，WPB函数是布尔函数研究的一个重要方向，主要集中在WPB函数的构造方法研究以及具有最优代数免疫度WPB函数的研究，下面给出一些主要示例。

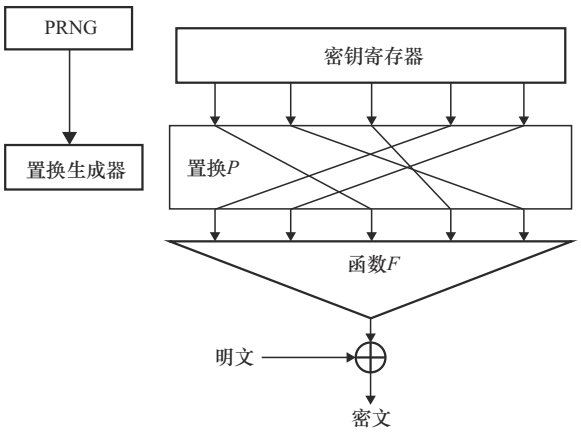


图1 滤波置换器的结构

Liu等[5]构造了一类新的2−旋转对称WPB函数，并给出了此类函数在k−重量非线性度方面的下界。

Tang等[6]构造了一类具有最优代数免疫度的WPB布尔函数。

Mesnager等[7]和Li等[8]通过修改一类线性函数[7]、两类不同的二次函数[7-8]和一类四次函数的重量支撑集来构造逐重量完美平衡布尔函数。

Zhao等[9]通过修改一类二次函数，使用迭代方法构建了一类新的WPB函数，这些函数的某些k−重量非线性度较以前的构造有明显提高。此外，Zhao等[10]推广了文献[7-8,11]中的迭代方法，并提出了一种统一的方法来构建WPB函数。

Gini等[12]研究了逐重量完美平衡布尔函数的代数免疫度，证明了WPB函数的最小代数免疫度是常数，并提出了一种生成具有最优代数免疫度的WPB函数的方法。

目前，WPB 函数的 k–重量非线性度的理论求解仍然是一个困难问题，通常采用的方法是对低元函数进行程序验证。对于低元函数，WPB 函数的 k–重量非线性度距离其上界仍有差距，构造具有更高 k–重量非线性度的 WPB 函数仍然是有必要的。本文提出一种通过调整 8 次基础函数的重量支撑集来构造 WPB 函数的方法，并对其代数次数进行分析，同时计算了其代数免疫度和 k–重量非线性度，结果表明，所构造的函数在 8 元和 16 元时的某些 k–重量非线性度超过了目前已有的最大值。

1　基础知识

1.1　布尔函数的定义与表示

令 $n \in \mathbb{Z}^+$，一个 n 元布尔函数 f 可以定义为从 n 维向量空间（$\mathbb{F}_2^n$）到 2 元有限域（$\mathbb{F}_2$）的映射。布尔函数可以通过多种方式表示，包括真值表以及代数正规型（ANF，algebraic normal form）等。为了便于阅读，本文使用+符号代替 $\oplus$ 来表示 $\mathbb{F}_2$ 中的加法。

令 $\mathcal{B}_n$ 表示所有 n 元布尔函数的集合，对于任意布尔函数 $f(x) \in \mathcal{B}_n$，其真值表可以列出所有 2^n 种输入组合对应的输出（0 或 1）。

例如，表 1 是一个 3 元函数布尔函数 $f(x_1,x_2,x_3) = 1 + x_1 + x_3 + x_1x_2 + x_1x_3 + x_1x_2x_3$ 的真值表。

表 1　　函数 $f(x_1,x_2,x_3)$ 的真值表

x_1	x_2	x_3	$f(x_1,x_2,x_3)$
0	0	0	1
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	0

ANF 是布尔函数的一种多项式表示，其中包含所有可能的变量乘积项，每个乘积项都有一个系数，系数只能是 0 或 1。对于一个 n 元布尔函数，ANF 可以表示为

$$f(x_1,x_2,\cdots,x_n) = \sum_{\boldsymbol{s} \in \mathbb{F}_2^n} c_{\boldsymbol{s}} x^{\boldsymbol{s}} \tag{1}$$

其中，$c_{\boldsymbol{s}} \in \mathbb{F}_2$，$\boldsymbol{s} = (s_1,s_2,\cdots,s_n) \in \mathbb{F}_2^n$，则 $x^{\boldsymbol{s}} = x_1^{s_1}x_2^{s_2}\cdots x_n^{s_n}$。

通过 ANF，可以计算布尔函数的代数次数，如一个 n 元布尔函数 f 代数次数为

$$\deg(f) = \max\left\{\mathrm{wt}(\boldsymbol{s}) \,\middle|\, \boldsymbol{s} \in \mathbb{F}_2^n, c_{\boldsymbol{s}} = 1\right\} \tag{2}$$

其中，$\mathrm{wt}(\boldsymbol{s})$ 为向量 $\boldsymbol{s}$ 的汉明重量，即向量 $\boldsymbol{s}$ 中非零值的个数。

若布尔函数的 ANF 表达式中只包含一次项或常数项，这意味着，布尔函数的表达式中不包含任何乘积项，即没有 2 个或更多变量相乘的情况，则将其称为仿射函数，集合记为 A_n。

Walsh 谱是分析布尔函数的非线性度、平衡性等性质的工具。一个布尔函数 f 在向量 $\boldsymbol{\alpha}$ 处的 Walsh 谱定义为

$$W_f(\boldsymbol{\alpha}) = \sum_{\boldsymbol{x} \in \mathbb{F}_2^n} (-1)^{f(\boldsymbol{x}) + \boldsymbol{x} \cdot \boldsymbol{\alpha}}, \boldsymbol{\alpha} \in \mathbb{F}_2^n \tag{3}$$

其中，$\cdot$ 表示 2 个 n 维向量的点积。

1.2　布尔函数的密码学性质

布尔函数的平衡性是密码学中一个重要的概念，它指的是一个布尔函数在所有可能的输入下输出 1 和 0 的次数相等。具体来说，对于一个 n 元布尔函数 $f(x_1,x_2,\cdots,x_n)$，如果它在 2^n 个可能的输入向量中，输出 1 的次数等于输出 0 的次数，均为 2^{n-1}，就称这个布尔函数是平衡的。

布尔函数的非线性度表示它与仿射函数的距离远近，距离越远其非线性度越高。高非线性度的布尔函数具有更好的抵抗线性攻击的能力。用 $\mathrm{NL}(f)$ 来表示布尔函数 f 的非线性度，定义式为

$$\mathrm{NL}(f) = \min_{h \in A_n} d(f,h) = \min_{h \in A_n} \left\{\boldsymbol{x} \in \mathbb{F}_2^n \middle| f(\boldsymbol{x}) \neq h(\boldsymbol{x})\right\} \tag{4}$$

其中，A_n 表示所有仿射函数的集合。

此外，非线性度还能通过 Walsh 谱来描述，如式(5)所示。

$$\mathrm{NL}(f) = 2^{n-1} - \frac{1}{2}\max_{\boldsymbol{\alpha} \in \mathbb{F}_2^n} \left|W_f(\boldsymbol{\alpha})\right| \tag{5}$$

布尔函数的代数免疫度[13]是密码学中评估算法抵抗代数攻击能力的一个重要指标。对于 $f \in \mathcal{B}_n$，其代数免疫度的表达式为

$$\mathrm{AI}(f)=\min\left\{\deg(h)\,\middle|\,f\cdot h=0 \text{ or } (f\oplus 1)\cdot h=0, 0\neq h\in\mathcal{B}_n\right\} \tag{6}$$

布尔函数密码算法的代数免疫度越高，其抵抗代数攻击的能力较强。代数免疫度的值是有上界的，上界为

$$\mathrm{AI}(f)=\left\lceil\frac{n}{2}\right\rceil \tag{7}$$

达到式(7)所示上界的布尔函数被称为具有最优代数免疫度的布尔函数。

1.3 逐重量完美平衡布尔函数

对于$0\leqslant k\leqslant n$，向量空间$\mathbb{F}_2^n$中的等重量子集$E_{n,k}$定义为

$$E_{n,k}=\left\{\boldsymbol{x}\in\mathbb{F}_2^n\,\middle|\,\mathrm{wt}(\boldsymbol{x})=k\right\} \tag{8}$$

其中，$\mathrm{wt}(\boldsymbol{x})$表示向量$\boldsymbol{x}$的汉明重量，$E_{n,0}$和$E_{n,n}$为平凡等重量子集，其余的为非平凡等重量子集。

逐重量完美平衡布尔函数f满足$f(\mathbf{0}_n)+f(\mathbf{1}_n)=1$（$\mathbf{1}_n$表示全1向量，$\mathbf{0}_n$表示全0向量），同时在所有的非平凡等重量子集上都具有平衡性，也就是满足条件$\sum_{\boldsymbol{x}\in E_{n,k}}(-1)^{f(x)}=0,\ 1\leqslant k\leqslant n-1$。

逐重量完美平衡布尔函数所满足的基本条件为：对于任意的$1\leqslant k\leqslant n$，必须满足$\binom{n}{k}$为偶数，这意味着n为2的幂次。

为了研究逐重量完美平衡布尔函数的密码学性质，下面介绍限制在等重量子集上的局部密码学性质的定义。

对于任意布尔函数f，其k-重量支撑集为

$$\mathrm{supp}_k(f)=\left\{x\in E_{n,k}\,\middle|\,f(x)=1\right\} \tag{9}$$

函数f的k汉明重量（简称k-重量）为

$$\mathrm{wt}_k(f)=\left|\mathrm{supp}_k(f)\right| \tag{10}$$

k-重量非线性度是布尔函数的输入限制在等重量子集$E_{n,k}$上的非线性性质，用$\mathrm{NL}_k(f)$表示。

命题1 k-重量非线性度的表达式[4]为

$$\mathrm{NL}_k(f)=\frac{|E_{n,k}|}{2}-\frac{1}{2}\max_{\boldsymbol{\omega}\in\mathbb{F}_2^n}\left|\sum_{\boldsymbol{x}\in E_{n,k}}(-1)^{f(x)+\boldsymbol{\omega}\cdot\boldsymbol{x}}\right| \tag{11}$$

命题2 k-重量非线性度的下界[4]是

$$\mathrm{NL}_k(f)\leqslant\left\lfloor\frac{|E_{n,k}|}{2}-\frac{\sqrt{|E_{n,k}|}}{2}\right\rfloor=\left\lfloor\frac{1}{2}\binom{n}{k}-\frac{1}{2}\sqrt{\binom{n}{k}}\right\rfloor \tag{12}$$

1.4 2个组合数公式

为了方便本文后续的证明和讨论，介绍2个基础的组合数公式。

引理1 Pascal公式。假设h和g是2个非负整数，则有

$$\binom{h}{g}+\binom{h}{g+1}=\binom{h+1}{g+1} \tag{13}$$

引理2 Chu-Vandermonde公式[14]。假设h、g和q是3个非负整数，则有

$$\sum_{i=0}^{q}\binom{h}{i}\binom{g}{q-i}=\binom{h+g}{q} \tag{14}$$

2 一类八次基础布尔函数

本节首先引入了一类具有2^m变量的八次基础布尔函数。随后，通过对此类基础函数的代数正规型的分析，求解其k-重量表达式。

令m为正整数且$m\geqslant 4$，定义一类2^m元八次布尔函数h_m为

$$h_m(\boldsymbol{x})=\sum_{i=1}^{2^{m-1}}x_i+\sum_{i=1}^{2^{m-1}}\prod_{q=0}^{1}x_{i+q2^{m-2}}+\sum_{i=1}^{2^{m-2}}\prod_{q=0}^{3}x_{i+q2^{m-3}}+\sum_{i=1}^{2^{m-3}}\prod_{q=0}^{7}x_{i+q2^{m-4}} \tag{15}$$

其中，$\boldsymbol{x}=\left(x_1,x_2,\cdots,x_{2^m}\right)\in\mathbb{F}_2^{2^m}$。

对于式(15)中所定义的基础函数h_m，下面给出$m=4$和$m=5$这2个例子。

当$m=4$时，函数$h_m(x_1,x_2,\cdots,x_{2^m})$的具体表达式为

$$h_4(x_1,x_2,\cdots,x_{16})=\sum_{i=1}^{8}x_i+\sum_{i=1}^{8}x_ix_{i+4}+\sum_{i=1}^{4}x_ix_{i+2}x_{i+4}x_{i+6}+\sum_{i=1}^{2}x_ix_{i+1}x_{i+2}x_{i+3}x_{i+4}x_{i+5}x_{i+6}x_{i+7}$$

当$m=5$时，函数$h_m(x_1,x_2,\cdots,x_{2^m})$的具体表达式为

$$h_5(x_1,x_2,\cdots,x_{32})=\sum_{i=1}^{16}x_i+\sum_{i=1}^{16}x_ix_{i+8}+\sum_{i=1}^{8}x_ix_{i+4}x_{i+8}x_{i+12}+\sum_{i=1}^{4}x_ix_{i+2}x_{i+4}x_{i+6}x_{i+8}x_{i+10}x_{i+12}x_{i+14}$$

通过执行计算机程序，得到了函数h_4的k-重

量分布，其结果如表2所示。表2表明，当k为奇数时，函数h_4在对应的等重量子集上输出是平衡的；当k为偶数时，输出是不平衡的。

表2　　函数h_4的k-重量分布

k	$\mathrm{wt}_k(h_4)$	$\frac{1}{2}\binom{16}{k}$
1	8	8
2	64	60
3	280	280
4	896	910
5	2 184	2 184
6	4 032	4 004
7	5 720	5 720
8	6 400	6 435
9	5 720	5 720
10	4 032	4 004
11	2 184	2 184
12	896	910
13	280	280
14	64	60
15	8	8

引理3　当$m \geqslant 5$时，式(15)中所定义的2^m元八次函数h_m满足

$$h_m(\boldsymbol{x}) = h_{m-1}(\boldsymbol{x}') + h_{m-1}(\boldsymbol{x}'') \tag{16}$$

其中，$\boldsymbol{x}' = (x_1, x_3, \cdots, x_{2^m-1})$，$\boldsymbol{x}'' = (x_2, x_4, \cdots, x_{2^m})$。

证明　当$m \geqslant 5$时，式(16)中的$h_{m-1}(\boldsymbol{x}')$和$h_{m-1}(\boldsymbol{x}'')$的函数表达式分别表示为

$$h_{m-1}(\boldsymbol{x}') = \sum_{i=1}^{2^{m-2}} x_{2i-1} + \sum_{i=1}^{2^{m-2}} \prod_{q=0}^{1} x_{2i-1+q2^{m-2}} + \sum_{i=1}^{2^{m-3}} \prod_{q=0}^{3} x_{2i-1+q2^{m-3}} + \sum_{i=1}^{2^{m-4}} \prod_{q=0}^{7} x_{2i-1+q2^{m-4}}$$

$$h_{m-1}(\boldsymbol{x}'') = \sum_{i=1}^{2^{m-2}} x_{2i} + \sum_{i=1}^{2^{m-2}} \prod_{q=0}^{1} x_{2i+q2^{m-2}} + \sum_{i=1}^{2^{m-3}} \prod_{q=0}^{3} x_{2i+q2^{m-3}} + \sum_{i=1}^{2^{m-4}} \prod_{q=0}^{7} x_{2i+q2^{m-4}}$$

因此有

$$h_{m-1}(\boldsymbol{x}') + h_{m-1}(\boldsymbol{x}'') = \sum_{i=1}^{2^{m-2}} (x_{2i-1} + x_{2i}) + \left(\prod_{q=0}^{1} x_{2i-1+q2^{m-2}} + \prod_{q=0}^{1} x_{2i+q2^{m-2}} \right) + \left(\prod_{q=0}^{3} x_{2i-1+q2^{m-3}} + \sum_{i=1}^{2^{m-3}} \prod_{q=0}^{3} x_{2i+q2^{m-3}} \right) + \sum_{i=1}^{2^{m-4}} \left(\prod_{q=0}^{7} x_{2i-1+q2^{m-4}} + \sum_{i=1}^{2^{m-4}} \prod_{q=0}^{7} x_{2i+q2^{m-4}} \right) = \sum_{i=1}^{2^{m-1}} x_i + \sum_{i=1}^{2^{m-1}} \prod_{q=0}^{1} x_{i+q2^{m-2}} + \sum_{i=1}^{2^{m-2}} \prod_{q=0}^{3} x_{i+q2^{m-3}} + \sum_{i=1}^{2^{m-3}} \prod_{q=0}^{7} x_{i+q2^{m-4}} = h_m(\boldsymbol{x})$$

证毕。

根据式(9)和式(16)，函数h_m的k-重量支撑集可以表示为

$$\begin{aligned} &\mathrm{supp}_k\left(h_m(\boldsymbol{x})\right) = \\ &\bigcup_{i=0}^{k} \left\{ \boldsymbol{x} \in \mathbb{F}_2^{2^m} \middle| \boldsymbol{x}' \in \mathrm{supp}_i\left(h_{m-1}(\boldsymbol{x}')\right), \right. \\ &\left. \boldsymbol{x}'' \in \mathrm{zeros}_{k-i}\left(h_{m-1}(\boldsymbol{x}'')\right) \right\} \cup \\ &\left\{ \boldsymbol{x} \in \mathbb{F}_2^{2^m} \middle| \boldsymbol{x}' \in \mathrm{zeros}_i\left(h_{m-1}(\boldsymbol{x}')\right), \right. \\ &\left. \boldsymbol{x}'' \in \mathrm{supp}_{k-i}\left(h_{m-1}(\boldsymbol{x}'')\right) \right\} \end{aligned}$$

其中，$\mathrm{zeros}_k(f)$表示布尔函数f的输出值为0时的汉明重量为k的输入向量集合。

根据式(10)，函数h_m的k-重量表达式为

$$\mathrm{wt}_k\left(h_m\right) = 2\sum_{i=0}^{k} \mathrm{wt}_i\left(h_{m-1}\right)\left[\binom{2^{m-1}}{k-i} - \mathrm{wt}_{k-i}\left(h_{m-1}\right)\right] \tag{17}$$

定理1　式(15)定义的函数h_m的k-重量的表达式为

$$\mathrm{wt}_k\left(h_m\right) = \begin{cases} \frac{1}{2}\binom{2^m}{k}, & k \not\equiv 0 \pmod 2 \\ \frac{1}{2}\binom{2^m}{k} - \frac{(-1)^{\frac{k}{2}}}{2}\binom{2^{m-1}}{\frac{k}{2}}, & k \equiv 0 \pmod 2 \end{cases} \tag{18}$$

其中，$0 \leqslant k \leqslant 2^m, m \geqslant 4$。

证明　利用数学归纳法证明。

由表2可知，当$m = 4$时，函数$h_4(x_1, x_2, \cdots, x_{16})$的$k$-重量满足定理1。假设当$m \geqslant 5$时，定理1

在$m-1$时成立，即

$$\mathrm{wt}_k(h_{m-1})=\begin{cases}\dfrac{1}{2}\binom{2^{m-1}}{k}, & k\not\equiv 0(\bmod 2)\\ \dfrac{1}{2}\binom{2^{m-1}}{k}-\dfrac{(-1)^{\frac{k}{2}}}{2}\binom{2^{m-2}}{\frac{k}{2}}, & k\equiv 0(\bmod 2)\end{cases}\tag{19}$$

接下来，将k分为偶数、奇数2种情况展开讨论。

1) 当$k\not\equiv 0(\bmod 2)$时，有2种情况，即$i\not\equiv 0(\bmod 2)$，$k-i\equiv 0(\bmod 2)$和$i\equiv 0(\bmod 2)$，$k-i\not\equiv 0(\bmod 2)$。

根据式(17)中函数h_m的k-重量表达式，可以得到

$$\mathrm{wt}_k(h_m)=2\sum_{i=0}^{k}\mathrm{wt}_i(h_{m-1})\left[\binom{2^{m-1}}{k-i}-\mathrm{wt}_{k-i}(h_{m-1})\right]$$

然后，将其代入式(19)中h_{m-1}的k-重量表达式得到

$$\mathrm{wt}_k(h_m)=2\sum_{\substack{i=0\\ i\not\equiv 0(\bmod 2)\\ k-i\equiv 0(\bmod 2)}}^{k}\left[\frac{1}{4}\binom{2^{m-1}}{i}\binom{2^{m-1}}{k-i}+\frac{(-1)^{\frac{k-i}{2}}}{4}\binom{2^{m-1}}{i}\binom{2^{m-2}}{\frac{k-i}{2}}\right]+$$

$$2\sum_{\substack{i=0\\ i\equiv 0(\bmod 2)\\ k-i\not\equiv 0(\bmod 2)}}^{k}\left[\frac{1}{4}\binom{2^{m-1}}{i}\binom{2^{m-1}}{k-i}-\frac{(-1)^{\frac{i}{2}}}{4}\binom{2^{m-1}}{k-i}\binom{2^{m-2}}{\frac{i}{2}}\right]$$

通过变量替换，令$j=k-i$，有

$$\sum_{\substack{i=0\\ i\not\equiv 0(\bmod 2)\\ k-i\equiv 0(\bmod 2)}}^{k}\frac{(-1)^{\frac{k-i}{2}}}{4}\binom{2^{m-1}}{i}\binom{2^{m-2}}{\frac{k-i}{2}}=\sum_{\substack{i=0\\ k-j\not\equiv 0(\bmod 2)\\ j\equiv 0(\bmod 2)}}^{k}\frac{(-1)^{\frac{j}{2}}}{4}\binom{2^{m-1}}{k-j}\binom{2^{m-2}}{\frac{j}{2}}=\sum_{\substack{i=0\\ k-i\not\equiv 0(\bmod 2)\\ i\equiv 0(\bmod 2)}}^{k}\frac{(-1)^{\frac{i}{2}}}{4}\binom{2^{m-1}}{k-i}\binom{2^{m-2}}{\frac{i}{2}}$$

所以，能够消除公式中$\frac{(-1)^{\frac{k-i}{2}}}{4}\binom{2^{m-1}}{i}\binom{2^{m-2}}{\frac{k-i}{2}}$和$\frac{(-1)^{\frac{i}{2}}}{4}\binom{2^{m-1}}{k-i}\binom{2^{m-2}}{\frac{i}{2}}$两部分，得到如下等式

$$\mathrm{wt}_k(h_m)=2\sum_{\substack{i=0\\ i\equiv 0(\bmod 2)\\ k-i\not\equiv 0(\bmod 2)}}^{k}\left[\frac{1}{4}\binom{2^{m-1}}{i}\binom{2^{m-1}}{k-i}\right]$$

最后，将其代入引理2中的式(14)得到

$$\mathrm{wt}_k(h_m)=\frac{1}{2}\binom{2^m}{k}$$

2) 当$k\equiv 0(\bmod 2)$时，有2种情况，即$i\not\equiv 0(\bmod 2)$，$k-i\not\equiv 0(\bmod 2)$和$i\equiv 0(\bmod 2)$，$k-i\equiv 0(\bmod 2)$。

与上述当$k\not\equiv 0(\bmod 2)$时的证明原理思路类似，由式(17)、式(19)、变量替换和引理2中的式(14)能够得出

$$\mathrm{wt}_k(h_m)=2\sum_{i=0}^{k}\mathrm{wt}_i(h_{m-1})\left[\binom{2^{m-1}}{k-i}-\mathrm{wt}_{k-i}(h_{m-1})\right]=\frac{1}{2}\binom{2^m}{k}-\frac{(-1)^{\frac{k}{2}}}{2}\binom{2^{m-1}}{\frac{k}{2}}$$

证毕。

由式(18)可知，当k为奇数时，函数在k-等重量子集上是平衡的；当k为偶数时，函数在k-等重量子集上是不平衡的。基于这个结果，接下来将通过修改函数h_m的重量支撑集来构造2^m变量的WPB函数。

3　逐重量完美平衡布尔函数

3.1　构造WPB函数

现在，对式(15)中定义的函数$h_m(\boldsymbol{x})$的支撑集进行修改构造2^m元WPB函数g_m，其表达式如下。

当$m=1$时

$$g_1(\boldsymbol{x})=x_1$$

当$m=2$时

$$g_2(\boldsymbol{x}) = x_1 + x_2 + x_1x_3$$

当$m = 3$时

$$\begin{aligned} g_3(\boldsymbol{x}) = {} & x_3 + x_4 + x_7 + x_8 + \\ & x_1x_4 + x_2x_3 + x_3x_4 + \\ & x_5x_8 + x_6x_7 + x_7x_8 + x_1x_2x_3 + \\ & x_1x_3x_4 + x_5x_6x_7 + x_5x_7x_8 + x_1x_2x_3x_4 \end{aligned}$$

当$m \geqslant 4$时

$$g_m(\boldsymbol{x}) = h_m(\boldsymbol{x}) + g_{m-1}\left(x_1,x_2,\cdots,x_{2^{m-1}}\right) \cdot \prod_{i=1}^{2^{m-1}}\left(x_i + x_{2^{m-1}+i} + 1\right) \tag{20}$$

其中，$\boldsymbol{x} = \left(x_1,x_2,\cdots,x_{2^m}\right)$，$h_m(\boldsymbol{x})$为式(15)所定义的函数。

通过程序验证，式(20)中$g_1(\boldsymbol{x})$、$g_2(\boldsymbol{x})$和$g_3(\boldsymbol{x})$为逐重量完美平衡布尔函数。为了证明当$m \geqslant 4$时$g_m(\boldsymbol{x})$的逐重量平衡性，接下来将分析函数$g_m(\boldsymbol{x})$的k–重量支撑集。

引理 4　当$m \geqslant 4$时，函数$g_m(\boldsymbol{x})$的k–重量支撑集的表达式为

$$\mathrm{supp}_k\left(g_m\right) = \begin{cases} \mathrm{supp}_k\left(h_m\right), & k \not\equiv 0 \pmod 2 \\ \mathrm{supp}_k\left(h_m\right) \cup A \backslash B, & k \equiv 0 \pmod 2 \end{cases} \tag{21}$$

其中，$A = \{(\ddot{\boldsymbol{x}},\ddot{\boldsymbol{x}}) | \ddot{\boldsymbol{x}} \in \mathrm{supp}_{\frac{k}{2}}\left(g_{m-1}\right)\}$，$B = \left\{(\ddot{\boldsymbol{x}},\ddot{\boldsymbol{x}}) | \ddot{\boldsymbol{x}} \in \mathrm{supp}_{\frac{k}{2}}\left(g_{m-1}\right), \mathrm{wt}(\ddot{\boldsymbol{x}}) \not\equiv 0 \pmod 2\right\}$，函数$h_m$为式(15)所定义的函数，$\boldsymbol{x}$是由2个相同的向量$\ddot{\boldsymbol{x}}$组成的，$\ddot{\boldsymbol{x}} = (x_1,x_2,\cdots,x_{2^{m-1}})$，并且$\boldsymbol{x} = (\ddot{\boldsymbol{x}},\ddot{\boldsymbol{x}}) \in \mathbb{F}_2^{2^m}$，$0 \leqslant k \leqslant 2^m$。

证明　当$m \geqslant 4$时，对于式(20)中所定义的函数$g_m(\boldsymbol{x})$中的累乘式部分进行分析。对于所有的i，只有当x_i和$x_{2^{m-1}+i}$相等时，表达式$\prod_{i=1}^{2^{m-1}}\left(x_i + x_{2^{m-1}+i} + 1\right)$的值为1。

根据k的不同取值，将证明过程分为2种情况。

1) 当$k \not\equiv 0 \pmod 2$时，其k–重量支撑集为

$$\begin{aligned} & \mathrm{supp}_k(g_m) = \\ & \mathrm{supp}_k(h_m) \cup \{(\ddot{\boldsymbol{x}},\ddot{\boldsymbol{x}}) | \ddot{\boldsymbol{x}} \in \mathrm{supp}_{\frac{k}{2}}(g_{m-1})\} \backslash \\ & \quad \{(\ddot{\boldsymbol{x}},\ddot{\boldsymbol{x}}) | \ddot{\boldsymbol{x}} \in \mathrm{supp}_{\frac{k}{2}}(g_{m-1}), h_m(\ddot{\boldsymbol{x}},\ddot{\boldsymbol{x}}) = 1\} = \\ & \mathrm{supp}_k(h_m) \end{aligned}$$

当$k \not\equiv 0 \pmod 2$时，$\frac{k}{2}$不是整数，所以$\mathrm{supp}_{\frac{k}{2}}(g_{m-1})$是空集。

2) 当$k \equiv 0 \pmod 2$时，其k–重量支撑集为

$$\begin{aligned} & \mathrm{supp}_k(g_m) = \\ & \mathrm{supp}_k(h_m) \cup \{(\ddot{\boldsymbol{x}},\ddot{\boldsymbol{x}}) | \ddot{\boldsymbol{x}} \in \mathrm{supp}_{\frac{k}{2}}(g_{m-1})\} \backslash \\ & \{(\ddot{\boldsymbol{x}},\ddot{\boldsymbol{x}}) | \ddot{\boldsymbol{x}} \in \mathrm{supp}_{\frac{k}{2}}(g_{m-1}), h_m(\ddot{\boldsymbol{x}},\ddot{\boldsymbol{x}}) = 1\} = \\ & \mathrm{supp}_k(h_m) \cup \{(\ddot{\boldsymbol{x}},\ddot{\boldsymbol{x}}) | \ddot{\boldsymbol{x}} \in \mathrm{supp}_{\frac{k}{2}}(g_{m-1})\} \backslash \\ & \{(\ddot{\boldsymbol{x}},\ddot{\boldsymbol{x}}) | \ddot{\boldsymbol{x}} \in \mathrm{supp}_{\frac{k}{2}}(g_{m-1}), \mathrm{wt}(\ddot{\boldsymbol{x}}) \not\equiv 0 \pmod 2\} \end{aligned}$$

其中，$h_m(\ddot{\boldsymbol{x}},\ddot{\boldsymbol{x}}) = 1$和$\mathrm{wt}(\ddot{\boldsymbol{x}}) \not\equiv 0 \pmod 2$等价的原因如下

$$\begin{aligned} & h_m(\ddot{\boldsymbol{x}},\ddot{\boldsymbol{x}}) = x_1 + x_2 + \cdots + x_{2^{m-1}} + \sum_{i=1}^{2^{m-2}} x_i x_{i+2^{m-2}} + \sum_{i=1}^{2^{m-2}} x_{2^{m-2}+i} x_i + \\ & \sum_{i=1}^{2^{m-3}} x_i x_{i+2^{m-3}} x_{i+2^{m-2}} x_{i+3\cdot 2^{m-3}} + \sum_{i=1}^{2^{m-3}} x_{2^{m-3}+i} x_{2^{m-2}+i} x_{3\cdot 2^{m-3}+i} x_i + \\ & \sum_{i=1}^{2^{m-4}} x_i x_{i+2^{m-4}} x_{i+2^{m-3}} x_{i+3\cdot 2^{m-4}} x_{i+2^{m-2}} x_{i+5\cdot 2^{m-4}} x_{i+3\cdot 2^{m-3}} x_{i+7\cdot 2^{m-4}} + \\ & \sum_{i=1}^{2^{m-4}} x_{2^{m-4}+i} x_{2^{m-3}+i} x_{3\cdot 2^{m-4}+i} x_{2^{m-2}+i} x_{5\cdot 2^{m-4}+i} x_{3\cdot 2^{m-3}+i} x_{7\cdot 2^{m-4}+i} x_i = \\ & x_1 + x_2 + \cdots + x_{2^{m-1}} = \mathrm{wt}(\ddot{\boldsymbol{x}}) \bmod 2 \end{aligned}$$

除了一次项，其他代数次数相同的项都可以抵消，所以最后结果为$\mathrm{wt}(\ddot{\boldsymbol{x}}) \bmod 2$。

证毕。

定理 2　当$m \geqslant 4$时，函数$g_m(\boldsymbol{x})$的k–重量的表达式为

$$\mathrm{wt}_k\left(g_m\right) = \begin{cases} \mathrm{wt}_k\left(h_m\right), & k \not\equiv 0 \pmod 2 \\ \mathrm{wt}_k\left(h_m\right) + \mathrm{wt}_{\frac{k}{2}}\left(g_{m-1}\right) - 2\gamma, & k \equiv 0 \pmod 2 \end{cases} \tag{22}$$

其中，$\gamma = |\{(\ddot{\boldsymbol{x}},\ddot{\boldsymbol{x}}) | \ddot{\boldsymbol{x}} \in \mathrm{supp}_{\frac{k}{2}}\left(g_{m-1}\right), \mathrm{wt}(\ddot{\boldsymbol{x}}) \not\equiv$

$0(\mathrm{mod}\,2)\}|$。

由引理4容易推出，证明从略。

定理3 对于正整数m，函数$g_m(\boldsymbol{x})$是逐重量完美平衡布尔函数。

证明 使用数学归纳法来完成证明。

对于函数$g_m(\boldsymbol{x})$，其中$g_1(\boldsymbol{x})$、$g_2(\boldsymbol{x})$和$g_3(\boldsymbol{x})$已经通过程序分析被验证为逐重量完美平衡布尔函数。当$m \geqslant 4$时，假设函数$g_{m-1}(\boldsymbol{x})$是WPB函数，在$1 \leqslant k \leqslant 2^{m-1}-1$情况下，满足

$$\mathrm{wt}_k\left(g_{m-1}\right)=\frac{1}{2}\binom{2^m}{k} \tag{23}$$

并且当$k=0$时，$\mathrm{wt}_0\left(g_{m-1}\right)=0$；当$k=2^{m-1}$时，$\mathrm{wt}_{2^{m-1}}\left(g_{m-1}\right)=1$。

接下来开始证明当$m \geqslant 4$时，函数$g_m(\boldsymbol{x})$是WPB函数。根据k的不同取值，计算函数$g_m(\boldsymbol{x})$的k–重量。

1) 当$k \not\equiv 0 \pmod 2$（即k为奇数）时，由式(18)和式(22)可得出

$$\mathrm{wt}_k\left(g_m\right)=\mathrm{wt}_k\left(h_m\right)=\frac{1}{2}\binom{2^m}{k}$$

2) 当$k \equiv 0 \pmod 2$（即k为偶数）时，分以下2种情况讨论。

① 当$k \equiv 0 \pmod 2$时，并且$k \neq 0,\ 2^m$且$\frac{k}{2}$为奇数时，由式(18)、式(22)和式(23)可得

$$\mathrm{wt}_k\left(g_m\right)=\mathrm{wt}_k\left(h_m\right)+\mathrm{wt}_{\frac{k}{2}}\left(g_{m-1}\right)-2\gamma=$$

$$\mathrm{wt}_k\left(h_m\right)+\mathrm{wt}_{\frac{k}{2}}\left(g_{m-1}\right)-2\left|\left\{\mathrm{supp}_{\frac{k}{2}}\left(g_{m-1}\right)\right\}\right|=$$

$$\frac{1}{2}\binom{2^m}{k}-\frac{(-1)^{\frac{k}{2}}}{2}\binom{2^{m-1}}{\frac{k}{2}}+\frac{1}{2}\binom{2^{m-1}}{\frac{k}{2}}-$$

$$2\times\frac{1}{2}\binom{2^{m-1}}{\frac{k}{2}}=\frac{1}{2}\binom{2^m}{k}$$

② 当$k \equiv 0 \pmod 2$时，并且$k \neq 0,2^m$且$\frac{k}{2}$为偶数时，由式(18)、式(22)和式(23)可得

$$\mathrm{wt}_k\left(g_m\right)=\mathrm{wt}_k\left(h_m\right)+\mathrm{wt}_{\frac{k}{2}}\left(g_{m-1}\right)=\frac{1}{2}\binom{2^m}{k}$$

成立，这是因为集合$\{(\ddot{\boldsymbol{x}},\ddot{\boldsymbol{x}})|\ddot{\boldsymbol{x}} \in \mathrm{supp}_{\frac{k}{2}}\left(g_{m-1}\right),\mathrm{wt}(\ddot{\boldsymbol{x}}) \not\equiv 0 \pmod 2\}$为空集。

3) 当$k=0$时，由$\mathrm{wt}_0\left(g_{m-1}\right)=0$、式(18)和式(22)可得

$$\mathrm{wt}_0\left(g_m\right)=\mathrm{wt}_0\left(h_m\right)+\mathrm{wt}_0\left(g_{m-1}\right)=0$$

4)当$k=2^m$时，由$\mathrm{wt}_{2^{m-1}}\left(g_{m-1}\right)=1$、式(18)和式(22)可得

$$\mathrm{wt}_{2^m}\left(g_m\right)=\mathrm{wt}_{2^m}\left(h_m\right)+\mathrm{wt}_{2^{m-1}}\left(g_{m-1}\right)=1$$

综上所述，函数$g_m(\boldsymbol{x})$是逐重量完美平衡布尔函数。证毕。

3.2 WPB函数结构分析

本文在文献[9]和文献[15]的理论基础上进行了进一步的分析和构造，采用基础函数h_m的表示形式，并借鉴文献[10]中基础函数$f_{m;d}(x)$的定义。

虽然本文的基础函数h_m和文献[10]中的基础函数$f_{m;4}(x)$在形式上看似相同，但在二次项中所选择的项数不同，导致所得基础函数的重量支撑集存在差异。这种差异进一步造成了WPB函数构造过程中的乘积项不同，使得最终得到的函数在代数次数、k–非线性度和代数免疫度等关键密码学性质上也不相同。因此，本文给出的构造函数与文献[10]所描述的函数不同。

本文采用迭代方法对基础函数的重量支撑集进行修改，以构造WPB函数。该构造方法在本质上依赖于所选用的基础函数的构造方式。为了便于分析，本文选择了3种不同的基础函数，它们的表示形式均参照文献[10]中定义的基础函数$f_{m;d}(x)$。

文献[9]中的基础函数定义为

$$h_m(\boldsymbol{x})=\sum_{i=1}^{2^{m-1}}x_i+\sum_{i=1}^{2^{m-1}}\prod_{q=0}^{1}x_{i+q2^{m-2}}$$

文献[15]中的基础函数定义为

$$h_m(\boldsymbol{x})=\sum_{i=1}^{2^{m-1}}x_i+\sum_{i=1}^{2^{m-1}}\prod_{q=0}^{1}x_{i+q2^{m-2}}+\sum_{i=1}^{2^{m-2}}\prod_{q=0}^{3}x_{i+q2^{m-3}}$$

通过比较可以观察到，尽管文献[15]中的基础函数在一次项和二次项上与文献[9]相同，但它还包含额外的四次项。

本文提出的基础函数定义为

$$h_m(\boldsymbol{x})=\sum_{i=1}^{2^{m-1}}x_i+\sum_{i=1}^{2^{m-1}}\prod_{q=0}^{1}x_{i+q2^{m-2}}+$$

$$\sum_{i=1}^{2^{m-2}}\prod_{q=0}^{3}x_{i+q2^{m-3}}+\sum_{i=1}^{2^{m-3}}\prod_{q=0}^{7}x_{i+q2^{m-4}}$$

与文献[15]相比，本文的基础函数在一次项、二次项和四次项上保持一致，并新增了一个八次项部分。

与文献[9]和文献[15]所描述的方法不同，本文构造的WPB函数需要从16元开始迭代，因此首先需要构造一个8元WPB函数。根据文献[4]中的定理1，如果f、e、f'是3个n元WPB函数，q是任意的n元布尔函数，则存在一个$2n$元的WPB函数$h(\boldsymbol{x},\boldsymbol{y})$，其定义为$h(\boldsymbol{x},\boldsymbol{y})=f(\boldsymbol{x})+\prod_{i=1}^{n}x_i+e(\boldsymbol{y})+(f(\boldsymbol{x})+f'(\boldsymbol{x}))q'(\boldsymbol{y})$，其中$\boldsymbol{x},\boldsymbol{y}\in\mathbb{F}_2^n$。

利用计算机程序搜寻4元WPB函数，共发现720个，用集合符号B_4表示。进一步计算这些函数的k−重量非线性度，并排除那些k−重量非线性度全为0的函数，得到B_4的子集b_4。接下来，将b_4中的每个函数作为定理中的$f(\boldsymbol{x})$和$e(\boldsymbol{y})$，令$q'(\boldsymbol{y})$为0，根据文献[4]中的定理1，构造出384个8元WPB函数，用集合符号B_8表示。再计算集合B_8中所有函数的k−重量非线性度，选取k−重量非线性度较高的48个函数并用集合符号b_8表示。最终，从b_8中选择一个合适的8元WPB函数作为g_3。

3.3　WPB函数代数次数

定理4　本文所构造的WPB函数$g_m(\boldsymbol{x})$的代数次数为

$$\deg(g_m)=\begin{cases}1, & m=1\\ 2, & m=2\\ 2^m-4, & m\geqslant 3\end{cases}\tag{24}$$

证明　利用数学归纳法证明。

由WPB函数$g_m(\boldsymbol{x})$具体表达式可知，$g_1(\boldsymbol{x})$、$g_2(\boldsymbol{x})$和$g_3(\boldsymbol{x})$的代数次数分别为1、2和4。

当$m\geqslant 4$时，假设式(24)在$m-1$时成立，即

$$\deg(g_{m-1})=2^{m-1}-4\tag{25}$$

由式(20)定义的函数$g_m(\boldsymbol{x})$的具体表达式和式(25)可以推出

$$\deg(g_m)=$$
$$\max\left\{\deg(h_m),\deg(g_{m-1})+\deg\left(\prod_{i=1}^{2^{m-1}}(x_i+x_{i+2^{m-1}}+1)\right)\right\}=$$
$$\max\{8,\ 2^{m-1}-4+2^{m-1}\}=2^m-4$$

证毕。

4　非线性度和代数免疫度

通过计算机程序计算本文所构造的WPB函数g_m在8元和16元情况下的k−重量非线性度，并与现有文献中通过修改重量支撑集构造的WPB函数进行比较。表3和表4分别为本文所构造的8元和16元WPB函数的k−重量非线性度与现有文献的对比。

从表3可以看出，本文构造的8元WPB函数g_3在$k=3$、4情况下的k−重量非线性度高于现有的构造。

从表4可以看出，与文献[9]相比，当$k=4$、12、13、14时，本文方法在k−重量非线性度上实现了提升；与文献[15]相比，本文方法在$k=1$、2、3、4、5、7、8时能够保持与原有结果相同的值，并在$k=6$、9、10、11、12、13、14时其k−重量非线性度都有所提升。此外，当$k=13$时，本文所构造的16元WPB函数的k−重量非线性度高于现有的同类函数，达到了160。

此外，本节计算了本文所构造的WPB函数在4元、8元和16元情况下的代数免疫度，结果如表5所示。由表5可以看出，当$m=2$、3时，本文构造的WPB函数具有最优代数免疫度；当$m=3$、4时，本文构造的WPB函数的代数免疫度均有所提高，且在$m=3$时达到了最优值4。

表3　　**8元WPB函数的k−重量非线性度**

k	NL							上界
	文献[7]	文献[8]	文献[9]	文献[11]	文献[15]	文献[16]	本文	
2	2	2	6	2	6	2	6	11
3	14	12	17	12	17	12	18	24
4	19	19	23	19	23	19	26	30
5	14	12	17	12	16	12	12	24
6	2	2	6	6	5	6	6	11

表4 16元WPB函数的k-重量非线性度

k	NL							上界
	文献[7]	文献[8]	文献[9]	文献[11]	文献[15]	文献[16]	本文	
2	4	4	12	4	12	4	12	54
3	112	56	104	56	104	56	104	268
4	686	350	590	350	594	350	594	888
5	1 806	1 312	1 765	1 288	1 750	1 288	1 750	2 150
6	3 436	3 176	3 487	3 108	3 440	3 108	3 446	3 959
7	4 994	4 782	5 154	4 774	5 036	4 774	5 036	5 666
8	5 603	5 443	5 827	5 539	5 581	5 539	5 581	6 378
9	4 994	4 782	5 154	4 902	4 826	4 902	4 840	5 666
10	3 436	3 176	3 491	3 228	3 219	3 236	3 265	3 959
11	1 806	1 312	1 765	1 664	1 580	1 672	1 650	2 150
12	686	350	590	638	578	654	648	888
13	112	56	104	152	128	152	160	268
14	4	4	12	12	16	28	22	54

表5 g_m的代数免疫度

m	AI			最优AI
	文献[9]	文献[15]	本文	
2	2	2	2	2
3	3	3	4	4
4	3	4	5	8

5 结束语

本文首先分析了2^m变元的基础八次函数h_m的迭代性质及k-重量分布，然后通过修改基础函数h_m的重量支撑集构造出了一类新的2^m变元的逐重量完美平衡函数g_m，最后，证明了g_m的代数次数是2^m-4，并通过计算机程序计算当变元个数较小时，WPB函数的k-重量非线性度和代数免疫度。通过选择不同的基础函数和采用不同的方法修改其重量支撑集，可以构造出更多的WPB函数。尽管存在多种构造方法，但这些WPB函数的k-重量非线性度还没有达到理论上的最大值。此外，如何在理论上求解WPB函数的k-重量非线性度是一个具有挑战性的问题，因此构造具有可证明的高k-重量非线性度的WPB函数是一个值得继续研究的方向。

参考文献：

[1] GENTRY C, GENTRY C. Fully homomorphic encryption using ideal lattices[C]//Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing. New York: ACM Press, 2009: 169-178.

[2] NAEHRIG M, LAUTER K, VAIKUNTANATHAN V, et al. Can homomorphic encryption be practical? [C]//Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop. New York: ACM Press, 2011: 113-124.

[3] MÉAUX P, JOURNAULT A, STANDAERT F X, et al. Towards stream ciphers for efficient FHE with low-noise ciphertexts[C]//Advances in Cryptology – EUROCRYPT 2016. Berlin: Springer, 2016: 311-343.

[4] CARLET C, MÉAUX P, ROTELLA Y. Boolean functions with restricted input and their robustness; application to the FLIP cipher[J]. IACR Transactions on Symmetric Cryptology, 2017(3): 192-227.

[5] LIU J, MESNAGER S. Weightwise perfectly balanced functions with high weightwise nonlinearity profile[J]. Designs, Codes and Cryptography, 2019, 87(8): 1797-1813.

[6] TANG D, LIU J. A family of weightwise (almost) perfectly balanced Boolean functions with optimal algebraic immunity[J]. Cryptography and Communications, 2019, 11(6): 1185-1197.

[7] MESNAGER S, SU S H. On constructions of weightwise perfectly balanced Boolean functions[J]. Cryptography and Communications, 2021, 13(6): 951-979.

[8] LI J J, SU S H. Construction of weightwise perfectly balanced Boolean functions with high weightwise nonlinearity[J]. Discrete Applied Mathematics, 2020, 279: 218-227.

[9] ZHAO Q L, JIA Y, ZHENG D, et al. A new construction of weightwise perfectly balanced functions with high weightwise nonlinearity[J].

Mathematics, 2023, 11(5): 1-11.

[10] ZHAO Q L, LI M R, CHEN Z X, et al. A unified construction of weightwise perfectly balanced Boolean functions[J]. Discrete Applied Mathematics, 2023, 337: 190-201.

[11] ZHANG R, SU S H. A new construction of weightwise perfectly balanced Boolean functions[J]. Advances in Mathematics of Communications, 2023, 17(4): 757-770.

[12] GINI A, MÉAUX P. On the algebraic immunity of weightwise perfectly balanced functions[C]//International Conference on Cryptology and Information Security in Latin America. Berlin: Springer, 2023: 3-23.

[13] MEIER W, PASALIC E, CARLET C. Algebraic attacks and decomposition of Boolean functions[C]// Advances in Cryptology - EUROCRYPT 2004. Berlin: Springer, 2004: 474-491.

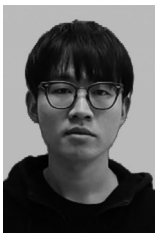
[14] ASKEY R. Orthogonal polynomials and special functions[M]. Philadelphia: Society for Industrial and Applied Mathematics, 1975.

[15] 李梦苒. 具有高非线性度的重量完美平衡布尔函数的构造[D]. 西安: 西安邮电大学, 2023.
LI M R. Construction of Boolean function of perfect weight balance with high nonlinearity[D]. Xi'an: Xi'an University of Posts and Telecommunications, 2023.

[16] 冯梦圆. 若干类逐重量完美平衡布尔函数的具体构造[D]. 开封: 河南大学, 2023.
FENG M Y. Concrete construction of some kinds of Boolean functions with perfect balance by weight[D]. Kaifeng: Henan University, 2023.

[作者简介]

赵庆兰（1981– ），女，山东曹县人，博士，西安邮电大学教授，主要研究方向为布尔函数、对称密码算法的设计和分析。



王富佳（1999– ），男，河北保定人，西安邮电大学硕士生，主要研究方向为布尔函数、对称密码算法的设计和分析。

秦宝东（1982– ），男，江苏徐州人，博士，西安邮电大学教授、博士生导师，主要研究方向为公钥密码学、机器学习安全等。