基于迹函数的negabent函数构造

赵海霞[①②] 李文宇[①②] 韦永壮*[③]

[①](桂林电子科技大学数学与计算科学学院，广西高校数据分析与计算重点实验室 桂林 541002)

[②](广西应用数学中心 桂林 541002)

[③](广西密码学与信息安全重点实验室 桂林 541002)

摘 要：Negabent函数是一种具有最优自相关性、较高非线性度的布尔函数，在密码学、编码理论及组合设计中都有着广泛的应用。该文基于有限域上的迹函数，将其与置换多项式相结合，提出两种构造negabent函数的方法。所构造的两类negabent函数均具备$\mathrm{Tr}_1^k(\lambda x^{2^k+1})+\mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)+\mathrm{Tr}_1^n(mx)\mathrm{Tr}_1^n(dx)$形式：构造方法1通过调整$\lambda$, u, v, m中的3个参数来获得negabent函数，特别地，当$\lambda\neq1$时，能得到$(2^{n-1}-2)(2^n-1)(2^n-4)$个negabent函数；构造方法2通过调整$\lambda$, u, v, m, d中的4个参数来获得negabent函数，特别地，当$\lambda\neq1$时，至少能够得到$2^{n-1}[(2^{n-1}-2)(2^{n-1}-3)+2^{n-1}-4]$个negabent函数。

关键词：Negabent函数；迹函数；置换多项式

中图分类号：TN918.2 **文献标识码**：A **文章编号**：1009-5896(2024)01-0335-09

DOI: 10.11999/JEIT230001

Construction of Negabent Function Based on Trace Function over Finite Field

ZHAO Haixia[①②] LI Wenyu[①②] WEI Yongzhuang[③]

[①](*School of Mathematics and Computing Science, Guangxi University Key Laboratory of Data Analysis and Calculation, Guilin University of Electronic Technology, Guilin* 541002, *China*)

[②](*Center for Applied Mathematics of Guangxi* (*GUET*), *Guilin* 541002, *China*)

[③](*Guangxi Key Laboratory of Cryptology and Information Security, Guilin* 541002, *China*)

Abstract: Negabent function is a Boolean function with optimal autocorrelation and high nonlinearity, which has been widely used in cryptography, coding theory and combination design. In this paper, by combining trace function on a finite field with permutation polynomials, two methods for constructing negabent functions are proposed. Both the two kinds of constructed negabent functions take on such form: $\mathrm{Tr}_1^k(\lambda x^{2^k+1})+\mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)+\mathrm{Tr}_1^n(mx)\mathrm{Tr}_1^n(dx)$. In the first construction method, negabent functions can be obtained by adjusting the three parameters in λ, u, v, m. In particular, when $\lambda\neq1$, $(2^{n-1}-2)(2^n-1)(2^n-4)$ negabent functions can be obtained. In the second construction method, negabent functions can be obtained by adjusting the four parameters in λ, u, v, m, d. In particular, when $\lambda\neq1$, at least $2^{n-1}[(2^{n-1}-2)(2^{n-1}-3)+2^{n-1}-4]$ negabent functions can be obtained.

Key words: Negabent function; Trace function; Permutation polynomial

1 引言

在现代的对称密码体系中，布尔函数是不可替代的重要角色，其抵御攻击的能力决定着密码系统的安全性，故对安全性能良好的布尔函数的构造显得极其重要。非线性度是布尔函数的最重要的性质之一，具有高非线性度的布尔函数能够有效抵御最佳仿射攻击。具有最高非线性度的布尔函数被称为bent函数[1]，这类函数满足n阶扩散准则且其Walsh-Hadamard谱值的绝对值都是相等的，故bent函数是一类密码学性质较好的布尔函数。然而bent函数也有不足之处，例如bent函数不平衡，且其变元个数只能是偶数。Riera等人[2]提出了与Walsh-Hadamard变换相类似的Nega-Hadamard变换，并借鉴bent函

收稿日期：2023-01-09；改回日期：2023-06-09；网络出版：2023-06-14

*通信作者： 韦永壮 walker_wyz@guet.edu.cn

基金项目：国家自然科学基金(62162016)，广西自然科学基金(2019GXNSFGA245004)

Foundation Items: The National Natural Science Foundation of China (62162016), Guangxi Natural Science Foundation (2019GXNSFGA245004)

数的谱值定义，将在任意点处Nega-Hadamard谱值的绝对值都为1的函数称为negabent函数。文献[3,4]指出negabent函数具有最优的自相关性，存在平衡的negabent函数，且其变元个数可为偶数也可为奇数。与bent函数一样，negabent函数在密码学、编码理论和组合设计中都有广泛的应用，故negabent函数的性质和构造成为布尔函数研究领域的一个重点问题。

目前，国内外的学者对negabent函数进行了若干的研究。Parker等人[5]讨论了既是bent又是negabent函数的构造和分类问题。Stănică等人[6]描述了nega-Hadamard变换的详细理论，研究了negabent函数级联后的结果，并刻画了M-M类中的bent-negabent函数所具备的特征。Stanica等人[7]继续证明了n元negabent函数代数次数的上界为$\lceil n/2\rceil$，提出了一种利用完全映射多项式构造bent-negabent函数的方法。Su等人[8]给出了函数是negabent的充要条件，基于该充要条件证明了negabent函数至多有4种nega-谱值，并提供了一种构造偶变元bent-negabent的方法。Mandal等人[9]对M-M类中的bent-negabent函数的存在性问题进行了研究。Sarkar[10]首次给出了通过迹函数的形式表示negabent函数，刻画了一类negabent 2次单项式函数，并给出了在M-M类中bent-negabent函数的充要条件。Zhou等人[11]利用迹函数给出了negabent函数的等价定义，分别构造了2次和3次的negabent单项式函数族。Wu等人[12]利用了2次置换的复合逆和3次置换的复合逆构造了一类新的negabent函数。Jiang等人[13]利用完全置换多项式给出了一类2次bent-negabent函数的充要条件，利用布尔函数和向量布尔函数组合的方法，计算了广义间接和的nega-Hadamard变换。Guo等人[14]分别通过间接与直接的方法对bent-negabent函数进行构造，并研究了多输出布尔函数的nega-Hadamard谱值。文献[15]利用基于迹函数定义的Kerdock码构造了2次bent–negabent函数族。迹函数是有限域上的一类线性函数，利用迹函数不仅可以更好地描述出negabent函数的性质，而且较其他方法而言，利用迹函数构造negabent函数也更加简便。

鉴于迹函数在刻画和构造negabent函数方面的优势，本文使用有限域上的迹函数与置换多项式相结合的方法构造了两类negabent函数，并完成了对这两类negabent函数的计数。所构造的第1类negabent函数具备$f(x)=\mathrm{Tr}_1^k(\lambda x^{2^k+1})+\mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)+\mathrm{Tr}_1^n(mx)\mathrm{Tr}_1^n(ux)$的形式，其中$(u,v,m)\in F_{2^n}^*\times F_{2^n}^*\times F_{2^n}^*$，$n=2k$，$\lambda\in F_{2^k}$，通过调整$\lambda$，$u$，$v$，$m$中的3个参数使其满足negabent函数的谱值特征，并计算出了这类negabent函数的数量。所构造的第2类negabent函数的形式为$f(x)=\mathrm{Tr}_1^n(\lambda x^{2^k+1})+\mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)+\mathrm{Tr}_1^n(mx)\mathrm{Tr}_1^n(dx)$，其中$n=2k$，$\lambda\in F_{2^k}$，$(u,v,m,d)\in F_{2^n}^*\times F_{2^n}^*\times F_{2^n}^*\times F_{2^n}^*$，通过调整$\lambda$，$u$，$v$，$m$，$d$中的4个参数，使其满足negabent函数的谱值特征，并计算出了这类negabent函数的数量。研究结果表明，利用该方法可以获得大量形式简洁的negabent函数。

本文内容的安排如下：第2节介绍了布尔函数及有限域上的迹函数的基本知识；第3节给出了利用迹函数构造negabent函数的方法，并解决了所构造的negabent函数的计数问题；第4节总结。

2 预备知识

本文用F_2表示只有两个元素0和1的有限域，F_2上定义了加法和乘法两种2元运算，F_2^n表示2元域上的n维向量空间。n元布尔函数是F_2^n到F_2上的映射[16]，用B_n表示所有的n元布尔函数构成的集合。

定义1[16] 设$f(x)\in B_n$，$x=(x_1,x_2,\cdots,x_n)\in F_2^n$，称多项式

$$f(x)=\sum_{e\in F_2^n}\alpha_e\left(\prod_{i=1}^n {x_i}^{e_i}\right) \tag{1}$$

为$f(x)$的代数正规型(Algebraic Normal Form, ANF)，这里的$\alpha_e\in F_2$，$e=(e_1,e_2,\cdots,e_n)\in F_2^n$，$f(x)$的代数次数为$\deg(f)=\max\{\mathrm{wt}(e)|\alpha_e\neq 0,e\in F_2^n\}$，其中$\mathrm{wt}(e)$为$e$的汉明重量，是$e$的分量中1的个数。代数次数至多为1的函数称为仿射函数。

设$f(x)\in B_n$，若$|\{x\in F_2^n|f(x)=0\}|=2^{n-1}$，则称该函数是一个平衡的布尔函数。两个布尔函数$f(x)\in B_n$，$g(x)\in B_n$之间的汉明距离为$f\oplus g$的汉明重量，记作$d(f,g)$，即$d(f,g)=\mathrm{wt}(f\oplus g)$。

定义2[16] 布尔函数$f(x)\in B_n$的walsh-Hadamard变换是F_2^n到R上的一个映射，其定义为

$$W_f(\mu)=2^{-\frac{n}{2}}\sum_{x\in F_2^n}(-1)^{f(x)+\mu\cdot x} \tag{2}$$

其中，$\mu\cdot x$为μ与x的内积。若对任意的$\mu\in F_2^n$，均有$|W_f(\mu)|=1$，则称$f(x)$为bent函数。

定义3[7] 布尔函数$f(x)\in B_n$，其nega-Hadamard变换是F_2^n到R上的一个映射，定义为

$$N_f(\mu)=2^{-\frac{n}{2}}\sum_{x\in F_2^n}(-1)^{f(x)+\mu\cdot x}\mathrm{i}^{wt(x)} \tag{3}$$

其中，$\mathrm{i}^2=-1$。

定义4[7] 设$f(x)\in B_n$，若对任意的$\mu\in F_2^n$，均有$|N_f(\mu)|=1$，则称函数$f(x)$为negabent函数。

定义5[17] 设$Q=F_{q^n}$，$K=F_q$为有限域，定义F_{q^n}上的函数为

$$\mathrm{Tr}_K^Q(x)=x+x^q+\cdots+x^{q^{n-1}},\ x\in Q \tag{4}$$

称此函数为F_{q^n}上的迹函数。

迹函数具备下述性质：

(1) $\mathrm{Tr}_1^n(\alpha+\beta)=\mathrm{Tr}_1^n(\alpha)+\mathrm{Tr}_1^n(\beta)$，任意的$\alpha,\ \beta\in Q$；

(2) $\mathrm{Tr}_1^n(x\alpha)=x\mathrm{Tr}_1^n(\alpha)$，任意的$x\in K$, $\alpha\in Q$；

(3) $\mathrm{Tr}_1^n(\alpha^q)=\mathrm{Tr}_1^n(\alpha)$，任意的$\alpha\in Q$；

(4) $\mathrm{Tr}_1^n(\alpha)=\mathrm{Tr}_1^m(\mathrm{Tr}_m^n(\alpha))$，任意的$\alpha\in Q$，其中$m|n$。

定理1[12]　设$f(x)\in B_n$, $f(x)$为negabent函数当且仅当对$a\in F_{2^n}^*$，均有

$$\sum_{x\in F_{2^n}}(-1)^{f(x)+f(x+a)+\mathrm{Tr}_1^n(ax)}=0 \tag{5}$$

定义6[17,18]　设F_{q^n}为有限域，多项式$z(x)\in F_{q^n}[x]$，若由$z(x)$诱导的多项式函数是F_{q^n}到F_{q^n}上的一个双射(置换)，则称$z(x)$是有限域F_{q^n}上的一个置换多项式。

引理1[12]　设q是某个素数幂，$z(x)=\sum_{i=0}^{n-1}a_ix^{q^i}$, $z(x)$是在F_{q^n}上的置换多项式，当且仅当

$$\gcd\left(\sum_{i=1}^{n-1}a_ix^i,\ x^n-1\right)=1 \tag{6}$$

引理2[12]　设$\lambda\neq1$, $b\in F_{2^n}$, $n=2k$，方程$\lambda y^{2^k}+y=b$有唯一解$y=b+b^{2^k}/(1+\lambda^2)$。

3　两类negabent函数的构造

本节使用了有限域上的迹函数构造了两类negabent函数，并讨论了所构造的negabent函数的计数问题。

基于引理2中置换多项式的结论，利用迹函数构造了第1类negabent函数：$f(x)=\mathrm{Tr}_1^k(\lambda x^{2^k+1})\mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)+\mathrm{Tr}_1^n(mx)\mathrm{Tr}_1^n(ux)$，其中$n=2k$, $\lambda\in F_{2^k}$, $(u,v,m)\in F_{2^n}^*\times F_{2^n}^*\times F_{2^n}^*$。通过调整参数$\lambda,\ u,\ v,\ m,\ d$中的3个，使得$f(x)+f(x+a)+\mathrm{Tr}_1^n(ax)$是平衡的，保障了$f(x)$满足定理1的条件。

定理2　令$f(x)=\mathrm{Tr}_1^k(\lambda x^{2^k+1})+\mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)+\mathrm{Tr}_1^n(mx)\mathrm{Tr}_1^n(ux)$，其中$(u,v,m)\in(F_{2^n}^*)^3$, $n=2k$, $\lambda\in F_{2^k}$。$f(x)$是negabent函数当且仅当$f(x)$满足下述4个条件之一。

(1) $\lambda\neq1$, $(A,B,C,D,E,F)\notin P\cup Q$，其中$P=\{(1,1,1),(0,0,1),(1,1,0),(0,0,0)\}\times\{(0,1,0),(0,1,1),(1,0,0),(1,0,1)\}$，$Q=\{(0,1,0),(0,1,1),(1,0,0),(1,0,1)\}\times\{(1,1,1),(0,0,1),(0,1,0),(1,0,0)\}$，$\mathrm{Tr}_1^n\left(\frac{v}{1+\lambda}\right)=A$, $\mathrm{Tr}_1^n\left(\frac{m}{1+\lambda}\right)=B$, $\mathrm{Tr}_1^n\left(\frac{v(m+\lambda m^{2^k})}{1+\lambda^2}\right)=C$, $\mathrm{Tr}_1^n\left(\frac{m(u+\lambda u^{2^k})}{1+\lambda^2}\right)=D$, $\mathrm{Tr}_1^n\left(\frac{u(v+\lambda v^{2^k})}{1+\lambda^2}\right)=E$, $\mathrm{Tr}_1^n\left(\frac{u}{1+\lambda}\right)=F$。

(2) $\lambda=1$, $k=3$, $u,\ v,\ m$, $u+v+m$, $u+v$, $u+m$, $v+m\notin F_{2^k}$。

(3) $\lambda=1$, $k=2$, $u,\ v,\ m$恰有一个属于F_{2^k}, $u,\ v,\ m$互不相同；或$u,\ v,\ m\notin F_{2^k}$, $u+v$, $u+m$, $v+m$至少有一个属于F_{2^k}；或$u,\ v,\ m\notin F_{2^k}$, $u+v+m\in F_{2^k}$。

(4) $\lambda=1$, $k=1$, $u,\ v,\ m$恰有两个属于F_{2^k}, $u,\ v,\ m$互不相同；或$u,\ v,\ m$恰有一个属于F_{2^k}，其余两个相异或后的结果属于F_{2^k}。

证明　根据定理1可知，要证明$f(x)$是negabent函数，只需证明对任意非零$a\in F_{2^n}$, $f(x)+f(x+a)+\mathrm{Tr}_1^n(ax)$是平衡的。通过计算可得

$$\begin{aligned}
&f(x)+f(x+a)+\mathrm{Tr}_1^n(ax)\\
&=\mathrm{Tr}_1^k\left(\lambda a^{2^k+1}\right)+\mathrm{Tr}_1^k\left(\lambda a^{2^k}x+\lambda a x^{2^k}\right)\\
&\quad+\mathrm{Tr}_1^n(ua)\mathrm{Tr}_1^n(va)+\mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(va)\\
&\quad+\mathrm{Tr}_1^n(ua)\mathrm{Tr}_1^n(vx)+\mathrm{Tr}_1^n(ua)\mathrm{Tr}_1^n(ma)\\
&\quad+\mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(ma)+\mathrm{Tr}_1^n(ua)\mathrm{Tr}_1^n(mx)\\
&\quad+\mathrm{Tr}_1^n(ax)\\
&=\mathrm{Tr}_1^n\left(\left(\lambda a^{2^k}+a\right)x\right)+\mathrm{Tr}_1^n\left((\mathrm{Tr}_1^n(va)u\right.\\
&\quad\left.+\mathrm{Tr}_1^n(ma)u\right)x)+\mathrm{Tr}_1^k\left(\lambda a^{2^k+1}\right)\\
&\quad+\mathrm{Tr}_1^n(ua)(\mathrm{Tr}_1^n(va)+\mathrm{Tr}_1^n(ma))\\
&\quad+\mathrm{Tr}_1^n((\mathrm{Tr}_1^n(ua)v+\mathrm{Tr}_1^n(ua)m)x)
\end{aligned}\tag{7}$$

由式(7)可知，对任意的$a\in F_{2^n}^*$, $f(x)+f(x+a)+\mathrm{Tr}_1^n(ax)$是平衡的当且仅当$\lambda a^{2^k}+a+u(\mathrm{Tr}_1^n(va)+\mathrm{Tr}_1^n(ma))+(v+m)\mathrm{Tr}_1^n(ua)\neq0$。

记　$H(a)=\lambda a^{2^k}+a+u(\mathrm{Tr}_1^n(va)+\mathrm{Tr}_1^n(ma))+(v+m)\mathrm{Tr}_1^n(ua)$，下面讨论当参数$\lambda,\ k,\ u,\ v,\ m$满足什么条件时，对任意的$a\in F_{2^n}^*$，有$H(a)\neq0$。注意到$H(a)$中的$\mathrm{Tr}_1^n(va)$, $\mathrm{Tr}_1^n(ma)$, $\mathrm{Tr}_1^n(ua)$可能取值0或1，故对于任意的$a\in F_{2^n}^*$, $u(\mathrm{Tr}_1^n(va)+\mathrm{Tr}_1^n(ma))+(v+m)\mathrm{Tr}_1^n(ua)$是关于$u,\ v,\ m$的解析式。结合引理2，得到下面的证明。

当$\lambda\neq1$时，有：

(1) 当$(\mathrm{Tr}_1^n(va),\ \mathrm{Tr}_1^n(ma),\ \mathrm{Tr}_1^n(ua))=(0,0,0)$时，$H(a)=0$当且仅当$a=0$。

(2) 当$(\mathrm{Tr}_1^n(va),\ \mathrm{Tr}_1^n(ma),\ \mathrm{Tr}_1^n(ua))=(0,0,1)$时，由方程$\lambda y^{2^k}+y=v+m$有唯一解$y=\frac{v+m+\lambda(v+m)^{2^k}}{\lambda^2+1}$，可得$H(a)=0$当且仅当$a=\frac{v+m+\lambda(v+m)^{2^k}}{\lambda^2+1}$。由$(\mathrm{Tr}_1^n(va),\mathrm{Tr}_1^n(ma),\mathrm{Tr}_1^n(ua))=(0,0,1)$得

$$\left.\begin{aligned}&\mathrm{Tr}_1^n\left(\frac{v}{1+\lambda}\right)+\mathrm{Tr}_1^n\left(\frac{v(m+\lambda m^{2^k})}{\lambda^2+1}\right)=0\\&\mathrm{Tr}_1^n\left(\frac{m}{1+\lambda}\right)+\mathrm{Tr}_1^n\left(\frac{m(v+\lambda v^{2^k})}{\lambda^2+1}\right)=0\\&\mathrm{Tr}_1^n\left(\frac{u(m+\lambda m^{2^k})}{\lambda^2+1}\right)+\mathrm{Tr}_1^n\left(\frac{u(v+\lambda v^{2^k})}{\lambda^2+1}\right)=1\end{aligned}\right\}\tag{8}$$

通过计算可得$\mathrm{Tr}_1^n\left(\frac{v(m+\lambda m^{2^k})}{\lambda^2+1}\right)=\mathrm{Tr}_1^n\left(\frac{(\lambda m v^{2^k})^{2^k}}{(\lambda^2+1)^{2^k}}\right)+\mathrm{Tr}_1^n\left(\frac{vm}{\lambda^2+1}\right)=\mathrm{Tr}_1^n\left(\frac{\lambda m v^{2^k}}{\lambda^2+1}\right)+\mathrm{Tr}_1^n\left(\frac{vm}{\lambda^2+1}\right)=\mathrm{Tr}_1^n\left(\frac{m(v+\lambda v^{2^k})}{\lambda^2+1}\right)$，故式(8)等价于

$$A+C=0,\ B+C=0,\ D+E=1\tag{9}$$

由式(9)可得$A=B=C,\ D\neq E$，从而当$(A,B,C,D,E)\notin\{(0,0,0,0,1),(0,0,0,1,0),(1,1,1,0,1),(1,1,1,1,0)\}$时$H(a)\neq 0$。

(3) 当$(\mathrm{Tr}_1^n(va),\mathrm{Tr}_1^n(ma),\mathrm{Tr}_1^n(ua))=(0,1,0)$时，由方程$\lambda y^{2^k}+y=u$有唯一解$y=\frac{u+\lambda u^{2^k}}{\lambda^2+1}$，可得$H(a)=0$当且仅当$a=\frac{u+\lambda u^{2^k}}{\lambda^2+1}$，由$(\mathrm{Tr}_1^n(va),\mathrm{Tr}_1^n(ma),\mathrm{Tr}_1^n(ua))=(0,1,0)$得

$$\left.\begin{aligned}&\mathrm{Tr}_1^n\left(\frac{v(u+\lambda u^{2^k})}{\lambda^2+1}\right)=0\\&\mathrm{Tr}_1^n\left(\frac{m(u+\lambda u^{2^k})}{\lambda^2+1}\right)=1\\&\mathrm{Tr}_1^n\left(\frac{u}{\lambda+1}\right)=0\end{aligned}\right\}\tag{10}$$

式(10)等价于

$$D=1,\ E=0,\ F=0\tag{11}$$

由式(11)可知，当$(D,E,F)\notin\{(1,0,0)\}$时，$H(a)\neq 0$。

(4) 当$(\mathrm{Tr}_1^n(va),\mathrm{Tr}_1^n(ma),\mathrm{Tr}_1^n(ua))=(1,0,0)$时，由方程$\lambda y^{2^k}+y=u$有唯一解$y=\frac{u+\lambda u^{2^k}}{\lambda^2+1}$，可得$H(a)=0$当且仅当$a=\frac{u+\lambda u^{2^k}}{\lambda^2+1}$，由$(\mathrm{Tr}_1^n(va),\mathrm{Tr}_1^n(ma),\mathrm{Tr}_1^n(ua))=(1,0,0)$可得

$$\left.\begin{aligned}&\mathrm{Tr}_1^n\left(\frac{v(u+\lambda u^{2^k})}{\lambda^2+1}\right)=1\\&\mathrm{Tr}_1^n\left(\frac{m(u+\lambda u^{2^k})}{\lambda^2+1}\right)=0\\&\mathrm{Tr}_1^n\left(\frac{u}{\lambda+1}\right)=0\end{aligned}\right\}\tag{12}$$

式(12)等价于

$$D=0,\ E=1,\ F=0\tag{13}$$

由式(13)可知，当$(D,E,F)\notin\{(0,1,0)\}$时，$H(a)\neq 0$。

(5) 当$(\mathrm{Tr}_1^n(va),\mathrm{Tr}_1^n(ma),\mathrm{Tr}_1^n(ua))=(1,1,0)$时，$H(a)=0$当且仅当$a=0$。

(6) 当$(\mathrm{Tr}_1^n(va),\mathrm{Tr}_1^n(ma),\mathrm{Tr}_1^n(ua))=(0,1,1)$时，由方程$\lambda y^{2^k}+y=u+v+m$唯一解$y=\frac{u+v+m+\lambda(u+v+m)^{2^k}}{\lambda^2+1}$，可得$H(a)=0$当且仅当$a=\frac{u+v+m+\lambda(u+v+m)^{2^k}}{\lambda^2+1}$，由$(\mathrm{Tr}_1^n(va),\mathrm{Tr}_1^n(ma),\mathrm{Tr}_1^n(ua))=(0,1,1)$可得

$$\left.\begin{aligned}&\mathrm{Tr}_1^n\left(\frac{v}{\lambda+1}\right)+\mathrm{Tr}_1^n\left(\frac{v(m+u+\lambda(m+u)^{2^k})}{\lambda^2+1}\right)=0\\&\mathrm{Tr}_1^n\left(\frac{m}{\lambda+1}\right)+\mathrm{Tr}_1^n\left(\frac{m(v+u+\lambda(v+u)^{2^k})}{\lambda^2+1}\right)=1\\&\mathrm{Tr}_1^n\left(\frac{u}{\lambda+1}\right)+\mathrm{Tr}_1^n\left(\frac{u(m+v+\lambda(m+v)^{2^k})}{\lambda^2+1}\right)=1\end{aligned}\right\}\tag{14}$$

又$\mathrm{Tr}_1^n\left(\frac{v(m+\lambda m^{2^k})}{\lambda^2+1}\right)=\mathrm{Tr}_1^n\left(\frac{m(v+\lambda v^{2^k})}{\lambda^2+1}\right)$，$\mathrm{Tr}_1^n\left(\frac{v(u+\lambda u^{2^k})}{\lambda^2+1}\right)=\mathrm{Tr}_1^n\left(\frac{u(v+\lambda v^{2^k})}{\lambda^2+1}\right)$，$\mathrm{Tr}_1^n\left(\frac{u(m+\lambda m^{2^k})}{\lambda^2+1}\right)=\mathrm{Tr}_1^n\left(\frac{m(u+\lambda u^{2^k})}{\lambda^2+1}\right)$，故式(14)等价于

$$A+C+E=0,\ B+C+D=1,\ D+E+F=1\tag{15}$$

由式(15)可知，当$(A,B,C,D,E,F)\notin\{(0,0,0,1,0,0),(0,1,0,0,0,1),(1,0,0,1,1,1),(1,1,0,0,1,0),(1,0,1,0,0,1),(1,1,1,1,0,0),(0,0,1,0,1,0),(0,1,1,1,1,1)\}$时，$H(a)\neq 0$。

(7) 当$(\mathrm{Tr}_1^n(va),\mathrm{Tr}_1^n(ma),\mathrm{Tr}_1^n(ua))=(1,0,1)$时，由方程$\lambda y^{2^k}+y=u+v+m$唯一解$y=\frac{u+v+m+\lambda(u+v+m)^{2^k}}{\lambda^2+1}$，可得$H(a)=0$当且仅当$a=\frac{u+v+m+\lambda(u+v+m)^{2^k}}{\lambda^2+1}$，由$(\mathrm{Tr}_1^n(va),\mathrm{Tr}_1^n(ma),\mathrm{Tr}_1^n(ua))=(1,0,1)$可得

$$\left.\begin{aligned}&\mathrm{Tr}_1^n\left(\frac{v}{\lambda+1}\right)+\mathrm{Tr}_1^n\left(\frac{v(m+u+\lambda(m+u)^{2^k})}{\lambda^2+1}\right)=1\\&\mathrm{Tr}_1^n\left(\frac{m}{\lambda+1}\right)+\mathrm{Tr}_1^n\left(\frac{m(v+u+\lambda(v+u)^{2^k})}{\lambda^2+1}\right)=0\\&\mathrm{Tr}_1^n\left(\frac{u}{\lambda+1}\right)+\mathrm{Tr}_1^n\left(\frac{u(m+v+\lambda(m+v)^{2^k})}{\lambda^2+1}\right)=1\end{aligned}\right\}\tag{16}$$

又 $\mathrm{Tr}_1^n\left(\frac{v(m+\lambda m^{2^k})}{\lambda^2+1}\right)=\mathrm{Tr}_1^n\left(\frac{m(v+\lambda v^{2^k})}{\lambda^2+1}\right)$，$\mathrm{Tr}_1^n\left(\frac{v(u+\lambda u^{2^k})}{\lambda^2+1}\right)=\mathrm{Tr}_1^n\left(\frac{u(v+\lambda v^{2^k})}{\lambda^2+1}\right)$，$\mathrm{Tr}_1^n\left(\frac{u(m+\lambda m^{2^k})}{\lambda^2+1}\right)=\mathrm{Tr}_1^n\left(\frac{m(u+\lambda u^{2^k})}{\lambda^2+1}\right)$，故式(16)等价于

$$A+C+E=1,\ B+C+D=0,\ D+E+F=1 \tag{17}$$

由式(17)可知，当$(A,B,C,D,E,F)\notin\{(0,1,1,0,0,1),(0,0,1,1,0,0),(0,0,0,0,1,0),(0,1,0,1,1,1),(1,0,0,0,0,1),(1,1,0,1,0,0),(1,1,1,0,1,0),(1,0,1,1,1,1)\}$时，$H(a)\neq 0$。

(8) 当$(\mathrm{Tr}_1^n(va),\mathrm{Tr}_1^n(ma),\mathrm{Tr}_1^n(ua))=(1,1,1)$时，由方程$\lambda y^{2^k}+y=v+m$的唯一解$y=\frac{v+m+\lambda(v+m)^{2^k}}{\lambda^2+1}$，可得$H(a)=0$当且仅当$a=\frac{v+m+\lambda(v+m)^{2^k}}{\lambda^2+1}$，由$(\mathrm{Tr}_1^n(va),\mathrm{Tr}_1^n(ma),\mathrm{Tr}_1^n(ua))=(1,1,1)$可得

$$\left.\begin{aligned}&\mathrm{Tr}_1^n\left(\frac{v}{\lambda+1}\right)+\mathrm{Tr}_1^n\left(\frac{v(m+\lambda m^{2^k})}{\lambda^2+1}\right)=1\\&\mathrm{Tr}_1^n\left(\frac{m}{\lambda+1}\right)+\mathrm{Tr}_1^n\left(\frac{m(v+\lambda v^{2^k})}{\lambda^2+1}\right)=1\\&\mathrm{Tr}_1^n\left(\frac{u(v+\lambda v^{2^k})}{\lambda^2+1}\right)+\mathrm{Tr}_1^n\left(\frac{u(m+\lambda m^{2^k})}{\lambda^2+1}\right)=1\end{aligned}\right\} \tag{18}$$

又 $\mathrm{Tr}_1^n\left(\frac{v(m+\lambda m^{2^k})}{\lambda^2+1}\right)=\mathrm{Tr}_1^n\left(\frac{m(v+\lambda v^{2^k})}{\lambda^2+1}\right)$，故式(18)等价于

$$A+C=1,\ B+C=1,\ D+E=1 \tag{19}$$

由式(19)可得$D\neq E$，当$(A,B,C,D,E)\notin\{(0,0,1,1,0),(1,1,0,0,1),(1,1,0,0,1),(0,0,1,0,1),(1,1,0,1,0)\}$时，$H(a)\neq 0$。

综上所述，当$\lambda\neq 1$时，若(A,B,C,D,E,F)不属于上述情形，则对任意$a\in F_{2^n}^*$，有$H(a)=\lambda a^{2^k}+a+u(\mathrm{Tr}_1^n(va)+\mathrm{Tr}_1^n(ma))+(v+m)\mathrm{Tr}_1^n(ua)\neq 0$。

当$\lambda=1$时，考虑$H(a)=0$，即$a^{2^k}+a+u(\mathrm{Tr}_1^n(va)+\mathrm{Tr}_1^n(ma))+(v+m)\mathrm{Tr}_1^n(ua)=0$解的个数问题。

(1) 当$(\mathrm{Tr}_1^n(va),\mathrm{Tr}_1^n(ma),\mathrm{Tr}_1^n(ua))\neq(0,0,0)$时，其证明与$\lambda\neq 1$时类似，故不赘述。

(2) 当$(\mathrm{Tr}_1^n(va),\mathrm{Tr}_1^n(ma),\mathrm{Tr}_1^n(ua))=(0,0,0)$时，记$L(v,m,u)$是在$F_{2^n}^*$中使得$(\mathrm{Tr}_1^n(va),\mathrm{Tr}_1^n(ma),\mathrm{Tr}_1^n(ua))=(0,0,0)$的$a$的个数，其中$(v,m,u)\in F_{2^n}^*\times F_{2^n}^*\times F_{2^n}^*$。

由迹函数的平衡性质可得$(\mathrm{Tr}_1^n(va),\mathrm{Tr}_1^n(ma),\mathrm{Tr}_1^n(ua))=(\mathrm{Tr}_1^n(a(v+v^{2^k})),\mathrm{Tr}_1^n(a(m+m^{2^k})),\mathrm{Tr}_1^n(a(u+u^{2^k})))$。

因此，易证：

(a) 当$v,\ m,\ u$恰好有两个属于$F_{2^k}^*$时，$L(v,m,u)=2^{k-1}-1$，在此情形下$H(a)\neq 0$当且仅当$k=1$。

(b) 当$v,\ m,\ u$恰有一个属于$F_{2^k}^*$时，$L(v,m,u)=2^{k-1}-1$，在此情形下$H(a)\neq 0$当且仅当$k=2$。

(c) 当$v,\ m,\ u\notin F_{2^k}^*$时，若$v+m+u\in F_{2^k}^*$，或$v+m,v+u,m+u$恰有一个属于$F_{2^k}^*$，则$L(v,m,u)=2^{k-2}-1$，在此情形下$H(a)\neq 0$当且仅当$k=2$；若$v+m+u,v+m,v+u,m+u\notin F_{2^k}^*$，则$L(v,m,u)=2^{k-3}-1$，在此情形下$H(a)\neq 0$当且仅当$k=3$。显然，当$k>3$时，$H(a)=0$至少有1个非零解，即$f(x)$不是negabent函数。

注1　在定理2中，当$v=u=m$时，文献[19]已证明$f(x)$是negabent函数。

例1　基于定理2的条件所构造的negabent函数。

(1) 当$\lambda\neq 1$时，取$\lambda=0,\ k=2$，相应的$n=4$，取$u=(1,0,0,1),v=(0,0,0,1),m=(0,1,1,0)$，则计算可得$(A,B,C,D,E,F)=(1,0,0,0,1,1)\notin P\cup Q$，由此可得negabent函数$f(x)={x_4}^2+x_1x_2+x_1x_3+x_1x_4+x_2x_4+x_3x_4$，其中$x=(x_1,x_2,x_3,x_4)$。

(2) 当$\lambda=1,\ k=3$时，相应的$n=6$，取$u=(0,0,0,0,0,1),v$=$(0,0,0,0,1,1,),m$=$(0,0,0,1,1,1)$，由此可得negabent函数$f(x)=\mathrm{Tr}_1^3(x^9)+x_4x_6$，其中$x=(x_1,x_2,x_3,x_4,x_5,x_6)$。

(3) 当$\lambda=1,\ k=2$时，相应的$n=4$，取$u=(1,1),v=(0,0,1,1),m=(0,0,0,1)$，由此可得negabent函数$f(x)=\mathrm{Tr}_1^2(x^5)+x_1x_3+x_2x_3$，其中$x=(x_1,x_2,x_3,x_4)$。

(4) 当$\lambda=1,\ k=1$时，相应的$n=2$，取$u=1,v=0,m=(1,1)$，由此可得negabent函数$f(x)=\mathrm{Tr}_1^1(x^3)+{x_1}^2+x_1x_2$，其中$x=(x_1,x_2)$。

命题1　当$\lambda\neq 1$时，定理2中所构造的negabent函数的数量为$(2^{n-1}-2)(2^n-1)(2^n-4)$。

证明　由定理2可知，当$\lambda\neq 1$时，若

$$\left(\mathrm{Tr}_1^n\left(\frac{v}{1+\lambda}\right),\mathrm{Tr}_1^n\left(\frac{m}{1+\lambda}\right),\mathrm{Tr}_1^n\left(\frac{u}{1+\lambda}\right)\right)\in\{(0,1,1),(0,0,0)\} \tag{20}$$

则$(A,B,C,D,E,F)\notin P\cup Q$，因此在定理2中所构造出的negabent函数的数量等于使得式(20)成立的(u,v,m)的数量。

在$F_{2^n}^*$中，使得$\mathrm{Tr}_1^n\left(\frac{v}{1+\lambda}\right)=0$的$v$有$2^{n-1}-1$个；在$F_{2^n}^*\backslash\{v\}$中，使得$\mathrm{Tr}_1^n\left(\frac{m}{1+\lambda}\right)=0$的$m$有

$2^{n-1}-2$个，在$F_{2^n}^*\backslash\{v,m\}$中，使得$\mathrm{Tr}_1^n\left(\frac{u}{1+\lambda}\right)=0$的$u$有$2^{n-1}-3$个，故使得$\left(\mathrm{Tr}_1^n\left(\frac{v}{1+\lambda}\right),\mathrm{Tr}_1^n\left(\frac{m}{1+\lambda}\right),\mathrm{Tr}_1^n\left(\frac{u}{1+\lambda}\right)\right)=(0,0,0)$的$(u,v,m)$的数量为$(2^{n-1}-1)(2^{n-1}-2)(2^{n-1}-3)$。

在$F_{2^n}^*\backslash\{v\}$中，使得$\mathrm{Tr}_1^n\left(\frac{m}{1+\lambda}\right)=1$的$m$有$2^{n-1}-1$个；在$F_{2^n}^*\backslash\{v,m\}$中，使得$\mathrm{Tr}_1^n\left(\frac{u}{1+\lambda}\right)=1$的$u$有$2^{n-1}-2$个，故使得$\left(\mathrm{Tr}_1^n\left(\frac{v}{1+\lambda}\right),\mathrm{Tr}_1^n\left(\frac{m}{1+\lambda}\right),\mathrm{Tr}_1^n\left(\frac{u}{1+\lambda}\right)\right)=(0,1,1)$的$(u,v,m)$的数量为$(2^{n-1}-1)^2(2^{n-1}-2)$。综上使式(20)成立的数组$(u,v,m)$数量为$(2^n-4)(2^{n-1}-1)(2^{n-1}-2)$。

若

$$\left(\mathrm{Tr}_1^n\left(\frac{v}{1+\lambda}\right),\mathrm{Tr}_1^n\left(\frac{m}{1+\lambda}\right),\mathrm{Tr}_1^n\left(\frac{u}{1+\lambda}\right)\right)\in\{(1,1,1),(1,0,0)\}\tag{21}$$

则$(A,B,C,D,E,F)\notin P\cup Q$，因此在定理2中所构造出的negabent函数的数量等于使得式(21)成立的(u,v,m)的数量。

在$F_{2^n}^*$中，使得$\mathrm{Tr}_1^n\left(\frac{v}{1+\lambda}\right)=1$的$v$有$2^{n-1}$个；在$F_{2^n}^*\backslash\{v\}$中，使得$\mathrm{Tr}_1^n\left(\frac{m}{1+\lambda}\right)=0$的$m$有$2^{n-1}-2$个，在$F_{2^n}^*\backslash\{v,m\}$中，使得$\mathrm{Tr}_1^n\left(\frac{u}{1+\lambda}\right)=0$的$u$有$2^{n-1}-3$个，故使得$\left(\mathrm{Tr}_1^n\left(\frac{v}{1+\lambda}\right),\mathrm{Tr}_1^n\left(\frac{m}{1+\lambda}\right),\mathrm{Tr}_1^n\left(\frac{u}{1+\lambda}\right)\right)=(1,0,0)$的$(u,v,m)$的数量为$2^{n-1}(2^{n-1}-2)(2^{n-1}-3)$个。在$F_{2^n}^*\backslash\{v\}$中，使得$\mathrm{Tr}_1^n\left(\frac{m}{1+\lambda}\right)=1$的$m$有$2^{n-1}-1$个；在$F_{2^n}^*\backslash\{v,m\}$中，使得$\mathrm{Tr}_1^n\left(\frac{u}{1+\lambda}\right)=1$的$u$有$2^{n-1}-2$个，故使得$\left(\mathrm{Tr}_1^n\left(\frac{v}{1+\lambda}\right),\mathrm{Tr}_1^n\left(\frac{m}{1+\lambda}\right),\mathrm{Tr}_1^n\left(\frac{u}{1+\lambda}\right)\right)=(1,1,1)$的$(u,v,m)$的数量为$2^{n-1}(2^{n-1}-1)(2^{n-1}-2)$个。综上，使得式(21)成立的数组$(u,v,m)$数量为$2^{n-1}(2^{n-1}-2)(2^{n-1}-4)$。

综上所述，当$\lambda\neq1$时，使$f(x)$为negabent函数的有序数组(u,v,m)的数量$(2^{n-1}-2)(2^n-1)(2^n-4)$。

将所构造第1类negabent函数$f(x)=\mathrm{Tr}_1^k(\lambda x^{2^k+1})+\mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)+\mathrm{Tr}_1^n(mx)\mathrm{Tr}_1^n(ux)$中的$u$调整为两个不同的参数，可得$\mathrm{Tr}_1^k(\lambda x^{2^k+1})+\mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)+\mathrm{Tr}_1^n(mx)\mathrm{Tr}_1^n(dx)$，下面讨论参数$\lambda,u,v,m,d$满足什么条件时，该函数仍为negabent函数。

定理3 令$f(x)=\mathrm{Tr}_1^k(\lambda x^{2^k+1})+\mathrm{Tr}_1^n(ux)\mathrm{Tr}_1^n(vx)+\mathrm{Tr}_1^n(mx)\mathrm{Tr}_1^n(dx)$，其中$(u,v,m,d)\in(F_{2^n}^*)^4$，$n=2k$，$f(x)$是negabent函数当且仅当$f(x)$满足下面的5个条件之一：

(1) $\lambda\neq1$，(A,B,C,D,E,F,G,H,I,J)不属于附录中的所有10元向量。其中，$A=\mathrm{Tr}_1^n\left(\frac{u}{\lambda+1}\right)$，$B=\mathrm{Tr}_1^n\left(\frac{v}{\lambda+1}\right)$，$C=\mathrm{Tr}_1^n\left(\frac{m}{\lambda+1}\right)$，$D=\mathrm{Tr}_1^n\left(\frac{d}{\lambda+1}\right)$，$E=\mathrm{Tr}_1^n\left(\frac{u(m+\lambda m^{2^k})}{\lambda^2+1}\right)$，$F=\mathrm{Tr}_1^n\left(\frac{u(v+\lambda v^{2^k})}{\lambda^2+1}\right)$，$G=\mathrm{Tr}_1^n\left(\frac{u(d+\lambda d^{2^k})}{\lambda^2+1}\right)$，$H=\mathrm{Tr}_1^n\left(\frac{m(v+\lambda v^{2^k})}{\lambda^2+1}\right)$，$I=\mathrm{Tr}_1^n\left(\frac{m(d+\lambda d^{2^k})}{\lambda^2+1}\right)$，$J=\mathrm{Tr}_1^n\left(\frac{v(d+\lambda d^{2^k})}{\lambda^2+1}\right)$。

(2) $\lambda=1$, $k=4$, u, v, m, $d\notin F_{2^k}$，且$u+v+m+d\notin F_{2^k}$, u, v, m, d互不相同。

(3) $\lambda=1$, $k=3$，u, v, m, $d\notin F_{2^k}$，且$u+v+m+d\in F_{2^k}$，u, v, m, d互不相同；或u, v, m, d恰有1个属于F_{2^k}，u, v, m, d互不相同。

(4) $\lambda=1$, $k=2$,u, v, m, d恰有2个属于F_{2^k}，u, v, m, d互不相同。

(5) $\lambda=1$, $k=1$,u, v, m, d恰有3个属于F_{2^k}。

注2 定理3的证明与定理2证明类似，这里不再赘述。

例2 基于定理3的条件所构造的negabent函数。

(1) 当$\lambda\neq1$时，取$\lambda=0$，$k=2$，相应的$n=2$，取$u=(0,1,1,1),v=(1,1,1,0),m=(1,0,1,1),d=(0,1,0,1)$，则计算可得$(A,B,C,D,E,F,G,H,I,J)=(1,0,1,0,0,0,0,1,1,1)$不在附表内，由此可得negabent函数$f(x)=x_2{}^2+x_3{}^2+x_4{}^2+x_1x_3+x_2x_3$，其中$x=(x_1,x_2,x_3,x_4,x_5,x_6)$。

(2) 当$\lambda=1$, $k=4$时，相应的$n=8$，取$u=(0,0,0,0,0,0,0,1),v=(0,0,0,0,0,0,1,1),m=(0,0,0,1,1,0,0,1)$，$d=(0,0,0,0,1,1,0,1)$，由此可得negabent函数$f(x)=\mathrm{Tr}_1^4(x^{17})+x_5{}^2+x_4x_5+x_4x_6+x_4x_8+x_5x_6+x_6x_8+x_7x_8$，其中$x=(x_1,x_2,x_3,x_4,x_5,x_6,x_7,x_8)$。

(3) 当$\lambda=1$, $k=3$时，相应的$n=6$，任取$u=(0,0,0,1)$，$v=(0,0,0,1,0,1)$，$m=(0,0,1,1,0,1)$，$d=(0,0,0,0,1,1)$，由此可得negabent函数$f(x)=\mathrm{Tr}_1^3(x^9)+x_4{}^2+x_6{}^2+x_3x_5+x_3x_6+x_4x_5+x_5x_6$，其中$x=(x_1,x_2,x_3,x_4,x_5,x_6)$。

(4) 当$\lambda=1$, $k=2$时，相应的$n=4$，取

$u=(0,1),v=(1,1),m=(0,0,0,1),d=(0,0,1,1)$，由此可得negabent函数$f(x)=\mathrm{Tr}_1^2(x^5)+{x_2}^2+{x_4}^2+x_1x_2+x_3x_4$，其中$x=(x_1,x_2,x_3,x_4)$。

（5）当$\lambda=1$，$k=1$时，相应的$n=2$，取$u=v=0,m=1,d=(0,1)$，由此可得negabent函数$f(x)=\mathrm{Tr}_1^1(x^3)+x_1x_2$，其中$x=(x_1,x_2)$。

在第2类negabent函数的构造中，同样基于引理2中置换多项式的结论，利用迹函数构造negabent函数。与所构造的第1类negabent函数相比较，第2类negabent函数中可调的参数更多，因此由第2种构造方法可获得更多negabent函数。

命题2　当$\lambda\neq1$时，定理3中所构造的negabent函数数量的下界为$2^{n-1}[(2^{n-1}-2)(2^{n-1}-3)+2^{n-1}-4]$。

证明　如定理3所示，$f(x)$中的u, v, m, d互不相同，确定有序数组(u,v,m,d)数量即可得到所构造出的negabent函数数量，将附表中的10元向量归纳可得：由定理3中的方法构造出的negabent函数的计数下界为$2^{n-1}[(2^{n-1}-2)(2^{n-1}-3)+2^{n-1}-4]$。

本文借鉴文献[12] 中利用有限域上的迹函数构造negabent函数的思想方法，通过增加可调参数获得了更多的negabent函数。文献[12]与本文所构造的negabent函数数量如表1所示。

表 1　不同调参方案所构造函数数量

	调整的参数	计数
文献[12]	u,v	$(2^{n-1}-2)(2^n-1)$
定理2	u,v,m	$(2^{n-1}-2)(2^n-1)(2^n-4)$
定理3	u,v,m,d	$\geq 2^{n-1}[(2^{n-1}-2)(2^{n-1}-3)+2^{n-1}-4]$

4　结论

Negabent函数作为bent函数的一种拓展，在密码学与编码理论中有着广泛应用，因此构造negabent函数具有重要实际意义。本文将迹函数与置换多项式相结合，提出了两种构造negabent函数的方法，解决了所构造出来的negabent函数的计数问题。研究结果表明，利用本方法可以获得大量的negabent函数。

参 考 文 献

[1] ROTHAUS O S. On “bent” functions[J]. *Journal of Combinatorial Theory, Series A*, 1976, 20(3): 300–305. doi: 10.1016/0097-3165(76)90024-8.

[2] RIERA C and PARKER M G. Generalized bent criteria for Boolean functions (I)[J]. *IEEE Transactions on Information Theory*, 2006, 52(9): 4142–4159. doi: 10.1109/TIT.2006.880069.

[3] 任明生. Nega-Hadamard变换和Negabent函数的研究[D]. [硕士论文], 淮北师范大学, 2017.
REN Mingsheng. Research on Nega-Hadamard transform and Negabent function[D]. [Master dissertation], Huaibei Normal University, 2017.

[4] SCHMIDT K U, PARKER M G, and POTT A. Negabent functions in the Maiorana–McFarland class[C]. 5th International Conference on Sequences and Their Applications-SETA 2008, Lexington, USA, 2008: 390–402. doi: 10.1007/978-3-540-85912-3_34.

[5] PARKER M G and POTT A. On Boolean functions which are bent and Negabent[C]. International Workshop on Sequences, Subsequences, and Consequences 2007, Los Angeles, USA, 2007: 9–23. doi: 10.1007/978-3-540-77404-4_2.

[6] STĂNICĂ P, GANGOPADHYAY S, CHATURVEDI A, *et al*. Nega-Hadamard transform, bent and Negabent functions[C]. 6th International Conference on Sequences and Their Applications-SETA 2010, Paris, France, 2010: 359–372. doi: 10.1007/978-3-642-15874-2_31.

[7] STANICA P, GANGOPADHYAY S, CHATURVEDI A, *et al*. Investigations on bent and Negabent functions via the Nega-Hadamard transform[J]. *IEEE Transactions on Information Theory*, 2012, 58(6): 4064–4072. doi: 10.1109/TIT.2012.2186785.

[8] SU Wei, POTT A, and TANG Xiaohu. Characterization of Negabent functions and construction of bent-Negabent functions with maximum algebraic degree[J]. *IEEE Transactions on Information Theory*, 2013, 59(6): 3387–3395. doi: 10.1109/TIT.2013.2245938.

[9] MANDAL B, MAITRA Su, and STĂNICĂ P. On the existence and non-existence of some classes of bent-Negabent functions[J]. *Applicable Algebra in Engineering, Communication and Computing*, 2022, 33(3): 237–260. doi: 10.1007/s00200-020-00444-w.

[10] SARKAR S. Characterizing Negabent Boolean functions over finite fields[C]. 7th International Conference on Sequences and Their Applications-SETA 2012, Waterloo, Canada, 2012: 77–88. doi: 10.1007/978-3-642-30615-0_7.

[11] ZHOU Yue and QU Longjiang. Constructions of Negabent functions over finite fields[J]. *Cryptography and Communications*, 2017, 9(2): 165–180. doi: 10.1007/s12095-015-0167-0.

[12] WU Gaofei, LI Nian, ZHANG Yuqing, *et al*. Several classes of Negabent functions over finite fields[J]. *Science China Information Sciences*, 2018, 61(3): 038102. doi: 10.1007/s11432-017-9096-0.

[13] JIANG Niu, ZHAO Min, YANG Zhiyao, *et al*. Characterization and properties of bent-Negabent

functions[J]. *Chinese Journal of Electronics*, 2022, 31(4): 786–792. doi: 10.1049/cje.2021.00.417.

[14] GUO Fei, WANG Zilong, and GONG Guang. Several secondary methods for constructing bent-Negabent functions[J]. *Designs, Codes and Cryptography*, 2023, 91(3): 971–995. doi: 10.1007/s10623-022-01133-0.

[15] STĂNICĂ P, MANDAL B, and MAITRA S. The connection between quadratic bent-Negabent functions and the Kerdock code[J]. *Applicable Algebra in Engineering, Communication and Computing*, 2019, 30(5): 387–401. doi: 10.1007/s00200-019-00380-4.

[16] 周宇, 胡予濮, 董新锋. 布尔函数的设计与分析[M]. 北京: 国防工业出版社, 2015: 20–55.
ZHOU Yu, HU Yupu, and DONG Xinfeng. Design and Analysis of Boolean Functions[M]. Beijing: National Defense Industry Press, 2015: 20–55.

[17] LIDL R and NIEDERREITER H. Finite Fields[M]. 2nd ed. London: Cambridge University Press, 1996: 54–62. doi: 10.1017/CBO9780511525926.

[18] WU Danyao and YUAN Pingzhi. Further results on permutation polynomials from trace functions[J]. *Applicable Algebra in Engineering, Communication and Computing*, 2022, 33(4): 341–351. doi: 10.1007/s00200-020-00456-6.

[19] SARKAR S. Some results on bent-Negabent Boolean functions over finite fields[EB/OL]. https://arxiv.org/abs/1406.1036, 2014.

赵海霞：女，副教授，研究方向为密码函数、对称密码算法设计与分析.

李文宇：男，硕士生，研究方向为密码函数、对称密码分析.

韦永壮：男，教授，研究方向为密码函数，对称密码算法设计与分析，侧信道攻击与防御科技.

责任编辑：余 蓉

附录A

定理3中$\lambda \neq 1$时$(A, B, C, D, E, F, G, H, I, J)$不取的10元向量

1100000000	1100000100	1111010001	1100000001	1111110001	1100000101	1111110110	1100000111	1110000000	1110000100	1111001100
1111110000	1111101100	1111100101	1111101111	1111111011	0000000010	1101000001	1111000100	1111100100	1111011101	1111001110
1111101011	1111111010	0000000101	0000000011	1110110101	1111100001	1111011010	1111000110	1111011111	1111110101	0000001101
0000000110	1110101001	1111000010	1111011000	1110101101	1111010101	1111101101	0000010101	0000001110	1110010010	1110111000
1111001111	1110100110	1111001101	1111101001	0000011010	0000010011	1110010001	1110110001	1111000011	1110011011	1111000101
1111100010	0000011101	0000100101	1110001110	1110100111	1110111100	1101011101	1110110011	1111000111	0001000010	0000111010
1110000010	1110100010	1110111001	1101011010	1110101000	1110111101	0001001000	0000111101	1101110111	1110011001	1110110010
1101011001	1110011101	1110110111	0001010000	0001000011	1101000100	1110000001	1110101110	1101010010	1110010110	1110110110
0001100000	0001000110	1100011111	1101110000	1110011100	1101000101	1110001111	1110101111	0001111100	0001001001	1100010010
1101100101	1110001000	1100110111	1110000110	1110000111	0010000010	0001010001	1100000010	1101100010	1110000011	1100101111
1101111111	1101111101	0010000110	0001100100	1011111010	1101000010	1101101011	1100100110	1101101001	1101111011	0010010000
0001101100	1011011100	1100111100	1101011110	1100010100	1101000110	1101111010	0010100001	0001110111	1011010011	1100101011
1101010110	1100001001	1100010110	1101101111	0010101101	0001111101	1011001010	1100100010	1101010000	1011111011	1100000110
1101101101	0010111001	0010000011	1010011110	1100010000	1101000011	1011110101	1011111101	1101101010	0011000000	0010101111
1010011100	1100001000	1100110010	1011100101	1011010111	1101010100	0011000010	0010111101	1010011011	1011111100	1100011101
1011100011	1011001011	1100111101	0011000101	0011000011	1010010010	1011110100	1100011010	1011001110	1010110011	1100111010
0011000111	0011100000	1010001010	1011100111	1100000011	1010111101	1010011111	1100110110	0011011010	0011100100	1001100101
1011100010	1011111110	1010110101	1010010110	1100100101	0011011101	0011100101	1001011111	1011011101	1011110110	1010101111
1010001011	1011111111	0011100110	0011100111	1001010101	1011011010	1011110011	1010101110	1001111010	1011110111	0100000000
0011111010	1001001010	1011000101	1011101010	1010100110	1001101101	1011101111	0100001000	0011111101	1000011110	1010111001
1011010000	1010100011	1001001011	1011101011	0100010000	0100000001	1000010010	1010110100	1011001000	1010010100	1000111000
1011001001	0100011000	0100001001	1000010001	1010100010	1010111110	1001111101	1000010111	1011000110	0100100000	0100010001
1000001100	1010010000	1010111011	1001110111	1000010110	1010111111	0100101000	0100011100	1000001010	1001111100	1010110010
1001100011	1000001011	1010110111	0100110000	0100100100	0111110010	1001110110	1010101100	1001001001	0111111101	1010110110
0100111000	0100101000	0111011010	1001101100	1010101010	1000111101	0111111010	1010101011	0101000000	0100101100	0111000100
1001100010	1010011000	1000111010	0111100101	1001101111	0110000000	0100110100	0110111100	1001010100	1010001110	1000100110
0111100010	1001101011	0110010000	0100111100	0110010010	1001001000	1001101110	1000100101	0111011011	1001011110	0111000000
0101000100	0110001000	1000100100	1001101010	1000100011	0111000101	1000111111	0111011000	0101001001	0110000010	1000100010

续表 2

定理3中$\lambda \neq 1$时$(A, B, C, D, E, F, G, H, I, J)$不取的10元向量

1001011101	0111110001	0110101110	1000110110	1000000010	0110000100	0101111001	1000011101	1001011010	0111101110	0110010110	
1000101011	1000100000	0110010001	0101110101	1000011100	1000110010	0111101100	0110010011	1000100111	1000101001	0111000001	
0101101011	1000011010	1000101010	0111011101	0110001001	0111111111	1000110111	0111011001	0101010000	1000001000	1000001110	
0111000011	0110000110	0111111000	1001000010	1000000011	0101001010	1000000101	0111101001	0110100110	0101111111	0111110110	
1001000101	1000000110	0101001000	0111110100	0111011110	0110010101	0101101111	0111101011	1001011000	1000100001	0101000010	
0111100111	0111000110	0110000101	0101010100	0111011111	1001100001	1000101000	0100111010	0111100000	0110110010	0101100100	
0101001011	0111000111	1001101000	1000110011	0100110010	0111011100	0110000011	0101100001	0101000110	0110111001	1001110001	
1001000011	0100101010	0111000010	0101110000	0101001101	0100111011	0110110110	1010000010	1001100000	0100100010	0110100010	
0101101000	0101000101	0100110011	0110101010	1010000101	1001101001	0100011010	0110010100	0101001110	0100111101	0100101011	
0110010111	1010001001	1010000011	0100010010	0110000001	0101000011	0100110101	0100100011	0110000111	1010010001	1010000110	
0100001010	0101100000	0100111110	0100101101	0100011011	0101111110	1010100111	1010001111	0100000010	0101001100	0100110110	
0100100101	0100010101	0101110100	1010110000	1010010111	0011111100	0101000001	0100101110	0100011101	0100001101	0101101001	
1011000010	1010101001	0011111001	0100111001	0100100110	0100010110	0100000101	0101001111	1011010100	1010110001	0011110110	
0100110001	0100011110	0100001110	0011110111	0101000111	1011100000	1011000011	0011010001	0100101001	0100010011	0100000011	
0011101111	0100111111	1011111000	1011000111	0011010000	0100100001	0100001011	0011111111	0011011011	0100110111	1100011000	
1011010101	0011001111	0100011001	0100000110	0011111000	0011010100	0100101111	1100101100	1011111001	0011001101	0100010100	
0011101010	0011101110	0011001011	0100100111	1100110001	1110001100	0011001010	0100001100	0011011111	0011100011	0011001001	
0100011111	1101000000	1110001101	0011001000	0100000100	0011011000	0010110001	0011000110	0100010111	1110001001	1111000001	
0010011001	0011100010	0010110010	0010101100	0010111011	0100001111	1111000000	0001110110	0010010010	0010100010	0010101010	
0010100110	0010010110	0100000111	0000100110	0001101011	0010001010	0010010101	0010100111	0010100011	0010010011	0011101011	
0000100011	0000111110	0001011000	0001110000	0010001000	0010011000	0010001011	0010111100	1110000101	0000111011	0001010010	
0001100010	0001111000	0010001111	0001011001	0010110110	0000110011	0000110110	0001001010	0001011111	0001110010	0001110001	
0001010110	0010101011	0000101110	0000101011	0000110101	0001011011	0001101010	0001100110	0001001011	0010011111	0000010110	
1101000111	0000101101	0001010111	0000110010	0001100011	0000011110	0001111110	0000001010	0000100010	0000010010	0001001101	
			0000101010	0001000101	0000011011	0001111001	0000001011				