doi:10.11959/j.issn.1000-436x.2017206

与 3 类向量值密码函数仿射等价的函数数量研究

袁峰[1]，江继军[1]，杨旸[2]，许盛伟[1]
（1. 北京电子科技学院信息安全研究所，北京 100070；2. 福州大学数学与计算机科学学院，福建 福州 350108）

摘 要：Qu-Tan-Tan-Li 函数、Zha-Hu-Sun 函数和 Tang-Carlet-Tang 函数是近些年提出的差分均匀度为 4、各项安全性指标均优良的向量值密码函数。研究与这 3 种密码函数仿射等价函数的计数问题。利用有限域的一些性质，分别计算出与 Zha-Hu-Sun 函数仿射等价函数数量的上下界，与 Qu-Tan-Tan-Li 函数和 Tang-Carlet-Tang 函数仿射等价函数数量的上界。此外，对于 Zha-Hu-Sun 函数仿射等价函数数量的精确值提出了猜测。研究结果表明，有限域 GF(2^8)上至少有 $2^{53}\left[\prod_{i=1}^{8}(2^i-1)\right]^2$ 个与 Zha-Hu-Sun 函数仿射等价的密码函数可直接用于分组密码的 *S* 盒。

关键词：密码学；密码函数；*S* 盒；仿射等价；计数
中图分类号：TP309.7 **文献标识码**：A

Research on affine equivalence enumeration of the three families vectorial function

YUAN Feng[1], JIANG Ji-jun[1], YANG Yang[2], XU Sheng-wei[1]
(1. Information Security Institute, Beijing Electronic Science and Technology Institute, Beijing 100070, China;
2. College of Mathematics and Computer Science, Fuzhou University, Fuzhou 350108, China)

Abstract: In recent years, Qu-Tan-Tan-Li function, Zha-Hu-Sun function and Tang-Carlet-Tang function have been proposed with differential uniformity 4 and many good cryptographic properties. the counting problem of affine equivalent to the three families cryptographic functions was investigated. By using some properties of finite fields, the upper and lower bound of the number of affine equivalent to the Zha-Hu-Sun function, and the upper bound of the number of affine equivalent to the Qu-Tan-Tan-Li function and Tang-Carlet-Tang function were computed, respectively. Moreover, a conjecture was given about the exact number of affine equivalent to the Zha-Hu-Sun function. Results show that there are at least $2^{53}\left[\prod_{i=1}^{8}(2^i-1)\right]^2$ cryptographic functions of affine equivalent to the Zha-Hu-Sun function over finite field GF(2^8), which can be chosen as *S*-boxes of block ciphers.

Key words: cryptography, cryptographic functions, *S*-box, affine equivalence, enumeration

1 引言

S 盒是大多数分组密码重要的非线性部件，它为分组密码的密文提供混淆性[1]。由于实际应用的需要，一般情况下，有限域 GF(2^{2n})上的 *S* 盒经常被设计成一个置换。在过去 20 年中，构造能抵抗差分攻击、线性攻击和代数攻击的 *S* 盒一直都是密码函数研究的重点和热点[2]。

收稿日期：2017-03-08；**修回日期**：2017-07-05
通信作者：袁峰，fyuan1234@aliyun.com
基金项目：国家自然科学基金资助项目（No.61402112）；中央高校基本科研业务费专项基金资助项目（No.2014XSYJ09, No.328201509）；北京电子科技学院科研团队基金资助项目（No.2014 TD2-OHW）
Foundation Items: The National Natural Science Foundation of China (No.61402112), The Fundamental Research Funds for the Central Universities (No.2014XSYJ09, No.328201509), The Fund of Beijing Electronic Science and Technology Institute (No.2014 TD2-OHW)

对于所有 $a\in \mathrm{GF}(q^n)^*$ 和 $b\in \mathrm{GF}(q^n)$，若方程 $F(x)+F(x+a)=b$ 至多有 2 个解，就称向量值密码函数 $F:\mathrm{GF}(q^n)\to \mathrm{GF}(q^n)$ 是几乎完全非线性函数，即 APN 函数[3]。有限域 GF(2^n)上的 APN 函数是抵抗差分攻击能力最强的密码函数[4]。然而，直到 2017 年，当 $n\geqslant 4$ 且 n 为偶数时，有限域 GF(2^{2n})上是否存在 APN 置换仍然是一个公开问题[5]。因而在实际应用中，差分均匀度为 4 的向量值密码函数就是 S 盒最佳的选择。最著名的差分均匀度为 4 的密码函数是逆函数，它的各项安全性指标均优良[6]。例如，著名的 AES 分组密码算法就采用有限域 GF(2^8)上与逆函数仿射等价的向量值函数来作为 S 盒。

2013 年，Qu 等[7]将特殊的布尔函数增加到逆函数，在偶变元情况下构造出 2 类新的差分均匀度为 4、各项密码学性能均优良的向量值函数。之后，Zha 等[2]利用仿射变换改变逆函数在子域上的值，构造出 2 类新的差分均匀度为 4、各项安全性指标均优良的向量值函数。2015 年，Carlet 等[8]通过“置换”逆函数的值，在偶变元情况下构造出一类新的差分均匀度为 4、各项密码学性能均优良的向量值函数。这 3 类向量值密码函数都是通过对逆函数进行“改造”间接构造的。

对于有限域 GF(q^n)上的 2 个向量值函数 $F(x)$和 $F'(x)$，如果存在 2 个可逆仿射变换 $S:\mathrm{GF}(q^n)\to \mathrm{GF}(q^n)$ 和 $T:\mathrm{GF}(q^n)\to \mathrm{GF}(q^n)$，以及一个仿射变换 $L:\mathrm{GF}(q^n)\to \mathrm{GF}(q^n)$，使 $F'=T\circ F\circ S+L$，则称 $F(x)$ 和 $F'(x)$是 EA 等价[9]。当 $L=0$ 时，就称函数 $F(x)$和 $F'(x)$为仿射等价，其中，“∘”表示映射的合成。

若能计算出与以上这 3 类向量值密码函数仿射等价的函数数量，在实际应用中就可知道有多少个与这 3 类函数仿射等价的 S 盒可供选择。本文研究与这 3 类向量值密码函数仿射等价函数的数量。通过使用有限域的一些性质分别计算出与 Zha-Hu-Sun 函数仿射等价函数数量的上下界，与 Qu-Tan-Tan-Li 函数和 Tang-Carlet-Tang 函数仿射等价函数数量的上界。当 $q=2$ 且 $n\leqslant 5$ 时，利用计算机作为辅助手段计算出与 Zha-Hu-Sun 函数仿射等价函数的数量。此外，当 $q\geqslant 2^2$ 且 $n\geqslant 3$ 时，或 $q=2$ 且 $n\geqslant 6$ 时，对 Zha-Hu-Sun 函数仿射等价函数的精确数量提出了猜测。

2　预备知识

设 k 是具有 q 个元素的有限域，其中，$q=p^m$，$p\geqslant 2$ 是一个素数，$m\geqslant 1$，即 $k=\mathrm{GF}(q)$。若 $f(x)$是域 k 上的 n 次不可约多项式，则 $K=k[x]/f(x)$ 是域 k 的 n 次扩域，即 $K=\mathrm{GF}(q^n)$。设 $\phi:K\to k^n$ 是域 K 到域 k 上 n 维线性空间的同构映射，即 $\phi(a_0+a_1x+\cdots+a_{n-1}x^{n-1})=(a_0,a_1,\cdots,a_{n-1})$。

引理 1[10]　若 $L:k^n\to k^n$ 是一个多项式映射 $L(x_1,x_2,\cdots,x_n)=(L_1,L_2,\cdots,L_n)$，其中，$L_i=L_i(x_1,x_2,\cdots,x_n)$ 是多项式环 $k[x_1,\cdots,x_n]$中代数次数至多为 1 的多项式，$i=1,\cdots,n$。令 $\bar{L}=\phi^{-1}\circ L\circ\phi$，则映射 $\bar{L}:K\to K$ 为

$$\bar{L}(X)=\sum_{i=0}^{n-1}A_iX^{q^i}+B$$

其中，$A_i,B\in K$，$\bar{L}(X)$ 被称作线性化多项式。并且，设 k^n 上多项式映射 $L:k^n\to k^n$ 的集合为 C_L，域 K 上映射 $\bar{L}:K\to K$ 的集合为 $C_{\bar{L}}$，则映射 $\varphi:C_L\to C_{\bar{L}}$ 是一个双射。

引理 1 揭示了域 K 上的线性化多项式与 k^n 上的线性仿射之间是一一对应的。

引理 2[11]

$$|GL_n(F_q)|=\prod_{i=0}^{n-1}(q^n-q^i)=q^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}(q^i-1)$$

其中，$GL_n(F_q)$为有限域 GF(q)上的一般线性群（可逆矩阵群）。

引理 2 给出了有限域 GF(q)上 $n\times n$ 阶可逆矩阵的数量。

定义 3 个映射 $S:k^n\to k^n$、$U:k^n\to k^n$ 和 $F:K\to K$ 的合成为 $U\circ\phi\circ F\circ\phi^{-1}\circ S:=U\circ F\circ S$，其中，$F:K\to K$ 是一个向量值函数，$(U,S)\in AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$，$AGL_n^{-1}(F_q)$是有限域 GF($q$)上 $n\times n$ 阶可逆仿射变换群。定义 (U_1,S_1) 和 (U_2,S_2) 之间的运算“$*$”为 $(U_2,S_2)*(U_1,S_1):=(U_2\circ U_1,\ S_1\circ S_2)$，其中，$(U_1,S_1),(U_2,S_2)\in AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$，则有以下结论。

引理 3　$AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$关于运算“$*$”构成一个群。

证明　1) 对于任意$(U_1,S_1),(U_2,S_2)\in AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$，有 $(U_2,S_2)*(U_1,S_1)=(U_2\circ U_1,S_1\circ S_2)\in AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$。

2) 对于任意 (U_1,S_1)，(U_2,S_2) 和 $(U_3,S_3)\in AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$，有

$$(U_3, S_3)*\big((U_2, S_2)*(U_1, S_1)\big)$$
$$=(U_3, S_3)*(U_2\circ U_1, S_1\circ S_2)$$
$$=(U_3\circ U_2\circ U_1, S_1\circ S_2\circ S_3)$$
$$\big((U_3, S_3)*(U_2, S_2)\big)*(U_1, S_1)$$
$$=(U_3\circ U_2, S_2\circ S_3)*(U_1, S_1)$$
$$=(U_3\circ U_2\circ U_1, S_1\circ S_2\circ S_3)$$

于是 $(U_3, S_3)*\big((U_2, S_2)*(U_1, S_1)\big)$
$=\big((U_3, S_3)*(U_2, S_2)\big)*(U_1, S_1)$

3) 对于任意$(U_1, S_1)\in AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$，都有一个单位元$(\boldsymbol{I}, \boldsymbol{I})$，其中，$\boldsymbol{I}$ 是一个单位矩阵，使 $(\boldsymbol{I}, \boldsymbol{I})*(U_1, S_1)=(U_1, S_1)*(\boldsymbol{I}, \boldsymbol{I})=(U_1, S_1)$。

4) 对于任意$(U_1, S_1)\in AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$，都存在一个逆元$(U_1^{-1}, S_1^{-1})\in AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$，使

$$(U_1^{-1}, S_1^{-1})*(U_1, S_1)$$
$$=(U_1, S_1)*(U_1^{-1}, S_1^{-1})=(\boldsymbol{I}, \boldsymbol{I})$$

设$(T, P)\in AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$是使等式 $F=T\circ F\circ P$ (事实上是 $\phi\circ F\circ\phi^{-1}=T\circ\phi\circ F\circ\phi^{-1}\circ P$) 成立的可逆仿射变换对，其中，$F:K\to K$ 是一个向量值函数。以下要证明的引理在后面将多次使用。

引理 4 使等式 $F=T\circ F\circ P$ 成立的可逆仿射变换对$(T, P)\in AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$关于运算“$*$”构成 $AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$的一个子群。

证明 1) 对于任意使等式 $F=T_1\circ F\circ P_1$ 和 $F=T_2\circ F\circ P_2$ 成立的$(T_1, P_1), (T_2, P_2)\in AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$，有 $(T_2, P_2)*(T_1, P_1)=(T_2\circ T_1, P_1\circ P_2)\in AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$。

并且，可逆仿射变换对 $(T_2\circ T_1, P_1\circ P_2)$ 使以下等式成立。

$$(T_2\circ T_1)\circ F\circ(P_1\circ P_2)$$
$$=T_2\circ(T_1\circ F\circ P_1)\circ P_2=T_2\circ F\circ P_2=F$$

2) 对于任意使等式 $F=T_1\circ F\circ P_1$ 成立的$(T_1, P_1)\in AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$，都存在一个逆元$(T_1^{-1}, P_1^{-1})\in AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$使等式 $F=T_1^{-1}\circ F\circ P_1^{-1}$ 成立。

下面给出 2 个容易证明的性质，这 2 个性质在后面会用到。

性质 1 设 e 和 n 都是正整数，$e\geqslant 2$ 且 $n\geqslant 1$，则有$1+e+e^2+\cdots+e^n<e^{n+1}$。

证明 由

$$1+e+e^2+\cdots+e^n=\frac{e^{n+1}-1}{e-1}\leqslant e^{n+1}-1<e^{n+1}$$

可推出以上性质。

性质 2 设 e 和 n 都是正整数，$e\geqslant 2$ 且 $n\geqslant 2$，则 n^2-n 个正整数 e^i-e^j $(i>j,\ i,j=0,1,\cdots,n-1)$和 $e^i-e^j+e^n-1$ $(i<j,\ i,j=0,1,\cdots,n-1)$全都不相等。

证明 采用反证法，可分成以下 4 种情形进行讨论。

1) 假设 $e^a-e^b=e^c-e^d$，其中，$a>b$，$c>d$，$0\leqslant a, b, c, d\leqslant n-1$，则有

$$e^b(e^{a-b}-1)=e^d(e^{c-d}-1)$$
$$e^b(e-1)(e^{a-b-1}+e^{a-b-2}+\cdots+1)$$
$$=e^d(e-1)(e^{c-d-1}+e^{c-d-2}+\cdots+1)$$
$$e^{a-1}+e^{a-2}+\cdots+e^b=e^{c-1}+e^{c-2}+\cdots+e^d$$

以下再分成几种情况进行详细讨论。

情形 1 当 $a\neq c$ 且 $b=d$ 时，有 $e^a=e^c$，这显然不正确。

情形 2 当 $a=c$ 且 $b\neq d$ 时，有 $e^b=e^d$，这显然也不正确。

情形 3 当 $a>c$ 且 $b\neq d$ 时，细分成以下 3 种情形进行分析。

① 当 $a>c$ 且 $d>b$ 时，即 $a>c>d>b$，于是

$$e^{a-1}+e^{a-2}+\cdots+e^b-(e^{c-1}+e^{c-2}+\cdots+e^d)$$
$$=e^{a-1}+e^{a-2}+\cdots+e^c+e^{d-1}+e^{d-2}+\cdots+e^b=0$$

这与 $e^{a-1}+e^{a-2}+\cdots+e^c+e^{d-1}+e^{d-2}+\cdots+e^b>0$ 相矛盾。

② 当 $a>c$ 且 $b\geqslant c$ 时，即 $a>b\geqslant c>d$，有

$$e^{a-1}+e^{a-2}+\cdots+e^b-(e^{c-1}+e^{c-2}+\cdots+e^d)=0$$

但由性质 1 可知，$e^b>e^{c-1}+e^{c-2}+\cdots+e^d$，进而可以推出 $e^{a-1}+e^{a-2}+\cdots+e^b-(e^{c-1}+e^{c-2}+\cdots+e^d)>0$，与上面结论矛盾。

③当 $a>c$，$c>b$ 且 $b>d$ 时，即 $a>c>b>d$，就有

$$e^{a-1}+e^{a-2}+\cdots+e^b-(e^{c-1}+e^{c-2}+\cdots+e^d)$$
$$=e^{a-1}+e^{a-2}+\cdots+e^c-(e^{b-1}+e^{b-2}+\cdots+e^d)=0$$

但由性质 1 可知，$e^c>e^{b-1}+e^{b-2}+\cdots+e^d$，进而可以推出 $e^{a-1}+e^{a-2}+\ldots+e^c-(e^{b-1}+e^{b-2}+\ldots+e^d)>0$，与上面结论矛盾。

情形 4 当 $a<c$ 且 $b\neq d$ 时，与 $a>c$ 且 $b\neq d$ 时的情形相类似，利用相同的方法可导出矛盾。

2) 假设 $e^a-e^b+e^n-1=e^c-e^d+e^n-1$，其中，$a<b$，$c<d$，$0\leqslant a, b, c, d\leqslant n-1$，则有 $e^b-e^a=e^d-e^c$。与情形 1 完全相同，利用相同的方法可推出矛盾。

3) 假设 $e^a-e^b=e^c-e^d+e^n-1$，其中，$a>b$，$c<d$，$0\leqslant a,b,c,d\leqslant n-1$，则有

$$e^b(e^{a-b}-1)=e^n-1-e^c(e^{d-c}-1)$$

$$e^b(e-1)(e^{a-b-1}+e^{a-b-2}+\cdots+1)$$
$$=(e-1)(e^{n-1}+e^{n-2}+\cdots+1)-$$
$$e^c(e-1)(e^{d-c-1}+e^{d-c-2}+\cdots+1)$$

$$e^{a-1}+e^{a-2}+\cdots+e^b$$
$$=e^{n-1}+e^{n-2}+\cdots+1-(e^{d-1}+e^{d-2}+\cdots+e^c),$$

$$e^{a-1}+e^{a-2}+\cdots+e^b+e^{d-1}+e^{d-2}+\cdots+e^c$$
$$=e^{n-1}+e^{n-2}+\cdots+1$$

不难发现，$e^{a-1}+e^{a-2}+\cdots+e^b$ 的项数为 $a-b$，$e^{d-1}+e^{d-2}+\cdots+e^c$ 的项数为 $d-c$，其中，$0<a-b,d-c\leqslant n-1$。容易得出

$$e^{a-1}+e^{a-2}+\cdots+e^b\leqslant e^{n-2}+e^{n-3}+\cdots+e+1$$
$$e^{d-1}+e^{d-2}+\cdots+e^c\leqslant e^{n-2}+e^{n-3}+\cdots+e+1$$

由于 $e\geqslant 2$，可得

$$2(e^{n-2}+e^{n-3}+\cdots+e+1)\leqslant$$
$$e^{n-1}+e^{n-2}+\cdots+e^2+e$$

由此可推出

$$e^{a-1}+e^{a-2}+\cdots+e^b+e^{d-1}+e^{d-2}+\cdots+e^c\leqslant$$
$$2(e^{n-2}+e^{n-3}+\cdots+e+1)<$$
$$e^{n-1}+e^{n-2}+\cdots+e^2+e+1$$

于是就又导出了矛盾。

4) 假设 $e^a-e^b+e^n-1=e^c-e^d$，其中，$a<b$，$c>d$，$0\leqslant a,b,c,d\leqslant n-1$，则有 $e^c-e^d=e^a-e^b+e^n-1$。与情形 3 完全相同，利用相同的方法可推出矛盾。

综上所述，以上 4 种情形均不成立。因而 n^2-n 个正整数 e^i-e^j ($i>j$，$i,j=0,1,\cdots,n-1$) 和 $e^i-e^j+e^n-1$ ($i<j$，$i,j=0,1,\cdots,n-1$)全都不相同。

3 Zha-Hu-Sun 函数、Qu-Tan-Tan-Li 函数和 Tang-Carlet-Tang 函数介绍

3.1 Zha-Hu-Sun 函数

设 n 和 s 是正整数，$q=2^s$ 且 $t\in \mathrm{GF}(q)^*$，当 $s\geqslant 2$ 时，有限域 $\mathrm{GF}(q^n)$上第一类 Zha-Hu-Sun 函数的形式如下所示。

$$f_1(x)=x^{-1}+t(x^q+x)^{q^n-1}+t=\begin{cases}x^{-1}+t, & x^q=x\\ x^{-1}, & x^q\neq x\end{cases}$$

当 $s=1$ 时，有限域 $\mathrm{GF}(2^n)$上第一类 Zha-Hu-Sun 函数的形式即为

$$f_1(x)=x^{-1}+(x^2+x)^{2^n-1}+1=\begin{cases}x^{-1}+1, & x^2=x\\ x^{-1}, & x^2\neq x\end{cases}$$

设 n 和 s 是正整数，$q=2^s$，迹函数 $Tr_1^n:\mathrm{GF}(q^n)\to\mathrm{GF}(q)$为 $Tr_1^n(x)=x+x^q+x^{q^2}+\cdots+x^{q^{n-1}}$，$x\in\mathrm{GF}(q^n)$，$t_1,t_2\in\mathrm{GF}(q)$且 $Tr_1^n(t_1^{-1})=1$，当 $s\geqslant 2$ 时，有限域 $\mathrm{GF}(q^n)$上第二类 Zha-Hu-Sun 函数的形式为

$$f_2(x)=t_1x^{-1}+(t_1+1)x^{-1}(x^q+x)^{q^n-1}+$$
$$t_2(x^q+x)^{q^n-1}+t_2=\begin{cases}t_1x^{-1}+t_2, & x^q=x\\ x^{-1}, & x^q\neq x\end{cases}$$

当 $s=1$ 时，易知此时 $t_1=t_2=1$ 且 n 是奇数，有限域 $\mathrm{GF}(2^n)$上第二类 Zha-Hu-Sun 函数的形式为

$$f_2(x)=x^{-1}+(x^2+x)^{2^n-1}+1=\begin{cases}x^{-1}+1, & x^2=x\\ x^{-1}, & x^2\neq x\end{cases}$$

容易发现，有限域 $\mathrm{GF}(2^n)$上第一类 Zha-Hu-Sun 函数和第二类 Zha-Hu-Sun 函数的形式完全相同。

3.2 Qu-Tan-Tan-Li 函数

设 n 是一个正偶数，$n=2t$，$2\leqslant k\leqslant t-1$，有限域 $\mathrm{GF}(2^n)$上第一类 Qu-Tan-Tan-Li 函数和第二类 Qu-Tan-Tan-Li 函数的形式分别为

$$f_1(x)=x^{-1}+Tr_1^n(x+(x^{-1}+1)^{-1})$$

$$f_2(x)=x^{-1}+Tr_1^n(x^{-3(2^k+1)}+(x^{-1}+1)^{3(2^k+1)})$$

其中，迹函数 $Tr_1^n:\mathrm{GF}(2^n)\to\mathrm{GF}(2)$ 为 $Tr_1^n(x)=x+x^2+x^{2^2}+\cdots+x^{2^{n-1}}$，$x\in\mathrm{GF}(2^n)$。

3.3 Tang-Carlet-Tang 函数

设 n 是一个正偶数，$n\geqslant 6$，集合 U 是有限域 $\mathrm{GF}(2^n)$的一个子集，满足以下 2 个条件。

1) 对于任意 $x\in U$，有 $x+1\in U$。

2) 对于任意 $x\in U$，有 $Tr_1^n(x^{-1})=1$。

满足以上 2 个条件的所有集合 U 的并集为

$$U_{\max}=\{x\in\mathrm{GF}(2^n)\,|\,Tr_1^n(x^{-1})=Tr_1^n((x+1)^{-1})=1\}$$

它是满足以上 2 个条件最大的一个集合。令

$$U_{m_0}=\{x\in U_{\max}\,|\,Tr_1^n(x)=0\}$$

$$U_{m_1}=\{x\in U_{\max}\,|\,Tr_1^n(x)=1\}$$

集合 U_{m_0} 和 U_{m_1} 都是满足以上 2 个条件的集合，并且 $U_{\max}=U_{m_0}\cup U_{m_1}$。

有限域 $\mathrm{GF}(2^n)$上 Tang-Carlet-Tang 函数的形式为

$$f(x)=\begin{cases}(x+1)^{-1}, & x\in U\\ x^{-1}, & x\in \mathrm{GF}(2^n)\setminus U\end{cases}$$

Tang-Carlet-Tang 函数的简化形式即为

$$f(x)=(x+\delta_U(x))^{-1}$$

其中，$\delta_U(x)=\begin{cases}1, & x\in U\\ 0, & x\in \mathrm{GF}(2^n)\setminus U\end{cases}$

容易得出

$$\delta_{U_{\max}}(x)=Tr_1^n(x^{-1})Tr_1^n((x+1)^{-1})$$

$$\delta_{U_{m_0}}(x)=(1+Tr_1^n(x))Tr_1^n(x^{-1})Tr_1^n((x+1)^{-1})$$

$$\delta_{U_{m_1}}(x)=Tr_1^n(x)Tr_1^n(x^{-1})Tr_1^n((x+1)^{-1})$$

4 与 3 类向量值密码函数仿射等价的函数数量

本节详细讨论如何计算与 Zha-Hu-Sun 函数仿射等价函数数量的上下界，与 Qu-Tan-Tan-Li 函数和 Tang-Carlet-Tang 函数仿射等价函数数量的上界，有了第 2 节和第 3 节的准备工作后，下面将证明本文的主要结论。

定理 1 对于有限域 $\mathrm{GF}(q^n)$ 上的第一类 Zha-Hu-Sun 函数

$$f_1(x)=x^{-1}+t(x^q+x)^{q^n-1}+t$$

其中，$t\in\mathrm{GF}(q)^*$，$q\geqslant 2$ 和 $n\geqslant 2$，使等式 $f_1=\sigma\circ f_1\circ\rho$ 成立的可逆仿射变换对 (σ,ρ) 的数量大于或等于 n。进一步，与第一类 Zha-Hu-Sun 函数仿射等价密码函数的数量 M 满足以下不等式。

$$\frac{\left[q^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}(q^i-1)\right]^2}{n}\leqslant M\leqslant\frac{\left[q^{\frac{n(n+1)}{2}}\prod_{i=1}^{n}(q^i-1)\right]^2}{n}$$

证明 由 $f_1=\sigma\circ f_1\circ\rho$ 可知，$\sigma^{-1}\circ f_1=f_1\circ\rho$。再由引理 1 可设

$$\rho(x)=\sum_{i=0}^{n-1}A_ix^{q^i}+B\text{ 和 }\sigma^{-1}(x)=\sum_{i=0}^{n-1}C_ix^{q^i}+D$$

其中，A_i、B、C_i、$D\in\mathrm{GF}(q^n)$。根据等式 $\sigma^{-1}\circ f_1=f_1\circ\rho$，有

$$\sum_{i=0}^{n-1}C_i(x^{-1}+t(x^q+x)^{q^n-1}+t)^{q^i}+D=\left(\sum_{i=0}^{n-1}A_ix^{q^i}+B\right)^{-1}+t\left(\left(\sum_{i=0}^{n-1}A_ix^{q^i}+B\right)^q+\sum_{i=0}^{n-1}A_ix^{q^i}+B\right)^{q^n-1}+t$$

可分成以下 4 种情况讨论该等式。

1) 当 $x^q=x$ 且 $(\rho(x))^q=\rho(x)$ 时，即 $x\in\mathrm{GF}(q)$ 且 $\rho(x)\in\mathrm{GF}(q)$，此时该等式为

$$\sum_{i=0}^{n-1}C_i(x^{-1}+t)^{q^i}+D=\left(\sum_{i=0}^{n-1}A_ix^{q^i}+B\right)^{-1}+t$$

2) 当 $x^q=x$ 且 $(\rho(x))^q\neq\rho(x)$ 时，即 $x\in\mathrm{GF}(q)$ 且 $\rho(x)\in\mathrm{GF}(q^n)/\mathrm{GF}(q)$，此时该等式为

$$\sum_{i=0}^{n-1}C_i(x^{-1}+t)^{q^i}+D=\left(\sum_{i=0}^{n-1}A_ix^{q^i}+B\right)^{-1}$$

3) 当 $x^q\neq x$ 且 $(\rho(x))^q=\rho(x)$ 时，即 $x\in\mathrm{GF}(q^n)/\mathrm{GF}(q)$ 且 $\rho(x)\in\mathrm{GF}(q)$，此时该等式为

$$\sum_{i=0}^{n-1}C_ix^{-q^i}+D=\left(\sum_{i=0}^{n-1}A_ix^{q^i}+B\right)^{-1}+t$$

4) 当 $x^q\neq x$ 且 $(\rho(x))^q\neq\rho(x)$ 时，即 $x\in\mathrm{GF}(q^n)/\mathrm{GF}(q)$ 且 $\rho(x)\in\dfrac{\mathrm{GF}(q^n)}{\mathrm{GF}(q)}$，此时该等式为

$$\sum_{i=0}^{n-1}C_ix^{-q^i}+D=\left(\sum_{i=0}^{n-1}A_ix^{q^i}+B\right)^{-1}$$

下面要研究 $B=D=0$ 时的情形，即可逆仿射变换 ρ 和 σ 的仿射部分均为 0 时的情形，此时上述等式可转化成以下这些形式。

1) 当 $x\in\mathrm{GF}(q)$ 且 $\rho(x)\in\mathrm{GF}(q)$ 时，有

$$\sum_{i=0}^{n-1}C_i(x^{-1}+t)^{q^i}=\left(\sum_{i=0}^{n-1}A_ix^{q^i}\right)^{-1}+t$$

2) 当 $x\in\mathrm{GF}(q)$ 且 $\rho(x)\in\mathrm{GF}(q^n)/\mathrm{GF}(q)$ 时，有

$$\sum_{i=0}^{n-1}C_i(x^{-1}+t)^{q^i}=\left(\sum_{i=0}^{n-1}A_ix^{q^i}\right)^{-1}$$

3) 当 $x\in\mathrm{GF}(q^n)/\mathrm{GF}(q)$ 且 $\rho(x)\in\mathrm{GF}(q)$ 时，有

$$\sum_{i=0}^{n-1}C_ix^{-q^i}=\left(\sum_{i=0}^{n-1}A_ix^{q^i}\right)^{-1}+t$$

4) 当 $x\in\mathrm{GF}(q^n)/\mathrm{GF}(q)$ 且 $\rho(x)\in\mathrm{GF}(q^n)/\mathrm{GF}(q)$ 时，有

$$\sum_{i=0}^{n-1}C_ix^{-q^i}=\left(\sum_{i=0}^{n-1}A_ix^{q^i}\right)^{-1}$$

由于 $0\in\mathrm{GF}(q)$ 且 $\rho(0)=0\in\mathrm{GF}(q)$，因此，$x=0$ 满足情形 1)时的等式，再根据 $t\in\mathrm{GF}(q)^*$，于是就有 $\sum_{i=0}^{n-1}C_it^{q^i}=\sum_{i=0}^{n-1}C_it=0^{-1}+t=t$，由此可得 $\sum_{i=0}^{n-1}C_i=1$。

若 $\alpha \in \mathrm{GF}(q)$且 $\rho(\alpha) \in \dfrac{\mathrm{GF}(q^n)}{\mathrm{GF}(q)}$，此时 $x=\alpha$ 满足情形 2)时的等式。然而，由 $\sum_{i=0}^{n-1} C_i = 1$ 和 $t \in \mathrm{GF}(q)^*$ 可以推出

$$\sum_{i=0}^{n-1} C_i(\alpha^{-1}+t)^{q^i} = \sum_{i=0}^{n-1} C_i(\alpha^{-1}+t) = \alpha^{-1}+t \in GF(q)$$

和 $\left(\sum_{i=0}^{n-1} A_i \alpha^{q^i}\right)^{-1} \in \dfrac{GF(q^n)}{GF(q)}$，容易发现，$\sum_{i=0}^{n-1} C_i(\alpha^{-1}+t)^{q^i} \neq \left(\sum_{i=0}^{n-1} A_i \alpha^{q^i}\right)^{-1}$，推出矛盾。因此，可知情形 2)不存在。

由于情形 2)不存在，再根据 $\rho(x)$ 是有限域 $\mathrm{GF}(q^n)$上的置换多项式可得，对于任意 $x \in \mathrm{GF}(q)$，都有 $\rho(x) \in \mathrm{GF}(q)$，$\rho(x)$ 在有限域 $\mathrm{GF}(q)$上也是一个置换多项式，由此可推出，情形 3)也不存在。

综上所述，当可逆仿射变换 ρ 和 σ 的仿射部分均为零时，只存在情况 1)和情况 4)，即

当 $x \in \mathrm{GF}(q)$且 $\rho(x) \in \mathrm{GF}(q)$时，有

$$\sum_{i=0}^{n-1} C_i(x^{-1}+t)^{q^i} = \sum_{i=0}^{n-1} C_i(x^{-1}+t) = x^{-1}+t = \left(\sum_{i=0}^{n-1} A_i x^{q^i}\right)^{-1} + t$$

当 $x \in \mathrm{GF}(q^n)/\mathrm{GF}(q)$且 $\rho(x) \in \mathrm{GF}(q^n)/\mathrm{GF}(q)$时，有

$$\sum_{i=0}^{n-1} C_i x^{-q^i} = \left(\sum_{i=0}^{n-1} A_i x^{q^i}\right)^{-1}$$

可将以上 2 个等式写成 1 个等式的形式，对于任意 $x \in \mathrm{GF}(q^n)$，都有

$$\left(\sum_{i=0}^{n-1} A_i x^{q^i}\right)^{-1} = \sum_{i=0}^{n-1} C_i x^{-q^i} = \sum_{i=0}^{n-1} C_i x^{(q^n-2)q^i}$$

其中，$\sum_{i=0}^{n-1} C_i = 1$。

当 $\rho(x) = \sum_{i=0}^{n-1} A_i x^{q^i} = 0$时，由于映射 ρ 是一个可逆线性映射，因此，等式 $\rho(x)=0$ 有且只有一个零解，即 $\rho(0)=0$。对于任意 $0 \neq \theta \in \mathrm{GF}(q^n)$，都有 $\rho(\theta) \neq 0$，进而

$$\left(\sum_{i=0}^{n-1} A_i \theta^{q^i}\right)\left(\sum_{i=0}^{n-1} C_i \theta^{(q^n-2)q^i}\right) = 1$$

展开等式左边的每一项，就有

$$\begin{aligned}
&A_0C_0\theta^{q^n-1} + A_0C_1\theta^{q^n-q} + A_0C_2\theta^{q^n-q^2} + \cdots + \\
&A_0C_{n-1}\theta^{q^n-q^{n-1}} + \\
&A_1C_0\theta^{q-1} + A_1C_1\theta^{q^n-1} + A_1C_2\theta^{q^n-q^2+q-1} + \cdots + \\
&A_1C_{n-1}\theta^{q^n-q^{n-1}+q-1} + \\
&A_2C_0\theta^{q^2-1} + A_2C_1\theta^{q^2-q} + A_2C_2\theta^{q^n-1} + \cdots + \\
&A_2C_{n-1}\theta^{q^n-q^{n-1}+q^2-1} + \cdots + \\
&A_{n-2}C_0\theta^{q^{n-2}-1} + A_{n-2}C_1\theta^{q^{n-2}-q} + \\
&A_{n-2}C_2\theta^{q^{n-2}-q^2} + \cdots + A_{n-2}C_{n-1}\theta^{q^n+q^{n-2}-q^{n-1}-1} + \\
&A_{n-1}C_0\theta^{q^{n-1}-1} + A_{n-1}C_1\theta^{q^{n-1}-q} + \\
&A_{n-1}C_2\theta^{q^{n-1}-q^2} + \cdots + A_{n-1}C_{n-1}\theta^{q^n-1} = 1
\end{aligned} \tag{1}$$

其中，单项式 $A_iC_j\theta^{q^i+(q^n-2)q^j}$（$i,\ j=0,1,\cdots,n-1$）的代数次数 $q^i+(q^n-2)q^j \equiv q^i-q^j \bmod q^n-1$ 如下所示。

1) 当 $i>j$ 时，代数次数为 q^i-q^j。

2) 当 $i<j$ 时，代数次数为 $q^i-q^j+q^n-1$。

3) 当 $i=j$ 时，代数次数为 q^n-1。

由性质 2 可知，当 $q \geqslant 2$ 且 $n \geqslant 2$ 时，式(1)中 n^2-n 个单项式 $A_iC_j\theta^{q^i+(q^n-2)q^j}$（$i \neq j$，$i,\ j=0,1,\cdots,n-1$）的代数次数均不相同，并且都小于 q^n-1。因此，式(1)的项数至多只能是 n^2-n+2。

易知 q^n-1 个非零元素 $0 \neq \theta \in \mathrm{GF}(q^n)$是式(1)全部的解，同时，这 q^n-1 个非零元素 $0 \neq \theta \in \mathrm{GF}(q^n)$也是等式 $x^{q^n-1}-1=0$ 全部的解。$x^{q^n-1}-1=0$ 的项数为 2，式(1)的项数至多只能是 n^2-n+2，当 $n \geqslant 2$ 时，易知 $n^2-n+2>2$。由此可知，式(1)的形式只能是 $x^{q^n-1}-1=0$。因此，对于式(1)的系数可得到

$$\sum_{i=0}^{n-1} A_iC_i = 1,\ C_iA_{i+r} = 0$$

其中，$0 \leqslant i \leqslant n-1$，$1 \leqslant r \leqslant n-1$，$i+r \bmod n$。

由于映射 σ^{-1} 是一个可逆线性映射，因此，映射 σ^{-1} 线性化多项式的系数不可能全为 0，至少得有一个系数非零。不妨设 $C_b \neq 0$，$0 \leqslant b \leqslant n-1$，由 $C_bA_{b+1}=0$，$C_bA_{b+2}=0$，$\cdots$，$C_bA_{b+n-2}=0$，$C_bA_{b+n-1}=0$ 可以推出 $A_{b+1}=0$，$A_{b+2}=0$，$\cdots$，$A_{b+n-2}=0$，$A_{b+n-1}=0$。并且，由于映射 ρ 也是一个可逆线性映射，因而可知 $A_b \neq 0$。利用相同的方法，由 $C_{b+1}A_b = C_{b+1}A_{b+1+n-1}=0$，$C_{b+2}A_b = C_{b+2}A_{b+2+n-2}=0$，$\cdots$，$C_{b+n-2}A_b =$

$C_{b+n-2}A_{b+n-2+2}=0$, $C_{b+n-1}A_b=C_{b+n-1}A_{b+n-1+1}=0$ 可以推出 $C_{b+1}=0$, $C_{b+2}=0$, …, $C_{b+n-2}=0$, $C_{b+n-1}=0$。进一步，根据 $\sum_{i=0}^{n-1}C_i=1$ 可得 $C_b=1$。最后，由 $\sum_{i=0}^{n-1}A_iC_i=A_bC_b=1$ 可推出 $A_b=1$。

综上，当 B=D=0 时，即可逆仿射变换 ρ 和 σ 的仿射部分均为零时，映射 ρ 和 σ^{-1} 线性化多项式的形式只能是 $\rho(x)=x^{q^b}$ 和 $\sigma^{-1}(x)=x^{q^b}$，容易计算出 $\rho(x)=x^{q^b}$ 和 $\sigma(x)=x^{q^{n-b}}$，其中，b=0,1,…,n−1。由此可知，当 B, $D\in$GF(q^n)时，使等式 $f_1=\sigma\circ f_1\circ\rho$ 成立的一般的可逆仿射变换对 (σ,ρ) 的数量一定大于或等于 n。

由引理 4 可知，可逆仿射变换对 (σ,ρ) 关于运算“∗”构成 $AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$的一个子群。利用可逆仿射变换对 (σ,ρ) 所形成的子群对群 $AGL_n^{-1}(F_q)\times AGL_n^{-1}(F_q)$划分等价类，陪集首的个数即为与第一类 Zha-Hu-Sun 函数仿射等价密码函数的数量。由于可逆仿射变换对 (σ,ρ) 的数量大于或等于 n，利用引理 2 可知，与第一类 Zha-Hu-Sun 函数仿射等价密码函数的数量小于或等于 $\dfrac{\left[q^{\frac{n(n+1)}{2}}\prod_{i=1}^{n}(q^i-1)\right]^2}{n}$。另外，当可逆仿射变换 ρ 和 σ 的仿射部分均为 0 时，利用引理 2 可知，此时与第一类 Zha-Hu-Sun 函数仿射等价密码函数的数量为 $\dfrac{\left[q^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}(q^i-1)\right]^2}{n}$，即与第一类 Zha-Hu-Sun 函数仿射等价密码函数的数量大于或等于 $\dfrac{\left[q^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}(q^i-1)\right]^2}{n}$。于是，与第一类 Zha-Hu-Sun 函数仿射等价密码函数的数量 M 满足

$$\frac{\left[q^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}(q^i-1)\right]^2}{n}\leqslant M\leqslant\frac{\left[q^{\frac{n(n+1)}{2}}\prod_{i=1}^{n}(q^i-1)\right]^2}{n}$$

定理 2 对于有限域 GF(q^n)上的第二类 Zha-Hu-Sun 函数

$$f_2(x)=t_1x^{-1}+(t_1+1)x^{-1}(x^q+x)^{q^n-1}+t_2(x^q+x)^{q^n-1}+t_2$$

其中，t_1, $t_2\in$GF(q)，$Tr_1^n(t_1^{-1})=1$，$q\geqslant 2$ 和 $n\geqslant 2$，使等式 $f_2=\sigma\circ f_2\circ\rho$ 成立的可逆仿射变换对 (σ,ρ) 的数量大于或等于 n。进一步，与第二类 Zha-Hu-Sun 函数仿射等价密码函数的数量 M 满足

$$\frac{\left[q^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}(q^i-1)\right]^2}{n}\leqslant M\leqslant\frac{\left[q^{\frac{n(n+1)}{2}}\prod_{i=1}^{n}(q^i-1)\right]^2}{n}$$

证明 与定理 1 的证明方法完全相同。

当 q=2 且 $n\leqslant$5 时，可以利用计算机作为辅助手段测试出与 Zha-Hu-Sun 函数仿射等价密码函数的数量。

定理 3 当 q=2 且 n=3 时，有限域 GF(2^3)上 Zha-Hu-Sun 函数的形式为

$$f_3(x)=x^6+(x^2+x)^7+1=\begin{cases}x^6+1, & x^2=x\\ x^6, & x^2\neq x\end{cases}$$

使等式 $f_3=\sigma\circ f_3\circ\rho$ 成立的可逆仿射变换对 (σ,ρ) 的数量为 96，进一步，与 Zha-Hu-Sun 函数仿射等价密码函数的数量为 18 816。

证明 对于等式 $f_3(x)=\sigma\circ f_3\circ\rho(x)$，经测试，满足该等式可逆仿射变换对 (σ,ρ) 的数量为 96。由引理 4 可知，可逆仿射变换对 (σ,ρ) 关于运算“∗”构成 $AGL_3^{-1}(F_2)\times AGL_3^{-1}(F_2)$的一个子群。利用可逆仿射变换对 (σ,ρ) 所形成的子群对群 $AGL_3^{-1}(F_2)\times AGL_3^{-1}(F_2)$划分等价类，陪集首的个数即为与 Zha-Hu-Sun 函数仿射等价密码函数的数量。利用引理 2 可得，当 n=3 时，与 Zha-Hu-Sun 函数仿射等价密码函数的数量即为 $\dfrac{\left[2^{\frac{3(3+1)}{2}}\prod_{i=1}^{3}(2^i-1)\right]^2}{96}$=18 816。

定理 4 当 q=2 且 n=4 时，有限域 GF(2^4)上 Zha-Hu-Sun 函数的形式为

$$f_4(x)=x^{14}+(x^2+x)^{15}+1=\begin{cases}x^{14}+1, & x^2=x\\ x^{14}, & x^2\neq x\end{cases}$$

当 q=2 且 n=5 时，有限域 GF(2^5)上 Zha-Hu-Sun 函数为

$$f_5(x)=x^{30}+(x^2+x)^{31}+1=\begin{cases}x^{30}+1, & x^2=x\\ x^{30}, & x^2\neq x\end{cases}$$

使等式 $f_4=\sigma\circ f_4\circ\rho$ 和 $f_5=\sigma\circ f_5\circ\rho$ 成立的可逆仿射变换对 (σ,ρ) 的数量分别为 4 和 5，进一步，与 Zha-Hu-Sun 函数仿射等价密码函数的数量

分别为 26 011 238 400 和 $2^{30}\times 19\ 071\ 045$。

证明　对于等式 $f_4(x)=\sigma\circ f_4\circ\rho(x)$，经测试，满足该等式可逆仿射变换对 (σ,ρ) 的数量为 4，并且可逆仿射变换 ρ 和 σ 线性化多项式的形式是 $\rho(x)=x^{2^a}$ 和 $\sigma(x)=x^{2^{4-a}}$，a=0、1、2、3；对于等式 $f_5(x)=\sigma\circ f_5\circ\rho(x)$，经测试，满足该等式可逆仿射变换对 (σ,ρ) 的数量为 5，并且可逆仿射变换 ρ 和 σ 线性化多项式的形式是 $\rho(x)=x^{2^a}$ 和 $\sigma(x)=x^{2^{5-a}}$，a=0、1、2、3、4。由引理 4 可知，可逆仿射变换对 (σ,ρ) 关于运算“$*$”构成 $AGL_4^{-1}(F_2)\times AGL_4^{-1}(F_2)$（或 $AGL_5^{-1}(F_2)\times AGL_5^{-1}(F_2)$）的一个子群。利用可逆仿射变换对 (σ,ρ) 所形成的子群对群 $AGL_4^{-1}(F_2)\times AGL_4^{-1}(F_2)$（或 $AGL_5^{-1}(F_2)\times AGL_5^{-1}(F_2)$）划分等价类，陪集首的个数即为与 Zha-Hu-Sun 函数仿射等价密码函数的数量。利用引理 2 可得，当 n=4 时，与 Zha-Hu-Sun 函数仿射等价密码函数的数量为 $\dfrac{\left[2^{\frac{4(4+1)}{2}}\prod_{i=1}^{4}(2^i-1)\right]^2}{4}$=26 011 238 400；当 n=5 时，与 Zha-Hu-Sun 函数仿射等价密码函数的数量为 $\dfrac{\left[2^{\frac{5(5+1)}{2}}\prod_{i=1}^{5}(2^i-1)\right]^2}{5}=2^{30}\times 19\ 071\ 045$。

当 q=2 且 $n\geqslant 6$ 时，无法利用计算机测试出与 Zha-Hu-Sun 函数仿射等价密码函数的数量。由于 q=2 且 n=4,5 时，使上述等式 $f_4=\sigma\circ f_4\circ\rho$ 和 $f_5=\sigma\circ f_5\circ\rho$ 成立的可逆仿射变换对 (σ,ρ) 的数量分别为 4 和 5，并且可逆仿射变换 ρ 和 σ 线性化多项式的形式分别为 $\rho(x)=x^{2^a}$ 和 $\sigma(x)=x^{2^{4-a}}$（a=0,1,2,3）；$\rho(x)=x^{2^a}$ 和 $\sigma(x)=x^{2^{5-a}}$（a=0,1,2,3,4）。基于该事实以及定理 1 和定理 2 所证明的使 $f_1=\sigma\circ f_1\circ\rho$ 或 $f_2=\sigma\circ f_2\circ\rho$ 成立的可逆仿射变换对 (σ,ρ) 的数量大于或等于 n，提出以下猜想。

猜想 1　对于有限域 GF(q^n)上第一类 Zha-Hu-Sun 函数

$$f_1(x)=x^{-1}+t(x^q+x)^{q^n-1}+t$$

其中，$t\in \mathrm{GF}(q)^*$，第二类 Zha-Hu-Sun 函数 $f_2(x)=t_1x^{-1}+(t_1+1)x^{-1}(x^q+x)^{q^n-1}+t_2(x^q+x)^{q^n-1}+t_2$ 其中，$t_1,t_2\in\mathrm{GF}(q)$ 且 $Tr_1^n(t_1^{-1})=1$，当 $q\geqslant 2^2$ 且 $n\geqslant 3$ 时，或当 q=2 且 $n\geqslant 6$ 时，使 $f_1=\sigma\circ f_1\circ\rho$ 或 $f_2=\sigma\circ f_2\circ\rho$ 成立的可逆仿射变换对 (σ,ρ) 的数量为 n，其中，可逆仿射变换 ρ 和 σ 线性化多项式的形式只能是 $\rho(x)=x^{q^t}$ 和 $\sigma(x)=x^{q^{n-t}}$，t=0,1,…,n−1。进一步，与第一类或第二类 Zha-Hu-Sun 函数仿射等价密码函数的数量为

$$\frac{\left[q^{\frac{n(n+1)}{2}}\prod_{i=1}^{n}(q^i-1)\right]^2}{n}$$

定理 5　对于有限域 GF(2^n)上的第一类 Qu-Tan-Tan-Li 函数

$$f_1(x)=x^{-1}+Tr_1^n(x+(x^{-1}+1)^{-1})$$

以及第二类 Qu-Tan-Tan-Li 函数

$$f_2(x)=x^{-1}+Tr_1^n(x^{-3(2^k+1)}+(x^{-1}+1)^{3(2^k+1)})$$

其中，n 是一个正偶数，$n\geqslant 6$，n=2t 和 $2\leqslant k\leqslant t-1$，使 $f_1=\sigma\circ f_1\circ\rho$ 或 $f_2=\sigma\circ f_2\circ\rho$ 成立的可逆仿射变换对 (σ,ρ) 的数量大于或等于 n。进一步，与第一类或第二类 Qu-Tan-Tan-Li 函数仿射等价密码函数的数量小于或等于 $\dfrac{\left[2^{\frac{n(n+1)}{2}}\prod_{i=1}^{n}(2^i-1)\right]^2}{n}$。

证明　容易验证线性化多项式 $\rho(x)=x^{2^a}$ 和 $\sigma(x)=x^{2^{n-a}}$（a=0,1,…,n−1）使 $f_1=\sigma\circ f_1\circ\rho$ 和 $f_2=\sigma\circ f_2\circ\rho$ 均成立，因此易知，使 $f_1=\sigma\circ f_1\circ\rho$ 或 $f_2=\sigma\circ f_2\circ\rho$ 成立的可逆仿射变换对 (σ,ρ) 的数量大于或等于 n。由引理 2 和引理 4 可得，与第一类 Qu-Tan-Tan-Li 函数或第二类 Qu-Tan-Tan-Li 函数仿射等价密码函数的数量小于或等于 $\dfrac{\left[2^{\frac{n(n+1)}{2}}\prod_{i=1}^{n}(2^i-1)\right]^2}{n}$。

定理 6　对于有限域 GF(2^n)上的 Tang-Carlet-Tang 函数 $f(x)=(x+\delta_U(x))^{-1}$，$n$ 是一个正偶数，$n\geqslant 6$，当 $U=U_{\max}$，$U=U_{m_0}$ 或 $U=U_{m_1}$ 时，即当 $\delta_{U_{\max}}(x)=Tr_1^n(x^{-1})Tr_1^n((x+1)^{-1})$，$\delta_{U_{m_0}}(x)=(1+Tr_1^n(x))\cdot Tr_1^n(x^{-1})Tr_1^n((x+1)^{-1})$ 或 $\delta_{U_{m_1}}(x)=Tr_1^n(x)Tr_1^n(x^{-1})\cdot Tr_1^n((x+1)^{-1})$ 时，使等式 $f=\sigma\circ f\circ\rho$ 成立的可逆仿射变换对 (σ,ρ) 的数量大于或等于 n。进一步，此时与 Tang-Carlet-Tang 函数仿射等价密码函数的数量小于或等于 $\dfrac{\left[2^{\frac{n(n+1)}{2}}\prod_{i=1}^{n}(2^i-1)\right]^2}{n}$。

证明 由于 $Tr_1^n(x^{2^t})=Tr_1^n(x)$，$Tr_1^n(x^{-2^t})=Tr_1^n(x^{-1})$，$Tr_1^n((x^{2^t}+1)^{-1})=Tr_1^n((x+1)^{-2^t})=Tr_1^n((x+1)^{-1})$，当 $U=U_{\max}$、$U=U_{m_1}$ 或 $U=U_{m_0}$ 时，容易验证线性化多项式 $\rho(x)=x^{2^a}$ 和 $\sigma(x)=x^{2^{n-a}}$ (a=0,1,…, $n-1$)使 $f=\sigma\circ f\circ\rho$ 成立，因此易知，使 $f=\sigma\circ f\circ\rho$ 成立的可逆仿射变换对 (σ,ρ) 的数量大于或等于 n。由引理 2 和引理 4 可得，此时与 Tang-Carlet-Tang 函数仿射等价密码函数的数量小于或等于 $\dfrac{\left[2^{\frac{n(n+1)}{2}}\prod_{i=1}^{n}(2^i-1)\right]^2}{n}$。

5 结束语

针对 3 类差分均匀度为 4，各项安全性指标均优良的向量值密码函数，本文提出一种方法去计算与这 3 类密码函数仿射等价函数数量的上下界。利用该方法，计算出与 Zha-Hu-Sun 函数仿射等价密码函数数量的上下界，与 Qu-Tan-Tan-Li 函数和 Tang-Carlet-Tang 函数仿射等价密码函数数量的上界。因此,在实际应用中，有限域 GF(2^8)上至少有 $2^{53}\left[\prod_{i=1}^{8}(2^i-1)\right]^2$ 个与 Zha-Hu-Sun 函数仿射等价的密码函数可作为分组密码的 S 盒使用。下一步，将继续深入研究与这 3 类向量值函数仿射等价密码函数的精确数量。

参考文献：

[1] DAEMEN J, RIJMEN V. The design of rijndael: AES-the advanced encryption standard[M]. Springer-Verlag, 2002.

[2] ZHA Z B, HU L, SUN S. Constructing new differentially 4-uniform permutations from the Inverse function[J]. Finite Fields and Their Applications, 2014, 25: 64-78.

[3] BERGER T P, CANTEAUT A, CHARPIN P, et al. On almost perfect nonlinear functions over GF(2^n)[J]. IEEE Transactions on Information Theory, 2006, 52(9):4160-4170.

[4] CARLET C, GONG G, TAN Y. Quadratic zero-difference balanced functions, APN functions and strongly regular graphs[J]. Designs, Codes and Crytography, 2016, 78(3): 629-654.

[5] BROWNING K A, DILLCN J F, MCQUISTAN M T, et al. An APN permutation in dimension six[C]//The 9th Interactional Conference on Finite Fields and Their Applications (FQ9). 2010: 33-42.

[6] CARLET C. On known and new differentially uniform functions[C]// The 16th Australasian Conference on Information Security and Privacy (ACISP 2011). 2011: 1-15.

[7] QU L, TAN Y, TAN C H, et al. Constructing differentially 4-uniform permutations over GF(22^k) via the switching method[J]. IEEE Transactions on Information Theory, 2013, 59(7): 4675-4686.

[8] TANG D, CARLET C, TANG X. Differentially 4-uniform bijections by permuting the inverse function[J]. Designs, Codes and Cryptography, 2015, 77(1): 117-141.

[9] CARLET C, CHARPIN P, ZINOVIEV V. Codes, bent functions and permutations suitable for DES-like cryptosystems[J]. Designs, Codes and Cryptography, 1998, 15(2): 125-156.

[10] LIDL R, NIEDERREITER H. Finite fields[M]. Second edition, Cambridge, U.K.: Cambridge University Press, 1983.

[11] WAN Z. Geometry of classical groups over finite fields[M]. Second edition, Bejing: Science Press, 2006.

作者简介：

袁峰（1982-），男，北京人，博士，北京电子科技学院助理研究员，主要研究方向为密码学及信息安全。

江继军（1976-），男，江西南昌人，北京电子科技学院工程师，主要研究方向为信息安全。

杨旸（1984-），女，湖北随州人，博士，福州大学副教授、硕士生导师，主要研究方向为密码学及信息安全。

许盛伟（1976-），男，江西吉安人，博士，北京电子科技学院副研究员、硕士生导师，主要研究方向为网络安全。