有限域 F_{p^n} 上与逆函数仿射等价的密码函数计数问题

袁 峰[1)] 江继军[2)] 杨 旸[3)] 欧海文[1)] 王敏娟[1)]

[1)](北京电子科技学院密码科学与技术系 北京 100070)

[2)](北京电子科技学院信息安全研究所 北京 100070)

[3)](福州大学数学与计算机科学学院 福州 350108)

摘 要 分组密码的安全性主要依赖于 S 盒(向量值密码函数)的各项安全性指标.分组密码 S 盒的最优选择就是差分均匀度为 4 的向量值密码函数.逆函数是最著名的差分均匀度为 4 各项安全性指标均优良的向量值函数.著名的 AES 分组密码算法、Camellia 分组密码算法、CLEFIA 分组密码算法和 SMS4 分组密码算法均采用有限域 F_{2^8} 上与逆函数仿射等价的向量值函数作为 S 盒.目前对于与逆函数仿射等价 S 盒的研究,主要侧重于研究分组密码算法经过多轮后活跃 S 盒的数量.与以往的研究角度有所不同,该文要研究有限域 F_{p^n} 上与逆函数仿射等价向量值密码函数的计数问题.若能计算出与逆函数仿射等价密码函数的数量,在实际应用中就知道有多少个与逆函数仿射等价的 S 盒可供算法设计者选择.将有限域 F_{2^n} 上的逆函数推广成有限域 F_{p^n} 上的逆函数,其中 $p\geq 2$ 是一个素数,这是一个更为一般的逆函数.首先,该文定义 (T_1,R_1) 和 (T_2,R_2) 之间的运算"$*$"为 $(T_2,R_2)*(T_1,R_1):=(T_2\circ T_1,R_1\circ R_2)$,其中 $(T_1,R_1),(T_2,R_2)\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$,$Aff_n^{-1}(F_q)$ 是有限域 F_q 上的 $n\times n$ 阶可逆仿射变换群,$q=p^m$,$p\geq 2$ 是一个素数,$m\geq 1$ 是一个正整数,"$\circ$"表示映射的合成.证明了 $Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$ 关于运算"$*$"是一个群;使得等式 $F=V\circ F\circ W$ 成立的可逆仿射变换对 $(V,W)\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$ 关于运算"$*$"是 $Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$ 的一个子群.然后,利用以上结论和有限域的一些性质证明了,当 $p\geq 3$ 且 $n\geq 2$ 时,或者 $p=2$ 且 $n\geq 4$ 时,对于有限域 F_{p^n} 上的逆函数 $F(x)=x^{-1}=x^{p^n-2}$,使得等式 $F=\nu\circ F\circ\mu$ 成立的可逆仿射变换 μ 和 ν 线性化多项式的形式只能是 $\mu(x)=S_t x^{p^t}$ 和 $\nu(x)=S_t^{p^{n-t}}x^{p^{n-t}}$,$0\neq S_t\in F_{p^n}$,$t=0,1,\cdots,n-1$.于是,使得等式 $F=\nu\circ F\circ\mu$ 成立的所有可逆仿射变换对 (ν,μ) 的数量为 $n(p^n-1)$.利用这些可逆仿射变换对 (ν,μ) 所形成的子群对群 $Aff_n^{-1}(F_p)\times Aff_n^{-1}(F_p)$ 划分等价类,商集中陪集首的个数即为与逆函数仿射等价密码函数的数量.因此,在这种情况下,与逆函数仿射等价密码函数的数量为 $\dfrac{\left[p^{n(n+1)/2}\prod\limits_{i=1}^{n}(p^i-1)\right]^2}{n(p^n-1)}$.最后,当 $p=2$ 且 $n=3$ 时,对于有限域 F_{2^3} 上的逆函数 $F(x)=x^{-1}=x^{2^3-2}$,利用计算机作为辅助手段测试出使得等式 $F=\nu\circ F\circ\mu$ 成立的可逆仿射变换对 (ν,μ) 的数量为 168.利用这些可逆仿射变换对 (ν,μ) 所形成的子群对群 $Aff_3^{-1}(F_2)\times Aff_3^{-1}(F_2)$ 划分等价类,商集中陪集首的个数即为与逆函数仿射等价密码函数的数量.因此,在这种情况下,与逆函数仿射等价密码函数的数量为 10752.研究结果表明,在实际应用中,有限域 F_{2^8} 上有 $2^{69}\times 255\times\left[\prod\limits_{i=1}^{7}(2^i-1)\right]^2$ 个与逆函数仿射等价的密码函数可作为分组密码的 S 盒使用.

关键词 密码学;密码函数;S 盒;逆函数;等价;数量

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2019.01126

收稿日期:2017-02-26;在线出版日期:2018-01-22.本课题得到国家重点研发计划资助项目(2018YFB0803600)、国家自然科学基金青年科学基金(61402112)、中央高校基本科研业务费专项资金(2014XSYJ09,328201509)、北京电子科技学院科研团队项目(2014TD2-OHW)资助.**袁 峰**,博士,助理研究员,主要研究方向为密码学与信息安全.E-mail:fyuan1234@aliyun.com.**江继军**,硕士,工程师,主要研究方向为信息安全与网络安全.**杨 旸**,博士,副教授,主要研究方向为密码学与信息安全.**欧海文**,博士,教授,主要研究方向为密码学与信息安全.**王敏娟**,硕士,副教授,主要研究方向为微分几何与密码学.

Enumeration of Cryptographic Functions Affine Equivalent to the Inverse Function Over F_{p^n}

YUAN Feng[1)]　JIANG Ji-Jun[2)]　YANG Yang[3)]　OU Hai-Wen[1)]　WANG Min-Juan[1)]

[1)] (*Department of Cryptography Science and Technology, Beijing Electronic Science and Technology Institute, Beijing* 100070)

[2)] (*Information Security Institute, Beijing Electronic Science and Technology Institute, Beijing* 100070)

[3)] (*College of Mathematics and Computer Science, Fuzhou University, Fuzhou* 350108)

Abstract　The security of modern block ciphers substantially relies on the cryptographic properties of its S-boxes (vectorial cryptographic functions), which are always the only source of nonlinearity. It is optimal to choose differentially 4-uniform permutations as S-boxes of block ciphers in real applications. The inverse function is the most famous differentially 4-uniform permutation with many desirable cryptographic properties. The vectorial functions of affine equivalent to the inverse function over F_{2^8} are frequently selected as the S-boxes of many important block ciphers, such as AES, Camellia, CLEFIA and SMS4. Now the research on the S-boxes of affine equivalent to the inverse function focuses the counting method of the minimum number of active S-boxes for several consecutive rounds of block ciphers. Unlike the previous research works, this paper investigates the counting problem of affine equivalent to the inverse function over F_{p^n}. If the exact number of affine equivalent to the inverse function is calculated, the designer of cryptographic algorithm knows that how many the S-boxes of affine equivalent to the inverse function should be selected in real applications. The inverse function over finite field F_{2^n} is generalized to the inverse function over finite field F_{p^n}, where $p\geq 2$ is a prime number. This is a generalization of the inverse function. Firstly, the product "$*$" of (T_1,R_1) and (T_2,R_2) is defined as $(T_2,R_2)*(T_1,R_1):=(T_2\circ T_1,R_1\circ R_2)$, where $(T_1,R_1),(T_2,R_2)\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$, $Aff_n^{-1}(F_q)$ is the $n\times n$ invertible affine transformation group over finite field F_q, $q=p^m$, $p\geq 2$ is a prime number, $m\geq 1$ is a positive integer, and "$\circ$" denotes the product of the mapping. This paper proves that $Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$ is a group and the pairs of invertible affine transformations $(V,W)\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$ satisfied by $F=V\circ F\circ W$ form a subgroup of the group $Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$ with respect to the operation "$*$". Secondly, when $p\geq 3$ and $n\geq 2$, or $p=2$ and $n\geq 4$, for the inverse function $F(x)=x^{-1}=x^{p^n-2}\in F_{p^n}[x]$, we utilize the above results and some properties of finite fields to prove that there exists the pairs of invertible affine transformations $(\nu,\mu)\in Aff_n^{-1}(F_p)\times Aff_n^{-1}(F_p)$ such that $F=\nu\circ F\circ\mu$, where the linearized polynomials of invertible affine transformations μ and ν must be $\mu(x)=S_t x^{p^t}$ and $\nu(x)=S_t^{p^{n-t}}x^{p^{n-t}}$, $0\neq S_t\in F_{p^n}$, $t=0,1,\cdots,n-1$. Then the pairs number of invertible affine transformations (ν,μ) is $n(p^n-1)$. The group $Aff_n^{-1}(F_p)\times Aff_n^{-1}(F_p)$ can be partitioned into equivalence classes by using the pairs of invertible affine transformations (ν,μ) form the subgroup. The number of coset representatives of the group $Aff_n^{-1}(F_p)\times Aff_n^{-1}(F_p)$ relative to the subgroup is equal to the number of affine equivalent to the inverse function. In this case, the number of affine equivalent to the inverse function is $\dfrac{\left[p^{n(n+1)/2}\prod\limits_{i=1}^{n}(p^i-1)\right]^2}{n(p^n-1)}$. Thirdly, when $p=2$ and $n=3$, for the inverse function $F(x)=x^{-1}=x^{2^3-2}\in F_{2^3}[x]$, the pairs number of invertible affine transformations $(\nu,\mu)\in$

$Aff_3^{-1}(F_2)\times Aff_3^{-1}(F_2)$ satisfied by $F=\nu\circ F\circ\mu$ is 168, which is calculated by the computer. The group $Aff_3^{-1}(F_2)\times Aff_3^{-1}(F_2)$ can be partitioned into equivalence classes using the subgroup that is formed by the pairs of invertible affine transformations (ν,μ). The number of coset representatives of the group $Aff_3^{-1}(F_2)\times Aff_3^{-1}(F_2)$ relative to the subgroup is equal to the number of affine equivalent to the inverse function. In this case, the number of affine equivalent to the inverse function is 10 752. Our results show that there exists $2^{69}\times 255\times\left[\prod_{i=1}^{7}(2^i-1)\right]^2$ cryptographic functions of affine equivalent to the inverse function over finite field F_{2^8} to be used in the S-boxes of block ciphers in real applications.

Keywords cryptography; cryptographic functions; S-box; inverse function; equivalence; number

1 引 言

S 盒是大多数分组密码算法唯一的非线性部件,分组密码的安全性主要依赖于 S 盒的各项安全性指标[1]. 寻找适合分组密码,可以抵抗差分攻击、线性攻击和代数攻击的 S 盒一直都是过去二十年中密码函数研究的重点和热点[2-3].

对于有限域 F_{p^n} 上的两个向量值函数 $F(x)$ 和 $F'(x)$,若存在两个可逆仿射变换 $L_1:F_{p^n}\to F_{p^n}$ 和 $L_2:F_{p^n}\to F_{p^n}$,以及一个仿射变换 $L_3:F_{p^n}\to F_{p^n}$,使得 $F'=L_2\circ F\circ L_1+L_3$,就称 $F(x)$ 和 $F'(x)$ 是 EA 等价[4]. 当 $L_3=0$ 时,则称函数 $F(x)$ 和 $F'(x)$ 是仿射等价.

一个向量值密码函数 $F:F_{p^n}\to F_{p^n}$ 是几乎完全非线性函数,即 APN 函数[5],当且仅当对于所有 $a\in F_{p^n}^*$ 和 $b\in F_{p^n}$,方程 $F(x)+F(x+a)=b$ 至多有两个解. 特征为 2 有限域 F_{2^n} 上的 APN 函数是抵抗差分攻击能力最强的密码函数[6]. 到目前为止,除了 Dillon 等人在有限域 F_{2^6} 上发现的仅有的一个 APN 置换[7]外,当 $n\geq 4$ 且 n 为偶数时,仍然不知道有限域 $F_{2^{2n}}$ 上是否存在着 APN 置换. 最近,Perrin 等人[8]提出了一类最高差分均匀度为 4 的置换函数,他们将这类置换函数命名为蝴蝶结构,这类置换有 $2n$ 个变量,$n\geq 3$ 是一个奇数,当 $n=3$ 时,Dillon 等人所发现的 APN 置换就包含在这类置换中. 随后,Canteaut 等人[9]推广了 Perrin 等人提出的蝴蝶结构,他们构造出一类差分均匀度为 4 的置换函数,在该类置换中只有一个 6 变元的置换 CCZ 等价于 Dillon 等人所发现的 APN 置换. 因此,有限域 $F_{2^{2n}}$ 上 APN 置换的存在性仍然是一个公开问题. 在实际应用中,分组密码 S 盒的最优选择就是差分均匀度为 4 的置换函数. 逆函数是最著名的差分均匀度为 4 的密码函数,它的各项安全性指标优良[10-11]. 著名的 AES 分组密码算法[12]、Camellia 分组密码算法[13]、CLEFIA 分组密码算法[14]和 SMS4 分组密码算法[15]均采用有限域 F_{2^8} 上与逆函数仿射等价的置换多项式作为 S 盒.

目前对于 S 盒的研究,主要侧重于设计、优化、对合性以及其逆与它自身有特殊的关系等[16-18]. 对于与逆函数仿射等价 S 盒的研究,主要侧重于研究分组密码算法经过多轮后活跃 S 盒的数量[19]. 与以往的研究角度有所不同,本文主要研究与逆函数仿射等价向量值密码函数的数量. 由于逆函数应用广泛,若能计算出与逆函数仿射等价密码函数的数量,在实际应用中就知道有多少个与逆函数仿射等价的 S 盒可供算法设计者选择. 将有限域 F_{2^n} 上的逆函数推广成有限域 F_{p^n} 上的逆函数,其中 $p\geq 2$ 是一个素数,这是一个更为一般的逆函数. 当 $p\geq 3$ 且 $n\geq 2$ 时,或者 $p=2$ 且 $n\geq 4$ 时,对于有限域 F_{p^n} 上的逆函数 $F(x)=x^{-1}=x^{p^n-2}$,通过使用有限域的一些性质计算出与逆函数仿射等价密码函数的数量. 该计算方法的基本思想是:发现所有使得等式 $F=\nu\circ F\circ\mu$ 成立的可逆仿射变换对 $(\nu,\mu)\in Aff_n^{-1}(F_p)\times Aff_n^{-1}(F_p)$ 的数量,其中 $Aff_n^{-1}(F_p)$ 是有限域 F_p 上的 $n\times n$ 阶可逆仿射变换群,然后利用可逆仿射变换对 (ν,μ) 所形成的子群对群 $Aff_n^{-1}(F_p)\times Aff_n^{-1}(F_p)$ 划分等价类,商集中陪集首的个数即为与逆函数仿射等价密码函数的数量. 此外,当 $p=2$ 且 $n=3$ 时,对于有限域 F_{2^3} 上的逆函数 $F(x)=x^{-1}=x^{2^3-2}$,利用计算机作为辅助手段测试出与逆函数仿射等价密码函数的数量.

本文第 2 节介绍并提出一些后面将会用到的预备知识；第 3 节详细描述如何计算与逆函数仿射等价密码函数的数量；第 4 节介绍第 3 节研究成果的应用价值；第 5 节是本文的结论.

2　预备知识

第 2 节介绍并提出一些结果，这些结果在后面将会用到.

设 k 是 q 阶元素的有限域，其中 $q=p^m$，$p\geq 2$ 是一个素数，$m\geq 1$ 是一个正整数，即 $k=F_q$. 若 $g(x)$是域 k 上的 n 次不可约多项式，则 $K=k[x]/(g(x))$是域 k 的 n 次扩域，即 $K=F_{q^n}$. 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 $\phi(b_0+b_1x+\cdots+b_{n-1}x^{n-1})=(b_0,b_1,\cdots,b_{n-1})$.

引理 1[20]. 若映射 $E:K\to K$ 的形式如下所示：$E(X)=\sum_{i=0}^{n-1}C_iX^{q^i}+D$，其中 $C_i,D\in K$，将 $E(X)$ 称为线性化多项式. 令 $\overline{E}=\phi\circ E\circ\phi^{-1}$，则多项式映射 $\overline{E}:k^n\to k^n$ 为：$\overline{E}(x_1,x_2,\cdots,x_n)=(\overline{E}_1,\overline{E}_2,\cdots,\overline{E}_n)$，其中 $\overline{E}_i=\overline{E}_i(x_1,x_2,\cdots,x_n)$是多项式环 $k[x_1,x_2,\cdots,x_n]$中代数次数至多为 1 的多项式，$i=1,2,\cdots,n$. 并且，设域 K 上映射 $E:K\to K$ 的集合为 B_E，k^n上多项式映射 $\overline{E}:k^n\to k^n$的集合为 $B_{\overline{E}}$，则映射 $\psi:B_E\to B_{\overline{E}}$是一个双射.

引理 1 揭示了 k^n上的线性仿射与域 K 上的线性化多项式之间是一一对应的.

引理 2[21].

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

其中 $GL_n(F_q)$为有限域 F_q上的可逆矩阵群(一般线性群).

引理 2 揭示了有限域 F_q上 $n\times n$ 阶可逆矩阵的数量.

定义三个映射 $R:k^n\to k^n$，$T:k^n\to k^n$和 $F:K\to K$ 的合成映射为 $T\circ\phi\circ F\circ\phi^{-1}\circ R:=T\circ F\circ R$，其中，$(T,R)\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$，$Aff_n^{-1}(F_q)$是有限域 F_q上的 $n\times n$ 阶可逆仿射变换群，$F:K\to K$ 是一个向量值函数. 定义(T_1,R_1)和(T_2,R_2)之间的运算“$*$”为$(T_2,R_2)*(T_1,R_1):=(T_2\circ T_1,R_1\circ R_2)$，其中$(T_1,R_1),(T_2,R_2)\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$，“$\circ$”表示映射的合成. 则有下述结论.

引理 3. $Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$对于运算“$*$”是一个群.

证明. (1) 关于封闭性. 对于任意(T_1,R_1)，$(T_2,R_2)\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$，则有

$$(T_2,R_2)*(T_1,R_1)=(T_2\circ T_1,R_1\circ R_2)\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q);$$

(2) 关于结合律. 对于任意(T_1,R_1)，(T_2,R_2)和$(T_3,R_3)\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$，则有

$$(T_3,R_3)*((T_2,R_2)*(T_1,R_1))=(T_3,R_3)*(T_2\circ T_1,R_1\circ R_2)=(T_3\circ T_2\circ T_1,R_1\circ R_2\circ R_3),$$

$$((T_3,R_3)*(T_2,R_2))*(T_1,R_1)=(T_3\circ T_2,R_2\circ R_3)*(T_1,R_1)=(T_3\circ T_2\circ T_1,R_1\circ R_2\circ R_3).$$

于是就有

$$(T_3,R_3)*((T_2,R_2)*(T_1,R_1))=((T_3,R_3)*(T_2,R_2))*(T_1,R_1);$$

(3) 关于单位元. 对于任意$(T_1,R_1)\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$，都有一个单位元$(\boldsymbol{I},\boldsymbol{I})$，其中 $\boldsymbol{I}$ 是一个单位矩阵，使得$(\boldsymbol{I},\boldsymbol{I})*(T_1,R_1)=(T_1,R_1)*(\boldsymbol{I},\boldsymbol{I})=(T_1,R_1)$；

(4) 关于逆元. 对于任意$(T_1,R_1)\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$，都存在一个逆元$(T_1^{-1},R_1^{-1})\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$，使得$(T_1^{-1},R_1^{-1})*(T_1,R_1)=(T_1,R_1)*(T_1^{-1},R_1^{-1})=(\boldsymbol{I},\boldsymbol{I})$. 证毕.

设$(V,W)\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$是使得等式 $F=V\circ F\circ W$ 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第 3 节中将会多次使用.

引理 4. 使得等式 $F=V\circ F\circ W$ 成立的可逆仿射变换对$(V,W)\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$对于运算“$*$”是 $Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$的一个子群.

证明. (1) 关于封闭性. 对于使得等式 $F=V\circ F\circ W$ 成立的任意(V_1,W_1)，$(V_2,W_2)\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$，即 $F=V_1\circ F\circ W_1$，$F=V_2\circ F\circ W_2$，都有

$$(V_2,W_2)*(V_1,W_1)=(V_2\circ V_1,W_1\circ W_2)\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q);$$

并且，可逆仿射变换对$(V_2\circ V_1,W_1\circ W_2)$使得等式

$$(V_2\circ V_1)\circ F\circ(W_1\circ W_2)=V_2\circ(V_1\circ F\circ W_1)\circ W_2=V_2\circ F\circ W_2=F$$

成立. 即$(V_2,W_2)*(V_1,W_1)$使得等式 $F=V\circ F\circ W$ 成立；

(2) 关于逆元. 对于使得等式 $F=V\circ F\circ W$ 成立的任意$(V_1,W_1)\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$，即 $F=V_1\circ F\circ W_1$，都有 $F=V_1^{-1}\circ F\circ W_1^{-1}$，即存在一个

逆元$(V_1^{-1},W_1^{-1})\in Aff_n^{-1}(F_q)\times Aff_n^{-1}(F_q)$使得等式$F=V\circ F\circ W$成立. 证毕.

下面给出4个性质,这4个性质很容易证明,将在第3节定理1的证明中使用.

性质1. 设F_{q^n}是具有q^n个元素的有限域,则有下列基本事实:

(1)对于任意$0\neq x\in F_{q^n}$,都有$x^{q^n-1}=1$;

(2)对于任意$\alpha^b\neq x\in F_{q^n}$,这里$\alpha$是有限域$F_{q^n}$的一个本原元,$0\leq b\leq q^n-2$,都有$x^{q^n-1}+\alpha^b x^{q^n-2}+\alpha^{2b}x^{q^n-3}+\cdots+\alpha^{(q^n-2)b}x=0$.

特别地,当$q=2$时,则有

(1)对于任意$0\neq x\in F_{2^n}$,都有$x^{2^n-1}=1$;

(2)对于任意$\alpha^b\neq x\in F_{2^n}$,这里$\alpha$是有限域$F_{2^n}$的一个本原元,$0\leq b\leq 2^n-2$,都有$x^{2^n-1}+\alpha^b x^{2^n-2}+\alpha^{2b}x^{2^n-3}+\cdots+\alpha^{(2^n-2)b}x=0$.

证明. (1)对于任意$x\in F_{q^n}$,都有$x^{q^n}=x$,进而对于任意$0\neq x\in F_{q^n}$,都有$x^{q^n-1}=1$.

(2)对于任意$x\in F_{q^n}$,都有

$$x^{q^n}-x=(x-\alpha^b)(x^{q^n-1}+\alpha^b x^{q^n-2}+\alpha^{2b}x^{q^n-3}+\cdots+\alpha^{(q^n-2)b}x)=0,$$

其中α是有限域F_{q^n}的一个本原元,$0\leq b\leq q^n-2$,进而对于任意$\alpha^b\neq x\in F_{q^n}$,都有

$$x^{q^n-1}+\alpha^b x^{q^n-2}+\alpha^{2b}x^{q^n-3}+\cdots+\alpha^{(q^n-2)b}x=0.$$ 证毕.

性质2. 设r和n都是大于或等于2的正整数,则n^2-n个正整数$r^i-r^j(i>j,\ i,j=0,1,\cdots,n-1)$和$r^i-r^j+r^n-1(i<j,\ i,j=0,1,\cdots,n-1)$全都不相同.

证明. 以下分3种情形进行讨论.

第1种情形:若存在a,b,c和d,这里$a>b$,$c>d$,$0\leq a,b,c,d\leq n-1$,使得$r^a-r^b=r^c-r^d$,由同余关系知,有$r^a-r^b-r^c+r^d\equiv 0 \bmod r^n-1$,该同余式成立当且仅当$a=c$且$b=d$.因此,当$i>j$时,这$\frac{n^2-n}{2}$个正整数$r^i-r^j$均不相等.

第2种情形:若存在a,b,c和d,这里$a<b$,$c<d$,$0\leq a,b,c,d\leq n-1$,使得$r^a-r^b+r^n-1=r^c-r^d+r^n-1$,则有$r^b-r^a=r^d-r^c$,与第1种情形完全相同.因此,当$i<j$时,这$\frac{n^2-n}{2}$个正整数$r^i-r^j+r^n-1$均不相等.

第3种情形:若存在a,b,c和d,这里$a>b$,$c<d$,$0\leq a,b,c,d\leq n-1$,使得$r^a-r^b=r^c-r^d+r^n-1$,根据同余关系,就有$r^a-r^b+r^d-r^c\equiv 0 \bmod r^n-1$,该同余式显然不成立.因此,$\frac{n^2-n}{2}$个正整数$r^i-r^j(i>j,\ i,j=0,1,\cdots,n-1)$中的任意一个整数均不等于$\frac{n^2-n}{2}$个正整数$r^i-r^j+r^n-1(i<j,\ i,j=0,1,\cdots,n-1)$中的任意一个整数.

综上所述,这n^2-n个正整数$r^i-r^j(i>j,\ i,j=0,1,\cdots,n-1)$和$r^i-r^j+r^n-1(i<j,\ i,j=0,1,\cdots,n-1)$全都不相同. 证毕.

性质3. 设r和n都是正整数,当$r\geq 3$且$n\geq 2$时,或者$r=2$且$n\geq 3$时,则$2n$个正整数$r^i(i=0,1,\cdots,n-1)$和$r^n-1-r^i(i=0,1,\cdots,n-1)$全都不相同.

证明. 若存在a和b,$0\leq a,b\leq n-1$,使得$r^n-1-r^b=r^a$.由同余关系可知,就有$r^a+r^b\equiv 0 \bmod r^n-1$,该同余式显然不成立. 证毕.

性质4. 对于n^2+n个正整数$r^i-r^j(i>j)$,$r^i-r^j+r^n-1(i<j)$,r^i和r^n-1-r^i,其中$i,j=0,1,\cdots,n-1$且$i\neq j$,则有以下事实.

(1)当$r\geq 3$且$n\geq 2$时,则n^2+n个正整数$r^i-r^j(i>j,\ i,j=0,1,\cdots,n-1)$,$r^i-r^j+r^n-1(i<j,\ i,j=0,1,\cdots,n-1)$,$r^i(i=0,1,\cdots,n-1)$和$r^n-1-r^i(i=0,1,\cdots,n-1)$全都不相等;

(2)当$r=2$且$n\geq 3$时,等式$2^i-2^j\equiv 2^t \bmod 2^n-1$成立当且仅当$i=j+1 \bmod n$且$t=j$;等式$2^i-2^j\equiv -2^t \bmod 2^n-1$成立当且仅当$j=i+1 \bmod n$且$t=i$.

证明. (1)当$r\geq 3$且$n\geq 2$时,以下分4种情形进行讨论:

第1种情形:若存在a,b和c,这里$a>b$,$0\leq a,b,c\leq n-1$,使得$r^a-r^b=r^c$,由同余关系可知,有$r^a-r^b-r^c\equiv 0 \bmod r^n-1$,该同余式显然不成立.

第2种情形:若存在a,b和c,这里$a>b$,$0\leq a,b,c\leq n-1$,使得$r^a-r^b=r^n-1-r^c$,由同余关系可知,有$r^a-r^b+r^c\equiv 0 \bmod r^n-1$,该同余式显然不成立.

第3种情形:若存在a,b和c,这里$a<b$,$0\leq a,b,c\leq n-1$,使得$r^a-r^b+r^n-1=r^c$,根据同余关系,就有$r^b-r^a+r^c\equiv 0 \bmod r^n-1$,该同余式显然不成立.

第4种情形:若存在a,b和c,这里$a<b$,$0\leq a,b,c\leq n-1$,使得$r^a-r^b+r^n-1=r^n-1-r^c$,根据同

余关系，就有 $r^b-r^a-r^c\equiv 0 \bmod r^n-1$，该同余式显然也不成立.

综上所述，这 n^2+n 个正整数 r^i-r^j $(i>j, i,j=0,1,\cdots,n-1)$，$r^i-r^j+r^n-1$ $(i<j,\ i,j=0,1,\cdots,n-1)$，$r^i$ $(i=0,1,\cdots,n-1)$ 和 r^n-1-r^i $(i=0,1,\cdots,n-1)$ 全都不相等.

(2) 当 $r=2$ 且 $n\geq 3$ 时，以下分 6 种情况进行详细分析：

第 1 种情形：若存在 a 和 b，其中 $a\geq b+2$，$0\leq a,b,c\leq n-1$，使得 $2^a-2^b=2^c$，但由于

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

这明显是一个矛盾.

第 2 种情形：若存在 a 和 b，其中 $a\geq b+2$，$0\leq a,b,c\leq n-1$，使得 $2^a-2^b=2^n-1-2^c$，即 $2^{a-1}+2^{a-2}+\cdots+2^b+2^c=2^n-1$. 再细分成两种情况进行讨论：

① 若 $a\neq n-1$ 或者 $b\neq 0$，由于 $2^{a-1}+2^{a-2}+\cdots+2^b+2^c<2^{n-1}+2^{n-2}+\cdots+1=2^n-1$，这显然是一个矛盾.

② 若 $a=n-1$ 且 $b=0$，则有 $2^{n-1}-2^0=2^n-1-2^{n-1}$ (此时 $c=n-1$).

第 3 种情形：若 $a=b+1$，$0\leq a,b\leq n-1$，容易发现，$2^a-2^b=2^{b+1}-2^b=2^b$.

第 4 种情形：若存在 a 和 b，其中 $b\geq a+2$，$0\leq a,b,c\leq n-1$，使得 $2^a-2^b+2^n-1=2^n-1-2^c$，即 $2^b-2^a=2^c$，但由于

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

这明显是一个矛盾.

第 5 种情形：若存在 a 和 b，其中 $b\geq a+2$，$0\leq a,b,c\leq n-1$，使得 $2^a-2^b+2^n-1=2^c$. 再细分成两种情况进行讨论：

① 若 $a\neq 0$ 或者 $b\neq n-1$，不难发现，

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

这显然是一个矛盾.

② 若 $a=0$ 且 $b=n-1$，则有 $2^0-2^{n-1}+2^n-1=2^{n-1}$ (此时 $c=n-1$).

第 6 种情形：若 $b=a+1$，$0\leq a,b\leq n-1$，容易发现，$2^a-2^{a+1}+2^n-1=2^n-1-2^a$.

综上所述，同余式 $2^i-2^j\equiv 2^t \bmod 2^n-1$ 成立当且仅当 $i=j+1 \bmod n$ 且 $t=j$；同余式 $2^i-2^j\equiv -2^t \bmod 2^n-1$ 成立当且仅当 $j=i+1 \bmod n$ 且 $t=i$. 证毕.

3　与逆函数仿射等价的密码函数数量

在第 3 节中，我们将详细讨论如何计算与逆函数仿射等价密码函数的数量. 有了第 2 节的准备工作后，下面将证明本文的主要结果.

定理 1.　对于有限域 F_{p^n} 上的逆函数 $F(x)=x^{-1}=x^{p^n-2}$，p 是一个素数. 当 $p\geq 3$ 且 $n\geq 2$ 时，或者 $p=2$ 且 $n\geq 4$ 时，使得等式 $F=\nu\circ F\circ\mu$ 成立的可逆仿射变换对 (ν,μ) 的数量为 $n(p^n-1)$，其中可逆仿射变换 μ 和 ν 线性化多项式的形式只能是 $\mu(x)=S_t x^{p^t}$ 和 $\nu(x)=S_t^{p^{n-t}}x^{p^{n-t}}$，$0\neq S_t\in F_{p^n}$，$t=0,1,\cdots,n-1$. 进一步，与逆函数仿射等价密码函数的数量为 $\dfrac{\left[p^{n(n+1)/2}\prod\limits_{i=1}^{n}(p^i-1)\right]^2}{n(p^n-1)}$.

证明.　由 $F=\nu\circ F\circ\mu$ 可知，$\nu^{-1}\circ F=F\circ\mu$. 根据引理 1 可设：$\mu(x)=\sum\limits_{i=0}^{n-1}S_i x^{p^i}+H$ 和 $\nu^{-1}(x)=\sum\limits_{i=0}^{n-1}U_i x^{p^i}+Q$，其中 $S_i,H,U_i,Q\in F_{p^n}$. 再根据等式 $\nu^{-1}\circ F=F\circ\mu$，有

$$\sum_{i=0}^{n-1}U_i x^{(p^n-2)p^i}+Q=\left(\sum_{i=0}^{n-1}S_i x^{p^i}+H\right)^{-1}=$$
$$\left(\sum_{i=0}^{n-1}S_i x^{p^i}+H\right)^{p^n-2}.$$

由以上等式不难发现，$Q=H^{p^n-2}$. 若 $H\neq 0$，则有 $Q\neq 0$；若 $H=0$，则有 $Q=0$.

当 $\mu(x)=\sum\limits_{i=0}^{n-1}S_i x^{p^i}+H=0$ 时，由于 μ 是一个可逆仿射变换，因此等式 $\mu(x)=0$ 有且只有一个解，不妨设这个解为 β，即 $\mu(\beta)=0$. 由于 β 是有限域 F_{p^n} 中的一个元素，β 可以是 0 或者是 α^b，这里 α 是有限域 F_{p^n} 的一个本原元，$0\leq b\leq p^n-2$.

对于任意 $\tau\in F_{p^n}$ 且 $\tau\neq\beta$，都有 $\mu(\tau)\neq 0$，进而

$$\left(\sum_{i=0}^{n-1}S_i\tau^{p^i}+H\right)\left(\sum_{i=0}^{n-1}U_i\tau^{(p^n-2)p^i}+Q\right)=1,$$

展开该等式左边的每一项，就有

$$S_0U_0\tau^{p^n-1}+S_0U_1\tau^{p^n-p}+S_0U_2\tau^{p^n-p^2}+\cdots+$$
$$S_0U_{n-1}\tau^{p^n-p^{n-1}}+S_0Q\tau^{p^0}+$$
$$S_1U_0\tau^{p-1}+S_1U_1\tau^{p^n-1}+S_1U_2\tau^{p^n-p^2+p-1}+\cdots+$$
$$S_1U_{n-1}\tau^{p^n-p^{n-1}+p-1}+S_1Q\tau^{p}+$$
$$S_2U_0\tau^{p^2-1}+S_2U_1\tau^{p^2-p}+S_2U_2\tau^{p^n-1}+\cdots+$$
$$S_2U_{n-1}\tau^{p^n-p^{n-1}+p^2-1}+S_2Q\tau^{p^2}+$$
$$\cdots+$$
$$S_{n-2}U_0\tau^{p^{n-2}-1}+S_{n-2}U_1\tau^{p^{n-2}-p}+S_{n-2}U_2\tau^{p^{n-2}-p^2}+\cdots+$$
$$S_{n-2}U_{n-1}\tau^{p^n+p^{n-2}-p^{n-1}-1}+S_{n-2}Q\tau^{p^{n-2}}+$$
$$S_{n-1}U_0\tau^{p^{n-1}-1}+S_{n-1}U_1\tau^{p^{n-1}-p}+S_{n-1}U_2\tau^{p^{n-1}-p^2}+\cdots+$$
$$S_{n-1}U_{n-1}\tau^{p^{n-1}}+S_{n-1}Q\tau^{p^{n-1}}+$$
$$U_0H\tau^{p^n-2}+U_1H\tau^{p^n-p-1}+U_2H\tau^{p^n-p^2-1}+\cdots+$$
$$U_{n-1}H\tau^{p^n-p^{n-1}-1}+HQ=1 \tag{1}$$

其中，单项式 $S_iU_j\tau^{p^i+(p^n-2)p^j}$ $(i,j=0,1,\cdots,n-1)$ 的代数次数 $p^i+(p^n-2)p^j\equiv p^i-p^j \bmod p^n-1$ 如下所示：当 $i>j$ 时，代数次数为 p^i-p^j；当 $i\leq j$ 时，代数次数为 $p^i-p^j+p^n-1$；当 $i=j$ 时，代数次数为 p^n-1.

根据性质 2 可知，当 $p\geq 2$ 且 $n\geq 2$ 时，等式(1)中单项式 $S_iU_j\tau^{p^i+(p^n-2)p^j}$ $(i\neq j,\ i,j=0,1,\cdots,n-1)$ 的代数次数均不相同，并且都小于 p^n-1. 此外，等式(1)中单项式 $S_iQ\tau^{p^i}$ $(i=0,1,\cdots,n-1)$ 的代数次数 $p^i \bmod p^n-1$ 为 p^i，单项式 $U_iH\tau^{(p^n-2)p^i}$ $(i=0,1,\cdots,n-1)$ 的代数次数 $(p^n-2)p^i\equiv -p^i \bmod p^n-1$ 为 p^n-1-p^i. 根据性质 3 可知，当 $p\geq 3$ 且 $n\geq 2$ 时，或者 $p=2$ 且 $n\geq 3$ 时，单项式 $S_iQ\tau^{p^i}$ $(i=0,1,\cdots,n-1)$ 和 $U_iH\tau^{(p^n-2)p^i}$ $(i=0,1,\cdots,n-1)$ 的代数次数全都不相同. 因此，由性质 4 可知，当 $p\geq 3$ 且 $n\geq 2$ 时，等式(1)的项数至多只能是 n^2+n+2；当 $p=2$ 且 $n\geq 3$ 时，等式(1)的项数至多只能是 n^2-n+2. 以下分两种情况进行详细讨论：

1) 当 $p\geq 3$ 且 $n\geq 2$ 时，若 $\mu(x)=0$ 的解为 $\beta=0$，由性质 1 可知，p^n-1 个元素 $0\neq\tau\in F_{p^n}$ 是等式 $x^{p^n-1}-1=0$ 全部的解，该等式的项数为 2；若 $\mu(x)=0$ 的解为 $\beta=\alpha^b$，$0\leq b\leq p^n-2$，根据性质 1 可知，p^n-1 个元素 $\tau\in F_{p^n}$ 且 $\tau\neq\alpha^b$ 是等式 $x^{p^n-1}+\alpha^bx^{p^n-2}+\alpha^{2b}x^{p^n-3}+\cdots+\alpha^{(p^n-2)b}x=0$ 全部的解，该等式的项数为 p^n-1. 然而，不管 β 等于 0 还是等于 α^b，p^n-1 个元素 $\tau\in F_{p^n}$ 且 $\tau\neq\beta$ 就是等式(1)全部的解，并且等式(1)的项数至多只能是 n^2+n+2. 当 $p\geq 3$ 且 $n\geq 2$ 时，容易知道等式 $x^{p^n-1}+\alpha^bx^{p^n-2}+\alpha^{2b}x^{p^n-3}+\cdots+\alpha^{(p^n-2)b}x=0$ 的项数 $p^n-1>n^2+n+1$，因此 β 只能等于 0. 于是等式(1)的形式只能是 $x^{p^n-1}-1=0$；

2) 当 $p=2$ 且 $n\geq 4$ 时，若 $\mu(x)=0$ 的解为 $\beta=0$，由性质 1 可知，2^n-1 个元素 $0\neq\tau\in F_{2^n}$ 是等式 $x^{2^n-1}-1=0$ 全部的解，该等式的项数为 2；若 $\mu(x)=0$ 的解为 $\beta=\alpha^b$，$0\leq b\leq 2^n-2$，根据性质 1 可知，2^n-1 个元素 $\tau\in F_{2^n}$ 且 $\tau\neq\alpha^b$ 是等式 $x^{2^n-1}+\alpha^bx^{2^n-2}+\alpha^{2b}x^{2^n-3}+\cdots+\alpha^{(2^n-2)b}x=0$ 全部的解，该等式的项数为 2^n-1. 然而，不管 β 等于 0 还是等于 α^b，2^n-1 个元素 $\tau\in F_{2^n}$ 且 $\tau\neq\beta$ 就是等式(1)全部的解，并且等式(1)的项数至多只能是 n^2-n+2. 当 $p=2$ 且 $n\geq 4$ 时，容易知道等式 $x^{2^n-1}+\alpha^bx^{2^n-2}+\alpha^{2b}x^{2^n-3}+\cdots+\alpha^{(2^n-2)b}x=0$ 的项数 $2^n-1>n^2-n+1$，因此 β 只能等于 0. 于是等式(1)的形式只能是 $x^{2^n-1}-1=0$.

因此，对于第 1)种情形，当 $p\geq 3$ 且 $n\geq 2$ 时，由等式(1)的系数可得到以下等式：

$$\sum_{j=0}^{n-1}S_jU_j=1,\ HQ=0,\ U_iH=0,$$
$$S_iQ=0,\ U_iS_{i+v}=0,$$

其中 $i=0,1,\cdots,n-1$，$v=1,2,\cdots,n-1$，$i+v \bmod n$；

对于第 2)种情形，当 $p=2$ 且 $n\geq 4$ 时，由等式(1)的系数可得到以下等式：

$$\sum_{j=0}^{n-1}S_jU_j=1,\ HQ=0,\ U_{i+1}S_i+U_iH=0,$$
$$U_iS_{i+1}+S_iQ=0,\ U_iS_{i+v}=0,$$

其中 $i=0,1,\cdots,n-1$，$v=2,3,\cdots,n-1$，$i+1 \bmod n$，$i+v \bmod n$.

不管对于第 1)种情形，还是对于第 2)种情形，都有 $Q=H^{p^n-2}$ 且 $HQ=0$，由此不难发现，$H=0$ 且 $Q=0$. 于是就有

$$\sum_{j=0}^{n-1}S_jU_j=1,\ U_iS_{i+v}=0,$$

其中 $i=0,1,\cdots,n-1$，$v=1,2,\cdots,n-1$，$i+v \bmod n$.

由于 ν^{-1} 是一个可逆仿射变换，因此映射 ν^{-1} 线性化多项式的系数不能全为 0，至少得有一个系数非零. 不妨设 $U_t\neq 0$，$0\leq t\leq n-1$，由 $U_tS_{t+1}=0$，$U_tS_{t+2}=0,\cdots,U_tS_{t+n-2}=0,U_tS_{t+n-1}=0$ 可推出 $S_{t+1}=0,S_{t+2}=0,\cdots,S_{t+n-2}=0,S_{t+n-1}=0$. 再根据 μ 也是一个可逆仿射变换，因而可知 $S_t\neq 0$. 采用同

样的方法，由 $U_{t+1}S_t=U_{t+1}S_{t+1+n-1}=0$，$U_{t+2}S_t=U_{t+2}S_{t+2+n-2}=0$，…，$U_{t+n-2}S_t=U_{t+n-2}S_{t+n-2+2}=0$，$U_{t+n-1}S_t=U_{t+n-1}S_{t+n-1+1}=0$ 可推出 $U_{t+1}=0$，$U_{t+2}=0$，…，$U_{t+n-2}=0$，$U_{t+n-1}=0$. 最后，由 $S_tU_t=1$ 可得，$U_t=S_t^{-1}$.

综上所述，当 $p\geq 3$ 且 $n\geq 2$ 时，或者 $p=2$ 且 $n\geq 4$ 时，可逆仿射变换 μ 和 ν^{-1} 线性化多项式的形式只能是 $\mu(x)=S_tx^{p^t}$ 和 $\nu^{-1}(x)=S_t^{-1}x^{p^t}$，由此易知，$\mu(x)=S_tx^{p^t}$ 和 $\nu(x)=S_t^{p^{n-t}}x^{p^{n-t}}$，其中 $0\neq S_t\in F_{p^n}$，$t=0,1,\cdots,n-1$. 于是，可逆仿射变换对 (ν,μ) 的数量即为 $n(p^n-1)$. 根据引理 4，可逆仿射变换对 (ν,μ) 关于运算“$*$”是 $Aff_n^{-1}(F_p)\times Aff_n^{-1}(F_p)$ 的一个子群. 利用可逆仿射变换对 (ν,μ) 所形成的子群对群 $Aff_n^{-1}(F_p)\times Aff_n^{-1}(F_p)$ 划分等价类，商集中陪集首的个数即为与逆函数仿射等价密码函数的数量. 利用引理 2，与逆函数仿射等价密码函数的数量为

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

证毕.

以上证明方法的主要思想是：对于等式 $F=\nu\circ F\circ\mu$，发现满足该等式的所有可逆仿射变换对 (ν,μ) 的形式和数量，然后利用可逆仿射变换对 (ν,μ) 所形成的子群对群 $Aff_n^{-1}(F_p)\times Aff_n^{-1}(F_p)$ 划分等价类，商集中陪集首的个数即为与逆函数仿射等价密码函数的数量. 定理 1 已证明了，当 $p\geq 3$ 且 $n\geq 2$ 时，或者 $p=2$ 且 $n\geq 4$ 时，满足等式 $F=\nu\circ F\circ\mu$ 的可逆仿射变换 μ 和 ν 线性化多项式的形式只能是 $\mu(x)=S_tx^{p^t}$ 和 $\nu(x)=S_t^{p^{n-t}}x^{p^{n-t}}$，$0\neq S_t\in F_{p^n}$，$t=0,1,\cdots,n-1$，没有其它形式. 从而，使得等式 $F=\nu\circ F\circ\mu$ 成立的所有可逆仿射变换对 (ν,μ) 的数量为 $n(p^n-1)$，进一步就可以计算出与逆函数仿射等价密码函数的数量.

然而，当 $p=2$ 且 $n=3$ 时，等式(1)的项数至多只能是 $3^2-3+2=8$. 若 $\mu(x)=0$ 的解为 $\beta=\alpha^b$，$0\leq b\leq 6$，此时等式 $x^7+\alpha^ix^6+\alpha^{2i}x^5+\cdots+\alpha^{6i}x=0$ 的项数 $2^3-1=3^2-3+1=7<8$；若 $\mu(x)=0$ 的解为 $\beta=0$，此时等式 $x^7-1=0$ 的项数 $2<8$. 由上述分析可知，当 $p=2$ 且 $n=3$ 时，等式(1)的系数有 8 种可能性，对于等式(1)的系数可得到 8 个不同的方程组，很难直接求解. 因此，在这种情况下，最简便的方法就是直接利用计算机作为辅助手段测试出与逆函数仿射等价密码函数的数量.

定理 2.　对于有限域 F_{2^3} 上的逆函数 $F(x)=x^{-1}=x^{2^3-2}$，当 $p=2$ 且 $n=3$ 时，使得等式 $F=\nu\circ F\circ\mu$ 成立的可逆仿射变换对 (ν,μ) 的数量为 168，进一步，与逆函数仿射等价密码函数的数量为 10752.

证明.　由 $F=\nu\circ F\circ\mu$ 可知，$\nu^{-1}\circ F=F\circ\mu$. 根据引理 1 可设，$\mu(x)=\sum_{i=0}^{2}s_ix^{2^i}+h$ 和 $\nu^{-1}(x)=\sum_{i=0}^{2}u_ix^{2^i}+z$，其中 $s_i,h,u_i,z\in F_{2^3}$. 再根据等式 $\nu^{-1}\circ F=F\circ\mu$，可得

$$\sum_{i=0}^{2}u_ix^{(2^2+2)2^i}+z=\left(\sum_{i=0}^{2}s_ix^{2^i}+h\right)^{-1}=\left(\sum_{i=0}^{2}s_ix^{2^i}+h\right)^{2^2+2}.$$

由以上等式不难发现，$z=h^6$. 若 $h\neq 0$，就有 $z\neq 0$；若 $h=0$，就有 $z=0$.

当 $\mu(x)=\sum_{i=0}^{2}s_ix^{2^i}+h=0$ 时，由于映射 μ 是一个可逆仿射变换，因此等式 $\mu(x)=0$ 有且只有一个解，不妨设这个解为 β，即 $\mu(\beta)=0$. 由于 β 是有限域 F_{2^3} 中的一个元素，β 可以是 0 或者是 α^c，其中 α 是有限域 F_{2^3} 的一个本原元，$0\leq c\leq 2^3-2$.

对于任意 $\tau\in F_{2^3}$ 且 $\tau\neq\beta$，都有 $\mu(\tau)\neq 0$，进而

$$\left(\sum_{i=0}^{2}s_i\tau^{2^i}+h\right)\left(\sum_{i=0}^{2}u_i\tau^{(2^2+2)2^i}+z\right)=1,$$

展开该等式左边的每一项可得

$$\begin{aligned}&s_0u_0\tau^{2^3-1}+s_0u_1\tau^{2^2+2^1}+s_0u_2\tau^{2^2}+s_0z\tau^{2^0}+\\&s_1u_0\tau^{2^0}+s_1u_1\tau^{2^3-1}+s_1u_2\tau^{2^2+2^0}+s_1z\tau^{2^1}+\\&s_2u_0\tau^{2^1+2^0}+s_2u_1\tau^{2^1}+s_2u_2\tau^{2^3-1}+s_2z\tau^{2^2}+\\&hu_0\tau^{2^2+2^1}+hu_1\tau^{2^2+2^0}+hu_2\tau^{2^1+2^0}+hz=1\end{aligned}\quad(2)$$

当 $\beta=0$ 时，即 $\mu(0)=0$，对于等式(2)的系数可得到以下等式：

$$\begin{aligned}&s_0u_0+s_1u_1+s_2u_2=1,\ hz=0,\\&s_0u_1+hu_0=0,\ s_1u_2+hu_1=0,\\&s_2u_0+hu_2=0,\ s_0u_2+s_2z=0,\\&s_1u_0+s_0z=0,\ s_2u_1+s_1z=0.\end{aligned}$$

由于 $z=h^6$ 且 $hz=0$，由此不难发现，$h=0$ 且 $z=0$. 于是

$$s_0u_0+s_1u_1+s_2u_2=1,\ s_iu_{i+1}=0,\ s_iu_{i-1}=0,$$

其中 $i=0,1,2$，$i+1\bmod 3$，$i-1\bmod 3$.

由于 μ 是一个可逆仿射变换，因此映射 μ 线性

化多项式的系数不能全为 0，至少得有一个系数非零. 不妨设 $s_t\neq 0, 0\leq t\leq 2$，由 $s_t u_{t+1}=0$ 和 $s_t u_{t-1}=0$ 可推出 $u_{t+1}=0$ 和 $u_{t-1}=0$. 再根据 ν^{-1} 也是一个可逆仿射变换，因而可知 $u_t\neq 0$. 利用相同的方法，由 $s_{t+1}u_t=0$ 和 $s_{t-1}u_t=0$ 可推出 $s_{t+1}=0$ 和 $s_{t-1}=0$. 最后，根据 $s_{t-1}u_{t-1}+s_t u_t+s_{t+1}u_{t+1}=1$ 可得，$u_t=s_t^{-1}$.

因此，在这种情况下，可逆仿射变换 μ 和 ν^{-1} 线性化多项式的形式只能是 $\mu(x)=s_t x^{2^t}$ 和 $\nu^{-1}(x)=s_t^{-1}x^{2^t}$，由此易知，$\mu(x)=s_t x^{2^t}$ 和 $\nu(x)=s_t^{2^{3-t}}x^{2^{3-t}}$，其中 $0\neq s_t\in F_{2^3}$，$t=0,1,2$. 于是可逆仿射变换对 (ν,μ) 的数量为 21.

当 $\beta=\alpha^c$ 时，即 $\mu(\alpha^c)=0$，其中 α 是有限域 F_{2^3} 的一个本原元，$0\leq c\leq 2^3-2$，对于等式(2)的系数可得到以下等式：

$$s_0u_0+s_1u_1+s_2u_2=1,\ hz=1,$$
$$s_0u_1+hu_0=\alpha^c,\ s_1u_2+hu_1=\alpha^{2c},$$
$$s_2u_0+hu_2=\alpha^{4c},\ s_0u_2+s_2z=\alpha^{3c},$$
$$s_1u_0+s_0z=\alpha^{6c},\ s_2u_1+s_1z=\alpha^{5c}.$$

经计算机测试，使得以上这些等式成立的 $(s_0,s_1,s_2,u_0,u_1,u_2,h,z)$ 的数量为 21. 于是，在这种情况下，可逆仿射变换对 (ν,μ) 的数量即为 $21\times 7=147$.

综上所述，使得等式 $F=\nu\circ F\circ\mu$ 成立的所有可逆仿射变换对 (ν,μ) 的数量为 168. 根据引理 4，可逆仿射变换对 (ν,μ) 关于运算“$*$”是 $Aff_3^{-1}(F_2)\times Aff_3^{-1}(F_2)$ 的一个子群. 利用可逆仿射变换对 (ν,μ) 所形成的子群对群 $Aff_3^{-1}(F_2)\times Aff_3^{-1}(F_2)$ 划分等价类，商集中陪集首的个数即为与逆函数仿射等价密码函数的数量. 利用引理 2，当 $p=2$ 且 $n=3$ 时，与逆函数仿射等价密码函数的数量即为

$$\frac{\left[2^{3(3+1)/2}\prod_{i=1}^{3}(2^i-1)\right]^2}{168}=10752.$$ 证毕.

定理 2 揭示了 $p=2$ 且 $n=3$ 这种特殊情况下与逆函数仿射等价密码函数的数量. 定理 1 和定理 2 给出了与逆函数仿射等价函数数量的一套完整结果.

4 应用价值

在第 4 节中，我们将介绍第 3 节研究成果的实际应用价值.

在实际应用中，有不少著名的分组密码算法都采用与逆函数仿射等价的向量值函数作为 S 盒，如 AES 算法、Camellia 算法、CLEFIA 算法和 SMS4 算法等，这些算法的 S 盒都是 8 比特输入，8 比特输出，它们均是有限域 F_{2^8} 上的向量值函数. 由定理 1 可知，当 $p=2$ 且 $n=8$ 时，使得等式 $F=\nu\circ F\circ\mu$（此时 $F(x)=x^{-1}=x^{254}$）成立的所有可逆仿射变换对 (ν,μ) 的数量为 $8\times 255=2040$. 于是，有限域 F_{2^8} 上与逆函数仿射等价密码函数的数量为

$$\frac{\left[2^{36}\prod_{i=1}^{8}(2^i-1)\right]^2}{8\times 255}=2^{69}\times 255\times\left[\prod_{i=1}^{7}(2^i-1)\right]^2.$$

5 结 论

本文提出了一种计算有限域 F_{p^n} 上与逆函数仿射等价密码函数数量的方法. 当 $p\geq 3$ 且 $n\geq 2$ 时，或者 $p=2$ 且 $n\geq 4$ 时，利用该方法可计算出与逆函数仿射等价密码函数的数量. 当 $p=2$ 且 $n=3$ 时，可利用计算机作为辅助手段测试出与逆函数仿射等价密码函数的数量. 因此在实际应用中，就可以知道有限域 F_{2^8} 上有 $2^{69}\times 255\times\left[\prod_{i=1}^{7}(2^i-1)\right]^2$ 个与逆函数仿射等价的密码函数可直接用于分组密码的 S 盒. 接下来，将进一步研究有限域 F_{p^n} 上与逆函数 EA 等价和 CCZ 等价密码函数的数量.

参 考 文 献

[1] Carlet C. S-boxes, Boolean functions and codes for the resistance of block ciphers to cryptographic attacks, with or without side channels//Proceedings of the 5th International Conference on Security, Privacy, and Applied Cryptography Engineering-SPACE'2015. LNCS 9354. Jaipur, India, 2015: 151-171

[2] Peng Jie, Tan C H. New explicit constructions of differentially 4-uniform permutations via special partitions of $GF(2^{2k})$. Finite Fields and Their Applications, 2016, 40: 73-89

[3] Carlet C. On known and new differentially uniform functions//Proceedings of the 16th Australasian Conference on Information Security and Privacy-ACISP'2011. LNCS 6812. Melbourne, Australia, 2011: 1-15

[4] Budaghyan L, Carlet C. CCZ-equivalence of bent vectorial functions and related constructions. Designs, Codes and Cryptography, 2011, 59(1-3): 69-87

[5] Berger T P, Canteaut A, Charpin P, Laigle-Chapuy Y. On

almost perfect nonlinear functions over $GF(2^n)$. IEEE Transactions on Information Theory, 2006, 52(9): 4160-4170

[6] Budaghyan L, Carlet C, Helleseth T, Li Nian. On the (non-) existence of APN (n,n)-functions of algebraic degree n //Proceedings of the IEEE International Symposium on Information Theory-ISIT'2016, Barcelona, Spain, 2016: 480-484

[7] Browning K A, Dillon J F, McQuistan M T, Wolfe A J. An APN permutation in dimension six//Proceedings of the 9th International Conference on Finite Fields and Their Applications-Fq'9. Dublin, Ireland, 2010, 518: 33-42

[8] Perrin L, Udovenko A, Biryukov A. Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem//Proceedings of the Advances in Cryptology-CRYPTO'2016, Part II. LNCS 9815. Santa Barbara, USA, 2016: 93-122

[9] Canteaut A, Duval S, Perrin L. A generalisation of Dillon's APN permutation with the best known differential and nonlinear properties for all fields of size 2^{4k+2}. IEEE Transactions on Information Theory, 2017, 63(11): 7575-7591

[10] Tang Deng, Carlet C, Tang Xiao-Hu. Differentially 4-uniform bijections by permuting the inverse function. Designs, Codes and Cryptography, 2015, 77(1): 117-141

[11] Qu Long-Jiang, Tan Yin, Li Chao, Gong Guang. More constructions of differentially 4-uniform permutations on $GF(2^{2k})$. Designs, Codes and Cryptography, 2016, 78(2): 391-408

[12] Tao Biao-Shuai, Wu Hong-Jun. Improving the Biclique cryptanalysis of AES//Proceedings of the 20th Australasian Conference on Information Security and Privacy-ACISP'2015. LNCS 9144. Brisbane, Australia, 2015: 39-56

[13] Dong Xiao-Yang, Li Lei-Bo, Jia Ke-Ting, Wang Xiao-Yun. Improved attacks on reduced-round Camellia-128/192/256// Proceedings of the Topics in Cryptology-CT-RSA'2015, LNCS 9048. San Francisco, USA, 2015: 59-83

[14] Tezcan C, Selçuk A A. Improved improbable differential attacks on ISO standard CLEFIA: Expansion technique revisited. Information Processing Letters, 2016, 116(2): 136-143

[15] Su Bo-Zhan, Wu Wen-Ling, Zhang Wen-Tao. Security of the SMS4 block cipher against differential cryptanalysis. Journal of Computer Science and Technology, 2011, 26(1): 130-138

[16] Li Yong-Qiang, Wang Ming-Sheng. Constructing S-boxes for lightweight cryptography with Feistel structure// Proceedings of the Cryptographic Hardware and Embedded Systems-CHES'2014. LNCS 8731. Busan, South Korea, 2014: 127-146

[17] Mishra P R, Sarkar S, Gupta I. Determining the minimum degree of an S-box. IACR Cryptology ePrint Archive, 2017: 376

[18] Stoffelen K. Optimizing S-box implementations for several criteria using SAT solvers//Proceedings of the 23rd International Conference on Fast Software Encryption-FSE'2016, LNCS 9783. Bochum, Germany, 2016: 140-160

[19] Sajadieh M, Mirzaei A, Mala H, Rijmen V. A new counting method to bound the number of active S-boxes in Rijndael and 3D. Designs, Codes and Cryptography, 2017, 83(2): 327-343

[20] Lidl R, Niederreiter H. Finite Fields. 2nd Edition. Cambridge, UK: Cambridge University Press, 1997

[21] Wan Zhe-Xian. Geometry of Classical Groups over Finite Fields. 2nd Edition. Beijing: Science Press, 2006

YUAN Feng, Ph. D., assistant researcher. His research interests include cryptography and information security.

JIANG Ji-Jun, M. S., engineer. His research interests include information security and network security.

YANG Yang, Ph. D., associate professor. Her research interests include cryptography and information security.

OU Hai-Wen, Ph. D., professor. His research interests include cryptography and information security.

WANG Min-Juan, M. S., associate professor. Her research interests include differential geometry and cryptography.

Background

The security of modern block ciphers substantially relies on the cryptographic properties of its substitution boxes (S-boxes), which are in most of the cases the only source of nonlinearity. The inverse function is the most famous differentially 4-uniform permutation with many very nice cryptographic properties over $F_{2^{2n}}$. It is appropriate to choose the permutation polynomials of affine equivalent to the inverse function on $F_{2^{2n}}$ as the S-boxes of block ciphers. For

example, the S-box of AES is affine equivalent to the inverse function over F_{2^8}.

At present, the research on the S-boxes of block ciphers focuses on design and optimization, etc. Moreover, the research on the S-boxes of affine equivalent to the inverse function is to find the counting method of the minimum number of active S-boxes for several consecutive rounds of block ciphers.

It is different from the previous researches. The present paper attempts to study the counting problem of affine equivalent to the inverse function. If the exact number of affine equivalent to the inverse function is computed, the cryptographic algorithm's designer knows that how many the S-boxes of affine equivalent to the inverse function can be chosen in real applications. The inverse function over finite field F_{2^n} is generalized to the inverse function over finite field F_{p^n}, where $p\geq 2$ is a prime number. This is a generalization of the inverse function. When $p\geq 3$ and $n\geq 2$, or $p=2$ and $n\geq 4$, for the inverse function $F(x)=x^{-1}\in F_{p^n}[x]$, we use some properties of finite fields to count the number of affine equivalent to the inverse function. The basic idea of the count method is to find all the pairs of invertible affine transformations $(\nu,\mu)\in Aff_n^{-1}(F_p)\times Aff_n^{-1}(F_p)$ such that $F=\nu\circ F\circ\mu$, where $Aff_n^{-1}(F_p)$ is the $n\times n$ invertible affine transformation group over finite field F_p. Then, the group $Aff_n^{-1}(F_p)\times Aff_n^{-1}(F_p)$ can be partitioned into equivalence classes by using the pairs of invertible affine transformations (ν,μ) form the subgroup. The number of coset representatives of the group $Aff_n^{-1}(F_p)\times Aff_n^{-1}(F_p)$ relative to the subgroup is equal to the number of affine equivalent to the inverse function. Moreover, when $p=2$ and $n=3$, for the inverse function $F(x)=x^{-1}\in F_{2^3}[x]$, the number of affine equivalent to the inverse function is obtained by using the computer. Our results show that there are $2^{69}\times 255\times\left[\prod_{i=1}^{7}(2^i-1)\right]^2$ cryptographic functions of affine equivalent to the inverse function over finite field F_{2^8}, which can be used in the S-boxes of block ciphers.

This work is supported by the National Key R&D Program of China under Grant No. 2018YFB0803600, the National Natural Science Foundation of China under Grant No. 61402112, the Fundamental Research Funds for the Central Universities: 2014 XSYJ09 and 328201509, and the Fund of Beijing Electronic Science and Technology Institute: 2014 TD2-OHW.