·安全技术· 文章编号：1000-3428(2019)09-0124-04 文献标志码：A 中图分类号：TP309

有限域上置换多项式的研究进展

郑彦斌[1]，易宗向[2,3]

（1. 桂林电子科技大学 广西密码学与信息安全重点实验室，广西 桂林 541004；
2. 广州大学 数学与信息科学学院，广州 510006；
3. 广东科技学院 公共基础部，广东 东莞 523083）

摘 要： AGW 准则和分段方法是构造有限域上置换多项式的两种主要方法。介绍有限域上置换多项式在密码学和编码理论中的应用，总结利用 AGW 准则和分段方法构造有限域上置换多项式和逆置换的研究进展，阐述置换多项式存在的问题，并对下一步研究工作进行展望。

关键词： 密码学；有限域；逆置换；多项式；AGW 准则；分段方法

中文引用格式： 郑彦斌，易宗向. 有限域上置换多项式的研究进展[J]. 计算机工程，2019，45(9)：124-127.

英文引用格式： ZHENG Yanbin，YI Zongxiang. Research progress on permutation polynomials in finite fields[J]. Computer Engineering，2019，45(9)：124-127.

Research Progress on Permutation Polynomials in Finite Fields

ZHENG Yanbin[1]，YI Zongxiang[2,3]

（1. Guangxi Key Laboratory of Cryptography and Information Security，
Guilin University of Electronic Technology，Guilin，Guangxi 541004，China；
2. School of Mathematics and Information Science，Guangzhou University，Guangzhou 510006，China；
3. Department of Public Foundation，Guangdong University of Science and Technology，Dongguan，Guangdong 523083，China）

【Abstract】 The Akbary-Ghioca-Wang（AGW）criterion and piecewise method are two main methods for constructing permutation polynomials of finite fields. This paper introduces the application of permutation polynomials in cryptography and coding theory，reviews the research progress of the permutation polynomials and their inverses constructed by AGW criterion and piecewise method，describes the problem of permutation polynomials，and finally the next step is to look into the research work.

【Key words】 cryptography；finite fields；inverses of permutation；polynomials；Akbary-Ghioca-Wang（AGW）criterion；piecewise method

DOI： 10.19678/j.issn.1000-3428.0050912

0 概述

有限域上置换多项式被广泛应用于密码学、编码理论、组合设计等领域。在密码学中，高级加密标准（Advanced Encryption Standard，AES）的 S 盒利用有限域上的置换 x^{-1} 进行设计[1]，置换多项式及其逆置换多项式可用来构造密钥交换协议[2]及差分均匀度较低的密码函数[3-4]。在编码理论和组合设计中，特殊 Dickson 置换多项式可用来构造新类型的 skew Hadamard 差集[5]，有限域上置换多项式还可构造循环码[6]、正交拉丁方[7-8]等。

关于有限域上置换多项式的研究较多[9-10]，但仍有问题尚未解决[9-10]。例如，置换二项式的完全刻画问题未得到解决，寻找有效算法计算已知置换多项式的逆置换多项式依然是一个开放性问题。因此，构造新类型的置换多项式具有重要的研究价值。

本文阐述利用 AGW（Akbary-Ghioca-Wang）准则和分段方法构造置换多项式的研究现状，介绍有限域上置换多项式的逆置换多项式，并展望下一步研究工作。

1 置换多项式的定义

从有限域到自身的每个函数都可用多项式表示，因此在有限域上只考虑多项式函数。设 $f(x)$ 是

基金项目： 国家自然科学基金（61602125，61502113）；广西自然科学基金（2016GXNSFBA380153，2017GXNSFAA198192）；广西密码学与信息安全重点实验室项目（GCIS201625）。

作者简介： 郑彦斌（1983—），男，讲师、博士，主研方向为密码学、有限域；易宗向，博士。

收稿日期： 2018-03-23 **修回日期：** 2018-04-27 **E-mail：** zhengyanbin@guet.edu.cn

系数在有限域 GF(q)上的多项式,若其导出的映射 $f:c\mapsto f(c)$ 是 GF(q)的置换,则称 $f(x)$ 为 GF(q)的置换多项式。

国内外学者对有限域上置换多项式进行了较多研究。文献[11]总结了 1983 年之前有限域上置换多项式的主要成果。文献[12-13]介绍了有限域上置换多项式的 Hermite 准则、计数与分布、群结构及其构造方法。

2　AGW 准则

文献[14]推导出 $f(x)=x^rh(x^{(q-1)/d})$ 是 GF(q)的置换多项式的充要条件。文献[15]用群置换的方法将 $f(x)$ 是否置换 GF(q)的问题转化为 $g(x)=x^rh(x)^{(q-1)/d}$ 是否置换 GF(q)中所有 d 次单位根组成的群 $U(d)$ 问题。

定理 1　设 d、s、r 均是正整数且 $ds=q-1$。对任意 $h(x)\in \mathrm{GF}(q)[x]$,$f(x)=x^rh(x^s)$ 是 GF(q)的置换多项式当且仅当 $(r,s)=1$,$x^rh(x)^s$ 置换 $U(d)$[15-16]。

定理 2(AGW 准则[17])设 R、S、$\bar{S}$ 是有限集合且 S 和 $\bar{S}$ 中元素个数相等,f、$\bar{\theta}$、θ、g 是图 1 中相应集合之间的映射。若 $\bar{\theta}\circ f=g\circ\theta$,则 f 置换 R 当且仅当 g 是从 S 到 $\bar{S}$ 的双射,且对任意 $s\in S$,映射 f 在 $\theta^{-1}(s)$ 上均是单射。其中,$\circ$ 表示函数复合运算。

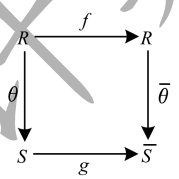

图 1　AGW 准则交换示意图

上述定理将 f 是否置换 R 的问题转化为 g 是否是从 S 到 $\bar{S}$ 的双射的问题。文献[12]称上述思想为 AGW 准则。该准则为构造置换多项式提供了一个非常重要的方法。该准则可应用到剩余类环和有限域等集合。在定理 2 中取 $\theta(x)=\bar{\theta}(x)=x^s$ 即可得到定理 1。

文献[18-19]利用 AGW 准则重点研究了形如 $f(x)=g(B(x))+\sum(L_i(x)+\delta_i)h_i(B(x))$ 和 $f(x)=g(x)h(\lambda(x))$ 的置换多项式。文献[20]利用 AGW 准则构造形如 $\theta x+\beta g(x^{p^k}-\beta^{p^k-1}x)Tr_n^k(x)$ 的置换多项式。文献[21]运用 AGW 准则构造了 GF(q^2)上形如 $(x^q-bx+c)^{(q^2-1)/d+1}+bx$ 的置换多项式,其中 $d\in\{2,3,4,6\}$ 且 d 整除 q^2-1。文献[22]推导出 $(ax^q+bx+c)^r\varphi((ax^q+bx+c)^{(q^2-1)/d})+ux^q+vx$ 是 GF(q^2)上置换多项式的充要条件,其中 a、b、c、u、$v\in$ GF(q^2),r 是任意正整数,d 是 q^2-1 的任意正因子,$\varphi(x)$ 是系数在 GF(q^2)上的任意多项式。文献[23]构造了特殊的交换图,进而利用 AGW 准则得到 GF(q^2)上形如 $x^rh(x^{q-1})$ 的置换多项式,将其结果统一并应用到已知的置换三项式。

综上,AGW 准则是构造置换多项式的重要方法,但是该准则也有一定的局限。如图 1 所示,给定一般的 R 和 f,如何构造 $\bar{\theta}$、θ、g 使图 1 可交换是一个非常困难的问题,目前还没有构造交换图的通用方法。

3　分段方法

分段构造置换多项式思想是将有限域 GF(q)划分成互不相交的三段:GF(q)$=\{0\}\cup D_1\cup D_2$,其中 D_1 是 GF(q)中非零平方元的集合,D_2 是非平方元的集合。当 $x\in D_1$ 时,$x^{(q-1)/2}=1$;当 $x\in D_2$ 时,$x^{(q-1)/2}=-1$。因此 $f(x)=x^{(q+1)/2}+ax$ 可写成:

$$f(x)=\begin{cases}0,x=0\\ f_1(x)=(a+1)x,x\in D_1\\ f_2(x)=(a-1)x,x\in D_2\end{cases}$$

显然,$f_1(x)$ 在 D_1 是单射,$f_2(x)$ 在 D_2 也是单射。若 $a+1$ 和 $a-1$ 同时属于 D_1 或 D_2,则集合 $f_1(D_1)$ 和 $f_2(D_2)$ 的交集为空集。此时 $\{0\}$、$f_1(D_1)$、$f_2(D_2)$ 构成 $GF(q)$ 的一个划分,因此可得到如下定理:

定理 3　设 q 是奇素数的方幂,$a\in$ GF(q),则多项式 $f(x)=x^{(q+1)/2}+ax$ 是 GF(q)的置换多项式当且仅当 $(a^2-1)^{(q-1)/2}=1$。

文献[7]推导出多项式 $x^{(q+1)/d}+ax$ 置换 GF(q)的充要条件,其中 d 是 $q-1$ 的任意正因子。文献[24]用分段方法证明了 reversed Dickson 多项式 $D_{3^{2n}+5}(1,x)$ 是 GF(3^{2n})上的置换多项式。文献[25]研究 GF(p^n)上形如 $(x^{p^k}-x+c)^{(p^n-1)/2+1}+x^{p^k}+x$ 的置换多项式。当 $n=2k$ 时,文献[26]将 $(p^{2k}-1)/2$ 推广到 $(p^{2k}-1)/3$。文献[19]将上述结果进行改进,并用分段方法证明了定理 4。

定理 4　设 p 是奇素数,$a,b,c\in$ GF(p^n),$1\leqslant k<n$,则 $f(x)=(ax^{p^k}-bx+c)^{(p^n+1)/2}+ax^{p^k}+bx$ 是 GF(p^n)的置换多项式当且仅当 ab 是非零的平方元。

文献[27]在研究广义割圆映射置换时证明了定理 5。

定理 5　设 $d,s,r_0,r_1,\cdots,r_{d-1}$ 是正整数且 $ds=q-1$,β 是 GF(q)的本原元,$\omega=\beta^s$,$a_0,a_1,\cdots,a_{d-1}\in$ GF$(q)^*$。则 $f(x)=(1/d)\sum_{i=0}^{d-1}a_ix^{r_i}\sum_{j=0}^{d-1}(x^s/\omega^i)^j$ 是 GF(q)的置换多项式当且仅当 $(r_i,s)=1(0\leqslant i\leqslant d-1)$ 且 $\{\log_\beta a_i+ir_i:i=0,1,\cdots,d-1\}$ 是模 d 的完全剩余系。

文献[28-29]总结了分段构造置换多项式的思想。下文定理用有限域的语言描述该思想。

定理 6　设 $D_1,D_2,\cdots,D_m$ 是 GF(q)的一个划分,$f_1(x),f_2(x),\cdots,f_m(x)\in$ GF$(q)[x]$,$f(x)=\sum f_i(x)I_{D_i}(x)$,其中,$I_{D_i}(x)$ 是 D_i 的特征函数,即当 $x\in D_i$ 时,

$I_{D_i}(x)=1$;当 $x\notin D_i$ 时,$I_{D_i}(x)=0$,则 $f(x)$ 是 $GF(q)$ 的置换多项式,当且仅当每个 $f_i(x)$ 在 D_i 上都是单射,且 $f_1(D_1),f_2(D_2),\cdots,f_m(D_m)$ 互不相交。

在定理 6 中,当 $x\in D_i$ 时,$f(x)=f_i(x)$,说明 $f(x)$ 是由片函数 $f_i(x)$ 构成的分段多项式函数。根据上述定理,分段构造置换多项式可分为如下 4 步:

1)把 GF(q)分成若干互不相交的子集 D_1,$D_2,\cdots,D_m$。

2)系数在 GF(q)上的任意多项式 $f(x)$ 都可写成分段的形式,即:

$$f(x)=\begin{cases}f_1(x),x\in D_1\\f_2(x),x\in D_2\\\vdots\\f_m(x),x\in D_m\end{cases}$$

3)研究 $f_i(x)$ 在对应子集 D_i 上的置换性质。

4)$f(x)$ 是 GF(q)的置换多项式当且仅当 $f_1(D_1)$,$f_2(D_2),\cdots,f_m(D_m)$ 是 GF(q)的一个划分。

虽然分段构造置换多项式的思想比较简单,但是对于一些特殊情况确实非常有效。

4 逆置换多项式

设 $f(x)$ 是 GF(q)的置换多项式,则存在一个系数在 GF(q)的多项式 $f^{-1}(x)$ 使得 $f^{-1}(f(e))=e$ 对任意 $e\in$GF(q)均成立,称 $f^{-1}(x)$ 是 $f(x)$ 在 GF(q)上的逆置换多项式,简称逆置换。给定 $f(x)$,当 q 较小时,可用如下拉格朗日插值公式计算其逆置换:

$$f^{-1}(x)=\sum_{c\in GF(q)}c(1-(x-f(c))^{q-1})$$

这是一个逐点求逆的方法。当 q 较大时,该方法不可行,因为计算量大。事实上,求有限域上的置换多项式的逆置换非常困难[15]。因此相关研究较少,关于多项式的递置换描述如下:

1)线性多项式。设 $a,b\in$GF(q)且 $a\neq0$,则 $ax+b$ 是 $GF(q)$ 的置换多项式,其逆置换为 $(x-b)/a$。

2)单项式。x^m 是 GF(q)的置换多项式当且仅当 $(m,q-1)=1$,逆置换为 x^n,其中,$mn\equiv1(\mathrm{mod}q-1)$。

3)Dickson 多项式。设 $a=\pm1$ 且 $mn\equiv1(\mathrm{mod}q^2-1)$,则第一类 Dickson 多项式 $D_m(x,a)$ 是 GF(q)的置换多项式,其逆置换为 $D_n(x,a)$。

4)形如 $x^rh(x^{(q-1)/d})$ 的多项式。文献[30]给出 $x^rh(x^{(q-1)/d})$ 在 GF(q)上的逆置换的系数表达式。

5)线性化多项式。文献[31]利用 Dickson 矩阵第一列元素的代数余子式构造了有限域上线性化置换多项式的逆置换。

6)双线性多项式。两个线性化多项式的乘积是双线性多项式。文献[32]构造了双线性置换多项式 $x(Tr_{q^n/q}(x)+ax)$ 在 GF(q^n)上的逆置换。在此基础上,文献[33]将 GF(q^n)分解成两个子空间的直和 GF(q)$\oplus$ker(Tr),然后计算两个相关函数在这两个子空间上的逆,利用这两个逆推导出原置换在 GF(q^n)上的逆置换。文献[34]构造了置换 $f(x)=h(\psi(x))\varphi(x)+g(\psi(x))$ 在 GF(q^n)上的逆置换。文献[35-36]将分段方法和求逆置换结合起来,提出用分段方法构造逆置换的思想。

定理 7 设 $D_1,D_2,\cdots,D_m$ 是 GF(q)的一个划分,$f_1(x),f_2(x),\cdots,f_m(x)\in$GF($q$)[$x$],$f(x)=\sum f_i(x)I_{D_i}(x)$。若 $f(x)$ 是 GF(q)的置换多项式,则其逆置换多项式为:

$$f^{-1}(x)=\sum f_i^{-1}(x)I_{f_i(D_i)}(x)$$

其中,$f_i^{-1}(x)$ 是 $f_i(x)$ 在 D_i 的逆函数,$I_{f_i(D_i)}(x)$ 是 $f_i(D_i)$ 的特征函数。

定理 7 描述了定理 6 中置换多项式的逆置换多项式的抽象表达式。定理 7 将计算逆置换多项式 $f^{-1}(x)$ 的问题转化为另一个问题:求若干个片函数 $f_i(x)$ 的逆函数 $f_i^{-1}(x)$ 和若干个像集合 $f_i(D_i)$ 的特征函数 $I_{f_i(D_i)}(x)$。一般情况下,该问题也是一个困难问题。但是,当片函数比较简单时,第 2 个问题通常容易解决。根据上述思路,文献[35-36]构造了已知置换的逆置换多项式,下文列出主要定理。

定理 8 设 d、s、q、r_i、a_i、β、ω、$f(x)$ 如定理 5 所定义。若 $f(x)$ 是 GF(q)的置换多项式,则有:

$$f^{-1}(x)=(1/d)\sum_{i=0}^{d-1}\omega^{ir_i}(x/a_i)^{\tilde{r}_i}\sum_{j=0}^{d-1}(x^s/a_i^s\omega^{ir_i})^j$$

其中,$\tilde{r}_i,t_i\in Z$ 满足 $1\leqslant\tilde{r}_i<s$ 且 $r_i\tilde{r}_i+st_i=1$。

定理 8 给出定理 5 中置换多项式的逆置换多项式的简明表达式。在定理 8 中取 $a_i=h(\omega^i)$ 且 $r_i=r$,可得到定理 1 中 $f(x)$ 的逆置换多项式。

定理 9 设 d、s、r 均是正整数且 $ds=q-1$。对任意 $h(x)\in$GF(q)[x],设 $f(x)=x^rh(x^s)$ 是 GF(q)的置换多项式,则 $f(x)$ 在 GF(q)上的逆置换多项式为:

$$f^{-1}(x)=(1/d)\sum_{i=0}^{d-1}\sum_{j=0}^{d-1}\omega^{i(t-jr)}(x/h(\omega^i))^{\tilde{r}+js}$$

其中,$\tilde{r},t\in Z$ 满足 $1\leqslant\tilde{r}<s$ 且 $r\tilde{r}+st=1$。

在定理 9 中取 $d=2$,$r=1$,q 是奇数,$h(x)=x+a$,可得到定理 3 中 $f(x)$ 的逆置换多项式。

定理 10 设 q 是奇数,$f(x)=x^{(q+1)/2}+ax$ 是 GF(q)的置换多项式。若 $(a+1)^{(q-1)/2}=(a-1)^{(q-1)/2}=-1$,则有:

$$f^{-1}(x)=(a^2-1)^{-1}(ax+x^{(q+1)/2})$$

若 $(a+1)^{(q-1)/2}=(a-1)^{(q-1)/2}=1$,则:

$$f^{-1}(x)=(a^2-1)^{-1}(ax-x^{(q+1)/2})$$

文献[35]给出定理 4 中 $f(x)$ 的逆置换多项式。

定理 11 设 a、b、c、p、k、n、$f(x)$ 如定理 4 所定义。若 $f(x)$ 是 GF(q)的置换多项式,则:

$$f^{-1}(x)=\frac{1}{2}(u(x)+v(x))-\frac{1}{2}a^{(p^n-1)/2}(u(x)-v(x))^{(p^n+1)/2}$$

其中,$u(x)=(x+c)/2b$,$v(x)=((x-c)/2a)^{p^{n-k}}$。

5　结束语

本文研究了有限域上置换多项式的进展,并阐述了构造有限域上置换多项式的 AGW 准则和分段方法,对置换多项式的逆置换进行分析与总结。目前,该领域的研究已经取得一定的成果,但仍存在一些问题,如 AGW 准则中交换图的构造、寻找计算已知置换的逆置换的有效算法,以及低次数置换多项式的分类、Reverse Dickson 置换多项式的完全刻画等。下一步将对以上问题进行深入研究与分析。

参考文献

[1] DAEMEN J,RIJMEN V. The design of Rijndael[M]. Berlin,Germany:Springer,2002.

[2] 曹喜望. 有限域上几个置换多项式及一个密钥交换协议[J]. 数学学报,2009,52(5):841-846.

[3] 吕述望,范修斌,王昭顺,等. 完全映射及其密码学应用[M]. 合肥:中国科学技术大学出版社,2008.

[4] 屈龙江,付绍静,李超. 密码函数安全性指标的研究进展[J]. 密码学报,2014,1(6):578-588.

[5] DING Cunsheng,YUAN Jin. A family of skew Hadamard difference sets[J]. Journal of Combinatorial Theory Series A,2006,113(7):1526-1535.

[6] DING Cunsheng,ZHOU Zhengchun. Binary cyclic codes from explicit polynomials over GF(2^m)[J]. Discrete Mathematics,2014,321:76-89.

[7] NIEDERREITER H,ROBINSON K H. Complete mappings of finite fields[J]. Journal of the Australian Mathematical Society,1982,33(2):197-212.

[8] TU Ziran,ZENG Xiangyong,HU Lei. Several classes of complete permutation polynomials[J]. Finite Fields and Their Applications,2014,25:182-193.

[9] LIDL R,MULLEN G L. When does a polynomial over a finite field permute the elements of the field? [J]. The American Mathematical Monthly,1988,95(3):243-246.

[10] LIDL R,MULLEN G L. When does a polynomial over a finite field permute the elements of the field? II[J]. The American Mathematical Monthly,1993,100(1):71-74.

[11] LIDL R,NIEDERREITER H. Finite fields[M]. Cambridge,UK:Cambridge University Press,1983.

[12] MULLEN G L,PANARIO D. Handbook of finite fields[M]. Boca Raton,USA:CRC Press,2013.

[13] HOU Xiangdong. Permutation polynomials over finite fields-a survey of recent advances[J]. Finite Fields and Their Applications,2015,32:82-119.

[14] WAN Daqing,LIDL R. Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure[J]. Monatshefte Für Mathematik,1991,112(2):149-163.

[15] PARK Y H,LEE J B. Permutation polynomials and group permutation polynomials[J]. Bulletin of the Australian Mathematical Society,2001,63(1):67-74.

[16] ZIEVE M E. Some families of permutation polynomials over finite fields[J]. International Journal of Number Theory,2008,4(5):851-857.

[17] AKBARY A,GHIOCA D,WANG Qiang. On constructing permutations of finite fields[J]. Finite Fields and Their Applications,2011,17(1):51-67.

[18] YUAN Pingzhi,DING Cunsheng. Permutation polynomials over finite fields from a powerful lemma[J]. Finite Fields and Their Applications,2011,17(6):560-574.

[19] YUAN Pingzhi,DING Cunsheng. Further results on permutation polynomials over finite fields[J]. Finite Fields and Their Applications,2014,27:88-103.

[20] ZHA Zhengbang,HU Lei,CAO Xiwang. Constructing permutations and complete permutations over finite fields via subfield valued polynomials[J]. Finite Fields and Their Applications,2015,31:162-177.

[21] YUAN Pingzhi,ZHENG Yanbin. Permutation polynomials from piecewise functions[J]. Finite Fields and Their Applications,2015,35:215-230.

[22] ZHENG Yanbin,YUAN Pingzhi,PEI Dingyi. Large classes of permutation polynomials over F_{q^2}[J]. Designs,Codes and Cryptography,2016,81(3):505-521.

[23] LI Kangquan,QU Longjiang,WANG Qiang. New constructions of permutation polynomials of the form $x^r h(x^{q-1})$ over F_{q^2}[J]. Designs,Codes and Cryptography,2018,86(10):2379-2405.

[24] HOU Xiangdong. Two classes of permutation polynomials over finite fields[J]. Journal of Combinatorial Theory,2011,118:448-454.

[25] ZHA Zhengba,HU Lei. Two classes of permutation polynomials over finite fields[J]. Finite Fields and Their Applications,2012,18(4):781-790.

[26] LI Nian,HELLESETH T,TANG Xiaohu. Further results on a class of permutation polynomials over finite fields[J]. Finite Fields and Their Applications,2013,22:16-23.

[27] WANG Qiang. Cyclotomy and permutation polynomials of large indices[J]. Finite Fields and Their Applications,2013,22:57-69.

[28] FERNANDO N,HOU X. A piecewise construction of permutation polynomials over finite fields[J]. Finite Fields and Their Applications,2012,18(6):1184-1194.

[29] CAO Xiwang,HU Lei,ZHA Zhengbang. Constructing permutation polynomials from piecewise permutations[J]. Finite Fields and Their Applications,2014,26:162-174.

[30] WANG Qiang. On inverse permutation polynomials[J]. Finite Fields and Their Applications,2009,15(2):207-213.

[31] WU Baofeng. The compositional inverse of a class of linearized permutation polynomials over F_{2^n}, n odd[J]. Finite Fields and Their Applications,2014,29:34-48.

[32] COULTER R,HENDERSON M. The compositional inverse of a class of permutation polynomials over a finite field[J]. Bulletin of the Australian Mathematical Society,2002,65(3):521-526.

[33] WU Baofeng,LIU Zhuojun. The compositional inverse of a class of bilinear permutation polynomials over finite fields of characteristic 2[J]. Finite Fields and Their Applications,2013,24:136-147.

[34] TUXANIDY A,WANG Qiang. On the inverses of some classes of permutations of finite fields[J]. Finite Fields and Their Applications,2014,28:244-281.

[35] ZHENG Yanbin,YUAN Pingzhi,PEI Dingyi. Piecewise constructions of inverses of some permutation polynomials[J]. Finite Fields and Their Applications,2015,36:151-169.

[36] ZHENG Yanbin,YU Yuyin,ZHANG Yuanping,et al. Piecewise constructions of inverses of cyclotomic mapping permutation polynomials[J]. Finite Fields and Their Applications,2016,40:1-9.

编辑　赵　辉