第 33 卷 第 7 期 计 算 机 工 程 2007 年 4 月
Vol.33 No.7 Computer Engineering April 2007
·博士论文· 文章编号：1000—3428(2007)07—0021—02 文献标识码：A 中图分类号：TN918.4

周期为 $p \equiv 7 \pmod 8$ 的一类新六次剩余序列的迹表示

杜小妮[1,2]，肖国镇[1]
(1. 西安电子科技大学 ISN 国家重点实验室，西安 710071；2. 西北师范大学数学与信息科学学院，兰州 730070)

摘 要：构造了一类新的周期为素数 $p = 4u^2 + 27 = 6f + 1$ 的六次剩余序列，利用有限域和差集理论给出了该序列在周期为素数 $p \equiv 7 \bmod 8$ 情形下的迹函数表示。新序列的线性复杂度为 $3f = (p-1)/2$，优于 Hall 六次剩余序列在相同条件下的线性复杂度。
关键词：流密码；迹函数；六次剩余序列

Trace Function Representation of a New Class of Sextic Residue Sequences of Period $p \equiv 7 \pmod 8$

DU Xiaoni[1,2], XIAO Guozhen[1]
(1. National Key Lab of ISN, Xidian University, Xi'an 710071;
2. College of Mathematic and Information Science, Northwest Normal University, Lanzhou 730070)

【Abstract】 The paper constructs a new kind of sextic residue sequences of period prime $p=4u^2+27=6f+1$. Based on the theory of finite fields and difference sets, trace function representation of this sequence of period $p \equiv 7 \pmod 8$ is determined. The linear complexity of the new sequence is $3f=(p-1)/2$, which outperforms that of Hall's sextic residue sequences.
【Key words】 Stream cipher; Trace function; Sextic residue sequences

序列构造及其随机性分析是伪随机性序列理论的重要问题。迹函数不仅是构造序列和研究序列的线性复杂度和相关性等密码学性质的重要工具，而且依据迹表示还可以得到生成该序列的线性反馈移位寄存器(LFSR)。Hall六次剩余序列是一种差集序列[1,2]。Kim 等研究了Hall六次剩余序列的线性复杂度[3]，给出了 $p \equiv 7 \pmod 8$ 情况下的迹表达式[4]。本文构造了一类新的周期为素数 $p=4u^2+27=6f+1$ 的六次剩余序列，并利用有限域和差集理论给出了该序列在周期为素数 $p \equiv 7 \pmod 8$ 情形下的六次剩迹函数表示。迹函数 $tr_1^n(\cdot)$ 是从有限域 F_{2^n} 到其子域 $F_2 = \{0,1\}$ 的映射，定义为 $tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$。有关迹函数和有限域的定义和性质，见文献[5]。

1 新的六次剩余序列的定义和基本性质

令 $p=4u^2+27=6f+1$ 是素数，g 是模 p 的本原根。则所有模 p 剩余的非零整数可以分成 6 类，记为 $C_l, l = 0,1,\ldots,5$。其中 $C_l = \{g^{6i+l} \mid i = 0,1,2,\ldots,f-1\}$。

则周期为 p 的新的六次剩余序列定义为

$$s_t = \begin{cases} 0, & t \in C_0 \cup C_1 \cup C_2 \\ 1, & \text{其它} \end{cases}$$

其中 $t = 0,1,2,\ldots,p-1$，由文献[2]可知，总可以选择恰当的生成元 g 使得 $3 \in C_1$，则 $-1 \in C_3$。

序列的生成多项式 $S(x)$ 为

$$S(x) = C_3(x) + C_4(x) + C_5(x) + 1$$

其中，$3 \in C_1$，$C_l(x) = \sum_{i \in C_l} x^i = \sum_{i=0}^{f-1} x^{g^{6i+l}} = \sum_{i=0}^{f-1} x^{3^j g^{6i}}, l = 0,1,\ldots,5$。

下面假定 $p \equiv 7 \pmod 8$。β 是多项式 $x^p - 1$ 的分裂域 $GF(2^n)$ 中的 p 次本原单位根，其中 n 为 $2 \bmod p$ 的阶。

下面的引理 1~引理 6 的证明见文献[3]。

引理 1 $|C_l| = (p-1)/6$ 对任意的 $a \in C_0$，有 $aC_l = C_l$ 且 $C_l(\beta) = C_0(\beta^{3^l})$。

引理 2 对任意的 $a \in C_0$ 有 $C_l(\beta^a) = C_l(\beta)$。

引理 3 如果 i 和 j 属于相同的剩余类，则 $C_l(\beta^i) = C_l(\beta^j)$。

引理 4 如果 $2 \in C_0$，则 $C_l(\beta) = 0$ 或 1。

引理 5 $\sum_{l=0}^{5} C_l(\beta) = 1$。

引理 6 $2 \in C_0$。

引理 7 $S(\beta)S(\beta^{-1}) = 0$。

证明 由 p 的定义可知 f 是奇数，$(C_i)^{-1} = C_{i+3}$ [6]，则 $S(x) = C_3(x) + C_4(x) + C_5(x) + 1$，$S(x^{-1}) = S(x^{3^3}) = C_0(x) + C_1(x) + C_2(x) + 1$。

将 β 带入上式，根据引理 4~引理 6，$S(\beta) \in \{0,1\}$，因而 $S(\beta^{-1}) = 1 + S(\beta)$，$S(\beta)S(\beta^{-1}) = 0$。

引理 8 $C_0(x) = \sum_{i=0}^{\frac{p-1}{6n}-1} tr_1^n(x^{g^{6i}})$。

证明 由引理 6，$2 \in C_0$。六次剩余类 C_0 为模 p 非零整数乘法群的子群。记 H_0 为由 2 生成的循环子群，则 $C_0 = \bigcup_{i=0}^{\frac{p-1}{6n}-1} g^{6i} H_0 = \bigcup_{i=0}^{\frac{p-1}{6n}-1} H_i$ 是 H_0 在 C_0 中的一些不相交的陪集的并。其中 $H_i = g^{6i} H_0$。若记 $H_i(x) = \sum_{j \in H_i} x^j$，

基金项目：国家自然科学基金资助项目(60473028)；国家“973”计划基金资助项目(G1999035804)
作者简介：杜小妮(1972－)，女，博士生，主研方向：密码学和信息安全；肖国镇，教授、博导
收稿日期：2006-10-12 **E-mail：**ymldxn@126.com

$i=0,1,\ldots,\frac{p-1}{6n}-1$ 。 则 $H_0(x)=\sum_{j\in H_0}x^j \quad \sum_{i=0}^{n-1}x^{2^i}=tr_1^n(x)$ ，$H_i(x)=tr_1^n(x^{g^{6i}})$。

同理可得

$C_1=gC_0=\bigcup_{i=0}^{\frac{p-1}{6n}-1}g^{6i+1}H_0=\bigcup_{i=0}^{\frac{p-1}{6n}-1}gH_i$，

$C_2=gC_1=\bigcup_{i=0}^{\frac{p-1}{6n}-1}g^{6i+2}H_0=\bigcup_{i=0}^{\frac{p-1}{6n}-1}g^2H_i$。

所以， $C_1(x)=\sum_{i=0}^{\frac{p-1}{6n}-1}tr_1^n(x^{g^{6i+1}})$， $C_2(x)=\sum_{i=0}^{\frac{p-1}{6n}-1}tr_1^n(x^{g^{6i+2}})$。

2 新的六次剩余序列的迹表示

定理 1 令 $p=6f+1\equiv 7\bmod 8$，则存在一个本原 p 次单位根 α 使得 $S(\alpha^{-1})=1$。

证明 令 γ 为一个本原 p 次单位根, 根据 g 的选取，有 $3\in C_1$， $3^i\in C_i$，则

$$\sum_{i=1}^{p-1}S(\gamma^i)=\sum_{i=1}^{p-1}C_3(\gamma^i)+\sum_{i=1}^{p-1}C_4(\gamma^i)+\sum_{i=1}^{p-1}C_5(\gamma^i)+1$$
$$=\sum_{j=0}^{5}C_3(\gamma^{3^j})+\sum_{j=0}^{5}C_4(\gamma^{3^j})+\sum_{j=0}^{5}C_5(\gamma^{3^j})$$
$$=\sum_{j=0}^{5}C_3(\gamma^{3^j})+\sum_{j=0}^{5}C_4(\gamma^{3^j})+\sum_{j=0}^{5}C_4(\gamma^{3^{j+1}})$$
$$=\sum_{j=0}^{5}C_3(\gamma^{3^j})=\sum_{k=0}^{p-2}\gamma^{g^k}=1$$

从而至少存在一个 i，使得 $S(\gamma^i)=1$。取 $\alpha=\gamma^{-i}$ 即为所求。

定理 2 令 $p=4u^2+27=6f+1\equiv 7(\bmod 8)$ 为素数，则新六次剩余序列的迹表示如下：

$$s(t)=\sum_{i=0}^{\frac{p-1}{6n}-1}tr_1^n(\alpha^{g^{6i}t})+\sum_{i=0}^{\frac{p-1}{6n}-1}tr_1^n(\alpha^{g^{6i+1}t})+\sum_{i=0}^{\frac{p-1}{6n}-1}tr_1^n(\alpha^{g^{6i+2}t})$$

证明 记 $C(x)=C_0(x)+C_1(x)+C_2(x)$ ，仅需证明 $C(\alpha^t)=0\Leftrightarrow t\in C_0\cup C_1\cup C_2$。

由 g 的选取，有 $3\in C_1$， $3^i\in C_i$。即需

$C(\alpha)=C(\alpha^{3^0})=C_0(\alpha)+C_1(\alpha)+C_2(\alpha)=0$

$C(\alpha^3)=C_0(\alpha^3)+C_1(\alpha^3)+C_2(\alpha^3)=C_1(\alpha)+C_2(\alpha)+C_3(\alpha)=0$

$C(\alpha^{3^2})=C_0(\alpha^{3^2})+C_1(\alpha^{3^2})+C_2(\alpha^{3^2})=C_2(\alpha)+C_3(\alpha)+C_4(\alpha)=0$

因为 $-1\in C_3$，由定理 1，有

$S(\alpha^{-1})=S(\alpha^{3^3})=C_0(\alpha)+C_1(\alpha)+C_2(\alpha)+1=1$

所以 $C(\alpha)=C_0(\alpha)+C_1(\alpha)+C_2(\alpha)=0$ 成立。

根据引理 7， $S(\alpha)=C(\alpha^{3^3})+1=0$，从而 $C(\alpha^{3^3})=1$。

$C(\alpha^{3^4})=C_0(\alpha)+C_4(\alpha)+C_5(\alpha)=1+C(\alpha^3)$ ；

$C(\alpha^{3^5})=C_0(\alpha)+C_1(\alpha)+C_5(\alpha)=1+C(\alpha^{3^2})$。

由以上证明过程可知：$C(\alpha^t)=0\Leftrightarrow t\in C_0\cup C_1\cup C_2$。

又因为 $f=\frac{p-1}{6}$ 为奇数， $t=0$ 时，有

$C(\alpha^0)=C(1)=|C_0|=\frac{p-1}{6}=f=1$

从而该定理得证。

3 结论分析

本文构造了一类新的周期为素数$p=4u^2+27=6f+1$ 的六次剩余序列，并给出了序列在周期为素数$p\equiv 7(\bmod 8)$情形下的迹函数表示。由得到的迹函数表达式可知，$\{s(t)\}$ 仅有 6 个循环不等价的采样，分别为d_l-采样，其中 $d_l\in C_l$，$l=0,1,\ldots,5$。因为 $\{s(d_it)\}=\{s(d_jt)\}$ 对所有 t 成立当且仅当 d_i,d_j 属于同一个六次剩余类。并且利用迹函数表达式和key方法[7]，可以得到该类序列的线性复杂度为 $3f=(p-1)/2$，优于Hall六次剩余序列在相同条件下的线性复杂度。

参考文献

1 Jensen J M, Jensen H E, Hodoldt T. The Merit Factor of Binary Sequences Related to Difference Sets[J]. IEEE Trans. on Inform. Theory, 1991, 37(3): 617-626.

2 Jr M H. A Survey of Difference Sets[C]//Proc. of Amer. Math. Soc.. 1956, 7: 975-986.

3 Kim J H, Song H Y. On the Linear Complexity of Hall's Sextic Residue Sequences[J]. IEEE Trans. on Inform. Theory, 2001, 47(5): 2094-2096.

4 Kim J H, Song H Y, Gong G. Trace Function Representatio of Hall's Sextic Residue Sequences of Period $p\equiv 7(\bmod 8)$ [DB/OL]. 2002. http://www.cacr.math.uwaterloo.ca/.

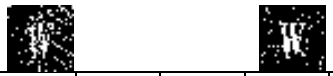
5 Lidl R, Neiderreiter H. Finite Fields[M]. MA: Addison-Wesley, 1983.

6 Storer T. Cyclotomy and Difference Sets[M]. Chicago: Markham, 1967.

7 Key E L. An Analysis of the Structure and Complexity of Nonlinear Binary Sequence Generators[J]. IEEE Trans. on Inform. Theory, 1976, 22(6): 732-736.

（上接第 20 页）

表 1 剪切强度和 BER 关系



剪切强度	1/16	1/8	1/4	1/2	3/4
BER	0	0	0	0.001 1	0.074 4

(a)剪切 3/4　　(b)质量因子 60 检测

图 5 水印

5 结论

本文通过对彩色图像的研究，引进了大量的数字通信技术，如调制、分集接收、自适应谱线增强器、数字积累、相关接收机，把这些技术和可读水印技术紧密地结合起来，提出了一个彩色图像的可读水印方案，该方法是一种自适应的盲检测方法。从理论和实验看，本文方法保证了图像的不可见性，加强了水印的鲁棒性，并且在实用上得到了提高。

参考文献

1 Craver S, Memon N, Yeo B L, et al. Resolving Rightful Ownerships with Invisible Watermarking Techniques: Limitations, Attacks, and Implications[J]. IEEE J. Select. Areas Comm., 1998, 16(4): 573-586.

2 黄继武, Elmasry G E, 程卫东, 等. 基于匹配滤波的有意义图像水印算法[J]. 电子学报, 2001, 29(4): 447-451.

3 张冠男, 王树勋, 温　泉. 一种嵌入可读水印的自适应盲水印算法[J]. 电子学报, 2005, 32(2): 308-312.

4 Chang Chip-Hong, Ye Zhi, Zhang Mingyan. Fuzzy-ART Based Adaptive Digital Watermarking Scheme[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2005, 15(1): 65-81.

5 唐世福, 苏理云, 马　洪, 等. 基于混沌置乱的 DCT 域彩色图像自适应水印算法[J]. 四川大学学报(自然科学版), 2004, 41(2): 256-261.

6 张荣跃, 倪江群, 黄继武. 基于小波域 HMM 模型的稳健多比特图像水印算法[J]. 软件学报, 2005, 16(7): 1323-1332.

7 Widrow B. Adaptive Noise Canceling: Principles and Applications[J]. Proc. of IEEE, 1975, 63(12): 1692-1716.