具有低相关值的新的修改的二元 Jacobi 序列*)

闫统江[1,2]　肖国镇[1]
(西安电子科技大学综合业务国家重点实验室　西安 710071)[1]
(中国石油大学数学与计算科学学院　东营 257061)[2]

摘　要　根据修改的二元 Jacobi 序列的构造方法，利用任意起点的二元 Jacobi 序列，构造了大量的新的二元序列。并利用 Legendre 特征函数的求和公式，给出了其中一类序列的自相关值及其它类序列在一定条件下的互相关值。结果表明，这类序列在一定条件下具有非常平坦的相关值分布。

关键词　Jacobi 序列，孪生素数序列，自相关函数，互相关函数

New Binary Modified Jacobi Sequences with Low Correlation Values

YAN Tong-Jiang[1,2]　XIAO Guo-Zhen[1]
(ISN National Key Laboratory, Xidian University, Xi'an 710071)[1]
(Institute of Mathematics and Computer Science, China University of Petroleum, Dongying 257061)[2]

Abstract　By means of the method to form binary Jacobi sequences, many new binary sequences are obtained from Jacobi sequences with arbitrary original points. Applying the equations related to the sums of Legendre characteristic functions, we get the autocorrelation values of one class of these new sequences and the cross-correlation values of each of them with each sequence from other classes on certain conditions. The results show that these values may be very low and distributed flatly under certain conditions.

Keywords　Jacobi sequences, Twin primes, Autocorrelation, Cross-correlation

伪随机序列在超声波探测、仿生、软件测试、全球定位系统、CDMA、雷达系统、广谱通信系统以及流密码中有着广泛的应用。在诸多应用中，所需要的序列集都应该具有以下两条性质：

1)序列集中的每一个序列应该易于和其自身的移位序列项区别；

2)序列集中的每一个序列应该易于和这个集合中的其它序列以及它们的移位序列相区别。

这两个性质分别要求序列具有低的周期自相关函数值和互相关函数值。对于一个周期为 n 的二元序列 $\{s(i)\}$，其周期自相关函数定义为

$$A_s(\omega)=\frac{1}{n}\sum_{i=1}^{n}(-1)^{s_i+s_{i+\omega}},0\leqslant\omega<n$$

函数

$$C_{s,t}(\omega)=\frac{1}{n}\sum_{i=1}^{n}(-1)^{s_i+t_{i+\omega}}(0\leqslant\omega<n)$$

称为 $\{s(i)\}$ 与另一个同周期序列 $\{t(i)\}$ 的周期互相关函数。具有平坦的低互相关值分布的序列信号具有很强的抗干扰能力。

1　问题的提出

令 p 和 q 是两个不同的素数，$N=pq$，

$P=\{p,2p,\cdots,(q-1)p\}$

$Q_0=\{0,q,2q,\cdots,(p-1)q\}$

修改的 Jacobi 序列(MJS)[1]又称为互素序列或 Whiteman 广义割圆序列[2]，它的定义可由式(1)给出。显然，它是由起点为 0 的 Jacobi 序列[3]经过简单的修改得到，而且包括著名的孪生素数序列。研究表明，这类序列具有高的线性复杂度、低的周期自相关值和互相关值以及很好的平衡性质[2]。本文指出，如果对于非零起点的 Jacobi 序列做类似的修改，得到的序列依然具有平坦的低相关值分布。既然一个序列和它的转移序列具有同样的相关性质，我们不妨只研究由(2)式给出的序列，记之为 $NMJS$。

$$s_i=\begin{cases}1, & \text{如果 } i \bmod N\in P\\ 0, & \text{如果 } i \bmod N\in Q_0\\ \left(1-\left(\frac{i}{p}\right)\left(\frac{i}{q}\right)\right)/2, & \text{否则}\end{cases}\tag{1}$$

$$s_i=\begin{cases}1, & \text{如果 } i\in P\\ 0, & \text{如果 } i=0 \text{ 或}(i+a)\in Q_0\\ & \text{并且 } i\notin P\\ \left(1-\left(\frac{i}{p}\right)\left(\frac{i+a}{q}\right)\right)/2, & \text{否则}\end{cases}\tag{2}$$

其中的$\left(\frac{\cdot}{\cdot}\right)$表示 Legendre 符号函数：

$$\left(\frac{i}{p}\right)=\begin{cases}1, & \text{如果 } i \text{ 是 } p \text{ 的二次剩余}\\ -1, & \text{如果 } i \text{ 是 } p \text{ 的二次非剩余}\\ 0, & \text{如果 } i=0\end{cases}$$

本文只讨论 $a=1$ 的情形。

2　主要结果

引理 1[4]

(1) $\sum_{i\in Z_p}\left(\frac{i}{p}\right)=0$，

*)国家自然科学基金项目(60473028)和 973 项目(G1999035804)。闫统江　博士研究生，讲师，主要研究方向为密码学；肖国镇　博士生导师，教授，主要研究方向为密码学和信息编码理论。

(2) $\sum_{i\in Z_p}\left(\frac{i}{p}\right)\left(\frac{1+\omega}{p}\right)=-1,\omega\in Z_p^*$,

(3) $\sum_{i\in Z_N}\left(\frac{i}{p}\right)\left(\frac{1+\omega}{p}\right)\left(\frac{i}{q}\right)\left(\frac{i+\omega}{q}\right)=1,\omega\in Z_N^*$。

由引理1的(1)和(2)可得

引理2

(1) $\sum_{i\in P}\left(\frac{i+\omega}{q}\right)=-\left(\frac{\omega}{q}\right)$,

(2) $\sum_{i\in P}\left(\frac{i+a}{q}\right)\left(\frac{i+a+\omega}{q}\right)=-1-\left(\frac{a}{q}\right)\left(\frac{a+\omega}{q}\right)$,

$\omega\in Z_q^*$。

引理3

$|(Q_0+a)\cap P|=1$

其中 $1\leqslant a\leqslant q-1$。

证明：由于 p 和 q 互素，对于任意的 $a(1\leqslant a\leqslant q-1)$，都存在惟一的整数对 (u,v)，使得

$up+vq=a, u \bmod q\neq 0, v\in Z_p$

从而可得引理的结论。

定理1 当 $a=1$ 时，NMJS的自相关

$$|A_s(\omega)|\leqslant\frac{\delta}{N}$$

这里 $\delta=\max\{q-p+4,8\}$。

注：由定理1的结论可以得到：当 $q-p$ 足够小时，NMJS具有非常平坦的低的自相关值分布，所以可以选择 p 和 q 为孪生素数。

证明：由NMJS的定义，即(2)式，可得

$$(-1)^{s_i}=\begin{cases}-1, & \text{如果 } i\in P\\ 1, & \text{如果 } i=0\\ & \text{或}(i+1)\in Q_0 \text{ 并且 } i\notin P;\\ \left(\frac{i}{p}\right)\left(\frac{i+1}{q}\right), & \text{否则}\end{cases}\tag{3}$$

如果 $\omega\in P$，由引理3和(3)式可得

$$(-1)^{s_i+s_{i+\omega}}=\begin{cases}1, & \text{如果 } i\in P\backslash\{N-\omega\}\\ -1, & \text{如果 } i\in\{N-\omega,0\}\\ \left(\frac{i}{p}\right)\left(\frac{\omega}{q}\right), & \text{如果}(i+1)\in Q_0,\\ & \text{且 } i\notin P\\ \left(\frac{i}{p}\right)\left(\frac{-\omega}{q}\right), & \text{如果}(i+\omega+1)\in Q_0,\\ & \text{且 } i+\omega\notin P\\ \left(\frac{i+1}{q}\right)\left(\frac{i+1+\omega}{q}\right), & \text{否则}\end{cases}\tag{4}$$

由引理1～3和(4)式可得

$$\begin{aligned}NA_s(\omega)&=q-2-2+\left(\frac{\omega}{q}\right)\sum_{i+1\in Q_0}\left(\frac{i}{p}\right)+\left(\frac{-\omega}{q}\right)\sum_{\substack{i+1+\omega\in Q_0\\ i+\omega\notin P}}\left(\frac{i}{p}\right)+\sum_{i\notin P\cup\{0\}}\left(\frac{i+1}{q}\right)\left(\frac{i+1+\omega}{q}\right)\\ &=q-4+\left(\frac{\omega}{q}\right)\sum_{u\in Z_p}\left(\frac{u}{p}\right)+\left(\frac{-\omega}{q}\right)\sum_{u\in Z_p}\left(\frac{u}{p}\right)\\ &\quad+\sum_{u\in Z_{pq}}\left(\frac{u}{q}\right)\left(\frac{u+\omega}{q}\right)\\ &\quad-\sum_{i\in P\cup\{0\}}\left(\frac{i+1}{q}\right)\left(\frac{i+1+\omega}{q}\right)\\ &=q-4+p\sum_{u\in Z_q}\left(\frac{u}{q}\right)\left(\frac{u+\omega}{q}\right)-(-1)\\ &=q-p-3\end{aligned}$$

如果 $\omega\in Q$，那么 $\omega+1,\omega-1\notin Q_0$，由引理3和(3)式可得

$$(-1)^{s_i+s_{i+\omega}}=\begin{cases}1, & \text{如果}(i+1)\in Q_0\\ & \text{且 } i,i+\omega\notin P\\ \left(\frac{\omega}{p}\right)\left(\frac{\omega+1}{q}\right), & \text{如果 } i=0\\ -\left(\frac{\omega}{p}\right)\left(\frac{i+1}{q}\right), & \text{如果 } i\in P\\ -\left(\frac{-\omega}{p}\right)\left(\frac{i+1}{q}\right), & \text{如果}(i+\omega)\in P\\ \left(\frac{i}{p}\right)\left(\frac{i+\omega}{p}\right), & \text{否则}\end{cases}\tag{5}$$

根据引理1～3和(5)式，我们有

$$\begin{aligned}NA_s(\omega)&=p-2+\left(\frac{\omega}{p}\right)\left(\frac{\omega+1}{q}\right)-\left(\frac{\omega}{p}\right)\sum_{i\in P}\left(\frac{i+1}{q}\right)\\ &\quad-\left(\frac{-\omega}{p}\right)\sum_{i+\omega\in P}\left(\frac{i+1}{q}\right)+\sum_{i+1\notin Q_0}\left(\frac{i}{p}\right)\left(\frac{i+\omega}{p}\right)\\ &=p-2+\left(\frac{\omega}{p}\right)\left(\frac{\omega+1}{q}\right)+\left(\frac{\omega}{p}\right)\left(\frac{1}{q}\right)-\left(\frac{-\omega}{p}\right)\left(\frac{1-\omega}{q}\right)+\sum_{i\in Z_{pq}}\left(\frac{i}{p}\right)\left(\frac{i+\omega}{p}\right)-\sum_{u\in Z_p}\left(\frac{u}{p}\right)\left(\frac{u+\omega}{p}\right)\\ &=p-2+\left(\frac{\omega}{p}\right)\left(\frac{\omega+1}{q}\right)-\left(\frac{\omega}{p}\right)\\ &\quad-\left(\frac{\omega}{p}\right)\left(\frac{-1}{p}\right)\left(\frac{1-\omega}{q}\right)-q-(-1)\\ &=p-q-1+\left(\frac{\omega}{p}\right)\\ &\quad\left(1+\left(\frac{\omega+1}{q}\right)-(-1)^{\frac{p+q}{2}}\left(\frac{\omega-1}{q}\right)\right)\end{aligned}$$

所以 $N|A_s(\omega)|\leqslant q-p+4$。

如果 $\omega\in Z_{pq}^*$ 且 $\omega+1,\omega-1\notin Q_0$，则由引理3和(3)式，我们有以下讨论：

①如果 $i\in P$ 且 $i+\omega+1\in Q_0$，或者 $i+\omega\in P$ 且 $i+1\in Q_0$，则

$(-1)^{s_i+s_{i+\omega}}=-1$

②如果 $i\in P$ 且 $i+\omega+1\notin Q_0$，则

$(-1)^{s_i+s_{i+\omega}}=-\left(\frac{\omega}{p}\right)\left(\frac{i+\omega+1}{q}\right)$

③如果 $i+\omega\in P$ 且 $i+1\notin Q_0$，则

$(-1)^{s_i+s_{i+\omega}}=-\left(\frac{-\omega}{p}\right)\left(\frac{i+1}{q}\right)$

④如果 $i+1\in Q_0$ 且 $i,i+\omega\notin P$，则

$(-1)^{s_i+s_{i+\omega}}=\left(\frac{i+\omega}{p}\right)\left(\frac{\omega}{q}\right)$

⑤如果 $(i+\omega+1)\in Q_0$ 且 $i,i+\omega\notin P$，则

$(-1)^{s_i+s_{i+\omega}}=\left(\frac{i}{p}\right)\left(\frac{-\omega}{q}\right)$

⑥如果 $i=0$，则

$(-1)^{s_i+s_{i+\omega}}=\left(\frac{\omega}{p}\right)\left(\frac{\omega+1}{q}\right)$

⑦如果 i 不属于以上6种情形，则

$(-1)^{s_i+s_{i+\omega}}=\left(\frac{i}{p}\right)\left(\frac{i}{q}\right)\left(\frac{i+\omega}{p}\right)\left(\frac{i+\omega}{q}\right)$

于是我们可得到

$$\begin{aligned}&NA_s(\omega)\\ &=-2-\left(\frac{\omega}{p}\right)\sum_{i\in P}\left(\frac{i+\omega+1}{q}\right)-\left(\frac{-\omega}{p}\right)\sum_{i+\omega\in P}\left(\frac{i+1}{q}\right)\end{aligned}$$

$$+\left(\frac{\omega}{q}\right)\sum_{\substack{i+1\in Q_0\\ i\notin P}}\left(\frac{i+\omega}{p}\right)+\left(\frac{-\omega}{q}\right)\sum_{\substack{i+\omega+1\in Q_0\\ i+\omega\notin P}}\left(\frac{i}{p}\right)$$

$$+\left(\frac{\omega}{p}\right)\left(\frac{\omega+1}{q}\right)+\sum_{\substack{i+1\notin Q_0\\ i+\omega+1\notin Q_0}}\left(\frac{i}{p}\right)\left(\frac{i}{q}\right)\left(\frac{i+\omega}{p}\right)\left(\frac{i+\omega}{q}\right)$$

$$=-2+\left(\frac{\omega}{p}\right)\left(\frac{\omega+1}{q}\right)+\left(\frac{-\omega}{p}\right)\left(\frac{1-\omega}{q}\right)-\left(\frac{\omega}{q}\right)\left(\frac{\omega}{p}\right)$$

$$-\left(\frac{-\omega}{q}\right)\left(\frac{-\omega}{p}\right)+\left(\frac{\omega}{p}\right)\left(\frac{\omega+1}{q}\right)+1$$

$$-\sum_{i+1\in Q_0}\left(\frac{i}{p}\right)\left(\frac{i}{q}\right)\left(\frac{i+\omega}{p}\right)\left(\frac{i+\omega}{q}\right)$$

$$-\sum_{i+\omega+1\in Q_0}\left(\frac{i}{p}\right)\left(\frac{i}{q}\right)\left(\frac{i+\omega}{p}\right)\left(\frac{i+\omega}{q}\right)$$

$$=-2+\left(\frac{\omega}{p}\right)\left(\frac{\omega+1}{q}\right)+\left(\frac{-\omega}{p}\right)\left(\frac{1-\omega}{q}\right)-\left(\frac{\omega}{q}\right)\left(\frac{\omega}{p}\right)$$

$$-\left(\frac{-\omega}{q}\right)\left(\frac{-\omega}{p}\right)+\left(\frac{\omega}{p}\right)\left(\frac{\omega+1}{q}\right)+1$$

$$+\left(\frac{1-\omega}{q}\right)+\left(\frac{1+\omega}{q}\right)$$

$$=-1+\left(\frac{\omega+1}{q}\right)\left(1+2\left(\frac{\omega}{p}\right)\right)+\left(\frac{1-\omega}{q}\right)\left(1+\left(\frac{-\omega}{p}\right)\right)$$

$$-\left(\frac{\omega}{q}\right)\left(\frac{\omega}{p}\right)(1-(-1)^{\frac{p+q}{2}})$$

从而 $N|A_s(\omega)|\leqslant 8$。

如果 $\omega\in Z_{pq}^*$ 且 $\omega-1\in Q_0$，那么 $\omega-1\notin Q_0$。根据引理 3 和(3)式，我们有以下讨论：

①如果 $i+\omega\in P$ 且 $i+1\in Q_0$，则

$(-1)^{s_i+s_{i+\omega}}=-1$

②如果 $i\in P$，则

$(-1)^{s_i+s_{i+\omega}}=-\left(\frac{\omega}{p}\right)\left(\frac{i}{q}\right)$

③如果 $(i+\omega)\in P$ 且 $i+1\notin Q_0$，则

$(-1)^{s_i+s_{i+\omega}}=-\left(\frac{-\omega}{p}\right)\left(\frac{i+1}{q}\right)$

④如果 $(i+1)\in Q_0$ 且 $i,i+\omega\notin P$，则

$(-1)^{s_i+s_{i+\omega}}=\left(\frac{i+\omega}{p}\right)\left(\frac{-1}{q}\right)$

⑤如果 $i\in Q_0$ 且 $i+\omega\notin P$，则

$(-1)^{s_i+s_{i+\omega}}=\left(\frac{i}{p}\right)$

⑥如果 $i=0$，则

$(-1)^{s_i+s_{i+\omega}}=1$

⑦如果 i 不属于以上任意一种情形，则

$(-1)^{s_i+s_{i+\omega}}=\left(\frac{i}{p}\right)\left(\frac{i}{q}\right)\left(\frac{i+\omega}{p}\right)\left(\frac{i-1}{q}\right)$

基于以上的讨论，我们有

$$NA_s(\omega)$$

$$=-1-\left(\frac{\omega}{p}\right)\sum_{i\in P}\left(\frac{i}{q}\right)-\left(\frac{-\omega}{p}\right)\sum_{i+\omega\in P}\left(\frac{i+1}{q}\right)$$

$$+\left(\frac{-1}{q}\right)\sum_{\substack{i+1\in Q_0\\ i\notin P}}\left(\frac{i+\omega}{p}\right)+\sum_{\substack{i\in Q_0\\ i+\omega\notin P}}\left(\frac{i}{p}\right)+1$$

$$+\sum_{i+1\notin Q_0}\left(\frac{i}{p}\right)\left(\frac{i}{q}\right)\left(\frac{i+\omega}{p}\right)\left(\frac{i-1}{q}\right)$$

$$=-\left(\frac{-\omega}{p}\right)\left(\frac{1-\omega}{q}\right)-\left(\frac{-1}{q}\right)\left(\frac{\omega}{p}\right)$$

$$-\left(\frac{-\omega}{p}\right)+1+\left(\frac{2}{q}\right)$$

所以 $N|A_s(\omega)|\leqslant 5$。

如果 $\omega\in Z_{pq}^*$ 且 $\omega-1\in Q_0$，那么 $\omega+1\notin Q_0$。根据引理 3 和(3)式，我们有以下讨论：

①如果 $i\in P$ 且 $i+\omega+1\in Q_0$，则

$(-1)^{s_i+s_{i+\omega}}=-1$

②如果 $i\in P$ 且 $i+\omega+1\notin Q_0$，则

$(-1)^{s_i+s_{i+\omega}}=-\left(\frac{\omega}{p}\right)\left(\frac{i}{q}\right)$

③如果 $i+\omega\in P$，则

$(-1)^{s_i+s_{i+\omega}}=-\left(\frac{-\omega}{p}\right)\left(\frac{i+1}{q}\right)$

④如果 $i+1\in Q_0$ 且 $i\notin P$，则

$(-1)^{s_i+s_{i+\omega}}=\left(\frac{i+\omega}{p}\right)$

⑤如果 $i+\omega+1\in Q_0$ 且 $i,i+\omega\notin P$，则

$(-1)^{s_i+s_{i+\omega}}=\left(\frac{i}{p}\right)\left(\frac{-1}{q}\right)$

⑥如果 $i=0$，则

$(-1)^{s_i+s_{i+\omega}}=\left(\frac{\omega}{p}\right)\left(\frac{2}{q}\right)$

⑦如果 i 不属于以上任意一种情形，则

$(-1)^{s_i+s_{i+\omega}}=\left(\frac{i}{p}\right)\left(\frac{i}{q}\right)\left(\frac{i+\omega}{p}\right)\left(\frac{i+1}{q}\right)$

由以上的讨论和引理 1～3，我们得到

$$NA_s(\omega)$$

$$=-1-\left(\frac{\omega}{p}\right)\sum_{\substack{i\in P\\ i+\omega+1\notin Q_0}}\left(\frac{i}{q}\right)-\left(\frac{-\omega}{p}\right)\sum_{i+\omega\in P}\left(\frac{i+1}{q}\right)$$

$$+\sum_{\substack{i+1\in Q_0\\ i\notin P}}\left(\frac{i+\omega}{p}\right)+\left(\frac{-1}{q}\right)\sum_{\substack{i+\omega+1\in Q_0\\ i+\omega\notin P}}\left(\frac{i}{p}\right)+\left(\frac{\omega}{p}\right)\left(\frac{2}{q}\right)$$

$$+\sum_{i+\omega+1\notin Q_0}\left(\frac{i}{p}\right)\left(\frac{i}{q}\right)\left(\frac{i+\omega}{p}\right)\left(\frac{i+\omega}{q}\right)$$

$$=-1-\left(\frac{\omega}{p}\right)\left(\frac{-2}{q}\right)-\left(\frac{\omega}{p}\right)-\left(\frac{-1}{q}\right)\left(\frac{-\omega}{p}\right)$$

$$-\left(\frac{\omega}{p}\right)\left(\frac{2}{q}\right)+1+\left(\frac{2}{q}\right)$$

$$=-\left(\frac{\omega}{p}\right)\left(\frac{2}{q}\right)\left(\frac{-1}{q}\right)-\left(\frac{\omega}{p}\right)-\left(\frac{-1}{q}\right)\left(\frac{-1}{p}\right)\left(\frac{\omega}{p}\right)$$

$$-\left(\frac{\omega}{p}\right)\left(\frac{2}{q}\right)+\left(\frac{2}{q}\right)$$

从而 $N|A_s(\omega)|\leqslant 5$。

由以上的讨论可得定理的结论。

为方便起见，令 $\{s_i^a\}$ 表示起点为 a 的 NMJS。我们考虑 $\{s_i^1\}$ 和 $\{s_i^a\}$ 的无转移的互相关性质。

定理 2 NMJS 的互相关函数

$$C_{s_i^1,s_i^a}(0)=\begin{cases}1, & \text{如果 } a=1\\ \dfrac{q-p+1}{N}, & \text{如果 } a\neq 1\end{cases}$$

证明：在 $a=1$ 时，结论是显然的。因为 $0\leqslant a\leqslant q-1$，则在 $a\neq 1$ 时，$i+1\in Q_0$ 和 $i+a\in Q_0$ 不能同时成立。所以我们根据(3)式可得

$$(-1)^{s_j^1+s_i^a}=\begin{cases}1, & \text{如果 } i\in P\cup\{0\}\\ \left(\frac{i}{p}\right)\left(\frac{i+a}{q}\right), & \text{如果 } i+1\in Q_0 \text{ 且 } i\notin P\\ \left(\frac{i}{p}\right)\left(\frac{i+1}{q}\right), & \text{如果 } i+a\in Q_0 \text{ 且 } i\notin P\\ \left(\frac{i+1}{q}\right)\left(\frac{i+a}{q}\right), & \text{否则}\end{cases}$$

（下转第 49 页）

53 Lipmaa H, Asokan N, Niemi V. Secure Vickrey auctions without threshold trust. In: M. Blaze, ed. Proc. of 6th FC Conference, volume 2357 of LNCS. Springer, 2002
54 Shneidman J, Parkes D C. Specification Faithfulness in Networks with Rational Nodes. In: Twenty-Third Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC 2004), July 2004
55 Shneidman J, Parkes D C, Massoulie L. Faithfulness in Internet algorithms. In: Proceedings of the ACM SIGCOMM workshop on Practice and theory of incentives in networked systems Sep. 2004
56 Phelps S, McBurney P, Parsons S, Sklar E. Applying genetic programming to economic mechanism design: evolving a pricing rule for a continuous double auction. In: Proceedings of the second international joint conference on Autonomous agents and multi agent systems. Jul. 2003
57 Conitzer V, Sandholm T. Automated mechanism design for a self-interested designer. In: Proceedings of the 4th ACM Conference on Electronic Commerce. Jun. 2003
58 Conitzer V, Sandholm T. Applications of automated mechanism design. In: Proceedings of the UAI Bayesian Modeling Applications Workshop, Acapulco, Mexico, 2003
59 Nisan N, Segal I. The communication requirements of efficient allocations and supporting prices. Journal of Economic Theory, 2006. Forthcoming. http:// www. stanford. edu/~ isegal/prices. pdf
60 Larson K, Sandholm T. Mechanism design and deliberative agents. In: Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems Jul. 2005

(上接第 19 页)

再根据引理 1～3，我们有

$$NC_{s_i^1,s_i^a}(0)$$
$$=q+\sum_{i\notin P_0}\left(\frac{i+1}{q}\right)\left(\frac{i+a}{q}\right)+\sum_{\substack{i+1\in Q_0\\ i\notin P}}\left(\frac{i}{p}\right)\left(\frac{i+a}{q}\right)$$
$$+\sum_{\substack{i+a\in Q_0\\ i\notin P}}\left(\frac{i}{p}\right)\left(\frac{i+a}{q}\right)$$
$$=q+\left(\frac{-1+a}{q}\right)-\sum_{i+1\in Q_0}\left(\frac{i}{p}\right)+\left(\frac{-a+1}{q}\right)\sum_{i+a\in Q_0}\left(\frac{i}{p}\right)$$
$$-p-\sum_{i\in P_0}\left(\frac{i+1}{q}\right)\left(\frac{i+a}{q}\right)$$
$$=q-p+1。$$

所以，当素数 p 和 q 恒定时，序列$\{s_i^1\}$和其它任意一个NMJS具有同样的无转移互相关值，这个值在 p 和 q 为孪生素数时取得最小。

对于任意非零的 ω，如果 $A_s(\omega)=C_{a,b}(\omega)=\frac{-1}{n}$，则称$\{s(i)\}$具有理想的相关值分布。实际上，满足这样的条件是非常困难的。对于密钥流序列，只要它们的相关值的分布相对比较平坦就可以了。为满足密钥流序列大周期的需要，本文中的 p 和 q 的取值都比较大(大于 48 比特)。由定理 1 和 2 可知，这时的相关值分布是非常平坦的。具有平坦的低相关值分布的序列也具有平坦的二元段(run)分布，其对应的密码函数也具有平坦的差分分布和高的非线性度[1]。从而，这种序列若作为密钥流，则具有很强的抗差分攻击的能力[1]。

结束语 笔者新设计了大量的二元序列，并给出了其中一类序列的自相关值以及它与其它类的序列在无转移情况下的互相关值。结果表明，这类序列在一定条件具有非常平坦的低相关值分布，并且这种分布是可控的。这类序列的实现方法和修改的 Jacobi 序列[2]非常类似。如果考虑这些序列在流密码中的应用，线性复杂度及游程分布等性质有待进一步研究。

参 考 文 献

1 Green D H, Green P R, Modified Jacobi sequences [J]. In: IEE Proc. Comput Dig Tech, July 2000, 147 (4): 241～251
2 Cusick T, Ding Cunsheng, Renvall A. Stream Ciphers and Number Theory [M]. North-Holland Mathematical Library 66. Elsevier Science Pub Co, April 1, 1998
3 Damgard I B. On the Randomness of Legendre and Jacobi Sequences [A]. In: Advances in Cryptograpy-CRYPTO' 88, LNCS403 [C]. Berlin: Springer-Verlag, 1990. 163～172
4 Brandstatter N, Winterhof A. Some Notes on the Two-prime Generator of Order 2 [J]. IEEE Trans Inf Theory, October 2005, 151(10): 3654～3657

(上接第 43 页)

6 Lee S C, Shields C. Tracing the Source of Network Attack: A Technical, Legal and Societal Problem[A]. In: Proceedings of the 2001 IEEE Workshop on Information Assurance and Security [C], 2001. 239～246
7 Stone R. CenterTrack: An IP Overlay Network for Tracking DoS Floods[A]. In: Proceedings of USENIX Security Symposium[C], 2000
8 Ferguson P, Senie D. Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing (RFC 2827). The Internet Society, 2000
9 Global Incident Analysis Center. Special Notice - Egress filtering. http://www. sans. org/y2k/egress. htm.
10 Dean D, Franklin M, Stubblefield A. An Algebraic Approach to IP Traceback[A]. In: Proceedings of the Network and Distributed System Security Symposium(NDSS)[C], 2001, 2: 119～137
11 Song Xiaodong, Perrig A. Advanced and Authenticated Marking Schemes for IP Traceback[A]. In: Proceedings of IEEE INFOCOMM[C], 2001. 878～886
12 Snoeren A C, Partridge C, Sanchez L A, et al. Hash-based IP Traceback[A]. In: Proceeding of SIGCOMM[C], 2001, 8: 3～14
13 Cheswick B, Burch H, Branigan S. Mapping and Visualizing the Internet[A]. In: Proceedings of USENIX Annual Technical Conference[C], 2000
14 Floyd S, Paxson V. Difficulties in Simulating the Internet. IEEE/ACM Transactions on Networking, 2001, 9(4): 392～403
15 Snoeren A C, Partridge C, Sanchez L A, et al. Hash-based IP Traceback[A]. In: Proceeding of SIGCOMM[C], 2001, 8: 3～14
16 Hastings J R. Incremental Bayesian Segmentation for Intrusion Detection: [Maseter's Thesis]. Massachusetts Institue of Technology, 2003
17 Park K, Lee Heejo. On the Effectiveness of Probabilistic Packet Marking for IP Traceback Under Denial of Service Attack[A]. In: Proceedings of IEEE INFOCOM[C], 2001. 338～347
18 徐永红. Internet 拥塞控制/信息可用性技术研究: [学位论文]. 南京理工大学, 2002
19 Sanchez L A, Milliken W C, Snoeren A C, et al. Hardware Support for a Hash-based IP Traceback[A]. In: Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEXII)[C], 2001. 146～152
20 Bellovin S. The ICMP Traceback Message. Internet Draft, IETF, March 2000