双素数 Sidel'nikov 序列的自相关函数

岳 墨*① 高军涛①② 谢 佳①
①(西安电子科技大学综合业务网理论及关键技术国家重点实验室 西安 710071)
②(中国科学院信息工程研究所 北京 100093)

摘 要：Brandstätter 等人(2011)结合割圆序列与 Sidel'nikov 序列的概念定义了一个新序列 —— 双素数(p,q) Sidel'nikov 序列，并且分析了双素数 Sidel'nikov 序列的均衡性、自相关函数、相关测度和线性复杂度轮廓，证明了双素数 Sidel'nikov 序列有好的伪随机特性。该文主要研究 $d=\gcd(p,q)=2$ 的双素数 Sidel'nikov 序列的自相关函数，借助于数论中的 Legendre 符号和有限域中的指数和理论，得到自相关函数的 3 个定理。通过与 Brandstätter 论文中自相关函数的界进行比较，本文定理 2 和定理 3 中的界 $O(q^{1/2})$和 $O(p^{1/2})$比 Brandstätter 的界 $O((p+q)/2)$更紧，同时当 $p>>q$ 或 $q>>p$ 时，本文定理 4 中的界 $O((p\ q)^{1/2})$比 Brandstätter 的界 $O((p+q)/2+(p\ q)^{1/2})$更优。

关键词：双素数 Sidel'nikov 序列；自相关函数；Legendre 符号；指数和
中图分类号：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2013)11-2602-06
DOI: 10.3724/SP.J.1146.2013.00147

Autocorrelation of the Two-prime Sidel'nikov Sequence

Yue Zhao① Gao Jun-tao①② Xie Jia①
①(*The State Key Laboratory of Integrated Services Network*, *Xidian University*, *Xi'an* 710071, *China*)
②(*Institute of Information Engineering*, *Chinese Academy of Sciences*, *Beijing* 100093, *China*)

Abstract: Brandstätter *et al.* (2011) combined the concepts of the two-prime generator and Sidel'nikov sequence to define a new sequence called two-prime (p, q) Sidel'nikov sequence, and analyzed the balance, the autocorrelation, the correlation measure and the linear complexity profile of the sequence. They showed that this sequence has many nice pseudorandom properties. With the help of the Legendre symbol in number theory and the exponential sums in finite field, this paper investigates the autocorrelation of the two-prime Sidel'nikov sequence with $d=\gcd(p, q)=2$. Three theorems are got about the autocorrelation functions. The detailed comparison results show that the bounds $O(q^{1/2})$ and $O(p^{1/2})$ on the autocorrelation function in theorem 2 and theorem 3 are tighter than the Brandstätter's bound $O((p+q)/2)$, besides, the bound $O((p\ q)^{1/2})$ in theorem 4 are tighter than the Brandstätter's bound $O((p+q)/2+(p\ q)^{1/2})$ when $p>>q$ or $q>>p$.

Key words: Two-prime Sidel'nikov sequence; Autocorrelation function; Legendre symbol; Exponential sums

1 引言

Sidel'nikov[1]构造了一类均衡的二元序列 —— Sidel'nikov 序列，并且证明了这种序列具有最优的自相关函数。Lempel 等人[2]独立地使用有限域理论构造了一类均衡的有最优的自相关性质的二元序列 —— Sidel'nikov 序列。Su 等人[3,4]用周期为 p 的 Legendre 序列和周期为 $q-1$ 的 Sidel'nikov 序列构造了一类新的周期为 $p(q-1)$ 的均衡序列 —— Legendre-Sidel'nikov 序列，对任意的奇素数 p 和一个奇素数的任意幂次 q，满足 p 和 $q-1$ 互素，给出了周期自相关函数的精确值、非周期自相关函数的一个较紧的界、相关测度和线性复杂度轮廓，证明了这个新序列具有好的伪随机性。文献[5]使用特征把 Legendre-Sidel'nikov 序列推广到 d 元广义的 Legendre-Sidel'nikov 序列。文献[6]结合 Sidel'nikov 序列和割圆序列的概念定义了一个新序列 —— 双素数 Sidel'nikov 序列。这个新序列在 $d=2$ 且 $p\equiv q\equiv 3 \bmod 4$ 的情况下是均衡的。同时给出了双素数 Sidel'nikov 序列自相关函数的一个界、相关测度和线性复杂度轮廓，证明了这个新序列有好的伪随机性质。

但文献[6]中给出的双素数 Sidel'nikov 序列自相关函数并不是最优的，本文主要是基于数论中 Legendre 符号和有限域中指数和理论研究了 $d=2$

2013-01-25 收到，2013-05-20 改回
国家自然科学基金(60833008)，中央高校基本科研业务费(K50511010007, K5051270003)和中国科学院信息工程研究所信息安全国家重点实验室开放课题基金资助
*通信作者：岳墨 yuezhao1020@163.com

时双素数 Sidel'nikov 序列的自相关函数。给出了 $d=2$ 时双素数 Sidel'nikov 序列自相关函数的 3 个定理。用 C++模拟数据并且和文献[6]中给出的自相关函数的界(定理 1)进行比较，当 $l\equiv 0 \bmod (p-1)$ 和 $l\equiv 0 \bmod (q-1)$，本文中的界 $O(q^{1/2})$ 和 $O(p^{1/2})$ 比定理 1 中的界 $O((p+q)/2)$ 要优；当 $l\not\equiv 0 \bmod (p-1)$ 且 $l\not\equiv 0 \bmod (q-1)$ 并且 $p\gg q$ 或 $q\gg p$ 时，本文定理 4 中的界 $O(p^{1/2}q^{1/2})$ 比定理 1 中的界 $O((p+q)/2+\sqrt{pq})$ 要优。

2　预备知识

定义 1　设 F_p 表示阶数为 p 的有限域，g 是 F_p 的一个本原元。$\forall i\geq 0$，当 $\left(\frac{g^i+1}{p}\right)=-1$ 时，定义 $c_i=1$，其它情况 $c_i=0$。其中 $[\cdot]$ 是 Legendre 符号，$c=c_0c_1c_2\cdots$ 称为 Sidel'nikov 序列[1,2]。

定义 2　设 p 和 q 是两个不同的奇素数，定义 $Q=\{q,2q,\cdots,(p-1)q\}$, $Q_0=Q\cup\{0\}$ 并且 $P=\{p,2p,\cdots,(q-1)p\}$。当 $(i \bmod pq)\in Q_0$ 时，$a_i=0$；当 $(i \bmod pq)\in P$ 时，$a_i=1$；其它情况

$$a_i=\left(1-\left(\frac{i}{p}\right)\left(\frac{i}{q}\right)\right)\Big/2$$

$a=a_0a_1a_2\cdots$ 称为割圆序列[7,8]。

定义 3[9]　设 $F_p=\{0,1,\cdots,p-1\}$，F_p^* 表示 F_p 的乘群。F_p 上的特征 χ 是指定义在 F_p^* 到复数域 $\mathbb{C}$ 内的一个映射，满足：对所有 $a,b\in F_p^*,\chi(ab)=\chi(a)\chi(b)$, $\chi(1)\neq 0$。

定义 4[9]　设 χ 是 F_p 上的一个特征，$a\in F_p$，设 $g_a(\chi)=\sum_{t=0}^{p-1}\chi(t)\eta^{at}$，$\eta=e^{2\pi i/p}$，$g_a(\chi)$ 称为一个特征和。

在 F_2 上周期为 t 的 $s=s_0s_1s_2\cdots$ 的自相关函数定义为 $AC(s_i,l)=\sum_{i=0}^{t-1}(-1)^{s_{i+l}+s_i}$。如果该序列的自相关函数的绝对值比周期小得多，那么这个序列就具有较好的伪随机性。Sideli'nikov 序列[1,2]，割圆序列[10,11]和 Legendre-Sidel'nikov[3−5] 序列具有较优的自相关函数。

文献[6]结合 Sidel'nikov 序列和割圆序列的概念定义了一个新序列——双素数 Sidel'nikov 序列，并给出双素数 Sidel'nikov 序列的自相关函数的估计：

定义 5[6]　p 和 q 是两个不同的奇素数，g 是模 p 和模 q 的本原元。令 $Q=\{q,2q,\cdots,(p-1)q\}$，$Q_0=Q\cup\{0\}$ 和 $P=\{p,2p,\cdots,(q-1)p\}$。令 $d=\gcd(p-1,q-1)$ 和 $t=(p-1)(q-1)/d$。$\forall i\geq 0$，周期为 t 的双素数 Sidel'nikov 序列定义为：当 $(g^i+1)\bmod pq\in Q_0$ 时，$s_i=0$；当 $(g^i+1)\bmod pq\in P$ 时，$s_i=1$；当 $\gcd(g^i+1,pq)=1$ 时，

$$s_i=\left(1-\left(\frac{g^i+1}{p}\right)\left(\frac{g^i+1}{q}\right)\right)\Big/2$$

定理 1[6]　当 $d=2$ 时，双素数 Sidel'nikov 序列的自相关函数满足：

$$AC(s_n,l)=\begin{cases}O\left((p+q)/2\right), & l\equiv 0 \bmod (p-1)\text{或}l\equiv 0 \bmod (q-1)\\ O\left((p+q)/2+\sqrt{pq}\right), & l\not\equiv 0 \bmod (p-1)\text{且}l\not\equiv 0 \bmod (q-1)\end{cases}\quad 1<l<t$$

本文的主要工作是使用数论中 Legendre 符号和有限域中指数和的理论研究了 $d=2$ 时双素数 Sidel'nikov 序列的自相关函数，并给出了比定理 1 中的界更优的界。

3　自相关函数

首先给出 3 个定理，然后再给出它们的证明。

定理 2　当 $l\equiv 0 \bmod (p-1)$ 时，则双素数 Sidel'nikov 序列的自相关函数满足：

$$AC(s_i,l)=\frac{q-1}{2}-(p-2)+O\left(q^{1/2}\right)-\begin{cases}0, & p\equiv 1 \bmod 4\text{且}q\equiv 3 \bmod 4\\ 2\left(\frac{-g^l+1}{q}\right), & p\equiv 3 \bmod 4\text{且}q\equiv 1 \bmod 4\\ 3, & p\equiv q\equiv 3 \bmod 4\end{cases}$$

定理 3　当 $l\equiv 0 \bmod (q-1)$，则双素数 Sidel'nikov 序列的自相关函数满足：

$$AC(s_i,l)=\frac{p-1}{2}-(q-2)-O\left(p^{1/2}\right)-\begin{cases}0, & p\equiv 3 \bmod 4\\ 2\left(\frac{-g^l+1}{p}\right), & p\equiv 1 \bmod 4\end{cases}$$

定理 4　当 $l\not\equiv 0 \bmod (p-1)$ 且 $l\not\equiv 0 \bmod (q-1)$，则双素数 Sidel'nikov 序列的自相关函数满足：

(1)当 $p\equiv q\equiv 3 \bmod 4$ 时，有

$$AC(s_i,l)=O\left(p^{1/2}q^{1/2}\right)+\begin{cases}2\left(\frac{-g^l+1}{p}\right)-2\left(\frac{-g^l+1}{q}\right), & l\text{为奇数}\\ 0, & l\text{为偶数}\end{cases}$$

(2)当 $p\not\equiv q \bmod 4$ 时

(a) $p\equiv 1 \bmod 4$ 且 $q\equiv 3 \bmod 4$ 时，有

$$AC(s_i,l)=O\left(p^{1/2}q^{1/2}\right)+\begin{cases}(-2)-2\left(\dfrac{-g^l+1}{q}\right), & l\text{为奇数}\\ 2+2\left(\dfrac{-g^l+1}{p}\right), & l\text{为偶数}\end{cases}$$

(b) $p\equiv 3 \bmod 4$ 且 $q\equiv 1 \bmod 4$ 时，有

$$AC(s_i,l)=O\left(p^{1/2}q^{1/2}\right)+\begin{cases}2\left(\dfrac{-g^l+1}{p}\right)-2, & l\text{为奇数}\\ 2-2\left(\dfrac{-g^l+1}{q}\right), & l\text{为偶数}\end{cases}$$

为了完成定理的证明，我们需要下面几个引理：

引理 1 对任意的素数 p，有 $\sum_{x=0}^{p-1}\left(\dfrac{x}{p}\right)=0$。

证明 因为从 $1,2,\cdots,p-1$，有一半是 p 的二次剩余，另一半是 p 的二次非剩余，0 的 Legendre 符号为 0。

引理 2 对任意的素数 p，如果 $1\le a\le p-1$ 且 $p\nmid a$，有 $\sum_{x=0}^{p-1}\left(\dfrac{x}{p}\right)\left(\dfrac{x+a}{p}\right)=-1$。

证明 参阅文献[12]。

引理 3 令 ψ 是 F_p 中的阶为 $m>1$ 的乘法特征，f 是 $F_p(x)$ 中次数不为 m 的首一多项式。c 是 f 在 F_p 的分裂域中不同根的个数，对于任意的 $a\in F_p$，有

$$\left|\sum_{x\in F_p}\psi(af(x))\right|\le(c-1)p^{1/2}$$

证明 参阅文献[12]。

定理 2 的证明 首先证明当 $l\equiv 0 \bmod (p-1)$ 时，有下面的公式：

$$(-1)^{s_i+s_{i+l}}=\begin{cases}-1, & (g^i+1)\bmod pq=0,\ (g^{i+l}+1)\bmod pq\in P\\ \left(\dfrac{g^i+1}{p}\right)\left(\dfrac{-g^l+1}{q}\right), & (g^i+1)\bmod pq\in Q_0\\ -1, & (g^{i+l}+1)\bmod pq=0,\ (g^i+1)\bmod pq\in P\\ 1, & (g^i+1)\bmod pq\in P\\ \left(\dfrac{g^i+1}{p}\right)\left(\dfrac{g^i+1}{q}\right), & \gcd(g^i+1,pq)=1,\ (g^{i+l}+1)\bmod pq\in Q_0\\ \left(\dfrac{g^i+1}{q}\right)\left(\dfrac{g^{i+l}+1}{q}\right), & \gcd(g^i+1,pq)=1\end{cases}$$

当 $p\equiv q\equiv 3 \bmod 4$ 时，只有一个 i 满足 $(g^i+1)\bmod pq=0$ 且 $(g^{i+l}+1)\bmod pq\in P$，同时也只有一个 i 满足 $(g^{i+l}+1)\bmod pq=0$ 且 $(g^i+1)\cdot \bmod pq\in P$。因此有 $(p-1)/2$ 个 $i\equiv(q-1)/2\cdot \bmod(q-1)$ 使得 $(g^i+1)\bmod pq\in Q_0$ 并且有 $(q-3)/2$ 个 $i\equiv(q-1)/2 \bmod(q-1)$ 使得 $(g^i+1)\bmod pq\in P$。

当 $p\not\equiv q \bmod 4$ 时，$(g^i+1)\bmod pq=0,(g^{i+l}+1)\cdot \bmod pq\in P$ 和 $(g^{i+l}+1)\bmod pq=0,(g^i+1)\bmod pq\in P$ 这两项不成立，因此有 $(p-1)/2$ 个 i 使得 $(g^i+1)\bmod pq\in Q_0$ 并且有 $(q-1)/2$ 个 i 使得 $(g^i+1)\bmod pq\in P$。

因此，对于 $(g^i+1)\bmod pq\in Q_0$ 有

$$\sum_{(g^i+1)\bmod pq\in Q_0}\left(\frac{g^i+1}{p}\right)\left(\frac{-g^l+1}{q}\right)=\sum_{j=0}^{\frac{p-1}{2}-1}\left(\frac{g^{\frac{q-1}{2}+j(q-1)}+1}{p}\right)\left(\frac{-g^l+1}{q}\right)$$

当 $g^{j(q-1)}$ 跑遍 x 模 p 的二次剩余时，j 的值只能是 $0,1,\cdots,(p-3)/2$。由引理 1 和引理 2 有

$$\begin{aligned}&\sum_{(g^i+1)\bmod pq\in Q_0}\left(\frac{g^i+1}{p}\right)\left(\frac{-g^l+1}{q}\right)\\ &=\sum_{x=1}^{p-1}\left(\frac{g^{\frac{q-1}{2}}x+1}{p}\right)\left(\frac{-g^l+1}{q}\right)\left(1+\left(\frac{x}{p}\right)\right)\Big/2\\ &=\frac{1}{2}\left(\frac{-g^l+1}{q}\right)\\ &\quad\cdot\left(\underbrace{\sum_{x=1}^{p-1}\left(\frac{g^{\frac{q-1}{2}}x+1}{p}\right)}_{-1}+\left(\frac{g^{\frac{q-1}{2}}}{p}\right)\underbrace{\sum_{x=1}^{p-1}\left(\frac{x+g^{-\frac{q-1}{2}}}{p}\right)\left(\frac{x}{p}\right)}_{-1}\right)\\ &=-\frac{1}{2}\left(\frac{-g^l+1}{q}\right)\left(1+(-1)^{\frac{q-1}{2}}\right)\end{aligned}\tag{1}$$

同样地，对于 $\gcd(g^i+1,pq)=1,(g^{i+l}+1)\cdot \bmod pq\in Q_0$ 有式(2)成立

$$\begin{aligned}&\sum_{\substack{\gcd(g^i+1,pq)=1\\(g^{i+l}+1)\bmod pq\in Q_0}}\left(\frac{g^i+1}{p}\right)\left(\frac{g^i+1}{q}\right)\\ &=\sum_{j=0}^{\frac{p-1}{2}-1}\left(\frac{g^{\frac{q-1}{2}+j(q-1)-l}+1}{p}\right)\left(\frac{g^{\frac{q-1}{2}+j(q-1)-l}+1}{q}\right)\\ &=\sum_{j=0}^{\frac{p-1}{2}-1}\left(\frac{g^{\frac{q-1}{2}+j(q-1)}+1}{p}\right)\left(\frac{-g^{-l}+1}{q}\right)\\ &=-\frac{1}{2}\left(\frac{-g^{-l}+1}{q}\right)\left(1+(-1)^{\frac{q-1}{2}}\right)\end{aligned}\tag{2}$$

对于最后一个和式有

$$\begin{aligned}
&\sum_{\gcd(g^i+1,pq)=1}\left(\frac{g^i+1}{q}\right)\left(\frac{g^{i+l}+1}{q}\right)\\
&=\sum_{i=0}^{t-1}\left(\frac{g^i+1}{q}\right)\left(\frac{g^{i+l}+1}{q}\right)\\
&\quad-\sum_{(g^i+1)\bmod pq\in P}\left(\frac{g^i+1}{q}\right)\left(\frac{g^{i+l}+1}{q}\right)\\
&=\frac{p-1}{2}\sum_{i=0}^{q-2}\left(\frac{g^i+1}{q}\right)\left(\frac{g^{i+l}+1}{q}\right)\\
&\quad-\sum_{j=0}^{\frac{q-1}{2}-1}\left(\frac{g^{\frac{p-1}{2}+j(p-1)}+1}{q}\right)\left(\frac{g^{\frac{p-1}{2}+j(p-1)+l}+1}{q}\right)\\
&=-\frac{p-1}{2}\left(\left(\frac{g^l}{q}\right)+1\right)\\
&\quad-\sum_{x=1}^{q-1}\left(\frac{g^{\frac{p-1}{2}}x+1}{q}\right)\left(\frac{g^{\frac{p-1}{2}+l}x+1}{q}\right)\left(1+\left(\frac{x}{q}\right)\right)\Big/2\\
&=-\frac{p-1}{2}\left((-1)^l+1\right)\\
&\quad-\frac{1}{2}\left(\sum_{x=1}^{q-1}\left(\frac{g^{\frac{p-1}{2}}x+1}{q}\right)\left(\frac{g^{\frac{p-1}{2}+l}x+1}{q}\right)\right.\\
&\quad\left.+\sum_{x=1}^{q-1}\left(\frac{g^{\frac{p-1}{2}}x+1}{q}\right)\left(\frac{g^{\frac{p-1}{2}+l}x+1}{q}\right)\left(\frac{x}{q}\right)\right)\\
&=-\frac{p-1}{2}\left((-1)^l+1\right)+\frac{1}{2}\left((-1)^l+1\right)\\
&\quad-\frac{1}{2}(-1)^l\sum_{x=1}^{q-1}\left(\frac{x+g^{-\frac{p-1}{2}}}{q}\right)\left(\frac{x+g^{-\frac{p-1}{2}-l}}{q}\right)\left(\frac{x}{q}\right)
\end{aligned}$$

通过引理 3，这里的特征是二次特征(Legendre 符号)，这里的 f 是 $x\left(x+g^{-\frac{p-1}{2}}\right)\left(x+g^{-\frac{p-1}{2}-l}\right)$，其在 F_p 的分裂域中不同根的个数是 3。因此，我们有 $\left|\sum_{x=1}^{q-1}\left(\frac{x+g^{-\frac{p-1}{2}}}{q}\right)\left(\frac{x+g^{-\frac{p-1}{2}-l}}{q}\right)\left(\frac{x}{q}\right)\right|\le 2q^{1/2}$ 且 l 是偶数，所以有

$$\sum_{\gcd(g^i+1,pq)=1}\left(\frac{g^i+1}{q}\right)\left(\frac{g^{i+l}+1}{q}\right)=-(p-2)-O\left(q^{1/2}\right)\quad(3)$$

综上，由式(1)，式(2)和式(3)，当 $l\equiv 0\bmod(p-1)$ 时，双素数 Sidel'nikov 序列的自相关函数如定理 2 所述。　　证毕

定理 3 的证明　当 $l\equiv 0\bmod(q-1)$ 时，有

$$\begin{aligned}
&(-1)^{s_i+s_{i+l}}\\
&=\begin{cases}
1, & (g^i+1)\bmod pq\in Q_0\\
-\left(\frac{g^i+1}{q}\right)\left(\frac{-g^l+1}{p}\right), & (g^i+1)\bmod pq\in P\\
-\left(\frac{g^i+1}{p}\right)\left(\frac{g^i+1}{q}\right), & \gcd(g^i+1,pq)=1,\\
 & (g^{i+l}+1)\bmod pq\in P\\
\left(\frac{g^i+1}{p}\right)\left(\frac{g^{i+l}+1}{p}\right), & \gcd(g^i+1,pq)=1
\end{cases}
\end{aligned}$$

当 $p\equiv q\equiv 3\bmod 4$ 时，有 $(g^i+1)\bmod pq=0$，$\gcd\left(g^{i+l}+1,pq\right)=1$ 和 $(g^{i+l}+1)\bmod pq=0,\gcd(g^i+1,pq)=1$ 这两项，但这两项的 $(-1)^{s_i+s_{i+l}}$ 值为 0，与 $p\not\equiv q\bmod 4$ 中的 $\gcd(g^i+1,pq)=1$ 的 $(-1)^{s_i+s_{i+l}}$ 值相同。因此，$p\equiv q\equiv 3\bmod 4$ 和 $p\not\equiv q\bmod 4$ 的双素数 Sidel'nikov 序列的自相关函数相同。

上面和式的证明同定理 2，当 $l\equiv 0\bmod(q-1)$ 时，可以得到双素数 Sidel'nikov 序列的自相关函数。

定理 4 的证明　当 $l\not\equiv 0\bmod(p-1)$ 且 $l\not\equiv 0\cdot\bmod(q-1)$ 时有

$$\begin{aligned}
&(-1)^{s_i+s_{i+l}}\\
&=\begin{cases}
-1, & (g^i+1)\bmod pq\in Q_0,\\
 & (g^{i+l}+1)\bmod pq\in P\\
\left(\frac{g^{i+l}+1}{p}\right)\left(\frac{-g^l+1}{q}\right), & (g^i+1)\bmod pq\in Q_0,\\
 & \gcd(g^{i+l}+1,pq)=1\\
-1, & (g^i+1)\bmod pq\in P,\\
 & (g^{i+l}+1)\bmod pq\in Q_0\\
-\left(\frac{-g^l+1}{p}\right)\left(\frac{g^{i+l}+1}{q}\right), & (g^i+1)\bmod pq\in P,\\
 & \gcd(g^{i+l}+1,pq)=1\\
\left(\frac{g^i+1}{p}\right)\left(\frac{g^i+1}{q}\right), & \gcd(g^i+1,pq)=1,\\
 & (g^{i+l}+1)\bmod pq\in Q_0\\
-\left(\frac{g^i+1}{p}\right)\left(\frac{g^i+1}{q}\right), & \gcd(g^i+1,pq)=1,\\
 & (g^{i+l}+1)\bmod pq\in P\\
\left(\frac{g^i+1}{p}\right)\left(\frac{g^{i+l}+1}{p}\right)\left(\frac{g^i+1}{q}\right)\left(\frac{g^{i+l}+1}{q}\right), & \\
 & \gcd(g^i+1,pq)=1,\\
 & \gcd(g^{i+l}+1,pq)=1
\end{cases}
\end{aligned}$$

当 $p\equiv q\equiv 3\bmod 4$ 时且 l 为偶数时，只有一个 i

满足$(g^i+1)\bmod pq\in Q_0,(g^{i+l}+1)\bmod pq\in P$，同时也只有一个 i 满足 $(g^i+1)\bmod pq\in P,(g^{i+l}+1)\cdot\bmod pq\in Q_0$。$l$ 为奇数时，$(g^i+1)\bmod pq\in Q_0$，$(g^{i+l}+1)\bmod pq\in P$ 和 $(g^i+1)\bmod pq\in P$，$(g^{i+l}+1)\cdot\bmod pq\in Q_0$ 这两项不成立。当 $p\not\equiv q\bmod 4$ 时与 $p\equiv q\equiv 3\bmod 4$ 的情况相反。

上面 4 个和式的证明同定理 2，对最后一个和式同样使用引理 3，有下面的公式：

$$\begin{aligned}
&\sum_{\substack{\gcd(g^i+1,pq)=1\\ \gcd(g^{i+l}+1,pq)=1}}\left(\frac{g^i+1}{p}\right)\left(\frac{g^{i+l}+1}{p}\right)\left(\frac{g^i+1}{q}\right)\left(\frac{g^{i+l}+1}{q}\right)\\
&=\sum_{i=0}^{p-2}\left(\frac{g^i+1}{p}\right)\left(\frac{g^{i+l}+1}{p}\right)\\
&\quad\cdot\sum_{j=0}^{(q-3)/2}\left(\frac{g^{i+j(p-1)}+1}{q}\right)\left(\frac{g^{i+l+j(p-1)}+1}{q}\right)\\
&=\sum_{i=0}^{p-2}\left(\frac{g^i+1}{p}\right)\left(\frac{g^{i+l}+1}{p}\right)\\
&\quad\cdot\sum_{x=1}^{q-1}\left(\frac{g^ix+1}{q}\right)\left(\frac{g^{i+l}x+1}{q}\right)\left(1+\left(\frac{x}{q}\right)\right)\Big/2\\
&=\frac{1}{2}\sum_{i=0}^{p-2}\left(\frac{g^i+1}{p}\right)\left(\frac{g^{i+l}+1}{p}\right)\left(\sum_{x=1}^{q-1}\left(\frac{g^ix+1}{q}\right)\left(\frac{g^{i+l}x+1}{q}\right)\right.\\
&\quad\left.+\sum_{x=1}^{q-1}\left(\frac{g^ix+1}{q}\right)\left(\frac{g^{i+l}x+1}{q}\right)\left(\frac{x}{q}\right)\right)\\
&=\frac{1}{2}\sum_{i=0}^{p-2}\left(\frac{g^i+1}{p}\right)\left(\frac{g^{i+l}+1}{p}\right)\\
&\quad\cdot\left(-(-1)^l-1+(-1)^lO\left(2q^{1/2}\right)\right)\\
&=\frac{1}{2}\left((-1)^l+1\right)^2+O\left(p^{1/2}q^{1/2}\right)
\end{aligned}$$

因此，我们可以得到 $l\not\equiv 0\bmod(p-1)$ 且 $l\not\equiv 0\cdot\bmod(q-1)$ 的自相关函数。 证毕

4 数据模拟与界的比较

当 $l\equiv 0\bmod(p-1)$ 和 $l\equiv 0\bmod(q-1)$ 时，我们给出的自相关函数的估计值 $O(q^{1/2})$ 和 $O(p^{1/2})$ 明显优于 Brandstätter 给出的估计值 $O((p+q)/2)$。当 $l\not\equiv 0\bmod(p-1)$且$l\not\equiv 0\bmod(q-1)$ 时，Brandstätter 给出的双素数 Sidel'nikov 序列自相关函数的估计值是 $O((p+q)/2+\sqrt{pq})$，定理 4 中自相关函数的估计值是 $O(p^{1/2}q^{1/2})$。当 $\sqrt{pq}$ 在数量级上小于 $(p+q)/2$ 时，我们给出的界优于定理 1 中的界。

当 $p<q<2p$ 时，取 $p=11,q=13$ 和 $p=7,q=11$ 的双素数 Sidel'nikov 序列自相关函数的实际值和定理中自相关函数的精确值的比较。如图 1 和图 2。

从图 1 和图 2 可以看出当 $p=11,q=13$ 和 $p=7,q=11$ 时的双素数 Sidel'nikov 序列自相关函数实际值和定理中的精确值的最大绝对差值分别是 16 和 10，与我们的估计值 $O(\sqrt{11\times 13})=11.958$ 和 $O(\sqrt{7\times 11})=8.775$ 很接近，最小差值都为 0。当 $p\gg q$ 或 $q\gg p$ 时，取 $p=3,q=997$ 的双素数 Sidel'nikov 序列自相关函数的实际值和定理中自相关函数的精确值的差值如图 3 所示。

从图 3 可以看出当 $p=3,q=997$ 时的双素数 Sidel'nikov 序列自相关函数的实际值和定理 4 中自相关函数的精确值的差值的绝对值最大是 31，与我们的估计值 $O(p^{1/2}q^{1/2})=54.690$ 很接近。由此表明定理中给出的自相关函数是双素数 Sidel'nikov 序列自相关函数的一个较紧的界。

5 结束语

本文主要计算当 $d=2$ 时双素数 Sidel'nikov 序列的自相关函数，根据 l 的取值分为 $l\equiv 0\cdot\bmod(p-1),l\equiv 0\bmod(q-1)$ 和 $l\not\equiv 0\bmod(p-1)$ 且 $l\not\equiv 0\bmod(q-1)$ 3 类，其中当 $l\equiv 0\bmod(p-1)$ 和 $l\equiv 0\bmod(q-1)$ 时自相关函数的实际值与定理中的精确值的差值最大是 $O(q^{1/2})$ 和 $O(p^{1/2})$，而当 $l\not\equiv 0\bmod(p-1)$且$l\not\equiv 0\bmod(q-1)$ 时自相关函数的实际值与定理中的精确值的差值最大是 $O(p^{1/2}q^{1/2})$。

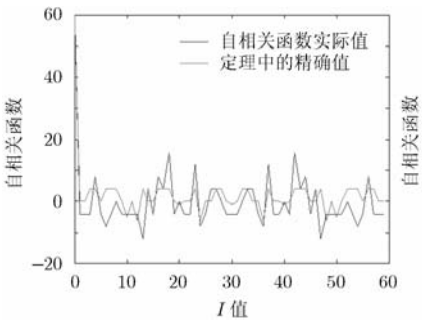

图 1 p=11, q=13 的双素数 Sidel'nikov 序列的自相关函数和定理中的精确值比较

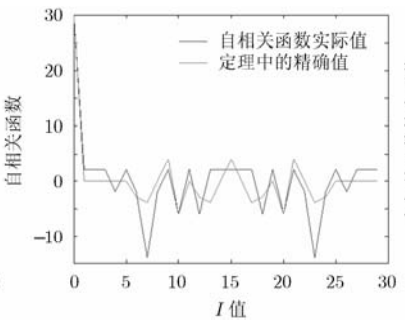

图 2 p=7, q=11 的双素数 Sidel'nikov 序列的自相关函数和定理中的精确值比较

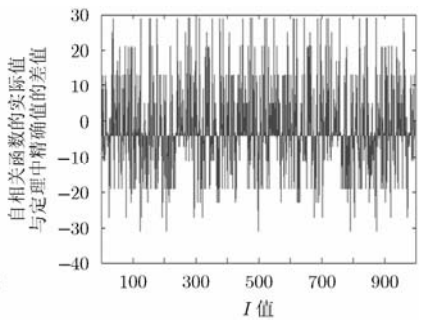

图 3 $p=3,q=997$ 的双素数 Sidel'nikov 序列的自相关函数和定理中的精确值的差值

通过与 Brandstätter 给出的双素数 Sidel'nikov 序列自相关函数的估计值的界进行比较，并且通过数据模拟验证，得出本文所给出的自相关函数是紧的。因此，双素数 Sidel'nikov 序列自相关函数可以根据定理中自相关函数计算出。

$d > 2$ 时双素数 Sidel'nikov 序列的自相关函数有待于进一步研究。

参 考 文 献

[1] Sidel'nikov V M. Some k-valued pseudo-random sequences and nearly equidistant codes[J]. *Problems of Information Transmission*, 1969, 5(1): 12–16.

[2] Lempel A, Cohn M, and Eastman W L. A class of balanced binary sequences with optimal autocorrelation properties[J]. *IEEE Transactions on Information Theory*, 1977, 23(1): 38–42.

[3] Su M and Winterhof A. Autcorrelation of Lengendre-Sidel'nikov sequences[J]. *IEEE Transactions on Information Theory*, 2010, 56(4): 1714–1718.

[4] Su M and Winterhof A. Correlation measure of order k and linear complexity profile of legrendre-sidelnikov sequences[J]. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science*, 2012, 95(11): 1851–1854.

[5] Su M. On the d-ary generalized Legendre-Sidelnikov sequence [C]. Sequences and Their Applications (SETA), Springer Berlin Heidelberg, Waterloo, 2012, 7280: 233–244.

[6] Brandstätter N, Pirsic G, and Winterhof A. Correlation of the two-prime Sidel'nikov sequence[J]. *Designs, Codes, Cryptography*, 2011, 59(1－3): 59–68.

[7] Brandstätter N and Winterhof A. Some notes on the two-prime generator of order 2[J]. *IEEE Transactions on Information Theory*, 2005, 51(10): 3654–3657.

[8] Cusick T W, Ding C, and Renvall A. Stream Ciphers and Number Theory[M]. Amsterdam: Elsevier Science Limited, 2004, Vol. 66: 195–226.

[9] 柯召, 孙琦. 数论讲义, (下册)[M]. 第 2 版, 北京: 高等教育出版社, 2003: 58–62.
Ke Zhao and Sun Qi. Number Theory Lecture Notes Rudin [M]. Second Edition, Beijing: Higher Education Press, 2003: 58–62.

[10] Ding C. Autocorrelation values of generalized cyclotomic sequences of order two[J]. *IEEE Transactions on Information Theory*, 1988, 44(4): 1699–1702.

[11] Topuzo lu A and Winterhof A. Pseudorandom Sequences[M]. Dordrecht: Springer Netherlands, 2007, Vol. 6: 135–166.

[12] Lidl R and Niedeerretiter H. Finite Fields[M]. Cambridge: Cambridge University Press, 1997, Vol. 20: 217–230.

岳　曌：　女，1989 年生，硕士生，研究方向为密码学、伪随机序列.

高军涛：　男，1979 年生，副教授，硕士生导师，主要研究方向为密码学、伪随机序列.

谢　佳：　女，1990 年生，硕士生，研究方向为密码学、伪随机序列.