一类椭圆曲线二元序列的伪随机性分析

赵 龙 韩文报 冀会芳

(解放军信息工程大学信息研究系 郑州 450002)

摘 要 基于二进制有限域上的椭圆曲线构造了一类二元伪随机序列,利用椭圆曲线上的指数和计算了该类序列的一致分布测度和 k 阶相关测度,利用线性复杂度和 k 阶相关测度之间的关系给出了序列的线性复杂度下界。计算结果表明,类序列具有非常好的伪随机性,在密码学和通信领域具有潜在的应用价值。

关键词 伪随机序列,椭圆曲线指数和,一致分布测度,k 阶相关测度

中图法分类号 TP309 **文献标识码** A

On a Family of Pseudorandom Binary Sequences from Elliptic Curve

ZHAO Long HAN Wen-bao JI Hui-fang

(Department of Information Research, PLA Information Engineering University, Zhengzhou 450002, China)

Abstract One family of pseudorandom binary sequences were constructed from elliptic curves over binary finite fields. With the help of exponential sums on elliptic curves, the well-distribution measure and correlation measure of order k were computed, and the low bound of linear complexity was derived by the relation between linear complexity and correlation measure of order k. The results show that these sequences have good randomness and provide strong potential applications in communication systems and cryptography.

Keywords Pseudorandom sequence elliptic curve, Exponential sums, Well-distribution measure, Correlation measure of order k

1 引言

伪随机序列在密码学和通信领域有着非常重要的应用。随着椭圆曲线密码体制的推广,椭圆曲线上的代数运算在各种软硬件平台上的实现效率得到不断提高,加上许多传统的基于有限域或环上的伪随机数生成器已被证明是不安全的,利用椭圆曲线构造伪随机序列逐渐成为热门问题。目前常见的椭圆曲线伪随机序列有椭圆曲线线性同余序列[1]、椭圆曲线幂生成器序列[2]、椭圆曲线线性反馈移位寄存器序列[3]、椭圆曲线 Naor-Reingold 序列[4]等。这些序列具有许多好的密码学性质,在流密码及公钥密码体制中有重要的应用价值。比如在条件有限的系统或设备中,如果采用的是椭圆曲线密码体制,就可以利用已有椭圆曲线运算部件来构造伪随机数生成器,用于生成密码协议中的随机数和密钥,从而节约硬件资源。

记 F_q 为 q 元有限域,E 表示定义在 F_q 上的椭圆曲线,$E(F_q)$ 表示 E 的 F_q-有理点集合,则 $E(F_q)$ 在椭圆曲线点加运算下构成 Abel 群,无穷远点 $\mathcal{O}$ 为群中的单位元。设 G 为 $E(F_q)$ 上的 N 阶点,记 $\Theta=(G,2G,\cdots,NG)$ 表示由 G 生成的点列,$iG=(x_i,y_i)\in F_q\times F_q$,其中 $1\leqslant i\leqslant N-1$。目前基于椭圆曲线构造的二元伪随机序列大多是通过将点列 Θ 进行变换得到的。

当 F_q 为素数域时,即 $q=p$ 且 $p\geqslant 5$,Chen 等[5]利用 x_i,y_i 的奇偶性、x_i,y_i 与 $p/2$ 的大小比较、x_i 与 y_i 的大小比较构造了 5 种二元序列。Merai 在文献[6]中将 Chen 的构造方式进行了推广,设 f 为 E 在 F_p 上的有理函数,Merai 利用 $f(iG)$ 与 $p/2$ 的大小比较构造二元序列。此外,Chen[7]还利用 $f(iG)$ 的 Legendre 符号构造二元序列。这些序列都已经被证明具有较小的一致分布测度和 k 阶相关测度,说明具有较好的伪随机性。

当 F_q 为二进制有限域时,即 $q=2^n$,记 $a_i=Tr(x_i)$,$b_i=Tr(y_i)$,其中 Tr 为有限域 F_q 到 F_2 上的迹函数。当 E 为超奇异椭圆曲线时,Gong 等[8]研究了交错序列 $(a_1,b_1,a_2,b_2,a_3,b_3,\cdots)$ 的平衡性、周期和线性复杂度;当 E 为非超奇异椭圆曲线时,根据椭圆曲线点加公式可知序列 $(a_2,a_4,a_6,\cdots)$ 为全 1 序列或全 0 序列,说明序列 $(a_1,a_2,a_3,\cdots)$ 的随机性很差。Gong 等研究了序列 $(b_1,b_2,b_3,\cdots)$ 的周期和线性复杂度。

本文构造的二元序列同样基于二进制有限域上的椭圆曲线,文中的 F_q 均指二进制有限域。设 f 为 E 在 F_q 上的有理函数,特别地可以取 $f=y$ 或 $f=x+y$。设 α 为 F_q 上的任意非零元,则由 f 和 α 可以构造二元序列:

$$S_N=(s_1,s_2,\cdots,s_N) \tag{1}$$

到稿日期:2010-12-02 返修日期:2011-02-27 本文受国家 973 基金(2007CB807902),国家 863 基金(2009AA01Z417),全国优秀博士学位论文作者专项基金(FANEDD—2007B74)资助。

赵 龙(1983—),男,博士生,主要研究方向为公钥密码学,E-mail:zhaolong_email@126.com;韩文报(1963—),男,博士生导师,主要研究方向为密码学与信息安全;冀会芳(1982—),女,博士生,主要研究方向为公钥密码学。

式中，$s_i=Tr(\alpha f(iG))$。如果 iG 是 f 的极点，则令 $s_i=0$。

序列 S_N 既可以基于超奇异椭圆曲线，也可以基于非超奇异椭圆曲线，它在某种程度上可以看作是 Gong 的构造方式的推广。序列 S_N 具有重要的代表意义，比如对于 F_q 在 F_2 上的一组基 $\eta_1,\cdots,\eta_n$，其对偶基记为 $\beta_1,\cdots,\beta_n$。如果 iG 不是 f 的极点，则 $f(iG)$可以唯一表示为：

$$f(iG)=b_{i,1}\eta_1+\cdots+b_{i,n}\eta_n$$

取 $\alpha=\beta_j$，则序列 S_N 即为$\{f(iG)\}$在 η_j 前的坐标序列：

$$(b_{1,j},b_{2,j},b_{3,j},\cdots)$$

对于二元伪随机序列，Mauduit 等在文献[9]中引入了两个最重要的随机性指标：一致分布测度和 k 阶相关测度。本文利用椭圆曲线上的指数并研究了序列 S_N 的一致分布测度和 k 阶相关测度，利用线性复杂度和 k 阶相关测度之间的关系，给出了序列的线性复杂度下界。计算结果表明，如果有理函数 f 选取得当，则序列 S_N 具有非常好的伪随机性。

2 预备知识

设 G 是有限 Abel 群，U 是复数域$\mathbb{C}$ 中单位圆群，任一群同态 $\chi:G\to U$ 称为 G 的一个特征。对于有限域 F_q，记 $\chi(x)=(-1)^{Tr(x)}$，则$\{\chi(\alpha x)\mid\alpha\in F_q\}$为 F_q 上的 q 个加法特征；对于剩余类环$\mathbb{Z}_m$，记 $e_m(z)=\exp(2\pi iz/m)$，则$\{e_m(az)\mid a\in\mathbb{Z}_m\}$为$\mathbb{Z}_m$上的 m 个加法特征。

引理 1[10] 设正整数 $m>1$，对于任意的正整数 T 及 $1\leqslant H\leqslant m$，有：

$$\sum_{c=0}^{m-1}\left|\sum_{u=T+1}^{T+H}e_m(cu)\right|\leqslant m(1+\ln m)$$

记 $F_q(E)$为 E 在 F_q 上的有理函数域，对于非零的有理函数 $f\in F_q(E)$，f 的除子记为：

$$\mathrm{div}(f)=\sum_P \mathrm{ord}_P(f)(P)$$

式中，P 跑遍 $F_q(E)$上的素除子，$\mathrm{ord}_P(f)$表示 f 在 P 上的是赋值，可以证明只有有限个素除子 P 使得 $\mathrm{ord}_P(f)\neq0$，当 $\mathrm{ord}_P(f)>0$ 时，P 为 f 的零点；当 $\mathrm{ord}_P(f)<0$ 时，P 为 f 的极点。

记 $\deg P$ 表示素除子 P 的次数，则 f 的零点除子次数为：

$$\deg^0(f)=\sum_{\mathrm{ord}_P(f)>0}\mathrm{ord}_P(f)\cdot\deg(P)$$

极点除子次数为：

$$\deg^\infty(f)=\sum_{\mathrm{ord}_P(f)<0}(-\mathrm{ord}_P(f))\cdot\deg(P)$$

可以证明 $\deg^0(f)=\deg^\infty(f)$，不妨把它们统一记为 $\deg f$。特别地，当 $f=x$ 时，$\deg f=2$；当 $f=y$ 时，$\deg f=3$。

引理 2 设 $f,g\in F_q(E)$，对 $F_q(E)$上的任意素除子 P，有：

$$\mathrm{ord}_P(f+g)\geqslant\min\{\mathrm{ord}_P(f),\mathrm{ord}_P(g)\}$$

当 $\mathrm{ord}_P(f)\neq\mathrm{ord}_P(g)$时，等号成立。

对于有理点 $W\in E(F_q)$，记 τ_W 表示 $E(F_q)$上由 W 确定的平移映射：

$$\tau_W:E(F_q)\to E(F_q)$$

$$P\to P+W$$

如果 Q 是 f 的极点，则 $Q-W$ 是 $f\circ\tau_W$ 的极点，而且：

$$\mathrm{ord}_Q(f)=\mathrm{ord}_{Q-W}(f\circ\tau_W)$$

引理 3[11] 设有理函数 $f\in F_q(E)$且不存在 $g\in\bar{F}_q(E)$，$\beta\in F_q$使得 $f=g^2+g+\beta$，G 为 $E(F_q)$上的 N 阶点，则：

$$\left|\sum_{x=0,f(xG)\neq\infty}^{N-1}\chi(\alpha f(xG))e_N(bx)\right|\leqslant2\deg(f)q^{1/2}$$

式中，$\alpha\in F_q^*$ 且 $0\leqslant b\leqslant N-1$。

3 序列的伪随机性指标

对于二元序列 $S_N=\{s_1,s_2,\cdots,s_N\}\in\{0,1\}^N$，Mauduit 等在文献[9]中引入了两个最重要的伪随机性指标：一致分布测度和 k 阶相关测度。

定义 1 序列 S_N 的一致分布测度定义为：

$$W(S_N)=\max_{a,b,m}\left|\sum_{j=0}^{m-1}(-1)^{s_{a+jb}}\right|$$

式中，$a,b,m\in\mathbb{N}$ 且 $1\leqslant a\leqslant a+(m-1)b\leqslant N$。

定义 2 序列 S_N 的 k 阶相关测度定义为：

$$C_k(S_N)=\max_{M,D}\left|\sum_{n=0}^{M-1}(-1)^{s_{n+d_1}+\cdots+s_{n+d_k}}\right|$$

式中，整数 $D=(d_1,\cdots,d_k)$与 M 满足 $0\leqslant d_1<\cdots<d_k\leqslant N-M$。

对于序列 S_N，如果它的一致分布测度和 k 阶相关测度相对于 N 都很小，即当 $N\to\infty$时，满足 $W(S_N)/N\to0$ 及 $C_k(S_N)/N\to0$，则认为 S_N 是一个好的二元伪随机序列。

定义 3 序列 S_N 前 M 项的线性复杂度 $L(S_N,M)$定义为满足 F_2 上的关系式：

$$s_{n+L}=c_{L-1}s_{n+L-1}+\cdots+c_0s_n,0\leqslant n\leqslant M-L-1$$

的最小正整数 L。

序列的线性复杂度是序列不可预测性的一个重要指标，它和 k 阶相关测度有以下关系。

引理 4[12] 对于二元序列 S_N 和任意的 $2\leqslant M\leqslant N-1$，有：

$$L(S_N,M)\geqslant M-\max_{1\leqslant k\leqslant L(S_N,M)}C_k(S_N)$$

4 序列的伪随机性分析

引理 5 设 N,b,m 为正整数且满足 $(m-1)b<N$，则：

$$\sum_{\lambda=0}^{N-1}\left|\sum_{x=0}^{m-1}e_N(\lambda bx)\right|\leqslant N(1+\ln N)$$

证明：令 $d=gcd(b,N)$，$M=N/d$，$c=b/d$，于是：

$$\sum_{\lambda=0}^{N-1}\left|\sum_{x=0}^{m-1}e_N(\lambda bx)\right|=\sum_{\lambda=0}^{N-1}\left|\sum_{x=0}^{m-1}e_M(\lambda cx)\right|=d\sum_{\lambda=0}^{M-1}\left|\sum_{x=0}^{m-1}e_M(\lambda cx)\right|$$

由于 $\gcd(M,c)=1$，当 λ 跑遍$\mathbb{Z}_M$时，λc 也跑遍$\mathbb{Z}_M$，从 $(m-1)b<N$可知 $m-1<M$，结合引理 1 即得：

$$d\sum_{\lambda=0}^{M-1}\left|\sum_{x=0}^{m-1}e_M(\lambda cx)\right|=d\sum_{\lambda=0}^{M-1}\left|\sum_{x=0}^{m-1}e_M(\lambda x)\right|\leqslant dM(1+\ln M)\leqslant N(1+\ln N)$$

引理 6 设有理函数 $f\in F_q(E)$且不存在 $g\in\bar{F}_q(E)$，$\beta\in F_q$ 使得 $f=g^2+g+\beta$，G 为 $E(F_q)$上的 N 阶点，则：

$$\left|\sum_{x=0,f((a+bx)G)\neq\infty}^{m-1}\chi(\alpha f((a+bx)G))\right|\leqslant2deg(f)q^{1/2}(1+\ln N)$$

式中，$\alpha\in F_q^*$，正整数 a,b,m 满足 $1\leqslant a\leqslant a+(m-1)b\leqslant N-1$。

证明：根据特征和的性质可知：

$$\left|\sum_{x=0,f((a+bx)G)\neq\infty}^{m-1}\chi(\alpha f((a+bx)G))\right|=\frac{1}{N}\left|\sum_{n=0,f(nG)\neq\infty}^{N-1}\chi(\alpha f(nG))\sum_{x=0}^{m-1}\sum_{\lambda=0}^{N-1}e_N(\lambda(n-(a+bx)))\right|$$

$$\leqslant\frac{1}{N}\sum_{\lambda=0}^{N-1}\left|\sum_{x=0}^{m-1}e_N(-\lambda(a+bx))\right|\cdot\left|\sum_{n=0,f(nG)\neq\infty}^{N-1}\chi(\alpha f(nG))e_N(\lambda n)\right|$$

$$=\frac{1}{N}\sum_{\lambda=0}^{N-1}\left|\sum_{x=0}^{m-1}e_N(\lambda bx)\right|\cdot\left|\sum_{n=0,f(nG)\neq\infty}^{N-1}\chi(\alpha f(nG))e_N(\lambda n)\right|$$

结合引理 3 和引理 5,结论即得。

定理 1 设 G 为 $E(F_q)$ 上的 N 阶点,$\alpha\in F_q^*$,有理函数 $f\in F_q(E)$ 且不存在 $g\in\overline{F}_q(E),\beta\in F_q$ 使得 $f=g^2+g+\beta$,序列 S_N 的构造如(1)所示,则 S_N 的一致分布测度满足:

$$W(S_N)\leqslant 2\deg(f)q^{1/2}(1+\ln N)+\deg f$$

证明:对于正整数 a,b,m 且满足 $1\leqslant a\leqslant a+(m-1)b\leqslant N$,由于 f 最多有 $\deg f$ 个极点,于是:

$$\left|\sum_{j=0}^{m-1}(-1)^{s_{a+jb}}\right|\leqslant\left|\sum_{x=0,f((a+bx)G)\neq\infty}^{m-1}\chi(\alpha f((a+bx)G))\right|+\deg f$$

结合引理 6,定理即证。

定理 2 设 G 为 $E(F_q)$ 上的 N 阶点,$\alpha\in F_q^*$,有理函数 $f\in F_q(E)$ 满足:对任意的整数 $0\leqslant d_1<\cdots<d_k\leqslant N$,都不存在 $g\in\overline{F}_q(E),\beta\in F_q$ 使得:

$$f\circ\tau_{d_1G}+f\circ\tau_{d_2G}+\cdots+f\circ\tau_{d_kG}=g^2+g+\beta$$

序列 S_N 的构造如式(1)所示,则 S_N 的 k 阶相关测度满足:

$$C_k(S_N)<2kdeg(f)q^{1/2}(1+\ln N)+2k\deg(f)$$

证明:对于任意的整数 $D=(d_1,\cdots,d_k)$ 与 M 满足 $0\leqslant d_1<\cdots<d_k\leqslant N-M$,记:

$$\Lambda_i=\{n\mid 1\leqslant n\leqslant N,f\circ\tau_{d_iG}(nG)=\infty\},\Lambda=\bigcup_{i=1}^{k}\Lambda_i$$

则 Λ_i 表示 $\langle G\rangle$ 中 $f\circ\tau_{d_iG}$ 的极点集合,于是:

$$\left|\sum_{n=0}^{M-1}(-1)^{s_n+d_1+\cdots+s_n+d_k}\right|\leqslant\left|\sum_{n=0,n\notin\Lambda}^{M-1}\chi(\alpha\sum_{i=1}^{k}f((n+d_i)G))\right|+\#\Lambda$$

$$\leqslant\left|\sum_{n=0,n\notin\Lambda}^{M-1}\chi(\alpha\sum_{i=1}^{k}f((n+d_i)G))\right|+k\deg f\qquad(2)$$

记 $h=\alpha\sum_{i=1}^{k}f\circ\tau_{d_iG}$,则 $\deg h\leqslant k\deg f$,记 Λ' 表示 $\langle G\rangle$ 中 h 的极点集合,即:

$$\Lambda'=\{n\mid 1\leqslant n\leqslant N,h(nG)=\infty\}$$

显然 $\Lambda'\subseteq\Lambda$,于是:

$$\left|\sum_{n=0,n\notin\Lambda}^{M-1}\chi(\alpha\sum_{i=1}^{k}f((n+d_i)G))\right|\leqslant\left|\sum_{n=0,n\notin\Lambda}^{M-1}\chi(\sum_{i=1}^{k}h(nG))\right|+(\#\Lambda-\#\Lambda')$$

$$\leqslant\left|\sum_{n=0,n\notin\Lambda}^{M-1}\chi(\alpha\sum_{i=1}^{k}h(nG))\right|+k\deg f\qquad(3)$$

结合引理 6 和式(2)、式(3),定理即证。

定理 3 设 G 为 $E(F_q)$ 上的 N 阶点,$\alpha\in F_q^*$,有理函数 $f\in F_q(E)$ 满足定理 2 中的条件,序列 S_N 的构造如式(1)所示,则 S_N 前 M 项的线性复杂度满足:

$$L(S_N,M)\geqslant\frac{M}{1+2\deg(f)(q^{1/2}(1+\ln N)+1)}$$

证明:将定理 2 中结论代入引理 4 中,化简即得。

根据 Hasse 定理,$E(F_q)$ 的阶满足 $|\#E(F_q)-q+1|\leqslant 2\sqrt{q}$,$E(F_q)$ 的群结构满足 $E(F_q)\simeq\mathbb{Z}_{n_1}\times\mathbb{Z}_{n_2}$,其中 n_1,n_2 为正整数且 $n_1\mid q-1,n_1\mid n_2$。在椭圆曲线密码体制中,选取的椭圆曲线通常满足 $E(F_q)$ 是一个循环群或者是殆循环的,即 $n_1=1$ 或 n_1 为小整数,因此在构造二元序列时,总可以选取 G 为 $E(F_q)$ 中的 n_2 阶元,此时序列的长度 $N=n_2=O(q)$。如果有理函数 f 选取得当,序列 S_N 的一致分布测度满足 $W(S_N)=O(N^{1/2}\ln N)$,k 阶相关测度满足 $C_k(S_N)=O(kN^{1/2}\ln N)$,线性复杂度满足 $L(S_N,N)>O(q^{1/2})$,这说明 S_N 具有非常好的伪随机性。

下面讨论如何选取有理函数 $f\in F_q(E)$,使得 f 能够满足定理 1 和定理 2 中的条件。

引理 7 设有理函数 $f\in F_q(E)$,如果存在 f 的某个极点 P,满足 $\mathrm{ord}_P(f)$ 为奇数,则 f 满足定理 1 中的条件。

证明:根据引理 2 可知,如果存在 $g\in\overline{F}_q(E),\beta\in F_q$ 使得 $f=g^2+g+\beta$,则对 f 的任意极点 P,都有 $\mathrm{ord}_P(f)=2\mathrm{ord}_P(g)$,于是 $\mathrm{ord}_P(f)$ 必然为偶数。

定理 4 设有理函数 $f\in F_q(E)$,记 f 的极点为 $\{P_1,P_2,\cdots,P_l\}$,如果存在某个极点 P_s,同时满足下面两个条件:

(1)$\mathrm{ord}_{P_s}(f)$ 为奇数;

(2)对于任意的 $1\leqslant i\leqslant l$ 且 $i\neq s$,$\deg P_s\neq\deg P_i$。

则 f 同时满足定理 1 和定理 2 中的条件。特别地,当 f 为多项式有理函数时,f 仅有一个极点 $\mathcal{O}$ 且极点除子次数 $\deg f$ 等于 f 的加权次数,其中变元 x,y 的权值分别为 2 和 3,如果 $\deg(f)$ 为奇数,则 f 满足定理 1 和定理 2 中的条件。

证明:根据引理 7,f 显然满足定理 1 中的条件,下面证明 f 也满足定理 2 中的条件。

对于任意的整数 $0\leqslant d_1<\cdots<d_k\leqslant N$,记 $h=\sum_{i=1}^{k}f\circ\tau_{d_iG}$,由于 P_s 的次数和 f 其它极点的次数都不相同,因此 $P_s-d_1G,\cdots,P_s-d_kG$ 必然均为 h 的极点,而且这 k 个极点互不相同,同时满足

$$\mathrm{ord}_{P_s-d_1G}(h)=\cdots=\mathrm{ord}_{P_s-d_kG}(h)=\mathrm{ord}_{P_s}(f)$$

由于 $\mathrm{ord}_{P_s}(f)$ 为奇数,因此 f 也满足定理 2 中的条件。

引理 8[6] 对于正整数 l,k,N,记 $p(N)$ 表示 N 的最小素因子,如果满足 $(4k)^l<p(N)$,则对任意的集合 $A,B\subset\mathbb{Z}_N$,其中 $\#A=l$ 且 $\#B=k$,都存在元素 $c\in\mathbb{Z}_m$,使得方程:

$$x+y=c,x\in A,y\in B$$

仅有一个解。

定理 5 设 G 是 $E(F_q)$ 上的 N 阶点,$p(N)$ 表示 N 的最小素因子,对于有理函数 $f\in F_q(E)$,f 的极点记为 $\{P_1,P_2,\cdots,P_l\}$,如果存在某个极点 P_s,同时满足下面两个条件:

(1)$\mathrm{ord}_{P_s}(f)$ 为奇数;

(2)$(4k)^l<p(N)$。

则对任意的整数 $0\leqslant d_1<\cdots<d_k\leqslant N$,都不存在 $g\in\overline{F}_q(E),\beta\in F_q$ 使得:

$$f\circ\tau_{d_1G}+f\circ\tau_{d_2G}+\cdots+f\circ\tau_{d_kG}=g^2+g+\beta$$

证明:对于两个素除子 P,Q,如果存在某个 i 使得 $P=Q+iG$,则称 P 和 Q 是等价的。将 f 的极点 $\{P_1,P_2,\cdots,P_l\}$ 按照等价关系划分为不同的等价类,不妨设 P_s 所在等价类为 $\{P_1,\cdots,P_m\}$,记 $P_i=P_s+a_iG,1\leqslant i\leqslant m$,构造集合:

$$A=\{a_1,\cdots,a_m\},B=\{-d_1,\cdots,-d_k\}$$

由于 $\#A=m\leqslant l$,于是 $(4k)^m\leqslant(4k)^l<p(N)$,根据引理 8 可知,必然存在元素 $c\in\mathbb{Z}_m$,使得方程:

$x+y=c, x\in A, y\in B$

仅有一个解，不妨把解记为 $x=a_u, y=-d_v$，于是 $P_s+a_uG-d_vG$ 为 $f\circ\tau_{d_vG}$ 的极点且不为 $f\circ\tau_{d_iG}, i\neq v$ 的极点。

记 $h=\sum_{i=1}^{k} f\circ\tau_{d_iG}$，则 $P_s+a_uG-d_vG$ 为 h 的极点且：

$ord_{P_s+a_uG-d_vG}(h)=\mathrm{ord}_{P_s}(f)$

由于 $\mathrm{ord}_{P_s}(f)$ 为奇数，根据引理 7，命题即证。

注：定理 5 对 k 阶相关测度中的 k 有所限制，当 N 是一个素数且 f 的极点个数较少时，k 可以取较大的值。而定理 4 则对 k 没有限制。

结束语 伪随机序列一直是密码学领域的热点问题之一。由于椭圆曲线运算效率的不断提高，加上许多传统的基于有限域或环上的伪随机数生成器已被证明是不安全的，利用椭圆曲线来构造伪随机序列得到了众多学者的关注。本文基于二进制有限域上的椭圆曲线构造了一类二元伪随机序列，利用椭圆曲线上的指数和计算了序列的一致分布测度和 k 阶相关测度，利用线性复杂度和 k 阶相关测度之间的关系，给出了序列的线性复杂度下界。计算结果表明，本文构造的二元序列具有非常好的伪随机性，在密码学和通信领域具有潜在的应用价值。

参 考 文 献

[1] Hess F, Shparlinski I E. On the linear complexity and multidimensional distribution of congruential generators over elliptic curve[J]. Designs, Codes and Cryptography, 2005, 35(1): 111-117

[2] Lange T, Shparlinski I E. Certain exponential sums and random walks on elliptic curves[J]. Canad. J. Math, 2005, 57(2): 338-350

[3] Gong G, Lam C Y. Linear recursive sequences over elliptic curves[C]// Proceedings of Sequences and Their Applications 2001. Berlin: Spring-Verlag, 2001: 182-196

[4] Cruz M, Gomez D, Sadornil D. On the linear complexity of the Naor-Reingold sequence with elliptic curves[J]. Finite Fields and Their Applications, 2010, 16: 329-333

[5] Chen Z, Xiao G. 'Good' Pseudo-random binary sequences from elliptic curves[EB/OL]. http://eprint.iacr.org/2007/275.pdf, 2007

[6] Merai L. Construction of pseudorandom binary sequences over elliptic curves[EB/OL]. http://www.renyi.hu/~merai/pub/ratfn-elliptic.pdf, 2009

[7] Chen Z. Elliptic curve analogue of Legendre sequences [J]. Monatsh. Math 2008, 154: 1-10

[8] Lam C Y, Gong G. Randomness of elliptic curve sequences[R/OL]. http://www.cacr.math.Uwaterloo.ca, Technical Repots, CORR2002-18, 2002

[9] Mauduit C, Sarkozy A. On finite pseudorandom binary sequences I: measures of pseudorandomness, the Legendre symbol[J]. Acta Arithmetica, 1997, 82: 365-377

[10] Shparlinski I E. Cryptographic applications of analytic number theory: complexity lower bounds and pseudorandomness[C]// Progress in Computer Science and Applied Logic. Birkhauser Verlag, Basel, 2003

[11] Kohel D, Shparlinski I E. Exponential sums and group generators for elliptic curves over finite fields[C]// Proc. Algorithmic Number Theory Symposium 2000. Berlin: Springer-Verlag, 2000: 395-404

[12] 刘华宁. 数论中的伪随机二进制序列[M]. 北京：科学出版社，2008

(上接第 39 页)

[3] Wittie M P, Harras K A, Almeroth K C, et al. On the implications of routing metric staleness in delay tolerant networks[J]. Computer Communications, 2009, 32(16): 1699-1709

[4] François J-M, Leduc G. Routing based on delivery distributions in predictable disruption tolerant networks [J]. Ad-hoc Networks, 2009, 7(1): 219-229

[5] Daly E M, Haahr M. The challenges of disconnected delay-tolerant MANETs[J]. Ad-hoc Networks, 2010, 8(2): 241-250

[6] Akyildiz I F, Pompili D, Melodia T. Underwater acoustic sensor networks: research challenges[J]. Ad-hoc Networks, 2005, 3(3): 257-279

[7] Sozer E M, Stojanovic M, Proakis J G. Underwater acoustic networks[J]. IEEE Journalof Oceanic Engineering, 2000, 25(1): 72-83

[8] Chitre M, Shahabudeen S, Stojanovic M. Underwater acoustic communications and networking: Recent advances and future challenges[J]. Marine Technology Science Journal, 2008, 42(1): 103-116

[9] Stojanovic M. Recent advances in high speed underwater acoustic communications[J]. IEEE Journal of Oceanic Engineering, 1996, 21(4): 125-136

[10] 于宏毅. 无线移动自组织网[M]. 北京：人民邮电出版社，2005: 249-258

[11] Rice J. SeaWeb acoustic communication and navigation networks [C]// The International Conference on Underwater Acoustic-Measurements: Technologies and Results. July 2005

[12] Crawley E, Nair R, Rajagopalan B, et al. Aframework for QoS-based routing in the internet[OL]. Aug. 1998. http://citeseerx.ist.psu.edu/viewdoc/summary? doi=10.1.1.136.6515

[13] Small T, Haas Z J. The shared wireless infostation model: A new ad hoc networking paradigm[C]// The 4th ACM international symposium on Mobile Ad-hoc Networking. 2003: 233-244

[14] Chen D, Varshney P K. QoS support in wireless sensor networks: a survey[C]// International Conference on Wireless Networks. 2004

[15] Vahdat A, Becker D. Epidemic routing for partially connected ad-hoc networks[R]. Department of Computer Science, Duke University, Durham, 2000

[16] Jones E P C, Li L, Ward P A S. Practical routing in delay-tolerant networks[C]// SIGCOMM'05 on Delay-Tolerant Networking. Philadelphia, USA, Aug. 2005: 237-243

[17] 于磊磊，柴乔林，刘鑫，等. 一种节能的无线传感器网络 QoS 路由算法[J]. 计算机应用，2007, 27(2): 376-379