基于超奇异椭圆曲线的序列*)

陈智雄[1,2] 邹 超[1] 肖国镇[1]

(西安电子科技大学 ISN 国家重点实验室 西安 710071)[1] (莆田学院数学系 福建莆田 351100)[2]

摘 要 Gong 等提出了利用超奇异椭圆曲线来构造伪随机序列,本文推广了此类序列的周期的结论,并简化了其证明方法;给出了此类序列的线性复杂度的下界;并对序列的构造方法加以修改,使得 0-1 分布平衡但不改变其线性复杂度的界和周期。

关键词 椭圆曲线,伪随机序列,流密码

Sequences from Supersingular Elliptic Curves

CHEN Zhi-Xiong[1,2] ZOU Chao[1] XIAO Guo-Zhen[1]

(National Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071)

(Department of Mathematics, Putian University, Putian, Fujian 351100)

Abstract G. Gong et al introduced a method for generating pseudorandom binary sequences by applying trace functions to supersingular elliptic curves over $GF(2^n)$, n odd. In this note, a generalized result on the period and the lower bound on linear complexity of such sequences are given. And a modified version of this method is presented to eliminate the 0-1 unbalance without changing the period and the bound of linear complexity of such sequences.

Keywords Elliptic curves, Pseudorandom sequences, Stream ciphers

1 引言

自从 Koblitz[1]和 Miller[2]提出利用椭圆曲线来构造公钥密码系统以来,椭圆曲线密码体制就得到广泛的研究,并已得到广泛的应用。椭圆曲线和序列的研究也开始结合起来[3]。20 世纪 90 年代末,Gong 等利用迹函数真正把椭圆曲线点群与伪随机序列结合起来,提出了构造椭圆曲线序列三种不同的方法[4],构造了椭圆曲线点群上的线性递归序列[5],并研究了它们的随机性质[4~6]。而文[7]则推广了上述的构造方法,分别利用椭圆曲线的加法特征与乘法特征来构造椭圆曲线序列。

在文[4]中,讨论了用有限域 $GF(2^n)$(其中 n 为奇数,本文始终假设 n 为奇数)上的超奇异椭圆曲线构造的序列的随机性质:周期、线性复杂度和 0-1 分布。

$GF(2^n)$上的超奇异椭圆曲线当 $y^2+y=x^3+c_4x+c_6$ 在 n 奇数时有三个同构类[8]:

(1)$y^2+y=x^3$;(2)$y^2+y=x^3+x$;(3)$y^2+y=x^3+x+1$。

在本文中,我们称(1)为Ⅰ-型椭圆曲线,(2)和(3)称为Ⅱ-型椭圆曲线。由它们构造的序列分别称为Ⅰ-型序列和Ⅱ-型序列。

事实上,文[4]研究了以上两种类型序列的周期、0-1 分布以及Ⅰ-型序列的线性复杂度。从有关结论知Ⅰ-型序列的 0-1 分布不平衡。因此,本文中,我们推广了关于Ⅱ-型序列周期的结论,并简化了其证明方法;给出了Ⅱ-型序列的线性复杂度的下界;并对Ⅰ-型序列的构造方法加以修改,使得 0-1 分布平衡但不改变其线性复杂度的界和周期。

下面简单介绍超奇异椭圆曲线的群运算和椭圆曲线序列的构造方式。

有限域 $GF(2^n)$上的超奇异椭圆曲线用标准形式表示为 $E: y^2+y=x^3+c_4x+c_6$。E 上的点集记为 $E(F_{2^n})=\{(x,y)\in GF(2^n)\mid y^2+y=x^3+c_4x+c_6\}$,$E$ 关于"弦切法"所定义的"加法"运算构成 Abel 群,其单位元为无穷远点 O。对 E 上不同的两点 $P=(x_1,y_1)$和 $Q=(x_2,y_2)$,E 的加法运算如下:

当 $x_1=x_2$ 时,$P+Q=O$。否则 $P+Q=(x_3,y_3)$:

$x_3=\lambda^2+x_1+x_3$, $y_3=\lambda(x_1+x_3)+y_1+1$

其中 $\lambda=(y_1+y_2)/(x_1+x_2)$。

特别地,$2P=P+P=(x_3,y_3)$:$x_3=x_1^4+c_4^2$, $y_3=(x_1^2+c_4)(x_1+x_3)+y_1+1$。

如果 $P+Q=O$,称 Q 是 P 的反点(负点),记为 $Q=\tilde{P}$,此时 $\tilde{P}=(x,1+y)$,如果 $P=(x,y)$。

根据文[8]第 104 页,上述三种同构类的超奇异椭圆曲线的有理点群都是循环群,它们的阶分别是 2^n+1, $2^n\pm 2^{m+1}+1$, $2^n\mp 2^{m+1}+1$,其中 n 为奇数,$n=2m+1$。故可从这些循环群中选择一个生成元 P,记 P 的阶为 v(即以上循环群的阶),构造序列的方法之一如下[4]:

由 $E\setminus\{O\}$上 $v-1$ 个不同的点 $P,2P,3P,\cdots,(v-1)P$,令 $iP=(x_i,y_i)$,计算 $a_i=Tr(x_i)$, $b_i=Tr(y_i)$,其中 $Tr: GF(2^n)\to GF(2)$为迹函数。于是得到序列 $S_0=(a_1a_2\cdots a_{v-1})$和 $S_1=(b_1b_2\cdots b_{v-1})$,并记 $S=(a_1b_1a_2b_2\cdots a_{v-1}b_{v-1})=(S_0,S_1)^T$,即 $S_{2i-1}=a_i$, $S_{2i}=b_i$, $i=1,2,\cdots,v-1$,那么 S 是长度为 $2(v-1)$的序列,称该序列为由超奇异椭圆曲线构造的序列,简称为椭圆曲线序列,即为上文所述的Ⅰ-型序列和Ⅱ-型序列。注意到以上超奇异椭圆曲线的特殊性质,由 iP 与 $(v-i)P$ 互为反点,从而 $x_{v-i}=x_i$, $y_{v-i}=1+y_i$,易知 $S_0=(A,\tilde{A})$, $S_1=(B,\tilde{B}+1)$,其中序列 $\overleftarrow{W}$ 表示序列 $W=(w_1w_2\cdots w_t)$的逆序,即 $\overleftarrow{W}=(w_tw_{t-1}\cdots w_1)$, $\overleftarrow{W}+1=(w_1+1,w_2+1,\cdots,w_t+$

*)基金项目:97-3 项目(G1999035804),福建省教育厅科学基金(JA04264)资助项目。陈智雄 博士研究生。

1)。并视 S 是以 $(a_0b_0a_1b_1\cdots a_{v-1}b_{v-1})$ 为一个周期段的无限序列。

对于二元序列 $S=(s_0s_1s_2\cdots)$，如果存在正整数 k 使得 $s_i=s_{k+i}$，$i=0,1,\cdots$，则称 k 为 S 的周期，满足该性质的最小的数 k 称为 S 的最小周期，记为 $per(S)$。多项式 $f(x)=x^l+c_{l-1}x^{l-1}+\cdots+c_1x+c_0\in F_2[x]$ 如果满足：$s_{l+i}=c_{l-1}s_{l-1+i}+\cdots+c_1s_{1+i}+c_0s_i$，$i=0,1,\cdots$，则称 $f(x)$ 为序列 S 的特征多项式，次数最低的一个特征多项式称为极小多项式。序列 S 的极小多项式的次数就是 S 的线性复杂度，记为 $L(S)$。

有关椭圆曲线和序列的详细内容可分别参见文[8,9]。

2 II-型序列的周期

本节给出Ⅱ-型序列的周期的简便证明，同时降低了文[4]中 Theorem 3 的条件，也即推广了文[4]的相关结论。

定理 1 设 m 为偶数，二元序列 $S_0=(c_1c_2\cdots c_{\frac{m}{2}}\cdots c_m)$。令 $m=2^tl=kl$，其中 $k=2^t$，l 为奇数且其最大真因子为 l_1。若 $c_m=c_{\frac{m}{2}}+1$ 且存在 $i,j:1\leqslant i<j\leqslant l/l_1$ 使得 $c_{il_1}=1+c_{jl_1}$，则 S_0 的最小周期 $per(S_0)=m$。

证明：首先证 $2^{t-1}l$ 不是 S_0 的周期。否则，$c_{\frac{m}{2}}$ 与 c_m 分别属于 S_0 的第一周期和第二周期的最后一项，与已知 $c_m=c_{\frac{m}{2}}+1$ 矛盾。从而 $2^{t-1}l$ 的任何因子也都不是 S_0 的周期；其次证 2^tl_1 也不是 S_0 的周期，因为存在 $i,j:1\leqslant i<j\leqslant l/l_1$ 使得 $c_{il_1}=1+c_{jl_1}$。从而 2^tl_1 的任何因子也都不是周期。故 kl 的任何真因子都不是周期，从而 $per(S_0)=m$。证毕。

定理 2 设 m 为偶数，二元序列 $S_0=(c_1c_2\cdots c_{\frac{m}{2}}\cdots c_m)$ 满足定理 1 的条件，$S_1=(d_1d_2\cdots d_m)$ 为任一二元序列，则序列 $S=(S_0,S_1)^T=(c_1d_1c_2d_2\cdots c_md_m)$ 的最小周期为 $per(S)=2m$。

证明：1) $per(S)$ 是偶数。若 $per(S)$ 为奇数，由 $per(S)\mid 2m$，知 $per(S)\mid m$，即 m 是 S 的一个周期，于是将序列 S 分成长度为 m 的两个周期段 $(c_1d_1\cdots c_{\frac{m}{2}}d_{\frac{m}{2}})(c_{\frac{m}{2}+1}d_{\frac{m}{2}+1}\cdots c_md_m)$，则对应项 $c_m=c_{\frac{m}{2}}$，与 S_0 的条件矛盾；

2) 设 $per(S)=2r$，由 $per(S)\mid 2m$ 得 $r\mid m$。如果 $r<m$，由 $s_{2i-1}=c_i$，$i=1,2,\cdots$，则对所有的 $j=1,2,\cdots$，有 $c_{r+j}=s_{2(r+j)-1}=s_{2r+2j-1}=s_{2j-1}=c_j$，从而 r 是 S_0 的一个周期，与定理 1 矛盾，故 $r=m$，从而 $per(S)=2m$。证毕。

由Ⅱ-型椭圆曲线的加法知，对点 $P=(x,y)$ 及其二倍点 $2P=(x',y')$，有 $a'=Tr(x')=Tr(x^4+1)=Tr(x)+1=a+1$，故 II-型序列满足定理 2 的条件，有如下推论。

推论 设 v 为Ⅱ-型超奇异椭圆曲线的有理点群的阶，则Ⅱ-型序列的周期为 $2(v-1)$。

3 II-型序列的线性复杂度

由于 II-型超奇异椭圆曲线的有理点群的阶 $v=2^n\pm2^{m+1}+1$，其中 $n=2m+1$，于是 II-型序列 $S=(a_1b_1a_2b_2\cdots a_{v-1}b_{v-1})$ 的最小周期为 $2(v-1)=2^{n+1}\pm2^{m+2}=2^{m+2}(2^{n-m-1}\pm1)$。这里考虑其中一种情况，即令 $k=2^{m+2}$，$l=2^{n-m+1}+1$。设 $f(x)$ 是 S 的极小多项式，则 $f(x)\mid(1+x^l)^k$。根据文[4]，S 的 Hamming 重量 $W_H(S)$ 为偶数（其实 II-型序列 0-1 分布平衡），从而 $f(x)$ 是 $(1+x^l)^k=(1+x)^k(x^{l-1}+\cdots+x+1)^k$ 的真因式。设 $f(x)=(1+x)^\alpha p_1(x)^{\beta_1}\cdots p_t(x)^{\beta_t}$ 为既约分解，其中 p_i 是 $x^{l-1}+\cdots+x+1$ 的既约因式，指数 $k\geqslant\alpha\geqslant0$，$k\geqslant\beta_i\geqslant1$，$i=1,2,\cdots,t$，则

1) α,β_i，$i=1,2,\cdots,t$ 至少有一个大于 $\frac{k}{2}$。如果 α,β_i，$i=1,2,\cdots,t$ 都小于或等于 $\frac{k}{2}$，则 $f(x)\mid(1+x^l)^{\frac{k}{2}}$，与 S 的最小周期为 kl 矛盾；

2) $f(x)$ 必含有 $x^{l-1}+\cdots+x+1$ 的既约因式。否则如果 $f(x)=(1+x)^\alpha$，则 $f(x)\mid(1+x)^k$，即 $f(x)$ 以 k 为周期，矛盾；

3) 设 $\gamma_1,\cdots,\gamma_t$ 分别是既约多项式 $p_1(x),\cdots,p_t(x)$ 的根，则 $\gamma_1,\cdots,\gamma_t$ 的阶的最小公倍数为 l。如果 $\gamma_1,\cdots,\gamma_t$ 的阶的最小公倍数为 $l_1<l$，由于 γ_i 的阶都是 l 的因子，显然 $l_1\mid l$，可知 $f(x)\mid(1+x^{l_1})^k$，同样与 S 的最小周期为 kl 矛盾。

于是当 $f(x)$ 含有 l 阶根时，可令 $f(x)=(1+x)^\alpha p(x)^\beta$，其中既约因式 $p(x)$ 的根的阶为 l，由 $2^{deg(p(x))}=1 \bmod l$，易知 $\deg(p(x))=n-1$。由 1)，当 $\alpha=\frac{k}{2}+1$，$\beta=1$ 时，$f(x)$ 的次数最低，即 $L(S)\geqslant\alpha+(n-1)\beta=n+2^{\frac{n+1}{2}}$；

当 $f(x)$ 不含有 l 阶根时，由 3)，设 $f(x)$ 含有根 $\gamma_1,\cdots,\gamma_t$，这些根的阶的最小公倍数为 l，且所对应的既约多项式分别为 $p_1(x),\cdots,p_t(x)$。于是令 $f(x)=(1+x)^\alpha p_1(x)^{\beta_1}\cdots p_t(x)^{\beta_t}$，由 1)，令 $\alpha=\frac{k}{2}+1$，$\beta_i=1$，$i=1,\cdots,t$ 时，

$$\deg(f(x))=(\frac{k}{2}+1)+\deg(p_1(x))+\cdots+\deg(p_t(x)),$$

即 $L(S)\geqslant2^{\frac{n+1}{2}}+1+\sum_{i=1}^{t}\deg(p_i(x))$。其中 $\deg(p_i(x))$ 可通过 $2^{\deg(p_i(x))}=1 \bmod|\gamma_i|$ 求得。于是有如下结论：

定理 3 II-型序列的线性复杂度的下界为 $\min\{2^{\frac{n+1}{2}}+1+\sum_{i=1}^{t}\deg(p_i(x)),n+2^{\frac{n+1}{2}}\}$。

例 1 取 $n=2m+1=7$，II-型序列 S 的周期 $per(S)=2^{m+2}(2^{n-m+1})=32\times9=288$，其极小多项式 $f(x)$ 是 $1+x^{288}=(1+x^9)^{32}=(1+x)^{32}(1+x+x^2)^{32}(1+x^3+x^6)^{32}$ 的因式，于是 $f(x)$ 至少含有 $1+x^3+x^6$ 的因子，当 $f(x)=(1+x)^{17}(1+x^3+x^6)$ 时，次数最低，即 $L(S)\geqslant23$。

注：由于 II-型序列的 0-1 分布平衡，故其线性复杂度可能大于此下界。

4 修改的 I-型序列

I-型序列是由同构与 $y^2+y=x^3$ 的超奇异椭圆曲线构造的序列，这类曲线的有理点群的阶为 2^n+1，故 I-序列 S 的最小周期为 2^{n+1}，线性复杂度 $2^n<L(S)\leqslant2(2^n-1)$，但 0-1 分布不平衡，有 $2^{\frac{n-1}{2}}$ 偏斜[4]。设 $S=(S_0,S_1)^T=(a_1b_1a_2b_2\cdots a_{v-1}b_{v-1})$，$v=2^n+1$。

首先我们指出，文[4]中 Theorem 4 关于线性复杂度的上界应为 $L(S)\leqslant2^{n+1}-1$，因为文[4]Proposition1 的结论是错误的，反例如下：

例 2[4] 利用本原多项式 $f(x)=x^5+x^3+1$ 构造域 $GF(2^5)$，设 β 是 $f(x)$ 的一个根。取椭圆曲线 $E:y^2+y=x^3$，则 $E(GF(2^5))$ 的阶为 33。$P=(\beta,\beta^{23})$ 是一个生成元，于是得到 I-序列 $S=(S_0,S_1)^T$：$S_0=(00101110111011110011110110111101100)$ 及 $S_1=(01101001101101101001001001101001)$。$S$ 的极小多项式为 $m(x)=(1+x)^{62}$，而 S_0 的极小多项式为 $m_0(x)=(1+x)^{28}$，显然 $m(x)$ 不整除 $m_0(x^2)$。

（下转第 69 页）

由于攻击者所选取的加密明文 $m>p$，则 $m=lp+m_i$，其中 l 为正整数。于是，密文

$$C=mG+rH=m_1G+lpG+rnG$$

因此，解密用户在 $E[P]$ 中执行的解密算法得到

$$\frac{\phi_p((p+2)C)}{\phi_p((p+2+G)} \bmod p=$$

$$\frac{\phi_p((p+2)m_1G+l(p+2)pG+r(p+2)nG)}{\phi_p((p+2)G)} \bmod p \qquad (1)$$

因为 $E_p(\bar{a},\bar{b})$ 的阶为 $p(p+2)$，于是在 $E_{p^2}(a,b)$ 中有

$$(p+2)m_1G+l(p+2)pG+r(p+2)nG$$
$$=(p+2)m_1G+O_{p^2}$$

这里的 O_{p^2} 是 $E_{p^2}(a,b)$ 中的单位元。所以

$$\frac{\phi_p((p+2)C)}{\phi_p((p+2)G)} \bmod p=\frac{\phi_p((p+2)m_1G+O_{p^2})}{\phi_p((p+2)G)} \bmod$$
$$p=m_1 \qquad (2)$$

由于 $p|m-m_q$，当攻击者得到解密明文 m_1 后，可以计算 $p=\gcd(m-m_1,n)$

攻击者求得素因子 p 后，能够完全分解模数 n。这样，攻击者可以运用第 2 节中的解密算法，计算

$$m=\frac{\phi_p((p+2)C)}{\phi_p((p\div2)G)} \bmod p$$

对所有的密文解密，从而成功攻击此加密体制。

结束语 本文对 Paillier 提出的基于椭圆曲线陷门离散对数加密体制的安全性进行了简单的分析，指出它存在的安全缺陷，不能抵抗选择密文攻击，在使用该加密体制时应当特别注意这一点。

为了避免这种不安全性，在实际应用中，不能向攻击者出示解密后的明文，然而，攻击者可以从解密结果的有效性得知他所选择的明文与素因子 p 的大小关系，这也为分解模数提供了重要的信息。

参 考 文 献

1 Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644～654

2 Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[A]. CACM, 1978, 21(2): 120～126

3 Koyama K, Maurer U, Okamoto T, Vanstone S. New Public-Key Schemes based on Elliptic Curves over the ring Z_n[A]. In: Advances in Cryptology, Proc. of Crypto'91, LNCS 576[C], Springer-Verlag, 1992. 252～266

4 Pallier P. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes[A]. Advances in Cryptology-EUROCRYPT'99, LNCS 1592[C], Springer-Verlag, 1999. 223～238

5 Catalano D, Gennaro R, Graham N H. The bit security of Paillier's encryption scheme and its applications[A]. Advances in Cryptology- EUROCRYPTO'01, LNCS 2045[C], Springer-Verlag, 2001. 229～243

6 Paillier P. Trapdooring Discrete Logarithms on Elliptic Curves over Rings[A]. Advances in Cryptology- ASIACRYPT 2000, LNCS 1976[C], Springer-Verlag, 2000. 573～584

7 Okamoto T, Uchiyama S. A new public key cryptosystem as secure as factoring[A]. Advances in Cryptology-EUROCRYPTO'98[C], LNCS 1043, 1998. 309～318

8 Semaev I A. Evaluation of Discrete Logarithms in a Group of p-Torsion Points of an Elliptic Curve in Characteristic p[J]. Math. Comp., 1998, 67: 353～356

9 Silverman J H. The Arithmetic of Elliptic Curves[M]. Springer-Verlag, GTM 106, 1986

(上接第 67 页)

既然 I-型序列的 0-1 分布不均，不妨假设 1 的个数比 0 多 $2^{\frac{n-1}{2}}$ 个，我们试图将 $2^{\frac{n-1}{2}}$ 个 1 改为 0，使得 0-1 分布均匀，而不改变该序列的周期和线性复杂度。下面提出三种方案。

方案一：1. 置 $a_v=a_{\frac{v}{2}}+1$；2. 随机改变除 a_v，$a_{\frac{v}{2}}$ 外的其它元素，使得 0-1 分布平衡。

方案二：1. 置 $a_v=a_{\frac{v}{2}}+1$；2. 随机改变除 a_v，$a_{\frac{v}{2}}$ 外的元素对 $\binom{a_i}{b_i}=\binom{1}{1}$ 为 $\binom{0}{0}$，使得 0-1 分布平衡。

方案三：1. 令 $S'_0=S_0\oplus S_1$，取 $S=(S'_0,S_1)^T$；2. 在 S'_0 中如果 $a_v=a_{\frac{v}{2}}$，则 a_1 与 a_v 对调。

方案一和方案二的(1)及方案三的(2)是为了保证修改后的 S 的周期仍为 2^{n+1}，可从定理 2 的证明看出。从而 S 的线性复杂度的界不变。方案三注意到 iP 与 $(v-i)P$ 互为反点，从而 $a_i=a_{v-i}$，$b_i=b_{v-i}+1$，于是 $\begin{pmatrix}a_i & a_{v-i}\\ b_i & b_{v-i}\end{pmatrix}=\begin{pmatrix}1 & 1\\ z & z+1\end{pmatrix}$ 或 $\begin{pmatrix}0 & 0\\ z & z+1\end{pmatrix}$，$z=0$ 或 1，那么把第二行加到第一行，得 $\begin{pmatrix}1+z & z\\ z & z+1\end{pmatrix}$ 或 $\begin{pmatrix}z & z+1\\ z & z+1\end{pmatrix}$，上下两行的 0、1 个数相同，从而使得 0-1 分布平衡。特别是方案三，在软件和硬件上都易实现。

例 3 条件同例 2，应用方案三，

$S'_0=S_0\oplus S_1=(01000111011010001110100100011101)$，那么

$S=(S'_0,S_1)^T=(00110100011010110110110110010100111010011000011000010110111000011)$，$S$ 的极小多项式为 $m(x)=(1+x)^{61}$。

参 考 文 献

1 Koblitz N. Elliptic curve cryptosystems[J]. Math. Comp., 1987, 48: 203～209

2 Miller V. Uses of elliptic curves in cryptography[A]. Advances in Cryptology-CRYPTO'85[C]. LNCS 218. Berlin: Spring-Verlag, 1986. 417～426

3 Kaliski B. A pseudorandom bit generator based on elliptic logarithms[A]. Advances in Cryptology-CRYPTO'86[C]. LNCS 263. Berlin: Spring-Verlag, 1986. 84～103

4 Gong G, Berson T, Stinson D. Elliptic curve pseudorandom sequence generator[A]. In: Proc. of the sixth annual workshop on selected areas in Cryptography, LNCS 1758, Berlin: Spring-Verlag, (Extended http://www.cacr.math.uwaterloo.ca:[Technical Reports, CORR1998-53]. 1998. 34～48

5 Gong G, Lam C. Linear recursive sequences over elliptic curves [A]. In: Proc. of Sequences and Their Applications-SETA'01 [C]. DMTCS series. Berlin: Spring-Verlag, 2001. 182～196

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

7 Beelen P H T, Doumen J M. Pseudorandom sequences from elliptic curves[A]. Finite Fields with Applications to Coding Theory, Cryptography and Related Areas [C]. Berlin: Spring-Verlag, 2002. 37～52

8 Enge A. Elliptic curves and their applications to cryptography: an introduction[M]. Kluwer Academic Publishers, Dordrecht, 1999

9 丁存生，肖国镇. 流密码及其应用[M]. 北京：国防工业出版社，1994