线性移位寄存器在安全 RSA 模数中应用的研究

姜正涛[1]，王勇[2]，王永滨[1]，王育民[3]

（1. 中国传媒大学 计算机学院，北京 100024；2. 北京工业大学 计算机学院，北京 100022；
3. 西安电子科技大学 ISN 国家重点实验室，陕西 西安 710071）

摘 要：运用线性移位寄存器（LFSR）序列模 2 个不同素数时的周期一般不同这一性质，尝试构造分解另一类 RSA 模数的方法；指出对于 RSA 模数 $n=pq$ 的一个素因子 p，当 p^2+p+1，p^3+p^2+p+1，…其中之一仅含有小的素因子时，给出的算法能够分解合数 $n=pq$，并给出了一个基于三级 LFSR 分解合数的实例来说明算法的具体运算步骤。根据该分解算法，在选取 RSA 模数时，为确保安全性，除避免已知的不安全因素以外，还需要保证 n 的素因子 p 满足 p^2+p+1，p^3+p^2+p+1，…均包含大的素因子。

关键词：LFSR；素数；整数分解；安全 RSA 模数

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2010)05-0135-06

Research on secure RSA modulus based on linear feedback shift register applications

JIANG Zheng-tao[1], WANG Yong[2], WANG Yong-bin[1], WANG Yu-min[3]

(1. School of Computer Science, Communication University of China, Beijing 100024, China;
2. School of Computer Science, Beijing University of Technology, Beijing 100022, China;
3. National Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an 710071, China)

Abstract: The periods of linear feedback shift register (LFSR) sequence modulo different primes were distinct in general. Using this property, a family of methods for factoring RSA modulus was constructed. For the RSA modulus $n=pq$, if the prime p satisfies that one of p^2+p+1, p^3+p^2+p+1,…was composed of small primes factors, it proposed a method for factorizing the composite integer $n=pq$. An instance was proposed to illustrate the specific procedure of the proposed factoring algorithm. Based on this factoring algorithm, to make security assurance in selecting RSA modulus, and in addition to avoid the already known insecure factors, one should also make sure that the prime factor p of n must satisfy that each of the p^2+p+1, p^3+p^2+p+1,…include a large prime factor.

Key words: LFSR; prime number; integer factorization; secure RSA modulus

---

收稿日期：2008-11-20；**修回日期**：2010-01-10

基金项目：中国博士后科学基金资助项目（20060400035）；国家自然科学基金资助项目（60672102, 60473027, 60963624）；国家重点基础研究发展计划（"973"计划）基金资助项目（2003AA144150）；国家"211"工程学科建设基金资助项目；2009 年度北京市文化创意产业发展专项基金资助项目

Foundation Items: China Postdoctoral Science Foundation (20060400035); The National Natural Science Foundation of China (60672102, 60473027, 60963624); The National Basic Research Program of China (973 Program) (2003AA144150); The National "211" Development Fund for Key Engineering Programs; 2009 Special Funds for Development of Beijing Culture and Creation Industry

1 引言

RSA 密码体制是目前最常用的一种密码体制[1]，它的出现是从纯粹数论走向应用的又一次伟大创举。现有的许多密码体制可以认为是 RSA 的变形[2,3]，它们基于的困难问题都是大整数分解问题，该问题被认为是 NP 问题，尽管整数的因子分解问题已经经历了长达几百年的研究，但目前仍未发现切实有效的算法，模数分解的方法研究问题在密码学和数学领域进展相对缓慢，通常整数分解算法都利用素因子本身的特殊结构。并不是所有的素因子都具有那样的代数结构使得分解变得容易，然而一个密码体制的安全性容不得半点运气，利用这些结构研究整数分解问题，以最大可能避免密码体制潜在的不安全因素，为进一步提高密码体制的安全性提供了核心和重要的参考依据[4]。

针对素因子的特殊代数结构，1974 年，J. M. Pollard 提出了一种整数分解算法，称为 $p-1$ 方法[5]，H. C. Williams 于 1982 年提出了另一种分解方法，称为 $p+1$ 方法[6]，当 $p-1$（相应的 $p+1$）仅有小的素因子时，可有效地分解 $n=pq$；相比之下，尽管后者的效率可能要略低一些，但这已有足够的理由要求安全的 RSA 模数避免这一情形（$p+1$ 仅含有小的素因子）的发生。这样在选取安全的 RSA 模数时，需要同时保证 $p-1$，$p+1$ 含有大的素因子，E. Bach 等运用分圆多项式对整数分解问题作了进一步研究，由于其中的结果基于代数数论知识以及在 Riemann 猜想为正确的假设情况下得到的，这一方法的效率比较低[7]。Gysin 等对 RSA 一类的密码体制运用循环攻击方法，对如何选取更安全的 RSA 模数做了比较详细的分析[8, 9]。

运用本文给出的“线性移位寄存器（LFSR）序列模 2 个不同素数时的周期一般不同”这一性质，研究 RSA 安全模数形式的基础性问题，探讨了一种新的基于 LFSR 的整数分解方法，并运用三级 LFSR，给出了一个分解示例。根据本文的分解方法，在选取安全的 RSA 模数 n 时，除需要避免选取含有目前已知的不安全因素的合数外，对于 n 的素因子 p，还需要满足 p^2+p+1，甚至 $p^3+p+1,\cdots$ 均包含大的素因子，这一结果在原有安全素数形式的基础上进一步认识了 RSA 安全模数形式这一核心安全问题。

2 三级线性反馈移位寄存器序列

假设多项式

$$f(x)=x^3-ax^2+bx-1 \tag{1}$$

是 $Z[x]$ 上的不可约多项式。

定义 1 三阶线性反馈移位寄存序列。给定 s_0，s_1，s_2，如果序列 $\bar{s}=\{s_k\}$ 满足

$$s_j+c_1s_{j-1}+c_2s_{j-2}+c_3s_{j-3}+d=0,\ j\geqslant 3 \tag{2}$$

其中，c_1,c_2,c_3 为整数，则称 $\bar{s}=\{s_k\}$ 为三阶线性反馈移位寄存序列。

根据 Newton 公式[10]，如果 $c_1=-a$，$c_2=b$，$c_3=-1$ 以及 $s_0=3, s_1=a, s_2=a^2-2b$，则

$$s_k=\alpha_1^k+\alpha_2^k+\alpha_3^k,\ k=0,1,\cdots,n$$

其中，$\alpha_1,\alpha_2,\alpha_3$ 为 $f(x)=0$ 的 3 个根。

此时，式(2)实际上就是

$$s_k=as_{k-1}-bs_{k-2}+s_{k-3}, k=3,4,\cdots,n \tag{3}$$

其中，$s_0=3, s_1=a, s_2=a^2-2b$。

不难证明，在有限域 GF(p)中，如果式(1)中的 $f(x)$ 不可约，则 $f(x)=0$ 的 3 个根均满足

$$\alpha_i^{p^2+p+1}\equiv 1(\mathrm{mod}\ p),\ i=1,2,3$$

因此，$\{s_k\}$ 在 GF(p)中是周期序列[11]，并且满足

$$s_{p^2+p+1}\equiv 3(\mathrm{mod}\ p) \tag{4}$$

由此可得，当素数 p,q 不相等时，$\{s_k\}$ 在 Z_p 和 Z_q 上的周期一般不同。

3 Pollard 的 $p-1$ 方法介绍

Pollard 的 $p-1$ 方法是当整数 n 的素因子 p 满足 $p-1$ 仅含有小的素因子时，给出的一种整数分解方法。

假设 $n=pq$，p,q 均为素数，其中，

$$p=\left(\prod_{i=1}^{m}p_i^{\alpha_i}\right)+1$$

这里 p_i 是第 i 个素数，满足对于某个给定的整数 B，

有 $p_i^{\alpha_i} \leqslant B$， $i=1,2,\cdots,m$。

令 $\beta_i = \lfloor \log_{p_i} B \rfloor$，并令

$$R = \prod_{i=1}^{m} p_i^{\beta_i} \tag{5}$$

显然有 $p-1 \mid R$，于是如果 $(a,p)=1$，则 $a^R \equiv 1 (\mathrm{mod}\ p)$，因此 $p \mid (n, a^R-1)$。Pollard 的 $p-1$ 方法运行过程如下。

对于给定的 B，假设 $R = r_1 r_2 \cdots r_l$，满足 $p_i^{\alpha_i} \mid r_i (i=1,2,\cdots,m,\ l \geqslant m)$，选取 $a_0 = a$，其中 $(a,n)=1$，定义

$$a_i \equiv a_{i-1}^{r_i} (\mathrm{mod}\, n),\ i=1,2,\cdots,l$$

最后，计算 $(a_m - 1, n)$。

类似地，当 $p+1$ 仅包含小的素因子时， Williams 方法使用 Lucas 序列对模数 n 进行分解[6]。

4　p^2+p+1 方法

4.1　分解方法 1

假设 $n = pq$，并且其中一个素因子 p 满足

$$p^2 + p + 1 = \prod_{i=1}^{m} p_i^{\alpha_i}$$

其中， p_i 是第 i 个素数，满足对某个给定的有界整数 B 和 B'，有 $p_i \leqslant B$， $p_i^{\alpha_i} \leqslant B' (i=1,2,\cdots,m)$。

令 $\beta_i = \lfloor \log_{p_i} B' \rfloor$，并令

$$R = \prod_{i=1}^{m} p_i^{\beta_i}$$

显然有 $p^2 + p + 1 \mid R$。

根据式(4)，当 $f(x) = x^3 - ax^2 + bx - 1$ 在 GF(p) 中不可约时，有 $p \mid s_R - 3$。

因此，计算 $\gcd(s_R - 3, n)$ 可能求得素因子 p。

算法分析如下。

引理 1　设 $\{s_k\}$ 如式(3)定义的递归序列，则对任意的整数 m, n 有[11]：

1) $s_{2n} = s_n^2 - 2s_{-n}$；

2) $s_{2n+1} = s_{2n} s_1 - s_{2n-1} s_{-1} + s_{2n-2}$。

计算 s_w：

令 $w = k_0 + k_1 2 + \cdots + k_{r-1} 2^{r-1} + k_r 2^r$，并令 $T_0 = 1$，$T_1 = 2T_0 + k_{r-1}$， $T_2 = 2T_1 + k_{r-2}$， …， $T_r = 2T_{r-1} + k_0$，因此

$$s_{T_i} = s_{2T_{i-1} + k_{r-1}} \ (i=1,2,\cdots,r)$$

若 $k_{r-i} = 0$，有：

$$s_{T_i} = s_{2T_{i-1}} = s_{T_{i-1}}^2 - 2s_{-T_{i-1}}$$

若 $k_{r-i} = 1$，有：

$$s_{T_i} = s_{2T_{i-1}+1} = s_{2T_{i-1}} s_1 - s_{2T_{i-1}} s_{-1} + s_{2T_{i-1}-2}$$

当 $w<0$ 时，用类似的算法可求得 s_w。

计算 s_{T_i} 需要构造三元组 $(s_{T_i-1}, s_{T_i}, s_{T_i+1})$，并可从三元组 $(s_{T_{i-1}-1}, s_{T_{i-1}}, s_{T_{i-1}+1})$ 计算得到，计算每一对 s_{T_i} 和 s_{-T_i} 约需要 3 个乘法运算，这样计算 $(s_{T_i-1}, s_{T_i}, s_{T_i+1})$ 大约需要 9 个乘法运算。因此，在 Z_n 中求 S_R 需要 $9\lg R$ 次模 n 乘法运算[11]。

事实上，由式(4)可知，当 $f(x)$ 在 GF(p) 上不可约时，序列 $\{s_k\}$ 在 GF(p) 上的周期为 p^2+p+1（或 p^2+p+1 的一个因子），仅知道 n，目前还无法求得 p^2+p+1 以及 $\lambda = (p^2+p+1)(q^2+q+1)$（可以证明知道两者之一均可以成功分解 n）；这里的分解算法就是当 p^2+p+1 仅含有小的素因子的情况下，通过随机选取 GF(p) 上的不可约多项式来分解 n。

由下述定理可知，通过随机选取获得 GF(p) 上不可约多项式的概率为 1/3。

定理 1[12]　q 元域中 n 次不可约多项式的个数为

$$I_n = \frac{1}{n} \sum_{d \mid n} u(d) q^{(n/d)}$$

其中， $u(d)$ 为 Moebius 函数。

4.2　分解方法 2

假设 $n = pq$，并且

$$p^2 + p + 1 = \delta R = \delta \prod_{i=1}^{m} p_i^{\alpha_i}$$

其中，p_i 是第 i 个素数，满足对给定的整数 B 和 B'，有 $p_i \leqslant B$， $p_i^{\alpha_i} \leqslant B' (i=1,2,\cdots,m)$，以及对于另外 2 个上界 B_1, B_2，素数 δ 满足 $B_1 \leqslant \delta \leqslant B_2$，在这种情况下显然有 $p \mid s_{R\delta} - 3$。

因此，计算 $\gcd(s_{R\delta} - 3, n)$ 可能求得素因子 p。

令 $\{\delta_i \mid i=1,2,\cdots,\sigma\}$ 是区间 $[B_1, B_2]$ 内的所有有

序素数，并令 $2d_j=\delta_{j+1}-\delta_j$，由于这样的差值增长很慢，于是不相同的 d_j 个数不是很多[6]。

令 $V=s_R$，$V_1=s_{R\delta_1}$，…，$V_{j+1}=s_{R(\delta_j+2d_j)}$（$j=1,2,\cdots,\sigma$）。

计算：

$$G_t=\gcd\left(\prod_{i=0}^{c}(V_{t+i}-3),n\right),\ t=0,c,2c,\cdots,\left\lfloor\frac{\sigma}{c}\right\rfloor c$$

不难证明，p 必整除某个 G_t，$t=0,c,2c,\cdots,\left\lfloor\frac{\sigma}{c}\right\rfloor c$。

计算顺序如下：

$$s_{R\delta_1}\rightarrow s_{R(\delta_1+2d_1)}=s_{R\delta_2}\rightarrow s_{R(\delta_2+2d_2)}=s_{R\delta_3}\rightarrow,\cdots,\rightarrow s_{R\delta_\sigma}$$

算法分析：

1）计算 $s_{R\delta_1}$ 需要 $9\lg(R\delta_1)$ 次模 n 乘法运算；

2）已知 $s_{R\delta_2}$，计算 $s_{R(\delta_1+2d_1)}$ 最多需要 $9\lg(Rd_1)$ 次模 n 乘法运算；

已知 $s_{R\delta_{\sigma-1}}$，计算 $s_{R(\delta_{\sigma-1}+2d_{\sigma-1})}$ 最多需要 $9\lg(Rd_{\sigma-1})$ 次模 n 乘法运算。

因此，平均约需要 $4.5(\sigma\lg R+\lg\delta_1+\lg d_1+\cdots+\lg d_{\sigma-1})$ 次模 n 运算。

注：当 p^2+p+1 含有小的素因子时，以上给出的针对 2 种不同情形的方法均可能分解 n。如果 p^2+p+1 含有大的素因子，此时不存在分解方法 1 和分解方法 2 中计算可行的上界 B、B_1，使得 p^2+p+1 中的素因子均满足 $p_i\leqslant B$（$i=1,2,\cdots,m$）以及 $B_1<\delta\leqslant B_2$，于是可以抵抗本文的分解方法。

在进行实际分解操作时，可以不考虑 3 次多项式的构造而直接随机选取式(3)形式的 LSFR 序列。如果 p^2+p+1 仅含有小的素因子，而 q^2+q+1 含有大的素因子，本文的算法总能成功分解 $n=pq$，可以把这样的合数 n 称为三级非对称合数（这是根据运用 LFSR 级数来定义安全合数的）（类似的对于 Pollard 的分解算法，若 $p-1$ 仅含有小的素因子，而 $q-1$ 含有大的素因子，可以把 n 称为一级非对称合数）；相反，p^2+p+1 和 q^2+q+1 都仅含有小的素因子就称 n 为三级对称合数（该类型的合数也是不安全的），若 p^2+p+1 和 q^2+q+1 均含有大的素因子就称 n 为三级安全合数。

5 举例

假设已知 $n=1846237$ 是 2 个素数的乘积，根据分解方法 2，分解步骤如下。

1) 构造 LFSR 序列

随机选取 Z_n 上的 LFSR 序列：

$$s_k=s_{k-1}+2s_{k-2}+s_{k-3}$$

该序列对应的多项式为 $f(x)=x^3-x^2+2x-1$（在 GF(P)上不可约的概率约为 1/3），其中初始值 $s_0=3,s_1=1,s_2=-3$。

2) 估计上界

假设 n 的其中一个素因子 p 满足

$$p^2+p+1=\delta\prod_{i=1}^{m}p_i^{\alpha_i}$$

本文估计相应的上界为 $B=15$，$B'=20$，$B_1=40$，$B_2=50$ 和 $B_1=400$，$B_2=500$。

由于 PC 机处理能力有限，适当缩小素数的上界，把 p^2+p+1 的小素因子的估计分为 3 类。

第 1 类：素因子 $p_i\leqslant 15$，$p_i^{\alpha_i}\leqslant 20$（如果计算能力强该值应取适当大一些，如 $p_i\leqslant 50$，$p_i^{\alpha_i}\leqslant 80$ 等）。

第 2 类：可能有比较大的一个素因子 p_i 在区间[40, 50]内（如果计算能力强，可把该类的估计放到在第 1 类中）。

第 3 类：更大一点的素因子 p_i 在区间[400, 450]内（根据计算资源的处理能力和允许时间，可适当把该区间放大一些，如[300, 500]）。

3) 运算

① 求 R

由于 $B=15$，则 $p_1=3$，$p_2=5$，$p_3=7$，$p_4=11$，$p_5=13$，由于 $\beta_i=\left\lfloor\lg_{p_i}B'\right\rfloor$，于是

$$R=\prod_{i=1}^{m}p_i^{\beta_i}=3^2\times7\times13=819$$

这里没有考虑素因子 5 和 11，是因为可以证明 p^2+p+1 形式的数不含有素因子 5 和 11。

② 求 G_t

列出区间[40, 50]内的所有素数：41, 43, 47；以及区间[400, 450]内的所有素数：401, 419, 421, 431, 433, 439, 443, 449；并计算以下 6 组数值：

$$G_1=\gcd((V_{41\times401R}-3)(V_{41\times419R}-3)(V_{41\times421R}-3)(V_{41\times431R}-3),\ 1846\,237)$$

$$G_2=\gcd((V_{41\times433R}-3)(V_{41\times439R}-3)(V_{41\times443R}-3)(V_{41\times449R}-3),\ 1846\,237)$$

$$G_3=\gcd((V_{43\times401R}-3)(V_{43\times419R}-3)(V_{43\times421R}-3)(V_{43\times431R}-3),\ 1846\,237)$$

$$G_4=\gcd((V_{43\times433R}-3)(V_{43\times439R}-3)(V_{43\times443R}-3)(V_{43\times449R}-3),\ 1846\,237)$$

$$G_5=\gcd((V_{47\times401R}-3)(V_{47\times419R}-3)(V_{47\times421R}-3)(V_{47\times431R}-3),\ 1846\,237)$$

$$G_6=\gcd((V_{47\times433R}-3)(V_{47\times439R}-3)(V_{47\times443R}-3)(V_{47\times449R}-3),\ 1846\,237)$$

经过计算求得 $G_1=1$，$G_2=1$，$G_3=1\,283$，$G_4=1$，$G_5=1$，$G_6=1$；于是，$p=1\,283$ 是 n 的一个因子，从而分解整数 $n=1\,846\,237$。

分析：$p-1=1\,282=2\times641$;

$$p^2+p+1=1\,647\,373=7\times13\times43\times421$$

此时，$p-1$ 的大素因子为 641 和一个素因子 2，无其他素因子，此时 p 为通常所说的“安全”素数，需要满足当 n 的素数因子很大时，Pollard 分解方法不可行。

从这一例子可以看出，当 Pollard 和现行的分解算法不可行时，不妨尝试本文给出的分解方法。

6　基于一般 LFSR 的整数分解

假设 $n=pq$，多项式

$$f(x)=x^d-a_{d-1}x^{d-1}-\cdots-a_1x-1$$

对应的 LFSR 为

$$s_{k+d}=a_{d-1}s_{k+d-1}+a_{d-2}s_{k+d-2}+\cdots+a_1s_{k+1}+s_k$$

其中，$k\in Z$，$(-1)^i a_{d-i}$ 为 $f(x)=0$ 根的初等对称多项式。

当 $f(x)$ 在 GF(p) 上不可约时，如果 $p^{d-1}+p^{d-2}+\cdots+p+1$ 是小的素因子的乘积，即

$$p^{d-1}+p^{d-2}+\cdots+p+1=\delta\prod_{i=1}^{m}p_i^{\alpha_i}$$

其中，p_i 是第 i 个素数，满足对某个给定的上界 B, B'，有 $p_i\leqslant B$，$p_i^{\alpha_i}\leqslant B'(i=1,2,\cdots,m)$；以及 B_1, B_2，有 $B_1\leqslant\delta\leqslant B_2$。

令 $\{\delta_i\mid i=1,2,\cdots,\sigma\}$ 是区间 $[B_1,B_2]$ 内的所有有序素数，类似于分解方法 2，计算

$$G_t=\left(\prod_{i=0}^{c}(V_{t+i}-3),n\right),\quad t=0,c,2c,\cdots,\left\lfloor\frac{\sigma}{c}\right\rfloor c$$

同样可以证明，p 必整除某个 G_t, $t=0,c,2c,\cdots,\left\lfloor\frac{\sigma}{c}\right\rfloor c$。

计算 $\gcd(G_t,n)$，可分解 n。

注：不经过认真筛选的模数 $n=pq$，很难保证 $p-1$, $p+1$, $p^2+p+1,\cdots$, $p^{d-1}+p^{d-2}+\cdots+p+1,\cdots$ 均不是小的素因子的乘积[13]，当 p 的指数 d 增大时，对计算资源的要求也随之增大；而当 d 不是很大时，本文的分解方法是可行的。

7　结束语

对于大整数 $n=pq$，当 p^2+p+1，p^3+p^2+, $p+1\cdots$仅有小的素因子时，本文给出了一种基于 LFSR 的分解方法，通过一个具体的分解实例，描述了具体的算法过程，简单分析了算法的效率。根据本文的 LFSR 分解方法以及已有的结果，如 Marc Gysin 等推广的 RSA 攻击[8]，在选取 RSA 密码体制的模数 n 时，为了确保 RSA 的安全性，RSA 模数的素因子 p 需要满足以下条件：

1) $p-1$ 和 $p+1$ 含有大的素因子 t,w；

2) $t-1$，$t+1$，$t+1,w-1$，$w+1$ 也均含有大的素因子；

3) p^2+p+1，甚至 $p^3+p^2+p+1,\cdots$也需要含有大的素因子。

以上 3 点是抵抗 LFSR 一类分解攻击需要避免的不安全因素，在实际中还需要同时考虑避免包含其他不安全因素[13,14]。本文从基本的运算过程入手，给了一类概率分解算法，进一步认识了安全 RSA 模数的结构这一核心安全问题，如何提高本文给出的分解算法的运算效率还需要进一步研究。

参考文献：

[1] RIVEST R, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Comm of the ACM, 1978, 21(2): 120-126.

[2] SMITH P, LENNON M. LUC: a new public-key system[A]. Proceeding of IFIP/Sec’93[C]. 1994. 103-117.

[3] KOYAMA K, MAURER U, OKAMOTO T, *et al*. New public-key schemes based on elliptic curves over the ring Z_n[A]. Advances in Cryptology- Crypto'91[C]. Springer-Verlag, 1992. 252-266.

[4] 姜正涛, 伍前红, 王育民. 关于 DH 密钥的多项式转化与比特安全性分析[J]. 通信学报, 2004, 25(10): 30-39.
JIANG Z T, WU Q H, WANG Y M. On analysis of polynomial transformation of DH secrete key and bit security[J]. Journal on Communications, 2004, 25(10): 30-39.

[5] POLLARD J M. Theorem on factorization and primality testing[A]. Proc Cambridge Philos Soc[C]. 1974.521-528.

[6] WILLIAMS H C. A p+1 method of factoring[J]. Math of Computation, 1982,39(159): 225-234.

[7] BACH E, SHALLT J. Factoring with cyclotomic polynomials[J]. Mathematics of Computation, 1989, 52(185): 201-219.

[8] GYSIN M, SEBERRY J. Generalized cycling attacks on RSA and strong RSA primes[A]. Information Security and Privacy, ACISP'99[C]. Springer-Verlag, 1999.149-163.

[9] GYSIN M. The discrete logarithm problem for lucas sequences and a new class of weak RSA moduli[A]. ICISC'98[C]. 1998. 201-209.

[10] EDWARDS H M. Galois Theory[M]. New York: Spring-Verlag, 1984. 6-13.

[11] GONG G, HARN L, WU H P. The GH public-key cryptosystems[A]. Proceedings of the Eighth Annual Workshop on Selected Areas in Cryptography[C]. Toronto, 2001.16-18.

[12] BERLAMKAMP E R. Algebraic Coding Theory[M]. New York: McGraw-Hill, 1968.

[13] WAGSTAFFJR S S. Cryptanalysis of Number Theoretic Ciphers[M]. Boca Raton: Chapman & Hall/CRC, 2002. 143-203.

[14] POMERANCE C. The quadratic sieve factoring algorithm[A]. Advances in Cryptology-EUROCRYPT'84[C]. Springer-Verlag, 1985. 169-182.

作者简介：

姜正涛（1976-），男，山东青岛人，中国传媒大学讲师，主要研究方向为密码算法理论、形式化安全、信息安全和信任管理等。

王勇（1974-），男，山东潍坊人，北京工业大学讲师，主要研究方向为网格计算、数字签名和信任管理等。

王永滨（1963-），男，北京人，中国传媒大学教授、博士生导师，主要研究方向为信息处理、计算机网络与信息安全等。

王育民（1936-），男，北京人，西安电子科技大学教授、博士生导师，主要研究方向为编码理论、密码学、信息安全等。