基于 LFSR 高次剩余问题构造公钥密码体制的研究

姜正涛 柳 毅 王育民
(西安电子科技大学综合业务网国家重点实验室 西安 710071)

摘 要 该文对用线性反馈移位寄存器(LFSR)构造公钥密码体制做了进一步的研究，定义了 LFSR 的高次(非)剩余问题，基于新的困难问题探讨了构造一种加解密不同于 GH 的密码原型，并给出了具体的加解密过程，证明了它的可行性；在此基础上，进一步把该体制改进为概率加密体制，克服了 GH 加密确定性的缺点，同时对体制的安全性和效率做了初步分析，具有单向性和语意安全性，最后证明了该体制的单向性等价于 LFSR 高次剩余问题，语意安全性等价于 LFSR 判断高次剩余问题。

关键词 公钥加密体制，LFSR 高次(非)剩余，单向性，语意安全性
中图分类号： TP309^{+}.7 **文献标识码**： A **文章编号**:1009-5896(2006)03-0542-04

Research on the Construction of Public-Key Cryptosystems Based on LFSR Residuosity Problem

Jiang Zheng-tao Liu Yi Wang Yu-min
(*National Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an* 710071, *China*)

Abstract Further research on the construction of public-key cryptosystem based on Linear Feedback Shift Register (LFSR) is provided, and the LFSR higher (non) residuosity problem is defined. Based on new intractability problems a new public-key encryption primitive with encryption/decryption procedures differ from GH is investigated. The encryption and decryption procedures are specified. It is further improved to be a probabilistic encryption scheme. Efficiency and security analysis of the proposed encryption scheme is provided. It has properties of one-wayness and semantic security. The one-wayness and semantic security are equivalent to higher LFSR residuosity and decisional LFSR residuosity problems respectively.

Key words Public-key encryption scheme, LFSR higher (non) residuosity, One-wayness, Semantic security

1 引言

几乎所有的公钥密码体制均基于数学函数，这些数学函数通常是陷门单向函数[1,2]。充分研究和利用数学中的困难问题，并应用于密码学研究领域历来是密码学研究的一个重要方面，不仅丰富了密码学理论，促进了密码应用的发展，同时也促进了数学领域对所涉及到的困难问题的深入探讨[3-5]。

基于 Lucas 序列，Smith 于 1994 年构造了一种公钥密码体制 LUC[6]。1999 年，Gong 等提出了一种基于三级线性移位寄存器序列(3-LFSR)的密码体制 GH，Gong 等同时也给出了一种效率较高的序列运算方法[7,8]。以上两种基于序列的密码体制的不足之处是它们的加密都是确定的，这就不适合用于某些需要加密体制具有语意安全性的特定场合，如对 0,1 或几个侯选人名单等数据的加密[9]。

2004-09-09 收到, 2005-04-21 改回
国家自然科学基金重点项目(69931010)和国家 973 计划(G1999035803)资助课题

本文对与 GH 相关的密码体制做进一步研究，定义了 3 次移位寄存器(3-LFSR)的(判断)高次剩余问题，基于 LFSR 的高次剩余困难问题尝试性地构造一种新的密码体制，并进一步把该体制改进成概率加密体制，能够克服原 GH 加密体制的确定性加密的缺点，具有语意安全性，最后简单分析了给出体制的安全性，其单向性和语意安全性分别等价于 LFSR 高次剩余问题和 LFSR 判断高次剩余问题。

2 三级线性反馈移位寄存器

定义 1 三级线性反馈移位寄存器序列 如果序列 $\overline{s}=\{s_k\}$，满足

$$s_j + c_1 s_{j-1} + c_2 s_{j-2} + c_3 s_{j-3} + d = 0,\quad j \geq 3 \tag{1}$$

则称 $\overline{s}=\{s_k\}$ 为三级线性反馈移位寄存器序列，简记为 3-LFSR。

假设多项式

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

是 $Z[x]$ 上的不可约多项式。

根据 Newton 公式，如果 $d=0$，$c_1=-a$，$c_2=b$，$c_3=-1$ 以

及 $s_0=3, s_1=a, s_2=a^2-2b$，则

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

其中 $\alpha_1,\alpha_2,\alpha_3$ 为 $f(x)=0$ 的 3 个根，为了不产生歧义我们可把 s_k 写成 $s_k(a,b)$，通常称 $s_k(a,b)$ (k=1,2, …)为由多项式: $f(x)=x^3-ax^2+bx-1$ 生成的 LFSR 序列。

此时，式(1)实际上就是

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

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(2)中的 $f(x)$ 不可约，则 $f(x)=0$ 的 3 个根均满足

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

因此，$\{s_k\}$ 在 GF(p)中是周期序列，并且满足

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

令 $\Delta=(p^2+p+1)(q^2+q+1)$，显然知道 n 的分解，就可以求得 Δ；反之，知道 Δ，也可以知道 n 的分解。

事实上，假设知道 Δ，攻击者的具体分解步骤如下：

$$\begin{aligned}\Delta&=(p^2+p+1)(q^2+q+1)\\&=p^2q^2+p^2q+p^2+pq^2+pq+q^2+q+1\\&=\left(p+q+\frac{n+1}{2}\right)^2-2pq-\left(\frac{n+1}{2}\right)^2+n^2+n+1\\&=\left(p+q+\frac{n+1}{2}\right)^2-3n+\frac{3}{4}(n+1)^2\end{aligned}$$

在整数范围内求平方根可以求得 $\xi=p+q$，于是 p, q 是方程:

$$x^2-\xi x+n=0$$

的两个根。

求解以上方程，可得 p, q，即可以分解 n。

注 1 以上关于周期与 RSA 模数分解的关系分析同样也适应于 GH 密码体制的安全性分析[7,8]。

定义 2 LFSR 生成元　对于式(2)和式(3)中式 $f(x)$和 $s_k(a,b)$，我们把 a,b 称为 LFSR 序列 s_k 的生成元，把数组(a,b)和 k 分别称为 LFSR 序列的底数和指数。

定义 3 LFSR 高阶元　当由(a,b)生成的 LFSR 序列是周期序列并且周期很大时，就称(a,b)为 LFSR 高阶元。

定义 4 Z_n上的LFSR δ-次剩余问题　假设 δ 为一整数，(a,b)为 Z_n^*中阶被 δ 整除的 LFSR 高阶元，其中$(\delta, \lambda/\delta)=1$，$\lambda=lcm(p^2+p+1, q^2+q+1)$，$r$ 为某一随机整数，$m\in Z_\delta$。由 $C=(s_{r\delta+m}(a,b), s_{-(r\delta+m)}(a,b))\ \mathrm{mod}n$ 求唯一的 m，称为 Z_n 上的 LFSR δ-次剩余问题。

定义 5 Z_n上的判断 LFSR δ-次剩余问题　参数同定义 4，已知 $C=(s_k(a,b), s_{-k}(a,b))\ \mathrm{mod}n$，判断 m 是否为零的问题称为 Z_n上的判断 LFSR δ-次剩余问题。

定义 6 语意安全　所谓语意安全，就是对任意两条明文 m_0和 m_1，随机选取其中之一加密，得密文 C，分析者在仅知道明文 m_0, m_1和密文 C 以及其它公开参数的情况下，不能在多项式时间内判断密文 C 对应的是哪一条明文。

本文在归约证明加密体制的语意安全性时，主要用到 LFSR 高次剩余问题的一个变形，即 LFSR 高次剩余加 1 问题。

定义 7 Z_n上的 LFSR δ-次剩余加 1 问题　参数同定义 4，已知 $C=(s_k(a,b), s_{-k}(a,b))\ \mathrm{mod}n$，判断 m 是否为 1 的问题称为 Z_n上的 LFSR δ-次剩余加 1 问题。

当 δ>2 时，我们把以上定义的 LFSR δ-次剩余问题统称为 LFSR 高次剩余问题[5]。

在模指数运算下，高次剩余问题与高次剩余加 1 问题是同等困难的，如假设群 $G=\langle g\rangle$，判断 $x\in G$ 是否具有 $x=g^{k\delta}$ 形式，当且仅当能够判断 x 是否具有 $g^{k\delta+1}$ 形式。对于 LFSR 序列，这两个问题的关系并不是如此明显，到底哪个问题更困难目前不得而知，关于这两个问题的确切关系需要在数学和密码学方面做进一步研究。

3　基于 LFSR 高次剩余的加密体制

3.1　体制描述(加密体制 1)

设 $\delta=p_1\cdots p_a q_1\cdots q_b$ 是 B-光滑的，B 为某个有界量，$p_1,\cdots,p_a,q_1,\cdots,q_b$ 为不同的小素数且$|\delta|=k$。令 $u=p_1\ldots p_a$，$v=q_1\cdots q_b$，$n=pq$ 为 RSA 模数，满足 $p^2+p+1=eup'$，$q^2+q+1=fvq'$ 且$(\delta, \lambda/\delta)=1$，其中 p',q' 均为大素数，通常情况下 $k\approx|n|/4$。(a,b)的选取见定义 2,定义 3。

简单的加、解密过程如下：

公开参数　$n, a, b, |\delta|=k$

秘密参数　p, q

加密　$m\in Z_\delta$，加密用户计算密文

$C=(s_m(a,b), s_{-m}(a,b))\ \mathrm{mod}n$

解密　解密用户在 Z_n上执行解密过程步骤如下：

(1) 计算 $C_{p_i}=s_{\lambda/p_i}(s_m, s_{-m})\ \mathrm{mod}n$；

(2) 对于 $j=0,\cdots,p_i-1$ 分别计算 $C_j=s_{j\lambda/p_i}(a,b)\ \mathrm{mod}n$，直到找到某个 j，满足 $C_j=C_{p_i}$，此时 $m_i\equiv j\equiv m\ \mathrm{mod}\ p_i$；

(3) 对于 $p_1,\cdots,p_a,q_1,\cdots,q_b$ 重复步骤(1),步骤(2)，可以求得 $m\ \mathrm{mod}p_1,\cdots,m\ \mathrm{mod}q_b$，运用中国剩余定理，可以恢复明文 $m\in Z_\delta$。

3.2　可行性分析

定理 1　执行加密体制 1 的解密过程能够恢复出明文消息。

证明　假设 α,β,γ 是方程 $f(x)=x^3-ax^2+bx-1$ 的 3 个根。当 $a=s_m, b=s_{-m}$ 时，则此时的根为 $\alpha^m,\beta^m,\gamma^m$，显然，密文 C 的第 1 分量 $s_m=\alpha^m+\beta^m+\gamma^m\mathrm{mod}n$。

对于 p_1，解密用户计算

$$C_{p_i} = s_{\lambda/p_i}(s_m, s_{-m}) \bmod n = \alpha^{m\lambda/p_1} + \beta^{m\lambda/p_1} + \gamma^{m\lambda/p_1} \bmod n$$

假设 $m=kp_1+m_1$，其中 $k\geq 0, 0\leq m_1<p_1$，则

$$\begin{aligned} C_{p_i} &= \alpha^{m\lambda/p_1} + \beta^{m\lambda/p_1} + \gamma^{m\lambda/p_1} \bmod n \\ &= \alpha^{m_1\lambda/p_1} + \beta^{m_1\lambda/p_1} + \gamma^{m_1\lambda/p_1} \bmod n \end{aligned} \tag{5}$$

由于 p_1 是小素数，对于 $j=0,\cdots,p_1-1$，通过逐个计算 $C_j = s_{\lambda/p_i}(s_m, s_{-m}) \bmod n$ 不难找到某个 j 满足 $C_j = C_{p_i}$。实际上，此时 $j\equiv m_1\equiv m \bmod p_1$。

对于 $p_1,\cdots,p_a, q_1,\cdots,q_b$ 重复以上过程，可以求得 $m \bmod p_1,\cdots, m \bmod q_b$，运用中国剩余定理可以恢复明文 m。

根据定义 2 中关于底数和指数的定义，我们可以认为 GH 密码体制利用公钥把明文隐藏在 LFSR 的底数位置，通过底数的周期运用相应的私钥恢复出加密的明文；而本文把明文隐藏在指数位置，利用 LFSR 的高次剩余可直接构造后面第 4 节中具有语意安全的加密体制，不必使用公私钥对，加密者仅需知道模数 n 以及 δ 的长度 k，解密者在已知模数分解的情况下(于是知道 λ)，即可恢复出加密在 LFSR 指数位置上的明文。

3.3 安全性分析

根据定义 4 中关于 LFSR 剩余的定义，不难证明下面的定理。

定理 2 加密体制 1 的单向的当且仅当 Z_n 上的 LFSR δ-次剩余问题是困难的。

如同 RSA 密码体制，该体制运用的也是陷门单向函数，知道 n 的分解就知道 λ，就能执行解密运算；反之，根据第 2 节中的分析，如果攻击者知道 λ 就可以求得 Δ，从而分解 RSA 模数 n，这样，攻击者从求 λ 入手攻击此加密体制等价于分解 RSA 模数，这一结果同样适应于对 GH 密码体制的分析[7,8]，在不知道 n 的分解的情况下无法执行加密体制 1 的解密过程。

目前，还没有对于“Z_n 上的 LFSR δ-次剩余问题是困难的”形式化证明，也没有对 Z_n 上的 LFSR δ-次剩余问题的有效攻击。从其它攻击方式，目前比较有效的攻击方法主要是二次筛法(QS)、数域筛法(NFS)和 Pollard's p-1 方法、Pollard's ρ 方法以及 Pohlig-Hellman 方法。当参数取 $k\approx|n|/4$ 比较大时(如 $k>160$)，攻击者无法运用 Pollard's ρ 方法恢复出随机明文；对于模数 n，我们通过选取大的 n 以及 $p-1$ 等含有大的素因子，可以抵抗以上几种主要的攻击方式。

关于 LFSR 的高次剩余问题是一个新的问题，对这一问题本身及其相关问题的困难性有待于进一步研究。

在有限域 GF(p)上选取 LFSR 生成元(a, b)需要满足以下两个方面：(1) 满足式(2)中的多项式 $f(x)=x^3-ax^2+bx-1$ 在 GF(p)上不可约；在 GF(p)上有 $\frac{1}{3}(p^3-p)$ 个形如 $f(x)=x^3-ax^2+bx-c$ 的一般多项式，当取定 c=1 时，任选 $f(x)=x^3-ax^2+bx-1$ 为不可约多项式的概率大约为 1/3。(2) 假设 α 为(1)中 $f(x)$=0 的一个根，由于 α 阶就是 LFSR 序列的周期，所以还需要满足 α 为高阶元且阶被 δ 整除，这可以通过验证 $s_{(p^2+p+1)/p'}(a,b)\neq 3 \bmod p$ 和 $s_{(p^2+p+1)/p_i}(a,b)\neq 3 \bmod p$ ($i=1,\cdots,a$)来保证，这一概率约为 $(1-1/p')(1-1/p_1)(1-1/p_a)$，当 a=10，$p_1,\cdots,p_a$ 为前 10 个奇素数时，此概率约为 1/3。所以在 GF(p)上找到满足安全要求的参数 (a,b)的概率约为 1/9。当 b=10，$q_1,\cdots,q_b$ 为接下来的 10 个奇素数时，在有限域 GF(q)上通过随机选取找到满足安全要求的多项式的概率约为 4/15，这样通过随机选取方法，在 Z_n 上找到满足安全要求的多项式的概率至少为 1/30，所以至多执行 30 次尝试就可以找到满足安全要求的多项式。此时能够加密 92 bit 的明文。

如果从比较大的 p_1 开始选取 δ 的素因子，需要尝试的次数明显减少，如当 p_1=37 时，大约至多需要 10 次尝试就可以找到满足条件的参数 (a,b)。此时能够加密 120 bit 的明文。

公开参数(a,b)已经选定可以长期使用；随着 δ 的最小素因子 p_1 增大，可加密的明文长度也增大，找满足安全要求的参数(a,b)也越容易，然而解密的复杂度也随之增大，实际中可以根据所处的运算和通信环境选取合适的参数 δ。

4 基于 LFSR 序列的高次剩余的概率加密体制

4.1 体制描述(加密体制 2)

参数选择 同于加密体制 1。

公开参数 $n, a, b, |\delta|=k$

秘密参数 p, q

加密 $m\in Z_\delta$，加密用户随机选取 $r\in Z_n$，计算密文

$$C=(s_{r\delta+m}(a,b),\ s_{-(r\delta+m)}(a,b)) \bmod n$$

解密 同于加密体制 1 的解密过程。

4.2 可行性分析

定理 3 执行本文给出的加密体制 2 的解密过程能够恢复出明文消息。

证明 由于 $C=(s_{r\delta+m}(a,b),\ s_{-(r\delta+m)}(a,b)) \bmod n$，所以类似于定理 1，对于 p_1，解密用户计算

$$\begin{aligned} C_{p_i} &= s_{\lambda/p_i}(s_m, s_{-m}) \bmod n \\ &= \alpha^{(r\delta+m)\lambda/p_1} + \beta^{(r\delta+m)\lambda/p_1} + \gamma^{(r\delta+m)\lambda/p_1} \bmod n \end{aligned}$$

由定理 1 的式(5)，实际上

$$C_{p_i} = \alpha^{m\lambda/p_1} + \beta^{m\lambda/p_1} + \gamma^{m\lambda/p_1} \bmod n$$

其它证明过程与定理 1 的证明类似。

4.3 安全性分析

与加密体制 1 相比，加密体制 2 具有单向性，同时还具有语意安全性。

定理 4 加密体制 2 是语意安全性的当且仅当 LFSR 高次剩余加 1 问题是困难的。

证明 假设加密体制 2 的密文 $C=(s_{r\delta+m}(a,b),\ s_{-(r\delta+m)}(a,b))$

mod$n$ 是明文 m_0 或 $m_1(m_1\neq 0)$对应的密文，攻击者首先计算 l，满足 $lm_1\equiv 1 \bmod \delta$，然后由式(3)计算

$$C_1 = s_{l(r\delta+m)}(a,b) \bmod n = s_{\eta\delta+(ml \bmod \delta)}(a,b) \bmod n$$

$$C_2 = s_{-l(r\delta+m)}(a,b) \bmod n = s_{-[\eta\delta+(ml \bmod \delta)]}(a,b) \bmod n$$

这里的 r_1 是一随机数。

如果加密体制 2 不具有语意安全性，攻击者可以判断 C 对应的明文是否为 m_1，于是攻击者可以判断 $ml \bmod \delta$ 是否为 1，即可以 LFSR 判断高次剩余加 1 问题。

反之，如果 LFSR 高次剩余加 1 问题是容易的，则不难证明概率加密体制 2 不具有语意安全性。

说明　本文给出的 LFSR 高次剩余问题与整数分解的确切关系有待于进一步探讨。目前，即使是一般模指数运算中的高次剩余问题与整数分解问题的关系尚不明确(如基于高次剩余问题的 Paillier 体制[10])，但普遍认为它们也是困难问题[11-13]。由于本文首次提出了关于 LFSR 的高次剩余问题，对这个问题还需要从数学和密码学角度做进一步的研究。

5　结束语

本文的主要目的是基于新的困难问题，对用 LFSR 序列构造密码体制做进一步研究，探讨了一种加密方式不同于 GH 的概率加密体制，该体制把明文隐藏在 LFSR 序列的指数位置，具有语意安全性，新体制克服了 GH 体制的加密确定性的不足，并对加密体制的可行性和安全性做了分析，该体制的单向性和语意安全性分别等价于 LFSR 高次剩余问题和 LFSR 判断高次剩余问题；同时本文也对所涉及到的困难问题以及参数的选取做了简单的讨论，对这些问题还需要做进一步深入的探讨。

参 考 文 献

[1] Diffie W, Hellman M E. New directions in cryptography[J]. *IEEE Trans. on of Information Theory*, 1976, IT-22 (6): 644 – 654.

[2] Rivest R, Shamir A, Adleman L. A method for abstaining digital signatures and public-key cryptosystems[J]. *Comm. of the ACM*, 1978, 21(2): 120 – 126.

[3] Rabin M O. Digital signatures and public key functions as intractable as factorization[R]. Cambridge: MIT/LCS/TR-212, 1979.

[4] Williams H C. An M3 public-key encryption scheme[A]. Advances in Cryptology-CRYPTO'85[C]. Berlin: Springer-Verlag, 1986: 358 – 368.

[5] Paillier P. Public-key cryptosystems based on composite degree residuosity classes. Advances in Cryptology- EUROCRYPT' 99[C], Berlin: Springer-Verlag, 1999, LNCS 1592: 223 – 238.

[6] Smith P, Lennon M. LUC: A new public-key system[A]. Proceeding of IFIP/Sec'93[C], Elsevier Science Publications, 1994: 97 – 111.

[7] Gong G, Harn L. Public-key cryptosystems based on cubic finite field extensions[J]. *IEEE Trans. on Information Theory*, 1999, IT-45(7): 2601 – 2605.

[8] Gong G, Harn L, Wu H P. The GH public-key cryptosystem[A]. Selected areas in cryptography[C]. SAC, Toronto, 2001: 284 – 300.

[9] Jiang Z T, Hao Y H, Wang Y M. A new public-key encryption scheme based on lucas sequence[J]. *Journal of Electronics-(China)*. 2005, 22(5):490 – 497.

[10] Paillier P, Pointcheval D. Efficient public-key cryptosystem provably secure against active adversaries[A]. Advances in Cryptology-ASIACRYPT'99[C], Berlin: Springer-Verlag, 1999, LNCS 1716: 163 – 179.

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

[12] Damgard I, Jurik M. A generalization, a simplification and some application of Paillier's probabilistic public-key system[A]. Advances in Cryptology-PKC'99[C], Berlin: Springer-Verlag, 2001, LNCS 1992: 119 – 136.

[13] 姜正涛, 庞辽军, 王育民. 一种高效的可选择验证完整性和消息源的加密体制[J]. 电子与信息学报, 2005, 27(4): 621 – 624.

姜正涛：　男，1977 年生，博士生，研究方向为密码算法理论的研究与分析、数论及其应用、通信网的安全、电子现金及相关技术等.

柳　毅：　男，1976 年生，博士生，研究方向为移动代理安全、电子商务中的安全理论与技术等.

王育民：　男，1936 年生，教授，博士生导师，从事编码理论、密码学、信息安全等领域的科研与教学工作.