一种新的等价于大整数分解的公钥密码体制研究

姜正涛[①]　张京良[②]　王育民[②]
[①](北京航空航天大学计算机学院　北京　100083)
[②](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：在弱的安全假设下构造可证明安全的密码体制原型可以有效提高密码体制的安全性，该文对用 Lucas 序列构造公钥密码体制做进一步研究，给出一种新的可证明安全的密码体制原型，该密码体制的加、解密效率比现有的 LUC 密码体制效率高，并证明它的安全性等价于分解 RSA 模数，最后给出该体制在签名方面的应用，伪造签名等价于分解 RSA 模数。

关键词：公钥加密体制；Lucas 序列；Lucas 二次(非)剩余；整数分解；签名
中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1009-5896(2008)06-1450-03

Research on a New Public Key Cryptosystem as Secure as Integer Factorization

Jiang Zheng-tao[①]　Zhang Jing-liang[②]　Wang Yu-min[②]
[①](*School of Computer Science and Technology*, *Beijing University of Aeronautics and Astronautics*, *Beijing* 100083, *China*)
[②](*National Key Lab. of Integrated Service Networks*, *Xidian Univ.*, *Xi'an* 710071, *China*)

Abstract: Constructing provably secure cryptographic primitives under weak assumptions can improve the security of cryptographic schemes efficiently. Further research on the construction of public-key cryptosystem is provided, and a new public-key encryption primitive is investigated. This scheme is more efficient than that of existing LUC cryptosystems. More over, the proposed scheme is provable secure and its security is proved to be equivalent to the factorization of RSA modulus. At last, an application in signature is suggested; forgery of signature is also equivalent to the factorization of RSA modulus.

Key words: Public-key encryption scheme; Lucas sequence; Lucas (non)quadratic residue; Integer factorization; Signature

1　引言

自从Diffie和Hellman提出了公钥密码体制概念以来[1]，研究者对这一领域进行了广泛深入的研究[2−5]。Rivest 等于1978年提出了一种基于大整数分解的密码体制RSA[6]，至今尚未证明 RSA 的安全性是否等价于大整数分解，目前公钥密码研究者所研究或探讨的密码体制原型大都基于但不等价于数学困难问题，只有 Rabin 和 Williams 提出的两种密码体制已经被证明等价于分解 RSA 模数[7, 8]。

利用 Lucas 序列，Smith 构造了另一种密码体制 LUC[9]。本文对 LUC 密码体制做进一步研究，尝试性地探讨一种新的密码体制原型，加密比现有所有的 LUC 密码体制效率都高，解密与现有的 LUC 密码体制效率相当，并证明了本文密码体制的安全性等价于分解 RSA 模数，最后在本文给出的 Lucas 二次(非)剩余定义的基础上，给出了在签名方面的一个应用。

2006-11-20 收到，2007-06-04 改回
中国博士后科学基金项目(20060400035)，国家自然科学基金重点项目(69931010)和国家 973 计划(G 1999035803)资助课题

2　Lucas 序列

假设 P,Q 为整数，α,β 是下列方程 $x^2-Px+Q=0$ 两个根，则称 $V_k=\alpha^k+\beta^k$，$U_k=(\alpha^k-\beta^k)/(\alpha-\beta)$，$k=0,1,2,\cdots$ 为 Lucas 序列。

本文主要用到 Lucas 序列的以下几条性质。

引理 1　对任意的整数 e,k，以下等式成立：

(1) $V_{k+1}=PV_k-QV_{k-1}$，$U_{k+1}=PU_k-QU_{k-1}$；

(2) $\begin{cases}U_{2k}=V_kU_k\\ V_{2k}=V_k^2-2Q^k\end{cases}$；

(3) $\begin{cases}U_{2k+1}=U_{k+1}^2-QU_k^2\\ V_{2k+1}=V_{k+1}V_k-PQ^k\end{cases}$；

(4) $V_e(V_k(P,Q),Q^k)=V_{ek}(P,Q)=V_k(V_e(P,Q),Q^e)$，$V_e(V_k(P,1),1)=V_{ek}(P,1)=V_k(V_e(P,1),1)$；

(5)设 N 为整数，则

$$V_k(P \bmod N, Q \bmod N)\equiv V_k(P,Q) \bmod N,$$
$$U_k(P \bmod N, Q \bmod N)\equiv U_k(P,Q) \bmod N;$$

(6)如果等式(1)的左端在 GF(p)上不可约，则

$$\alpha^{p+1}\equiv 1 \bmod p,$$

其中 p 为素数，α 是 Q=1 时等式(1)的一个根。

在用 Lucas 序列构造密码体制时，通常令 Q=1。

3　密码体制的构造

假设 $n=pq$ 为 RSA 模数，其中 $p=4p_1+1$，$q=4q_1+1$，p_1，q_1 均为素数，$m\in Z_n^*$ 为待加密的消息。

本文方案的简单加、解密过程如下：

加密　$m\in Z_n^*$，加密用户计算 $C=V_2(m)\bmod n$。

解密　分别在有限域 GF(p)和 GF(q)中执行解密过程：

解密用户知道 n 的分解，首先验证 $f(x)=x^2-Cx+1$ 在 GF(p)和 GF(q)中是否可约，假设 $\Delta=C^2-4$，$\left(\frac{?}{?}\right)$ 为 Legendre 符号，解密过程为以下 4 种情况之一：

第 1 种情况　$\left(\frac{\Delta}{p}\right)=\left(\frac{\Delta}{q}\right)=-1$

在 GF(p)中解密得两条明文：$m_p=V_{(p+3)/4}(C)\bmod p(C)$ 和 $p-m_p$，

在 GF(q)中同样可解密得两条明文：$m_q=V_{(q+3)/4}(C)\cdot\bmod q$ 和 $q-m_q$。

根据中国剩余定理，可求得 4 条明文 m_1,m_2,m_3,m_4。

可根据加、解密规则(如从 4 条明文中选取有意义的明文，或加密前在明文中加入必要的冗余信息等)，找出相应的明文。

第 2 种情况　$\left(\frac{\Delta}{p}\right)=1,\ \left(\frac{\Delta}{q}\right)=-1$

在 GF(p)中求 $C+2$ 的两个平方根，得两条明文 m_p 和 $p-m_p$，

在 GF(q)中解密得两条明文：$m_q=V_{(q+3)/4}(C)\bmod q$ 和 $q-m_q$。

由中国剩余定理，类似于第 1 种情况求得明文消息。

第 3 种情况　$\left(\frac{\Delta}{p}\right)=-1,\ \left(\frac{\Delta}{q}\right)=1$

类似于第 2 种情况可解密明文。

第 4 种情况　$\left(\frac{\Delta}{p}\right)=1,\ \left(\frac{\Delta}{q}\right)=1$

根据第 2 种情况中 $\left(\frac{\Delta}{p}\right)=1$ 时的情形，可解密明文。

与原 LUC 密码体制的效率比较：

加密　原 LUC 密码体制加密需要计算 $C=V_e(m)\cdot\bmod n$ [9]，根据引理 1，计算 $C=V_e(m)\bmod n$ 平均需要 $\log_2 e$ 次 Z_n 上的平方运算和 $(1/2)\log_2 e$ 次 Z_n 上的乘法运算；

本文体制的加密仅需计算 $C=V_2(m)\bmod n$。

解密　原 LUC 密码体制解密需要计算 $C=V_d(m)\cdot\bmod n$，通常为提高解密效率做以下过程的解密运算。计算 Legendre 符号 $\left(\frac{\Delta}{p}\right),\left(\frac{\Delta}{q}\right)$，这里 $\Delta=C^2-4$，然后类似于本文中的解密过程计算 $m_p=V_d(C)\bmod p$ 和 $m_q=V_d(C)\bmod q$，其中 $de\equiv 1\bmod\left(\left(p-\left(\frac{\Delta}{p}\right)\right)\left(q-\left(\frac{\Delta}{q}\right)\right)\right)$。这里的 d 是在选择系统公钥时计算的，由于 $\left(\frac{\Delta}{p}\right)$ 和 $\left(\frac{\Delta}{q}\right)$ 可能各有两个不同的值，于是需要事先计算 4 个可能的 d 值，d_1, d_2, d_3, d_4：$d_1e\equiv 1\bmod(p-1)$，$d_2e\equiv 1\bmod(p+1)$，$d_3e\equiv 1\bmod(q-1)$，$d_4e\equiv 1\bmod(q+1)$。解密时计算 $m_p\equiv V_{d_i}(C)\bmod p$，$i$=1 或 2，以及 $m_q\equiv V_{d_j}(C)\bmod q$，$j$=3 或 4，最后根据中国剩余定理求得 $m\in Z_n$。

本文加密体制的解密需要计算(1)Legendre 符号 $\left(\frac{\Delta}{p}\right)$，$\left(\frac{\Delta}{q}\right)$，与原体制相同；(2) 解密过程的运算为以下两类运算之一：

(a)计算 $V_{(p+3)/4}(C)\bmod p$，运算复杂度不大于原体制的计算 $V_d(C)\bmod p$；

(b)在 GF(p)中计算平方根大约需要 $\log_2 p$ 次平方运算和 $\log_2 p$ 次乘法运算[10]，而根据引理 1 中的性质(1), (2), (3)，计算 $V_d(C)\bmod p$ 大约平均需要 $\log_2 p$ 次平方运算和 $(1/2)\log_2 p$ 次乘法运算，解密过程中计算 $V_d(C)\bmod p$ 复杂度更低。

纵上所述，本文体制的加、解密效率比原体制的效率高，大约少 $\log_2 p$ 次平方运算；并且加密只需做一次运算，即计算 $C=V_2(m)\bmod n$。因此相对于原加密体制，本文的体制更适合加密用户的计算资源相对有限的终端，如移动用户等。

4　可行性与安全性分析

这一节证明第 3 节给出加密体制的可行性和安全性。

定理 1　执行本文给出的加密体制的解密过程能够恢复出明文消息。

证明　对于第 1 种情况，即 $f_C(x)=x^2-Cx+1$ 在 GF(p)中不可约，所以 Lucas 序列 $V_k(C)$ (k=0,1,2,$\cdots$) 在 GF(p)中的周期 $\pi_p(C)$ 满足 $\pi_p(C)\mid p+1$，并且由性质(6)有

$$\alpha_1^{p+1}\equiv 1\bmod p,\ \ \beta_1^{p+1}\equiv 1\bmod p$$

其中 α_1,β_1 是 $f_C(x)=0$ 的两个根。

如果 α,β 是 $f_m(x)=x^2-mx^2+1=0$ 的两个根，不难证明 $\alpha_1=\alpha^2,\beta_1=\beta^2$ 或 $\alpha_1=\beta^2,\beta_1=\alpha^2$。

于是 $V_2(V_{(p+3)/4}(C))\bmod p=[(\alpha^2)^{[(p+3)/4]\times 2}+(\beta^2)^{[(p+3)/4]\times 2}]\cdot\bmod p=(\alpha^2+\beta^2)\bmod p=C\bmod p$。所以，$V_{(p+3)/4}(C)\bmod p$ 实际上就是 $m\bmod p$ 或 $p-m\bmod p$。

当 $f_C(x)=x^2-Cx+1$ 在 GF(q)中不可约时，用类似的方法可求得 $m\bmod q$ 和 $q-m\bmod q$。

由中国剩余定理，可以求得包含 m 在内的 4 条明文消息。

对于第 2 种情况，由于 $\left(\frac{\Delta}{p}\right)=1$，所以 $f_C(x)=x^2-Cx+1$ 在 GF(p)中可约。

假设 α,β 是 $f_m(x)=x^2-mx+1=0$ 的两个根，于是 $C=V_2(m)=\alpha^2+\beta^2 \bmod n$，其中 $\alpha+\beta=m$，$\alpha\beta=1$。

所以 $C=(\alpha+\beta)^2-2$，以及 $m^2=C+2 \bmod n$。所以 $m \bmod p$ 为 $C+2$ 在 GF(p)中的两个平方根之一。

于是，根据 GF(p)求平方根算法可求得 m_p 和 $p-m_p$ [10]；

根据第 1 种情况，可求得 m_q 和 $q-m_q$。

其它情况的明文恢复与第 1, 2 种情况类似。 证毕

定理 2 如果存在算法 A 成功地攻击本文的加密体制，则运用此算法 A 可分解 RSA 模数。

证明 假设存在算法 A 可求得第 3 节中密文 C 对应的明文 $m_1,m_2(=n-m_1),m_3,m_4(=n-m_3)$。

由于 $m_i^2 \equiv C+2 \bmod n$，$i=1,2,3,4$，所以 $m_1^2-m_3^2 \equiv 0 \bmod n$，即 $(m_1+m_3)(m_1-m_3) \equiv 0 \bmod n$。

又因为 $m_1+m_3 \neq 0 \bmod n$，$m_1-m_3 \neq 0 \bmod n$。因此 $(m_1+m_3,n) \neq 1$ 并且 $(m_1-m_3,n) \neq 1$。

这样必有 $(m_1+m_3,n)=p$，$(m_1-m_3,n)=q$ 或 $(m_1+m_3,n)=q$，$(m_1-m_3,n)=p$，从而成功分解 RSA 模数 $n=pq$。 证毕

5 应用举例

5.1 在签名中的简单应用

本节给出第 3 节中的密码体制在数字签名中的一个应用，在这里假设素数 $p=2^ht+1$，其中 $h \geqslant 2$，t 为素数。

定义 1 设 $R \in Z_p$，称 R 为模 p 的 Lucas 二次剩余，如果满足下列条件之一：

(1) $f(x)=x^2-Rx+1$ 在 GF(p) 上不可约，且 $V_{(p+1)/2}(R) \equiv 2 \bmod p$，

(2) $f(x)=x^2-Rx+1$ 在 GF(p) 上可约，且 $V_{(p-1)/2}(R) \equiv 2 \bmod p$；

反之，称 R 为模 p 的 Lucas 二次非剩余。

把模 p 的 Lucas 二次剩余与 Lucas 二次非剩余分别记为 LQR_p 和 LNR_p。

把序列 $V_k(R),k=0,1,2,\cdots$ 称为由参数 R 生成的 Lucas 序列，事实上

$$V_k(R)=\alpha^k+\beta^k,\ k=0,1,2,\cdots$$

其中 α,β 是方程 $f(x)=x^2-Rx+1=0$ 的两个根。

若 $m \in \{V_k(R),k=0,1,2,\cdots\}$，称 m 属于由 R 生成的 Lucas 序列，记为 $m \in L(R)$；进一步，如果 m 为模 p 的 Lucas 二次剩余，记为 $m \in \mathrm{LQR}_p(R)$，如果 m 为模 p 的 Lucas 二次非剩余，记为 $m \in \mathrm{LNQR}_p(R)$。

体制参数 $n=pq$，令集合 $\Omega=\mathrm{LQR}_p \cap \mathrm{LQR}_q$。

签名过程 明文消息 M，$0<M<n$，设 $M \in \mathrm{LQR}_p \cap \mathrm{LQR}_q$（若 M 不满足次条件，可将其映射成 $M'=f(M)$，使得 $M' \in \mathrm{LQR}_p \cap \mathrm{LQR}_q$），求 M 的平方根，作为对消息 M 的签名：

$$S=V_{1/2}(M) \bmod n$$

签名验证 签名验证者计算 $M''=V_2(S) \bmod n$，如果 $M''=M$，签名通过验证；否则不通过验证。

注：关于签名、验证的效率分析与第 3 节中加、解密的效率分析类似。

5.2 安全性分析

给定一条消息 M，如果攻击者可以伪造签名，即攻击者可以求得 $S=V_{1/2}(M) \bmod n$，实际上相当于恢复第 3 节加密体制中密文对应的明文，根据定理 2，等价于分解 RSA 模数。

6 结束语

本文的主要工作是对用 Lucas 序列构造形式化可证明安全的密码体制做初步的研究，给出了关于 Lucas 二次(非)剩余等几个定义，探讨了一种用模 n Lucas 二次剩余构造的密码体制，并证明了它的安全性等价于分解 RSA 模数，于是在最弱的假设条件下是可证明安全的，加解密效率比现有的 LUC 类密码体制的效率高。最后示例给出了它在签名方面的一个简单应用，伪造签名也等价于分解 RSA 模数。

参 考 文 献

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

[2] Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. *IEEE Trans. on Inform. Theory*, 1985, IT-31(4): 469–472.

[3] Miller V. Uses of elliptic curves in cryptography[A]. Advances in Cryptography-CRYPTO'85[C], LNCS 218. Berlin: Springer-Verlag, 1985: 412–426.

[4] Hostein J, Pipher J, and Silvernab J H. NTRU: A ring based public key cryptosystem[A]. ANTS'97[C], LNCS 1423. Berlin: Springer-Verlag, 1998: 267–288.

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

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

[7] Rabin M O. Digital Signatures and Public Key Functions as Intractable as Factorization[R]. Cambridge: MIT/LCS/TR–212, 1979.

[8] Williams H C. An M3 public-key encryption scheme[A]. Advances in Cryptology-CRYPTO'85[C]. Berlin: Springer-Verlag, 1985: 358–368.

[9] Smith P and Lennon M. LUC: A new public-key system[A]. Proceedings of the IFIP TC11, Ninth International Conference on Information Security, IFIP/Sec '93[C], Toronto, Canada, 1993: 91–111.

[10] 卢开澄. 计算机密码学(第 2 版)[M]. 北京: 清华大学出版社, 1998: 73–84.

姜正涛： 男，1976 年生，博士后，主要研究方向为密码算法理论的研究与分析、数论及其应用、可信计算、信任管理、抗毁生存等.

张京良： 男，1971 年生，博士生，研究方向为密码算法理论、数字签名和公平协议等.

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