一种新的基于 Lucas 序列的公钥密码体制

王衍波 张凯泽 王开华 端木庆峰 雷凤宇
(解放军理工大学通信工程学院 南京 210007)

摘 要：该文分析了 LUC 公钥密码体制，提出了基于 Lucas 序列的新的公钥密码体制 LUC-RSA，LUC-Rabin，其安全性比 LUC，RSA 强，数据吞吐率大于 LUC。

关键词：公钥密码体制；RSA；LUC
中图分类号：TN918 文献标识码：A 文章编号：1009-5896(2007)01-0185-04

A New Public-Key Cryptosystems on Lucas Sequence

Wang Yan-bo Zhang Kai-ze Wang Kai-hua Duanmu Qing-feng Lei Feng-yu
(*Institute of Communications Engineering, PLA Univ. of Sci. & Tech., Nanjing* 210007, *China*)

Abstract: LUC public-key cryptosystem is analyzed, two new public-key cryptosystems on Lucas sequence LUC-RSA, LUC-Rabin are presented, their security are stonger than LUC, RSA, and the rate of throughput of the data are greater than LUC.

Key words: Public-key cryptosystem; RSA; LUC

1 引言

Lucas 序列(或函数)，也称为 Dickson 多项式是数论中一个重要的工具，被广泛地应用于素性检验、不可约多项式构造、有限域正规基构造以及椭圆曲线群点数计算等等[1]，是数论中经典、永具活力的一个重要内容。1993 年，Smith 和 Lennon[2] 首次提出了一个基于 Lucas 序列的公钥密码体制。对一些已知的攻击，可以证明 LUC 比 RSA 更安全，而对其他情况，LUC 至少具有 RSA 的安全性，从而，可以认为，LUC 比 RSA 更安全。然而，一般情况下，LUC 的加、解密速度比 RSA 慢一半。LUC 的提出除本身的价值外，在公钥密码理论研究上还具有另外一个重要意义，它把序列技术引入公钥密码算法的构造中，揭示了公钥密码体制的序列本质以及基于线性移位寄存器公钥密码体制的构造原理。例如：RSA 本质上是一种基于一阶线性移位寄存器的公钥密码体制，LUC 是一种基于二阶线性移位寄存器公钥密码体制，GH-PKS[3]就是一种基于三阶线性移位寄存器公钥密码体制，XTR[4]作为 GH-PKS 的特例，也是一种基于三阶线性移位寄存器公钥密码体制。按照这一思路，我们可以研究构造四阶、五阶，甚至更高阶的基于线性移位寄存器公钥密码体制，或者构造基于非线性移位寄存器公钥密码体制。可见 LUC 的提出，为构造新的公钥密码体制指出了一条可行的道路。

本文提出了 LUC-RSA，LUC-Rabin 公钥密码体制，安全性比 RSA 强，且数据吞吐率大于 LUC。

2 Lucas 序列及其性质

定义 设 P ，Q 是正整数，则 Lucas 序列定义为：$V_0=2$ ，$V_1=P$ ，$V_n=PV_{n-1}-QV_{n-2}$ ；$U_0=0$ ，$U_1=1$ ，$U_n=PU_{n-1}-QU_{n-2}$ ，V_n ，U_n 也分别记为 $V_n(P,Q)$ ，$U_n(P,Q)$ 。

直接计算容易得到，对任意正整数 k ，N ，有 $U_k\left(P \bmod N, Q \bmod N\right)\equiv U_k(P,Q) \bmod N$ 。

性质 1 $U_{m+n}=U_mV_n-Q^nU_{m-n}$ ，$V_{m+n}=V_mV_n-Q^nV_{m-n}$ 。

性质 2 设 $f(x)=x^2-Px+Q$ 是域 F 上的不可约多项式，$F\left(\sqrt{\Delta}\right)$ 是 F 的二次扩域，α ，β 是 $f(x)=0$ 在 $F\left(\sqrt{\Delta}\right)$ 上的两个根，则有 $V_n=\alpha^n+\beta^n$ ，$U_n=\dfrac{\alpha^n-\beta^n}{\alpha-\beta}$ ，$n=0,1,2,\cdots$ 。

性质 3 记 $D=P^2-4Q$ ，则有

(1) $V_{km}(P,Q)=V_k\left(V_m(P,Q),Q^m\right)$ ；

(2) $U_{km}(P,Q)=U_k(P,Q)U_k\left(V_m(P,Q),Q^m\right)$ ；

(3) $4Q^k=V_k^2(P,Q)-\Delta U_k^2(P,Q)$ ；

(4)
$$V_{k+m}(P,Q)=\frac{V_k(P,Q)V_m(P,Q)}{2}+\frac{\Delta U_k(P,Q)U_m(P,Q)}{2};$$

(5)
$$U_{k+m}(P,Q)=\frac{U_k(P,Q)V_m(P,Q)}{2}+\frac{V_k(P,Q)U_m(P,Q)}{2}。$$

2005-06-08 收到，2005-11-30 改回

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

记 $(D/p)=\begin{cases}1, & \exists x, \ni x^2 \equiv D \bmod p\\ 0, & p \mid D\\ -1, & \text{其它}\end{cases}$，为 Legendre 符号，则有

性质 4 如果 p 是一个奇素数，$p \nmid Q$，或者 $p \nmid D$，则对正整数 k，记 $\varepsilon=(D/p)$，

(1) $U_{k(p-\varepsilon)}(P,Q) \equiv 0 \bmod p$；

(2) $V_{k(p-\varepsilon)}(P,Q) \equiv 2Q^{\frac{k(1-\varepsilon)}{2}} \bmod p$。

特别地 $U_{k(p-\varepsilon)}(P,1) \equiv 0 \bmod p$，$V_{k(p-\varepsilon)}(P,1) \equiv 2 \bmod p$。

3 Lucas 公钥密码体制

设 p,q 是两个奇素数，$N=pq$。$e \in Z_N$，$(e,(p-1)(p+1)(q-1)(q-1))=1$。

(1) 公开密钥：e，N。

(2) 加密算法：$C=V_e(M,1) \bmod N$，对任意信息 $M \in Z_N$。

(3) 解密密钥：d，$ed \equiv 1 \bmod S(N)$，$S(N)=\mathrm{lcm}(p-(D/p),p-(D/q))$，$D=C^2-4$。

(4) 解密算法：$M=V_d(C,1) \bmod N$。

(5) 解密原理：

$$\begin{aligned}V_d(C,1)&=V_d(V_e(M,1),1)=V_{ed}(M,1)=V_{kS(N)+1}(M,1)\\&=MV_{kS(N)}(M,1)-V_{kS(N)-1}(M,1)\\&=MV_{kS(N)}(M,1)-\frac{1}{2}\Big(V_{kS(N)}(M,1)V_1(M,1)\\&\quad-DU_{kS(N)}(M,1)U_1(M,1)\Big)\\&\equiv 2M-\frac{1}{2}(2M-0) \bmod N=M\end{aligned}$$

(6) 算法分析：

(a) 计算速度可以根据性质 1，2，3 进行改进，主要有“倍-加”算法，一般地，它需要 RSA 两倍的时间。

(b) 解密密钥不能事先计算好，需要根据密文及时计算，这一方面可以使解密密钥与密文相关，增加安全性，另一方面，增加了解密时的计算量。主要需要计算 $D=C^2$，Legendre 符号，欧几里德展转相除法求逆。

(c) 因为

$$\left(\frac{C^2-4}{p}\right)=\left(\frac{V_e^2(M,1)-4}{p}\right)=\left(\frac{(M^2-4)U_e^2(M,1)}{p}\right)=\left(\frac{M^2-4}{p}\right)$$

$$\left(\frac{C^2-4}{q}\right)=\left(\frac{V_e^2(M,1)-4}{q}\right)=\left(\frac{(M^2-4)U_e^2(M,1)}{q}\right)=\left(\frac{M^2-4}{q}\right)$$

所以

$$\begin{aligned}S(N)&=\mathrm{lcm}\left(p-\left(\frac{C^2-4}{p}\right),q-\left(\frac{C^2-4}{q}\right)\right)\\&=\mathrm{lcm}\left(p-\left(\frac{M^2-4}{p}\right),q-\left(\frac{M^2-4}{q}\right)\right)\end{aligned}$$

可见，Lucas 公钥密码算法关于加密、解密是对称的，也就是说，可以根据明文计算 $S(N)$，从而该算法也可以用于数字签名，相应地，它用于签名时的验证密钥是与明文有关的，这是与其他公钥签名体制不同的地方，Lucas 签名体制在发布签名消息的同时发布验证密钥。

4 基于 Lucas 序列的新公钥密码体制

4.1 LUC-RSA 公钥密码体制

在 Lucas 公钥密码体制中，作了 $Q=1$ 的限制，使信息量减少了一半。下面，我们取消这个限制，给出一个基于 Lucas 序列及 RSA 公钥算法的混合公钥密码体制。我们称为 LUC-RSA 公钥密码体制。

设 p，q 是两个奇素数，$N=pq$。$e \in Z_N$，$(e,(p-1)(p+1)(q-1)(q-1))=1$。

(1) 公钥：e 和参数 N。

(2) 加密：对 $\forall (P,Q) \in Z_N \times Z_N$，计算并发送：$C_0=U_e(P,Q) \bmod N$，$C_1=V_e(P,Q) \bmod N$，$C_2=Q^e \bmod N$。

(3) 解密密钥：

令 $D'=C_1^2-4C_2$，$\varepsilon_p'=(D'/p)$，$\varepsilon_q'=(D'/q)$，则

d：$ed \equiv 1 \bmod \phi(N)$，$\phi(N)=\mathrm{lcm}(p-1,q-1)$，

l：$el \equiv 2 \bmod S'(N)$，$S'(N)=\mathrm{lcm}(p-\varepsilon_p',q-\varepsilon_q')$。

(4) 解密算法：

令 $s_p=\dfrac{(el-2)(1-\varepsilon_p')}{2(p-\varepsilon_p')}$，$s_q=\dfrac{(el-2)(1-\varepsilon_q')}{2(q-\varepsilon_q')}$，则

(a) $Q=C_2^d \bmod N$。

(b) 用中国剩余定理求解同余方程组：

$\begin{cases}x=Q^{-S_p}C_0U_l(C_1,\ C_2) \bmod p\\ x=Q^{-S_q}C_0U_l(C_1,\ C_2) \bmod q\end{cases}$，则 $P=x \bmod N$。

设 $\tilde{q}$ 为 q 模 p 的逆，$\tilde{p}$ 为 p 模 q 的逆，则

$$P=(q\tilde{q}Q^{-s_p}+p\tilde{p}Q^{-s_q})C_0U_l(C_1,C_2) \bmod N。$$

(5) 解密原理：

(a) Q 的解密方法是 RSA 的解密方法。

(b) $\varepsilon_p=\left(\dfrac{D}{p}\right)=\left(\dfrac{DU_e^2}{p}\right)=\left(\dfrac{V_e^2-4Q^e}{p}\right)=\left(\dfrac{C_1^2-4C_2}{p}\right)=\left(\dfrac{D'}{p}\right)=\varepsilon_p'$，同理 $\varepsilon_q=\varepsilon_q'$，所以

$$S'(N)=\mathrm{lcm}(p-\varepsilon_p',q-\varepsilon_q')=\mathrm{lcm}(p-\varepsilon_p,q-\varepsilon_q)=S(N)$$

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

$$C_0U_l(C_1,C_2)\equiv U_e(P,Q)U_l(V_e(P,Q),Q^e)\bmod N$$
$$\equiv U_{el}(P,Q)\bmod N\equiv U_{kS(N)+2}(P,Q)\bmod N$$
$$\equiv\frac{1}{2}\big(U_{kS(N)}(P,Q)V_2(P,Q)$$
$$+U_2(P,Q)V_{kS(N)}(P,Q)\big)\bmod N$$

所以，

$$C_0U_l(C_1,C_2)\equiv\frac{1}{2}\big(U_{kS(N)}(P,Q)V_2(P,Q)$$
$$+U_2(P,Q)V_{kS(N)}(P,Q)\big)\bmod p$$
$$\equiv\frac{1}{2}U_2(P,Q)V_{kS(N)}(P,Q)\bmod p$$
$$\equiv\frac{1}{2}\cdot P\cdot 2Q^{s_p}\bmod p\equiv PQ^{s_p}\bmod p$$

所以，$p\nmid Q$ 时，$P\equiv Q^{-s_p}C_0U_l(C_1,C_2)\bmod p$。

同理，$q\nmid Q$ 时，$P\equiv Q^{-s_q}C_0U_l(C_1,C_2)\bmod q$。

所以，P 满足同余式：$\begin{cases}x=Q^{-S_p}C_0U_l(C_1,\ C_2)\bmod p。\\ x=Q^{-S_q}C_0U_l(C_1,\ C_2)\bmod q。\end{cases}$

由中国剩余定理知，存在唯一解 $x\equiv\left(q\tilde{q}Q^{-s_p}+p\tilde{p}Q^{-s_q}\right)\cdot C_0U_l(C_1,C_2)\bmod N$，由于 $0<P<N$，所以，$P=\left(q\tilde{q}Q^{-s_p}+p\tilde{p}Q^{-s_q}\right)C_0U_l(C_1,C_2)\bmod N$。

(6) 算法分析：

(a) 算法是 RSA 与 LUC 两种公钥算法的复合，从而，其安全性至少同等于其中最安全的一种；

(b) LUC 公钥体制中，由于 $Q=1$，从而减小了体制的强度，在 LUC-RSA 中，Q 是任意的，从而相对而言，安全强度比 LUC 增强了。

(c) 如果以 RSA 作为时间数据标准，那么 LUC 加、解密需要 4 个 RSA 时间，处理 1 个数据，数据吞吐率为 1/4，而 LUC-RSA 用 8 个 RSA 时间，处理的 2 个数据，数据吞吐率为 2/8=1/4，所以，LUC-RSA 的数据吞吐率等于 LUC。

(d) 解密密钥 l 的计算，用欧几里德算法求解 $el'\equiv 1\bmod S'(N)$，然后令 $l=2l'\bmod S'(N)$ 即可。

(e) 如果 $p\mid Q$（或 $q\mid Q$），那么，算法失效，这时 $(N,Q)=p$（$(N,Q)=q$），从而 N 被分解。所以，应用此公钥体制，或者可以破译该密码体制，或者可以正常解密。

如果结合 Rabin 公钥算法，可以将解密算法改进，使解密速度更快。如果把改进后的算法称为 LUC-Rabin 公钥密码算法，那么讨论如下。

4.2 LUC-Rabin 公钥密码体制

设 p,q 是两个奇素数，使得对任意 c，$x^2\equiv c\bmod p$，$x^2\equiv c\bmod q$ 可以在有效时间内求解。令 $N=pq$。$e\in Z_N$，$(e,(p-1)(p+1)(q-1)(q-1))=1$。

(1) 公开密钥：e，N。

(2) 加密算法：对 $\forall(P,Q)\in Z_N\times Z_N$，

计算：$C_0=U_e(P,Q)\bmod N$，$C_1=V_e(P,Q)\bmod N$，$C_2=Q^e\bmod N$，$\tilde{D}=\left(C_0^2\right)^{-1}\left(C_1^2-4C_2\right)\bmod N$。

发送：$(C_2,\tilde{D})$。

(3) 解密密钥：d：$ed\equiv 1\bmod\phi(N)$。

(4) 解密算法：$Q=C_2^d\bmod N$；求解 $\begin{cases}x^2=\tilde{D}+4Q\bmod p\\ x^2=\tilde{D}+4Q\bmod q\end{cases}$ 得 4 个可能解 P_i，$i=1,2,3,4$，再根据 $V_e(P_i,Q)\bmod N=C_1$ 是否成立判断正确的解，或根据 P 中设置的标志来确定正确的 P，以节省计算时间。

(5) 解密原理：

(a) $Q=C_2^d\bmod N$ 即 RSA 解密；

(b) 由性质 3(3)，$D=\left(C_0^2\right)^{-1}\left(C_1^2-4C_2\right)\equiv\tilde{D}\bmod N$，于是有：$P^2=D+4Q\equiv\tilde{D}+4Q\bmod N$，而 $x^2\equiv\tilde{D}+4Q\bmod N$ 与二次同余方程组 $\begin{cases}x^2=\tilde{D}+4Q\bmod p\\ x^2=\tilde{D}+4Q\bmod q\end{cases}$ 有同解，根据 p,q 的选择，同余方程组中每一个方程都可有效求解，且有两个解，再根据中国剩余定理可求得方程组的 4 个可能解：$P_i\bmod N$，$i=1,2,3,4$。

(6) 算法分析：

(a) 算法是 LUC 与 RSA 和 Rabin 公钥算法的复合，从而，其安全性至少同等于其中最安全的一种；

(b) 与 LUC-RSA 一样，由于 LUC-Rabin 中，Q 是任意的，从而相对而言，安全强度比 LUC 增强了；

(c) LUC-Rabin 一次处理 2 个数据。由于解密时使用了 RSA 和 Rabin 密码的解密算法，且减少了 LUC 解密密钥计算时间，所以，解密速度比 LUC 快得多。由于 Rabin 密码的解密时间比 RSA 快得多，相对 RSA 而言可以忽略，那么 LUC-Rabin 加、解密共需 6 个 RSA 时间，所以，其数据吞吐率为 2/6=1/3。

5　LUC-RSA 公钥密码体制示例

设 LUC-RSA 公钥密码体制参数为：$p=1907$，$q=12889$，$N=24579323$。

公钥：$e=789331$。

待加密消息为：$P=2319111$，$Q=323$。

信源计算并发送：$C_0=U_e(P,Q)=23092437$，$C_1=V_e\cdot(P,Q)=9262219$，$C_2=Q^e\bmod N=24217425$。

信宿计算：$\phi(N)=\mathrm{lcm}(p-1,q-1)=12282264$，$D'=C_1^2-4C_2=85788603934261$，$\varepsilon_p'=\left(\frac{D'}{p}\right)=1$，$\varepsilon_q'=\left(\frac{D'}{q}\right)=-1,\ S(N)=S'(N)=\mathrm{lcm}\left(p-\left(\frac{D'}{p}\right),q-\left(\frac{D'}{q}\right)\right)=12284170$。

求得解密密钥：$d=3488443$，$ed\equiv 1\bmod\phi(N)$；$l=6769132$，$el\equiv 2\bmod S(N)$。

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

(1)$Q = C_2^d \bmod N = 323$。

(2)进一步计算：

$$s_p = \frac{(el-2)\left(1-\varepsilon_p'\right)}{2\left(p-\varepsilon_p'\right)}, \quad s_q = \frac{(el-2)\left(1-\varepsilon_q'\right)}{2\left(q-\varepsilon_q'\right)}$$

$s_p \equiv 0 \bmod p-1$, $-s_q \equiv 2723 \bmod q-1$, $\tilde{q} = q^{-1} \bmod p = 427$, $\tilde{p} = p^{-1} \bmod q = 10003$, $U_l\left(C_1, C_2\right) = 598702$，解得

$$\begin{aligned} P &= (q\tilde{q} + p\tilde{p}) C_0 U_l\left(C_1, C_2\right) \bmod N \\ &= (12889 \times 427 + 1907 \times 10003) \times 23092437 \\ &\quad \times 598702 \bmod 24579323 \\ &= 2319111 \end{aligned}$$

类似地可以给出 LUC-Rabin 公钥密码体制的示例。

参 考 文 献

[1] Lidl R, Mullen G L, and Turnwald G. Dickson polynomials. Longman Scientific & Technical, 1993.

[2] Smith P J and Lennon M J J. LUC: A public-key cryptosystem. Ninth IFIP Symposium on Computer Security, E. G. Douglas, ed, Elsevier Science Publishers, 1993: 103–117.

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

[4] Lenstra A K and Verheul E R. The XTR public key system. Crypto'2000, California, USA, Springer LNCS 1880, Springer-Verlag 2000: 1–19.

王衍波： 男, 1961 年生, 硕士, 教授，研究方向为网络安全、现代密码学, 目前主要从事椭圆曲线密码体制的研究工作.

张凯泽： 男, 1968 年生, 博士, 副教授，研究方向为网络安全.

王开华： 男, 1963 年生, 硕士, 教授，研究方向为代数应用、优化与运筹理论.

端木庆峰：男, 1980 年生, 硕士生，研究方向为应用密码学.

雷凤宇： 女, 1980 年生, 硕士生，研究方向为应用密码学.

(C)1994-2022 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net