基于5F-L序列类ElGamal公钥密码体制和数字签名

端木庆峰[1,2] 张雄伟[1] 王衍波[1] 李兵兵[1] 雷凤宇[3]
(解放军理工大学通信工程学院 南京 210007)[1] (南海舰队92146部队 湛江 524001)[2]
(华中科技大学计算机学院信息安全系 武汉 430074)[3]

摘 要 对一类特殊五阶Fibonacci-Lucas序列及其性质进行深入研究,并以五阶Fibonacci-Lucas序列来替代Lucas序列和三阶Fibonacci-Lucas序列,提出基于五阶Fibonacci-Lucas序列类ElGamal的5FLELG公钥密码体制和数字签名方案,验证其正确性和有效性,给出序列项计算方法,并分析体制的安全性和效率。

关键词 LUCELG,3F-LELG,Fibonacci-Lucas序列,公钥密码体制
中图法分类号 TN918.1 **文献标识码** A

ElGamal-like Public-key Cryptosystem and Digital Signature Scheme Based on 5F-L Sequence

DUANMU Qing-feng[1,2] ZHANG Xiong-wei[1] WANG Yan-bo[1] LI Bing-bing[1] LEI Feng-yu[3]
(Institute of Communications Engineering, PLA University of Science & Technology, Nanjing 210007, China)[1]
(Unit 92146 of the South China Sea Fleet, Zhanjiang 524001, China)[2]
(College of Computer Science & Technology, Huazhong University of Science & Technology, Wuhan 430074, China)[3]

Abstract The characteristics of fifth-order Fibonacci-Lucas sequence were deeply researched, and based on it 5FLELG public-key cryptosystem and digital signature scheme were presented which replace the Lucas sequence and 3F-L sequence by fifth-order Fibonacci-Lucas sequence. The correctness and validity were studied and the fast computational algorithm for evaluating the term of fifth-order Fibonacci-Lucas sequence was given. At last, efficiency and security analysis of the scheme was provided.

Keywords LUCELG, 3F-LELG, Fibonacci-Lucas sequence, Public-key cryptosystem

1 引言

线性反馈移位寄存器序列具有良好的伪随机性和周期性,利用其构造公钥密码体制和数字签名方案是公钥密码学研究的重要方向。新西兰Smith等在1994年提出基于二阶LFSR序列的Lucas公钥密码体制[1],进而构造类似ElGamal的LUCELG PK和LUCELG DS[2,3]。1999年,王丽萍[4]详细研究三阶Fibonacci-Lucas序列性质,将Lucas函数替换为密码特性更好的三阶Fibonacci-Lucas函数,提出3F-L公钥密码体制。文献[5]根据3F-L序列性质提出类ElGamal的3F-LELG公钥密码体制和数字签名方案。随后,Guang Gong和Lein Harn[6]提出GH-PKC。Lenstra[7]等人提出XTR公钥密码体制。Kenneth Giuliani和Guang Gong研究五阶LFSR序列的性质并提出类似的五阶XTR体制和GH体制[8]。在此基础上,本文提出基于五阶Fibonacci-Lucas序列类ElGamal的5FLELG公钥密码体制和数字签名方案,验证其正确性和有效性,并对其安全性和效率进行比较分析。

2 5F-L序列及其基本性质

令 $X_{n+k}=a_1X_{n+k-1}+a_2X_{n+k-2}+\cdots+a_kX_n$,$(a_k,X_k\in Z,a_k\neq 0,n\geqslant 0,k\geqslant 1)$,$(X_0=c_0,X_1=c_1,\cdots,X_{k-1}=c_{k-1})$,则$\{X_n\}$称为整数$Z$上的$k$阶Fibonacci-Lucas序列[4]。设$P,Q,R,S\in Z$,五次方程$f(x)=x^5-Px^4+Qx^3-Rx^2+Sx-1$的5个根为$\alpha_1,\alpha_2,\alpha_3,\alpha_4$和$\alpha_5$,称序列$\{V_n\}=\{V_n(P,Q,R,S,1)\}=\{\sum_{i=1}^{5}\alpha_i^n\}$为五阶Fibonacci-Lucas主相关序列(5F-L序列),$\{\bar{V}_n\}=\{\bar{V}_n(P,Q,R,S,1)\}=\{\sum_{i=1}^{5}\alpha_i^{-n}\}$为$\{V_n\}$的对偶序列。$\forall n\in Z$,$V_{n+5}=PV_{n+4}-QV_{n+3}+RV_{n+2}-SV_{n+1}+V_n$。定义序列$\{U_n\}=\{U_n(P,Q,R,S,1)\}=\{\sum_{1\leqslant i<j\leqslant 5}\alpha_i^n\alpha_j^n\}$,$\{\bar{U}_n\}=\{\bar{U}_n(P,Q,R,S,1)\}=\{\sum_{1\leqslant i<j\leqslant 5}\alpha_i^{-n}\alpha_j^{-n}\}$为其对偶序列。

由$P=\sum_{i=1}^{5}\alpha_i$,$Q=\sum_{1\leqslant i<j\leqslant 5}\alpha_i\alpha_j$,$R=\sum_{1\leqslant i<j<k\leqslant 5}\alpha_i\alpha_j\alpha_k$,$S=\sum_{1\leqslant i<j<k<l\leqslant 5}\alpha_i\alpha_j\alpha_k\alpha_l$,$\prod_{i=1}^{5}\alpha_i=1$,可计算$\{V_n\}$序列项$V_0=5,V_1=P,V_2=P^2-2Q,V_3=P^3-3PQ+3R,V_{-1}=S,V_{-2}=S^2-2R,V_{-3}=S^3-3SR+3Q$。$\{U_n\}$序列项$U_0=10,U_1=Q,U_2=Q^2+2S-2PR,U_3=Q^3-3SQ-3PQR+3P^2S+3R^2-3P,U_{-1}=R,U_{-2}=R^2+2P-2SQ,U_{-3}=R^3-3PR-3SRQ+3S^2P+3Q^2-3S$。据此,$f(x)=x^5-V_1x^4+U_1x^3-U_{-1}x^2+V_{-1}x-1$。令$\alpha_1,\alpha_2,\alpha_3,\alpha_4$和$\alpha_5$为其根,则$g(x)=x^5-V_mx^4+U_mx^3-$

到稿日期:2009-06-11 返修日期:2009-08-17 本文受国家自然科学基金课题(60703048)资助。
端木庆峰(1980-),男,博士生,主要研究方向为应用密码学和信息隐藏,E-mail:duanmuziyun@126.com;张雄伟(1965-),男,教授,主要研究方向为语音信号处理、网络信息处理和数字通信等;王衍波(1961-),男,教授,主要研究方向为网络安全和现代密码学;李兵兵(1984-),男,硕士生,主要研究方向为信息隐藏;雷凤宇(1980-),女,博士生,主要研究方向为密码学理论和实践。

$U_{-m}x^2+V_{-m}x-1$ 的 5 个根为 $\alpha_1^m,\alpha_2^m,\alpha_3^m,\alpha_4^m$ 和 α_5^m。

定理 1 m 和 n 为整数，则

(1) $V_{2n}=V_n^2-2U_n,V_{3n}=V_n^3-3V_nU_n+3U_{-n}$；

(2) $U_{2n}=U_n^2+2V_{-n}-2V_nU_{-n},U_{3n}=U_n^3-3V_{-n}U_n-3V_nU_nU_{-n}+3V_n^2V_{-n}+3U_{-n}^2-3V_n$；

(3) $V_{n+2m}=V_{n+m}V_m-V_nU_m+V_{n-m}U_{-m}-V_{n-2m}V_{-m}+V_{n-3m}$；

(4) $U_nU_m-V_{-m}U_{n-m}+3U_{n+m}=V_nV_mV_{n+m}-V_{n-2m}V_{n-m}+V_{2n-3m}-V_{n+2m}V_n-V_{2n+m}V_m+V_{n+m}^2$。

定理 2 设 p 为素数，$\{V_n\}$ 为 $f(x)$ 生成的 5F-L 序列，$\forall n\in Z,V_n(P \bmod p,Q \bmod p,R \bmod p,S \bmod p,1)=V_n(P,Q,R,S,1) \bmod p$。

证明：由 $V_0=5,V_1=P,V_2=P^2-2Q,V_3=P^3-3PQ+3R,V_4=P^4-4P^2Q+2Q^2-4S+4PR,V_{n+5}=PV_{n+4}-QV_{n+3}+RV_{n+2}-SV_{n+1}+V_n$，则 V_n 是关于 P,Q,R 和 S 的关系式，$V_n \bmod p$ 是关于 $P \bmod p,Q \bmod p,R \bmod p,S \bmod p$ 的关系式，可得 $V_n(P \bmod p,Q \bmod p,R \bmod p,S \bmod p,1)=V_n(P,Q,R,S,1) \bmod p$。

定理 3 令 p 和 q 为两不同素数，取 $n=pq$，令 $r=lcm(p^4+p^3+p^2+p+1,p^4-1,p^3-1,q^4+q^3+q^2+q+1,q^4-1,q^3-1)$，$\{V_n\}$ 和 $\{\overline{V}_n\}$ 分别为 $f(x)=x^5-Px^4+Qx^3-Rx^2+Sx-1$ 五阶 Fibonacci-Lucas 主相关序列和对偶序列，则 $\forall k\in Z,V_{kr+1}(P,Q,R,S,1)=P \bmod n,\overline{V}_{kr+1}(P,Q,R,S,1)=S \bmod n,U_{kr+1}(P,Q,R,S,1)=Q \bmod n$ 和 $\overline{U}_{kr+1}(P,Q,R,S,1)=R \bmod n$。

证明：首先针对模 p 情形进行论证。由域多项式性质，$GF(p)$ 上 n 次不可约多项式 $g(x)$ 必整除 $x^{p^n-1}-1$，则 $g(x)=0$ 的根 α 满足 $\alpha^{p^n-1}=1 \bmod p$。

若 $f(x)$ 在 $GF(p)[x]$ 上不可约，令其在分裂域全部根为 $\alpha_i,i\in\{1,2,3,4,5\}$，则 $\alpha_i,\alpha_i^p,\alpha_i^{p^2},\alpha_i^{p^3}$ 和 $\alpha_i^{p^4}$ 为其在分裂域中全部根。由多项式根与系数关系 $\alpha_i^{p^4+p^3+p^2+p+1}=1 \bmod p,i\in\{1,2,3,4,5\}$。

若 $f(x)$ 在 $GF(p)[x]$ 可分解为 $f(x)=(x-a)(x^4-bx^3+cx^2-dx+e)$，$x^4-bx^3+cx^2-dx+e$ 不可约，其在分裂域内根满足 $\beta_{i=1}^{p^4-1} \bmod p,i\in\{1,2,3,4\}$。$f(x)$ 5 个根满足 $\alpha_{i=1}^{p^4-1} \bmod p,i\in\{1,2,3,4,5\}$。

若 $f(x)$ 在 $GF(p)[x]$ 可分解为 $f(x)=(x^2-ax+b)(x^3-cx^2+dx-e)$，其中两因式都不可约，$x^2-ax+b$ 在分裂域内根满足 $\beta_{i=1}^{p^2-1} \bmod p,i\in\{1,2\}$，$x^3-cx^2+dx-e$ 在分裂域内根满足 $\lambda_i^{p^3-1}=1 \bmod p,i\in\{1,2,3\}$，则 $f(x)5$ 个根满足 $\alpha_i^{km(p^2-1,p^3-1)}=1 \bmod p,i\in\{1,2,3,4,5\}$。

若 $f(x)$ 在 $GF(p)[x]$ 可分解为 $f(x)=(x-a)(x+b)(x^3-cx^2+dx-e)$，$x^3-cx^2+dx-e$ 不可约，其在分裂域内根满足 $\beta_i^{p^3-1}=1 \bmod p,i\in\{1,2,3\}$。由于 $abe \bmod p=1,a^{p-1}=1 \bmod p,b^{p-1}=1 \bmod p,a^{p^3-1}=1 \bmod p,b^{p^3-1}=1 \bmod p,f(x)$ 所有根满足 $\alpha_i^{p^3-1}=1 \bmod p,i\in\{1,2,3,4,5\}$。

若 $f(x)$ 在 $GF(p)[x]$ 上可分解为 $f(x)=(x-a)(x^2-bx+c)(x^2-dx+e)$，$x^2-bx+c$ 和 x^2-dx+e 不可约，其在分裂域内根分别满足 $\beta_i^{p^2-1}=1 \bmod p,i\in\{1,2\}$ 和 $\gamma_i^{p^2-1}=1 \bmod p,i\in\{1,2\}$。由于 $ace=1 \bmod p,a^{p-1}=1 \bmod p,a^{p^2-1}=1 \bmod p,f(x)$ 所有根满足 $\alpha_i^{p^2-1}=1 \bmod p,i\in\{1,2,3,4,5\}$。

若 $f(x)$ 在 $GF(p)[x]$ 可分解为 $f(x)=(x-a)(x^2-dx+e)$，x^2-bx+c 和 x^2-dx+e 不可约，其在分裂域内根满足 $\beta_i^{p^2-1}=1 \bmod p,i\in\{1,2\}$。由于 $abce=1 \bmod p,y^{p-1}=1 \bmod p,y^{p^2-1}=1 \bmod p,y\in\{a,b,c\}$，$f(x)$ 根满足 $\alpha_i^{p^2-1}=1 \bmod p,i\in\{1,2,3,4,5\}$。

若 $f(x)$ 在 $GF(p)[x]$ 上可分解为 $f(x)=(x-a)(x+b)(x-c)(x+d)(x-e)$，则 $f(x)$ 根满足 $\alpha_i^{p-1}=1 \bmod p,i\in\{1,2,3,4,5\}$。

综上所述，$f(x)$ 根满足 $\alpha_i^r=1 \bmod p,i\in\{1,2,3,4,5\}$，其中 $r=lcm(p^4+p^3+p^2+p+1,p^4-1,p^3-1,q^4+q^3+q^2+q+1,q^4-1,q^3-1)$。$\forall k\in Z,V_{kr+1}(P,Q,R,S,1) \bmod p=\sum_{i=1}^{5}\alpha_i^{kr+1} \bmod p=\sum_{i=1}^{5}\alpha_i \bmod p=P \bmod p,U_{kr+1}(P,Q,R,S,1) \bmod p=\sum_{1\leqslant i<j\leqslant 5}(\alpha_i\alpha_j)^{kr+1}=\sum_{1\leqslant i<j\leqslant 5}\alpha_i\alpha_j=Q \bmod p$。同理可证 $V_{kr+1}(P,Q,R,S,1)=P \bmod q$ 和 $U_{kr+1}(P,Q,R,S,1)=Q \bmod q$，由中国剩余定理 $V_{kr+1}(P,Q,R,S,1)=P \bmod n$ 和 $U_{kr+1}(P,Q,R,S,1)=Q \bmod n$。

依次类推，可证 $\overline{V}_{kr+1}(P,Q,R,S,1)=S \bmod n$ 和 $\overline{U}_{kr+1}(P,Q,R,S,1)=R \bmod n$。

定理 4 $\{V_n(P,Q,R,S,1)\}$ 和 $\{\overline{V}_n(P,Q,R,S,1)\}$，对正整数 d 和 $e,V_{de}(P,Q,R,S,1)=V_d(V_e,U_e,U_{-e},V_{-e},1),\overline{V}_{de}(P,Q,R,S,1)=\overline{V}_d(V_e,U_e,U_{-e},V_{-e},1),U_{de}(P,Q,R,S,1)=U_d(V_e,U_e,U_{-e},V_{-e},1)$ 和 $\overline{U}_{de}(P,Q,R,S,1)=\overline{U}_d(V_e,U_e,U_{-e},V_{-e},1)$。

3 5FLELG 公钥密码体制和数字签名方案

类似离散对数 ElGamal 公钥密码体制，可构造基于五阶 Fibonacci-Lucas 序列 5FLELG 公钥密码体制和数字签名方案。

Alice 随机选取素数 p，选择 P,Q,R 和 S 使得 $f(x)=x^5-Px^4+Qx^3-Rx^2+Sx-1$ 为 $GF(p)[x]$ 上不可约多项式，其周期 T 整除 $p^4+p^3+p^2+p+1$。选择秘密密钥 $0\leqslant x<T$，计算 $y_1=V_x(P,Q,R,S,1) \bmod p,y_2=U_x(P,Q,R,S,1) \bmod p,y_3=\overline{U}_x(P,Q,R,S,1) \bmod p$ 和 $y_4=\overline{V}_x(P,Q,R,S,1) \bmod p$。5FLELG 公钥密码体制如下：

(1) Alice 的公开密钥为 p,P,Q,R,S 和 (y_1,y_2,y_3,y_4)，秘密密钥为 x；

(2) 明文空间与密文空间相同，为 $\Omega=\{0,1,\cdots,p-1\}$；

(3) Bob 欲向 Alice 发送消息 $m(0\leqslant m<p)$，则随机选取正整数 $0\leqslant k<T$，加密计算 $d_1=V_k(P,Q,R,S,1) \bmod p,d_2=U_k(P,Q,R,S,1) \bmod p,d_3=\overline{U}_k(P,Q,R,S,1) \bmod p,d_4=\overline{V}_k(P,Q,R,S,1) \bmod p,G=V_k(y_1,y_2,y_3,y_4,1) \bmod p$ 和 $C=mG \bmod p$，则加密密文为 (d_1,d_2,d_3,d_4,C)。Bob 将其发送给 Alice；

(4) Alice 收到密文 (d_1,d_2,d_3,d_4,C) 后，计算 $G=V_x(d_1,d_2,d_3,d_4,1) \bmod p,m=CG^{-1} \bmod p$，则 m 为解密明文。

由 $G=V_k(y_1,y_2,y_3,y_4,1) \bmod p=V_k(V_x(P,Q,R,S,1),U_x(P,Q,R,S,1),\overline{U}_x(P,Q,R,S,1),\overline{V}_x(P,Q,R,S,1),1) \bmod p=V_x(V_k(P,Q,R,S,1),U_k(P,Q,R,S,1),\overline{U}_k(P,Q,R,S,1),\overline{V}_k(P,Q,R,S,1),1) \bmod p=V_x(d_1,d_2,d_3,d_4,1)$

mod p

$m=CG^{-1} \bmod p=mGG^{-1} \bmod p=m$。因而5FLELG公钥密码体制是正确的。

类似地，替换加密函数 $G=V_k(y_1,y_2,y_3,y_4,1) \bmod p$ 为 $G=U_k(y_1,y_2,y_3,y_4,1) \bmod p$，$G=\overline{U}_k(y_1,y_2,y_3,y_4,1) \bmod p$ 或者 $G=\overline{V}_k(y_1,y_2,y_3,y_4,1) \bmod p$，体制仍然正确。因而，可将明文编码为4段 m_1,m_2,m_3 和 m_4，同时应用4个序列进行加密，并分别解密，以此提高系统吞吐率。

基于5FLELG公钥密码体制可以构造5FLELG数字签名方案。假定签名者Alice的公开密钥为 p,P,Q,R,S 和 (y_1,y_2,y_3,y_4)，秘密密钥为 x，签名消息为 m。Alice随机选择密钥 k 满足 $(k,T)=1$，计算 $r_1=V_k(P,Q,R,S,1) \bmod p$，$r_2=U_k(P,Q,R,S,1) \bmod p$，$r_3=\overline{U}_k(P,Q,R,S,1) \bmod p$ 和 $r_4=\overline{V}_k(P,Q,R,S,1) \bmod p$，$s=k^{-1}(m-xr) \bmod T$，$c_1=V_{ks-xr}(P,Q,R,S,1) \bmod p$，$c_2=V_{ks-2xr}(P,Q,R,S,1) \bmod p$，$c_3=V_{ks+2xr}(P,Q,R,S,1)-V_{ks-3x}(P,Q,R,S,1) \bmod p$，则 $(m,r_1,r_2,r_3,r_4,c_1,c_2,c_3)$ 即为消息 m 的数字签名。Bob在收到Alice对消息 m 的签名 $(m,r_1,r_2,r_3,r_4,c_1,c_2,c_3)$ 后，计算 $L=V_m(P,Q,R,S,1)V_r(y_1,y_2,y_3,y_4,1)-c_3 \bmod p$ 和 $R=V_s(r_1,r_2,r_3,r_4)U_r(y_1,y_2,y_3,y_4,1)-c_1\overline{U}_r(y_1,y_2,y_3,y_4,1)+c_2\overline{V}_r(y_1,y_2,y_3,y_4,1) \bmod p$，若 $L=R$ 则签名正确，否则签名错误。

由上述可知，$V_{n+2m}=V_{n+m}V_m-V_nU_m+V_{n-m}U_{-m}-V_{n-2m}V_{-m}+V_{n-3m}$，则

$$\begin{aligned}L&=V_mV_{xr}-c_3=V_{ks+xr}V_{xr}-(V_{ks+2xr}-V_{ks-3x})\\&=V_{ks}U_{xr}-V_{ks-xr}U_{-xr}+V_{ks-2xr}V_{-xr} \bmod p\\&=V_{ks}U_{xr}-c_1U_{-xr}+c_2V_{-xr}\\&=V_{ks}U_{xr}-c_1\overline{U}_{xr}+c_2\overline{V}_{xr} \bmod p\\&=V_s(r_1,r_2,r_3,r_4)U_r(y_1,y_2,y_3,y_4,1)-c_1\overline{U}_r(y_1,y_2,y_3,y_4,1)+c_2\overline{V}_r(y_1,y_2,y_3,y_4,1) \bmod p=R\end{aligned}$$

因此，5FLELG数字签名方案是正确的。

$$\text{令}\begin{cases}P=\sum_{i=1}^{5}\alpha_i \bmod p\\C=V_x(P,Q,R,S,1)=\sum_{i=1}^{5}\alpha_i^x \bmod p\\D=U_x(P,Q,R,S,1)=\sum_{1\leqslant i<j\leqslant 5}\alpha_i^x\alpha_j^x \bmod p\\E=U_{-x}(P,Q,R,S,1)=\sum_{1\leqslant i<j\leqslant 5}\alpha_i^{-x}\alpha_j^{-x} \bmod p\\F=V_{-x}(P,Q,R,S,1)=\sum_{i=1}^{5}\alpha_i^{-x} \bmod p\end{cases},$$

式中，P,Q,R,S 和 p 已知，若攻击者能够从 (C,D,E,F) 求解出 x，则体制将被攻破，该问题称为5F-L序列离散对数困难问题(5FLS-DLP)。因而，5FLELG公钥密码体制和数字签名方案是基于5F-L序列离散对数困难问题的。可以证明，5F-L序列离散对数困难问题等价于一般有限域上的离散对数困难问题[8]。基于此，该体制类似于LUCELG和3F-LELG也存在亚指数时间攻击算法。此外，由 $V_d(P_1,Q,R,S,1)V_d(P_2,Q,R,S,1)\neq V_d(P_1P_2,Q,R,S,1)$，5F-L序列具有不可乘性，可防止伪造签名攻击。

4 序列项计算

类似5FLELG加解密过程，需要计算5F-L序列项 V_m，V_{-m}，U_m 和 U_{-m}，其中 $0<m<r$。对5F-L序列，通过 V_k 和 U_k 计算 V_{2k+1} 和 U_{2k+1} 比较复杂，因而无法采用类似Lucas和3F-L倍点加算法计算序列项。根据文献[8]给出的 $GF(q)$ 上五阶特征序列递推关系式，可直接由 $\{V_n\}$ 和 $\{U_n\}$ 的第 $k-3$ 至 $k+3$ 项，第 $-k-3$ 至 $-k+3$ 项计算第 $3k-3$ 至 $3k+3$ 项和第 $-3k-3$ 至 $-3k+3$ 项。序列项递推关系如下：

(1) $V_{3k+2}=V_kV_{2(k+1)}-V_{-k+2}V_{-k}-V_{k+2}U_k+V_2U_{-k}+V_{2(-k+1)}$

(2) $V_{3k+1}=V_{2k}V_{k+1}-V_{-k-1}V_{-k-3}+V_{-2}U_{-k-1}-V_{k-1}U_{k+1}+V_{2(-k-2)}$

(3) $V_{3k}=V_k^3-3V_kU_k+3U_{-k}=V_k(V_{2k}-U_k)+3U_{-k}$ $V_{3k+3}=V_{3(k+1)}$ $V_{3k-3}=V_{3(k-1)}$

(4) $V_{3k-1}=V_{2k}V_{k-1}-V_{-k+1}V_{-k+3}+V_2U_{-k+1}-V_{k+1}U_{k-1}+V_{2(-k+2)}$

(5) $V_{3k-2}=V_kV_{2(k-1)}-V_{-k-2}V_{-k}-V_{k-2}U_k+V_{-2}U_{-k}+V_{2(-k-1)}$

(6) $U_{3k+2}=(V_{-2k}U_{-k+2}-U_{k+2}U_{2k}+V_{k+2}V_{2k}V_{3k+2}-V_{-3k+2}V_{-k+2}+V_{4(-k+1)}-V_{5k+2}V_{k+2}-V_{4(k+1)}V_{2k}+V_{3k+2}^2)/3$

(7) $U_{3k+1}=(V_{-k-1}U_{k-1}-U_{2k}U_{k+1}+V_{2k}V_{k+1}V_{3k+1}-V_{-2}V_{k-1}+V_{k-3}-V_{4k+2}V_{2k}-V_{5k+1}V_{k+1}+V_{3k+1}^2)/3$

(8) $U_{3k}=U_k^3-3V_{-k}U_k-3V_kU_kU_{-k}+3V_k^2V_{-k}+3U_{-k}^2-3V_k$ $U_{3k+3}=U_{3(k+1)}$ $U_{3k-3}=U_{3(k-1)}$

(9) $U_{3k-1}=(V_{-k+1}U_{k+1}-U_{2k}U_{k-1}+V_{2k}V_{k-1}V_{3k-1}-V_2V_{k+1}+V_{k+3}-V_{4k-2}V_{2k}-V_{5k-1}V_{k-1}+V_{3k-1}^2)/3$

(10) $U_{3k-2}=(V_{-2k}U_{-k-2}-U_{k-2}U_{2k}+V_{k-2}V_{2k}V_{3k-2}-V_{-3k-2}V_{-k-2}+V_{4(-k-1)}-V_{5k-2}V_{k-2}-V_{4(k-1)}V_{2k}+V_{3k-2}^2)/3$

将以上各关系式中的 k 用 $-k$ 代入，即得 V_{-3k-3} 至 V_{-3k+3} 和 U_{-3k-3} 至 U_{-3k+3} 的递推关系式。对任意正整数 m，其有符号三进制展开形式为 $m=\sum_{i=0}^{n}a_i3^i$，$a_i\in\{-1,0,1\}$，$a_n=1$，展开长度约为 $\lfloor \log_3 m \rfloor+1$。根据 m 的三进制展开式以及序列项递推公式，可以计算 $\{V_n\}$ 和 $\{U_n\}$ 第 m 和 $-m$ 序列项的值，将其称为三倍点加算法。算法具体描述如下：

(1)初始化。令 $k=1$，$i=n-1$，计算 $V_+=(V_{-1},V_0,V_1,V_2,V_3)$，$V_-=(V_1,V_0,V_{-1},V_{-2},V_{-3})$，$U_+=(U_{-1},U_0,U_1,U_2,U_3)$，$U_-=(U_1,U_0,U_{-1},U_{-2},U_{-3})$；

(2)令 $l=3k+a_i$；

(3)计算 $V_{l+}=(V_{l-2},V_{l-1},V_l,V_{l+1},V_{l+2})$，$V_{l-}=(V_{-l+2},V_{-l+1},V_{-l},V_{-l-1},V_{-l-2})$，$U_{l+}=(U_{l-2},U_{l-1},U_l,U_{l+1},U_{l+2})$ 和 $U_{l-}=(U_{-l+2},U_{-l+1},U_{-l},U_{-l-1},U_{-l-2})$；

(4)令 $k=l$，$i=i-1$；如果 $i\geqslant 0$，转到(2)，否则转到(5)；

(5)输出 $V_{m+}=(V_{m-2},V_{m-1},V_m,V_{m+1},V_{m+2})$，$V_{m-}=(V_{-m+2},V_{-m+1},V_{-m},V_{-m-1},V_{-m-2})$，$U_{m+}=(U_{m-2},U_{m-1},U_m,U_{m+1},U_{m+2})$ 和 $U_{m-}=(U_{-m+2},U_{-m+1},U_{-m},U_{-m-1},U_{-m-2})$。

与大整数乘法运算相比，加减运算以及小常数与大整数乘法运算的计算量可忽略，以大整数乘法运算的数量来衡量算法效率。为提高算法性能，需对部分公式进行优化，以减少算法总乘法运算数量。计算 V_{-ak+b} 和 U_{-ak+b} 仅需要将 V_{ak+b} 和 U_{ak+b} 公式中的 k 用 $-k$ 代入即得，因而 V_{-ak+b} 和 V_{ak+b}，U_{-ak+b} 和 U_{ak+b} 运算量相同。可以看出，该算法运算量主要集中在步骤(3)迭代计算上，每次迭代需要计算 V_{l+}，V_{l-}，U_{l+} 和 U_{l-} 值，第一步需首先计算 $V_{\pm k\pm 3}$，$V_{\pm 2k}$，$V_{\pm 4k}$，$U_{\pm 2k}$，$V_{2(\pm k\pm 1)}$，$U_{2(\pm k\pm 1)}$，$V_{\pm 4k\pm 2}$，$V_{\pm 5k\pm 1}$，$V_{4(\pm k\pm 1)}$，$V_{\pm 5k\pm 2}$，$V_{\pm 3k-2}$，$V_{\pm 3k-1}$，

$V_{\pm 3k}$, $V_{\pm 3k+1}$, $V_{\pm 3k+2}$, $U_{\pm 3k-1}$, $U_{\pm 3k}$ 和 $U_{\pm 3k+1}$，其总共需要 80×2 次大整数模乘运算，其次当 $a_i=1$ 约需 12×2 次大整数模乘运算。当 $a_i=-1$ 约需 12×2 次大整数模乘运算。当 $a_i=0$ 约需16×2 次大整数模乘运算，假定 m 三进制展开式中，1，−1 和 0 出现的概率相等，则第二步平均需要 80/3 次大整数模乘运算。因而，计算 V_{l+}, V_{l-}, U_{l+} 和 U_{l-} 总共平均需要 560/3 次大整数模乘运算。该算法需要⌊$\log_3 m$⌋次循环，因而算法总共平均需要 560/3⌊$\log_3 m$⌋次大整数模乘运算。令加密密钥为 e，模数为 n，则 RSA 平方乘模幂算法大约平均需要 1.5⌊$\log_2 e$⌋次模 n 乘法运算，Lucas 序列项计算需要约 3⌊$\log_2 e$⌋次模 n 乘法运算，3F-L 序列项计算需要约 9⌊$\log_2 e$⌋次模 n 乘法运算。与其它密码体制相比，该算法运算速度相对比较慢。为提高 5FLELG 公钥密码算法效率，可将明文编码为 4 段同时进行加解密，该方法将算法的数据吞吐率提高了 3 倍，计算时间和存储空间大幅降低。但是由于其每次迭代计算的模乘运算数量比较多，因而性能还是比 LUCELG 和 3F-LELG 要差。进一步提高序列项计算算法效率，是 5FLELG 公钥密码体制走向实用的关键。

结束语 本文详细研究五阶 Fibonacci-Lucas 序列相关性质，提出 5FLELG 公钥密码体制和数字签名方案，其以五阶 Fibonacci-Lucas 序列来替代 Lucas 序列和三阶 Fibonacci-Lucas 序列，在序列周期、签名认证以及安全性等方面都比较优越。当然，5FLELG 公钥密码体制自身还存在许多缺陷，要想走向实用还需提高其运算速度，验证其安全性等，这也是今后进一步研究的方向。

参 考 文 献

[1] Smith P. LUC public key encryption-a secure alternative to RSA [J]. Dr. Dobb's Journal, 1993, 18(1): 44-49

[2] Smith P, Skinner C. A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms[C]// Advances in Cryptology-Asiacrypt'94. Berlin: Springer -Verlag, 1995: 355-364

[3] Bleichenbacher D, Bosma W, Lenstra A K. Some remarks on lucas-based Cryptosystem[C]// Advances in Cryptology-CRYPTO'95. Berlin: Springer-Verlag, 1995: 386-396

[4] 王丽萍，周锦君. F-L 公钥密码体制[J]. 通信学报，1999，20(4)：1-6

[5] 王丽萍，韩付成. 基于三阶 Fibonacci-Lucas 序列的一种新的公钥密码体制和数字签名[C]// 密码学进展-ChinaCrypt'2000. 北京：科学出版社，2000：140-144

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

[7] Lenstra A K, Verheul E R. The XTR public key system[C]// Advances in Cryptology-CRYPTO' 2000. LNCS 1880. Berlin: Springer-Verlag, 2000: 1-19

[8] Giuliani K, Gong G. Analogues to the Gong - Harn and XTR Cryptosystems[EB/OL]. http://www. cacr. math. uwaterloo. ca/techreports/2003/corr2003-34. ps, 2003

[9] 陈小松，唐勇民. 基于 n 阶 Dickson 多项式的公钥密码系统[J]. 系统工程，2005，22(3)：124-126

[10] 姜正涛，柳毅，王育民. 基于 LFSR 高次剩余问题构造公钥密码体制的研究[J]. 电子与信息学报，2006，28(3)：542-545

(上接第 67 页)

密性、不可伪造性、不可否认性、强可识别性和抗滥用性等安全特性，而且设计简单、易于实现，无需交互式验证，在通信时不必要使用安全信道，不存在证书管理、存储、撤消等开销问题和密钥托管问题。

参 考 文 献

[1] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)[C]// Advances in Cryptology- CRYPTO' 97. Lecture Notes in Computer Science 1294. Berlin: Springer-Verlag, 1997: 165-179

[2] Gamage C, Leiwo J, Zheng Y. An efficient scheme for secure message transmission using proxy signcryption[C] // Proceedings of 22nd Australasian Computer Science Conference. Berlin: Springer-Verlag, 1999: 420-431

[3] Chan W K, Wei V K. A threshold proxy signcryption[C]//Proceedings of International Conference on Security and Management. Monte Carlo Resort, Las Vegas, Nevada, USA, 2002: 24-27

[4] Li X, Chen K. Identity based proxy signcryption scheme from pairings[C]// Proc. of the 2004 IEEE International Conference on Services Computing. Shanghai, 2004: 494-497

[5] Wang Q, Cao Z F. Two proxy signcryption schemes from bilinear pairings[C]//Proceedings of CANS 2005. Berlin: Springer- Verlag, LNCS 3810. 2005: 161-171

[6] Wang M, Li H, Liu Z J. Efficient identity based proxy-signcryption schemes with forward security and public verifiability[C]// ICCNMC 2005. LNCS3619. Berlin: Springer-Verlag, 2005: 982-991

[7] Li X X, Ch K F. Identity based proxy-signcryption scheme from pairings[C]// IEEE International Conference on Services Computing. Los Alamitos, California: IEEE Computer Society Press, 2004: 494-497

[8] 张学军，王育民. 高效的基于身份的代理签密[J]. 计算机工程与应用，2007，43(3)：109-111

[9] 胡振鹏，钱海峰，李志斌. 基于身份的多接收者的代理签密方案[J]. 华东师范大学学报：自然科学版，2008(1)：83-87

[10] 于刚，黄根勋. 一个前向安全的基于身份的代理签密方案[J]. 计算机工程与应用，2008(2)：157-159

[11] 冯登国，赵险峰. 信息安全技术概论[M]. 北京：电子工业出版社，2009：97-99

[12] WENBO MAO[英]. 现代密码学理论与实践[M]. 北京：电子工业出版社，2004：169-171

[13] 俞惠芳，王彩芬，刘丹青. 基于椭圆曲线的自认证多代理签密方案[J]. 西北师范大学学报：自然科学版，2010，45(6)：43-45

[14] 俞惠芳，王彩芬. 一种新的基于自认证的门限代理签密方案[J]. 计算机工程与设计，2010，30(24)：5588-5590