基于8阶LFSR序列的可证明安全性公钥密码体制*

王泽辉
（中山大学科学计算与计算机应用系，广东 广州 510275）

摘 要：为了满足在带宽受限制且带宽费用高的受限制环境下，实施高效率的加密解密与数字签名的需要，使用了数论、近世代数、算法分析等工具，研究节省公钥、私钥存储量和传输信息量的方案。提出基于8阶系数属于GF（p）LFSR序列的公钥密码体制，称之为8LFSR体制。给出8LFSR上的2个重要协议：可证明安全性加密协议和可证明安全性数字签名协议。分析表明，该密码体制的密钥生成简单，速度远快于ECC，其私钥压缩率高达8倍，优于XTR的3倍私钥压缩率，在多种环境下既能显著地提高运算效率又能保证安全性。

关键词：公钥密码体制；受限制环境；LFSR；IND－CCA2安全；数字签名；快速算法
中图分类号：TP309 **文献标识码：**A **文章编号：**0529-6579（2008）05-0028-05

公钥密码体制十数年来已有了丰硕的成果，然而许多数学上很完美的密码算法，其计算代价是昂贵的，不太适合于受限制（如带宽受限且带宽费用高）信息环境之中。为此国内外提出不少旨在适应受限环境的公钥体制，通过压缩私钥长度节省带宽提高效率。1994年Smith[1]提出LUC体制，1999年Gong等[2]提出G－H体制，同年王丽萍[3]提出3F－L体制及其签名算法，2000年Lenstra等[4]提出XTR体制，上述体制把私钥长度压缩为原来的1/2与1/3。文［5］指出XTR原型存在的参数衔接问题，提出XTR$^+$体制，解决了参数衔接问题并把私钥长度压缩为1/4。文［6］提出6LFSR体制又把私钥长度压缩为1/6。还有许多新成果无法一一列举。此类体制须解决问题是进行数字签名所需的公钥相关信息（嵌入待验证私钥）也需要压缩。

另一方面，可证明安全的密码协议是当前国际上的研究热点，但可证明安全的代价是需要传输的信息量更加庞大，更不适合于受限制信息环境，需解决密文或签名信息膨胀率过大问题。

本文将致力于解决上述两方面问题，将提出一个新型公钥体制8LFSR，其密钥相关信息的压缩率甚高，其加密与签名协议是可证明安全的，但与功能一致的同类协议相比，可明显节省信息存储量、传输信息量和带宽资源。

本文中p、q为素数，$\mathbb{Z}$,$\mathbb{N}$分别为整数集与自然数集，$m,n\in\mathbb{N}$，$\mathbb{Z}_n^*=\{1,2,\cdots,n-1\}$；$GF(p^m)$为有限域，$GF(p^m)^*$为其乘法群，$GF(p^m)[x]$为系数在$GF(p^m)$多项式环，$\#S$表示有限集合$S$的元素数目，$\dagger$为不整除符号，^为幂运算符号，$a\hat{}b=a^b$。

1 可证明安全的公钥体制8LFSR

定义1 假定p是一个大奇素数，$p>8$，p^4+1有一个大素数因子q,$q\dagger(p^k-1)$，$k\in\{1,2,\cdots,7\}$，记$L=(p^4+1)/q$,$k=(p^4-1)L$,取$GF(p^8)$上异于0、1的任一元素a，记$g=a^k$。

命题1 设g如定义1所述，则$<g>=\{g,g^2,\cdots,g^{q-1},1\}$构成了以$g$为本原元的$q$阶循环群。

定义2 令$h_1=g$，$h_2=g\hat{}\{p^4\}$，$h_3=g\hat{}\{p\}$，$h_4=g\hat{}\{p^5\}$，$h_5=g\hat{}\{p^2\}$，$h_6=g\hat{}\{p^6\}$，$h_7=g\hat{}\{p^3\}$，$h_8=g\hat{}\{p^7\}$，$n\in\mathbb{Z}_q^*$，$d_n=\sum_{i=1}^{8}(h_i)^n=\sum_{i=1}^{8}g\hat{}\{np^{i-1}\}$；且记$\sigma_{1,n}=d_n$，$\sigma_{2,n}=(2^{-1}\bmod p)((d_n)^2-d_{2n})$，$\sigma_{3,n}=(6^{-1}\bmod p)((d_n)^3-3d_nd_{2n}+2d_{3n})$，$\sigma_{4,n}=(24^{-1}\bmod p)((d_n)^4+3(d_{2n})^2-6(d_n)^2d_{2n}+5d_nd_{3n}-6d_{4n})$。

定理1 在前述定义下有如下结论：

1）$g\hat{}\{p^4+1\}=1$，$g\hat{}\{p^4\}=g^{-1}$，$g\hat{}\{p^8\}=g$；

2）$(h_{2i-1})^{-1}=h_{2i}$,$h_{2i-1}h_{2i}=1$,$i=1,\cdots,4$；

$\{(h_1)^{-1},\cdots,(h_8)^{-1}\}=\{h_1,\cdots,h_8\}$；

3）当$n\in\mathbb{Z}_q^*$,$(h_1)^n,(h_2)^n,\cdots,(h_8)^n$互不等；

4）$\sigma_{1,n}=d_n\in GF(p)$，$d_n=d_{-n}$；

5）$\sigma_{2,n}$，$\sigma_{3,n}$，$\sigma_{4,n}\in GF(p)$。

证明 由域论对$x,y\in GF(p^m)$,$k\in N$成立

* **收稿日期：**2008－01－16
基金项目：广东省自然科学基金资助项目（7003624）
作者简介：王泽辉（1963年生），男，副教授；E-mail：mcswzh@mail.sysu.edu.cn

$$(x+y)^{\{p^k\}} = x^{\{p^k\}} + y^{\{p^k\}} \quad (1)$$

1) 因 $g^q = 1$, $q \mid p^4+1$, $q \mid (p^8-1)$, 故 $g^{\{p^4+1\}} = 1$, $g^{\{p^4\}} = g^{-1}$, $g^{\{p^8\}} = g$。

2) $h_2 = g^{\{p^4\}} = g^{\{-1\}} = (h_1)^{-1}$, $h_1 h_2 = 1$, 其他类似。

3) 由定义 1 中 $q \dagger (p^k-1)$ 易证。

4) 由 1) 易验证 $(d_n)^p = d_n$, 故 $d_n \in GF(p)$, 因 $\{(h_1)^{-1}, \cdots (h_8)^{-1}\} = \{h_1, \cdots, h_8\}$; 故 $d_n = d_{-n}$。

类似可证 5)。

定义 3　定义迹函数 $Tr: GF(p^8) \to GF(p)$,

$$Tr(g^n) = d_n = \sum_{i=1}^{8} g^{\{np^{i-1}\}},\ n \in \mathbb{Z}_q^* \quad (2)$$

及 $GF(p)[x]$ 上代数方程 $(n \in \mathbb{Z}_q^*)$

$$F_{8,n}(x) = x^8 - \sigma_{1,n}x^7 + \sigma_{2,n}x^6 - \sigma_{3,n}x^5 + \sigma_{4,n}x^4 - \sigma_{3,n}x^3 + \sigma_{2,n}x^2 - \sigma_{1,n}x + 1 = 0 \quad (3)$$

定理 2　对任意 $n \in \mathbb{Z}_q^*$, 方程 (3) 的根恰好是 $(h_i)^n \in GF(p^8)$, $i = 1, \cdots, 8$。

证明: 令 $\prod_{i=1}^{8}(x - (h_i)^n)$, 用定理 1 结论展开系数, 恰好是 $F_{8,n}(x)$ 的系数, 结论成立。

命题 2　记 $\rho_n = (h_1)^n + (h_2)^n = g^{\{n\}} + g^{\{np^4\}}$. 冻结 n 值令 $u_1 = \rho_n$, $u_2 = (\rho_n)^{\{p\}}$, $u_3 = (\rho_n)^{\{p^2\}}$, $u_4 = (\rho_n)^{\{p^3\}}$, 则任意 $n \in \mathbb{Z}_q^*$ 成立

1) $u_2 = (h_3)^n + (h_4)^n$, $u_3 = (h_5)^n + (h_6)^n$, $u_4 = (h_7)^n + (h_8)^n$ (4)

$u_j \in GF(p^4)$, $j = 1,2,3,4$;

2) $u_1 + u_2 + u_3 + u_4 = \sigma_{1,n}$;

3) $u_1(u_2+u_3+u_4) + u_2(u_3+u_4) + u_3u_4 = \sigma_{2,n} - 4$;

4) $u_1u_2(u_3+u_4) + (u_1+u_2)u_3u_4 = \sigma_{3,n} - 3\sigma_{1,n}$;

5) $u_1u_2u_3u_4 = \sigma_{4,n} - 2\sigma_{2,n} + 2$。

证明　由定义 2、定理 1 及式 (1) 并利用韦达定理, 经过逐一检验可证。

定理 3　代数方程 (3) 之根可用下法求出:

1) 先利用方程 (3) 的系数构造 $GF(p^4)$ 中 4 次方程如下:

$$F_{4,n}(x) = x^4 - \sigma_{1,n}x^3 + (\sigma_{2,n}-4)x^2 - (\sigma_{3,n} - 3\sigma_{1,n})x + (\sigma_{4,n} - 2\sigma_{2,n} + 2) = 0 \quad (5)$$

求解 (5) 得到 u_1, u_2, u_3, u_4。

2) 再解 $GF(p^8)$ 2 次方程 $(j = 1, 2, 3, 4)$:

$$y^2 - u_j y + 1 = 0 \quad (6)$$

得 $(h_{2j-1})^n$, $(h_{2j})^n$, 即得到方程 (3) 的全部根。

证明　由命题 2、定理 1 及韦达定理得证。

推论 1　对任意 $n \in \mathbb{Z}_q^*$, $\{(h_i)^n\}_{i=1,\cdots,8}$ 由 4 个 $GF(p)$ 中元素 d_n、d_{2n}、d_{3n}、d_{4n} 唯一确定。

推论 2　d_n 满足递推式

$$d_{n+4} = \sigma_1 d_{n+3} - \sigma_2 d_{n+2} + \sigma_3 d_{n+1} - \sigma_4 d_n + \sigma_3 d_{n-1} - \sigma_2 d_{n-2} + \sigma_1 d_{n-3} - d_{n-4} \quad (7)$$

我们将建立的新型公钥体制的密码学原始模型是 $GF(p^8)$ 上求解迹函数 Tr 的离散对数困难性, 即 $q \mid (p^4+1)$ 足够大使得已知 $g \in GF(p^8)^*$, 和 $Tr(g^n) = d_n \in GF(p)^*$, 反求 $n \in \mathbb{Z}_q^*$ 之值在计算上不可行。由 (7) 知 d_n 满足 8 阶 LFSR (线性反馈移位寄存器), 我们称该体制为 8LFSR 体制。构建其密码学原始模型必须 生成循环群 $<g>$ 的本原元 g 以及快速计算 $d_n = g^{\wedge}n + g^{\{np\}} + \cdots + g^{\{np^7\}}$。

命题 3　从 $GF(p^8)^*$ 中任意一个元素 $a \neq 1$ 出发, 仅需 $O(\log_2 p)$ 次模 p 乘法可生成 g。已知 $n \in \mathbb{Z}_q^*$ 计算 d_n 仅需 $O(\log_2 p)$ 次模 p 乘法, 总比特时间复杂度为 $O((\log_2 p)^3)$。

定义 4　设 p、q 如定义 1 所述, $GF(p^8)^*$ 上的乘法依赖于一个 8 次首一不可约多项式 $P_8(x)$, 不妨设 $P_8(x) = x^8 + x^4 + x^3 + x^2 + 1$, θ 为 $P_8(x)$ 在 $GF(p^8)$ 之根, $GF(p^8)$ 有如下基底表示

$$GF(p^8) = \{\sum_{i=0}^{7} a_i\theta^i \mid a_i \in \mathbb{Z}_p, i = 0,..,7\} \quad (8)$$

在 $GF(p^8)$ 定义一种序关系, 对相异的 $a = \sum_{i=0}^{7} a_i\theta^i$, $b = \sum_{i=0}^{7} b_i\theta^i \in GF(p^8)$, 如 $a_0 < b_0$ 或 $k \in \{1, \cdots, 7\}$ 使 $a_i = b_i$, $i = 0, \cdots, k-1$, $a_k < b_k$ 则定义 a 小于 b。

定义 5　设 $p, q, g, g^{-1} \in GF(p^8)$ 为 8LFSR 体制的公开参数, $n \in \mathbb{Z}_q^*$ 为私钥, 定义

$$\boldsymbol{R}_n(d) = (d_n^0, d_n, d_{2n}, d_{3n}, d_{4n}) \quad (9)$$

为公钥, 3bit 信息 $d_n^0 \in \{0, \cdots, 7\}$ 记录 g^n 的顺序位置, 按定义 4 序关系将 g^n, $g^{np}, \cdots, g^{\{np^7\}}$ 从小到大排序, g^n 的顺序位置是第 $1 + d_n^0$ 个, 再定义

$$\boldsymbol{S}_n(d) = (d_{n-3}, d_{n-2}, d_{n-1}, d_n, \cdots, d_{n+4}) \in GF(p)^8 \quad (10)$$

称为等价公钥。

推论 3　由私钥 n 求公钥 $\boldsymbol{R}_n(d)$ 与等价公钥 $\boldsymbol{S}_n(d)$, 总时间复杂度为 $O((\log_2 p)^3)$, 忽略 3 bit 附加信息, $GF(p^8)$ 上公钥 $\boldsymbol{R}_n(d)$ 仅需 4 个 $GF(p)$ 上元素。

等价公钥 $\boldsymbol{S}_n(d)$ 将用于 Diffie - Hellman 密钥交换、数字签名, 其实施需要隐藏 n、m 计算 d_{nm}, d_{n+m} 的快速算法, 可由如下定理解决。

定理 4　设 n, m 为正整数,

$$A = \begin{pmatrix} 0 & 1 \\ I_7 & \sigma \end{pmatrix}, Q_n = \begin{pmatrix} S_{n-7}(d) \\ \vdots \\ S_{n-1}(d) \\ S_n(d) \end{pmatrix},$$

其中 I_7 为7维单位矩阵，0为7维（行）零向量，$\sigma = (\sigma_1, -\sigma_2, \sigma_3, -\sigma_4, \sigma_3, -\sigma_2, \sigma_1)^T$ 为7维列向量，则当 $\det(Q_0) \neq 0$ 时成立

$$Q_n = Q_0 A^n, A^n = (Q_0)^{-1} Q_n \quad (11)$$

$$Q_{n+m} = Q_m A^n, S_{m+n}(d)^T = Q_m C(A^n) \quad (12)$$

$$C(A^n) = (Q_0)^{-1} S_n(d)^T, d_{n+m} = S_{m-4}(d) C(A^n) \quad (13)$$

$$d_n = (d_7, d_6, \cdots, d_2, d, 8) C(A^n) \quad (14)$$

$C(B)$ 表示矩阵8阶矩阵 B 的第8列.

证明 思路类似于文［6］，略。

算法8L－1 由公钥求出等价公钥.

输入：$p, q, g, R_n(d) = (d_n^0, d_n, d_{2n}, d_{3n}, d_{4n})$；

输出：g^n, $S_n(d)$（n 未知被隐藏）。

（1）依定义2求 $\sigma_{i,n}, i = 1,2,3,4$；解方程(5)得到 $\{u_1, u_2, u_3, u_4\}$，再解(6)得到 $v_i = (h_i)^n, i = 1, \cdots, 8$。

（2）将 $v_i, i = 1, \cdots, 8$ 按从小到大排序，取第 $1 + d_n^0$ 个为 g^n. 不妨设 $v_1 = g^n$，同一方程（6）可验证出解 $v_2 = g^{\wedge}\{np^4\}$，分别对 $\{v_1, v_2\}$ 求 p 次、p^2 次、p^3 次幂可确定 $v_3 = g^{np}, v_4 = g^{\wedge}\{np^5\}$, $v_5 = g^{\wedge}\{np^2\}, v_6 = g^{\wedge}\{np^6\}, v_7 = g^{\wedge}\{np^3\}$, $v_8 = g^{\wedge}\{np^7\}$。

（3）令 $d_{n+1} = h_1 v_1 + h_2 v_2 + h_3 v_3 + \cdots h_8 v_8$，类似得 $d_{n+2}, \cdots d_{n+4}, d_{n-1}, \cdots d_{n-3}$，从而得到 $S_n(d)$。

命题4 执行算法8L－1的时间复杂性是 $O((\log_2 p)^3)$，即用增加 $O((\log_2 p)^3)$ 时间的代价，可以得到公钥 $R_n(d)$ 等价的公钥 $S_n(d)$，从而节省 $S_n(d)$ 的公钥信息约一半的存储或传输量。

算法8L－2 积式求迹函数算法。

输入：$p, q, g, m, R_n(d)$（n 未知被隐藏）；

输出：d_{mn}。

（1）在由算法8F－1求出 $S_n(d)$ 过程中再利用式（7）求 $d_{n-j}, j = 4,5,\cdots 10$，得到 Q_n。

（2）由（11）右式求出 $B = A^n$，再由方阵幂反复－平方乘快速算法求出 $B^m = A^{mn}$。

（3）由式（14）求出 d_{mn}。

推论4 8F－2的时间复杂度为 $O((\log_2 p)^3)$。

由命题3、4可知，8LFSR的公钥、私钥生成快捷，密钥资源丰富，可从任意一个 $GF(p^8)$ 中非0与1的元素出发去构造，达到充分的随机性，比RSA、ECC的密钥生成要快捷得多。

如上所述，设 p 是一个大奇素数，$p > 6$，$p^4 + 1$ 有一个大素数因子 q，且 $q \dagger (p^k - 1)$，$k \in \{1,2, \cdots, 7\}$，$g \in GF(p^8)$ 为阶是 q 的本原元. p, q, g, g^{-1} 为可公开参数，$key = x \in Z_q^*$ 为私钥，$R_x(d) = (d_x^0, d_x, d_{2x}, d_{3x}, d_{4x})$ 为公钥，明文 $M \in GF(p^8)$。设 l 为 p 的比特长度，则公钥与明文的比特长度分别是 $3 + 4l$ 与 $8l$。选择一个对称加密算法（可由现有对称加密算法改造而成），密钥长度为 b_1 bit，加密变换，解密变换分别为 $\mathbf{E}$, $\mathbf{D}$，密文 $c \in GF(p^8)$；选择一个安全程度与c相应的消息认证码算法 $\mathbf{MAC}: GF(p^8) \to \{0,1\}^{\wedge}\{b_3\}$，其内嵌密钥长度为 b_2 bit，b_2, b_3 与1比偏小；选择 $\mathbf{KDF}: GF(p)^2 \to \{0,1\}^{\wedge}\{b_1 + b_2\}$ 为一个由杂凑函数级联而成的密钥导出函数。

8LFSR加密算法。

输入：公开参数 p, q, g, g^{-1}，公钥 $R_x(d)$，明文 M；

输出：密文组 $C = (r, c, v)$。

（1）任意选择 $s \in \mathbf{Z}_q^*$，计算 $r = R_s(d) = (d_s^0, d_s, d_{2s}, d_{3s}, d_{4s})$；

（2）由公钥 $R_x(d)$ 用算法8F－2求出 d_{sx}；

（3）计算 $\mathbf{KDF}(d_s, d_{sx}) \to (K_1, K_2)$；

（4）计算 $c = \mathbf{E}_{K1}(M), v = \mathbf{MAC}_{K2}(c)$，返回3元密文组 $C = (r, c, v)$。

8LFSR解密算法。

输入：公开参数 p, q, g, g^{-1}，私钥 x，密文组 $C = (r, c, v)$。

输出：明文 M 或者“拒绝 C”。

（1）将 r 析取前3 bit记为 r_0，其余4均分记为 r_1, r_2, r_3, r_4，如 $r_0 \in \{0, 1, \cdots, 7\}$，$r_j \in GF(p), j = 1, \cdots, 4$ 有一个不成立，则返回“拒绝该密文组”否则得 $r = R_s(d)$；

（2）由x，d_s 调用算法8F－2，求出 d_{xs}，计算 $\mathbf{KDF}(d_s, d_{sx}) \to (K_1, K_2)$；

（3）计算 $v' = \mathbf{MAC}_{K2}(c)$，如 $v' \neq v$ 则返回“拒绝该密文组”；

（4）计算 $M = \mathbf{D}_{K1}(c)$，返回明文 M。

定义6 设 $\underline{\mathbf{M}} = GF(p^8)$ 为明文空间，$\underline{\mathbf{C}} = \{0,1\}^{3+4l} \times GF(p^8) \times \{0,1\}^{\wedge}\{b_3\}$ 为密文空间，$\underline{\mathbf{K}} = \{\mathrm{Ke}, \mathrm{kd}\}$ 为密钥空间，加密变换定义为

$$E_{ke}(M, s) = C = (r, c, v) \in \underline{\mathbf{C}} \quad (15)$$

定义解密变换为

$$D_{kd}(C) = M \in \underline{\mathbf{M}} \quad (16)$$

由（15），（16）所定义的加密、解密变换集合全体 $\underline{\mathbf{E}}$, $\underline{\mathbf{D}}$ 为加密、解密变换空间，则五元组（$\underline{\mathbf{M}}$,

$\underline{C},\underline{K},\underline{E},\underline{D}$) 构成 8LFSR 公钥密码体制。

下文的 IND – CCA2 安全性定义的概念见[7]，来源于 Rackoff 和 Simon。应用非交互式零知识（NIZK）证明技术，结合文［8］的证明技巧，容易证明

命题 5　如果对称加密算法和消息认证码算法 MAC 是安全的，计算 Diffie – Hellman 问题是不可行的，KDF 是随机函数，则定义 6 所述的 8LFSR 体制是可证明 IND – CCA2 安全的。

2　公钥体制效能评价及签名方案

公钥密码体制所从属的困难问题称为密码学原始模型，XTR 的原始模型等同于 GF（p^6）上群离散对数问题的求解困难性，3F – L 的密码学原始模型从属于 $GF(p^3)$，效能评价必须统一到相同的集合上。

定义 7　设一个公钥密码体制的密码学原始模型是基于集合 G_2 上困难问题，如该体制可使用集合 G_1 上的算术来达到集合 G_2 上的安全性，且 $\#G_2/\#G_1 = r$，则称其私钥压缩率为 r 倍。

命题 6　LUC 体制的私钥压缩率是 2 倍，G – H 体制、3F – L 体制、XTR 体制，私钥压缩率均为 3 倍，XTR$^+$ 与 6LFSR 则为 4 倍与 6 倍。

证明：XTR 体制使用 $GF(p^2)$ 上的算术来达到 $GF(p^6)$ 上的安全性，故私钥压缩率 $r = \#GF(p^6)/\#GF(p^2) = 3$；其余作类似分析可得。

定义 8　设一个公钥签名体制的密码学原始模型是基于集合 G_2 上困难问题，如果执行签名密码协议时需传输的公钥信息可压缩至只需要 k 个集合 G_3 上元素，则称 $r' = \#G_2/(k * \#G_3)$ 为该体制的公钥压缩率。

命题 7　对签名体制，3F – L 的公钥压缩率是 3/4 倍，XTR 的公钥压缩率是 3 倍，XTR$^+$ 与 6LFSR 则是 1 倍与 2 倍。

证明　XTR 体制要传输的信息是 1 个 $GF(p^2)$ 上元素 $Tr(g^n)$，故 $r' = \#GF(p^6)/(1 * GF(p^2) = 3$。对 $3F-L$，$r' = \#GF(p^3)/(4 * GF(p) = 3/4$；对 XTR$^+$，$r' = \#GF(p^8)/(2 * GF(p^4)) = 1$；6LFSR 证明见文[6]。

定理 5　定义 6 所述的 8LFSR 公钥密码体制的私钥压缩率为 8 倍，高于 XTR 体制的 3 倍，XTR$^+$ 体制的 4 倍，6LFSR 的 6 倍。

证明　8LFSR 的密码学原始模型是由 $d_n = Tr(g^n) \in GF(p)$ 求解 n 的迹离散对数难题，用算法 8F – 1 可从 d_n 恢复 $g^n \in GF(p^8)$，反之由 g^n 易求出 d_n，故由 d_n 求解 n 等同于由 g^n 求 n；故类似于 XTR 体制，8LFSR 用 $GF(p)$ 上的算术来达到 $GF(p^8)$ 上的安全性，由定义其私钥压缩率 $= \#GF(p^8)/\#GF(p) = 8$ 倍，优于 XTR 与 XTR$^+$ 的 3 倍与 4 倍。

定理 6　定义 6 所述的 8LFSR 公钥密码体制的公钥压缩率约为 2 倍，低于 XTR 体制的 3 倍，高于 3F – L 与 XTR$^+$ 体制，与 6LFSR 相同。

证明　由定义 6，忽略 3bit 附加信息，8LFSR 的公钥压缩率为 $\#GF(p^8)/(4 * \# GF(p)) = 2$ 倍。

8LFSR 公钥压缩率虽然低于 XTR 的 3 倍，但 XTR 原型没有可证明安全协议，8LFSR 与主流的可证明安全加密协议比较，优势是要传输的密文信息量的压缩。为方便比较我们将 8LFSR 的加密解密协议改写成 Cramer – Shoup 型[9]的协议，限于篇幅不详细列出，仅给出结论。

推论 5　8LFSR 公钥体制的 Cramer – Shoup 型加密解密协议，是可证明 IND – CCA2 安全的，其密文膨胀率（密文比特数与明文比特数之比）为 2.5 倍，明显低于从属于普通循序群的 Cramer – Shoup 原体制的 4 倍密文膨胀率。

类似于前述，设 p,q,g,g^{-1} 为可公开参数，q 的 bit 数与 p 相当，不妨设 p，q 长度均为 l bit，$\boldsymbol{R}_x(d) = (d_x^0, d_x, d_{2x}, d_{3x}, d_{4x})$ 为公钥，x 为私钥由乙方保管，甲方有信息 $M \in GF(p^8)$ 需乙方作签名，**SHA** 是安全杂凑函数. 下描述三元组 EIGamal 族签名协议：

1）乙方选择随机数 $s \in Z_q^*$，计算

$r = \boldsymbol{R}_s(d) = (d_x^0, d_x, d_{2x}, d_{3x}, d_{4x})$ 传给甲方；

2）甲方收到后把 $\alpha = \mathbf{SHA}(M,r)$ 及待定值 β 传输给乙方；

3）乙方收到后计算 $\delta = (\alpha x + \beta s) \bmod q$，把签名信息 (r,δ) 传输给甲方；

4）甲方就得到乙方的签名（r, δ），如果 $d_\delta = d_{\alpha x+\beta s}$ 则验证了签名的有效性。

甲方求 $d_{\alpha x+\beta s}$ 必须采取下列措施：

先由 $R_x(d)$ 调用算法 8F – 1 求出 g^x，由 $R_s(d)$ 调用算法 $8F-1$ 求出 g^s，再由 α,β 计算 $g^{\alpha x}, g^{\beta s}$，得到 $g^{\alpha x+\beta s} = g^{\alpha x} \times g^{\beta s}$，又再计算 $g\hat{}\{(\alpha x + \beta s)p\}$，…，$g\hat{}\{(\alpha x + \beta s)\, p^7\}$，最后得到 $d_{\alpha x+\beta s}$。

待定值 β 有多种选择用于设计不同协议。

命题 8　上述协议是可证明安全数字签名方案，签名数据量约为一般签名方案的 1/（3.2）。

证明　类似于文［10］，使用基于 ROM（随机预言机模型）的分叉归约技术容易证明上述协议是一种强可证明安全的协议。对于明文 $M \in GF(p^8)$，传输的签名信息量仅 $4l + l + 3$ 比特，而一

般签名协议传输的签名信息量需要 $8l+8l$ 比特，比值是 $(4l+l+3)/(8l+8l)\approx 1/(3.2)$。

3 结 论

本文给出一个新型的可证明安全加密体制和数字签名体制，可把私钥长度压缩为原来的1/8而公钥相关信息可节省约一半的传输信息量，执行可证明 IND－CCA2 安全密码协议的密文膨胀率，明显优于安全协议的原型。结果可用于条件受限制的信息环境，在现代电子金融、无线通信、网络通信等领域有重大的应用前景。而在不受限环境，同等私钥长度下可为更长的信息加密或签名。下一步研究将提出新的公钥体制，争取在公钥压缩率不低于 XTR 前提下再提高私钥压缩率。

参考文献：

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

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

[3] 王丽萍，周锦君. F-L 公钥密码体制[J]. 通信学报，1999, 20(4): 1 －6.
WANG Liping, ZHOU Jinjun. F-L Public －key Cryptosystem [J]. Journal of China institute of communications, 1999, 20(4): 1 －6.

[4] LENSTRA A K, VERHEUL E R. The XTR public system [C]// Crypto2000. LNCS 1880. Berlin: Springer, 2000: 1 －19.

[5] WANG Zehui, ZHANG Zhiguo. XTR +: A provable secure public key cryptosystem[C]// Proc of the 2006 International Conference on CIS. Berlin: Springer-Verlag, LNAI 4456, 2007: 534 －544.

[6] 王泽辉. 基于6阶 LFSR 序列的可证明安全性公钥密码体制[J]. 计算机研究与发展，2006, 43(Sup): 232 －238.
WANG Zehui. The provable security public key cryptosystem based on 6-th order lfsr sequence [J]. Journal of Computer Research and Development, 2006, 43(Sup): 232 －238.

[7] RACKOFF C, SIMON D. Non-interactive zero-knowledge proof of knowledge and choeen ciphertext attack[C]// Advances in Cryptology-Proceedings of CRYPTO '91. LNCS 2259. Berlin: Springer, 1992: 443 －444.

[8] SMART N. The exact security of ECIES in the generic group model[C]// Cryptography and Coding 2001. volume 2260 of Lecture Notes in Computer Science, 73 － 84. Springer-Verlag, 2001.

[9] 冯登国. 可证明安全性理论与方法研究[J]. 软件学报，2005, 16(1): 1743 －1756.
FENG Dengguo, Research on theory and approach of provable security [J]. Journal of Software, 2005, 16(1): 1743 －1756.

[10] POINTCHEVAL D, STERN J. Security proofs for signature schemes [C] // U. Maurer, editor. Advances in Cryptology-Proceedings of EUROCRYPT-'96. LN CS 1070. Berlin: Springer, 1996: 387 －39.

The Provable Security Public Key Cryptosystem Based on 8-th Order LFSR Sequence

WANG Ze-hui

(Department of Scientific Computation and Computer Applications, Sun Yat-sen University, Guangzhou 510275, China)

Abstract: Aiming for the efficient encryption/decryption and digital signature in the resource restricted environments, a solution for reducing public and private key spaces and amount of data transmitted over network is investigated with the help of number theory and algebraic theory. A novel public key cryptosystem based on 8-th order LFSR called 8LFSR sequence on GF (p) is given. Over the 8LFSR, two protocols are presented: provable IND-CCA2 security encryption protocol and provable security digital signature protocol. The key generation is much simple and faster than that of ECC, the private key compression ratio is up to 8 which is better than XTR's 3, and show that the 8LFSR can be more effectively used for security requirements in cryptographic protocols in many cases.

Key words: public key cryptosystem; resource restricted environments; LFSR; IND-CCA2 security; digital signature; quick algorithm