# 3F-L 数字签名方案的分析与改进

胡清峰[1], 胡 磊[2], 刘合国[1,2]
(1. 湖北大学数学与计算机科学学院, 湖北武汉 430062; 2. 信息安全国家重点实验室(中国科学院研究生院), 北京 1000349)

摘 要: 本文对 3F- L 数字签名方案进行分析, 给出了对该方案的一般性签名伪造攻击; 针对该方案签名数据太长的缺点, 基于 GF($p^3$) 上离散对数的计算困难性, 提出了一个 Nyberg-Rueppel 型的修改方案, 其签名规模由 5log($p$) 比特约减为 2log($p$) 比特; 并对改进方案的计算效率进行了分析。

关键词: Fibonacci-Lucas 序列; 3F-L 密码系统; Nyberg-Rueppel 型数字签名
中图分类号: TP309. 18 文献标识码: A 文章编号: 0372-2112 (2005) 03-0492-04

# Cryptanalysis on 3F- L Digital Signature and Its Modification

HU Qing-feng[1], HU Lei[2], LIU He-guo[1,2]
(1. *School of Mathematics and Computer Science, Hubei University, Wuhan, Hubei* 430062, *China*;
2. *State Key Lab of Information Security (Graduate School of Chinese Academy of Sciences), Beijing* 100049, *China*)

**Abstract:** A universal forgery attack on the 3F- L digital signature scheme is given. To avoid the flaw of long signature result, a modified version of the 3F- L signature scheme of Nyberg-Ruppel type is proposed. The security and computation efficiency of the modified scheme are analyzed, and the result shows that the security is based on the computational infeasibility of discrete logarithms on GF($p^3$).

**Key words:** fibonacci-lucas sequence; 3F-L cryptosystem; digital signature of Nyberg-Ruppel type

## 1 引言

1985 年提出的 ElGamal 公钥密码[1] 开创了将离散对数问题应用到密码学的先河. 至今, RSA 体制和离散对数体制是实际应用中的两类主要的公钥密码. ElGamal 离散对数密码利用了如下问题的困难性: 给定模 $p$ 有限域的一个元素 $\alpha$, 确定它在一阶递归序列$(1, g, g^2, g^3, \cdots)$中的位置, 其中 $g$ 是模 $p$ 有限域的一个生成元. 该序列称为一阶递归的是因为它由一次多项式 $x- g$ 递归生成. Smith 对此问题作了推广, 他利用一种称为 Lucas 序列的二阶递归序列的相应困难问题构作了 LUC 公钥密码[2,3]. 他认为这样可避免 RSA 公钥密码具有的同态性质的弱点, 但 Bleichenbacher 等人的工作[4] 表明, LUC 公钥密码仍然具有同态加密的弱点. 实际上, 同态性质并不构成对 RSA 体制和 LUC 体制的本质威胁, 采用诸如 OAEP 填充的设计技术[5], 较大规模的公钥能保证这些公钥体制的安全性.

将上述一阶序列的困难性问题推广到三阶递归序列, 并用来构作公钥密码的工作有[6~9]. 相应构作的密码为 Gong-Harn 密码系统和 3F-L 密码系统. Lenstra 和 Verheul 精心设计的 XTR 公钥密码[10] 也属于此类工作. XTR 公钥密码具有密钥规模小、运算速度快的优势, Verheul 本人用很强的密码学证据[11] 表明, XTR 比一类超奇异椭圆曲线公钥密码安全. 最近, Giuliani 和 Gong 提出了一类五阶递归序列导出的公钥密码[12]. 自然, 它是 Gong-Harn 和 XTR 密码系统的进一步推广. 关于此类工作的一个很好的深层次理论评述, 请参见[13].

在本文中, 我们指出文献[9] 中利用上三阶 Fibonacci-Lucas 序列构成的 3F-L 数字签名方案存在本质缺陷, 即存在对方案的一般性伪造攻击(universal forgery). 针对该方案签名数据太长的缺点, 我们提出一个 Nyberg-Rueppel 型的修改方案, 其签名规模为 2log$p$ 比特, 安全性为 $GF(p^3)$ 上离散对数计算的困难性.

## 2 3F- L 数字签名体制

选取素数 $p$, 使得 $p^2+ p+ 1$ 包含有大的素因子. 以 $GF(p)$ 表示 $p$ 元域, $a, b \in GF(p)$, 定义 $GF(p)$ 上两个三阶 Fibonacci-Lucas 序列$(V_0, V_1, V_2, \cdots)$和$(U_0, U_1, U_2, \cdots)$如下:

$$V_0= 3,\ V_1= a,\ V_2= a^2- 2b,\ V_{n+3}= aV_{n+2}- bV_{n+1}+ V_n \quad (n \geqslant 0),$$

$$U_0= 3,\ U_1= b,\ U_2= b^2- 2a,\ U_{n+3}= bU_{n+2}- aU_{n+1}+ U_n \quad (n \geqslant 0).$$

上述两个三阶递归序列与递归系数 $a, b$ 有关, 在需要指明递归系数的地方, $U_n$、$V_n$ 分别记作 $U_n(a, b)$、$V_n(a, b)$. 实际上, $U_n(a, b)= V_n(b, a)$.

收稿日期: 2004-03-15; 修回日期: 2004-11-28
基金项目: 国家自然科学基金(No. 60373041; No. 90104034); 信息安全国家重点实验室开放课题

不难验证, 这两个序列满足如下性质.

性质 **1([6–9]):** (1) $V_{2n}=V_n^2-U_n$, $U_{2n}=U_n^2-V_n$;

(2)若 $n\geqslant 2m>0$, 则 $V_{n+m}=V_nV_m-V_{n-m}U_m+V_{n-2m}$, $U_{n+m}=U_nU_m-U_{n-m}V_m+U_{n-2m}$.

性质 **2([6–9]):** 设 $n\geqslant 0$, $m\geqslant 0$, 则 $V_{mn}(a,b)=V_m(V_n(a,b),U_n(a,b))$, $U_{mn}(a,b)=U_m(U_n(a,b),V_n(a,b))$.

性质 **3:** 若 $f(x)=x^3-ax^2+bx-1$ 是 $GF(p)$ 上不可约多项式, 则 $p^2+p+1$ 是序列 $\{U_n(a,b)\}_{n\geqslant 0}$ 和 $\{V_n(a,b)\}_{n\geqslant 0}$ 的一个周期.

证明　设 $\alpha,\beta=\alpha^p$ 和 $\gamma=\alpha^{p^2}$ 是 $f(x)$ 在 $GF(p^3)$ 中的三个根. 由根与系数的关系知

$$\alpha+\beta+\gamma=a,\ \alpha\beta+\beta\gamma+\gamma\alpha=b,\ \alpha^{p^2+p+1}=1$$

由定义, $f(x)$ 是序列 $\{V_n(a,b)\}_{n\geqslant 0}$ 的零化多项式, 易知([14])该序列具有如下迹表示:

$$V_n(a,b)=\alpha^n+\beta^n+\gamma^n=Tr(\alpha^n),$$

其中 $Tr$ 是 $GF(p^3)$ 对 $GF(p)$ 的迹表示. 由于 $\alpha^{p^2+p+1}=1$, 所以 $p^2+p+1$ 是 $\{V_n(a,b)\}_{n\geqslant 0}$ 的一个周期(不一定是最小周期). 由于不可约多项式的互反多项式也是不可约的, 我们知 $x^3-ax^2+bx-1$ 是不可约多项式, 同样的道理知 $p^2+p+1$ 是的一个周期.

由性质 1 和序列的递归关系, 我们不难在常数时间内, 由六元组 $\pi_n=(V_{n-1},V_n,V_{n+1},U_{n-1},U_n,U_{n+1})$ 计算出六元组 $\pi_{2n}$; 按照序列的递归定义, 由 $\pi_n$ 计算 $\pi_{n+1}$ 是容易的. 因此, 按照经典的"二元重复加倍一加"方法, 我们可在 $O(\log p)$ 时间内计算出任一整数 $n\in[1,p^2+p+1]$ 对应的 $V_n(a,b)$ 和 $U_n(a,b)$.

下面描述 3*F-L* 数字签名体制.

设系数参数为 $p$, $a$, $b$, 其中 $p$ 是大素数, 使得 $p^2+p+1$ 包含有大的素因子; $a,b\in GF(p)$ 使得 $x^3-ax^2+bx-1$ 在 $GF(p)$ 上不可约, 且 $\{V_n(a,b)\}_{n\geqslant 0}$ 的最小周期是 $p^2+p+1$. 一个用户的私钥为 $x\in[1,p^2+p+1]$, 相应的公钥为 $(V_x,U_x)=(V_x(a,b),U_x(a,b))$. 设 $h(\cdot)$ 为公开的 Hash 函数, 将消息映射成 $[1,p^2+p+1]$ 之间的一个整数. 用户对消息 $m$ 的签名步骤如下:

(1)选取随机数 $k\in[1,p^2+p+1]$ 使得 $gcd(k,p^2+p+1)=1$;

(2)计算 $(r_1,r_2)=(V_k,V_k)$;

(3)计算 $s=k^{-1}(h(m)-x\bar{r}_1)\bmod(p^2+p+1)$, 其中 $r_1\in GF(p)$ 按照一个固定公开的方式视为整数 $\bar{r}_1\in[1,p^2+p+1]$;

(4)计算 $(w_1,w_2)=(V_{ks-x\bar{r}_1},V_{ks-2x\bar{r}_1})$;

(5)将 $(r_1,r_2,s,w_1,w_2)$ 作为用户对的签名发出.

签名的验证步骤为判断如下等式是否成立:

$$V_{h(m)}(a,b)=V_s(r_1,r_2)V_{\bar{r}_1}(y_1,y_2)-w_1U_{\bar{r}_1}(y_1,y_2)+w_2 \tag{1}$$

这个验证的根据是: 由性质 1(2), 我们有

$$V_{h(m)}(a,b)=V_{ks+x\bar{r}_1}(a,b)=V_{ks}V_{x\bar{r}_1}-V_{ks-x\bar{r}_1}U_{\bar{r}_1}x+V_{ks-2x\bar{r}_1}$$

而由性质 2,

$$V_{ik}(a,b)=V_s(V_k(a,b),U_k(a,b))=V_s(r_1,r_2),$$

$$V_{x\bar{r}_1}(a,b)=V_{\bar{r}_1}(V_x(a,b),U_x(a,b))=V_{\bar{r}_1}(y_1,y_2),$$

$$U_{\bar{r}_1}(a,b)=U_{\bar{r}_1}(V_x(a,b),U_x(a,b))=U_{\bar{r}_1}(y_1,y_2).$$

注 **1:** 原文[9]关于上述签名验证等式的右边的表达式有印刷错误, 应为本文现在的表达式. 另外, 由于 $\{U_n(a,b)\}_{n\geqslant 0}$ 和 $\{V_n(a,b)\}_{n\geqslant 0}$ 均是周期序列, 可以扩充为双向无限序列 $\{U_n(a,b)\}_{n\in Z}$ 和 $\{V_n(a,b)\}_{n\in Z}$, 并且实际上性质 1 和性质 2 对任意 $n\in Z$ 和 $m\in Z$ 都成立, 这可由迹表示 $V_n=Tr(\alpha^n)$ 和 $U_n=Tr(\alpha^{-n})$ 不难推导出. 原文关于签名生成的第 4 步的 $ks$ 和 $x\bar{r}_1$ 的大小比较和分情形计算是不必要的和琐碎的, 对原体制不作实质改动, 我们按照如上形式对其进行分析.

## 3　3F-L 数字签名体制的分析与改进

3F-L 数字签名的一个明显缺陷是签名数据太长, 签名是一个五元组 $(r_1,r_2,s,w_1,w_2)$. 由签名验证等式(1), 不难发现, 因为 $y_1$, $y_2$ 是公钥, 任何人可按照如下方式对任何消息 $m$ 伪造一个合法签名: 他首先任意选取 $r_1$, $r_2$, $s$, $w_1$, 再按(1)式计算出 $w_2$, 所得 $(r_1,r_2,s,w_1,w_2)$ 即是一个合法签名. 这是对 3F-L 数字签名体制的一个一般性伪造攻击.

下面我们提出一个改造的数字签名方案. 该方案可以保证签名数据很短, 更重要地, 避免了上述一般性伪造性攻击. 改进签名方案是 Nyberg-Rueppel 签名机制的变型, 其签名结果是两个小于的整数, 签名验证由一个消息认证码完成, 这不同于 XTR-Nyberg-Rueppel 签名机制([10], 使用分组密码完成签名验证). 我们的改进方案可对任意长度的消息生成签名.

设系统参数 $p$, $a$, $b$ 同 3F-L 体制, 一个用户的私钥为 $x\in[1,p^2+p+1]$, 相应的公钥为 $(y_1,\cdots,y_6)=(V_{x-1},V_x,V_{x+1},U_{x-1},U_x,U_{x+1})$. 设 $MAC(m,z)$ 是以 $z\in GF(p)$ 为密钥的对消息 $m$(可为长度任意)进行压缩的消息认证码(message authentication code)结果, 其值 $\in[1,p^2+p+1]$. 我们可要求该消息认证码的实现是快速的, 采用带密钥的 hash 函数、用分组密码、或用泛 hash 函数簇(参见[15]或[16])均可以构造快速实现的消息认证码([17]).

设用户要签名的消息为 $m$. 计算签名的步骤如下:

(1)选取随机数 $k\in[1,p^2+p+1]$, 计算 $V_k$;

(2)计算 $h=MAC(m,V_k)$, 若 $h$ 与 $p^2+p+1$ 不互素, 则返回步骤 1, 直到 $gcd(h,p^2+p+1)=1$;

(3)计算 $s=-xh+k\bmod(p^2+p+1)$;

(4)签名结果为 $(h,s)$.

检验签名的步骤为:

(1)检验是否 $h$, $s$ 都属于 $[1,p^2+p+1]$ 且 $gcd(h,p^2+p+1)=1$. 若否, 则拒绝接收签名; 若是, 则计算 $n=sh^{-1}\pmod{p^2+p+1}$;

(2)由 $(V_{x-1},V_x,V_{x+1})$ 和 $n$ 计算出 $V_{x+n}$(按下面性质 4(4));

(3)由 $(U_{x-1},U_x,U_{x+1})$ 和 $n$ 计算出 $U_{x+n}$(按下面性质 4(4));

(4) 计算 $v = V_{s+xh} = V_{h(x+n)} = V_h(V_{x+n}, U_{x+n})$;

(5) 验证是否有 $h = MAC(m, v)$. 若是, 则接收签名, 否则拒绝接收.

性质 **4:** 令

$$\boldsymbol{M}_n = \begin{pmatrix} V_{n-2} & V_{n-1} & V_n \\ V_{n-1} & V_n & V_{n+1} \\ V_n & V_{n+1} & V_{n+2} \end{pmatrix}, \boldsymbol{A} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -b \\ 0 & 1 & a \end{pmatrix}$$

则

(1) $M_n = M_{n-1}A = M_0A^n$;

(2) $det(M_n) = det(M_0) = a^2b^2 - 4a^3 - 4b^3 + 18ab - 27$;

(3) $A^n = M_0^{-1}M_n$;

(4) 由 $(V_{x-1}, V_x, V_{x+1})$ 和 $n$ 容易求出 $V_{x+n}$.

证明 (1)和(2)是显然的. 不难计算, $f(x) = x^3 - ax^2 + bx - 1$ 和它的形式导数的结式为 $-det(M_0)$, 因为 $f(x)$ 不可约, 所以 $det(M_0) \neq 0$, 这证明了(3). 给定 $n$, 由于 $V_{n-1}$、$V_n$ 和 $V_{n+1}$可在 $O(\log p)$ 时间内计算出, 由(3), $A^n$ 和 $M_{x+n} = M_xA^n$ 可在 $O(\log p)$ 时间内计算出. 具体地, 给定 $(V_{x-1}, V_x, V_{x+1})$和 $n$, 计算 $V_{x+n}$的步骤依次是: 计算 $V_{n-1}$, $V_n$, $V_{n+1}$得的第二列; 计算乘积矩阵 $A^n = NM_n$ 的第二列(其中 $N = M_0^{-1}$ 可预计算作为系统参数); 由 $M_x$ 的第二行 $(V_{x-1}, V_x, V_{x+1})$ 计算乘积矩阵 $M_xA^n (= M_{x+n})$ 的第(2, 2)元即得 $V_{x+n}$.

## 4 改进签名方案的安全性与效率分析

基于递归序列的 XTR 公钥密码的安全基础是基本有限域的扩域上的离散对数问题的难解性([10, § 5]). 改进签名方案的安全基础是 $GF(p^3)$上的离散对数问题的难解性.

性质 **5:** 给定 $(V_{n-1}, V_n, V_{n+1}, U_{n-1}, U_n, U_{n+1})$ 求 $n$ 的问题和给定 $\alpha^n$ 求 $n$ 的问题是等价的.

证明 $\{1, \alpha, \alpha^2\}$ 是 $GF(p^3)$ 对 $GF(p)$ 的一组基, 设 $\{\theta_1, \theta_2, \theta_3\}$ 是 $\{1, \alpha, \alpha^2\}$ 的对偶基, 即对任意 $1 \leqslant i \neq j \leqslant 3$, $Tr(\alpha^{i-1}\theta_i) = 1$ 和 $Tr(\alpha^{i-1}\theta_j) = 0$. 设 $y = a_1\theta_1 + a_2\theta_2 + a_3\theta_3 \in GF(p^3)$, $a_1, a_2, a_3 \in GF(p)$, 则 $a_i = Tr(y\alpha^{i-1})$. 给定 $y \in GF(p^3)$ 相当于给定 $a_1, a_2, a_3 \in GF(p)$, 亦即相当于给定 $(Tr(y), Tr(y\alpha), Tr(y\alpha^2))$. 由于 $U_n = Tr(\alpha^{-n})$, 我们可知, 给定 $(V_{n-1}, V_n, V_{n+1}, U_{n-1}, U_n, U_{n+1})$ 求 $n$ 的问题相当于给定 $\alpha^{n-1}$ 和 $\alpha^{-n-1}$ 求 $n$ 的问题, 后者相当于给定 $\alpha^n$ 求 $n$ 的问题.

当 $p$ 大于 340 比特时, $GF(p^3)$ 上的离散对数问题是目前公认难解的. 在这个离散对数问题难解的基础上, 假设所使用的消息认证码是安全的, 类似于 XTR-Nyberg-Rueppel 签名机制([10]), 作为 Nyberg-Rueppel 签名机制的变型, 该方案是安全的.

该方案具有 Nyberg-Rueppel 签名机制签名规模小的优点, 其签名规模为 $2\log p$ 比特.

给定一组 $a, b \in GF(p)$, 将计算 $k \in [1, p^2 + p + 1]$ 对应的 $(V_{k-1}(a, b), V_k(a, b), V_{k+1}(a, b))$(或 $V_k(a, b)$或$(U_{k-1}(a, b), U_k(a, b), U_{k+1}(a, b))$(或 $U_k(a, b)$)的运算称为一次广义指数运算, 由改进签名方案的步骤和性质 4(4)不难发现, 签名生成的计算成本主要是一次广义指数运算, 而签名验证的计算成本则主要是三次广义指数运算, 因此其计算效率是高的. 该方案的签名生成三倍快于签名验证, 适合对签名生成要求高的应用环境.

改进签名方案的一个不足是公钥规模较大, 但私钥仍然同 Gong-Harn 体制[6, 7]、3-LUC 体制[8]、3-LUC 体制[9]、以及 XTR 体制[10]同等规模, 因此, 在典型的基于证书的公钥技术应用中这一不足处并不是严重缺陷(一般情况是可能仅需要用户安全地存贮私钥, 而在线查找其它用户的公钥证书). 另外, 这一不足之处可用下面性质 6 得到一定程度的弥补.

性质 **6:** 由 $V_{n-1}$, $V_n$ 和两个额外的比特信息可以有效且唯一地确定出 $V_{n+1}$.

证明 设 $M_n$ 同性质 4. 因为 $V_{n+2}$和 $V_{n-2}$都是 $V_{n-1}$, $V_n$, $V_{n+1}$的线性组合, 由 $det(M_n)$等于一个与 $n$ 无关的常数(性质 4)可得出一个关于 $V_{n+1}$的三次方程, 其系数是 $V_{n-1}$和 $V_n$ 的多项式. 存在有效算法([18, § 3. 4])计算有限域上一个低次数(三次)多项式的根, 这些根(至多三个)可由附加的额外两个比特唯一地确定.

由性质 6, 连续二个元素的状态 $(V_{x-1}, V_x)$ 的值在周期为 $p^2 + p + 1$ 的三阶递归序列 $\{V_n(a, b)\}_{n \geqslant 0}$中最多出现三次, 在公钥存储受限的环境中, 利用两个附加的额外比特, 我们可将公钥 $(V_{n-1}, V_n, V_{n+1}, U_{n-1}, U_n, U_{n+1})$ 中的三元组 $(V_{x-1}, V_x, V_{x+1})$缩减为二元组 $(V_{x-1}, V_x)$. 同样, 利用另外两个额外的比特信息, 我们可将三元组 $(U_{x-1}, U_x, U_{x+1})$ 缩减为二元组 $(U_{x-1}, U_x)$, 这样, 利用最多四个附加的额外比特, 公钥 $(V_{n-1}, V_n, V_{n+1}, U_{n-1}, U_n, U_{n+1})$ 可减少到 4 个 $GF(p)$ 元素. 相比较而言, 文献[6, 7]没有提出数字签名体制, Gong-Harn 提出的密钥交换体制[6, 7]的公钥大小为 2 个 $GF(p)$ 元素, 而加密体制[7]则不是基于离散对数问题而是基于另一个计算问题——大整数因子分解问题的困难性. Lenstra 和 Verheul 的 XTR 数字签名体制[10]则使用分组密码, 其缺陷是它的应用可能会因对称加密算法的使用而受到密码出口政策的限制. 这些在一定程度上说明了基于递归序列构造安全签名体制的困难性.

## 5 结论

利用低阶递归序列构造公钥加密、数字签名和密钥协商方案是公钥密码研究的重要课题. 对文献[9]中利用三阶 Fibonacci-Lucas 序列构成的 3-LUC 数字签名方案, 本文给出了对该方案的一般性伪造攻击, 因此该方案是完全不安全的. 针对该方案签名数据太长的缺点, 我们提出一个安全的、签名规模小的 Nyberg-Rueppel 型的修改方案.

参考文献:

[1] T ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms [J]. IEEE Transactions on Information Theory, 1985, 31: 469-472.

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

[3] P Smith, C Skinner. A public key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms [A]. Advances in Cryptology-Asiacrypt' 94[C]. Berlin: Springer-Verlag, 1995, LNCS 917: 357- 364.

[4] D Bleichenbacher, B Wieb, A K Lenstra. Some remarks on Lucas based cryptosystem[A]. Advances in Cryptology—CRYPTO' 95[C]. Berlin: Springer-Verlag, 1995, LNCS 963: 386- 396.

[5] E Fujisaki, T Okamoto, D Pointcheval, J Stern. RSA-OAEP is under the RSA assumption[A]. Advances in Cryptology-CRYPTO' 2001[C]. Berlin: Springer-Verlag, 2001, LNCS 2139: 260- 274.

[6] G Gong, L Harn. A new approach on public key distribution[A]. 密码学进展—Chinacrypt' 98[C]. 北京: 科学出版社, 1998. 50- 55.

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

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

[9] 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[A]. 密码学进展—Chinacrypt' 2000[C]. 北京: 科学出版社, 2000. 140- 144.

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

[11] E R Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems[A]. Advances in Cryptology-Eurocrypt' 2001[C]. Berlin: Springer-Verlag, 2001, LNCS 2045: 195- 210.

[12] K Giuliani, G Gong. Analogues to the Gong-Harn cryptosystems[R]. Technical Report CORR 2003-34, available at http://www.cacr.math.uwaterloo.ca

[13] K Rubin, A Silverberg. Torus-based cryptography[R]. to appear, available at http://eprint.iacr.org/2003/039

[14] R Lidl, H Niederreiter. Finite Fields[M]. Addison Wesley, Reading, MA, 1983.

[15] J Black, S Halevi, H Krawczyk, et al. UMAC: Fast and secure message authentication[A]. Advances in Cryptology-CRYPTO' 99[C]. Berlin: Springer-Verlag, 1999, LNCS 1666: 216- 233.

[16] T Krovetz, P Rogaway. Fast universal hashing with small keys and no preprocessing: the PolyR construction[A]. Information Security and Cryptology-ICICS 2000[C]. Berlin: Springer-Verlag, 2000, LNCS 2015: 73- 89.

[17] A J Menezes, P C van Oorschot, S A Vanstone. Handbook of applied cryptography[M]. Boca Raton: CRC Press, 1996.

[18] H Cohen. A course of computational algebraic number theory[M]. Berlin Heidelberg/ New York: Springer-Verlag, 1993.

作者简介:

胡清峰　男, 1964 年出生于湖北, 硕士, 主要研究兴趣为: 计算机算法分析、密码学与应用. E-mail: qingfenghu@yahoo.com.cn.

胡　磊　男, 信息安全国家重点实验室教授, 博士生导师, 主要研究兴趣为: 密码学与信息安全.