第 16 卷第 4 期,增刊 广西科学院学报 Vol. 16,No. 4 & Supplement
2000 年 11 月 Journal of Guangxi Academy of Sciences November 2000

一种 P 公钥网络全公开口令系统的设计实现*

Design and Implementation of an All Public Password System of P Public Key of Network

彭典长 李业清** 彭宏祥***
Peng Dianchang Li Yeqing Peng Hongxiang

(广西玉林维宇信息安全应用技术有限公司 玉林 537000)
(Yulin Weiyu Information Security Application Technology Co. Ltd., Yulin, 537000)

摘要 基于 PDX 体制构造理论,设计出一种网络全公开口令系统. 论述该口令系统单向密码的创新性和实用性. 安全性分析证明 P 公钥网络公开口令系统具有高强度安全性能.

关键词 P 公钥 网络 公开口令系统 单向密码

中图法分类号 TP 393.08

Abstract On the base of structural theorem of PDX system, an all public password system of network is released. its innovation and practicality of one-way cipher is expounded. Safety analysis showed that public password system of P public key of network possessed high security.

Key words P public key, network, public password system, one-way cipher

当今信息安全领域中,随着信息化和网络化的迅猛发展,对信息的各种攻击方式在逐年更新递增[1]. 根据公开的统计数据,现行的攻击手段已超过 4 000 种. 在众多的攻击手段中,口令攻击发生频率是最高的,口令攻击与反攻击是影响最大的攻防战术,因此研究解决口令的安全认证技术,显得尤为重要. 许多计算机安全事故起源,就是“口令”被破译引起的. 黑客攻击计算机系统常常把破译“口令”作为攻击的开始,然后非法潜入系统获取机密信息. 另外,部分计算机系统内部操作人员容易窃取用户的口令作案,其行踪隐蔽不易发觉,发现案情时,往往已造成重大损失. 传统口令基本模式是:①不公开口令,秘密储存口令. ②秘密认证口令. 目前因特网 UNIX 操作系统基本是这种模式,这是现有众多攻击手段得到″生存″的基础. 本系统技术彻底更新传统口令模式,将其变为全公开口令及公开口令认证程序,不储存口令,试图解决当前“口令”受到攻击的根本问题.

2000-08-05 收稿。
* 广西自然科学基金资助项目(0009008)。
** 广西计算中心,南宁,530022(Guangxi Computer Center, Nanning, 530022)。
*** 广西农业科学院,南宁,53007(Guangxi Academy of Agri. Sci., Nanning, 530007)。

1 算法描述

1.1 加密算法

1.1.1 前置复合函数

明文口令数码 $\{K_j\} = K_1, K_2, \cdots, K_n$,另外,口令数码特征函数 $W = f_j(k_1, k_2, \cdots, k_n)$ 可以是任意一种代数函数.用 $\cos(x)$. $\sin(x)$. $\mathrm{SQR}(x)$ 等函数再作一次前置函变,$V_1 = f_1(K_1), V_2 = f_2(k_2), \cdots, V_n = f_n(K_n), (K_j, W_j, V_j, \in Z)$. $\{K_j\}$ 获第 1 次加密.

1.1.2 自由模函数[3] 矩阵

设 $m_j, w_j (j = 1, 2, \cdots, i)$ 分别为自由模函数 F 的模与生成元,不限 $m_j > w_j$ 及 $\gcd(m_j, w_j) = 1$ 条件,m_j, w_j 可以随机选择.

矩阵 $[D] = \begin{vmatrix} d_1 \\ \cdots \\ d_i \end{vmatrix}$.

$[D]$ 是用 $F(V_j)$ 构造的 $i \times n$ 矩阵,其中

$d_i = F(V_n, C_n) = V_1 \cdot C_1 \cdot W_1 - \mathrm{INT}(V_1 \cdot C_1 \cdot W_1 / m_1) \cdot m_1 + \cdots + V_n \cdot C_n \cdot W_n - \mathrm{INT}(V_n \cdot C_n \cdot w_n / m_n) \cdot m_n$. $\{K_j\}$ 第 2 次加密.

1.1.3 单向函数矩阵

自由模复合函数传导定义为:$F_0(a_0^m) \to a_1^m$:$F_1(a_0^m, a_1^m) \to a_2^m$:$F_2(a_0^m, a_1^m, a_2^m) \to a_3^n \to \cdots \to a_{k-1}^m$:$F_k(a_0^m, a_1^m, \cdots, a_{k-1}^m)^m \to a_k^m$. $(m = 1, 2, \cdots, i)$. 这是 $a_0^m (a_i^m \in Z)$ 连续模复合变换一种形式.

$\{a_j^m\} (j = 1, 2, \cdots, k)$ 组成 $K \times i$ 矩阵$[A]$.

$$[A] = \begin{vmatrix} a_0^1 & \cdots & a_0^i \\ \cdots & & \\ a_k^1 & \cdots & a_k^i \end{vmatrix} \quad (k < i).$$

F_j 是异模自由函数,由 $a_0^m \to a_1^m \to \cdots \to a_k^m$ 求 a_k^m 容易,逆 $a_k^m \to a_{k-1}^m \to \cdots \to a_0^m$ 求 a_0^m 困难,$[A]$ 构成单向密码函数.经过$[D] \cdot [A]$ 运算,$\{K_j\}$ 得到第 3 次加密.

上述加密算法全过程是明文口令$\{Kj\}$ 的连续映射过程:

$$K_j \to f_i(K_j) \to [D] \to [D] \cdot [A] = \begin{vmatrix} q_l \\ \cdots \\ q_k \end{vmatrix} \to [H] \to (b_1, \cdots, b_k)(\text{密值}),$$

其中$[H]$是后置初等代数变换 $K \times K$ 矩阵.

$\{K_j\}$ 通过$[H]$运算得到第四次加密.

1.2 解密算法

本系统解密算法不是逐个求解公开口令 $K_1 \sim K_n$,而是通过单向密码函数式解出 M,与公开口令特征函数值 W 进行条件判断运算.

$$R = \begin{cases} 0 \quad (M \neq W) \quad (\text{假}), \\ 1 \quad (M = W) \quad (\text{真}), \end{cases}$$

解出 M 的单向函数式为

$$M = (\cdots((b_1 - n_1 \cdot (((n_2 \cdot b_2 - b_3)/n_3 + b_2) \cdot n_4 - b_1)/n_5) \cdot n_6 - b_4)/N_7 \cdots b_k)/n_k.$$

M 的导出式与自由模传导函数是一个两种不同算法的等价关系.另外,$[D]$映射于$[A]$的

结果，使$(b_1,\cdots,b_k)$与$(k_1,\cdots,k_n)$的某种各自线性组合的模值相等，有模映射式：

$$(S_1 \cdot b_1 + \cdots + S_k \cdot b_k) \equiv (p_1 \cdot k_1 + \cdots + p_n \cdot k_n) \bmod n_j.$$

上述单向函数式和模映射式必须同时满足两种（或若干种）不同性质的数学规则，是现代密码学一种创新．以下给出$[A]$取$k=4$的一种公开解密程序．（加密程序略）

公开解密判程序

```
10  INPUT " A?", A#," B?", B#," C?", C#," D?", D#," K1?", K1," K2?", K2," K3?", K3
20  M#=((A#-7*(((2584*C#-B#)/6549+C#)*276-A#)/1244)*545-D#)/2812
30  V#=A#+B#+C#+D#+137*M#+221*INT(SQR(K1)*99)-159*INT(SQR(K2)*99)-38*INT(SQR(K3)*99)
40  N#=V#-INT(V#/148)*148
50  IF N#^2>0 THEN GOTO 100
60  W1#=K1+K2+K3
70  W#+265*W1#-INT(265*W1#/77777)*77777
80  IF (M#-W#)^2>0 THEN GOTO 100
90  PRINT K1; K2; K3: END
100  PRINT "??": END
```

2　公开口令系统配置方案

本技术的创新在于完全能够公开口令和判断程序，“公开判断程序”实现了长使用周期和短字节数两项指标，可以设计成：①用户自己保存口令加密软盘，供网络访问时证明身份使用．②将公开口令判断程序（或软盘）提供给网络管理机构（或服务器 Web），公布于公共网页上．③用户网页上公开自己的口令判断程序，供别人调用．

用户 A 访问 Web（或网管中心），A 插入口令软盘，输入随机数，产生 A 的 ID 地址码和密码，Web 根据 ID 码调出 A 的公开判断程序解译密值，识别身份真假．

用户 A→B 之间访问，被访者 B 同时在网管中心和 A 的网页上调出 A 的公开判断程序．首先进行 2 种调用程序的“比较”字符运算，结果为 0，再进行解译密码运算；若字符运算结果非 0，则退出．在某种特殊的使用环境，还可以简化配置方案．

本技术系统的加密软件和解密软件由另一个独立密密钥发生器软盘（或芯片）产生，这样便于权威部门统一管理．对于任何对象来说，加、解密的原始构造参数都是“零知识”的，这是“公开口令系统”的一种优良密码性能．

3　高强度安全性分析

本系统的加密算法不公开．1.1.2 描述表明d_j为c_j,w_j,m_j，三因素“NP 问题”构造，1.1.3 描述表明$[D]\cdot[A]$的复合矩阵元素对于$(q_1,\cdots,q_k)$也是“NP 问题”构造．第 2 次加密至第 4 次加密，$[D]$、$[A]$、$[H]$全部矩阵元素为 10 进制内部参数，数目分别是：$r_1=n\times i$、$r_2=k\times(i+1)$、$r_3=k\times k$．考察最小构造规模$(n=2,i=4.k=3)$；情况，当 3 个矩阵的向量基底构造元素分别取 2 位、4 位、2 位（10 进数）参数时，加密强度$r=10^{2.n.i+4.k.(i+1)+2.k.k}=10^{94}$，现有计算机技术条件破译$10^{94}$密钥空间是不可能的．

考察解密程序20行，单向密码解译式7个常量参数是$[A]$元素“子集和”复合代数运算产生的，其中包含自由模运算、和、差、积、商、移项通约等等交替转换复杂运算．很难由这些常量参数逆向导出1.1.3定义中系列$(w_1,\cdots,w_j)$、$(m_1,\cdots,m_j)$等异模参数及一些外部加入参数，所以单向密码解译式是安全的．

考察解密程序30行，模映射式4个系数常量是$[D]\cdot[A]$矩阵向量关于m_j对$k_1,\cdots,k_n$的项求模后的计数结果，属于“NP问题”和“自由模”双重构造参数，不可能由这些参数逆推$[D]\cdot[A]$矩阵元素，所以模映射是安全的．另外，由于自由模变换作用，密值$(b_1,\cdots,b_k)$呈高度离散状态(表1)，用密值间的相关性或频率分析等破译方法破译密值也是不可行的．综上所述，本系统的加、解密算法是安全的．

表1 部分口令密值离散状态

口令			密值			
K_1	K_2	K_3	b_1	b_2	b_3	b_4
1	1	1	+56676	−1071186	+04335	+23571300
1	1	2	−02320	−1181611	−14896	+13177985
1	1	3	−06516	−0375726	−10491	+05037700
1	1	4	−18392	−0105525	−01782	−12461325
1	1	5	−49196	+0155872	−03569	−27946030
1	1	6	+03776	+0275671	+20476	−28025765

4 结语

公开口令系统是一种高强度安全网络身份认证软件，实现了P公钥认证体制的低数位运行．它也符合一类规范的“零知识证明”模型，在以后信息产业中会得到更广泛的应用．

参考文献

1 陈 倩．口令攻击技术研究．密码与信息，2000，(1)：45～54.

2 李业清等．一种实用票证防伪系统的设计实现．密码与信息，2000，(1)：22～26.

3 彭典祥等．P公钥随机矩阵及解决Catch22问题的方案．计算机应用研究，2000，(5)：1～3.

4 卢开澄．计算机密码学．北京：清华大学出版社，1998. 7.

5 Bruce Schneier. Applied cryptography: protocols, algorithms, and source code in C. Second edition. John Wiley & Sons. Inc. 1996.

(责任编辑：蒋汉明)