DOI: 10.13656/j.cnki.gxkx.2000.02.003
广西科学 Guangxi Sciences 2000, 7 (2): 88~89

一种实用票证防伪系统的设计实现*
Designing Implement of a Practical Anti-counterfeit System of Document

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

(广西计算中心 南宁市星湖路 32号 530022)
(Guangxi Computing Center, 32 Xinghulu, Nanning, Guangxi, 530022, China)

摘要 基于 PDX体制构造理论,设计出一个单向认证票证防伪系统,分析该系统的安全性和推广应用的技术优势。结果表明该系统的密钥与密值具备较强的抗破译能力,易于推广应用。
关键词 票证防伪 单向认证 密码
中图法分类号 TP 309.7

Abstract On the base of structural theorem of PDX system, An anti-counterfeit system of document in one-way certification was released. Its safety, popularization and technology superiority were discussed. The cryptographic key and cryptographic value of this system possesses stronger anti-translated capability and is easy expanded.
Key words anti-counterfeit system of document, one-way certification, cipher

电话电码防伪系统和网络票证防伪系统为目前应用较多的高科技密码防伪产品。这两种系统是通过信息多次传输实现双向认证防伪,需建立大型数据库及相应网络建模,成本造价高昂。本票证防伪系统采用 PDX体制随机矩阵构造技术设计,突破密码学"保密解密钥,公开或不公开加密钥"的重要法则,公开解密钥给用户自己判断真伪,实现了单向认证防伪。它脱离了庞大网络和大型数据库,让出宝贵的通讯信道,减少了双向认证多余时间开销和费用。

1 防伪系统的原理和设计

本系统的单向认证机理是:票证开出方用"保密加密程序"加密明码 M和关键内容数据 N,得 2对随机识别暗码 $\begin{matrix}A_1B_1C_1D_1\\A_2B_2C_2D_2\end{matrix}$做成"防伪标志"贴在票证一个角上,另得到关键数据 N的密文 $W_1W_2W_3W_4$,将 N和 $W_1W_2W_3W_4$打印在票证专用栏上;收(验)票证方,可以任意刮去"防伪标志"的一面,见密码 A、B、C、D,对照"尾数特征码"的一个与 A、B、C、D的尾数相同,再采用"公开解密程序"输入 A、B、C、D得到 M^*,若 $M=M^*$ 票证无假,$M\neq M^*$ 表示票证假。若票证真再看 N是否属实?如果怀疑 N被改动,再输入 W_1、W_2、W_3、W_4得 N^*,若 $N=N^*$,表示怀疑错,$N\neq N^*$ 表示怀疑对,票证作废。2套密码设计保证了票证的绝对真实性。公开解密判断程序为:

```
10  INPUT  A,B,C,D,K(I 面码按 K→1,II 面码按 K→2)
20  W=((A-9*(((171*C-B)/1902+C)*1896-A)/3093)*277-D)/1509
30  V=A+B+C+D+287*(W+1)*(K-1)-63*W
40  N=V-INT(V/503)*503
50  IF N<>0 THEN GOTO 70
60  PRINT"M=";W:END
70  PRINT"?":END
```

上述解密程序 20行为内部随机参数"自由模函数"连续变换及若干次代数组合的乘加表达式,30行中的 287 ($\triangle_1$)、-63 ($\triangle_2$)为函变参数,可以扩展成"$A+B+C+D+\triangle_1*K_1+\triangle_2*K_2+\cdots\cdots+\triangle_N*K_n$"其中 K_1、$K_2\cdots\cdots K_n$是与 M、A、B、C、D相关的动态参数,30和 40行为 M及动态参数 K_j连续自由模变换映射于 A、B、C、D的结果,50行是逻辑判断选择,60与 70行判断真伪。

2 安全性分析

解密程序的破译难度有如下几点:(1) 自由模函

1999-12-14收稿。
* 广西自然科学基金资助项目(9811028)。
** 广西玉林维宇信息安全应用技术有限公司,玉林, 537000 (Weiyu Information Security Application Technology CO. Ltd., Yulin, Guangxi, 537000)。
*** 广西农业科学院,南宁, 530007(Guangxi Academy of Agri. Sci., Nanning, Guangxi, 530007)。

数不可逆，不能由密值逆推原值；(2) 原值的关键参数是向量组合值，为 NP问题结构。W 表达式的各个参数都是转化变换参数，不能由此推导内部自由模函数的 M_j (模值)，W_j (乘法因子) 及内部向量参数值；(3) 自由模函数使密值呈离散状态，组合的变元取机器随机数，用各种数学分析方法破译密值是无规律的。内部加密矩阵是 4× 6矩阵，是由 6个机器随机数 (RND 298)、3对自由模函数及 3对向量参数复合函变生成。密钥构造强度 $f(M) = 298^6 \times (10^6)^3 \times (10^4)^3 = 7 \times 10^{44}$；(4) 若攻击者利用 "公开解密程序" 破译 A、B、C、D，由于 A、B、C、D 在程序中是一种连续加、减、乘、除的重叠代数运算，而且必须满足 40行 M 及 K_j 的对于它们的映射条件，很难在满足 2个条件下用一般代数方法或者直接凑合法求解。如果第 20行 W 不作展开式，而是 $W = 144068254 * A/782556837 + 175064 * B/164393981 - 241557036 * C/164393981 - D/1509$ (调用高精度子程序辅助计算)，则破译更困难；(5) 全部不知道密值情况下，破译一个密值概率是 $1/10^{32}$。公开用加密算法得到的一段连续区间密值，有了计算参数，则局部密码强度 $f'(M)$ 是该区间密值矩阵各列元素符号种数之连乘积 (见表 1)。

表 1 密值矩阵

Table 1 Cryptographic value matrix

Q	A	B	C	D
01	+ 0926934	- 11296986	+ 0853892	- 1173808953
02	- 4057059	+ 23639010	- 2170410	+ 2506939500
03	+ 0337383	- 06150531	+ 0463535	- 0683280981
04	+ 1442205	- 10987248	+ 0960736	- 1208378094
05	+ 0850911	+ 01521990	+ 0071166	+ 0119069769
06	- 0046710	+ 03033636	- 0205750	+ 0332148294
07	+ 1421781	- 13556682	+ 1117880	- 1477859301
08	+ 1882260	- 15404070	+ 1324850	- 1696149552
09	- 3741549	+ 21016782	- 1976102	+ 2268834141
10	- 1746417	+ 14437170	- 1203760	+ 1531396584
符号种数 The number of symbols	24655777	236877766	23767574	23677685666

$f'(M) = 3.3 \times 10^{25}$。

上表为 II 面码，明文 Q 区间 = [0, 5556789]，超出此范围需要高精度辅助计算软件支持。下面给出加密明码 Q = 5556789的 I、II 面密码：

I. A_1 - 1712889, B_1 + 21432408, C_1 - 1649386, D_1 - 609661565;

II. A_2 + 1602657, B_2 - 7844754, C_2 + 750406, D_2 - 91961425 71

M 5556789(明文) 9865· 7461(特征值)。

这表明密钥与密值具有较高的破译算法能力，要加强密码强度，可加大密值数位或增加密值项数。

3 推广应用的技术优势

3.1 程序短小

票证防伪标志和标识内容可以交给唯一管理机构制作，而作为用户使用的公开解密判断程序可以制成软件广为散发。没有计算机时也可以用普通计算器运算 20和 30两行程序，验算 30行结果时，用 503除之，整除是 "真"，不整除是 "假"。

3.2 数字签名

主管部门分配 n 个用户 n 种不同内部签名信息矩阵的软件或硬件，各取不同参数输入后即获得 $\triangle_1 \sim \triangle_n$ N 个不同签名参数，并公开报主管部门登录备案。即 $V = A + B + C + D + \triangle_1 K_1 + \cdots \triangle_n K_n$，改为扩展式，替换原程序 30行，实现广播签名的判断效果。

3.3 防涂改软件

根据判断程序 10~ 70行，去掉输入变量 K，成为一种 "防涂改软件"，是公安部门或重要证件、文件印发部门的一种应用软件，作重要内容记录或签发内容加解密鉴别使用。

3.4 移动电话密码芯片

本系统技术制成用户加密芯片和网端解密识别软件，可用于移动电话密码保护上。这种芯片计算层次简化，成本降低，用户在网端参数固化，取消同步数据生成器，是一种既安全又造价低廉的创新产品。

3.5 网络认证部件

目前网络通讯用户向服务器输入口令作为用户身份验证重要参数，存有隐患：口令存在滞留期，容易泄密或被破译和服务器操作员可以利用用户口令滞留期作案。应用本系统技术加解密用户口令和地址，消除口令滞留期和他人盗用口令的条件，并能简化目前复杂的用户验证过程。

4 结语

本文是基于 PDX体制构造理论的单向认证票证防伪系统，它采用的是 4× 6的加解密矩阵，有较强的抗破译能力，将在实践应用中得到验证。

参考文献

1 卢开澄. 计算机密码学. 北京：清华大学出版社，1991. 119~ 169.

2 彭典长，彭宏祥，李业清. Lm公开加密认证矩阵. 通信保密，1999，(3)：67~ 73.

3 彭宏祥，彭典长，李业清. $P(r)n$公钥外部参数和嵌套函数的等概率性. 广西科学，1999，6 (4)：259~ 262.

4 Peter J, Smith L U C. Public-key encryption a secure alternativeto RSA. Dr Dobb's Journal, January, 1993: 90~ 92.

(责任编辑：黎贞崇)