智模数(IFN)在密码科学中的研究及应用

叶球孙

(武夷学院计算机科学与信息工程系,福建武夷山 354300)

[摘要] 为了消除传统的纯数字加密技术(PNCT)保密性的缺陷,即泄密性、期限性和死密性,提出了一种新的基于变进数(VCN)智能特性的PNCT。传统的PNCT生成的准密码数均是恒进数(FCN),其变化规则(FCR)的单一性、机械性和难记性,造成其保密性缺陷。VCN则是FCN的拓展,是一种新的更为广义概念上的数,但其变化规则(VCR)的复杂性、智能性和灵活性,可以克服FCN的保密性缺陷。

[关键词] 变进数;密码学;恒进数;人工智能;智模数

[中图分类号] TP309.7;TP18;TB115 [文献标识码] A [文章编号] 1009-1742(2008)05-0051-07

1 前言

纯字母加密技术(pure characters cyphering technology,PCCT)的发散性较好,而且也有一定的智能性,但其收敛性较差。传统的纯数字加密技术(pure numerals cyphering technology,PNCT)的发散性最好,但其收敛性最差,计算成本高,而且其智能性低。采用字母和数字加密技术具有操作性强、实现容易和拓展性好等优点。为提升加密技术的智能性效果,常常将PCCT和PNCT紧密地组合在一起使用。如基于公钥密码体制或私钥密码体制均可实现的数字签名和数字水印技术等。当然,有些签名或水印信息还可以是一些图形、图像或单位标志等为基本内容或对象。

对数的应用研究局限于恒进制数的计数规则,最常用的是十进数,始于中国商代,但一直到了公元6世纪才推广普及使用到世界各地。1995年,笔者提出了变进制数(VCN)理论及其相关处理技术[1,2],进制数中相邻即位数字间的进退计数换算关系,是可以不断变化的[3]。VCN创新了广义概念上的数(numbers),有独到的观点和许多潜在的科学研究及应用价值;VCN不但可用于密码通信与信息安全方面,而且可用于各种变结构、变参数、复杂系统的建模、分析与综合,研究开发人工智能的新理论、新方法和新技术。笔者尝试将VCN智能技术用于信息加密技术。

2 基本概念

2.1 恒进数(FCN)与变进数(VCN)

在某一进制数中,相邻的位与位之间的即位数字的进退变换关系恒守同一规则的,称为恒进制(fixed carrying rule,FCR),采用FCR描述的数称为恒进制数,简称恒进数(fixed carrying numbers,FCN)。常用的恒进数有十进数(decimal numbers,D)、十六进数(hexadecimal numbers,H)、八进数(octonal numbers,Q)、二进数(binary numbers,B)等。在某一进制数中,相邻位与位之间的即位数字的进退变换关系的规则是可以任意设定和不断变化的,可称其为变进制(variable carrying rule,VCR),采用VCR描述的数称为变进制数,简称变进数(variable carrying numbers,VCN),如年、月、日、时、分、秒的进退变换关系,而且每月不都是30 d的,有28 d,29 d,31 d的,其实质上就是一些地道而典型的变进数。

[收稿日期] 2006-06-27;修回日期 2007-10-10

[基金项目] 福建省自然科学基金项目资助(2006J0414,A0640015);福建省教育厅高校自然科学基金项目资助(JB03264,JB05190)

[作者简介] 叶球孙(1964-),男,福建浦城县人,武夷学院高级工程师、副教授,主要研究领域为计算机科学与技术,模糊数学,人工智能,图形学等,E-mail:qsye2005@yahoo.com.cn

FCN 是 VCN 中的一些特例。当取变进数中相邻位允许的最大即位数字值相等时，即 $F_n = F_{n-1} = \cdots = F_1 = \max(\text{Figures}) \equiv r$，而且 $r_n = r_{n-1} = \cdots = r_1 = r$，$\text{FM}_n = \text{FM}_{n-1} = \cdots = \text{FM}_1 = r+1$，$r \in N$，$N = \{1, 2, 3, 4, 5, \cdots\}$ 时，该 VCN 就变成了 FCN，且即位数字的模（figures' module，FM）没有最大值，只有最小值为 2。

当前，国际上数学或计算机科学领域所研究和使用的数，大都局限于 FCR 的变化规则。这将使得人们对数的研究、发展及使用陷入困惑境地。如某计算机允许使用有效数字位数不够（有限）而带来数值计算的扰动，从而导致 2 个缺陷：a. 有着严密定义的高频率的正向数学运算的计算结果误差得到了延续不断的放大；b. 利用有着严密定义的高频率的正向数学运算结果做反向的数学逆运算时，输出将不能复现输入。

2.2 人工智能（AI）与智模数（IFN）

人工智能（artificial intelligence，AI）是一门新兴的边缘学科。AI 不但已引起众多学科的日益重视，而且还极易诞生一些新的学科研究领域，如作为其姐妹篇的人工情感（artificial emotion，AE）等，并且有越来越重要的实用意义[4~6]。许多由脑科学和认知科学交叉而诞生的新概念、新理论及新方法，如信息可拓技术、意识计算模型[7]、微粒种群算法（particle swarm optimization，PSO）优化极值的拓展技术[8]等，均是可能的深入探索 AI 的新思路。

VCN 的模糊性、计算性和可拓性极强，利用 VCN 可以很好地架起精密数学与模糊数学相互转换的桥梁。智能模糊变进数简称智模数（AI－fuzzy VCN，IFN），就是一种其数制变进关系规则可以人工智能地任意灵活设置的变进数。

2.3 密码科学与纯数字加密技术

密码科学（cypher science，CS）研究的主要对象是密码与密码的拓展技术。CS 中全部用数字字符加密的技术称 PNCT。在日常现实生活的 PNCT 中，FCN 数字密码的使用尤为常见，如银行和家用的钱柜保险箱所采用的开箱密码，而 VCN 数字密码的使用却从未有过。FCN 加密技术的保密性有 3 个缺陷：泄密性，易遭计算机的穷举攻击而破解；期限性，穷举攻击完所有准密码数所需时间有限；死密性，为有效克服 FCN 密码的泄密性和期限性，只有加大海量准密码数的容量，但这会造成无法顺利解密的死密后果。VCN 是 FCN 的变形数，因此 VCN 密码不易泄密，需能破解的期限无常或不定，VCR 设置者能够永远拥有解密权而不会带来死密性后果。

探寻密码的工作中，利用传统经典的宽度优先搜索（breadth－first searches）技术，在巨型计算机上，实现对数字密码的穷举攻击，测试亿万个数，也只是一瞬间的事。因此，CS 的研究和应用，需要有能将“模糊”变“精确”和“精确”变“模糊”的双向快捷变换的智能处理技术。

3 整数型 VCN 与 FCN 及其相互转换

3.1 整数型 FCN 特性及其计算

3.1.1 任意 n 位恒进制整数 FCN 特性

1）等模性（same figures' module，SFM），任意位上即位数字模 FM 均等，$\text{FM} = \text{FM}_i \equiv r+1$，$r \in N$；

2）有界性（limited figures' module，LFM），任意恒进数的即位数字模 $\text{FM} = \text{FM}_i \equiv r+1 \geqslant 2$，$r \in N$；

3）幂权性（different powers on numbers' module，DPN），n 位恒进数模 $\text{NM} = (\text{FM})^n = (r+1)^n$，$r \in N$。

3.1.2 任意 n 位恒进制整数 FCN 的计算

设 $F_{n-1}F_{n-2}\cdots F_1F_0$ 为一个任意的 n 位 $r+1$ 进制的恒进制整数。其中 $r \in N$，$F_{n-1} \in F_n$，$F_{n-2} \in F_n$，$\cdots$，$F_0 \in F_n$，$N = \{1, 2, 3, 4, 5, \cdots\}$，$F_n = \{0, 1, 2, 3, \cdots, r\}$。则一个 n 位 $r+1$ 恒进制整数的数值（按权值展开式）为

$$F_{n-1}F_{n-2}\cdots F_1F_0(n\text{ 位数}) = F_{n-1}(r+1)^{n-1} + F_{n-2}(r+1)^{n-2} + \cdots + F_0(r+1)^0 = N_{\text{FCN}}$$

即

$$N_{\text{FCN}} = \sum_{i=0}^{n-1} F_i(r+1)^i \tag{1}$$

式中 $r = \max(\text{Figures})$。显然，n 位 $r+1$ 恒进制整数的最大数的数值为

$$N_{\max} = rr\cdots r\ (n\text{ 个 }r) = (r+1)^n - 1 = r(r+1)^{n-1} + r(r+1)^{n-2} + \cdots + r(r+1)^0$$

$F_i \equiv r$，即

$$N_{\max} = \max(N_{\text{FCN}}) = r\sum_{i=0}^{n-1}(r+1)^i \tag{2}$$

3.2 整数型 VCN 特性及其计算

3.2.1 任意 n 位变进制整数 VCN 特性

1）可拓性/压缩性。相同数值大小的数由低进制向高进制转换时，其数据的外在表示形式可以得到压缩，节约计算机存储空间，因而其数据[9]的表示及存储既是可拓（extensive）的[10]，也是可压缩（compressible）的，其容量的溢出特性（变溢性）也是

可变的。如0，1，2，3，4，5，6，7，8，9共10个阿拉伯数字字符还不够用，还可拓展用A，B，C，…，X，Y，Z等26个英文字母分别表示10，11，12，…，33，34，35的数值。这样就可以得到2，…，36的任意VCN（含FCN的最小的2进数到最大的36进数）。

2）模糊性/保密性。任意位上的权值为其系列相邻低位即位数字的模的卷积（连乘），其外表组合排列数字的数值大小也是难以精确估算而模糊的，颇具模糊性。外在数据表示的数值大小模糊性越强，其对外保密性越好。

3）智能性/设密性。n位VCN中相邻位即位数字间的进退换算规则是可以事先人工而智能地设定的，所以该进制数的精确换算是可以实现的，颇具智能性[3~5]。

3.2.2 任意n位变进制整数VCN的计算

设$F_nF_{n-1}\cdots F_1$为一个任意的n位变进制整数。其中，$F_n\in R_n$，$F_{n-1}\in R_{n-1}$，…，$F_1\in R_1$；$r_n\in N$，$r_{n-1}\in N$，…，$r_1\in N$；$N=\{1,2,3,4,5,\cdots\}$，$R_n=\{0,1,2,3,\cdots,r_n\}$，$R_{n-1}=\{0,1,2,3,\cdots,r_{n-1}\}$，$R_1=\{0,1,2,3,\cdots,r_1\}$，则一个$n$位变进制整数的数值（按卷积展开式）为

$$\begin{aligned}N_{VCN}&=F_nF_{n-1}\cdots F_1=F_n(r_{n-1}+1)(r_{n-2}+1)\cdots\\&\quad(r_1+1)+F_{n-1}(r_{n-2}+1)(r_{n-3}+1)\cdots\\&\quad(r_1+1)+\cdots+F_1(r_1+1)^0=\\&F_n\prod_{i=1}^{n-1}(r_i+1)+F_{n-1}\prod_{i=1}^{n-2}(r_i+1)+\cdots+\\&F_1(r_1+1)^0\text{，即}\end{aligned}$$

$$N_{VCN}=\sum_{k=2}^{n}F_K\prod_{i=1}^{k-1}(r_i+1)+F_1\qquad(3)$$

式中$r_i=\max(F_i)$，$i\in N$。显然，n位变进制整数的最大数的数值为$N_{max}=100\cdots0-1$（n个0），即

$$\begin{aligned}N_{max}&=r_nr_{n-1}\cdots r_1=r_n(r_{n-1}+1)(r_{n-2}+1)\cdots\\&\quad(r_1+1)+r_{n-1}(r_{n-2}+1)(r_{n-3}+1)\cdots\\&\quad(r_1+1)+\cdots+r_1(r_1+1)^0=\\&r_n\prod_{i=1}^{n-1}(r_i+1)+r_{n-1}\prod_{i=1}^{n-2}(r_i+1)+\cdots+\\&r_1(r_1+1)^0\text{，即}\end{aligned}$$

$$N_{max}=\max(N_{VCN})=\prod_{i=1}^{n}(r_i+1)-1\qquad(4)$$

3.3 整数型VCN与FCN的相互转换

从FCN与VCN的数值计算公式可以看出，当取变进数中相邻位允许的最大即位数字模值恒等，$FM_{n-1}=FM_{n-2}=\cdots=FM_1=FM_0\equiv r+1$，$r\in\{1,2,3,\cdots\}=N$，且$r=\max$（Figures）时，VCN就变成了FCN。所以，FCN只是VCN中的特例。

在FCN中，常用十进数D转换成其他非D的FCN的方法主要有两种：a. 整数用“除模（基）取余”法，小数用“乘模（基）取整”法；b. 利用按权值展开公式的逆运算的求解法。而其他非D的FCN转换成常用十进数D时只有唯一的按权展开式的求解法。

根据VCN的智能特性，它既可以将FCN中常用十进数D转换为$2\leqslant FM<10$的任意低模（基）值FCN，又可以转换为$FM>10$的任意高模（基）值FCN。任何一种FCN或VCN均可以用来准确描述任意物质量值的大小；任意循环或非循环的数也均可用某种逼近的分式，或开奇偶次方根函数，或其他数学函数诸如各种插值/分段函数法来逼近，均能精确地描述。

4 纯VCN加密技术及应用

在PNCT中，FCN数字密码的使用尤为常见，如箱密码为6位十进数的保险箱，假如人工机械地穷举攻击，约用3 a时间才可打开该保险箱，并具有期限性、泄密性和死密性。当然，用计算机进行穷举攻击只是一瞬间的事，不堪一击。

4.1 智模数IFN（516）例

VCN的理论及实践提供一种双向快捷变换而准确定位的智能处理技术。如某IFN的数字代码串516，且设其十进数的有效数字位数为10位，即max（decimal integers）=9 999 999 999 D，由加密者任意设置所有即位数字模FM值为$2\leqslant FM_i\leqslant\max$（integers），$i\in\{1,2,3\}$，$FM_1$，$FM_2$，$FM_3$值同时被破解的可能性极小；即使一旦被破解，其位权卷积值及其求和结果的数值计算，也会受到有效数字位数或精度有限产生的扰动影响而不能求解其真实的数值，它真实数值大小可能是无数个数值（十进数D表示）中的一个，例如：

1）$IFN(516)=(516)_{10,2,9}=5\times2\times9+1\times9+6\times9^0=105$ D；

2）$IFN(516)=(516)_{6,10\,000\,000\,000,20\,000\,000\,000}=5\times10^{10}\times2\times10^{10}+1\times2\times10^{10}+6\times(2\times10^{10})^0=(10^{11}+2)\times10^{10}+6\approx1\times10^{21}$ D；

3）$IFN(516)=(516)_{6,1\,234\,567\,891,9\,876\,543\,212}=5\times1\,234\,567\,891\times9\,876\,543\,212+$

$1 \times 9\,876\,543\,212 + 6 \times 9\,876\,543\,212^{0} = 60\,966\,315\,627\,922\,572\,678 \approx 6 \times 10^{19}$ D 等。例 3 中 FM_1 = 9 876 543 212 D, FM_2 = 1 234 567 891 D, FM_3 = 8 D。

假如某计算机允许使用十进制有效数字位数仅为 10 位,硬件条件不能满足要求,只有通过软件办法的精确运算来处理这种特大整数。用宽度优先搜索法来测试海量的准密码数,估算执行的计算机 CPU 运算指令条数 $> 1 \times 10^{22}$(条),用运算速度为 10^{10}/s (10^{4} MI/s,计算机内每秒执行的百万条指令数)的银河Ⅲ号巨型计算机来运算, 所需时间估算为 3085.18 a。但若采用以 VCR 作密钥的纯 VCN 数字加密技术,只需 1 台通用小微型计算机来准确定位计算,可在相对很短时间内顺利完成。如果采用深度优先搜索(depth - first searches)技术,或是宽度与深度有机结合的启发式双向智能信息搜索技术,由于启发性信息的存在,有些流水线式的"输入"和"输出"是相"串行"特点的工作任务,是多台计算机难以协作"并行"工作来完成的特殊任务。

4.2 ASCII 字符明文用 IFN 加密技术的实验

4.2.1 ASCII 字符信息加密和解密

以 IFN 实现的 ASCII 字符信息加密和解密大致步骤见图 1。

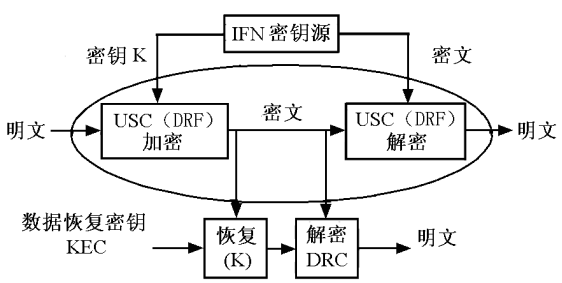

图 1 IFN 密钥托管加密流程

Fig. 1 IFN key escrow proccess of cyphering

1) USC (user security component) 为用户安全分量,由硬件设备或软件程序组成,负责加密和解密,支持密钥托管与数据恢复,其中 DRF 为通用密钥分配机制的构成部分;

2) KEC (key escrow component)为密钥托管分量,由密钥托管代理、数据恢复密钥及其业务 (含 DRC 显露信息和授权指导业务,可人工和自动将数据传入或传出 DRC)、托管密钥防护等 4 部分构成,主要负责密钥托管代理(可信赖的第三方或 USC 和 DRC 的联合机构)操作,数据恢复密钥 (KEC 中心分发的数据加密密钥,建立数据加密的用户密钥,多个 USC 共享且直接与 KEC 相关的主密钥,USC 专有的产品密钥)的存储、显露和使用,以及其他部分业务如托管密钥保护等的业务服务;

3) DRC (data recovery component) 为数据恢复分量,由 IFN 专用算法、协议及必要设备组成。在执行规定的合法数据恢复时,DRC 负责实时解密并截获信息,解密已截获信息和历史记录的通信,非完全知识参与的透明性的解密操作,获取密钥及资源就可从事独立性的解密工作。

4.2.2 以 IFN 实现 ASCII 字符信息加密和解密的实例

在 0, …, 63 的 64 个整数值中:用 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 表示十进制数的 10 个阿拉伯数码字符;用 A, …, Z 的 26 个大写英文字母表示十进制数的 10, 11, 12, …, 35;用 a, …, z 的 26 个小写英文字母表示十进制数的 36, 37, 38, …, 61;还可任意选 2 个公认的或自定义的半角字符(如■, ●等符号)来表示十进制数的 62, 63。英文的明文信息如下:

A great deal of researches on numbers have been shown recently in International Mathematics & Computer Science, much of the attraction of such a FCN (fixed carrying numbers) of n - figures is that it offers an alternative to the growing problems of regularity & movement in calculating for the more.

上述明文按 ASCII 码字符值取 2 位 IFN(FM_1 = 3, FM_2 = 64)作为密钥加密成如下密文:

L2A2W1a0V2U1a2A2V1V2U1Y0A2Z0W0A2a0
V2a1V2U1a0V0W2V2a1A2Z0Y2A2Y2b0Y1U2V2a0a
1A2W2U1a1A2U2V2V2Y2A2a1W2Z0b2Y2A2a0V2V
0V2Y2a2Y0c1A2X0Y2A2O1Y2a2V2a0Y2U1a2X0Z0Y
2U1Y0P2U1a2W2V2Y1U1a2X0V0a1A2C2A2M1Z0Y
1Z1b0a2V2a0A2R2V0X0V2Y2V0V2E2A2Y1b0V0W
2A2Z0W0A2a2W2V2A2U1a2a2a0U1V0a2X0Z0Y2A
2Z0W0A2a1b0V0W2A2U1A2N1M1Q0A2D1N1X0c0
V2V1A2M1U1a0a0c1X0Y2W1Q0b0Y1U2V2a0a1D2
A2Z0W0A2Y2E2W0X0W1b0a0V2a1A2X0a1A2a2W
2U1a2A2X0a2A2Z0W0W0V2a0a1A2U1Y2A2U1Y0a
2V2a0Y2U1a2X0b1V2A2a2Z0A2a2W2V2A2W1a0Z0
b2X0Y2W1A2Z1a0Z0U2Y0V2Y1a1A2Z0W0a0V2W1b
0Y0U1a0X0a2c1A2C2A2Y1Z0b1V2Y1V2Y2a2A2X0
Y2A2V0U1Y0V0b0Y0U1a2X0Y2W1A2W0Z0a0A2a2

W2V2A2Y1Z0a0V2F1

4.2.3 英文信息明/密文变换的精确性及计算的时间复杂性分析

英文信息明/密文变换实现的方法：加密时，通过计算将一个 ASCII 码的明文字符（含空格符），用 J（$J \geq 2$ 的整数）位能表示唯一 IFN 的 ASCII 码字符来置换；解密时，通过计算将每 J 位 ASCII 码的密文字符（IFN），用一个能表示唯一 ASCII 码值的 ASCII 码字符串来反置换。记 $S_{k,m}$ 为第 k 个密文分组中出现第 m（$1 \leq m \leq J$）个明文字符中的单个 ASCII 码字符的集合 $S_m \in S_{k,m}$，而且 $S_m = \mathrm{FM}_i = \{0, 1, 2, \cdots, \max(\mathrm{Figures})\}$，$1 \leq \max(\mathrm{Figures}) \leq 63$，$S_{m,i} = \bigcap_{i=1}^{J} S_{k,m}$，$|S_{k,m}| = 128$，$2 \leq |\mathrm{FMi}| \leq 64$，当且仅当 $S_{m,0}$，$S_{m,1}$，$S_{m,2}$，$\cdots$，$S_{m,63}$ 均为单点集合时，映射 p 就能唯一确定，其中 $p = p_0$，p_1，p_2，$\cdots$，p_{127} 表示所有 ASCII 字符值的相应 VCN 的单值函数。实验可知：若加密时，通过计算将 2 个或 2 个以上 ASCII 码的明文字符排列分组，用 2 个能表示唯一 IFN 的 ASCII 码字符来置换；解密时，亦能通过计算将每 2 个 ASCII 码的密文字符（IFN），用 2 个或 2 个以上能表示唯一 ASCII 码值组合与排列的 ASCII 码字符串来反置换，其加密和解密程序运行时间 $\geq 2^t$（$t \geq J$）倍以上。

采用 VCN 技术对 ASCII 码半角字符加密的基本特性如下。

1）数据处理的吻合性。取 $J = 2$ 时的数据处理的最基本单位正好吻合通用计算机内 CPU 的数据处理规格，因任何一个被加密的 ASCII 码的明文半角字符，须且仅须一个字节空间即 8 bits 二进数（8 bits = 1 Byte）来表示和处理，需计算技术支持的时间复杂度，远远低于明文全角字符如汉字等字符的加密计算时间复杂度。

2）数据分组的缩放性。明文字符数可取等长或不等长值进行分组，加密分组字符数据后得到的密文字符数，既可多于或等于明文字符数，也可少于明文字符数。

3）数据加密的模糊性。明文分组字符数取等长值或不等长值时，可用 VCR 加密，也可用 FCR 加密。当取 $\mathrm{FM}_i > 10$ 以上时的 FCN，其加密模糊性可接近于 VCN，加密后密文字符的模糊性极强。

4）加密技术的安全性。由于 FCR 与 VCR 的独用或混用，以及明文分组字符数可取等长值或不等长值情况，这给计算机用穷举攻击所带来的时间复杂度极高，甚至还远高于全角字符如汉字等字符的加密计算，故其密码遭破译的可能性极小。

5）加密管钥的智能性。由于 FCR 与 VCR 是可以人工智能地独用或混用来设置，被设置的数是一种不易分辨其值大小的智能模糊的变进数（IFN）。其中，FCR 与 VCR 的进制换算关系就是 IFN 加密的密钥 K（Key）。

6）加密用钥的可靠性。人工智能（AI）的搜索技术中[5]，有传统的无信息搜索（或称为盲目搜索）和有信息搜索（启发式搜索）两种。无信息搜索中，又有传统经典的宽度优先搜索（或称为广度优先搜索，breadth - first searches）和深度优先搜索（或称为厚度优先搜索，depth - first searches），对用纯宽度办法设置海量准密码数的密码破译，有且仅有穷举攻击的唯一工作方式，用 IFN 设置的纯数字加密技术的密码，必须采用宽度与深度有机结合的启发式双向智能信息搜索技术才能破译，因此，不用密钥 K 作启发性信息的计算技术支撑的解密破译工作，是采用先进的计算机支持协同工作（CSCW）技术也无能为力的，所以，IFN 的密钥既安全又可靠。

7）密钥托管的可行性。密钥托管的争论焦点有多方面[11]，从维护国家民族或社会团体的整体利益出发，政府或社团对信息加密技术应有至高无上的控制权。民间意见则认为，密钥托管政策把公民的个人隐私置于政府情报部门手中，这违反了诸如美国宪法和个人隐私法，同时也迫使美国公司的密码产品出口受到巨大的限制和影响；学术界认为，应宣扬和推动密钥托管技术的研究与开发；以 Deffie 为代表的反对意见则认为，密钥托管系统的技术还不成熟，投资成本过高；但笔者认为，用 IFN 对信息数据加密，能使密钥托管系统的管理和控制技术逐渐走向成熟，数据安全性能逐渐提高，而且其投资成本也不会过高（只要不做诸如取字节：1 Byte > 8 bits的集成芯片上的硬件设计等），密钥托管的可行性好。

4.3 讨论

上述密钥 K 取为 2 位智模数加密 1 个 ASCII 码字符，其密文字符数（含空格字符）正好是明文字符数的 2 倍。其模值 NM（IFN）= 64 × 3 = 192，max（IFN）= 191，min（IFN）= 0，除 128 个 ASCII 基本字符集外，用户还可拓展 64 个新半角字符使用。

若上述密钥 K 取为 m 位 IFN 加密 n 个顺序排列 ASCII 码字符，其密文字符数（含空格字符）正好

是明文字符数的(m/n)倍。m 与 n 取值情形如下。

1)当 $m>n$ 时,信息字符数量增多而被稀释,须稀释映射函数计算技术支持,加密/解密速度稍慢。

2)当 $m=n$ 时,信息字符数等量置换,不用 IFN 时,只须密码本或密码手册而无须计算技术支持,加密/解密速度快;用 IFN 时,须计算技术支持,加密/解密速度稍慢。

3)当 $m<n$ 时,信息字符数量减少而被浓缩,须浓缩映射函数计算技术支持,加密/解密速度会明显下降)。

此外,当密文中一旦有缺失或缺损字符的现象存在时,使用 IFN 密钥的解密工作将变得十分困难,甚至有时将无法恢复其明文原样。该情形应当极力避免。

这里,稀释映射函数或浓缩映射函数的计算均与 IFN 的 NM 计算公式有关。而 IFN 的模值 NM 为 m 个基模值 $FM_i(0\leqslant i\leqslant m-1, m\geqslant 2)$ 的卷积,它与利用密钥产生古典移位密码的基于混沌序列的分组密码算法有些相似[12],但古典的移位密码既不能抵抗已知明文攻击,也不能抵抗唯密文攻击,没有安全性可言,根本原因是其移位计算的固定规则不变,数模值计算多数情况呈现出"同底 k 次幂有序或无序"关系,$1\leqslant k\leqslant m$,所以古典移位密码的破译问题极易解决。而 IFN 的数模值计算多数情况呈现出"不同底 1 次幂有序"或"不尽同底而有序"关系,其移位计算的变化规则灵活多变,左右移位时须做不同规则的伸缩变形与调整,硬件上无从实现,软件上难以入手。因此,用 IFN 设置密码安全可靠。

市场上已销售各种防盗门上使用的 A/B 机械锁等产品,那只是 VCN 技术的萌芽产品,还没有使用复杂的数值计算技术,VCN 加密技术的应用还有很多工作要做,如序列(流)密码的密钥序列均采用了伪随机序列,而 IFN 可完全用于伪随机序列的产生;用 IFN 设计分组密码可以有足够大的密码分组长度,有足够大的密钥空间,有足够强的时间计算复杂度;RSA 公钥密码系统的安全依据,在于求 2 个大素数的乘积在计算上是容易的,但要分解一个大数的素因子则是相当困难的,IFN 是建立在 VCN 基础上的广义数,它比传统 FCN 的大数的素因子的分解更加困难,也更加复杂,故采用 IFN 的 RSA 公钥密码系统更加安全。

5 结语

利用 VCN 可拓性/压缩性、模糊性/保密性、智能性/设密性,即 VCR 自身计算技术的复杂性、智能性和灵活性,按其变换规则生成的准密码数,可很好地消除 FCR 所造成的单一性、机械性和难记性等缺点。

现代网络高级密码体系中,不管哪种网络系统安全机制、通信网的安全技术及实现、网络系统集成安全技术的信息处理,还是哪种网络安全测试工具的操作使用,只要涉及数字化而可做数值计算的数据(data),均可先将其智模化为 IFN 的各种形式,而后再做各种 IFN 形式数据的加工处理。因此,IFN 设置技术在现代网络高级密码体系中有极其广阔的应用前景。

参考文献

[1] 叶球孙. n 位变进数研究与应用[A]. 第三届中南模糊数学与系统科学学术大会(SCI)论文集[C]. 北京:中国气象出版社, 1995

[2] Ye Qiusun. Research & application on the variable carrying numbers [A]. IEEE International Conference on Neural Networks & Signal Processing Vol 2 [C]. ICNNSP'95 (ISTP), Nanjing, China, 1995: 910 - 914

[3] Ye Qiusun. Research & application of breadth - first search and depth - first search [A]. The 3rd Pacific Rim International (IFIP TC12/IEEE CS & CCF) Conference on Artificial Intelligence, Vol 1 [C]. PRICAI'94 (ISTP), Beijing, China, 1994:142 - 147

[4] 傅京孙, 蔡自兴, 徐光祐,等. 人工智能及其应用[M]. 北京:清华大学出版社, 1988

[5] 吴文俊. 计算机时代的脑力劳动机械化与科学技术现代化[R]. 中国人工智能学进展(特邀报告)[C],北京:北京邮电大学出版社, 2003

[6] 涂序彦. 人工情感[R]. 中国人工智能进展(特邀报告)[C],北京:北京邮电大学出版社, 2003,1. 27 - 32

[7] 周昌乐. 意识计算模型的研究综述[A]. 中国人工智能进展[C]. 北京:北京邮电大学出版社, 2003. 71 - 76

[8] 吕艳萍, 李绍滋, 周昌乐,等. 自适应扩散混合变异机制微粒群算法[J]. 软件学报, 2007, 18(11): 2740 - 2750

[9] 叶球孙. 空间三维立体真实图形可视性的数值表示[J]. 计算机辅助工程, 1997,6(4): 38 - 44

[10] 蔡 文, 杨春燕, 林伟初, 等. 可拓工程方法[M]. 北京:科学出版社, 1997

[11] 林柏钢. 网络与信息安全[M]. 北京:机械工业出版社, 2004

[12] 金晨辉. 一个基于混沌序列的分组密码算法的分析[J]. 中国工程科学, 2001, 3(6): 75 - 80

Research & application of IFN in cypher science

Ye Qiusun

(*Dept. of Computer Science & Engineering, Wuyi University, Wuyishan, Fujian 354300, China*)

[**Abstract**] To overcome 3 shortcomings of the traditional PNCT (pure numerals ciphering technology) of that, properties of the divulging a secret, the allotted time and the dead secrets. This paper gives a novel ciphering technique based on specific properties of intelligent VCN (variable carrying numbers). All allowed cipher numbers are FCN (fixed carrying numbers), in the traditional PNCT, and their changing rules of FCN are both very simple, mechanism and too difficult to be remembered, so that they make the mentioned shortcomings of being sure secrecy in the course of nature. The VCN are extension of the FCN, which are also a new concept of numbers in a broad sense, but their complex, intelligence and flexibility in changing rules are just to overcome the 3 shortcomings of PNCT in FCN.

[**Key words**] variable carrying numbers (VCN); cypher science (CS); fixed carrying numbers (FCN); artificial intelligence(AI); AI-Fuzzy VCN (IFN)