基于矩阵运算的数字仪表－传感器通讯代码加密算法

□上海瑞仪动态称重研究工作室　王卫民

【摘　要】本文以矩阵运算为工具，对数字称重仪表和数字传感器之间的通讯代码进行实时动态加密、解密运算。采用帕斯卡矩阵、其逆矩阵为矩阵运算因子，实现通讯代码编码、解码的整数型，并给出了MATLAB 语言下的运算举例和一个具体的随机动态加密方法的描述。

【关键词】矩阵运算编码的算法；动态加密解密矩阵；帕斯卡矩阵；随机动态加密方法

引言

数字称重仪表和数字传感器之间的通讯代码是数字称重系统信息交换的桥梁。由于称重结算过程中存在着作弊现象，其作弊方法往往是通过截获通讯代码，修改通讯代码的手段来实现的。因此，对数字称重仪表和数字传感器之间的通讯代码提出了加密要求。然而，道高一尺，魔高一丈，加密和破译不断进行博弈。为了衡器称重的公正性，寻找一种有效灵活的加密、解密算法来提高数字称重系统防作弊能力是非常必要的。

1　算法原理

加密、解密原理

根据n 阶满秩矩阵A，一定存在其逆矩阵A^{-1}的原理，对于$n\times 1$ 阶的明码向量X，可以通过矩阵A 的变换变为$n\times 1$ 阶的暗码向量Y（n=1,2,3,…）。

即：

$$Y=AX \tag{2.1}$$

其中

$$A=\begin{pmatrix} a_{11} & a_{12}\ldots A_{1n} \\ a_{21} & a_{22}\ldots A_{2n} \\ \vdots & \vdots \quad \vdots \\ a_{n1} & a_{n2}\ldots a_{nn} \end{pmatrix} \quad X=\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \quad Y=\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} \tag{2.2}$$

同理，明码向量X 可以由暗码向量Y 通过矩阵A 的逆矩阵A^{-1}反向求出，即

$$X=A^{-1}Y \tag{2.3}$$

其中

$$A^{-1}=\frac{1}{|A|}A^{*} \tag{2.4}$$

|A| 为A 的行列式，A* 为A 的伴随矩阵，(2.1) 式和(2.3) 式构成了编码和解码对。

将仪表的通讯序列码X 分解为k 个长度为n 的向量序列$X_i=\{x_{i1}; x_{i2}; \cdots; x_{in}\}$(i=1,2,3,…，k)，用剩余部分通讯序列码和数字1，组成最后一个向量序列$X_{k+1}=\{x_{k+1,1}; x_{k+1,2}; \cdots; 1,1,\cdots; 1\}$，使其长度为n。

将X_i（i=1,2, …,k+1）代入(2.1) 式经过和矩阵A 的乘积运算，求出加密码向量序列Y_i，(i=1,2,3,…，k+1)，即完成了对通讯序列码中的向量序列X_i 加密运算过程。

由(2.4) 式可以看出，在由矩阵A 求其逆矩阵A^{-1}的运算过程中含有除法运算。因此，逆矩阵A^{-1}的元素可能会出现非整数元素，即元素含有小数部分。由于非整数元素的出现，在运用(2.3) 式所求解还原的通讯序列码中，也会出现含有小数部分的码元素，而被加密的通讯序列码都是整数。因此，必须寻找

一种变换矩阵A 和它的逆矩阵A^{-1} 元素都是整数元素的矩阵。

解决上述问题的方法就是使矩阵A 为帕斯卡(pascal) 矩阵，帕斯卡矩阵的元素均为整数，它的逆矩阵的元素也为整数。因此，可以避免在运用(2.3) 式所求解还原的通讯序列码中出现含有小数部分的码元素问题。

MATLAB7.0 中pascal(i,1)(i=1,2,3,⋯,7)、pascal(i)(i=1,2,3,⋯,5)、pascal(i,2)(i=1,2,3,⋯,6) 所产生的矩阵和其逆矩阵均为整数矩阵。

设代码序列X={ x_1；x_2；x_3；x_4；x_5；x_6 }，其中x_i(i=1,2,3,⋯,6) 的长度为2−7，选择pascal(i,1)(i=2,3,⋯,7) 为加密矩阵。那么，每个x_i(i=1,2,3,⋯,6) 对应的加密矩阵pascal(i,1)(i=2,3,⋯,7) 有6 种可供选择，由此所产生的代码序列X 的加密种类组合数为6^6=46656。若将 pascal(i,1) (i=1,2,3,⋯,7)、pascal(i)(i=1,2,3,⋯,5)、pascal(i,2)(i=1,2,3,⋯,6) 一起进行组合加密，由此所产生的代码序列X 的加密种类组合数将更大。

因此，用帕斯卡(pascal) 矩阵进行组合加密，足以满足数字称重系统的通讯加密要求。

2 举例

2.1 举例

设通讯序列码X={ 22，12，100，34，5，87，9，203，45，34, 56，82, 90, 35，75,45 }

用MATLAB 语言中的pascal(n) 函数，产生一个n 阶帕斯卡矩阵A，令n=3，有

$$A=\begin{bmatrix}1&1&1\\1&2&3\\1&3&6\end{bmatrix}, \tag{3.1}$$

其逆矩阵为：

$$A^{-1}=\begin{bmatrix}3&-3&1\\-3&5&-2\\1&-2&1\end{bmatrix} \tag{3.2}$$

用MATLAB 语言实现(2.1) 式和(2.3) 式的语句为：

```
Yi=A*Xi;      % 求(2.1) 式;
Xi=A^(-1)*Yi;  % 求(2.3) 式;
```

将X 分为6 组，X={ x_1；x_2；x_3；x_4；x_5；x_6 }, 其中x_1=[22，12，100]；x_2=[34，5，87]；x_3=[9，203，45]；x_4=[34, 56，82]；x_5=[90, 35，75]；x_6=[45, 1，1], 其中x_6 的两个“1”是为了凑齐数组长度n=3 而添加。

将x_1；x_2；x_3；x_4；x_5；x_6 分别代入(2.1) 式进行矩阵的乘积运算(其中A 为(3.1) 式), 可求得暗码：y_1；y_2；y_3；y_4；y_5；y_6。其中y_1=[134，346，658]；y_2=[126，305，571]；y_3=[257，550，888]；y_4=[172，392，694]；y_5=[200，385，645]；y_6=[47，50，54]。

再将y_1；y_2；y_3；y_4；y_5；y_6 分别代入(2.3) 式进行矩阵的乘积运算(其中A^{-1} 为(3.2) 式), 可求得明码：x_1；x_2；x_3；x_4；x_5；x_6。其中x_1=[22，12，100]；x_2=[34，5，87]；x_3=[9，203，45]；x_4=[34，56，82]；x_5=[90，35，75]；x_6=[45，1，1]。

2.2 动态加密的方法

动态加密的方法可分为本地随机动态加密和远程随机动态加密。本地随机动态加密是数字称重仪表和数字传感器之间的加密方法。远程随机动态加密是物联网、数字称重仪表、数字传感器之间的加密方法。

在数字称重仪表和数字传感器的实时通讯中，可将通讯序列码X 分成不同长度的向量序列X={ x_1；x_2；⋯; x_k }(i=1,2,3,⋯，k)，设x_i 长度为P_i（P_i 可以等于或不等于P_{i+1}），用与之对应的P_i 阶帕斯卡矩阵A 和其逆矩阵A^{-1} 对x_i 进行编码和解码。因此，可形成对x_i 编码和解码方式的组合：（1）对x_i 长度为P_i 的分配。（2）对x_i 在向量序列X 中位置的分配。（3）对P_i 阶帕斯卡矩阵的选择。由此产生“通讯数据编码方式”表和“通讯数据解码方式”表，并将这两个表格分别嵌入数字传感器和数字称重仪表的程序中，以供调用。

2.2.1 本地随机动态加密方法

图1 是一个由数字称重仪表和数字传感器所组成的通讯系统，其通讯模式为：数字称重仪表为主机，数字传感器为从机。数字称重仪表的通讯数据格式如图2 所示。当此格式中的“数字传感器地址”字段为零时，数字称重仪表以广播方式向各数字传感器发送握手信号。系统上电初期，数字称重仪表就以此方式和各数字传感器建立通讯联系。

数字称重仪表每发送一个如图2 所示的通讯命令，对应地址的数字传感器就回送一个如图3 所示的

数据序列。

为了实现数字称重仪表和数字传感器之间的随机动态加密通讯，可在数字称重仪表程序中实时调用随机函数rand(void)（rand 函数可产生–90 ~ 32767之间的随机整数）来产生“通讯数据编码方式”代号值，形成图2 中的“通讯数据编码方式码”字段，并将此“通讯数据编码方式码”代号值通过发送如图2 所示的通讯命令的方式发送给某号地址与该通讯命令中“数字传感器地址”字段相同的数字传感器。该号数字传感器程序以此代号值索引内置的“通讯数据编码方式”表，用此代号值对应的“通讯数据编码方式”对要回送的重量数据进行编码加密，形成图3 中的“数据暗码”字段。数字称重仪表程序收到该号数字传感器程序回送的如图3 所示的数据序列，用所发的代号值索引内置的“通讯数据解码方式”表，用此代号值对应的“通讯数据解码方式”对该号数字传感器回送的“数据暗码”字段予以解码，以获得该号数字传感器解码的重量数值。这样就完成数字称重仪表和一个数字传感器的数据通讯。如法炮制，数字称重仪表就完成和系统内每个数字传感器的数据通讯

由于数字称重仪表程序每次调用的随机函数rand(void) 所产生“通讯数据编码方式”代号值是一个随机数。因此，它每次对每个数字传感器要求的数据加密方式也是随机动态变化的，各不一样。显然，“通讯数据编码方式”表容量越大，系统加密的冗余度就越高。

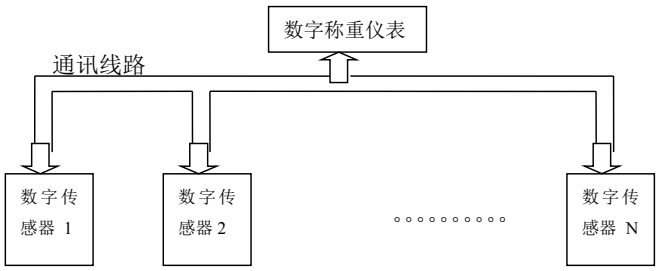

图1　数字称重仪表和数字传感器通讯系统

起始码	数字传感器地址	通讯数据编码方式码	校验码	结束码

图2　数字称重仪表通讯数据格式

起始码	数字传感器地址	数据暗码	校验码	结束码

图3　数字传感器通讯数据格式

2.2.2　远程随机动态加密方法

图4 是一个由远程物联网、数字称重仪表、数字传感器组成的通讯系统

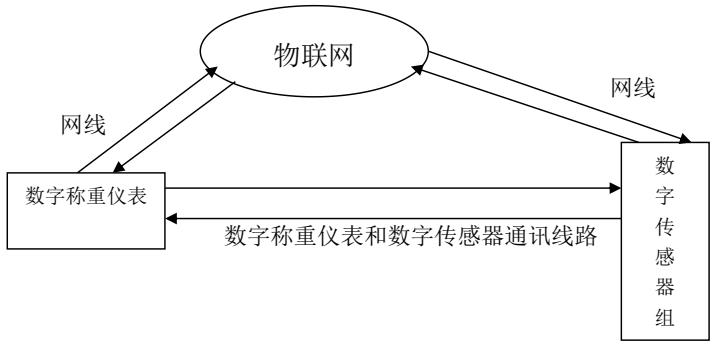

图4　远程物联网、数字称重仪表、数字传感器通讯系统

在物联网模式下，数字称重仪表、数字传感器通常用网络芯片和物联网联通。因此，数字称重仪表、每个数字传感器都有自己唯一的IP 地址。IP 地址的唯一性，使得在网线上侦听通讯内容几乎成为不可能。

有了上述条件的保证，物联网可以运用实时调用随机函数rand(void) 所产生的随机数值来产生“通讯数据解码方式”代号值和“通讯数据编码方式”代号值，并将其分别传送到数字称重仪表、每个数字传感器。数字称重仪表程序、每个数字传感器程序根据各自收到代号值按照3.2.1 中描述的方法进行编码、解码通讯。

由于数字称重仪表程序和每个数字传感器程序都知晓当下自己的代号值，所以在图 2 中的“通讯数据编码方式码”字段无需说明，冠以“0”即可。这时图 4 中“数字称重仪表和数字传感器通讯线路”上的通讯数据是用何种方式编码、解码的，几乎无人知晓，这就是远程随机动态加密方法的优点。

3　结论

运用矩阵运算实现通讯代码的加密、解密是一种基于数学运算的加密、解密方法。因此，它具有加密、解密方法变换灵活简便、种类繁多的特点。同一明码通过改变运算矩阵的选取就可获得不同加密暗码，不必为设计加密、解密方案而苦思冥想。尤其是随机动态加密方法的引入使得通讯线上的数据流瞬息万变，使破译者难以从通讯数据流中找到编码的规律，给破译者破译密码带来了巨大困难。

参考文献

[1] 同济大学数学教研室，高等数学（下册）. 人民教育出版社，1978.

[2] 刘浩，韩晶. MATL ABR2016a，完全自学一本通. 电子工业出版社，2016.

作者简介：王卫民（1959.1.7—），工程师，1989.9—1992.6 在合肥工业大学电力传动及其自动化专业学习，获该专业工学硕士。1997.9—至今一直从事动态称重信号处理研究及动态称重仪表的研发。