第9卷 第1期 华东交通大学学报 Vol.9 No.1
1992年 3月 Journal of East China Jiaotong University Mar. 1992

计算机数据安全存储系统的实现*

杨列亮 聂 涛

（电气工程系） （北方交通大学）

摘 要

本文介绍了一种实用的微机加密系统，并且提出了一种便利于单个用户和多个用户管理的密钥产生技术。该系统具有操作简便、安全可靠、加密速度快等特点。

关键词：加密；解密；密钥

0 引 言

随着电子计算机应用范围的扩展与普及，利用电子计算机犯罪的案例也越来越多。如果不重视对系统安全性的建设，一个缺乏可靠安全保证的系统会使拥有者蒙受巨大的损失。特别是对那些要害部门，例如：银行、股票证券公司、政府部门、公安机关、军工仓库等等。因此计算机数据安全保密问题越来越成为人们十分关心的问题。

在现代这个信息极为广泛的时代，要求计算机处理的数据也越来越多。这就要求计算机具有很高的处理数据速度。然而当要对计算机里的数据进行保密时，又要占用一定的系统资源。这就使得在肯定一个保密系统安全可靠的同时，它的加／解密速度成为判别一个密码系统好坏的标准。如果一个保密系统处理数据的速度太慢，占用计算机系统的资源太多，那么它也是不实用的。本文提出一种在微机环境下，保护计算机数据以防止非授权查询与篡改的系统。它的硬件设计上采用多存储体结构，做到加密操作与计算机的CPU之间并行处理。实验证明该系统具有很高的数据处理能力，完全可以满足加／解密速率的要求。另外，本文提出了一种计算机内文件加密钥的生产方法，它非常便利于多层次管理。证明是有效和实用的。

1 加密卡的硬件设计

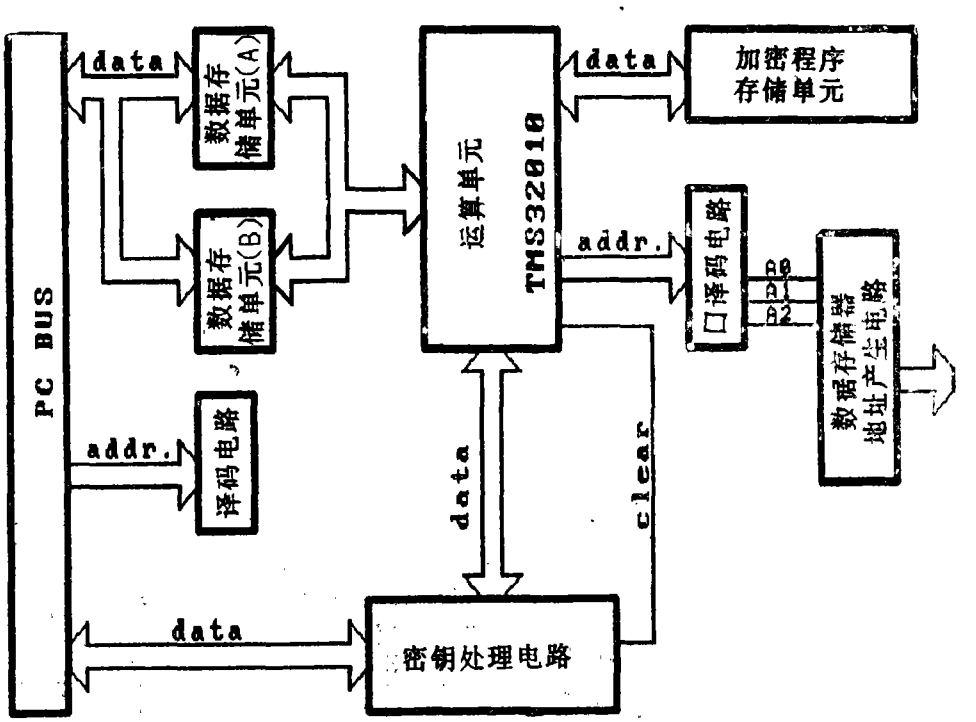
1.1 加密卡的基本组成

加密卡主要由实现数据加密运算的高速微处理器TMS32010、数据存储单元（分为A、

本文于1991年6月20日收到

*注：国家自然科学基金资助课题

中国知网 https://www.cnki.net



图一：加密硬卡基本结构图

B两组）、加密程序存储单元、密钥处理电路、PC口译码电路、TMS32010口译码电路等六个主要部分组成。其中加密程序存储单元用于装载TMS32010需要运行的加密程序。加密程序固化在高速PROM里，它和TMS32010一道共同构成加密算法的基本实现单元。PC口译码电路用于产生一系列的控制信号。诸如控制数据存储器切换、控制TMS32010软起动、产生存储器状态检测信号等。TMS32010的口译码信号分为两部分：其中一部分用于产生存储器状态检测信号和密钥处理电路的清零信号；另一部分用于产生数据存储器的读／写地址。加密卡电路结构如图一所示。数据存储器用于存储待加密的数据和／或加密好了的数据。密钥处理电路用于产生加／解密密钥。两者的实现方法在后面讨论。

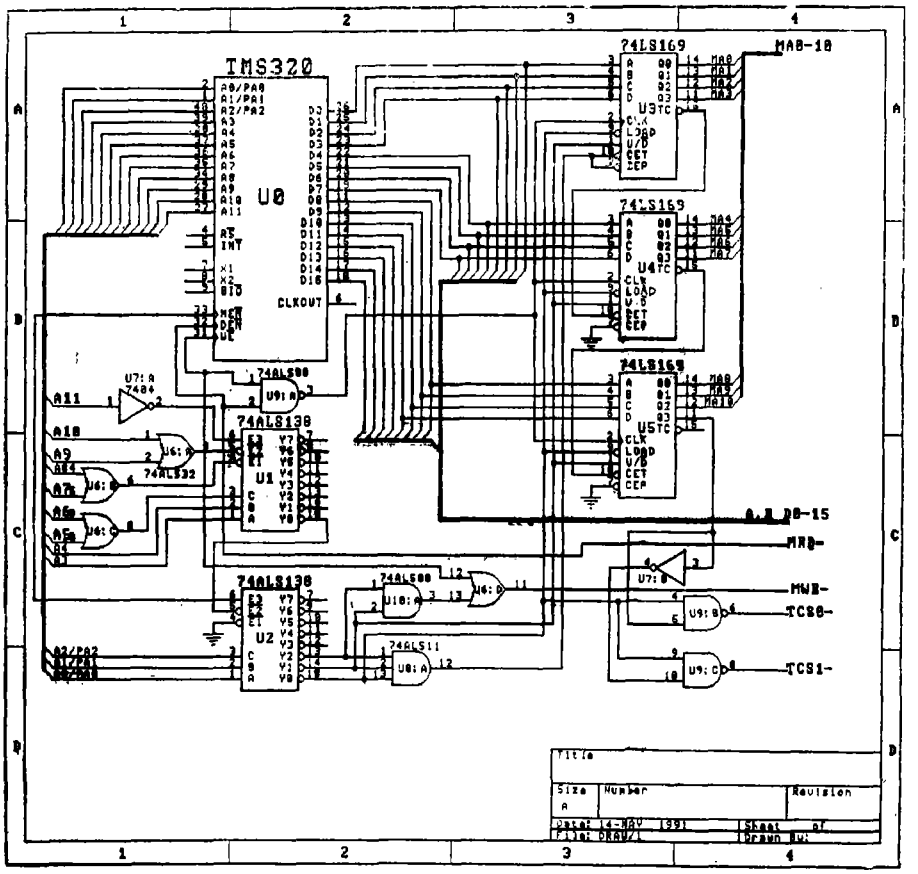
1.2 数据存储器地址产生电路简介

为了更大的数据存储器的需要，可以采用间接扩展的存储器接口。在这种设计中，使用了两个时钟周期，前一个时钟周期用于装入地址信息；后一个时钟周期用于控制这个地址中数据的输入输出。

连接数据存储器的12位地址由3个4bit的加／减计数器74LS169产生。图二是数据存储器地址产生电路的原理图。对电路图分析可以知道，通过端口0输出一个地址数据，就可以将该地址装载到计数器中，锁存输出到数据存储器上。在下一周期里，就可以通过端口1或端口2向该地址中写入或者读出数据。在这一周期结束时，计数器的输出相应地增1或减1，产生下一个存储器读写地址。由此可知，当数据存储器中的数据是连续存放时，就不需在每次读写数据之前装载地址，而是直接从端口1或端口2读写数据。从而可以提高数据的存取速

中国知网　https://www.cnki.net

度。在加密系统中，要加密的数据和加密好了的数据都是连续存放在数据存储器中的。因此这种设计是比较合理的。



图二 数据存储器地址产生电路

1.3 密钥处理电路

密钥处理电路的逻辑功能是对输入的几个密钥进行处理，使之产生一个用于加密数据的56b密钥。基本结构如图三所示。其中$x_{11}\ x_{12}\ \cdots\ x_{1n}$是第一个用户输入的密钥；$x_{21}\ x_{22}\ \cdots\ x_{2n}$是第二个用户输入的密钥；$x_{31}\ x_{32}\ \cdots\ x_{2n}$是第三个用户输入的密钥。输出的密钥是：

$$Z_1 = f1_{k1}(x_{11}, x_{12}, \cdots, x_{1n}; x_{21}, x_{22}, \cdots, x_{2n}; x_{31}, x_{32}, \cdots, x_{3n})$$

$$Z_2 = f2_{k2}(x_{11}, x_{12}, \cdots, x_{1n}; x_{21}, x_{22}, \cdots, x_{2n}; x_{31}, x_{32}, \cdots, x_{3n})$$

$$\vdots$$

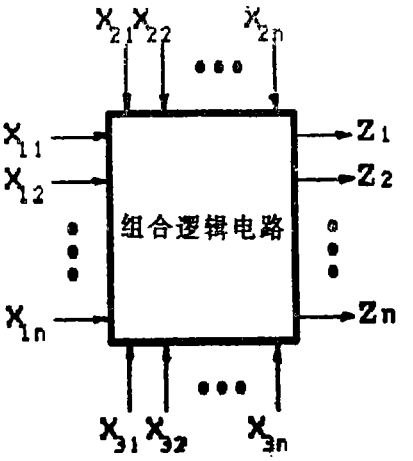
$$Z_m = fn_{kr}(x_{11}, x_{12}, \cdots, x_{1n}; x_{21}, x_{22}, \cdots, x_{2n}; x_{31}, x_{32}, \cdots, x_{3n})$$

从上面的表示式可以知道，Z_i与f函数；K_i；$x_{11}, x_{12}, \cdots, x_{1n}; x_{21}, x_{22}, \cdots, x_{2n}; x_{31}, x_{32}, \cdots, x_{3n}$有关。对于每一位输出，$f_i$函数是不同的，$K_i$也是不同的，而$x_{11}, x_{12},$

中国知网 https://www.cnki.net

…，X_{1n}；X_{21}，X_{22}，…，X_{2n}；X_{31}，X_{32}，…，X_{3n}是相同的。

这种密钥产生的设计是极为灵活的，人们可以根据其应用场所的不同和具体要求的不同对其设计进行改进。当是单用户应用该系统时，用户可以根据其对保密强度的要求，将输入三组中的一组或二组置成全0或全1，以便于用户的记忆。在多用户管理同一个数据系统时，

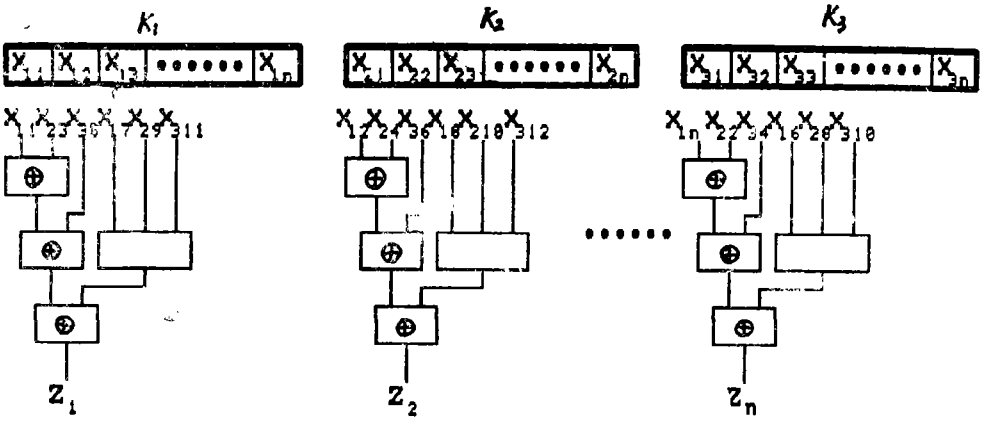


图三：密钥处理电路结构框图

在数据系统的多级保密管理时，而且对系统的安全强度要求特别苛刻时，用户可以根据其要求将一个或更多个相同的电路级联起来，以达到其要求。

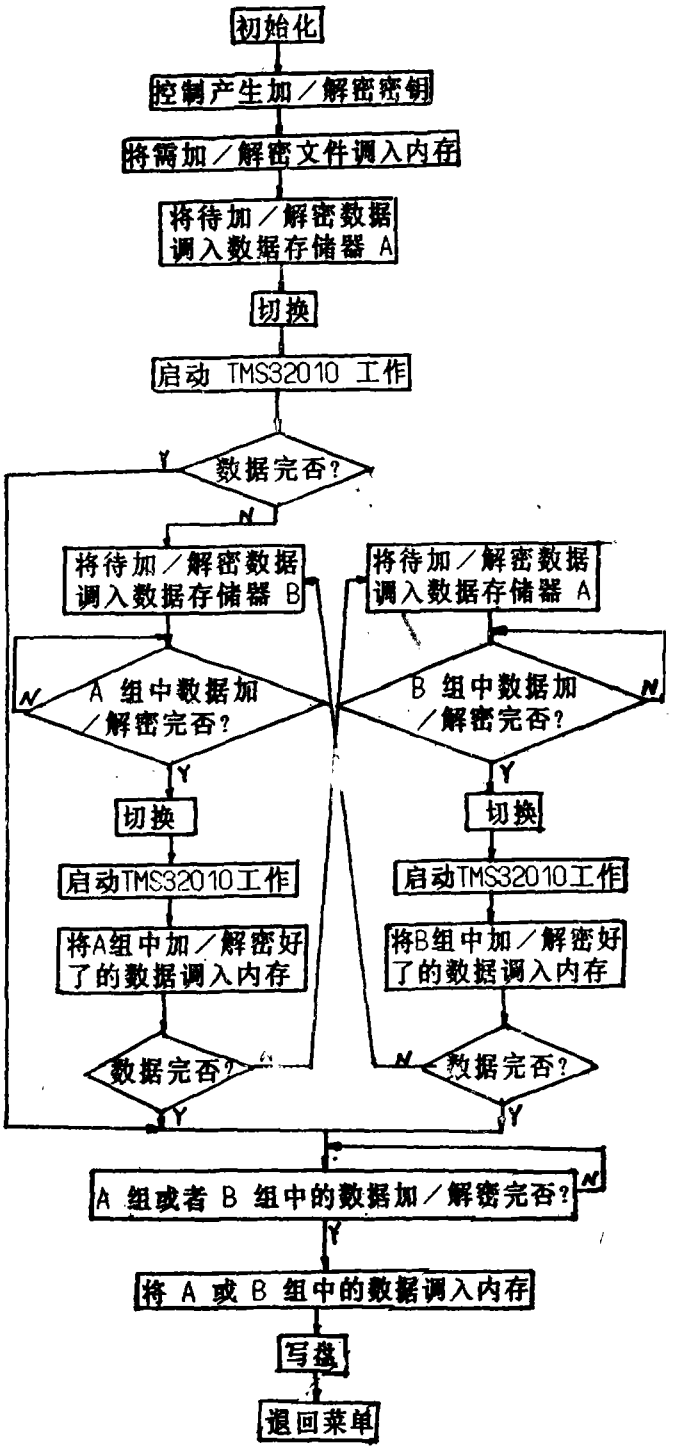
下面是一个实现这种密钥处理的组合逻辑电路。该电路由8＊24个移位寄存器和一系列二输入异或门，三输入与门组成。24个移位寄存器被分成3组，每组是8个共64bit移位寄存器，它们各自是循环移位的。用K_1，K_2，K_3分别控制它们的移位位数。由逻辑电路理论可知，当它们的输入相同时，控制K_1，K_2，K_3，就可以产生一个伪随机系列。这样，用户可以利用同一个密钥，采用不同的K值，产生很多个数据加密密钥。因而有助于用户的记忆和管理。

如图四所示，输出的64 bit数$\vec{Z}=\{Z_1, Z_2, \cdots\cdots, Z_n\}$就是文件加密存储所需的文件加密钥。

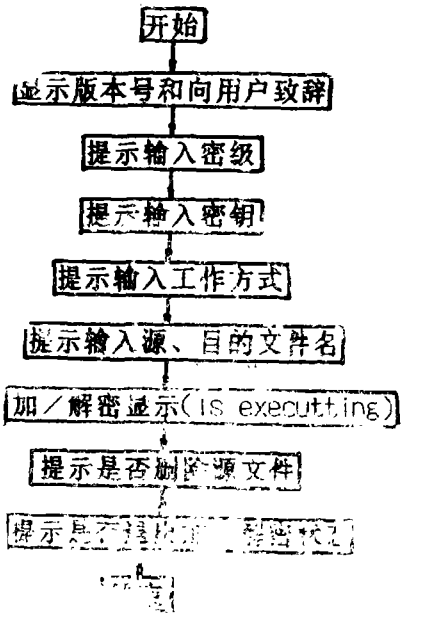


图四　密钥产生电路

中国知网　https://www.cnki.net



图五： 加密控制软件流程图



图六 系统管理软件流程图

中国知网 https://www.cnki.net

电路中设计有自动清零电路，当TMS32010读入密钥后，就从译码电路端口3产生一个译码信号CLEAR，CLEAR信号将密钥处理电路的输出全部置零。

2 系统软件设计

在这个加密系统中，实现加密运算的加密程序由TMS32010汇编语言完成，加密程序固化在高速PROM程序存储器中。其余功能均由软件来完成。这些软件包括加密控制软件和系统管理软件，前者由IBM PC XT/AT汇编语言编程，它主要是面向TMS32010的，控制着TMS32010进行加／解密运算及其密钥处理；并且控制着数据的输入输出。它的程序流程图如图五所示。后者是面向操作员的，由C语言编程。全部操作在菜单提示下进行，用户可以很方便地掌握其操作。它的功能是负责指挥微机进行操作，便于操作人员对系统进行管理。图六是它的程序流程图。

3 结束语

DES自公布以来，尽管有很多专家和学者怀疑其安全强度以及怀疑设计中存在有陷门，但至今尚未有人公开证明存在一种有效的破译方法。因而，只要将DES进行改进（从密钥上或者从算法上），DES还是具有广泛的应用前景的。

本文提出了一种在微机环境下实现数据加密的设计方案，系统中大部分软硬件均已完成，证明该系统具有很高的数据处理速率（加密速度比纯粹用软件实现在286上运行快50多倍）和很强的安全性（具有DES同样的安全级数），具有较好的实用价值。

参 考 文 献

〔1〕朱传乃，郑筑鸣，杨福平·微型计算机系统原理分析与维修·北京：科学出版社，1989

〔2〕TMS320 16/32 bit数字信号处理单片机·北京：中科院声学所，1986

〔3〕E.Okamot. oDigital Signal Processing Applications With the TMS320 Family, Theory Algorithms and Implementation, Advance in Cryptology—Crypto'87, pp, 284—290

〔4〕［美］Ray Duncan著，贺志强，李昌译·DOS磁盘操作系统高级程序员指南·北京：中科院希望电脑技术公司，1987

〔5〕卡尔H. 梅尔，司蒂芬. 马脱耶斯·密码学：计算机数据安全的一个新领域·北京：国防工业出版社，1988

〔6〕C语言程序设计（上、中、下）·北京：中科院希望电脑技术公司，1988

中国知网 https://www.cnki.net

The Realization of a Security System for Computer Data Memory

Yang Lieliang Nie Tao

Abstract

A practical microcomputer data encryption system is introduced, and a scheme of KEY generation is discussed, which can be easily managed for single user and mutitudinal users. The system is used simply and has rapid encryption speed and high strength.

key Words: Encryption; Decryption; keys

中国知网 https://www.cnki.net