研究报告

增值税防伪税控系统及其安全性设计

魏庆福
（航天金穗高技术有限公司，北京 100080）

[摘要] 增值税防伪税控系统是国家金税工程的主要组成部分之一，是为控管增值税、扼制利用发票偷税、骗税，防止税收流失而研制的。该系统采用数字密码技术，解决票据的防伪识伪，由微控制器、DSP 和 Flash 存贮器构成的“黑盒子”和智能 IC 卡等技术集成，从税源的源头和票源的源头控制税收的征管。该技术发明的推广使用已成为辅助我国税收征管的强有力手段。它为解决国民经济中有关增值税征管中的重大难题作出了贡献。

系统为特殊的商用密码设备，运行环境极为恶劣，它既要防止国内外利益集团的集团攻击，又要抵御一些不法之徒，包括与税务部门内部人员勾结的个人攻击。为此，采用了一整套安全性设计技术，按照系统的安全模型，从核心硬件、密码算法、密钥管理、设备连接通道、运行环境、信息记录与审计、业务功能以及管理诸方面层层设防，综合治理。

[关键词] 增值税；防伪；密码；安全性

1 前言

增值税防伪税控系统是国家金税工程的主要部分之一。它是为控、管增值税和防止国家税收流失而专门研制的。

1994 年，我国开始实施税制改革，采用以增值税为主体的流转税体制，增值税已占税收总量的大部分。增值税的征收采用多联发票，采用层层抵扣的办法征收产品增值部分的税收。因此，发票在层层抵扣过程中成为链条和依据，由于其成为有价证券，且价值很高，一些不法之徒，包括有些认识模糊的企业领导人，利用专用发票偷税、骗税。作案的主要手段是印制并开具假发票，或真票假开、虚开、代开以及大头小尾的阴阳票，致使国家税收大量流失。现象之严重，数额之巨大，影响面之广，令人触目惊心。

1993 年年中开始，财政部、电子部和航天工业总公司三家联合攻关。1994 年初，航天系统提出了概念样机。1994 年 10 月起经珠海、镇江、鞍山三市两期试点和修改，百万元版系统自 1996 年 1 月 1 日开始在全国各地推广应用并获得成功。在此基础上，经安全性审查和改进，于 1997 年底通过了国家级技术鉴定，并开始在全国范围推广应用。至 1999 年底，全国凡开具 10 万元增值税专用发票的企业已全部装备了这套系统，经 10 多万户企业（控制税源 50 %以上）成功的应用，已产生明显的成效。自 1994 年实行新税制以来，全国税收每年递增 1 000 亿元，然而，2000 年上半年即增收近1 000亿元，其中防伪税控系统发挥了重大作用是增收的原因之一。2000 年 2 月，国务院下达文件，决定扩大该系统的推广应用，要求在 2002 年年底前将其推广应用到全国所有一般纳税人企业（约 126 万户）。

增值税防伪税控系统，经国家级鉴定，给予很高评价：“这是一项具有中国特色的创造发明，总体技术居国内领先水平，该项目的研制成功和推广应用，将为我国增值税征管手段带来巨大变化，将产生重大的社会、经济效益。”

[收稿日期] 1999－07－12； 修回日期 2000－09－08

[作者简介] 魏庆福（1941－），男，江苏栗阳市人，航天金穗高技术有限公司研究员

2　增值税发票防伪识伪和税控原理

防伪税控系统采用了两项关键技术措施：其一，采用数字签名认证技术解决发票的防伪识伪；其二，用电子信息存贮技术，即“黑盒子”控制税源和票源，解决有抵扣税而无纳税的问题。

2.1　发票防伪识伪原理

采用数字密码技术解决增值税专用发票防伪识伪问题的原理和方法：取消人工手写发票，改用计算机打印发票。在用计算机打印发票的同时，将发票上之诸要素，即时间、发票特征码、购销双方的全国统一税号、货款金额和税额以及税率等，经加密处理形成一串密文也打印在发票上，如图 1 所示：

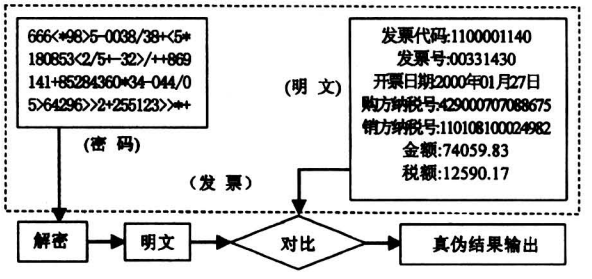

图 1　带防伪密码的增值税专用发票

Fig. 1　The special invoices of value added tax with cipher

判别打印有密文的发票之真伪在税务部门完成。其原理是：采用扫描装置如同点钞机一样，将发票的图像自动录入计算机，见图 2。在计算机中，采用图像识别技术识别出其密文和诸项明文，将密文经解密恢复出参与加密的发票要素，与发票上打印的明文信息一一比对，若相一致，则为真发票；否则为假发票。

图 2　高速扫描识别认证系统的组成

ig.2　The configuration of the high-speed scanning identification and authenticating subsystem

2.2　关于控制税源和票源的原理

利用多联单形式的增值税专用发票作案（偷、漏、骗税），其主要手段是印制并开具假发票或真票假开、虚开、代开及阴阳票等，形成的局面是有抵扣联而无存根联，即有抵扣税而无纳税。因此，应从税源的源头和发票的源头进行控制。其原理是采用微控制器和大容量半导体存贮器构成“黑盒子”控制发票的打印和税源。

具体做法是：将每次打印发票的交易金额、税额等，以及发票使用情况登录在“黑盒子”中。“黑盒子”中的数据只许读取，不许更改。每月用 IC 卡抄取“黑盒子”中的数据作为报税的依据。

2.3　防伪税控专用部件的构成

防伪税控专用部件由金税卡、与之直接联接的 IC 卡读卡器以及带 CPU 的智能 IC 卡构成，并有一整套相应的专用软件。金税卡由专门研制的超大规模专用芯片 KT－1 为核心，加上总线接口电路以及实时时钟等电路构成。KT－1 芯片包含带高速数据处理器（DSP）的超级微处理器、大容量半导体存贮器以及辅助逻辑电路，采用专门工艺集成。

由于密码算法以及管理软件封装于 1 片智能式 KT－1 芯片之中，对于外部来说，只是明文进、密文出或密文进、明文出，在总线上无法获得加、解密过程的信息；并用 IC 卡抄写“黑盒子”中的数据，因此，可以排除人为的消极因素。

2.4　增值税防伪税控系统的构成与功能

增值税防伪税控系统由如下子系统组成（见图 3）：企业开票子系统，企业发行子系统，报税子系统，发票发售子系统，发票认证子系统，税务发行子系统。各子系统由 PC 机、票据打印机和由金税卡等防伪税控专用部件构成，运行相应的配套软件。各子系统必须按总局—省局—地市局—县区级四级管理体系，经逐级发行后才能运行。

税务发行子系统的功能是上级对下级税务部门的各税务发行子系统进行发行和授权。企业发行子系统的功能是对各企业开票子系统进行初始发行和授权。发票发售子系统是税务部门用来对企业发售专用发票。

税务部门用的报税子系统功能是接受企业的纳税申报，包括 IC 卡数据读取以及与软盘数据的比较等，并形成与计算机稽核系统的接口数据文件。

发票认证子系统由扫描仪和具有数字图像的扫描输入、识别和解密、比较、管理功能的软件构

成，其主要功能是对企业申报的发票之真伪进行认证。发票图像的扫描输入和识别也是本系统研制工作的难点之一。

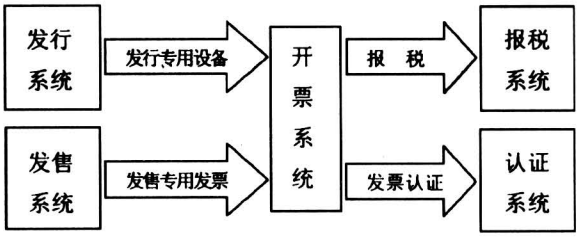

图3 增值税防伪税控系统的系统组成

Fig.3 The configuration of the system of value added tax anti-fake and control

将企业管理和税务征管的电算化和现代化作为主要系统功能之一，使之与防伪税控功能相结合，这是本系统之所以得到企业和税务欢迎的重要因素。基于防伪税控系统的基本功能，已有并将推出一系列开票、自动报税、进销存、财务和集成管理等功能软件，为企业管理和税务征管的现代化提供强有力的支持。

金税工程坚持“数据共享、功能互补、统一管理、结合并举”的方针，并按照增值税计算机稽核系统与防伪税控系统相结合方式进行“捆绑”式推行。防伪税控系统是计算机稽核系统的前端数据采集手段，它提供的企业纳税信息和发票信息能保证其完整性、准确性，为稽核系统提供了良好的基础。

3 系统的安全性设计

数字密码技术是解决票据防伪的有效手段，也是本系统的核心技术。由其工作原理可知，本密码系统本质上是一种可逆向解密的认证签名体制。由于以下原因：**a.** 用户数量特别巨大（百万级）；**b.** 发票上明文与密文成对出现；**c.** 由于发票本身可用空间有限，密文长度受到限制；**d.** 基于PC机的环境下运行，由于PC机的开放性，特别易于被攻击；**e.** 对于机要通信和军用通信来说，其密码设备的使用者又是其保护者。而对于本系统这种商用密码设备，各用户既是用户，又是潜在的攻击对手。因此，研制了一种复合式密码系统HTJS-2。

由于这套系统的运行环境十分恶劣，它既要防止潜在的国内外利益集团的集团攻击，如破译、仿制等，还要防止社会上一些不法之徒，包括税务系统内部作为管理者的个人与企业勾结作案的个人攻击，为此，要对系统的安全性进行严密设计。这是一套与机要通信、军事通信密码系统不同的设计，从核心硬件、密码算法、密钥管理、设备连接信道、运行环境、信息记录与审计方法、业务功能以及管理诸方面采用了有效的安全措施，层层设防，综合治理，以保证系统的安全性。

除了前述的密码算法，KT-1芯片以及智能式IC卡外，按照系统的安全模型，采取了如下几项安全性措施：

1）*最小权力原则* 即将研制、用户、管理三方分隔开，将开票、认证、发行三种功能分离，相互隔离；将税务部门用的几个子系统也予以分割。

2）*密码算法的分散化、个性化、动态化* 将密码系统之内容分散在不同金税卡和IC卡中，对复合式密码算法进行地区分割和个性化处理，使之具有一机一钥、一票一密的特点，并可定期或不定期更换密钥。

3）*IC卡操作的双向认证* 对于作为安全核心之一的IC卡，该系统选用带CPU的智能式IC卡，其操作必须经随机信息的双向认证才能执行。所记录的重要信息均为密文形式。

4）*系统的发行采用密文交互* PC BUS和IC卡信道操作均为包含随机数的密文交互，可以进行严格的监控。

5）*加强信息记录及审计* 加强管理，特别是加强审计功能，是用好防伪税控系统的关键之一。重要操作必须留下痕迹。包括税务部门所用的各子系统的重要操作，在系统中有相应的记录，以提供审计之用。特别是认证子系统还设置了“黑名单”功能，可防止利用丢失或盗用的设备开具发票。

6）*加装PC机安全保护装置* 由于PC机的总线和操作系统的开放性，对于利用这种开放性对应用软件的篡改、跟踪和分析等攻击。本系统参照安全计算机有关技术标准，利用KT-1芯片、IC卡和扩展的监控系统，设计成微机安全保护装置，以加强通用PC机应用系统的安全保护能力。

4 结语

增值税防伪税控系统的保密性和安全性已经国家主管部门审查认定。

这套系统的研制和推广应用受到了国务院、财政部、国税总局、航天工业总公司和各级税务机

关、企业以及各地技术服务单位的关心和支持，这也是各方面技术专家的智慧和辛劳的结晶。该系统获得了 1998 年国家科技进步二等奖。该技术发明已获国家发明专利。众多高科技人员为此作出了重大贡献。主要研制和作出突出贡献的人员有刘纪原、夏国洪、王雨生、张庆汉、张相海、陈志恒、温立新、韦红文、刘畅、张飚、崔志民、姚德谊、陈江宁、赵健青、孟小虎等。沈昌祥院士、蔡吉人院士和国税总局信息中心蔡金荣主任等提出了许多宝贵的改进意见。

The Value Added Tax Anti-Fake and Control System and Its Security Design

Wei Qingfu

(*Aerospace Jinsui High Technology Ltd.*, *Beijing* 100080, *China*)

[**Abstract**] The Value Added Tax (AVT) anti-fake and control system, which is one of the main parts of the National Golden Taxes Project, is developed for VAT supervising and preventing the tricks in VAT invoice that lead to the tax evasion. A special data encryption mechanism is adopted in the system to implement the detection and countercheck of the fake invoices. The " black box", which is the combination of microprocessor, DSP, smart IC card and flash memory, can realize taxation supervising from the sources of the tax and invoice. The invention and popularization of the system greatly benefit the taxation and government finance. The system has been contributive to the national tax supervision.

As an especial commercial encryption application, the system must work properly under all kinds of complex condition. To obtain high security, the system adopts a systematic security design technique according to the secure model for the system in respect of the kernel hardware, encryption algorithm, key management, device connection channels protection, running conditions, information recording and auditing, system function and system management. The system now is proved safe enough to defend the attacks from the criminal organizations as well as any persons from the tax departments.

[**Key words**] value-added tax; anti-fake; encryption; security

《中国工程科学》2000 年第 12 期要目预告