文章编号：1005-8451（2013）08-0043-04

商用密码在铁路的应用

魏晓燕，纪　方
（铁道部　信息技术中心，北京　100844）

摘　要：铁路信息化的发展使信息安全问题日益重要，商用密码技术是实现信息安全的关键技术，通过密码技术可以实现信息的真实性、机密性、完整性和不可抵赖性。本文介绍了商用密码技术和商用密码产品在铁路电子认证系统和其他信息系统中的应用。

关键词：商用密码；商用密码技术；电子认证
中图分类号：U285：TP39　**文献标识码：**A

Application of commercial passwords in railway

WEI Xiaoyan, JI Fang
(Information Technology Center, Ministry of Railways, Beijing　100844, China)

Abstract: The development of Railway Information based made the problem of information security more and more important, the commercial password techniques was the key technology of information security, the commercial password techniques could implement the information authenticity, confidentiality, integrity and non repudiation. This paper introduced the application of the commercial password techniques and the commercial password products in Railway Electronic Authentication System and other information systems.

Key words: commercial password; commercial password techniques; electronic authentication

随着铁路信息化的发展，网络安全问题日益突出，用户重要信息的机密性和用户安全认证的需求也日益迫切，商用密码是实现信息安全的重要手段，可以实现信息的真实性、机密性、完整性和不可抵赖性等功能。随着铁路电子认证系统、铁路大客户系统、铁路行包管理系统等便民服务措施的实施，商用密码在铁路信息系统中得到了广泛的应用。

1　商用密码技术

商用密码是指对不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的密码技术和密码产品，包括密码算法编程技术和密码算法芯片、加密卡等的实现技术。

1.1　数据加密原理

1.1.1　数据加密

在计算机上实现的数据加密，其加密或解密变换是由密钥控制实现的。密钥（Keyword）是用户按照一种密码体制随机选取，它通常是一随机字符串，是控制明文和密文变换的唯一参数。

1.1.2　数字签名

密码技术除了提供信息的加密解密外，还提供对信息来源的鉴别、保证信息的完整和不可否认等功能，而这3种功能都是通过数字签名实现。

数字签名的原理是将要传送的明文通过一种函数运算（Hash）转换成报文摘要（不同的明文对应不同的报文摘要），报文摘要加密后与明文一起传送给接受方，接受方将接受的明文产生新的报文摘要与发送方的发来报文摘要解密比较，比较结果一致表示明文未被改动，如果不一致表示明文已被篡改。

1.1.3　密码杂凑算法

密码杂凑算法（也称消息摘要或哈希算法），就是把任意长的输入消息串变化成固定长的输出串的一种函数。这个输出串称为该消息的杂凑值。

一个安全的杂凑函数应该至少满足以下几个条件：（1）输入长度任意；（2）输出长度固定；（3）对每一个给定的输入，很容易计算输出即杂凑值；（4）给定杂凑函数的描述，找到两个不同的输入消息杂凑到同一个值是计算上不可行的，或给定杂凑函数的描述和一个随机选择的消息，找到另

收稿日期：2012-12-21
作者简介：魏晓燕，工程师；纪　方，工程师。

一个与该消息不同的消息使得它们杂凑到同一个值是计算上不可行的。

1.2 加密体制及比较

根据密钥类型不同将现代密码技术分为两类：（1）对称加密系统；（2）公开密钥（非对称）加密系统。

1.2.1 对称加密系统

对称加密系统是加密和解密均采用同一把秘密钥匙，而且通信双方都必须获得这把钥匙，并保持钥匙的秘密。对称加密有分组密码和序列密码。

对称密码系统的安全性依赖于以下两个因素。（1）加密算法必须是足够强的，仅仅基于密文本身去解密信息在实践上是不可能的；（2）加密方法的安全性依赖于密钥的秘密性，而不是算法的秘密性，因此，没有必要确保算法的秘密性，而需要保证密钥的秘密性。对称加密系统的算法实现速度很快。对称加密系统最大的问题是密钥的分发和管理非常复杂、代价高昂。比如对于具有n个用户的网络，需要$n(n-1)/2$个密钥，在用户群不是很大的情况下，对称加密系统是有效的。但是对于大型网络，当用户群很大，分布很广时，密钥的分配和保存就成了大问题。对称加密算法另一个缺点是不能实现数字签名。

1.2.2 公开密钥（非对称）加密系统

公开密钥加密系统采用的加密钥匙（公钥）和解密钥匙（私钥）是不同的。由于加密钥匙是公开的，密钥的分配和管理就很简单，比如对于具有n个用户的网络，仅需要2n个密钥。公开密钥加密系统还能够很容易地实现数字签名。因此，最适合于电子商务应用需要。公开密钥加密系统安全性更高，但它实现速度却远赶不上对称密钥加密系统。在实际应用中可利用二者的各自优点，采用对称加密系统加密文件，采用公开密钥加密系统加密“加密文件”的密钥（会话密钥），这就是混合加密系统，它较好地解决了运算速度问题和密钥分配管理问题。因此，公钥密码体制通常被用来加密关键性的、核心的机密数据，而对称密码体制通常被用来加密大量的数据。

2 商用密码产品

2.1 产品分类

2.1.1 按功能分类

密码算法类产品：构成密码应用基础的能提供密码运算功能的产品，例如：密码算法实现、密码算法芯片等。

数据加解密类产：能提供数据加解密功能的产品，例如：加密机、机密卡、智能密码钥匙等。

认证鉴别类产：提供身份认证、密码鉴别功能的产品，例如：动态口令系统，身份认证系统等。

证书管理类产：能提供证书的产生、分发管理功能的产品，例如：数字证书认证系统等。

密钥管理类产：能提供密钥的产生、分发、更新、归档和恢复等功能的产品，例如：密钥管理系统等。

密码防伪类产：能提供密码防伪功能的产品，例如：电子印章系统、支付密码器、数字水印等。

综合类产品：能提供含上述产品功能的两种或两种以上的产品，例如：电子商务安全平台等。

2.1.2 按形态分类

商用密码产品按形态分为6类，分别为：软件、芯片、模块、板卡、整机、系统。

铁路信息系统中大量使用商用密码产品主要为数据加解密类产品和证书管理类产品。主要形态为软件、板卡和系统。

2.2 管理要求

国家对商用密码产品实行定点研制，品种和型号审批的管理原则。

2.2.1 定点研制

商用密码产品作为一种特殊产品，其研制生产单位必须首先取得商用密码产品生产定点资质。首先申请单位要提交《商用密码产品生产定点单位申请表》，经国家密码管理局审查并实地考察合格后发给《商用密码产品生产定点单位证书》。

2.2.2 品种和型号审批

国家对密码算法按应用领域进行配用。生产定点单位向国家密码管理局提交拟研制产品的算法需求表，介绍研制产品的主要功能，应用领域、需求算法的类别等；国家密码管理局根据应用领域进行算法配用，并书面回复研制单位；研制单位采用配用算法进行产品研制，研制完成后申请商用密码产品品种和型号，审批通过后即可进入市场进行销售。

3　商用密码在铁路信息系统中应用

3.1　商用密码在铁路电子认证系统中的应用

3.1.1　系统工作依据

2005 年，《中华人民共和国电子签名法》正式实施，从法律层面解决了数据电文的合法性问题。由密码技术介绍可知，密码杂凑算法和非对称密码算法的性质很好地解决了电子签名的需求；当一份文件需要签署时，首先用密码杂凑算法压缩为固定长度文件，用私钥进行签名，形成签名文件。由于私钥是随机产生的，且用户唯一拥有，伪造用户私钥在计算上是不可行的，这就保障了电子签名的专有性；同时，对文件的任何改动，都会导致杂凑值的不同，验证就不能获得通过，这就保障了对签名、数据电文的任何改动能够被发现。

3.1.2　系统功能

铁路电子认证系统是数字证书的签发系统，它是公钥基础设施（PKI，Public Key Infrastructure)的核心。系统部署一个电子认证 CA 系统和多个 RA（Registration Authority）系统。铁路电子认证系统负责签发数字证书、管理已发放数字证书，包括数字证书的发放、更新、冻结和注销等功能。系统发放的数字证书即可用于电子签名。系统的网络结构图如图 1 所示。

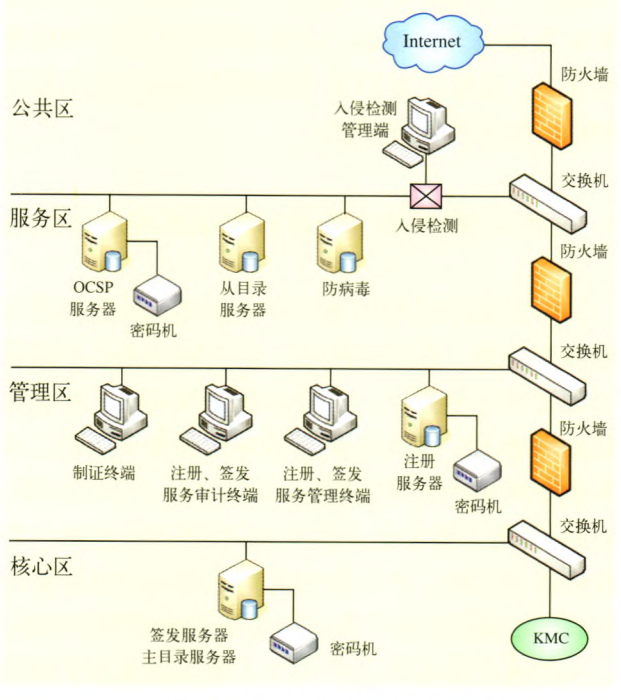

图1　铁路电子认证服务系统CA网络结构图

系统根据实际需要，下设多个 RA 机构，用于完成大批量制证需求。CA 系统和多个 RA 机构的网络连接图如图 2 所示。

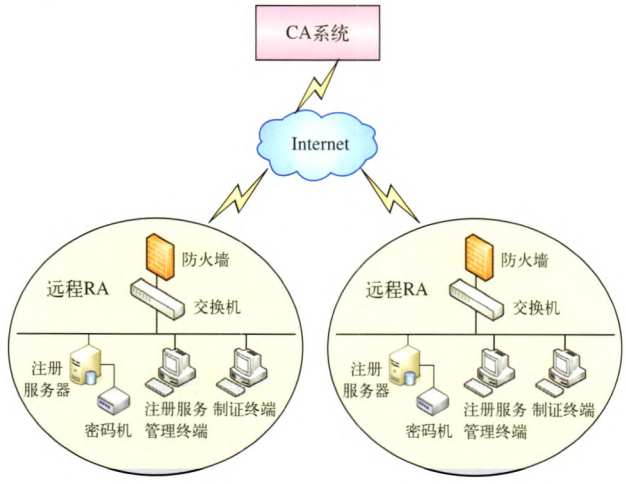

图2　铁路电子认证服务系统CA网络结构图

3.1.3　系统中使用的商用密码产品

系统中使用的商用密码产品有电子证书认证系统（软件）、密码机和智能密码钥匙，智能密码钥匙为数字证书载体。系统中使用的商用密码产品都是国家密码管理局公布的“商用密码通用产品名单”中的产品。

3.1.4　系统的合法性

铁路电子认证系统已经获得国家密码管理局批准的电子认证服务使用密码许可单位资格。

3.2　商用密码在铁路其它系统中的应用

商用密码在铁路大客户系统、铁路行包管理系统和铁路口岸信息平台系统中也得到广泛应用。

3.2.1　铁路大客户系统

铁路大客户系统包括铁路货运大客户系统和集中受理优化装车系统，系统运行于互联网。铁路货运大客户系统部署在铁路总公司级，集中受理优化装车系统部署于 18 个铁路局，实现铁路签约货运大客户通过互联网提报月计划和日请求车功能。铁路总公司货运大客户有 120 家左右、路局级的签约大客户超过 2 000 家。系统用户众多，地域范围广。为了确保在互联网确认每个货运大客户的身份，系统要求登录的大客户使用智能密码钥匙进行身份认证，确保授权的铁路签约货运大客户安全访问系统，其它未授权的人员不能访问系统，保证铁路签约货运大客户的合法权益。

（下转 P49）

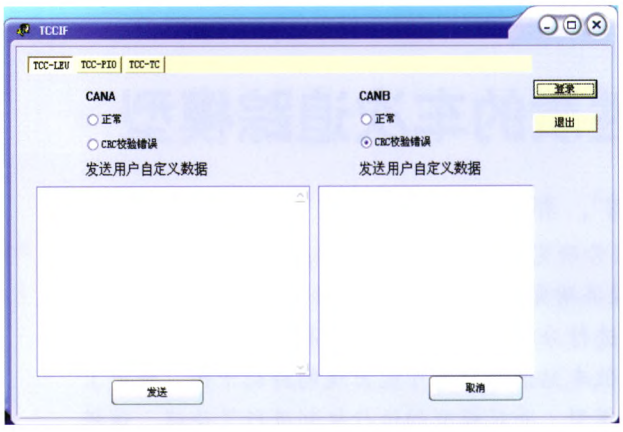

图6　TCC接口平台用户界面

文 CRC 校验包后，TCC 主机不能和 LEU 建立通信，监测维护机 TCC 与 LEU 通信中断故障报警，LEU 向有源应答器发送应答器默认报文。当 TCC 接口平台发送正确的应答器报文数据长度包、正确的应答器报文数据帧序号包和正确的应答器报文 CRC 校验包后，TCC 主机和 LEU 建立通信，监测维护机 TCC 与 LEU 通信中断故障报警解除，LEU 向有源应答器发送正常有源应答器报文。通过 TCC 接口平台对 TCC 与 LEU 间通信数据的故障注入与解除，验证 TCC 主机在通信数据的故障 - 安全准确性。

同样，在对 TCC- 轨道电路和 TCC-PIO 间的接口测试过程中，通过 TCC 接口平台验证 TCC 主机发送通信数据和校验数据的故障 - 安全设计也得到很好的应用。

4　结束语

本文设计了 TCC 接口平台的总体结构，实现了接口平台的功能，解决了 TCC 主机与各模块间的通信困难，通过接口平台将列控中心接入到 CTCS-3 级列控系统半实物仿真平台中进行仿真测试，同时对 TCC 与各模块接口间增加了故障注入功能，有效地验证了列控中心对故障的正确处理，为 TCC 系统的安全性以及交付使用提供一定技术支持和保障。

参考文献：

[1] 张大威 . 列控中心仿真测试技术的发展与应用 [J]. 铁道通信信号，2012（12）：5-10.

[2] 胡延朝 . 车站列控中心接口系统功能概述 [J]. 科技资讯，2012（17）：28-30.

[3] 张仕雄 . 客运专线列控中心测试平台的构建研究 [J]. 铁道运输与经济，2012（2）：82-86.

[4] XU TianHua, TANG Tao, GAO ChunHai & CAI BaiGen. Dependability analysis of the data communication system in train control system[J]. 2009 (9): 2605-2618.

[5] 郭永泉，王　勇 . CTCS-2 级列控系统接口故障机制探讨 [J]. 现代城市轨道交通，2008（5）：20-25.

责任编辑　陈　蓉

（上接 P45）

系统使用的商用密码产品为智能密码钥匙，用数字证书认证保证大客户用户合法性。

3.2.2　铁路行包管理系统

铁路行包管理信息系统实现铁路运输行包的管理，系统依托于互联网，利用 VPN 设备建立虚拟专用网络，保证系统信息的安全。系统部署于全路 18 个铁路局，分布于主要铁路车站和客运行包办理站。系统利用商用密码设备 IP 协议密码机构建 VPN 网络，用于保证系统信息安全。

3.2.3　铁路口岸信息平台系统

铁路口岸信息平台系统在铁路总公司建立了经中国电子口岸数据中心与海关总署进行信息交换的平台，通过中国电子口岸数据中心，实现了铁路与海关之间运单（舱单）信息、执法指令等的联网互通、信息共享。系统中使用密码机保证信息安全。

以上系统中使用的商用密码产品都是国家密码管理局公布的“商用密码通用产品名单”中的产品。

4　结束语

商用密码在铁路现有信息系统安全中起到了重要作用。随着铁路电子商务的发展，信息安全问题日益重要，为了保障信息安全，商用密码在铁路信息系统中必将得到更加广泛的应用。

参考文献：

[1] 斯廷森 . 密码学原理与实践 [M]. 冯登国，译 . 北京：电子工业出版社，2009.

责任编辑　徐侃春