文章编号：1005-8451（2020）06-0039-05

# 国产密码在铁路调度应急指挥系统中的应用研究

冯小芳
（中国铁道科学研究院集团有限公司　电子计算技术研究所，北京　100081）

**摘　要：**通过研究国产密码（简称：国密）的核心算法、典型应用场景及应用现状，结合铁路调度应急指挥系统的实际需求，解决系统中的安全方案设计、数据传输加密问题。详细阐述了国密在铁路调度应急指挥系统中的应用，得出铁路调度应急指挥系统的安全架构、身份认证和数据加密传输等方案，对于维护系统数据完整性，保障信息安全、提高安全防护等级等有着重要的作用。

**关键词：**国产密码；铁路调度应急；安全架构；加密传输；身份认证
**中图分类号：**U29 : TP393　**文献标识码：**A

## Domestic password applied to railway dispatching emergency command system

FENG Xiaofang
( Institute of Computing Technologies, China Academy of Railway Sciences Corporation Limited, Beijing　100081, China )

**Abstract:** This paper studied the core algorithm, typical application scenarios and application status of the domestic password (referred to as "national password"), solved the security scheme design and data transmission encryption problems in the system in combination with the actual requirements of the railway dispatching emergency command system, expounded the application of national password in the railway dispatching emergency command system in detail, and obtained the security architecture scheme, identity authentication scheme and data encryption transmission scheme of the railway dispatching emergency command system, which played an important role in maintaining the data integrity of the system, ensuring the information security and improving the security protection level.

**Keywords:** domestic password; railway dispatching emergency; security architecture; encrypted transmission; identity authentication

2014 年，中华人民共和国国务院办公厅印发相关文件，要求率先在金融领域实现国产密码（简称：国密）应用突破，力争到 2020 年实现国密全面应用 [1]。国密是自主可控技术的重要基础。从 2015 年起，国密应用从金融领域拓展到其他重要领域，证券、广电、能源、教育、公安、党政等国民经济重大行业主管部门陆续实现基于国密的实施升级工作 [2]。铁路运输是关乎国民经济发展的重要行业，铁路信息技术及信息化建设是保障铁路安全运营、安全生产的重中之重，是国家要求尽快推进安全保障自主可控的重点行业之一。铁路调度应急指挥系统（简称：调度应急系统）中的一些重要的信息，如调度命令、行车信息、铁路信号、客票数据等均通过网络进行传输 [3]。本文研究调度应急系统中的国密应用，为国密在铁路运输生产系统中的推广提供参考。

收稿日期：2020-01-25
基金项目：国家自然科学基金资助项目（U1934216）；中国国家铁路集团有限公司科技研究开发计划课题（N2019X002）；中国铁道科学研究院集团有限公司科研项目（2019YJ109）；中国铁路北京局集团有限公司科技研究开发计划课题（2019AY03）
作者简介：冯小芳，高级工程师。

## 1　国密核心算法及应用

国密算法是我国自主研发创新的一套数据加密算法，经过多年的发展，已经颁布多个算法标准，包括 SM1、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法等，大致分为 3 类，其中：SM1、SM4、

SM7、祖冲之密码是对称加解密算法；SM2、SM9是非对称加解密算法；SM3是哈希杂凑算法[4]。

### 1.1 国密算法对比分析

国密算法与国际密码算法的对比[4-5]如下：

（1）SM4算法是一种分组对称加解密算法，与国际数据加密标准（DES，Data Encryption Standard）算法类似，两者的目的都是为了加密保护静态储存和传输信道中的数据。SM4算法采用基本轮函数（32 bit）加迭代算法，分组长度和密钥长度均为128 bit，其安全性高于DES算法。

（2）SM2算法是一种非对称加解密算法，和国际公钥加密（RSA，Rivest-Shamir-Adleman）算法类似。SM2算法基于椭圆曲线进行计算，RSA算法基于可逆幂运算；SM2算法复杂度为完全指数级，RSA算法复杂度为亚指数级。国密SM2算法解决了RSA算法中的亚指数级问题。在同等安全等级上，SM2算法所需的密码位数较少，且密钥生成和解密速度都比RSA算法快，实现较为容易，且加解密效率更高。

（3）SM3算法是一种杂凑算法，与信息－摘要（MD5）算法、安全散列（SHA）–1算法相似。SM3算法适用于商用密码应用中的数字签名和验证，是在SHA-256基础上改进实现的一种算法。SM3算法消息分组长度为512 bit，摘要值长度为256 bit，设计更加复杂，安全性相对较高。

各类加密算法对应的国密算法替换关系如表1所示[5-6]。

表1 国密与国际密码对应关系

| 算法类别 | 目前常用算法 | 可替代的国密算法 |
|---|---|---|
| 非对称加解密算法 | RSA，DES | SM2 |
| 哈稀杂凑算法 | MD5，SHA–1 | SM3 |
| 对称加解密算法 | DES，AES，RC4 | SM4 |

### 1.2 国密应用现状

国密技术在既有系统改造和新系统建设中的典型应用场景如下。

（1）电子认证服务系统

传统公钥基础设施（PKI，Public Key Infrastructure）及应用安全产品都是基于国际RSA算法，无法兼容国密算法，根据国家密码管理局要求，全国大部分电子认证服务机构目前已完成了电子认证服务系统公钥密码算法升级，支持SM2算法。

（2）安全网关

通过对安全网关进行升级，使其支持与客户端建立基于国密SM4算法的双向安全套接层（SSL，Secure Sockets Layer）加密链路，并使用支持国密算法的OpenSSL支撑库[5]，提高SSL协议传输的加密强度。

（3）签名验签服务

签名验签服务器作为底层硬件密码设备，为应用服务器提供硬件密码生成和核验服务，需支持对国密SM系列算法密钥的加密和解密。

（4）客户端硬件

客户端硬件设备选用内置国密算法的USB Key设备，同时该设备作为数字证书的载体需兼容国密算法的数字证书。

## 2 调度应急系统

### 2.1 系统概述

铁路调度应急指挥工作是指，在运输调度指挥过程中，当铁路线路、通信信号、供电等固定设施，机车、车辆、动车组等移动设备发生故障或遭遇恶劣天气等自然灾害和突发客流等突发事件时，借助相关设备、设施和支撑系统，制定应急处置方案，指挥应急处置实施，努力恢复运输秩序，减少突发事件影响的过程[7]。调度应急系统在中国国家铁路集团有限公司（简称：国铁集团）集中统一部署，为国铁集团、铁路局集团有限公司（简称：铁路局）及站段三级提供应用，同时集成了大量的运输生产核心数据，包含大量的数据交互和传输。系统的安全架构设计极为关键，对于身份认证和安全传输方面的安全防护需求极为强烈。

### 2.2 系统应用架构

用户通过统一的用户授权和校验后，方可访问相应的系统应用。系统采用统一的消息传输通道，为参与调度应急工作的国铁集团各部门和各铁路局各部门之间提供消息共享和传递[7]。系统主要有调度应急辅助、应急处置过程管理、应急值守、应急决策支撑、应急演练、应急基础资料管理、应急预案管理、应急移动App、应急智能通信、系统管理10个模块[7-8]。

系统的应用架构如图 1 所表示。

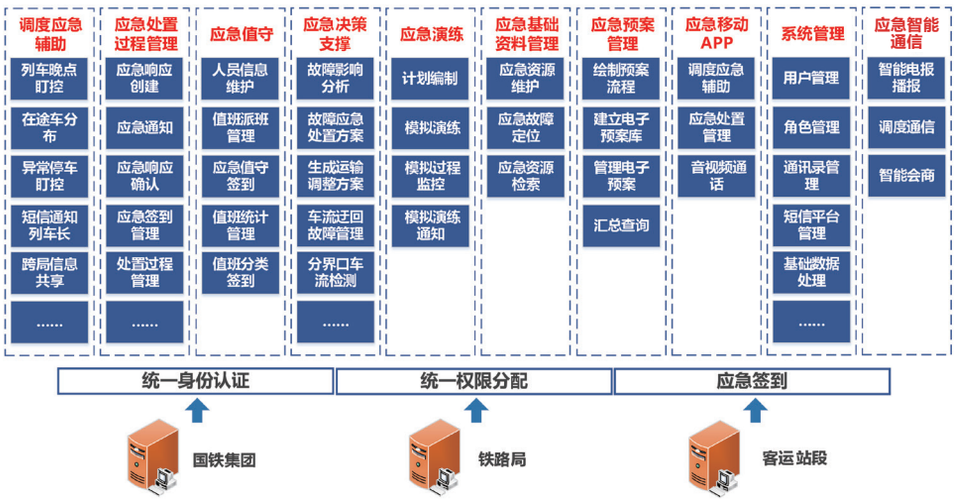


图1　系统应用架构

## 3　国密在调度应急系统中的应用

国密在调度应急系统中的应用主要从安全架构、身份认证和安全传输 3 方面进行研究。系统为用户提供 USB Key，通过认证机构（CA，Certificate Authority）颁发用户国密证书进行用户签名认证，建立互联网协议安全（IPSec，Internet Protocol Security）通道，实现传输安全。

### 3.1　基于国密的安全架构方案

调度应急系统基于国密的安全架构包含物理安全、网络安全、主机安全、应用安全和数据安全等方面。系统安全架构按照统一标准、顶层设计、分步实施的原则，其整体安全架构设计如图 2 所示。

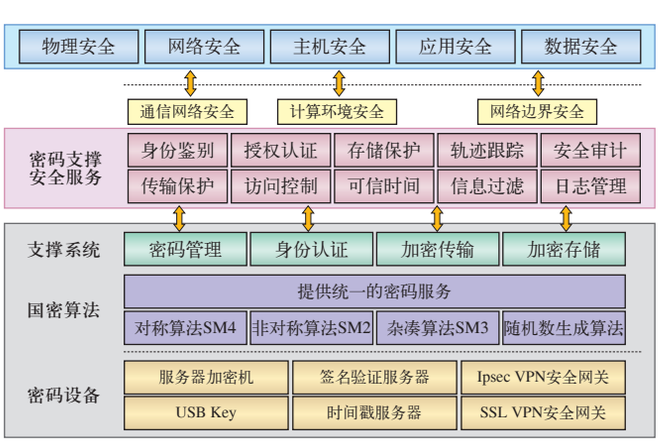


图2　系统安全架构

系统安全架构分为密码设备层、国密算法层、支撑系统层及密码支撑安全服务层，以保障系统的网络和信息安全。

（1）密码设备层

该层提供服务器加密机、签名验证服务器、USB Key、时间戳服务器、IPSec 虚拟专用网（VPN，Virtual Private Network）安全网关、SSL VPN 安全网关等设备。通过服务器加密机，可以解决密钥分配、密钥管理、加密和解密计算等问题；时间戳服务器和签名验证服务器可以辅助实现系统的抗抵赖性，保证数据的真实性；通过 USB Key 下载和安装基于国密算法的用户数字证书，完成重要用户的身份认证；IPSec VPN 安全网关、SSL VPN 安全网关可进行通道隔离，保障传输通道的可靠性和数据完整性。

（2）国密算法层

利用国密算法去研发和改造既有应用系统中的加密程序。同时，利用支撑国密算法的设备、服务器等，对各子系统提供统一的密码服务。

（3）支撑系统层

研发基于国密算法的支撑系统，包括身份认证、加密传输、加密存储、密码管理等。

（4）密码支撑安全服务层

基于通信网络安全提供身份鉴别、传输保护服务；基于计算环境安全提供授权认证、存储保护、访问控制、可信时间服务；基于网络边界安全提供安全设计、日志管理、轨迹跟踪、信息过滤等密码安全服务。

### 3.2　基于国产密码的身份认证方案

调度应急系统身份认证过程为：客户端将获取到的用户输入账号、密码信息连同客户端 IP 一起发送给服务器，服务器从数据库获取对应用户信息进行校验，若校验通过，则登录成功，否则登录失败。

系统采用非对称加密算法和对称加密算法结合的方式对用户信息进行保护。客户端使用服务器生成的公钥对密码进行加密，服务器则可以通过私钥解密来获取真实的用户信息。为了避免用户信息明

文存储，系统使用对称算法对用户数据进行加密存取。系统加解密过程为：

（1）客户端请求获取服务器的 SM2 公钥，使用公钥对用户输入的密码进行加密，并将账号、密码密文、IP 信息发送给服务器；

（2）服务器使用 SM2 私钥对密文进行解密，获取账号、明文密码、IP 信息；

（3）服务器从数据库中获取用户信息，使用本地存储的 SM4 密钥对密码进行解密，获取明文密码，执行校验。

身份认证过程中，调度应急系统根据服务器生成 SM2 密钥的不同，产生不同的加密结果，还为核心岗位提供支持国密算法的用户数字证书来解决用户身份认证的问题。

### 3.3 基于国密的加密传输方案

#### 3.3.1 安全传输通道设计

系统中的数据传输协议并不仅限于 Http 协议，还包括基于 TCP/IP 的 Java 远程调用协议和 Java 消息服务。为了支持国密算法，系统采用 IPSec 网络传输协议来建立安全通道，安全通道架构如图 3 所示。

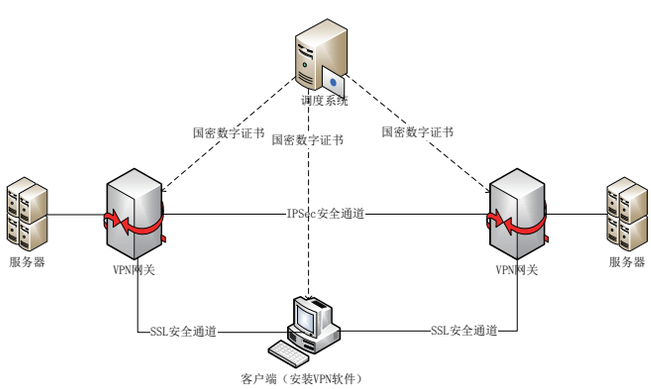


图3 安全传输通道架构

CA 系统为 VPN 网关颁发国密证书，VPN 网关基于 IPSec 协议建立安全通道。数据在安全通道中传输时，在 IP 层进行加密，即便传输数据被截取，也无法对其进行解密解读，从而保证传输过程中数据的安全性。选择支持国密算法的 IPSec VPN 网关 [1] 建立传输通道，实现服务器之间的安全传输。在客户端安装 VPN 软件，利用 Open SSL 解决方案来实现客户端与服务器之间的安全传输 [9]。

#### 3.3.2 数据传输安全设计

对调度应急信息进行安全传输的数字签名方案设计 [10] 如图 4 所示。

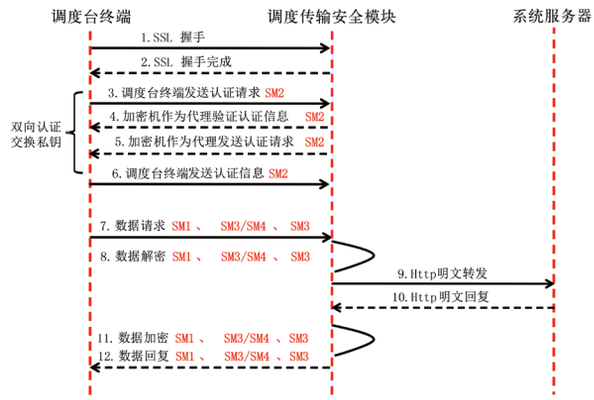


图4 数字签名方案流程

（1）调度台终端与调度传输安全模块建立握手消息；

（2）调度传输安全模块向调度台终端发送握手完成消息；

（3）调度台终端向调度传输安全模块发送基于 SM2 算法加密的认证请求；

（4）调度传输安全模块加密机作为代理验证基于 SM2 算法加密的认证信息；

（5）调度传输安全模块加密机作为代理发送基于 SM2 算法加密的认证请求；

（6）调度台终端向调度传输安全模块发送 SM2 算法加密的认证信息；

（7）调度台终端向调度传输安全模块发送基于 SM1、SM3/SM4、SM3 算法加密的数据请求；

（8）调度传输安全模块解密 SM1、SM3/SM4、SM3 算法加密的数据请求；

（9）调度传输安全模块与系统服务器采用 Http 明文转发；

（10）系统服务器与调度传输安全模块采用 Http 明文回复；

（11）调度传输安全模块基于 SM1、SM3/SM4、SM3 算法加密数据；

（12）调度传输安全模块回复基于 SM1、SM3/SM4、SM3 算法加密的数据。

#### 3.3.3 安全传输过程

安全传输过程包含 3 个阶段：客户端密钥注册、

数据加密传输和客户端密钥注销。

（1）客户端密钥注册

客户端生成 SM4 密钥对用户输入的密码信息进行加密，请求服务器 SM2 公钥对客户端 SM4 密钥进行加密，并将账号、密码密文、IP、SM4 密钥密文发送给服务器。服务器接收数据后，使用 SM2 私钥对 SM4 密钥密文进行解密，获取客户端 SM4 密钥，对密码密文进行解密并对用户信息进行校验。

（2）数据加密传输

客户端使用 SM4 密钥对数据进行加密，将加密后的数据发送到服务器。服务器接收加密数据后，使用客户端 SM4 密钥对数据进行解密，执行业务处理，并用客户端 SM4 密钥对处理结果进行加密处理后，发送给客户端。客户端接收响应信息后，使用 SM4 密钥对数据进行解密，读取真实信息。

（3）客户端密钥注销

客户端发起注销请求，服务器接收请求后，执行注销逻辑，同时移除对应客户端密钥信息，并返回处理结果给客户端，客户端执行注销操作。

## 4　结束语

本文研究了国产密码技术在铁路调度应急系统的安全架构、身份认证和安全传输 3 个方面的应用。可为铁路运输生产系统利用国产密码技术构建安全架构设计提供参考。国产密码在铁路信息化领域的运用才刚刚起步，对其软硬件支撑产品的可靠性和稳定性仍需进行大量的探索，还需制定相应的升级改造规划和分期改造过渡方案，做到自主、安全、可控的同时，稳步有序推进 [11]。

## 参考文献

[1] 中华人民共和国国务院办公厅 . 金融领域密码应用指导意见：国办发 [2014]6 号文件 [Z]. 北京：中华人民共和国国务院办公厅，2014.

[2] 文　学 . 国密算法在央行应用的实践分析 [J]. 金融科技时代，2017（2）：58-60.

[3] 刘　俊，冯小芳 . 铁路客运应急调度指挥系统构建研究 [J]. 铁道运输与经济，2018(7):43-48.

[4] 王　勇，岑荣伟，郭　红，等 . 国家电子政务外网电子认证系统 SM2 国密算法升级改造方案研究 [J]. 信息网络安全，2012（10）：83-85.

[5] 赵　鹏，赵　云，辉胡杰 . 基于国产密码构建 ChinaDRM 版权保护云服务 [J]. 广播电视信息，2018（z1）：50-53.

[6] 姚　键 . 国产商用密码算法研究及性能分析 [J]. 计算机应用及软件，2019（6）：327-333.

[7] 韩国兴 . 突发事件下列车大面积晚点分析与应急处置系统研究 [D]. 北京：北京交通大学，2014.

[8] 韩旭辉 . 基于分布式云架构的铁路客运站智能应急指挥系统设计 [J]. 铁路计算机应用，2018，27（11）：27-31.

[9] 魏　来，陈　睿，张　帆，等 . 支持国产密码算法的 OpenSSL 设计实现及应用 [J]. 中国新通信，2019，21（7）：109-110.

[10] 沈　阳，张智军，薛子立 . 应急广播商用密码研究 [J]. 广播电视信息，2019（9）：74-77.

[11] 柳彩云，陈雪鸿，杨帅锋 . 国产密码算法与工业互联网平台的结合势在必行 [J]. 中国信息安全，2019（4）：86-89.

责任编辑　李依诺