

城市轨道交通门禁系统加密方案研究

张化军¹ 何治达¹ 邹 洋²

(1. 郑州地铁集团有限公司, 450018, 郑州; 2. 中国船舶重工集团公司第七一三研究所, 450015, 郑州//第一作者, 工程师)

摘 要 城市轨道交通门禁系统通常采用的 Mifare 1 技术因被破解而存在严重的安全隐患,且随着城市轨道交通在各个城市的快速发展以及轨道交通运营管理部门的人员流动需求,各条线路的门禁卡需进行统一的授权管理。提出采用 CPU 卡技术、运用加密算法的方案,实践证明将可有效地解决上述两个问题。通过对门禁系统技术的分析,提出城市轨道交通门禁系统的技术方案,并从卡的类型、通信原理及加密可靠性等角度,研究分析其特点;论述了城市轨道交通门禁系统的加密方案及发展方向。

关键词 城市轨道交通; 门禁系统; 加密算法

中图分类号 U231+.92

DOI:10.16037/j.1007-869x.2019.03.038

Research on the Encryption Scheme of Access Control System in Urban Rail Transit

ZHANG Huajun, HE Zhida, ZOU Yang

Abstract At present, the access control systems usually adopt Mifare 1 card technology, which has been cracked and exposed to serious security risks. With the rapid network development of rail transit in Chinese cities and the urgent personnel flow demands of rail operation management departments, each rail transit line needs a unified authorization management of access card. For this reason, a scheme of adopting CPU card technology and using encryption algorithm is proposed, which will effectively solve the above-mentioned problems. In this paper, through analyzing the access control system technology, a technical scheme of access control for urban rail transit is put forward. Then, from the viewpoint of card type, communication principle and encryption reliability, the characteristics of the new scheme is analyzed. Finally the encryption scheme of access control system and the development direction in urban rail transit are discussed.

Key words urban rail transit; access control system; encryption algorithm

First-author's address Zhengzhou Metro Group Co., Ltd., 450018, Zhengzhou, China

营,保证授权人员在受控情况下方便地进入设备管理区域,防止非授权人员进入限制区所设立的系统。它一直扮演着保障城市轨道交通安全的重要角色。随着门禁系统应用领域的扩展和深入,目前,城市轨道交通门禁系统所采用的 Mifare 1 卡难以满足更高的安全性和更复杂的多应用需求,尤其是在 Mifare 1 卡的安全被破解的情况下,用户信息的安全性得不到保障,卡片几乎都可以被完整复制,限制了目前一卡通的发展。随着集成技术和加密技术的发展,近几年 CPU(中央处理器)卡技术逐渐成熟,交易过程的信息安全性和可定制开发的灵活性不断提升,因此 CPU 卡技术正成为非接触 IC(集成电路)卡技术的重要发展趋势。

1 城市轨道交通门禁系统卡

1.1 门禁系统卡类型

目前,城市轨道交通门禁系统应用的非接触式 IC 卡主要包括 Mifare 1 卡、DESfire 卡和 CPU 卡,其特点见表 1。

较为流行的非接触式 IC 卡为 Mifare 1 卡和 CPU 卡;DESfire 卡为准 CPU 卡,属于 Mifare 1 卡与 CPU 卡之间的过渡产品。以下主要介绍 CPU 卡与 Mifare 1 卡的相关技术。

1.2 门禁系统卡的通信原理及特点

Mifare 1 卡、CPU 卡的通信原理以及 CPU 卡的双向认证原理如图 1~3 所示。由 Mifare 1 卡和 CPU 卡的通信原理可知,Mifare 1 卡的密码进行明文传输,一旦被窃取,卡片即可被复制,因此此卡采用密码认证的方式,存在一定的安全隐患;CPU 卡采用随机码加密结果认证方式,即同一张 CPU 卡每次刷卡的认证密码均不相同,只要密钥系统不泄露,卡被窃取后通信数据依然不会被破解。

1.3 卡结构对比

1.3.1 卡结构

CPU 卡芯片产品支持 ISO 14443-A 协议,CPU

门禁系统是为确保城市轨道交通正常、安全运

表 1 常用非接触式 IC 卡特点

项目	Mifare 1 卡	DESfire 卡	CPU 卡
卡片类型	非接触逻辑加密卡	非接触 Mifare DESfire 4 KB 卡	非接触 CPU 卡
工作频率/MHz	13.56	13.56	13.56
RF(射频)接口协议	ISO/IEC 14443 A	ISO/IEC 14443 A	ISO/IEC 14443 A
读写距离/cm	2.5 ~ 10	2.5 ~ 10	2.5 ~ 10
加密模块	无实现算法的硬件加密模块	采用协处理器执行加密	采用硬件运算模块执行加密
加密方式	Crypto 加密流,符合 ISO 9798-2 的三轮认证	RF 通道实现 DES(数据加密算法)、3DES 数据加密	支持 DES、3 DES 等加密算法
密钥长度/B	6	8	16
终端安全性	采用“固定 ID + 逻辑加密”	采用“随机 ID + RF 加密”	采用的“动态密钥、密钥存储、交易验证与加密计算”均由 SAM(安全存储模组)卡独立完成

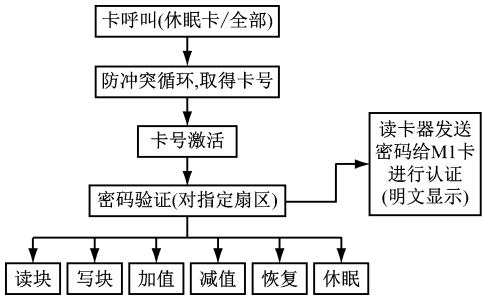


图 1 Mifare 1 卡通信原理

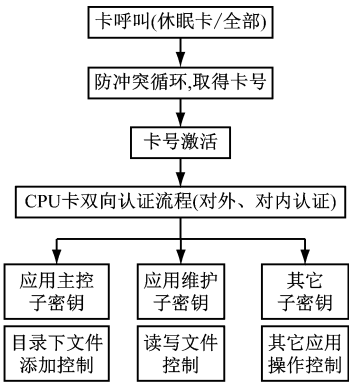


图 2 CPU 卡通信原理

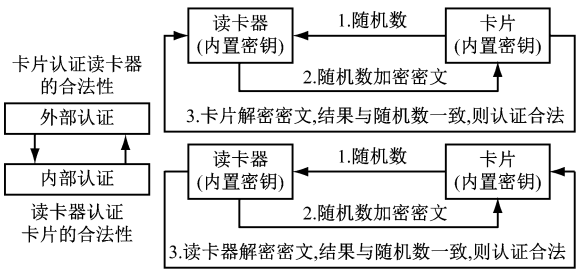


图 3 CPU 卡双向认证原理

国人民银行颁布的《中国金融集成电路(IC)卡规范(2.0)》(以下简为“PBOC 2.0”)中对电子存折/电子钱包的要求,也符合 CJ/T 306—2009《建设事业非接触式 CPU 卡芯片技术要求》的规定。COS 系统则同时支持上述两规范的要求,且具有较好的安全性。

Mifare 卡是 NXP 公司生产的一系列遵守 ISO 14443A 标准的射频卡。该卡包括 0 ~ 15 共 16 个扇区,并且每个扇区都有独立的密码,每个扇区配备了 0 ~ 3 共 4 个块,16 个扇区的 64 个块按绝对地址编号为 0 ~ 63,每个块可以保存 16 B 的内容,16 个扇区共可保存 1 024 B 内容。每个扇区的第 4 段用来保存 KeyA、KeyB 和控制位(门禁系统控制读写权限)。0 扇区 0 块是特殊的数据块,用于存放制造商代码,包括芯片序列号,此块仅具只读功能。

1.3.2 软件

非接触 CPU 卡拥有独立的 CPU 处理器和芯片操作系统,所以可以更灵活地支持各种不同的应用需求,以及更安全地设计交易流程。但同时,非接触 CPU 卡的系统显得更为复杂,需要进行诸如密钥管理、交易流程、PSAM(销售点终端安全存取模块)卡以及卡片个性化等方面的系统改造。

Mifare 1 通常被认为是一种制造智能卡的技术,这是因为 Mifare 1 卡兼具读写功能。事实上,Mifare 1 卡仅具记忆功能,必须搭配处理器卡才能达到读写功能,且卡片内不存在系统软件。

1.3.3 对比

非接触 CPU 卡可以通过内外部认证的机制,如定义的电子钱包的交易流程,更加可靠地满足不同的业务流程对安全和密钥管理的需求。

指令兼容通用 8051 指令和内置硬件 DES(数据加密标准)协处理器,数据存储器为 8 kB 的 EEPROM(带电可擦写可编程只读处理器)。该芯片符合中

CPU 卡支持多种密钥分类,对电子钱包圈存可以使用圈存密钥,同时可以使用消费密钥进行消费,使用 TAC(交易认证码)密钥进行清算,使用卡片应用维护密钥进行数据的更新。卡片个人化过程中,可以使用卡片传输密钥、卡片主控密钥及应用主控密钥等,真正做到一钥一用。

通过由 CPU 卡发送至 SAM 卡的 MAC(报文鉴

别代码)1、由 SAM 卡发送至 CPU 卡的 MAC 2,以及由 CPU 卡返回的 TAC,可以实现数据传输验证的计算。而 MAC 1、MAC 2 和 TAC 在同一张 CPU 卡每次传输的过程中都是不同的,因此无法使用空中接收的办法来破解 CPU 卡的密钥。

CPU 卡与 Mifare 1 卡对比详见表 2 和表 3。

表 2 CPU 卡与 Mifare 1 卡的参数对比表

项目	CPU 卡	Mifare 1 卡
操作系统	COS 系统	非 COS 系统
加密模块	硬件运算模块	无实现算法的硬件加密模块
密钥长度/B	16	6
交易安全性	钱包不可被非法访问,PSAM 之间严格采用双向认证流程,交易自动生成 TAC 码	通过口令保护钱包,不校验口令错误次数;口令更换是明文,在传输过程中可被截取,且卡片不能验证设备合法性
终端安全性	采用的动态密钥、密钥存储、交易验证与加密运算均由 SAM 卡独立完成	采用固定密钥,不支持 SAM 卡双向认证

表 3 CPU 卡与 Mifare 1 卡的加密安全性对比表

项目	CPU 卡	Mifare 1 卡
密码传输方式	密码在线路上不以明文出现	密码在线路上是明文传输的,易被截取
数据加密情况	每次传输均通过随机数进行加密,随机数的参加,确保了每次传输内容的不同	密码和算法均透明
认证合法性	具有持卡人合法性认证、卡合法性认证和系统合法性认证	逻辑加密卡无法认证应用的合法性
加密模块	采用硬件运算模块执行加密	无实现算法的硬件加密模块
加密算法	支持 SM 1 国密算法和支持 3 DES 商密算法	无加密算法

2 门禁系统 CPU 卡加密方案

2.1 CPU 卡加密方法

2.1.1 CPU 卡规划情况

CPU 卡主要包括主控制区、一卡通专用文件区(用于员工乘坐地铁)、预留文件区和卡预留空间,如图 4 所示。

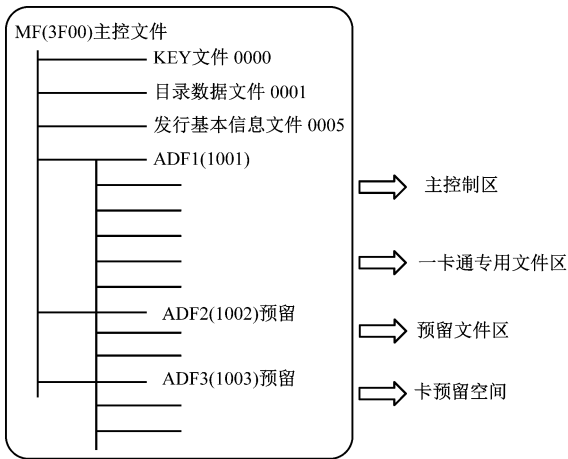


图 4 CPU 卡规划和当前使用情况

2.1.2 门禁系统对于 CPU 卡的使用需求建议

CPU 卡的一卡通业务应用均授权了密钥文件,若车站门禁系统使用既有的密钥文件,不同业务间的信息交互存在安全风险,也不便于不同专业间的用卡管理,因此,车站门禁系统应使用 CPU 卡的预留应用 ADF 3(1003)空间。

2.2 门禁系统加密工作

(1) 首先在 CPU 卡中找到需要操作的文件,通过文件标志表进行标记,并利用 CPU 卡预留区域空间,单独设置门禁系统的车站级应用,同时建立目录文件。

(2) 加密方式按商密 3DES 或国密标准,采用对称密钥加密法。

(3) 为保证既有线路、在建线路和新建线路对于门禁系统的卡授权统一管理,轨道公司需建立密钥文件和业务应用文件标准。

(4) 发卡中心负责 CPU 员工卡的重新授权工作,以激活预留区域门禁系统建立的密钥文件和业务应用文件。

(5) 由门禁厂家根据已确定的密钥文件和业务

应用文件标准,根据读卡协议进行 CPU 读卡器的二次程序开发。

2.3 既有门禁系统改造方案

既有门禁系统的改进方案如表 4 所示。

表 4 既有门禁系统的改造方案

项目	内容
接口确认	门禁厂家应与 ACC 进行技术对接,以确定门禁卡使用规划和门禁系统业务文件建立的标准,签订接口技术规格书,需注意门禁系统密钥文件和业务应用不能与一卡通系统合用
接口开发	门禁厂家根据确定的接口技术规格书进行读卡器程序开发
接口测试	各门禁厂家所制定的技术方案不同,因此须提前与发卡中心进行接口测试,通过 CPU 读卡器与 CPU 员工卡配合使用来完成测试工作
生产制造	根据测试情况进行 CPU 读卡器的批量生产

3 结语

门禁系统作为城市轨道交通中最重要的安全

(上接第 96 页)

端。设备舱中部区域空气流动相对稳定,两端空气流速较大,这样使得空气扰动性增强,从而利于设备进行散热。

4 结语

本文通过 CFD 数值模拟仿真对地铁列车车型设备舱的压力场和温度场进行了计算。因为夏季温度最高,对列车设备运行最为不利,因此本文选取夏季(隧道及明线空气温度 40 ℃)、明线和高架运行工况,以及考虑太阳辐射等条件来进行计算。通过仿真计算得到隧道运行、明线运行、高架运行及隧道停站 4 种工况下列车设备舱内部空气温度分布和压力分布情况。

结合理论与模拟结果,对地铁列车设备舱内温度场的优化提出以下建议:一是通过在裙板两侧开通风口加大进入设备舱的冷却风量来进行散热,二是将发热量较大的设备布置于设备舱的两端。

系统,更新本系统所采用的技术已迫在眉睫,这样才能保证设备和人员安全,从而进一步保障城市轨道交通的运营安全。采用 CPU 卡技术运用加密算法,可以保证认证信息不被解析,从而保障门禁系统安全使用;可以使用 CPU 卡预留区域的空间开发新的应用,扩展门禁系统功能。门禁系统采用 CPU 卡技术运用加密算法的方案将是轨道交通门禁系统新的发展方向。

参考文献

[1] 程媛. 城市轨道交通门禁系统线网授权方案研究[J]. 铁路通信信号工程技术,2016,13(4):68.
[2] 王建文. 地铁门禁系统与综合监控系统集成案例[J]. 都市轨道交通,2013,26(2):108.
[3] 张道,王文荣,徐强. 上海轨道交通 10 号线门禁系统设计方案[J]. 城市轨道交通研究,2011(3):92.
[4] 张森. 宁波轨道交通门禁线网授权管理平台的设置[J]. 自动化应用,2012(6):19.

(收稿日期:2018-07-17)

参考文献

[1] 关永久. 高速列车在隧道内会车过程的气动特性研究[D]. 成都:西南交通大学,2010.
[2] TOMOSHIGE H. Method of measuring the aerodynamic drag of trains[J]. Bulletin of JSME, 1965,8(31):390.
[3] TOMOSHIGE H. Aero dynamical problems when train is running into tunnel with large velocity[J]. Railway Techincal Research Report, 1960(153):169471.
[4] 田红旗. 中国列车空气动力学研究进展[J]. 交通运输工程学报,2006,6(1):1.
[5] 田红旗. 列车交会空气压力波研究及应用[J]. 铁道科学与工程学报,2004(1):83.
[6] 李志伟,梁习锋,周丹. 快速集装箱平车在明线和隧道内会车时的气动性能[J]. 中南大学学报(自然科学版),2008,39:1029.
[7] 白刚. 高速列车设备舱通风散热影响因素分析[J]. 发电与空调,2016(4):86.
[8] 胡文锦. 高速列车设备舱通风散热及气动响应研究[D]. 成都:西南交通大学,2013.

(收稿日期:2018-07-20)

欢迎投稿《城市轨道交通研究》
投稿网址:tougao. umt1998. com