

国产商用密码技术在城市轨道交通 AFC 系统的应用

李一玮

(郑州市工程质量监督站, 450018, 郑州 // 高级工程师)

摘要 随着网络信息的迅猛发展, 用户身份认证盗用、黑客攻击、数据意外泄露等信息安全事件频发, 越来越多的企事业单位开始关注信息系统的安全问题, 尤其是一些关系国计民生的重点单位。加密技术作为加强信息系统安全的重要手段被广泛使用。国产商用密码技术为我国自主可控的加密技术, 已成为我国信息加密的首选技术。介绍了国产商用密码技术在城市轨道交通自动售检票系统中的应用方案。测试结果表明, 国产商用密码技术适用于城市轨道交通自动售检票系统, 且性能优于现用的国外密码技术。

关键词 城市轨道交通; 自动售检票系统; 国产商用密码

中图分类号 U293.22

DOI: 10.16037/j.1007-869x.2021.09.042

Application of National Commercial Cryptography Technology in Urban Rail Transit AFC system

LI Yiwei

Abstract With the rapid development of network information, information security incidents such as user identity theft, hacker attacks and accidental data leakage occur frequently. More and more enterprises and institutions begin to pay attention to information system security, especially the key units related to national economy and people's livelihood. Encryption technology is widely used as an important means to strengthen the security of information system. As an independent and controllable encryption technology, domestic commercial encryption technology has become the preferred technology of information encryption in China. Application scheme of domestic commercial encryption technology in urban rail transit AFC (automatic fare collection) system is introduced. Test results show that domestic commercial encryption technology is suitable for urban rail transit AFC system and performs better than the foreign encryption technology currently in use.

Key words urban rail transit; AFC (automatic fare collection) system; domestic commercial cryptography

Author's address Zhengzhou Engineering Quality Supervision Station, 450018, Zhengzhou, China

《中华人民共和国密码法》已于 2020 年 1 月 1 日起施行。该密码法中规定密码分为核心密码、普通密码和商用密码。商用密码用于保护不属于国家秘密的信息。目前国内各地城市轨道交通 AFC (自动售检票) 系统的密钥系统均采用国际通用的 3DES 算法(分组加密算法), 密钥长期采用国外算法, 并未应用国家商用密码标准算法。国家商用密码算法在城市轨道交通 AFC 系统应用仍属空白。

国家商用密码管理办公室制定了一系列密码标准, 包括 SM1、SM2、SM3、SM4、SM7、SM9、祖冲之密码算法(ZUC)等。SM1、SM4、SM7 是分组算法, 但目前 SM1、SM7 算法不公开。因此, 考虑 AFC 系统在保留现有密码算法的前提下, 增加 SM4 算法应用。AFC 系统的密钥系统兼容两种密码算法, 以分阶段替换的方式, 优先采用 SM4 算法更新票卡密钥, 最终实现对 3DES 算法的自然淘汰。

密钥系统是城市轨道交通 AFC 系统的核心, 密钥的安全关系到整个地铁票卡系统的安全。SM4 在城市轨道交通 AFC 系统的应用, 填补了我国自主研发的密码算法在城市轨道交通行业技术应用的空白, 可摆脱对国外技术和产品的依赖, 保证 AFC 系统密码自主可控。

1 国产商用密码技术在 AFC 系统的应用

1.1 地铁票卡选用

AFC 系统主要由车站设备、密钥管理系统及发卡系统组成。密钥管理系统涉及的主要设备是支持 SM4 算法的加密机、密钥管理系统、读写器、CPU 卡、AFC 后台管理系统等。

地铁票卡一般分为 UL、MF1 和 CPU 卡。因为卡厂家主要供给金融业, 而金融业不使用 UL、MF1 卡, 所以目前国内支持国家商用密码算法的只有 CPU 卡。目前 UL、MF1 卡主要用于地铁单程票。随着二维码等互联网支付系统的普及, 单程票占全部交易的 5% 且逐年下降。而 CPU 卡也可与道路公

交换乘,因此其占比达 25%。综合以上两点,目前国家商用密码算法只需用在 CPU 卡即可,因受制于厂家生产问题目前也只能应用于 CPU 卡。

1.2 国密算法应用

SM4 算法是分组算法,与国外的 3DES 算法相对应。在计算过程中,SM4 算法通过增加非线性变换,理论上能大大提高其安全性,比 3DES 算法更加安全。

主要应用方案为:通过软件开发使读写器和清分系统同时适配 3DES 和 SM4 两种算法;在 AFC 系统增加采用 SM4 算法的加密机,采用 SM4 算法实现票卡发卡;采用国密算法的票卡在终端设备产生票卡交易后,TAC(交易验证码)采用 SM4 算法加密后上传到清分服务器;清分服务器连接加密机,验证 TAC;已发行的票卡仍然采用 3DES 算法进行业务处理,两套密码算法各司其职,互不干涉。具体系统架构如图 1 所示。

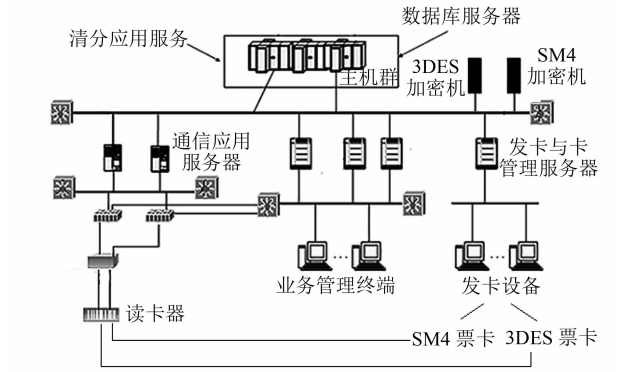


图 1 应用 SM4 算法的 AFC 系统架构

1.3 SM4 密钥管理系统

SM4 密钥管理系统遵循 SM4 算法标准规范,采用支持 SM4 算法的密码机实现对网络上传输的信息进行保护或鉴别,以保证 AFC 系统信息的正确性,能够有效防止对通信数据的非法窃取或篡改;完成密钥的产生、分发、注入和销毁;重点完成 AFC 系统中各类 SAM 卡、CPU 卡密钥的加载和分散卡片的各类密钥。

1.3.1 SM4 密钥分散

SM4 密钥分散,主要是利用每张卡片的唯一卡号作为分散因子,对加密机中的各类密钥进行分散,得到各个密钥的母密钥及子密钥,实现一卡一密。密钥分散过程如图 2 所示。

1.3.2 发卡系统

发卡系统重点是将密钥导入加密机,实现票卡

发行过程中将支持 SM4 算法的密钥加载到 SAM 卡和 CPU 卡中。

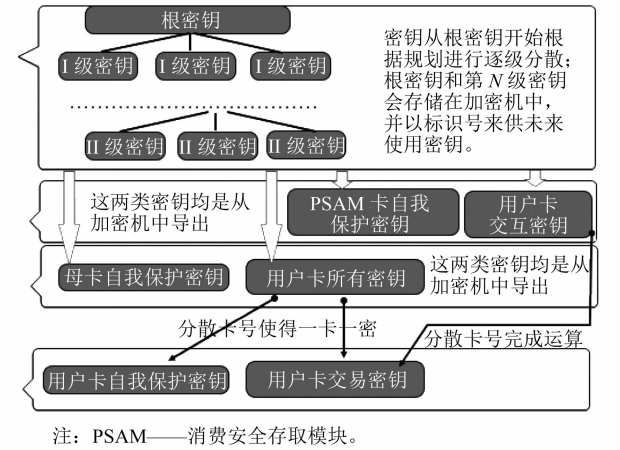


图 2 SM4 密钥管理系统密钥分散示意图

发卡系统采用 C/S(客户端/服务器)架构。发卡系统软件为客户端,重点处理 SAM 卡的类型,以及用户卡的卡种、金额、有效期等信息;而加密机为服务端,时刻处理发卡系统的请求,进行密钥计算。

采用自顶向下、逐步扩大的设计思路。首先在加密机上统一分配好密钥的对应关系;其次,根据 SAM 卡分配好要加载的密钥和加载步骤,然后再分配好 CPU 卡的密钥加载和加载步骤。

1.4 基于国密算法的加密要求

从 AFC 系统得整体框架设计、票卡安全、密钥管理、发卡系统设计等方面信息,综合考虑重构制发 SAM 卡、制发 CPU 卡、用户卡复合消费和 TAC 验证等关键步骤。

1) 制发 SAM 卡:制发过程中,所有密钥均被密文传送,即:加密源头为加密机加密导出密钥密文,解密终点为 SAM 卡解密并存储密钥。被存储的密钥受 SAM 卡的物理保护。在此过程中,卡密钥均不能以明文方式暴露。制卡指令采用随机授权保护,任何人在没有取得密钥授权的前提下无法重复或伪造制卡。

2) 制发 CPU 卡:制发过程中,所有密钥均被密文传送,被存储的密钥受 CPU 卡的物理保护。在此过程中,卡密钥均不能以明文方式暴露。制卡采用卡号作为分散因子,实现一卡一密。

3) 用户卡复合消费:首先机具与卡片进行交互认证,此认证依赖 SM4 算法提供的安全性保护,确保双方身份和数据的一致性。同时,通过一卡一密、一次一密措施确保认证过程和交易结果的安全性。

4) TAC 验证:对交易结果的确认采用了 SM4 算法的 TAC 码,保障了后台清算过程中对交易可信性的确认。具体流程如图 3 所示。

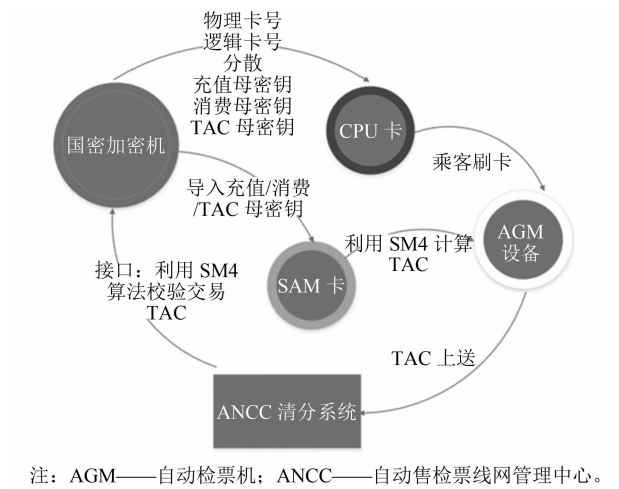


图 3 TAC 验证流程

1.5 应用效果测评

应用效果测评包括实验室测试和现场测试。实验室测试的目的是验证 SM4 算法应用后 AFC 系统的功能、性能和兼容性是否满足使用需求;现场测试的目的在于测试 AFC 系统 SM4 算法应用是否满足国家标准和系统运行需求。

1.5.1 实验室测试

实验室测试主要分为原型开发、环境搭建、功能测试、性能测试及兼容性测试几个步骤。主要测试内容如表 1 所示。

表 1 AFC 系统 SM4 算法应用实验室测试内容			
功能类别	测试项	测度目的	预期结果
功能性	国密 SAM 卡发卡	验证国密加密机中密钥 SM4 算法加解密 验证 SAM 卡种 SM4 密钥装载和使用	成功发售国密 SAM 卡
	国密 CPU 卡发卡	验证 CPU 卡中 SM4 密钥装载和使用	成功发售国密 CPU 卡
	国密 CPU 卡进出站	验证 CPU 卡消费中国密 SM4 算法的应用	国密 CPU 卡成功进出站
	ANCC 国密 TAC 验证	验证国密 CPU 卡消费的 TAC	国密 TAC 验证一致
兼容性	非国密 CPU 卡进出站	验证 CPU 卡消费非国密 3DES 算法的应用	非国密 CPU 卡成功进出站
	ANCC 非国密交易 TAC 验证	验证非国密 CPU 卡消费的 TAC	非国密 CPU 卡 TAC 验证一致
性能	国密和非国密 CPU 卡进出站	国密卡和非国密 CPU 卡进出站单次耗时小于 300 ms	单次进出站小于 300 ms

1.5.2 现场测试

现场测试的目的,除了验证采用 SM4 算法后 AFC 系统的功能、性能和兼容性外,还需验证各个子系统的连网连通功能,并测试各项业务能否按照要求完成自动连通处理。现场测试主要包括环境搭建(6 个站)、功能测试、性能测试、兼容测试及连通测试。主要测试内容如表 2 所示。

表 2 AFC 系统 SM4 算法应用现场测试内容			
功能类别	测试项	测度目的	预期结果
功能性/连通性	国密 SAM 卡发卡	验证国密加密机中密钥 SM4 算法加解密验证 SAM 卡中 SM4 密钥装载和使用	成功发售国密 SAM 卡
	国密 CPU 卡发卡	验证 CPU 卡中 SM4 密钥装载和使用	成功发售国密 CPU 卡
	国密 CPU 卡进出站	验证 CPU 卡消费中国密 SM4 算法的应用国密 CPU 成功交易连网上传	国密 CPU 成功进出站
	ANCC 国密 TAC 验证	验证国密 CPU 卡消费的 TAC	国密 TAC 验证一致
兼容性	非国密 CPU 卡进出站	验证 CPU 卡消费非国密 3Des 算法应用	非国密卡成功进出站
	ANCC 非国密 TAC 验证	验证非国密 CPU 卡消费的 TAC	非国密 CPU 卡 TAC 验证一致
性能	国密卡和非国密卡进出站	国密卡和非国密卡进出站耗时小于 300 ms	单次进出站小于 300 ms
	加密机 TAC 验证	加密机 TAC 验证小于 40 ms	单次验证 TAC 小于 40 ms

1.5.3 测试结果分析

实验室测试和现场测试结果如表 3 所示。

表 3 AFC 系统 SM4 算法应用测试结果			
测试法	非国密 CPU 卡 (3DES 算法)	SM4 CPU 卡 (实验室测试)	SM4 CPU 卡 (现场测试)
单次耗时/ms	进站	295.64	234.57
	出站	299.49	239.06

由表 3 的测试数据可以明显看出,在性能上,采用 SM4 算法的 CPU 卡单次刷卡时间比采用 3DES 算法的 CPU 卡的快 60 ms。这证明 SM4 算法在 AFC 系统上的应用更具优势。结合 SM4 算法的安全性考虑,可以说 SM4 算法更适用于 AFC 系统。

2 结语

通过实验室及现场的充分测试,验证了交易、票卡、密钥三个重要方面的数据安全性、业务连通

(下转第 203 页)

4) 与 PIS、PA 的接口改造:信号系统与 PIS 和 PA 间的基本协议保持不变。协议中有一项 train ID 参数,为适应不同编组列车的乘客信息告知,信号系统对不同编组列车分配不同的 train ID。PIS 和 PA 可每次依据收到的 train ID 参数来关联不同的车长信息,以呈现不同的列车信息。

3 经济效益分析

城市轨道交通的能耗主要包括固定设施能耗和移动能耗。固定设施能耗主要指地面设施,如通风空调、照明、电扶梯等的能耗;移动能耗又由列车牵引能耗和列车辅助能耗组成。列车牵引能耗占城市轨道交通总能耗的一半以上,降低牵引能耗可产生巨大的经济效益^[5]。

根据深圳地铁 9 号线的能耗统计数据,9 号线(含一期、二期)年总用电量为 19 710 万 kWh,其中牵引用电量为 7 884 万 kWh,占总用电量的 40%。平峰期列车开行对数占比约为 60%,故 9 号线平峰期日均牵引用电量约为 12.96 万 kWh。

根据 9 号线已运营阶段的能耗统计数据的预测计算结果为:在同一运行图运营情况下,平峰期若采用 3 节编组列车替代 6 节编组列车进行运营,节能率能达到 40%。即当 9 号线平峰期全部采用 3 节编组列车时,日均节电量约为 5.18 万 kWh。每度电按照 0.7 元计算^[6],全年可节省 1 323.49 万元。

(上接第 199 页)

性。通过对测试数据的统计分析,证明了在 AFC 系统的整个交易业务链条中,国密算法的功能和性能满足 AFC 系统的要求,可以替换国外算法。

目前,核心技术自主可控是国内技术发展的大趋势。城市轨道交通行业更应采用更安全、效率更好的国密算法。本文方案在不改变目前 AFC 系统密钥体系的前提下,通过增加支持 SM4 算法的应用,并考虑分阶段替换的方式更新票卡密钥,最终实现国外密钥卡的逐步自然淘汰。

参考文献

- [1] 杨旭方.一款基于 89C51 单片机实现的非接触式 IC 卡 AFC 系统[J].电子测试,2014(8):52.
- [2] 杨毅,车高峰.非接触式 IC 卡读卡器的二次开发[J].电脑与

4 结语

采用灵活编组运营模式可以在平衡运营能力的同时,降低运营成本,符合运营部门的客观需求。本文从灵活编组的功能需求入手,分析联挂和解编的功能需求和实现方式,并从经济效益角度论证灵活编组方式具备良好的经济效益。灵活编组技术已逐渐成熟,未来,灵活的编组运营与全自动运行技术^[7]结合,在正线混编运营、列车联挂救援等运营场景下将得到更多的应用。

参考文献

- [1] 唐玉川,马保仁.城市轨道交通灵活编组运营组织研究[J].铁道工程学报,2014(8):96.
- [2] 潘丽莎,龚玲,冒玲丽.城市轨道交通车辆关键系统可靠性研究[J].中国铁路,2012(7):80.
- [3] 赵文凤,梁永华.深圳龙华储能式低地板有轨电车项目日常维保执行模式解析[J].技术与市场,2018(10):177.
- [4] 蒋晓东,刘厚林,尚江傲.宁波轨道交通 1 号线一期工程车辆辅助供电系统[J].电力机车与城轨车辆,2013(1):25.
- [5] 唐玉川,马保仁.城市轨道交通灵活编组运营组织研究[J].铁道工程学报,2014(8):96.
- [6] 赵家炜,刘婧婧.地铁列车在线联挂、解编功能分析[J].城市轨道交通研究,2012(8):152.
- [7] 王冬海,黄荣光.列车灵活编组在城市轨道交通全自动运行线路中的应用[J].城市轨道交通研究,2019(增刊2):102.

(收稿日期:2021-01-28)

电信,2013(10):29.

- [3] 高峰.浅谈信息加密技术在网络安全中的运用[J].黑龙江教育学院学报,2014(3):193.
- [4] 吕迪,贾志洋.常用数据加密技术的对比研究[J].网络安全技术与应用,2014(2):35.
- [5] 王卓人.智能卡大全——智能卡的结构、功能、应用[M].3版.北京:电子工业出版社,2002:112-118.
- [6] 杨振野.IC卡技术及其应用[M].北京:科学出版社,2006:54-56.
- [7] 陆永宁.非接触 IC 卡原理与应用[M].北京:电子工业出版社,2006:340-352.
- [8] 赖明.建设事业 IC 卡应用技术与发展[M].北京:中国建筑工业出版社,2003:260-263.
- [9] (美)BRUCE S.应用密码学[M].北京:机械工业出版社,2007:136-140.

(收稿日期:2021-03-20)