

车载排放终端密码功能测试方法研究及应用

李新福¹, 陈圳艳², 吴超², 柯馨沁²

(1. 重庆经济技术开发区建设服务中心, 重庆 400000; 2. 招商局检测车辆技术研究院有限公司, 重庆 401329)

摘 要:基于 GB 17691—2018 要求, 针对车载排放终端密码功能提出一套可行、准确的测试方案, 并进行应用验证。

关键词:GB 17691—2018; 车载排放终端; 密码功能

中图分类号:U463. 6; U467. 4

文献标志码:A

文章编号:1006-3331(2022)05-0052-03

Research and Application of Cryptographic Function Test Method for Vehicle Emission Terminal

LI Xinfu¹, CHEN Zhenyan², WU Chao², KE Xinqin²

(1. Chongqing Economic and Technological Development Zone Construction Service Center, Chongqing 400000, China;

2. China Merchants Testing Vehicle Technology Research Institute Co., Ltd., Chongqing 401329, China)

Abstract:Based on the requirements of GB 17691—2018, this paper proposes a feasible and accurate test scheme for cryptographic function of vehicle emission terminal and does the application verification.

Key words:GB 17691—2018; vehicle emission terminal; cryptographic function

随着汽车智能化和网联化进程的加快, 车载终端作为汽车内外通信的桥梁, 其信息安全性越来越受到关注^[1]。目前, 各种车辆搭载的车载终端大部分欠缺有效的信息安全防护^[2], 为了保障车载终端的良性发展, 需进一步分析其安全威胁和安全需求, 探究相关信息安全问题和测试方法^[3-4]。GB 17691—2018《重型柴油车污染物排放限值及测量方法(中国第六阶段)》(以下简称国六)^[5]在附录 Q. 4“安全策略”的第一个方面对保护数据安全所采用的密码算法和硬件提出了要求。由于目前对此还没有标准的测试方法, 因此为评价车载排放终端的该功能是否达到规定要求, 本文对该终端密码功能的测试方法进行研究和应用。

1 终端密码功能要求

文献[5]附录 Q. 4 要求:“车载终端应提供技术可行的安全策略, 保证产品各种性能和功能处于安全范围内”, 并且规定从五个方面来实现, 其中一个方面是“车载终端存储、传输的数据应是加密的, 应采用非

对称加密算法, 可使用国密 SM2 算法或者 RSA 算法, 并且需要采用硬件方式对私钥进行严格保护”。

国密 SM2 非对称加密算法的密钥分为公钥和私钥两部分, 其中公钥可以进行加密、签名验证, 私钥可以进行解密和数字签名, 很好地解决了对称密码算法中加密和解密使用相同密钥(即不分公钥、私钥)的密钥管理难题, 从而能够保证车载终端信息的完整性和准确性^[6-7]。本文所研究的车载终端, 据其产品介绍采用了国密 SM2 非对称加密算法和安全芯片加密。因此本文构建了终端 SM2 算法密码功能测试系统, 通过测试终端的数据签名验签过程来验证其采用 SM2 非对称加密算法的符合性, 通过测试总线数据内容来验证其所采用的硬件是否对私钥进行了严格保护。

2 测试系统构建

该车载排放终端密码功能测试系统主要由算法验签模块、示波器解码模块组成, 从算法测试、总线测

收稿日期:2022-02-09。

第一作者:李新福(1986—), 男, 硕士; 工程师; 主要从事机电一体化方面的研究工作。E-mail:506589939@qq.com。

试两个层面测试验证算法和芯片的真实性、有效性和可靠性^[8-9]。系统架构如图1所示。

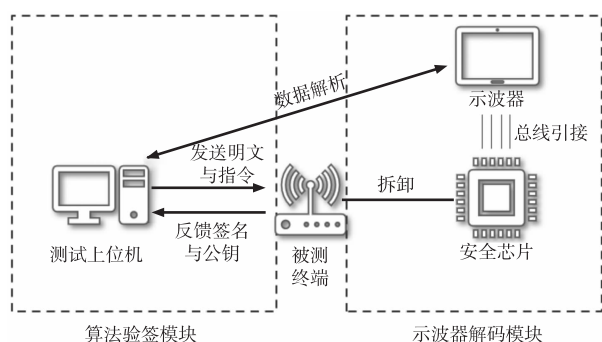


图1 测试系统总体框架

3 测试过程及结果

3.1 国密 SM2 算法测试

1) 将厂家委托的车载终端通过 Uart 串口连接至图1中的测试上位机,并启动上位机中的算法测试工具,如图2所示,执行国密 SM2 签名验证测试初始化,判断车载终端的 Agent 程序是否正常运行。



图2 车载终端安全芯片算法测试工具

2) 测试过程中,算法测试工具将产生随机明文,依次发送给车载终端 Agent 程序并通过车载终端中的加密芯片进行签名,Agent 程序将签名后的数据反馈给算法测试工具。

3) 算法测试工具对签名后的明文数据进行国密 SM2 算法验签,参加验签的数据正确率不低于 99%则认为符合标准要求。本次测试中,对 100 条明文数据进行了 SM2 算法验签,验签的数据正确率为 100%,与标准要求相符。说明该车载终端存储、传输的数据是采用国密 SM2 算法加密的。

3.2 加密芯片测试

1) 将上述所测终端的加密芯片总线引脚连接至

图1中的示波器,同时给示波器分配 IP 地址。

2) 使用上位机算法测试工具产生一组随机的明文,并通过车载终端的 Uart 串口发送至终端 Agent 程序进行签名。

3) 使用示波器对加密芯片所接 SPI 总线进行电平采集,如图3所示。解析下发明文数据至返回签名数据全过程中的总线数据,并与下发和接收的数据进行比对。

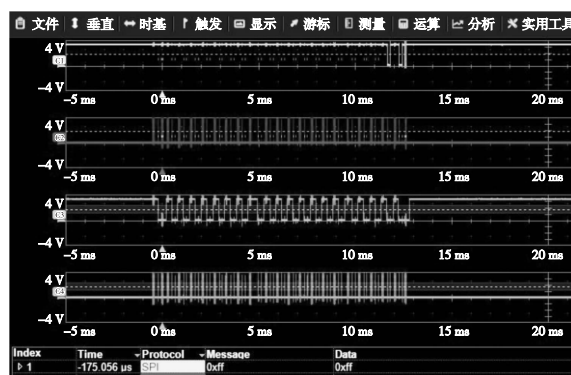


图3 示波器电平采集

4) 如果总线数据中包含有 Agent 程序通过车载终端 Uart 串口返回的公钥、明文、用户 ID 及签名值,则可以认定签名是由安全芯片完成的,符合标准要求。本次测试中,示波器基于 MISO、MOSI 引脚电平解析到的总线数据包含有公钥、明文、用户 ID 及签名值,且与 Agent 程序通过车载终端 Uart 串口返回的数据一致,与标准要求相符,如图4所示。说明该车载终端采用加密芯片的硬件方式实现了数字加密、数字签名和对私钥的严格保护。

检测记录	2022-07-20 13:24:50	删除	清空
SM2验签信息 (第1次测试)			
事项	结果	操作	
第1次测试	成功	查看	验签明文 e1225ff51766c89e7c4e
第2次测试	成功	查看	验签用户ID 313233343536
第3次测试	成功	查看	验签公钥 fe341f86cc87c1a77c9d0869c658af36e9b7
第4次测试	成功	查看	验签签名R 42588bd68889dee6b363
第5次测试	成功	查看	验签签名S dbc61918f4ae

图4 总线数据解析

4 结束语

本文构建了车载排放终端密码功能测试系统,从国密 SM2 算法测试、加密芯片测试两个方面检验了车载排放终端的信息安全防护能力。可为建立可行、明确的测试流程,保证测试结果的一致性和准确性提供参考。

参考文献:

- [1] 罗瓊路,方强. 车载终端信息安全威胁与防范[J]. 电信网技术,2016(6):35-39.
- [2] 韩艳艳,贺可勋,王长园. 国六车载终端信息安全检测方法研究[C]//中国汽车工程学会. 2019 中国汽车工程学会年会论文集. 北京:机械工业出版社,2019:765-768.
- [3] 贾世准,麦松涛,李冬,等. 智能网联汽车软件安全测试关键技术研究[J]. 信息安全研究,2018,4(11):1025-1028.
- [4] 王玮. 车辆 T-BOX 系统安全测试和评价[J]. 信息通信技术 & 政策,2018(1):85-88.
- [5] 生态环境部,国家市场监督管理总局. 重型柴油车污染物排放限值及测量方法(中国第六阶段):GB 17691—2018[S]. 北京:中国环境科学出版社,2018:358.
- [6] 中华人民共和国国家质量监督检验检疫总局,中国国家标准化管理委员会. 信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分:数字签名算法:GB/T 32918.2—2016[S]. 北京:中国标准出版社,2017:1-2.
- [7] 中华人民共和国国家质量监督检验检疫总局,中国国家标准化管理委员会. 信息安全技术 SM2 椭圆曲线公钥密码算法 第 4 部分:公钥加密算法:GB/T 32918.4—2016[S]. 北京:中国标准出版社,2017:1-2.
- [8] 钱国平,夏宝华,武锡斌,等. 符合国六排放监控要求的车载终端设计[J]. 电子技术与软件工程,2021(1):68-72.
- [9] 陈华,习伟,范丽敏,等. 密码产品的侧信道分析与评估[J]. 电子与信息学报,2020,42(8):1836-1845.

欢迎刊登广告

《客车技术与研究》创刊于 1979 年,国内外公开发刊,双月刊,国内邮发代号:78-115,国外发行代号:BM 2856,中国标准连续出版物号:ISSN 1006-3331;CN 50-1109/U。

本刊主要发行至客车及其配套件企业、科研单位和大专院校,深受广大读者的欢迎和好评。多年来,本刊在宣传和推广客车配件和设备等新产品、提高产品知名度、促进产品销售以及传播信息等方面发挥了重要作用,已成为客车主机厂选择配套件及设备的主要参考资料。

为了使您的产品能快速赢得市场,提高企业的经济效益,我们竭诚欢迎客车(汽车)及相关企业在本刊刊登广告。

详情咨询:023-62653044。