DOI:10.13878/j.cnki.jnuist.2022.05.005

李敏[1,2]　陈付龙[1]　庞辉[3]

基于国密算法 SM4 的车载 PEPS 和 EMS 安全认证方法研究

摘要

随着 ICV(智能网联汽车)产业的快速发展,车与人、车与车以及车与外部环境的数据交换成为常态,汽车安全受到严重威胁,研究汽车安全认证方法则显得至关重要.车载 PEPS(无钥匙进入及启动系统)和 EMS(发动机管理系统)的安全认证决定整车安全性能,是保证汽车安全运行的前提条件.目前业界广泛采用 128 bits AES 算法实现 PEPS 和 EMS 的安全认证,而由于 AES 密钥生成和密钥调度算法较国密算法 SM4 复杂,加解密时间较长,且算法实现的代码量较大,占用过多的 MCU 资源,因此,本文提出将国密 SM4 算法应用于车载 PEPS 和 EMS 的安全认证,缩短加解密时间,有效提高数传效率,同时采用高级语言实现该算法并移植到国产 MCU GD32F103,实现产品国产化,降低成本.将国密算法 SM4 进行推广,为 ICV 安全认证提供研究基础.

关键词

国密算法 SM4;无钥匙进入及启动系统(PEPS);发动机管理系统(EMS);安全认证

中图分类号 TP274

文献标志码 A

收稿日期 2022-01-24

资助项目 国家自然科学基金(61972438);安徽省高校优秀青年骨干人才国内访学研修项目(gxgnfx2020142)

作者简介

李敏,男,副教授,研究方向为汽车智能技术、信息安全.qingchang2014@126.com

1 安徽师范大学 计算机与信息学院,芜湖,241003

2 芜湖职业技术学院 信息与人工智能学院,芜湖,241006

3 埃泰克汽车电子(芜湖)有限公司,芜湖,241006

0 引言

随着智能网联汽车(Intelligent Connected Vehicle,ICV)产业的快速发展,汽车安全认证越来越被业界所重视[1].而无钥匙启动及进入系统(Passive Entry Passive Start,PEPS)是汽车关键部件之一,它不仅对用户进行身份认证,而且也决定了汽车发动机能否正常起动,是保证汽车安全运行的前提条件.车载 PEPS 系统主要包括智能钥匙、线圈、集成 IMMO 基站的 PEPS 等部件,PEPS 通过 SPI 总线与 IMMO 基站连接,并通过 CAN 总线与发动机管理单元(Engine Management System,EMS)连接,系统如图 1 所示.根据车载 PEP 和 EMS 通信机制,业界广泛采用 128 bits AES 加密算法或 XTEA 算法实现 PEPS 和 EMS 的动态加密安全认证.由于 128 bits AES 算法密钥生成和密钥调度算法较国密算法 SM4 复杂,加解密代码量较大,数据加密时间长,消耗过多的 MCU(微处理器)资源,影响数传效率.

目前,SM4 算法应用在车载设备 CAN 通信加密场合较少,特别是将 SM4 算法移植到车规级嵌入式处理器并验证其运行效率的文献也不多[2],多数文献是针对 CAN 总线提出安全认证机制,如文献[3]根据 CAN 总线特性提出一种安全认证方法抵御网络入侵,文献[4]提出了类似 TESLA 协议的具有消息认证的 CAN 总线安全认证机制,文献[5]提出了基于 EVITA-HSM 消息认证的安全认证机制.为有效防止 CAN 总线的重放攻击、网络入侵等汽车安全问题,探索采用国密算法 SM4 取代 128 bits AES 算法实现 PEPS 和 EMS 安全认证具有重要的实用价值[6].国密算法 SM4 是我国自主研发的商用密码体系,它相比 128 bits AES 算法具有更强的安全性,且密钥调度算法简单,计算量少,从而加快运算速度[7-9].目前国外车规级 MCU 严重短缺,且价格昂贵,因此在保证系统稳定性和安全性前提下,使用国产 MCU,可以不受外部环境制约,降低 PEPS 生产成本,实现车载 PEPS 国产化.

1 PEPS 系统硬件架构

PEPS 系统硬件由 MCU、ATA5785 RF 接收电路、电源输出电路、开关量采集电路、低频天线驱动电路、CAN 通信电路、ESCL 通信电路等组成.其中,电源输出模块连接继电器组,提供发动机 ACC、IGN 点

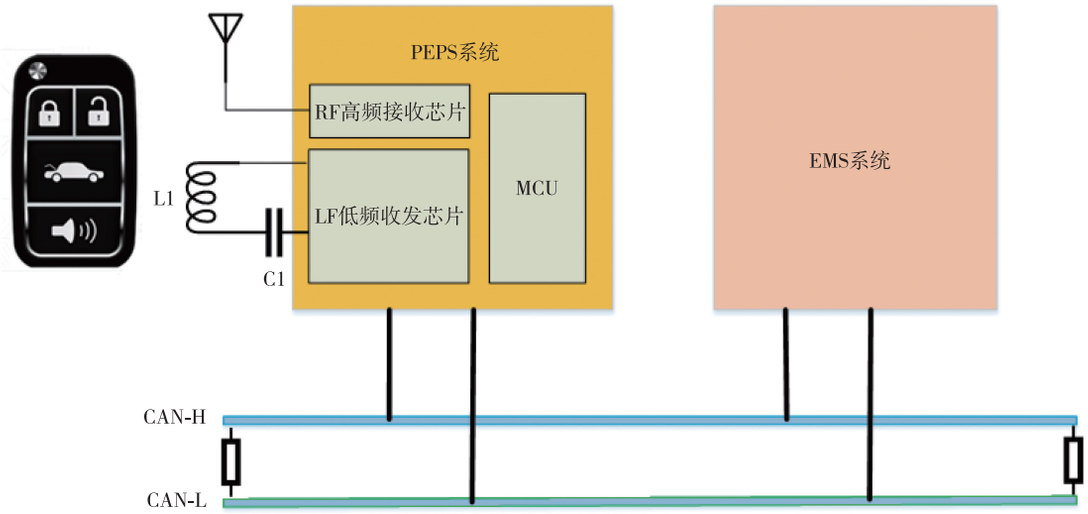

图 1　PEPS 系统框图

Fig. 1　Block diagram of PEPS system

火信号、Cranking 信号,ESCL 提供电子转向柱锁电源和控制信号,CAN 总线连接 EMS,PEPS 开关量采集信号包含点火按钮开关、驾驶门、副驾驶门、后备箱微动开关,低频天线驱动连接主副驾驶门把手天线、行李箱外部天线以及车内前后部天线等.PEPS 电气原理如图 2 所示,PEPS 上电找钥匙时序如图 3

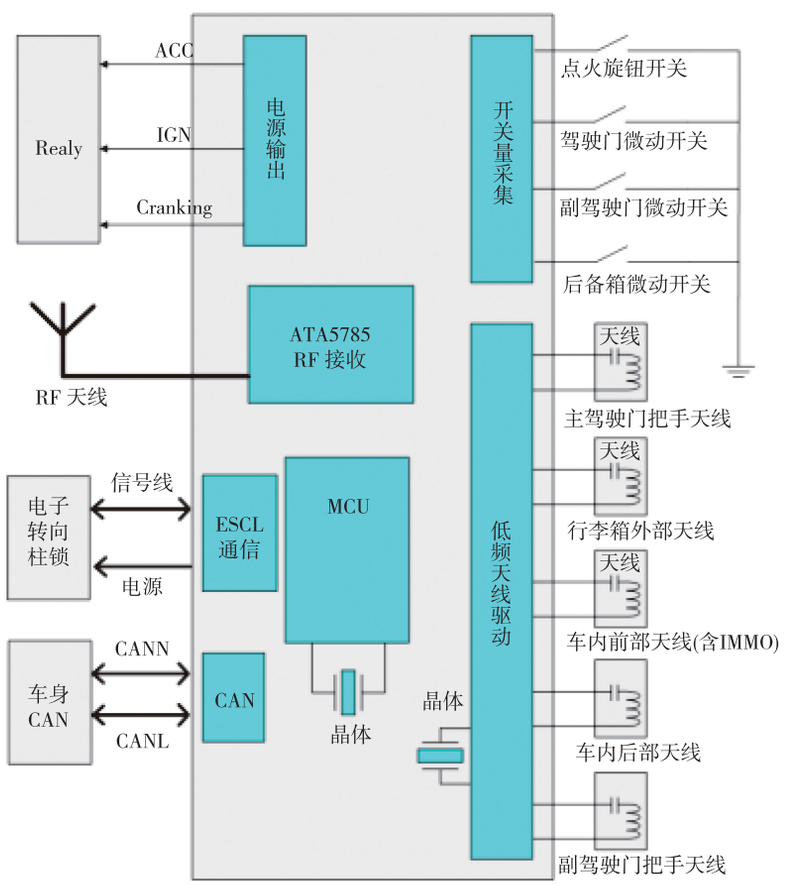

图 2　PEPS 系统电气原理

Fig. 2　Electrical schematic diagram of PEPS system

所示.

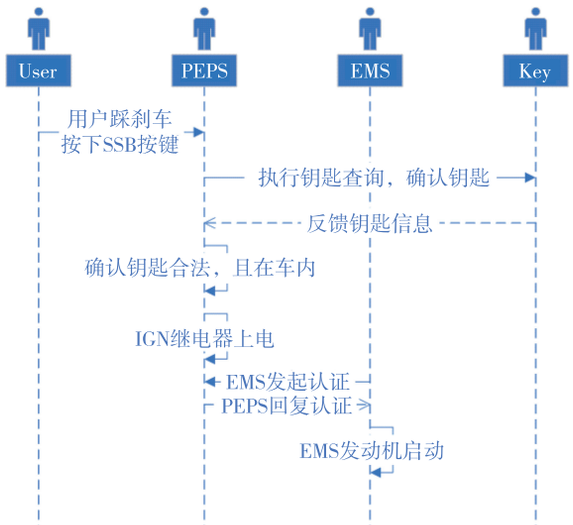

图 3　PEPS 上电找钥匙时序

Fig. 3　PEPS power-on time sequence to find the key

2　PEPS 和 EMS 的安全认证过程

车载 PEPS 与 EMS 通信采用 CAN 2.0B 协议,帧结构中包含 11 位 ID 标识符.PEPS 与 EMS 通信采用双向两级认证,双向是指 EMS 通过加密算法发送密文至 PEPS,PEPS 收到正确的加密数据后回复 EMS,两级是指第一级为钥匙与 PEPS 系统的认证,第二级为 PEPS 与 EMS 认证.在第二级认证中,PEP 和 EMS 共享 SK 和 PIN,其中 SK 为 128 bits 数据,PIN 为 32 bits 数据,SK 和 PIN 通过机器学习存放到 PEPS 和 EMS 的 EEPROM 中.第二级认证过程具体如下:

1)PEPS 控制 IGN 继电器使能,并等待 EMS 发送认证信息.

2)EMS 初始化后以每隔 150 ms 发送 DATA 至 PEPS.由于 CAN 报文的一帧有效数据为 8 bytes,DATA 包含加密的 4 bytes PIN 和 4 bytes 的随机数,EMS 在 2 s 内未接收到 PEPS 的应答信息,则本次认证失败.

3)PEPS 接收到 EMS 发送的 DATA 后,采用加密算法和 SK 对 DATA 进行解密,获得 PIN 数据与 EEPROM 中的 PIN 匹配,PEPS 发送认证信息至 EMS,该信息包含加密的 4 bytes PIN 和 4 bytes 随机数.如果 PEPS 接收到的 PIN 与本地 EEPROM 存储中的 PIN 不匹配,PEPS 将发送 8 byte 的 0xFF.

4)EMS 接收到认证信息后,采用加密算法和 SK 对 DATA 进行解密,判断 PIN 码和 EEPROM 存储的 PIN 是否匹配,如果匹配,则双向认证通过.反之,将发送 8 bytes 的 0xFF,其双向认证信息如表 1 所示.

3　SM4 算法原理

通过分析 PEPS 和 EMS 认证过程,并依据 CAN 报文数据结构,提出基于国密算法 SM4 实现数据加解密.SM4 是国家密码管理局于 2012 年发布的商用密码体系,是一种对称加密算法,算法结构为非平衡 Feistel,密钥长度 128 位,采用分组且 32 轮非线性迭代加密,生成的密明文长度一致[10].根据文献[10]的加密算法得出:

1)通过 32 轮迭代运算后将数据反序得出密文 $(X_{35},X_{34},X_{33},X_{32})$:

$X_{i+4}=F(X_i+X_{i+1},X_{i+2},X_{i+3},rk_i)=X_i\oplus T(X_i\oplus X_{i+1}\oplus X_{i+2}\oplus X_{i+3}\oplus rk_i)$, $i=0,1,2,\cdots,31$,

$(Y_0,Y_1,Y_2,Y_3)=R(X_{32},X_{33},X_{34},X_{35})=(X_{35},X_{34},X_{33},X_{32})$.

2)T 变换与 L 变换:

在上述迭代运算中,所运用的 T 变换由 s,L 变换得出:

$(b_0,b_1,b_2,b_3)=(Sbox(a_0),Sbox(a_1),Sbox(a_2),Sbox(a_3))$,

$C=L(B)=B@(B\lll 2)@(B\lll 10)@(B\lll 18)@(B\lll 24)$,

其中 (a_0,a_1,a_2,a_3) 为 128 位数据输入,(b_0,b_1,b_2,b_3) 为 128 位数据输出.

3)轮密钥 rk_i 生成:

$rk_i=K_i\oplus T'(CK_{i+1}\oplus CK_{i+2}\oplus CK_{i+3}\oplus CK_{i+4})$,

$i=0,1,2,\cdots,31$.

表 1　双向认证信息

Table 1　Two-way authentication information

MESSAGE	SEND	RECEIVE	ID	DATA FEILED							
				Byte0	Byte1	Byte2	Byte3	Byte4	Byte5	Byte6	Byte7
EMS_DATA	EMS	PEPS	0x111	RN(High)	RN	RN	RN(Low)	PIN(High)	PIN	PIN	PIN(Low)
PEPS_DATA	PEPS	EMS	0x222	RN(High)	RN	RN	RN(Low)	PIN(High)	PIN	PIN	PIN(Low)

4 PEPS 系统软件

PEPS 系统软件由主程序、*T* 变换、随机数生成、轮密钥、SM4 加解密、CAN 发送和接收程序等构成.主程序实现 PEPS 系统时钟配置、GPIO 初始化、高低频芯片初始化、CAN 初始化、CAN 发送和接收、ADC 初始化、DMA 初始化、定时器初始化等.如图 4 所示.

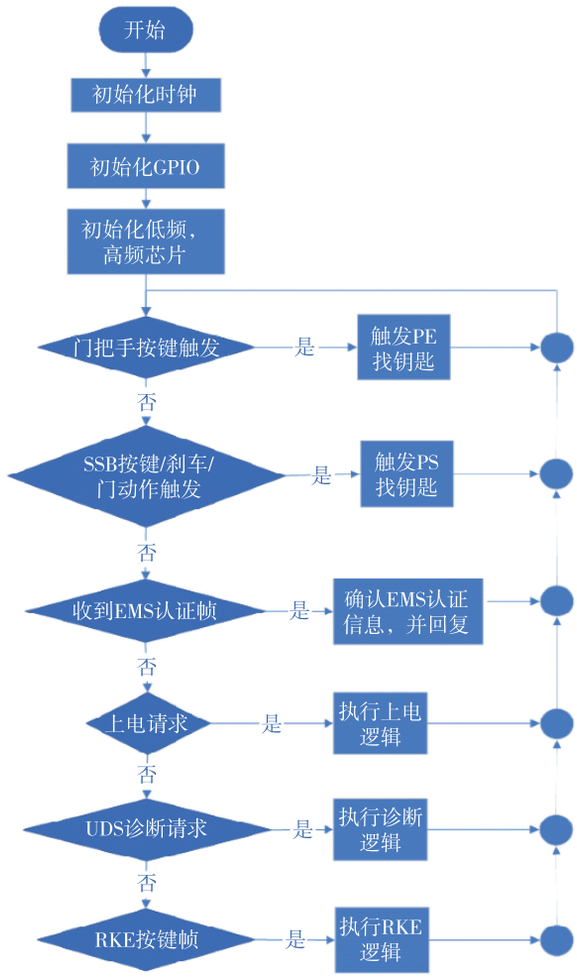

图 4 PEPS 系统主程序流程

Fig. 4 Flow chart for the main program of the PEPS system

5 实验结果验证

分别将 128 bits AES 算法和国密 SM4 算法移植到 32 位 MCU GD32F103,分析两种算法的运行效率.依据产品标准,PEPS 系统与 EMS 的安全认证需满足三项指标[11]:第一,数据的实时性,即保证 PEPS 和 EMS 需在规定时间内完成数传,行业中规定 30 ms 以内;第二,节点身份的合法性,即保证数据是由 PEPS 节点发送的;第三,数据的正确性,即保证 PEPS 发送和 EMS 接收的数据内容一致.

本系统采用 GD32F103 为核心处理器的嵌入式系统板模拟 PEPS 和 EMS 节点,使用 Kvaser CAN 分析仪、具备 CAN 解析功能的 ZLG 的 ZDS2024 Plus 数字示波器,Saleae Logic8 逻辑分析仪等设备开展测试.首先,基于 PC 端的 C-Free5 IDE 平台设计并调试国密 SM4 算法,然后,将该算法移植到主频为 108 MHz 的 MCU GD32F103,在 KEIL 开发环境中运行程序并调试,加解密测试程序如图 5—8 所示.为获取

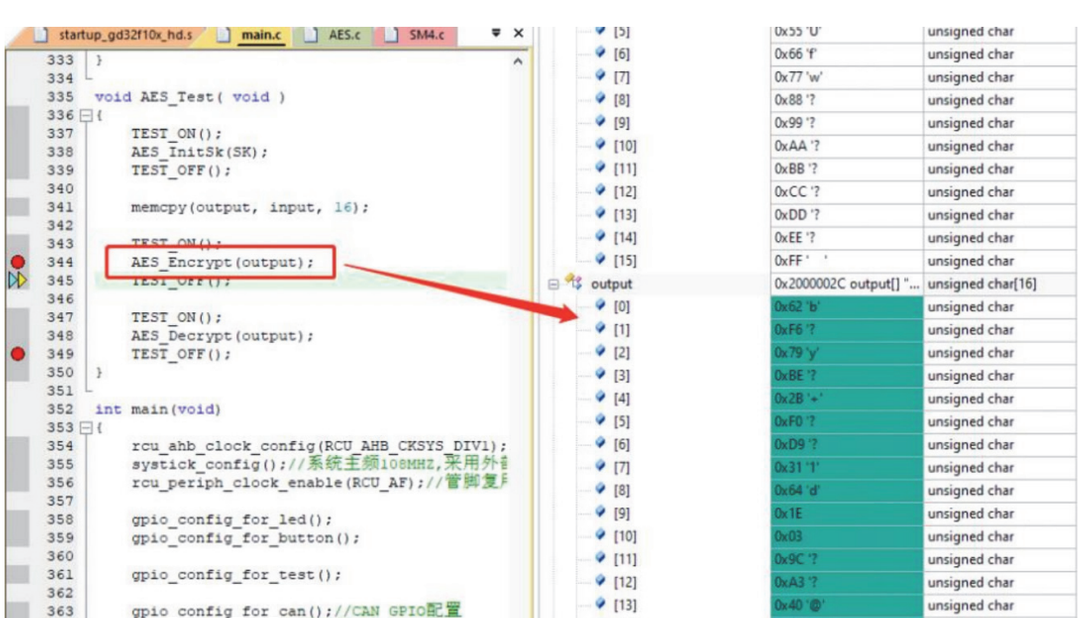

图 5 128 bits AES 加密程序

Fig. 5 128 bits AES encryption program

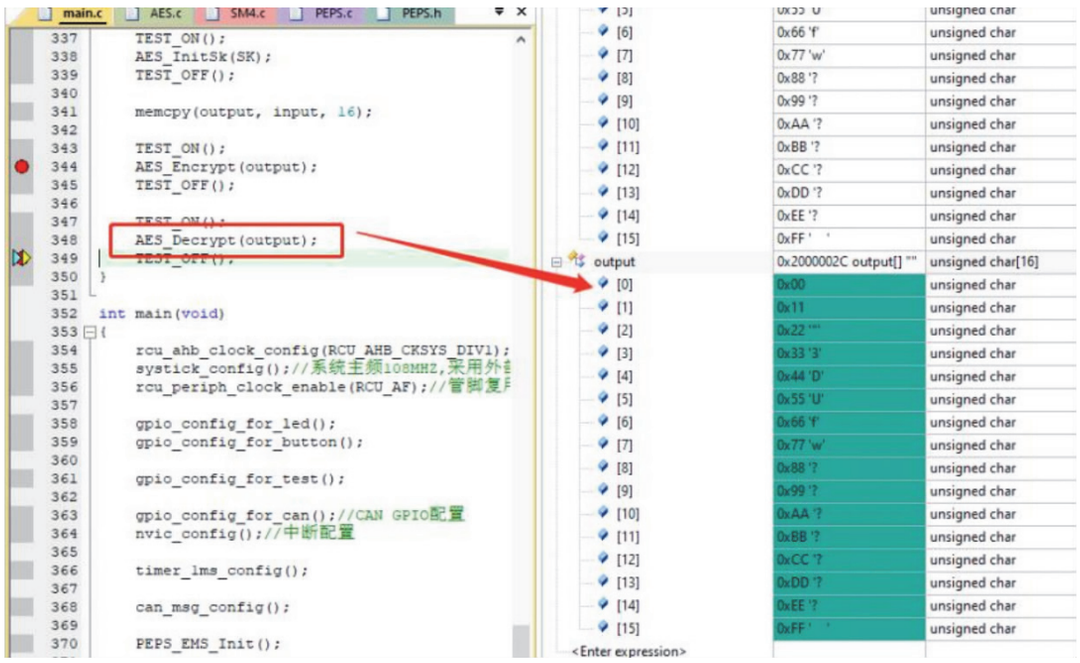

图 6　128 bits AES 解密程序

Fig. 6　128 bits AES decryption program

图 7　SM4 加密程序

Fig. 7　SM4 encryption procedure

SM4 算法中的加解密时间,将 MCU 的 GPIO 口设置为输出模式,通过 GPIO 口电平翻转策略判断,并使用逻辑分析仪捕获 IO 电平状态,通过 Saleae 平台测试两种算法的加解密时间.采用国密 SM4 算法,加密时间为 57.75 μs,解密时间为 57.75 μs,采用 128 bits AES 算法加密时间为 0.906 5 ms,解密时间为 0.141 ms,上述数据表明 AES 算法的加密时间接近 SM4 算法的 15 倍,解密时间接近 SM4 算法的 3 倍,显然 SM4 有效提高了加解密效率和缩短数传时间.

5.1　SM4 加密实时性验证

要保证车载 PEPS 和 EMS 的 CAN 通信实时性要求,按照 EMS 规范,采用 SM4 加密算法的函数调度和加密算法时间之和 T' 必须小于 EMS 规范时间 T,即 $T' \leqslant T$[12-13].为了验证 CAN 总线的实时性,通过 Kvaser CAN 分析仪和上位机 CANKIING 平台循环发送定量数据,观察发送方、接收方时间戳,在相同的

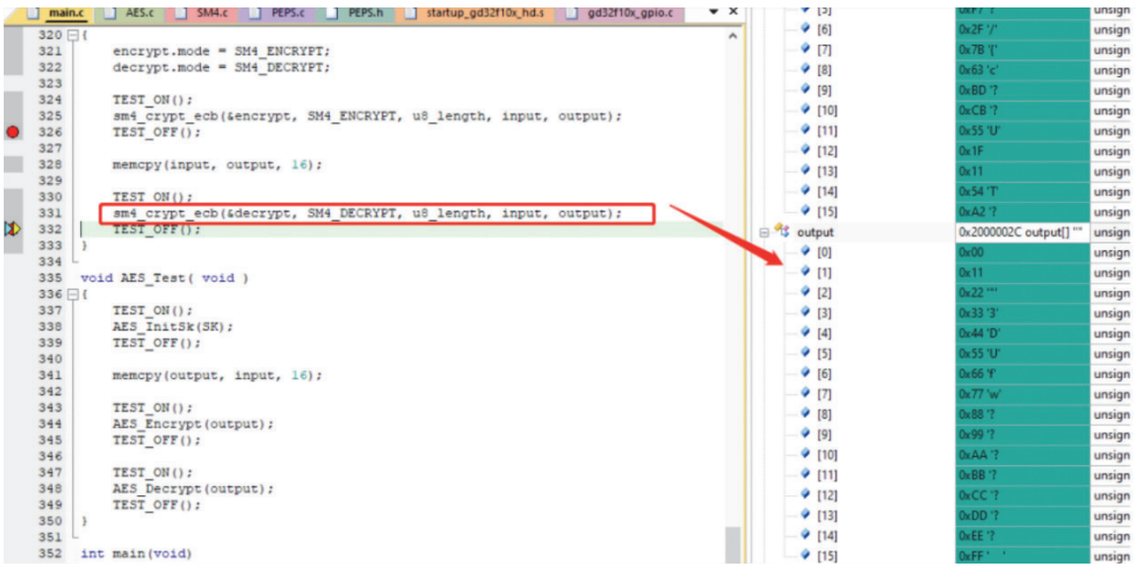

图 8　SM4 解密程序

Fig. 8　SM4 decryption procedure

时间序列下,记录 EMS 发送的起始时间和 PEPS 接收数据时间,从图 9 和表 2 中可以得出基于 SM4 算法的函数调度和加密时间之和远小于 EMS 规范中的 30 ms,完全满足系统实时性要求.

5.2　节点身份合法性和数据正确性验证

系统设置 EMS 节点的发送 CAN ID 为 0X111,PEPS 节点的发送 CAN ID 为 0X222,EMS 生成随机数 0X11223344,将 PIN 码、随机数和常量构成的 16 bytes 明文加密,提取密文中的 4 bytes 数据 0XCC66DCC6 和随机数 0X11223344 构成 8 bytes 的 CAN 报文通过总线发送至 PEPS,PEPS 收到 CAN 报文后,将收到的 4 bytes 随机数,以及自身 EEPROM 中存储的 4 bytes PIN 码,使用 16 bytes 的 SK 通过 SM4 加密之后,发现前 4 bytes 与 CAN 报文的后 4 bytes 一致,则表明第一次认证成功,PEPS 再生成随机数 0X55667788,按照 SM4 算法加密明文,同理将密文的前 4 bytes 0X42B14E78 以及随机数 0X55667788 发送到 EMS 端,EMS 收到数据后同理

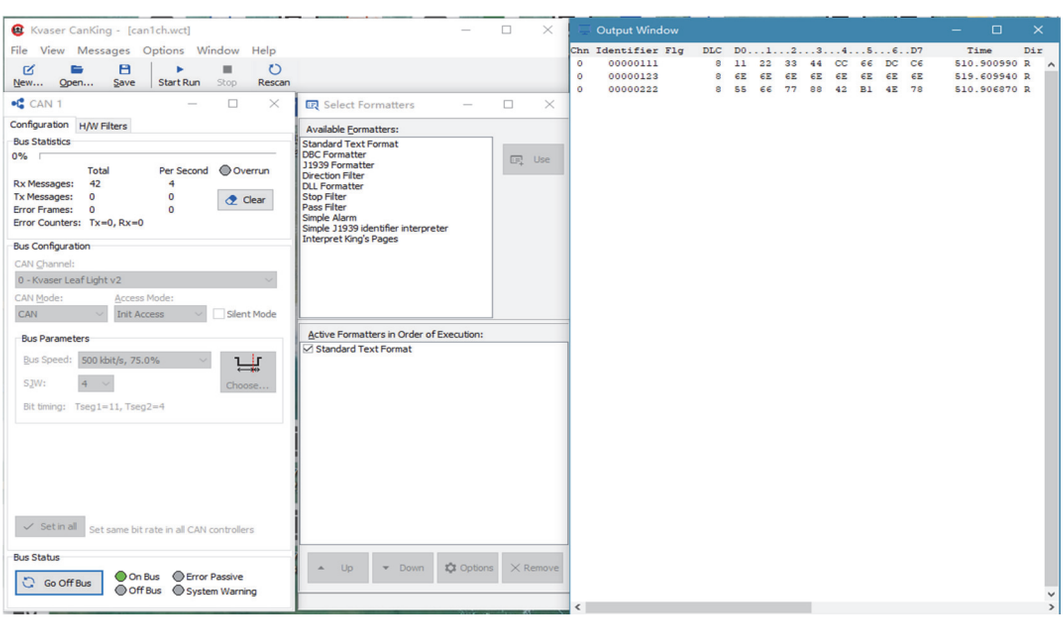

图 9　PEPS 和 EMS 接发时间戳

Fig. 9　PEPS and EMS receiving and sending time stamps

表 2 加解密时间

Table 2 Encryption and decryption timetable

EMS 发送数据时间/s	PEPS 接收数据时间/s	函数调度和加密算法时间之和 T'/ms	规范标准 T/ms	$T'<T$
510.900 990	510.906 870	5.88	30	是
535.338 320	535.344 290	5.97	30	是
549.502 710	549.506 810	4.10	30	是

加密,确认密文的前 4 bytes 与 PEPS 发送的 CAN 报文后 4 bytes 比对一致,也表明认证成功,验证数据如表 3 所示.

6 结论

本文基于国密算法 SM4,设计了车载 PEPS 和 EMS 的 CAN 通信安全认证系统,其关键方法总结如下:

1)分析 128 bits AES 算法在车载 PEPS 和 EMS 的 CAN 通信加密原理.由于 AES 密钥生成和密钥调度算法较 SM4 复杂,加解密时间较长,加解密代码量大,因此,将国密 SM4 算法应用于 PEPS 和 EMS 的安全认证,缩短加解密时间,有效提高数传效率.

2)搭建 PEPS 和 EMS 通信测试平台,采用 32 位 108 MHz GD32F103 作为 PEPS 的核心处理器,接口电路包括 GPIO、AD、CAN、SPI 等,基于 KEIL 集成开发环境设计 PEPS 的主程序、随机数生成、SM4 加解密、CAN、SPI 等函数.

3)将 SM4 算法移植到 MCU GD32F103,比较 128 bits AES 算法和 SM4 算法的运行效率,通过 Saleae Logic8 逻辑分析仪测试 SM4 的加解密时间远低于 128 bits AES 算法,且代码量小,并基于 Kavase CANKing 平台验证 PEPS 和 EMS 的节点合法性、数据正确性等指标,为 ICV 安全认证方案提供研究基础.

4)对 PEPS 和 EMS 通信的 CAN 明文进行加密处理,有效防止重放攻击、网络入侵等汽车安全问题.

表 3 PEPS 身份合法性和数据正确性验证

Table 3 Verification of PEPS identity legitimacy and data correctness

帧类型	EMS 和 PEPS 节点发送明文	密文	总线数据
标准帧	RN:0X11223344 PIN:0XF1B08A34 CC 常量:0XC136FABB7BCD3BF3	0XCC66DCC6FA3DFA57A6E0468AE8BC8D9F	RN:0X11223344 密文:0XCC66DCC6
	RN:0X23456789 PIN:0XF1B08A34 CC 常量:0XC136FABB7BCD3BF3	0XAEBC417D18934B36908F2C2C78AD80C4	RN:0X23456789 密文:0XAEBC417D
	RN:0X55667788 PIN:0XF1B08A34 CC 常量:0XC136FABB7BCD3BF3	0X42B14E78231d9d19d26eafc32799a703	RN:0X55667788 密文:0X42B14E78
	RN:0XABCDEF01 PIN:0XF1B08A34 CC 常量:0XC136FABB7BCD3BF3	0X8A440E20abace4489ad90ad7a152ff	RN:0XABCDEF01 密文:0X8A440E20

参考文献

References

[1] 朱立民,李仁发.一种基于 AES-CCM 算法的安全车载 CAN 网络协议[J].汽车技术,2018(8):54-59
ZHU Limin,LI Renfa.A secure in-vehicle CAN network protocol based on AES-CCM algorithm[J].Automobile Technology,2018(8):54-59

[2] 罗峰,胡强,刘宇.基于 CAN-FD 总线的车载网络安全通信[J].同济大学学报(自然科学版),2019,47(3):386-391
LUO Feng, HU Qiang, LIU Yu. Secure communication method for in-vehicle network based on CAN-FD bus[J]. Journal of Tongji University (Natural Science),2019,47(3):386-391

[3] Woo S,Jo H J,Lee D H.A practical wireless attack on the connected car and security protocol for in-vehicle CAN[J].IEEE Transactions on Intelligent Transportation Systems,2015,16(2):993-1006

[4] Groza B, Murvay S. Efficient protocols for secure broadcast in controller area networks[J].IEEE Transactions on Industrial Informatics,2013,9(4):2034-2042

[5] Schweppe H, Roudier Y. Securty and privacy for in-vehicle networks [C]//IEEE 1st International Workshop on Vehicular Communications, Sensing, and Computing (VCSC),2012:12-17

[6] 孙瑶,王小妮,刘鹏,等.车载 CAN 总线认证与加密机制研究[J].北京信息科技大学学报(自然科学版),2019,34(3):73-78
SUN Yao, WANG Xiaoni, LIU Peng, et al. Research on vehicle CAN bus authentication and encryption mechanism[J].Journal of Beijing Information Science & Technology University,2019,34(3):73-78
[7] 冯凯,李巍,龚洁中.车联网中密码算法应用现状分析[J].中国信息安全,2019(9):97-99
FENG Kai, LI Wei, GONG Jiezhong. Analysis of the current situation of the application of cryptographic algorithms in the internet of vehicles [J].China Information Security,2019(9):97-99
[8] 陈刚.国密 SM4 算法在车载 CAN 总线的加密应用[J].信息通信,2019,32(3):149-151
CHEN Gang.The encryption application of national secret SM4 algorithm in vehicle CAN bus [J].Information & Communications,2019,32(3):149-151
[9] 修佳鹏,田超宇,杨正球,等.SecOC 安全机制中国密算法应用方案研究[J].信息安全研究,2020,6(9):775-782
XIU Jiapeng, TIAN Chaoyu, YANG Zhengqiu, et al. Research on application scheme of national secret algorithm in SecOC security mechanism[J].Journal of Information Security Research,2020,6(9):775-782
[10] 国家密码管理局.GB/T 0002—2012 SM4 分组密码算法[S].2012
State Cryptography Administration. GB/T 0002—2012 SM4 block cipher algorithm [S].2012
[11] 罗禹.基于加密算法的车载 CAN 总线安全通信研究[D].长沙:湖南师范大学,2020
LUO Yu. Research on secure communication of vehicle CAN bus based on encryption algorithm[D].Changsha: Hunan Normal University,2020
[12] 张悠熠,朱元,毛威.车载 CAN 总线安全验证机制及性能检测[J].信息通信,2018,31(8):15-17
ZHANG Youyi,ZHU Yuan,MAO Wei.Safety verification mechanism and performance test of vehicle CAN bus [J].Information & Communications,2018,31(8):15-17
[13] 郭志刚,潘俊家,韩光省,等.基于车载 CAN 总线的安全通信机制研究[J].中国汽车,2020,30(7):46-50,57
GUO Zhigang,PAN Junjia,HAN Guangsheng,et al.Security onboard communication for in-vehicle bus on CAN bus[J].China Auto,2020,30(7):46-50,57

Vehicle PEPS and EMS security certification based on encryption algorithm SM4

LI Min[1,2] CHEN Fulong[1] PANG Hui[3]
1 School of Computer and Information,Anhui Normal University,Wuhu 241003
2 School of Information and Artificial Intelligence,Wuhu Institute of Technology,Wuhu 241006
3 Atech Automotive (Wuhu) Co.Ltd.,Wuhu 241006

Abstract With the rapid development of ICV (Intelligent Connected Vehicle) industry,data exchange between vehicle and human,vehicle and vehicle as well as between vehicle and external environment has become common, which imposes serious threat to automobile security.Security certification of vehicle PEPS (Passive Entry Passive Start) and EMS (Engine Management System) is the prerequisite to ensure the safe operation of the vehicle.However,the widely used 128 bits AES for PEPS and EMS security certification is complex in algorithm,time consuming in encryption and decryption,and occupies more MCU resources,compared with encryption algorithm SM4.Here,the SM4 algorithm is used to carry out security certification of vehicle PEPS and EMS,which can shorten the encryption and decryption time,and effectively improve the data transmission efficiency.Then,it is implemented by advance language and transplanted to domestic MCU GD32F103.The proposed approach applies encryption algorithm SM4 and provide a research basis for ICV security certification.

Key words encryption algorithm SM4;passive entry passive start (PEPS);engine management system (EMS); security certification