

关于 2026 年度党政机要密码科学技术奖受理项目的公示

项目通过国家密码局形式审查并受理，现对该项目进行如下公示：

项目名称：智能网联汽车商用密码应用关键技术及产业化

推荐奖种：党政机要密码科学技术奖

申报方式：提名申报

项目简介：

（1）主要内容

本项目依托国家密码管理局《自主可控密码技术在汽车信息安全领域应用研究》项目，研究自主可控密码技术对智能网联汽车进行全面安全防护的关键技术与产品研发，实现密码在复杂车联网环境中的有效合规性应用，在车载密码基础模块、车载设备层、网络层、应用层创新研发车联网安全产品，构建了完整的基于商用密码的智能网联汽车安全防护体系，实现产业化应用：

1) 密码基础层：研发了适用于汽车复杂电磁、电气干扰环境及汽车板级嵌入式设备资源受限条件下的商用密码算法应用技术，国内首家获得汽车密码模块商用密码产品型号认证，支持车载端稳定实时的 SM2/SM3/SM4 国密算法加解密性能。

2) 设备平台层：构建了基于可信硬件的双系统密码隔离架构，实现了密码运算与应用系统的物理隔离，支持安全启动和运行时完整性校验，研发了高安全级车载电子设备。

3) 网络防护层：针对车联网异构化网络研发了多维度入侵检测方法，支持实时防御和流量加密，实现总线网络、汽车以太网、无线网的一致性防护，检测性能获中国汽研认证，误报率低于 2%。

4) 应用服务层：建立了智能网联汽车多层次密码认证体系，研究车联网数据可信交换的密码协议体系，提供身份认证、密钥管理、数据加密、数据存证等密码应用服务，支撑 V2X 身份认证消息加密及车联网功能的安全应用，保障汽车的信息共享和网联控制安全。

（2）技术特点

1) 采用针对性的电路设计，屏蔽汽车环境中的强电磁干扰、浪涌电流冲击等问题，解决了在复杂车载环境中 SM2/SM3/SM4 等国产密码算法应用的稳定性

问题，保障了密码应用实时性，有力推进自主可控密码在智联网联汽车领域的落地实现。

2)可信执行环境技术，应用于车载设备密码应用安全，实现安全系统硬件物理隔离，密码运算与安全功能在独立的可信执行环境中进行。优化双系统共享内存安全通信机制，将跨系统通信延迟降至 5ms 以内，兼顾了安全性与车载实时性要求，形成物理级密码安全应用。

3)突破传统单一特征检测局限，提出融合报文 ID、时间周期、数据域语义与流量统计的多维检测方法，引入神经网络集群处理未知攻击识别，构建 CAN 总线与汽车以太网统一防护框架。检测准确率达>98%，实时响应时间<10ms，国内首家通过中国汽研认证。

4)构建完整汽车信息安全纵深防御体系：形成从密码模块、车载设备到汽车网络安全、应用安全的全栈安全防护，覆盖车内到车外全链路，全面立体的保护汽车联网后的信息安全。

（3）解决的关键问题和主要创新点

创新点 1：进行硬件抗干扰设计，保障密码模块稳定性，提出 Flash 安全存储根密钥的加密方法，防止物理攻击；设计设备唯一标识生成方法，防止设备克隆。车载资源受限环境中密钥存储易被物理攻击提取，传统密钥管理方案难以适配。

创新点 2：可信硬件双系统隔离。针对普通操作系统中运行密码应用存在的安全风险，在保障车载环境实时性要求的前提下，研发安全系统与应用系统的设备级硬件物理隔离方案，设计了高效的双系统共享内存安全通信机制，解决了实时性与安全性的矛盾。密码运算在可信执行环境中独立执行，防止密钥泄露，支持安全启动和运行时完整性校验，实现毫秒级安全通信延迟。该创新点解决了车载设备层级下密码应用的安全隔离问题。

创新点 3：车载网络防护的多维入侵检测方法。突破传统单一特征检测局限，融合报文、数据域特征，提出基于神经网络集群的智能检测算法，实现了 CAN 总线和汽车以太网的统一防护框架。中汽研对所研发的汽车信息安全网关进行权威测试，检测准确率>98%，实时响应时间<10ms，解决了车联网异构网络的入侵检测的问题。

创新点 4：支持车联网数据可信交换的密码协议体系，针对当前智能网联汽车服务层密码应用单一，在异构系统下无法支持可溯源存证的数据高效流转问题，设计了面向数据高效交换的前置轻量级认证协议以及异构密码体制的多层次交换方案，实现数据敏感等级差异化交换，并采用“平台+物理”双重验证架构保障数据可信可查。针对数据外泄取证难题，依托区块链搭建可信取证底座，有效提升车联网数据安全交换与溯源取证能力。

（4）成果推动科技创新发展的作用

本项目攻克了智能网联汽车商用密码应用的核心技术难题，在车载入侵检测、可信执行环境、密钥管理、身份认证等技术领域拥有自主知识产权，共获 41 项发明专利授权，以自主知识产权推进产业化落地；积极进行密码应用与安全理论的研究创新，共发表学术论文 11 篇；主导制定国家标准 1 项（GB/T 30290.3-2025）及团体标准 1 项，推动智能网联汽车行业密码应用标准化，引领行业发展。同时通过产学研用深度融合，培养车联网安全领域技术人才，增强企业自主创新能力；在宇通、东风等龙头车企成功应用，产值 2 个亿以上，为汽车行业提供坚实的安全保障，促进国产商用密码在智能网联汽车领域的深入发展。

主要完成单位：

厦门雅迅智联科技股份有限公司、中国科学技术大学

主要完成人及其贡献：

1、涂岩恺（厦门雅迅智联科技股份有限公司）：项目负责人，对创新点 1、2、3、4 做出了主要贡献，包括：1）设计汽车总线硬件防护电路与防御方法，进行总线入侵信号的干扰与防御。2）研发基于硬件资源抢占式的数据加密方法，保护车辆数据隐私。3）参与机双系统的虚拟化隔离技术，实现车载智能终端 SOC 级安全域的隔离，从根本上解决了汽车进入互联网后被动引入互联网安全威胁的问题。4）设计并研发了汽车总线安全网关，实现总线加密。5）发明多程应用层安全应用，包括安全组群查询技术，位置查询在加密坐标系内进行，从而避免车辆位置泄露风险。参与汽车工程协会团体标准《智能网联汽车车载端信

息安全技术要求》制定，授权相关发明专利 12 项。

2、赵国开（厦门雅迅智联科技股份有限公司）：本项目研发的主要负责人之一，负责本项目的密码基础层、设备平台层、网络防护层及应用服务层技术架构的设计，并重点攻关其中的核心关键技术车载密码模块硬件抗干扰设计与国产密码算法车载适配、车载环境下密钥安全存储、车载 CAN 总线多维入侵检测、汽车以太网加密流量监控、车载双系统密码隔离架构、车联网场景多层次密码认证体系、车联网密钥全生命周期安全管理、车联网 OTA 全流程密码应用与升级包安全分发方法。对本项目的 1，2，3，4 的四个创新点做出了直接贡献，形成授权发明专利 22 项，参与国家标准 1 项。

3、吕伟煌（厦门雅迅智联科技股份有限公司）：本项目研发的主要负责人，对创新点 1、3、4 做出了主要贡献，包括：1）提出了以硬件抗干扰加固设计为基础的密码模块架构，以覆盖多层次密钥全生命周期的管理机制；2）设计融合报文与数据域特征的神经网络集群智能检测算法，构建了 CAN 总线与汽车以太网统一防护框架，提供异构网络环境下异常行为的精准识别与毫秒级实时响应；3）设计了面向数据高效交换的前置轻量级认证协议及异构密码体制的多层次交换方案，实现数据敏感等级差异化交换；4）基于动态口令认证、车载终端与中心平台双向认证及密码强度评估等方向形成配套技术储备，为车联网数据可信交换提供了全链路密码保障。同时主导完成国家标准 GB/T 30290.3-2025 《北斗卫星定位车辆信息服务系统 第 3 部分：信息安全规范》，参与完成了 9 篇专利。

4、黄朝阳（厦门雅迅智联科技股份有限公司）：本项目研发的主要参与人员，主要负责项目资源配置与落地，进行项目进度管理与技术创新规划，指导车载网络密码防护的多维入侵检测方法的具体需求分析与应用实现规划，总结产业化需求，制定信息安全防护体系的技术需求并审核产品技术指标，推动产业化落地，参与完成了专利 1 篇。

5、郭加平（厦门雅迅智联科技股份有限公司）：本项目研发的主要参与人员，主要负责创新点二：车载网络密码防护的多维入侵检测方法的相关研究，并作出直接贡献。基于车内网智能检测算法与相关分析的车载网络异常检测方法，构建了融合报文特征与数据域特征的多维协同检测模型，实现了 CAN 总线与汽

车以太网统一防护框架下的精准入侵识别与毫秒级实时响应。参与完成了专利 3 篇。

6、张驰（中国科学技术大学）：本项目研发的主要参与人员，主要负责创新点四支持车联网数据可信交换的密码协议体系的相关研究，并作出直接贡献。统筹开展区块链扩容技术、数据交换技术等核心方案的研究。参与完成了代表性论文 11 篇。

7、解岩凯（中国科学技术大学）：本项目研发的主要参与人员，主要负责创新点四支持车联网数据可信交换的密码协议体系的相关研究，并作出直接贡献。提出区块链扩容技术、数据交换技术以及数据泄露数据追踪技术的核心方案，并统筹其中认证技术、虚假数据识别等技术的研究。参与完成了代表性论文 11 篇。

8、唐磊（厦门雅迅智联科技股份有限公司）：本项目研发的主要参与人员，主要参与创新点二可信硬件双系统隔离中毫秒级安全通信延迟的关键技术研发，提出基于 CPU 负担动态平衡的任务调度优化方案，将关键任务响应时间控制在毫秒级；以及参与创新点三车载网络防护的多维入侵检测方法中的专用车辆识别方法及方案，用技术手段实现了专用车辆的合法性及安全性，这是实现车辆统一防护的基础。支撑授权发明专利 2 项。

9、刘伟峰（厦门雅迅智联科技股份有限公司）：本项目研发的主要参与人员，主要负责创新点二：基于可信硬件的车载双系统密码隔离架构的相关研究，并作出直接贡献。主要负责为车载终端环境提供高精度、低误差的总线流量原始数据，打造精准网帧筛选逻辑，适配可信硬件双系统低时延安全通信需求，为车载密码运算提供实时可靠的数据源；同时通过标准化网帧解析能力支撑多层次密码认证与数据可信采集，打通车内总线感知、设备安全隔离、异构网络智能防御、车联网数据可信交换的全链路。参与完成了专利 1 篇。

10、肖振隆（厦门雅迅智联科技股份有限公司）：本项目研发的主要参与人员，主要负责创新点一：复杂车载环境下商用密码算法适配与密钥安全存储技术的相关研究，并作出直接贡献。提出硬件级双 CPU 延迟控制与时序同步方案，可有效抑制车载复杂电磁环境下的信号干扰与运算失步问题，保障密码模块稳定运行，并统筹推进硬件抗干扰加固、双 CPU 时序协同控制等相关技术研

究。参与完成了专利 1 篇。

主要知识产权和标准规范等目录:

知识产权 (标准)类 别	知识产权 (标准)具 体名称	国家 (地 区)	授权号 (标 准 编 号)	授权(标准 实施)日 期	证书编号 (标准批准 发布部门)	权利人 (标准起 草单位)	发明人 (标准起 草人)
发明专利	一种设备内大容量电容的放电保护方法与该设备	中国	CN112531802B	2025/11/28	8530211	厦门雅迅智联科技股份有限公司	陈茹涛、赵国开、曾佳兴
发明专利	CAN 异常入侵检测方法 & 计算机可读存储介质	中国	CN113055341B	2025/08/26	8199125	厦门雅迅智联科技股份有限公司	赵国开、黄运峰、邓超、吕伟煌、陈茹涛
发明专利	车辆 CAN 网络的 DOS 攻击检测方法 & 存储介质	中国	CN112866183B	2025/2/7	7713898	厦门雅迅智联科技股份有限公司	赵国开、刘经所、张鹏、柯金铃、黄运峰、陈茹涛
发明专利	内核运行时的完整性校验方法及计算机可读存储介质	中国	CN109753788B	2024/4/19	6919903	厦门雅迅智联科技股份有限公司	赵国开、涂岩恺、刘炯钟、池炜宾
发明专利	一种汽车以太网通讯方法、终端设备及存储介质	中国	CN111435945B	2023/11/07	6469449	厦门雅迅智联科技股份有限公司	王敏效、赵国开、邓超
发明专利	客户端认证方法及计算机可读存储介质	中国	CN109474431B	2023/11/03	6454612	厦门雅迅智联科技股份有限公司	刘炯钟、赵国开、池炜宾
发明专利	车载端对接入设备的可信验证方法及其系统、车载端	中国	CN109495269B	2023/11/03	6453474	厦门雅迅智联科技股份有限公司	赵国开、涂岩恺、池炜宾、刘炯钟
发明专利	一种汽车网关上实现网络入侵检测的方法及系统	中国	CN113132298B	2023/10/27	6438663	厦门雅迅智联科技股份有限公司	赵国开、戴智超、黄朝阳、陈茹涛、黄运峰
发明专利	检测车内 CAN 网络遭受非法行为的方法、装置及存储介质	中国	CN113132307B	2023/09/01	6286911	厦门雅迅智联科技股份有限公司	赵国开、黄运峰、邓超、陈茹涛、吕伟煌

发明专利	系统安全冗余方法及计算机可读存储介质	中国	CN110018925B	2023/08/29	6281846	厦门雅迅智联科技股份有限公司	开、钟、恺、荣、宾	赵国刘炯涂岩韦昌池炜
发明专利	双系统通信访问控制方法及计算机可读存储介质	中国	CN109784045B	2023/8/22	6251937	厦门雅迅智联科技股份有限公司	钟、开、超、峰、恺	刘炯赵国牛方黄运涂岩
发明专利	双系统通信密钥生成方法及计算机可读存储介质	中国	CN109586898B	2023/08/22	6254174	厦门雅迅智联科技股份有限公司	钟、宾、开、超	刘炯池炜赵国牛方
发明专利	基于双系统共享内存的数据交互方法及系统	中国	CN109783245B	2023/07/18	6153494	厦门雅迅智联科技股份有限公司	钟、开、超、峰、恺	刘炯赵国牛方黄运涂岩
发明专利	双系统的通信方法及计算机可读存储介质	中国	CN110347517B	2023/05/30	6012981	厦门雅迅智联科技股份有限公司	开、宾、恺、荣、钟、东	赵国池炜涂岩韦昌刘炯赖荣
发明专利	一种汽车以太网流量监控方法、终端设备及存储介质	中国	CN111245773B	2023/04/18	5895203	厦门雅迅智联科技股份有限公司	开、效、超、峰、涛、荣	赵国王敏邓黄运陈茹韦昌
发明专利	提高非实时性操作系统实时性的方法及其系统	中国	CN109522099B	2023/03/31	5832183	厦门雅迅智联科技股份有限公司	开、恺、钟、宾	赵国涂岩刘炯池炜
发明专利	数据防泄漏方法及计算机可读存储介质	中国	CN109657479B	2023/03/28	5823043	厦门雅迅智联科技股份有限公司	开、恺、宾、钟	赵国涂岩池炜刘炯
发明专利	基于trustzone技术的双系统启动方法及计算机可读存储介质	中国	CN109426523B	2022/12/06	5627818	厦门雅迅智联科技股份有限公司	钟、开、恺、宾	刘炯赵国涂岩池炜
发明专利	双系统外设资源的配置方法、	中国	CN109446847B	2022/08/19	5396173	厦门雅迅智联科技股份有限公司	宾、开、钟	池炜赵国刘炯

	终端设备及存储介质						
发明专利	基于 TrustZone 的 CAN 总线数据防护方法及系统	中国	CN108090376B	2021/01/12	4199253	厦门雅迅智联科技股份有限公司	刘炯、钟开、赵国、涂岩、恺、池炜、宾
发明专利	一种反克隆的车载系统及其工作方法	中国	CN105512520B	2020/09/11	3980749	厦门雅迅智联科技股份有限公司	赵国、开、陈从、任、陈华、许、华、赋、云、宁、弟
发明专利	一种在 FLASH 安全存储加密认证所需根密钥的方法	中国	CN105426772B	2019/07/02	3440568	厦门雅迅智联科技股份有限公司	赵国、开、任、陈华、郑福、赋、云、弟
发明专利	抗静电保护与对地或电源短路保护的多态开关及实现方法	中国	CN109756113B	2020/12/11	4149672	厦门雅迅智联科技股份有限公司	陈茹、涂岩、林晓文、涛、恺、龙、陈文、顺、
发明专利	一种 CAN 总线入侵防御电路与方法	中国	CN112929150B	2025/08/19	8176195	厦门雅迅智联科技股份有限公司	涂岩、恺、华、兰伟
发明专利	基于神经网络集群的车内网入侵检测方法和终端设备	中国	CN112291184B	2024/03/01	6750001	厦门雅迅智联科技股份有限公司	涂岩、郭加、恺、平
发明专利	基于双系统的 CAN 总线波特率自适应方法、存储介质	中国	CN111565138B	2023/03/14	5768213	厦门雅迅智联科技股份有限公司	池炜、宾、罗明、涂岩、宇、恺、叶旭、辉
发明专利	防撞库的用户登录安全认证方法、终端设备及存储介质	中国	CN110365626B	2022/12/06	5631053	厦门雅迅智联科技股份有限公司	涂岩、陈义、恺、华
发明专利	一种动态口令认证方法及系统	中国	CN105391556B	2022/02/15	4936915	厦门雅迅智联科技股份有限公司	涂岩、吕伟、黄运、罗明、曹洪、恺、煌、峰、宇、霞
发明专利	一种安全组群位置查询方法及系统	中国	CN106060024B	2021/11/02	4772143	厦门雅迅智联科技股份有限公司	涂岩、罗明、吕伟、恺、宇、煌、曹洪

							霞、刘炯钟
发明专利	基于MEMS传感器生成终端唯一性标识的方法	中国	CN108875419B	2021/06/22	4499464	厦门雅迅智联科技股份有限公司	涂岩恺、汪文芳、张航其
发明专利	一种车载终端与中心平台双向认证方法及系统	中国	CN111314274B	2023/02/10	5735358	厦门雅迅智联科技股份有限公司	吕伟煌、罗明宇、郭加平
发明专利	一种图形密码强度识别方法与装置	中国	CN105279424B	2020/09/11	3983915	厦门雅迅智联科技股份有限公司	涂岩吕伟、谭芳明
发明专利	一种车内数据安全监控方法	中国	CN104820723B	2019/01/01	3199640	厦门雅迅智联科技股份有限公司	涂岩吕伟、陈典全、陈义华、谭芳慧
发明专利	一种数据加密系统及方法	中国	CN103378971B	2017/10/13	2654456	厦门雅迅智联科技股份有限公司	涂岩陈义、汤益明、杨磊
发明专利	一种基于相关分析的车载网络异常检测方法	中国	CN112787984B	2023/11/14	6483800	厦门雅迅智联科技股份有限公司	曲建罗明、郭加平、吕伟煌、牛方超
发明专利	车载网络入侵检测方法	中国	CN111030962B	2023/03/24	5803822	厦门雅迅智联科技股份有限公司	曲建罗明、吕伟煌
发明专利	一种采集车辆状态信号的方法	中国	CN103810768B	2018/01/02	2764477	厦门雅迅智联科技股份有限公司	刘伟峰、郑福弟、许宁、郑振贵
发明专利	专用车辆识别方法及其系统	中国	CN106981199B	2020/10/16	4035995	厦门雅迅智联科技股份有限公司	许宁、许振唐、坪、郭亚磊、松、黄鹏
发明专利	一种车载终端利用串口实现CPU负担动态平衡的方法	中国	CN103713957B	2018/12/14	3181363	厦门雅迅智联科技股份有限公司	唐磊、许宁、林德辉、陈华云、黄鹏、蔡珊

发明专利	一种双CPU延迟控制电路	中国	CN105680837B	2019/03/22	3302267	厦门雅迅智联科技股份有限公司	肖振隆、文、其、涛、平、蔡运航、张航、陈茹、蔡炎
发明专利	一种用于抑制车载智能终端电源系统振荡的装置	中国	CN106972746B	2020/6/26	3861127	厦门雅迅智联科技股份有限公司	张航、蔡运、陈茹、汤益、陈勇
国家标准	北斗卫星定位车辆信息服务系统 第3部分：信息安全规范	中国	GB/T 30290.3-2025	2025-10-05	国家市场监督管理总局、国家标准化管理委员会	厦门雅迅智联科技股份有限公司、奇瑞汽车股份有限公司、重庆长安汽车股份有限公司、中汽创智科技有限公司、国汽(北京)智能网联汽车研究院有限公司、东风汽车股份有限公司、上汽大通汽车有限公司、上汽通用五菱汽车股份有限公司、一汽解放汽车有限公司、宇通客车股份有限公司、大运汽车股份有限公司、北京梆梆安全科技有限公司	吕伟、赵国、王川、汪向、胡红、薛晓、朱震、黄建、郑庆、李晓、卢佐
团体标准	智能网联汽车车载终端信息安全技术要求	中国	T/CSAE 101-2018	2018-06-19	中国汽车工程学会	北京航空航天大学、中国信息通信研究院、中国汽车工程学会、浙江吉利控股集团有限公司、中国汽车技术研究中心有限公司、惠州市德赛西威汽车电	王云、风束、余贵、于海、秦洪、公维、刘建、王尚、董长、张亚、邵学、张裁、何承

					子股份有限公司、工业和信息化部计算机与微电子发展研究中心(中国软件评测中心)、长城汽车股份有限公司、威马汽车科技集团有限公司、广州汽车集团有限公司、重庆长安汽车股份有限公司、北京洋浦伟业科技发展有限公司、厦门雅迅网络股份有限公司、东软集团股份有限公司、中兴通讯股份有限公司、惠州华阳通用电子有限公司、中国联合网络通信集团有限公司	坤、薛晓巍、王立崇、张小东、王赵闻、汪向阳、张金池、杨角、卢佐华、涂岩恺、陈静祁、赵孝帅、赵苗武、张注锋、张曼君
--	--	--	--	--	--	--

推广应用情况:

1、本项目研发的智能网联汽车商用密码终端产品，目前已广泛应用于中国重汽集团、福田等运营车辆上，构建完整汽车信息安全纵深防御体系:形成从密码模块、车载设备到汽车网络安全、应用安全的全栈安全防护，覆盖车内到车外全链路，全面立体的保护汽车联网后的信息安全，为中国重汽集团创造了良好的经济效益和社会效益。同时本项目成果也已部署覆盖郑州宇通客车、东风汽车集团等龙头企业，并在全国多个 5G-V2X 示范区成功落地。2022-2025 年内实际实现销售收入 16,707.49 万元，净利润 10,554.34 万元，上缴税金 3,176.460 万元，完成单位主导或参与了多个项目，包括郑州东三环示范项目、武汉智能网联汽车与智慧交通应用示范区二期、长城汽车智慧汽车交通融合创新试验平台、长沙国家先导区广汽丰田 V2X 项目、延崇高速 V2X 项目、无锡市滨湖区车

联网应用示范项目、深圳智能网联交通测试示范平台等国家级和省级车联网示范工程。累计装车超过 3 万台，产品已稳定运行超过 4 年。

2、本项目成果形成了可复制推广的智能网联汽车密码安全解决方案，已在物流、公交、客车、乘用车等多个细分领域规模化应用，为车联网、车路协同、自动驾驶等新兴业态提供了安全基座，推动了国产密码在汽车行业的深度融合与创新发展，无重大安全事故发生，获得用户高度认可。

特此公示！

中国科学技术大学
2026 年 9 月 24 日