·汽车芯片技术专题·

车载信息安全芯片趋势研究

刘泓余　王强　李家玲　鲍瑞　张凯

（中国第一汽车股份有限公司研发总院，长春 130013）

【欢迎引用】刘泓余，王强，李家玲，等．车载信息安全芯片趋势研究[J]．汽车文摘，2026(9)：22-29.

【Cite this paper】LIU H Y, WANG Q, LI J L, et al. Research on the Trend of In-Vehicle Information Security Chips[J]. Automotive Digest (Chinese), 2026(9): 22-29.

【摘要】为了应对智能网联汽车快速发展所带来的车载计算类芯片数据交互量呈爆炸式增长的趋势，同时满足车载数据作为车企最宝贵核心资产所必需的高等级安全防护需求，探讨了现行信息安全标准及算法对车载信息安全芯片的影响，分析了国密算法在车载芯片领域的替代路径与发展趋势。结果表明：未来随着车载芯片相关标准的陆续落地，国密等级认证将成为行业规范，通过该认证的车载信息安全芯片将占据国内主流市场。

关键词：信息安全；车载信息安全芯片；国密等级认证；加密算法

中图分类号：U463.6　　**文献标志码：**A　　**DOI:** 10.19822/j.cnki.1671-6329.20240291

Research on the Trend of In-Vehicle Information Security Chips

Liu Hongyu, Wang Qiang, Li Jialing, Bao Rui, Zhang Kai

（Global R&D Center, China FAW Corporation Limited, Changchun 130013）

【Abstract】 To address the rapid growth of data exchange volume in onboard computing chips driven by the rapid development of intelligent connected vehicles, while satisfying the high-level security protection requirements for in-vehicle data as the most valuable core asset of automotive manufacturers, the paper discusses the impact of current information security standards and algorithms on in-vehicle information security chips and analyzes the replacement path and development trend of national cryptographic algorithms in the field of in-vehicle chips. The results show that as relevant standards for in-vehicle chips are successively implemented, national cryptography level certification will become an industry norm, and in-vehicle information security chips that pass such certification will occupy the mainstream domestic market.

Key words: Information security, In-vehicle information security chips, National commercial cryptography product grade certification, Cryptographic algorithm

0　引言

信息安全不仅是技术层面的核心问题，更是企业持续运营的关键保障，同时也构成维护国家安全与利益的重要防线[1]。随着智能网联汽车智能化水平不断提升，智能座舱系统所承载的数据类型日益丰富，辅助驾驶技术逐步向高阶演进，数据交互频率与规模呈指数级增长。该趋势在提升驾乘体验与行车效率的同时，也使汽车信息安全面临前所未有的挑战[2]。

其中，汽车芯片的安全性直接影响整车的信息防护能力。保障信息芯片安全不仅需要实现传统的数据加密与身份认证，也需要在算力提升、低功耗设计、实时响应与系统兼容性之间实现平衡[3]。面对日益复杂多变的信息安全威胁，需要通过持续的技术创新与前瞻性的战略布局，构建覆盖芯片设计、制造、部署及运维全生命周期的安全防护体系。提升芯片层面的信息安全能力，可以增强汽车应对新型网络攻击与安全威胁时的协同防御与快速恢复能力，为产业智能化转型保驾护航[4]。

本文分析车载信息安全芯片技术的发展趋势，系统梳理国内外信息安全标准进展、关键算法的升级路径及应用实践，并结合当前车载信息安全芯片的现状与发展动态，展望其未来发展方向。

1 信息安全标准进展

随着智能网联汽车电子电气架构向域集中式演进，信息安全防护的重要性逐渐凸显。电子电气架构虽实现了功能集成与效能提升，也扩大了系统攻击面并使内部架构极度复杂化。一方面，大量外部互联接口与内部跨域通信使攻击向量激增，传统单点防护难以应对。另一方面，不同安全级别的功能域（如娱乐域与控制域）之间频繁交互，需建立严格的硬件级隔离与跨域认证机制，以防止局部风险扩散为系统性安全危机。

面对上述挑战，构建以硬件可信为基础的深层、主动防御体系已成为必然要求。底层安全芯片需与主控系统级芯片（System on Chip，SoC）协同工作，为复杂的软件环境提供从启动、运行到数据传输的全方位安全服务。同时，安全防护必须从事后补救转向实时响应，这要求安全芯片具备支撑高性能密码运算与入侵检测的算力，实现动态、在线的主动防御。国内外监管机构与标准组织相继推出了一系列信息安全标准[5]。从顶层设计入手，不仅明确了以安全芯片为核心构建硬件可信任的技术框架，规定了其在保障密钥安全、实现安全启动、支撑安全通信等关键环节的核心要求，更从方针上确立了纵深防御、全生命周期管理与供应链安全的基本原则，为车载信息安全芯片的技术研发、测试认证与规模化应用建立了统一基准与明确指引。

1.1 ISO/SAE 21434

国际标准化组织（International Organization for Standardization，ISO）以ISO 26262框架为参考[6]编制了汽车信息安全领域的首个国际标准——ISO/SAE 21434（Road Vehicles-Cybersecurity Engineering）[7]，并于2021年8月发布。其具体框架如图1所示。



图1 ISO/SAE 21434框架

该标准详细阐述了建立网络安全流程和管理方法的步骤，指导企业在特定项目中实施网络安全活动并进行有效管理，明确了网络安全活动中供应商和客户之间的互动、依赖关系及责任分配。此外，该标准涵盖了项目生命周期中各阶段应执行的网络安全活动，包括产品概念、开发、网络验证、生产以及运营和售后服务阶段目标，并规定了零部件或整车报废时的安全要求以及系统性危害分析和风险评估方法[8]。

虽然该标准并未明确车载信息安全芯片的具体技术规格，但是可以推导出车载信息安全芯片的技术映射，如表1所示。

表1　ISO/SAE 21434技术映射

标准要求	芯片技术映射
具备风险评估及对应解决措施	硬件安全模块（Hardware Security Module，HSM）、可信执行环境（Trusted Execution Environment，TEE）
具备完备的安全架构设计，避免引入弱点	安全启动、安全调试、硬件隔离
具备安全验证及测试功能，对已实现的安全功能进行有效验证	支持诊断与测试接口、内置自检机制
供应链安全，确保组件来源可信且安全	具备唯一身份标识、证书管理
生产与运营安全，确保生产等过程中不会引入安全漏洞	密钥管理、签名、安全升级

车载信息安全芯片需通过ISO/SAE 21434认证，这就要求在芯片设计各阶段充分考虑并满足该标准的各项准则。因此，ISO/SAE 21434为车载信息安全芯片的设计提供了全面的网络安全需求框架。

1.2　信息技术安全性评估准则

为建立国际通用的信息安全评估体系，美国、加拿大、英国、法国、德国以及荷兰于1996年共同提出了信息技术安全评估通用准则（The Common Criteria for Information Technology security Evaluation，CC标准），其综合了已有的信息安全准则和标准，形成了一个更全面的框架。1999年，CC标准被正式纳入国际标准ISO/IEC 15408。2001年，中国信息安全测评中心根据ISO/IEC 15408，发布国家标准GB/T 18336—2001《信息技术 安全技术 信息技术安全性评估准则》[9]，现行版本为GB/T 18336—2024[10]。

GB/T 18336—2024标准分为3个部分：第一部分为简介和一般模型，阐述了IT安全评估的基本概念与原理，并提出了评估的通用模型；第二部分为安全功能组件，建立了一套标准化的功能组件库，按类和族进行组织；第三部分为安全保障组件，同样以类和族的方式组织了保障组件，并定义了保护轮廓（Protection Profile，PP）和安全目标（Security Target，ST）的评估准则，同时提出了7个预定义的评估保障级（Evaluation Assurance Level，EAL），如表2所示。

产品所获认证级别越高，代表其安全性与可信度越高，能够抵御更高级别的威胁，适用于风险更高的应用环境[11]。

车载信息安全芯片需要实现安全通信保证与外界数据传输的保密性和完整性，还需提供可靠的密码运算服务（加解密、签名验签等），确保具备安全存储功能，保障芯片内用户数据的机密性和完整性，并能够对芯片的所有安全功能进行管理。

表2　评估保障等级EAL1–EAL7[11]

EAL级别	安全保障要求
EAL1	功能测试
EAL2	结构测试
EAL3	系统测试和检查级
EAL4	系统设计、测试和复查级
EAL5	半形式化设计和测试级
EAL6	半形式化验证、设计和测试级
EAL7	形式化验证、设计和测试级

目前，国内外车载安全芯片普遍通过信息技术安全性评估准则进行安全等级认证。该标准为车载信息安全芯片提供了评估和验证其安全性的通用框架，根据产品定位划分不同的评估等级，确保产品的安全性获得国际认可。

1.3　安全芯片密码检测准则

国家密码管理局于2012年11月发布了GM/T 0008—2012《安全芯片密码检测准则》[12]，用于认证汽车、支付、多媒体等的安全芯片。该标准将安全能力划分为密码算法、安全芯片接口、密钥管理、敏感信息保护、安全芯片固件安全、自检、审计、攻击的削弱与防护以及生命周期保证。除此之外，该标准将每个部分的安全能力分解为依次递增的3个安全等级，即国家密码管理局商用密码产品认证等级。目前，国密二级为国内现行最高的安全认证等级。

此外，为进一步建立并完善商用密码产品认证体系，市场监管总局联合国家密码管理局发布了《商用密码产品认证目录（第一批）》，其中明确了安全芯片所采用的密码算法应包括GM/T 0001祖冲之序列密码算法[13]、GM/T 0002 SM4分组密码算法[14]、GM/T 0003 SM2椭圆曲线公钥密码算法[15]、GM/T 0004 SM3密码杂凑算法[16]、GM/T 0009 SM2密码算法使用规范[17]、GM/T 0010 SM2密码算法加密签名消息语法规范[18]、GM/T 0044 SM9标识密码算法[19]一系列国家密码管理局发布的国密算法。信息安全芯片除了需支持国密算法外，国密二级对其他安全技术也提出了严格要求。表3为国密二级技术要求。

目前，国内已建立成熟的国密等级认证测试体系与认证机构。为智能网联汽车提供了更高级别的安全保障。此外，推行国密认证有助于加强国密算法的

推广应用，降低对国外技术的依赖。

表3　国密二级技术要求

项目	要求
随机数	具备至少4路物理随机源产生真随机数
密码算法	密码算法核心运算环节需采用专用硬件电路实现
密钥管理	支持密钥生成、存储、使用、更新、导入、导出、清除功能
敏感信息保护	支持敏感信息的存储、清除、运算、传输功能
攻击削弱及防护	物理版图保护、密钥及敏感信息自毁、计时攻击防护、能量分析防护、电磁分析防护、故障攻击防护

1.4　小结

ISO/SAE 21434标准、信息技术安全性评估准则和安全芯片密码检测准则共同构成车载信息安全芯片安全框架，如图2所示。

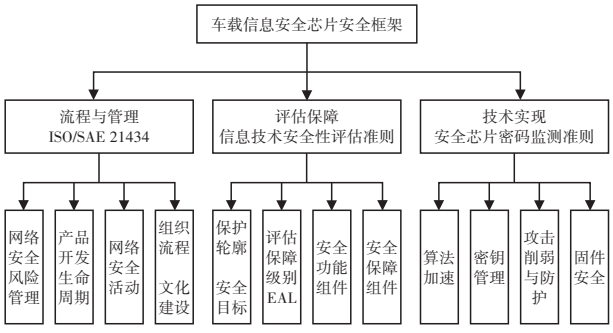


图2　车载信息安全芯片标准体系架构

车载信息安全芯片的发展将持续受到ISO/SAE 21434标准、信息技术安全性评估准则和安全芯片密码检测准则的影响。上述标准不仅为车载信息安全芯片的设计和实现提供了严格的技术规范，也引导着行业的技术发展和创新方向。总体来看，标准体系的完善将推动车载信息安全芯片向更安全、更可靠的方向演进。随着技术进步与市场需求增长，车载信息安全芯片将更加注重性能与安全的协同优化。同时，芯片国产化趋势也促使国内企业在技术创新与市场应用方面发挥更大作用。

根据工业和信息化部发布的《国家汽车芯片标准体系建设指南》[20]，中国加快制定汽车芯片重点标准，为汽车芯片产品的安全可靠应用与试点示范提供基础指导。预计到2030年，将制定超过70项汽车芯片相关标准为目标，以满足构建安全、开放和可持续汽车芯片产业生态的需要。这表明在政策与市场的双重驱动下，国产芯片正快速发展，为车载信息安全芯片的未来发展提供了广阔的市场空间与潜力。

2　信息安全算法进展

在车载芯片的信息安全技术中，数据加密是保障车辆通信安全的核心手段，其确保了车辆内部及与外部网络交互数据的机密性，防止车辆位置、行驶习惯、用户个人信息等敏感数据被未授权访问或泄露。密码算法是实现数据加密与隐私保护的关键技术。

2.1　对称加密算法

对称加密是最常见的一种数据加密技术[21]。使用同一个密钥实现数据的加密和解密过程，如图3所示。

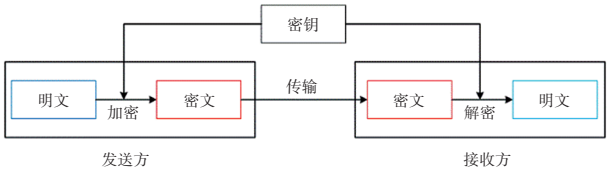


图3　对称加、解密过程示意

发送方通过加密算法和加密密钥将明文加密为密文，接收方接收到密文后通过解密密钥结合解密算法将密文解密。由于该过程中加、解密使用相同密钥和算法，所以加、解密速度快，适合用于有大量数据加密的场景。但在向接收方分配密钥的过程中，若密钥泄露，则攻击方可以直接破解密文。因此，在对称加密中，保证密钥的安全性非常重要，一般采用专属安全通道的方式进行密钥分配，或采用非对称加密的方式加密密钥以保证安全性。

数据加密标准（Data Encryption Standard，DES），是一种对称加密算法，于1976年被美国联邦政府的国家标准局确定为联邦信息处理标准（Federal Information Processing Standards，FIPS）。该算法为分组算法，即每次处理固定长度的数据段，密钥长度为64位（实际为56位）。1999年，在联邦信息处理标准出版物46-3：数据加密标准（Federal Information Processing Standards Publication 46-3: Data Encryption Standard，FIPS PUB 46-3）中，第4次延长DES标准期限，该标准规定普通DES只允许在遗留的系统中应用。2005年，美国国家标准技术研究所（National Institute of Standards and Technology，NIST）确认DES不再作为国际通用的安全加密标准。

三重数据加密标准（Triple Data Encryption Standard，TDES）是DES的强化版本[22]。该算法对加密的数据段应用3次DES加密，其本质是通过多次执行DES增加密钥长度从而提高安全性，并不是一种新的加密算法。1999年10月发布的FIPS PUB 46-3标准规定优先使用TDES。2005年，FIPS PUB 46-3被NIST

官方拒绝，但NIST确认TDES在2030年以前均可用于敏感政府信息的加密。

高级加密标准（Advanced Encryption Standard，AES）[23]用于替代DES，并于2001年发联邦信息处理标准出版物197：高级加密标准（AES）（Federal Information Processing Standards Publication 197: Advanced Encryption Standard (AES), FIPS PUB 197），并于2002年生效[24]。AES可以根据不同的安全等级要求选用不同长度的密钥，如128、192、256位。AES在设计结构及密钥的长度上均满足保护机密信息的要求。目前，AES仍是对称加密中最流行的算法之一。

我国采用SM4分组密码标准，并颁布了GB/T 32907—2016《信息安全技术 SM4分组密码算法》[25]。该算法分组长度与密钥长度均为128位。在安全芯片的国密认证中，支持SM4国密算法是一项强制性技术指标。

2.2 非对称加密算法

1974年，Ralph Merkle提出使用2个不同的密钥实现数据加解密过程，即非对称加密。1976年，Whitfield Diffie和Martin Hellman提出了“Diffie-Hellman密钥交换算法”，该算法是最早的非对称加密算法实例。非对称加、解密过程示意如图4所示。其中，用于加密的密钥被称为公钥，可以被公开，而且不会损害密码系统的安全性，解密密钥通常被称为私钥，必须保密。公钥是私钥经过单向数学函数计算得出，即无法通过公钥反推计算得出私钥。

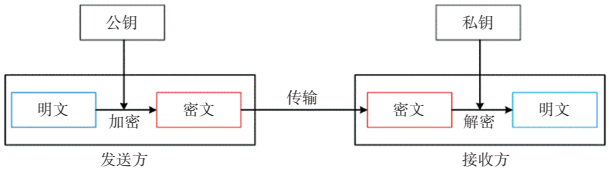


图4 非对称加解密过程示意

由于非对称加密算法实现过程更复杂、速度较慢，其通常不适用于直接加密海量数据。然而，非对称加密的安全性更好，可用于加密少量、重要的数据。在混合加密算法中，使用非对称加密交换对称加密算法的密钥，然后通过对称加密算法数据。除此之外，非对称加密还可以用于数字签名[26]。

RSA（Rivest Shamir Adleman）算法是国际标准算法[27]，由Ron Rivest、Adi Shamir和Leonard Adleman于1977年提出。该算法的安全性源自于其密钥由2个大素数的乘积N构成，且N难以被因式分解。因此只要N足够大，则RSA算法就无法被破解。1999年至2009年期间，密钥长度为512位和768位的RSA被成功破解。据此，美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）建议RSA的密钥长度至少为2 048位。RSA信息安全公司制定了一系列公钥加密标准（Public Key Cryptography Standards，PKCS），规定了RSA密码编译标准，PKCS被信息安全界广泛产业认同，是目前使用最广泛的非对称加密算法。

椭圆曲线加密（Elliptic Curve Cryptography，ECC）是一种基于椭圆曲线的非对称加密算法[28]。该算法将椭圆曲线应用于密码学的理念在1985年被提出。与RSA相比，在同等安全等级下，ECC使用的密钥长度更短，ECC算法也因其高效性被广泛应用。

SM2是中华人民共和国采用的一种非对称加密标准，该算法最初作为行业标准于2012年发布，标准号为GM/T 0003—2012[16]。2017年，其升级为国家标准，标准号为GB/T 35276—2017[29]。在商用密码体系中，该算法主要用来替代RSA加密算法。

2.3 消息摘要算法

消息摘要算法（Message-Digest Algorithm，MD）通过一个单向的哈希函数将任意长度的消息转换为长度固定的哈希值，即消息摘要[30]。所有消息摘要算法均具有以下基本特性：（1）不同的输入对应不同的输出；（2）算法是单向函数，不可恢复。消息摘要算法主要用于消息认证码的生成和数字签名。

消息摘要算法包括MD2、MD3、MD4和MD5。其中，MD5于1992年公开，取代了上一代的MD4算法，与MD4相比增强了算法复杂度与不可逆性。2011年，RFC 6151禁止将MD5应用于消息认证码，被安全哈希算法（Secure Hash Algorithm，SHA）系列算法取代。

SHA是国际标准消息摘要算法[31]，由美国国家安全局提出。其中，SHA-1是NIST于1995年公布的第一代SHA算法，可以生成160位的消息摘要。但后续研究发现，SHA-1无法抵御碰撞攻击，许多组织建议使用SHA-2和SHA-3取代SHA-1。SHA-2是SHA-1的上位替代。SHA-2分为6个不同的算法标准：SHA-224、SHA-256、SHA-384、SHA-512、SHA-512/224和SHA-512/256，其中后缀的数字代表SHA-2生成的消息摘要长度。SHA-3原本名为Keccak算法，其实现方式不同于SHA-1和SHA-2。该算法发布的初衷源自于NIST需要一个与之前算法不同且可替换的消息摘要算法。SHA-3在2015年由NIST通过联邦信息处理标准出版物202：SHA-3标准（SHA-3 Standard: Permutation-Based Hash and Extendable-Output

Functions，FIPS PUB 202）发布[32]。SHA-2 和 SHA-3 是目前国际上最常用的消息摘要算法。

SM3 是一种消息摘要算法标准，国家密码管理局于 2010 年发布行业标准 GM/T 0004—2012 SM3《密码杂凑算法》[17]。2016 年，升级为中国国家密码标准“GB/T 32905—2016”[33]。SM3 主要用于数字签名、生成消息认证码，其安全性和效率与 SHA-256 相同。

2.4 消息认证码

虽然消息摘要算法能够验证数据的完整性，确保数据在传输或存储过程中未遭篡改，但其无法确定数据是否来自可信发送者。因此，消息认证码（Message Authentication Code，MAC）的概念应运而生。MAC 结合了密钥和算法，为数据提供了一个额外的安全层，不仅能够检测数据是否被篡改，还能确保数据的来源经过认证[34]。消息认证过程如图 5 所示。

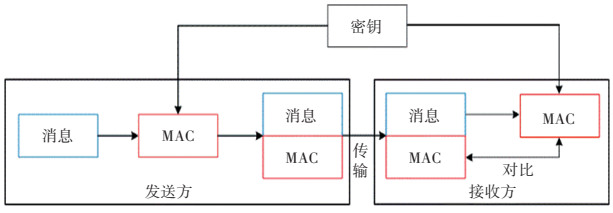


图 5 消息认证过程示意

通信双方持有相同密钥，发送方将消息与密钥作为输入通过消息认证算法生成 MAC 值，并附加在消息后发信至接收方；接收方将接收到的消息和密钥作为输入通过同样的消息认证算法生成 MAC 值，并与收到的 MAC 对比，确认数据来源完整性以及是否被篡改与摘要算法相比，由于计算 MAC 的过程中加入了只有通信双方才知道的密钥 K，当接收到的信息是由不可信的第三方发送时，生成的 MAC 值一定与接收方生成的 MAC 值不同，由此完成消息的身份验证。此外，由于消息认证码对消息本身做对称加密，或对消息和 MAC 的组合做对称加密，具有较高信息安全性。

基于哈希的消息认证码（Hash-based Message Authentication Code，HMAC）是一种基于 Hash 函数进行消息认证的方法。HMAC 与不同的 Hash 函数结合可以产生不同的工作模式，如 HMAC-SM3、HMAC-SHA1、HMAC-SHA224 等。

2.5 小结

对称加密、非对称加密、消息摘要与消息认证码等算法共同构成了信息安全的多层次防御体系。随着信息技术的演进，各类算法持续迭代以满足日益提升的安全需求[35]。目前，国密算法 SM2、SM3 与 SM9 已纳入 ISO 国际标准体系。随着国内密码体系的不断完善，未来将有更多国密算法跻身国际标准体系，并在车载信息安全芯片中的应用日益广泛。

信息安全技术需随计算能力的提升而持续演进，尤其在量子计算兴起的背景下，现有算法需进一步提高安全强度以抵御量子攻击。同时，后量子密码算法的研发与部署也至关重要，以确保其在高速量子计算环境下的安全性[36]。

3 车载信息安全芯片现状及趋势

前文已讨论了智能网联汽车的信息安全标准进展与密码技术。然而，技术的有效落地与产业的健康发展离不开对整体发展脉络的清晰把握。本章节旨在系统梳理当前国内外车载信息安全芯片的技术与标准现状，并在此基础上，阐述其未来演进的关键趋势，以期为构建安全、可靠的智能网联汽车产业生态提供宏观视角与发展路径参考。

3.1 现状

随着车载信息安全技术的快速发展及相关标准的不断完善，国内外芯片企业积极布局，以应对日益增长的市场需求与严格的安全法规。

国外车载计算类芯片具有较强的技术积累和市场份额，英伟达和高通等企业在高性能计算芯片领域占据主导地位。在芯片信息安全方面，国外企业积极研发硬件安全模块[37]，并部署国际通用信息安全算法以保障芯片信息安全。如英伟达推出的 Orin 系列芯片占据了较高的智驾芯片市场份额。该系列芯片集成了信息安全岛，即信息安全子系统。提供算法硬件加速、关键存储、可信执行环境和密钥管理等一系列信息安全技术。此外，其安全引擎支持 NIST 批准的一系列国际通用算法。高通 8295 智能座舱芯片在信息安全技术方面提升显著，并对国际通用算法及其组成部分进行密码算法验证程序（Cryptographic Algorithm Validation Program，CAVP）的认证。可见，国外主流芯片产品均遵循国际安全标准，依托国际通用算法保障芯片安全。

国内车载计算芯片虽起步较晚，但已推出多款具备竞争力的产品。国内企业的产品普遍同时支持国际与国密算法，以满足国内外标准要求。黑芝麻智能武当系列芯片集成独立信息安全岛，支持全系国密算法并通过国密二级认证。芯擎科技的智能座舱和辅助驾驶芯片均支持国密算法。

除在 SoC 中集成安全模块外，部分企业推出独立

安全芯片方案。紫光同芯的T97-315E安全芯片可用于不同的平台和操作系统，具备防护物理和逻辑攻击的能力。该芯片通过CC认证，等级为EAL5+，而且支持国际通用算法和全系国密算法，并通过了国密二级认证。

3.2 趋势

随着未来车载芯片相关标准的进一步完善，国内车载芯片的准入条件将日趋严格，对信息安全的等级提出更高的要求[21]。在此背景下，越来越多国内企业积极支持国密算法并通过国密二级认证，以确保产品安全性与合规性。可见，国密认证将逐渐变为车企审核芯片信息安全特性的重要标准。

目前，车载计算芯片主要采用2种安全实现方式：独立安全芯片与SoC内集成信息安全岛。独立安全芯片适用性广，可为各类ECU与网络通信提供安全增强。而集成信息安全岛则针对具体SoC定制开发，为其提供全方位安全保障。为提升产品竞争力，更多企业选择在SoC中集成信息安全岛，但独立安全芯片仍在特定应用场景中保持其优势。未来，2种方案将长期并存，共同推动车载信息安全技术的发展。

3.3 展望

尽管国内信息安全芯片产业进展显著，但仍缺乏系统性的行业指导规范。为确保其健康发展，需在相关机构或领军企业的推动下，联合整车企业、芯片企业，共同构建信息安全芯片技术发展生态体系。

为实现该目标，需重点推进以下工作：一是建立健全法律法规、标准体系、认证机制、产业合作生态与研发布局，为行业提供制度保障；二是重点攻关软硬件安全、安全认证、芯片设计、国产制造与安全攻防等关键技术；三是持续优化并推广国密算法，增强芯片的抗攻击能力。

4 结束语

本文分析了智能网联汽车信息安全标准的发展进程、密码算法的迭代历程以及车载信息安全芯片发展现状，并展望了车载信息安全芯片的发展趋势。当前，国外主流芯片产品遵循国际安全标准，大多集成信息安全子系统依托国际通用算法保障芯片安全。国内车载计算芯片高度重视信息安全，并普遍在芯片产品中同时集成国际与国密算法以满足国内外相关标准，且有部分芯片已经通过国密二级认证。未来，随着车载信息安全芯片相关标准的进一步完善，芯片准入条件也将越来越严苛，对信息安全的等级提出更高要求。作为国内现行最高标准的信息安全产品认证，越来越多的国内芯片产品会支持国密算法并进行国密二级认证。为保障我国智能网联汽车信息安全技术的良好发展，相关机构在积极推进行业规范的同时，也应注重国密算法的更新迭代，持续优化并推广，联合整车企业、芯片公司推进智能网联汽车信息安全发展。

参 考 文 献

[1] MULDER V, MERMOUD A, LENDERS V, et al. Trends in Data Protection and Encryption Technologies[M]. Cham: Springer Nature Switzerland, 2023.

[2] WOLF M, WEIMERSKIRCH A, WOLLINGER T. State of the Art: Embedding Security in Vehicles[J]. EURASIP Journal on Embedded Systems, 2007: 1-16.

[3] SHON T. In-Vehicle Networking/Autonomous Vehicle Security for Internet of Things/Vehicles[J]. Electronics, 2021, 10(6): 637.

[4] DE VINCENZI M, COSTANTINO G, MATTEUCCI I, et al. A Systematic Review on Security Attacks and Countermeasures in Automotive Ethernet[J]. ACM Computing Surveys, 2024, 56(6): 1-38.

[5] 沈昌祥, 张焕国, 冯登国, 等. 信息安全综述[J]. 中国科学, 2007, 37(2): 1-22.

[6] International Organization for Standardization. Road Vehicles-Functional Safety: ISO 26262[S]. Geneva: International Organization for Standardization, 2018.

[7] International Organization for Standardization. Road Vehicles-Cybersecurity Engineering: ISO/SAE 21434[S]. Geneva: International Organization for Standardization, 2021.

[8] RATHORE R S, HEWAGE C, KAIWARTYA O, et al. In-Vehicle Communication Cyber Security: Challenges and Solutions[J]. Sensors, 2022, 22(17): 6679.

[9] 全国网络安全标准化技术委员会. 信息技术 安全技术 信息技术安全性评估准则: GB/T 18336—2001[S/OL]. (2021-04-25) [2026-7-10]. https://www. bzchaxun. com/view/8136056010000000.html.

[10] 全国网络安全标准化技术委员会. 网络安全技术 信息技术安全评估准则: GB/T 18336—2024[S/OL]. (2021-04-25) [2026-7-10]. https://www. bzchaxun. com/view/8136056 010000000.html.

[11] 邸丽清. 工控产品信息安全评估准则的探讨[J]. 自动化博览, 2016(3): 56-60.

[12] 国家密码管理局商用密码检测中心, 信息安全重点实验室. 安全芯片密码检测准则: GM/T 0008—2012[S/OL].

(2012-11-22)[2026-7-10]. https://saas-chengdu.oss-cn-chengdu.aliyuncs.com/uploads/20220418/101f10ec6226fe03153219161a1fe6ef.pdf.

[13] 国家密码管理局. 祖冲之序列密码算法: GM/T 0001—2012[S/OL]. (2012-03-21)[2026-07-10]. https://std.samr.gov.cn/hb/search/std HBDetailed?id=8B1827F1E807BB19E05397BE0A0AB44A.

[14] 国家密码管理局. SM4 分组密码算法: GM/T 0002—2012[S/OL]. (2012-03-21)[2026-07-10]. https://std.samr.gov.cn/hb/search/stdHBDetailed? id=8B1827F22B99BB19E05397BE0A0AB44A.

[15] 国家密码管理局. SM2 椭圆曲线公钥密码算法: GM/T 0003—2012[S/OL]. (2012-03-21)[2026-07-10]. https://std.samr.gov.cn/hb/search/stdHBDetailed?id=8B1827F1E5FDBB19E05397BE0A0AB44A.

[16] 国家密码管理局. SM3 密码杂凑算法: GM/T 0004—2012[S/OL]. (2016-08-29)[2026-07-10]. https://std.samr.gov.cn/gb/search/gbDetailed? id=71F772D8119BD3A7E05397BE0A0AB82A.

[17] 国家密码管理局. SM2 密码算法使用规范: GM/T 0009—2023[S/OL]. (2023-12-04)[2026-07-10]. https://std.samr.gov.cn/hb/search/stdHBDetailed?id=1BF26B7A9FF6FD76E06397BE0A0A81D8.

[18] 国家密码管理局. SM2 密码算法加密签名消息语法规范: GM/T 0010—2023[S/OL]. (2023-12-04)[2026-07-10]. https://std.samr.gov.cn/hb/search/stdHBDetailed? id=1BF 26B7A9FF7FD76E06397BE0A0A81D8.

[19] 国家密码管理局. SM9 标识密码算法: GM/T 0044—2016[S/OL]. (2016-03-28)[2026-07-10]. https://std.samr.gov.cn/hb/search/stdHBDetailed? id=8B1827F1D5A1BB19E05397BE0A0AB44A.

[20] 上海汽车.《国家汽车芯片标准体系建设指南(2023版)》(征求意见稿)精神解读[J]. 上海汽车, 2023(6): 1-3.

[21] CHANDRA S, BHATTACHARYYA S, PAIRA S, et al. A Study and Analysis on Symmetric Cryptography[C]// 2014 International Conference on Science Engineering and Management Research (ICSEMR). IEEE, 2014: 1-8.

[22] BARKER E, MOUHA N. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher[R]. National Institute of Standards and Technology, 2017.

[23] RIJMEN V, DAEMEN J. Advanced Encryption Standard[J]. Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology, 2001(19): 22.

[24] National Institute of Strandards and Technology. Advanced Encryption Standard (AES): FIPS PUB 197[S]. (2001-11-26)[2026-04-16]. http://doi.org/10.6028/NIST.FIPS.197.wpdl.

[25] 全国网络安全标准化技术委员会. 信息安全技术 SM4 分组密码算法: GB/T 32907—2016[S]. 北京: 全国网络安全标准化技术委员会, 2016.

[26] KAUR R, KAUR A. Digital Signature[C]// 2012 International Conference on Computing Sciences. IEEE, 2012: 295-301.

[27] MILANOV E. The RSA Algorithm[J]. RSA Laboratories, 2009(9): 1-11.

[28] KOBLITZ N, MENEZES A, VANSTONE S. The State of Elliptic Curve Cryptography[J]. Designs, Codes and Cryptography, 2000, 19(2): 173-93.

[29] 全国网络安全标准化技术委员会. 信息安全技术 SM2 密码算法使用规范: GB/T 35276—2017[S]. 北京: 全国网络安全标准化技术委员会, 2017.

[30] MAETOUQ A, DAUD S M, AHMAD N A, et al. Comparison of Hash Function Algorithms Against Attacks: A Review[J]. International Journal of Advanced Computer Science and Applications, 2018, 9(8): 10-18.

[31] DEBNATH S, CHATTOPADHYAY A, DUTTA S. Brief Review On Journey of Secured Hash Algorithms[C]// 2017 4th International Conference on Opto-Electronics and Applied Optics (Optronix). IEEE, 2017: 1-5.

[32] National Institute of Strandards and Technology. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions: FIPS PUB 202[S]. (2025-08-01)[2026-07-16]. https://cloi.org/10.6028/NIST.FIPS.202.

[33] 全国网络安全标准化技术委员会. 信息安全技术 SM3 密码杂凑算法: GB/T 32905—2016[S]. 北京: 中国标准出版社, 2016.

[34] BELLARE M, KILIAN J, ROGAWAY P. The Security of the Cipher Block Chaining Message Authentication Code[J]. Journal of Computer and System Sciences, 2000, 61(3): 362-99.

[35] KUMAR A, GHOLVE A, KOTALWAR K. Automotive Security Solution Using Hardware Security Module (HSM)[J]. SAE Technical Paper, 2024: 2024-28-0037.

[36] LOHMILLER N, KANIEWSKI S, MENTH M, et al. A Survey of Post-Quantum Cryptography Migration in Vehicles[J]. IEEE Access, 2025(13): 10160-10176.

[37] KUMAR A, GHOLVE A, KOTALWAR K. Automotive Security Solution Using Hardware Security Module (HSM)[J]. SAE Technical Paper, 2024: 2024-28-0037.

（责任编辑　**梵玲**）