民用无人机商用密码技术应用与安全性评估研究

唐明环，陈小庆，康晓宁
（中国工业互联网研究院，北京　100102）

摘　要：针对无人机网络安全现状和挑战，深入研究了商用密码技术在民用无人机网络安全防护中的作用，提出了商用密码应用与测试验证方案。该方案构建了无人机系统在实际业务环境中的运行场景，设计了密码应用验证流程，对身份认证、数据传输、数据存储等环节进行了功能及性能测试，对无人机劫持场景进行了对比测试。测试数据显示，应用商用密码后，无人机系统的安全性得到有效提升；加密处理时延对性能影响较小，保证了实时通信性能；国密算法和国际算法性能持平。该研究为无人机密码应用提供了技术支撑，有利于无人机网络安全能力提升。

关键词：民用无人机；网络安全；商用密码；安全性测试
中图分类号：TP309　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2025.07.001
引用格式：唐明环，陈小庆，康晓宁. 民用无人机商用密码技术应用与安全性评估研究［J］. 网络安全与数据治理，2025，44(7)：1-8.

Research on application and security test of commercial cryptography technology for civilian UAV

Tang Minghuan, Chen Xiaoqing, Kang Xiaoning
(China Academy of Industrial Internet, Beijing 100102, China)

Abstract: In view of the current situation and challenges of Unmanned Aerial Vehicle (UAV) network security, the role of commercial cryptography technology in civilian UAV network security protection was deeply studied, and the application and verification scheme of commercial cryptography was proposed. The scheme constructs the operational scenarios of UAV system in practical application environments, designs the cryptography application and verification process, conducts functional and performance tests on identity authentication, data transmission and data storage, and conducts comparative tests on UAV hijacking scenario. Test data shows that after applying commercial cryptography, the security of the UAV system is effectively improved; The impact of processing latency on performance is minimal, ensuring real-time communication performance; The performance of national cryptography algorithms is on par with that of international algorithms. It provides technical support for UAV cryptography application and is beneficial for enhancing UAV network security capabilities.

Key words: civilian UAV; network security; commercial cryptography; security testing

0　引言

近年来，国家鼓励发展低空经济，发展低空经济离不开先进飞行器，以无人机为代表的通用航空装备制造业取得快速发展，民用无人机产业在低空经济发展中的作用越来越明显。随着民用无人机技术的蓬勃发展，无人机网络安全问题日益凸显，成为制约无人机广泛应用的关键因素。无人机在执行各类任务时，需与地面站保持通信，传输的数据包含敏感信息，一旦泄露或被篡改，将对任务完成及隐私安全造成严重威胁。因此，如何有效提升无人机的网络安全，成为当前亟待解决的重要问题。

针对这一挑战，本文深入研究了商用密码技术在民用无人机网络安全防护中的作用，提出了商用密码应用及测试验证方案。该方案构建了密码技术在无人机身份认证、数据传输、数据存储等环节及无人机劫持场景下的实际应用环境，并设计了全面的密码应用验证流程，以验证密码技术在无人机网络安全防护中的有效性和可靠性。通过功能测试和性能测试，评估了不同密码算法在无人机系统中的表现，特别是中国商用密码算法（简称国密算法）SM2 和 SM4 的应用效果。实验数据表明，密码技术不仅能够有效提升无人机系统的安全防护能力，

而且加解密处理时延对性能影响微小，确保了无人机与地面站之间的实时通信。通过性能对比发现，国密算法 SM4 与国际通用算法 AES 的性能持平，并且在传输飞行状态信息时，SM4 的时延低于 AES。

本研究为无人机密码应用提供了实践案例和测试实例，为无人机网络安全能力提升提供了坚实的技术基础。

1 民用无人机网络安全与商用密码技术应用进展

1.1 民用无人机网络安全现状与挑战

民用无人机应用场景已从传统航拍、农业监控扩展到物流配送、灾害响应、环境监测等多个新兴领域。然而，这些新兴应用对无人机的网络安全提出了更高要求，现有安全防护手段[1]却难以满足需求。无人机，特别是民用无人机，正面临着严峻的网络安全威胁。民用无人机主要通过无线通信实现任务指令的下达和数据的回传，其通信的开放性使得无人机易被监听、篡改，甚至被劫持，通信链路的安全问题成为无人机应用面临的重大挑战[2]。

远程劫持：通信协议设计缺陷与软件架构安全短板成为攻击者远程操控的主要路径，攻击者可通过利用通信协议、软件架构等安全漏洞来远程操控无人机[3]；或利用身份验证机制漏洞伪装成授权用户，向无人机注入虚假信息或未授权指令。

拒绝服务攻击和重放攻击：网络被恶意节点劫持时，通过发送大量垃圾信息或干扰信息使网络资源不可用[4]，干扰无人机的正常工作，造成系统瘫痪；攻击者截获合法的通信数据包并重复发送以欺骗系统，导致无人机做出错误响应。

数据窃取与篡改：攻击者可截获并破解无人机与地面站、其他无人机以及基础设施之间的未加密或加密强度不足的通信链路数据，获取重要数据内容，威胁用户隐私安全[5]；或篡改无人机传输的数据，破坏数据完整性，对无人机系统造成损害。

综上，民用无人机网络安全具有防劫持、防窃取、防篡改、高可用等需求，以保障无人机飞行安全和数据安全。商用密码已广泛应用于国民经济发展和社会生产生活的方方面面，通过运用先进的加密算法、科学的密钥管理技术以及严密的身份认证机制，商用密码技术能够为民用无人机的飞行安全和数据安全提供有效防护。

1.2 商用密码在民用无人机网络安全中的应用

目前，已有研究提出了多种无人机网络认证和密钥协商协议，如基于椭圆曲线密码体制的无人机网络认证方案（Authentication Scheme for UAV Network with Support from Ground Control Station, ASUSG）和无控制站支持的无人机网络认证方案（Authentication Scheme for UAV Network Without Support from Ground Control Station, ASWGS)[6]，以及基于国密算法的轻量级无人机网络认证密钥协商协议[7-8]等。然而，这些方案主要集中在解决无人机网络中的身份认证和会话密钥共享问题，对于无人机在实际应用中面临的更广泛的安全需求，如数据完整性、抗重放攻击、非否认性等，并未提供充分的支持。此外，尽管有研究提出了针对无人机系统的安全通信协议[9]，如使用多级认证策略的无人机物联网（Internet of Drones, IoD）安全通信[10]，基于门限安全的对密钥管理方案[11]，但这些研究往往侧重于特定的安全威胁或攻击模型，缺乏对无人机实际应用场景下复杂安全需求的全面考虑。

在民用无人机的安全防护中，商用密码技术的正确应用至关重要。当前许多无人机的设计者和使用者对商用密码技术缺乏深入了解，导致在选择和应用密码算法时存在明显不足，比如倾向于采用已经过时或不符合当前商用密码安全强度的算法。为了提升无人机系统的安全性，应选择合适的商用密码算法，并结合具体应用场景进行综合设计。例如，采用中国国家密码管理局公布的国密算法（包括 SM1、SM2[12]、SM3、SM4[13]、SM7、SM9[14]、祖冲之序列密码算法（ZUC)[15-16]等），这些算法具有较高的安全性和适应性。同时，无人机系统的设计应考虑密钥管理、身份认证和数据完整性等方面的需求，确保通信过程中的数据安全。

具体来说，商用密码技术可以对本地存储数据进行加密保护，防止攻击者入侵设备后获取重要数据内容[17-18]，并建立加密通道保护网络传输数据，确保数据的机密性；可以对存储和传输数据提供识别信息篡改的完整性保护[19]，并通过对固件进行签名和验签，提供数据的可认证性保护；可以通过数字签名等技术强化身份认证与访问控制机制，确保身份的真实性；还可以通过身份鉴别、防重放等措施，降低系统资源被非法请求消耗，抵御拒绝服务攻击，从而防止系统因恶意攻击而瘫痪，确保系统的可用性和稳定性。同时，为了持续应对不断变化的安全威胁，应加强对无人机系统的定期安全评估和及时更新[20]。

依赖国外密码技术不仅增加了技术成本，也带来了潜在的安全风险。一旦发生技术封锁或安全漏洞，将直接影响无人机的正常运行和数据安全。因此，推动无人机系统使用国产商用密码算法[21]并开展安全性评估，是增强无人机网络安全的关键一步。

2 民用无人机商用密码的应用与测试方案

2.1 民用无人机商用密码应用主要环节

民用无人机系统是一个复杂而精细的系统，它主要

由无人机、地面站、地面控制中心构成。无人机根据接收到的指令，结合自身的飞行控制系统和传感器信息，进行飞行动作和任务执行。地面站作为无人机与地面控制中心之间的桥梁，负责接收并转发来自控制中心的指令，同时接收无人机回传的飞行状态信息和传感器数据。地面控制中心是整个控制系统的中枢，它根据任务需求制定飞行计划，并通过地面站向无人机发送具体的操控指令。商用密码技术作为一种有效的安全手段，能够在无人机运行的多个关键环节提供信息安全保障，提升无人机系统整体的安全性，如图 1 所示。

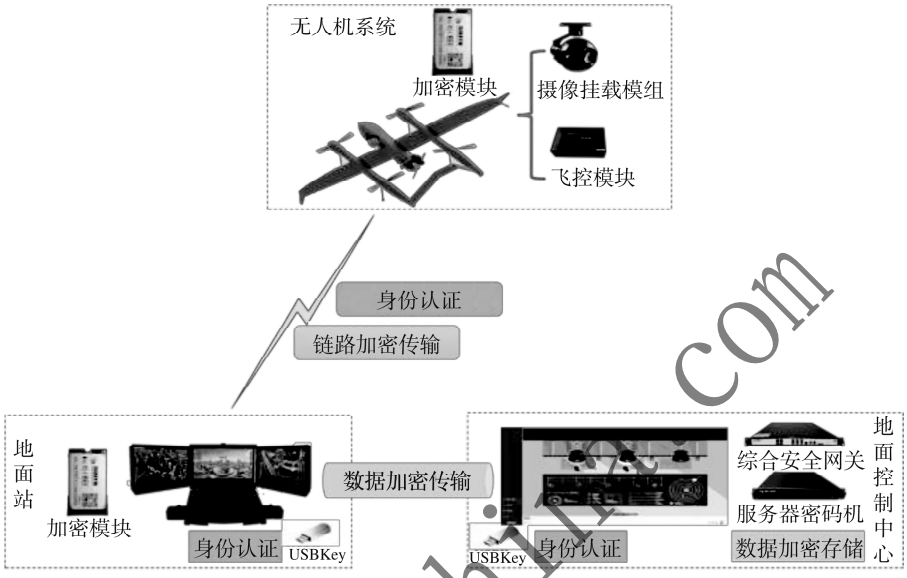

图 1　民用无人机密码应用的主要环节

（1）身份认证环节。身份认证是网络安全的第一道防线，是防止非授权访问、数据泄露和其他安全威胁的关键措施，对于无人机系统安全至关重要。在身份认证环节，主要使用公钥加密算法，例如基于国密算法 SM2 的数字签名技术。当无人机与地面站建立通信连接时，使用数字签名技术对无人机和地面站进行身份互认，确保无人机和地面站身份可信；当操作用户登录地面站及地面控制中心时，使用数字签名技术对用户进行身份认证，确保只有授权的用户能够登录。此外，该环节也能对未授权用户发送的请求进行快速过滤，抵御拒绝服务攻击。

（2）数据传输环节。通信链路作为无人机与地面站之间的核心连接，承担着遥控指令、飞行状态信息及载荷数据等大量数据的交换任务。这些数据通过特定通信协议（如微型空中飞行器链路通信协议（Micro Air Vehicle Link，MAVLink）、Wi-Fi、4G/5G 等）和传输方式，在无人机与地面站之间实现高效、准确的信息传递，是无人机系统稳定运行的基石。由于通信链路中传输的数据往往涉及敏感信息，因此在通信链路中实施链路加密技术以保障数据传输的安全性。在无人机与地面站的数据传输过程中，主要使用对称加密算法（如国密算法 SM4 或国际通用算法 AES）对飞控指令、遥测数据、图像数据等关键信息进行加密处理，从源头上保障数据的机密性。此加密措施直接作用于数据源，有效防止了数据在传输过程中被窃取或篡改，从而确保了无人机与地面站之间通信的可靠性。

（3）数据存储环节。民用无人机广泛应用于涉及国计民生的重要行业，如偏远或危险地区的电网、油气管道、地质灾害等巡检，地形测绘和资源勘察等地质勘探，空气质量、水质、土壤质量等实时环境监测等。无人机在飞行过程中可采集大量地理信息数据、自然资源数据、基础设施布局等敏感信息。如果无人机数据安全得不到保障，可能引起重要数据和核心数据泄露，直接危害经济运行、社会稳定甚至国家安全。因此，在数据存储环节，使用对称加密算法（如国密算法 SM4 或国际通用算法 AES）对重要数据进行加密存储，确保数据的机密性。此外，还可以使用消息认证码（Message Authentication Code，MAC）等商用密码技术对数据进行完整性保护，防止数据在存储过程中被篡改。

2.2　民用无人机商用密码应用场景

本文重点关注无人机劫持场景。劫持是通过技术手段远程接管或干扰无人机的控制权，从而使其脱离合法

操作者的管控。常见的劫持方式包括通信链路劫持（截获或伪造无人机与地面站之间的通信信号）、导航欺骗（通过虚假 GPS 信号诱导无人机偏离航线）、协议漏洞利用（利用无人机控制协议的未加密或弱认证缺陷注入恶意指令）等。

无人机劫持的潜在威胁已经引起了广泛关注。无人机被劫持后，可能与公共基础设施碰撞，甚至对其进行恶意攻击，造成重大安全事故，威胁公共安全；可能飞入禁飞区，利用高清摄像头对涉密要害部位进行拍摄，泄露国家秘密，威胁国家安全；劫持者可能窃取无人机采集的重要数据，造成重要数据泄露。

密码技术是应对劫持威胁的有效防御手段，采用密码技术对控制指令和回传数据进行端到端加密和完整性保护，则非授权地面站将无法解析、伪造或篡改无人机所传输的指令和数据。采用数字证书等方式验证地面站与无人机的合法性，可阻断非授权设备接入。密码技术显著提升了未授权设备劫持的难度，为无人机的安全提供了有力保障。

2.3 民用无人机商用密码应用测试方案

为验证无人机商用密码应用的安全性和可靠性，本文提出了一种系统化的测试方案。该方案构建了民用无人机商用密码应用测试验证平台，包括无人机密码应用系统和无人机密码测试系统两部分。无人机密码应用系统基于真实的无人机系统构建，并集成商用密码能力，作为测试验证的核心对象。可根据预定义的任务在特定业务场景下实现无人机身份认证、数据传输、存储加解密等功能。无人机系统、密码基础设施可进行灵活替换，以实现对多型无人机、多款密码设备的测试。无人机密码测试系统集成了数据采集模块及商用密码应用检测工具，负责从无人机、地面站及地面控制中心等节点收集关键数据并基于该数据对无人机系统中的商用密码应用情况进行测试。测试验证平台部署在实验室，未考虑无人机飞行高度及信号干扰等因素。测试验证平台框架图如图 2 所示。

图 2　无人机密码应用测试验证平台框架图

详细测试步骤如下：

（1）创建测试任务

在测试工作的初始阶段，首先需要基于无人机实际业务场景规划测试任务，确定测试需求，包括身份认证、数据传输、数据存储等密码应用关键环节测试及无人机劫持场景测试。同时，还需设定清晰、可量化的测试评估指标（如测试结果的合规性、加解密时延的长短等），以确保整个测试过程的有效性和针对性。

（2）采集数据

为了获取真实、有效的测试数据，需基于无人机商用密码应用的实际场景，采集无人机系统运行过程中产生的数据。在采集过程中，应特别关注密码应用数据，如验证签名数据、商用密码的加解密操作记录等，这些数据为后续的测试分析提供了支撑。

（3）数据筛选与过滤

在数据采集完成后，需要对这些原始数据进行筛选与过滤。筛选过程可基于时间范围、数据特征、事件类型等多个维度进行，以确保提取出的数据能够贴合测试需求。通过这一步骤，可以去除无关或冗余的数据，保留与测试目标高度相关的测试数据。同时，为了便于后续的分析与处理，还应对这些测试数据进行分段存储。

（4）执行任务并分析结果

任务执行过程中，需要确保系统的稳定运行和数据的实时传输与处理，以便及时获取准确的测试结果。同时，还应对整个任务执行过程进行严密的监控和详细的记录。最终，根据预设的检测规则和测试指标，对测试结果进行深入的分析与比对，得出测试结果。

以上无人机密码应用测试方案涵盖了无人机密码应

用的各个环节，确保了测试的全面性和系统性。该方案能根据不同的测试需求进行配置和调整，从而适应多样化的实际应用场景。同时，利用自动化的测试手段和数据分析工具，提高了测试效率，降低了人力成本。

3 民用无人机商用密码应用安全性测试实例

本节基于测试验证平台进行了民用无人机身份认证、数据传输、数据存储等关键环节及无人机劫持场景中的商用密码应用安全性测试。测试验证平台配置如表 1 所示，无人机及地面站通过集成密码硬件实现身份鉴别、数据传输加密等安全能力。

表 1 民用无人机商用密码应用测试验证平台配置

组件	功能/性能参数
无人机	翼展 >1.6 m，包含全套动力系统、飞控系统、无线电收发系统，挂载光学摄像系统，满足 1 机 2 站通信和控制功能，巡航额定功率 800 W； 主板上集成密码硬件，硬件能力：SM4 加解密速率 140 Mb/s
授权地面站	CPU i5-12500，内存 16 GB，固态硬盘 500 GB，满足与无人机之间的通信和控制功能； 主板上集成密码硬件，硬件能力：SM4 加解密速率 140 Mb/s
非授权地面站	CPU i5-12500，内存 16 GB，固态硬盘 500 GB，满足与无人机之间的通信和控制功能
地面控制中心	部署在通用服务器，服务器硬件配置为 CPU：Intel（R）Xeon（R）Silver 4314 CPU @ 2.40 GHz 64 核；内存：256 GB DIMM DDR4 3 200 MHz；硬盘：1 T SSD； 集成服务器密码机，提供密码运算功能，硬件能力：SM4 加解密速率 850 Mb/s； 集成签名验签服务器，提供数字签名功能，硬件能力：SM2 签名 18 000 次/s，SM2 验签 9 700 次/s

3.1 身份认证环节测试验证

3.1.1 身份认证环节商用密码功能测试

无人机身份认证包括无人机与地面站之间互认、操作员登录地面站、操作员登录地面控制中心 3 类身份认证过程。本文主要论述地面站与无人机的身份认证测试，包括身份认证过程中数字证书的有效性及签名验签流程的正确性。测试内容如表 2 所示。

通过以上测试，验证了无人机与地面站的多个关键安全要素，包括证书的有效期、撤销状态、颁发机构的可信度、密码算法的安全性，以及数字签名过程的有效性。同时，为了确保无人机系统的整体安全性，还对操作员与地面站、操作员与地面控制中心之间的身份认证机制进行了验证，此处不再赘述。

表 2 地面站与无人机身份认证功能测试

序号	测试步骤	测试结果
1	设置测试任务为身份认证测试，启动数据采集	任务启动成功
2	操作被测无人机系统，触发无人机与地面站之间进行身份认证操作，建立连接	无人机与地面站之间成功建立连接
3	测试系统对采集的身份认证数据进行分析	
3.1	获取无人机、地面站数字证书，进行以下验证： （1）证书有效期验证：获取数字证书的起始和结束日期，并将这些日期与当前日期进行比较； （2）证书撤销状态验证：对数字证书撤销状态进行查询，并验证该证书是否在撤销列表中； （3）证书颁发机构验证：获取数字证书的颁发机构信息，并检查该颁发机构是否在可信列表中； （4）密码算法验证：获取数字证书中的密码算法信息，并验证该算法是否为国密算法，安全强度是否符合要求	证书在有效期内，验证了证书的有效性； 证书不在撤销列表中，证明了证书未被撤销； 颁发机构在可信任列表中，验证了证书的颁发机构可信； 算法及安全强度符合要求，验证了密码算法安全性
3.2	签名过程验证： （1）获取发送方数字签名过程中的原始数据、对应的签名值和用于验证签名的公钥，测试系统根据以上数据进行签名验证； （2）获取接收方的验签数据包，将上一步骤中的验签结果与接收方验签结果进行对比	发送方签名数据验证通过，与接收方验签数据对比一致

3.1.2 身份认证环节商用密码性能测试

性能测试指标为身份认证过程中应用商用密码后的时延，以评估商用密码应用对无人机与地面站之间实时通信性能的潜在影响。此处时延指在身份认证过程中，由于采用密码技术进行签名验签操作所导致的额外处理时间。不进行签名验签作为基准测试，因此，身份认证时延约为签名与验签时延的总和。在测试过程中，采用了基于国密算法 SM2 的数字签名和验签技术。为充分评估算法在实际应用中的稳定性，消除偶然影响，每种身份认证操作均测试了 100 次。测试设备选用了高性能计算平台，旨在最大限度地减少测试设备性能对测试结果可能产生的干扰，从而确保测试数据的准确性和可靠性。测试结果如表 3 所示。

表 3　地面站与无人机身份认证性能测试

测试项目	测试次数/次	平均时延/ms
无人机和地面站互认	100	2
操作员登录地面站	100	2
操作员登录地面控制中心	100	2

根据测试结果可以得出以下结论：（1）SM2 签名验签对身份认证时延影响小。测试结果显示，在所有身份认证环节中，采用 SM2 进行签名与验签的平均时延仅为 2 ms。在实际应用场景中，这一时延几乎可以忽略不计，表明 SM2 在保障网络安全的同时，对身份认证性能没有产生显著影响。（2）SM2 表现出高稳定性，适用于无人机身份认证环节。测试结果显示身份认证过程平均时延保持一致，展现出良好的稳定性和可靠性。综上，SM2 算法在实际应用中具备高效性和稳定性，满足无人机身份认证环节对安全和性能的要求。

3.2　数据传输环节测试验证

3.2.1　数据传输环节商用密码功能测试

本小节进行了地面站与无人机之间的数据传输加密测试，以验证数据在加密传输过程中的安全性和可靠性。测试内容如表 4 所示。

表 4　数据传输加密功能测试

序号	测试步骤	测试结果
1	设置测试任务为数据传输测试，启动数据采集	任务启动成功
2	操作被测无人机系统，触发无人机与地面站之间的数传链路、图传链路进行数据传输	无人机与地面站之间成功进行数据传输
3	测试系统对采集的数据传输数据进行分析	
3.1	获取接收端收到的密文数据	在不掌握密钥的情况下，无法正确获得消息内容
3.2	获取发送端原始数据、接收端解密后的明文，并进行对比	解密后的明文与原始数据一致

通过以上测试，验证了数据在传输过程中进行了加密，只有授权方能够解密并正确读取内容。

3.2.2　数据传输环节商用密码性能测试

本小节的关注点为无人机与地面站之间数据加密传输的性能。分别测试了采用国密算法 SM4 以及国际通用算法 AES 进行传输加密带来的额外处理时间。其中，飞行状态数据、飞行控制数据加密的分组模式为输出反馈模式（Output-FeedBack，OFB），视频数据加密的分组模式为密码分组链接模式（Cipher Block Chaining，CBC）。不加密传输作为基准测试，因此，数据传输时延约为明文加密为密文、密文解密到明文的时延总和。无人机向地面站传输的视频数据为 1 080 P，视频传输速率约为 4 Mb/s。该测试重复进行了 100 次以消除偶然误差。测试结果如表 5 所示。

表 5　数据传输加密功能性能测试

测试场景		传输类型	测试次数/次	平均传输时延/ms
无人机向地面站传输	SM4 算法	飞行状态数据	100	1.002
		视频数据	100	1.3
	AES 算法	飞行状态数据	100	1.03
		视频数据	100	1.54
地面站向无人机传输	SM4 算法	飞行控制数据	100	1.003
	AES 算法	飞行控制数据	100	1.002

根据测试结果可以得出以下结论：（1）加密对传输性能影响小。对于飞行控制数据和飞行状态数据的传输，无论是使用国密算法 SM4 还是国际通用算法 AES 进行传输加密，引入的时延均较小（大多在 1 ms 左右），对无人机与地面站之间的实时通信性能影响有限；对于视频数据的传输，加密处理引入的时延相对略大，例如使用国密算法 SM4 时，时延为 1.3 ms。尽管如此，这些时延仍在可接受的范围内，不会严重影响视频数据的实时传输。（2）国密算法与国际算法性能相当。在飞行控制数据和飞行状态数据的数传链路中，国密算法 SM4 与国际通用算法 AES 的加解密时延相差无几；对于视频数据的传输，SM4 时延（1.3 ms）略小于 AES（1.54 ms）的时延。表明在不同传输类型下，国密算法与国际算法的性能可能存在差异，但性能表现相当。（3）根据传输类型合理选择加密算法。鉴于不同传输类型对时延的敏感度不同，应在实际应用中根据具体需求合理选择加密算法。

3.3　数据存储环节测试验证

3.3.1　数据存储环节商用密码功能测试

本小节的数据存储环节指地面控制中心接收飞行日志和视频数据并进行加密存储的过程。测试内容如表 6 所示。

通过以上测试，验证了地面控制中心接收的飞行日志和视频数据在存储过程中采用对称加密算法进行保护的有效性，确保了数据的机密性。

表 6　数据存储加密功能测试

序号	前置条件与测试步骤	测试结果
1	设置测试任务为数据存储测试，启动数据采集	任务启动成功
2	操作被测无人机系统，触发地面站将数据发送至地面控制中心存储	地面控制中心接收地面站传输的数据并加密存储
3	测试系统对采集的数据进行分析	
3.1	获取地面站发送的原始数据、地面控制中心加密后的密文和对应的加密算法及密钥	数据获取成功
3.2	测试系统使用步骤 3.1 中的对称密钥对飞行日志密文和视频数据密文进行解密，并将解密后的数据与原始数据进行比对	解密后的明文与原始数据一致

3.3.2　数据存储环节商用密码性能测试

本小节的关注点为地面控制中心数据加密存储的性能。分别测试了采用国密算法 SM4-CBC 以及国际通用算法 AES-CBC 进行存储加密带来的额外处理时间。不加密存储作为基准测试，因此，数据存储时延约为明文加密为密文的时延。该测试重复进行了 100 次以消除偶然误差。测试结果如表 7 所示。

表 7　数据存储加密性能测试

测试场景		存储类型	测试次数/次	平均时延/ms
地面站往控制中心存储文件	SM4 算法	飞行数据	100	1.003
		视频数据	100	4.81
	AES 算法	飞行数据	100	1.022
		视频数据	100	2.52

根据测试结果可以得出以下结论：（1）加密处理对存储过程影响较小且因存储文件类型而异。对于飞行数据存储，无论是使用国密算法 SM4 还是国际通用算法 AES 进行加密，其平均时延均非常接近基准测试的不加密情况，且均在 1 ms 左右，表明加密处理对这类数据的存储过程性能影响很小；对于视频存储，加密处理引入的时延相对明显，如 SM4 的平均时延为 4.81 ms，但考虑到存储视频对时延的容忍度相对较高，因此这一时延仍在可接受范围内。（2）国密算法与国际通用算法综合性能相当。在存储飞行数据中，国密算法 SM4 的平均时延（1.003 ms）略低于国际通用算法 AES（1.022 ms），表明在处理这类数据时，SM4 算法可能具有更高的性能；在存储视频中，SM4 的平均时延（4.81 ms）虽然高于 AES（2.52 ms），但考虑到 SM4 作为国密算法在安全性上具有额外优势，因此 SM4 的综合性能仍然具有竞争力。

3.4　无人机劫持场景测试验证

在无人机劫持场景测试中，无人机在明文传输模式和密文传输模式下，分别通过授权地面站和非授权地面站对无人机进行操控，验证无人机抵御劫持攻击的能力。对比测试内容如表 8 所示。

表 8　无人机劫持场景对比测试

序号	测试步骤	测试结果
1	明文传输模式下，启动授权地面站并与无人机建立连接，发送控制指令，检查无人机的运行情况	明文指令发送成功，无人机运行正常
2	启动非授权地面站，并向无人机发送控制指令，检查无人机的运行情况	非授权地面站与无人机建立连接并能操控无人机，非授权地面站劫持无人机成功
3	开启密文传输模式，授权地面站发送控制指令，检查无人机的状态和响应	指令传输成功，无人机根据指令进行响应
4	操作非授权地面站与无人机建立连接，并检查无人机的响应及状态	无人机未响应非授权地面站指令，劫持失败

测试结果表明，明文数据能够正常传输，但存在被劫持的安全隐患；而密文传输能有效保障无人机数据传输的安全，降低劫持风险。

本文所述测试环境中，无人机巡航时的额定功率为 800 W，无人机上密码设备的电源适配器规格为输出 12 V、1 000 mA，在正常工作情况下，该设备功耗为 12 W。密码设备最大功耗占无人机总功耗的 1.5%，从电力供应的角度来看，密码设备引入的功耗基本无影响。

4　结束语

本文分析了民用无人机网络安全现状与需求，研究了商用密码技术在无人机网络安全防护中的关键作用和实际应用，提出了民用无人机商用密码应用与测试验证方案。通过全面分析无人机在身份认证、数据传输、数据存储等环节和无人机劫持场景下的安全需求，制定密码应用方案和验证流程，完成了商用密码功能和性能测试。测试结果显示，基于密码技术的身份认证、传输加密、存储加密时延均保持在可接受的范围内，确保了无

人机与地面站之间的实时通信性能不受影响。同时，对比国密算法 SM4 与国际通用算法 AES 的性能时，发现国密算法的表现与国际算法持平，甚至在数传链路上优于国际算法。特别是在安全性方面，国密算法符合我国密码算法标准，为无人机系统提供了更为坚实的安全保障。

参考文献

[1] 王兆轩，李扬，吕洋，等. 无人机系统信息安全前沿技术发展趋势［J］. 软件导刊，2021，20（10）：7－12.

[2] 吴仕豪，潘泉，李扬，等. 无人机“数据链路”信息安全综述［J］. 无人系统技术，2023，6（2）：1－12.

[3] 王云涛，苏洲，邓毅，等. 无人机网络安全综述［J］. 网络空间安全科学学报，2025，3（1）：2－18.

[4] 何道敬，杜晓，乔银荣，等. 无人机信息安全研究综述［J］. 计算机学报，2019，42（5）：1076－1094.

[5] 张凌寒，杜婧. 民法典背景下无人机侵害个人隐私的法律规制［J］. 西北工业大学学报（社会科学版），2020（3）：85－92.

[6] 朱辉，张业平，于攀. 面向无人机网络的密钥管理和认证协议［J］. 工程科学与技术，2019，51（3）：158－166.

[7] 郭锐. 基于国密算法的轻量级无人机网络认证密钥协商协议设计［D］. 西安：西安电子科技大学，2021.

[8] 张敏，许春香，张建华. 无人机网络中基于多因子的认证密钥协商协议研究［J］. 信息网络安全，2022，22（9）：21－30.

[9] 陈世康，周冰，曹宝，等. 无人机安全通信协议研究综述［J］. 通信技术，2024，57（3）：213－221.

[10] PERUMALLA S，CHATTERJEE S，KUMAR A S. Secure communication using multilevel authentication strategy in Internet of Drones［J］. Concurrency and Computation：Practice and Experience，2023，35（12）：e7667.1－e7667.16.

[11] 施君宇. 基于密钥管理的无人机网络通信安全研究［D］. 济南：山东大学，2019.

[12] 谢宗晓，李达，马春旺. 国产商用密码算法 SM2 及其相关标准介绍［J］. 中国质量与标准导报，2021（1）：9－11，22.

[13] 符天枢，李树国. SM4 算法 CBC 模式的高吞吐率 ASIC 实现［J］. 微电子学与计算机，2016，33（10）：13－18.

[14] 谢振杰，刘奕明，蔡瑞杰，等. 国密算法 SM9 的性能优化方法［J］. 计算机科学，2024，52（6）：390－396.

[15] 信息安全技术 祖冲之序列密码算法第 1 部分：算法描述（GB/T 33133.1—2016）［S］. 2016.

[16] 靳文京，郑学欣，孟玉飞. 基于不同密码算法的 MAVSec 安全协议性能研究［J］. 信息安全研究，2023，9（8）：771－776.

[17] 孙国梓，陈丹伟，吴登荣. 一种安全移动存储系统的研究与实现［J］. 计算机工程，2009，35（11）：116－119.

[18] 石翠华. 存储器完整性保护技术研究［D］. 哈尔滨：哈尔滨工程大学，2014.

[19] 韩瑜，孙合敏，邱实，等. 基于混沌序列的无人机测控信息加密方法研究［J］. 空天预警研究学报，2023，37（3）：198－203.

[20] 于攀. 无人机通信安全保障技术研究与实现［D］. 西安：西安电子科技大学，2018.

[21] 滕杰，英吴岚. 探究国产商用密码算法的应用［J］. 信息与电脑（理论版），2023，35（16）：215－217.

（收稿日期：2025－04－03）

作者简介：

唐明环（1988－），女，硕士，高级工程师，主要研究方向：基础通信网络安全、工业互联网安全、商用密码应用安全等。

陈小庆（1986－），女，硕士，工程师，主要研究方向：密码应用安全。

康晓宁（1987－），通信作者，男，硕士，经济师、工程师，主要研究方向：网络安全、信息安全、商用密码应用安全等。E-mail：kangxiaoning@ china-aii. com。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部