



基于国密算法的农业农村安全体系研究

陈洁, 芦天罡, 王彩虹*, 卢月静, 梁建平, 叶旭, 程旭, 杨莹莹, 靳守业

北京市数字农业农村促进中心, 北京 100117

摘要: 随着数字乡村战略的深入推进, 农业农村领域上下级协同和数据共享, 其开放性与智能化带来严峻的安全挑战, 直接关系到国家粮食安全、产业安全和农民切身利益。本文系统梳理了 SM2、SM3、SM4、SM9 及祖冲之算法等国密的特性及其在农业场景中的适用性, 分析了农业农村领域信息系统在终端、传输、平台、数据等方面面临的安全风险, 并依据国家标准, 从物理环境、网络通信、设备计算、应用数据四个层面阐述了密码应用需求。区别现有研究对商用密码方案的简单移植, 本文的核心创新在于面向农业农村差异化场景的“分级密码适配”机制, 并在此基础上, 构建了一个“端、传、云、数”四位一体的国密算法应用的总体框架, 详细阐述了利用 SM2、SM3、SM4、SM9 等国密算法, 实现终端轻量化认证、通道安全传输、云端加密存储、数据可控共享的综合防护方案。本文提出的分级密码适配体系与全链路数据安全控制链, 为破解农业农村领域“安全强度与资源受限矛盾”“数据共享与隐私保护矛盾”提供了可落地的技术路径。最后, 文章提出应从政策标准、技术创新、密码评估等方面协同推进, 构建安全、可信、高效的农业农村安全底座。

关键词: 国密; 数据安全; SM 系列算法; 密码体系; 综合防护

0 引言

近年来, 国家层面推出数字乡村发展行动计划, 旨在推进农业农村大数据平台建设及应用, 加快推进数据资源共享和政务信息化建设, 构建数据资源“一张图”; 完善数据资源目录体系, 规范数据采集、存储、分析, 管理和运用好数据要素, 实现农业农村领域上下级协同和数据共享, 提高农业农村数据流通、使用效率; 同时推动农业农村与政府数字化转型。政府、企业、研发机构等都加快推进数字农业农村发展行动计划。因此, 农业农村大数据平台融合农业农村各类信息数据, 如“人、财、物”相关的基础数据、农业生产发展及交易相关的动态数据和行政许可信息等。随着农业农村大数据平台系统的开放性和智能化程度的不断提升, 数据共享所带来的安全风险也呈现多样化和复杂化的特点, 安全形势日益严峻。

密码是解决网络与信息化安全最有效、最经济、最可靠的手段。现阶段密码技术广泛用于金融、能源、交通、广播电视、政务办公等领域, 但在农业农村领

域需求迫切却基础薄弱, 农业农村领域基础设施薄弱; 农民从业者重视程度不高; 密码成本投入产出比不高; 现有适用于农业农村的“轻量化”密码产品少; 农业领域如育种信息保护等价值未被充分挖掘。

值得注意的是, 农业大数据安全具有区别于工业物联网的差异化需求。首先, 农业传感器多部署于野外环境, 缺乏稳定电源供应, 对密码算法的功耗有严格限制, 需采用轻量级实现方案。其次, 农业生产场景对实时性要求呈现两极分化: 农机自动控制需要毫秒级响应, 而土壤墒情监测等数据采集可容忍较高延迟, 这为算法选型提供了弹性空间。第三, 农业数据具有典型的多源异构特征, 既包含结构化数据库记录, 也包括遥感影像、视频流等非结构化数据, 要求密码方案具备对不同类型数据的适配能力。此外, 农村网络基础设施相对薄弱, 通信链路不稳定, 密码协议需考虑断网续传、离线认证等场景支持。

现在研究多将通用密码方案直接移植到农业领域, 忽略了上述差异化需求, 导致农业农村领域“安

全强度与资源受限矛盾”“数据共享与隐私保护矛盾”进一步放大。为此,本文提出面向农业农村差异化场景的“分级密码适配”机制,构建一个“端、传、云、数”四位一体的国密算法应用的总体框架,旨在实现安全能力与农业场景的精准适配。

国密算法在农业农村领域发展空间广阔,可以用于智慧农业与物联网安全、农村电商与电子支付、农产品溯源与防伪、数字身份与政务管理、育种等敏感数据保护等。国密算法具备保护网络空间实体的身份真实性、数据机密性和完整性及行为不可否认性的能力,实现万物安全可信互联^[1]。

1 国密概况

我国自主研发设计并受到国际认可的核心国密体系,包括祖冲之序列密码算法、SM2、SM3、SM4、SM9等。

祖冲之序列密码算法(ZUC)主要用于智能加密移动终端及链路密码机,在农业农村领域保障无人驾驶农机、北斗导航播种机等设备的位置坐标、作业路径等数据在传输过程中不被篡改或泄露。SM2算法涵盖数字签名、密钥协商与加解密,常用于农产品产销合同的签署、农机购置补贴、农产品保险投保及理赔、电子政务审批等,常与SM3算法协同实现身份认证与安全通信。支持SM3算法的商用密码产品已超3000款,包括安全芯片、终端设备 and 应用系统等多种类型^[2]。在农业农村领域用于农业数据传输的完整性验证和农产品溯源哈希值比对。SM4算法集成于智能密码钥匙、综合安全网关、云服务器密码机密码模块等安全硬件、为农业物联网设备(如无人机、传感器)的实时数据加密传输和农业数据库存储加密提供支持。SM9标识密码算法省去数字证书管理,适用于计算资源受限的农业物联网场景。

在全球数字经济浪潮中,国密成为国际标准,是筑牢全球数据安全基石、提升我国产业核心竞争力的关键所在。现阶段,实现密码运算、密钥管理等核心功能的国密产品,已形成覆盖全面、应用成熟的生态体系。依据功能划分为七大类别:密码算法类(算法芯片、安全芯片)、数据加解密类(密码机、加密硬盘)、认证鉴别类(认证网关、动态口令系统)、证书管理类(CA系统)、密钥管理类(KMS)、密码防伪类(印章系统、数字水印系统)、综合类(安全平台)^[3]。

2 农业农村领域信息系统的安全挑战分析

农业农村领域信息系统由于其应用场景的特殊性,面临着比一般信息系统更为严峻和复杂的安全挑战。同时已建农业农村领域信息系统的加密算法存在不符合国家标准、行业标准的情况,存在恶意软件植入、未授权访问平台资源等风险。

2.1 终端侧风险

数据采集源头广,涵盖物联网传感器、无人机、农机装备、农户手机APP、执法PAD等多种终端。终端设备数量庞大、分布广泛,且普遍存在计算与存储能力不足的问题,难以运行复杂的安全协议,未使用密码技术进行访问身份认证,存在非法设备接入和数据伪造的风险。同时,也存在现有安全方案对终端“一刀切”地采用相同认证强度,强算力终端(如边缘网关)被强制采用与传感器相同的低强度认证,造成算力浪费;弱算力终端(如土壤温湿度传感器)无法运行高强度密码算法,导致认证形同虚设,亟需一种基于算力分级的轻量化认证机制。

2.2 传输侧风险

农业农村的种植业、宅基地、农村金融保险、农业执法、农产品质量、种业等数据在政府部门及科研院所的系统之间进行调用,数据传输过程中未国产加密或加密强度不够,极易被不法分子抓取与监控,敏感数据存在被截取、篡改等风险。智慧农业场景下,差异化业务对网络性能与安全等级的需求存在显著冲突。例如,农机远程控制要求毫秒级低延迟与高安全强度,而墒情监测则能容忍秒级延迟。现有传输加密机制普遍为静态策略,缺乏根据异构网络环境与业务需求进行动态自适应调整的能力。

2.3 平台侧风险

农业农村数据存储在云平台或者本地机房,数据集中化存储面临高风险。各地建设的农业农村大数据平台汇聚全域农业农村数据,形成了价值巨大的“数据富矿”,必然成为黑客攻击的重点目标。若未按照国家密码管理部门要求设置有效的门禁系统、监控系统;云平台未做好租户管理、租户之间密钥未做安全隔离、未提供加解密、签名验签等云密码服务,就会造成恶意篡改或非法访问,影响数据的可信度。

2.4 数据侧风险

各地建设的农业农村大数据平台需要向政府、科研机构、企业、农户等不同主体提供数据服务。在数据共享与交易过程中,确保“数据可用不可见”,同时应用系统重要数据存储传输的机密性、敏感信息资源安全标记的完整性等都需要采用符合密码安全要求的技术,防止程序被恶意卸载、账号被非法破解、敏感信息被越权访问、重要文件日志被删除等,影响平台安全性和责任划分。当前农业农村数据共享普遍采用粗放式授权,缺乏基于数据分类分级的精细化访问控制,导致敏感数据(如育种基因序列、高精度遥感影像)在共享过程中易被滥用。

农业农村领域密码应用监管过程中,存在多网多域密码应用数据采集难、敏感数据明文传输动态监测难、信息系统密码应用方案一致性分析难等问题^[4],同时各个信息系统操作行为责任难追溯,安全审计体系有待完善。平台上的数据查询、分析、下载等操作,特别是涉及关键决策或资金补贴的业务,需要明确的操作责任认定。缺乏有效的不可否认性机制,会导致在发生安全事件或纠纷时,无法追溯和定责。

3 农业农村领域密码应用需求

2021年3月,国家市场监督管理总局、中国国家标准化委员会正式发布GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》,用于规范信息系统密码应用的建设,指导开展信息系统商用密码安全性评估,标准分为五个等级,从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面提出密码应用技术要求,保障信息系统的实体身份真实性、重要数据的机密性和完整性、操作行为的不可否认性;并从信息系统的管理制度、人员管理、建设运行和应急处置四个方面提出密码应用管理要求,为信息系统提供管理方面的密码应用安全保障^[5]。

3.1 物理和环境安全需求

农业农村领域信息系统应建立完善的物理环境安全机制,落实物理环境中的操作管理,防止未授权的访问、损坏和干扰,以保证数据的可用性、保密性和完整性。重点需要使用密码技术对物理环境的访问人员进行身份鉴别,对机房电子门禁进出记

录和视频记录进行完整性保护,保障系统所处的物理和环境安全。

3.2 网络和通信安全需求

农业农村领域数据通信需在各类异构网络信道中实现安全防护,在通信前采用合规的密码算法和数字证书对通信实体进行身份鉴别;在通信过程中采用合规的密码算法保证数据的完整性、重要数据的机密性;采用具有商用密码产品认证证书的安全认证网关以确保网络边界访问控制信息的完整性及接入设备身份的真实性。针对农业场景中窄带物联网(NB-IoT)、5G专网、卫星通信并存的异构网络,需设计能够根据网络类型动态协商密码套件的自适应安全通信协议。

3.3 设备和计算安全需求

农业农村领域各类场景涉及的基础设施及设备包括服务器、数据库、堡垒机以及密码产品等。对各类设备和计算环境的安全防护要采用密码技术做好身份鉴别;服务器、云堡垒机远程管理采用国家密码管理部门核准的密码算法,采用经商用密码产品认证的密码产品进行密钥管理;采用密码技术保护服务器、数据库日志记录的完整性、重要可执行程序的完整性和真实性;可信计算环境的建立等。

3.4 应用和数据安全需求

农业农村领域系统应用和数据安全主要是对应用程序安全漏洞和数据全生命周期各个环节进行防护。在应用程序方面做好身份鉴别、访问控制、完整性校验、安全审计等;在数据安全方面,做好重要数据入库或落盘保存后以密文形式存储、数据传输过程中采用密码技术实现机密性和完整性保护、同步开展数据分类分级工作^[6],采用数据加密方案和数字签名技术实现访问控制和日志防篡改。数据分类分级构成密码动态适配的先决条件,亟需构建各省市农业农村业务场景的数据分类分级标准体系,并据此形成“分类分级-加密策略-访问控制”的自动映射闭环。

4 农业农村领域国密安全体系构建

为解决平台的全生命周期安全挑战,本文提出“端、传、云、数”四位一体的国密算法应用的总体框架,并针对农业场景的差异化需求进行优化设计,实现国密算法从静态密码组件向动态密码适配能力的范式跃迁——以终端算力、数据敏感度、网络状态、

业务实时性为决策因子，自动协商最优国密算法组合与安全策略，达到安全与效率的动态平衡。

4.1 国密保障端侧轻量化认证与数据源头可信

从田间地头的智能传感器、控制器到加工包装环节的防伪标识，从实验室的基因测序仪到冷链物流环节的环境监测，这些海量、资源受限的农业物联网终

端在农业生产、经营、管理和服务中广泛使用，通常采用轻量级国密方案实现安全接入（如表 1 所示）。SM4 硬件加速效率高，辅以轻量化设计后，适用于资源受限的物联网设备；SM2 在同等的安全强度下，计算速度快，可优先选择；SM3 抗碰撞性强，适合数据完整性保护。

表 1 国密算法终端应用
Table 1 Terminal Applications of Chinese Cryptographic Algorithms

终端类别	计算能力	典型设备	推荐算法	认证特点	管理开销
强算力	高	智能农机、边缘网关	SM2 双向认证	指令签名与验证、通信加密	数字证书，安全性高，适合关键控制节点
中等算力	中	农事作业监管手持终端、智能耳标、植保无人机	SM2 精简认证或 SM9	数据签名转发	SM2 基于证书，SM9 基于 ID，管理简化
低算力	低	温湿度传感器、土壤探头	SM9	单向验证，SM3 哈希+SM9 签名	设备 ID 为公钥，即插即用，无需证书
极简	极低	水产监测标签、无线按钮	轻量级 SM9	基于标识的单向认证	免证书

采用 SM2 替代 RSA 进行终端身份认证，可将单次认证耗时从百毫秒级压缩至数十毫秒级，有效缓解农业传感器在弱网络条件下的认证超时问题。SM3 通常不单独使用，与 SM2/SM9 等签名算法协同工作，从源头保障数据可信。强算力终端使用过程中，SM3 提供远程控制指令、软件升级包、重要日志等生成哈希值并签名，防止指令被篡改，保障设备安全；中等算力终端使用过程中，SM3 提供传感器数据、转发的控制命令生成哈希值并签名，确保数据在汇总和转发过程中不失真；低算力/极简终端使用过程中，SM3 提供采集的原始数据生成哈希值并签名，确保上传数据的真实性，防止伪造。在资源受限的边缘设备上，采用选择性加密方案相较于全量 AES-256 加密，可显著提升性能^[7]。采用 SM4 进行数据加密传输，其硬件加速特性可在资源受限的边缘网关上实现 70 Mbps 级别的加密吞吐率，满足多路传感器数据并发的处理需求。

4.2 国密构建异构网络安全传输通道

农业农村领域通过在传输协议中采用国密算法、轻量级国密数字证书技术，实现通信双方身份鉴别和协议报文的机密性。云平台在政务外网接入域部署支持国密算法套件的安全认证网关，对数据进行高强度加密和完整性保护；在国密浏览器中采用国密算法进行业务访问，实现业务人员、运维人员等各类用户通信的安全性；私有无线路由器通过硬件集

成，在链路层的无线通信环节采用国密算法加密，增强底层通信保障。

农业农村数据安全传输就要保障从农业耕种管收各环节传感器的数据到边缘网关，再从边缘网关到云平台中心的数据传输通道安全。从安全风险角度分析，这些数据量巨大而且涉及的使用权限复杂，不适宜使用单一的密钥对整个系统进行加密设计^[8]。在私有无线路由器，通过高速的 SM4 算法对传输的业务数据（作物长势图像、土壤墒情与墒情图像）进行加密，实现密文传输^[9]；应用系统应在数据传输中采用密码机为每个环节提供可信，同时做好密码资源配额。等保三级/四级需满足对密码设备“分区、分权、分域”管理的强制要求（如图 1 所示）。

4.3 国密筑牢云端集中管控与合规审计

平台云端国密体系以租户层和平台层双层部署，云平台依托基础设施、平台密钥统一管理和服务安全防护，为租户提供了底层的安全运行支撑。云租户通过应用层加密、租户密钥控制、业务数据保护，保障了自身业务数据的安全控制（如图 2 所示）。原则上，云上应用系统所处的云平台的安全级别应不低于云上应用系统^[10]，平台层密钥与租户密钥必须严格分离，对密钥、证书等密码资源实施全生命周期管理。同时，密码资源池可以实时监控密码设备或密码应用服务的情况，如果发现异常及时预警，保证云端系统的稳定加密运行^[11]。

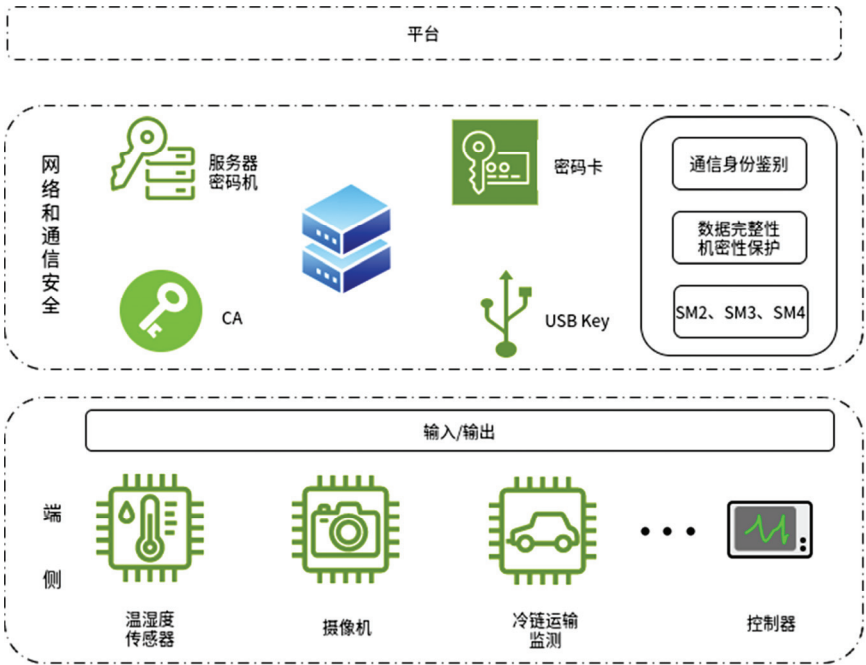


图 1 安全通信应用架构

Fig. 1 Secure communication application architecture



图 2 云平台商用密码应用服务

Fig. 2 Cloud platform commercial cipher application services

在云平台环境中，通过国密技术构建全栈数据安全体系。通过云端密码资源池实现密码计算资源的弹性伸缩与统一调度，避免分散部署密码设备带来的重

复投资。数据库透明加密（TDE）采用 SM4 算法对存储层的农户身份、地块信息、补贴金额等敏感数据进行自动加密，密钥由集中管控的云密码机统一管理，

实现存储安全。数字签名存证利用 SM3 生成土地确权、作物产量、畜牧质检等核心数据的摘要，并通过 SM2 进行数字签名，确保数据在生命周期内的完整性与防篡改性，满足审计与溯源要求。国密与隐私计算融合则结合 SM2 同态加密与 SM4 密钥共享技术，在农业信贷风控、产量预测、作物病虫害分析等联邦学习或多方计算场景中支持密文状态下的协同分析，实现“数据不动价值动”的安全数据共享。整体方案形成覆盖数据存储、传输、使用全流程的云端密码保护闭环。

在密文检索方面，崔永杰等提出了基于国密算法的多用户公平可搜索加密方案。该方案利用 CP-ABE 对属性私钥指定树形访问结构实现细粒度访问控制，结合 SM4 分组算法处理数据集，基于区块链解决交易公平性问题。实验表明，安全索引生成时间处于毫秒级，且密文检索效率不呈线性增长，具有一定的稳定性^[12]。Huang 等研究无配对可搜索加密方案计算时间较双线性对方案减少 7 至 28 倍，同时引入并行搜索机制，进一步提高搜索效率^[13]。

4.4 国密实现全链路数据加密与防篡改

通过国密算法的有机结合，构建了数据产生、存储、传输、使用、共享和销毁的全生命周期安全防护体系（如图 3 所示），特别是 SM9 与属性基加密的结合，为复杂数据畅通场景提供了灵活、可扩展的安全保障，实现了比传统 RBAC 更细粒度的访问控制。祁

嘉琪等提出了基于 SM2 和 CP-ABE 的医疗访问控制改进方案，采用多属性机构授权架构，与传统 CP-ABE 方案相比加解密性能提升约 10%^[14]。例如农产品溯源数据可支持“生产基地查看种植记录、物流企业获取运输信息、监管部门审阅质检报告”的分段式权限控制；“伏羲农场”OODA 循环各阶段产生的数据（观察数据、融合信息、决策指令、行动反馈）均可设定为伴随业务演进的动态属性加密策略。

农业农村数据在农业农村大数据平台中流动共享，网络入侵、漏洞攻击、端口开放、非法接入等都成为风险点，面临数据破坏、窃取、篡改、伪造、非法使用等安全挑战，需要对农业农村数据进行分类分级，明确数据保护策略^[15]。同时，采用国密算法构建体系化的安全防护架构，实现算法协同运作。SM2 建立信任基础，农业补贴发放环节采用 SM2 签章对公示名单进行电子签章，实现“阳光补贴”的可信溯源；SM3 确保数据真实，种质资源的特征基因序列生成 SM3 哈希值写入区块链存证，确保种源知识产权可验证；SM4 实现高效加密，农业遥感分辨率卫星影像采用 SM4 高效加密，保障国家空间地理信息安全；SM9 支持标识密码，农业信贷敏感信息经 SM9 加密后，满足属性的用户即可解密评估，杜绝数据滥用；ZUC 保障通信安全，农田水利系统通过 ZUC 算法生成加密流进行传输远程控制指令，实现“一次一密”的安全控制。

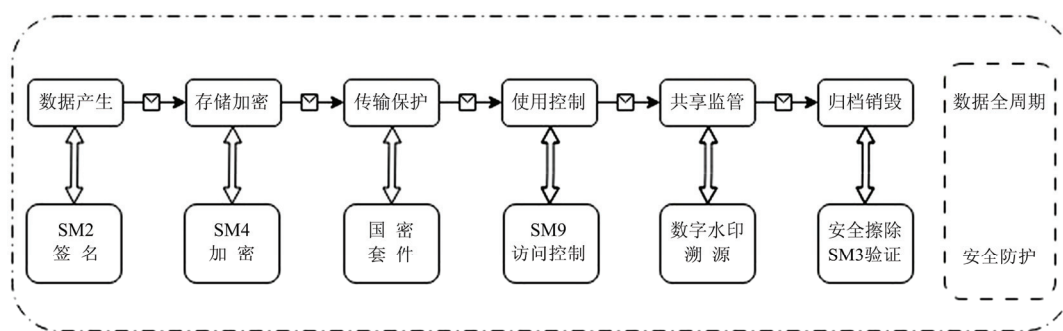


图3 数据全生命周期安全控制链

Fig 3 Data full life cycle security control chain

4.5 GB/T 39786—2021 标准符合性分析

本保障体系在物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面全面对接 GB/T 39786—2021 的技术要求。物理和环境

安全层面，采用密码技术实现机房门禁身份鉴别与视频监控记录完整性保护。网络和通信安全层面，通过安全认证网关实现通信实体双向身份鉴别，采用国密算法保障传输数据的机密性与完整性。设备

和计算安全层面,对登录用户进行身份鉴别,远程管理建立安全传输通道,并利用密码技术保护日志完整性。应用和数据安全层面,对重要数据实施传输与存储的机密性保护,满足标准对身份鉴别、访问控制、安全审计等要求。

针对农业农村数据分散、主体多元的特点,密码应用应贯穿数据分类分级、加密保护、访问控制全流程,实现数据机密性、完整性保护与日志防篡改^[16]。管理层面应建立覆盖密码人员管理、密钥管理、软硬件及介质管理、建设运行与应急处置的完整制度,实行密钥管理员、安全审计员、密码操作员“三员分立”,并定期开展密码应用安全性评估,确保管理体系符合 GB/T 39786—2021 的管理要求。

为了进一步强化标准中网络通信、设备计算、应用数据等层面的技术落地能力,本保障体系借鉴了电力行业成熟的国密应用经验。电力行业标准 DL/T 2767—2024 与 T/ZJSEE 0049—2025 从物理环境、网络通信、设备计算、应用数据四个层面提出密码应用要求,与 GB/T 39786—2021 架构高度契合。在终端轻量化认证方面,电力物联网采用基于 SM9 的两级密钥分发架构,由 KMC 为终端生成标识私钥实现双向身份认证,有效解决资源受限终端的证书管理难题,该方案已在国网山东电力等单位得到验证^[17],农业农村系统可结合终端算力分级优化端侧差异化认证策略。在野外终端密钥管理方面,电力物联网基于 LKH 实现组密钥管理,支持单播与广播数据的轻量级加密,并按密钥用途采取混合式存储管理,农业农村传感器可借鉴此方案,在边缘网关部署轻量级 KMS 模块。在安全传输通道方面,电力系统采用 SM2/SM3/SM4 算法实现双向认证与加密传输,通信延迟控制在毫秒级,农业农村系统可结合 NB-IoT、5G 专网等异构网络特点设计自适应安全通信协议。上述电力行业实践经验在技术实现层面与 GB/T 39786—2021 各层面的安全要求形成有效映射,为本保障体系全面符合国家标准提供了坚实的技术支撑。

5 结语

本文解释了“算力分级-算法协同-策略动态调整”的内在机理,为解决农业物联网中安全强度与资源受限的冲突提供了系统化方案;构建了覆盖端、传、云、数的一体化防护链路,实现了安全策略与

业务属性的深度耦合,支撑涉农数据“可用不可见”可信流通;在分级终端认证、网络感知加密、租户级资源隔离及标签化策略映射等层级取得技术突破,打造了覆盖农业全产业链的可信安全底座。

在农业农村数字化转型的关键时期,数据已成为驱动发展的核心要素。面对海量涉农数据的深度整合与安全共享、数据质量提升与标准化治理、数据价值的深度分析与智能挖掘以及创新应用的孵化和智能决策支持等多重挑战^[18],国密作为保障农业农村领域的“安全底座”,其重要性愈发明显。特别是在“端、传、云、数”四位一体中,国密技术的系统性应用,不仅是筑牢智慧农业与数字乡村的安全屏障的关键支撑,更是推进涉农数据要素可信流通的基础保障。因此,必须协同各方力量,系统性推进国密的应用与创新,为智慧农业筑牢可信基石。

一是政府与监管机构要高度重视,明确在高标准农田监测、种质资源库、农村金融、农产品溯源等核心领域的密码应用强制性或指导性标准;科研与产业机构重点研发适用于农业场景“轻量化”国密芯片、促进密码技术与农业 AI、大数据等融合创新;农业企业与合作社将密码安全纳入企业核心风险管理体系,主动开展密码化改造,确保合规;农业技术从业者掌握基础知识和配置技能,同时切实提升广大农民群体的密码素养与保密自觉。

二是任何国密都有各自的优势和不足,在实际使用过程中并非互相替代,而是相辅相成的关系。根据具体的安全需求、业务场景和预算限制,可以单一采用也可以有机组合。从商用密码顶层设计来看,深刻理解并推动各类国密技术和产品的战略级协同,通过将认证、加密、密钥管理等功能模块化、服务化,并进行有机组合,为不同等级的信息系统构建可扩展、内生可靠的主动防御体系。

三是农业农村领域等保三级信息系统每年开展一次商用密码应用安全性评估,对网络与信息系统使用商用密码技术、产品、服务和管理的正确性、合规性、有效性进行检测分析和评估验证。如密评结果未达到国家合规要求,为解决安全隐患,需及时制定全面的密码应用整改方案、申请密码应用整改专项经费,采购和部署必要的密码产品(如加密机、密钥管理系统等),并引入专业的技术服务,确保快速构建有效的密码防护体系。

参考文献

- [1] 霍炜,郭启全,马原,等. 商用密码应用与安全性评估[M]. 北京: 电子工业出版社, 2025.
- Huo W, Guo Q Q, Ma Y, et al. Commercial Cryptography Application and Security Assessment[M]. Beijing: Electronic Industry Press, 2025.
- [2] 姜海舟,潘文伦,陈彦平,等. 商用密码权威指南[M]. 北京: 机械工业出版社, 2025.
- Jiang H Z, Pan W L, Chen Y P, et al. Authoritative Guide to Commercial Cryptography[M]. Beijing: Machinery Industry Press, 2025.
- [3] 曹春杰,韩文报,等. 密码科学与技术概论[M].北京: 清华大学出版社,2023.
- Cao C J, Han W B, et al. Introduction to Cryptozoology and Technology[M]. Beijing: Tsinghua University Press, 2023.
- [4] 丁杰,袁智伟,马丽,等. 政务领域商用密码应用监管平台架构与关键技术研究. 信息安全与通信保密,2025(9):52-61.
- Ding J, Yuan Z W, Ma L, et al. Research on the architecture and key technologies of commercial cryptography application supervision platform in the government field. Information Security and Communications Confidentiality, 2025(9):52-61.
- [5] GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求[S]. GB/T 39786-2021 Information security technology-Basic requirements for information system cipher application [S].
- [6] 张永伟,张新红,等. 数据安全时代[M]. 北京: 机械工业出版社,2023.
- Zhang Y W, Zhang X H, et al. Data Security Era[M]. Beijing: Machinery Industry Press, 2023.
- [7] Jagatha A, Kappala A, Kamepalli M, et al. A novel approach to quantum-resistant selective encryption for agricultural sensors with limited resources[C]//2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC). January 6-8, 2025. Las Vegas, NV, USA. IEEE, 2025: 00262-00271.
- [8] 黄宏基. 商用密码技术在水利信息系统的设计与应用.广东水利水电,2022(9): 77-81.
- Huang H J. Design and application of commercial cryptography technology in water conservancy information systems. Guangdong Water Conservancy and Hydropower, 2022(9): 77-81.
- [9] Gong R, Zhang H, Li G, et al. Edge computing-enabled smart agriculture: Technical architectures, practical evolution, and bottleneck breakthroughs. Sensors, 2025,25(17):5302.
- [10] 彭浩楠,唐明环,查奇文,等. 云计算场景商用密码应用研究.信息安全研究,2023(9):375-381.
- Peng H N, Tang M H, Zha Q W, et al. Research on the application of commercial cipher in cloud computing scenarios. Information Security Research, 2023(9):375-381.
- [11] 梁鹏. 政务云商用密码应用技术研究.福建电脑,2025(59):29-33.
- Liang P. Research on commercial encryption application technology of government cloud. Fujian Computer, 2025(59):29-33.
- [12] 崔永杰,彭长根,丁红发,等. 一种支持多用户的公平密文检索方案. 计算机技术与发展, 2022(10): 100-107,113.
- Cui Y J, Peng C G, Ding H F, et al. A fair ciphertext retrieval scheme supporting multi-user. Computer Technology and Development, 2022(10): 100-107,113.
- [13] Huang M J, Gan J J, Yang B, et al. Efficient public key authenticated searchable encryption scheme without bilinear pairings. Computer Standards & Interfaces,2025,94:104016.
- [14] 祁嘉琪,莫欣岳,周永恒,等. 基于国密算法 SM2 和 CP-ABE 的医疗访问控制系统的设计与实现. 网络安全与数据治理, 2023, 42(7): 37-42,48.
- Qi J Q, Mo X Y, Zhou Y H, et al. Design and implementation of medical access control system based on national secret algorithms SM2 and CP-ABE. Network Security and Data Governance, 2023, 42(7): 37-42,48.
- [15] 王伟忠,闫瑞泽,查奇文,等.工业互联网商用密码应用体系研究.信息安全研究,2024(10):519-525.
- Wang W Z, Yan R Z, Zha Q W, et al. Research on commercial cryptography application system of industrial Internet. Information Security Research, 2024(10):519-525.
- [16] 薛亚东,秦琳,黄宁辉,等. 林业数据分类分级方法研究. 农业大数据学报, 2025, 7(2): 213-219.
- Xue Y D, Qin L, Huang N H, et al. Classification and grading method for forestry data. Journal of Agricultural Big Data, 2025, 7(2):213-219.
- [17] 王辉,袁家辉,时振通,等. 电力物联网下终端密钥全生命周期安全管理方案. 电子技术应用, 2025, 51(1): 103-112.
- Wang H, Yuan J H, Shi Z T, et al. Full lifecycle security management scheme for terminal keys under power IoT. Application of Electronic Technique, 2025,51(1):103-112.
- [18] 哈晓琳,李杰,原育慧,等. 农业农村数据融合服务平台的设计与应用实践. 农业大数据学报, 2025, 7(4): 468-484.
- Ha X L, Li J, Yuan Y H, et al. Research on the architecture and key technologies of agricultural and rural data fusion service platforms. Journal of Agricultural Big Data, 2025, 7(4): 468-484.

引用本文: 陈洁, 芦天罡, 王彩虹, 卢月静, 梁建平, 叶旭, 程旭, 杨莹莹, 靳守业. 基于国密算法的农业农村安全体系研究[J]. 农业大数据学报, 2026, 8(3): 338-346. DOI: 10.19788/j.issn.2096-6369.000156.

CITE: CHEN Jie, LU TianGang, WANG CaiHong*, LU YueJing, LIANG JianPing, YE Xu, CHENG Xu, YANG YingYing, JIN ShouYe. Research on Agricultural and Rural Security System Based on State Commercial Cryptography Algorithms[J]. Journal of Agricultural Big Data, 2026, 8(3): 338-346. DOI: 10.19788/j.issn.2096-6369.000156.

Research on Agricultural and Rural Security System Based on State Commercial Cryptography Algorithms

CHEN Jie, LU TianGang, WANG CaiHong*, LU YueJing, LIANG JianPing, YE Xu, CHENG Xu, YANG YingYing, JIN ShouYe

Beijing Digital Agriculture and Rural Promotion Center, Beijing 100117, China

Abstract: With the further advancement of the digital rural strategy, collaboration and data sharing in the agricultural and rural fields, its openness and intelligence have brought severe security challenges, which are directly related to national food security, industrial security and the vital interests of farmers. This article systematically sorts out the characteristics of State Commercial Cryptography such as SM2, SM3, SM4, SM9 and Zu Chongzhi's algorithm and their applicability in agricultural scenarios. It analyzes the security risks faced by information systems in the agricultural and rural areas in terms of terminals, transmission, platforms, data, etc., and elaborates on the cryptographic application requirements from the four levels of physical environment, network communication, equipment computing, and application data based on national standards. Different from the simple transplantation of commercial cryptographic schemes in existing research, the core innovation of this article lies in the "graded cipher adaptation" mechanism for differentiated scenarios in agriculture and rural areas. On this basis, this article constructs an overall framework for the application of State Commercial Cryptography algorithms that integrates "terminal, transmission, cloud, and digital". It elaborates on the use of State Commercial Cryptography algorithms such as SM2, SM3, SM4, and SM9 to achieve comprehensive protection solutions for lightweight terminal authentication, secure channel transmission, cloud encrypted storage, and controllable data sharing. The hierarchical cipher adaptation system and full-link data security control chain proposed in this article provide a practical technical path to solve the "contradiction between security intensity and resource limitation" and the "paradox between data sharing and privacy protection" in the agricultural and rural fields. Finally, the article proposes that policy standards, technological innovation, cipher assessment and other aspects should be promoted collaboratively to build a safe, credible and efficient agricultural and rural security base.

Keywords: State Commercial Cryptography; data security; SM series algorithms; cryptography system; comprehensive protection