

面向新型关键基础设施的密码应用安全性评估技术综述

李高磊¹, 李建华¹, 周志洪¹, 张昊²

(1. 上海交通大学电子信息与电气工程学院, 上海 200240; 2. 中国信息安全测评中心, 北京 100085)

摘要: 随着5G/6G、人工智能、区块链等新技术在各领域的深度融合发展, 以高速率全时段信号覆盖、智能化精细化城市管理以及深空深海科学创新实验场为代表的新型关键基础设施建设迈进新阶段。作为保障国家信息、融合、创新基础设施安全的关键技术资源, 密码应用安全性评估亟须深入数据生命周期内构建全方位、细粒度、自演进的密码安全性评估体系。结合近年来能源、医疗、交通等行业新型关键基础设施面临的典型APT攻击、勒索病毒攻击等, 重点分析了在防范内生数据安全风险、实现差异化隐私保护、支撑可认证攻击溯源等新业态需求下日益增长的密码应用安全性评估需求。分析了新型信息基础设施(包括大数据、5G通信、基础软件等)、融合基础设施(包括智能网联汽车、智能网联工业控制系统等)、创新基础设施(包括大数据、人工智能、区块链等)给密码应用安全性评估带来的新挑战, 阐述了部署在高性能计算芯片、超高速通信模组、大容量存储介质上的国产密码算法与协议对密码应用安全性评估技术的新要求。对发展自动化、智能化密码应用安全性评估技术进行了展望。

关键词: 新型关键基础设施; APT攻击; 密码应用; 安全性评估; 国产化; 智能化

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023079

Review of cryptographic application security evaluation techniques for new critical infrastructures

LI Gaolei¹, LI Jianhua¹, ZHOU Zhihong¹, ZHANG Hao²

1. School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China

2. China Information Security Evaluation Center, Beijing 100085, China

Abstract: The construction of new critical infrastructure, represented by high-speed full-time signal coverage, intelligent and fine-grained urban management, and deep space and deep sea scientific innovation experimental fields, has entered a new stage with the deep integration and development of new technologies such as 5G/6G, artificial

收稿日期: 2023-03-08; 修回日期: 2023-08-05

通信作者: 李建华, lijh888@sjtu.edu.cn

基金项目: 国家自然科学基金(62202303, U20B2048), 上海市扬帆计划项目(21YF1421700), 国防基础科研项目(JCKY2020604B004)

Foundation Items: The National Nature Science Foundation of China (62202303, U20B2048), Shanghai Sailing Program (21YF1421700), Defence Industrial Technology Development Program(JCKY2020604B004)

引用格式: 李高磊, 李建华, 周志洪, 等. 面向新型关键基础设施的密码应用安全性评估技术综述[J]. 网络与信息安全学报, 2023, 9(6): 1-19.

Citation Format: LI G L, LI J H, ZHOU Z H, et al. Review of cryptographic application security evaluation techniques for new critical infrastructures[J]. Chinese Journal of Network and Information Security, 2023, 9(6): 1-19.

intelligence, and blockchain in various fields. The security evaluation of cryptography applications, as a key technological resource for ensuring the security of national information, integration, and innovation infrastructure, has risen to the level of international law and national development strategy. It is urgent to construct a comprehensive, fine-grained, and self-evolving cryptography security evaluation system throughout the data lifecycle. The typical APT attacks and ransomware attacks faced by new critical infrastructure in industries such as energy, medicine, and transportation in recent years were considered. And then the growing demand for security evaluation of cryptography applications was analyzed in the face of new business requirements such as preventing endogenous data security risks, achieving differentiated privacy protection, and supporting authenticated attack traceability. The new challenges were also examined, which were brought by new information infrastructure (including big data, 5G communication, fundamental software, etc.), integration infrastructure (including intelligent connected vehicles, intelligent connected industrial control systems, etc.), and innovation infrastructure (including big data, artificial intelligence, blockchain, etc.) to the security evaluation of cryptography applications. Furthermore, the new requirements were revealed about domestically produced cryptography algorithms and protocols deployed on high-performance computing chips, ultra-high-speed communication modules, and large-capacity storage media for cryptography application security evaluation technology. Finally, the development of automated and intelligent cryptography application security evaluation technology was explored.

Keywords: new critical infrastructure, APT attack, cryptography application, security evaluation, domestication, intelligentization

0 引言

新型关键基础设施以信息网络为基础,向数字化、智能化、无人化产业应用转型升级提供基础性、公共性、通用性服务,并支撑战略科技创新发展的物质工程设施。信息、融合和创新3方面内容构成了当前新型关键基础设施的技术体系架构,如图1所示。关键信息基础设施主要是指基于5G/6G、人工智能、区块链、星链等新一代信息通信技术演化生成的基础性设施^[1]。关键融合基础设施主要是指在传统关键信息基础设施的基础上应用万物智联技术进行智能化、自动化改造后所形成的新形态,包括以智能工厂、智慧物流、孪生城市等为代表的社会服务型公共设施。创新关键基础设施是指支撑前沿交叉学科基础理论研究、战略新兴技术突破、全产业链服务集成的具有长远发展布局属性的关键基础设施。新型关键基础设施具有与传统基础设施不同的鲜明特点,除具备基础性、公共性和强外部性等一般特征外,新型基础设施具有许多区别于传统基础设施的鲜明特点。

1) 新型关键基础设施尚处于发展的初级阶段。与经过百十年技术迭代而来的传统基础设施不同,新型关键基础设施的市场需求、产品形态、

主导技术、商业模式等尚未稳定成型。

2) 新型关键基础设施的自然垄断性较低。在信息网络之上构建的新型关键基础设施通常支持“一点接入,全网服务”,快速的传播复制使其相关技术核心的迭代周期被进一步缩短,给国家透明监管带来严峻挑战^[2]。

3) 数据和网络安全的重要性进一步突显。一方面,必须构建有效促进数据流通的制度环境和技术标准体系。另一方面,对基础设施的网络安全可靠要求更高^[3]。数字世界和物理世界高度融合、孪生,各类新型关键基础设施联网运行、共享数据,数据和网络安全成为最基础的保障条件之一。

商用密码应用安全性评估(简称“密评”)旨在对已采用商用密码技术、产品和服务集成建设的网络和信息系统进行密码应用合规性、正确性、有效性测评验证。面向新型关键基础设施安全的密评工作直接关系到国家安全、国计民生和公共利益,加快构建新型关键基础设施密评体系是应对日益严峻的网络安全形势的基础。但新型关键基础设施不同于传统的信息系统,传统的密码算法与密码应用技术无法直接迁移到新型关键基础设施上,这给面向新型关键基础设施的密码应用及密评技术带来了新需求与新挑战。

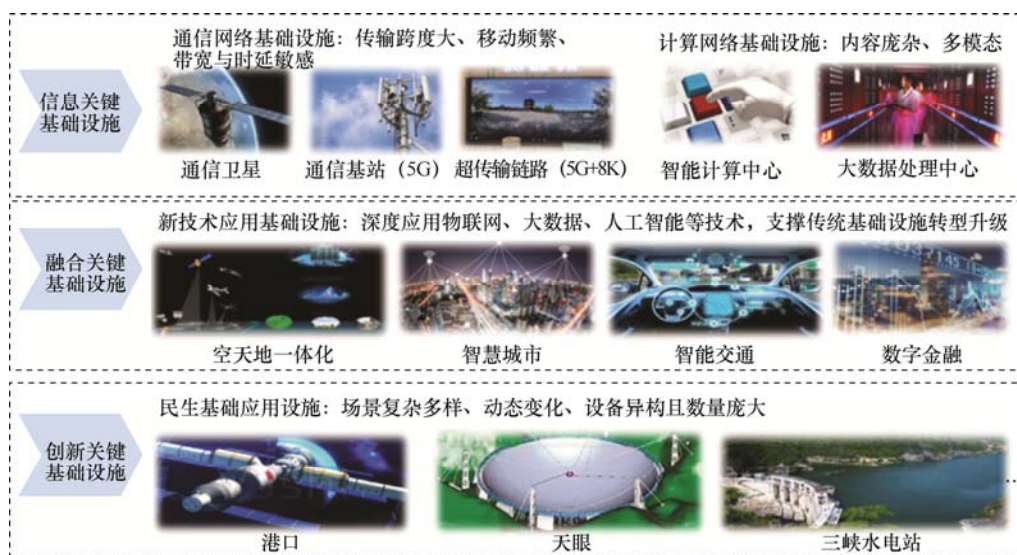


图1 新型关键基础设施的技术体系架构

Figure 1 The technical system architecture of new critical infrastructure

1) 密码算法存在设计缺陷, 导致新型关键基础设施易被攻击。MD-SHA 系列是知名的 Hash 函数家族, MD5、SHA-1 和 SHA-2 均被广泛应用于互联网服务。2013 年, 文献[4]提出一种构造 SHA-1 碰撞的新方法, 将攻击复杂度从 2^{69} 降低到了 2^{61} , 并在 2017 年公布了 SHA-1 算法碰撞实例。文献[5]发现了被 NIST 选定的抗量子加密算法 CRYSTALS-Kyber 的安全漏洞, 攻击者利用该漏洞可建立侧信道攻击。

2) 密码算法效率低, 无法在通信时延敏感以及高密度计算场景下部署^[6]。在美国, NIST FIPS 140 是国家强制标准^[7]。2021 年, FIPS 140 已更新至第三版, 设定了更高的安全性基准以适用医疗保健与金融等产业敏感数据保护需求, 但是 FIPS 140 认证过程时间长、成本高。我国在认证标准的制定上仍然处于跟随状态, 现行的 GM/T 0028-2014 参考 FIPS 140-2 编写。提升自主创新能力, 突破密码算法设计、标准制定长期受制于人的被动局面是我国面向新常态的战略目标之一^[8]。

3) 大量密码应用中存在组件重用、安全管理不规范等问题, 亟须构建基于需求分析、设施建设、电子认证、密码监管的密码应用管理体系。根据《2022 年 APT 威胁趋势预测》报告^[9], 针对云安全 and 外包服务的攻击激增, 关键密码

或 API 密钥的失窃导致大量数据资源甚至业务功能中断。同时, 勒索软件即服务^[10]成为一种利益化、产业化的新型黑客攻击模式, 具有极强的抗检测、反溯源能力。我国许多关键行业如金融、电信、航空等领域的关键基础设施仍采用国外的密码算法和测评标准, 一旦有人利用潜在漏洞发起规模化攻击, 会对关键基础设施甚至国家安全造成严重威胁^[11]。例如, 2021 年黑客组织利用被盗的旧 VPN 凭据获得了对美国管道运营商燃气管道基础设施网络的访问权限, 并发起了震惊全球的勒索病毒攻击。为应对日益频发的大规模网络攻击, 国家市场监督管理总局联合国家标准化管理委员会于 2021 年正式发布了《信息安全技术 信息系统密码应用基本要求》, 进一步规范了关键信息系统尤其是工业控制系统、关键办公系统中密码技术、产品、服务的使用。

新型关键基础设施安全保护体系的建立健全依赖于网络安全防护能力的提升, 需运用密码学基础理论与核心技术达到防泄密、防篡改、防假冒和抗抵赖的目的; 同时, 为确保新型关键基础设施中密码算法、密码协议等相关密码应用实现的正确性、合规性、有效性, 亟须构建专用于新型关键基础设施的密码安全性评估技术体系。

1 密码应用安全性评估的基本需求

密码应用安全性评估与关键信息基础设施安全检测评估、网络安全等级测评制度、分级保护测评制度紧密衔接,是夯实安全基础、满足多方合规、保证整体安全的关键技术手段。但密码应用安全性评估与三者之间存在明显的区别,创新发展和掌握密码测评这一网络安全核心技术,是牢牢掌握网络安全主动权、争夺网络空间话语权的重要举措。密码应用安全性评估的主要依据是《信息安全技术 信息系统密码应用测评要求》和《信息系统密码应用测评过程指南》,二者的制定主要是依据国家密码管理局最新发布的 GM/T

0054-2018《信息安全技术 信息系统密码应用基本要求》,针对待测信息系统中所使用的商用密码产品和密码技术,测试其密钥管理、密码配用策略、密码实现机制、密码安全防护策略、网络和通信安全、应用和数据安全等各方面的主要内容,以确定其通过密码产品和密码技术实现的信息系统真实性、机密性、完整性和抗抵赖性。

根据《商用密码应用安全性评估管理办法(试行)》给出的定义,商用密码应用安全性评估主要针对信息系统已采用的商用密码技术、产品和服务进行合规性、正确性和有效性检测和评估。其发展历程主要包括4个阶段,如表1所示。

表1 密码应用安全性评估的发展历程
Table 1 The development history of cryptography application security assessment

发展阶段	时间	标志性文件
第一阶段: 制度奠基期	2007.11—2016.08	《信息安全等级保护商用密码管理办法》 《<信息安全等级保护商用密码管理办法>实施意见》
第二阶段: 再次集结期	2016.09—2017.04	《商用密码应用安全性评估管理办法(试行)》 《关于开展密码应用安全性评估试点工作的通知》
第三阶段: 体系建设期	2017.05—2017.09	《商用密码应用安全性测评机构管理办法(试行)》 《商用密码应用安全性测评机构能力评审实施细则(试行)》 《信息安全技术 信息系统密码应用基本要求》(GM/T 0054-2018)
第四阶段: 密评试点开展期	2017.10—至今	《信息安全技术 信息系统密码应用基本要求》(GB/T 39786-2021) 《关于规范商用密码应用安全性评估结果备案工作的通知》(国家密码管理局[2021]392号) 《信息安全技术 信息系统密码应用测评要求》(GM/T 0115-2021) 《商用密码应用安全性评估管理办法》(2023.11) 《信息安全技术 信息系统密码应用测评过程指南》(GM/T 0116-2021)

为了适应新型关键基础设施安全保障需求,提高我国网络安全整体意识,近年来《中华人民共和国国家安全法》《中华人民共和国网络安全法》《中华人民共和国密码法》《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》和《信息安全技术 网络安全等级保护基本要求》相继发布和正式实施。其中,《中华人民共和国网络安全法》第五条明确规定国家应采取措施对关键信息基础设施进行保护;第十条明确指出网络数据的完整性、保密性和可用性应加以维护;第三十八条要求运营者每年至少进行一次检测评估。《中华人民共和国密码法》旨在规范密码应用和管理,促进密码事业发展,保障网络与信息安

全,其中第八条规定公民、法人和其他组织可依法使用商用密码保护网络与信息安全;第二十七条明确提出关键信息基础设施应当使用商用密码进行保护,并自行或者委托第三方商用密码评估机构开展商用密码应用安全性评估。同时,《信息安全技术 网络安全等级保护基本要求》强化了对通信传输、数据存储、身份鉴别、密钥管理等环节的密码应用与管理要求。《中华人民共和国数据安全法》规定在鼓励数据流动、共享乃至交易的情况下应确保数据安全,对在合作研发、履行义务、执行任务中知悉的个人隐私、个人信息、商业秘密等相关数据应依法予以保密,不得非法向他人泄露或者提供。相关法律法规的频繁颁布和

实施标志着我国对密码应用与测评工作的推动力度正在不断加大。

1.1 密评技术体系建设的基本需求

密评工作的责任主体是涉及国家安全、社会公共利益等重要领域的数据采集系统、网络传输系统、信息分析系统、决策控制系统的建设、使用、管理单位。密评对象包括基础信息网络、重要信息系统、重要工业控制系统、政务信息系统，以及关键信息基础设施、网络安全等级保护中第三级及以上的信息系统^[12]。密评技术体系建设的基本需求（如图2所示）主要包括密评理论基础、密评研发工具、密评工程管理以及密评服务平台4个方面。其中，密评服务平台必须依托密评技术，按照密评标准规范进行建设。

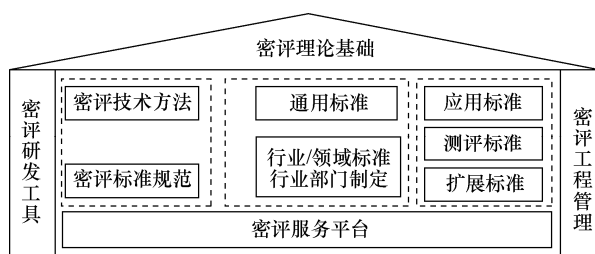


图2 密评技术体系建设的基本需求
Figure 2 The basic requirements for the construction of technical system for cryptography evaluation

常用的密评技术包括密码算法评测、密码协议评测、数字证书评测和密钥管理评测。依托上述密评技术，密评工作可实现对不同安全等级信息系统的商用密码应用是否达到具有相应等级安全保护能力的评估。在实际应用中，密评工作能够有效支撑对物理安全、网络安全、主机安全、应用安全、数据安全的等级保护测评。

(1) 密评工作的理论基础

为满足各领域密评工作的基本需求，研究人员提出了诸多理论模型。其中，密评工作的理论基础（如图3所示）包括4个方面：① 统计学；② 软件/固件完整性校验；③ 侧信道分析；④ 黑/白盒测试。

在统计学方面，常用的关键理论包括时间序列分析、抽样与抽样分布、参数估计与有限机模型、假设检验等。对于序列密码（即流密码），将明文串按位加密成密文字符，具有实现简单、速度快、错误传播少等特点。序列密码算法的关键

是密钥序列生成器，而密钥序列通常具有极大的周期性，现代密码机数据传输率高达 10^8 bit/s，如果10年内不使用周期重复的密钥序列，则要求密钥序列的周期 $T \geq 3 \times 10^6$ 或 255。序列密码具有良好的统计特征，在一个周期内0、1游程的频率大抵相当，因此，可用统计方法由密钥序列提取密钥生成器的结构或密钥的信息进而建立密码安全性评估模型^[13]。

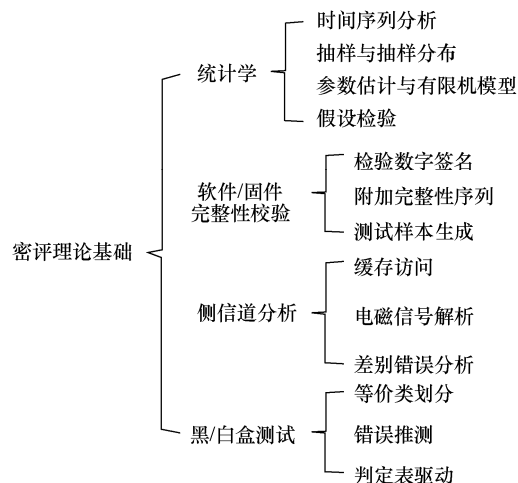


图3 密评工作的理论基础
Figure 3 The theoretical foundation of cryptography evaluation work

在软件/固件完整性校验方面，常用的关键理论包括校验数字签名、附加完整性序列、测试样本生成等^[14]。与统计学方法不同，软件/固件完整性校验既适用于序列密码也适用于分组密码。它是通过软件/硬件产生的随机数作为密码验证的样本，从而测试密码算法的验签速率、正确性等。

在侧信道分析方面，常用的关键理论包括缓存访问、电磁信号解析以及差别错误分析等。侧信道分析技术主要是针对密码芯片、密码协议、密码系统等进行信息窃取的一类网络攻击手段，首先获取硬件设备在密码算法运行过程中泄露的能量、电磁等多种类型的物理信息，在此基础上直接或间接获取密码算法产生的中间值信息。随着人工智能和密码学的融合发展，基于深度学习的芯片侧信道攻击与防御技术在近年来得到了快速发展。

在黑/白盒测试方面，常用的关键理论包括等价类划分、错误推测、判定表驱动等。黑盒测试

通常假设攻击者对设备终端不了解或不完全了解,也无法对设备上的软硬件进行更改;而白盒测试假设攻击者对设备终端(即应用程序的运行环境)拥有完全的控制能力,能够观测并更改软件运行时的所有内部数据。白盒环境下,攻击者具有更强的攻击能力。传统黑盒环境下设计的密码学原语在白盒环境下通常极度脆弱。通过生成大量黑盒测试样本库和白盒测试样本库对密码应用安全性开展评估有助于提升密码算法、密码管理以及系统整体的安全性^[15]。

(2) 密码应用安全性评估工具

密码应用安全性评估工具的主要目标包括:

① 统一评估对象管理,确保无漏项,可视化评估进程中各环节的评估对象和评估维度;② 统一评估流程、报告标准,提高评估效率,支持高效规范的密评操作,生成标准统一、合规的密评报告。根据国家密码管理局发布的《商用密码应用安全性评估测评工具使用需求说明(试行)》,密码应用安全性评估的相关工具(如图4所示)通常分为通用测评工具、专用工具和管理平台3个部分,密评机构在使用测评工具开展现场测评时,应依据测评方案中确定的测评对象、测评指标、测评工具接入点及测评内容实施,具体如下。

在通用测评工具中,密码破解工具支持字典破解、暴力破解、彩虹表破解和带掩码攻击的暴力破解以及GPU加速破解等。根据密码分析者可能取得的分析资料的不同,密码分析工具主要包括以下4类:① 唯密文分析,密码分析者仅能获

取一个或多个用同一密钥加密的密文;② 已知明文分析,密码分析者不仅可以获取待破译的密文,还可以获取一些用同一密钥加密的明文与密文对;③ 选择明文分析,密码分析者可取得同一密钥加密的任何明文(不包括待恢复的明文)所对应的密文对;④ 选择密文分析,密码分析者可取得其所选择的任何密文(要破译的密文除外)所对应的明文,这些密文和要破译的密文是用同一解密密钥解密的。目前主流的密码分析工具包括 iCrypto PRO、CrypTool 2。

密码协议分析工具^[16]对密码协议的保密性、可信性、有序性和高效性进行分析测试。其中密码协议是以现有密码体制为基础构建的、主要运行在计算机通信网或分布式系统中的交互通信协议,借助于密码算法来达到密钥分配、身份认证^[17]等目的。例如,商用加密算法 AES 和 DES 需要在安全通信之间实现通信双方的密钥共享,因而构建了基于 RSA 的密钥交换协议、基于 KDC 的密码分发协议、基于 DH 的密钥交换协议以及基于物理层的密钥交换协议等,同时为了实现安全多方计算、电子货币、电子选举等,还设计了 Shamir 秘密共享、不经意传输等密码协议。

在专用工具中,算法性能检测工具应支持对商用密码算法 SM2、SM3、SM4、SM9 的测试,具备 BASE64 进行编解码、随机数检测及字符与进制之间的相互转化等操作功能,通过算法性能测试工具可以精准地确认密码算法是否正确、合规、有效。协议安全检测工具首先对待测密码协

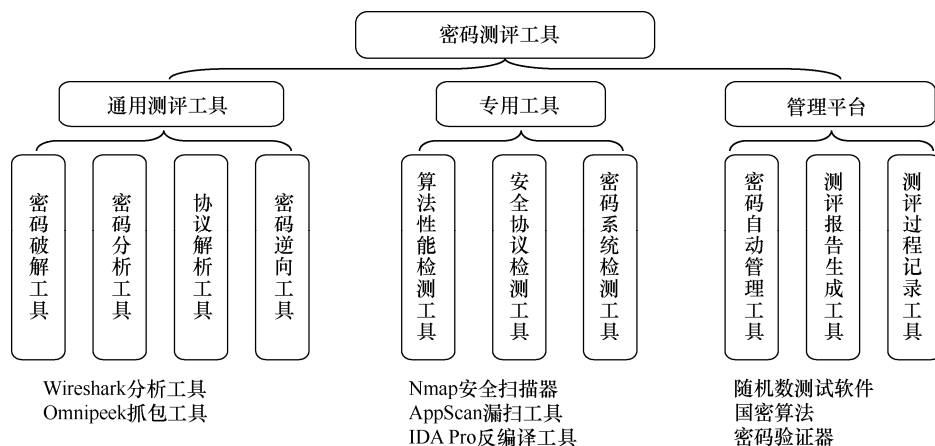


图4 密码应用安全性评估的相关工具
Figure 4 Tools for cryptography application security assessment

议进行形式化建模,然后利用时序逻辑等刻画待测协议的特性,并利用基于状态搜索的方法检测安全协议验证分析过程中的漏洞。密码系统检测工具旨在检测密码系统自身的安全性,它会模拟多种密码破解的方式来攻击待测密码系统,从而评估出待测密码系统的安全程度,发现安全隐患并提升密码安全性,进而降低被破解的风险。对密码系统的检测通常会集成对称密码算法性能检测、非对称密码算法性能检测和摘要计算性能检测以及密码实现过程的安全检测,进而判断密码系统的运算能力是否满足业务应用需求。

在管理平台中,传统的密码管理、测评报告生成和过程记录均依赖专业人员在现场进行分析,效率低、周期长。近年来,自动化、智能化的管理平台建设逐渐得到重视。一方面,测评过程记录逐渐可视化、电子化;另一方面,密码管理和测评报告生成引入了人工智能、区块链等新技术,大幅缩短了测评周期^[18]。

我国非常重视商用密码产品的监督检查技术和装备的研究,国家密码管理局先后下达商用密码行政执法——IPSec/SSL VPN 便携式取证工具以及商用密码行政执法——智能密码钥匙和接触式智能 IC 卡检查工具的研制任务,国家密码管理局检测中心联合上海交通大学完成了相关课题样机研究,并于 2014 年取得了国家首个“SST1301 商用密码产品信息采集与算法验证平台”的工具型号,该工具可对网络中的 IPSec/SSL VPN 协议进行合规性检查分析,并对智能密码钥匙和接触式智能 IC 卡进行密码算法合规性检查和正

确性验证。中海闻达推出了商用密码基线检测仪、商用密码基线在线监测系统等测评工具,可分析网络中常用加密协议、加密算法,发现安全隐患,并能够生成密码应用安全性评估报告。安恒信息发布密评工具箱,针对客户使用的密码产品、密码技术进行使用正确性、配置正确性以及管理正确性的安全检查。

1.2 密码应用安全性评估的基本流程

密码应用安全性评估的基本流程与等保测评 2.0、关键信息基础设施安全检测评估的基本流程相比,具有诸多鲜明特征。首先,在实际开展过程中的密码应用安全性评估的评估周期有所差异。针对被识别为关键基础设施的系统,为避免重复测评,可先确定等级保护对象,确定安全级别、进行关键基础设施识别/安全防护、开展密码应用方案/等级保护建设方案评估、开展等级测评及密评工作以及进行关键基础设施安全检测评估。针对三级以上的等级保护对象、关键基础设施,商用密码应用安全的评估周期为每年至少一次。其次,商用密码应用安全评估的工作流程具有独特的特征,主要包括确定评估对象、开展测评工作、输出密评报告、上报密评结果 4 个阶段。而等级保护测评包括定级、备案、建设整改、等级测评、监督检查 5 个规定动作;关键基础设施安全检测评估则主要包括识别认定、安全防护、检测评估、监测预警、事件处置 5 个环节。为了更清晰地展示三者的区别,图 5 展示了网络安全等级保护测评和关键基础设施安全检测评估的基本流程。不同测评技术的适用范畴如表 2 所示。

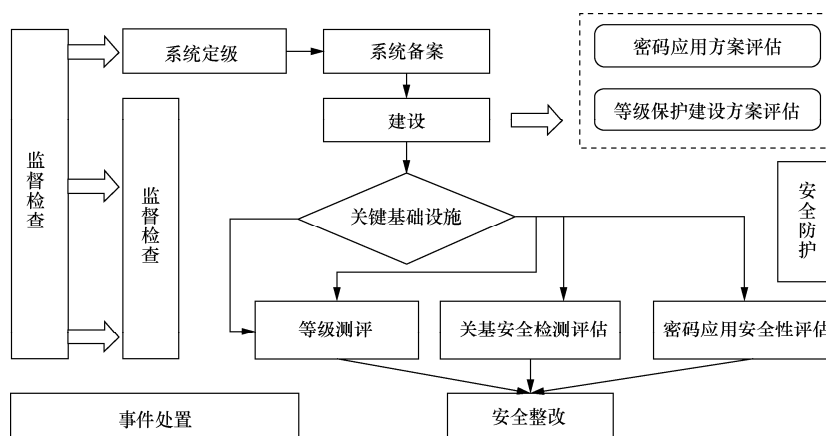


图5 网络安全等级保护测评和关键基础设施安全检测评估的基本流程

Figure 5 The basic processes of network security level protection assessment and critical infrastructure security evaluation

表 2 不同测评技术的适用范畴
Table 2 The application scope of different evaluation techniques

技术类别	评估对象	参考标准	评估内容
密评	关键信息基础设施、网络安全保护第三级以上系统、国家政务信息系统	《商用密码应用安全性评估测评过程指南》	总体要求
			密码功能要求
			技术应用要求
			密钥管理
等保测评	通信网络设施、信息系统、数据资源	《信息安全技术网络安全等级保护测评过程指南》 (GB/T28449-2018)	安全管理
			安全物理环境
			安全通信网络
			安全区域边界
			安全计算环境
			安全管理中心
			安全管理制度
			安全管理机构
			安全管理人员
			安全建设管理
关基安全检测评估	关键信息基础设施	《信息安全技术 关键信息基础设施安全检查评估指南》	安全运维管理
			合规检查
			安全技术检测
			分析评估

等保测评 2.0 是依据国家信息安全等级保护制度和技术标准规定的，由国家授权的测评机构对非涉及国家秘密的信息系统进行检测评估。其中，“等保 2.0”是按新的等级保护标准规范开展工作的统称，新标准新规范是指《中华人民共和国网络安全法》《商用密码应用安全性评估管理办法》颁布实行更新的网络安全等级保护基本要求、测评要求和设计技术要求。

关键信息基础设施安全检测评估（简称“关基安全检测评估”）是对关键信息基础设施安全性和可能存在的风险进行检测评估的活动。检测评估内容包括但不限于网络安全制度（国家和行业相关法律法规政策文件及运营者制定的制度）落实情况、组织机构建设情况、人员和经费投入情况、教育培训情况、网络安全等级保护工作落实情况、密码应用安全性评估情况、技术防护情况、云服务安全评估情况、风险评估情况、应急演练情况、攻防演练情况等，尤其关注关键信息基础设施跨系统、跨区域间的

信息流动，以及关键业务流动过程中所经资产的安全防护情况。

1.3 新型关键基础设施的密码安全性评估要求

新型关键基础设施将以国产密码为核心构建密码体系。国产密码使传统信息系统密码评测模型面临新挑战，增加了对人工智能、5G、区块链等新技术的扩展要求，保护对象覆盖更全面，强化了密码技术的应用和管理要求，包括通信传输、数据存储、身份鉴别、产品采购、使用和密钥管理中均有与密码相关的要求，有必要更好地使用密码技术夯实安全基础、满足多方合规、保证整体安全^[19-20]。因此，新型关键基础设施中采用的密码体系将具备以下特征：① 商用密码标准体系；② 商用密码算法检测认证体系；③ 商用密码产品检测认证体系；④ 关键信息基础设施由商用密码检测机构开展商用密码应用安全性评估；⑤ 电子认证服务采用商用密码。新型关键基础设施的密码安全性评估要求（如图 6 所示）是在通用要求的基础上实现技术要求和安全管理要求指导下的双重指标。

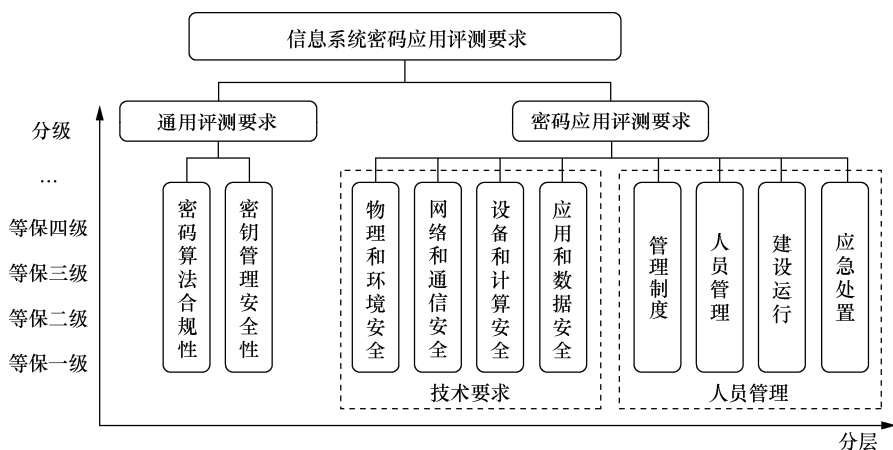


图6 密码应用安全性评估要求

Figure 6 New requirements for cryptography security assessment

2 信息基础设施的密码安全性评估

信息基础设施是提供数字转型、智能升级、融合创新等方面的物质工程设施，在国务院印发的《“十四五”数字经济发展规划》中，大数据、5G 通信和关键软件被列为加快推动数字产业化的战略性前瞻性领域。一方面，基于新技术实现设施升级，如推动移动通信网络从4G向5G升级、加快下一代互联网规模应用等；另一方面，适应新需求优化提升性能，如适应智能社会发展需求推动大数据中心体系向多层次算力供给体系演进，适应数据流量增长和流向变化趋势，推进云网协同和算网融合发展。此外，软件已成为信息时代的核心战略资源，与此同时，软件安全风险日益凸显。

2.1 面向大数据的密评框架

在大数据安全存储方面，现有云端数据完整性验证协议要求数据拥有者直接参与验证，不能由第三方托管^[21]。例如，REDACT^[22]协议每次仅能验证一个数据块，难以支撑对大规模数据的完整性验证。依赖于第三方的大数据完整性验证协议效率高、速度快，但可能会将数据拥有者的机密数据泄露给审计机构。面向大数据安全存储的密评技术主要是确保所采用的大数据完整性验证协议能够提供安全可信的大数据存储服务、阻止数据拥有者将数据泄露给第三方。

大数据检索分为明文检索和密文检索两种模式。明文检索的核心是提升数据发布和数据查询

服务的并行性；密文检索主要用于机密数据的发布和查询，密文检索的关键技术包括基于加密索引的密文检索、全同态加密、可搜索加密、安全多方技术等。近年来，隐私保护的明文检索算法被提出，此类算法以差分隐私技术为代表，通常假设敌手已掌握一些有关目标系统的背景知识（如系统版本号、数据类型等），但这种假设与网络攻防条件相矛盾，因此现有隐私保护的明文检索算法并未得到广泛部署。密文检索比明文检索更安全，但这类算法的安全性主要依赖于敌手的计算能力，与敌手的背景知识无关。因此，对于密文检索算法中使用的加密算法、密钥管理协议等进行安全性评估至关重要。面向大数据中心的密码安全性评估框架如图7所示。

2.2 面向5G通信的密评框架

密码学原理是解决5G/B5G终端的接入安全和数据安全的重要手段之一。对于接入安全，可采用的关键技术包括有证书/无证书密码体制、Token授权验证^[23]等；对于数据安全，可采用的关键技术包括属性基加密机制、抗密钥泄露机制、访问控制加密机制等^[24]。

5G赋能的自组织物联网、软件供应链管理、监管科技、金融科技、工业互联网、智能网联汽车等应用场景成为发展商用密码的主要驱动力，统一密码管理、统一认证、海量数据加密、云端数据保护、移动安全认证、合规校验是5G通信中密码应用安全性评估的重中之重。但5G通信中密码应用体系繁杂，密码服务数量、种类繁多，

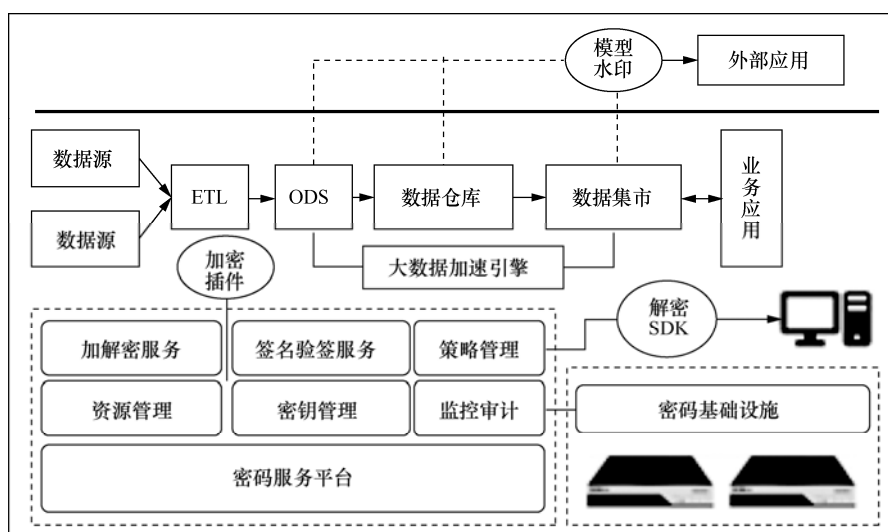


图7 面向大数据中心的密码安全性评估框架

Figure 7 Cryptography security assessment framework for big data centers

多系统密码应用整合给密码应用安全性评估带来诸多挑战^[25-26]。此外,越来越多的数据和业务功能被迁移到云端,而5G通信功能的虚拟化、托管化也给密码应用安全性评估带来新的挑战^[27-28]。因而,5G通信的密码安全性评估框架亟须解决的问题如下。① 如何对虚拟切片中的密码应用建立高效、可信的密评方案,并动态生成相关密评报告? ② 如何针对异构网络中采用的多系统密码应用建立高效的密评实施规范,以降低冗余评测带来的资源浪费等。

基于云边协同计算的密码应用安全性评估将密码应用、密码应用安全性评估迁移到了云端,通过密码基础设施层、加密通信服务层、密码管理层实现密码安全性评估一体化框架。密码基础设施层的核心是云密码服务资源池,它利用虚拟化技术将大规模密码硬件设备云化成可统一管理、按需配置的密码服务资源池,在提供基于SM2、SM3、SM4、SM9国密算法加解密、签名验签、密码杂凑算法等密码服务的同时提高资源利用率。加密通信服务层主要面向基于5G通信的数据传输系统提供密码服务,包括数字证书系统、密钥管理系统、随机数生成器和时间戳等通用性的密码服务。数字证书系统提供数字证书认证中心、证书注册审批系统的密码安全服务;密钥管理系统负责密钥生成、分发、使用、注销等全生命周期的安全管理^[29];随机数生成器负责根

据密码算法的相关参数生成指定长度的随机数;时间戳是由数字签名生成的标识数据,用于验证被加密数据在产生后是否被篡改过。支撑IaaS、PaaS、SaaS层密码应用的主要是通用密码服务;设备接入认证和用户身份鉴别是通过在通信网络中部署的SSL VPN或IPSec VPN实现的,为了防止敏感信息泄露或被非法授权篡改,边缘侧还需使用加密通信服务对所采集和处理的数据进行机密性、可用性和完整性保护。同时,对于启用虚拟网络功能的用户,可使用云密码进行信道加解密、会话安全认证、资源访问授权以及协同签名等云端加密服务。例如,徐子钧等^[30]提出一种适用于5G mMTC网络切片的基于SM2国密算法的二次认证与安全隔离模型,通过引入批量认证和预认证机制提升了大规模用户场景下的安全认证效率。密码管理层主要是对各类密码服务、生成密钥、密码模块隐匿、密码算法库访问控制策略的管理。

前文提及的云密码服务主要位于云端的硬件环境中,用户通常只能远程登录云密码服务的管理界面,对云密码服务的管理主要包括云密钥管理和访问权限管理。在云密钥管理方面,为了防止密钥泄露、重用并满足国家密码应用管理要求,不同用户拥有的不同类型的数据均需设置不同的密钥,因而密钥数量繁多、类型多样,建立多层级密钥隔离机制是基础^[31]。在访问权限管理方

面, 云密码服务通过集成 PKI 证书认证、OAuth 认证、无证书认证、OpenID 认证等多种形态提供多种模式的访问控制策略。

当前, 移动通信正在从 5G 到 6G 演进, 通感一体化、智能反射表面、生成式人工智能等新技术不断涌现, 给设备接入安全、身份认证、关键业务防抵赖和敏感数据安全存储等密码应用提出了新的要求。例如, 新一代工业控制系统已经开始通过提供数据原发证据和数据接收证据实现数据原发行为的抗抵赖和数据接收行为的抗抵赖; 利用深度学习追踪用户行为状态进而构建连续认证体系的方法也逐渐增多。

2.3 面向基础软件的密评框架

软件在各行业领域的渗透使得其对密码应用的需求不断增长。为了保护应用软件以及系统软件的安全性, 软件设计过程中通过调用密码算法库实现敏感数据的加解密传递。软件安全中常用的密码技术是注册保护, 它通过限制软件运行时间、功能等方法要求用户提供个人信息来进行软件注册, 从而实现软件与用户信息的绑定以达到软件保护的目的, 主要实现方法可分为用户名+注册码、机器码+注册码和组合方式+注册码。其中, 注册码可由对称加密或非对称加密技术进行构建^[32]。在基于对称加密的注册码生成算法中, 加解密双方协商统一的密钥来实现对明文的加密和对密文的解密; 在基于非对称加密的注册码生成算法中, 加密和解密是相互独立的, 且采用不同的密钥, 即“公钥加密, 私钥解密”。

对于新型关键基础设施的软件运行环境, 传统的密评框架不再适用。首先, 通用评测准则发生变化, 如 Egele 等^[33]针对 Android 开发中日益增长的密码误用现象提出了两个新的通用评判准则: ① 抵抗选择明文攻击; ② 抗碰撞性。选择明文攻击是指攻击者通过访问加密机构造任意明文所对应的密文, 然后推测密钥的一种攻击模式, 能否抗选择明文攻击是衡量密码安全性的基本指标。抗碰撞性是针对不同的输入得到不同的输出。其次, 密评工具将集成机器学习算法, 以实现自动化和智能化的评估, 如文献^[34]提出了一种基于机器学习的软件加密功能识别技术, 这将为识

别恶意软件(如勒索病毒^[35]、DNS 欺骗^[36]等)提供新思路。

3 融合基础设施的密码安全性评估

融合基础设施是应用新一代信息与通信技术对早期的基础设施进行智能化、数字化改造后所形成的新型关键基础设施形态, 包括以智能网联工控系统、智慧网联汽车等为代表的一体化设施。融合基础设施的层次化、异构性使密码安全性评估的复杂度剧增。研究表明, 网络规模越大, 结构越复杂, 所需测试的频次越多, 测试用例越难生成, 测试方法的覆盖范围越小^[37]。

3.1 智能网联工控系统的密评框架

智能网联工控系统由众多采集和控制子系统, 以及计算服务器、存储服务器、专用工作站等构成。智能网联工控系统的核心数据主要在专用工作站、计算服务器和存储服务器上整合、共享和分析。为了加强专用工作站、存储服务器、计算服务器等智能网联工控系统核心软硬件设备的物理安全性, 需对上述软硬件设备所在的物理区域部署安防安保措施, 包括安置具有密码模块的电子门禁系统、视频监控系统; 通过服务器密码机、加密存储设备、视频加密系统等实现音视频数据完整性保护。

智能网联工控系统主要通过网络技术来实现与外界的互联互通, 在通信建立前或者某外部设备接入内部网络时, 可根据智能网联工控系统的安全等级要求, 考虑采用基于密码杂凑算法的消息鉴别码机制, 或基于公钥密码算法的数字签名机制进行单向或双向身份鉴别, 并将证书信息存储在安全介质中, 而后对证书的申请、发放、使用、吊销等过程建立严格的管控策略^[38]。此外, 对于工控主机登录、访问过程中常见的身份冒用、越权访问等安全风险, 可部署角色判定、权限分配、统一身份认证等安全措施进行缓解。其中, 动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)机制、基于公钥密码算法的数字签名机制等密码技术对设备操作人员等登录设备的用户进行身份鉴别, 如采用合规的智能密码密钥。

与传统的工控系统不同, 智能网联工控系统

允许用户远程访问,并通过互联网远程控制部分工控资源,这使攻击面被大大扩展。因此,在确需远程访问的情况下,应采用商密 IPsec/SSL VPN 等方式建立专用通道连接,这条专用通道需采用数字签名的方式进行身份鉴别,通道上的所有通信数据需要采用加密算法和杂凑算法保护其机密性和完整性。对不联网的工业控制设备、软件和主机等,也应按照国家规定的信息安全法律法规进行管控和测评。在密码设置时,避免使用默认密码、易猜测密码、空口令,尽量覆盖数字、字母、特殊符号、大小写以提高密码强度,并要不定期更新,从而防止暴力破解。对于特定系统,建议采用一次一密的验证机制,最大限度防止密钥伪造。

智能网联工控系统的密码安全性评估由白盒、灰盒和黑盒 3 个阶段组成,并分别从智能网联工业控制系统方面(简称“系统侧”)与密码应用方面(简称“密码侧”)执行两类测试。二者的共同之处是:将密码基础应用与测评体系中的指标体系、测试技术、度量方法与等级保护体系下的相应要素集结合,共同形成针对工控系统密码的评估指标体系、评估/度量方法和测试技术体系^[39]。

面向智能网联工控系统的密码应用安全性评估指标体系可按密码侧指标类与系统侧指标类进行划分,在当前的评测实施过程中二者仍是独立进行的。实现密码侧指标与系统侧指标融合的方法有两种。一是建立智能网联工控系统密码应用安全分级体系与密码载体安全分级体系之间的映射机制,具体来说就是将密码载体所提供的各类密码服务(如加密、认证、标识、鉴别等)通过关键安全属性与工控系统安全应用建立对齐规则,从而构建密码侧与系统侧指标之间的语义关联通量,进而实现两个指标体系的深度融合。二是在密码侧指标类及其指向的关键安全属性集中加入系统侧指标类作为约束项。具体地,智能网联工控系统是最典型的时间敏感系统,它对业务连续性、系统可靠性以及信息物理安全性等有很严格的要求,密码应用部署必须考虑其对系统功能的影响,即信息安全和功能安全之间存在未知耦合问题,因此在密码侧指标的

基础上引入系统侧指标约束,形成适配智能网联工控系统业务需求的融合安全指标体系也是一种备选研究思路^[40]。

3.2 智能网联汽车的密评框架

在车联网智能化和网联化的进程中,智能网联汽车安全问题日益重要。密码技术作为保障车联网安全的核心技术和基础支撑,在车联网数据加密和身份认证等方面发挥着不可替代的作用,我国的车联网密码应用还处于起步阶段,2022 年 11 月,我国正式发布《车联网(智能网联汽车)密码支撑标准体系建设指南》。基于车联网的“云-管-端”三级体系架构,从云端安全、传输安全和终端安全分别介绍密码学的应用。

(1) 车辆云中的密码应用

车辆云中的密码应用是近年来的研究热点,它主要依赖虚拟化密码机为云环境下的大规模用户提供密码服务。例如,李荣泰等^[41]曾构建了一种适用于虚拟密码机但不需要改造虚拟密码机的密码应用,密钥、登录凭证等重要信息是通过国密 SSL 协议进行安全传输的,对于关键敏感数据则使用数字签名和完整性校验进行安全加固。Yoshizawa 等^[42]提出面向 LTE-V2X 数字签名体系,可实际应用于 LTE-V2X 业务部署及系统开发设计。

(2) 车路人协同场景下的密码应用

车路人协同场景下,在车辆终端、路边单元、可穿戴式设备以及通信基站之间进行数据传输时,应当对网络信令、敏感数据进行加密,并支持完整性以及抗重放保护。其中,对用户数据进行加密保护旨在确保各类实体间数据传输过程中信息不被窃听、伪造、篡改、重放;对车载终端与服务网络之间建立双向认证,可确保双方身份的合法性,防止信息泄露给第三方。车路人协同场景下的安全认证主要是基于 PKI (public key infrastructure) 架构的,但 PKI 架构每次通信必须传递和验证证书,增加了网络负载。董晓露等^[43]提出一种基于切比雪夫混沌映射和生物识别的车联网认证方案,利用切比雪夫多项式的半群性质构建对称密钥,提高了消息认证阶段的计算效率;Xun 等^[44]在基于移动边缘计算框架的软件定义车联网体系结构下,提出一种基于车辆行为预测的身份认证方案,可在保证较高车辆认证

准确率的同时满足车联网的低时延需求；郝敏等^[45]融合区块链和零知识证明对身份验证进行优化，将零知识证明作为高性能系统的核心组件与联盟链结合，实现 6G 零信任网络环境的可信接入，在保护数据隐私的基础上进一步提升了系统效率。

(3) 车辆终端内的密码应用

车辆终端内的密码应用需求主要体现在密钥管理、OTA（Over-the-Air）升级过程中的双向身份认证、用户隐私数据加密传输与存储等方面^[46]。在智能驾驶汽车、新能源汽车中，应用密码芯片、国产密码算法实现的智能钥匙、车载加密软件等层出不穷。其中，“数字密钥”技术允许汽车制造商使用可信传输通道将数字密钥安全地传输到车主的智能终端上，使车主能够通过智能终端来锁车、解锁、启动引擎或分享车辆的使用权等。在我国，由于国家政策的支持和相关标准的不断完善，基于国产密码体系的轻量级安全证书分发、车路人协同认证、车联网隐私保护等密码应用已经得到示范应用和推广。

综上，智能网联汽车的密评需要以“云-管-端”三级体系架构为基础进行开展，从智能网联汽车的充电系统、电控系统、多媒体系统的设计阶段就应引入密码应用安全性评估工作，并将评估结果作为车辆质量测试验证分析的重要依据。智能网联汽车制造和运行阶段同样要通过密码应用安全性评估，以保证智能网联汽车全产业链中商用密码应用的合规性、正确性和有效性。

4 创新基础设施的密码安全性评估

创新基础设施是指支撑科学研究、技术开发、产品研制的具有公益属性的基础设施，与“天眼”“空间站”“电子对撞机”等基础学科支撑设施不

同，人工智能和区块链均是构建上层应用技术体系的底座，基于大模型开启的生成式回答模型^[47]，一举解决了行业共通性的长尾问题，单条回答建设成本降低 99%；而区块链则在“加密货币”的基础上构建了去中心化账本，赋予人们支付隐私化的权利。基于区块链甚至可以使人工智能实现分布式协同^[48]。为了确保用户隐私，密码应用在人工智能和区块链领域均占有举足轻重的地位。

4.1 面向人工智能应用的密评框架

在人工智能应用中所使用的密码算法、密码模块以及密码系统与传统密码学应用存在很大不同，这给密评技术提出了新的发展需求。首先，安全可信人工智能中的加密算法通常在人工智能芯片、人工智能软件和人工智能平台上部署，其应用环境复杂多样，既包括云计算中的虚拟机、Docker，又包括边缘计算平台和各类智能物联网终端，因此亟须建立云边协同的密码测评规范。2016 年，Abadi 等^[49]提出利用生成对抗网络保护通信，设计了基于生成对抗网络的公钥加密和私钥解密算法；Zeadally 等^[50]重点总结并分析了物联网设备上正在使用或已推荐使用的最新加密协议标准。其次，安全可信人工智能尤其是分布式学习将大量使用同态加密、门限加密和函数加密，对密文空间开展密码测评将成为未来发展的重要趋势^[51-54]。我国中科院信息工程研究所、中国电子科技集团三十所等单位的 10 余位专家通过了国内首个密文查询算法团体标准《基于整数同态加密的密文查询算法标准》。

人工智能技术给密评工作带来挑战的同时，也给密评工作带来了新的发展际遇。不同 AI 模型的密评挑战与机遇如表 3 所示。一直以来，困扰密评工作发展的一大难题是测评工作需要专业的、有资质的从业人员来承担，安全人才培养方

表 3 不同 AI 模型的密评挑战与机遇
Table 3 Challenges and opportunities in cryptography security assessment for different AI models

AI 模型	简介	挑战	机遇
DNN	深度神经网络，用于构建分类、预测等深度学习任务	依然无法对加密流、密文信息直接进行评测	可识别加密流类型、恶意软件家族等
GAN	对抗生成网络，用于数据去噪、数据生成等	仅能对模拟构建早期的加密算法实现加密传输通道	开辟了实现加密算法和加密协议的新途径
AIGC/ChatGPT	大模型，用于各领域构建生成式问答系统	辅助构建自动化密评工具，还需对大模型进行个性化微调	增强安全知识检索能力，有助于提升安全意识

面的不完善导致我国各行业密码测评工作长期处于无人开展或未及时开展状态,基于人工智能技术有助于将流程化、交互式的密码测评工作自动化或半自动化。2018年,Gomez等^[55]首次提出利用GAN破译移位密码和维吉尼亚密码,为研发新型密评工具提供了可行思路;Hitaj等^[56]利用GAN来改进基于规则的密码生成工具,可从密码数据中高效、自主地推断密钥分发信息;2019年,我国密码科学技术国家重点实验室对基于生成对抗模型的密码算法/协议设计分析方法以及密码系统智能攻防技术开展研究,提出了基于人工智能技术的密码算法与协议形式化分析方法、基于神经网络的加密和混淆算法、基于GPU/TPU/FPGA等计算器件的人工智能密码算法分析工具构建方法以及基于机器学习的密码设备性能测评与调优等一系列技术思路^[57];2023年,Kwon等^[58]利用ChatGPT实现了一种新型的加密算法。但是,人工智能应用在可解释性、可信性上还存在诸多缺陷,利用人工智能构建灵活、高效、智能的密码分析工具的同时,还需要对其自身的安全性进行评估^[59]。

4.2 面向区块链应用的密评框架

基于区块链构建的弱中心、去中心信任框架与固有的中心化信任框架不同,鉴于其在分布式存储、点对点传输、多节点共识、数字加密方面的特点,它能够支持更高效的数据和价值传递,在移动互联网时代与多业务融合场景中具有重大应用前景^[60-62]。密码学算法,包括数字签名、哈希算法、零知识证明、环签名等,是区块链应用的基础和核心,因此合理采用符合国家密码管理政策的密码算法、密码协议、密钥管理机制等密码应用技术,遵循我国密码标准规范要求,并深入开展密码测评认证,是保证区块链公开透明、不易伪造、可溯可信的重要前提^[63]。目前,密码杂凑算法、公钥加密算法、门限加密算法、零知识证明等密码技术在区块链中已得到广泛应用,成为实现区块链基本功能、保障区块链安全稳定运行的关键技术^[64]。

近年来,我国新型基础设施建设日新月异、海量多模态数据持续累积、网络安全相关政策法律相继出台,都为我国区块链的发展创造了有利条件。但是,我国在区块链底层核心技术(如

共识算法、智能合约、加密机制等)上的自主创新程度还不够高,区块链应用开发严重依赖国外开源平台,导致其供应链安全面临恶意代码注入、后门植入等安全威胁。为此,我国区块链应用整体还处于以满足用户需求、支撑业务流程为主的初级阶段。如何充分利用密码技术对区块链安全提供支撑保障,形成面向区块链应用的轻量级密码算法、产品和合规检测方法,是引导和促进区块链密码正确、有效应用的关键^[65]。此外,区块链标准化研究工作中关于密码算法、性能、评估的规定逐渐得到各国政府和组织机制的重视,国际标准化组织技术委员会ISO/TC307、国际电信联盟安全组ITU-T SG17启动了多个区块链应用标准预研、标准草案的编写工作,如区块链跨链标准(P3205)等。2023年,我国首个区块链技术领域国家标准《区块链和分布式记账技术参考架构》(GB/T 42752-2023)获批发布,从用户视图和功能视图分别定义了区块链应用的基本组件、服务接口和审计要求。此外,我国也发布了面向区块链应用的密码技术团体标准与企业标准,但整体上覆盖面较窄,成熟度较低,保障区块链应用核心安全的密码技术及测评标准仍十分欠缺,难以支撑区块链应用的大规模规范部署。

区块链应用中的各层组件均依赖密码技术的安全保障^[66]。对区块链应用开展密码安全测评,对于强化区块链应用中密码技术使用规范、切实保障区块链应用中各层组件的安全性具有不可替代的重要作用。目前,很多区块链应用中使用的基于密码的身份管理、隐私保护、交易加密技术,缺乏严密的形式化证明和验证,区块链应用开发平台底层所采用的随机数、密码算法、函数库存在安全漏洞,诸多区块链应用上部署的密码产品自身存在安全隐患,所运行的加密服务、密码管理平台的合规性、正确性和有效性难以得到保障,因此必须深入开展面向区块链应用的密码测评技术研究。

本文所构想的面向区块链应用的多层次密评框架如图8所示,主要包括设备层密评、功能层密评和应用层密评。其中,设备层密评将在区块链密码标准体系的基础上,对密码机、加密卡、时间戳服务器、验签服务器、VPN登录模块以及软件密码模块进行测试验证,依据区块链技术特点,

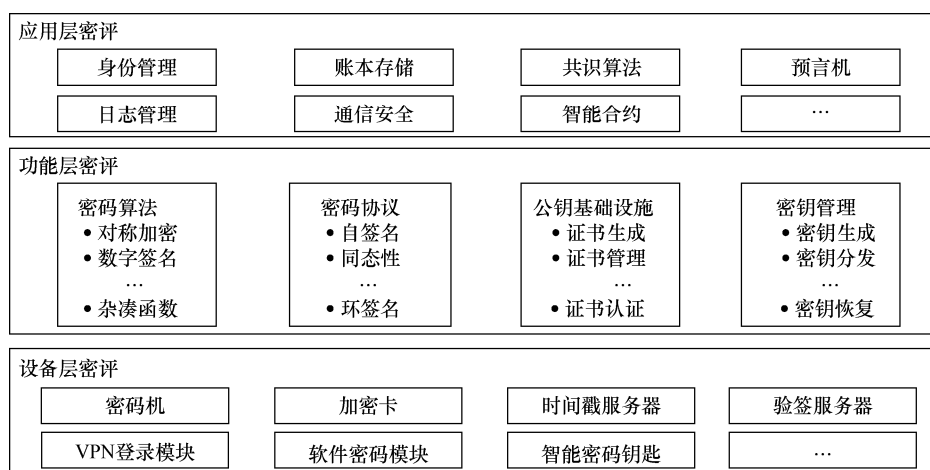


图 8 面向区块链应用的多层次密评框架

Figure 8 Multi-level cryptography assessment framework for blockchain applications

研究专用设备密码测评方法和技术，建设专业的区块链设备层密码测评工具和平台；功能层测评将围绕密码算法、密码协议、公钥基础设施、密钥管理服务分别制定科学有效的区块链密码产品功能检测认证规则^[67]；应用层密评主要从身份管理、账本存储、智能合约等方面实现对典型区块链应用系统的测评规范，并通过完善区块链安全测评体系（如图 9 所示）构建合乎《中华人民共和国密码法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》等国家规章制度的密评流程，从而确保区块链应用中密码技术的合规性、正确性和有效性。

为加强关键基础设施安全保障，《国务院关于加强数字政府建设的指导意见》中指出，应开展对新技术新应用的安全评估，建立健全对算法的审核、运用、监督等管理制度和技术措施。2019 年《中华人民共和国密码法》的出台以及 2021 年 GB-39786《信息安全技术 信息系统密码应用基本要求》的发布，推动了我国密评合规进入快速发展阶段，带动国密改造业务在各领域加速落地。考虑到密码建设仍处于以密评合规为主要驱动的加速渗透期，未来密码行业要重点关注密码应用安全性评估、国产密码应用改造、新安全场景下密码平台建设等三大建设需求。

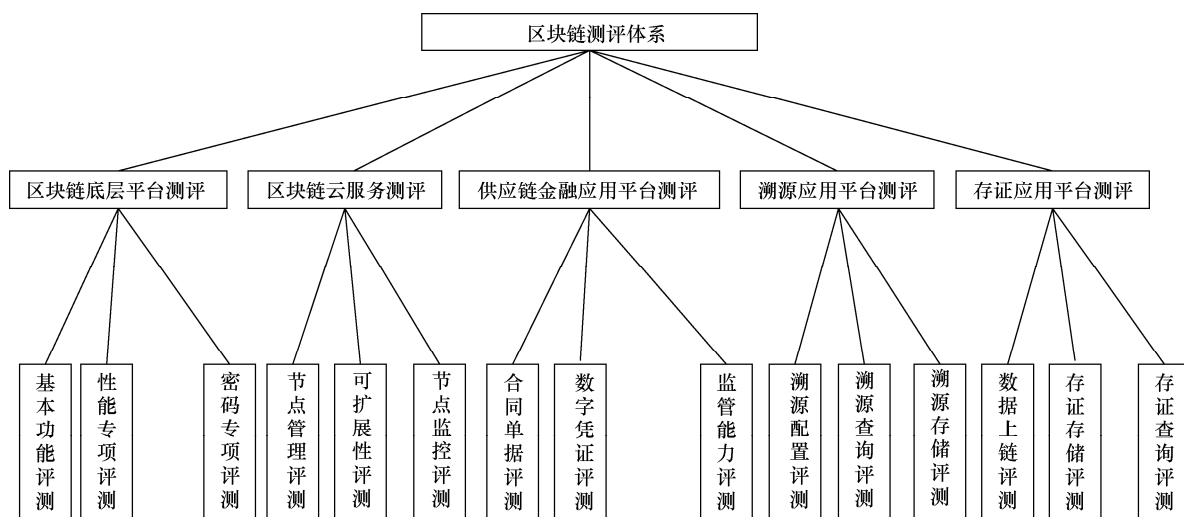


图 9 区块链安全测评体系

Figure 9 Blockchain security assessment framework

5 结束语

新型关键基础设施密码应用安全性评估涉及算法评测、密码协议评测、数字证书评测和密钥管理等多个层面。密码应用的正确性、有效性和合法性是确保新型关键基础设施安全的首要前提。面对信息、融合和创新方面的新型关键基础设施安全保障要求,研发支持智能化、无人化,且可解释、可追溯的密码应用安全性评估技术与工具将成为未来发展的重要方向。同时,随着《中华人民共和国密码法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》以及关键信息基础设施安全保护条例等相关法律法规的出台,综合5G、大数据、区块链、人工智能等新兴技术的服务和应用系统将逐步采用同态加密、无证书密码体制、零知识证明等方法进行安全加固,建立功能高度集成的一体化密码服务平台是未来发展的重要方向之一。

参考文献:

- [1] 唐新华. 新型基础设施在国家治理现代化建设中的功能研究[J]. 中国科学院院刊, 2021, 36(1): 79-85.
TANG X H. Research on the function of new infrastructure in the modernization of national governance[J]. Bulletin of Chinese Academy of Sciences, 2021, 36(1): 79-85.
- [2] 邱洁, 韩瑞, 魏志丰, 等. 网络空间公共基础设施体系及安全策略研究[J]. 网络与信息安全学报, 2021, 7(6): 56-67.
QIU J, HAN R, WEI Z F, et al. Research of public infrastructure system and security policy in cyberspace[J]. Chinese Journal of Network and Information Security, 2021, 7(6): 56-67.
- [3] KHAN S, MADNICK S. Cybersafety: a system-theoretic approach to identify cyber-vulnerabilities & mitigation requirements in industrial control systems[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(5): 3312-3328.
- [4] STEVENS M. New collision attacks on SHA-1 based on optimal joint local-collision analysis[C]//32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2013: 245-261.
- [5] STEVENS M, BURSSTEIN E, KARPMAN P, et al. The first collision for full SHA-1[C]//37th Annual International Cryptology Conference. 2017: 570-596.
- [6] CAO H, ZHU P, LU X, et al. A layered encryption mechanism for networked critical infrastructures[J]. IEEE Network, 2013, 27(1): 12-18.
- [7] National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, FIPS 140-3[S]. 2019.
- [8] SYLVAIN G, YOUSSEF S, ZHANG F, et al. Post-quantum cryptography—having it implemented right[J]. Journal of Cryptologic Research, 2023, 10(3): 650-666.
- [9] Global Research & Analysis Team, Kaspersky Lab. Advanced threat predictions for 2022[R]. 2022.
- [10] GOPINATH M, SIBI C S. A comprehensive survey on deep learning-based malware detection techniques[J]. Computer Science Review, 2023 (47): 100529.
- [11] 王建华, 张岚. 检测类型缺陷的形式化构造攻击方法[J]. 密码学报, 2021, 8(6): 1058-1073.
WANG J H, ZHANG L. A formal construction attack method for detecting type defects[J]. Journal of Cryptologic Research, 2021, 8(6): 1058-1073.
- [12] 陈华, 范丽敏. 密码测评—信息安全领域的核心技术[J]. 中国科学院院刊, 2011, 26(3): 297-302.
CHEN H, FAN L M. Password evaluation: the core technology in the field of information security [J]. Bulletin of Chinese Academy of Sciences, 2011, 26(3): 297-302.
- [13] HAN S, JAGER T. Authenticated key exchange and signatures with tight security in the standard model[C]//CRYPTO 2021. 2021: 670-700.
- [14] 董建阔, 刘哲, 陆盛, 等. 椭圆曲线密码高效软件实现技术研究进展[J]. 计算机学报, 2023, 46(5): 909-928.
DONG J K, LIU Z, LU S, et al. Research progress on efficient software implementation of elliptic curve cryptography[J]. Chinese Journal of Computers, 2023, 46(5): 909-928.
- [15] 张跃宇, 徐东, 陈杰. 白盒 SM4 的分析与改进[J]. 电子与信息学报, 2022, 44(8): 2903-2913.
ZHANG Y Y, XU D, CHEN J. Analysis and improvement of white Box SM4 [J]. Journal of Electronics & Information Technology, 2022, 44(8): 2903-2913.
- [16] 董玲, 陈克非, 来学嘉. 密码协议分析的信任多集方法[J]. 软件学报, 2009, 20(11): 3060-3076.
DONG L, CHEN K F, LAI X J. Trust multiset method for cryptographic protocol analysis[J]. Journal of Software, 2009, 20(11): 3060-3076.
- [17] LI G, ZHAO Y, LI Y. CATFL: certificateless authentication-based trustworthy federated learning for 6g semantic communications[C]//IEEE WCNC. 2023.

- [18] LEE T R, TEH J S, JAMIL N, et al. Lightweight block cipher security evaluation based on machine learning classifiers and active S-boxes[J]. *IEEE Access*, 2021, (9): 134052-134064.
- [19] JALALI N A, CHEN H. Federated learning security and privacy-preserving algorithm and experiments research under internet of things critical infrastructure[J]. *Tsinghua Science and Technology*, 2023, 29(2): 400-414.
- [20] 姚前, 张大伟. 区块链系统中身份管理技术研究综述[J]. *软件学报*, 2021, 32(7): 2260-2286.
- YAO Q, ZHANG D W. Survey on identity management in blockchain[J]. *Journal of Software*, 2021, 32(7): 2260-2286.
- [21] 王子园, 杜瑞忠. 边缘环境下基于无证书公钥密码的数据完整性审计方案[J]. *通信学报*, 2022, 43(7): 62-72.
- WANG Z Y, DU R Z. Data integrity auditing scheme based on certificateless public key cryptography in edge environment[J]. *Journal on Communications*, 2022, 43(7): 62-72.
- [22] DEVRAJ A, WANG L, REXFORD J. REDACT: refraction networking from the data center[J]. *ACM SIGCOMM Computer Communication Review*, 2021, 51(4): 15-22.
- [23] 杨国强, 丁杭超, 邹静, 等. 基于高性能密码实现的大数据安全方案[J]. *计算机研究与发展*, 2019, 56(10): 2207-2215.
- YANG G Q, DING H C, ZOU J, et al. Big data security scheme based on high-performance cryptography[J]. *Journal of Computer Research and Development*, 2019, 56(10): 2207-2215.
- [24] DANG L, DONG M, OTA K, et al. Resource-efficient secure data sharing for information centric e-health system using fog computing[C]//*IEEE ICC*. 2018: 1-6.
- [25] XIANG B, ZHANG J, DENG Y, et al. Fast blind rotation for bootstrapping FHEs[C]//*Crypto 2023*. 2023.
- [26] LI G, WU J, LI J, et al. Fog computing-enabled secure demand response for internet of energy against collusion attacks using consensus and ACE[J]. *IEEE Access*, 2018, (6): 11278-11288.
- [27] BOATENG G O, SUN G, MENSAH D A, et al. Consortium blockchain-based spectrum trading for network slicing in 5G RAN: a multi-agent deep reinforcement learning approach[J]. *IEEE Transactions on Mobile Computing*, 2023, 22(10): 5801-5815.
- [28] NGUYEN V L, LIN P C, CHENG B C, et al. Security and privacy for 6G: a survey on prospective technologies and challenges[J]. *IEEE Communications Surveys & Tutorials*, 2021, 23(4): 2384-2428.
- [29] ZHOU Z, GAURAV A, GUPTA B B. A fine-grained access control and security approach for intelligent vehicular transport in 6G communication system[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2022, 23(7): 9726-9735.
- [30] 徐子钧, 刘建伟, 李耕. 面向 5G mMTC 的网络切片安全研究[J]. *网络与信息安全学报*, 2022, 8(1): 95-105.
- XU Z J, LIU J W, LI G. Research on network slice security for 5G mMTC[J]. *Journal of Network and Information Security*, 2022, 8(1): 95-105.
- [31] BELLARE M, HOANG V T. Efficient schemes for committing authenticated encryption[C]//*EUROCRYPT 2022*. 2022: 845-875.
- [32] 邓从政. 基于公钥密码体制 RSA 算法的注册码生成器[J]. *成都大学学报 (自然科学版)*, 2015, 34(1): 44-47.
- DENG C Z. Registration code generator based on RSA algorithm of public key cryptosystem [J]. *Journal of Chengdu University (Science & Technology Edition)*, 2015, 34(1): 44-47.
- [33] EGELE M, BRUMLEY D. An empirical study of cryptographic misuse in android applications[C]//*ACM CCS*. 2013: 73-84.
- [34] FAHL S, HARBACH M. Why eve and mallory love android: an analysis of android SSL security[C]//*ACM CCS*. 2012: 50-61.
- [35] LYU M, HASSAN H. G, VIJAY S. A survey on DNS encryption: Current development, malware misuse, and inference techniques[J]. *ACM Computing Surveys*, 2022, 55(8): 1-28.
- [36] TRIVIKRAM M. File packing from the malware perspective: techniques, analysis approaches, and directions for enhancements[J]. *ACM Computing Surveys*, 2022, 55(5): 1-45.
- [37] HU Z, HAN J, PENG H, et al. Locating sources in multiplex networks for linear diffusion systems[C]//*IEEE Transactions on Network Science and Engineering*, 2022, 9(5): 3515-3530.
- [38] 张磊. 民航商用密码应用分析与安全体系研究[J]. *民航学报*, 2022, 6(3): 92-95.
- ZHANG L. Research on civil aviation commercial cryptography application analysis and security system[J]. *Journal of Civil Aviation*, 2022, 6(3): 92-95.
- [39] 唐士杰, 袁方, 李俊, 等. 工业控制系统关键组件安全风险综述[J]. *网络与信息安全学报*, 2022, 8(3): 1-17.
- TANG S J, YUAN F, LI J, et al. Review on security risks of key components in industrial control system[J]. *Chinese Journal of Network and Information Security*, 2022, 8(3): 1-17.
- [40] ZHANG K. Impossible differential cryptanalysis and a security evaluation framework for AND-RX Ciphers[J]. *IEEE Transactions on Information Theory*, 2023.
- [41] 李荣泰, 常瑞, 苗新亮, 等. 异构平台设备安全启动机制研究[J]. *信息工程大学学报*, 2022, 23(2): 198-205.
- LI R T, CHANG R, MIAO X L, et al. Secure boot mechanism of

- Heterogeneous Platform Devices, 2022, 23(2): 198-205.
- [42] YOSHIKAWA T. A survey of security and privacy issues in v2x communication systems[J]. *ACM Computing Surveys*, 2023, 55(9): 1-36.
- [43] 董晓露, 黎妹红, 杜晔, 等. 基于切比雪夫混沌映射和生物识别的身份认证方案[J]. *北京航空航天大学学报*, 2019, 45(5): 1052-1058.
- DONG X L, LI M H, DU Y, et al. A biometric verification-based authentication scheme using chebyshev chaotic mapping [J]. *Journal of Beijing University of Aeronautics and Astronautics*, 2019, 45(5): 1052-1058.
- [44] XUN, Y, WEI G, LIU J. G-driverAUT: a growable driver authentication scheme based on incremental learning[J]. *IEEE Transactions on Vehicular Technology*, 2023.
- [45] 郝敏, 叶东东, 余荣, 等. 区块链赋能的6G零信任车联网可信接入方案[J]. *电子与信息学报*, 2022, 44(9): 3004-3013.
- HAO M, YE D D, YU R, et al. Blockchain empowered trustworthy access scheme for 6G zero-trust vehicular networks[J]. *Journal of Electronics & Information Technology*, 2022, 44(9): 3004-3013.
- [46] 智能网联汽车密码模块安全技术要求: T/GHDQ 79-2021[S]. 2021.
- Security technical requirements of intelligent connected vehicle password module: T/GHDQ 79-2021[S]. 2021.
- [47] CAO Y, LI S, LIU Y, et al. A comprehensive survey of ai-generated content (AIGC): a history of generative AI from GAN to ChatGPT[J]. *arXiv preprint arXiv: 2303.04226*, 2023.
- [48] WARNAT-HERRESTHAL S. Swarm learning for decentralized and confidential clinical machine learning[J]. *Nature*, 2021, 594(7862): 265-270.
- [49] ABADI M, ANDERSEN D G. Learning to protect communications with adversarial neural cryptography[C]//International Conference on Learning Representations (ICLR). 2016.
- [50] ZEADALLY S, DAS A K, SKLAVOS N. Cryptographic technologies and protocol standards for internet of things[EB].
- [51] JKENNEY J B. Dedicated short-range communications (DSRC) standards in the United States[J]. *Proceedings of the IEEE*, 2011, 99(7): 1162-1182.
- [52] LI G, WU J, LI S, et al. Multitentacle federated learning over software-defined industrial internet of things against adaptive poisoning attacks[J]. *IEEE Transactions on Industrial Informatics*, 2023, 19(2): 1260-1269.
- [53] 蒋瀚, 刘怡然, 宋祥福, 等. 隐私保护机器学习的密码学方法[J]. *电子与信息学报*, 2020, 42(5): 1068-1078.
- JIANG H, LIU Y R, SONG X F, et al. Cryptographic method of Machine learning for privacy protection[J]. *Journal of Electronics and Information Technology*, 2020, 42(5): 1068-1078.
- [54] MYUNGSUN K. Private compound wildcard queries using fully homomorphic encryption[J]. *IEEE Transactions on Dependable and Secure Computing*, 2017, 16(5): 743-756.
- [55] GOMEZ A. N, HUANG S, ZHANG I, et al. Unsupervised cipher cracking using discrete GANs[J]. *arXiv: 1801.04883v1*, 2018.
- [56] HITAJ B, GASTI P, ATENIESE G, et al. PassGAN: a deep learning approach for password guessing[C]//International Conference on Applied Cryptography and Network Security. 2019: 217-237.
- [57] 宁晗阳, 马苗, 杨波, 等. 密码学智能化研究进展与分析[J]. *计算机科学*, 2022, 49(9): 288-296.
- NING H Y, MA M, YANG B, et al. Intelligent cryptography research progress and analysis [J]. *Journal of Computer Science*, 2022, 49 (9): 288-296.
- [58] KWON H, SIM M, SONG G, et al. Novel approach to cryptography implementation using ChatGPT[R]. 2023.
- [59] ZHOU Z, BIN H, LI J, et al. Malicious encrypted traffic features extraction model based on unsupervised feature adaptive learning[J]. *Journal of Computer Virology and Hacking Techniques*, 2022, 18: 453-463.
- [60] 王利朋, 关志, 李青山, 等. 区块链数据安全服务综述[J]. *软件学报*, 2023, 34(1): 1-32.
- WANG L P, GUAN Z, LI Q S, et al. Survey on blockchain-based security services[J]. *Journal of Software*, 2023, 34(1): 1-32.
- [61] YANG Z, LI G, WU J, et al. Propagable backdoors over blockchain-based federated learning via sample-specific eclipse[C]//IEEE GLOBECOM. 2022: 2579-2584.
- [62] SHI Y, LI G, XU X, et al. PFCC: predictive fast consensus convergence for mobile blockchain over 5G slicing-enabled IoT[C]//IEEE GLOBECOM. 2021: 1-6.
- [63] 朱岩, 张艺, 王迪, 等. 网络安全等级保护下的区块链评估方法[J]. *工程科学学报*, 2020, 42(10): 1267-1285.
- ZHU Y, ZHANG Y, WANG D, et al. Research on blockchain evaluation methods under the classified protection of cybersecurity[J]. *Chinese Journal of Engineering*, 2020, 42(10): 1267-1285.
- [64] GUO F, GUSILO W. Optimal tightness for chain-based unique signatures[C]//EUROCRYPT 2022. 2022: 553-583.
- [65] 唐飞, 甘宁, 阳祥贵, 等. 基于区块链与国密 SM9 的抗恶意 KGC 无证书签名方案[J]. *网络与信息安全学报*, 2022, 8(6): 9-19.
- TANG F, GAN N, YANG X G, et al. Anti-malicious KGC certifi-

cateless signature scheme based on blockchain and domestic cryptographic SM9[J]. Chinese Journal of Network and Information Security, 2022, 8(6): 9-19.

- [66] LI, G, DONG M, YANG L T, et al. Make edge intelligence immune: decentralized service orchestration for secure learning via blockchain[J]. IEEE Transactions on Engineering Management, 2023, (99): 1-12.

- [67] 刘峰, 杨杰, 齐佳音. 区块链密码学隐私保护技术综述[J]. 网络与信息安全学报, 2022, 8(4): 29-44.

LIU F, YANG J, QI J Y. Review of blockchain cryptography privacy protection technology[J]. Journal of Network and Information Security, 2022, 8(4): 29-44.

[作者简介]



李高磊（1992- ），男，河南开封人，博士，上海交通大学助理教授、博士生导师，主要研究方向为人工智能安全、隐私保护。



李建华（1965- ），男，江西九江人，博士，上海交通大学教授、博士生导师，主要研究方向为网络安全、密码应用、内容安全。



周志洪（1979- ），男，江西九江人，博士，上海交通大学讲师，主要研究方向为密码应用、网络靶场。



张昊（1980- ），男，北京人，中国信息安全测评中心工程师，主要研究方向为信息安全、等保测评。