CSTC中国评测 见证质量 技术白皮书

商用密码应用安全性评估白皮书（2021 年）

中国软件评测中心·网络空间安全测评工程技术中心

中国计算机行业协会数据安全专业委员会

2021 年 9 月

版权声明

本白皮书版权属于中国软件评测中心，并受法律保护。转载、摘编或利用其他方式使用本白皮书文字或观点的，应注明“来源：中国软件评测中心”。违反上述说明的，本单位将追究其相关法律责任。

编写小组：（按姓氏首字母排序）

陈　靖	高振鹏	高志欢	韩志峰	胡建勋	黄斐一
黄学臻	计晓军	姜玉琳	李世斌	李晓明	李松恬
李志鹏	李　研	梁　潇	林　青	刘　欣	刘　元
刘芮汐	刘金春	卢佐华	马多贺	孟　斌	宋岳峰
唐　刚	田　峰	王东阳	魏向杰	吴连勇	文雪刚
肖光雁	徐赵虎	薛竹君	叶茂祥	于　乐	张　兵
张　宏	张　峰	张弘扬	张久珍	张士莹	张晓娜
张建荣	郑　东	周庆山	朱宇泽		

编写单位:

中国软件评测中心（工业和信息化部软件与集成电路促进中心）

中国计算机行业协会数据安全专业委员会

参研单位：（按笔画排序）

上海观安信息技术股份有限公司

公安部第一研究所

中国电信集团系统集成有限责任公司

中国科学院信息工程研究所

中国移动通信集团有限公司

中国联合网络通信有限公司

中科信息安全共性技术国家工程研究中心有限公司

中核核信信息技术(北京)有限公司

北京大学信息管理系

北京梆梆安全科技有限公司

北京天融信网络安全技术有限公司

北京安瑞科技有限公司

北京数盾信息科技有限公司

北京瀛和律师事务所

西安邮电大学

全球能源互联网研究院有限公司

远江盛邦（北京）网络安全科技股份有限公司

启明星辰信息技术集团股份有限公司

国家互联网应急中心

奇安信科技集团股份有限公司

金蝶国际软件集团有限公司

陕西泽众维密信息技术有限公司

绿盟科技集团股份有限公司

联通数字科技有限公司

新华三信息安全技术有限公司

ISC2 北京分会

中国评测

目 录

CSTC 中国评测

CSTC中国评测

前　言

为加强商用密码管理，保护信息安全，保护公民和组织的合法权益，维护国家的安全和利益，1999 年 10 月 7 日，国务院发布《商用密码管理条例》。2020 年 1 月 1 日，《中华人民共和国密码法》正式实施，这是全面坚持总体国家安全观，规范密码应用和管理，促进密码事业发展的技术性、专业性法律。商用密码应用安全事关国家安全、社会公共利益，以及公民、法人和其他组织的合法权益。因此，建立和完善商用密码应用安全性评估制度，规范商用密码安全性评估工作流程，确保商用密码应用的合规性、正确性、有效性具备重要意义，既是应对我国网络安全严峻形势的迫切需要，也是落实国家重要领域和关键行业网络安全防护责任的有效手段，更是全面贯彻落实《密码法》基本要求，推进商用密码法治建设的重要举措。

为确保大力推进和普及商用密码应用，做好商用密码应用安全性评估工作，本白皮书基于商用密码的行业应用现状，首先说明了密码的重要性，并对商用密码及当前商用密码的标准化进展进行了概述；其次举例说明了商用密码在不同行业的应用需求；然后总结了商用密码当前存在的系列问题，并做出原因分析；再后对商用密码应用安全性评估工作做出陈述，强调了进行商用密码应用安全性评估的必要性，介绍了评估内容；最后针对当前商用密码应用存在的问题，提出了管理建议，并且对商用密码的发展趋势做出了进一步展望。

中国软件评测中心（工业和信息化部软件与集成电路促进中

心），简称“中国评测”，是工业和信息化部直属单位，创立于1990年。成立30年来，中国评测秉承“诚信、担当、唯实、创先”的核心价值观和“专业就是实力”的宗旨，先后承担了10万余款软硬件产品和1万余项信息系统工程的测试任务，已成为国内权威的第三方软、硬件产品及信息系统工程质量安全与可靠性检测机构。中国评测的业务网络覆盖全国500多个城市，出具的测试报告在61个国家和地区实现互认。

中国软件评测中心网络空间安全测评工程技术中心致力于信息系统的网络安全防护和安全运行，支撑政府主管部门履行网络安全相关的社会管理和公共服务职能。长期服务和支撑国家部委、地方政府以及电信、交通、能源、银行、证券、保险、教育、卫生、广电等各大行业，提供网络信息安全战略咨询规划、网络安全平台设计咨询、信息安全风险评估、网络安全等级保护测评、关键信息基础设施保护评估、数据安全能力和合规性评估、APP安全认证检测、商用密码应用安全性评估等网络信息安全相关服务。

在编写《商用密码应用安全性评估白皮书（2021）》的过程中，白皮书编写小组获得了众多专家的指导与帮助，各参编单位专家给予了专业的宝贵建议，为白皮书的撰写提供了重要参考。在此，中国软件评测中心对各参编单位表示衷心的感谢。由于行业发展和技术迭代迅速，编写者能力有限，本书难免存在不足，期待各位读者积极发现问题，并予以批评指正。同时，中国软件评测中心非常期待能够与网络安全行业、密码行业的机构和专家深入合作，推进产学研用协同发展，共同推动我国密码安全事业高质量发展。

一、密码的重要性

应用先进的密码技术能够使公民、法人或其他组织的合法权益得到有效保障。随着经济社会数字化发展步伐加快，密码所承载的商用价值和社会价值愈发受到各界重视。

近年来，各类网络安全事件时有发生。2011 年，国内某知名程序员社区数据库被攻破，大约 600 万条用户注册信息和密码等资料在互联网被公开，该公司证实在 2009 年前确实使用过明文密码的方式存储用户数据，就此埋下了安全隐患，大量用户被通知建议修改密码。2012 年，某全球职场社交网站的 650 万条经过加密的密码数据遭到泄露，事发原因是由于该社交网站使用了未加盐的方法存储加密密码，从而加大了攻击者破解密码的可能性，进而给了黑客进入到用户数据库的可乘之机。2016 年，某全球互联网网站用户个人账户的保密算法被攻破，从而导致上亿用户的个人信息遭黑客窃取，其中涉及用户姓名、电子邮箱、电话号码、出生日期、部分登录密码等信息。2019 年，美国某知名图形图像和排版软件生产商旗下一处数据库由于没有采取密码技术做安全措施，导致任何人皆可访问该数据库，从而致使 750 万个软件用户的个人信息遭到泄露。

这些网络安全事件进一步提高了企业对信息安全保护的重视程度，加快了密码发展应用步伐。只有充分保障网络信息的机密性、可用性、信息来源的真实性、数据的完整性以及行为的不可否认性，信息系统才能够安全稳定运行。密码是维护网络安全最有效、最可靠、最经济的技术手段，其作用可以概括简述为三点：

一是密码可作为网络安全的核心技术和基础支撑，密码可以完整实现网络空间信息防泄密、内容防篡改、身份防假冒、行为抗抵赖等功能，满足网络与信息系统对机密性、完整性、真实性和不可否认性等安全需求；**二是密码可承担网络信任体系的构建基础，**密码算法和密码协议可解决人、机、物的身份标识、身份鉴别、统一管理、信任传递和行为审计问题，是实现安全、可信、可控的互联互通的核心技术手段，密码是网络空间传递价值和信任的重要媒介及手段；**三是密码技术可作为重要的战略性资源，**近年来，我国密码算法设计分析能力达到国际先进水平，我国自主设计的 ZUC 序列密码、SM2 公钥密码、SM3 杂凑密码、SM4 对称密码、SM9 标识密码等商用密码算法已成为国际标准，这是与世界先进密码算法同台竞争、反复论证的结果[1]。商务部、国家密码管理局、海关总署联合发布的商用密码进口许可清单、出口管制清单中，进口许可清单包括加密电话机、加密传真机、密码机（密码卡）、加密 VPN 设备等；出口管制清单中包括安全芯片、密码机（密码卡）、加密 VPN 设备、密钥管理产品、专用密码设备、量子密码设备、密码分析设备、密码研制生产设备、密码测试验证设备，以及相关软件和技术。因而密码技术和产品已经成为一种重要战略资源。

[1] 霍炜，郭启全，马原：《商用密码应用与安全性评估》，北京：电子工业出版社，2020 年版，第 13 页。

二、商用密码概述

（一）商用密码概念

根据《商用密码管理条例》中的定义，**商用密码**是指对不涉及国家秘密内容的信息进行加密保护或者安全认证所使用的密码技术和密码产品。公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。

商用密码具有广泛的应用前景，主要面向不涉及国家秘密内容但又具有敏感性的内部信息、行政事务信息、经济信息等数据进行加密保护。例如企业敏感信息的传输与存储加密、防止非法第三方获取数据、安全认证与数字签名等。

（二）商用密码发展现状

党的十八大以来，以习近平总书记为核心的党中央高度重视互联网、发展互联网、治理互联网，形成了网络强国战略思想，走出了一条中国特色治网之道，指引我国网信事业取得历史性成就，商用密码由此得到全面发展。工业和信息化部党组高度重视商用密码应用推进工作，团结商用密码各方力量，助力商用密码产业做大做强。2021 年 3 月 11 日，工业和信息化部商用密码应用产业促进联盟成立。联盟贯彻落实《密码法》有关要求，推动工业和信息化领域商用密码应用和创新发展，进而做大做强商用密码产业，推动商用密码产业健康、高质量发展。当前，商用密码在科技创新、产业发展和应用推广等方面的落实工作已经初见

成效[2]。

在科技创新方面，商用密码理论和技术研究取得重要进展。我国商用密码的自主创新能力持续增强，已取得一系列高水平、原创性科研成果。部分密码算法例如 ZUC 算法已经成为 3GPP 中 4G 国际标准，SM2/SM9 数字签名算法、SM3 密码杂凑算法、SM4 分组密码算法、SM9 标识加密算法也已达到国际先进水平，成为国际标准。这些算法标准的发布实施，标志着我国商用密码算法具有国际领先的技术理论基础，已经具备了可以广泛应用商用密码的条件。国家密码管理局密码标准查询的统计结果显示，截至 2021 年 5 月，我国现行密码行业标准共有 116 项，现行和即将实行的密码国家标准共有 36 项，这些标准覆盖了密码算法、产品、技术、检测、应用等多个方面，意味着我国密码标准体系正在日益完善。

在产业发展方面，商用密码产业总体规模保持高增长率，商用密码供给质量不断提高，基础支撑能力持续增强。据《2020-2021 中国商用密码产业发展报告》显示，2016 年至 2020 年，我国商用密码产业总体规模持续增长，2020 年我国商用密码产业规模突破 466 亿，同比增速超 33%，详见表 1 所示。

表 1：2016-2020 年商用密码产业总体规模及同比增长率[3]

年份（年）	2016	2017	2018	2019	2020
产业规模（亿元）	151.64	239.41	283	350	466
同比增速（%）	19.05	57.88	18.21	23.67	33.14

[2] 霍炜，郭启全，马原：《商用密码应用与安全性评估》，北京：电子工业出版社，2020 年版，第 99 页。

[3] 数据来源于《2020-2021 中国商用密码产业发展报告》

据国家密码管理局商用密码检测中心报告显示，截至 2021 年 4 月，我国已有 2447 款密码产品获得了商用密码产品认证证书，密码产品品类丰富，较完整的商用密码产品体系已初步形成。当前，我国商用密码产品种类正在持续增多，性能正在不断优化，能够有效保障供给质量。与此同时，商用密码管理体系也在不断健全完善，商用密码应用安全性评估（简称“密评”）试点正在有序展开，商用密码的社会认可度在大幅提升。

在应用推广方面，商用密码已经在一些重要领域和关键行业中得到广泛应用。在通信、金融、教育、医疗健康、交通、社保、能源、国防工业等领域中都能找到商用密码的应用场景。据国家密码管理局行政审批查询结果显示，截至 2021 年 5 月，我国有 59 家电子认证服务使用密码许可单位，及 53 家电子政务电子认证服务机构。2021 年 6 月 16 日，国家密码管理局发布了最新的《商用密码应用安全性评估试点机构目录》，并且明确了 48 家商用密码应用安全性评估试点机构。根据国家密码管理局发文统计，当前国内有超过 80 家金融保险机构通过应用商用密码技术，在电子保单、投保等业务方面实现了国产密码数字证书的全面应用；使用商用密码的第二代居民身份证和港澳台居民居住证共累计发行超 19 亿张；机动车检验标志电子凭证覆盖超过 1.5 亿辆；第三代社会保障卡覆盖超过 4800 万户；10 个省（区、市）已完成基于密码技术的政务云试点建设，覆盖服务用户超过 5000 万人次。

（三）商用密码研究热点

在商用密码技术研究方面，目前研究热点集中在硬件加密、

软件加密、白盒密码、量子密码等领域。

一是硬件加密。硬件加密的密码运算通过专用加密芯片或独立的处理芯片来实现。硬件加密在确保加密硬件中的密钥和关键参数的安全、硬件验证、加密运算与特定设备绑定、无需在主机安装驱动程序或软件、预防冷启动攻击、恶意代码、暴力破解攻击等方面具备优势，有更开阔的应用场景。目前国内的硬件加密解决方案技术提供商已将加密技术和芯片应用于消费电子、汽车电子、物联网和医疗设备等行业。

二是软件加密。软件加密是一种典型的加密解密技术，通过安全加密模块及加密算法对信息进行加密，经过通信过程中的路由和中转到达接收节点，由接收端用户使用相应的解密算法进行解密并还原。从明文生成密文的步骤称为加密算法，解密的步骤为解密算法，加密、解密的算法合在一起统称为密码算法。对称密码算法中通信双方共享一个密钥，用于加密任意大小的数据块或数据流的内容，包括消息、文件、密钥口令。非对称密码算法（公钥密码）中加密和解密分别使用不同的密钥（私钥和公钥），该算法多用于加密较小的数据块，如加密密钥或者数字签名中使用的 Hash 函数值等。

三是白盒密码。白盒密码技术是一项能够抵抗白盒攻击（攻击者对设备终端拥有完全的控制能力）的密码技术。一般从技术实现方式上可以分为静态白盒和动态白盒。静态白盒指密码算法结合特定的密钥经过白盒密码技术处理后形成特定的密码算法库，其能在白盒攻击环境下有效保护原有密钥的安全。动态白盒指生成白盒库后不再更新，原始密钥经过同样的白盒密码技术转

化为白盒密钥。

四是量子密码。量子密码以量子力学和密码学结合，目前学界对量子密码的研究主要集中在协议设计与分析、密钥分发、身份认证、秘密共享、安全直接通信等方面。量子密码的安全性由量子力学基本原理保证，与攻击者的计算能力无关。量子密码学利用量子的不确定性，构造安全的通信通道，保障任何发生在信道上的窃听行为不对通信本身产生影响，从而达到窃听失败的目的，以保证信道的安全[4]。这相比于经典密码是一大优势，因而量子密码正逐渐成为密码新技术中的一个重要研究分支。

三、商用密码标准化进展

2017 年 6 月 1 日我国颁布《中华人民共和国网络安全法》，2018 年 1 月 1 日新修订的《中华人民共和国标准化法》颁布实施，2020 年 1 月 1 日《中华人民共和国密码法》颁布实施。三部法律的实施，加快推进了我国网络空间领域密码应用的发展，也进一步推进密码标准化体系的建立和密码标准化成果的输出。密码标准化既是在密码领域实施标准化战略的直接体现，也是密码技术与密码产品互联互通、走向大规模商用的必然要求[5]。

（一）密码标准体系

《中华人民共和国密码法》第二十二条规定，国家建立和完

[4] 黄静，席博，李鹏，张帆，赵新杰：《一种基于量子密码的卫星网络窃听攻击检测方法》，载《计算机科学》2016 年 43 卷 7 期，第 157-161 页。

[5] 田敏求：《我国密码标准体系研究综述》，载《信息安全与通信机密》2018 年第 5 期，第 94-99 页。

善商用密码标准体系。密码标准体系的建设居于密码标准化工作的核心地位，是具有全局性、引领性、基础性的顶层设计，建设完善标准体系能够促进标准全面、健康、有序、协调发展。国务院标准化行政主管部门和国家密码管理部门依据各自职责，组织制定商用密码国家标准、行业标准。国家支持社会团体、企业利用自主创新技术制定高于国家标准、行业标准相关技术要求的商用密码团体标准、企业标准。参照《中华人民共和国标准化法》确立的我国新型标准体系，密码标准同样可按照国家标准、行业标准、团体标准、企业标准等进行划分。我国商用密码标准体系一级结构如图 1 所示。

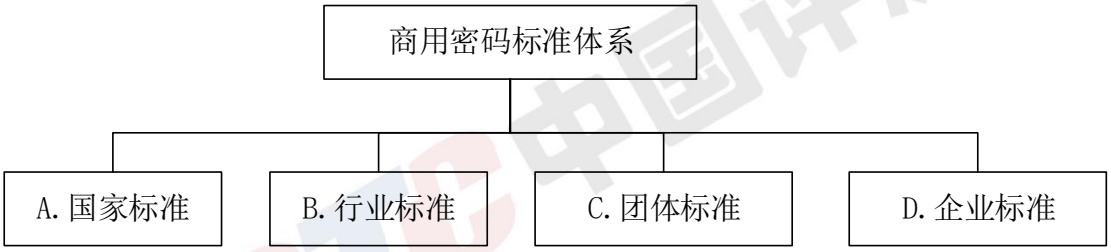

图 1　商用密码标准体系框架[6]

针对商用密码标准体系中的行业标准，当前划分的行业标准体系分为基础类标准、应用类标准、检测类标准和管理类标准。行业密码标准体系将上述各类标准有机组织在一起，形成一个具有逻辑关系的集合，这些标准既可以支撑密码产品研制、密码应用和密码管理，也可以用于支撑其他行业用户构建自己的密码应用标准[7]。行业密码标准体系框架如图 2 所示。

[6] 该图出自中国软件评测中心网络空间安全测评工程技术中心。

[7] 刘平：《密码支撑与密码应用》，载《信息安全与通信机密》2018 年第 5 期，第 22 页。

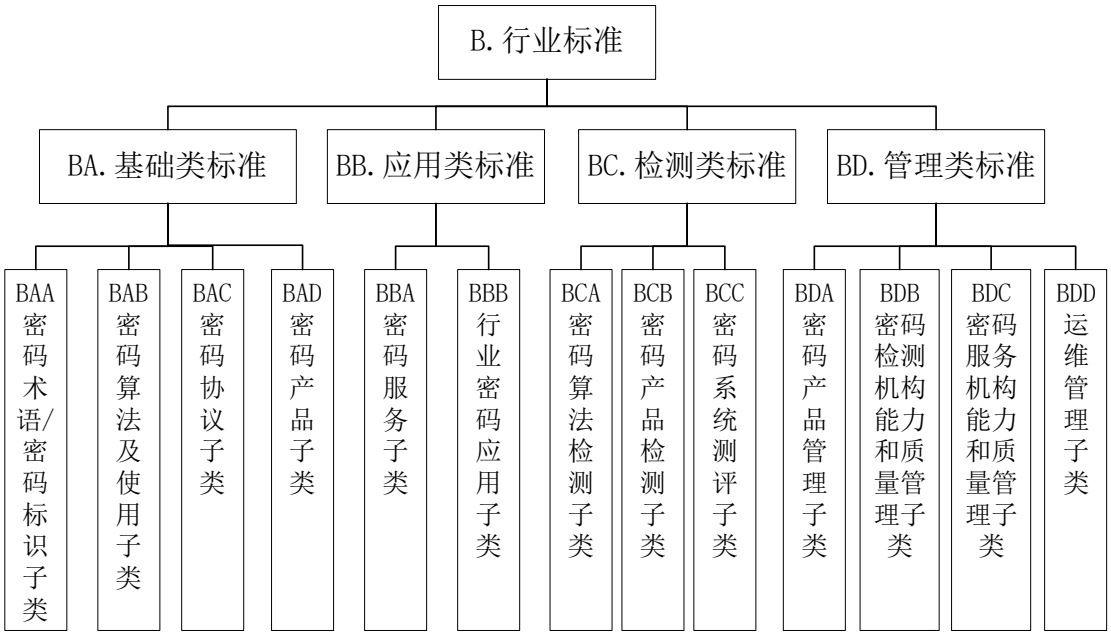

图 2　行业密码标准体系框架[8]

基础类标准为其他三类标准提供了基础、共性支撑（如术语、算法、协议、产品等）；检测类标准保障了基础类标准和应用类标准的合法性检测；管理类标准对其他三类标准进行统一管理；应用类标准为上层具体的密码产品、服务应用提供支持。

近年来，在全国信息安全标准化技术委员会和密码行业标准技术委员会的大力推动下，我国成功将密码算法标准 SM2、SM3、SM4、SM9 推动成为 ISO/IEC 等国际标准，这是我国密码领域在国际标准化工作中的重要进展。随着技术的相互融合和快速发展，也会出现标准“跨类”或是分类界限难以界定的情况，密码标准体系应随技术进步等情况变化而不断被修正、调整和完善。

（二）密码标准成果

在国家标准制订方面，密码国家标准由全国信息安全标准化技术委员会归口管理，具体标准化工作由其下设 WG3 密码工作

[8] 该图出自中国软件评测中心网络空间安全测评工程技术中心。

组负责，根据全国标准信息公共服务平台数据，截止本白皮书发布，我国现行密码国家标准共有35项，即将实施的标准有1项，现行和即将实施的密码国家标准如表2所示。

表2：现行和即将实施的密码国家标准

序号	标准号	标准名称	实施日期
1	GB/T 18238.2-2002	信息技术 安全技术 散列函数 第2部分:采用n位块密码的散列函数	2002/12/1
2	GB/T 21082.4-2007	银行业务 密钥管理(零售) 第4部分: 使用公开密钥密码的密钥管理技术	2007/12/1
3	GB/T 17964-2008	信息安全技术 分组密码算法的工作模式	2008/11/1
4	GB/T 15843.4-2008	信息技术 安全技术 实体鉴别 第4部分: 采用密码校验函数的机制	2008/11/1
5	GB/T 15852.1-2008	信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制	2008/12/1
6	GB/T 16649.15-2010	识别卡 集成电路卡 第15部分：密码信息应用	2011/4/1
7	GB/T 27909.2-2011	银行业务 密钥管理(零售) 第2部分：对称密码及其密钥管理和生命周期	2012/2/1
8	GB/T 27909.3-2011	银行业务 密钥管理(零售) 第3部分：非对称密码系统及其密钥管理和生命周期	2012/2/1
9	GB/T 29829-2013	信息安全技术 可信计算密码支撑平台功能与接口规范	2014/2/1
10	GB/T 32905-2016	信息安全技术 SM3密码杂凑算法	2017/3/1
11	GB/T 32907-2016	信息安全技术 SM4分组密码算法	2017/3/1
12	GB/T 32918.1-2016	信息安全技术 SM2椭圆曲线公钥密码算法 第1部分：总则	2017/3/1
13	GB/T 32918.2-2016	信息安全技术 SM2椭圆曲线公钥密码算法 第2部分：数字签名算法	2017/3/1
14	GB/T 32918.3-2016	信息安全技术 SM2椭圆曲线公钥密码算法 第3部分：密钥交换协议	2017/3/1
15	GB/T 32918.4-2016	信息安全技术 SM2椭圆曲线公钥密码算法 第4部分：公钥加密算法	2017/3/1
16	GB/T 33133.1-2016	信息安全技术 祖冲之序列密码算法 第1部分：算法描述	2017/5/1
17	GB/T 33560-2017	信息安全技术 密码应用标识规范	2017/12/1

序号	标准号	标准名称	实施日期
18	GB/T 32918.5-2017	信息安全技术 SM2 椭圆曲线公钥密码算法 第5部分：参数定义	2017/12/1
19	GB/T 35291-2017	信息安全技术 智能密码钥匙应用接口规范	2018/7/1
20	GB/T 35276-2017	信息安全技术 SM2 密码算法使用规范	2018/7/1
21	GB/T 35275-2017	信息安全技术 SM2 密码算法加密签名消息语法规范	2018/7/1
22	GB/T 36322-2018	信息安全技术 密码设备应用接口规范	2019/1/1
23	GB/T 25056-2018	信息安全技术 证书认证系统密码及其相关安全技术规范	2019/1/1
24	GB/T 37033.1-2018	信息安全技术 射频识别系统密码应用技术要求 第1部分：密码安全保护框架及安全级别	2019/7/1
25	GB/T 37033.2-2018	信息安全技术 射频识别系统密码应用技术要求 第2部分：电子标签与读写器及其通信密码应用技术要求	2019/7/1
26	GB/T 37092-2018	信息安全技术 密码模块安全要求	2019/7/1
27	GB/T 37033.3-2018	信息安全技术 射频识别系统密码应用技术要求 第3部分：密钥管理技术要求	2019/7/1
28	GB/T 38540-2020	信息安全技术 安全电子签章密码技术规范	2020/10/1
29	GB/T 38541-2020	信息安全技术 电子文件密码应用指南	2020/10/1
30	GB/T 38556-2020	信息安全技术 动态口令密码应用技术规范	2020/10/1
31	GB/T 38636-2020	信息安全技术 传输层密码协议（TLCP）	2020/11/1
32	GB/T 38625-2020	信息安全技术 密码模块安全检测要求	2020/11/1
33	GB/T 38635.2-2020	信息安全技术 SM9 标识密码算法 第2部分：算法	2020/11/1
34	GB/T 38635.1-2020	信息安全技术 SM9 标识密码算法 第1部分：总则	2020/11/1
35	GB/T 15852.1-2020	信息技术 安全技术 消息鉴别码 第1部分：采用分组密码的机制	2021/7/1
36	GB/T 39786-2021	信息安全技术 信息系统密码应用基本要求	2021/10/1

在行业标准制订方面，密码行业标准由国家密码管理局归口

管理。2011 年密码行业标准化技术委员会正式成立，标志着密码标准化工作正式被纳入国家标准管理体系。根据国家密码管理局标准规范查询数据，我国现行密码行业标准共有 116 项，基本形成了较为齐全的密码行业标准。SSL、TLS、IPSec、HTTPS 等协议的设计充分发挥了密码技术的作用，因此密码行业标准的制定工作应当与时俱进。面对新一代信息技术产业高速发展的现状，目前存在标准资源受限问题，以 5G 通信、云计算、大数据、物联网、移动互联网、人工智能等技术构建的新产业新业态中亟需加强新型密码算法的研究及标准制定，大力发展密码产业，护航我国数字经济高质量发展。现行密码行业标准如表 3 所示。

表 3：密码行业标准

序号	标准编号	标准名称	实施日期
1	GM/T 0001.1	祖冲之序列密码算法 第 1 部分 算法描述	2012/3/21
2	GM/T 0001.2	祖冲之序列密码算法 第 2 部分 基于祖冲之算法的机密性算法	2012/3/21
3	GM/T 0001.3	祖冲之序列密码算法 第 3 部分 基于祖冲之算法的完整性算法	2012/3/21
4	GM/T 0002	SM4 分组密码算法	2012/3/21
5	GM/T 0003.1	SM2 椭圆曲线公钥密码算法 第 1 部分 总则	2012/3/21
6	GM/T 0003.2	SM2 椭圆曲线公钥密码算法 第 2 部分 数字签名算法	2012/3/21
7	GM/T 0003.3	SM2 椭圆曲线公钥密码算法 第 3 部分 密钥交换协议	2012/3/21
8	GM/T 0003.4	SM2 椭圆曲线公钥密码算法 第 4 部分 公钥加密算法	2012/3/21
9	GM/T 0003.5	SM2 椭圆曲线公钥密码算法 第 5 部分 参数定义	2012/3/21
10	GM/T 0004	SM3 密码杂凑算法	2012/3/21
11	GM/T 0005	随机性检测规范	2012/3/21

序号	标准编号	标准名称	实施日期
12	GM/T 0006	密码应用标识规范	2012/3/21
13	GM/T 0008	安全芯片密码检测准则	2012/11/22
14	GM/T 0009	SM2 密码算法使用规范	2012/11/22
15	GM/T 0010	SM2 密码算法加密签名消息语法规范	2012/11/22
16	GM/T 0011	可信计算 可信密码支撑平台功能与接口规范	2012/11/22
17	GM/T 0013	可信计算 可信密码模块符合性检测规范	2012/11/22
18	GM/T 0014	数字证书认证系统密码协议规范	2012/11/22
19	GM/T 0015	基于 SM2 密码算法的数字证书格式规范	2012/11/22
20	GM/T 0016	智能密码钥匙密码应用接口规范	2012/11/22
21	GM/T 0017	智能密码钥匙密码应用接口数据格式规范	2012/11/22
22	GM/T 0018	密码设备应用接口规范	2012/11/22
23	GM/T 0019	通用密码服务接口规范	2012/11/22
24	GM/T 0020	证书应用综合服务接口规范	2012/11/22
25	GM/T 0021	动态口令密码应用技术规范	2012/11/22
26	GM/Z 0001	密码术语	2013/6/20
27	GM/T 0022	IPSec VPN 技术规范	2014/2/13
28	GM/T 0023	IPSec VPN 网关产品规范	2014/2/13
29	GM/T 0024	SSL VPN 技术规范	2014/2/13
30	GM/T 0025	SSL VPN 网关产品规范	2014/2/13
31	GM/T 0026	安全认证网关产品规范	2014/2/13
32	GM/T 0027	智能密码钥匙技术规范	2014/2/13

序号	标准编号	标准名称	实施日期
33	GM/T 0028	密码模块安全技术要求	2014/2/13
34	GM/T 0029	签名验签名服务器技术规范	2014/2/13
35	GM/T 0030	服务器密码机技术规范	2014/2/13
36	GM/T 0031	安全电子签章密码技术规范	2014/2/13
37	GM/T 0032	基于角色的授权与访问控制技术规范	2014/2/13
38	GM/T 0033	时间戳接口规范	2014/2/13
39	GM/T 0034	基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范	2014/2/13
40	GM/T 0035.1	射频识别系统密码应用技术要求 第 1 部分：密码安全保护框架及安全级别	2014/2/13
41	GM/T 0035.2	射频识别系统密码应用技术要求 第 2 部分：电子标签芯片密码应用技术要求	2014/2/13
42	GM/T 0035.3	射频识别系统密码应用技术要求 第 3 部分：读写器密码应用技术要求	2014/2/13
43	GM/T 0035.4	射频识别系统密码应用技术要求 第 4 部分：电子标签与读写器通信密码应用技术要求	2014/2/13
44	GM/T 0035.5	射频识别系统密码应用技术要求 第 5 部分：密钥管理技术要求	2014/2/13
45	GM/T 0036	采用非接触卡的门禁系统密码应用技术指南	2014/2/13
46	GM/T 0037	证书认证系统检测规范	2014/2/13
47	GM/T 0038	证书认证密钥管理系统检测规范	2014/2/13
48	GM/T 0039	密码模块安全检测要求	2015/4/1
49	GM/T 0040	射频识别标签模块密码检测准则	2015/4/1
50	GM/T 0041	智能 IC 卡密码检测规范	2015/4/1
51	GM/T 0042	三元对等密码安全协议测试规范	2015/4/1
52	GM/T 0043	数字证书互操作检测规范	2015/4/1
53	GM/T 0044.1	SM9 标识密码算法 第 1 部分：总则	2016/3/28

序号	标准编号	标准名称	实施日期
54	GM/T 0044.2	SM9 标识密码算法 第 2 部分：数字签名算法	2016/3/28
55	GM/T 0044.3	SM9 标识密码算法 第 3 部分：密钥交换协议	2016/3/28
56	GM/T 0044.4	SM9 标识密码算法 第 4 部分：密钥封装机制和公钥加密算法	2016/3/28
57	GM/T 0044.5	SM9 标识密码算法 第 5 部分：参数定义	2016/3/28
58	GM/T 0045	金融数据密码机技术规范	2016/3/28
59	GM/T 0046	金融数据密码机检测规范	2016/12/23
60	GM/T 0047	安全电子签章密码检测规范	2016/12/23
61	GM/T 0048	智能密码钥匙密码检测规范	2016/12/23
62	GM/T 0049	密码键盘密码检测规范	2016/12/23
63	GM/T 0050	密码设备管理 设备管理技术规范	2016/12/23
64	GM/T 0051	密码设备管理 对称密钥管理技术规范	2016/12/23
65	GM/T 0052	密码设备管理 VPN 设备监察管理规范	2016/12/23
66	GM/T 0053	密码设备管理 远程监控与合规性检验接口数据规范	2016/12/23
67	GM/T 0054	信息系统密码应用基本要求	2018/2/8
68	GM/T 0055-2018	电子文件密码应用技术规范	2018/5/2
69	GM/T 0056-2018	多应用载体密码应用接口规范	2018/5/2
70	GM/T 0057-2018	基于 IBC 技术的身份鉴别规范	2018/5/2
71	GM/T 0058-2018	可信计算 TCM 服务模块接口规范	2018/5/2
72	GM/T 0059-2018	服务器密码机检测规范	2018/5/2
73	GM/T 0060-2018	签名验签服务器检测规范	2018/5/2
74	GM/T 0061-2018	动态口令密码应用检测规范	2018/5/2

序号	标准编号	标准名称	实施日期
75	GM/T 0062-2018	密码产品随机数检测要求	2018/5/2
76	GM/T 0063-2018	智能密码钥匙密码应用接口检测规范	2018/8/20
77	GM/T 0064-2018	限域通信(RCC)密码检测要求	2018/8/20
78	GM/T 0065-2019	商用密码产品生产和保障能力建设规范	2019/7/16
79	GM/T 0066-2019	商用密码产品生产和保障能力建设实施指南	2019/7/16
80	GM/T 0067-2019	基于数字证书的身份鉴别接口规范	2019/7/16
81	GM/T 0068-2019	开放的第三方资源授权协议框架	2019/7/16
82	GM/T 0069-2019	开放的身份鉴别框架	2019/7/16
83	GM/T 0070-2019	电子保单密码应用技术要求	2019/7/16
84	GM/T 0071-2019	电子文件密码应用指南	2019/7/16
85	GM/T 0072-2019	远程移动支付密码应用技术要求	2019/7/16
86	GM/T 0073-2019	手机银行信息系统密码应用技术要求	2019/7/16
87	GM/T 0074-2019	网上银行密码应用技术要求	2019/7/16
88	GM/T 0075-2019	银行信贷信息系统密码应用技术要求	2019/7/16
89	GM/T 0076-2019	银行卡信息系统密码应用技术要求	2019/7/16
90	GM/T 0077-2019	银行核心信息系统密码应用技术要求	2019/7/16
91	GM/T 0012-2020	可信计算 可信密码模块接口规范	2021/7/1
92	GM/T 0078-2020	密码随机数生成模块设计指南	2021/7/1
93	GM/T 0079-2020	可信计算平台直接匿名证明规范	2021/7/1
94	GM/T 0080-2020	SM9 密码算法使用规范	2021/7/1
95	GM/T 0081-2020	SM9 密码算法加密签名消息语法规范	2021/7/1

序号	标准编号	标准名称	实施日期
96	GM/T 0082-2020	可信密码模块保护轮廓	2021/7/1
97	GM/T 0083-2020	密码模块非入侵式攻击缓解技术指南	2021/7/1
98	GM/T 0084-2020	密码模块物理攻击缓解技术指南	2021/7/1
99	GM/T 0085-2020	基于 SM9 标识密码算法的技术体系框架	2021/7/1
100	GM/T 0086-2020	基于 SM9 标识密码算法的密钥管理系统技术规范	2021/7/1
101	GM/T 0087-2020	浏览器密码应用接口规范	2021/7/1
102	GM/T 0088-2020	云服务器密码机管理接口规范	2021/7/1
103	GM/T 0089-2020	简单证书注册协议规范	2021/7/1
104	GM/T 0090-2020	标识密码应用标识格式规范	2021/7/1
105	GM/T 0091-2020	基于口令的密钥派生规范	2021/7/1
106	GM/T 0092-2020	基于 SM2 算法的证书申请语法规范	2021/7/1
107	GM/T 0093-2020	证书与密钥交换格式规范	2021/7/1
108	GM/T 0094-2020	公钥密码应用技术体系框架规范	2021/7/1
109	GM/T 0095-2020	电子招投标密码应用技术要求	2021/7/1
110	GM/T 0096-2020	射频识别防伪系统密码应用指南	2021/7/1
111	GM/T 0097-2020	射频识别电子标签统一名称解析服务安全技术规范	2021/7/1
112	GM/T 0098-2020	基于 IP 网络的加密语音通信密码技术规范	2021/7/1
113	GM/T 0099-2020	开放式版式文档密码应用技术规范	2021/7/1
114	GM/T 0100-2020	人工确权型数字签名密码应用技术要求	2021/7/1
115	GM/T 0101-2020	近场通信密码安全协议检测规范	2021/7/1
116	GM/T 0102-2020	密码设备应用接口符合性检测规范	2021/7/1

在团体标准制定方面，《中华人民共和国标准化法》中新确立了团体标准的地位，目前已有部分团体标准化组织依照《团体标准管理规定（试行）》的要求开展密码团体标准的探索实践。在《中华人民共和国标准化法》中将标准制定主体由政府扩展到行业协会、产业联盟以及广大企业，鼓励社会团体协调相关主体，共同制定满足市场需要和创新需要的团体标准，这标志着我国标准由单一供给向多元供给的重大转变；同时，国家鼓励企业自行制定严于国家标准或者行业标准的企业标准，企业标准由企业制定，由企业法人代表或法人代表授权的主管领导批准、发布。在密码领域的标准化工作中，团体标准、企业标准是国家标准和行业标准的有益补充，表 4 中列出目前制订的一些密码团体标准。

表 4：部分密码团体标准

序号	标准号	标准名称	批准或归口单位	实施日期
1	T/SCCIA 007-2020	区块链密码检测规范	深圳市商用密码行业协会	2020/3/26
2	T/SCCIA 009—2020	区块链密码服务接口标准及安全要求	深圳市商用密码行业协会	2020/4/11
3	T/SCCIA 010-2020	区块链密码应用验证规范	深圳市商用密码行业协会	2020/6/12
4	T/EMCG 002—2020	移动智能终端密码技术政企应用指南	中关村网络安全与信息化产业联盟	2020/8/16

四、商用密码典型应用场景

商用密码在各领域内的推广应用是我国迈向网络化、现代化、数字化的重要基础。《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》提出要加快数字化发展，建设数字中国，推动数字产业化和产业数字化。目前我国电信和

互联网、工业互联网、车联网、物联网、智慧交通、电子政务、金融等领域信息化水平不断提升，大力推动商用密码在相关领域的应用，是保障重要领域网络安全的重要举措，也是推动信创产业发展，带动产业实现数字化转型的安全保障。

（一）电信和互联网领域

电信和互联网行业是全球数字化进程的先驱。《中国互联网络发展状况统计报告》显示，截至 2020 年 12 月，我国网民规模达 9.89 亿，互联网普及率达 70.4%。同时，《数字中国发展报告（2020 年）》统计数据指明，我国已经建成全球规模最大的光纤网络和 4G 网络，固定宽带家庭普及率由 2015 年底的 52.6%提升到 2020 年底的 96%；移动宽带用户普及率由 2015 年底的 57.4%提升到 2020 年底的 108%；移动互联网用户接入流量由 2015 年底的 41.9 亿 GB 增长到 2020 年的 1656 亿 GB。坚实的电信网络用户基础催生了丰富的行业数据资源，行业发展迎来新机遇的同时也面临着新的网络安全风险和数据安全风险，而应用商用密码可以为数据的处理、存储、共享安全保驾护航，为信息系统安全运维提供技术解决方案，促进电信互联网产业健康发展。

中国电信在业界首次创新提出“商密云”的应用理念，其主导研发的“商密云存储系统”创新采用“云+端”体系架构，具有自主、可控的安全属性，基于分布式用户端计算及控制机制，采用一文一密、双证书、两级密钥管理等自主专利技术方案，实现商用密码技术和云存储技术的有机融合，为用户提供高安全强度、自主可控的数据安全处理、存储、共享及保障服务，有效提升了用户数据的安全性，在云存储应用的安全性探索中具有强示

范作用。另外，对于数据存储和共享安全问题，还可以采用属性基加密和抗密钥泄露技术来解决。在密文上传到云服务前，可以将访问控制策略或属性进行隐藏 ，使用属性布隆过滤器将属性隐藏在匿名的访问控制结构中，这样能够实现数据和属性的同时隐藏。抗密钥泄漏基于身份加密算法可以对数据进行加密上传，解密下载，从而可以避免现有密码算法没有考虑各种攻击存在的情况下而导致的部分隐私泄漏问题[9]。

商用密码应用在云平台运维系统中也能充分发挥作用。某电信增值业务提供商为了保障云平台运维系统的网络安全，分别在网络和通信、设备和计算、应用和数据等方面应用商用密码以保障系统在安全的状态下运维。在网络和通信安全方面，该运营商在系统机房之间使用了专线连接，办公区内终端远程访问机房局域网时通过 VPN 建立的通信信道，VPN 采用用户名+PIN+UKey 方式进行身份鉴别；在设备和计算安全方面，通过堡垒机远程管理服务器及服务器本地的数据库，堡垒机同时采用用户名/口令和已获认证的动态令牌两种鉴别技术对登录用户进行身份鉴别，远程管理堡垒机、服务器、数据库时采用了 SSH 协议；在应用和数据安全方面，云平台运维系统的登录采用了账号 ID+PIN 码+Ukey 的方式，通过手指遮挡 Ukey 上的光源触发设备并发送一串随机数字进行校验；另外，互联网访问云平台运维系统时采用了 HTTPS 协议以保护传输数据的完整性和机密性，同时也采用了 SSL 证书。商用密码在电信和互联网中的应用如图 3 所示。

[9] 郑东，张应辉：《密码技术在 5G 安全中的应用》，载《信息安全与通信机密》2019 年第 1 期，第 52-53 页。

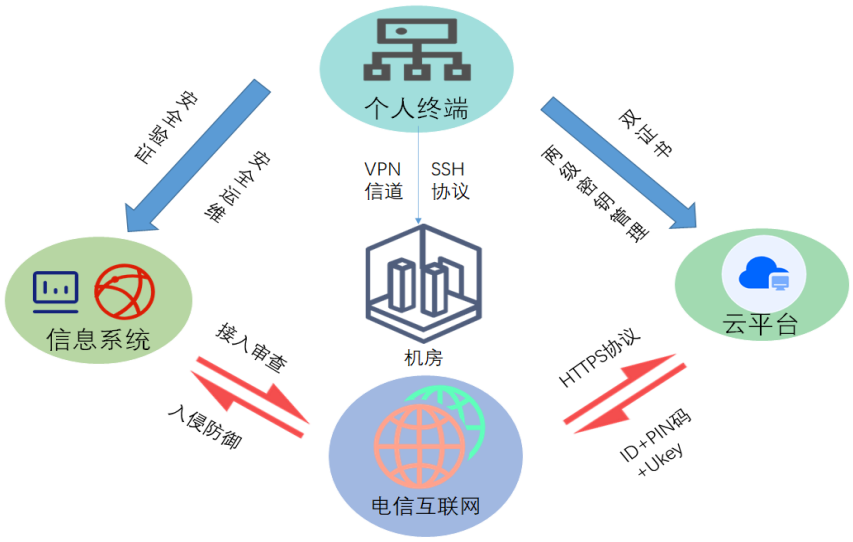

图 3　商用密码在电信和互联网领域的应用视图[10]

（二）工业互联网领域

我国高度重视商用密码算法尤其是轻量级密码算法的研究及其在工业互联网领域的应用。2021 年 1 月 13 日，工信部官网发布《工业互联网创新发展行动计划（2021-2023 年）》，行动计划中提出要“统筹工业互联网发展和安全，提升新型基础设施支撑服务能力，拓展融合创新应用，深化商用密码应用”“加快密码应用核心技术突破和标准研制，推动需求侧、供给侧有效对接和协同创新，推动密码技术深入应用”“加强工业互联网密码应用安全性评估能力建设”。工业互联网平台的数字化、网络化、智能化离不开安全体系的保障，安全体系中的身份鉴别、认证鉴权、访问控制、数据加密、安全可信等防护过程离不开密码技术的支撑。在工业互联网的平台、应用、数据三大体系建设推进过程中，密码技术发挥重要作用。

一是应用于工业互联网平台基础设施建设。密码技术可以应

[10] 该图出自中国软件评测中心网络空间安全测评工程技术中心。

用在互联网信息系统的网络和通信、设备和计算、应用和数据等各个方面，工业互联网平台是以云计算、大数据、物联网等技术为依托的工业基础应用设施，在工业互联网平台的边缘层、IaaS 层、PaaS 层、SaaS 层建设中都需要用到通用密码服务、密码管理以及密码应用。在 IaaS 层，密码应用在租户的数据和虚拟机镜像的加密保护以及用户的身份鉴别方面。在 PaaS 层，目前常见的服务包括数据库服务、对象存储服务、地图服务、电子签名等，密码应用主要体现在数据加解密、安全认证、授权管理以及协同签名等方面 。在 SaaS 层，密码技术的应用主要体现在为工业互联网用户提供安全接入、身份认证、访问控制、数据加密、数据防篡改、工业敏感数据保护等方面，例如采用 SM2 和 SM3 算法提供数字签名和完整性校验，进行数据原发证据和数据接收证据，实现抗抵赖防护。

二是应用于工业互联网身份鉴别和访问控制。身份认证与鉴别贯穿工业互联网应用的各个层次，在工业互联网标识解析体系建设中具备重要应用意义。工业互联网边缘接入层有海量的设备接入平台，常规的黑名单技术只能抵御已知有害设备引入的网络威胁，而采用白名单机制、强制访问控制等安全机制可以对接入的主体和客体进行细粒度的访问控制；在 IaaS 层，需要对服务器用户进行身份鉴别；在 PaaS 层及 SaaS 层，需要对登录用户进行身份认证和鉴别[11]，并且对登录校验码设置时效。国产商用密码算法 SM2 是基于 ECC 的椭圆曲线公钥密码算法，签名速度与密

[11] 柳彩云，陈雪鸿，杨帅锋：《国产密码算法与工业互联网平台的结合势在必行》，载《中国信息安全》2019 年第 4 期，第 86-89 页。

钥生成速度都快于 RSA 算法，安全强度高于 RSA2048，已经成为国际标准，应用 SM2 算法和强制访问控制等安全机制能更好地实现工业互联网中的身份认证鉴别，实现基于主体身份和客体属性的细粒度访问控制，提升工业互联网边缘层设备接入安全性。

三是应用于工业互联网数据全生命周期安全保护。网络安全保护的目标是确保系统和数据的机密性、完整性、可用性，在工业互联网应用中应重点突出系统可用性，同时确保数据存储过程、通信过程的机密性和完整性。工业互联网应用大力推动传统工业企业进行数字化转型，包括企业上云、设备上云、数据上云，因而要在 IaaS 层的基础资源池和设施建设、PaaS 层的数据挖掘和海量数据汇聚分析、SaaS 层的工业软件和微服务开发应用中进行数据的存储加密、通信加密、完整性校验。然而在工业互联网中应用密码算法时，要警惕攻击的存在和恶意嵌入的发生，如 MD5 算法存在可碰撞性攻击、RSA 算法存在共模攻击，另外还可能存在恶意嵌入远程木马等危险程序的算法。路透社曾爆料 RSA 在其软件 Bsafe 中嵌入了美国国家安全局（NSA）开发的被植入后门的伪随机数生成算法 Dual_EC-DRBG，NSA 还利用美国国家标准与技术研究院（NIST）认证该漏洞算法为安全加密标准，使得该算法成为大量软件产品默认使用的随机数生成器。由此可见，在工业互联网等新型基础设施建设过程中，国产密码技术的应用占据着举足轻重的地位。目前我国已经有与 AES、RSA、MD5、ECC 等国际密码算法相对应的国产商用密码算法。在数据通信、数据存储中使用 SM1、SM2、SM3、SM4、SM7、SM9、祖冲之等国产密码算法是保证工业互联网网络、平台、数据的安

全的重要途径。

密码技术和产品在工业互联网中具备一些常见且典型的应用模式。2020 年 4 月，工业互联网产业联盟发布《工业互联网体系架构（2.0）》，对工业互联网网络架构进行了阐述。2020 年 11 月 28 日，国内一些工业互联网和密码安全技术研究公司发布《工业互联网密码应用模式白皮书（V1.0.1）》，从应用层、终端与基础设施层、基础密码产品三个维度，对 20 种密码应用模式进行了剖析。中国软件评测中心网安中心总结了商用密码在工业互联网场景下的应用，参考工业互联网 IaaS、PaaS、SaaS 的分层结构，将工业互联网网络结构视图分为设备层、边缘层、企业层、产业层，并研究梳理了每层内部功能、层间网络连接过程应用的密码技术和产品，包括了基于微内核加密算法的加密芯片、基于密码机和动态令牌的可信计算环境、实现设备授信过程的 IBC 信任体系、PKI 信任体系等密码产品，以及基于 SM3 算法的校验与防篡改、基于 SM2/SM4 的通信消息加密和文件存储加密、可追溯的数字水印、基于 SSL VPN 的访问控制、基于 SM2 私钥签名的身份鉴别、应用内数据加密等技术。具体的商用密码在工业互联网中的应用视图如图 4 所示。

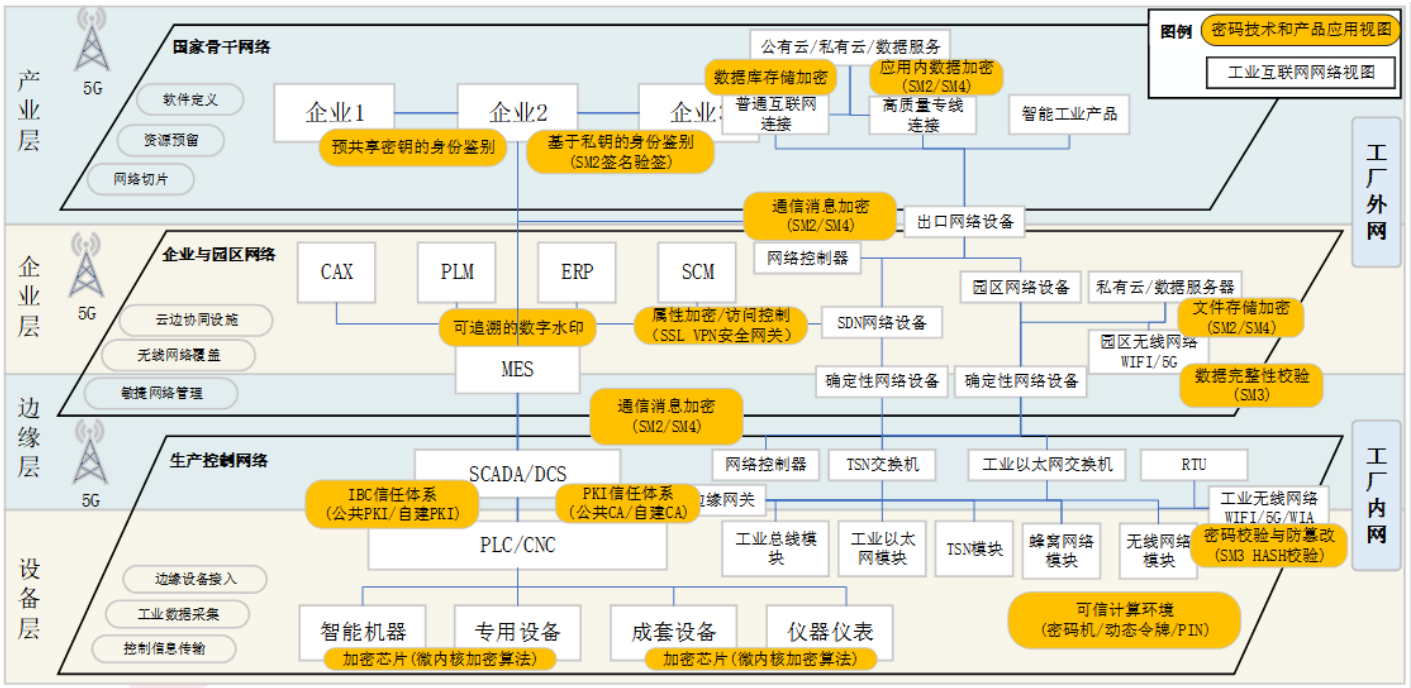

图 4　商用密码在工业互联网领域的应用视图[12]

（三）车联网领域

2021 年 6 月 10 日，工业和信息化部办公厅发布《关于开展车联网身份认证和安全信任试点工作的通知》，通知中明确指出车联网身份认证和安全信任试点工作的开展目的之一是为推动商用密码应用，保障蜂窝车联网（C-V2X）通信安全。密码技术是解决车联网安全问题既可靠又有效的手段，其为车与云安全通信、车与车安全通信、车与路安全通信、车与设备安全通信、车与网络安全通信五个方面提供了基础支撑，是保障车联网网络和信息系统安全的重要基石。

一是支撑车与云安全通信。车载信息交互系统、汽车网关、C-V2X 车载通信设备等与车联网服务平台间的安全通信需要通过基于商用密码的数字证书、数字签名、数据加密等密码技术来

[12] 该图出自中国软件评测中心网络空间安全测评工程技术中心，参考自《工业互联网体系架构》（2020）。

实现。车云通信安全隧道的建立以及车云通信数据机密性和完整性保护，需要基于安全通信协议进行构建和保护。车端消息封装和证书管理的实现以及平台侧证书验证和数据解析的实现，均需要基于密码应用中间件进行。为防止用户资源非授权访问的发生，确保业务接入者及服务者身份的真实性、业务内容访问的合法性，需要应用密码技术建立用户资源隔离机制[13]。密钥等重要数据的传输需要通过国密 SSL 协议，并对关键敏感数据进行加密保护和完整性校验。此外，为保障车联网用户密钥安全，应建立密钥管理体系对密钥的产生、分发、使用和销毁进行系统管理。

二是支撑车与车安全通信。密钥管理、证书管理、安全计算等车端安全凭证管理和数据处理功能的实现，需要在车端应用基于商用密码的安全芯片和软件模块等组件。车载设备证书的初始化需要通过车辆生产环节配置、运营商通道配置、服务器令牌授权等方式实现。建立车载设备证书管理系统，可以为车载设备提供证书发布、更新、撤销等证书管理服务。车与车安全通信密码应用可以在重点城市、高速公路、物流园区、港口、矿山、科技园区等场景中，实现基于安全通信的辅助驾驶和有条件自动驾驶，包括碰撞预警、盲区预警、变道辅助、异常车辆提醒、编队行驶等。

三是支撑车与路安全通信。路侧设备通过搭载基于商用密码的安全芯片、软件模块等组件，可以实现安全凭证管理和数据处理功能。为路侧设备提供证书发布、更新、撤销等证书管理服务，

[13] 宋飞，董贵山，邓子健，张岳公：《发挥密码基础支撑作用，整体保障云计算安全》，载《信息安全与通信机密》2018 年第 5 期，第 63-68 页。

可以通过建立路侧设备证书管理系统来实现。车与路安全通信密码应用可以在重点城市、高速公路、封闭测试场、车路协同试点路段等场景中，实现基于安全通信的安全预警、效率提升，包括红绿灯提醒及绿波通行、道路交通信息提示、弱势交通参与者提醒、公交优先通行、自动驾驶测试等。

四是支撑车与设备安全通信。车载信息交互系统与手持移动智能终端、新能源汽车与充电桩等车与外部设备交互场景的安全通信，通过基于商用密码的数字证书、数字签名、数据加密技术方实现。车载短距无线通信场景中的密钥可信交换和安全保护的实现，通过采用安全协议对通信链路进行加密来完成。合理应用身份认证和加密技术等密码应用，能够保证车和设备之间的安全通信，比如用户手持移动智能终端的车辆远程控制、车辆信息查询、安全预警、无钥匙进入、新能源汽车充电、车载设备互联等车载短距无线通信等。

五是支撑车与网络安全通信[14]。数据或信令遭窃听或者篡改及重放、假冒终端、伪基站等问题是蜂窝通信接口场景下的车联网通信系统面临的主要安全风险。在蜂窝通信和直连通信过程中，需要应用密码技术在终端与服务网络之间对网络信令进行加密处理、完整性保护和抗重放保护，确保信令传递过程中信息不被窃听、篡改、重放、伪造。为进一步保证车联网网络安全，还需要应用密码技术在终端与服务网络之间进行双向认证，确认对方身份合法性；系统需要对消息来源进行认证，确保消息的合法性；

[14] 徐秀，唐明环，马聪，于润东：《车联网密码应用体系研究》，载《信息通信技术与政策》2020 年第 8 期，第 48-49 页。

与此同时，系统还需要隐藏真实身份标识及位置信息，对用户数据进行加密保护，以防用户隐私遭泄露。具体的商用密码在车联网中的应用视图如图 5 所示。

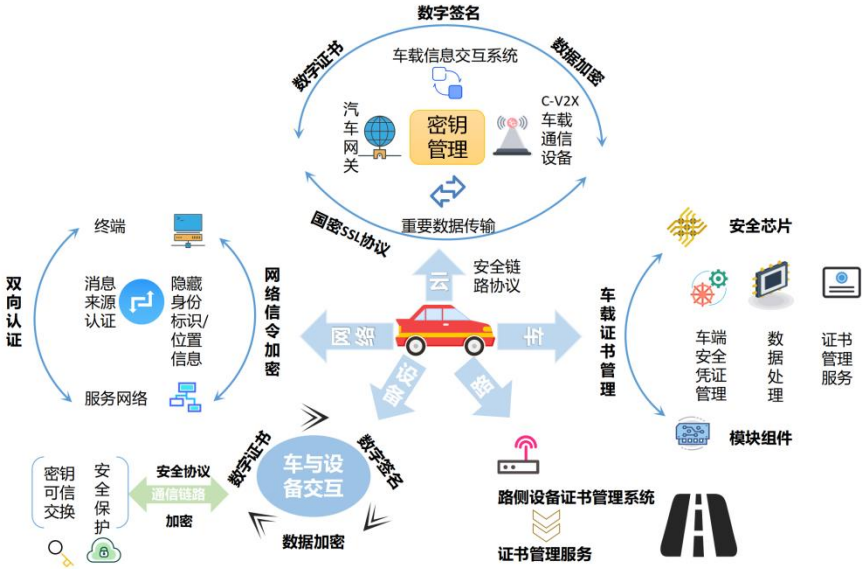

图 5　商用密码在车联网领域的应用视图[15]

（四）物联网领域

物联网系统身份认证过程中，一般包括设备与设备、设备与用户、设备与平台之间的认证。传统的身份认证方式中，采用普通的用户名和口令认证方式，无法避免弱口令、撞库攻击、字典攻击等问题。物联网系统中数据传输过程中，一般以明文形式传输，尽管有些采取了密钥加密的安全措施，但通常采用的是对称算法，加密解密为同一把密钥，一旦密钥被破解或被内部人员泄露，存在巨大安全隐患；若是使用低强度密钥进行加密，依靠目前发达的计算条件，通过穷举等方式存在破解的可能。物联网系统智能摄像头、智能家居等应用情景中，终端设备数量多，网络

[15] 该图出自中国软件评测中心网络空间安全测评工程技术中心。

环境复杂，安全漏洞较多；业务交互过程中，一旦网络被监听，数据被窃取或篡改，则会致使敏感数据或重要数据泄露。

针对以上物联网系统中存在的网络安全脆弱性，国内某商用密码解决方案提供厂商研究开发基于商用密码的物联网安全防护解决方案。物联网由应用系统、物联网运营平台、设备/芯片生产系统、终端应用组成，贯穿云—管—端三个层面，提供全部物联网服务。在防护体系中，由安全管理平台、密钥基础设施、安全中间件组成，提供用户、终端、平台、系统的全方位安全支撑，实现密钥安全分发、身份认证、数据加密/签名等安全服务。当业务、芯片、设备的规模较大时，可单独管理和使用密钥基础设施，同时在系统端直接部署密钥基础设施，独享全部资源，实现灵活的基础设施建设。除了支持各类传统的密码算法如 SM2、SM3、SM4 国家标准密码算法和 AES256、SHA256 以上系列等国际算法外，特别支持 SM9 标识密码算法，提供包括 SM9/ SM4 等密钥生成、数据的非对称加解密、消息的签名验签、数据的对称加解密等功能。商用密码在物联网中的应用视图如图 6 所示。

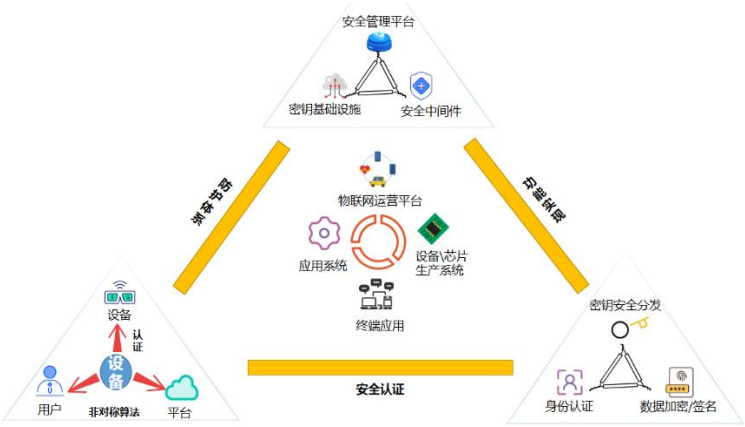

图 6　商用密码在物联网领域的应用视图[16]

[16] 该图出自中国软件评测中心网络空间安全测评工程技术中心。

（五）智慧交通领域

《数字中国发展报告（2020 年）》统计数据显示，当前我国高速公路电子不停车收费（ETC）车道达到 6.6 万条，客车 ETC 使用率超过 70%，货车 ETC 使用率超过 56%。互联网出行服务体系不断完善。2020 年 8 月，交通运输部印发《关于推动交通运输领域新型基础设施建设的指导意见》，提出要打造融合高效的智慧交通基础设施，切实推进商用密码等技术应用。在智慧公路建设中，全国高速公路联网 ETC 系统的特点表现为部、省两级共同管理，业务互通系统关联度高，服务范围广（遍及全国）。围绕系统特点，商用密码在 ETC 系统中的应用主要体现在以下三个方面。

一是应用在部、省级密钥管理系统中，通过利用各省市金融数据密码机，实现分发管理 PSAM 卡、OBU 设备和 ETC 卡的一次发行和二次发行、设备初始化、用户管理、消费交易和清分对账等功能。**二是应用在部、省级间的交易通信中**，省级业务系统发起访问请求后网关首先会拦截访问请求，而后客户端和网关间进行多次“握手”，客户端对服务端进行认证通过后，建立 SSL 安全通道，服务端应用网关的 SSL 服务进行数据加密，最终部级业务系统与省级业务系统互相验证双方数字证书，实现系统设备实体身份的真实性验证。**三是应用在证书认证系统中**，当用户到 RA 中心申请证书时，USBKEY 会生成签名密钥对并产生 CSR，RA 向 CA 提交用户信息和 CSR 后，CA 中心会请求加密秘钥并提交用户签名公钥请求。证书认证系统采用多级部署架构（顶层为离线部署根 CA，二级为交通运输行业运营 CA），主要为交通

运输行业各类应用提供统一的基础认证服务，包括数字证书申请、签发、发布、更新、冻结、解冻、恢复、归档等全生命周期的管理。商用密码在智慧交通中的应用视图如图 7 所示。

随着交通信息化、便捷化的不断推进，精准感知、精确分析、精心服务的交通功能体系和网络安全体系将被打造。在建设交通运输领域新型基础设施过程中，ETC、城市交通一卡通、电子证照等系统将与商用密码技术不断融合，商用密码应用在交通运输领域正在迎来前所未有的发展机遇。

图 7　商用密码在智慧交通领域的应用视图[17]

（六）电子政务领域

2020 年 2 月 1 日，国务院发布的《国家政务信息化项目建设管理办法》开始实施，该办法规定，国家政务信息化项目在规划和审批管理中，要对密码应用方案和密码应用安全性评估报告等内容进行备案；在项目建设中，要同步规划、同步建设、同步

[17] 该图出自中国软件评测中心网络空间安全测评工程技术中心。

运行密码保障系统并定期进行评估。监督管理国家政务信息化项目时，要按照要求采用密码技术，并定期开展密码应用安全性评估，确保政务信息系统运行安全和政务信息资源共享交换的数据安全。《数字中国发展报告（2020 年）》统计数据显示，截至 2020 年 11 月底，我国有 23 个省级和 31 个重点城市地方政府明确了政务数据统筹管理机构，有力推进本地数字政府建设。

目前全国各省政府机构已不断开展电子政务系统建设，并促进商用密码的全面应用。如何判断信息交换双方的身份真实性、如何保护数据传输过程中的安全性是发展电子政务过程中亟需解决的两个重要问题。

政务外网在这两方面基于商用密码技术与密码产品已经完成了诸多安全性改造。比如政务外网公共安全基础支撑方面，基于 PKI 技术的电子认证，对网络上传输的数据进行加密、解密、数字签名和数字认证，保证网上传递数据的真实性、完整性、机密性；采用 SM9 算法和数字签名、数据加密技术实现强身份认证机制和邮件内容加密，全方位保障邮件安全。政务 CA 自 2007 年建设，目前已基本覆盖全国各省、自治区和直辖市，除此之外，部分省市还部署有地方 CA 系统，以保障身份认证安全、数据传输安全、抗抵赖等问题。经过技术发展，政务外网中支持商用密码算法的密钥管理中心基础设施已被改造升级；政务 CA 的密码算法也已被改造。目前，政务 CA 支持 SM2 等密码算法，并已协调部分业务应用完成了算法升级工作，如广东省已在 2012 年建成政务外网密钥管理中心，形成了自主可控的密码认证体系

[18]。在政务外网接入移动办公系统中，也同样使用了商用密码技术与产品进行人员的安全认证和传输通道的安全防护，为政务外网的扩展和移动业务提供了安全保障。

随着云计算技术的发展，政务外网上云成为越来越多政府部门的选择，由于政务外网云平台、各接入网络、业务应用等都需要使用身份认证、权限管理、访问控制、加解密等安全的密码服务，因此在政务云的建设和使用以及政务信息资源整合共享过程中，商用密码产品和技术将进一步发挥更加重要的作用。商用密码在电子政务中的应用视图如图 8 所示。

图 8　商用密码在电子政务领域的应用视图[19]

（七）金融领域

根据《2020-2021 年金融行业网络安全研究报告》的调查结果，当前我国已经有 86%的金融企业具备安全团队或设置安全职

[18] 崔玉华，陈月华，唐鸣：《商用密码在政务外网的应用思考》，载《信息安全与通信机密》2018 年第 5 期，第 35-42 页。

[19] 该图出自中国软件评测中心网络空间安全测评工程技术中心。

能岗位，其中23%的企业还设立了专门的网络安全管理部门，数据表明金融行业高度重视网络安全防范。2018 年 7 月，中共中央办公厅及国务院办公厅印发《金融和重要领域密码应用与创新发展工作规划（2018-2022）》，规划中指出金融领域在密码应用方面的主要任务，包括持续深化金融领域密码应用，加强基础设施网络密码应用，促进密码与数字经济融合应用，推进信息惠民密码应用，增强密码科技创新和基础支撑能力。商用密码在金融领域的应用主要体现在银行业务、保险业务和证券业务中。

对于银行业务而言，采用商用密码技术可以提高金融业信息系统中关键节点的安全性，降低核心业务、客户服务渠道、中心节点等关键部分在面对威胁时的风险，比如金融 IC 卡、动态令牌、智能密码钥匙等密码产品的使用能够实现对客户身份、服务器身份等的认证；使用密码技术，能够加密保护系统存储的用户口令、用户隐私、重要交易数据等信息，确保信息系统机密性的实现。

对于保险业务和证券业务而言，采用商用密码技术的电子保单能够确保网络保险业务开展过程中各类电子单证的合法性，并且通过网上出单，既降低了保险企业的营运费用，又提高了保险公司的营销效率；采用基于商用密码的数字签名技术，能够有效解决网上业务的法律效力问题，提高证券业务的办理效率。

五、商用密码应用中存在的问题

国家正在大力推进密码工作，普及密码技术的应用，但是我

国的商用密码应用仍有极大的发展空间。虽然当前正在积极开展网络安全产品的研发工作，但是还未形成大规模的商品市场，与信息化高速发展的实际需求仍存在差距，商用密码在应用的过程中还存在一些问题[20]。

（一）商用密码应用领域不够广泛

目前，我国整体网络安全防护能力较为脆弱，网络安全投入比重较低，占整个 IT 产业的比重为 1%~2%，远低于西方国家 10%的平均水平[21]，系统防御体系尚未建立或不完善的情况是常态。随着云计算、物联网、大数据、人工智能等新业态的出现，密码技术的应用成为保障系统安全不可缺少的手段，但是就目前来看，密码应用范围和程度还不够广泛和深入。网络和信息系统中商用密码的应用比重较低，大量网络数据并没有得到密码技术的安全防护，即使使用了密码技术，也往往没有被正确、合规、有效地使用。因此，很多数据处在缺失密码技术保护的状态，网络和信息系统由此产生了巨大的安全隐患。

（二）商用密码应用方式不够规范

重信息化建设、轻信息系统网络安全保护是当前业内的常态。虽然近年来国家层面、地方层面和各行业都相继出台了关于商用密码应用的相关要求，但是实施效果并不理想，主要体现在两方面，一方面，一些规定和制度在部分地区和部门并未得到有效落

[20] 霍炜，郭启全，马原：《商用密码应用与安全性评估》，北京：电子工业出版社，2020 年版，第 100 页。

[21] 霍炜，郭启全，马原：《商用密码应用与安全性评估》，北京：电子工业出版社，2020 年版，第 97 页。

地实施，依然有大量信息系统运营者或开发者不能按要求合规、正确地执行密码标准和应用密码技术。另一方面，系统运营者或开发者缺乏密码应用技能和经验、不清楚合规性要求、不了解密码算法和关键参数的类型、错误调用密码技术。密码的不规范使用，会造成信息系统不可避免地产生安全漏洞，从而为信息系统带来极大的安全风险。

（三）商用密码应用服务不够安全

现有大量系统依旧在使用有风险的密码算法，以及有风险的密码算法提供的不安全密码服务，比如容易被破解的 MD4、MD5、SHA-0、SHA-1、RSA-512、RSA-1024、DES、SKIPJACK、RC2 等密码算法，这些算法均已被警示过是有风险的密码算法。信息系统运营者和开发者为节省资源或成本，在开发工作中有意忽视密码技术，或者规避使用密码产品，那么此类系统中信息的机密性、真实性、完整性和不可否认性等安全特性必然会缺乏相应密码算法、协议的支撑，从而致使整个信息系统缺乏安全保障。

（四）商用密码应用需求难以契合

在国家政策的引导与支持下，工业互联网、物联网、车联网、移动互联网、大数据、云计算、区块链等新业态正在崛起，而不同的应用场景对应着不同的商用密码技术需求，不同行业对密码技术的性能也有着不同的要求。但是商用密码在这些场景中的应用需求难以和密码产业发展步伐相契合。一些新业态的密码产品和密码服务往往会要求高性能的密码技术做支撑，而当前的密码算法较为低效，很难与新业态对密码性能的高要求相匹配，因此容易导致商用密码产品或服务难以匹配到行业应用中，从而制约

新业态信息系统得到及时、有效的安全保护。

六、商用密码应用问题原因分析

（一）商用密码管理体制仍需健全

不同行业的信息系统对密码技术的性能要求、商用密码应用场景、手段和管理方法等都不尽相同，因此面向不同行业的商用密码应用指导性文件有待加速出台。网络安全新形势下的商用密码产品还处于起步阶段，网络运营者尚在规则换挡的磨合适应期，相关规则的解释和执行需要结合实际应用情况及时调整。另外，由于前期非涉密单位的网络运营者并无明确强制性的密码应用安全要求，网络运营者面对陆续出台的密码管理规定，可能会面临管理、技术、成本等各方面的磨合适应问题，这在一定程度上制约了商用密码的应用发展。

（二）商用密码标准体系尚待完善

我国虽然在密码标准化工作中取得积极进展，并已发布系列密码算法，但密码应用方面可以起到指导性作用的标准依然需要加快制定出台，标准支撑体系尚待完善。随着工业互联网、移动互联网、物联网、云计算等新业态的快速发展，适用于这些新兴行业和重点领域密码应用标准的缺失将成为阻碍行业发展、阻碍数据互联互通的障碍。现行密码标准与关键信息基础设施、重点行业的密码应用要求难以契合，商用密码标准化推进难度大，由此直接或间接导致了商用密码未能规范应用。

（三）商用密码产业支撑力量不足

伴随着商用密码的推广普及，我国的商用密码产品供给体系已经初步建立，但是仍然存在产业支撑力量不足的问题。一方面，商用密码供应端能力不能充分与设备和应用系统需求端要求相耦合。密码设备生产商决定着密码算法的选择和产品的实现方式，目前的算法往往以内嵌的形式固化于主流设备系统中，缺失选择密码算法的灵活性，这就会造成行业对密码产品的高性能或多性能需求与设备生产商生产的低性能或单一性能的密码产品不匹配的后果。另一方面，当前还存在密码产业缺乏协同、供应链上下游缺少凝聚力的问题，有较强影响力的权威行业协会或产业联盟等组织没有突显出推动商用密码产业发展的带头示范作用。

（四）商用密码技术缺乏自主可控

国家网络安全自主可控的核心和关键在于具备先进的密码技术，实现核心技术自主可控。然而我国互联网信息技术的发展过程中，长期以来在某些领域（芯片、操作系统等）中依赖西方发达国家技术体系，直至当前，我国信息化建设中的“信息孤岛”问题也未能得到妥善解决。一方面，我国研究密码算法的基础薄弱，研究密码技术起步较晚，和发达国家在密码行业的发展相比还存在一定差距，类似于密码芯片等关键硬件产品或技术长期以来受制于西方国家的垄断。另一方面，专业的密码技术人才缺乏，企业对商用密码技术了解不够，这在很大程度上阻碍了企业根据密码应用需求来规划密码研发方案的进程，难以实现高性能密码技术或产品的自给自足。因此，加强密码技术研究，大力开发先进密码算法是网络强国建设的迫切需求。

七、商用密码应用安全性评估概述

（一）密评开展背景

为发挥密码在维护安全与促进发展综合平衡中的重要支撑作用，国家密码管理局印发《商用密码应用安全性评估管理办法（试行）》。该办法将进一步明确国家和省（部）密码管理部门在商用密码应用安全性评估中的指导、监督和检查职责；明确重要信息系统的建设、使用、管理单位在评估工作中的主体责任；依法培育测评机构，规范评估行为，形成规范有序的商用密码应用安全性评估审查机制，并与网络安全等级保护、关键信息基础设施安全检测评估等已有制度做好衔接。

商用密码应用安全性评估是保障密码应用合规、正确、有效的重要手段，它使密码应用管理过程构成闭环，促进密码应用管理体系不断完善，并能够持续改进密码在网络和信息系统中应用的安全性，保障密码应用动态安全，为信息系统的安全提供坚实的基础支撑[22]。

（二）密评发展历程

商用密码应用安全性评估最早于 2007 年提出，经过十余年的积累，密评制度体系正在不断地成熟。我国密评发展经历了四个阶段[23]。

[22] 张智军，薛子育，沈阳：《探讨广播电视商用密码应用安全性测评》，载《信息安全》2019 年 8 月刊，第 70-73 页。

[23] 霍炜，郭启全，马原：《商用密码应用与安全性评估》，北京：电子工业出版社，2020 年版，第 119 页。

第一阶段，制度奠基期（2007 年 11 月至 2016 年 8 月）。2007 年 11 月 27 日，国家密码管理局印发 11 号文件《信息安全等级保护商用密码管理办法》，要求信息安全等级保护商用密码测评工作由国家密码管理局指定的测评机构承担。2009 年 12 月 15 日，国家密码管理局印发管理办法实施意见，进一步明确了与密码测评有关的要求。

第二阶段，再次集结期（2016 年 9 月至 2017 年 4 月）。国家密码管理局成立起草小组，研究起草《商用密码应用安全性评估管理办法（试行）》。2017 年 4 月 22 日，正式印发《关于开展密码应用安全性评估试点工作的通知》（国密局（2017）138 号文），在七省五行业开展密评试点。

第三阶段，体系建设期（2017 年 5 月至 2017 年 9 月）。国家密码管理局成立密评领导小组，研究确定了密评体系总体架构，并组织有关单位起草 14 项制度文件。经征求试点地区、部门意见和专家评审，2017 年 9 月 27 日，国家密码管理局印发《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）》《信息系统密码应用基本要求》（2018 年以密码行业标准 GM/T 0054-2018 形式发布）和《信息系统密码测评要求（试行）》，国标密评制度体系初步建立。

第四阶段，密评试点开展期（2017 年 10 月至今）。试点开展过程同时也是机构培育过程，包括机构申报遴选、考察认定、发布目录、开展试点测评工作、提升测评机构能力、总结试点经验、完善相关规定等。2021 年 3 月 8 日，在对密码行业标准 GM/T

0054-2018 进一步修改完善后，密码国家标准 GB/T 39786-2021《信息安全技术信息系统密码应用基本要求》正式发布，并于 2021 年 10 月 1 日正式实施。

（三）密评总体流程

密评工作包括四项基本测评活动，即测评准备活动、方案编制活动、现场测评活动、分析与报告编制活动。测评方与受测方之间的沟通与洽谈应贯穿整个测评过程。商用密码应用安全性评估过程框架见图 9 所示。需要注意的是，在测评活动开展之前，信息系统的密码应用方案需要通过测评机构的评估或者密码应用专家的评审，按要求通过评估或评审的密码应用方案可以作为密评实施的依据。密码应用方案评审主要审查是否涵盖了所有需要采用密码保护的核心资产及敏感信息，以及采取的密码保护措施是否能够达到相应等级的使用要求。

测评准备活动是开展测评工作的前提和基础，主要任务是掌握被测信息系统的详细情况，准备测评工具，为编制测评方案做好准备。

方案编制活动是开展测评工作的关键，主要任务是确定与被测信息系统相适应的测评对象、测评指标及测评内容等，形成测评方案，为实施现场测评提供依据。

现场测评活动是开展测评工作的核心，主要任务是依据测评方案的总体要求，分步实施所有测评项目，包括单项测评和单元测评等，以了解系统的真实保护情况，获取足够证据，发现系统存在的密码应用安全性问题。

分析与报告编制是给出测评工作结果的活动，主要任务是根

据现场测评结果和《信息系统密码应用基本要求》《信息系统密码测评要求》的有关要求，通过单项测评结果判定、单元测评结果判定、整体测评和风险分析等方法，找出整个系统密码的安全保护现状与相应等级的保护要求之间的差距，并分析这些差距可能导致的被测信息系统面临的风险，从而给出测评结论，形成测评报告。

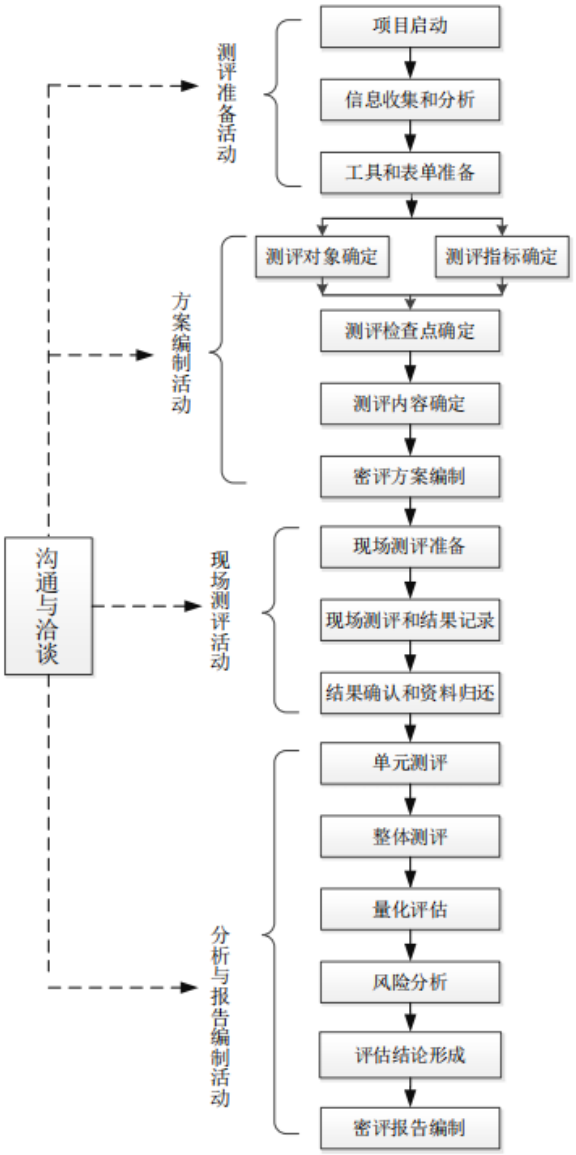

图 9　商用密码应用安全性评估总体流程[24]

[24] 引用于《信息系统密码应用测评过程指南》第 3 页“图 1 测评过程工作流程图”。

（四）密评必要性

商用密码应用安全性评估是指在采用商用密码技术、产品和服务集成建设的网络和信息系统中，对其密码应用的合规性、正确性和有效性进行评估。商用密码应用安全性评估是商用密码检测认证体系的重要组成部分。维护网络空间安全、规范商用密码应用是密评工作开展的客观要求，开展密评是加强密码工作监管的重要举措，也是重要领域信息系统运营主管部门必须要履行的法定义务[25]。

1. 开展密评是保障系统安全的必然要求

密码技术是保障网络与信息系统安全的重要抓手，构建起成体系的、安全有效的密码保障系统，对重要信息系统有效抵御网络攻击具有重要作用。商用密码应用的合规性、正确性和有效性测评，涉及到密码算法、产品、协议、技术体系、密钥管理等多个方面。因此，企业有必要委托专业机构的专业技术人员，运用专业的测评工具和技术手段，对网络和信息系统整体的商用密码应用安全进行专项测试和综合评估，并根据测评结果编制出科学准确的评估报告，以便网络和信息系统运营者或主管部门及时掌握商用密码的安全状况，并采取必要的技术手段和管理措施对密码应用方案及时进行调整和改进。

2. 开展密评是相关责任主体的法定职责

开展密评是相关责任主体依法履行网络安全、数据安全保障

[25] 霍炜，郭启全，马原：《商用密码应用与安全性评估》，北京：电子工业出版社，2020 年版，第 100-101 页。

职责的措施。《中华人民共和国密码法》中明确指出“法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估”“商用密码从业单位开展商用密码活动，应当符合有关法律、行政法规、商用密码强制性国家标准以及该从业单位公开标准的技术要求”。

《商用密码管理条例（修订草案征求意见稿）》第六章内容提到“非涉密的关键信息基础设施、网络安全等级保护第三级以上网络、国家政务信息系统等网络与信息系统，其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，自行或者委托商用密码检测机构开展商用密码应用安全性评估”。

《网络安全等级保护条例》和《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》的内容同样强调了密码应用要求，突出强调网络安全等级保护第三级及以上系统应当注重强化密码应用监管工作，应当正确、有效采用密码技术进行保护，并使用符合相关要求的密码产品和服务，必须认真落实密码应用安全性评估制度。因此，对网络安全等级保护在第三级及以上等级的信息系统和关键信息基础设施开展密评工作，是网络运营者或主管部门需要承担的法定责任。

3. 开展密评是建设网络强国的重要保障

《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》中指出要推进网络强国建设，营造良好数字生态，健全国家网络安全法律法规和制度标准，加强重要

领域数据资源、重要网络和信息系统安全保障。而应用商用密码产品并进行安全性评估有利于建立健全关键信息基础设施保护体系，提升数字化应用场景中的网络安全防护能力，提升网络安全产业综合竞争力。

密评体系针对信息系统从而系统性地发现自身的密码应用不足，其为重要领域网络和信息系统的安全提供了科学评价方法。逐步规范商用密码的使用和管理，坚持做好以评促建、以评促改、以评促用工作，确保商用密码在网络和信息系统中正确、有效地使用，建立完善密评体系，切实构建起坚实可靠的网络空间安全密码屏障。

八、商用密码应用安全性评估内容要求

（一）密评要点

集中采用商用密码产品、技术、服务而建成的网络和信息系统是商用密码应用安全性评估的评估对象，密评要点涵盖了密码应用安全的三个方面，分别是合规性、正确性、有效性。

一是商用密码应用合规性评估。主要指判定网络和信息系统使用的密码算法、密码协议、密钥管理是否符合法律法规的规定和密码相关国家标准、行业标准的有关要求。网络和信息系统使用的密码产品和密码服务是否经过国家密码管理部门核准或由具备资格的机构认证合格。

二是商用密码应用正确性评估。主要指判定密码算法、密码协议、密钥管理、密码产品和密码服务是否使用正确，即系统中

采用的标准密码算法、协议和密钥管理机制是否按照相应的国家和行业密码标准进行正确的设计和实现；自定义密码协议、密钥管理机制的设计和实现是否正确，安全性是否满足要求，密码保障系统建设或改造过程中密码产品和服务的部署和应用是否正确。

三是商用密码应用有效性评估。主要指判定网络和信息系统中的密码保障系统是否在网络和信息系统运行过程中发挥了实际效用，是否满足了信息系统的安全需求，是否切实解决了信息系统面临的安全问题。

（二）通用测评要求

1. 算法和技术合规性测评

GB/T 39786-2021《信息系统密码应用基本要求》是密评工作的总体要求，密码系统中涉及到的密码算法、密码技术、密码产品、密码服务等都需要满足总体要求中的规定。在进行密评工作时，测评人员需要对密码算法实现、密码技术实现、密码产品、密码服务进行测评。

在进行密码算法实现的测评时，测评人员应当首先了解信息系统使用的算法名称、用途、位置、执行算法的设备及其实现方式（软件、硬件或固件等）。针对信息系统使用的每个密码算法，测评人员应当核查密码算法是否以国家标准或行业标准形式发布，或是否取得国家密码管理部门同意其使用的证明文件，信息系统中使用的密码算法应符合法律、法规的规定和相关国家标准、行业标准的有关要求。

在进行密码技术实现的测评时，测评人员应当基于密码算法

核查，进一步核查密码协议、密钥管理等密码技术是否符合相关国家、行业标准的有关要求。需要注意的是，若密码技术由已经获得审批或检测认证合格的商用密码产品实现，即意味着其内部实现的密码技术已经符合相关标准，在测评过程中，测评人员应当重点评估这些密码技术的使用是否符合标准规定。例如，《信息系统密码应用基本要求》等标准规定了使用证书或公钥之前应对其进行验证，因此，在使用数字证书之前应当按照验证策略对证书的有效性和真实性进行验证。

在进行密码产品测评时，信息系统中使用的密码产品应符合法律法规的相关要求，测评人员应首先确认，所有实现密码算法、密码协议或密钥管理的部件或设备是否获得了国家密码管理部门颁发的商用密码产品认证证书，或国家密码管理部门认可的商用密码检测机构出具的合格检测报告。已满足上述要求的密码产品，证明该产品标准符合性和安全性已经通过了检测。在测评过程中，测评人员应当重点评估这些密码产品是否被正确、有效使用。一种常见的情况是，采用了已审批过或检测认证合格的产品，但使用了未经认可的密码算法或密码协议，针对这种情况的测评，可与密码算法核查和密码技术核查一并进行。另一种更复杂的情况是，密码产品被错误使用、配置，实际并没有发挥预期作用，此时需要测评人员通过配置检查、工具检测等方式进行综合判定。

在进行密码服务测评时，信息系统中使用的密码服务应符合法律法规的相关要求，采用的密码服务需要依法接受检测认证的，应经商用密码认证机构认证合格。如果信息系统使用了第三方提供的电子认证服务等密码服务，测评人员应当核查信息系统所采

用的相关密码服务是否获得了国家密码管理部门或商用密码认证机构颁发的相应证书，如《电子认证服务使用密码许可证》，且证书是否在有效期内。

2. 密钥管理安全性测评

密钥管理是指根据安全策略，对密钥的产生、分发、存储、更新、归档、撤销、备份、恢复、销毁等密钥全生命周期的管理。根据《信息系统密码应用测评要求》中的规定，在实施测评时，测评人员需要核查信息系统密钥体系中的密钥（除公钥外）是否不能被非授权的访问、使用、泄露、修改和替换，公钥是否不能被非授权的修改和替换；了解密码产品的型号和版本等配置信息，核查密码产品是否经检测认证合格，属于GB/T 37092《信息安全技术密码模块安全要求》相应密码模块安全等级；核查密码产品的使用是否满足其安全运行的前提条件，如其安全策略或使用手册说明的部署条件。

与此同时，测评人员还应当核查信息系统中用于密钥管理和密码计算的密码产品和密码服务是否符合法律法规的相关要求，需要依法接受检测认证的，核查是否经商用密码认证机构认证合格。

（三）单元测评要求

密码应用安全测评所涵盖的测评单元包括物理和环境安全测试、网络和通信安全测试、设备和计算安全测试、应用和数据安全测试，涉及的测评指标体系详见表5所示。密码安全功能测评贯穿了单元测评的始终，密码安全功能的维度体系包括机密性、完整性、真实性、不可否认性四个方面，密码基本安全目标的实

现与否可以通过测评密码的应用情况进行检验。

对机密性实现的测评，可以利用协议分析工具或读取存储的重要数据，分析和判断传输或存储的重要数据、密钥数据、身份鉴别信息是否为密文，数据格式(如分组长度等)是否符合预期。

对完整性实现的测评，可以利用协议分析工具或读取存储的重要数据，分析和判断受完整性保护的数据在传输或存储时的数据格式（如签名长度、MAC 长度）是否符合预期；如果是使用数字签名技术进行完整性保护的，测评人员可以使用公钥对抓取或存储的签名结果进行验证。条件允许的情况下，测评人员可尝试对存储数据进行篡改（如修改 MAC 或数字签名），验证完整性保护措施的有效性。

对真实性实现的测评，如果身份鉴别未使用证书，测评人员要验证公钥或密钥与实体的绑定方式是否可靠，实际部署过程是否安全。对于不能复用密码产品检测结果的，要查看实体鉴别协议是否符合 GB/T 15843 中的要求，特别是对于“挑战一响应”方式的鉴别协议，可以通过协议抓包分析，验证每次挑战值是否不同；对于基于静态口令的鉴别过程，抓取鉴别过程的数据包，确认鉴别信息（如口令）未以明文形式传输；对于采用数字签名的鉴别过程，抓取鉴别过程的挑战值和签名结果，使用对应公钥验证签名结果的有效性。

对不可否认性实现的测评，可以使用相应的公钥对作为不可否认性证据的签名结果进行验签，如果使用第三方电子认证服务，则应对密码服务进行核查。

表 5：密码技术应用测评指标体系

单元测评内容	测评指标
物理和环境安全测评	身份鉴别
	电子门禁记录数据存储完整性
	视频监控记录数据存储完整性
	密码服务
	密码产品
网络和通信安全测评	身份鉴别
	通信数据完整性
	通信过程中重要数据的机密性
	网络边界访问控制信息的完整性
	安全接入认证（第三级到第四级信息系统适用）
	密码服务
	密码产品
设备和计算安全测评	身份鉴别
	远程管理通道安全
	系统资源访问控制信息完整性
	重要信息资源安全标记完整性
	日志记录完整性
	重要可执行程序完整性、重要可执行程序来源真实性
	密码服务
	密码产品
应用和数据安全测评	身份鉴别
	访问控制信息完整性
	重要信息资源安全标记完整性
	重要数据传输机密性
	重要数据存储机密性
	重要数据传输完整性
	重要数据存储完整性
	不可否认性
	密码服务
	密码产品

商用密码安全管理测评涉及到的测评内容包括制度管理测评、人员管理测评、建设运行测评、应急处置测评四个方面，各项测评内容的测评指标体系详情如表 6 所示。

表 6：安全管理测评指标体系

单元测评内容	测评指标
管理制度测评	具备密码应用安全管理制度
	密钥管理规则
	建立操作规程
	定期修订安全管理制度
	明确管理制度发布流程
	制度执行过程记录留存
人员管理	了解并遵守密码相关法律法规和密码管理制度
	建立密码应用岗位责任制度
	建立上岗人员培训制度
	定期进行安全岗位人员考核
	建立关键岗位人员保密制度和调离制度
建设运行	制定密码应用方案
	制定密钥安全管理策略
	制定实施方案
	投入运行前进行密码应用安全性评估
	定期开展密码应用安全性评估及攻防对抗演习
应急处置	应急策略
	事件处置
	向有关主管部门上报处置情况

（四）整体测评要求

整体测评应该从单元间和层面间两个方面进行测评和综合安全分析。

1. 单元间测评

单元间测评是指对同一安全层面内的两个或者两个以上不同测评单元间的关联进行测评分析，其目的是确定这些关联对信息系统整体密码应用防护能力的影响。在单元测评完成后，如果信息系统的某个测评单元的结果判定存在不符合或部分符合，应进行单元间测评，重点分析信息系统中是否存在单元间的相互弥补作用。

根据测评分析结果，综合判定该测评单元所对应的信息系统密码应用防护能力是否缺失，如果经过综合分析单元测评中的不符合项或部分符合项不造成信息系统整体密码应用防护能力的缺失，则对该测评单元的测评结果予以调整。

2. 层面间测评

层面间测评是指对不同安全层面之间的两个或者两个以上不同测评单元间的关联进行测评分析，其目的是确定这些关联对信息系统整体密码应用防护能力的影响。在单元测评完成后，如果信息系统的某个测评单元的结果判定存在不符合或部分符合，应进行层面间测评，重点分析信息系统中是否存在层面间的相互弥补作用。

根据测评分析结果，综合判定该测评单元所对应的信息系统密码应用防护能力是否缺失，如果经过综合分析单元测评中的不符合项或部分符合项不造成信息系统整体密码应用防护能力的缺失，则对该测评单元的测评结果予以调整。

（五）风险分析和评价

在进行整体测评过程中，部分单项测评结果可能会有变化，需进一步对单项和单元测评结果进行修正。修正完成之后，测评人员还应根据被测信息系统所承载的业务、部署环境以及与其他系统的连接等情况，综合分析判断信息系统密码应用安全可能面临的外在安全风险。针对单元测评结果中存在的不符合项或部分符合项，分析所产生的安全问题被威胁利用的可能性，判断信息系统密码应用在合规性、正确性和有效性方面的不符合所产生的安全问题被威胁利用后对信息系统造成影

响的程度，以及受到威胁利用的资产自身价值。通过渗透测试、逆向分析等手段对信息系统存在的安全风险进行有效验证，综合评价测评结果的不符合项或部分符合项对信息系统造成的安全风险，并对安全风险进行有效验证和分析，从而形成最终的被测信息系统密码应用安全性评估结论。

对于高风险的判定依据和评估量化细则，可参考标准《信息系统密码应用高风险判定指引》和《商用密码应用安全性评估量化评估规则》，并且对于未满足密码应用的正确性、有效性或未使用经国家密码管理部门核准的密码技术且存在明显安全风险等措施，应结合具体业务场景做出高风险判定。

九、商用密码应用管理建议

针对我国商用密码应用当前存在的系列问题，为保障网络空间安全、规范商用密码的应用和管理，在健全密码管理机制、完善标准支撑体系、优化密码产业生态环境、提升密码技术自主可控能力以及培养密码人才等方面提出了建议[26]。

（一）建立健全商用密码管理机制

为了保证《中华人民共和国密码法》能够有效落地实施，加大商用密码应用推广力度，各行业领域应当**贯彻落实国家密码相关的工作方针，协助国家密码管理部门和县级以上地方各级密码管理部门共同做好各行业、各地区商用密码的应用和管理工作**。

[26] 王榕，谢玮，曹珩，路鹏：《我国商用密码管理现状与发展对策建议》，载《信息安全与通信机密》2020 年第 3 期，第 83-89 页。

2021 年 7 月 30 日，国务院公布《关键信息基础设施安全保护条例》，因此，为保障我国关键信息基础设施网络安全，建议关键行业和重要领域加快制定、修订行业、领域内商用密码应用规范及商用密码应用管理要求。建议政、产、学、研、用等全链条参与者协力研究出台《中华人民共和国密码法》《商用密码管理条例》的配套文件，实现《中华人民共和国密码法》与《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》《网络安全等级保护条例》等法律法规之间的相互衔接，加快构建以《中华人民共和国密码法》为核心的密码管理法律制度体系，建立健全商用密码管理机制。

（二）持续完善密码标准支撑体系

产业发展，标准先行。密码标准化成果是引领技术和产业发展的支撑力量，在密码工作领域中起到强导向性作用。因此，**一是建议持续完善密码标准体系、检测认证体系**，保证密码标准顶层设计的全面性、科学性、与时俱进性，全面建成科学先进的密码标准体系和检测认证体系，建成完备的密码评估与验证环境。二是建议在 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等标准基础上，**加快制订面向不同行业、不同领域的商用密码应用标准**，尤其要重点关注重要领域和关键行业对密码应用的安全需求，从整体上提升各行业对规范应用密码标准的重视程度，以期实现不同行业系统间数据的互联互通。在此基础上，做好密码应用标准与网络安全等级保护和关键信息基础设施安全保护之间的衔接，以此为全行业网络运营者、信息系统规划开发者提供标准依据，规范建设网络系统，保障网络安全。**三是高**

度重视标准化成果要与国际接轨，实现我国自主研发的商用密码算法与国际密码算法的互联互通。我国自主研发的商用密码算法的国际标准化进程应当持续积极推进，从而尽早打破西方的技术壁垒，增强我国密码产业的国际竞争力。

（三）优化商用密码产业生态环境

一是优化商用密码产业生态环境，营造供应链和产业链优势互补、合作创新的局面。电信和互联网、交通、金融等重点行业企业、新兴融合领域企业应加大商用密码投入，有较强影响力的权威行业协会或产业联盟在重大工程或重大专项中应该起到积极带头作用，以此激发供应链上下游的凝聚力与协作力，进而推动商用密码产业发展。**二是推进产融合作试点城市的商用密码应用力度，**深化商用密码产融合作，积极倡导国家有关部门、各地政府、测评机构、商用密码产品生产商、科研院所以及高校等不同社会分工部门统筹利用政、产、学、研、用等各类资源，突破原有的界限壁垒，实现商用密码协同创新，确保密码保障系统同步规划、同步建设、同步运行。**三是推动建立符合商用密码产业特征的密码应用安全性评价体系，**支持开展高成长企业、高价值项目评估，协同做好信息共享和密评成果转换工作。

（四）提升密码技术自主创新能力

一是积极开展密码技术创新、加强密码核心技术攻关、促进商用密码技术成果转化，扭转当前面临的密码核心技术受制于人的被动局面。**二是重视高性能密码技术和产品的研发，**随着网络安全风险日渐增多，全行业对高性能密码产品的刚性需求渐增，而密码产品的高性能体现在对主动安全的解决上。通过采用数据

加密、消息认证和数字签名等密码技术，可以在不安全的环境下对通信和存储数据加以保护，防止未经授权的访问、篡改、伪造、抵赖等行为，这些都是密码技术高性能的体现。**三是进行密码自主创新产品的推广应用，**可重点推动能源、金融、交通、水利、卫生医疗、教育等关键行业以及工业互联网、物联网、车联网、智慧交通、政务云等重要领域加强设备防护、边界防护、身份认证、数据安全、应用安全等密码技术建设，提升重要系统、关键节点及数据的安全防护能力，尤其是基于密码技术自主创新的安全防护。

（五）着力培养密码行业人才队伍

着力培养密码行业人才队伍，补足商用密码算法研发、产品设计、安全攻防、测评认证等方面的人才缺口。

一是完善密码人才培养机制。积极探索产、学、研协作创新的人才培养模式，推进密码领域的校企合作，支持鼓励高等院校、研究机构与企业共建密码产业实训基地、联合实验室等，打造“双师型”师资队伍，增强密码人才实践能力。发挥密码行业特色高校、职业院校作用，发展更多技能型、服务型的密码人才。

二是加强密码学科建设和人才培养输出。随着网络空间技术飞速发展和密码攻防对抗的内在驱动，密码学科形成了理论、工程和应用相互促进的完整体系，密码已经从军政安全走向社会大众，密码学科设置层级过低、密码人才紧缺现象十分突出。因此要加紧推动实施密码学科建设和人才培养，提升密码学科设置层级，加强密码专业研究生等高端人才学位设置和培养，加强密码职业人才教育和培训，培养一批有深厚理论积淀和专业素养的密

码人才，并通过实训演练等方式进行长期、系统的训练。

十、商用密码发展展望

为适应国家安全环境的深刻变化，落实党的十九大作出的战略部署，贯彻落实总体国家安全观和网络强国战略，发挥密码在构建网络信任体系、提升国家治理能力现代化中的重要作用，商用密码工作需要始终坚持以习近平新时代中国特色社会主义思想指导，进一步推进法治化、科学化、规范化管理，进一步强化自主创新，进一步健全市场体系。站在新的历史起点上，我国商用密码工作定将迎来更加广阔的发展空间[27]。

（一）商用密码将得到广泛应用

工业和信息化部发布的《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中提到“到 2023 年，网络安全产业规模超过 2500 亿元，年复合增长率超过 15%”。密码技术作为国家自主可控的核心技术，在网络安全产业中发挥着越来越重要的作用。随着云计算、物联网、车联网、工业互联网等新业态的蓬勃发展，国家鼓励重点行业企业加大网络安全投入，单独列支网络安全预算，推动了网络安全技术、产品和服务的部署应用。商用密码技术作为不可或缺的重要手段，其行业应用将会得到深入融合与拓展。

（二）密码产业将得到强势发展

[27] 张平武：《商用密码发展历程与展望》，载《中国信息安全》2018 年第 8 期，第 51-53 页。

随着应用需求不断增大，以及打造“多点支撑、辐射全国、优势互补、协同发展”的网络安全产业园区布局，商用密码产业将形成自主可控的完整产业链，产业生态环境将不断得到优化。未来密码市场的内涵将从单一的“国密合规”中呈现出分层次叠加的“实战防护、密评合规、信创合规”的特征，并且也将出现一批具有较大产业规模和市场竞争力的商用密码领军企业。据《2021 密码产业洞察报告（V1.0）》显示，当前我国密码产业的产业规模仅占信息产业的千分之三；同时，《2020-2021 中国商用密码产业发展报告》的统计预测结果显示，预计 2023 年，我国商用密码产业规模将超过 900 亿元。因此，我国商用密码产业还有非常广阔的发展空间，未来几年，密码市场将迎来新发展机遇，商用密码产业必将迎来强势发展期。

（三）标准体系将得到日益完善

《中华人民共和国密码法》的颁布实施以及《商用密码管理条例（修订草案征求意见稿）》的出台，都促使商用密码法律法规体系趋于系统化、完善化，未来对商用密码的管理工作也将走向集中化、统一化。《2021 商用密码创新应用指南》中明确指出“合规需求仍然是目前企业对商用密码技术应用的主要驱动力，统一密管、统一认证等是企业用户重点关注的商用密码应用诉求”。因此，在未来，建设统一标准体系和统一密码平台、实施统一的安全防护和运维管理、打造一体化的密码支撑体系是开展商用密码管理支撑工作的大势所趋，商用密码管理体制将更加科学合理。与此同时，在《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《关

键信息基础设施安全保护条例》等法律条例的持续驱动下，商用密码支撑体系将会得到进一步优化和完善，新的网络安全体系和网络安全文明正在加速形成。

（四）科创能力将得到显著提升

我国商用密码产品的自主研制、生产和推广一直以来都备受国家主管部门重视，尤其在数据作为新的生产要素的新时代下，数据将全面赋能密码的创新发展。在密码技术发展创新方面，将会出现机密计算、差分隐私、同态加密等多种新兴技术，实现数据“可用不可见”；密码应用场景也将会拓展到例如区块链、边缘计算、人工智能等新型信息技术应用场景中去，且有望解决数据生产要素化的信任和安全问题；传统密码技术和多种安全机密技术也将得到融合创新，使数据在业务系统中兼得安全和共享。目前我国自主设计的 SM 系列算法经过多轮安全性分析评估，在设计、实现方面均体现出了独特优势，能够有力支撑商用密码的产业化、规模化发展。总而言之，积极争夺技术制高点并及早推出拥有自主知识产权的高强度密码、芯片及产品，既具有重要的现实意义，又具有广泛的商业前景，在数据要素的激励下，密码技术自主创新能力必会得到显著提升。

（五）密评工作将得到有力推进

《网络安全产业高质量发展三年行动计划（2021-2023 年）（征求意见稿）》中提到，“支持开展网络安全产品服务能力评价、网络安全工程建设与系统运行维护质量评价，和面向新技术、新业务的安全评估”“鼓励地方在财政投资的信息化项目中同步配套建设网络安全技术措施，在项目验收阶段加强对网络安全方

面的评审”。《中华人民共和国数据安全法》同样提到“国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动”。《中华人民共和国密码法》和《网络安全等级保护条例》的出台实施，以及密码产品技术和检测标准规范的发布，使得商用密码应用安全性评估必将在信息系统的网络安全规划、建设、运行中发挥强有力的保障作用。

——正文结束——

注意事项：

- 未经中国软件评测中心同意，不得用于其它商业运作。
- 未经中国软件评测中心书面批准，不得部分复印报告。

- 单位地址： 北京市海淀区紫竹院路 66 号
- 邮政编码： 100048
- 通信地址： 北京市海淀区紫竹院路 66 号赛迪大厦 4 层
- 电子信箱： linqing@cstc.org.cn
- 联系电话： 010-88558326