

2021-2022年中国商用密码行业发展白皮书

赛迪研究院网络安全研究所
赛迪区块链研究院

2022年9月

Part

01

商用密码背景



(一) 商用密码相关概念

根据《中华人民共和国密码法》（以下简称《密码法》）第一章第二条，密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。

商用密码是指商用密码技术、商用密码产品和商用密码服务的总称，主要用于“不涉及国家秘密内容的信息”领域，即非涉密信息领域。

商用密码产业是指采用密码技术，为不涉及国家秘密的信息提供加密保护、安全认证相关技术、产品和服务行业的总称。

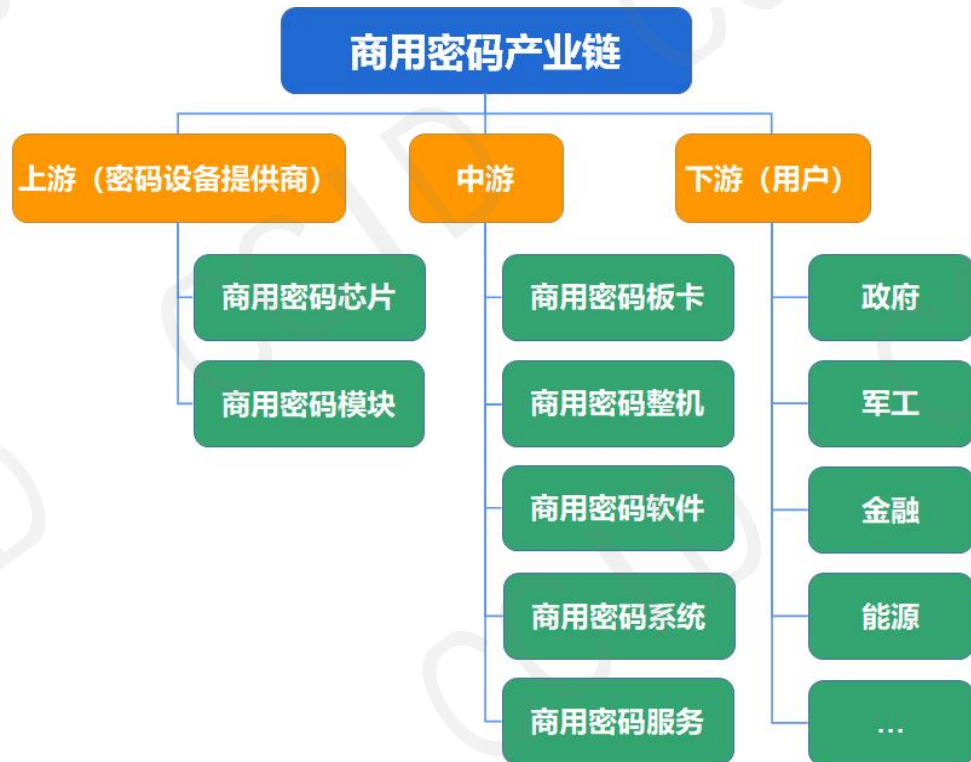


图1-1 商用密码产业链

(二) 密码发展历程



(三) 密码算法体系



图1-2 商用密码算法体系

(四) 商用密码重要意义

1

密码是保障网络与信息系统的基础支撑，密码技术是保护数据安全的有效手段。

2

密码是构建网络可信身份服务体系的重要基石，是实现国家治理体系与治理能力现代化的重要支撑。

3

密码是保护国家利益的战略性资源，是贯彻习近平总书记网络强国战略思想、落实国家网络空间安全战略、保障网络安全与数据安全的核心技术和基础支撑。

Part

02

我国商用密码行业发展现状



(一) 商用密码法律法规体系基本形成

我国现已初步形成了以《网络安全法》《密码法》《数据安全法》为核心组成的新时期国家安全法律制度体系，积极推动密码工作在网络强国、数字中国建设中实现跨域式发展。从《密码法》对商用密码的法定化管理，到《信息安全技术网络安全等级保护基本要求》（即等保2.0）对商用密码的升级化保护，国家在政策法规层面逐步完善现行商用密码管理制度，促进商用密码应用改造，进一步规范商用密码的使用和管理，引导商用密码产业健康有序发展。

(二) 商用密码标准体系基本完善

截至2021年12月底，国家标准化管理委员会已发布现行商用密码国家标准47项，国家密码管理局已发布商用密码行业标准133项，各商密协会、联盟发布现行团体标准37项，覆盖商用密码技术、产品、服务、应用、检测和管理等多个领域，构建了较为齐全完备的商用密码标准体系，充分发挥了商用密码标准在推动产业发展、促进互联互通、助力应用推进、优化管理服务等方面的重要作用。

(三) 商用密码技术产品创新丰富

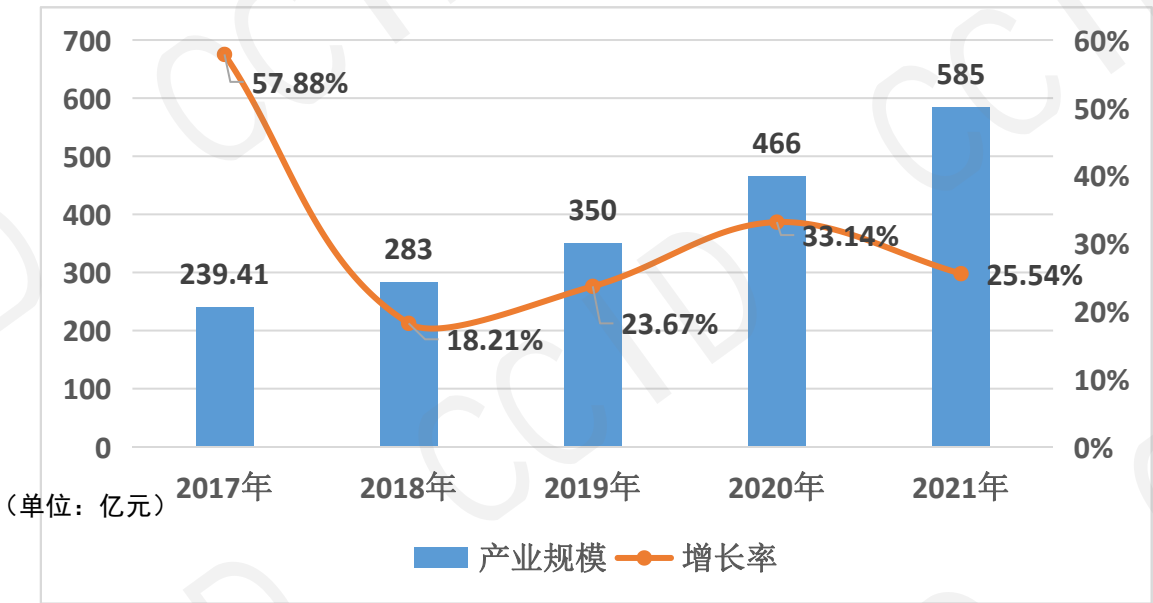
在基础理论研究方面，在国家密码发展基金等国家级科技项目的引导和支持下，我国在序列密码设计、分组密码算法设计与分析、密码杂凑算法分析、密码协议基础理论与分析、抗量子密码等密码基础理论研究方面取得了一系列的创新科研成果。

在密码基础软硬件方面，随着密码及其他信息技术的不断升级完善，各类密码产品和服务也随之迭代丰富，国内商用密码产品、服务自主创新能力持续增强，现已取得142项国家或省部级科技成果，10余项达到国际先进水平。

(四) 商用密码产业初具规模

表2-1 2017年-2021年商用密码产业总体规模及增长率

	2017年	2018年	2019年	2020年	2021年
产业规模 (亿元)	239.41	283	350	466	585
增长率	57.88%	18.21%	23.67%	33.14%	25.54%



近年来我国商用密码产业规模不断扩大，产业规模整体呈上升趋势。2021年我国商用密码产业规模达到585亿元，较2020年增长25.54%。

图2-1 2017-2021年商用密码产业规模变化趋势

(五) 商用密码应用领域基本实现全覆盖

商用密码应用情况

近年来密码应用已拓展到社会生产生活的方方面面，从涉及政府安全的保密通信，到涉及国民经济的金融交易、防伪税控，再到涉及公民权益的电子支付、网上办事等。密码技术渗透到各领域信息系统的业务环节，构建了密码保障体系，从而发挥出信息安全基础支撑作用，并初步实现了商用密码产品与行业场景特点的融合应用。

据统计，国内现有商用密码产品3000余款，品类涵盖了密码芯片、密码板卡、密码模块、密码机、密码系统等全产业链条，形成了完整的商用密码产品供给体系。

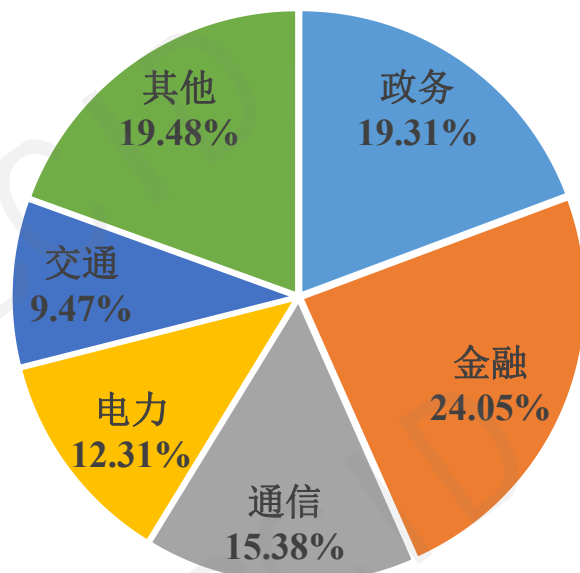


图2-2 商用密码产品应用领域占比

2021年我国商用密码产品应用领域主要分布在金融、政务、通信、电力、交通、教育、医疗、电子商务等领域，应用领域日益丰富。其中商用密码在**金融领域**应用占比24.05%，在**政务领域**应用占比19.31%，在**通信领域**占比15.38%，在**电力领域**占比12.31%，在**交通领域**占比9.47%，在税务、医疗、电子商务等**其他领域**占比共计19.48%。

(六) 商用密码人才队伍逐步壮大

中国科学院大学、中国科学技术大学、北京航空航天大学、北京理工大学、北京邮电大学、北京电子科技学院等高校均开设了密码学课程，并积极推动密码专业学科建设。各地方也积极推动国家密码学科能力建设相关工作。



2021年3月，人力资源社会保障部公告新增“密码技术应用员”职业，相关管理部门协同推动密码技术人员标准编制，为后续密码人才培养奠定坚实基础。

各级密码管理部门、中国密码学会、各地密码行业协会等机构分别组织开展商用密码产业情况、技术创新趋势与标准解读、商用密码应用安全性评估等相关培训工作，持续强化专业密码人才储备。

Part

03

我国商用密码行业发展主要问题



1

产业政策环境需进一步改善

- 商用密码法律法规配套文件尚未齐全
- 商用密码管理体制仍需改革
- 密码检测和评估机制有待完善

2

商用密码行业实力需进一步提升

- 产业规模仍需扩大
- 产品结构仍需改善
- 大型企业数量较少
- 行业组织缺乏协同

3

商用密码技术创新需进一步加强

- 现有商用密码产品难以满足新技术新应用对产品性能的要求
- 商用密码应用环境和适配性受限
- 密码技术理论基础研究有待加强

4

商用密码专业人才严重缺乏

- 密码人才培养顶层设计不完善
- 部分密码从业人员专业性不足

5

商用密码应用生态需加快完善

- 缺乏有效产业支撑平台
- 行业组织之间缺乏协同
- 密码安全保障需求不足

Part

04

我国商用密码重点法规分析



我国商用密码重点法规分析

近年来，国家高度重视密码相关工作，以密码为核心的法律法规体系逐步完善。截止到2021年12月，我国已发布密码相关领域的法律法规共7项，形成了以《密码法》为核心的商用密码法制体系，旨在强调密码在维护国家安全、促进经济社会发展、保护人民群众利益方面的重要作用，对我国商用密码行业进行规范，引导我国商用密码产业合理合规发展。

表4-1 我国商用密码相关法律法规

序号	名称	实施日期
1	《中华人民共和国网络安全法》	2017/06/01
2	《中华人民共和国电子签名法（修正案）》	2019/04/23
3	《中华人民共和国密码法》	2020/01/01
4	《国家政务信息化项目建设管理办法》	2020/02/01
5	《关键信息基础设施安全保护条例》	2021/09/01
6	《中华人民共和国数据安全法》	2021/09/01
7	《中华人民共和国个人信息保护法》	2021/11/01

Part

05

我国商用密码重点政策分析



我国商用密码重点政策分析

各部委相关政策

国家密码管理局先后出台了《商用密码应用安全性评估管理办法（试行）》和《商用密码管理条例（修订草案征求意见稿）》，对我国密码工作进行规范。自《密码法》开始实施到2021年底，工信、金融、教育、公安、住建、交通、卫生、工商、能源、资源等领域主管部门均出台了针对各行业的密码相关政策，**累计发布各行业领域政策共27项**，对密码在各行业中的管理、使用、评测及相关标准的制定等方面进行了规范，明确密码技术对各行业信息安全的保障要求。

各地方配套细化政策

各地方为响应中央和各部委密码相关政策，纷纷出台相应配套政策，规范促进地方密码工作发展，形成了中央与地方的良性互动，共同促进商用密码产业蓬勃发展。为积极响应中央政策，各地方各部门按照《密码法》要求，不断加大密码应用推进力度。基础信息网络、重要信息系统、重要工业控制系统和政务信息系统等重要领域密码应用持续深化，密码技术积极护航5G、云计算、物联网等新基建安全发展，为网络空间安全秩序提供了高质量的密码技术和服 务。从《网络安全法》开始实施到2021年12月底，**我国已有21个省、自治区、直辖市出台了共31项公开密码应用相关政策要求。**

Part

06

我国商用密码标准建设现状



(一) 商用密码标准体系

我国商用密码标准体系

技术维度

将我国商用密码标准分为密码基础类标准、密码设施类标准、密码产品类标准、密码应用支撑类标准、密码应用类标准、密码检测类标准及密码管理类标准等七类标准。

管理维度

依据《密码法》中的规定，将商用密码标准分为国家标准、行业标准和团体标准。其中，商用密码国家标准由国家标准化管理委员会组织制定；商用密码行业标准由国家密码管理局组织制定，报国家标准化管理委员会备案；商用密码团体标准由商用密码领域的学会、协会等社会团体制定。

行业维度

根据标准所适配的不同行业进行分类的商用密码标准体系，如物联网应用类标准、云计算应用类标准、交通行业应用类标准、社保行业应用标准、电力行业应用标准、金融行业应用标准等。

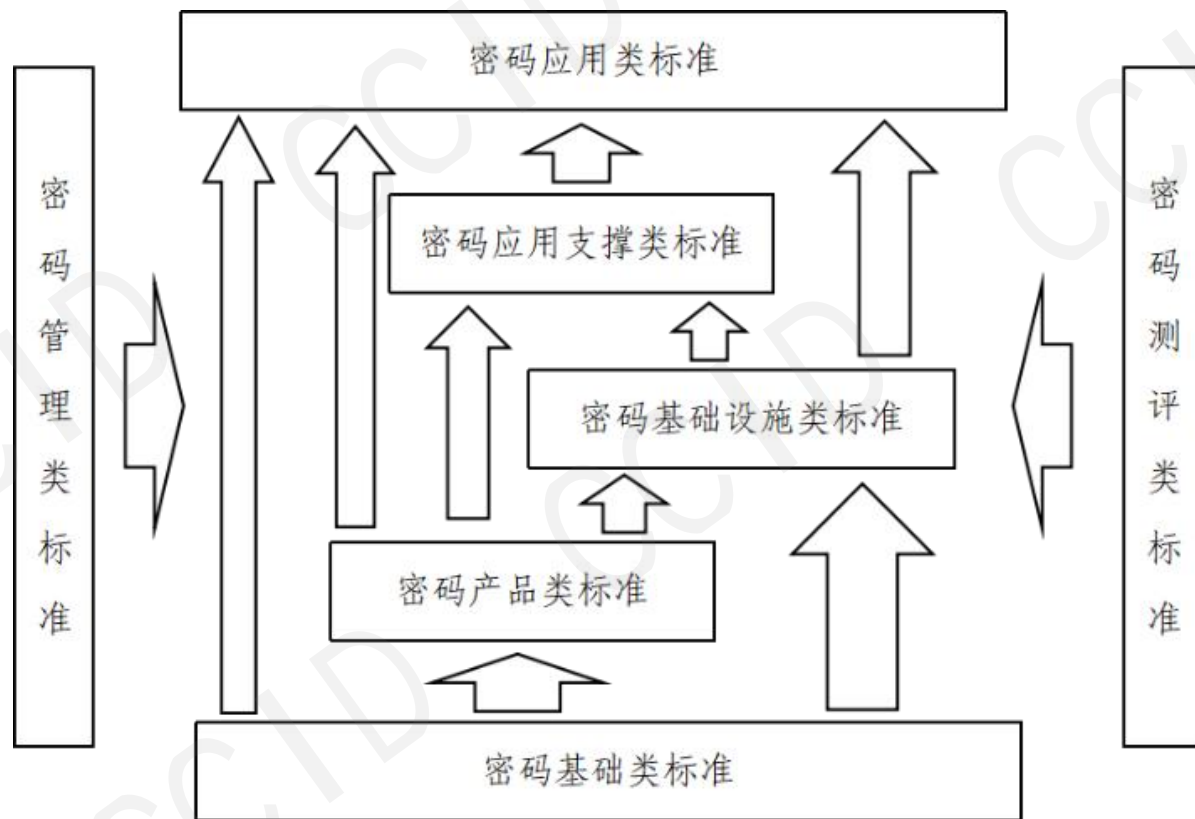


图6-1 商用密码技术维度标准体系

(二) 商用密码标准现状

商用密码国家标准

- 截至2021年12月底，国家标准化管理委员会已发布现行商用密码**国家标准47项**，其中密码基础类标准15项、密码设施类标准8项、密码产品类标准5项、密码应用支撑类标准8项、密码应用类标准6项、密码检测类标准1项、密码管理类标准4项。

商用密码行业标准

- 截至2021年12月底，国家密码管理局已发布商用密码**行业标准133项**，其中2021年新增16项。新增的行业标准中有密码基础类标准1项、密码设施类标准1项、密码应用类标准9项、密码检测类标准5项。

商用密码团体标准

- 截至2021年12月底，各商密协会、联盟发布现行**团体标准37项**，其中2021年新增9项。新增团体标准主要涉及商用密码检测领域，对移动端密码设备、汽车密码模块及云平台密码应用进行了规范，其中密码设施类标准2项、密码检测类标准7项。

Part

07

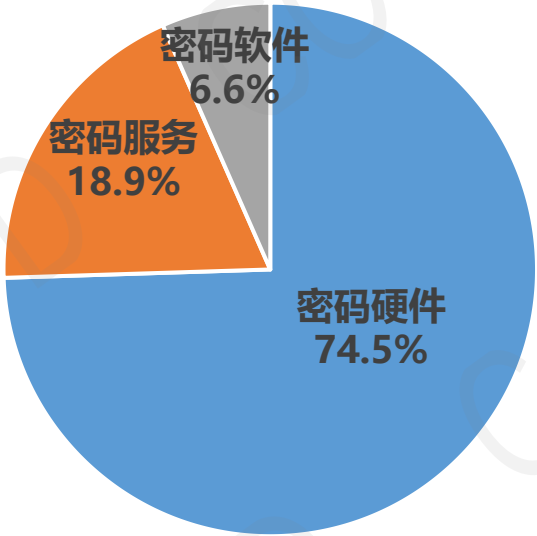
我国商用密码产业发展现状



(一) 产业结构持续优化

2021年，我国商用密码产业硬件产品市场规模435.83亿元，占比为74.5%；软件产品市场规模38.61亿元，占比为6.6%；服务市场规模110.57亿元，占比为18.9%。我国商用密码产品依然以硬件为主导，与国外软硬产品均衡、产品通用性较强等特征形成对比。相较2016年硬件产品市场规模占95%以上的状态，我国商用密码产业结构正在逐步优化。

图7-1 我国商用密码产业结构占比情况



(二) 产业链条逐步完善

狭义的商用密码产业链可分为上游密码设备提供商、中游商用密码软硬件产品制造商和下游商用密码服务提供商。广义的商用密码产业链可根据企业间的供需关系拓展为合作层、基础层和用户层。近年来商用密码产业链条不断完善，现已基本建成种类丰富、链条完整、安全适用的商用密码产业体系。

(三) 创新驱动产业发展

- 依托商用密码前沿技术推动与5G、工业互联网、物联网、车联网、人工智能、区块链、量子通信等新技术、新业态的融合发展。
- 以创新为导向，对于密码科技创新型人才的需求迫切，企业团队成员以研发人员为主。
- 商用密码企业注重技术研发，据统计，商用密码企业中研发人员占比超过36.7%。



图7-2 商用密码供需关系产业链

Part

08

我国商用密码技术产品进展



我国商用密码技术产品进展

01

产品创新日趋活跃

- 在硬件方面，现已有国产化商用密码卡实现主控器使用国产化芯片，且算法及配套外设均实现国产化，密码卡的制造工艺、综合性能、兼容性、安全性等方面取得长足进步。
- 在软件方面，数据加密平台产品可实现密码保密一体化、分布式加密、集中式管控等功能，实现了在现有系统上的安全能力叠加增强。
- 在与新技术新应用结合方面，物联网安全密码应用解决方案实现了物联网环境身份认证、传输加密、信息防篡改的安全需求，轻量化密钥管理身份标识与密钥信息占用极小的物联网终端系统资源，在保障物联网终端安全的基础上不影响其工作效率。

02

技术取得长足进步

- 在国家政策的大力引导下，商用密码的应用正在向工业互联网、车联网、智慧城市等新兴领域融入。
- 不同领域的应用诉求对密码技术和相关适配设备提出差异化要求，特别是新兴领域对密码功能和性能的要求更高，如面向云和大数据场景的同态加密技术、高性能密码技术，面向智慧城市等场景的轻量级加密技术。



03

算法体系不断突破

- 已建成基于SM2算法的国家电子认证信任体系。
- ZUC、SM2、SM3、SM4、SM9等一系列商用密码算法构成了我国完整的密码算法体系，部分密码算法被采纳为国际标准，为促进国际密码学发展、丰富产业选择和保障应用安全提供了中国方案。

04

通过认证的产品日益丰富

- 截止到2021年底，共有2155款产品获得了公开有效的商用密码产品认证，以上产品分别由536家商用密码产业链企业生产或制造。
- 获得商用密码产品认证的硬件产品1677种，占比为78%；软件产品478种，占比为22%。

Part

09

我国商用密码服务进展



我国商用密码服务进展

01

密码应用安全性评估加快落实

依据《密码法》及商用密码应用安全性评估有关管理规定，经持续培育、实战测评和综合考察，2020年7月，国家密码管理局正式公布了全国首批24家密评试点机构目录。2021年6月，国家密码管理局更新了《商用密码应用安全性评估试点机构目录》，密评试点单位增至48家。

02

电子认证服务愈发规范

随着我国信息化程度的不断加深，电子认证服务发展愈发规范，电子数据法律效力愈发受到重视。各行业主管部门出台多项政策，明确电子签名的法律效力，拓展电子签名的适用范围，促进电子签名广泛应用。

03

第三方电子签名平台服务影响力显著增强

疫情加速了远程办公趋势兴起，推动第三方电子签名平台相关产品和服务不断丰富，应用场景持续拓宽，目前已延伸到金融、人力资源、房地产、政务、物流、医疗、教育等多个领域。

Part

10

我国商用密码重点领域应用情况



我国商用密码重点领域应用情况

为加强重要领域网络与信息系统的安全风险防控能力，切实加强各行业的密码应用工作，金融、交通、工商、能源、教育、公安、水利等领域主管部门陆续出台系列政策文件，制定了本领域密码应用总体规划或工作方案，对密码应用提出了明确的要求。



金融领域：在网上银行、电子保单和网上证券安全方面，通过基于密码技术的数字证书、数字签名、电子签章、时间戳等，提供身份认证以及业务数据和电子合同的机密性完整性保护。



通信领域：三大运营商建设的600多万个基站系统全部支持ZUC算法，高通、华为、展讯、MTK等主流基带芯片厂商的产品都支持ZUC算法，基于这些基带芯片生产的数亿部移动智能手机默认支持ZUC算法。



工业互联网领域：工业互联网平台应用密码技术实现不同层级间的安全传输及跨平台的身份互认需求，建设以密码为核心的云安全保障体系。



电子政务领域：国家电子政务外网基于商用密码SM2算法建立身份认证系统，确保网络行为主体身份的唯一性、真实性和合法性；利用密码技术确保网络数据的安全传输；基于PKI技术的电子认证保证网上传递数据的真实性、完整性、保密性；采用SM9标识密码算法和数字签名、数据加密技术实现强身份认证机制和邮件内容加密。



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%。截止到2021年9月，全国已实现314个地级以上城市交通一卡通互联互通。



电力领域：在电力行业重要信息系统中，提供了体系化、规模化的安全保障，可保障发电环节、输电环节、变电环节、配电环节及用电信息采集环节的安全稳定运行。



医疗领域：满足医疗云/医疗信息系统上各项业务应用的安全需求，为构建一体化“互联网+医疗服务”提供密码支撑保障，助力数字化转型，全面提升各类医疗信息系统密码应用水平。



教育领域：主要应用于全国教育管理信息化业务和教育卡等方面。按照教育部要求，在教育和科研计算机网、教育管理、教育资源、电子校务、教育基础数据、教育卡等信息系统，以及面向社会服务的教育政务系统中加强密码应用。

Part

11

我国商用密码产业投融资情况



(一) 资本市场关注度显著提高

自2017年以来，国家陆续出台相关政策，鼓励和促进了商用密码产业发展，使密码成为刚性合规需求，产业受到资本市场关注度也持续升温。近年来资本力量赋能商用密码产业发展，许多商用密码企业融资、并购、上市情况持续活跃，部分企业受到资本青睐已获得多轮融资，且融资金额不断攀升，单轮融资金额有达到10亿元人民币以上。

(二) 投融资细分领域持续扩大

基础研究和
技术服务领域

数据安全领域

安全芯片领域

电子签名领域

(三) 兼并收购事件数量增多

- 2020年12月，豆神教育科技（北京）股份有限公司（原北京立思辰科技股份有限公司）以2.5亿元出售江南信安（北京）科技有限公司100%股权，江南信安携手中电信息和奇安投资完成新一轮战略重组。
- 2021年10月，信安世纪以861万元收购北京千茂100%股权，以1985万元收购宏福锦泰100%股权。信安世纪通过北京安瑞君恒、北京千茂、宏福锦泰合计间接持有应用交付、应用安全领域的产品和解决方案提供商华耀科技（Array Networks）100%股权。
- 2021年1月，字节跳动收购北京世纪速码信息科技有限公司。
- 2021年1月，腾讯收购内蒙古网信电子认证有限责任公司。

Part

12

我国商用密码行业组织发展情况



我国商用密码行业组织发展情况

截止到2021年底，我国商用密码行业组织已成立**24家**，遍布北京、上海、江苏、江西、广东、四川、陕西、甘肃、宁夏等19个省、自治区和直辖市。其中北京市3家，江苏省2家，广东省2家。

在《密码法》出台的背景下，近三年我国商用密码行业组织成立速度尤为迅猛，2019年新成立4家，2020年新成立5家，2021年新成立7家，相比2019年以前的速度有了大幅增长。

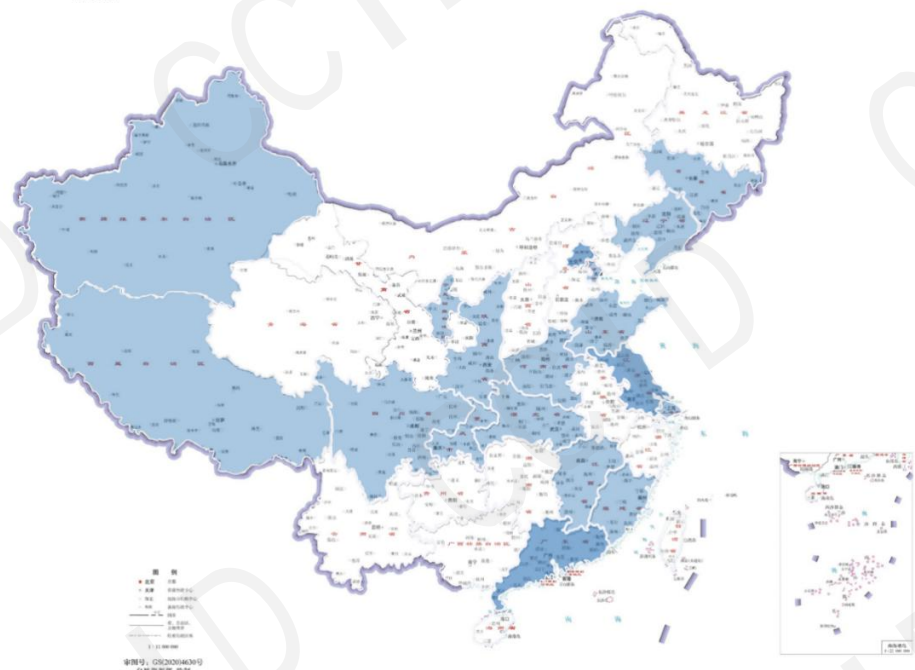


图12-1 我国商用密码行业组织地域分布情况

序号	名称	成立时间
1	中国密码学会	2007.03.25
2	工业和信息化部商用密码应用产业促进联盟	2021.07.21
3	北京商用密码行业协会	2015.04.02
4	天津市商用密码行业协会	2018.07.27
5	辽宁省商用密码协会	2021.09.10
6	吉林省密码协会	2021.10.26
7	上海市商用密码行业协会	2019.11.26
8	江苏省密码学会	2020.11.08
9	江苏省商用密码产业协会	2016.01.28
10	福建省商用密码行业协会	2014.12.31
11	江西省商用密码应用协会	2017.08.01
12	山东省商用密码协会	2019.01.24
13	河南省密码协会	2021.09.28
14	湖北省商用密码协会	2020.09.07
15	广东省商用密码协会	2020.04.29
16	重庆商用密码行业协会	2016.05.26
17	四川省密码行业协会	2019.10.29
18	西藏自治区商用密码协会	2021.05.07
19	陕西省商用密码协会	2019.10.28
20	甘肃省商用密码行业协会	2020.07.28
21	宁夏商用密码协会	2021.09.14
22	新疆商用密码行业协会	2020.12.11
23	杭州市商用密码应用协会	2021.01.15
24	深圳市商用密码行业协会	2013.03.26

Part

13

我国商用密码企业发展情况



(一) 企业数量持续增长

截止到2021年底，我国从事生产和销售商用密码硬件产品、生产和销售商用密码软件产品、提供商用密码相关服务等业务，具有投入和产出的商用密码企业已达1400余家。企业数量由2017年的737家，增长到2021年的1477家。

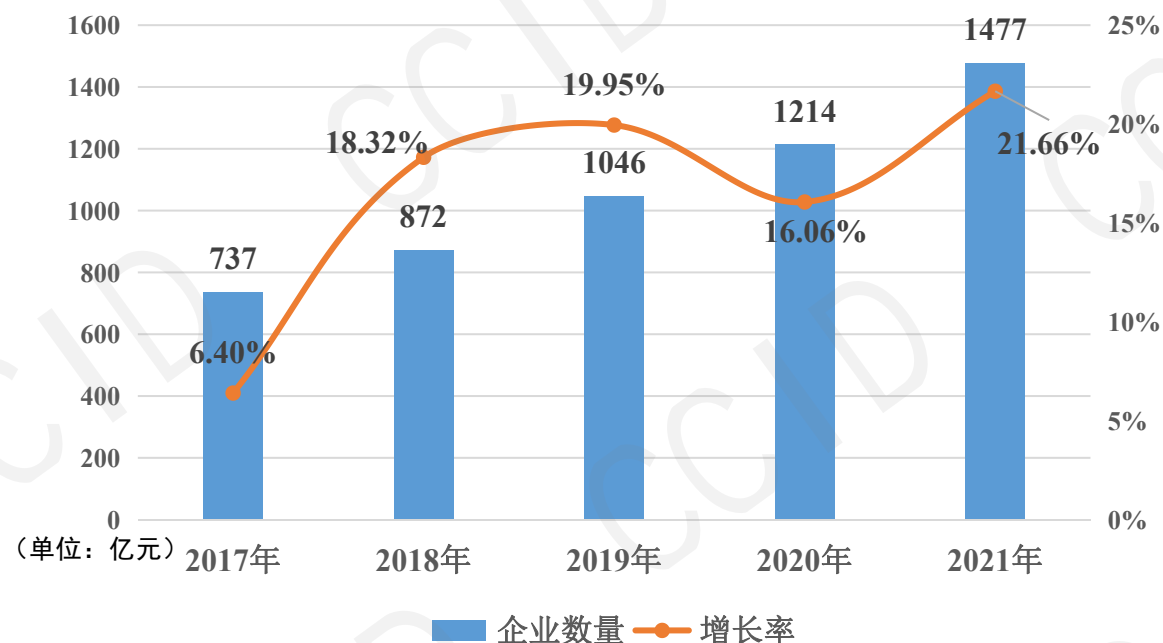


图13-1 2017-2021年我国商用密码企业数量及增长率

(二) 人员团队规模普遍较小

根据国家密码管理局统计，商用密码企业从业人员在2017年就已超过5万人。经过近些年的发展，商用密码企业从业人员数量已达到10万人以上。但商用密码企业人员规模普遍较小，且近五年来人员增长幅度较为平稳。

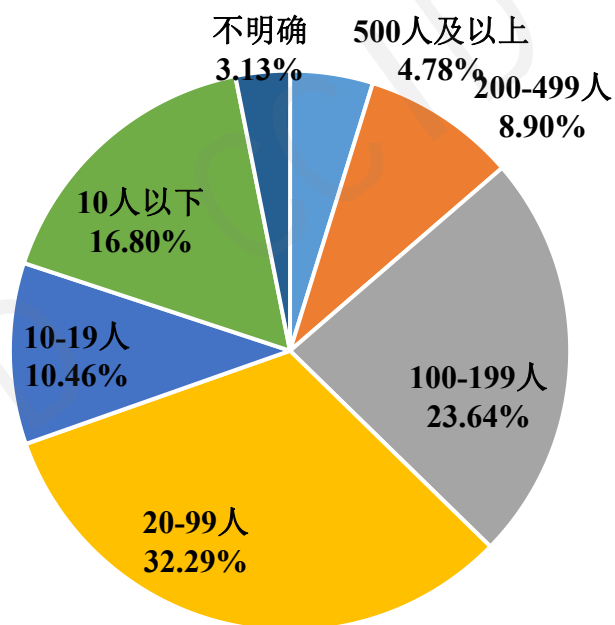


图13-2 商用密码企业从业人员各区间企业数量占比

(三) 企业地域分布相对集中

据统计，北京、广东、浙江、上海的商用密码企业数量之和占整个行业半数以上，北京和广东的商用密码企业居多。截止到2021年底，我国商用密码企业主要集中在北京、广东两省市，合计占全国数量的41.76%，商用密码企业向一线及发达城市聚集的态势十分明显。

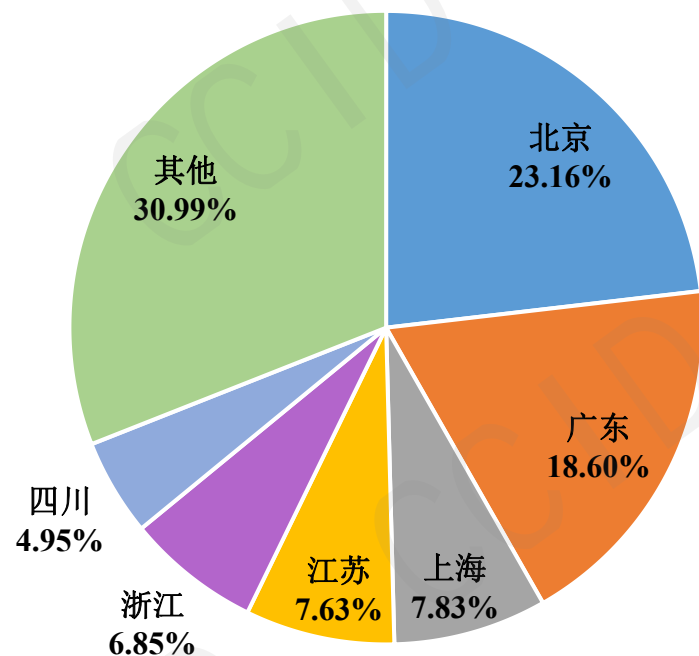


图13-3 各省市商用密码企业数量占比

华北、华东和华南是我国商用密码企业三大聚集地区，华中和西南地区商用密码企业已具有一定规模，东北和西北地区的商用密码企业数量较少。同时电子认证服务企业和商用密码应用安全性评估试点机构也大多分布在北京和华东、华南地区，其他地区的商用密码企业发展有进一步提升的空间。

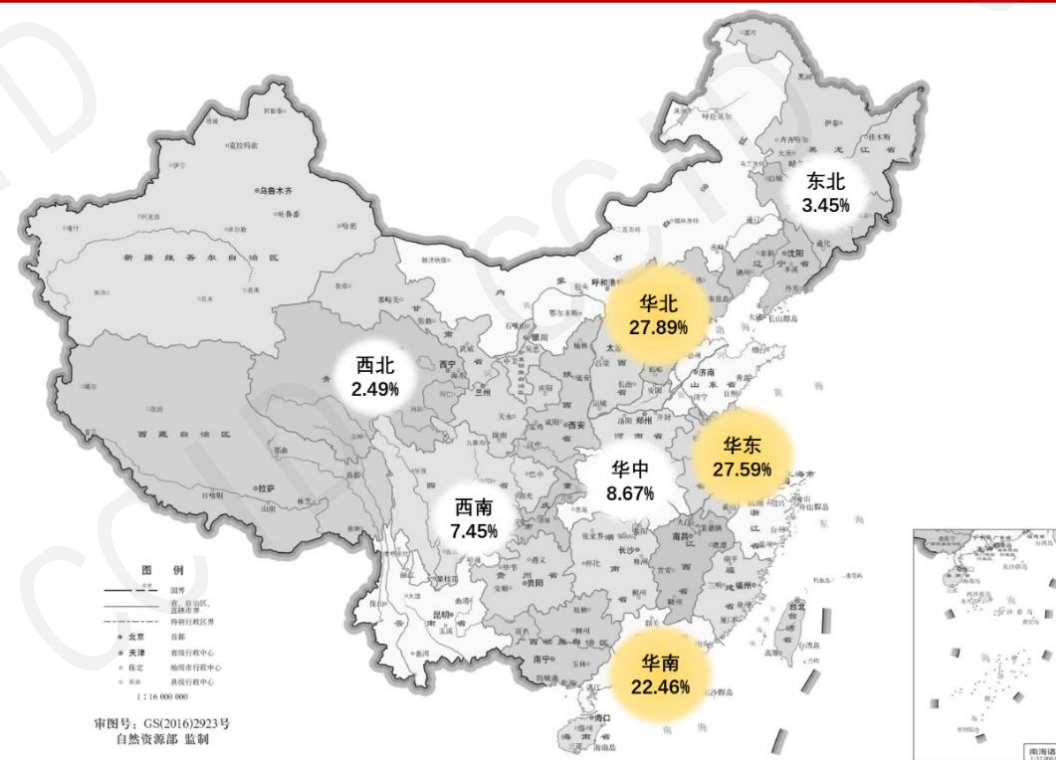


图13-4 商用密码企业数量地域分布情况

(四) 上市企业经营情况良好

截止到2021年底，我国商用密码上市企业总体数量达到76家。近5年，我国商用密码上市企业整体保持营业收入持续增长的趋势，市场需求的增加驱动企业网络安全产品的拓展和完善。

报告选取以密码为核心业务的5家主要上市公司作对比，分别为北京数字认证股份有限公司（以下简称数字认证）、成都卫士通信息产业股份有限公司（以下简称卫士通）、长春吉大正元信息技术股份有限公司（以下简称吉大正元）、北京信安世纪科技股份有限公司（以下简称信安世纪）、格尔软件股份有限公司（以下简称格尔软件），梳理商用密码上市企业发展情况。

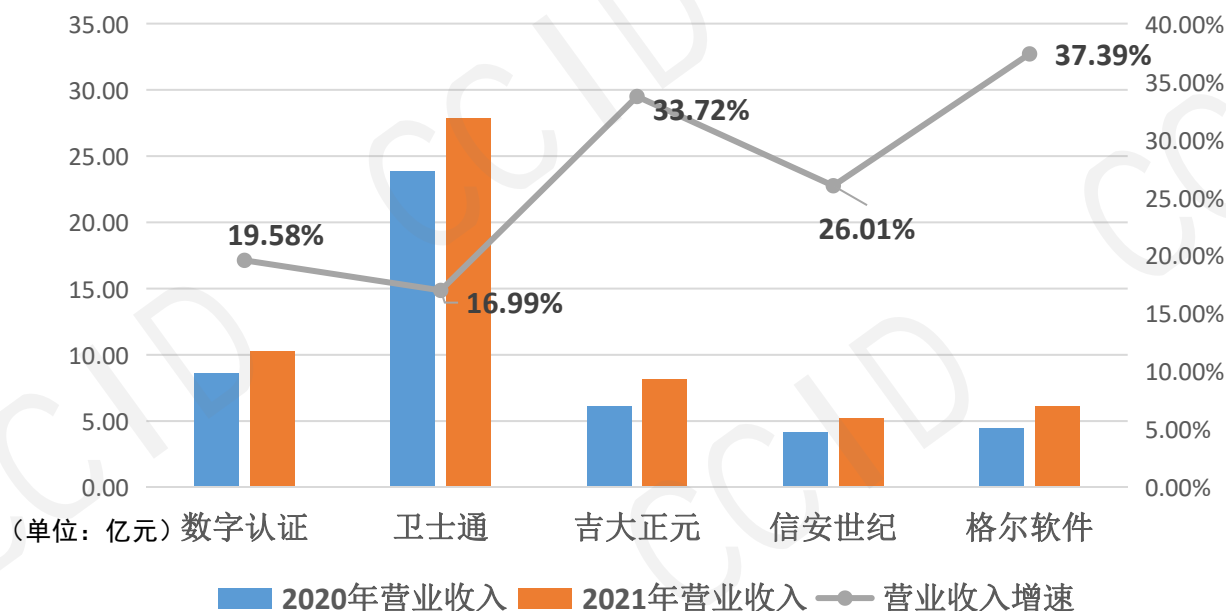


图13-5 2021年主要上市商用密码企业营收情况

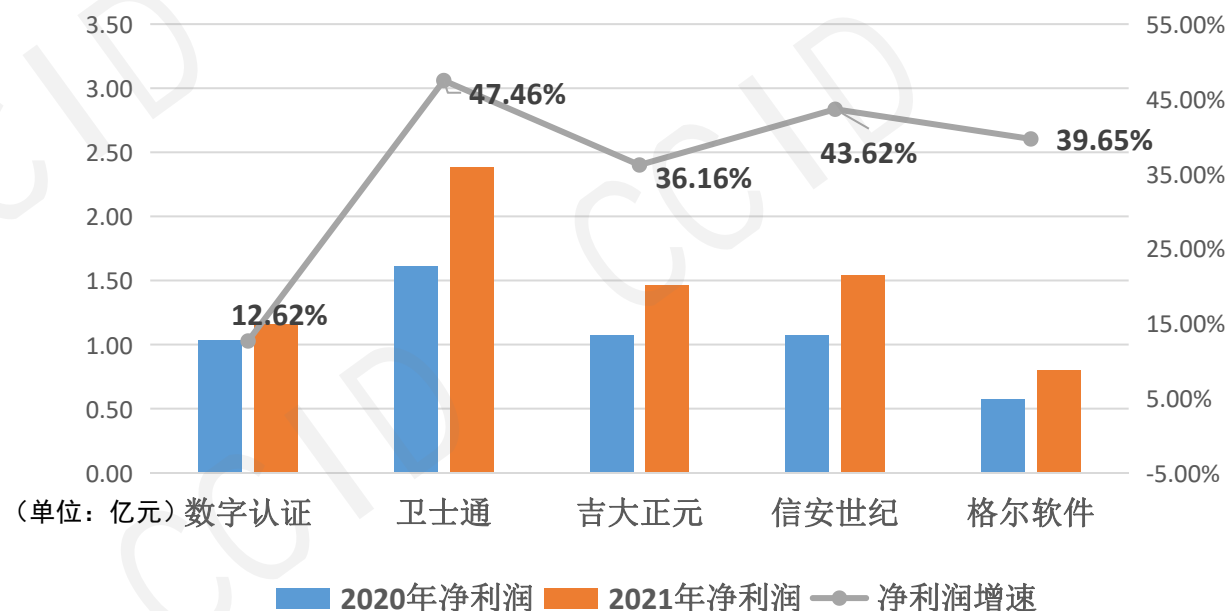


图13-6 2021年主要上市商用密码企业净利润情况

Part

14

我国商用密码行业发展趋势预测



我国商用密码行业发展趋势预测

01

政策环境持续向好

产业规模快速增长

02

03

产品结构加快优化

密码技术与新兴技术加速融合

04

05

高速密码细分领域发展进入快车道

应用范围不断扩大

06

07

应用生态稳步完善

行业投融资愈加活跃

08



谢谢观看