2021 密码产业洞察报告

V1.0.1

2021 年 7 月 26 日

目 录

前言

密码是国之重器，是信息化发展的安全基因，是保障网络与数据安全的核心技术，也是推动我国数字经济高质量发展，构建网络强国的基础支撑。近年来，国家高度重视商用密码工作，先后发布相关政策法规、采取系列重大举措，以促进商用密码的推广普及、深度融合。纵观当下，我国正处于数字经济高速发展期，密码产业供给侧、需求侧、监管侧均有长足发展，密码实战与合规需求强劲，技术自主可控逐步实现，“放管服”改革进一步深化。站在“十四五”开局新起点，密码前沿技术与应用的引领企业，应抓住时代机遇窗口，加速布局密码业务，深化技术创新研究，扎实推进我国商用密码产业建设及发展。

注 1：本文仅代表作者观点，水平认知有限，后续将陆续更新迭代，欢迎业界同仁共同完善。

注 2：本文部分内容或数据借鉴了《商用密码发展报告（2012-2017）》（国家密码管理局组织，负责编写）、《商用密码知识与政策干部读本》、《商用密码应用与安全性评估》，《2020-2021 中国商用密码产业发展报告》（赛迪研究所网络安全研究所发布）、《数据安全白皮书》（2021 年由国家工信安全中心联合华为发布）等权威素材或书籍，以及从互联网公开获取到的相关政策权威材料。

观点提要

1. 密码监管侧政策带来市场红利

在《密码法》及相关法规政策推动下，密码市场蓬勃发展，“放管服”新政策推动密码企业的竞争发展更公平公正，以产品质量决定竞争力，而非准入门槛。

2. 密码分层市场兼顾实战与合规

新密码市场呈现“实战防护、密评合规、信创合规”分层次叠加的多样化需求。实战与合规双重驱动下，新密码市场正步入快速增长阶段，预计 2023 年我国商用密码规模将超 900 亿。

3. 密码供给结构正向高质量升级

密码能用、密码好用、密码用好是提升密码高质量供给的关键，密码产品形态正从“以产品为主”升级到“产品+服务”，产品构成侧重向软件、或软硬混合形态发展。

4. 新数据安全紧密融合密码技术

企业安全防护正从“应对式”向“主动式”转变，密码对数据本身可以进行主动式加密等保护，是实现数据安全最直接有效的手段。融合密码的主动式防护安全框架，重视从业务风险映射视角列举数据保护需求，将密码功能融入业务流程，以数据为中心，构建全方位的数据安全治理体系，为信息化建设、企业业务架构设计提供数据安全能力参考。

一、密码产业筑牢坚实基础

信息化和网络安全整体水平是衡量一个国家综合国力和竞争力的重要标志，密码作为保障网络安全最有效、最可靠、最经济的关键核心技术，在维护国家安全、促进经济发展、保护人民群众利益中发挥着越来越重要的作用，并在科技创新、产业发展、应用推进、生态构建等方面取得系列成果。随着《密码法》出台，以及商用密码技术的不断推陈出新，密码产业已形成坚实发展基础，并步入创新协同、高质量发展的快车道。

（一）密码是信息化发展安全基因

密码作为历史最悠久、最具传奇色彩的安全技术，从诞生以来就自带安全产品属性，由攻防对抗推动发展。3000 年前，著名兵书《六韬》记载了姜太公使用阴符、阴书等古典密码技术来保护军事秘密通信。甲午战争期间，中方高级电报密码被日方破译，在一定程度上导致清军在战争的多方面陷入被动局面。

现代密码学演进，则与计算机技术、电子通信技术密切相关。随着计算机的发明以及信息化时代的到来，密码的加解密工作有了更好工具和载体，密码技术迎来千载难逢的发展机遇。这一阶段，密码理论百花齐放，密码算法的设计与分析互相促进，出现了大量的加密算法及分析方法，比如：序列密码、分组密码、公钥密码、HASH 函数等，技术与算法逐步成熟完善。

数字时代的来临，使得密码技术进入高速发展期。基于密码技术的身份鉴别、访问控制、数据加密、可信计算、密文计算、数据脱敏等措施，能实现信息系统安全防护架构的“真实性、机密性、完整性、不可否认性、限定性”等基本安全目标，有效解决信息系统的信息安全问题，成为支撑构建信息系统安全防护体系的基石。

信息化是密码技术演进的土壤，密码技术为信息化系统提供安全支撑。两者的深度融合，能够加速密码技术安全价值的释放。而随着信息技术演进升级，密码产品本身和对外服务形态也会发生适应性的转变。以云计算为例，虚拟机技术催生云交付形态的云密码机、云密钥管理系统等，同时企业应用云化又对密码产品和服务能力提出云兼容、弹性扩展、灵活管理等新需求，因此，“用云交付密码”和“让密码服务于云”逐步被企业所接受，且发展空间非常广阔。

（二）密码产业已构建出坚实基座

近年来，我国密码产业立足自主，开拓创新，在法律法规、算法标准、产业应用、监管体系等方面进展显著，夯实了自身发展基础，也为后续的快速发展积攒动力。

1. 法律标准体系逐步健全

早在 1996 年 7 月，中央办公厅就印发《关于发展商用密码和加强对商用密码管理工作的通知》,体现了对商用密码工作的重视。

如今，从顶层设计到法律法规，行业标准到产业要求的密集颁布，商用密码法律标准实现了自上而下的体系化发展，市场进一步被激活，海量非涉密信息的加密保护和安全认证等具体应用获得了充分发展的沃土。

1）顶层设计

《中华人民共和国国家安全法》第二十五条提出，国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。

《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，加快数字化发展，培育壮大网络安全等新兴数字产业；提高数字政府建设水平，建立健全数据要素市场规则，加强网络安全保护，推动构建网络空间命运共同体；统筹发展和安全，加强国家安全体系和能力建设。

十三届全国人大四次会议《政府工作报告》中提出，加快数字化发展，打造数字经济新优势，协同推进数字产业化和产业数字化转型，加快数字社会建设步伐，提高数字政府建设水平，营造良好数字生态，建设数字中国。同时，强调加强网络安全、数据安全和个人信息保护。

《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》第六部分“加快培育数据要素市场”第 22 条：加强数据资源整合和安全保护。推动完善适用于大数据环境下的数据分类分级安全保护制度，加强对政务数据、企业商业秘密和个人数据的保护。

2）法律法规

● 密码“一法三规一条例”

表 1 密码一法三规一条例

密码政策法规、条例标准		
层级	名称	条例
一法	《密码法》	二十七条：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。关键信息基础设施运营者，应当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。
三规	《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知》（国办发〔2019〕57 号）	第四章第三十条：各部门应当严格遵守有关保密等法律法规规定，构建全方位、多层次、一致性的防护体系，按要求采用密码技术，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。

	《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》（公网安〔2020〕1960号）	第二部分第六点：落实密码安全防护要求。网络运营者应贯彻落实《密码法》等有关法律法规规定和密码应用相关标准规范。第三级以上网络应正确、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。
	《关键信息基础设施安全保护条例（征求意见稿）》	第四章第二十三条第四点：采取数据分类、重要数据备份和加密认证等措施。
一条例	《商用密码管理条例》（修订草案征求意见稿）	第六章第三十八条：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。
密评行标升国标	GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》	“密码产品”方面的基本要求相比行标有重要变化，信息系统等级保护第三级安全要求，从行标的“宜采用GM/T 0028三级及以上”，放宽为国标的“应达到GB/T 3

		7092 二级及以上”；对等级保护第二级安全要求，从行标的“宜采用 GM/T 0028 二级及以上”，放宽为国标的“应达到 GB/T 37092 一级及以上”。其次，“密码服务”成为行业技术要求的必选项。（注：GM/T 0028 是 GB/T 37092 密码模块安全技术要求的行标版本，行标升国标后的具体变化见文末好文推荐）

● 各地区密码应用政策要求

北京市明确将密码应用建设过程中的新建项目所需经费列入同级政府固定资产投资，升级改造和运行维护经费列入同级财政预算，并对密码应用情况进行事前审查。

吉林省制定出台 13 项密码应用“增量”管控措施，部署在项目立项、项目论证、招标采购等环节，对项目建设实施管控，明确采用密码进行保护的刚性约束。吉林省还出台 36 项密码供给能力建设扶持政策，涵盖金融、土地、税收、出口等方面，对密码产业、产品和服务等供给侧给予优惠扶持。

江苏省财政厅、省密码管理局联合印发通知并颁布《江苏省密码产品采购管理目录》，明确密码产品相关采购要求。

天津市委办公厅、市政府办公厅联合印发《关于重要领域网络与信息系统规范使用密码的通知》。

贵州省委办公厅、省政府办公厅印发《贵州省重要领域网络与信息系统密码应用审核实施意见》，要求使用财政性资金新建或改造重要领域网络与信息系统，应当报密码管理部进行常码使用合规性审查，密码部门出具的审核意见应作为财政部门审批资金的必备材料。

河北省财政厅、密码管理局、公共资源交易监督办公室联合印发《关于面向社会服务的政务信息系统使用国产密码技术设备的通知》，要求相关信息系统在新建、改建、扩建时，与商用密码应用同步规划、同步建设、同步运行、定期评估。

河南省制定《河南省金融和重要领域密码应用与创新发展实施方案（2018—2022年）》。到2022年，全省应用密码技术保护网络安全的意识普遍增强，密码发展与我省承担的国家重大战略和新技术新应用深度融合，供给体系和测评认证体系基本建立，密码保障金融和重要领域网络安全的作用得到充分发挥，有力支撑信息领域核心技术突破，切实维护国家安全、促进经济社会发展、保护人民群众利益。

湖北省人民政府办公厅印发《湖北省政务信息化项目建设管理办法》，要求项目建设单位应开展网络与信息安全风险评估，严格落实等级保护、分级保护和国家密码管理的要求，同步规划、同步建设、同步运行密码保障系统并定期评估，切实保障政务信息化项目安全稳定运行。

安徽省密码管理局、安徽省财政厅印发《关于重要领域信息系统密码应用工作的通知》，要求凡申报使用财政性资金建设的重要领域信息系统项目，必须提供密码应用方案。

江西省人民政府办公厅印发《江西省政务信息化项目建设管理办法》，要求各部门应当严格遵守有关保密等法律法规规定，构建全方位、多层次、一致性的防护体系，按要求采用密码技术，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。

3）行业要求

2021 年 7 月 12 日，为深入贯彻党中央、国务院关于制造强国和网络强国的战略决策部署，落实《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》有关要求，加快推动网络安全产业高质量发展，提升网络安全产业综合实力，**工业和信息化部发布《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）》，并提出：“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%**；一批网络安全关键核心技术实现突破，达到先进水平；网络安全产品、服务、解决方案单项冠军企业数量逐步壮大；电信等重点行业网络安全投入占信息化投入比例达 10%;建成一批网络安全人才实训基地、公共服务平台和实训靶场；产融对接更加精准高效，资本赋能作用持续加大”的发展目标。

2021 年 5 月 1 日由国家互联网信息办公室、工业和信息化部、公安部、市场监管总局发布《常见类型移动互联网应用程序必要个人信息范围规定》，该规定在明确 App 基本功能服务和必要个人信息范围的基础上，明确要求 App 运营者不得因用户不同意收集非必要个人信息，而拒绝用户使用其基本功能服务。该规定的出台科学地平衡了个人信息保护与促进 App 发展应用的关系，保障了用户对 App 基本功能服务的使用权，以及对收集使用非必要个人信息的知情权和决定权，有利于促进 App 的健康发展。

2021 年 4 月 26 日由国家互联网信息办公室、工业和信息化部、公安部、市场监管总局联合发布了《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》，该规定界定了适用范围和监管主体，明确了“知情同意”“最小必要”两项原则。这一新政释放出全力捍卫公民隐私权的强烈信号，而 APP 也将面临精细监管。

2021 年 2 月 1 日发布的《保险中介机构信息化工作监管办法》由中国银行保险监督管理委员会正式发布，对保险中介机构信息化工作提出全面要求，提出实施后的一年整改自查期内，若不完成信息化系统建设，将不得经营保险中介业务。《办法》将进一步提高保险中介机构的信息化工作水平和经营管理水平，构建新型保险中介市场体系，促进保险业高质量发展。

2021 年 1 月 15 日发布的《监管数据安全管理办法（试行）》由中国银行保险监督管理委员会正式发布，旨在建立健全监管数据

安全协同管理体系，推动银保监会有关业务部门、各级派出机构、受托机构等共同参与监管数据安全保护工作，加强培训教育，形成共同维护监管数据安全的良好环境。

2020 年 6 月 12 日发布的《民用航空旅客服务信息系统信息安全保护规范》规定了民用航空旅客服务信息系统需要满足的相关信息安全技术要求和管理要求，适用于民航旅客服务信息系统的规划、设计、开发、运行及维护等各个阶段。

2020 年 3 月 5 日发布的《关于深化医疗保障制度改革的意见》由中共中央、国务院印发，提出统一医疗保障业务标准和技术标准，建立全国统一、高效、兼容、便捷、安全的医疗保障信息系统，实现全国医疗保障信息互联互通，加强数据有序共享。规范数据管理和应用权限，依法保护参保人员基本信息和数据安全。

2020 年 2 月 1 日施行的《国家政务信息化项目建设管理办法》由国务院办公厅印发，对国家政务信息系统的规划、审批、建设、共享和监管作出规定，提出建立统一、集约化信息基础设施和安全保障大平台，对共性应用与分散系统提供集中统一基础设施支撑，将更加有利于提高政务信息系统的安全保障能力，提高系统建设的集约水平，避免重复建设。

2020 年 2 月 13 日发布的《个人金融信息保护技术规范》由中国人民银行正式发布，将个人金融信息按敏感程度、泄露后造成的危害程度，从高到低分为 C3、C2、C1 三个类别；同时，规定了个

人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求，从安全技术和安全管理两个方面，对个人金融信息保护提出了规范性要求。

2020 年 2 月 26 日发布的《2020 年教育信息化和网络安全工作要点》由教育部办公厅印发，对 2020 年教育信息化和网络安全重点工作进行了安排部署。《工作要点》提出，落实《教育行业密码与应用创新发展实施方案》，推进密码基础设施和支撑体系建设，有序推动教育重要业务信息系统开展密码应用安全性评估，完善教育数字认证（CA）基础支撑体系建设，推动国家教育管理信息系统密码普遍应用，提升系统安全和数据安全。

4）标准规范

在国际标准化方面，自 2015 年 5 月起，我国陆续向 ISO 提出了将 SM2、SM3、SM4 和 SM9 算法纳入国际标准提案。2017 年，SM2 和 SM9 数字签名算法正式成为 ISO/IEC 国际标准；2018 年，SM3 算法正式成为 ISO/IEC 国际标准；2020 年 4 月，ZUC 算法正式成为 ISO/IEC 国际标准;2021 年 3 月,SM9 标识加密算法正式成为 ISO/IEC 国际标准。2021 年 6 月 25 日，我国 SM4 分组密码算法由国际标准化组织 ISO/IEC 正式发布，成为 ISO/IEC 国际标准。

在商用密码标准体系建设方面，截至 2021 年 3 月 15 日，累计发布密码国家标准 39 项，密码行业标准 115 项。

表 2：密码相关的 39 项国家标准：

国标号	标准名称（中文）	采用国际标准形式	采用国际标准号	发布时间	实施时间
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	修改采用	ISO/IEC 9797-1:2011	2020/12/14	2021/7/1
GB/T 38625—2020	信息安全技术 密码模块安全检测要求	未采用		2020/4/28	2020/11/1
GB/T 38635.1—2020	信息安全技术 SM9 标识密码算法 第 1 部分：总则	未采用		2020/4/28	2020/11/1
GB/T 38635.2—2020	信息安全技术 SM9 标识密码算法 第 2 部分：算法	未采用		2020/4/28	2020/11/1

GB/T 38636—2020	信息安全技术 传输层密码协议（TLCP）	未采用		2020/4/28	2020/11/1
GB/T 38647.2—2020	信息技术 安全技术 匿名数字签名 第2部分：采用群组公钥的机制	修改采用	ISO/IEC 20008-2:2013	2020/4/28	2020/11/1
GB/T 38540—2020	信息安全技术 安全电子签章密码技术规范	未采用		2020/3/6	2020/10/1
GB/T 38541—2020	信息安全技术 电子文件密码应用指南	未采用		2020/3/6	2020/10/1
GB/T 38556—2020	信息安全技术 动态口令密码应用技术规范	未采用		2020/3/6	2020/10/1
GB/T 17901.1—2020	信息技术 安全技术 密钥管理 第1部分:框架	修改采用	ISO/IEC 11770-1:2010	2020/3/6	2020/10/1

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	未采用		2018/12/28	2019/7/1
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	未采用		2018/12/28	2019/7/1
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	未采用		2018/12/28	2019/7/1
GB/T 37092—2018	信息安全技术 密码模块安全要求	未采用		2018/12/28	2019/7/1

GB/T 36624—2018	信息技术 安全技术 可鉴别的加密机制	修改采用	ISO/IEC 19772:2009	2018/9/17	2019/4/1
GB/T 34953.2—2018	信息技术 安全技术 匿名实体鉴别 第2部分：基于群组公钥签名的机制	等同采用	ISO/IEC 20009-2:2013	2018/9/17	2019/4/1
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	未采用		2018/6/7	2019/1/1
GB/T 36322—2018	信息安全技术 密码设备应用接口规范	未采用		2018/6/7	2019/1/1
GB/T 20518—2018	信息安全技术 公钥基础设施 数字证书格式	未采用		2018/6/7	2019/1/1

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	未采用		2017/12/29	2018/7/1
GB/T 35276—2017	信息安全技术 SM2 密码算法使用规范	未采用		2017/12/29	2018/7/1
GB/T 35291—2017	信息安全技术 智能密码钥匙应用接口规范	未采用		2017/12/29	2018/7/1
GB/T 15843.2—2017	信息技术 安全技术 实体鉴别 第 2 部分：采用对称加密算法的机制	等同采用	ISO/IEC 9798-2:2008	2017/12/29	2018/7/1
GB/T 35285—2017	信息安全技术 公钥基础设施 基于数字证书的可靠电子签名生成及验证技术要求	未采用		2017/12/29	2018/7/1

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	未采用		2017/5/12	2017/12/1
GB/T 33560—2017	信息安全技术 密码应用标识规范	未采用		2017/5/12	2017/12/1
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	未采用		2016/10/13	2017/5/1
GB/T 32905—2016	信息安全技术 SM3 密码杂凑算法	未采用		2016/8/29	2017/3/1
GB/T 32907—2016	信息安全技术 SM4 分组密码算法	未采用		2016/8/29	2017/3/1

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	未采用		2016/8/29	2017/3/1
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	未采用		2016/8/29	2017/3/1
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	未采用		2016/8/29	2017/3/1
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	未采用		2016/8/29	2017/3/1

GB/T 32213—2015	信息安全技术 公钥基础设施 远程口令鉴别与密钥建立规范	未采用		2015/12/10	2016/8/1
GB/T 31503—2015	信息安全技术 电子文档加密与签名消息语法	未采用		2015/5/15	2016/1/1
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	未采用	无	2013/11/12	2014/2/1
GB/T 17964—2008	信息安全技术 分组密码算法的工作模式	未采用	无	2008/6/26	2008/11/1
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	等同采用	ISO/IEC 9798-4:1999	2008/6/19	2008/11/1

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	等同采用	ISO/IEC 10118-2:2000	2002/7/18	2002/12/1

2. 产业正处于高速发展期

当前，商用密码市场主要参与者可分为政府、需求方、国内供给方和全球化供给方。政府负责发展规划、法规制定、市场准入、推动产业补贴等统筹性工作；需求方主要是具有合规和实战防护需求的党政机关、央企国企、金融及重要领域行业等；供给方主要是可提供商用密码技术、产品和解决方案的供应商。

纵观商用密码技术和市场演变，可归类和推演出三个关键时期、一个转折点：

- **美国科技引领的全球化期：**2000 年至 2015 年，是美国科技引领的、自由竞争的全球化期。在本阶段，美国密码技术占有绝对技术和市场领先地位。以数字证书为例，基于 RSA 等国外算法的 PKI 产品，占据国内网站的绝大部分市场占有率，此时自主可控等政策处于酝酿阶段。

- **内循环转折点：** 2015 年前后，密码技术和市场迎来内循环转折点。在此之前，**SM2、SM3、SM4 等国密算法陆续公开，**2012 年 3 月,国家密码管理局批准了六项密码行业标准:GM/T0001-2012《祖冲之序列密码算法》,GM/T0002-2012《SM4 分组密码算法》(原 SMS4 分组密码算法)，GM/T0003-2012《SM2 椭圆曲线公钥密码算法》，GM/T0004-2012《SM3 密码杂凑算法》，GM/T0005-2012《随机性检测规范》，GM/T0006-2012《密码应用标识规范》。紧接着，2012 年 12 月，国家密码管理局又批准了 GM/T0009-2012《SM2 密

码算法使用规范》等14项密码行业标准。此外，2013年开始，随着斯诺登陆续曝光美国“棱镜计划”和不断披露的“后门”事件，我国“十三五”规划中战略性提出自主可控等要求，随着后续2017年中美贸易摩擦开始并持续升级，信息技术领域暴露出“卡脖子”风险。从此，完善技术和产业供应链、改变受制于人的局面成为体系化坚定共识。

- **商用密码高速发展期：**2015年至预估2030年，是商用密码高速发展期。在本阶段，密码技术需要持续提升产业竞争力。在《金融和重要领域密码应用与创新发展工作规划(2018-2022年)》、《密码法》、“三规一条例”等相关政策法规引导下，密码需求侧和国内供给侧充分发展，辅以政策补贴扶持，密码产业技术创新加速推进，商用密码应用推广不断加速。

- **商用密码成熟期：**演进到商用密码成熟期后，密码技术和产业有望达到国际领先水平，密码技术将从技术、产品、应用等方面形成较强综合竞争力，为数字经济提供基础性安全支撑，为中国乃至全球的信息技术及供应链安全提供保障。

当下，密码产业正处商用密码高速发展期，诸多行业及用户都对信息安全提出较高要求，比如政府、军工、央企、科研院所、金融、能源等行业，以及云计算、物联网等领域的各级用户。这些行业的总体信息化进程仍处快速发展阶段，刺激密码产品、集成及服务需求持续增长，激发市场潜力。

3. 监管体系取得丰硕成果

从初创到规范管理，再到成为我国安全保障体系中的关键部分的发展演变，在检测认证体系、安全评估机制、进出口管理等监管体系建设方面，也均取得丰硕成果。

初步建立商用密码检测认证体系。国家密码管理局、市场监管总局共同发布《关于调整商用密码产品管理方式的公告》《关于开展商用密码检测认证工作的实施意见》《商用密码产品认证目录（第一批）》《商用密码产品认证规则》等，取消“商用密码产品品种和型号审批”，由市场监管总局会同国家密码管理局建立国家统一推行的商用密码认证制度，采取支持措施鼓励商用密码产品获得认证。截至2020年7月，商用密码产品型号证书换发认证证书工作已顺利完成。

密码应用安全性评估机制不断完善。2021年6月16日，国家密码管理局第42号公告，发布最新的《商用密码应用安全性评估试点机构目录》，明确了48家商用密码应用安全性评估试点机构。在《商用密码应用与安全性评估》中则全面介绍了密码的概念、作用、技术和功能，密码应用与安全性评估相关政策法规，以及商用密码产品的基本形态、遵循标准和应用要点，并以8种典型应用场景为案例，阐释密码应用方案和安全性评估的实施要求和关键点。

商用密码进出口管理进一步规范。根据密码法规定，商务部、国家密码管理局依法对涉及国家安全、社会公共利益且具有加密保护功能的商用密码实施进口许可，对涉及国家安全、社会公共

利益或者中国承担国际义务的商用密码实施出口管制。国家密码管理局、商务部、海关总署共同发布第38号公告，对商用密码进口许可清单和出口管制清单公布前后的操作进行了说明，商用密码进口许可清单和出口管制清单由商务部会同国家密码管理局和海关总署制定并公布。

总体来看，**密码监管市场可以概括为“一收一放”**。“一收”是指通过《国务院办公厅关于印发国家政务信息化项目建设管理办法的通知》（国办发〔2019〕57号）、《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》（公网安〔2020〕1960号），对政务、网络安全等级保护（简称“等保”）、关键信息基础设施安全保护（简称“关保”）等头部市场“收”紧监管力度，拉动合规需求规模，提升合规供给质量；“一放”是指对商业市场落实“放管服”，“放”宽市场准入，充分唤醒密码需求。差异化的市场监管营造了更加公平开放的密码商业环境，有效激活国内密码市场潜力，并鼓励商用密码产业“走出去”，构建国内大循环为主体、国内国际双循环相互促进的新格局。

4. 融合应用取得长足发展

《2020-2021中国商用密码产业发展报告》显示，**2016年到2020年，我国商用密码产业总体规模保持高增长率，2020年商用密码产业规模突破466亿元，年复合增长率超33%**。

表 3：2016-2020 年商用密码产业总体规模及增长率

年度	2016年	2017年	2018年	2019年	2020年
产业规模（亿元）	151.64	239.41	283	350	466
增长率	19.05%	57.88%	18.21%	23.67%	33.14%

数据来源：《2020-2021 中国商用密码产业发展报告》

随着信息技术产业的持续发展和完善，密码产品也随之迭代丰富，已经有 2200 余款产品取得商用密码产品认证证书，品类涵盖了密码芯片、密码板卡、密码机、密码系统、密码模块等全产业链条，形成了完整的商用密码产品供给体系。据国家商用密码检测中心报告披露，截止到 2021 年 4 月 1 日，我国发放的密码产品认证证书已达 2447 张。我国商用密码产品自主创新能力持续增强，产品支撑能力不断提升，部分产品性能指标已达到国际先进水平。

如今，密码应用深度融合到了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。

目前，国内有超过 80 家金融保险机构在电子保单、电子投保等业务方面，基于商用密码技术实现了国密数字证书的全面应用。基于密码模块生产的智能电表超 5 亿只，用户卡发放超 1 亿张；采

用密码技术的二代身份证和港澳台居民居住证共累计发行超过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；近2700万台移动智能终端基于密码技术实现了数字版权保护；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，累计签发数字证书超过数亿；密码技术在交通、能源等基础设施的密码支撑体系已初具规模。（注：数据引用于国家密码管理局发文）

在应用需求的带动下，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崭露头角，正影响并引领商用密码产业强势发展。目前，我国已有1200余家商用密码企业，对比2017年的740家，商用密码企业数量呈现持续增长的趋势，主要分布在北京、广东、浙江、上海、江苏等区域，主要客户集中于政府机构、金融、交通、大型企事业、电信运营商等行业和领域。国内商用密码行业已上市企业包括卫士通、数字认证、飞天诚信、格尔软件、吉大正元、信安世纪等，营业收入高达3-20亿元以上。同时，行业也涌现出一批新锐密码创业企业，以技术创新为驱动，不断提升产品研发、专利成果、服务能力及管理水平，践行责任与担当，为政府、金融、教育、医疗、文旅、央企、制造业、电信及互联网等行业，提供高价值的基于密码技术的数据安全服务，构筑数据安全防线，为国家安全建设添砖加瓦。

（三）关键领域密码技术应用发展

当前，以网络安全为代表的非传统安全威胁持续蔓延，我国信息领域核心技术设备受制于人的局面没有从根本上改变，关键信息基础设施安全防护能力仍然薄弱。面对日益严峻的安全形势，密码技术在重要信息系统、关键领域的关键作用凸显，引起了各关键领域的高度重视和大力推进。

1. 金融领域

在党中央的坚强领导下，金融和重要领域商用密码应用稳妥有序推进，带动了商用密码技术和产品持续发展，突破了一批关键核心技术，研制了一批满足应用的商用密码产品，商用密码产品市场占有率稳步提升，服务领域快速拓展，产业发展势头十分迅猛。

2018 年 7 月 15 日，中共中央办公厅及国务院办公厅印发 36 号文《金融和重要领域密码应用与创新发展工作规划(2018—2022 年)》，文件指出金融领域在密码应用方面的主要任务：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。此外还提出在 2022 年之前，要实现目标：“全社会应用密码技术保护网络安全的意识普遍增强，密码与国家重大战略和新技术新应用深度融合，高质量密码供给体系和测评认证体系基本建立，密码保障金融和重要领域网络安全的作用得到充分发挥，有力支撑信息领域核心技术突破，切实维护国家安全、促进经济社会发展、保护人民群众利益”。

针对银行业，采用商用密码技术提高金融业信息系统中的核心业务、客户服务渠道、中心节点等关键部分在安全保护、防欺诈、业务监管等方面的安全性。具体的应用包括，使用金融 IC 卡、动态令牌、智能密码钥匙等密码产品实现对客户身份、服务器身份等的认证；使用密码技术对柜面终端、ATM 机、POS 机等进行设备认证；使用密码技术建立安全通道，实现终端与银行业务系统间、银行业务系统与非银行业第三方对接系统间、银行业务系统与银行业中心节点关键系统间重要敏感信息的加密传输；使用密码技术，实现对系统存储的用户口令、用户隐私信息、重要交易数据等的加密保护；发送方使用密码技术对关键数据进行数字签名，接收方对签名进行验证，以确认数据完整、身份真实，确保行为不可抵赖。

提高金融系统抵御安全风险能力的同时，推动金融软件和硬件产品的升级换代。促进金融 IC 卡、POS 机、ATM 机、网银设备等诸多商用密码产品的研发、生产和应用。银行业各项交易业务，包括线下交易、网银交易、跨行交易等都不断刷新历史交易规模。商用密码在这些业务和系统中的广泛应用，将有效遏制银行卡伪造、网上交易身份仿冒等违法犯罪活动，显著提升敏感信息和交易数据的安全防护能力，有力保障金融信息安全和金融系统安全稳定运行，保护公民个人隐私和金融财产安全。

针对保险业，在网络保险发展过程中，电子保单采用商用密码技术确保了保险业务过程中各类电子单证的合法性。通过网上出

单，省去保险单证印刷、发放、机构盖章等环节，简化了保险公司内部管理流程，降低了复杂的交互环节可能引起的操作风险，降低了保险企业的营运费用，提升了投保用户使用体验，提高了保险公司营销效率。

针对证券业，通过以商用密码为基础的数字签名技术，有效解决了网上业务的法律效力问题，大大提高了办理效率，节省了成本。商用密码为证券业务的正常有序开展也将提供更强有力的安全保障。

2. 政务领域

当下随着政务外网的基础作用越来越明显，如何切实提升政务外网安全保障能力，有效支撑国家在经济调节、市场监管、社会管理和公共服务等方面的需要，成为当务之急。

政务外网的建设要按照信息安全等级保护的有关要求，分别采用相应的保护措施，通过建立统一的密码和密钥管理体系、网络信任体系和安全管理体系，分级、分层、分域地保障信息安全。根据政务外网的安全需求，要建设政务外网安全信任体系，提供在线身份认证、授权管理和责任认定，确保政务外网资源不被非法用户访问；建设政务外网数据交换中心，确保不同安全域之间的安全数据交换；确保政务外网的安全保障体系具有高可靠性，并具有可审计、可监控等特性。及时发现并修正网络系统中的漏洞，采取有效的安

全保障措施；实施政务外网统一的安全管理体系，为政务外网提供制度上的保证；确保政务外网与互联网的安全互联。

2014 年 11 月 13 日，国家电子政务外网管理中心发布《国家电子政务外网信息安全标准体系框架》等 7 项安全标准，成为规范国家电子政务外网信息安全标准体系建设以及指导各级政务外网开展安全接入、安全交换、安全监测以及各级政务部门局域网安全连接政务外网等技术管理工作的依据。商用密码在政务外网的信息安全保障体系中应用不断推进，有效提升了政务外网的安全性。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，保护网络空间中各种主体的安全利益；利用密码技术为数据通道增加安全防护，确保网络数据的安全传输，为政务外网的扩展和移动业务提供安全保障；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、数字签名和数字验证，保证网上传递数据的真实性、完整性、保密性，确保网络应用的安全；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。

政务外网积极响应国家商用密码的推进计划，发布密码应用系列标准，并牵头制定了一项密码应用方面的国家标准 GB/T 32922—2016《信息安全技术 IPSec VPN 安全接入基本要求与实施指南》，明确了采用 IPSec VPN 技术实现安全接入的场景，提出了 IPSec VPN 安全接入应用过程中有关网关、客户端以及安全管理等方面的要

求。政务外网公共安全基础支撑方面，政务 CA 已基本覆盖全国各省、自治区和直辖市。政务 CA 在建设之初，仅支持 RSA 密码算法；根据国家政策要求，政务外网升级建设了支持商用密码算法的密钥管理中心基础设施。

此外，随着斯诺登事件和“邮件门”事件的曝光，我国党政部门也越来越意识到邮件安全的重要性。基于商用密码的全国政务安全邮件公共服务将逐步构建，采用国密算法实现邮件的安全交互，为政务部门人员之间的邮件往来增加安全保障。公共应用和部门专有应用系统，均展现出采用商用密码算法进行保护的趋势，商用密码在政务安全领域拥有极为广阔的应用空间。

3. 教医旅领域

在教育领域，商用密码主要应用于全国教育管理信息化业务和教育卡等方面。教育部在国家教育管理公共服务平台上全面推进个人数字证书、教育数据安全防护以及电子签章等基于商用密码技术应用，教育部办公厅关于印发的《2019 年教育信息化和网络安全工作要点》第 15 条明确规定加强教育系统密码应用于管理：“制定《教育行业密码应用实施方案（2018—2022）》，加强密码宣传教育和业务培训工作，逐步提高密评工作水平，开展教育行业密评服务，推进国家教育管理信息系统密码应用，进一步做好商用密码推广使用工作。”目前，全国中小学生学籍信息管理等多个全国性教育管理信息系统已应用商用密码数字证书，建立了数据存储加密

和传输加密等平台应用。教育电子身份认证服务体系方面，2013年，教育部立项“教育数字认证系统”子项目，对教育CA系统进行SM2的升级改造，完成教育CA软硬件基础环境和相关支撑体系建设，正在推动覆盖到大中小学的电子身份认证。**教育将在总体设计、标准制定、系统建设、应用试点等方面，全面采用商用密码。**2021年3月教育部发布的《教育部关于加强新时代教育管理信息化工作的通知》中提出：“构建数字认证体系。完善教育数字认证基础支撑体系总体规划，建立统一的教育系统密码基础设施和支撑平台。建设基于“一校一码、一人一号”的数字认证互联互通互认体系，实现跨平台的单点登录。推动以智能终端为载体的多因子认证，探索手机短信、移动协同签名等多种认证方式，提升服务体验。数字认证使用的密码技术和产品应符合国家密码管理部门要求。探索推动区块链技术在招生考试、学历认证、学分互认、求职就业等领域的应用，提高数字认证可信性。”由此可见，未来很长一段时间，密码应用将与教育相关场景数据安全防护逐步融合。

在医疗健康领域，居民健康卡有效带动医药健康行业商用密码的应用。2012年开始发行采用商用密码算法的居民健康卡，2017年则开始发行电子健康卡，并使用商用密码 SM2、SM3、SM4算法生成密钥和身份验证。同时，医疗健康领域的人口健康信息平台、数字证书互信互认系统、电子证照（执照）、医院电子病历系统都采用了商用密码算法。医疗健康重要信息系统将加速应用密码技术，实现数字证书身份认证和责任认定机制，保障公共卫生重要疫

情数据、卫生计生统计上报数据的完整性和机密性，实现医疗卫生机构电子病历与电子处方的真实合法性，未来5-10年，医药健康行业各领域应用商用密码的场景也将会愈加普遍。

在交通运输领域，根据交通运输行业重要领域密码应用推进总体规划，以建设行业密钥管理系统和认证服务为支撑，以高速公路不停车收费（ETC）系统、交通一卡通系统及电子证照系统示范、试点工程为依托，推进密码技术在交通运输行业的应用。2015年，交通运输行业基于SM4算法的对称密钥管理系统和证书认证系统正式启用；2017年，基于SM2算法的交通一卡通证书认证系统和密钥管理系统正式启用，为行业重要领域的跨地域互通、跨行业互通提供了坚实的安全保障。2021年3月21日公开的《交通运输部办公厅关于加快推广应用道路运输电子证照提升数字化服务与监管能力的通知》中提出了“统一开发电子证照系统。根据相关标准规范要求，采用国产密码算法技术，建设开发部级电子证照系统，同时推进与部级运政系统、网上便民运政系统、部移动客户端和微信公众号、国家政务服务平台等相关信息系统的对接工作。统一开发省级电子证照系统基础软件。”的主要任务。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，使城市生活更加信息化、便捷化、安全化，推动智慧城市发展，随着城市数字化转型的不断推进，商用密码应用在交通运输等领域将迎来更大机会。

4. 其他重要领域

商用密码在工业互联网领域大有可为。工业互联网平台面向制造业数字化、网络化、智能化需求，构建基于海量数据采集、汇聚、分析的服务体系。作为一个新兴事物，工业互联网的安全边界不清晰，安全责任不够明确，迫切需要商用密码的融入。综合来看，主要是以下几方面的应用。

一是认证和鉴别。认证和鉴别贯穿工业互联网平台的各个层次，在工业互联网边缘接入层，需要采用白名单机制对接入的设备和用户进行身份认证和鉴别；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。我国的 SM2 椭圆曲线公钥密码算法秘钥生成速度快，安全性高，可以很好实现身份认证和鉴别功能。

二是账户管理。设备和用户账户管理贯穿工业互联网平台，其中账号和口令的安全关系到用户对于平台的信任度，一旦账户信息发生泄漏，对于平台的口碑将会产生负面影响。可以采用商用密码算法，实现对账户和用户的加密存储。

三是通信保护。工业互联网平台应确保通信的保密性、完整性、不可否认和不可篡改性，比如在 PaaS 层进行数据挖掘和分析时，要保证原始数据不被篡改，且不被泄露，这就需要对通信过程中的数据实施保护。在平台通信过程中使用商用密码算法，可确保工业互联网平台通信过程安全、可靠、可控，保障数据安全。

商用密码在电力等能源领域的应用不断得到推广。国家电网系统从安全芯片到相关设备，目前已完全采用商用密码技术和产品。用电采集系统是商用密码在电力系统的首次规模化应用，体现了商用密码与用电信息安全控制的紧密结合。在上海世博会和纪念抗战胜利70周年大阅兵期间，用电采集系统在电力保障中发挥了关键作用，对维护社会稳定、支持阶梯电价政策、推动节能减排等方面具有重要作用。国家电网公司用电信息密码基础设施，为用电信息采集系统提供全方位的密码服务，已安全可靠运行多年，有力保障了用电采集系统的安全稳定高效运行。基于商用密码的专用安全芯片、电能计量密码机等密码产品正大规模应用于电力行业，也将直接或间接创造大量经济效益。

此外，**商用密码也在基础信息网络、社保、移动办公、视频监控、网联汽车、广播电视、物联网等越来越多的领域得到了应用，相关应用需求不断得到激发。**对于密码行业来讲，一方面需要从行业需求出发，提供针对性更强的服务；另一方面需要从独立自主的角度出发，实现国密的技术突破及广泛应用。

二、多重因素驱动产业发展

密码应用的普及、推进、评估和监督检查，已成为密码产业的重点工作。国家“十四五”规划指出：“发展数字经济，推进数字产业化和产业数字化，推动数字经济和实体经济深度融合”。面向“十四五”，在产业挑战、高质量升级、实战合规等诸多因素影响下，密码作为数字经济的“安全基因”，正迎来前所未有的叠加演进和发展升级。

（一）密码技术演进促进产业发展

1. 密码产品形态“软硬协同”

FIPS 密码模块安全评估认证是全球目前接受度最为广泛的密码认证体系。国外密码产品较我国起步早，其产品体系更为成熟，参与 FIPS 认证的密码产品类型、构成、能够代表先进密码体系发展趋势，具有重要参考借鉴意义。

从 NIST 官方网站上查询到截止到 2021 年 6 月底，共有 3959 款产品获得了 FIPS140-1 或 FIPS140-2 的不同安全级别认证，其中 1288 件在有效状态，硬件形态占比 56.6%，软件形态占比 39.4%，两种形态的密码产品发展比较均衡，软硬结合，从而更好发挥安全产品的防护作用，软件密码产品灵活满足多种应用场景，包括云端、移动端、IoT 等应用场景密码的使用需求。值得一提的是，国外市场具有软件固件产品的厂商占比超过 50%，FIPS 密码模块产品定级情况中，软件产品也能通过较高安全级别，有若干纯软件密码产品

通过了二级认证。通过二级认证的软件产品类型包含密码应用安全中间件产品、操作系统内核密码模块、网络设备软件密码模块等。

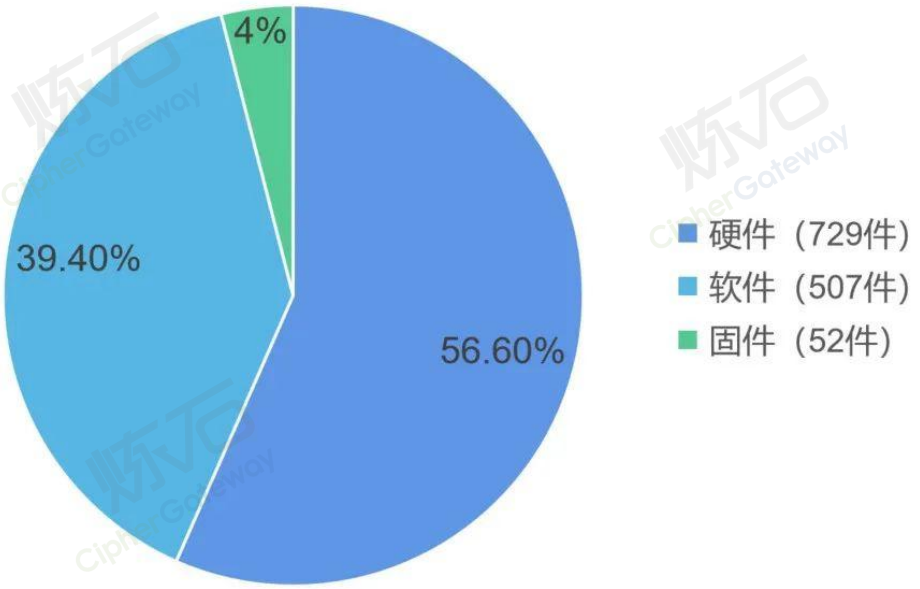

图 1：密码产品形态比例分布概览（FIPS）

国外 FIPS 密码体系较我国起步更早，其产品体系更为成熟，FIPS 密码产品类型构成能够代表先进密码体系的发展趋势。反观我国，**截至 2021 年 4 月，通过国家密码管理局审批的商用密码通用产品有 2400 余款，形成了从芯片、板卡、整机到系统和服务的完整产业链。但是，我国密码市场硬件产品占比超九成，多数为特定领域专用产品，软件形态产品占比不超过 5%，距离国外的 39.4% 依然有较大差距，**可见，我国仍以硬件产品为主，这种供给结构与国外软硬产品均衡、产品通用性较强等特征形成鲜明对比。

当前，我国密码产品种类齐全，形成了从芯片、板卡、整机到系统和服务的完整产业链。然而，我国密码市场硬件产品占比相对

较大，多数为特定领域专用产品，且同质化较严重，软件产品占比偏低。

此外，在密码硬件主导的阶段，在当前产业工艺水平限制、服务器密码机网络延时与带宽限制下，性能提升逐步逼近极限，而软件性能提升方面仍有较大优化空间，这恰恰为从“软硬协同”层面提升性能提供了方向。有数据显示，硬件架构的每一个数量级的性能提升潜力，通过“软硬协同”能带来两个数量级的整体性能提升。当前，商用密码产业涉及以基础密码设备为主的硬件产品及安全信息系统为主的软件产品。发展尚未成熟的软件产品市场是未来实现性能大幅提升的重点探索领域。

2021 年 3 月 9 日，GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》（以下简称“国标”）国家标准正式发布，实现了行业标准上升为国家标准，其中对密码软件要求进行明确，**GM/T 0054-2018《信息系统密码应用基本要求》（以下简称“行标”）的指标“密码模块实现”改进为国标“密码产品”，并增加了“密码服务”。“密码产品”方面的基本要求相比行标有重要变化，信息系统等级保护第三级安全要求，从行标的“宜采用 GM/T 0028 三级及以上”，放宽为国标的“应达到 GB/T 37092 二级及以上”；对等级保护第二级安全要求，从行标的“宜采用 GM/T 0028 二级及以上”，放宽为国标的“应达到 GB/T 37092 一级及以上”。（注：GB/T 37092 是 GM/T 0028 密码模块安全技术要求的国标版本），放宽了密码产品的入市标准，将进一步促进密码软件市场发展。**《商

用密码应用与安全性评估》发布，我国商用密码服务能力逐渐提升，商用密码产业结构逐渐优化，利好软件形态密码产品发展。

2. 密码发展应用“危机并存”

时代要求方面，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、智慧城市等领域融入。不同领域的应用诉求对密码产品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。目前一些新业态的密码产品应用面临与本身的设备及系统的耦合程度不够、高性能需求与低效算法实现间难以协调以及应用软件密码集成门槛高等挑战，使得商用密码产品难以完美契合到基础设施和行业应用中。

国产化替代方面，目前我国仍然存在依赖国外密码产品、底层平台多使用国外密码协议的情况，核心基础芯片主导权掌握在国外管理者手中，密码应用随时面临“卡脖子”风险。商用密码在国产化替代方面还存在诸多不友好现象，产品技术和安全可靠应用契合度不佳，完全替代国外产品协议仍有难度。

密码检测评估方面，密码检测评估体系主要包括商用密码产品检测和商用密码应用安全性评估。我国目前已出台一系列密码产品技术和检测标准规范，商用密码产品检测工作基本实现有章可依、有据可循。但商用密码安全性评估仍处于初步阶段，制度建设尚有

空缺、实践能力有待提升。同时，各应用领域信息化发展水平不一、不同垂直领域的密码应用评估体系建设也应当有所侧重。

密码人才培养方面，一是我国密码人才培养尚未形成系统性顶层规划和设计，人才数量与质量、结构比例与用人单位实际需求不匹配。在密码及网络安全人才培养和产学研合作模式方面，需要科学的顶层规划设计加以引导，在企业的发展和高校人才的培养之间找到平衡点。二是大专院校等高校中，更侧重密码算法和密码协议的理论方面，在应用、实现、产品和测评等方面有所欠缺，相关高校应该建立系统性的教育体系，保证人才在密码方面的综合素质。三是商用密码应用于实际业务系统或平台紧密耦合，牵扯背景知识较多，涵盖密码标准、密码算法、密钥管理等内容，对密码从业人员的要求较高，需要企业内部体系化的人才培养计划。

不管是时代发展过程中的新业态方面，还是国产化替代、密码检测评估以及人才培养等方面，都存在大量危机与矛盾需要解决，但“危”与“机”往往相伴而生，国家和密码厂商在解决这些问题的过程中，必然会激发新的产业需求，新的历史机遇，这对勇于创新、踏实发展以及积极响应国家标准和要求的密码厂商来讲,是弯道超车和快速发展的好机会。

（二）供给质量升级拉动产业发展

2020 年 12 月 11 日中央政治局会议要求：“要扭住供给侧结构性改革，同时注重需求侧改革，打通堵点，补齐短板，贯通生产、

分配、流通、消费各环节，形成需求牵引供给、供给创造需求的更高水平动态平衡，提升国民经济体系整体效能。要整体推进改革开放，强化国家战略科技力量，增强产业链供应链自主可控能力。”当然，密码产业也需形成“需求牵引供给、供给创造需求的更高水平动态平衡”。

1. 高质量供给夯实基础支撑

一直以来，国家大力推广密码，社会也急需密码，密码测评认证体系和高质量密码供给体系以构建国家和社会之间的供需桥梁。目前，我国密码测评认证体系稳步有序发展，创新驱动的高质量密码供给也在逐步增强。

高质量密码供给关键在于三方面：一是密码能用，SM 系列算法性能持续优化，使得替换国外密码算法后不影响业务效率，同时完善场景覆盖，逐步优化软件形态产品，覆盖云端、移动端、物联网端等新型场景。二是密码好用，在降低使用门槛，为用户提供易用的密码数据安全产品的同时，降低集成难度，对密码接口进行业务级封装，提炼密码中间件，让应用软件开发者更便于使用；三是密码好管，能够结合企业实际业务需求，匹配密钥、加密策略、降低实施维护难度，满足合规管理要求，提供融入业务流程的密码安全能力。

图 2：高质量密码需求分析说明

高质量密码升级加速也将激发产业创新能力。一是商用密码技术趋于创新。2020 年 3 月，中共中央政治局常务委员会召开会议提出，加快 5G 网络、数据中心等新型基础设施建设进度，随着新基建等基础设施的加速构建，未来将有数以万亿计的新设备接入网络，人工智能、边缘计算、区块链等新技术将加速与传统产业融合，利用我国新基建发展的安全需求，未来网络空间安全离不开以密码为基础的安全可控技术体系，从而带动核心技术的突破与跨越。二是商用密码产品趋于创新。新技术与传统产业融合，未来将面对 5G 的超高速网络以及超大规模的网络空间，对于超高速网络以及超大规模网络空间需要高性能密码产品加快传统密码运算效率。三是商用密码服务模式趋于创新，服务将成为产业竞争力的核心指标之一，面对大规模的网络空间需要专业化、平台化的密码服务。

2. 新场景应用赋能数字经济

新场景下的“高质量密码应用”，将发挥在促进产业数字化转型升级中的独特作用。具体而言，包括：

瞄准消费升级方向：随着信息化消费的不断发展，个人隐私泄露成为社会高度关注的共同话题。使用密码产品实现个人信息的防护和数据资产的保全，构建起基于密码的个人信用体系，将为密码产业带来由个人消费者构成的广阔市场前景，得到更强劲的发展动力。

瞄准产业升级方向：新基建是促进产业升级的重要方向，也是国家和社会运行的重要物质基础，尤其是在5G、工业互联网、数据中心等关键信息基础设施领域的安全保障显得尤为重要，密码的应用将成为“刚需”，上述领域的实际安全需求也将为密码产业发展提供指引和方向。

瞄准治理能力升级方向：随着智慧城市、数字货币、电子政务、电子商务等新型数字经济模式的不断涌现，社会经济数字化转型已成为主流趋势，相应的数字化治理能力也成为国家治理能力提升的重要内容，而数字化治理的核心问题在于数据信息的安全治理，应用密码保障数据的安全，为社会治理保驾护航，也将成为密码产业发展和产品服务创新的重要方向。

随着各行业信息技术的发展，互联网技术、云计算大数据技术、物联网技术等逐步应用到重要信息系统，在给系统带来便利的同时也带来了安全性挑战，为了增强系统的安全性，防止重要信息泄露，应对新的攻击手段，需要开展互联网密码体系建设、重要信息系统密码应用纵深体系建设、云计算大数据环境下隐私保护体系建设、物联网环境下轻量级密码应用技术体系建设等基于新技术的密码保障体系。目前，随着密码技术的发展以及技术演进，防护重点已经从网络转移到数据，但如何解决密码性能问题、密码安全性问题、密码合规性问题以及多场景适应性问题，都将成为一种挑战。

（三）安全实战合规引领产业发展

密码市场蓬勃发展，离不开密码实战与合规并举的产业导向。

1. 实战合规并举成发展动力

1）实战是密码技术应用的内在需求

实战层面，密码技术能够抵御外部黑客攻击、防止内部人员窃取。当下的数据泄露事件频发，面对新安全挑战与新合规要求，**企业安全防护体系正在从“以网络为中心的安全”，升级到“侧重以数据为中心的安全”**。通过密码技术能够实现对核心数据的机密性和完整性保护，将明文变为密文，配合健壮的密钥管理体系，可以防止明文存储引起的数据泄密、突破边界防护的外部黑客攻击以及来自于内部越权用户的数据窃取，从而在根本上解决敏感数据泄漏

带来的业务风险问题。商用密码产业的发展依托信息安全产业为基础，并长期存在依存关系，安全的迫切性和重要性为商用密码行业和企业的发展带来广阔空间。

随着云计算、大数据、物联网、人工智能、5G等数字经济新技术的发展，密码技术应用也不断深入，最终实现密码基础设施的创新性应用，这也对用户合规和攻防对抗提出极高要求。对此，**亟需构建以密评合规为起点，以真实对抗结果为导向，构建敏捷实施、细粒度防护、机制可靠的密码实战化防护体系。**通过将加密通信技术、加密存储技术、芯片等密码核心技术研发，将密码融入系统组件以及通信协议、存储协议、数据处理协议、业务交互协议中，使基于密码的安全机制成为其内生要素和必选环节，引领信息领域关键核心技术的创新与突破，进一步协同创新保障信息安全。

2）合规为密码技术推广提供加速引擎

合规层面，以密评为核心的综合性合规，是推广密码技术直接有效的手段。《2021商用密码创新应用指南》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**”。当前的应用系统复杂多样，丰富的密码应用场景对用户运维和攻防对抗提出极高要求，而密码合规将偶发的、高技术水平的对抗风险，转化成常态的、可重复验证的非对抗风险，显著降低了密码使用门槛。同时密码合规也解决了“外部经济学”中的消费方与受益方不一致问题，强制要求信息服务运营商加强数据保护。在实际应用中，合规的内

涵包括两个方面：一是网络信息系统使用的密码算法、密码技术是否符合法律法规的规定和密码相关标准；二是使用的密码产品和密码服务是否由具备资格的机构认证合格。

监管侧的密集发力，推动商用密码领域的持续健康发展。长远来看，一方面将加速适应我国在当今国际环境下，自主信息安全和发展的新形势新要求，发挥密码技术在维护信息安全与促进发展综合平衡中的重要支撑作用；另一方面伴随着监管侧红利持续释放，密码产业体系将呈现与数字化生态深度融合新走势，涉密保护相关企业将充分受益。

具体来看，红利内容涵盖：

- 破除商用密码应用推进过程中的难点，产业发展进入快车道和窗口期，密码企业迎来产业红利期；
- 推动密码大中小企业融通发展，鼓励密码骨干企业整合密码创新链、产业链、价值链，建立密码技术研发、标准验证、成果转化平台，畅通创新能力对接转化渠道；
- 平等对待商用密码所有从业单位，鼓励与外商之间基于商业规则的合作交流，由市场配置资源，以产业能力和产品质量决定市场竞争力；
- 培育细分领域密码企业龙头，鼓励以专业化分工、共享研发等方式与大企业合作，构建覆盖理论、算法、芯片、产品、系统、服务的完整密码产业供给链。

可以想象，未来密码产品与服务、密码技术将更广泛地应用到重要领域和关键信息的基础设施当中，并逐步向普通数字化产品渗透，成为新时代下数据安全、网络安全、信息安全最重要的守护者。

3）实战合规共同驱动新密码市场

企业安全建设更加注重结果导向，密码市场正演化为“实战防护、国密合规、信创合规”分层次叠加的新格局。从实战需求看，日趋严峻的网络安全威胁让企业面临业务风险，数字产业化迫切需要密码安全能力，而产业数字化转型带来密码新需求，例如互联网医院需要强身份鉴别和数字签名，这些都要求企业增强以密码技术为核心的安全建设。从合规需求看，以密码应用与安全性评估（简称“密评”）为主要抓手、并结合信创的系统化合规将会持续深入，《网络安全法》《数据安全法》《个人信息保护法（征求意见稿）》《关键信息基础设施安全保护条例（征求意见稿）》等也在持续带动企业使用密码技术的新需求。在不同场景需求的共同驱动下，实战与合规叠加推动的新密码应用市场正在加速形成。

综合来看，合规监管与实战防护共同驱动新密码市场表现在：一方面以实战为导向的需求市场被充分激活，另一方面“密码新合规”拉动新需求。用户需要以合规为起点，以真实对抗结果为导向，进一步构建有效的密码实战化防护体系。进一步来看，密码实战化防护指标包含三部分：第一，应满足密码防护能力融入业务流程，提供多场景细粒度有效防护；第二，能够融合访问控制、审计等其

他安全技术，实现安全机制可靠有效运行；第三，支持敏捷部署、实施周期短、对业务影响小等特性。

2. 密码市场迎时代发展契机

密码产业发展机遇前所未有，全球的网络安全产业还未发展到成熟状态，投资与创业机会将聚焦网络安全领域，未来可能催生万亿级别的大市场。目前，我国网络安全投入还很不够，相比于西方发达国家，我国尚有增长空间，这既是短板也是市场。按照国家有关部署，金融和重要领域正在强化密码应用，大量网络和信息系统涉及密码保障系统的新建或改造，市场空间很大。可以说，密码应用将会带动更多安全投入，拓展更大安全市场空间。谁投入早，创新多，谁成为网络安全行业龙头的可能就更大。对此，产业单位要有更加积极的认识。

从产业市场来看，首先，《中华人民共和国密码法》出台造就商用密码发展黄金窗口期，密码建设从国家层面将迎来最好时机，SM 算法将加速在上中下游的全面融合和推广应用。其次，新技术、新业态成就商用密码发展新机遇，云计算、物联网、大数据、5G 等信息技术升级可以促进算法协议以更低成本完成升级工作，尤其是信创产业带来的历史契机。密码既是信创的重要组成部分，又为信创提供安全保障。最后，我国具有充沛的技术人才保障，以及“一带一路”巨大市场潜力，为商用密码发展奠定重要基础。

从商业市场来看，兼并收购趋于频繁，窗口期来临。商用密码产业目前产品类别较多，行业较为分散，而预计该行业将继续以创新为主导，频繁的收购和战略联盟将成为参与者增强行业存在感的关键战略。同时，资本对头部企业的偏好和集中以及行业内小规模的兼并收购事件预示着行业逐渐走向集中，马太效应初步显现。**目前的商用密码产业具有“小而多”的特点，从行业发展的角度来讲，这个行业正处于“最初阶段”，正是布局重大机会的关键时期。**

当下，密码技术正在以前所未有的广度和深度与信息技术相互促进、融合发展，为网络空间的云计算、大数据、物联网等应用保驾护航；另一方面，密码服务也正在广泛覆盖政府、企业、组织和民众，并逐步成为全民服务。随着时代不断发展，密码技术的应用场景将愈加复杂且繁多，一种安全技术已难以满足相关业务需求，**因此在实战化防护中，“以密码技术为核心、多种安全技术相互融合”的密码安全一体化正在成为安全建设主思路。**可以预见，集密码和访问控制、审计等多种安全保密技术一体化的厂商，将有望在未来密码市场中脱颖而出。

（四） 数据安全挑战助推产业发展

1. 中国将成为全球最大数据圈

新冠疫情加速了人们的日常生活及经济等领域向数字化转型，并在新出行方式、个性化医疗、远程办公等方面落地更多应用并使人受益，数字经济已成为全球经济发展的重要组成部分。与此同时，

持续增加的数据资源正逐步成为一种潜在增长、可持续累积的社会资源。

2019 年，全球数字经济规模达到 31.8 万亿美元。从单一国家经济体来看，美国仍然走在全球数字经济前列，以 13.1 万亿美元的规模排名全球第一。而中国经过多年的市场化发展，配以技术创新和模式创新，以 5.2 万亿美元的经济规模排名世界第二。德国、日本、英 国、法国分列三至六名，数字经济规模合计超过 3 万亿美元。韩国、印度、加拿大、墨西哥、巴西、俄罗斯、新加坡、印度尼西 亚、比利时等 17 国数字经济规模介于 1000 亿至 8000 亿美元之间，另有 24 国的数字经济规模不足 1000 亿美元。随着时代发展，全球层面的数字经济规模还会继续呈现较长时间的增长趋势，数据资源也将成为各国家重视的战略资源。

图 3：全球数字经济规模分布图

据著名咨询机构 IDC 预测，2025 年全球数据量将高达 175ZB。其中，中国数据量增速最为迅猛，预计 2025 年将增至 48.6ZB，占全球数据圈的 27.8%，平均每年增长的速度比全球平均水平快 3%，将成为全球最大的数据圈（数据圈是指被创建、采集或是复制的数据集合）。（数据来源：《数据安全白皮书》<2021 年由国家工信安全中心联合华为发布>）

大量且持续爆发增长的数据必然存在数据泄露等潜在危险，数据作为支撑国家实现创新发展、重塑人们生活，以及国家经济社会发展的关键要素之一，实现数据的安全防护是需要慎重对待的重中之重。在全球合作日益密切的今天，数据安全对于提升用户信心、保护数据、促进数字经济发展有着重要意义。

2. 密码技术应用保障数据安全

数据安全的难点，在于如何对流转中的数据主动实施加密等保护，确保数据不被泄露或篡改，这里的数据包括结构化与非结构化等类型。结构化数据一般是指可以使用关系型数据库存储和表示，表现为二维形式的数据，一般来讲，结构化数据也就是传统数据库中的数据形式；非结构化数据，就是指没有固定结构的数据，包括各种文档、图片、视频、音频等。

传统的“数据库加密”往往体现为密文数据存储到数据库后的情形，一般局限于结构化数据，而在企业实战化场景中，数据库只

是数据处理的一个环节，因此，传统的“数据库存储加密”是“数据存储加密”的子集。

当前数据产业面临的威胁和风险不仅针对数据本身，也包括承载数据的关键信息基础设施，因此，我们需要以数据为中心，构建全方位的数据安全治理体系，保护数据资源，在风险可控的基础上实现数据的增值和自由流转。从这个角度出发，沿着数据流转路径，在典型 B/S 三层信息系统架构的多个数据业务处理点基础上，综合业内数据加密技术现状，选取了 10 种代表性的存储加密技术。

十种数据存储加密技术在应用场景以及优势挑战方面各有侧重点，DLP 终端加密技术侧重于企业 PC 端的数据安全防护；CASB 代理网关、应用内加密（集成密码 SDK）、应用内加密（AOE 面向切面加密）侧重于企业应用服务器端的数据安全防护；数据库加密网关、数据库外挂加密、TDE 透明数据加密、UDF 用户自定义函数加密则侧重于数据库端的数据安全防护；TFE 透明文件加密、FDE 全磁盘加密则侧重于文件系统数据安全防护。

表 4：十种典型数据存储加密技术对比

加密技术	部署位置	加密粒度	性能	防 DBA	数据库复杂计算	实施成本	可靠性
DLP 终端加密	终端	文件	中	/	/	中	中
CASB 代理网关	终端-应用服务器间	文件/字段	中	支持	影响	高	低
应用内加密（集成密码 SDK）	应用服务器	文件/字段	高	支持	影响	高	高
应用内加密（AOE 面向切面加密）	应用服务器	文件/字段	高	支持	影响	低	高
数据库加密网关	应用服务器-数据库之间	字段	中	支持	影响	中	中
数据库外挂加密	数据库	字段	低	支持	影响	中	中

TDE 透明数据加密	数据库	字段/表空间	高	不支持	不影响	低	中
UDF 用户自定义函数加密	数据库	字段	中	不支持	不影响	高	高
TFE 透明文件加密	文件系统	文件	中	不支持	不影响	低	高
FDE 全磁盘加密	文件系统	磁盘/卷	高	不支持	不影响	低	高

在实际应用中，要结合用户场景和适用性需求，选择一种或者组合多种存储加密技术，优势互补，并结合其他安全技术，打造“以密码技术为核心，访问控制、审计等多种安全技术相互融合”的数据安全防护体系，保障数据安全。

可以说，密码技术是保障数据安全的必经之路，且关系扭结缠绕、不可分割。随着数据要素爆发式增长的趋势不可逆转，也将会带动“应用密码技术保障数据安全”的相关需求。中国在逐渐成为最大数据圈的过程中，将会持续助推密码产业的发展。

三、密码产业发展趋势分析

密码产业持续健康发展是大势所趋，这对打造以密码为基础的网络安全体系、构建网络空间安全保障体系以及维护国家网络空间安全具有重要意义，我国网络信息安全防护迎来从被动防御向主动免疫的战略转变。因此，提前判断密码产业发展趋势并进行布局是密码厂商在激烈市场竞争中能否占据先机的关键点之一。

（一） 市场蓬勃发展

1. 密码国产化替代正加速

密码的国产化替代是大势所趋。随着密码法的实施以及国家对国产化的支持，底层芯片、卡、装置性能要求将不断提高，引导产品技术和产品大幅度性能升级，国产密码的“高质量升级”成为时代的需求。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、实现方面均有独特优势和特点，能够有力支撑商用密码的产业化、规模化发展。面对激烈的国际竞争，将国外产品进一步替换为国产产品的趋势不可逆反，商用密码产品将大量国产化。

2. 信创带来新的历史机遇

信创带来历史机遇。信创的核心在于，通过行业应用拉动构建国产化信息技术软硬件底层架构体系和全周期生态体系，解决核心技术关键环节“卡脖子”问题。芯片、整机、操作系统、数据库、

中间件等技术封锁下，中国信创产业必将迎来发展黄金期。据智库机构预计，未来三年市场总规模有望达到上万亿元人民币。国产密码本身就是信创产业的核心部分，密码又能为蓬勃发展的信创产业保驾护航，所以，适配优化信创平台、在信创安全体系中全面应用密码等新需求对密码产品形态会产生深刻影响。

3. 市场呈现分层次多样化

密码市场的内涵将愈加丰富合理。过去，密码市场分为监管市场和商业市场两部分。监管市场由合规手段强制推动，用户规模小但市场占比庞大，在过去占据密码市场的主导地位。而商业市场用户规模数倍于监管市场，但过去市场体量不足监管市场的一半。从产业规模看，当前密码产业规模仅占信息产业的千分之三，仍有较大发展空间。同时，密码产业以众多中小型密码企业为主，有待诞生真正的龙头企业。**随着时代发展，未来密码市场的内涵，将从单一的“国密合规”变得更加丰富和细化，并呈现出分层次叠加的多样化特征，即“实战防护、密评合规、信创合规”。**

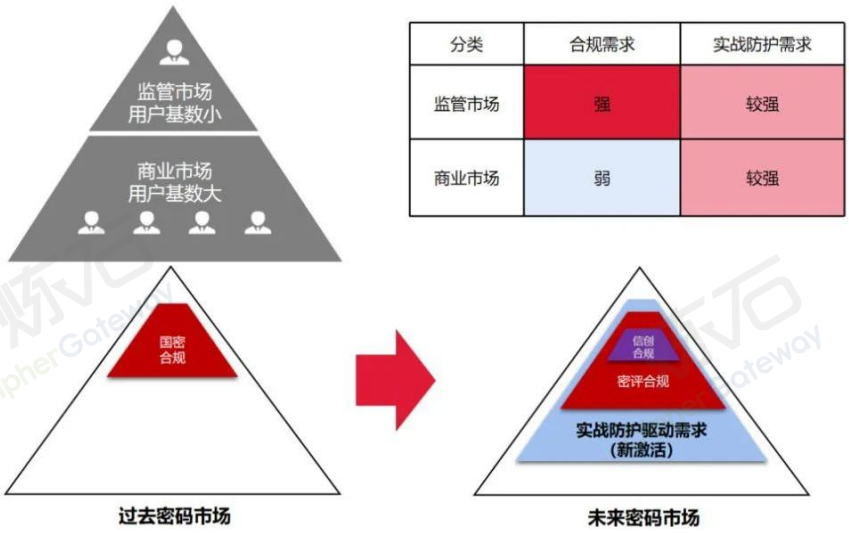

图 4：密码市场内涵演进方向说明

4. 密码市场发展规模预测

未来几年，商用密码产业将保持高增长率。面向“十四五”时期，在密码技术、需求和监管等诸多因素影响下，密码产业供给侧正迎来前所未有的叠加演进和发展升级。密码市场将迎来新发展机遇，据预测，未来几年，商用密码产业都将迎来高增长，2023 年我国商用密码规模预计将超过 900 亿。

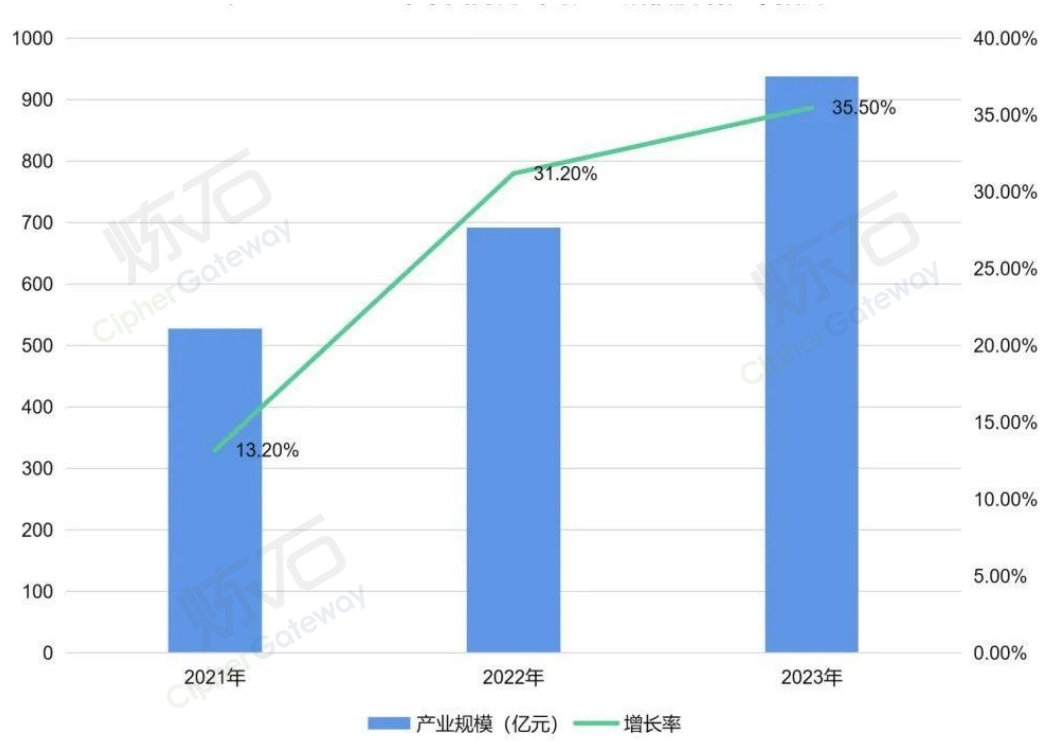

图 5：2021-2023 年商用密码产业规模及增长率预测

数据来源：《2020-2021 中国商用密码产业发展报告》

（二）技术加速创新

1. 数据要素激励密码技术创新

数据作为新的生产要素将全面赋能密码创新发展。数据生产要素具备自身特性，难以从技术上分割使用权和所有权，而通过创新的密码技术和方案可实现多个企业或机构间的数据共享互联，具有广阔发展空间。一是密码技术的发展创新，如隐私增强计算技术的联邦学习、安全多方计算、机密计算、差分隐私、同态加密等，实现“数据可用不可见”；二是新兴信息技术的密码应用场景的创新，例如区块链，

就是加密技术、分布式网络、智能合约等多种技术集成的新型数据库软件，通过数据透明、不易篡改、可追溯，有望解决数据生产要素化的信任和安全问题；三是传统密码技术和多种安全保密技术的融合创新，使数据在共享时实现“最少可用原则”和“最小权限原则”，让数据在业务系统中实现共享与安全兼得。

2. 密码能力紧密融入业务应用

密码和业务应用融合。传统密码产品开发改造应用的密码集成模式门槛高、周期长、风险大，用户面临“难用、难管”，很难将密码能力深入融合到信息系统，而业务应用改造也正是密码防护和密评整改的难点，与金融、交通、医疗等行业应用场景紧密结合的密码需求也会更加细化。业内提出基于“面向切面安全”的密码中间件模式，将安全与业务在技术上解耦、但又在能力上融合交织，提供轻量级改造应用的密码应用实施模式，有效防护企业应用与数据，让密码“好用、好管”。

3. 全生态亟待密码实战化覆盖

商用密码的健壮发展亦离不开信息技术整体生态的支撑，按技术链条划分，密码技术链可大致分为上、中、下游三个环节。

上游包括密码算法标准、网络协议及规范，如 IETF RFC 等；中游包括网络协议栈实现、软件开发工具链，以及硬件密码模块和驱动、CPU 密码指令集支持等；下游包括各种应用软件，涉及基础应用软件、行业应用软件等环节。对于整个产业链来说，下游各类

应用软件内含丰富的重要数据，包括姓名、身份证号、银行卡号等敏感信息，因此越往下游走，密码应用保障个人信息安全将愈加重要。下游行业总体的信息化进程仍处于快速发展阶段，信息化发展正促进信息安全及密码产品、集成及服务需求持续增长。

目前，技术生态环节存在商用密码覆盖盲区。上游的网络层协议及规范尚不支持 SM 算法。中游的通用协议栈实现与开发工具链没有充分支持 SM 算法。上中游盲区导致下游应用软件普遍不支持 SM 算法。

因此，需要增强技术生态覆盖，全面打造商用密码实战化。针对上游通过 RFC 等规范制定，布局 SM 算法进入标准和协议；针对中游，通过多个重点工程，抓住协议栈和工具链；针对特定行业或领域，结合中国市场，联合多家国际主导厂商，以密码合规等市场准入条件为契机，反向推动上游协议接纳 SM 算法；针对下游，结合法律法规和密评整改等手段，从下游应用软件反向推动，依赖下游广泛应用生态发挥出商用密码的巨大价值，不断开拓商业密码市场和国际市场，做强密码产业生态。

4. 密码安全一体化成为主思路

安全一体化的密码技术的创新和发展。数据加密只是把明文安全问题转移到密钥安全问题，但是如果没有结合业务的密钥访问控制，防护价值非常有限。过去，由于市场准入等因素，密码和安全技术在建设落地时相对分离，但是，随着密码“放管服”落实以及监管侧改革，“以密码技术为核心、多种安全技术相互融合”将成为主流思路，

并统筹实施等保与密评。通过加密技术，为流转的数据重新定义了虚拟防护边界，在边界上施加访问控制、审计等技术，实现“防绕过的访问控制”以及“高置信度审计”，进一步集成企业 IAM 身份认证管理，打造同时满足传统场景和零信任场景的有效数据保护。

（三）产品叠加演进

1. 密码交付向产品加服务演进

多重需求拉动密码服务蓬勃发展。过去，合规主导的密码市场侧重产品本身，而当下企业更注重有效防护，要将安全产品转化为有效防护能力，需要提供服务，尤其是结合安全运维。所以，密码交付形态正在从“以产品为主”演进为“产品与服务相结合”。**密码企业交付模式从单纯的产品交付转变到产品与服务综合性交付模式，“一站式”满足客户多样化需求。**

2. 产品软硬均衡支撑自主可控

产品形态的“软硬兼备”将成未来的主流。当下，我国软硬件密码产品的发展并不均衡，亟待软件密码产品的技术创新，从目前国际密码产品的发展情况来看，国内密码产品的走向也将会朝着“软硬结合，以软为主”的方向发展，预计未来国内密码产业软硬件格局将与美国结构趋于一致：侧重软件形态为主的软硬件均衡发展。因此，未来密码软件应用市场将迎来爆发，从机卡 Key 等强调安全合

规型，到“识别和防护”的实战化安全产品将百花齐放，内嵌式密码产品或将成为市场主流。

3. 密码产品强化自身安全防护

加强自身安全保护和形态多样化的密码产品创新和发展。这是威胁对抗常态化带来的必然要求，密码厂商会更加重视形态多样化的密码产品研发、生产和全生命周期中的安全管理，同时，监管机构持续完善密码产品认证体系和优化密码产品的安全性检测认证要求，用“安全的密码产品”有效保护企业数字化安全。

4. 亟待一体化的密码支撑体系

一体化的密码平台集约建设。企业业务需求持续变化决定了企业应用系统复杂多样，而在密码全方位应用要求背景下，针对每个应用分别实施密码防护会面临技术、管理等挑战，因此，亟待结合企业数字化现状和具体问题，遵循统一标准体系，建设统一密码平台，实施统一安全防护，落实统一运维监管，打造一体化的密码支撑体系。

（四） 体系实战升级

1. 探索融入业务流转的密码防护

数据作为一种新型生产要素，正以更深度的方式为经济社会发展赋能。在大数据时代，数据作为一种新型生产要素，具有区别于其他生产要素的显著特征。从信息化延伸视角看，数据具有如下特

征：一是个人信息数据量不断增加，具备自我繁衍性；二是数据类型复杂，不仅包含各种复杂的结构化数据，而且图片、指纹、声纹等非结构化数据日益增多；三是业务实时性逐渐增强，对数据处理速度要求越来越高，同时对系统可用性要求也逐渐提高；四是高价值数据主要在应用层共享流转，海量个人信息与复杂业务流程扭结缠绕，接触人员更多，数据安全风险敞口也更突出，给数据安全防护带来严峻技术挑战。

同时，数字化时代，数据一旦生产出来后就会进入传输、存储、处理、分析、访问与服务应用等环节，从而形成丰富的信息共享路径。这些环节涉及到业务用户、研发运维人员、外包人员、第三方机构等，传统的数据之间简单的线性联动变成复杂的网状数据流，大量环节面临数据安全威胁。因此，保护数据安全应“以数据为中心”构建防护策略，将安全保护贯穿于数据的全生命周期，即对数据的收集、传输、存储、使用、共享、删除、销毁等各流程实施安全防护，并结合数据业务与技术属性，全环节主动式重建数据访问规则，构筑有效的数据安全纵深防线，保障数据的流转、共享与安全兼得。

密码应用目的是保护数据安全，安全是促进商用密码应用最大的动力。基于企业目前 IT 架构，包含基础设施、软件平台以及业务应用等不同层级，企业数据在不同层之间高效流转，实现互联共享，为企业创造价值。数据越朝上层流动，价值点越多。数据在基

础设施层，就是一些没有业务含义的二进制数字；在软件平台层，表现为各种形式的文件格式；在业务应用层，数据才具备了丰富的业务含义。

从传统角度来看，安全和业务是关联的，有时候也是对立的。但换个角度，**安全其实就是一种业务需求。“传统业务需求”侧重于“希望发生什么”，而“安全需求”则侧重于“不希望发生什么”，从而确保“发生什么”。**另外“安全”在英文中对应 Security（安全防攻击）、Safety（安全可靠）、Reliability（可靠性）、Trustiness（诚信度）、Sureness（确定性）等词汇，从业务角度来看，这些词汇都可以映射到相应的业务需求。结合到企业或机构的信息系统中，数据安全则来自于业务处理中的风险映射。时间维度看，数据在流转的全生命周期中的每个环节都会有相应的安全需求；空间维度看，数据在基础设施层、平台层以及应用层之间流转，不同层次又有着不同颗粒度的防护需求。

而传统的城防式数据安全，主要用于保护被传统物理网络多层包围的数据，这种防护体系仅适用于保护静态数据。但当下，数据作为新型生产要素，在被充分共享流转中产生更多价值，传统城防式数据安全已很难以满足相关防护需求。另外，数据与“网络/主机/数据库/应用”作为正交关系，数据安全的本质其实就是在数据流转的多个层次环节中，通过密码等安全技术重建业务规则，对数据施加主动式安全防护。

因此，兼顾数据利用和安全的技术，**需要将加密等安全能力结合到业务流程中，一方面可以根据不同业务场景，定制不同的商业秘密保护方案;另一方面不会改变用户的操作习惯,方便用户使用，不影响数据的高效共享流转，并基于高性能的密码技术支撑，将安全机制与用户现有流程无缝对接,实现在业务高效流转和安全防护之间的平衡。**

当然企业真实的业务需求往往更复杂，很难框定边界，因此对应的数据安全也几乎没有边界。所以**在实施数据安全防护的时候，数据安全需要结合具体业务展开，很难有“一招鲜”的数据安全解决方案。**

2. 打造融合密码的数据安全框架

数据安全的防护会涉及到很多场景，同时会有多种加密技术的应用，因此，以数据安全的多种场景为中心，绘制一张数据安全的技术地图，则非常有意义，且有必要。针对数据进行安全防护的技术，可以先回顾经典网络安全攻击模型：ATT&CK，作为当前权威的网络安全技术模型，ATT&CK 包涵 14 个攻击战术、205 个攻击技术以及 573 个攻击流程，覆盖了大多数网络攻击手段，从而给网络安全防护提供了专业的技术参考。

图 6：经典网络安全攻击模型 ATT&CK 架构概览

但是，ATT&CK 模型更侧重网络攻防视角，从“主动式保护数据”的角度来看，ATT&CK 并没有针对内部业务人员威胁，也没有将数据进行分级分类等。在基于 ATT&CK 模型的攻防对抗思路下，传统“以网络为中心的安全”主要通过“防漏洞、堵漏洞”的方式去保护数据，而当下来看，网络漏洞在所难免，因此直接针对数据本身进行主动式加密等保护，是实现数据安全的最直接有效的手段。信息安全技术发展的大趋势也正从“以网络为中心的安全”转向为如今的“侧重以数据为中心的安全”，美国国防部对这种理念也非常认可，并将防护重点从边界开始转向数据和服务。

图 7：“以数据为中心的安全”与“以网络为中心的安全”逻辑关系图

依据这个新思路，炼石网络从“以数据为中心”的角度提出新的数据安全技术框架，全称是：“Data-centric Tactics, Techniques And Common Knowledge”（简称 DTTACK），“以数据为中心的战术、技术和通用知识”。**DTTACK 不是网络服务器或应用程序安全性的模型，它更强调数据本身的安全性，并从对数据的“应对式”防护，向“主动式”防护转变，重视从业务风险映射视角列举数据保护需求，可以为信息化建设、企业业务架构设计提供数据安全能力参考。**

通过结合 NIST 安全能力模型和安全滑动标尺模型，两者有交集、但也各有侧重。DTTACK 当前版本选择了六大战术作为基本结构：I(识别)、P(防护)、D(检测)、R(响应)、R(恢复)、C(反制)。

数据安全技术列举方面，参考了工信部相关机构正在编制的行业标准《电信网和互联网数据安全管控平台技术要求和测试方法》，

将 114 个具体技术流程分类并对号入座，I（识别）战术目前包括数据资产地图、数据资产稽核、数据接口管理、数据内容识别等方面的技术；P（防护）战术目前包括加密技术、脱敏技术、数字签名、访问控制、隐私保护、数据防泄漏等方面的技术；D（检测）战术目前包括风险检测、安全审计、共享监控等方面的技术；R（响应）战术目前包括事件处理、应急响应、动态流转等方面的技术；R（恢复）战术目前包括一体机、备份软件、融合备份、云灾备等方面的技术；C（反制）战术目前包括水印、溯源等方面的技术。

DTTACK 的定位是数据安全领域的全地图技术框架，能给数据安全厂商提供通用知识库，也能为甲方用户的数据安全规划和技术对比提供参考依据。（关注本公众号，实时了解 DTTACK 最新动态）

图 8：数据安全领域全技术框架 DTTACK 架构概览

3. 构建以密码为核心的防护体系

密码技术为 DTTACK 六大战术提供了重要价值。比如：识别方面，密码可以为数据识别提供身份安全能力，为接口通道实现安全加密；防护方面，数据加密技术本身就是在开放式信道中，构建了强制的防护措施，并结合身份实现访问控制。检测、响应、恢复和反制方面，密码也能够为其分别提供身份鉴别、数据保护、水印追溯等不同能力。

尤其对于流转数据防护，密码技术可提供独特价值。共享流转的数据很难有边界，在做访问控制时，如果数据库或归档备份中的数据是明文，访问控制机制很容易被绕过。而通过数据加密技术，可以打造一个强防护场景，用户在正常访问应用的过程中数据才会解密，并结合身份访问控制、审计等安全技术，从而实现“防绕过的访问控制”、以及“高置信度的审计”。密码技术为数据重新定义了虚拟的“防护边界”，从而更好的对数据实施防护与管控。

密码技术结合其他安全技术产生的安全方案，可以满足多维度的实战化需求。第一，方案无需开发改造应用，即可实现将安全能力融入到应用，以配置方式敏捷部署实施，满足实战防护和新合规两类需求，且对应用运行无影响，不会因实施加密带来业务风险；第二，方案支持国密算法的同时，支持国际算法，并支持手机号、证件号、邮箱等字段保留格式加密。开发高性能国密技术，做到对企业业务系统效率和使用体验零影响，比如炼石网络在高性能国密技术方面拥有深厚，且具有竞争优势的技术积累；第三，方案可基

于属性和角色的访问控制，访问控制主体可细化到用户，实现对企业内部人员的敏感数据访问授权最小化，并提供丰富的数据脱敏策略，当用户对敏感数据风险访问时，如过量导出、异常频繁访问等，可根据规则阻断；第四，方案提供可定责的数据访问审计，记录识别到的主客体信息，在记录操作行为的同时，能够对每条审计日志进行签名，不仅做到独立于应用系统的第三方审计，还能够通过数字签名技术确保审计日志的不可篡改，以及在事后追溯问题过程中提供重要依据。

总结，我国密码产业当下已形成坚实发展基础，伴随复杂多变的国际形势，我们正处于建设“平安中国”的关键时期。一方面密码的实战合规需求强劲发展，另一方面，密码供给结构也处于变革前夜，密码产业进入了发展新时代。一是分层化密码市场将兼顾实战与合规，二是密码供给结构正在向高质量升级，三是监管侧推进新密码市场正在释放更多红利。面向新时代，金融、政务、教育、医疗、文旅、制造等多领域都迎来重大发展机遇，安全服务商可以从实战化角度出发，应用密码等安全技术，全面赋能数据安全实战化，为建设“平安中国”贡献力量。

作者介绍

北京炼石网络技术有限公司是一家基于密码与系统安全技术的数据安全创新公司，提倡“以数据为中心的新安全理念”，自主研发了 CASB 业务数据安全平台和高性能国密产品，开创性的实现免开发改造应用、敏捷实施细粒度数据保护，该产品入选工信部 2020 年网络安全技术应用试点示范推荐项目，并夺得第七届互联网安全大会(ISC 2019)首届“创新独角兽沙盒大赛”总冠军。基于 AOE 面向切面数据安全技术，将安全与业务在技术上解耦、但又在能力上融合交织 ，实现主体到应用内用户、客体到字段级的防护，打造“以密码技术为核心，访问控制、审计等多种安全技术互相融合”的实战化数据安全防护体系。炼石为政府、金融、教育医疗文旅、工业央企商业等行业用户，提供个人信息保护、商业秘密保护以及国密合规改造方案，创新安全技术，让数据共享更有价值。欢迎感兴趣的合作伙伴,随时和我们联系,共同掘金“数据安全市场”。

- 交流合作、信息反馈请发送邮件至：market@ciphergateway.com
- 注：本文如有侵权，请联系改正。

创新安全技术，让数据共享更有价值

www.ciphergateway.com
400-819-0181
sales@ciphergateway.com