

## 三未信安 (688489.SH) 商密领军，创“芯”未来

2023年04月26日

### ——公司首次覆盖报告

投资评级：买入（首次）

陈宝健（分析师）

刘逍遥（分析师）

chenbaojian@kysec.cn

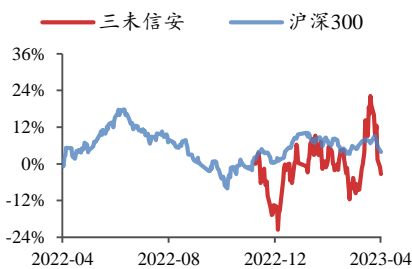
liuxiaoyao@kysec.cn

证书编号：S0790520080001

证书编号：S0790520090001

日期	2023/4/25
当前股价(元)	115.53
一年最高最低(元)	155.00/93.27
总市值(亿元)	88.90
流通市值(亿元)	18.77
总股本(亿股)	0.77
流通股本(亿股)	0.16
近3个月换手率(%)	449.29

#### 股价走势图



数据来源：聚源

#### ● 国内商密领军，技术实力业内领先，首次覆盖给予“买入”评级

作为国内领先的密码基础设施提供商，公司业务覆盖密码芯片、密码板卡、密码整机和密码系统等商用密码全产业链。自成立以来，公司坚持进行产品研发与升级迭代，技术实力行业领先，并且公司将云计算安全作为重要的战略方向，是国内最早布局云计算密码产品的厂商之一。我们预计公司2023-2025年归母净利润为1.59、2.23、2.97亿元，EPS分别为2.07、2.90、3.86元/股，当前股价对应PE分别55.8、39.9、29.9倍。公司估值高于同行可比公司平均估值，考虑公司在商密市场全产业链布局及在密码芯片领域的领先地位，首次覆盖给予“买入”评级。

#### ● 政策环境逐渐完善，下游市场需求旺盛，密码行业迎来发展黄金期

(1) 政策法规端：随着密码法的落地，我国商用密码进入立法规范阶段。同时，根据商密安全性评估管理办法及等保条例规定，国内等保三级以上信息系统每年至少进行一次密评。根据我们测算，密改与密评有望带来108亿增量市场/年。(2) 需求端：一方面，随着数据要素市场的发展，数据安全需求旺盛，有望推动隐私计算等密码技术创新发展；另一方面，信创与密码市场有望实现相互促进，协同发展。根据赛迪智库报告，2021年我国商用密码产业规模达到585亿元，较2020年增长25.54%。我们认为在多重利好刺激下，2022-2025年商用密码市场有望实现25%的复合增长率，预计到2025年市场规模将达到1400亿元。

#### ● 布局自主密码芯片，进一步打开成长空间

历经6年布局，公司于2021年成功推出自主密码芯片XS100。XS100集合FPGA、主控芯片等6个芯片的功能，可以大幅提升产品的稳定性、安全性，同时提升产品性价比，也是目前唯一支持硬件虚拟化的密码安全芯片。未来公司芯片发展战略将重点关注两个领域：一是面向云计算和大数据安全领域，研制高性能、高可靠、支持虚拟化技术的密码芯片；二是面向物联网安全领域，研制适用于边缘网的高安全、高可靠的密码安全芯片，有望实现大规模产业化推广。

#### ● 风险提示：市场竞争加剧风险；密码芯片业务拓展不及预期。

#### 财务摘要和估值指标

指标	2021A	2022A	2023E	2024E	2025E
营业收入(百万元)	270	340	473	654	883
YOY(%)	33.5	25.7	39.1	38.3	35.1
归母净利润(百万元)	75	107	159	223	297
YOY(%)	42.8	43.5	48.7	39.9	33.4
毛利率(%)	73.6	75.5	75.1	74.9	74.5
净利率(%)	27.6	31.6	33.7	34.1	33.7
ROE(%)	19.3	5.7	7.8	9.8	11.6
EPS(摊薄/元)	0.97	1.39	2.07	2.90	3.86
P/E(倍)	119.0	82.9	55.8	39.9	29.9
P/B(倍)	23.0	4.7	4.4	3.9	3.5

数据来源：聚源、开源证券研究所

## 目 录

1、 公司概况：国内领先的密码基础设施提供商.....	4
1.1、 业绩高速增长，盈利能力快速提升.....	5
1.2、 股权结构稳定，实控人产业背景深厚.....	7
1.3、 客户覆盖度高，形成直接与间接需求双轮驱动的业务模式.....	8
2、 政策环境逐渐完善，下游市场需求旺盛，密码行业迎来发展黄金期.....	10
2.1、 法律标准体系逐渐健全，为商用密码行业发展奠定基石.....	12
2.2、 以密评为抓手，合规驱动下商用密码市场有望加速发展.....	14
2.3、 数据安全需求旺盛，有望推动密码行业创新发展.....	16
2.4、 信创与密码有望实现相互促进，协同发展.....	18
2.5、 我们预测，到 2025 年国内商用密码市场有望超千亿元.....	18
3、 核心竞争力分析：技术实力领先，全产业链布局优势明显.....	19
3.1、 坚持产品研发、升级迭代，技术实力行业领先.....	19
3.2、 全产业链布局，有望实现规模化发展.....	21
4、 布局自主密码芯片，进一步打开成长空间.....	21
5、 盈利预测与投资建议.....	26
5.1、 核心假设.....	26
5.2、 盈利预测与投资建议.....	26
6、 风险提示.....	26
附：财务预测摘要.....	27

## 图表目录

图 1： 自成立以来公司专注于密码关键技术的创新突破和核心产品的研发、销售及服务.....	4
图 2： 公司业务覆盖密码芯片、密码板卡、密码整机和密码系统等商用密码全产业链.....	5
图 3： 2018-2022 年公司收入复合增长率为 34.5%.....	5
图 4： 2018-2022 年公司归母净利润复合增长率为 72.8%.....	5
图 5： 公司收入主要来源于密码板卡、密码整机和密码系统.....	6
图 6： 2018-2022 年公司销售毛利率逐年提升.....	6
图 7： 2018-2022 年公司期间费用率逐年下降.....	7
图 8： 公司控股股东及实际控制人是张岳公先生.....	7
图 9： 公司下游客户既包括网络安全产品和解决方案厂商，也包括最终行业客户.....	9
图 10： 我国密码分为三类，分别是核心密码、普通密码和商用密码.....	10
图 11： 我国商用密码经历了起步形成、快速发展、立法规范三个发展阶段.....	11
图 12： 我国商用密码产业链涵盖从密码安全芯片、密码板卡、密码整机、密码系统、密码测评等多个方面.....	12
图 13： 我国密评发展经历了四个阶段.....	15
图 14： 横向联邦学习主要应用于各个参与方的数据集有相同的特征空间和不同的样本空间的场景.....	17
图 15： 纵向联邦学习主要适用于数据集上具有相同的样本空间、不同的特征空间的参与方所组成的场景.....	17
图 16： 多方安全计算提供更加安全的联合数据分析能力.....	17
图 17： 我国商用密码产业规模不断扩大.....	19
图 18： 云密码机实现了云应用环境下网络管理员维护设备，用户自行管理密钥的工作模式.....	21
图 19： 云密码服务平台基于微服务架构，实现应用系统统一安全接入、密码资源统一管理和调度.....	21
图 20： XS100 密码安全芯片主要用于 PKI、VPN、云计算、大数据等信息安全场景.....	22

表 1: 公司核心技术人员均有深厚的行业背景.....	8
表 2: 公司积累了一批各行业、各领域的高质量用户.....	9
表 3: 密码安全法律法规体系逐渐完善.....	12
表 4: 多行业也出台了密码应用相关政策要求.....	14
表 5: 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.....	15
表 6: 由于技术路径的不同, 各类隐私计算技术均有其更加适用的场景.....	18
表 7: 国内目前仅有少数几家企业具备安全等级三级产品的资质.....	19
表 8: 公司的安全等级二级和三级产品数量均位于行业前列.....	19
表 9: 公司在全球密码硬件安全市场中位列第九.....	20
表 10: 公司密码板卡综合各项指标整体处于行业先进水平.....	20
表 11: XS100 密码安全芯片集合 6 个芯片的功能.....	22
表 12: 相较于外购芯片, XS100 密码安全芯片的核心性能指标大幅提升.....	23
表 13: XS100 密码芯片的综合核心功能指标达到国内公司先进水平.....	23
表 14: 公司在密码领域有明显优势, 密码芯片的核心密码技术先进.....	25
表 15: 公司 PE 高于行业可比公司平均水平 (截止 2023.4.25 收盘).....	26

## 1、公司概况：国内领先的密码基础设施提供商

三未信安成立于2008年8月，总部位于北京，在山东设立有研发中心。公司是国内主要的密码基础设施提供商，专注于密码关键技术的创新突破和核心产品的研发、销售及服务，为网络信息安全领域提供全面的商用密码产品和解决方案。此外，公司是全国信息安全标准化技术委员会和密码行业标准化技术委员会成员单位，牵头和参与制定了二十余项密码领域国家标准或行业标准。

图1：自成立以来公司专注于密码关键技术的创新突破和核心产品的研发、销售及服务



资料来源：公司招股说明书

公司业务覆盖密码芯片、密码板卡、密码整机和密码系统等商用密码全产业链。其中，密码芯片和密码板卡是密码系统的基础部件，公司密码板卡在国内有着较高的市场占有率，被众多的信息安全设备厂商集成在产品中。

密码整机以更集成化的功能提供密码服务，按照不同应用场景，包括服务器密码机、金融数据密码机、签名验签服务器、云密码机、数据库加密机、密钥管理(KMS)密码机、加密存储网关、SSL VPN、IPSec VPN等，公司密码整机服务于各个行业的最终用户，并被众多网络安全厂商和系统集成商集成在解决方案中。

公司密码系统主要包括密钥管理系统、密码服务平台、身份认证系统、软件加密中间件等软件系统，以更加完整的功能和友好的界面满足用户对大容量的密钥管理、多密码设备管理和统一接口服务、身份管理、多种形态数据加密等场景需求。

图2：公司业务覆盖密码芯片、密码板卡、密码整机和密码系统等商用密码全产业链



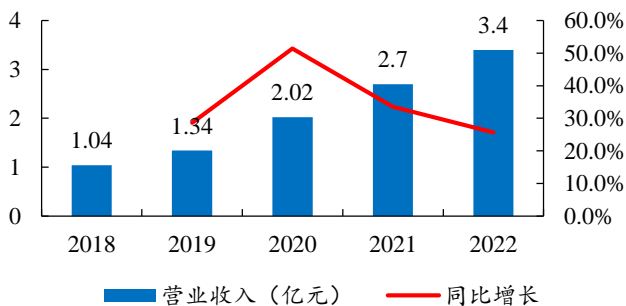
资料来源：公司招股说明书

### 1.1、业绩高速增长，盈利能力快速提升

公司收入和利润维持高速增长。2018-2022 年公司收入年复合增长率为 34.5%，收入快速增长的原因为：一是随着密码相关法律法规落地，国内商用密码市场快速发展；二是随着客户资源、品牌效应和立体化的市场布局优势不断巩固，公司客户粘性不断增强；三是公司通过持续的核心技术迭代提升了核心竞争力。

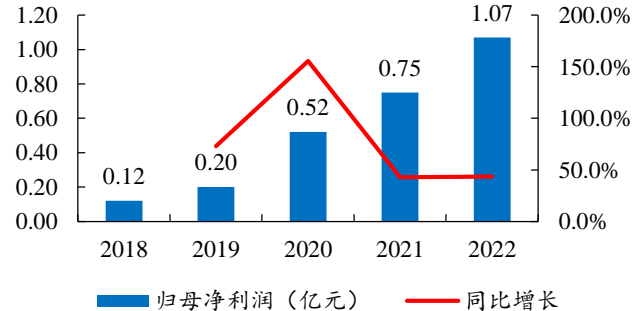
2018-2022 年公司归母净利润年复合增长率为 72.8%，增速快于收入增速，主要原因为：一是随着业务结构变化，公司毛利率逐年提升；二是业务规模逐渐显现，公司期间费用率逐年降低。

图3：2018-2022 年公司收入复合增长率为 34.5%



数据来源：Wind、开源证券研究所

图4：2018-2022 年公司归母净利润复合增长率为 72.8%



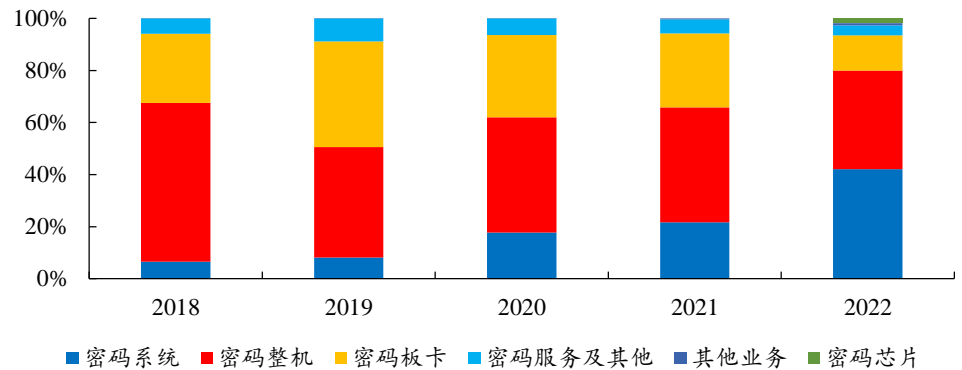
数据来源：Wind、开源证券研究所

公司收入主要来源于密码板卡、密码整机和密码系统。其中，密码板卡和密码整机收入占比稳中有降，密码系统收入占比逐年提升。主要系公司持续投入密码系统产品的升级迭代和性能优化，解决了多项数据密码服务的短板，使密码系统的使



捷性和安全性得到了大幅提高。随着密码系统进入信创采购目录，密码系统在公司收入中的占比将不断提升。

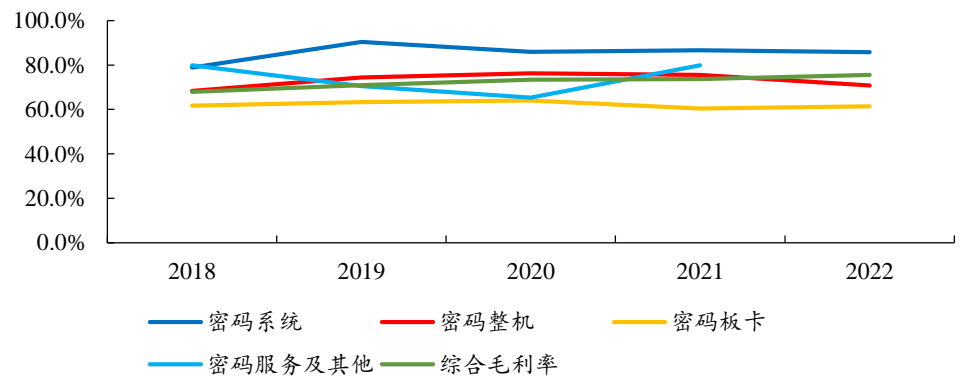
图5：公司收入主要来源于密码板卡、密码整机和密码系统



数据来源：Wind、开源证券研究所

公司销售毛利率逐年提升，主要由于业务结构变化，毛利率较高的密码系统业务占比提升。分业务来看，各项业务毛利率虽然年度之间有所波动，但整体保持较为稳定。

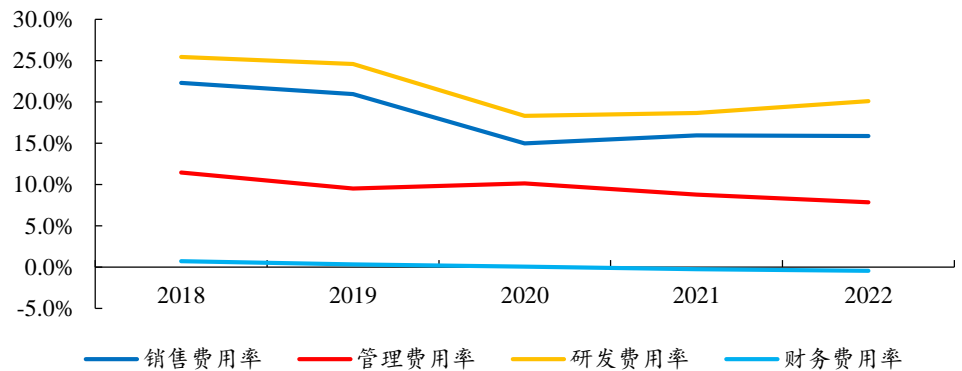
图6：2018-2022 年公司销售毛利率逐年提升



数据来源：Wind、开源证券研究所

公司期间费用率逐年下降。2018-2022 年，公司销售费用率、管理费用率和研发费用率均有所下降，说明随着业务体量的扩大，公司规模效应逐渐显现。

图7：2018-2022 年公司期间费用率逐年下降

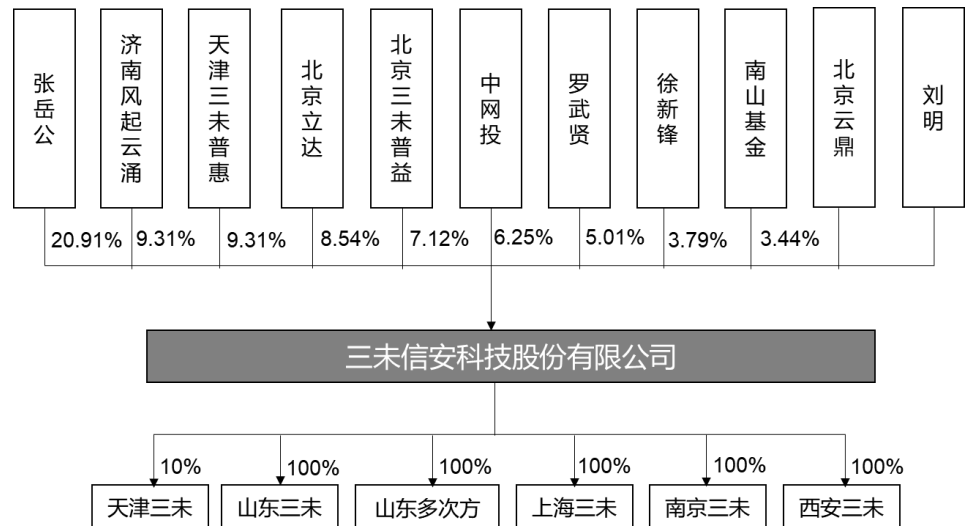


数据来源：Wind、开源证券研究所

## 1.2、股权结构稳定，实控人产业背景深厚

公司控股股东及实际控制人是张岳公先生。截至 2022 年底，张岳公先生直接持有公司 1600.87 万股股份，占公司总股本的 20.91%。此外，张岳公通过济南风起云涌、北京三未普益及天津三未普惠分别间接持有公司 3.32%、0.95%及 0.72%的股权，故张岳公直接及间接持有公司 25.90%的股权，为公司控股股东。同时，张岳公作为济南风起云涌、天津三未普惠及北京三未普益的普通合伙人及执行事务合伙人分别间接控制公司 9.31%、9.26%和 7.12%的表决权；张岳公合计控制公司 46.6%的表决权，为公司实际控制人。

图8：公司控股股东及实际控制人是张岳公先生



资料来源：公司招股说明书、开源证券研究所

公司核心技术人员均有深厚的行业背景。其中，张岳公先生是山东大学应用数学博士，曾任教于山东大学网络信息安全研究所，在山东大学从事密码技术教学与科研工作，现任公司董事长兼总经理。张岳公先生为公司技术带头人之一，国家密码行业标准化技术委员会委员、国家商用密码技术总体专家组专家、北京商用密码行业协会副会长、山东计算机学会网络空间安全专委会副主任委员，曾参与多项国家标准或行业标准的制订，两次荣获党政机要密码科学技术进步三等奖，2015 年被科技部评为“科技创新创业人才”。

**表1: 公司核心技术人员均有深厚的行业背景**

姓名	职位	履历
张岳公	董事长兼总经理	山东大学应用数学博士，曾任教于山东大学网络信息安全研究所，在山东大学从事密码技术教学与科研工作。张岳公先生为公司技术带头人之一，国家密码行业标准化技术委员会委员、国家商用密码技术总体专家组专家、北京商用密码行业协会副会长、山东计算机学会网络空间安全专委会副主任委员，曾参与多项国家标准或行业标准的制订，两次荣获党政机要密码科学技术进步三等奖，2015年被科技部评为“科技创新创业人才”。
高志权	董事、副总经理、核心技术人员	公司产品研发带头人之一，全国信息安全标准化技术委员会委员，累计获已授权国家发明专利2项，牵头制定GM/T0098-2020《基于IP网络的加密语音通信密码技术规范》等密码行业标准，参与制定GB/T39786-2021《信息安全技术信息系统密码应用基本要求》等国家标准4项，参与制定密码行业标准12项，主导或参与的“SRJ1203签名验证服务器”和“支持云计算的密码解决方案及产品”分别于2013年和2018年获密码科技进步奖三等奖，曾多次参与国家863计划课题(高速密码设备研制)、国家发改委金融领域安全IC卡和密码应用专项(高性能金融数据密码机产业化)、中关村高精尖项目(支持云计算的国产密码算法技术与产品成果转化)等课题研究工作。
刘会议	研发中心总经理	公司技术、产品研发带头人之一，累计获已授权国家发明专利6项，曾获得密码科技进步奖三等奖(2019年)、党政机要密码科学技术奖励三等奖(2020年)，发表论文3篇，参与省级以上重点研发项目2项，带领技术团队实现密钥分割协同签名技术方案，高性能白盒密码技术、数据流转溯源技术实现等。
杨国强	山东多次方总经理	公司技术、产品研发带头人之一，累计获已授权国家发明专利6项，曾获得密码科技进步奖三等奖(2013年)、党政机要密码科学技术奖励三等奖(2020年)，发表论文4篇，参与省级以上重点研发项目2项，带领技术团队完成高性能国密算法软硬件实现、高性能密码安全芯片的设计与实现等。

资料来源：公司招股说明书、开源证券研究所

### 1.3、客户覆盖度高，形成直接与间接需求双轮驱动的业务模式

公司下游客户既包括网络安全产品和解决方案厂商，也包括最终行业客户。一方面，公司为PKI、IPSec VPN、SSL VPN等网络安全产品和解决方案厂商提供密码核心产品，由网络安全厂商将密码产品整合融入其解决方案，应用于电子政务、金融、证券、税务、电力、能源、海关、公安等行业客户。另一方面，随着公司密码技术的积累和重要行业客户的发展需求，公司正在逐步向同时服务厂商客户和最终客户的业务模式发展，形成间接需求和直接需求结合下双轮驱动的业务模式。



图9：公司下游客户既包括网络安全产品和解决方案厂商，也包括最终行业客户



资料来源：公司招股说明书

优质的客户资源为公司树立了良好的品牌形象。公司凭借领先的密码技术、高性能的密码产品、完善的解决方案和优质专业的服务，在网络安全、政府、金融、证券、能源、电信、医疗、教育等行业拥有广泛的市场，积累了各行业、各领域的高质量用户，包括吉大正元、数字认证、格尔软件、信安世纪、深信服、启明星辰、绿盟、天融信等网络安全企业，中华人民共和国公安部、中华人民共和国财政部、国家医疗保障局、国家税务总局等众多国家部委用户以及国家电网、中石油、中石化、中国电信、中国联通、中国移动、中国人民银行、中国银联、中国农业银行、中国民生银行、中国平安、华泰证券、新华三、浪潮、腾讯、IBM、AWS、Visa、三星、戴姆勒等国内国际大型企业客户。

表2：公司积累了一批各行业、各领域的高质量用户

项目	主要合作厂商	终端客户产品形态	产品使用方式及作用
密码板卡	吉大正元	PKI 网络安全产品	需要产品适配开发，提供加密/解密、签名/验证等密码运算，提高加密的速度和安全产品的整体性能
	数字认证	PKI 网络安全产品	
	五舟科技	PKI 网络安全产品	
	格尔软件	PKI 网络安全产品	
	深信服	VPN 网络安全产品	
	天融信	VPN 网络安全产品	
密码整机	郑州釜之昕	医保支付终端	需要产品适配开发，提供签名/验签等密码运算
	吉大正元	网络安全系统集成	直接安装使用，以整机形态提供密码运算、密钥保护等基础支撑和密码服务
	格尔软件	网络安全系统集成	
	航天信息	网络安全系统集成	
	博雅中科	网络安全系统集成	
	优信云	网络安全系统集成	
国家电网	网络安全系统集成		
密码系统	优信云	网络安全系统集成	直接安装使用，提供密码运算、证书管理、密

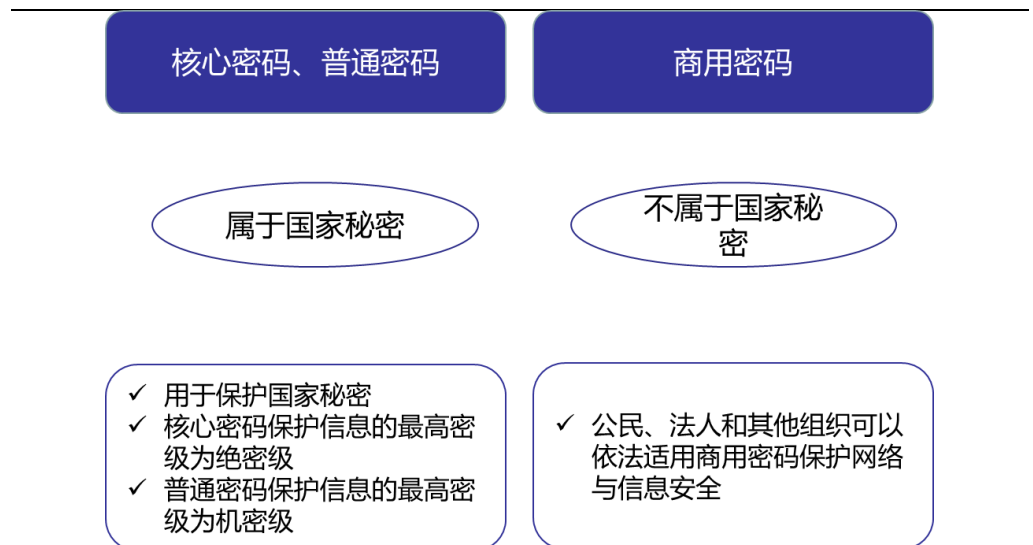
项目	主要合作厂商	终端客户产品形态	产品使用方式及作用
			钥管理、密码资源管理服务

资料来源：公司公告、开源证券研究所

## 2、政策环境逐渐完善，下游市场需求旺盛，密码行业迎来发展黄金期

我国《密码法》将密码分为三类，分别是核心密码、普通密码和商用密码，其中，商密产品应用最为广泛。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。

图10：我国密码分为三类，分别是核心密码、普通密码和商用密码

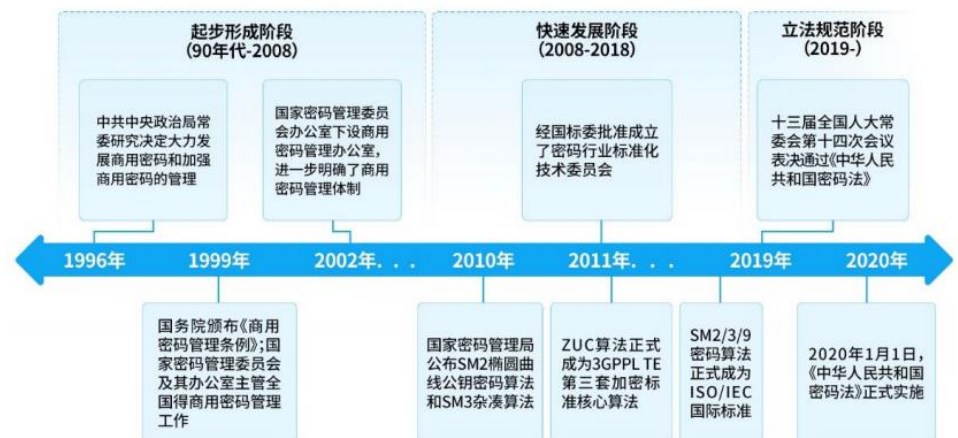


资料来源：深圳盐田法院公众号、开源证券研究所

我国商用密码经历了起步形成、快速发展、立法规范三个发展阶段。(1) 起步阶段：我国商用密码的发展起步起源于 20 世纪 90 年代开启的“金字”工程。随着一系列信息化工程的实施，国家对信息技术应用的要求不断提高，信息化成为一项全局性战略，在经济社会各个领域全面推进。在此背景下，信息安全保护的紧迫性日益凸显，商用密码的应用需求应运而生。商用密码技术、产品开始出现，在各个行业开始得到初步应用。

(2) 快速发展阶段：2008-2018 年，受电子政务、电子商务等数字化社会经济新模式的不断带动，政务、金融等重要领域的商用密码应用需求快速增长，商用密码产业得到了广泛的市场空间和发展机遇。与此同时，商用密码的技术标准体系在不断完善，自主创新能力不断增强，为商用密码产业的快速发展奠定了重要基础。商业密码产业引导政策陆续出台，市场需求不断增加，刺激商用密码产业快速发展。

(3) 立法规范阶段：2019 年《密码法》颁布，商用密码发展进入了有法可依的新历史时期。《密码法》按照国家的发展与改革要求，大力促进商用密码产业健康发展，未来商用密码市场规模将不断扩大。

**图11：我国商用密码经历了起步形成、快速发展、立法规范三个发展阶段**


资料来源：公司招股说明书

我国商用密码产业链涵盖从密码安全芯片、密码板卡、密码整机、密码系统、密码测评等多个方面。

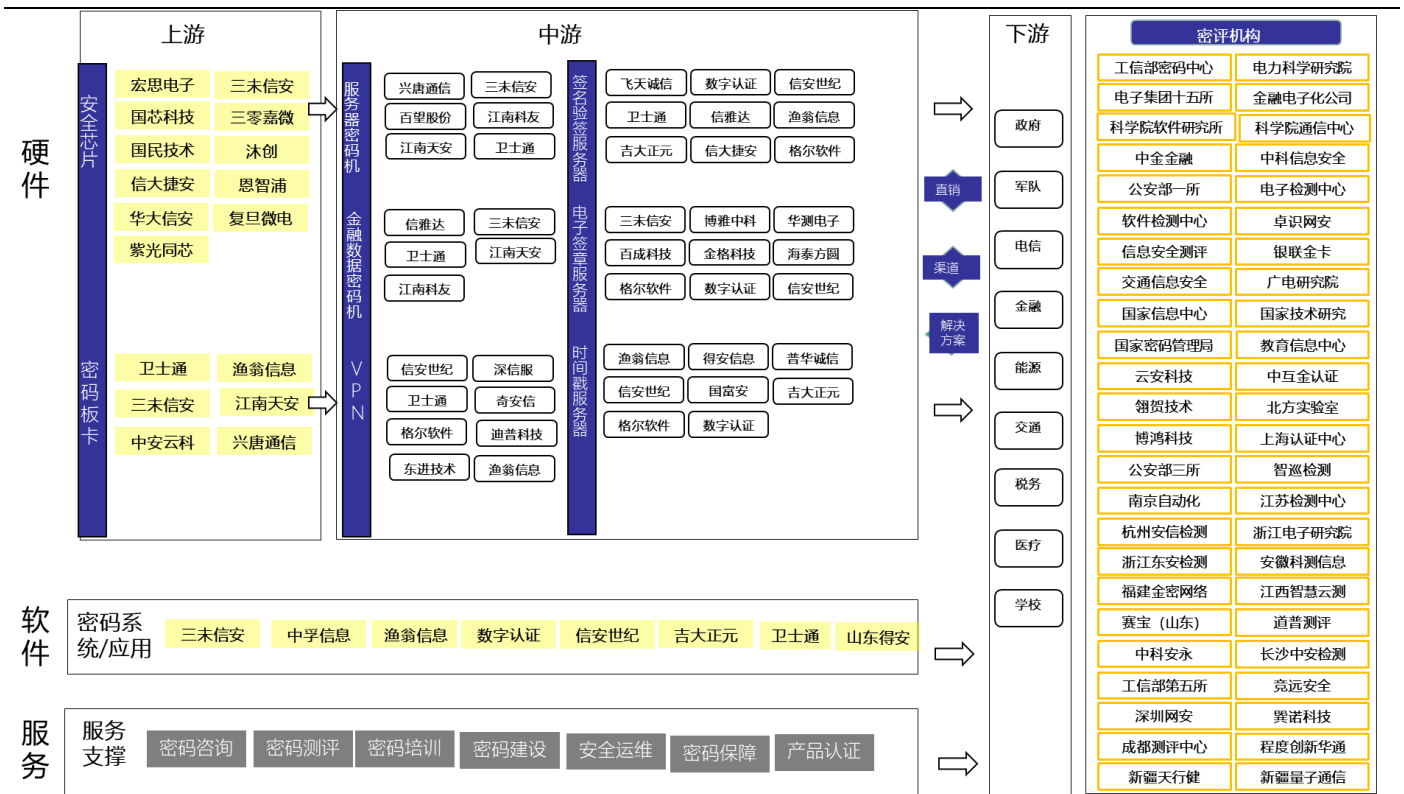
**密码安全芯片**是指芯片内带有微处理器 CPU、随机数发生器、硬件密码算法、存储单元（包括随机存储器 RAM、程序存储器 ROM (FLASH)、用户数据存储单元 EEPROM）以及芯片操作系统 COS 的智能芯片，相当于一台微型计算机，不仅具有数据存储功能，同时具有命令处理和数据安全保护等功能。安全芯片是集成了密码算法的专用芯片。密码技术是保护信息安全的主要手段，它通过对信息进行重新编码，在保证信息的完整性和正确性的同时，也保证信息的机密性，防止信息被篡改、伪造和泄露。**国内主要密码安全芯片厂商包括：**宏思电子、三未信安、国芯科技、国民技术、恩智浦、沐创集成电路、卫士通（二零嘉微）、信大捷安等。

**密码板卡**为软硬件一体产品，硬件部分主要包括芯片（FPGA 芯片、主控芯片等）和 PCB 板卡。密码板卡属于专用高性能密码设备，作为密码整机、IPSec VPN、SSL VPN、安全服务器等网络信息安全类安全设备的密码核心部件，可以满足系统的加密/解密、签名/验证等密码运算功能要求，保证数据的机密性、完整性、真实性和抗抵赖性，同时提供安全、完善的密钥管理机制，是网络信息安全系统中重要的硬件保障。**国内主要密码板卡厂商包括：**卫士通、三未信安、渔翁信息、江南天安、中安云科、兴唐通信等。

**密码整机**是软硬一体产品，是密码应用系统的基础支撑。密码整机包括签名验签服务器、金融数据密码机、服务器密码机、时间戳服务器、数据库加密机、存储加密机、国密 VPN/网关、电子签章服务器等产品。**国内密码整机参与厂商较多，**包括卫士通、三未信安、江南天安、渔翁信息、信安世纪、吉大正元、格尔软件、博雅中科等密码领域专业厂商，也包括深信服、奇安信等网络安全厂商。

**密码系统**作为管理系统，提供密码运算、证书管理、密钥管理、密码资源管理等基础支撑。密码系统可以作为软硬件一体产品，硬件部分由密码板卡和组装修配件构成，也可以软件形式交付并配合内置密码板卡的服务器或密码整机使用。**国内主要密码系统厂商包括：**卫士通、三未信安、山东得安、渔翁信息、江南天安、海泰方圆、中安云科、兴唐通信等。

图12：我国商用密码产业链涵盖从密码安全芯片、密码板卡、密码整机、密码系统、密码测评等多个方面



资料来源：数观天下、开源证券研究所

## 2.1、法律标准体系逐渐健全，为商用密码行业发展奠定基石

从顶层设计到法律法规，行业标准到产业要求的密集颁布，密码法律标准实现了自上而下的体系化发展，商用密码市场进一步被激活。2016年11月，全国人民代表大会常务委员会发布《中华人民共和国网络安全法》，将网络信息安全上升到国家安全的战略高度，规定“国家实行网络安全等级保护制度”，密码是保障网络信息安全的核心技术。2019年10月26日《中华人民共和国密码法》正式发布并于2020年1月1日起施行。我国商用密码进入立法规范阶段，作为我国密码领域第一部法律，以立法形式来明确包括商用密码在内的密码管理和应用，体现了国家对于密码这一网络安全核心技术的高度重视。

表3：密码安全法律法规体系逐渐完善

部门	时间	文件	内容
中共中央办公厅、国务院办公厅	2015年	《关于加强重要领域密码应用的指导意见》	新建网络和信息系统应当采用国产密码进行保护，已建网络和信息系统应当进行密码国产化改造
全国人大常委会	2016年11月	《中华人民共和国网络安全法》	将网络信息安全上升到国家安全的战略高度，规定“国家实行网络安全等级保护制度”。
国家密码管理局	2018年10月	《国家密码管理局关于进一步加强商用密码产品管理工作的通知》	加强商用密码产品品种和型号申报指导、初审把关和审批管理。
全国人大常委会	2019年10月	《中华人民共和国密码法》	法律、行政法规和国家有关规定要求使用



部门	时间	文件	内容
会		《密码法》	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。
国务院办公厅	2020年1月	《国家政务信息化项目建设管理办法》	项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。 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。
国家密码管理局	2020年8月	《商用密码管理条例（修订草案征求意见稿）》	在中华人民共和国境内的商用密码科研、生产、销售、服务、检测、认证、进出口、应用等活动及监督管理进行具体规定。
全国人大常委会	2021年6月	《中华人民共和国数据安全法》	国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。

资料来源：公司招股说明书、国家密码管理局网站等、开源证券研究所

**商用密码算法体系与标准体系基本形成。**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、量子密钥分配等密码基础理论研究方面取得了一系列的创新科研成果。同时，由我国自主设计的椭圆曲线公钥密码算法 SM2、杂凑算法 SM3、分组密码算法 SM4、序列密码算法 ZUC、标识密码算法 SM9 等已经成为国际标准、国家标准或密码行业标准，标志着我国商用密码算法体系已经基本形成。

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。

**各行业出台密码应用相关政策要求。**以金融行业为例，2012 年，工信部和公安部通告了 RSA1024 算法被破解的风险，中国人民银行要求各银行对网上银行等信息系统进行国产密码算法改造，向多家银行发布了《银行业国产密码应用总体规划》及《总体方案》征求意见稿；同年，人民银行转发了发改委的试点通知并建议网银用户 5000 万以上的银行参与网银系统国密算法改造试点项目。2014 年国务院转发了多部门联合制定的《金融领域密码应用指导意见》（国办发【2014】6 号），要求各金融机构 5 年内完成在网上银行、移动支付、网上证券等重点领域国产密码算法的全面应用。2018 年中共中央办公厅、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 年)》，再次强调在金融和重要领域推动密码升级改造，并在任务分工清单中明确指出，加快推进采用我国密码技术的基础软硬件产品研制和规模应用。

**表4：多行业也出台了密码应用相关政策要求**

行业	时间	部门	文件
金融	2012 年	中国人民银行	《银行业国产密码应用总体规划》
	2014 年	国务院	《金融领域密码应用指导意见》
	2014 年	证监会	《关于加强证券期货领域国产密码应用推进工作的通知》
	2018 年	中共中央办公厅、 国务院办公厅	《金融和重要领域密码应用与创新发展工作规划（2018-2022 年）》
政府	2020 年	国务院办公厅	《国家政务信息化项目建设管理办法》
教育	2019 年	教育部	《教育行业密码应用与创新发展实施方案》
	2018 年	国家能源局	《关于加强电力行业网络安全工作的指导意见》
交通	2021 年	工信部	《关于开展车联网身份认证和安全信任试点工作的通知》

资料来源：FreeBuf 网站、中国电子银行网等、开源证券研究所

## 2.2、以密评为抓手，合规驱动下商用密码市场有望加速发展

商用密码应用安全性评估（简称“密评”）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、正确性和有效性等进行评估。密评工作的责任主体是涉及国家和社会公共利益的重要领域网络和信息系统的建设、使用、管理单位。

密评最早于 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：**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。

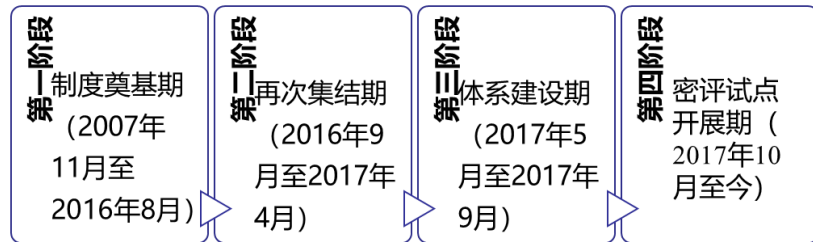
**第二阶段，再次集结期（2016 年 9 月至 2017 年 4 月）**。国家密码管理局成立起草小组，研究起草《商用密码应用安全性评估管理办法（试行）》。2017 年 4 月 22 日，正式印发《关于开展密码应用安全性评估试点工作的通知》（国密局（2017）138 号文），在七省五行业开展密评试点。

**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-43-0054-2018 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。

图13：我国密评发展经历了四个阶段



资料来源：江苏省国家密码局网站、开源证券研究所

密评主要依据被测信息系统通过评审的密码应用方案和 GM/T 0054-2018《信息系统密码应用基本要求》，从总体要求、物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、密钥管理以及安全管理等方面开展评估。

表5：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

单元测评内容	测评指标
物理和环境安全测评	物理和环境安全测评
	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
网络和通信安全测评	密码服务
	密码产品
	身份鉴别
	通信数据完整性
设备和计算安全测评	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
设备和计算安全测评	密码产品
	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
	系统资源访问控制信息完整性
设备和计算安全测评	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

单元测评内容	测评指标
应用和数据安全测评	密码产品
	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
	重要数据传输机密性
	重要数据传输机密性
	重要数据传输机密性
	不可否认性
	密码服务
	密码产品

资料来源：中国评测、开源证券研究所

**等保三级以上信息系统每年至少进行一次密评。**根据 2017 年国家密码管理局发布的《商用密码应用安全性评估管理办法(试行)》第十条规定“关键信息基础设施、网络安全等级保护第三级及以上信息系统，每年至少评估一次”。同时，《网络安全等级保护条例（征求意见稿）》第四十七条：第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，委托密码应用安全性测评机构开展密码应用安全性评估。网络通过评估后，方可上线运行，并在投入运行后，每年至少组织一次评估。

**密改与密评有望带来 108 亿增量市场/年。(1)密评有望带来 36 亿/年市场空间。**根据我们估算，全国等保三级以上信息系统数量在 3 万个左右；根据我们对采招网密评项目的统计，密评价格平均在 12 万/次，由此测算密评有望带来 36 亿/年市场空间。**(2)密评有望催生更大的国密改造市场。**根据我们对采招网国密改造项目的统计，假设国密改造项目平均金额在 120 万元左右，则国密改造存量市场空间为 360 亿元左右。我们保守假设国密改造在未来 5 年内做完，那么平均每年的增量市场在 72 亿左右。综合来看，密改与密评有望带来 108 亿增量市场/年。

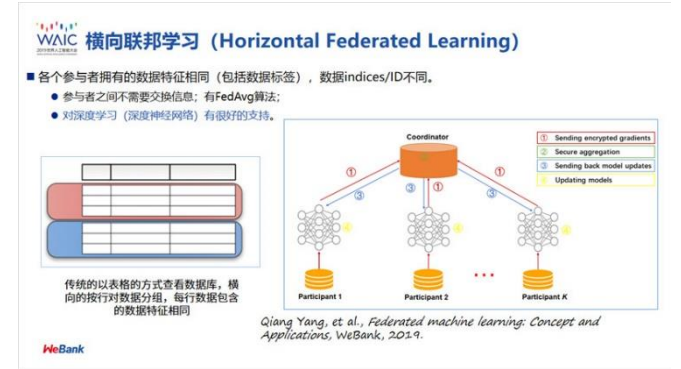
### 2.3、数据安全需求旺盛，有望推动密码行业创新发展

**数据交易市场加速落地，数据安全问题首当其冲，密码技术在数据安全中扮演日益重要的角色。**密码技术作为促进数据流动的主要保障能力，能够促进法律监管制度的软着陆，实现数据价值挖掘和隐私保护的平衡，有助于数据流通共享和协同应用。借助于多方安全计算、同态加密、零知识证明、差分隐私和可信计算等为代表的现代密码技术，在保证原始数据安全隐私性的同时，可实现对数据的计算和分析，可为多数据流通融合场景提供安全、高效的合作模式。

#### (1) 联邦学习

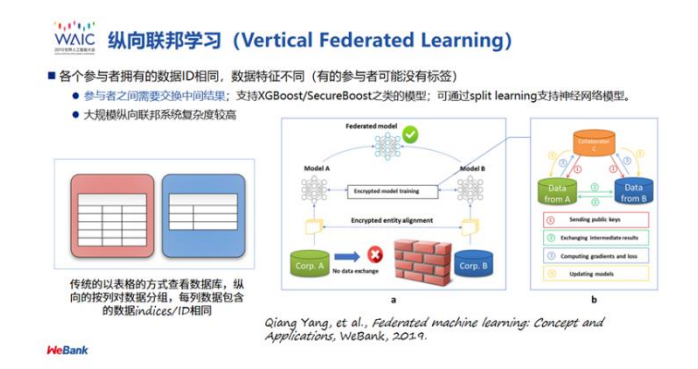
联邦学习是一种分布式机器学习技术和系统，其核心思想是通过在多个拥有本地数据的数据源之间进行分布式模型训练，在不需要交换本地个体或样本数据的前提下，仅通过交换模型参数或中间结果的方式，构建基于虚拟融合数据下的全局模型，从而实现数据隐私保护和数据共享计算的平衡，即“数据可用不可见”、“数据不动模型动”的应用新范式。

图14：横向联邦学习主要应用于各个参与方的数据集有相同的特征空间和不同的样本空间的场景



资料来源：第一财经、开源证券研究所

图15：纵向联邦学习主要适用于数据集上具有相同的样本空间、不同的特征空间的参与方所组成的场景

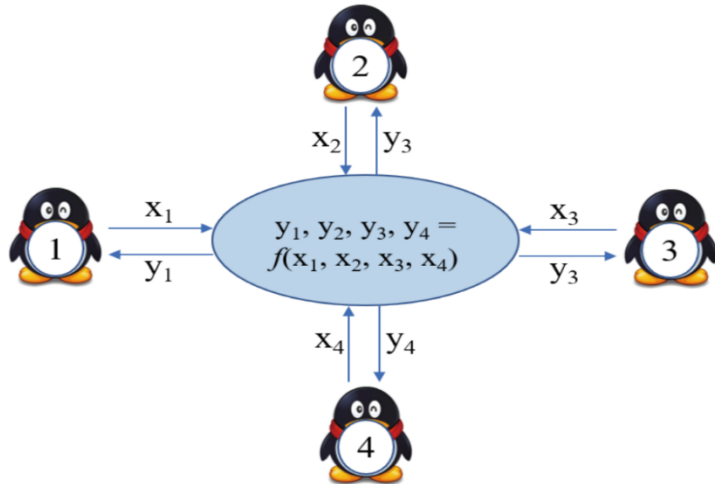


资料来源：第一财经、开源证券研究所

## (2) 多方安全计算

多方安全计算是一种在参与方不共享各自数据且没有可信第三方的情况下安全地计算约定函数的技术和系统。通过安全的算法和协议，参与方将明文形式的数据加密后或转化后再提供给其他方，任一参与方都无法接触到其他方的明文形式的数据，从而保证各方数据的安全。安全多方计算的基本安全算子包括同态加密、秘密分享、混淆电路、不经意传输、零知识证明、同态承诺等。解决特定应用问题的安全多方计算协议包括隐私集合求交、隐私信息检索及隐私统计分析等。由于多方安全计算需要消耗大量的计算和通信资源，目前应用更加适用于小规模数据量，并且应用主要是聚焦相对简单的统计、查询等类型的计算，而基于多方安全计算的联合建模框架只能支持相对简单的机器学习模型，如逻辑回归模型等。

图16：多方安全计算提供更加安全的联合数据分析能力



资料来源：腾讯隐私计算白皮书

## (3) 可信计算

可信计算指借助硬件 CPU 芯片实现可信执行环境 (TEE)，从而构建一个受保护的“飞地” (Enclave)，对于应用程序来说，它的 Enclave 是一个安全的内容容器，用于存放应用程序的敏感数据与代码，并保证它们的机密性与完整性。可信计算 (TEE) 是基于硬件和密码学原理的隐私计算方案，相比于纯软件解决方案，具有较高的通用性、易用性和较优的性能。其缺点是需要引入可信方，即信任芯片厂商。此外由



于 CPU 相关实现属于 TCB，侧信道攻击也成为不可忽视的攻击向量，需要关注相关漏洞和研究进展。

由于技术路径的不同，各类隐私计算技术均有其更加适用的场景：多方安全计算技术不依赖硬件且具备较高的安全性，但是仅支持一些相对简单的运算逻辑；可信执行环境技术具备更好的性能和算法适用性，但是对硬件有一定依赖；联邦学习技术则可以解决复杂的算法建模问题，但是性能存在一定瓶颈。

**表6：由于技术路径的不同，各类隐私计算技术均有其更加适用的场景**

技术	多方安全计算	可信执行环境	联邦学习
安全机制	基于密码学原理 对数据加密	引入可信硬件	数据不动、模型动
性能	低-中	高	高
通用性	高	中	低
高效性	中	中	低
准确性	高	高	中-高
可控性	高	中	高
保密性	高	中-高	中
可信方	不需要	需要	不需要
整体描述	开发难度大、性能提升迅速	易开发、性能佳、 但需信任芯片厂商 (Intel\ARM)	综合运用各类密码学方法、主要针对机器学习

资料来源：信通院、开源证券研究所

## 2.4、信创与密码有望实现相互促进，协同发展

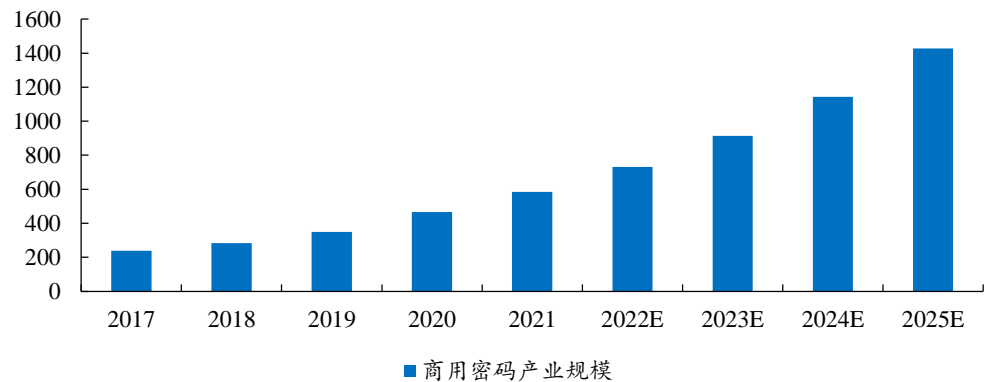
**信创布局中亟待补齐密码技术安全对抗能力。**密码作为保障数据安全的关键核心技术，本身就属于信创重要的组成部分，反过来又能为信创提供最经济有效的安全防护。以国家政务信息化建设为例，根据 2020 年国务院办公厅发布的《国家政务信息化项目建设管理办法》，项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。这就意味着在政务信息系统进行信创改造的同时，需要同步进行密码保障系统的建设。

**密码安全本身也是信创产业的重要环节。**过去的密码产品大多基于国外的芯片/操作系统进行设计开发，随着国内芯片/操作系统等基础硬件和软件产品的成熟，密码产品的全面国产化也成为必然趋势。简言之，我们认为信创与密码有望实现相互促进，协同发展。

## 2.5、我们预测，到 2025 年国内商用密码市场有望超千亿元

**近年来我国商用密码产业规模不断扩大。**根据赛迪智库报告，2021 年我国商用密码产业规模达到 585 亿元，较 2020 年增长 25.54%。我们认为在多重利好刺激下，2022-2025 年商用密码市场有望实现 25% 的复合增长率，预计到 2025 年国内商用密码市场将达到 1400 亿元。



**图17：我国商用密码产业规模不断扩大**


数据来源：赛迪智库、开源证券研究所（2022-2025 年数据由开源证券研究所预测）

### 3、核心竞争力分析：技术实力领先，全产业链布局优势明显

#### 3.1、坚持产品研发、升级迭代，技术实力行业领先

公司的安全等级二级和三级产品数量均位于行业前列。密码产品的安全等级越高，其自身的安全防护能力越强，密码产品的安全性越高，可应用于更高安全等级的网络信息系统。安全等级三级密码产品的安全要求提升较大，研制技术难度高，一定程度上反映了商用密码企业的研发创新能力，国内目前仅有少数几家企业具备安全等级三级产品的资质。

**表7：国内目前仅有少数几家企业具备安全等级三级产品的资质**

安全等级	数量
安全三级	5
安全二级	982
安全一级	369

数据来源：公司公告、开源证券研究所

公司的密码板卡于 2019 年 4 月获得国内首个密码模块安全等级三级认证、密码整机于 2020 年 12 月获得密码模块安全等级三级认证、FIPS 密码整机于 2019 年 10 月获得国内首个 FIPS 140-2 Level 3（美国联邦信息处理标准 3 级）安全认证。截至目前，公司的安全等级二级和三级产品数量均位于行业前列。

**表8：公司的安全等级二级和三级产品数量均位于行业前列**

排名	公司名称	安全等级三级	安全等级二级	安全等级一级
1	三未信安	2	24	6
2	江南天安	1	18	8
3	渔翁信息	0	21	0
4	卫士通	0	18	3

数据来源：公司公告、开源证券研究所

根据 Market Research Intellect 2021 年统计，公司在 2020 年全球密码硬件安全市场（Global Hardware Security Module Market）中位列第九、国内第三，说明公司在行业内的综合实力领先。

**表9：公司在全球密码硬件安全市场中位列第九**

全球排名	公司名称
1	Gemalto
2	Yubico
3	Atos SE
4	THALES
5	Ultra Electronics
6	卫士通
7	江南天安
8	Ultimaco
9	三未信安

资料来源：公司招股说明书、开源证券研究所

密码板卡与卫士通的主要性能指标相近，综合各项指标整体处于行业先进水平。公司在密码板卡的核心技术方面不断突破创新，经历了从 DSP 处理器、FPGA 芯片到自主研发密码芯片的新型技术体系的演变。2019 年，公司推出了国内第一款安全三级密码板卡 SJK1926。2020 年，公司研发的全平台云密码板卡使密码技术在云计算场景中得到广泛运用。2021 年，公司基于自主研发的 XS100 密码安全芯片，完成了新一代 PCI-E 密码板卡的研发，是公司密码板卡历史上具有里程碑式的重要节点，将成为公司将来主推的密码板卡产品。公司将持续不断地对进行产品研发、升级迭代，保持密码板卡在行业中的技术领先优势。

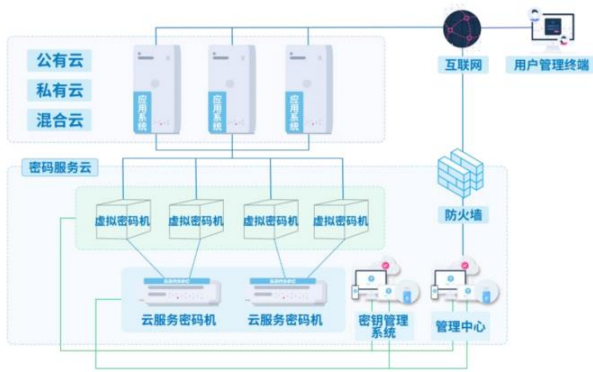
**表10：公司密码板卡综合各项指标整体处于行业先进水平**

性能指标	三未信安	三未信安	卫士通	卫士通
	SJK1828	SJK1926	SJK1752	SJK1866-G
SM2 加密/解密 (Tps)	1500/2600	30000/40000	30/30	-
SM2 签名/验签 (Tps)	2400/1500	56000/39000	30/30	50000/45000
SM2 密钥对生成(Tps)	3000	56000	-	-
SM3 (Mbps)	50	1100	1000	700
SM4 (Mbps)	135	7800	1000	700

数据来源：公司招股说明书、开源证券研究所

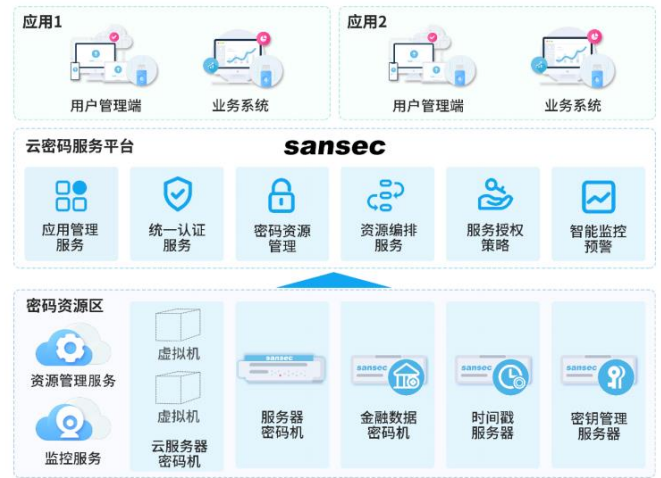
公司将云计算安全作为重要的战略方向，是国内最早布局云计算密码产品的厂商之一。目前，公司已经研发出业内领先的云密码机和云密码服务平台。云密码机解决了传统密码机在云环境下部署的资源效率低等问题，其采用密钥管理与设备管理分离的核心理念，实现了云应用环境下网络管理员维护设备，用户自行管理密钥的工作模式。公司的云密码机具备业内领先的内置集群能力，通过密码机集群与虚拟化技术的结合扩充密码运算能力，提高密码设备资源的利用率，并通过集中的密钥管理及配套的安全策略保护用户密钥整个生命周期的安全。云密码服务平台基于微服务架构，实现应用系统统一安全接入、密码资源统一管理和调度，并面向合作伙伴开放密码服务接口规范，保证了密码服务灵活扩展。

图18：云密码机实现了云应用环境下网络管理员维护设备，用户自行管理密钥的工作模式



资料来源：公司招股说明书

图19：云密码服务平台基于微服务架构，实现应用系统统一安全接入、密码资源统一管理和调度



资料来源：公司招股说明书

根据公司发展战略，公司将构建完善丰富的云密码产品体系，研发更高性能的SR-IOV 硬件虚拟化技术的云密码板卡，为云应用提供硬件级密钥隔离能力，有效解决云中的密钥安全问题；研发云密码资源池，为云计算提供具备虚拟化能力的密码服务，通过弹性扩容和灵活调度实现云中密码资源的高效利用；研发云密钥管理系统，支持海量密钥安全管理能力，采用 KMIP 协议实现密钥的安全管理。

### 3.2、全产业链布局，有望实现规模化发展

回顾公司发展历程，公司起家于密码板卡业务，并不断向产业链上下游延伸。2009 年，公司开发研制了 SJK0930 密码板卡及 SJJ0930 服务器密码机产品；2015 年，公司成功研制密钥管理系统，通过国际通用的 KMIP 操作协议完成密钥安全使用；2020 年，公司首款 X100 芯片成功流片，至此公司形成了完备的拥有自主知识产权的商用密码产品体系。

(1) 向下游拓展密码系统业务有利于拓展市场空间，提升与用户的粘性。密码系统通过整合公司密码软件和硬件产品优势，形成综合性的整体密码解决方案，通过丰富的密码功能有效支撑大型业务系统的多样化的密码需求。

(2) 向上游拓展密码芯片业务有利于提升产品性能，满足自主可控要求。公司密码芯片的投产将实现公司现有密码板卡、密码整机等产品的芯片国产化替代和性能提升，保障公司核心技术的自主可控和供应链安全、提高公司产品的竞争力。

## 4、布局自主密码芯片，进一步打开成长空间

历经 6 年布局，公司于 2021 年成功推出自主密码芯片。2015 年开始，为了解决现有密码芯片性能低、功能弱以及 FPGA 芯片依赖国外进口的不利局面，公司开始布局密码芯片研发，重点聚焦密码算法高性能运算、FPGA 开发和 PCI-E 高速数据传输三大核心技术的研发，为密码芯片奠定了良好的技术积累。2016 年，完成了 SM2、SM3、SM4、SM9 等国产密码算法软件研发，建立完善的具有自主知识产权的密码算法体系，并集成到公司的密码产品中；2017 年，完成了 SM2、SM3、SM4、SM9 等国产密码算法的 FPGA 硬件研发，突破了密码板卡的高速 PCI-E 数据通信、SR-IOV 硬件虚拟化等技术瓶颈，并应用到密码产品中；2018 年，将国产密码算法、

高速 PCI-E 接口、SR-IOV 硬件虚拟化等核心技术在 FPGA 芯片板卡进行验证，进行密码芯片的前期研发工作。

2018 年 11 月，公司成立全资子公司山东多次方，专注于密码芯片研发；2019 年，集中进行密码芯片的研发工作，完成密码芯片设计、编码、后端设计、验证等主要工作；2020 年，完成密码芯片的全部开发和 MPW 工作；2020 年 12 月，公司第一款密码芯片 XS100 流片成功，全部功能和性能均达到预期目标；2021 年，完成基于 XS100 芯片的 PCI-E 密码板卡、密码整机的开发和验证；2021 年 10 月，通过国家密码管理局商用密码检测中心检测，并取得商用密码产品认证证书。2022 年 9 月，公司完成了第一批密码芯片 XS100 的量产，正在全面推向市场。

**XS100 密码安全芯片**主要用于 PKI、SSL VPN、IPSec VPN、云计算、大数据等信息安全场景，可集成在 PCI-E 密码板卡、密码整机、安全服务器等产品中，为云计算、大数据等场景提供海量数据加密和高性能数字签名等功能。XS100 芯片采用 RISC-V 指令集 CPU，支持各种对称、非对称和杂凑算法，采用 PCIE2.0 接口，支持 SR-IOV 硬件虚拟化，公司 XS100 密码安全芯片除外购的通用 IP 核及涉及技术外，其他核心密码技术具有自主知识产权。

**图20：XS100 密码安全芯片主要用于 PKI、VPN、云计算、大数据等信息安全场景**

 <p><b>XS100</b></p>	<ul style="list-style-type: none"> <li>●采用 RISC-V 处理器，最高工作频率 400Mhz</li> <li>●国内领先的高性能密码算法引擎，主流国密算法性能达到先进水平</li> <li>●支持 SM1、SM2、SM3、SM4、SM7、SM9 国密算法</li> <li>●支持 AES、DES、3DES、RSA1024、RSA2048、RSA4096 等国际算法</li> <li>●真随机数发生器，符合 GM/T 0005-2012 及 NIST SP800-22 标准</li> <li>●SR-IOV 硬件虚拟化功能，单芯片最大支持 64 个虚拟机</li> <li>●安全可靠的密钥管理功能</li> <li>●丰富的通信接口：UART、I2C、SPI、QSPI、SMC、GPIO 等</li> </ul>
---	---

资料来源：公司招股说明书

**XS100 密码安全芯片集合 6 个芯片的功能。**公司 XS100 密码安全芯片通过多种关键技术协同应用，实现芯片内部各个功能模块的高速互联能力，将公司原密码板卡中 FPGA 芯片、主控芯片、SM1 算法芯片、SM2 算法芯片、RSA 算法芯片、随机数芯片等 6 个独立芯片及其功能高度集成为 1 芯片，集中完成了包括对称算法引擎、非对称算法引擎、算法调度模块、片内 COS、片内高速总线模块、硬件虚拟化模块等密码功能。

**表11：XS100 密码安全芯片集合 6 个芯片的功能**

原独立芯片名称	原独立芯片功能	XS100 密码功能	对应的核心技术
FPGA 芯片	可编程器件芯片，公司使用该芯片进行自研编码设计以实现 PCI-E 高速链路功能及 AES、DES、SM4、SM3、SM2、RSA 等算法	算法调度模块、片内高速总线模块、硬件虚拟化模块	1、高性能密码算法硬件实现技术 2、SR-IOV 硬件虚拟化技术 3、高速 PCI-E 通信技术
主控芯片	为公司自研的密钥管理及算法调度等程序提供计算资源	片内 COS	4、高可靠的硬件设计



原独立芯片名称	原独立芯片功能	XS100 密码功能	对应的核心技术
SM1 算法芯片	提供 SM1 算法功能	对称算法引擎	技术
SM2 算法芯片	提供 SM2 算法功能	非对称算法引擎	5、高安全密码模块设计技术
RSA 算法芯片	提供 RSA 算法功能	非对称算法引擎	
随机数芯片	提供真随机数功能	对称算法引擎	

资料来源：公司公告、开源证券研究所

**XS100 密码安全芯片可以大幅提升产品的稳定性、安全性，同时提升产品性价比。**公司通过高性能密码算法硬件实现技术、高速 PCI-E 通信技术等核心技术的协同应用，研制出的 XS100 密码安全芯片集合了 6 芯片的功能，芯片的核心性能指标大幅提升，同时基于 XS100 单芯片的产品设计，可以大幅降低产品的复杂度，提高产品的可靠性。此外 XS100 芯片可以有效降低采购成本，提高产品的性价比。根据公司招股说明书，XS100 密码芯片的 SM1 加解密速度 9.8Gbps、SM2 签名速度 30 万次每秒；同时相对于原独立芯片组合，XS100 还增加了对 SM3、SM9 等国密算法的支持，其中 SM3 运算速度 9.6Gbps、SM9 签名速度 1,000 次每秒，以上算法性能指标较外购芯片实现了大幅提升。

**表12：相较于外购芯片，XS100 密码安全芯片的核心性能指标大幅提升**

项目	外购芯片						XS100 芯片
	FPGA 芯片	主控 芯片	SM1 芯片	SM2 芯片	RSA 芯片	随机数 芯片	
PCI-E 通信	✓	×	×	×	×	×	✓
CPU	×	✓	×	×	×	×	✓
SM1 加解密 (Gbps)	×	×	1	×	×	×	9.8
SM2 签名 (Tps)	×	×	×	50,000	×	×	300,000
SM3 (Gbps)	×	×	×	×	×	×	9.6
SM4 加解密 (Gbps)	7	×	×	×	×	×	9.5
SM7 加解密 (Gbps)	×	×	×	×	×	×	0.9
RSA2048 签名 (Tps)	×	×	×	×	1,000	×	10,000
SM9 签名 (Tps)	×	×	×	×	×	×	1,000
AES 加解密 (Gbps)	1	×	×	×	×	×	8
DES 加解密 (Gbps)	0.4	×	×	×	×	×	3
随机数 (Mbps)	×	×	×	×	×	20	40

数据来源：公司公告、开源证券研究所

**XS100 密码芯片的综合核心功能指标达到国内公司先进水平。**公司 XS100 密码芯片与苏州国芯、北京宏思、恩智浦等密码芯片公司的主流产品相比，核心指标各有优势，公司在产品设计中选择多项指标领先的原则，以便适应不同合作厂商不同场景的广泛性需求，因此公司产品功能较为全面。

**表13：XS100 密码芯片的综合核心功能指标达到国内公司先进水平**

芯片厂商	三未信安	苏州国芯	苏州国芯	北京宏思	恩智浦
芯片型号	XS100	CCP903T-H	CCP908T	HSMD1-H	C291
CPU	32 位 RISC-V	32 位 C9000	32 位 C9000	-	32 位 E500



芯片厂商	三未信安	苏州国芯	苏州国芯	北京宏思	恩智浦
芯片型号	XS100	CCP903T-H	CCP908T	HSMD1-H	C291
主频	400MHz	600MHz	1.2GHz	-	667MHz
通用接口					
PCI-E	2.0X4	2.0X4	3.0X8	-	2.0X4
USB	-	有	有	有	无
SPI	有	有	有	有	有
UART	有	有	有	有	有
I2C	有	有	有	有	有
GPIO	有	有	有	有	有
EMIF	有	-	-	有	-
算法					
SM1 加解密 (Gbps)	9.8	-	-	3	-
SM4 加解密 (Gbps)	9.5	7	30	3	-
AES 加解密 (Gbps)	9	7	30	-	6
DES 加解密 (Gbps)	4	3.2	30	-	-
SM3 (Gbps)	9.6	8.5	30	3	-
SM2 签名 (Tps)	300,000	18,000	150,000	120,000	40,000
SM9 签名 (Tps)	1,000	-	-	-	-
RSA2048 签名 (Tps)	10,000	7,400	8,000	6,800	8,000
随机数	有	有	有	-	有
安全启动	有	有	有	-	有
密钥封装保护	有	有	有	-	有
访问权限控制	有	有	有	-	有
温度检测	-	有	有	-	有
电压检测	-	有	有	-	-
硬件虚拟化 (VF)	64	-	-	-	-

资料来源：公司招股说明书、开源证券研究所（注：“-”代表该公司在公开渠道未披露相关指标数据，为其产品的非核心功能）

**XS100 芯片系目前唯一支持硬件虚拟化的密码安全芯片。**XS100 密码芯片中采用的 SR-IOV 硬件虚拟化技术可以将一个密码设备虚拟成多个密码设备，并确保各密码虚机之间密钥互相隔离，杜绝越界访问及非法访问。XS100 密码芯片的硬件虚拟化技术在提升密码资源性能的同时并降低了多虚机环境下的密码资源集成成本，灵活有效地满足云计算环境下的海量密码需求。XS100 核心功能指标的先进和硬件虚拟化功能来源于公司自主研发的高性能密码算法软硬件实现技术、高速 PCI-E 传输和数据处理技术和云计算的密码服务虚拟化及海量密钥管理技术。

**表14：公司在密码领域有明显优势，密码芯片的核心密码技术先进**

核心技术	技术先进性	技术来源	知识产权
高性能密码算法硬件实现技术	密码算法的快速实现是密码芯片和设备最重要的核心技术，该技术有效优化了运算性能，解决了传统密码运算性能的衰减和密码设备的性能瓶颈，实现网络加密的高性能调度。公司密码芯片 SM2 签名速度突破 30 万次每秒、SM1 加解密速度 9.8Gbps、SM3 运算速度 9.6Gbps、SM4 加解密速度 9.5Gbps。	自研	一种基于椭圆曲线的分布式签名方法及系统；一种基于 RSA 的分布式签名方法。
SR-IOV 硬件虚拟化技术	该技术在提升密码资源性能的同时并降低了多虚拟机环境下的密码资源集成成本，灵活有效地满足云计算环境下的海量密码需求。虚拟化和密钥管理技术集成到密码芯片中，是高性能密码芯片的重要功能。公司密码芯片系目前唯一支持硬件虚拟化芯片产品。	自研	一种 SR-IOV 环境下多虚拟机并发 DMA 的顺序调度方法及系统。
高速 PCI-E 通信技术	该技术解决了密码芯片的通信瓶颈问题，为密码芯片的高性能实现奠定了基础。	自研+外购	自研主要包括基于 PCI-E 协议的高速数据处理方法，解决密码芯片的通信瓶颈，形成两个相关专利：一种对 CPLD 数据包进行有序存储的方法及系统；一种基于 PCIe 接口的密码卡及该密码卡的数据加密方法。 外购主要是通用的 PCI-E 协议相关 IP，分为两部分：PCI-E 控制器和 PCI-E PHY
高可靠的硬件设计技术	该技术可以提升产品的可靠性，设计研发高性价比、低成本的产品，满足物联网、工业互联网等场景的需求。	自研	一种 PCI 密码卡和海量密钥密码运算方法及系统
高安全密码模块设计技术	该技术设计了高安全密码模块的安全防护机制，实现了高安全物理安全防护、防测信道攻击保护、软件固件安全防护等技术，可以达到密码模块安全三级水平，是公司高安全等级产品的核心技术。	自研	一种安全升级 PCI 码卡卡内程序的方法及系统

资料来源：公司公告、开源证券研究所

密码芯片 XS100 的推出不仅能够提升公司自身产品的性能及安全性，同时也有望实现批量化销售，进一步打开公司成长空间。一方面，密码芯片 XS100 首先将满足公司自用需求，完成公司现有密码板卡、密码整机等产品的芯片国产化替代和性能提升，保障公司核心技术的自主可控和供应链安全、提高公司产品的竞争力。而且 XS100 集合 6 个芯片的功能，能够降低公司生产成本，提升毛利率水平。

另一方面，公司未来的芯片发展战略将重点关注两个领域：一是面向云计算和大数据安全领域，研制高性能、高可靠、支持虚拟化技术的密码芯片，为 PCI-E 密码板卡、密码整机、IPSec VPN、SSL VPN、安全服务器等提供核心密码部件；二是

面向物联网安全领域，研制适用于边缘网关的高安全、高可靠的密码安全芯片，支持各种物联网终端的安全接入和安全协议，用于物联网边缘安全网关的核心密码部件，实现大规模产业化推广。未来公司芯片有望实现批量化销售，打开更大的市场空间。

## 5、盈利预测与投资建议

### 5.1、核心假设

**(1) 收入端：**在密评、信创及数据安全多重驱动下，随着下游市场的拓展，公司密码系统业务有望高速发展，预计 2023-2025 年增速分别为 50%、40%、35%；预计密码整机收入维持快速增长，2023-2025 年增速分别为 20%、20%、20%；预计密码板卡收入保持稳定增长，2023-2025 年收入增速分别为 15%、15%、15%；

**(2) 毛利率：**未来几年公司毛利率有望保持较高水平，我们预计公司 2023-2025 年销售毛利率为 75.07%、74.92%、74.46%。

**(3) 期间费用率：**我们预计公司 2023-2025 年销售费用率为 14.50%、14.50%、14.50%；管理费用率为 8.42%、8.22%、8.22%；研发费用率为 18.00%、17.50%、17.00%。

### 5.2、盈利预测与投资建议

我们预计公司 2023-2025 年归母净利润为 1.59、2.23、2.97 亿元，EPS 分别为 2.07、2.90、3.86 元/股，当前股价对应 PE 分别 55.8、39.9、29.9 倍。公司估值高于同行可比公司平均估值，考虑公司在商密市场全产业链布局及在密码芯片领域的领先地位，首次覆盖给予“买入”评级。

表15：公司 PE 高于行业可比公司平均水平（截止 2023.4.25 收盘）

证券代码	公司简称	当前市值（亿元）	归母净利润（亿元）			PE		
			2023E	2024E	2025E	2023E	2024E	2025E
688201.SH	信安世纪	66.00	2.65	3.36	-	24.91	19.64	-
003029.SZ	吉大正元	58.00	2.56	3.50	4.50	22.66	16.57	12.89
603232.SH	格尔软件	37.00	1.44	2.20	-	25.69	16.82	-
688262.SH	国芯科技	154.00	3.03	4.70	-	50.83	32.77	-
	行业平均					31.02	21.45	-
<b>688489.SH</b>	<b>三未信安</b>	<b>89.00</b>	<b>1.59</b>	<b>2.23</b>	<b>2.97</b>	<b>55.83</b>	<b>39.91</b>	<b>29.93</b>

数据来源：Wind、开源证券研究所（注：吉大正元、格尔软件、国芯科技盈利预测来自 Wind 一致预期；信安世纪和三未信安盈利预测来自开源证券研究所）

## 6、风险提示

**(1) 市场竞争加剧风险。**随着国家政策的大力支持，我国网络信息安全行业市场规模保持快速增长的趋势，良好的市场机遇可能导致新的竞争者数量不断增多，网络信息安全市场竞争将更加激烈，公司面临市场竞争加剧的风险。

**(2) 密码芯片业务拓展不及预期。**如果密码芯片推向市场延期时间较长，可能对公司的经营和发展产生不利影响。

**附：财务预测摘要**

资产负债表(百万元)	2021A	2022A	2023E	2024E	2025E
<b>流动资产</b>	363	1848	2139	2349	2758
现金	134	1471	1577	1691	1850
应收票据及应收账款	177	317	410	524	654
其他应收款	2	3	60	28	90
预付账款	4	11	5	17	13
存货	42	40	84	85	147
其他流动资产	4	6	4	5	5
<b>非流动资产</b>	106	126	115	128	136
长期投资	0	0	0	0	0
固定资产	21	25	31	39	49
无形资产	7	13	13	13	12
其他非流动资产	78	88	71	76	76
<b>资产总计</b>	469	1974	2255	2477	2894
<b>流动负债</b>	67	70	196	194	314
短期借款	5	0	0	0	0
应付票据及应付账款	21	27	91	127	173
其他流动负债	41	44	105	67	141
<b>非流动负债</b>	15	20	15	17	17
长期借款	0	0	0	0	0
其他非流动负债	15	20	15	17	17
<b>负债合计</b>	82	90	212	211	331
少数股东权益	0	0	0	0	0
股本	57	77	77	77	77
资本公积	208	1577	1577	1577	1577
留存收益	122	229	389	612	909
<b>归属母公司股东权益</b>	387	1883	2043	2266	2563
<b>负债和股东权益</b>	469	1974	2255	2477	2894

现金流量表(百万元)	2021A	2022A	2023E	2024E	2025E
<b>经营活动现金流</b>	30	-6	113	136	182
净利润	75	107	159	223	297
折旧摊销	5	7	10	14	14
财务费用	-1	-2	-2	-2	1
投资损失	0	0	0	0	0
营运资金变动	-56	-128	-59	-98	-131
其他经营现金流	7	9	4	-1	-0
<b>投资活动现金流</b>	-71	-20	-4	-25	-22
资本支出	71	20	5	6	9
长期投资	0	0	0	0	0
其他投资现金流	0	0	1	-19	-14
<b>筹资活动现金流</b>	-7	1362	-3	3	-1
短期借款	-5	-5	0	0	0
长期借款	0	0	0	0	0
普通股增加	0	20	0	0	0
资本公积增加	10	1370	0	0	0
其他筹资现金流	-13	-22	-3	3	-1
<b>现金净增加额</b>	-48	1337	106	114	159

利润表(百万元)	2021A	2022A	2023E	2024E	2025E
<b>营业收入</b>	270	340	473	654	883
营业成本	71	83	118	164	226
营业税金及附加	2	2	3	3	4
营业费用	43	54	69	95	128
管理费用	24	27	40	54	73
研发费用	50	68	85	114	150
财务费用	-1	-2	-2	-2	1
资产减值损失	-0	-2	-13	-15	-18
其他收益	9	16	17	21	25
公允价值变动收益	0	0	0	0	0
投资净收益	0	0	0	0	0
资产处置收益	0	-0	-0	-0	-0
<b>营业利润</b>	85	111	165	231	308
营业外收入	0	0	0	0	0
营业外支出	1	0	0	1	1
<b>利润总额</b>	84	111	165	231	307
所得税	9	4	5	8	10
<b>净利润</b>	75	107	159	223	297
少数股东损益	0	0	0	0	0
<b>归属母公司净利润</b>	75	107	159	223	297
EBITDA	85	74	130	195	269
EPS(元)	0.97	1.39	2.07	2.90	3.86

主要财务比率	2021A	2022A	2023E	2024E	2025E
<b>成长能力</b>					
营业收入(%)	33.5	25.7	39.1	38.3	35.1
营业利润(%)	42.9	31.0	48.7	39.9	33.4
归属于母公司净利润(%)	42.8	43.5	48.7	39.9	33.4
<b>获利能力</b>					
毛利率(%)	73.6	75.5	75.1	74.9	74.5
净利率(%)	27.6	31.6	33.7	34.1	33.7
ROE(%)	19.3	5.7	7.8	9.8	11.6
ROIC(%)	17.4	3.4	5.6	7.7	9.5
<b>偿债能力</b>					
资产负债率(%)	17.5	4.6	9.4	8.5	11.4
净负债比率(%)	-28.8	-77.0	-76.4	-73.9	-71.5
流动比率	5.4	26.2	10.9	12.1	8.8
速动比率	4.7	25.4	10.4	11.6	8.2
<b>营运能力</b>					
总资产周转率	0.6	0.3	0.2	0.3	0.3
应收账款周转率	1.9	1.4	1.3	1.4	1.5
应付账款周转率	3.9	3.5	2.0	1.5	1.5
<b>每股指标(元)</b>					
每股收益(最新摊薄)	0.97	1.39	2.07	2.90	3.86
每股经营现金流(最新摊薄)	0.39	-0.08	1.47	1.77	2.37
每股净资产(最新摊薄)	5.03	24.48	26.55	29.45	33.31
<b>估值比率</b>					
P/E	119.0	82.9	55.8	39.9	29.9
P/B	23.0	4.7	4.4	3.9	3.5
EV/EBITDA	102.7	100.5	56.6	37.0	26.3

数据来源：聚源、开源证券研究所

请务必参阅正文后面的信息披露和法律声明

## 特别声明

《证券期货投资者适当性管理办法》、《证券经营机构投资者适当性管理实施指引（试行）》已于2017年7月1日起正式实施。根据上述规定，开源证券评定此研报的风险等级为R4（中高风险），因此通过公共平台推送的研报其适用的投资者类别仅限定为专业投资者及风险承受能力为C4、C5的普通投资者。若您并非专业投资者及风险承受能力为C4、C5的普通投资者，请取消阅读，请勿收藏、接收或使用本研报中的任何信息。因此受限于访问权限的设置，若给您造成不便，烦请见谅！感谢您给予的理解与配合。

## 分析师承诺

负责准备本报告以及撰写本报告的所有研究分析师或工作人员在此保证，本研究报告中关于任何发行商或证券所发表的观点均如实反映分析人员的个人观点。负责准备本报告的分析师获取报酬的评判因素包括研究的质量和准确性、客户的反馈、竞争性因素以及开源证券股份有限公司的整体收益。所有研究分析师或工作人员保证他们报酬的任何一部分不曾与，不与，也将不会与本报告中具体的推荐意见或观点有直接或间接的联系。

## 股票投资评级说明

	评级	说明
证券评级	买入（Buy）	预计相对强于市场表现 20%以上；
	增持（outperform）	预计相对强于市场表现 5%~20%；
	中性（Neutral）	预计相对市场表现在-5%~+5%之间波动；
	减持（underperform）	预计相对弱于市场表现 5%以下。
行业评级	看好（overweight）	预计行业超越整体市场表现；
	中性（Neutral）	预计行业与整体市场表现基本持平；
	看淡（underperform）	预计行业弱于整体市场表现。

备注：评级标准为以报告日后的 6~12 个月内，证券相对于市场基准指数的涨跌幅表现，其中 A 股基准指数为沪深 300 指数、港股基准指数为恒生指数、新三板基准指数为三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）、美股基准指数为标普 500 或纳斯达克综合指数。我们在此提醒您，不同证券研究机构采用不同的评级术语及评级标准。我们采用的是相对评级体系，表示投资的相对比重建议；投资者买入或者卖出证券的决定取决于个人的实际情况，比如当前的持仓结构以及其他需要考虑的因素。投资者应阅读整篇报告，以获取比较完整的观点与信息，不应仅仅依靠投资评级来推断结论。

## 分析、估值方法的局限性说明

本报告所包含的分析基于各种假设，不同假设可能导致分析结果出现重大不同。本报告采用的各种估值方法及模型均有其局限性，估值结果不保证所涉及证券能够在该价格交易。



## 法律声明

开源证券股份有限公司是经中国证监会批准设立的证券经营机构，已具备证券投资咨询业务资格。

本报告仅供开源证券股份有限公司（以下简称“本公司”）的机构或个人客户（以下简称“客户”）使用。本公司不会因接收人收到本报告而视其为客户。本报告是发送给开源证券客户的，属于商业秘密材料，只有开源证券客户才能参考或使用，如接收人并非开源证券客户，请及时退回并删除。

本报告是基于本公司认为可靠的已公开信息，但本公司不保证该等信息的准确性或完整性。本报告所载的资料、工具、意见及推测只提供给客户作参考之用，并非作为或被视为出售或购买证券或其他金融工具的邀请或向人做出邀请。本报告所载的资料、意见及推测仅反映本公司于发布本报告当日的判断，本报告所指的证券或投资标的的价格、价值及投资收入可能会波动。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。客户应当考虑到本公司可能存在可能影响本报告客观性的利益冲突，不应视本报告为做出投资决策的唯一因素。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。本公司未确保本报告充分考虑到个别客户特殊的投资目标、财务状况或需要。本公司建议客户应考虑本报告的任何意见或建议是否符合其特定状况，以及（若有必要）咨询独立投资顾问。在任何情况下，本报告中的信息或所表述的意见并不构成对任何人的投资建议。在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。若本报告的接收人非本公司的客户，应在基于本报告做出任何投资决定或就本报告要求任何解释前咨询独立投资顾问。

本报告可能附带其它网站的地址或超级链接，对于可能涉及的开源证券网站以外的地址或超级链接，开源证券不对其内容负责。本报告提供这些地址或超级链接的目的纯粹是为了客户使用方便，链接网站的内容不构成本报告的任何部分，客户需自行承担浏览这些网站的费用或风险。

开源证券在法律允许的情况下可参与、投资或持有本报告涉及的证券或进行证券交易，或向本报告涉及的公司提供或争取提供包括投资银行业务在内的服务或业务支持。开源证券可能与本报告涉及的公司之间存在业务关系，并无需事先或在获得业务关系后通知客户。

本报告的版权归本公司所有。本公司对本报告保留一切权利。除非另有书面显示，否则本报告中的所有材料的版权均属本公司。未经本公司事先书面授权，本报告的任何部分均不得以任何方式制作任何形式的拷贝、复印件或复制品，或再次分发给任何其他人，或以任何侵犯本公司版权的其他方式使用。所有本报告中使用的商标、服务标记及标记均为本公司的商标、服务标记及标记。

## 开源证券研究所

### 上海

地址：上海市浦东新区世纪大道1788号陆家嘴金控广场1号楼10层  
邮编：200120  
邮箱：research@kysec.cn

### 深圳

地址：深圳市福田区金田路2030号卓越世纪中心1号楼45层  
邮编：518000  
邮箱：research@kysec.cn

### 北京

地址：北京市西城区西直门外大街18号金贸大厦C2座9层  
邮编：100044  
邮箱：research@kysec.cn

### 西安

地址：西安市高新区锦业路1号都市之门B座5层  
邮编：710065  
邮箱：research@kysec.cn