

西部证券股份有限公司

关于

渔翁信息技术股份有限公司

首次公开发行股票并在科创板上市

之

上市保荐书

保荐机构（主承销商）

  
WESTERN

**西部证券股份有限公司**  
WESTERN SECURITIES CO.,LTD.

（陕西省西安市新城东大街319号8幢10000室）

## 目 录

目 录 .....	1
声 明 .....	2
一、发行人概况 .....	3
(一) 发行人基本情况 .....	3
(二) 主营业务 .....	3
(三) 发行人的技术与研发情况 .....	4
(四) 近三年主要财务数据和财务指标 .....	19
(五) 发行人存在的主要风险 .....	20
二、本次发行情况 .....	24
三、保荐代表人、项目协办人及项目其他组成员情况 .....	25
四、保荐人与发行人的关联关系、保荐人及其保荐代表人是否存在可能影响公正履行保荐责任情形的说明 .....	26
五、保荐人对发行人是否就本次证券发行上市履行相关决策程序的说明 .....	27
(一) 董事会 .....	27
(二) 股东大会 .....	27
六、保荐人对发行人是否符合科创板定位的专业判断 .....	27
(一) 公司符合科创板行业领域要求 .....	27
(二) 公司符合科创属性指标 .....	28
七、保荐人对公司是否符合上市条件的说明 .....	29
八、保荐人按照有关规定应当承诺的事项 .....	30
九、对公司持续督导期间的工作安排 .....	31
十、保荐人认为应当说明的其他事项 .....	32
十一、保荐人对本次股票上市的推荐结论 .....	32

## 声 明

保荐人及其保荐代表人已根据《中华人民共和国公司法》(以下简称《公司法》)、《中华人民共和国证券法》(以下简称《证券法》)等法律法规和中国证监会及上海证券交易所的有关规定,诚实守信,勤勉尽责,严格按照依法制定的业务规则和行业自律规范出具上市保荐书,并保证所出具文件真实、准确、完整。

如无特别说明,本上市保荐书中简称与《渔翁信息技术股份有限公司首次公开发行股票并在科创板上市招股说明书(申报稿)》中具有相同含义。

## 上海证券交易所：

渔翁信息技术股份有限公司（以下简称“渔翁信息”、“发行人”或“公司”）拟申请首次公开发行股票并在科创板上市。西部证券股份有限公司（以下简称“西部证券”、“保荐人”或“保荐机构”）认为发行人的上市符合《公司法》《证券法》及《上海证券交易所科创板股票上市规则》的有关规定，特推荐其股票在贵所科创板上市交易。现将有关情况报告如下：

### 一、发行人概况

#### （一）发行人基本情况

公司名称：渔翁信息技术股份有限公司

英文名称：Fisherman Information Technology Co., Ltd.

注册资本：5,539.2960 万元

法定代表人：郭刚

成立日期：1998 年 11 月 26 日

整体变更日期：2008 年 6 月 10 日

住所：山东省威海市火炬高技术产业开发区初河北路 12-1 号

邮政编码：264209

公司电话：0631-5706168

传真号码：0631-5706168

互联网网址：<https://www.fisec.cn>

电子信箱：[ywxxzq@fisherman-it.com](mailto:ywxxzq@fisherman-it.com)

负责信息披露和投资者关系的部门：董事会办公室

负责人：房宝龙

#### （二）主营业务

渔翁信息是国内领先的商用密码产品和解决方案提供商，是国家级专精特新“重点小巨人”企业。公司致力于服务“信创产业”国家战略，现为国家“信创

工委”密码应用组组长单位，是国产密码信创战略的重要推动者。公司多项技术成果经国家科学技术委员会鉴定为“填补国内空白，整体技术达到了国内领先水平”。

公司是商用密码产业链典型中上游厂商，以信创产业为牵引，以密码技术为支撑，逐步向产业链下游拓展。公司已形成“基础密码+云数据安全+工控安全”三大密码产品和服务体系。产品主要包括密码模块、密码设备和密码系统等，广泛应用于政府、金融、能源和电信等国民经济重点领域，为国家网络安全建设提供有力支撑。

### **（三）发行人的技术与研发情况**

#### **1、公司核心技术情况**

经过二十多年的技术和经验积累，公司掌握了 15 项具有自主知识产权的核心技术。截至本报告签署日，公司已经累计取得 20 项发明专利、111 项软件著作权。

##### **（1）公司主要核心技术及技术来源**

公司主要产品中的核心技术、技术来源、技术特点和技术成熟度等方面的具体情况如下：

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品与服务	所处阶段
1	高性能密码运算多核并行技术	该技术基于 FPGA 半定制能力，内部采用流水线方式设计算法运算指令，算法运算过程中可同时执行不同的算法指令，提高密码算法运算速度。同时将核心运算模块拆分为多个运算核，每个核心都能独立完成密码算法运算，从而让密码模块能够同时并行处理多个请求	自主研发	原始创新	ZL201711259834.4	已授权	基础密码产品	成熟应用
					ZL201710891937.6			
2	高性能密码 DMA 异构处理技术	该技术可将 CPU 从繁重的读写任务中解放出来，转而执行其他任务。既支持传统 DMA 方式，也支持离散聚合的 DMA 方式，配合散列表等相关技术，优化算法执行效率，在高性能密码运算场景下更具优势	自主研发	原始创新	ZL201710891936.1	已授权	基础密码产品	成熟应用
					ZL201710891966.2			
					ZL201710891146.3			
3	密码芯片堆叠技术	该技术采用密码芯片堆叠及并行处理的方式提升密码运算性能，通过运算过程中密钥安全同步，保证芯片之间协同计算结果一致性。通过并行处理极大的提升了算法运算能力，该技术尤其适用于对加解密要求高的大数据处理场景	自主研发	原始创新	ZL201710891146.3	已授权	基础密码产品	成熟应用
					ZL201710854402.1			
4	高并发架构密码服务技术	该技术结合高并发网络框架和多线程资源池实现了密码处理过程的高并发，能够同时为多个应用系统提供长链接条件下的数据并发处理能力，并能够实现断链修复及设备故障切换功能	自主研发	原始创新	ZL201910349532.9	已授权	基础密码产品	成熟应用
					ZL202111133462.7			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品与服务	所处阶段
5	全加密状态下数据透明处理技术	该技术实现数据库中结构化数据加密过程的透明处理，应用系统代码零改动。同时解决了数据库加密密文检索效率低下的问题，能够防止非授权用户查看数据库敏感信息和对数据库进行拖库操作	自主研发	原始创新	ZL202111065801.2	已授权	云数据安全产品	成熟应用
					ZL201310642937.4			
6	面向云计算的高封装密码服务中台技术	该技术实现各类密码设备、密码服务的资源化管理，在逻辑上将系统密码服务分为为基础密码中台和业务密码服务中台，屏蔽底层密码设备，降低应用使用密码的复杂度。该技术实现了密码服务资源统一管理，通过密码服务中台技术实现对云上各类密码设备的管理和分析	自主研发	原始创新	ZL201711080191.7	已授权	云数据安全产品	成熟应用
					ZL201810200505.0			
					ZL201610885095.9			
7	容器云安全防护技术	该技术可提升容器云环境下安全防护能力，基于国产密码技术，结合容器云可信识别架构，自动识别跟踪数据包在整个容器云中的流向。并能够根据不同安全策略实现对容器云中应用和主机的安全防护，同时能够对网络攻击包进行追溯、告警、拦截	自主研发	原始创新	ZL202111083778.X	已授权	云数据安全产品	成熟应用
8	基于无 IP 网络隐身通信加密技术	该技术结合网络数据包透明传输技术，将设备模拟成一个不需要 IP 地址的网络透传设备，并对流经的 MAC 和 IP 地址数据进行加密处理。对访问位于该设备后的服务器的数据包进行过滤，可以有效保护后方设备的安全。同时未经授权的探测请求被接受前，探测包会被我方设备屏蔽，从而让后端设备隐身	自主研发	原始创新	ZL200910020501.5	已授权	工控安全产品	成熟应用
					ZL202111083778.X			
					ZL201910290866.3			

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品与服务	所处阶段
9	基于虚拟网卡国密SSL通信技术	该技术可实现国密 SSL VPN 数据包透明转发，应用系统无感知，应用系统零改造即可与国密 SSL VPN 结合，该技术可广泛拓展国密 SSL VPN 适用场景及数据加密层级	自主研发	原始创新	ZL200910020501.5	已授权	云数据安全产品	成熟应用
					ZL201610318667.5			
					ZL201810200505.0			
					ZL201910349532.9			
10	超大带宽网络数据高并发 VPN 协议技术	该技术利用异步处理技术，通过改造 LINUX 内核源码，优化 IPSec 数据包处理机制，配合密码模块及 CPU 多核并行处理能力，从而提升国密 IPSec VPN 网络数据包处理能力	自主研发	原始创新	ZL200910020501.5	已授权	云数据安全产品	成熟应用
					ZL201710891937.6			
11	国密高性能标识密钥认证体系	该技术基于国产密码算法实现标识密码认证体系，主要应用于 IOT 工控环境下，用于加强边缘工控设备的密码应用及服务能力，提升边缘设备安全接入能力	自主研发	原始创新	ZL202111065801.2	已授权	工控安全产品	成熟应用
					ZL202111565961.3			
12	工控边缘计算安全技术	该技术兼容多种终端工控协议，能够将工控场景下多种协议转换成加密网络数据，并能打通工控终端设备与后台控制系统的安全传输通道，解决工业互联网对异构终端协议与网络协议兼容性和控制指令的安全保护的问题	自主研发	原始创新	ZL201710054906.5	已授权	工控安全产品	成熟应用
13	可重构编程密码芯片技术	该技术通过 FPGA 硬件电路编程，实现密码算法硬件电路层面设计，将复杂的数学原理转换成硬件电路，极大提升密码算法运行效率。通过电路设计封装出 FPGA IP 算法核，便于移植和复用	自主研发	原始创新	ZL201711259834.4	已授权	基础密码产品	成熟应用
14	云环境下大型数据库加	该技术采用大数据缓存结合网络高并发设计，降低云上数据库大量数据申请加	自主研发	原始创新	ZL201711080191.7	已授权	云数据安全产品	成熟应用

序号	技术名称	技术特点	技术来源	技术创新类型	对应的专利及非专利技术	专利状态	相关产品与服务	所处阶段
	解密性能提升技术	密请求时的网络传输瓶颈，提升数据库与密码服务之间的交互能力，降低密码运算过程中数据传输的时间损耗。优化数据库加密过程，从系统内核层优化，降低需要加密的数据量，提升数据库加密速度						
15	IPv6 协议高性能国密算法优化技术	该技术通过对 IPv6 协议数据包进行组包、排序、超时设计，实现 IPv6 网络数据包快速加密处理。设计高效的带有标识的密文数据包异步处理算法，将加密后的数据包能精确返回给原 IPv6 网络包，同时当网络协议处理数据包过程中无需等待，从而提升 IPv6 协议中使用国密算法的效率	自主研发	原始创新	ZL201910349532.9	已授权	云数据安全产品	成熟应用

## (2) 公司核心技术的先进性及具体表征

公司专注于以密码技术为基础的网络安全产品的技术研发与创新应用，凭借优秀的技术研发团队和科技创新能力，目前公司共拥有 15 项核心技术，核心技术的先进性及具体表征如下：

### 1) 高性能密码运算多核并行技术

该技术基于 FPGA 半定制能力，内部采用流水线方式设计算法运算指令，算法运算过程中可以同时执行不同的算法指令，提高密码算法运行速度。同时将核心运算模块拆分为多个运算核，每个核心都能独立完成密码算法运算，从而让密码模块能够同时并行处理多个密码算法请求。

该技术从硬件层面解决密码运算处理瓶颈，大幅度提升密码运算性能，为大文件存储加解密、高带宽网络数据传输加解密等场景提供有力支撑。应用系统通过其提供的密码运算接口即可实现高速数据加解密，业务密码运算过程交由密码卡处理，减少密码运算对硬件 CPU 的占用，极大提升自身业务处理能力。基于上述技术可大幅提升密码卡并行运算能力，在高并发应用场景下显著提升处理性能。

### 2) 高性能密码 DMA 异构处理技术

该技术创新性结合高速的 PCI-E 协议数据传输通道，实现应用层数据与系统内核层数据快速交互，从而提高数据加解密速度。本技术基于 PCI-E 协议实现硬件密码模块与上层操作系统进行高速数据交互。上层应用能够通过 PCI-E 驱动将待加密的数据快速、低延时地发送给密码处理硬件模块进行加密处理，密码计算模块处理完成后能够及时反馈给上层应用。将 CPU 从繁重的读写任务中解放出来，执行其他任务。该技术既支持传统 DMA 方式，也支持最新的、离散聚合的 DMA 方式，配合散列表等相关技术，优化算法执行效率，在高性能密码运算场景下更具优势。

该技术从系统层面进行优化，在系统与密码卡交互通道上充分利用其带宽，将 PCI-E 通道利用率发挥到极致，降低应用与底层密码卡之间的数据传输损耗和延时，全面提升密码卡性能指标。上述技术可广泛应用于密码卡系列产品，通过异步处理机制，显著提升相关产品加解密吞吐能力。

### 3) 密码芯片堆叠技术

在现有密码芯片处理能力一定的情况下,该技术将密码设备密码运算能力再提升一个台阶,从而满足对性能有着更高要求的场景需求。该技术可充分发挥密码芯片的并行处理能力,以提供密码服务的方式提升密码运算性能,同时保证运算过程中密钥安全同步。该技术通过芯片并行处理极大地提高了算法运算能力,尤其适用于对加解密要求高的大数据加密运算场景。

密码芯片堆叠技术能够在国产基础密码芯片由于制程或者算力原因导致性能瓶颈时,通过堆叠方式显著提升密码模块的整体运算能力,完成高性能密码卡构建,并进一步满足大规模密码计算场景下的算力需求。

### 4) 高并发架构密码服务技术

随着云计算、物联网、大数据、5G 等新兴技术的发展,网络安全边界不断弱化,安全防护内容不断增加,对密码服务的性能提出了更高的要求。而传统上要提升系统并发量与性能,一般依赖于增加硬件配置,硬件性能的提升会造成成本增加。本技术将高速密码技术与高并发架构相结合,能够在不增加硬件成本的前提下,更加合理的利用硬件资源以提供高性能、高并发的密码运算服务,使密码服务不再成为业务性能的瓶颈。

该技术使用自主研发的网络高并发架构,优化网络并发能力,实现长链接支持万级并发量,短链接支持百万并发量。能够显著提高系统在大量并发链接下 CPU 的利用率,并且解决了大量并发带来的效率线性下降的问题。与业界普遍采用的技术相比,大幅降低了对 CPU 性能的依赖,提升了 I/O 效率。上述技术可广泛应用于加密机、签名验签服务器等网络服务型密码产品,可大幅度提升密码服务的被调用能力,增强最大并发处理能力。

### 5) 全加密状态下数据透明处理技术

随着密码应用技术推广,对数据的安全要求越来越高,尤其是结构化数据存储都是存放到各类型数据库中,国外或开源数据库本身没有对国密算法的支持,数据库内结构化数据加密已成为一个世界难题。当前大量应用系统开发人员对密码技术了解不深,应用系统设计过程中没有考虑密码安全功能,也没有预留对接接口,如何保证应用无感知状态下完成数据库数据加密变得非常困难。

该技术基于高速缓存技术实现对数据库空间列加密或全库加密，在数据库的数据加密过程中对应用系统完全透明，应用系统代码零改动，同时解决了数据库加密密文检索效率低下的问题。该技术能够防止非授权用户查看数据库敏感信息，防止非法用户拖库，既解决已有应用系统数据加密改造对接困难问题，又能保证数据库存储数据安全可靠。基于本技术可以完成结构化数据加密系统的整体构建，提升结构化数据加解密处理效率，解决信创或非信创等异构数据库的结构化数据加密存储问题。

#### 6) 面向云计算的高封装密码服务中台技术

该技术实现各类密码设备密码服务资源化管理，在逻辑上将系统密码服务分为基础密码中台和业务密码中台两部分，屏蔽底层密码设备，简化应用使用密码服务的复杂度。通过密码服务中台技术实现对云上各类密码设备管理和分析，并结合数字孪生技术，实现密码设备数字化管理，并完成对密码资源使用的精准预警和判断。以“虚拟化”“可视化”“一体化”的理念为云上应用提供可按需分配、弹性伸缩的密码服务。

#### 7) 容器云安全防护技术

基于国产密码技术，结合创新的容器云可信识别架构，能够有效保证容器云中各节点身份的真实性、合法性和不可否认性，防止网络中存在伪造终端，实现 K8S 网络管理的扩展。该技术能够灵活监控 K8S 容器云中网络数据信息，并对各节点的网络包进行控制。对 K8S 框架及业务系统透明部署，对原系统零改造，并能够实现 K8S 容器云中网络数据的全要素采集，实现对网络数据包整个流转生命周期的监控、分析和追溯，为云服务提供更强的网络安全管控能力。

#### 8) 基于无 IP 网络隐身通信加密技术

大量网络设备被攻击根本原因是暴露自身 IP 地址，攻击者针对 IP 地址发起攻击，对服务造成严重破坏。基于无 IP 网络隐身通信加密技术可以将接在隐身设备后方的服务器 IP 地址隐藏，外部的攻击者无法扫描到后方应用服务器，无法发起网络攻击。该技术主要思路是在服务器前串联由该技术实现的隐身设备，隐身设备本身无需配置 IP 地址，在数据经过该隐身设备时，对网络数据包中的 Mac 和 IP 地址进行加密处理，使攻击者无法嗅探被保护设备的 Mac 和 IP 地址，

从而能够保护后方设备。

该技术以创新的方式从网络层面解决网络攻击问题，同时利用该技术的设备可以不用配置 IP 地址，在网络上部署简单方便，可以做到即插即用，大大简化了运维管理及部署工作。该技术适用于工控环境、视频监控等场景，解决接入终端设备数量较多，改造困难等问题，利用该技术可以方便、迅速提升整体网络安全传输及边界安全防护能力。

#### 9) 基于虚拟网卡国密 SSL 通信技术

SSL 协议是在数据传输加密领域广泛应用的网络协议，其为应用层数据加密提供了标准化的解决路径，用于完成应用层密钥协商、数据加密、身份验证等安全控制过程，传统 SSL 通信的应用场景一般局限于应用层，当相关数据基于网络层或传输层传输时，则难以进行加密处理。

通过该技术可将应用层数据加密能力拓展至 IP 层，不仅能够支持 B/S 应用，还能够支持基于 TCP、UDP 协议的其他应用场景，拓展了 SSL 传输加密应用场景及适用性，并保留了 SSL 简易配置易使用的特点，为数据传输加密提供广泛的技术支撑能力，支持 SM1、SM2、SM3、SM4、SM9 等多种国密算法。视频数据、指令数据、路由数据等网络数据信息也可以交由基于虚拟网卡技术的国密 SSL 服务引擎进行处理，数据报文能够在虚拟网卡进行细粒度多层次的处理及访问控制，强化网络访问控制能力，基于虚拟网卡的技术特性，提升了数据加密处理速度，并可扩展至多种数据传输加密应用场景。

#### 10) 超大带宽网络数据高并发 VPN 协议技术

传统 IPSec 协议及网络协议实现依赖 Linux 内核，其调用方式由于 Linux 内核特性，只能基于单一核心进行数据处理及数据处理调度，导致难以发挥加密卡及设备整体性能，其整机加密吞吐量也受限于调用机制，整体性能无法满足越来越高的网络加密带宽需求。

该技术可以解决 IPSec 性能瓶颈问题，大幅提升了网络数据加解密速度和整机吞吐能力，为满足云双活、大型机构加密网络构建等提供支撑能力。

#### 11) 国密高性能标识密钥认证体系

随着物联网技术应用发展，密码技术作为现代网络安全技术的核心，在物联网环境下的安全需求也需要通过密码技术体系解决。传统上物联网安全体系基于的 PKI 证书模式构建，但是由于物联网场景的特殊性，设备运算能力及资源不足，PKI 体系在物联网及工控应用中无法满足分布式、轻量化、实时性和高可用性的安全需求。通过采用标识密钥管理技术，从管理、运维、技术特性等方面更轻量级的满足物联网密码应用需求，成为更好的技术路径。

该技术基于国密算法实现标识密钥认证体系，可以直接使用物联网边缘设备硬件标识码生成标识密钥，降低数据交换量和管理成本，且标识与设备唯一对应，更适合在物联网场景下进行应用。当物联网设备入网时，根据设备唯一性硬件信息生成标识密钥对，标识密钥作为设备入网的认证基础，通过标识算法完成设备本地数据存储加密、数据传输加密、设备身份认证。在技术实践过程中，通过基于国密算法的标识管理系统，对应不同应用场景及性能需求，优化标识管理系统架构，平衡性能与适用性要求。国密算法标识密钥认证技术也可以拓展至视频领域、车联网领域等多种工控应用场景。

#### 12) 工控边缘计算安全技术

工控环境下终端设备数量较为庞大，数据采集、整理、分析工作较为繁琐，大量的计算工作也导致后端服务压力巨大。为解决该问题，当前做法是将部分计算工作前移，放在终端设备中进行。但是，终端设备如何保证数据安全也成为待解决的难题。该技术为适应工控终端设备，兼容多种终端工控协议如 MODBUS-RTU、MODBUS-TCP 和 MQTT 等，能够将工业控制中多种协议转换成加密网络数据，并能打通工控终端设备与后台控制系统的安全传输通道，解决工业控制中对异构终端协议与网络协议兼容性问题和对中数据传输和控制指令的安全保护问题。

该技术将数据采集、数据加密转发和协议处理融为一体，采用国密 SM3、SM4、SM9 等国密算，解决水利、交通、能源等领域大量终端边缘计算安全问题，同时也降低工控终端系统对接开发的难度。

#### 13) 可编程密码芯片技术

FPGA 芯片包含了可重构编程逻辑模块的数量、固定功能逻辑模块（如乘法

器)的数目及存储器资源的大小。该技术基于可重构编程逻辑实现的算法是硬件密码算法,通过与、或、非等基础门电路,配合 RAM、状态机等实现算法,通过串并转换和乒乓操作的方式提升芯片的运算主频,通过流水线、模块复制的方式实现多个逻辑模块的并行处理,使得基于可重构编程逻辑实现的算法在性能上都远超过基于 CPU 指令等实现的软件算法。

可重构编程逻辑处理器系统的建立,不但需要快速的算法运算能力,还要有完整的管理能力。该处理器系统无需外部芯片,直接使用内部逻辑处理完成全部运算过程,外设配置灵活,与可重构编程逻辑通信便利,并且节省硬件设计资源。基于该技术实现 SM9 等算法电路设计和 IP 核封装,为标识密码算法提供硬件支撑,提高了算法运算效率,推动算法快速普及。

#### 14) 云环境下大型数据库加解密性能提升技术

该技术采用大数据缓存结合网络高并发设计,降低云上数据库大量数据申请加密请求时的网络传输瓶颈,提升数据库与密码服务之间的交互能力,降低密码运算过程中数据传输的时间损耗。优化数据库加密过程,对于数据库文件采用 FDE 模式加密防护,加密过程在操作系统内核层面,无用户态与内核态的数据交互,极大提升数据加解密速度。在系统内核层提升数据保护的安全性,在内核中精准对应需要加密的数据库文件,从而降低需要加密的数据量,提升数据库加密速度。

该技术从数据库访问到加密数据存取等各个环节进行优化,最大限度降低各个环节的性能损失,保证云环境下大型数据库在大数据量操作情况下,数据加解密性能能够满足业务需要,从而促进密码技术在云上大数据保护场景下落地生效。

#### 15) IPv6 协议高性能国密算法优化技术

IPv6 安全性机制和服务更加紧密结合,并将安全作为自身标准的有机组成部分,通过 IPv6 中的 IPSec 可以对 IP 层上的通信提供加密/授权,可以实现远程企业内网的无缝接入和连接。认证报头(AH)用于保证数据的一致性,而封装的安全负载报头(ESP)用于保证数据的保密性和数据的一致性。在 IPv6 包中,AH 和 ESP 都是扩展报头,可以同时使用,也可以单独使用其中一个。无论是 AH 还是 ESP,都需要使用国密算法进行国密改造,从而加强 IPv6 协议自身的安

全性。该技术通过对 IPv6 协议数据包进行组包、排序、超时设计，实现 IPv6 网络数据包快速加密处理。设计高效的带有标识的密文数据包异步处理算法，将加密后的数据包精确返回给原有 IPv6 网络包中，同时网络协议处理数据包过程中无需等待，从而提升 IPv6 协议中使用国密算法的效率。

该技术通过国密算法改造提升了 IPv6 协议自身的安全性，且提升了网络数据加解密的吞吐效率，减少由于加密运算带来的网络延时，保障 IPv6 网络环境下数据传输的安全高效，有利于 IPv6 技术的全面推广。

### （3）公司来源于核心技术的收入金额和占比情况

公司主营业务为商用密码产品的研发、生产、销售及服务，打造了“基础密码+云数据安全+工控安全”三大密码产品及服务体系，上述产品及相关技术服务的销售收入均来源于公司的核心技术。

报告期内，公司来源于核心技术的收入占营业收入比例如下表所示：

单位：万元、%

项目	2022年1-6月	2021年度	2020年度	2019年度
来源于核心技术的销售收入	2,954.67	10,298.25	5,620.44	2,743.10
营业收入	3,087.77	10,699.69	5,731.83	2,976.32
占营业收入的比例	95.69	96.25	98.06	92.16

### （4）核心技术保护措施

为保护核心技术和知识产权，公司建立知识产权贯标体系、信息安全管理体系统、保密管理体系，通过相关认证并保持有效运行与不断改进。同时，公司也对核心技术人员提供有竞争力的薪酬待遇、股权激励等机制，避免核心技术人员的流失。

公司重要的技术保护措施包括但不限于：

1) 知识产权保护：公司贯彻《企业知识产权管理规范》国家标准，对于公司核心技术积极申请专利、软件著作权等，提高核心技术的法律保护力度。

2) 物理和环境安全防护：定义安全区域，配备门禁、监控等设备，防止对办公场所和信息的未授权访问，破坏和干扰。

3) 访问控制：制定访问控制策略，避免信息系统的非授权访问，包括网络访问控制，操作系统访问控制，应用系统和信息访问控制，监视系统访问和使用，定期检测未授权的活动。

4) 保密管理：公司成立以总经理为组长的保密委员会，明确各相关负责人的保密管理职责与分工，定期进行保密培训与保密检查，确保保密工作得到有效实施。重大项目开始前，组织专题保密培训会议，根据需要签订《保密责任书》，以减少人为差错、泄密或误操作的风险。

5) 人员管理：所有员工入职时签订《劳动合同》《保密协议》，并进行专题培训，确定任职期间的知识产权归属，承诺保守公司的技术秘密与商业秘密信息。调离岗位时，必须移交其掌握的商业秘密、核心技术资料，工作电脑在保密委员会的监督下做好清理工作。

## 2、在研项目

目前公司正在从事的研发项目具体情况如下：

序号	项目名称	研发子项目	所处阶段	预算投入 (万元)	预计达到的目标	研发项目及成果技术水平	研究领域
1	基础密码产品 关键技术研究 及产品开发	基于国产芯片的高性能密码卡研发	已完成关键技术实现,处于产品测试阶段	202	实现低功耗密码卡,提升密码卡兼容性和性能	实现高速 SM2、SM3、SM4 算法 降低加密卡功耗,拓展应用领域 统一密码卡驱动框架,优化算法调用步骤	基础密码领域
2		支持多场景应用的安全协同签名系统研发	目前项目已完成需求分析,处于设计开发阶段	131	丰富系统支持场景,提升算法性能	支持安卓、苹果等常用终端设备,支持 PC 端环境,提升系统签名能力	基础密码领域
3		支持全系列类型的密钥管理系统 V2.0 开发	目前项目已完成需求分析,处于设计开发阶段	137	完成 JS 组件升级,实现国密 0051 规范,完成 KMIP 支持	符合国标 0051 规范,支持 KMIP 规范	基础密码领域
4	面向云计算及大数据的新一代密码技术及产品研发	基于云计算的密码服务及监管平台研发	已完成项目设计开发,处于系统测试阶段	382	实现标准化、一体化密码服务管理系统,实现密码设备监管	实现密码资源的集中管理 实现密码资源的统一监控 实现密码资源的分配管理 实现域内设备监管 实现设备运行数据分析 实现动态监测	云计算密码服务应用领域
5		云数据加密存储系统研发	已完成项目设计开发,处于系统测试阶段	53	实现基于国产密码算法的数据安全存储	数据存储加密性能大幅提升 数据存储细粒度控制 数据加密存储高可用	云数据安全领域
6		基于国密技术的万兆加密网关研发	已完成项目设计开发,处于集成测试阶段	157	实现万兆加密能力	充分发挥 CPU+加密卡性能 拓展协议及算法应用模式	大数据网络通信安全领域
7	基于国产密码技术的终端安全应用开发	基于国产密码技术的终端安全应用系统研发	已完成关键技术的研究,处于系统开发阶段	117	实现硬盘及数据保护、手机通信保密	基于国密技术的手机通信保密,支持语音、信息、文件加密;保护硬盘被非法拿走,防止数据泄密	数据安全领域
8	区块链安全技术研究与产品开发	基于复杂客体的大规模区块链安全协同技术研究与产品研发	基础研究阶段	700	实现区块链及应用安全的密码支撑服务	提出复杂数据处理智能合约模型,完成复杂客体数据的可信传递 研发区块链协同管理平台,实现大规模分布式区块链数据的安全协同	区块链密码应用领域

### 3、研发投入情况

为保持技术领先优势，增强公司的核心竞争力，公司高度重视技术和新产品的研发工作。2019年-2022年6月，研发费用分别为744.57万元、890.36万元、1,128.30万元和536.89万元，占营业收入的比重分别为25.02%、15.53%、10.55%和17.39%。

报告期内，公司研发费用的构成及占营业收入的比例如下：

单位：万元、%

项目	2022年1-6月	2021年度	2020年度	2019年度
研发支出	536.89	1,128.30	890.36	744.57
营业收入	3,087.77	10,699.69	5,731.83	2,976.32
占比	17.39	10.55	15.53	25.02

### 4、研发人员和核心技术人员情况

#### （1）公司研发人员情况

截至2022年6月30日，公司拥有研发人员52人，占总人数28.11%。公司主要研发人员具有丰富的专业理论知识和实践操作经验。报告期内主要研发人员未发生重大变动。

#### （2）核心技术人员情况

公司核心技术人员认定依据如下：

1) 为公司核心技术领域的主导或主要人员，拥有深厚且与公司业务相匹配的资历背景和丰富的研发及技术经验；

2) 在公司研发及技术方面承担重要职责，为提升公司核心技术水平做出重要贡献；

3) 为公司获得专利等知识产权或研发项目落地发挥重要作用；

4) 认同公司的核心价值观，愿意与公司长期发展。

报告期内，公司的核心技术人员共4人，报告期内，公司核心技术人员没有发生变化。

#### （3）核心技术人员对公司研发的具体贡献情况

序号	姓名	参与专利情况
1	郭刚	一种防止可读写数据被复制的方法及装置, JCE 调用密码卡实现内置 RSA 密钥运算方法及装置, 一种数据加解密方法及系统, 一种网络数据并行加解密处理方法、装置和介质, 密钥处理方法、装置及电子装置, 一种数据处理系统及方法, 数据处理方法、装置及电子装置, 一种无 IP 设备的工作状态检测方法、装置和介质, 一种便携式应用登录装置, 一种身份认证装置, 一种密码卡及安全数据终端
2	宋志华	一种防止可读写数据被复制的方法及装置, JCE 调用密码卡实现内置 RSA 密钥运算方法及装置, 一种 DMA 读操作的处理方法、系统及相关设置, 一种密码卡多算法并列执行的方法、系统及相关装置, 一种密码卡中 DMA 请求的处理方法、系统及相关装置, 一种加解密装置及方法, 一种密码卡算法资源的分配方法、系统及相关装置, 一种基于云网络的安全通道建立系统, 一种数据加解密方法及系统, 一种密码卡及对数据处理的方法, 一种调用 USB KEY 底层库的方法及装置, 密钥处理方法、装置及电子装置, 一种密码卡及安全数据终端
3	徐波	JCE 调用密码卡实现内置 RSA 密钥运算方法及装置, 一种 DMA 读操作的处理方法、系统及相关设置, 一种密码卡多算法并列执行的方法、系统及相关装置, 一种密码卡中 DMA 请求的处理方法、系统及相关装置, 一种加解密装置及方法, 一种密码卡算法资源的分配方法、系统及相关装置, 一种基于云网络的安全通道建立系统, 一种密码卡及对数据处理的方法
4	殷秀静	一种账户注册方法、系统、设备和计算机可读存储介质(已授权, 尚未取得证书), 一种账户管理方法、系统、设备及计算机可读存储介质(已受理, 未授权), 一种对等短信传输方法、系统、设备及计算机存储介质(已受理, 未授权); 密钥申请方法及装置、电子设备、计算机可读存储介质(已受理, 未授权), 基于区块链的数据交易方法、装置、存储介质及电子装置(已受理, 未授权)

#### (4) 核心技术人员实施的约束激励措施

核心技术人员均与公司签订了《劳动合同》和《保密协议》，确定任职期间的知识产权归属，承诺保守公司的技术秘密或商业秘密信息。公司对核心技术人员实施了股权激励，核心技术人员直接持有或通过员工持股平台间接持有公司股份。

#### (四) 近三年主要财务数据和财务指标

项目	2022.6.30 /2022年1-6月	2021.12.31 /2021年度	2020.12.31 /2020年度	2019.12.31 /2019年度
资产总额(万元)	18,579.19	21,808.01	8,741.95	6,204.55
归属于母公司股东权益(万元)	15,172.07	17,489.13	6,341.27	3,238.34
资产负债率(合并)(%)	18.34	19.80	27.36	47.81
资产负债率(母公司)(%)	17.39	19.00	26.64	47.07
营业收入(万元)	3,087.77	10,699.69	5,731.83	2,976.32

项目	2022.6.30 /2022年1-6月	2021.12.31 /2021年度	2020.12.31 /2020年度	2019.12.31 /2019年度
净利润(万元)	497.03	3,927.67	1,926.29	554.37
归属于母公司股东的净利润(万元)	497.03	3,925.18	1,932.15	554.37
扣除非经常性损益后归属于母公司股东的净利润(万元)	348.84	3,778.05	1,773.40	346.05
基本每股收益(元/股)	0.09	0.76	0.46	0.16
稀释每股收益(元/股)	0.09	0.76	0.46	0.16
加权平均净资产收益率(%)	3.24	46.06	41.24	18.77
经营活动产生的现金流量净额(万元)	-276.35	1,867.93	1,230.87	108.08
现金分红(万元)	2,999.81	-	-	-
研发投入占营业收入的比例(%)	17.39	10.55	15.53	25.02

## (五) 发行人存在的主要风险

### 1、技术风险

#### (1) 技术升级迭代风险

当前，新兴技术的快速发展对密码技术提出了新的挑战。在激烈的市场竞争下，若公司不能及时对市场需求和技术发展趋势做出精准研判，及时对现有技术和产品进行迭代升级并研发出市场认可的新产品，或市场上出现在功能、性能等方面更具优势的密码产品，则可能对公司的竞争能力和持续发展产生不利影响。

#### (2) 技术泄露风险

公司在长期研发创新和生产实践中积累了一系列使公司保持竞争优势的核心技术。当前，公司通过专利、软件著作权申请等方式对核心技术进行有效保护，同时与核心技术人员签署了保密及竞业禁止协议，有效约束技术涉密人员的个人行为。未来如果公司经营过程中由于人员的重大疏忽或舞弊等行为导致公司核心技术泄密，将对公司的市场竞争力和持续发展产生不利影响。

### 2、经营风险

#### (1) 产业政策变化风险

近年来，国家相继出台了《网络安全法》《密码法》《数据安全法》《软件和

信息技术服务业发展规划（2021—2025年）》和《关于推动资本市场服务网络强国建设的指导意见》等法律法规和一系列产业政策，为行业的快速发展提供了良好的政策支持环境。未来如果国家相关产业政策支持力度发生变化，将会对公司的经营业绩和业务发展产生不利影响。

#### （2）经营业绩季节性波动风险

报告期内，公司第四季度收入占比较高，存在明显的行业季节性特征，2019-2021年，第四季度收入占比分别为55.98%、43.35%和55.07%。公司经营业绩季节性波动主要系最终用户的采购特点所致。公司最终用户主要集中在政府、金融、能源和电信等重要领域，上述用户实行集中采购制度和预算管理制度，通常上半年对年度采购进行预算立项、设备选型测试，下半年进行集中招标、采购和项目建设、验收。与之相匹配，公司的收入主要集中在第四季度确认，而公司人员薪酬、研发费用及折旧摊销等各项费用发生相对均衡，导致公司经营业绩存在季节性波动。

#### （3）密码产品所需进口外围芯片存在价格上涨或供应紧张的风险

公司商用密码产品的核心芯片均为国产，产品所需外围芯片正逐步国产替代，近期申请认证的信创产品已全部采用国产芯片。报告期内，公司对进口外围芯片需求整体呈下降趋势，但因进口芯片的价格上涨和提前备货等因素影响，进口芯片采购金额占比依然较高。2019-2021年，公司进口外围芯片的采购金额占比分别为33.33%、42.84%和28.78%。

未来，若国际贸易摩擦、地缘政治加剧等因素造成公司进口芯片价格大幅上涨或供应紧张，一方面，进口芯片的价格上涨，导致公司产品成本增加；另一方面，供应紧张甚至断供情况下，公司需对进口外围芯片进行国产替代，届时可能面临国产芯片价格上涨或因性能适配等延长产品交付周期的问题，进而对公司的生产经营造成不利影响。

#### （4）原材料价格波动的风险

公司商用密码产品生产需要的原材料主要为芯片、主板、PCB等，报告期内，公司产品的直接材料占营业成本的比例为80%以上。未来若宏观经济形势、半导体行业波动及市场供需发生变化，可能会导致公司原材料采购价格上升，进

而导致公司产品的生产成本增加，对公司的经营业绩产生不利影响。

#### （5）市场竞争风险

国家政策的大力支持，新兴技术的不断发展，催生了新的信息安全需求，行业将迎来快速增长期。虽然公司产品和技术具有一定先发优势，但目前市场参与者较多，市场集中度较低。未来，随着越来越多的企业参与到行业中，公司将面临更加激烈的市场竞争，进而对公司经营业绩产生一定影响。

#### （6）人力资源风险

公司所处行业是知识密集型的行业，业务发展高度依赖核心技术团队的研发能力和技术水平，稳定的核心技术团队对公司持续经营至关重要。若公司未来无法为核心技术人才提供有竞争力的薪酬水平、激励措施和发展空间，将可能导致核心技术人才流失。同时，在国家信创产业的浪潮下，如果公司人才储备不能满足业务快速发展的需求，将对公司的持续经营带来不利影响。

#### （7）公司规模相对较小、抗风险能力较弱的风险

报告期内，公司营业收入分别为 2,976.32 万元、5,731.83 万元、10,699.69 万元和 3,087.77 万元，净利润分别为 554.37 万元、1,926.29 万元、3,927.67 万元和 497.03 万元，收入及利润规模相对较小。相比于同行业上市公司，发行人抗风险能力较弱。未来若行业政策、市场竞争环境、公司经营状况或下游市场需求等因素出现重大不利变化，将会对公司经营业绩产生一定影响。

### 3、内控风险

#### （1）内控及公司治理风险

随着公司业务的发展和本次募投项目的实施，公司将进入一个新的发展阶段，将在战略规划、业务拓展、产品研发、内部控制等方面对管理层提出更高的要求。若公司的组织模式和管理制度未能及时进行调整与完善，管理水平未能随着规模扩张而进一步提升，公司将一定程度上面临因规模扩张导致的管理风险。

#### （2）实际控制人不当控制的风险

本次发行前，郭刚、刘桂华合计控制公司 90.35% 的股份。本次发行完成后，郭刚、刘桂华仍将控制公司 67.76% 的股份，公司股权较为集中。虽然公司已建

立较为完善的治理结构，但若实际控制人利用其控制地位，通过行使表决权对发行人发展战略、经营决策、关联交易和利润分配等重大事项进行不当控制，则可能损害公司及中小股东的利益。

#### 4、财务风险

##### (1) 应收账款回收风险

报告期各期末，公司应收账款账面价值分别为 1,222.37 万元、2,005.12 万元、5,150.69 万元和 3,267.09 万元，占流动资产的比例分别为 30.04%、30.03%、26.40% 和 20.17%，应收账款金额占比较高。

未来随着业务规模不断扩大，公司应收账款占比仍可能保持在较高水平。如果因宏观经济形势、行业景气度、客户资金周转等因素发生重大不利变化，客户延迟付款或无法支付货款，公司应收账款面临不能及时回收或无法回收的风险，将对公司资产质量和财务状况产生不利影响。

##### (2) 存货减值风险

报告期各期末，公司存货账面价值分别为 1,232.97 万元、1,916.03 万元、3,209.15 万元和 4,426.85 万元，占当期期末流动资产的比例分别为 30.30%、28.70%、16.45% 和 27.33%。

报告期内，公司未发生大额存货减值的情形。随着公司业务规模不断扩大，公司存货金额预计将持续增长。若未来公司市场开拓不力，则可能产生因产品滞销带来的存货跌价风险，对公司经营业绩产生不利影响。

##### (3) 税收优惠政策变化的风险

报告期内，公司享受企业所得税和软件产品增值税即征即退等税收优惠政策，公司享受的税收优惠金额占当期利润总额的比例分别为 37.09%、16.63%、22.25% 和 34.39%。如果未来公司不满足上述税收优惠政策，无法继续享有税收优惠，公司经营业绩将受到不利影响。同时若未来国家上述税收优惠政策发生重大不利变化，将对公司经营成果带来不利影响。

#### 5、募集资金投资风险

##### (1) 募投项目效益不达预期的风险

目前,公司已根据当前的行业政策、宏观经济环境和市场竞争情况对募集资金投资项目进行了充分的可行性论证,并做好人才储备及市场调研等前期准备工作。但项目实施过程中,行业政策、市场竞争情况及项目研发进展存在不确定性,如果上述因素发生重大不利变化,则存在募投项目效益不达预期的风险。

## (2) 摊薄即期回报风险

本次公开发行完成后,公司资金实力随净资产和股本规模的扩大而增强。由于本次公开发行募集资金所投资项目需要建设周期,同时,募投项目中的综合运营服务中心项目不直接产生经济效益,短期内公司经营业绩仍主要依赖于现有业务。因此,在公司净资产和股本规模均大幅增长的情况下,每股收益和加权平均净资产收益率等收益指标均存在短期被摊薄的风险。

## 6、法律风险

发行人所处行业属于知识密集型和技术密集型行业,公司拥有一系列核心技术和专利。鉴于行业内竞争日趋激烈,如果公司未能有效保护自有知识产权免受他人侵犯,或因疏漏在产品开发过程中侵犯了他人的知识产权,将可能面临知识产权诉讼或纠纷的风险。若采取诉讼等法律措施后仍无法对公司的知识产权进行有效保护,可能会对公司的品牌形象、竞争地位和生产经营造成不利影响。

## 7、发行失败风险

按照《证券发行与承销管理办法》《上海证券交易所科创板股票发行与承销实施办法》等相关法律法规的规定,如果发行人出现有效报价投资者或网下申购的投资者数量不足,或者发行时总市值不满足其选择的市值与财务指标上市标准等情形,应当中止发行,若发行人中止发行上市审核程序超过交易所规定的时限或者中止发行注册程序超过3个月仍未恢复,或者存在其他影响发行的不利情形,或将会出现发行失败的风险。

## 二、本次发行情况

股票种类	人民币普通股(A股)		
每股面值	1.00元		
发行股数	不超过1,846.4320万股	占发行后总股本比例	不低于25%
其中:发行新股数量	不超过1,846.4320万股	占发行后总股本比例	不低于25%

股东公开发售股份数量	-	占发行后总股本比例	-
发行后总股本	不超过 7,385.7280 万股（行使超额配售选择权之前）		
每股发行价格	【】元/股		
发行市盈率	【】倍		
发行前每股净资产	【】元/股	发行前每股收益	【】元/股
发行后每股净资产	【】元/股	发行后每股收益	【】元/股
发行市净率	【】倍		
发行方式	采用网下向询价对象询价配售与网上资金申购发行相结合的方式，或中国证监会认可的其他方式		
发行对象	符合国家法律法规和监管机构规定的询价对象和在上海证券交易所开设人民币普通股（A 股）股票账户的境内自然人、法人等投资者（国家法律、法规和规范性文件禁止的认购者除外）		
承销方式	余额包销		
拟公开发售股份股东名称	本次发行不涉及公开发售股份的股东		
发行费用的分摊原则	本次发行费用全部由发行人承担		
募集资金总额	【】万元		
募集资金净额	【】万元		
募集资金投资项目	商用密码系列产品升级项目		
	新兴技术研究及新产品研发项目		
	综合运营服务中心建设项目		
	补充流动资金项目		
发行费用概算	保荐及承销费用：【】万元 审计费用：【】万元 律师费用：【】万元 与本次发行相关的信息披露费用：【】万元 发行手续费及其他：【】万元 合计：【】万元		

### 三、保荐代表人、项目协办人及项目其他组成员情况

本保荐机构指定高峰、苏华峰作为本次发行的保荐代表人，指定高原为发行人本次发行的项目协办人。保荐代表人、项目协办人和项目组人员相关情况如下：

高峰：保荐代表人，注册会计师，经济学硕士，拥有多年会计师事务所及投资银行相关业务经验，从业项目主要包括南新制药（688189.SH）科创板 IPO、信安世纪（688201.SH）科创板 IPO。证券执业证书编号 S0800720120015。

苏华峰：保荐代表人，注册会计师，具有多年的投资银行从业经验，近年主办已上市或已过会的企业包括新疆火炬（630080.SH）IPO 及重大资产重组；2021

年九典制药（300705.SZ）可转债发行；信安世纪（688201.SH）科创板 IPO；美能能源 IPO（001299.SZ）。证券执业编号 S0800718010001。

高原：项目协办人，西北大学国民经济管理硕士、投资学学士，拥有十多年投行工作经验，负责及参与立昂股份（300603.SZ）、博通股份（600455.SH）、圣莱达等上市公司重大资产重组；负责武钢股份（600005.SH）、湖北联投、宝钛集团（600456.SH）、中小企业集合债等十多家公司债券融资项目；负责佛山青松（834813.OC）、麦克传感（835304.OC）、嘉禾生物（833799.OC）等企业改制重组及新三板挂牌；负责宝钛股份（600456.SH）非公开再融资项目等，具有丰富的投资银行业务经验，执业记录良好。

项目组其他成员：史哲元、颜丹、江爱杨、冯晓娟、李晨、矫福昌、魏权。

#### **四、保荐人与发行人的关联关系、保荐人及其保荐代表人是否存在可能影响公正履行保荐责任情形的说明**

（一）除西部证券全资子公司西部证券投资（西安）有限公司参与本次发行战略配售之外，不存在保荐机构或其控股股东、实际控制人、重要关联方持有或者通过参与本次发行战略配售持有发行人或其控股股东、实际控制人、重要关联方股份的情况；

（二）截至本上市保荐书出具日，不存在发行人或其控股股东、实际控制人、重要关联方持有保荐人或其控股股东、实际控制人、重要关联方股份的情况；

（三）截至本上市保荐书出具日，不存在保荐人的保荐代表人及其配偶，董事、监事、高级管理人员，持有发行人或其控股股东、实际控制人及重要关联方股份，以及在发行人或其控股股东、实际控制人及重要关联方任职的情况；

（四）截至本上市保荐书出具日，不存在保荐人的控股股东、实际控制人、重要关联方与发行人控股股东、实际控制人、重要关联方相互提供担保或者融资等情况；

（五）截至本上市保荐书出具日，保荐人与发行人之间不存在其他关联关系。

## 五、保荐人对发行人是否就本次证券发行上市履行相关决策程序的说明

### （一）董事会

2022年4月22日，公司召开第五届董事会第十四次会议，审议通过了《关于公司申请首次公开发行人民币普通股股票（A股）并在科创板上市的议案》等与本次发行相关的议案，并提请股东大会审议。

### （二）股东大会

2022年5月9日，公司召开2022年第三次临时股东大会，审议通过了《关于公司申请首次公开发行人民币普通股股票（A股）并在科创板上市的议案》等与本次发行相关的议案。

保荐机构及保荐代表人核查了本次股东大会的决议及有关会议文件，认为发行人本次公开发行股票并在科创板上市已履行了必要的决策程序，获得了必要的批准和授权，符合《公司法》《证券法》及中国证监会、上海证券交易所规定的决策程序。

## 六、保荐人对发行人是否符合科创板定位的专业判断

### （一）公司符合科创板行业领域要求

公司主营业务为商用密码产品的研发、生产、销售及服务。根据国家统计局《国民经济行业分类》（GB/T4754-2017），公司所处行业属于“C39 计算机、通信和其他电子设备制造业”中的“C3915 信息安全设备制造”。根据国家统计局《战略性新兴产业分类（2018）》，公司所属行业为“新一代信息技术产业”中的“1.1.3 信息安全设备制造”。

保荐机构认为，公司所属行业符合《上海证券交易所科创板企业发行上市申报及推荐暂行规定》第三条（一）中规定的“新一代信息技术领域”行业领域。

## (二) 公司符合科创属性指标

### 1、公司符合科创属性评价标准一相关指标情况

科创属性评价标准一	是否符合	公司指标情况
最近三年累计研发投入占最近三年累计营业收入比例 $\geq 5\%$ ，或最近三年累计研发投入金额 $\geq 6000$ 万元。其中，软件企业最近三年累计研发投入占最近三年累计营业收入比例应在10%以上	是	公司最近三年累计研发投入为2,763.22万元，最近三年公司累计营业收入为19,407.84万元，研发累计投入占最近三年累计营业收入的比例为14.24%
研发人员占当年员工总数的比例 $\geq 10\%$	是	报告期内各期末，公司研发人数分别为33人、48人、50人和52人，占当年员工总数的比例分别为37.08%、38.40%、30.86%和28.11%
形成主营业务收入的发明专利(含国防专利) $\geq 5$ 项	是	截至目前，公司拥有的形成主营业务收入的发明专利为20项
最近三年营业收入复合增长率 $\geq 20\%$ ，或最近一年营业收入金额 $\geq 3$ 亿	是	公司最近三年营业收入分别为2,976.32万元、5,731.83万元、10,699.69万元，复合增长率为89.60%

### 2、公司符合科创属性评价标准二相关指标情况

科创属性评价标准二	是否符合	主要依据
拥有的核心技术经国家主管部门认定具有国际领先、引领作用或者对于国家战略具有重大意义	否	-
作为主要参与单位或者核心技术人员作为主要参与人员，获得国家自然科学奖、国家科技进步奖、国家技术发明奖，并将相关技术运用于公司主营业务。	否	-
独立或者牵头承担与主营业务和核心技术相关的“国家重大科技专项”项目	是	(1) 公司于2006年独立承担了科技部科技型中小企业技术创新基金“基于PCI-E总线的嵌入式通信安全系统”项目 (2) 公司于2007年独立承担了国家发改委信息安全专项产品产业化项目“基于PCI-E总线的高速加解密系统产业化项目”项目 (3) 公司于2008年独立承担了科技部科技型中小企业技术创新基金“基于下一代互联网安全协议的高速VPN系统”项目 (4) 公司于2008年独立承担了国家发改委信息安全专项项目“基于下一代互联网安全协议的高速VPN系统产业化项目”项目

科创属性评价标准二	是否符合	主要依据
		(5) 公司于 2009 年独立承担了国家发改委信息安全专项项目“基于国产 PKI 设备的网上统计系统示范工程项目”项目 (6) 公司于 2010 年独立承担了国家发改委信息安全专项项目“基于国产密码技术的内网安全综合管理平台产品产业化项目”项目 (7) 公司于 2012 年独立承担了科技部科技型中小企业技术创新基金“基于国产密码技术的物联网安全平台”项目 (8) 公司于 2012 年独立承担了国家发改委金融领域安全 IC 卡和密码应用专项产业化和检测服务类项目“基于国产密码技术的高性能签名验签服务器产业化”项目 (9) 公司于 2012 年独立承担了国家发改委信息安全专项项目“基于国产密码技术的高性能云计算密码服务平台产业化”项目 (10) 公司于 2014 年独立承担了科技部科技型中小企业技术创新基金“渔翁信息安全综合服务中心”项目 (11) 公司于 2015 年独立承担了国家火炬计划产业化示范项目基于密码技术的互联网信任体系云管理平台项目 (12) 公司于 2021 年牵头承担了工信部车联网身份认证和安全信任试点项目“车联网安全防护及国产密码综合应用项目”项目
依靠核心技术形成的主要产品（服务），属于国家鼓励、支持和推动的关键设备、关键产品、关键零部件、关键材料等，并实现了进口替代	是	信创服务器密码机、高速密码卡、综合安全网关等产品被纳入国家信创产业密码产品目录，在网络安全领域“补短板”，实现密码产品国产化替代，可替代美国 Cisco、IBM，瑞士 Crypto 公司产品
形成核心技术和主营业务收入相关的发明专利（含国防专利）合计 50 项以上	否	-

综上，发行人符合《科创属性评价指引（试行）》和《上海证券交易所科创板股票发行上市审核规则》的相关规定，符合科创属性评价标准、符合科创板定位。

## 七、保荐人对公司是否符合上市条件的说明

渔翁信息股票上市符合《公司法》《证券法》和《上海证券交易所科创板股票上市规则》规定的上市条件：

(一) 发行前公司股本总额为人民币 5,539.2960 万元, 公司新股发行总数合计不超过 1,846.4320 万股。本次发行后公司总股本不超过 7,385.7280 万股;

(二) 本次公开发行股份总数为不超过 1,846.4320 万股, 占发行后总股本的 25.00%, 公司公开发行的股份不低于本次发行后股份总数的 25.00%;

(三) 市值及财务指标

#### 1、市值结论

综合渔翁信息报告期内外部股权融资估值、可比上市公司比较法得到的评估结果, 渔翁信息预计市值不低于 10 亿元。

#### 2、财务指标

根据天职国际会计师事务所(特殊普通合伙)出具的《审计报告》(天职业字[2022]23128号), 公司 2021 年营业收入为 10,699.69 万元。2020 年度和 2021 年度经审计的扣除非经常性损益前后归属于母公司净利润孰低的金额分别为 1,773.40 万元和 3,778.05 万元。

#### 3、标准适用判定

依据《上海证券交易所科创板股票上市规则》等相关法律法规, 发行人选择具体上市标准如下: (一) 预计市值不低于人民币 10 亿元, 最近两年净利润均为正且累计净利润不低于人民币 5,000 万元, 或者预计市值不低于人民币 10 亿元, 最近一年净利润为正且营业收入不低于人民币 1 亿元。

综上所述, 发行人满足所选择的上市标准。

本次股票发行申请尚需上海证券交易所审核并由中国证监会作出同意注册决定。

## 八、保荐人按照有关规定应当承诺的事项

(一) 保荐人已按照法律法规和中国证监会及上海证券交易所的规定, 对发行人及其控股股东、实际控制人进行了尽职调查、审慎核查, 充分了解了发行人经营状况及其面临的风险和问题, 履行了相应的内部审核程序, 已具备相应的保荐工作底稿支持, 同意推荐发行人证券发行并上市, 并据此出具本上市保荐书。

(二) 保荐人有充分理由确信发行人符合法律法规及中国证监会有关证券发行上市的相关规定。

(三) 保荐人有充分理由确信发行人申请文件和信息披露资料不存在虚假记载、误导性陈述或者重大遗漏。

(四) 保荐人有充分理由确信发行人及其董事在申请文件和信息披露资料中表达意见的依据充分合理。

(五) 保荐人有充分理由确信申请文件和信息披露资料与证券服务机构发表的意见不存在实质性差异。

(六) 保荐人保证所指定的保荐代表人及本保荐机构的相关人员已勤勉尽责，对发行人申请文件和信息披露资料进行了尽职调查、审慎核查。

(七) 保荐人保证保荐书与履行保荐职责有关的其他文件不存在虚假记载、误导性陈述或者重大遗漏。

(八) 保荐人保证对发行人提供的专业服务和出具的专业意见符合法律、行政法规、中国证监会的规定和行业规范。

(九) 保荐人自愿接受中国证监会依照《证券发行上市保荐业务管理办法》采取的监管措施。

## 九、对公司持续督导期间的工作安排

事项	安排
(一) 持续督导事项	在本次发行股票上市当年的剩余时间及以后 3 个完整会计年度内对发行人进行持续督导
1、督导发行人有效执行并完善防止大股东、其他关联方违规占用发行人资源的制度	1、强化发行人严格执行中国证监会和上海证券交易所有关规定的意识，督导发行人有效执行并进一步完善已有的防止大股东、其他关联方违规占用发行人资源的制度； 2、与发行人建立经常性沟通机制，持续关注发行人上述制度的执行情况及履行信息披露义务的情况
2、督导发行人有效执行并完善防止高级管理人员利用职务之便损害发行人利益的内控制度	1、督导发行人有效执行并进一步完善已有的防止高级管理人员利用职务之便损害发行人利益的内控制度； 2、与发行人建立经常性沟通机制，持续关注发行人上述制度的执行情况及履行信息披露义务的情况
3、督导发行人有效执行并完善保障关联交易公允性和合规性的制度，并对关联交易发表意见	1、督导发行人有效执行并进一步完善关联交易决策权限、表决程序、回避情形等工作规则； 2、督导发行人及时向保荐机构通报将进行的重大关联交易情况，保荐机构将对关联交易的公允性、合规

事项	安排
	性发表意见； 3、督导发行人严格执行有关关联交易的信息披露制度
4、督导发行人履行信息披露的义务，审阅信息披露文件及向中国证监会、上海证券交易所提交的其他文件	1、督导发行人严格按照《公司法》《证券法》及《上海证券交易所科创板股票上市规则》等有关法律、法规及规范性文件的要求，履行信息披露义务； 2、在发行人发生须进行信息披露的事件后，审阅信息披露文件及向中国证监会、上海证券交易所提交的其他文件
5、持续关注发行人募集资金的使用、投资项目的实施等承诺事项	1、督导发行人执行已制定的《募集资金管理制度》等规定，保证募集资金的安全性和专用性； 2、持续关注发行人募集资金的专户储存、投资项目的实施等承诺事项
6、持续关注发行人为他人提供担保等事项，并发表意见	1、督导发行人严格按照中国证监会和上海证券交易所所有文件的要求规范发行人担保行为的决策程序； 2、要求发行人对所有担保行为与保荐人进行事前沟通
（二）保荐协议对保荐人的权利、履行持续督导职责的其他主要约定	按照保荐制度有关规定积极行使保荐职责；严格履行保荐协议、建立通畅的沟通联系渠道
（三）发行人和其他中介机构配合保荐人履行保荐职责的相关约定	会计师事务所、律师事务所持续对发行人进行关注，并进行相关业务的持续培训
（四）其他安排	无

## 十、保荐人认为应当说明的其他事项

无其他需要说明的事项。

## 十一、保荐人对本次股票上市的推荐结论

西部证券作为渔翁信息本次证券发行上市的保荐机构，遵循诚实守信、勤勉尽责的原则，根据法律、法规和中国证监会及上海证券交易所的有关规定，对发行人进行了充分的尽职调查。经过审慎核查，保荐机构认为，渔翁信息申请其股票上市符合《公司法》《证券法》及《上海证券交易所科创板股票上市规则》等法律、法规及规范性文件的有关规定，其股票具备在上海证券交易所科创板上市的条件，同意推荐渔翁信息的股票在上海证券交易所科创板上市交易，并承担相关保荐责任。

请予批准！


（以下无正文）

(此页无正文,为《西部证券股份有限公司关于渔翁信息技术股份有限公司首次公开发行股票并在科创板上市之上市保荐书》之签字盖章页)

项目协办人:

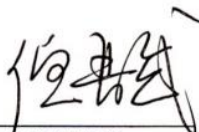
  
高原 2022年12月20日

保荐代表人:

  
高峰 2022年12月20日

  
苏华峰 2022年12月20日

内核负责人:

  
倪晋武 2022年12月20日

保荐业务负责人:

  
范江峰 2022年12月20日

保荐机构总经理:

  
齐冰 2022年12月20日

保荐机构董事长、法定代表人:

  
徐朝晖 2022年12月20日

