# 渔翁数据库安全加密网关
# 技术白皮书

版本：V3.1

网　站：www.fisec.cn

电　话：400-6686-188

邮　箱：support@fisherman-it.com

地　址：山东省威海市火炬高技术产业开发区初河北路12-1号

| 版本更新记录表 | | | |
|---|---|---|---|
| 序号 | 版本号 | 版本更改说明 | 更改日期 |
| 1 | V1.0 | 首次发布 | 2022.05.26 |
| 2 | V1.1 | 产品名称更改 | 2022.06.20 |
| 3 | V2.0 | 产品定位调整 | 2022.09.07 |
| 4 | V3.0 | 更新技术路线 | 2024.03.15 |
| 5 | V3.1 | 更新相关内容描述 | 2024.07.26 |
| 6 | | | |
| 7 | | | |
| 8 | | | |
| 9 | | | |
| 10 | | | |

# 声 明

**版权声明：**

本文档的版权属渔翁信息技术股份有限公司所有。

本文档的版权受到中华人民共和国国家法律和国际公约的保护。未经书面许可，任何单位和个人不得以任何形式或通过任何途径非法使用、拷贝、修改、扩散本文档的全部或部分内容。

**警告和承诺：**

我们做了大量的努力使本文档尽可能的完备和准确，但疏漏和缺陷之处在所难免。任何人或实体由于本文档提供的信息造成的任何损失或损害，渔翁信息技术股份有限公司不承担任何义务或责任。

渔翁信息技术股份有限公司保留未经通知用户对本文档内容进行修改的权利。

**反馈信息：**

如果您对本文档有任何疑问、意见或建议，请与我们联系。对您的帮助，我们十分感激。

# 目 录

# 1 背景概述

随着信息技术产业革命浪潮，数据逐渐成为物质、能源后第三大国家基础战略资源和创新生产要素。在大数据行业快速发展的背景下，数据安全面临以下三种趋势：

- 高价值的数据向数据节点汇聚，出现海量敏感数据泄露的问题；
- 数据泄露后的危害越来越大，影响范围越来越广；
- 数据泄露的方式和途径也愈发多样和不可预测。

数据库系统作为信息的聚集体，是计算机信息系统的核心部件，其安全性至关重要，而之前市场上缺乏有效的应用系统和数据库安全统一解决方案，导致数据库中的数据明文存储、被动防御的网络安全产品只能检测已知攻击、审计产品更是只能时候追责，无法真正保护数据安全。

政策方面等级保护 2.0 标准规定：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。国家密码管理局于 2018 年 2 月 8 日发布《信息系统密码应用基本要求》明确提出：等保二级及以上信息系统要求应采用符合《GM/T0028-2014 密码模块安全要求》中响应等级密码模块或通过国家密码管理部门核准的硬件密码产品实现密码运算和密码管理等。而在 2021 年 9 月 1 日，国家正式颁布《中华人民共和国数据安全法》，从国家层面强调数据安全的重要性，规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益。

# 2 产品定义

## 2.1 产品介绍

渔翁数据库安全加密网关基于自主创新的同态算法 FPHE、敏感数据自适应 AI 脱敏技术、数据缓存及并包处理技术 FNIO 技术，实现百万级并发情况下数据库高速加解密、密态模糊查询以及数据安全脱敏功能，为数据识别、数据存储、数据使用提供安全合规的解决方案，可广泛应用于金融、教育、能源、国企等领域分布式应用系统以及应用和大数据系统。

## 2.2 产品模式

应用程序将明文数据提交给数据库加密管理系统，数据库加密管理系统将对数据进行格式解析，完成格式解析后进行字段加密并落盘处理；读取时，数据库加密管理系统从数据库中读取密文数据，解密并脱敏后将明文数据返回给应用程序。

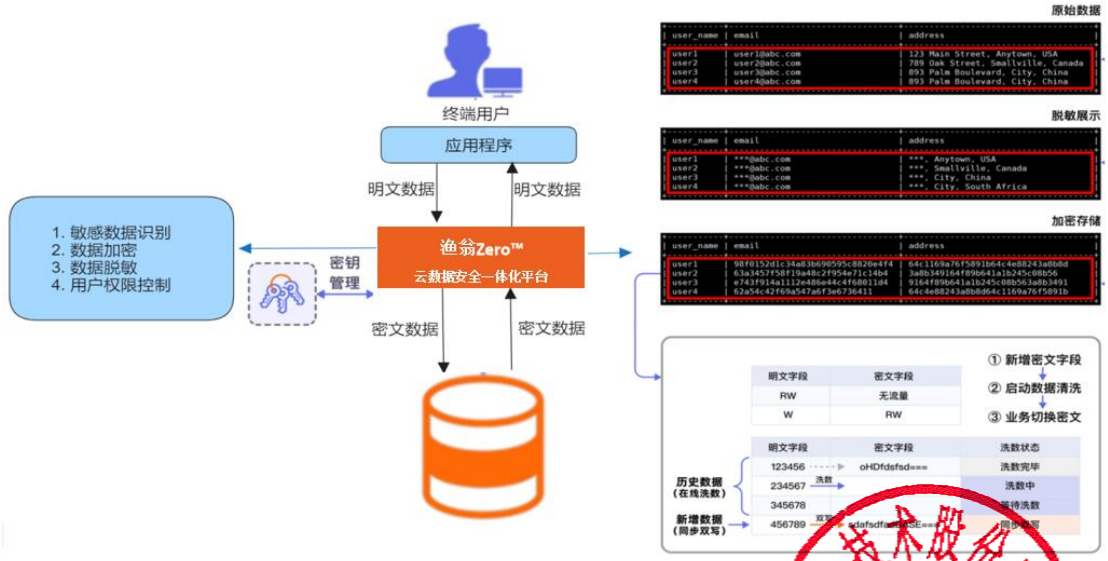



图2-1 加解密模式

## 2.3 产品建设标准

渔翁数据库安全加密网关基于自主创新的同态算法 FPHE、敏感数据自适应 AI 脱敏技术、数据缓存及并包处理技术 FNIO 技术，循遵 GM/T 0028-2014《密码模块安全技术要求》等密码行业标准。

# 3 产品架构

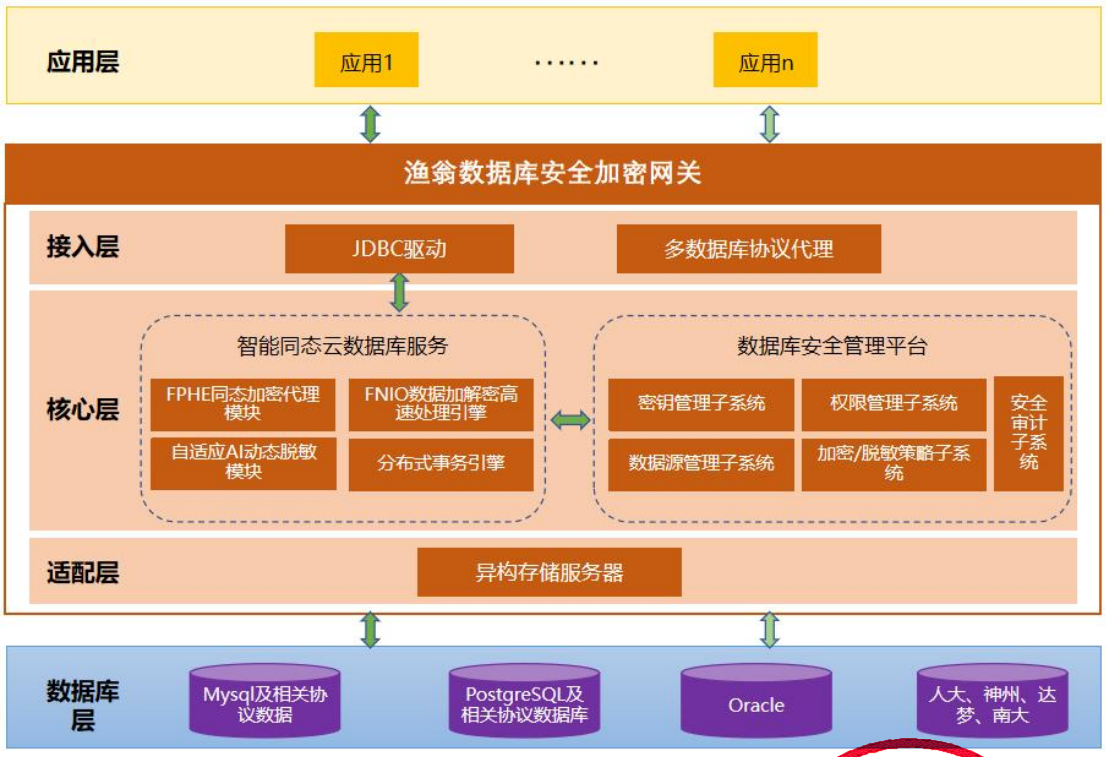



图3-1 产品架构

渔翁数据库安全加密网关包括适配层、核心层、接入层。

适配层作为适配器，可以兼容各种异构存储服务器。

核心层提供智能同态云数据库服务和数据库安全管理平台。其中智能同态云数据库服务包含了同态算法 FPHE 模块、敏感数据自适应 AI 脱敏模块、数据缓存及并包处理 FNIO 模块及分布式事务引擎模块。数据库安全管理平台包含：密钥管理子系统、权限管理子系统、数据源管理子系统、加密脱敏策略子系统、安全审计子系统等。

接入层提供了 JDBC 驱动接入模式和多数据库协议代理接入模式，用于接入应用层的各种应用。

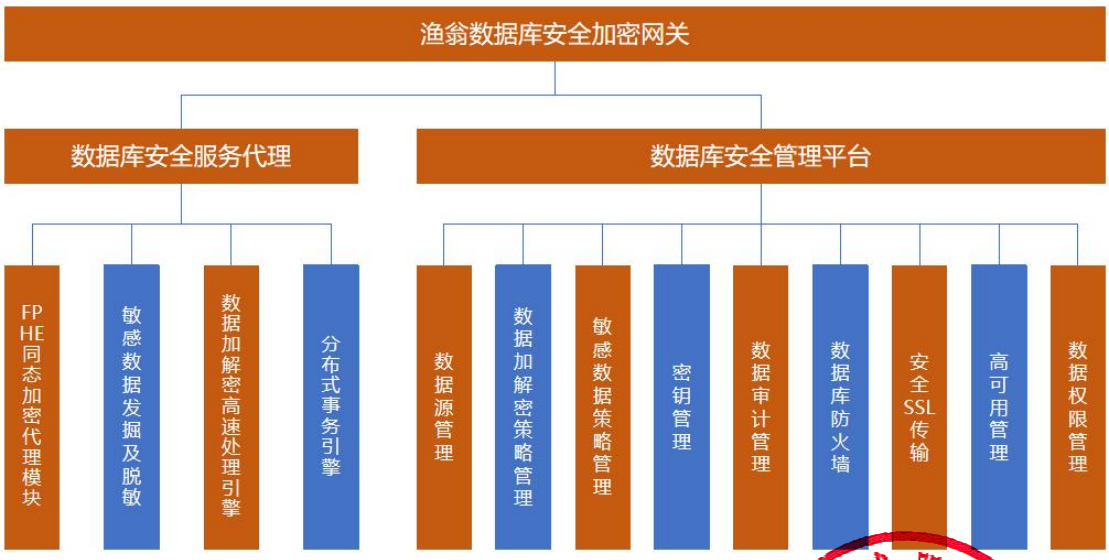
# 4 标准依据

GM/T 0028-2014《密码模块安全技术要求》

GM/T 0039-2015《密码模块安全检测要求》

GM/T 0062-2018《密码产品随机数检测要求》

# 5 产品功能架构




# 6 产品优势

➢ **Zero™应用免改造**：应用免改造实现“一字段一密”、“一文一密”，满足 GB/T 39786 应用层数据防护要求，**高分过密评**，平均实施周期较应用开发商改造缩短 **60%~80%**。

➢ **安全可逃生**：数据脱敏、在线洗数技术，**省事**；提供逃生通道，安全可回退，**省心**。

➢ **极致高性能**：使用数据缓存及并包处理技术 FNIO，轻松支撑百万级并发，可靠性达 **100%**，极限性能损耗控制在 **2.9%以内**。

➢ **平滑零停机**：在线完成洗数，一站式加密处理，一键完成迁移。

➢ **密态可查询**：通过全栈自研的同态 FPHE 算法，实现密态计算及密态模糊查询。

- **云及分布式数据库加密：**支持分布式应用加密、适配云上环境。

# 7 功能参数

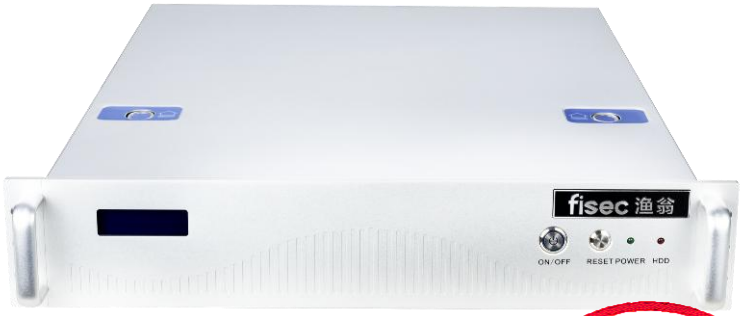
- 支持多种类型的数据库品牌和版本，包括国际主流数据库和国产化数据库类型，包括但不限于：Oracle 系列、SQL Server 系列、My SQL 系列、Gbase 8a 及以上版本、华为 GaussDB 系列、达梦系列、人大金仓系列、TDSQL 系列数据库所有版本。支持主流开发语言，包括：Java、C、Python 等。支持 Linux 系列操作系统。
- 支持统一的加密策略和密钥管理功能，策略以图形化方式展示操作。数据加解密在应用内完成，明文数据不会传出应用系统或者数据库之外。
- 支持多种类型的数据加密，包括但不限于 CHAR、VARCHAR2、VARCHAR、LOB、NUMBER 等数据类型。
- 支持密文数据模糊查询功能，通过全栈自研的动态 FPHE 算法，实现密态计算及密态模糊查询。
- 支持各种类型的格式保留加密，基于 SM4 算法的格式保留加密算法，包括但不限于身份证格式保留加密、护照号格式保留加密、电子邮箱格式保留加密、数字格式保留加密。
- 支持应用免改造，运维者和应用系统通过安装插件等实现应用免改造方式，明文访问数据库；相同业务压力时加密后应用系统、数据库服务整体性能损失相比加密前不超过 10%，实现高效的数据访问。
- 支持字段级加密和保留格式加密；支持应用免改造字段级加密，支持保留格式加密，加密后的数据以密文形态存储。应用免改造实现“一字段一密”、“一文一密”，满足 GB/T 39786 应用层数据防护功能，符合密评要求。
- 数据加密算法全面兼容多种国密、国际标准算法，支持 SM 国密系列算法，国密 SM4 加解密性能不低于 41Gbps。
- 支持 IPv6 协议，兼容 IPv6 环境下加密机主服务器之间、加密机与数据库服务器之间以 IPv6 协议通信；
- 支持系统冗余热备配置，支持 HA 高可用方式部署，支持主、从互备。

管理平台支持旁路部署，路由可达，无需改造系统网络结构，不会影响业务系统对数据库系统的访问。

- 支持 DBA 明文数据管理方式管理密文数据，不改变原有数据管理习惯。包括：1）支持密文数据不解密可视化运维，具有权限的数据库管理员可通过管理工具以查阅明文的方式查看密文，但密文本身并没有解密为明文。数据导出和爬取内存得到的也不是明文，将数据管理权与所有权彻底分离；2)支持密文查询功能，不仅支持密文精准查询，还支持模糊查询、关联查询；3)支持密态计算，支持密文计算功能，可对密文数据直接进行函数运算，运算结果与明文保持一致。
- 支持用户绑定应用系统，同一用户只能通过指定的应用系统访问密文数据，使用命令行、管理工具等其他任何方式均无法访问密文数据；
- 支持数据库列名加密，对数据库列名数据进行加密以隐藏真实数据库元数据信息；
- 支持密钥的安全管理功能，支持三层密钥体系，包括根密钥、模块主密钥和工作密钥；支持安全服务组件实现对密钥的管理，包含加密密钥生成、分配、备份和恢复，密钥不出设备（卡）；支持由密码卡根据周围环境（噪音、温度）生成随机数，保护根密钥；支持与客户现有密钥管理系统对接。
- 支持数据的安全备份和恢复功能；支持加密不影响数据库自身的数据库恢复、备份、同步等操作；支持额外的离线数据恢复工具，保证极端情况下数据也能恢复到原始状态，保证数据的高可用性；
- 支持可视化的系统管理功能，具有 Web 图形化管理界面，易于安装及加密策略部署，具备快速、准确的整体拆除能力；支持数据库中原有的存储过程、函数、视图等在加密后数据库上正常运行，运行结果与明文保持一致；支持对数据库列名等元数据进行混淆以隐藏真实数据库元数据信息；
- 支持数据密态运维，支持密文数据不解密可视化运维。具有权限的运维者可通过管理工具以查阅明文的方式查看密文，但密文本身并没有解密为明文。

# 8 技术参数

## 8.1 物理规格




| 指标 | | 数据 |
|---|---|---|
| 物理规格 | 规格 | 2U 机架式 |
| | 外形尺寸（宽×深×高 cm） | 43×53×8.9 |
| | 工作电源 | 冗余电源，支持断电保护备份等安全机制 |
| | 网络接口 | RJ-45 10/100/1000Mb *4 |
| | 工作协议 | TCP/IP |
| | 平均无故障时间 | 50000 小时 |
| | 工作温度 | 10℃-50℃ |
| | 工作湿度（非凝结） | 5%-85% |
| | 存储温度 | 0℃-60℃ |
| | 存储湿度（非） | 5%-95% |

| 序号 | 规格参数 | 备注 |
|---|---|---|
| 1 | 2U 机架式机箱，冗余电源；国产海光 16 核 CPU，128G 内存，1 块 1TB SAS 硬盘，支持存储空间扩展；4 个千兆电口，支持万兆网络环境监听。 | / |

## 8.2 性能指标

| 项目 | 数据 |
| --- | --- |
| 支持数据库 | MySQL、Oracle、PostgreSQL、DM（达梦）、Kingbase（人大金仓）等 |
| 支持加密数据记录 | >3500000000 |
| 百万级加密性能 | <5min |
| 百万级加密数据还原性能 | <5min |
| 加密状态下插入百万级数据 | <2min |
| 插入性能达未加密前 | >95% |
| 查询性能达未加密前 | >95% |
| 支持加密算法 | AES、DES、3DES、SM4、SM2、RSA2048 |
| 支持加密模式 | ECB、CBC、OFB、CFB、GCM、CCM |
| 脱敏标准 | GDPR、GB/T 35273 |
| 脱敏策略算法 | MD5、KEEP_FIRST_N_LAST_M、KEEP_FROM_X_TO_Y、MASK_FIRST_N_LAST_M、MASK_FROM_X_TO_Y、MASK_BEFORE_SEECIAL_CHARS、MASK_AFTER_SPECIAL_CHARS |

# 9 产品应用

渔翁数据库安全加密网关可满足不同客户对于性能、数据库特性、数据库类型等要求，广泛应用于电子政务、金融业务、医疗健康、能源电力、智慧城市等行业领域。

- **政府：**Xx 省大数据系统，私有云，数据库：Oracle、HBase、Hive，数据规模：300 万。
- **金融：**商业银行分布式核心系统，私有云，数据库：人大金仓，采用功能：数据加密、数据脱敏、在线洗数。

➢ **教育：**某市教育局综合信息管理系统，自建机房，数据库：Oracle，加密字段 200+。

➢ **国企：**某国有企业网上业务大厅系统，自建机房，数据库：MySQL、SQL Server，数据规模：最大表 4.5 亿记录。

➢ **能源：**某大型能源央企能源管理系统，私有云，数据库：达梦，采用功能：数据加密。

**典型案例**

- **某医院网上预约挂号系统的数据库加密免改造项目**

➢ **背景介绍：**某市三甲医院的网上预约挂号系统，承接了本院 60%以上的挂号业务，作为该医院挂号业务的主要入口，一旦出现长时间停机或报错等异常情况，对院内的业务运转影响极大，且会产生不良的社会负面舆情。由于系统已上线验收多年，开发商配合意愿低，业主要求对数据库进行免改造的实施方案，同时要对用户无感，不能造成挂号业务的异常。之前院内也测试过其他厂家的产品，但是都因为需要协调开发商进行二次开发而造成无法实施的困境。

➢ **解决思路：**根据该客户提出的系统免改造，稳定运行等需求，我们采用了平台的串联模式部署方案，通过平台的数据库代理引擎接管业务系统对原数据库的操作，并结合在线洗数等功能达到业务系统不停机平滑切换的要求。

➢ **实施效果：**本平台改造全程由我司工程师实施，未协调开发商，顺利进行了业务切换，没有产生任何异常情况。自实施起平台已稳定运行 2 年多，我司专业的服务团队和技术能力得到了业主方的一致认可。

# 10 常见问题解答（FAQ）

➢ **面对上线数年的应用系统，开发商配合度低，如何实现合规性改造？**

本平台不挑应用，适配的数据库多，可真正可以做到应用系统、数据库免改造的数据加密防护，改造后的结果完全符合 GB/T 39786 应用层数据防护功能要求，助您高分过密评。

➢ **改造后模糊查询会失效吗，影响业务查询怎么办？**

通过全栈自研的同态 FPHE 算法，数据加密后的所有模糊查询、精准查询均不会失效，所有针对数据库的增删改查 sql 都不受影响，真正实现“一字段一密”、

“一文一密”，业务均可正常运行，同态密态可查询。

- **数据库中的敏感数据比较多，存储在各种表中，没有开发商的支持，如何进行识别？**

本平台使用自适应 AI 动态脱敏技术实现 GDPR、GB/T 35273 脱敏规则，对敏感数据自动发掘并进行动态脱敏，没有开发商的支持，让我们的平台来支持您。

- **平台的加解密性能如何，改造后是否会使业务响应变慢？**

平台在进行加解密运算过程中确实会产生一定的性能损耗，但是通过自研的数据缓存及并包处理技术 FNIO，在各种大数据量、高并发场景下性能损耗可控，通过大量的客户处实践验证，对业务应用产生的影响很小，极限性能损耗可控制在 2.9%以内。

- **堡垒往往是从内部被攻破的，系统能做到防住我们的自己人吗？**

平台独立权控体系，防止数据被违规修改、窃取，保护高价值数据安全。不仅能防止您的内部人员的非授权访问而导致数据泄露，作为系统的开发商，我们的“攻城狮”们也没法破解加密数据。

- **我们的业务系统要求 24 小时不间断运行，你们能做到不停机部署吗？**

平台在部署期间确实会中断业务系统，但是我们已经在做到尽量避免长时间停机的同时，提供在线完成密文转换机密钥轮转的机制，使得业务停机时间做到最小。我们的口号是：在线完成洗数，一站式加密处理，一键完成迁移。

- **我这边的环境是云及分布式数据库，系统能否支持？**

平台支持分布式应用加密、适配云上环境。

- **我还是不放心，万一平台部署失败或者运行一段时间发现有问题怎么办?**

我们的“攻城狮”们研发了后悔药，提供逃生通道，保障数据安全可回退。

- **平台超过维保期，或者在你们部署实施完后，我的业务人员想操作怎么办？**

平台提供一键自动执行加密到明文数据的双向转换，即使是小白也能一键“攻城狮”附体；

- **我这边的应用有多个，开发商技术路线各不相同，数据库有多种怎么办？**

平台支持的数据库有：MySQL、PostgreSQL、Oracle、SQL Server、Hive、Presto 等国际数据库以及达梦、人大金仓、神州通用等国产数据库。

# 11 公司简介

渔翁信息技术股份有限公司（简称：渔翁信息）成立于 1998 年，是拥有自主知识产权的密码产品及方案提供商。公司为国家信创工委会密码应用工作组组长单位，国家密码行业标准化技术委员会成员单位，国家级专精特新“小巨人”企业。

以总体国家安全观为指引，渔翁信息率先布局信创密码产业，发起成立国家信创密码应用工作组，推进密码产品与国产化环境的兼容适配；同时公司为首批入围信创目录的企业，并多次承接国家信创示范工程项目。

渔翁信息作为较早从事国产密码技术创新与应用的高新技术企业，建有博士后科研工作站及密码应用技术工程实验室等五大国家级创新平台。公司 10 余次承担十三五规划、核高基等国家及省级重大课题研究，8 次参与国家及行业密码标准制定，14 次荣获国家级及省级科学技术进步奖，拥有发明专利等知识产权 117 项。

经过 20 余年发展，渔翁信息搭建了从软件到硬件，从底层应用到上层运管平台完整的密码产品体系，涵盖基础密码产品、PKI 密码支撑系统、通用安全产品、工控安全产品、密码应用方案等。广泛服务于党政、金融、税务、交通、能源、通信等重点行业和关键领域，可解决多场景下的认证安全、传输安全、存储安全等问题。

渔翁信息建立以北京、上海、深圳为中心，覆盖全国 30 个省市自治区的分支机构和办事处，可为客户提供 7×24 小时优质的本地化服务。公司拥有知识产权贯标体系及 ISO9001、ISO27001、ISO20000 管理体系认证，建立了一整套规范的服务体系，能够向客户提供全方位密码应用服务和网络安全保障。

没有网络安全，就没有国家安全。渔翁信息以“立潮头，安天下”为使命，立足技术创新与发展，致力于为客户提供高安全、高稳定、高性能的密码产品及服务，以不变的初心和奋斗，为网络强国建设保驾护航！