# 一种基于量子加密与 AI 驱动的智能安全法务系统及方法

## 专利申请文件（示例框架）

### **说明书**

#### **技术领域**

本发明涉及智能安全法务技术领域，具体为一种融合量子加密、区块链存证、AI 风险分析的电子签约与安全管理系统及方法。

#### **背景技术**

传统电子签约系统存在以下不足：

1. 加密技术易受量子计算攻击，安全性不足；
2. 合同风险分析依赖人工，效率低且准确率有限；
3. 认证体系单一，无法应对复杂攻击场景；
4. 存证与合规流程缺乏自动化与多链兼容性。现有技术未实现量子安全、AI 智能与区块链的深度融合，亟需一种高安全性、智能化的法务管理系统。

#### **发明内容**

**发明目的**：提供一种基于量子加密与 AI 驱动的智能安全法务系统，实现高安全性电子签约、自动化法务流程及智能风险管控。

**技术方案**：一种智能安全法务系统，包括：

1. **量子安全认证模块**：
   * 利用量子随机数生成设备指纹（专利技术 GXAUTH-20240626-03），结合多因素认证（密码 / TOTP / 生物识别 / 地理位置），通过量子加密算法（Kyber1024/NTRU/SABER）传输认证数据；
   * 动态切换 3 种自适应加密算法，集成 Redis 集群存储设备指纹（TTL 30 天）。
2. **电子签约与存证模块**：
   * 支持本地合同模板创建、多方签署流程，采用 RSA/ECC/ 国密 SM2 等多算法签名，生成签名数据（如数字签名图片或生物特征数据）；
   * 合同内容加密存储，可选区块链多链存证（Fabric/Ethereum/Hyperledger），结合零知识证明确保不可抵赖性。
3. **AI 辅助风险分析模块**：
   * 集成 LSTM 神经网络分析用户行为数据，实时检测异常操作；
   * 利用 AI 模型对合同文本进行合规性检查，自动标注高风险条款，输出风险评分。
4. **动态防御与自动化模块**：
   * 虚拟认证陷阱系统（专利技术 GXSEC-20240626-02）实时提取攻击特征，同步更新 WAF 规则；
   * 合同归档、到期提醒、合规审计全流程自动化，支持本地知识库管理与智能问答。

**方法流程**：

1. **合同签署流程**：
   * 用户通过多因素认证登录系统，选择合同模板并生成实例；
   * 调用量子加密模块生成签名密钥，支持数字签名或生物识别签名；
   * 签署后数据本地存证，并可选上链存证，触发 AI 风险分析与法务归档。
2. **动态认证流程**：
   * 设备接入时生成量子设备指纹，结合行为生物认证引擎验证；
   * 基于实时威胁情报调整认证策略，如动态增加多因素认证步骤。

#### **附图说明**

1. **系统架构图**：展示量子加密、AI、区块链等模块的交互关系；
2. **电子签约流程图**：

|  |
| --- |
| graph LR  A[合同创建] --> B[量子认证]  B --> C[多算法签名]  C --> D[本地存证]  D --> E[区块链存证]  E --> F[AI风险分析]  F --> G[法务归档] |

1. **认证体系流程图**：展示五维认证（密码 / 设备指纹 / 地理位置 / 生物识别 / 行为分析）的动态组合机制。

#### **具体实施方式**

1. **量子加密实现**：
   * 使用 PQCrypto 扩展实现 Kyber1024 算法，生成量子安全密钥对；
   * 数据传输前先用 AES-256 加密，再用量子公钥加密 AES 密钥，组合生成密文。
2. **AI 模型应用**：
   * 训练 LSTM 模型识别用户登录行为特征，设置异常阈值触发二次认证；
   * 基于自然语言处理（NLP）解析合同文本，匹配合规规则库进行风险标注。
3. **区块链存证**：
   * 签署完成后，将合同哈希值、签名时间戳等上链，支持多链同步存证；
   * 提供链上查询接口，生成不可篡改的存证证明。

### **权利要求书**

1. 一种智能安全法务系统，其特征在于，包括：
   * 量子安全认证模块，用于生成量子设备指纹并实现多因素认证；
   * 电子签约模块，支持多算法签名、本地存证与区块链存证；
   * AI 风险分析模块，用于合同合规检查与行为异常检测；
   * 动态防御模块，包括虚拟认证陷阱系统与自动化 WAF 规则同步。
2. 根据权利要求 1 所述的系统，其特征在于，所述量子安全认证模块包括：
   * 基于量子随机数的设备指纹生成单元；
   * 支持 Kyber1024/NTRU/SABER 算法的量子加密传输单元。
3. 根据权利要求 1 所述的系统，其特征在于，所述电子签约模块实现流程包括：
   * 合同模板本地化管理与多方签署流程；
   * 签名数据（数字签名 / 生物特征）的加密存储与区块链存证。
4. 一种基于权利要求 1 所述系统的电子签约方法，其特征在于，包括：
   1. 用户通过量子安全认证登录系统；
   2. 生成合同实例并选择签名算法（RSA/ECC/ 国密 SM2）；
   3. 签署后数据经量子加密本地存证，并可选上链存证；
   4. 触发 AI 模型进行合同风险分析与法务流程自动化。

### **说明书摘要**

本发明公开了一种基于量子加密与 AI 驱动的智能安全法务系统及方法，通过量子设备指纹认证、多算法签名、区块链存证与 AI 风险分析，实现高安全性电子签约与自动化法务管理。系统支持动态防御、合规审计与多链存证，解决了传统系统在安全性、智能化与合规性上的不足，适用于政企、金融、法律等高安全需求场景。

## **说明**

1. **创新点聚焦**：突出量子加密、AI 驱动、区块链存证等核心技术，结合具体实施例说明技术优势。
2. **权利要求**：需根据技术细节进一步细化，确保覆盖核心方案（如量子指纹生成方法、AI 分析流程、多链存证机制等）。
3. **法律建议**：建议委托专利代理机构进一步完善技术点，确保新颖性、创造性与实用性，避免与现有技术冲突。

如需更详细的专利申请文件，可提供具体技术参数或补充实施例进行细化。