严翼共享 安全技术介绍

后量子安全 · 端到端加密 · 算法可切换

严翼共享 采用行业前沿的**后量子混合加密架构**：以 NIST 标准化的 **Kyber-768** 进行密钥交换，协商出临时会话密钥；数据加密层采用高效的 **CTR 流加密模式**，并**同时支持 AES-256-CTR 与 SM4-CTR** 两种对称加密算法，可根据部署环境与合规需求灵活切换。

核心逻辑遵循 **“密钥仅在两端、传输无明文”** 的安全原则，彻底升级传统 RSA/ECC 方案，既保留高速传输性能，又具备抗量子攻击能力，同时满足国际标准与中国国密合规要求。

核心技术特性

✓ 后量子安全

基于 Kyber-768（NIST FIPS 203 标准）密钥交换算法，可抵御现有及未来量子计算机的破解攻击，规避“现在收集、未来解密”的潜在风险。

✓ 算法可切换

数据加密层同时支持 AES-256-CTR（国际通用，硬件加速）与 SM4-CTR（中国国密标准），通过配置即可灵活切换，适配不同合规场景。

✓ 端到端安全

密钥仅在通信两端生成并留存，不经过网络明文传输、不落地存储。中间人即使截获传输流量，也无法获取有效密钥及解密数据。

✔✔ 合规可靠

遵循 NIST 后量子密码标准，天然支持前向保密（PFS）。单次会话密钥泄露不影响其他会话安全，符合高安全等级场景需求。

核心安全原则

密钥仅在两端，传输无明文

密钥仅在通信两端生成并留存，不经过网络明文传输

密钥不落地存储，会话结束即销毁

服务端无法解密传输内容

单次会话密钥泄露不影响其他会话安全

加密技术详解

🔐 **Kyber-768 后量子密钥交换**

Kyber 是 NIST 正式选定的后量子密码标准算法（FIPS 203，亦称 ML-KEM），属于基于格的密码体系。严翼共享 采用 Kyber-768 参数集，提供相当于 AES-192 的安全强度，能够在量子计算机时代依然保持可靠的密钥交换安全性。

Kyber-768 **NIST FIPS 203** 抗量子攻击

传统 RSA/ECC 在量子计算机面前将变得脆弱，Kyber-768 基于格难题，目前已知的任何量子算法都无法在有效时间内破解。密钥协商过程无需预共享密钥，天然支持前向保密。

⚡ AES-256-CTR / SM4-CTR 流式加密（可切换）

严翼共享 在数据加密层采用 CTR（Counter）流加密模式，支持边传输边加密、边接收边解密的流式处理，无需等待完整文件即可开始加解密，大幅提升大文件传输效率。

可选算法：**AES-256-CTR** **SM4-CTR**

- **AES-256-CTR**：国际通用标准，利用 AES-NI 硬件指令集实现极高的加解密吞吐量，适合对性能要求苛刻的场景。
- **SM4-CTR**：国家密码管理局公布的商用密码算法（GB/T 32907-2016），满足等保、密评等合规要求。

🔐 混合加密体系

严翼共享 采用**后量子混合加密架构**：

- **密钥交换层**：使用 Kyber-768 进行安全的密钥交换，协商出临时会话密钥（后量子安全）
- **数据加密层**：使用协商出的会话密钥，配合 **AES-256-CTR 或 SM4-CTR** 对实际文件数据进行高速流式加密

这种设计既保证了密钥交换的后量子安全性，又充分发挥了对称加密（AES 硬件加速 / SM4 国密合规）的高性能优势，同时通过算法可切换机制兼顾了国际标准与中国合规的双重要求。

端到端安全架构

密钥生命周期管理

- **生成**：密钥仅在发送端和接收端各自生成，服务端不参与密钥生成过程
- **交换**：通过 Kyber-768 后量子密钥封装机制安全交换，无需预共享密钥
- **使用**：密钥仅存在于两端内存中，用于本次会话的加解密操作
- **销毁**：会话结束后，密钥立即从内存中清除，不留任何痕迹

服务端零知识：信令服务仅负责连接协商和会话管理，不接触任何密钥材料；中继服务在跨网转发时，转发的也是加密后的数据流，无法解密查看内容。整个传输链路中，只有通信双方能够解密数据。

前向保密（PFS）

严翼共享 天然支持前向保密特性。每次传输会话都会生成全新的临时密钥对，互不关联。即使某个会话的密钥被破解，也不会影响其他会话的安全，更无法追溯解密历史传输内容。