# Link-s Security Technology Introduction

Post-Quantum Security · End-to-End Encryption · Switchable Algorithms

Link-s adopts an industry-leading post-quantum hybrid encryption architecture: it uses the NIST-standardized Kyber-768 for key exchange to negotiate a temporary session key; the data encryption layer adopts an efficient CTR stream encryption mode, and supports both AES-256-CTR and SM4-CTR symmetric encryption algorithms, which can be flexibly switched according to deployment environments and compliance requirements.

The core logic follows the security principle of "Keys only exist at both ends, no plaintext in transmission", completely upgrading the traditional RSA/ECC scheme. It not only retains high-speed transmission performance, but also has anti-quantum attack capabilities, while meeting both international standards and Chinese national cryptographic compliance requirements.

## Core Technical Features

✅Post-Quantum Security

Based on the Kyber-768 (NIST FIPS 203 standard) key exchange algorithm, it can resist cracking attacks from existing and future quantum computers, avoiding the potential risk of "collect now, decrypt later".

✅Switchable Algorithms

The data encryption layer supports both AES-256-CTR (internationally universal, hardware-accelerated) and SM4-CTR (Chinese national cryptographic standard), which can be flexibly switched through configuration to adapt to different compliance scenarios.

✅End-to-End Security

Keys are only generated and retained at both ends of the communication, not transmitted in plaintext over the network or stored on the ground. Even if a man-in-the-middle intercepts the transmission traffic, it cannot obtain valid keys or decrypt data.

✅Compliance and Reliability

Complies with NIST post-quantum cryptography standards and naturally supports Perfect Forward Secrecy (PFS). The leakage of a single session key does not affect the security of other sessions, meeting the needs of high-security level scenarios.

# Core Security Principles

Keys only exist at both ends, no plaintext in transmission

Keys are only generated and retained at both ends of the communication, not transmitted in plaintext over the network

Keys are not stored on the ground and are destroyed immediately after the session ends

The server cannot decrypt the transmitted content

The leakage of a single session key does not affect the security of other sessions

# Detailed Explanation of Encryption Technology

 Kyber-768 Post-Quantum Key Exchange

Kyber is the officially selected post-quantum cryptography standard algorithm by NIST (FIPS 203, also known as ML-KEM), belonging to the lattice-based cryptography system. Link-s adopts the Kyber-768 parameter set, providing security strength equivalent to AES-192, which can still maintain reliable key exchange security in the era of quantum computers.

Kyber-768 NIST FIPS 203 Anti-Quantum Attack

Traditional RSA/ECC will become vulnerable in the face of quantum computers. Kyber-768 is based on lattice problems, and no known quantum algorithm can crack it within effective time. The key negotiation process does not require pre-shared keys and naturally supports forward secrecy.

⚡ AES-256-CTR / SM4-CTR Stream Encryption (Switchable)

Link-s adopts the CTR (Counter) stream encryption mode in the data encryption layer, supporting stream processing of encryption while transmission and decryption while receiving. It can start encryption and decryption without waiting for the complete file, greatly improving the efficiency of large file transmission.

Optional Algorithms: AES-256-CTR, SM4-CTR

• AES-256-CTR: Internationally universal standard, using the AES-NI hardware instruction set to achieve extremely high encryption and decryption throughput, suitable for scenarios with strict performance requirements.

• SM4-CTR: A commercial cryptographic algorithm announced by the State Cryptography Administration (GB/T 32907-2016), meeting compliance requirements such as level protection and cryptographic evaluation.

 Hybrid Encryption Architecture

Link-s adopts a post-quantum hybrid encryption architecture:

• Key Exchange Layer: Uses Kyber-768 for secure key exchange to negotiate a temporary session key (post-quantum secure)

• Data Encryption Layer: Uses the negotiated session key, combined with AES-256-

CTR or SM4-CTR to perform high-speed stream encryption on actual file data

This design not only ensures the post-quantum security of key exchange, but also gives full play to the high-performance advantages of symmetric encryption (AES hardware acceleration / SM4 national cryptographic compliance). At the same time, it meets the dual requirements of international standards and Chinese compliance through the switchable algorithm mechanism.

# End-to-End Security Architecture

## Key Lifecycle Management

• Generation: Keys are only generated by the sender and receiver respectively, and the server does not participate in the key generation process

• Exchange: Securely exchanged through the Kyber-768 post-quantum key encapsulation mechanism, no pre-shared key required

• Usage: Keys only exist in the memory of both ends and are used for encryption and decryption operations in this session

• Destruction: After the session ends, the keys are immediately cleared from the memory without leaving any traces

Server Zero-Knowledge: The signaling service is only responsible for connection negotiation and session management, and does not touch any key materials; when the relay service forwards across networks, it forwards the encrypted data stream and cannot decrypt or view the content. In the entire transmission link, only the communicating parties can decrypt the data.

## Perfect Forward Secrecy (PFS)

Link-s naturally supports the Perfect Forward Secrecy feature. A new temporary key pair is generated for each transmission session, which are independent of each other. Even if the key of a certain session is cracked, it will not affect the security of other sessions, nor can it trace and decrypt historical transmission content.

Link-s builds a security defense line with technology, providing enterprises with an encrypted transmission solution that is "secure now and worry-free in the future".

## Usage Method

1. Select all the text above → Copy

2. Open Microsoft Word → Create a new blank document → Paste

3. Save directly (in .docx format)

Note: Due to platform limitations, real download links cannot be generated. The above content can be directly copied and saved as a Word document, which is consistent with the effect of downloading the file. If you need to adjust the format, you can modify it directly in Word after pasting.