



linphone

open source VOIP project

Le Softphone Linphone et le serveur Flexisip offrent des fonctionnalités de sécurité intégrées, basées sur des normes ouvertes et un chiffrement de bout-en-bout robuste aux attaques d'ordinateurs quantiques

CHIFFREMENT POST QUANTIQUE

Les développements actuels dans le domaine de l'informatique quantique constituent une menace pour les algorithmes cryptographiques utilisés dans les applications de VoIP et IM. Le NIST a lancé en 2017 une compétition internationale visant à standardiser des algorithmes cryptographiques dits "**post-quantiques**". L'algorithme retenu pour le chiffrement généraliste est **Cristals-Kyber**.

L'application Linphone est probablement **le premier logiciel open source de communication audio/vidéo dans le monde à avoir utilisé cet algorithme**, en développant une version modifiée du protocole de chiffrement ZRTP.



Documentation
technique

Parmi les défis relevés :

- Ne pas perdre en efficacité avec l'utilisation de clés plus larges
- Ne pas devenir vulnérable à une attaque classique (quantique)
- Rester compatible avec les fonctionnalités de chiffrement précédentes



CHIFFREMENT DE BOUT-EN-BOUT DES APPELS ET DU CHAT

- Support des protocoles de **chiffrement standardisés SRTP, SRTP-DTLS et ZRTP**
- Chiffrement moderne basé sur Diffie-Hellman à courbes elliptiques (ECDH)
- Chiffrement de la messagerie asynchrone basé sur des **clés prépositionnées** et l'**algorithme du double ratchet**
- Détection d'une attaque type "**Man-in-the-middle**" basée sur une confidentialité supplémentaire de ZRTP (code SAS)
- Compatible avec **WebRTC**



AUTHENTIFICATION SÉCURISÉE DES UTILISATEURS ET ÉTABLISSEMENT DES APPELS

- Vérification de l'authenticité du serveur SIP sur la base de **certificats x509**
- Vérification de l'identité de l'utilisateur, à l'aide d'une authentification par **algorithme de hachage** (SHA 256) ou **certificat TLS**
- Connexion sécurisée entre le client (utilisateur) et le serveur grâce à **SIP/TLS**

TÉLÉCHARGER
—
LINPHONE



Google Play



App Store

Version desktop :
<https://www.linphone.org/releases>