

[Apple CryptoKit](#) /  / [HPKE.Ciphersuite](#) / XWingMLKEM768X25519_SHA256_AES_GCM_256

Type Property

XWingMLKEM768X25519_SHA256_AES_GCM_256

A cipher suite for HPKE that uses the X-Wing KEM (ML-KEM-768 with X25519), SHA-2 key derivation with a 256-bit digest, and the Advanced Encryption Standard cipher in Galois/Counter Mode with a key length of 256 bits.

iOS 26.0+ | iPadOS 26.0+ | Mac Catalyst 26.0+ | macOS 26.0+ | tvOS 26.0+ | visionOS 1.0+ | watchOS 26.0+

```
static let XWingMLKEM768X25519_SHA256_AES_GCM_256: HPKE.Ciphersuite
```