

[Apple CryptoKit](#) / Curve25519

Enumeration

Curve25519

An elliptic curve that enables X25519 key agreement and Ed25519 signatures.

iOS 13.0+ | iPadOS 13.0+ | Mac Catalyst 13.0+ | macOS 10.15+ | tvOS 13.0+ | visionOS 1.0+ | watchOS 6.0+

`enum` Curve25519

Topics

Performing operations

`enum` KeyAgreement

A mechanism used to create a shared secret between two users by performing X25519 key agreement.

`enum` Signing

A mechanism used to create or verify a cryptographic signature using Ed25519.

Relationships

Conforms To

Sendable, SendableMetatype

See Also

Public key cryptography

`enum P521`

An elliptic curve that enables NIST P-521 signatures and key agreement.

`enum P384`

An elliptic curve that enables NIST P-384 signatures and key agreement.

`enum P256`

An elliptic curve that enables NIST P-256 signatures and key agreement.

`struct SharedSecret`

A key agreement result from which you can derive a symmetric cryptographic key.

`enum SecureEnclave`

A representation of a device's hardware-based key manager.

`enum HPKE`

A container for hybrid public key encryption (HPKE) operations.