Curve 25519 Signatures & Key Exchanges

A quick intro and brief demo

Ed25519 is a...

EdDSA Signature scheme using **Curve25519** with **SHA-512**

- Being standardized during for SSH protocol authentication
- BouncyCastle-provider, NaCL, OpenSSL has implementation of the Ed25519 signature scheme.

Advantages of Ed25519

ed25519.cr.yp.to/index.html

1. Fast Single Signature verification, batch verification, signing & key-generation.
2. High Security with small keys. (Key size : 256bits)
3. Collision resilience, system does not break if hash function collides.
4. No secret array indices/ branch conditions. (Immunity towards side-channel attacks, cache timing attacks or hyperthreading attacks)
5. Foolproof session keys : Deterministic signatures.
6. Not NIST, therefore not NSA.

[ed25519] 23pp. Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, Bo-Yin Yang. High-speed high-security signatures. Journal of Cryptographic Engineering 2 (2012), 77-89. Document ID: a1a62a2f76d23f65d622484ddd09caf8. URL: https://cr.yp.to/papers.html#ed25519. Date: 2011.09.26

OpenSSL & Bouncy Castle JAVA Demo
https://github.com/ToraNova/25519demo