EC Ciphersuites for TLS 1.2

draft-ietf-tls-rfc4492bis-07

Yoav Nir - IETF 95

Changes since Yokohama

- Added EdDSA
- Updated references
- Textual improvements
- Reflected early assignment of ecdh_x25519 (29) and ecdh_x448 (30)

Next Steps

- Are we done?
- Move to WGLC next?