draft-mavrogiannopoulos-chacha-tls

IETF 89

A. Langley
W. Chang
N. Mavrogiannopoulos
J. Strombergson
S. Josefsson

- Goal: Provide alternative stream cipher to RC4

- draft-josefsson-salsa20-tls – March 2013
  - Salsa20 with ”traditional” HMAC-based MACs
- CFRG suggested ChaCha instead of Salsa20
- draft-agl-tls-chacha20poly1305 – Sep 2013
  - ChaCha with Poly1305 MAC
- draft-mavrogiannopoulos-chacha-tls-00
  - ChaCha with HMAC-SHA1
- draft-mavrogiannopoulos-chacha-tls-01
  - ChaCha with HMAC-SHA1 and Poly1305
  - Superset of all drafts - everyone co-authors
  - Details in the draft!

Moving forward

- Please review and implement the draft!
- Can we adopt this as WG item?