ChaCha20-Poly1305

Adam Langley <agl@google.com>

Chip	**AES-128-GCM**	**ChaCha20-Poly1305**
OMAP 4460	24.1 MB/s	75.3 MB/s
SnapDragon S4 Pro	41.5 MB/s	130.9 MB/s
Sandy Bridge Xeon	1272 MB/s	727 MB/s

(1350 byte chunk sizes)

16 byte authentication tag, no padding.

Nonce input is the sequence number.

Nonce/counter split changed from 64/64 to 96/32 - useful for IPSec. Maybe call it ‘NChaCha’.

Poly1305 input moved around a little from original draft.

Initial draft in use between Chrome and Google.