draft-nir-cfrg-chacha20-poly1305-01

ChaCha20 and Poly1305 for IETF protocols

Yoav Nir
CFRG
IETF 89

What is this draft?

- A description of the ChaCha20 stream cipher, the Poly1305 authenticator, and Adam's AEAD combination of them both.
- Enough details and test vectors for a competent coder to make a correct implementation
- Security considerations to allow a good coder to avoid pitfalls in implementations, such as side-channels.
- A stable reference for IETF protocols
  - Such as ESP and TLS.

What this draft is not

- We don't define the algorithms
  - Suggestions and criticiques are welcome, but should really be taken up with DJB in other venues.
- The draft does not contain any security proofs, although we might want to reference some.
- The draft doesn't contain specific instructions on how to avoid timing attacks on Poly1305, or whether that is even a concern.
- We don't explain the reasoning behind the design.

Changes from regular ChaCha

- The nonce : block sequence number split was changed from 64:64 to 96:32
  - Existing AEAD constructions have 96-bit nonces
  - 2^32 64-byte blocks should be enough (256 GB)
    - For an ESP packet or a TLS record. Tarball?
- Adam's AEAD construction:
  - Encrypt
  - One-time MAC key by running ChaCha20 on a nonce
  - Poly1305 (AAD||AADlen||ciphertext||ciphertext_len)

Design decisions

- Lengths, and conversion from external to internal representation is little-endian, unlike the "network order" that was common in earlier specs
- Bit instead of byte count in lengths
- The 96:32 split for nonce:counter
- Poly1305 one-time key generation using Chacha20
- Use only the 20-round 256-bit key variation of ChaCha
  - 8- and 12- round variations exist, as well as 128-bit key
  - Performance for 256-bit and 128-bit is the same
  - But reduced rounds would be faster

What's missing

- More test vectors at every stage
  - Need someone else to check the test vectors
  - Othewise we're setting the implementers up for failure.
- Can probably get an undergrad to do it next year.
- Better discussion of the security considerations
- References to security proofs
- More?

Questions?

Comments?

Volunteer to review?

Volunteer to provide references?

Volunteer to check the test vectors?