AEAD Limits

draft-irtf-cfrg-aead-limits

IETF 111 - CFRG - Online

Updates

Current version:

- Added backing analysis for TLS 1.2 (no nonce randomization)
- Added example limits for reference
- Editorial cleanup

Next revision

- Fixed TLS 1.2 numbers
- Updated ChaCha20+Poly1305 analysis (from upcoming CCS paper)

Open Issues

Account for AAD-length in analysis (#16)

- Status: Requires extended analysis based on 2018/993
- Proposal: Park until complete, currently working with Stefano on updates

Add SIV limits (#18)

- Status: Needs work
- Proposal: Close and punt to future draft

Next Steps

Close and resolve open issues

Commence RGLC