draft-irtf-cfrg-aead-limits-01

Günther/Thomson/Wood

Status

draft-irtf-cfrg-aead-limits-01 (current), updated

- Updated limits based on analysis in IACR 2018/993

draft-irtf-cfrg-aead-limits-02 (next), help needed for remaining issues

- SIV mode limits
- PQ implications
- Tweaks for where AAD >> P