draft-irtf-cfrg-hpke

IETF 106 – CFRG – Singapore

Updates

Minor technical changes

“Single-shot” API

Lots of API clarification and editorial cleanup

Test vectors

Interop on Base/PSK between Go (Barnes) and C (Wood) implementations

Analysis

Assuming:

- Gap-DH for DH
- IND-CCA2 for AEAD
- ROM for Extract and Hash
- PRF for Expand

Goals:

- IND-CCA2 Public Key Encryption
- Relevant authentication properties by mode

	no key compromise		long-term key compromise	
Mode	**Secrecy**	**Auth[1]**	**Secrecy**	**Auth[1]**
Base	Done	–	–	–
PSK	Done	Done	WIP	WIP
Auth	Done	Done	WIP	WIP
AuthPSK	Done	Done	WIP	WIP

CryptoVerif proofs from Ben Lipp at Inria. [1]All messages are replayable. Valid for P-256 and P-521; Curve25519 and Curve448 are WIP.

Status and Next Steps

Status

- Implementation and interop done on Base, PSK modes
- Interop still pending for Auth, AuthPSK modes
- Analysis in progress for key compromise cases, Curve25519 and Curve448, and more correspondence properties e.g. identity binding

Start RGLC?