Adding new Crypto to HIP

draft-moskowitz-hip-new-crypto
IETF 106 TM-RID BOF
Nov 19, 2019
Robert Moskowitz
What is New?

- New signature algorithms
  - EdDSA 25519 and 448
- New hashing algorithms
  - FIPS 202 and SP800-185
    - SHA3, SHAKE, cSHAKE, KMAC
      - These change EVERYTHING!
- New NIST AEAD lightweight competition
  - Keyak as placeholder
This changes EVERYTHING in HIPv2 crypto

Smaller
Lighter
Faster

...
EdDSA

• RFC 8032
  – Only EdDSA 25519 and 448
    • I really do not like 25519 using SHA512 rather than SHAKE128. It is what it is.

• Smaller key size!
  – 32 and 57 bytes
    • Why 57 not 64? It is not called Goldilocks for nothing!
  – Signatures twice key size
Curve25519 et al.

- RFC 7748
  - Curve25519 and Curve448
  - ‘Natural’ compressed representation
    - Applies to EdDSA as well
    - No patent issues as in NIST p256

- Already specified in HIP DEX
  - But static for use as HI
  - Now added for ephemeral DH
Hashing in All manners

- HIP uses hashing in many places in many ways
  - Keccak is a major change to approach to hashing and has a significant impact on many aspects of HIP
  - Sponges are AMAZING things!
    - Goto https://keccak.team to learn about them
    - FIPS 202 has details
    - SP800-185 expands considerably on variable outputs
    - Plus SP800-56Cr1 for keying material generation
Hashing – SHAKE rattle and rock

- SHAKE and its derivatives provide variable length output with known crypto strength
  - Maybe should have been called SQUEEZE?
  - No more truncating hashes
    - Important impact on ORCHID generation. Just output 96 bits (or 64 for HHit!) instead of which bits to select
  - SHAKE128 for RHASH in HIP
KMAC rather than HMAC

• KMAC does in one sponge function
  – For what HMAC needs two hashes

• And no truncation needed for HIP_MAC and HIP_MAC2
KMAC for KEYMAT

• KMAC does in one sponge function
  – For what HIP KEYMAT needs two HMAC operations

• Jury is still out on this construction
  – Only a couple cryptographers have commented
    • Seems I have it right
    • But warrants more review
Lightweight AEAD cipher

- NIST conducting Lightweight cipher completion
  - https://csrc.nist.gov/Projects/lightweight-cryptography
- No winner yet, but.
  - Keyak is Keccak based
    - And thus same code base and FPRG implementation
    - Good for a starting point
- Use in ESP (addendum to 7402?)
- Use in HIP_CIPHER
Finally, the PRF

- And no pudding today
- See sp800-185 Appendix B for PRF construction
Questions?