SHA3-based MACs

Ray Perlner
Computer Security Division, NIST
Ray.Perlner@nist.gov
SHA-3 2014 Workshop
August 22, 2014

Outline

- Predecessors
  - FIPS 198 (HMAC)
  - SP 800-108 (KDFs from PRFs)
  - Key Pack
- New specifications
  - KMAC
  - XMAC
  - XKDF
  - Block sizes for SHA3-HMAC

FIPS 198

- Specifies HMAC

  HMAC (K, text)= H(K⊕opad || H(K ⊕ ipad || text))

- Extra complication needed because of the length extension property of SHA1 and SHA2
- Parameterized by a Block Size
- Allows Truncation

SP 800-108

- Specifies KDF Constructions built from a PRF
  - Counter, Feedback, Double-Pipeline
  - PRF can be (untruncated) HMAC or CMAC
  - Ambiguities can occur if the PRF is variable length (e.g. a MAC based on the SHAKEs)
    - E.g. Counter mode could produce outputs related as A|B|C|D,

      A|C|E|G
    - We will solve this problem by only considering KMAC, but not XMAC, to be a PRF

Key Pack

- Defined by the Keccak team in “Keyak” and “Ketje” CAESAR entries
- Suggested for KMAC
- Definition:

$$\textbf{Keypack}(K, \ell) = \textbf{enc}_8(\ell/8) \,||\, K \,||\, 1\,0^{\ell - \text{len}(K) - 9}$$

- ℓ is the length of the whole key pack in bits.
- ℓ must be a multiple of 8 between len(K) + 9 and 255*8.
- Need ℓ to be defined further for compatibility.

KMAC

- Usable as a MAC or PRF
- Defined in terms of drop ins.
- Definition:

  ***MAC(text) = KMAC*(*K, text) = H*(Keypack(*K,* ℓ*)* || *text*)**

- ℓ =8*⌈(len(*K*)+9)/8⌉

XMAC

- Usable as a MAC, but not a PRF
- Defined in terms of XOFs
- Definition:

  $MAC(text) = XMAC(K, text, \lambda) = X(\text{Keypack}(K, \ell) \,||\, text, \lambda)$

- $\ell = 8 * \lceil (\text{len}(K) + 9)/8 \rceil$
- Choice of λ is based on FIPS 198 rules for truncation of HMAC (at least 32 bits.)

XKDF

- Since SP 800-108 KDFs can't use XMAC, we define a KDF that can use XMAC.

- Definition:

$$K_O := \text{XMAC}(K_I,\ \text{Label} \,||\, 0x00 \,||\, \text{Context} \,||\, [L]_2,\ L)$$

HMAC block sizes

Algorithm	HMAC Block Size (in Bits)
SHA3-224	1152
SHA3-256	1088
SHA3-384	832
SHA3-512	576

Questions?