# Extendable-Output Functions (XOFs)

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

# What is a XOF (pronounced “Zoff”)?

*“A function on bit strings in which the output can be extended to any desired length.”*

- Two input parameters: Message, Output Length
  - If XOF(*M*, 128) = *AB*,

    then XOF(*M*, 256) = *ABCD*

# XOFs in draft FIPS 202

- Draft FIPS 202 defines SHAKE128, SHAKE256

- The numbers 128 and 256 are the security strengths the XOFs "generally support"
  - Exceptions on the low side (short outputs)
    - e.g. Collisions in SHAKE128 outputs shorter than 256 bits
    - e.g. Preimages in SHAKE128 outputs shorter than 128 bits
  - Exceptions on the high side
    - e.g. MAC key recovery attack (XMAC)

# What are XOFs good for?

- Signatures
  - RSA Full Domain Hash (FDH)
  - RSA OAEP: The Mask Generation Function (MGF)
  - These things are currently implemented with a complex construction of fixed length hashes and counters.
- Stream Ciphers
  - Seems like a pretty straightforward implementation of a keystream.
- KDFs
  - NIST plans to define “XKDF” (see my KMAC presentation.)

# Additional Security Consideration

- XOFs can produce related outputs
- This can be a problem for KDFs
  - Example 3des keys generated as SHAKE128(K,L)
  - Confusion over whether L=112 or 168

  *SHAKE128(K, 112) = ab; SHAKE128(K,168) = abc*
  - Two shared keys allow an adversary to decrypt in $2^{56}$ operations
  - The above KDF is improbably naïve, but even SP 800-108 KDFs can be made to give related outputs with XOFs used in place of hash functions.
- Thus: **we cannot give general approval for use of XOFs in place of hash functions**

# What does Approved mean?

- It's specified as Approved in a FIPS or SP

- SHAKE128 and SHAKE256 are Approved
  - You can still implement them and get FIPS 140-2 certification
  - **But not if you use them in place of existing Approved hash functions, PRFs etc.**
  - We will explicitly Approve some applications of XOFs in the near future

# What should we do about it? (Input Requested)

White list  Approved uses of XOFs

**Options:**

1. Focus on existing Approved applications for hash functions
2. Focus on specialized applications designed for XOFs
    - Define domain-separated “variable-length hashes” for existing hash applications? (See Morrie’s talk on Domain Extensions)