SHA3:
FIPS 202 is Out--Now What?

John Kelsey, NIST

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html

FIPS 202 is Out!

Coming up Next: SHA3-Derived Functions:

- KMAC = Keyed hash
- TupleHash = hash of a tuple of strings
- Fast Parallel Hash = depth-one tree hash

ALL *domain separated* and *customizable*

Domain Separated?

- This means you can't compute KMAC by calling SHAKE or SHA3
- Outputs of different functions ***completely unrelated***
- This should make it a little harder to shoot yourself in the foot with these functions

Customization Strings?

This is domain separation controlled by the user

- KMAC["KDF"](K,X)

is *completely unrelated to*

- KMAC["Message Block"](K',X')

Like strong typing for uses of a hash function

Customization Strings

- All new SHA3-derived functions will support "customization strings" to let users further domain-separate them

- We plan to introduce a new SP to allow customization strings for Shakes and SHA3, too

For More Information

http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

http://csrc.nist.gov/groups/ST/toolkit/secure_hashing.html