

DRAFT FIPS 202  
SHA-3 Permutation-Based Hash Standard  
– Status Update –

Quynh Dang  
Computer Security Division  
ITL, NIST

# Proposed SHA-3 Algorithms

- ▶ Four fixed-length algorithms with two capacities; alternatives to SHA-2s
  - ▶ SHA3-224 (c=256)
  - ▶ SHA3-256 (c=256)
  - ▶ SHA3-384 (c=512)
  - ▶ SHA3-512 (c=512)
- ▶ Two variable-length “sponge” algorithms with two capacities
  - ▶ SHAKE256 (c=256)
  - ▶ SHAKE512 (c=512)

# Expected Security Strengths of SHA-3s

	SHA3-224	SHA3-256	SHA3-384	SHA3-512
Collision Resistance Strength (in bits)	112	128	192	256
Preimage/Second Preimage Resistance Strength (in bits)	128	128	256	256

# Expected Security Strengths of SHA-3s

## – Continued –

	SHAKE256	SHAKE512
Collision Resistance Strength (in bits)	Min(128, hash length in bits/2)	Min(256, hash length in bits/2)
Preimage/Second Preimage Resistance Strength (in bits)	Min(128, hash length in bits)	Min(256, hash length in bits)

# Future Specification Possibilities

- ▶ Single-pass MAC function
- ▶ Tree hashing mode(s)
- ▶ Pseudo random function
- ▶ Stream cipher, and
- ▶ Authenticated encryption function

# Comments

NIST's Crypto Toolkit:

<http://csrc.nist.gov/groups/ST/toolkit/index.html>

SHA-3 Standardization Timeline:

[http://csrc.nist.gov/groups/ST/hash/sha-3/timeline\\_fips.html](http://csrc.nist.gov/groups/ST/hash/sha-3/timeline_fips.html)

Any comments/questions?

Discussion mailing list: Hash-forum@nist.gov

Comments for NIST: internal-hash@nist.gov