SHA-3 Standard: Overview, Status, Public Comment

Morris Dworkin

SHA-3 2014 Workshop

August 22, 2014

SHA-3 Background

- Wang hash function analysis (2004-2005)
  - Breaks many Merkle-Damgård hash functions
- NIST initiates SHA-3 competition (Nov. 2007)
  - SHA-2 family remains secure
  - Develop SHA-3 family of alternatives
    - "Drop-in replacements"
  - Offer special features
- NIST selects KECCAK for SHA-3 (Oct. 2012)

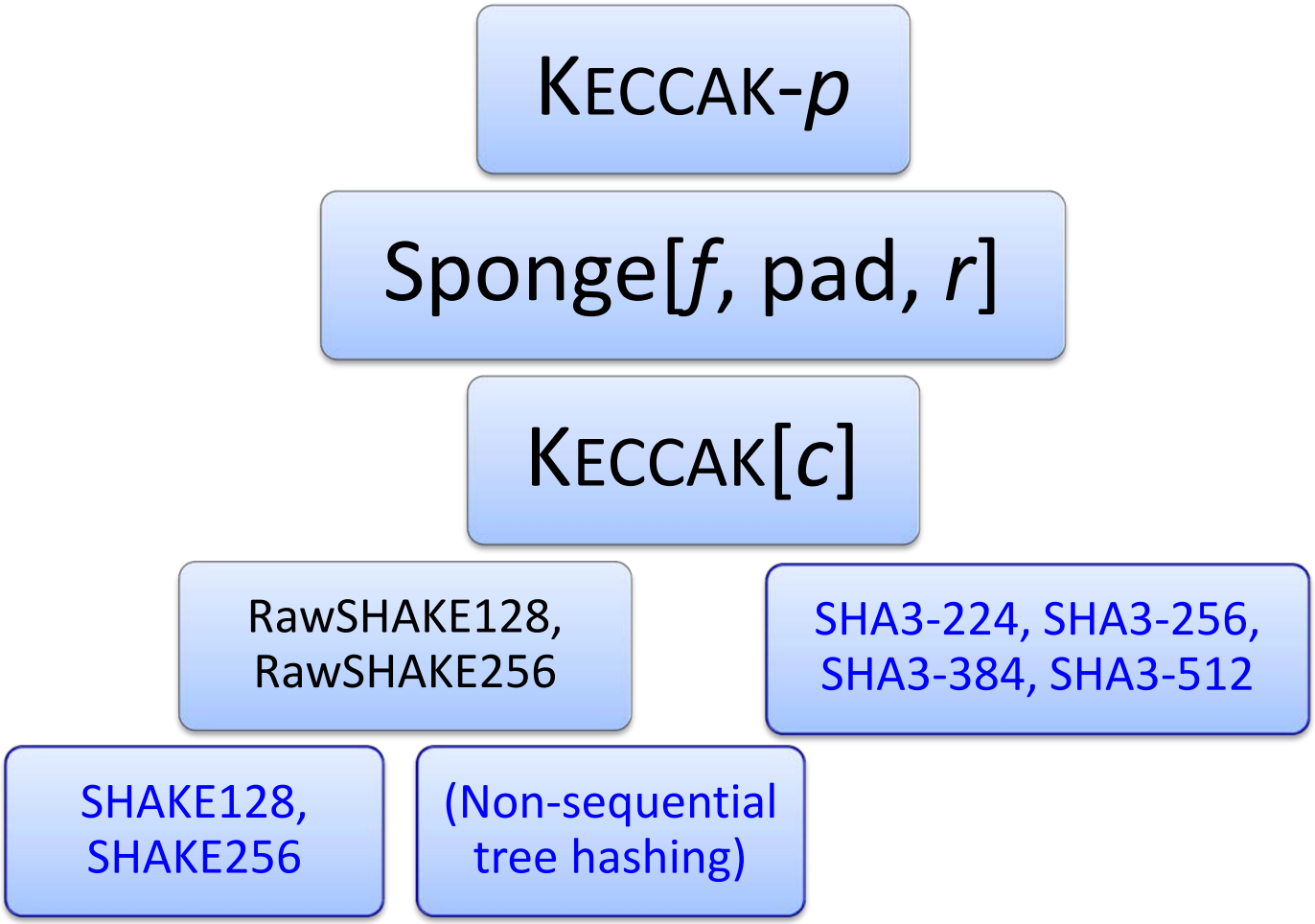
Draft Federal Information Processing Standard (FIPS) Publication 202

- *SHA-3 Standard: Permutation-based Hash and Extendable Output Functions*
  - Developed in consultation with KECCAK team
- March 2014 draft posted initially
- May 2014 draft posted currently
  - http://csrc.nist.gov/publications/drafts/fips-202/fips_202_draft.pdf
  - A few editorial corrections to March draft

Main Procedural Decisions

- Form:
  - New FIPS vs. revising FIPS PUB 180-4
- Hybrid Structure:
  - Permutation standard
    - Regard hash functions as permutation modes
    - Facilitates future specifications
      - e.g. duplex construction/authenticated encryption
  - Hash function standard
    - Expected from SHA-3 Competition

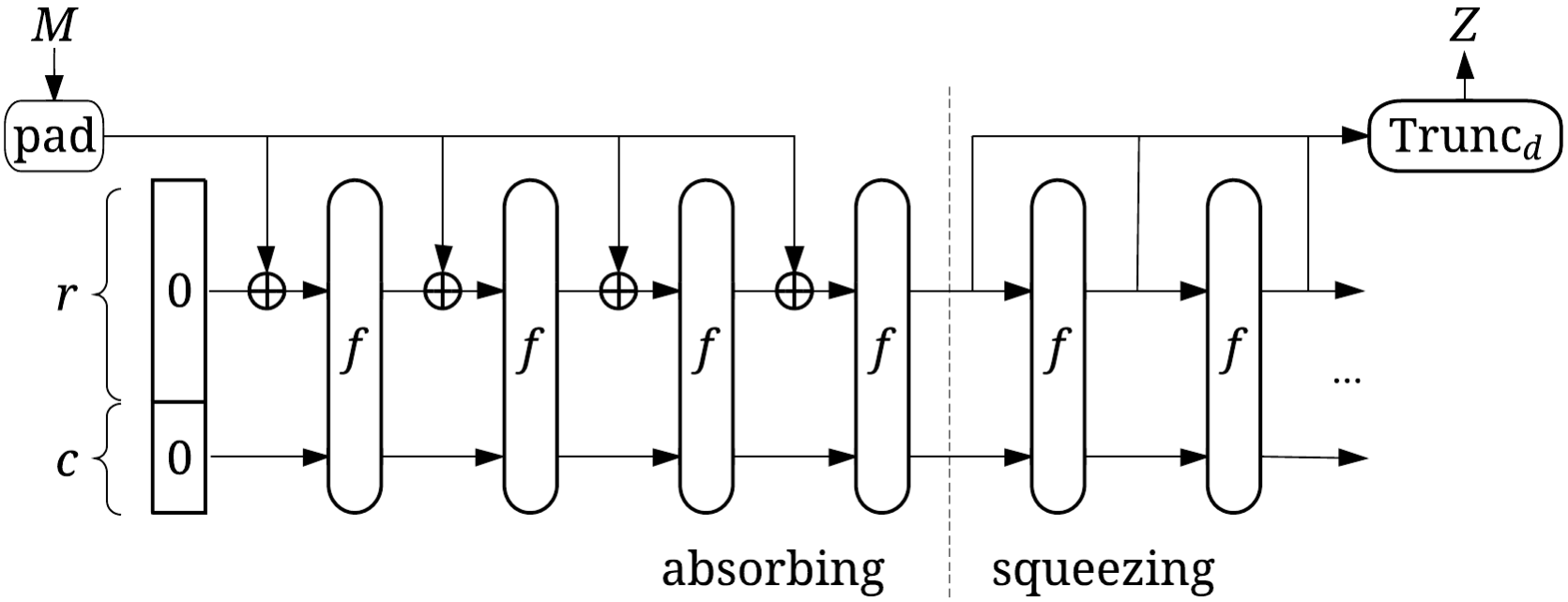
Layers of Functions



Main Technical Decisions

- Use submitted capacities of hash functions
- Specify two new/additional sponge functions
  - with arbitrary/flexible output length
- Supplement padding scheme
- Generalize KECCAK-*f* permutations
- Switch bit ordering convention for hexadecimal strings

Sponge Functions



Tunable parameter

- Suggested in call for candidate algorithms
  - *Federal Register* Nov. 2, 2007
  - "…allows the selection of a range of possible security/performance tradeoffs ."
- In KECCAK, the capacity *c*
  - determines generic security
  - determines rate *r* = 1600 – *c* (throughput)
- For each KECCAK candidate *c*=2*d*
  - minimum *c* for 2^{nd} preimage requirement in call

Withdrawn NIST Proposal for Capacities

- Two different capacities instead of four
  - Simplify testing, interoperability
  - Still promote flexible implementations
- Trade preimage resistance for performance
  - c=256 for SHA3-224, SHA3-256
  - c=512 for SHA3-384, SHA3-512
- Presented in several venues starting Feb. 2013
- Withdrawn in Nov. 2013

Extendable-Output Functions (XOFs)

- Sponge functions have “infinite” output
  - Truncated to fixed output length → hash function
    - SHA3-224, SHA3-256, SHA3-384, SHA3-512
  - User/implementer chooses output length → XOF
    - SHAKE128, SHAKE256
- Rationale for XOFs
  - Flexibility to tailor to applications
- A new category of NIST-approved functions
  - Extendability can affect security
  - Guidance, applications pending

Three Types of Padding Bits

- Multi-rate padding
  - 10*1
  - for all KECCAK[*r*, *c*] functions
- Domain Separation
  - 11 → RawSHAKE function
  - 01 → SHA-3 hash function
- Sakura coding for parallel hashing
  - 11 → sequential RawSHAKE = SHAKE

Generalize Permutation

- KECCAK-*f*[*b*]
  - family of seven KECCAK permutations
  - b is 25, 50, 100, 200, 400, 800 or 1600
  - round consists of five step mappings
- KECCAK-*f*[1600] underlies each SHA-3 function
  - 24 rounds
- FIPS 202 defines KECCAK-*p*[*b, n_r*]
  - generalizes KECCAK-*f*[*b*]
  - number of rounds is input parameter

Bit-Ordering Convention

- Hexadecimal representations of inputs
  - test vectors
- Which bit of the byte is “first”?
  - most significant bit 0xB4 = 10110100
  - least significant bit 0xB4 = 00101101
- SHA-3 specified with LSB ordering, like KECCAK
  - minor change on non-byte aligned messages
  - other NIST algorithms use MSB ordering

90-day Public Comment Period

- On Draft FIPS 202
  - and revised applicability clause of FIPS 180-4
- Closes August 26, 2014
- Announced in Federal Register Notice
  - Dated May 28, 2014
  - https://www.federalregister.gov/articles/2014/05/28/2014-12336/announcing-draft-federal-information-processing-standard-fips-202-sha-3-standard-permutation-based

Public Comments (as of Aug. 14)

- National Security Agency
- European Telecommunications Standards Institute—*Technical Committee "Security Algorithms Group of Experts" (TC SAGE)*
- Thales e-Security
- Clinton M. Bowen

Addresses for Public Comments

- Email:
  - SHA3comments@nist.gov
  - subject line
    - Comment on Draft FIPS 202, or
    - Comment on draft revision to the Applicability Clause of FIPS 180
- Mail:

  Chief, Computer Security Division
  Information Technology Laboratory
  ATTN: Comments on Draft FIPS 202 for SHA-3
  National Institute of Standards and Technology
  100 Bureau Drive, Stop 8930
  Gaithersburg, MD 20899-8930.