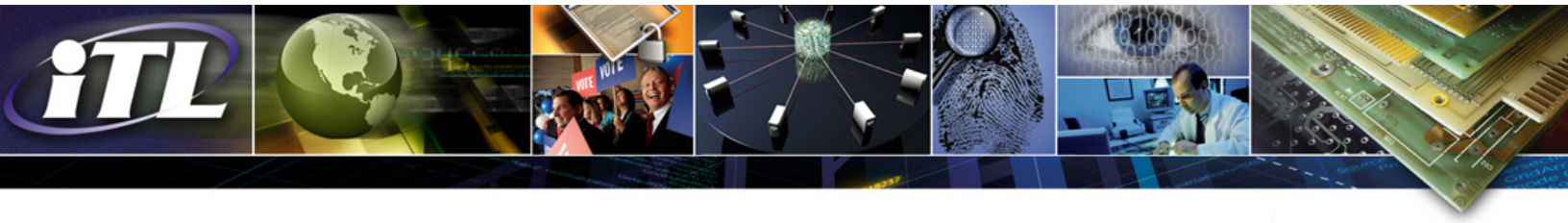


ITL BULLETIN FOR SEPTEMBER 2015

ADDITIONAL SECURE HASH ALGORITHM STANDARDS OFFER NEW OPPORTUNITIES FOR DATA PROTECTION

Morris Dworkin, Larry Feldman, and Greg Witte, Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Background

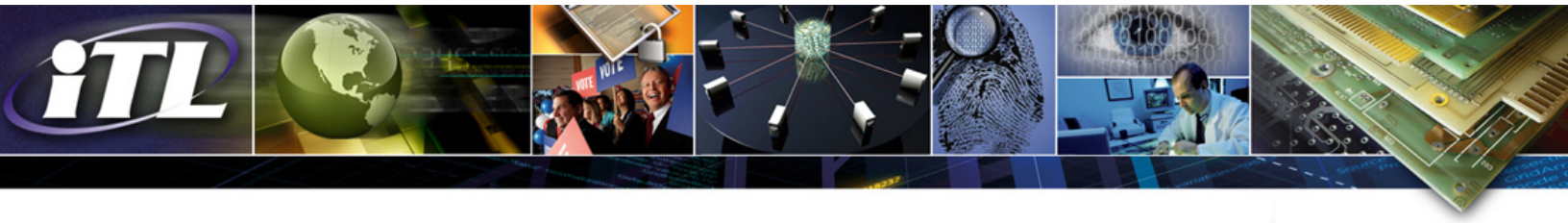
NIST published a *Federal Register* Notice, 80 FR 46543, on August 5, 2015, to announce the publication of Federal Information Processing Standard (FIPS) 202, *SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. FIPS 202 specifies the SHA-3 (Secure Hash Algorithm-3) family of hash functions, as well as mechanisms for other cryptographic functions to be specified in the future. The use of these hash functions for the protection of sensitive, unclassified information in federal applications is approved by a revision to the Applicability Clause of FIPS 180–4, *Secure Hash Standard (SHS)*.

SHA-3

FIPS 202 specifies a new family of functions that supplement SHA-1 and the SHA-2 family of hash functions specified in FIPS 180-4. This new family, called SHA-3, is based on KECCAK, the algorithm that NIST selected as the winner of the public SHA-3 Cryptographic Hash Algorithm Competition.[1] The SHA-3 family consists of four cryptographic hash functions and two extendable-output functions. These functions use the sponge construction, which is a simple, iterated construction for building a function with variable-length inputs and outputs from a fixed-length permutation.

A *hash function* is a function on binary data (i.e., bit strings) for which the length of the output is fixed. The input to a hash function is called the *message*, and the output is called the (*message*) *digest* or *hash value*. The digest often serves as a condensed representation of the message. The four SHA-3 hash functions are named SHA3-224, SHA3-256, SHA3-384, and SHA3-512; in each case, the suffix after the dash indicates the fixed length of the digest, e.g., SHA3-256 produces 256-bit digests. The SHA-2 family of hash functions, i.e., SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256, offers the same set of digest lengths. Thus, the SHA-3 hash functions offer alternatives to the SHA-2 functions.

[1] NIST documented its selection of KECCAK in NISTIR 7896, *Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition* (November 2012).



An *extendable-output function* (XOF) is a function on bit strings (also called messages) in which the output can be extended to any desired length. The two SHA-3 XOFs are named SHAKE128 and SHAKE256. The suffixes “128” and “256” indicate the security strengths that these two functions can generally support, in contrast to the suffixes for the hash functions, which indicate the digest lengths. SHAKE128 and SHAKE256 are the first XOFs that NIST has standardized.

The six SHA-3 functions are designed to provide special properties, such as assurance that they only work “one-way” (i.e., one cannot derive the originating message from the cryptographic hash) and are collision-resistant (i.e., it is unlikely that two different inputs will produce the same hash value.) Cryptographic hash functions are fundamental components in many information security applications, such as digital signatures, message authentication codes, key derivation, and pseudorandom bit generation.

Each of the six SHA-3 functions employs the same underlying permutation as the main component in the sponge construction. In effect, the SHA-3 functions are *modes of operation* (modes) of the permutation.

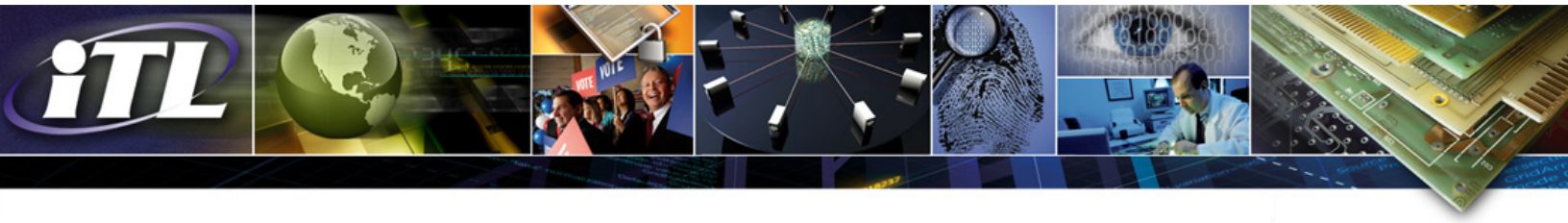
The four SHA-3 hash functions differ slightly from the instances of KECCAK that were proposed for the SHA-3 competition. In particular, a two-bit suffix is appended to the input messages, in order to distinguish the SHA-3 hash functions from the SHA-3 XOFs, and to facilitate the development of new variants of the SHA-3 functions that can be dedicated to individual application domains.

Extendable-Output Functions (XOFs)

The introduction of extendable-output functions is a significant feature of the standard. An XOF, like SHAKE128 or SHAKE256, can be seen as a generalization of hash functions where the output length is not fixed, but is potentially infinite. Concretely, XOFs can be used instead of complex constructions involving hash functions and counters, such as key derivation functions and stream ciphers.

Another important conceptual difference between XOFs and traditional hash functions is that an XOF's security strength can be chosen (e.g., through a KECCAK parameter called the capacity) and is not bound to its output length. This flexibility allows for better security performance trade-offs. For instance, with a key derivation function, the length of the derived key material can vary greatly from one application to another, in a way that is generally not related to the required security strength.

The digest lengths in FIPS-approved hash functions are 160, 224, 256, 384, and 512 bits. When an application requires a cryptographic hash function with a different digest length, an XOF is a natural alternative to constructions that involve multiple invocations of a hash function and/or truncation of the output bits. However, XOFs are subject to the additional security consideration that is described in FIPS 202, Section A.2.



FIPS 180-4

FIPS 180-4 specifies seven cryptographic hash algorithms: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256. FIPS 180-4 (2015) supersedes FIPS 180-4 (2012), with the only change being made in the Applicability Clause. The revision to the Applicability Clause of FIPS 180-4 approves the use of hash functions specified in either FIPS 180-4 or FIPS 202 when a secure hash function is required for the protection of sensitive, unclassified information in federal applications, including hash functions used as components within other cryptographic algorithms and protocols.

Conformance

Implementations of the six SHA-3 functions—SHA3-224, SHA3-256, SHA3-384, SHA3-512, SHAKE128, and SHAKE256—may be tested for conformance to FIPS 202 under the auspices of the Cryptographic Algorithm Validation Program (CAVP). SHA3-224, SHA3-256, SHA3-384, and SHA3-512 are approved cryptographic hash functions.

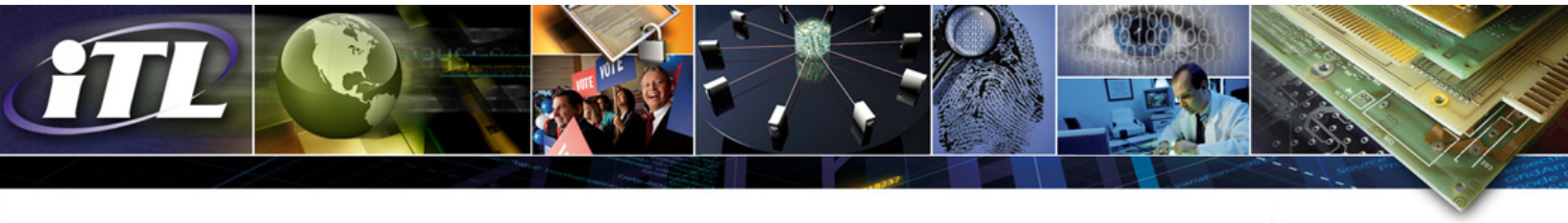
Future Plans

The SHA-3 algorithms offer additional flexibility to security designers. While SHA-2 has held up well, and NIST considers SHA-2 to be secure and suitable for general use, SHA-3 may create new opportunities for implementing security in networks. In particular, KECCAK–based modes could be developed for other types of cryptographic functions. The benefit would be that they could be implemented alongside SHA-3 with minimal additional overhead, and may be useful for embedded or "smart" devices that are networked and sometimes described as being part of the Internet of Things.

NIST has expressed its intention to approve other KECCAK–based modes of operation by way of NIST Special Publications that refer to FIPS 202. At the SHA-3 2014 Workshop,[2] NIST presented plans for standardizing the following additional KECCAK–based modes:

- Parallelizable hashing;
- Message authentication codes and key derivation functions;
- Authenticated encryption; and
- Generic domain separation mechanisms.

[2] See the workshop program and presentations.



Additional Resources

FIPS 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions

FIPS 180-4, Secure Hash Standard *(SHS)*

NISTIR 7896, *Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition*

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov