SHA-3 Selection Announcement

The National Institute of Standards and Technology (NIST) is pleased to announce the selection of **KECCAK** as the winner of the SHA-3 Cryptographic Hash Algorithm Competition and the new SHA-3 hash algorithm. KECCAK was designed by a team of cryptographers from Belgium and Italy, they are:

- Guido Bertoni (Italy) of STMicroelectronics,
- Joan Daemen (Belgium) of STMicroelectronics,
- Michaël Peeters (Belgium) of NXP Semiconductors, and
- Gilles Van Assche (Belgium) of STMicroelectronics.

NIST formally announced the SHA-3 competition in 2007 with an open call for the submission of candidate hash algorithms, and received 64 submissions from cryptographers around the world. In an ongoing review process, including two open conferences, the cryptographic community provided an enormous amount of expert feedback, and NIST winnowed the original 64 candidates down to the five finalist candidates – BLAKE, Grøstl, JH, KECCAK and Skein. These finalists were further reviewed in a third public conference in March 2012.

NIST chose KECCAK over the four other excellent finalists for its elegant design, large security margin, good general performance, excellent efficiency in hardware implementations, and for its flexibility. KECCAK uses a new "sponge construction" chaining mode, based on a fixed permutation, that can readily be adjusted to trade generic security strength for throughput, and can generate larger or smaller hash outputs as required. The KECCAK designers have also defined a modified chaining mode for KECCAK that provides authenticated encryption.

Additionally, KECCAK complements the existing SHA-2 family of hash algorithms well. NIST remains confident in the security of SHA-2 which is now widely implemented, and the SHA-2 hash algorithms will continue to be used for the foreseeable future, as indicated in the NIST hash policy statement. One benefit that KECCAK offers as the SHA-3 winner is its difference in design and implementation properties from that of SHA-2. It seems very unlikely that a single new cryptanalytic attack or approach could threaten both algorithms. Similarly, the very different implementation properties of the two algorithms will allow future application and protocol designers greater flexibility in finding one of the two hash algorithms that fits well with their requirements.

NIST thanks the many people in companies, universities, laboratories and organizations around the world that participated in and contributed to the SHA-3 competition, especially the submitters of all the candidate algorithms, and the many others who contributed expert cryptanalysis, and performance studies. NIST could not have done the competition without them.

A detailed report of the final round of the competition will be published in the near future. Information about the SHA-3 competition is available at: www.nist.gov/hash-competition.