Le NIST vient de désigner KECCAK comme gagnant de la compétition destinée à définir la nouvelle classe de primitives de hachage SHA-3.

"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 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."

L'introduction de la notion de "sponge function" est un apport important.