Keccak

Guido Bertoni[1], Joan Daemen[1], Michaël Peeters[2], and Gilles Van Assche[1]

[1] STMicroelectronics
[2] NXP Semiconductors

In October 2012, the American National Institute of Standards and Technology (NIST) announced the selection of Keccak as the winner of the SHA-3 Cryptographic Hash Algorithm Competition [10,11]. This concluded an open competition that was remarkable both for its magnitude and the involvement of the cryptographic community. Public review is of paramount importance to increase the confidence in the new standard and to favor its quick adoption. The SHA-3 competition explicitly took this into account by giving open access to the candidate algorithms and everyone in the cryptographic community could try to break them, compare their performance, or simply give comments.

While preparing for the SHA-3 competition, we developed and presented the *sponge construction* [1]. Our initial goal of this effort was to solve the problem of compactly expressing a comprehensive security claim. It turned out to be a powerful tool for building a hash function and we adopted it for our SHA-3 candidate Keccak. Additionally, with its variable output length it can be used as a mask generating function, a stream cipher or a MAC computation function. To support more sophisticated modes such as single-pass authenticated encryption and reseedable pseudorandom sequence generation, we additionally introduced the *duplex construction* [3]. We have proven both sponge and duplex constructions sound in the indifferentiability framework [8,2,3]. Our permutation-based modes can be seen as an alternative to the block-cipher based modes that have dominated mainstream symmetric cryptography in the last decades. They are simpler than the traditional block cipher modes and offer at the same time more flexibility by allowing to trade in security strength level for speed and vice versa.

At the core of Keccak is a set of seven permutations called Keccak-$f[b]$, with width b chosen between 25 and 1600 by multiplicative steps of 2 [4]. Depending on b, the resulting function ranges from a toy cipher to a wide function. The instances proposed for SHA-3 use exclusively Keccak-$f[1600]$ for all security levels [5], whereas lightweight alternatives can use for instance Keccak-$f[200]$ or Keccak-$f[400]$, leaving Keccak-$f[800]$ as an intermediate choice [6]. Inside Keccak-f, the state to process is organized in 5×5 *lanes* of $b/25$ bits each, or alternatively as $b/25$ *slices* of 25 bits each. The round function processes the state using a non-linear layer of algebraic degree two (χ), a linear mixing layer (θ), inter- and intra-slice dispersion steps (ρ, π) and the addition of round constants (ι). The choice of operations in Keccak-f makes it very different from the SHA-2 family or even Rijndael (AES) [9,7]. On the implementation side, these operations are efficiently translated into bitwise Boolean operations and circular shifts, they lead to short critical paths in hardware implementations and they are well suited for protections against side-channel attacks.

References

1. G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, *Sponge functions*, Ecrypt Hash Workshop 2007, May 2007, also available as public comment to NIST from `http://www.csrc.nist.gov/pki/HashWorkshop/Public_Comments/2007_May.html`.
2. _____, *On the indifferentiability of the sponge construction*, Advances in Cryptology – Eurocrypt 2008 (N. P. Smart, ed.), Lecture Notes in Computer Science, vol. 4965, Springer, 2008, `http://sponge.noekeon.org/`, pp. 181–197.
3. _____, *Duplexing the sponge: single-pass authenticated encryption and other applications*, Selected Areas in Cryptography (SAC), 2011.
4. _____, *The* Keccak *reference*, January 2011, `http://keccak.noekeon.org/`.
5. _____, *The* Keccak *SHA-3 submission*, January 2011, `http://keccak.noekeon.org/`.
6. G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, and R. Van Keer, Keccak *implementation overview*, May 2012, `http://keccak.noekeon.org/`.
7. J. Daemen and V. Rijmen, *The design of Rijndael — AES, the advanced encryption standard*, Springer-Verlag, 2002.
8. U. Maurer, R. Renner, and C. Holenstein, *Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology*, Theory of Cryptography - TCC 2004 (M. Naor, ed.), Lecture Notes in Computer Science, no. 2951, Springer-Verlag, 2004, pp. 21–39.
9. NIST, *Federal information processing standard 180-2, secure hash standard*, August 2002.
10. _____, *NIST selects winner of secure hash algorithm (SHA-3) competition*, October 2012, `http://www.nist.gov/itl/csd/sha-100212.cfm`.
11. _____, *Third-round report of the SHA-3 cryptographic hash algorithm competition*, November 2012, `http://dx.doi.org/10.6028/NIST.IR.7896`.