Changes in the KECCAK submission package since the round 1 submission

Guido BERTONI[1], Joan DAEMEN[1], Michaël PEETERS[2] and Gilles VAN ASSCHE[1]
[1]STMicroelectronics
[2]NXP Semiconductors

http://keccak.noekeon.org/

September 10, 2009

The changes in the KECCAK submission package since the round 1 submission consist of a change of parameter values, improvements in optimized implementations and additional analysis results.

The changes in the parameter values are the following:

- The number of rounds of KECCAK-f has changed from $12 + \ell$ to $12 + 2\ell$ (from 18 to 24 rounds for KECCAK-f[1600]).
- The capacity and bitrate of the four fixed-output-length candidates has been changed. Now for each of them the capacity is equal to twice the output length.

The content and structure of the KECCAK submission package is described in the file README in the top-level folder. The changes in the package can be summarized as:

- Changes in the specifications, listed in Section 6 of Keccak-specifications-2.pdf.
- Changes in the main document, listed in Appendix A of Keccak-main-2.0.pdf.
- Changes in the reference implementation reflecting the new parameter values.
- Update of the KAT and MCT according to the new parameter values.
- Improvements in optimized implementations, both in software and in hardware (see Keccak-main-2.0.pdf for more details).