# Changes in the KECCAK submission package since the round 2 submission

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

http://keccak.noekeon.org/

January 10, 2011

The changes in the submission package since the round 2 submission consists mainly of changing the padding rule of KECCAK. Test vectors and implementations have been updated accordingly. Improvements in optimized implementations and additional analysis results can also be found.

The changes to KECCAK are the following.

- The padding rule has been shortened and simplified. The new padding rule is the pad10*1 rule.
- The diversifier parameter $d$ has been removed.
- The restriction on the supported values of $r$ has been removed. Previously, the bitrate $r$ could only take values that are multiple of 8 bits. Now all the values $0 < r \leq b$ are supported.

Note that no changes to KECCAK-$f$ have been made.