Subject: OFFICIAL COMMENT: Keccak From: Joan DAEMEN <joan.daemen@st.com> Date: Fri, 23 Jan 2009 15:13:30 +0100 To: <hash-function@nist.gov> CC: <hash-forum@nist.gov>

Dear all,

Version 1.1 of the main document and of the implementation are available from the Keccak web page http:://keccak.noekeon.org/

This version includes:

\* Additional usage modes on top of Keccak, including the possibility to do tree and parallel hashing;
\* Improved optimized software implementations, using new techniques to reduce the number of NOT instructions and to use only 32-bit rotations on 32-bit platforms;
\* New hardware implementations, with better performance and code suitable for FPGAs, considering the work published by Joachim Strömbergson.

A change log in the appendix of the main document brings you directly to the changed sections.

Note that the Keccak algorithm, specifications and test vectors have not changed since the initial NIST submission.

Kind regards, Guido, Joan, Michaël and Gilles The Keccak Team - http://keccak.noekeon.org Subject: OFFICIAL COMMENT: Keccak (from Joan DAEMEN) From: Shu-jen Chang <shu-jen.chang@nist.gov> Date: Mon, 26 Jan 2009 12:39:35 -0500 To: Multiple recipients of list <hash-forum@nist.gov>

X-Sieve: CMU Sieve 2.3 From: Joan DAEMEN <joan.daemen@st.com> To: <hash-function@nist.gov> Cc: <hash-forum@nist.gov> Subject: OFFICIAL COMMENT: Keccak Date: Fri, 23 Jan 2009 15:13:30 +0100 X-Mailer: Microsoft Office Outlook 11 Thread-Index: Acl9ZMAFLG2k7bYvScapaqdf5H25Hg== X-Proofpoint-Virus-Version: vendor=fsecure engine=1.12.7400:2.4.4,1.2.40,4.0.166 definitions=2009-01-23\_04:2009-01-21,2009-01-23,2009-01-23 signatures=0 X-PP-SpamDetails: rule=spampolicy2\_notspam policy=spampolicy2 score=0 spamscore=0 ipscore=0 phishscore=2 bulkscore=0 adultscore=0 classifier=spam adjust=0 reason=mlx engine=5.0.0-0811170000 definitions=main-0901230075 X-PP-SpamScore: 0 X-NIST-MailScanner: Found to be clean X-NIST-MailScanner-From: joan.daemen@st.com X-NIST-MailScanner-Information:

Dear all,

Version 1.1 of the main document and of the implementation are available from the Keccak web page http:://keccak.noekeon.org/

This version includes:

\* Additional usage modes on top of Keccak, including the possibility to do tree and parallel hashing;

\* Improved optimized software implementations, using new techniques to reduce the number of NOT instructions and to use only 32-bit rotations on 32-bit platforms; \* New hardware implementations, with better performance and code suitable for FPGAs, considering the work published by Joachim Strömbergson.

A change log in the appendix of the main document brings you directly to the changed sections.

Note that the Keccak algorithm, specifications and test vectors have not changed since the initial NIST submission.

Kind regards, Guido, Joan, Michaël and Gilles The Keccak Team - http://keccak.noekeon.org