

**Subject:** OFFICIAL COMMENT: MCSSHA-3  
**From:** "Mikhail Maslennikov" <mikhail@nets.co.kr>  
**Date:** Tue, 16 Dec 2008 14:20:37 +0900  
**To:** <hash-function@nist.gov>  
**CC:** <hash-forum@nist.gov>

Hi,  
A new optimized C version of MCSSHA hash function (MCSSHA-4) can be downloaded from:  
[http://registercsp.nets.co.kr/hash\\_competition.htm](http://registercsp.nets.co.kr/hash_competition.htm)

There are also test program with source codes for speed and some other tests.

Regards,  
Mikhail Maslennikov

---

**From:** hash-forum@nist.gov on behalf of Jean-Philippe Aumasson  
[jeanphilippe.aumasson@gmail.com]  
**Sent:** Thursday, June 04, 2009 7:31 AM  
**To:** Multiple recipients of list  
**Subject:** OFFICIAL COMMENT: MCSSHA-3

We found shortcut second-preimage attacks for MCSSHA-3, and for its tweaked versions MCSSHA-4 and MCSSHA-5. We also found a preimage attack that works only for MCSSHA-4.

The URL below links to a description of these attacks:  
<http://131002.net/data/papers/AN09.pdf>

---

**From:** Mikhail Maslennikov [mikhail@nets.co.kr]  
**Sent:** Monday, June 08, 2009 9:18 PM  
**To:** hash-function@nist.gov  
**Subject:** OFFICIAL COMMENT: MCSSHA-3

Dear all,

A new optimized C version of MCSSHA hash function (MCSSHA-6) can be downloaded from:

[http://registercsp.nets.co.kr/hash\\_competition.htm](http://registercsp.nets.co.kr/hash_competition.htm)

There are also change list and supporting documentation.

Regards,  
Mikhail Maslennikov