No Tweak of JH for Round 2

September 15, 2009

Hongjun Wu

Institute for Infocomm Research, Singapore
wuhongjun@gmail.com

1. There is no tweak of JH algorithms for Round 2.

2. There is no update of codes and test vectors of JH for Round 2.

3. The JH document is updated to include more security analysis and introducation material. About 10 pages are added to the JH document.

4. The code error and typos in the original JH submission (October 31, 2008) were corrected by January 15, 2009, as listed in the document "jh_changelist.pdf" (it was submitted to NIST on January 15, 2009).