

Statement by the Submitter

I, Dai Watanabe do hereby declare that, to the best of my knowledge, the practice of the algorithm, reference implementation, and optimized implementations that I have submitted, known as Luffa, may be covered by the following U.S. and/or foreign patents:

“Apparatus for generating hash values,” Japanese patent application number: P2008-213466, 22/08/2008.

I do hereby declare that the following pending patent applications may cover the practice of my submitted algorithm, reference implementation or optimized implementations:

“Apparatus for generating hash values,” Japanese patent application number: P2008-213466, 22/08/2008.

I do hereby understand that my submitted algorithm may not be selected for inclusion in the Secure Hash Standard. I also understand and agree that after the close of the submission period, my submission may not be withdrawn from public consideration for SHA-3. I further understand that I will not receive financial compensation from the U.S. Government for my submission. I certify that, to the best of my knowledge, I have fully disclosed all patents and patent applications relating to my algorithm. I also understand that the U.S. Government may, during the course of the lifetime of the SHS or during the FIPS public review process, modify the algorithm’s specifications (e.g., to protect against a newly discovered vulnerability). Should my submission be selected for SHA-3, I hereby agree not to place any restrictions on the use of the algorithm, intending it to be available on a worldwide, non-exclusive, royalty-free basis.

I do hereby agree to provide the statements required by Sections 2.D.2 and 2.D.3, below, for any patent or patent application identified to cover the practice of my algorithm, reference implementation or optimized implementations and the right to use such implementations for the purposes of the SHA-3 evaluation process.

I understand that NIST will announce the selected algorithm(s) and proceed to publish the draft FIPS for public comment. If my algorithm (or the derived algorithm) is not selected for SHA-3 (including those that are not selected for the second round of public evaluation), I understand that all rights, including use rights of the reference and optimized implementations, revert back to the submitter (and other owner[s], as appropriate). Additionally, should the U.S. Government not select my algorithm for SHA-3 at the time NIST ends the competition, all rights revert to the submitter (and other owner[s] as appropriate).

Signed: 

Title

Dated: 29/10/2008

Place: Leuven

Statement by Patent (and Patent Application) Owner(s)

If there are any patents (or patent applications) identified by the submitter, including those held by the submitter, the following statement must be signed by each and every owner of the patent and patent applications above identified.

I, Dai Watanabe, of 1099, Ozenji, Asao-ku, Kawasaki-shi, Kanagawa-ken, 215-0013 Japan, am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and or patent application(s): An apparatus for generating hash values, Japanese patent application number: P2008-23466, 22/08/2008, and do hereby agree to grant to any interested party if the algorithm known as Luffa is selected for SHA-3, an irrevocable nonexclusive royalty-free license to practice the referenced algorithm, reference implementation or the optimized implementations. Furthermore, I agree to grant the same rights in any other patent application or patent granted to me or my company that may be necessary for the practice of the referenced algorithm, reference implementation, or the optimized implementations.

Signed: 

Title:

Dated: 14/08/2008

Place: Paris

Statement by Patent (and Patent Application) Owner(s)

If there are any patents (or patent applications) identified by the submitter, including those held by the submitter, the following statement must be signed by each and every owner of the patent and patent applications above identified.

I, Hisayoshi Sato, of 1099, Ozenji, Asao-ku, Kawasaki-shi, Kanagawa-ken, 215-0013 Japan, am the owner or authorized representative of the owner (print full name, if different than the signer) of the following patent(s) and or patent application(s): An apparatus for generating hash values, Japanese patent application number P2008-213466, 22/08/2008, and do hereby agree to grant to any interested party if the algorithm known as Luffa is selected for SHA-3, an irrevocable nonexclusive royalty-free license to practice the referenced algorithm, reference implementation or the optimized implementations. Furthermore, I agree to grant the same rights in any other patent application or patent granted to me or my company that may be necessary for the practice of the referenced algorithm, reference implementation, or the optimized implementations.

Signed: *Hisayoshi Sato*

Title:

Dated: *14/08/2008*

Place: *Paris*

Statement by Reference/Optimized Implementations' Owner(s)

The following must also be included:

I, Dai Watanabe , am the owner of the submitted reference implementation and optimized implementations and hereby grant the U.S. Government and any interested party the right to use such implementations for the purposes of the SHA-3 evaluation process, notwithstanding that the implementations may be copyrighted.

Signed: 渡邊 大

Title:

Dated: 14/08/2008

Place: Paris