The Difference betweeen the Round 1 Package and the Round 2 Package of *Luffa*

This document shows the difference between the Round 1 package and the Round 2 package in abstract level. There are two significant differences: One is the modification of the algorithm and updates of the documents accompanied by the modification. The other is the additional implementation which is used to evaluate the performances of *Luffa*.

Num.	Directory	File	Change
1	\Supporting_Documentation	Luffa_Specification.pdf	Finalization (Sec.3.3) and SubCrumb (Sec.4.2) are modified. Appendix C and D are also updated due to these changes of the specification. Please refer to [4] for the reasons of the changes of the specification.
2	\Supporting_Documentation	Luffa_SupportingDocument.pdf	The basic properties of Sbox (Sec.3.1.1) and the implementation aspects (Sec. 6) are modified due to the changes of the specification. The security against the higher order differential attack (Sec. 3.4) and the importance of the (semi)-free-start setting are newly put in contents.
3	\Supporting_Documentation	Reason4Mod.pdf	Newly added document which explains which part of the algorithm is changed and the reason of the change.
4	\Supporting_Documentation	HigherOrderDifferentialAttack OnLuffa_v1.pdf	Newly added document which presents the attack on the step-reduced variants of the algorithm submitted to Round 1.
5	\Supporting_Documentation	Round2Mod.pdf	This file. Newly added document for the list of the changes in the package.
6	\Reference Implementation	luffa.c luffa.h	They are modified due to these changes of the specification.
7	\KAT_MCT	All files	They are modified due to these changes of the specification.
8	\Optimized_32 bit	luffa_for_32.c luffa_for_32.h	They are modified due to these changes of the specification.
9	\Optimized_64 bit	luffa_for_64.c luffa_for_64.h	They are modified due to these changes of the specification.
10	\Additional_Implementations\SSE2	All files	Newly added directory which includes an optimized C code using Visual C++ SSE intrinsics.
11	\	README	It is modified due to all the updates of the files above.