Errata for the submission package of *Luffa*

This document specifies the errors of the documents in the submission package of *Luffa* and their corrections. These errors are corrected in the updated document [2]. We classify errors into three types: A *technical error* is the most serious error, it may have influence on the specification itself or the security evaluation results, and so on. An *editorial error* includes typos and grammatical mistakes. Not technical nor editorial error is labeled *miscellaneous*. In the following table, The types of errors are denoted by **Te**, **Ed**, and **Mi** respectively. We add the reason of correction to clarify that they are not forbidden (nor undesirable) updates.

Num.	Position	Type	Error	Correction	Reason of correction
1	[1] Section 2.1.1, Line 18	**Ed**	Q_j The permutation dealing with…	Q_j: The permutation dealing with…	Lack of a colon.
2	[1] Section 3, Line 6	**Ed**	The starting variables… are given in Appendix A	The starting variables… are given in Appendix A.	Lack of a period.
3	[1] Section 4.1, Pseudo-code, Line 4, 5	**Ed**	`SubCrumb(a[0],a[1],[2],a[3]);` `SubCrumb(a[4],a[5],[6],a[7]);`	`SubCrumb(a[0],a[1],a[2],a[3]);` `SubCrumb(a[4],a[5],a[6],a[7]);`	Lack of the variables `a`.
4	[1] Section 4.1, Pseudo-code, Line 7	**Ed**	`MixColumn`	`MixWord`	Typo of the function name.
5	[1] Appendix D-1	**Mi**	Intel 686	Intel Core2	Intel 686 architecture has only two ALUs (Arithmetic Logic Units).

Related documents:

[1] Hash Function Luffa Specification, Christophe De Canniere, Hisayoshi Sato, Dai Watanabe, in the submission package, 31 October 2008.
[2] Hash Function Luffa Specification Ver. 1.0.1, Christophe De Canniere, Hisayoshi Sato, Dai Watanabe, 15 January 2009.

15 January 2009
Dai Watanabe