Errata for the submission package of *Luffa*

This document specifies the errors of the specification document of *Luffa* [1] 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 3.3, Line 7	**Te**	$Z_i = \bigoplus_{j=0}^{w-1} H_j^{(N+i')}$, where $i'=i$ if $N=1$ and $i'=i+1$ otherwise.	$Z_i = \bigoplus_{j=0}^{w-1} H_j^{(N+i+1)}$.	The description has not been updated according to the change of the specification as explained in [3].

Related documents:

[1] Hash Function Luffa Specification Ver. 2.0, Christophe De Canniere, Hisayoshi Sato, Dai Watanabe, 15 September 2009.
[2] Hash Function Luffa Specification Ver. 2.0.1, Christophe De Canniere, Hisayoshi Sato, Dai Watanabe, 2 October 2009.
[3] The Reasons for The Change of Luffa, Christophe De Canniere, Hisayoshi Sato, Dai Watanabe, 15 September 2009.

2 October 2009
Dai Watanabe