Errata for the submission package of *Luffa*

This document specifies the error of the reference and optimized implementations in the submission package of *Luffa* and the correction. The error is corrected in the updated implementations [4] [5] [6]. We add the reason of correction to clarify that they are not forbidden (nor undesirable) updates.

1. Updated implementations in the package

Types	File name	Version for updated source codes
Reference	luffa.h, luffa.c	1.1
Optimized 32-bit	luffa_for_32.h, luffa_for_32.c	1.1
Optimized 64-bit	luffa_for_64.h, luffa_for_64.c	1.1

2. Errata for the package

Num.	File name	Error	Correction	Reason of correction
1	[1] luffa.h	Datalength	DataLength	The data definition is different from the cryptographic API specified by NIST.
	[1] luffa.c			
	[2] luffa_for_32.h			
	[2] luffa_for_32.c			
	[3] luffa_for_64.h			
	[3] luffa_for_64.c			

Related codes:

[1] Reference implementation (luffa.h, luffa.c), in the submission package, 31 October 2008.
[2] Optimized 32-bit implementation (luffa_for_32.h, luffa_for_32.c), in the submission package, 31 October 2008.
[3] Optimized 64-bit implementation (luffa_for_64.h, luffa_for_64.c), in the submission package, 31 October 2008.
[4] Reference implementation version 1.1 (luffa.h, luffa.c), in the submitter's website, 12 February 2009.
[5] Optimized 32-bit implementation version 1.1 (luffa_for_32.h, luffa_for_32.c), in the submitter's website, 12 February 2009.
[6] Optimized 64-bit implementation version 1.1 (luffa_for_64.h, luffa_for_64.c), in the submitter's website, 12 February 2009.

12 February 2009
Dai Watanabe