

## Errata for the submission package of *Lesamnta*

This document specifies the errors of the documents in the submission package of *Lesamnta* 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 1, Annotation 1	<b>Ed</b>	Lesamnta is pronounced like "Lezanta"	Lesamnta is pronounced like "Lezanta".	Typo of a quotation, and lack of a period.
2	[1] Section 5.3.2.2, Line 2	<b>Ed</b>	cyclically shifted over different numbers of bytes (offsets).	cyclically shifted over one byte (offset).	Change the plural form of the sentence to the simple form.
3	[1] Section 5.3.2.2, Line 4	<b>Ed</b>	$S'_{1,c} = S_{1,(c+1) \bmod 4}$ , for $0 \leq c < 4$ .	$s'_{1,c} = s_{1,(c+1) \bmod 4}$ , for $0 \leq c < 4$ .	Typo of symbols " $\mathcal{S}$ ".
4	[1] Section 5.5.2.2, Line 4	<b>Ed</b>	$S'_{r,c} = S_{r,(c+r) \bmod 4}$ , for $0 < r < 4$ and $0 \leq c < 4$ ,	$s'_{r,c} = s_{r,(c+r) \bmod 4}$ , for $0 < r < 4$ and $0 \leq c < 4$ .	Typo of symbols " $\mathcal{S}$ ", and the last comma should be a period.
5	[1] Section 5.7.2, Page 41	<b>Ed</b>	$H_0^{(0)} \dots = 3e7fee25cf51d123$ ... $H_7^{(0)} \dots = 08cd3bb067a2b546$	$H_0^{(1)} \dots = 3e7fee25cf51d123$ , ... , $H_7^{(1)} \dots = 08cd3bb067a2b546$ .	Typo of round numbers of $H$ , and lack of commas and a period.
6	[1] All	<b>Ed</b>	-	Enabled hyperlinks reference.	Improve usability of the document of the proposal.

### Related documents:

- [1] SHA-3 Proposal: Lesamnta Ver 1.0, Shoichi Hirose, Hidenori Kuwakado, Hirotaka Yoshida, in the submission package, 30 October 2008.
- [2] SHA-3 Proposal: Lesamnta Ver 1.0.1, Shoichi Hirose, Hidenori Kuwakado, Hirotaka Yoshida, 15 January 2009.

15 January 2009  
Hirotaka Yoshida