

[MB¹] comments on ISO/IEC 3rd CD 19772

Date: 2007-08-16	Document: SC27 N5820
------------------	-----------------------------

1	2	(3)	4	5	(6)	(7)
NB ¹	Clause No./ Subclause No./ Annex (e.g. 3.1)	Paragraph/ Figure/Table/ Note (e.g. Table 1)	Type of comment ²	Comment (justification for change) by the NB	Proposed change by the NB	Resolution on each comment
[MB] 1.	11.2	last item	te	To be consistent with McGrew and Viega's specification of GCM, and their test vectors, the "little-endian" convention for interpreting a block as a polynomial needs to be specified.	Insert a sentence like, "Blocks are interpreted elements in GF(2 ¹²⁸) under the "little endian" convention (so that the leftmost bit of the block becomes the constant term of its polynomial representation.	
[MB] 2.	11.3	last	ed	Typographical error.	Replace "n=12 8" with "n=128."	
[MB] 3.	11.4	EDITOR'S NOTE	te	The proposed change responds to the editor's request. Any equivalent revision should be acceptable.	Replace the EDITOR'S NOTE with "When W is empty, then k=0, and Steps b) and c) should be omitted. When k=1, Step b) should be omitted. Similarly, when Z is empty, Steps d) and e) should be omitted, and when l=1, Step d) should be omitted."	
	A.2`	Table 1	ge	Mechanism 6 can be expected to perform significantly better than the other mechanisms in hardware.	Indicate either in the table or in a note that Mechanism 6 is suitable for high-throughput hardware implementations because it can be implemented without pipeline stalls.	
	A.8	n/a	ge	The requirement that IVs never repeat for a given key is crucial to the security of GCM.	Indicate that the requirement that IVs never repeat for a given key is crucial to the security of GCM.	
	A.8	Par 2	te	McGrew and Viega's specification actually allows len(IV) to range from 1 to 2 ⁶⁴ . It's not clear whether the text here is a typo, missing the '2.' If a restriction is intended, 64 is too small; there are implementations with IVs of 128 bits or greater.	Replace "64" with either 2 ⁶⁴ or 1024	

1 **MB** = Member body (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)

2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial

NOTE Columns 1, 2, 4, 5 are compulsory.