Code Updates

File	What	Reason	Effect on the Specification
hamsi-exp.c	Updated the table: Const Word T512[8][256][16]	We corrected an error in the construction of the linear code used for the message expansion of Hamsi-512 (and Hamsi-384 resp.).	Yes:This correction is due to a correction in the specification, the linear code is the same but the construction is corrected.
words.h	removed the line:"typedef unsigned int Row_attribute_((vector_size(16)));//128 bits"	it is not used anywhere	No
i.hamsi-ref.c	"#define Exp512(i) (T5(0)^T5(1)^T5(2)^T5(3))" is changed to "#define Exp512(i) (T5(0)^T5(1)^T5(2)^T5(3)^T5(4)^T5(5)^T5(6)^T5(7))"	corrected a bug	No

nist-wrapper.c	"// copy
	int already=(state->leftbits/8);
	for (i=already; i < s_blocksize; ++i) state->leftdata[i]=block[i-already];" is added.
		corrected a bug	No

nist-wrapper.c	"U64 length = ((U64)(state->cvsize)*state->counter)+state->leftbits;" is changed to "U64 length = ((U64)(state->cvsize/8)*state->counter)+state->leftbits;"	corrected a bug	No

Spec. Updates

Chapter	Where	What	Reason	Effect on the ref. code
1	Introduction	changed	update	No
2.2.4	4th paragraph	GF(4) changed to F_4	To be consistent with the terminology	No
2.2.4	4th paragraph	Magma changed to Magma (6)	citation to magma is added	No
2.2.4	4th paragraph 1st sentence	The sentence "The generator matrices of the codes used in Hamsi are given in Appendix" is removed.	We provide the construction method.	No
2.2.4	Construction of the linear code [256,32,131]	we updated the construction	there was a bug	yes
2.2.4	Construction of the linear code [128,16,70]	we provide the construction method instead of generator matrix	update	No
Appendix	Appendix	Removed the generator matrices of the linear codes	Include the construction method of the linear codes	No
2.3.1	2.3.1	\alpha_{2} is changed to s_{2}	correct an error	No
Chapter 2	Table 2.4	ordering of constants	correct an error	No
2.6	Second paragraph	we added new variants	update the parameters	No

3	all	removed	We will provide a supporting documentation in hamsi website	
Sub. Package Changes				
Folder	**What**	**Changes**		
\Reference_Implementation	hamsi-exp.c, words.h, i.hamsi-ref.c, nist-wrapper.c We also removed the files ShortMsgKAT.txt, MonteCarlo.txt, LongMsgKAT.txt, ExtremelyLongMsgKAT.txt	see Code Updates		
\KAT_MCT	new test values			
\Optimized_32bit	addition of optimized implementation			
\Supporting_Documentation	HamsiSpec13Jan.pdf	updated with the document Hamsi_Spec_2ndRound.pdf (see Spec. Updates)		
\Supporting_Documentation	Hamsi_IPS1.pdf	renamed as Cover_Sheet.pdf		
\Supporting_Documentation	Hamsi_IPS4.pdf	IP statement of the owner of the ref/opti. implementation is added		
\Supporting_Documentation	Round2Mod.pdf	is included		
\Supporting_Documentation	HamsiCodeChanges.pdf	removed		
\Supporting_Documentation	HamsiDocChanges.pdf	removed		