| id | Description | Reason | Function | File |
|---|---|---|---|---|
| | Changes introduced to the code are described below. None of them requires a design fix. In only one case, a simple ambiguity fix in the design caused some code change (item 6). All the rest is refactoring or debugging. | | | |
| | | | | |
| 1 | changes in filenames | Refactoring (A better naming convention applied, giving way to multiple implementations of Hamsi) | hamsi.c -> i.hamsi-ref.c hamnist.c -> nist-wrapper.c | |
| 2 | hamsi-tables.c split into hamsi-tables.c and hamsi-exp.c | Refactoring (hamsi-exp.c is generated by code) | | |
| 3 | Made the State matrix two dimentional | For simplicity and clarity of reference code | | i.hamsi-ref.c |
| 4 | Tables are changed | For consistency in endianness, the table is BIG Endian now | T256, T512 | hamsi-tables.c |
| 5 | a256 and a512 are converted into a single array: alpha | For simplicity and clarity of reference code | hash256, hash512 | i.hamsi-ref.c |
| 6 | an error is fixed in the final truncation of hash256 | see fix 5 in the document | hash256 | i.hamsi-ref.c |
| 7 | Extra application of L which is erronously forgotten in the reference code is removed, which makes it consistent with the design document | Debugging | diffuse512 | i.hamsi-ref.c |
| 8 | L was defined incompletely, missing two final instructions that were in the design | Debugging | L | i.hamsi-ref.c |
| 9 | in the final rounds, the length of the message is padded into the message. In the old code, this was little-endian. We now changed it to BIG endian. | For consistency in endianness, and compliance with the design document | Final | nist-wrapper.c |
| 10 | A bug is corrected, that caused the last block to be unprocessed in some circumstances | Debugging | Final | nist-wrapper.c |