Fugue Errata Submitted Oct 14 2009

1. The .c files SHA3api_ref.c in each of the directories
   (a) Reference_Implementation
   (b) Optimized_32bit
   (c) Optimized_64bit
   (d) Additional_Implementations

   have been modified in line 62:

   ```
      memset ((uint8*)state->Partial+(((state->TotalBits&31)+7)/8), 0, need/8);
   replaces
      memset ((uint8*)state->Partial+((state->TotalBits&31)/8), 0, need/8);
   ```

2. The directory KAT_MCT has been updated, with all KAT files affected.
3. The Optimized 64 bit code has been further optimized.
4. The Optimized 32 bit code has also been further optimized.
5. A new SSE implementation has been given in the Additional Implementations Directory.
6. The document fugue_Oct14_09.pdf replaces fugue.pdf in Supporting_Documentation directory. The *only* change is in Section 5.3 on page 27, where the Fugue-224 IV had a typo. The fifth column of the IV now *correctly* reads `a1-12-7c-62`. The programs and the KATs had it correct all along.
7. The software speed table on page 33 has also been updated to reflect new optimized codes.