Round 2 Changes in Fugue Submission

1. There is absolutely **no change** in the Fugue specification.
2. The Fugue specification section in Fugue.pdf is unaltered.
3. There are a few changes to the rest of the Fugue.pdf document:
   - The introduction section has been spruced up with new figures.
   - A new subsection has been added in the Security Analysis section, which proves that Fugue is a Universal Hash Function under minimal assumptions (Section 12.5).
   - The software speed figures have been updated to reflect performance on Intel Core 2 processor (Section 6).
4. There is *no change* in the implementations. But, Makefiles for Windows named NMakefile have been added. We recommend using the Intel Compiler for Windows, which runs on top of Visual C++ or Visual Studio. The directory structure has also been brought in line with the recommended structure.