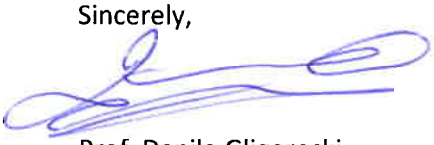
List of changes for this CD and documentation for Edon-R

1. Rotations defined in the documentations were different from the rotations used in the C code (both reference and optimized version). Now, the rotations used in the C code are the same as those defined in the documentation.
2. Accordingly, HMAC test vectors in the documentation are now changed to match the changes in the source code.
3. Accordingly, KAT_MCT and intermediate values in the CD are now changed to match the changes in the source code.
4. Re-measuring of the speed with Microsoft Visual Studio 2005 has been performed on the corrected C code. The measured speed has changed very little. But, additionally measurements performed with Intel C++ v 11.0.066 compiler are added in the documentation. That compiler gives faster speeds.
5. A remark in the beginning of the section 3.14 is added (that our claims for free-start collisions are not correct), but the rest of the section is the same as in the original documentation.
6. A typo mistake forgetting one of my collaborators and contributors for Edon-R is corrected: I added the name of Mr. Vlastimil Klima in the list of authors.

12 January 2009

Sincerely,



Prof. Danilo Gligoroski