RIPEMD-160 - Verification of a SPARK/ADA Implementation

Fabian Immler

February 23, 2021

Abstract

This work presents a verification of an implementation in SPARK/ADA [1] of the cryptographic hash-function RIPEMD-160. A functional specification of RIPEMD-160 [2] is given in Isabelle/HOL [3]. Proofs for the verification conditions generated by the static-analysis toolset of SPARK certify the functional correctness of the implementation. The verification conditions are translated to Isabelle/HOL with a modified version of Victor-0.8.0 [4].

This entry is now obsolete, it is contained as example in the Isabelle distibution.

1 RIPEMD-160-SPARK

theory *RIPEMD-160-SPARK*
imports
HOL−SPARK−Examples.F
HOL−SPARK−Examples.Hash
HOL−SPARK−Examples.K-L
HOL−SPARK−Examples.K-R
HOL−SPARK−Examples.R-L
HOL−SPARK−Examples.Round
HOL−SPARK−Examples.R-R
HOL−SPARK−Examples.S-L
HOL−SPARK−Examples.S-R
begin

This entry is empty, because the verification of *rmd* is now contained in the Isabelle distibution.

end

References

[1] J. Barnes. *High Integrity Software*. Addison-Wesley, 2006.

[2] B. P. H. Dobbertin, A. Bosselaers. Ripemd-160, a strengthened version of ripemd. In D. Gollmann, editor, *Fast Software Encryption*, number 1039 in LNCS, pages 71–82. Springer-Verlag, 1996. updated and corrected version: http://www.esat.kuleuven.ac.be/~cosicart/pdf/AB-9601/AB-9601.pdf.

[3] T. Nipkow, L. Paulson, and M. Wenzel. *Isabelle/HOL — A Proof Assistant for Higher-Order Logic*, volume 2283. 2002. http://www.in.tum.de/~nipkow/LNCS2283/.

[4] B. J. E. Paul B. Jackson and K. Sharp. Using smt solvers to verify high-integrity programs. In *2nd International Workshop on Automated Formal Methods*, AFM. ACM, November 2007. http://homepages.inf.ed.ac.uk/pbj/papers/afm07.pdf.