Salsa20 robustness statement

Daniel J. Bernstein *

Department of Mathematics, Statistics, and Computer Science (M/C 249)
The University of Illinois at Chicago
Chicago, IL 60607–7045
snuffle@box.cr.yp.to

The Salsa20 design is quite conservative, allowing more confidence in its security conjectures than in the analogous conjectures for some other functions. I have not inserted any weaknesses into Salsa20; I do not know any way that a function with a similar definition to Salsa20 could be weak.

* The author was supported by the National Science Foundation under grant CCR–9983950, and by the Alfred P. Sloan Foundation. Date of this document: 2005.04.27.