Salsa20 cover sheet

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

Name of submitted algorithm: Salsa20, also known as "Snuffle 2005"

Type of submitted algorithm: stream cipher; profile 1 (high performance)

Security goal: 256 bits of security using 256-bit keys (recommended);
128 bits of security using 128-bit keys

Anticipated environments: 32-bit processors;
64-bit processors;
8-bit processors;
hardware

Submitter: Daniel J. Bernstein,
Department of Mathematics, Statistics, and Computer Science,
University of Illinois at Chicago,
MC 249,
851 S. Morgan Street,
Chicago, IL 60607–7045,
USA;
312–413–9322, fax 312–996–1491;
snuffle@box.cr.yp.to

Auxiliary submitters: None

Author: Daniel J. Bernstein

---

* 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.