Cryptology ePrint Archive: Report 2011/646

The security impact of a new cryptographic library

Daniel J. Bernstein and Tanja Lange and Peter Schwabe

Abstract: This paper introduces a new cryptographic library, NaCl, and explains how the design and implementation of the library avoid various types of cryptographic disasters suffered by previous cryptographic libraries such as OpenSSL. Specifically, this paper analyzes the security impact of the following NaCl features: no data flow from secrets to load addresses; no data flow from secrets to branch conditions; no padding oracles; centralizing randomness; avoiding unnecessary randomness; extremely high speed; and cryptographic primitives chosen conservatively in light of the cryptanalytic literature.

Category / Keywords: implementation / confidentiality, integrity, simplicity, speed, security

Publication Info: expanded version of LatinCrypt 2012 paper

Date: received 1 Dec 2011, last revised 24 Jul 2012

Contact author: tanja at hyperelliptic org

Available formats: PDF | BibTeX Citation

Version: 20120725:055253 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]