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.

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

Date: received 1 Dec 2011

Contact author: tanja at hyperelliptic org