

libpqcrypto

PQCRYPTO consortium: See pqcrypto.eu.
22 PQCRYPTO submissions to NIST: 0 broken.
47 non-PQCRYPTO submissions: 16 broken.

New software library, libpqcrypto.org:
77 cryptographic systems (50 sig, 27 enc)
from 19 of the 22 PQCRYPTO submissions.

Unified compilation framework; stringent tests;
C API following NaCl/SUPERCOP/libsodium;
Python API; command-line tools; benchmarking.