The SUPERCOP API

Daniel J. Bernstein

13 August 2020

Executive summary: SUPERCOP is the primary benchmarking framework for cryptographic software, and the primary source of performance data for the NIST Post-Quantum Cryptography Standardization Project. SUPERCOP's API supports both pre-quantum and post-quantum cryptographic algorithms and is designed for robust production usage. The API is supported by several cryptographic libraries, including NaCl, TweetNaCl, libsodium, and libpqcrypto.

Details: SUPERCOP is an open benchmarking framework that (as of August 2020) measures 3664 implementations of 1240 different cryptographic functions in more than 300 different families. Measurements are collected on a wide range of CPUs and posted centrally at https://bench.cr.yp.to. For example, https://bench.cr.yp.to/results-sign.html shows the measured speeds and sizes of various pre-quantum and post-quantum signature systems, including all round-2 NISTPQC submissions. Round-3 NISTPQC submissions have been announced and are preparing software now.

On each CPU, for each cryptographic function, SUPERCOP automatically measures each implementation of that function with various compiler options and selects the fastest implementation that passes tests. Programmers can easily submit new optimized implementations to SUPERCOP without worrying about how to inspect the CPU and decide which implementation will be fastest: SUPERCOP collects the data automatically. Nearly 200 programmers have contributed implementations.

The SUPERCOP API is designed not just for benchmarking but also for production use of cryptography, with the details systematically designed to make correct use easy and incorrect use hard. For example, in most libraries, verifying a signature requires several steps for storage allocation, input conversions, the mathematical part of signature verification, storage deallocation, and error handling. Library users often make mistakes: mishandling verification errors, for example, or simply forgetting to verify a signature. In the SUPERCOP API, there is a simple all-in-one function to extract a verified message from a signed message. There are no extra steps to get wrong or forget: the inputs and outputs are in wire format, and the signature is not treated as a separate object that one can forget to verify. Some implementations supporting the API avoid all memory allocation and are suitable for use on embedded devices.

NIST cited SUPERCOP's hashing results ("eBASH") 30 times in its final report on the SHA-3 competition, and then required that submitters to the PQC and LWC competitions use the SUPERCOP API from the outset. Libraries supporting the API include https://nacl.cr.yp.to, https://tweetnacl.cr.yp.to, https://libsodium.org, and https://libpqcrypto.org.