From: David Jao <djao@math.uwaterloo.ca>
Sent: Wednesday, April 17, 2019 10:57 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: [pqc-forum] ROUND 2 OFFICIAL COMMENT: SIKE

To all concerned,

It has come to our attention that the 2nd round SIKE submission contains erroneous ARM64 performance benchmarks. The error is due to some (as yet
unfixed) bug in our time measurement code, which only manifests on some devices. The existence of the error has been confirmed by hand-timing with a stopwatch.

We have re-run the ARM64 performance benchmarks on an error-free device and posted the corrected results on our web site at https://sike.org/changes.html

A corrected copy of the entire submission package is also available for download from our web site at https://sike.org/

Generally speaking, our original (erroneous) performance numbers were 30-40% faster than reality on ARM64 for the optimized (portable) implementation, and 300-400% faster than reality for the ARM64 assembly optimized implementation.

Apologies to all for the mistake. I would be happy to discuss further with anyone who has questions. As far as I know, there are no errors in our other performance benchmarks other than ARM64.

On behalf of the SIKE team,

-David

--