From: Joost Rijneveld <joost@joostrijneveld.nl>
Sent: Tuesday, March 13, 2018 10:03 AM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: SPHINCS+

Dear all,

It was brought to our attention that the SPHINCS+ reference code contains an error that causes a longer-than-necessary message digest to be generated and signed (contradicting the specification). We have fixed the code and updated it on our web page. Note that, as this also affects the leaf index selection, the fix causes incompatibility with the previous version of the code.

Thanks go to Dorian Amiet for spotting the bug and alerting us to it.

Cheers,
Joost Rijneveld, on behalf of the SPHINCS+ team