From: Andreas Hülsing <andreas@huelsing.net>
To: pqc-comments@nist.gov
CC: pqc-forum@list.nist.gov
Subject: ROUND 3 OFFICIAL COMMENT: SPHINCS+
Date: Friday, June 10, 2022 03:49:42 AM ET
Attachments: sphincs_-r3.1-specification.pdf
r3.1_modifications.pdf

Dear all,

In response to the recently posted issue with the SHA2 instantiation of SPHINCS+, we decided to change the function we use in the concerned implementations from SHA2-256 to SHA2-512. The problem was caused by the small internal state of SHA2. With this change, this problem is solved.

We updated our specification, also including other changes that we announced on this list since the 3rd round submission. In the attachment you also find a list of all the modifications we made. The code in our public github repository (https://github.com/sphincs/sphincsplus) is also updated.

Best wishes,

Andreas