From: Sydney Antonov <ska84@protonmail.com> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum@list.nist.gov
Subject: [pqc-forum] Re: Changes to SPHINCS+ specification to prevent multi-user attacks
Date: Monday, April 18, 2022 03:26:40 PM ET

> 2.) We change the initialization value of OptRand from the all zero
> string to PK.seed. This ensures that also PRF_msg takes a unique, user
> dependent input or a random value.

I find this a bit concerning because OptRand might not be unique among multiple users signing with bad randomness.

I'd instead suggest

PRF_msg(SK.prf, OptRand, M) = HMAC-SHA-256(PK.Seed || SK.prf, OptRand || M)

for SHA256,

PRF_msg(PK.Seed, SK.prf, OptRand, M) = SHAKE256(PK.seed || SK.prf || OptRand || M, 8n)

for SHAKE256 and making no change for Haraka:

PRF_msg(PK.seed, SK.prf, OptRand, M) = HarakaS_PK.seed(SK.prf || OptRand || M, 8n)

Sydney