

From: Sydney Antonov <ska84@protonmail.com> via pqc-forum <ppc-forum@list.nist.gov>
To: ppc-forum@list.nist.gov
Subject: [ppc-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

--

You received this message because you are subscribed to the Google Groups "ppc-forum"
group.

To unsubscribe from this group and stop receiving emails from it, send an email to
ppc-forum+unsubscribe@list.nist.gov.

To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/ppc-forum/ExKfcQZT0zc3HklytZQCxr8afQ2Jbe8s-7v_C4N8ziqNcC5gMf31-1gHM-wGc4GuvSqONJidQ86_IYU0j_7-UK94TUMSk82TwwkrRB8TMr0%3D%40protonmail.com.