**From:** Blumenthal, Uri - 0553 - MITLL <uri@ll.mit.edu> via pqc-forum@list.nist.gov
**To:** pqc-forum <pqc-forum@list.nist.gov>
**Subject:** Re: [pqc-forum] Request for feedback on possible SPHINCS+ variant
**Date:** Wednesday, November 30, 2022 11:06:29 AM ET
**Attachments:** smime.p7m

Given that the likely use case is signing firmware (and software?) updates and (maybe) Root CA certs – we should be OK with smaller-than-2^64 allowed number of faster/smaller signatures.

--

Regards,

Uri

*There are two ways to design a system. One is to make is so simple there are obviously no deficiencies.*

*The other is to make it so complex there are no obvious deficiencies.*

*- C. A. R. Hoare*

**From:** "'Moody, Dustin (Fed)' via pqc-forum"
**Reply-To:** Dustin Moody
**Date:** Wednesday, November 30, 2022 at 07:28
**To:** pqc-forum
**Subject:** [pqc-forum] Request for feedback on possible SPHINCS+ variant

All,

The design of SPHINCS+ imposes a limit on the number of allowable signatures from a given public key. For any number of signatures using the public key, g, there is some very low probability that they will reveal enough of the private key to allow an attacker to forge a signature. As g grows, so does the probability of this disaster. The total number of signatures must be kept low enough that this probability remains negligible. NIST’s Call for Proposals required the ability to securely perform 2^64 signatures, which imposes requirements on the parameters of SPHINCS+. A smaller maximum number of signatures would result in somewhat smaller and faster signatures.

> NIST asks for public feedback on whether such a version of SPHINCS+ would be beneficial.
>
> NIST PQC team
>
> --
> You received this message because you are subscribed to the Google Groups "pqc-forum" group.
> To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
> To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/SA1PR09MB8669CC55FD9EF5432F6B9C51E5159%40SA1PR09MB8669.namprd09.prod.outlook.com.

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/063A88E8-BBE9-4111-B481-6EF1323A919A%40ll.mit.edu.