

From: Doge Protocol <dogeprotocol1@gmail.com> via ppc-forum@list.nist.gov
To: ppc-forum <ppc-forum@list.nist.gov>
Subject: [ppc-forum] Will Sqisign be submitted for additional digital signature schemes?
Date: Saturday, January 21, 2023 04:12:07 PM ET

Dear Sqisign inventors:

Are you considering submitting Sqisign to "NIST call for Additional Digital Signature Schemes"?

Does SIKE being broken have any impact on this scheme? (isogeny based)

Characteristics of Sqisign appear to be attractive and in-line with expectations for the additional call (March 1 deadline). The signature and public key sizes are attractive for applications like blockchains (sign time is high though).

Signature: 204 bytes

Secret Keys: 16 bytes

Public Keys: 64 bytes

Performance:

The following are timings (medians) obtained running the benchmarks above on an Intel Core i7-6700 CPU @ 3.40GHz with Turbo Boost disabled.

<https://github.com/SQISign/sqisign>

Key Gen: 575ms

Sign: 2279ms

Verify: 42ms

Sqisign: compact post-quantum signatures from quaternions and isogenies

<https://eprint.iacr.org/2020/1240>

<https://csrc.nist.gov/Projects/ppc-dig-sig/standardization/call-for-proposals>

--

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/c593aab2-fcad-4045-9af6-d9643f5cc3f7n%40list.nist.gov>.