From: Doge Protocol <dogeprotocol1@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: [pqc-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/pqc-dig-sig/standardization/call-for-proposals

--