

**From:** michal.r.a...@gmail.com <[michal.r.andrzejczak@gmail.com](mailto:michal.r.andrzejczak@gmail.com)> via [pqc-forum@list.nist.gov](mailto:pqc-forum@list.nist.gov)  
**To:** pqc-forum <[pqc-forum@list.nist.gov](mailto:pqc-forum@list.nist.gov)>  
**Subject:** [pqc-forum] Request for Dilithium version selection  
**Date:** Saturday, January 14, 2023 05:22:16 PM ET

---

Dear Crystals Team,

Please clarify what version of Dilithium is currently correct:

- 1) published by NIST,
- 2) published on your official github page (<https://github.com/pq-crystals/dilithium>).

These two versions vary significantly (e.g. size of SK) and this situation is misleading.

If the NIST version is correct, could you update your github?

Kind regards,

Michal

--

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](mailto: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/335bb79a-53d3-4d3a-91eb-8a9e4c36a596n%40list.nist.gov>.