From:	建方 牛 <niux_dannyniu@icloud.com>
Sent:	Friday, November 19, 2021 1:10 AM
To:	pqc-comments
Cc:	pqc-forum
Subject:	ROUND 3 OFFICIAL COMMENT: FALCON

Hi NIST PQC Team, and participants.

I would like to express my desire for NIST to select BOTH Dilithium and Falcon for standardization.

Dilithium is a considerate design - it made best effort attempt at minimizing ciphergram sizes while ensuring correct implementations are relatively easy. I would like NIST consider choosing this scheme as the primary lattice-based digital signature scheme.

Falcon on the other hand is sophisticated - it made every attempt at minimizing ciphergram size, at the sacrifice of quite some simplicity. As noted in some presentations at the workshop, there are desire for NIST at least to include such a compact signature scheme, e.g. in automobile communication network, as bandwidth in such environments are a scarce resource.

I propose selecting all 3 primary parameters of Dilithium for general-purpose use, while approving Falcon for limited use, where side-channel protections are adequate, even if this means hardware components would be involved (e.g. approving Falcon with hardware Gaussian sampler or hardware-only implementations of Falcon as is the case with stateful hash-based signatures).

Regards, DannyNiu/NJF.

From:	Evan Kuhn <evkuhn1994@gmail.com>
Sent:	Saturday, April 2, 2022 8:51 PM
To:	pqc-comments
Cc:	pqc-forum
Subject:	ROUND 3 OFFICIAL COMMENT: FALCON

Hello,

I would like to bring to your attention a twitter post (https://twitter.com/bwesterb/status/1509583201848672258?cxt=HHwWhICykZH7jvMpAAAA) that states that there is "a constant-time issue with NIST post-quantum signature scheme Falcon on ARMv7… there is no native C-style double -> int64 cast. It depends on the runtime, but LLVM branches on the sign." The post links to the article https://eprint.iacr.org/2022/405. If this is correct, the issue should be fixed before implementation if Falcon is chosen.

Thank you for your time and consideration.
--
Sent from my iPhone