

From: Evan Kuhn <evkuhn1994@gmail.com>
To: pqc-comments@nist.gov
CC: pqc-forum@list.nist.gov
Subject: ROUND 3 OFFICIAL COMMENT: FALCON
Date: Saturday, April 02, 2022 08:51:35 PM ET

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