From: Andersen Cheng <ac@post-quantum.com>
Sent: Thursday, April 26, 2018 11:38 AM
To: Moody, Dustin (Fed)
Cc: pqc-forum@list.nist.gov
Subject: [pqc-forum] NTS-KEM

Dear Dustin and NIST colleagues,

As you know, NTS-KEM was an invention from PQ Solutions Limited and is subject to a patent.

We declared to NIST during the submission last year that we would be willing to grant a royalty free worldwide licence for use should it become adopted as standard.

Following a number of approaches from the crypto community wanting to collaborate with us now, we have decided to eliminate any uncertainty by abandoning the patent with immediate effect. Our submission will no longer be subject to any patents and is free for anyone to experiment with.

We are particularly excited that one entity is already going to perform a substantial test on the performance and resilience of NTS-KEM in the not too distant future. We will share the results when they become available.

Best regards,

Andersen

Andersen Cheng
CEO
PQ Solutions Limited(trading as Post-Quantum)
--

From: Martin Tomlinson <mt@post-quantum.com>
Sent: Wednesday, July 04, 2018 12:40 PM
To: pqc-comments
Cc: pqc-forum@list.nist.gov
Subject: OFFICIAL COMMENT: NTS-KEM
Attachments: signature.asc

Dear All,

Dan Bernstein has recently posted a comparison of NTS-KEM and Classic McEliece authored by the "Classic McEliece Comparison Task Force". We are currently analysing this comparison, and in due course we will post a detailed response.

Best wishes,

The NTS-KEM team