From:	Apon, Daniel C. (Fed)
To:	Robinson, Angela Y. (Fed); Alperin-Sheriff, Jacob (Fed); Perlner, Ray A. (Fed)
Subject:	Re: Dear D.B.A.,
Date:	Monday, December 10, 2018 4:29:44 PM

Ya, I originally advocated axing it because it was 2x worse bytes/cycles than similar lattice KEMs from Jacob's numbers
(It is very, very similar to other such lattice schemes -- as are they all, amen)
At the time, it was the "closest-to-margin cut" among the lattice KEMs -- I compared it with NTRU Prime in particular.

From: Robinson, Angela Y. (Fed)
Sent: Monday, December 10, 2018 4:27:16 PM
To: Apon, Daniel C. (Fed); Alperin-Sheriff, Jacob (Fed); Perlner, Ray (Fed)
Subject: RE: Dear D.B.A.,

Was LIMA only removed for inefficiency?

From: Apon, Daniel C. (Fed)
Sent: Monday, December 10, 2018 4:25 PM
To: Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: Dear D.B.A.,

My opinion on LIMA is really up to Jacob~

From: Robinson, Angela Y. (Fed)
Sent: Monday, December 10, 2018 4:21:36 PM
To: Apon, Daniel C. (Fed); Alperin-Sheriff, Jacob (Fed); Perlner, Ray (Fed)
Subject: RE: Dear D.B.A.,

I'm Switzerland.

From: Apon, Daniel C. (Fed)
Sent: Monday, December 10, 2018 4:21 PM
To: Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>
Subject: Re: Dear D.B.A.,

Don't Remove Alliance?

From: Alperin-Sheriff, Jacob (Fed)
Sent: Monday, December 10, 2018 4:20:31 PM
To: Apon, Daniel C. (Fed); Perlner, Ray (Fed); Robinson, Angela Y. (Fed)
Subject: Re: Dear D.B.A.,

Putting things back in is wholely contrary to the ethos of the DBA Daniel.

From: "Apon, Daniel C. (Fed)" <daniel.apon@nist.gov>
Date: Monday, December 10, 2018 at 4:19 PM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Robinson, Angela Y. (Fed)" <angela.robinson@nist.gov>
Subject: Dear D.B.A.,

To both those Willing and Un-Willling Members in the D.B.A.,

Tomorrow at 10am is our last PQC meeting to finalize decisions before the next round.

I would like to advocate for LIMA to be moved through to the next round.
(BLahblahblAh, it'll be eliminated eventually, etc.)

There are two factors to consider:
1) SUPERCOP benchmarking results, which we haven't fully looked through yet (which offsets the "2x overhead" of LIMA in the comparison talk..)
and more importantly, 2) LIMA has working code for distributed decryption https://eprint.iacr.org/2018/1034.pdf

Jacob and I have discussed looking into real-world PQC threshold signatures recently, and LIMA is -- now, in my view -- the best jumping-off-point to approach that.
I don't see why would eliminate them (given that we kept both of Classic McEliece and NTS-KEM, zzzz)

Get in there,
--Daniel