From: Apon, Daniel C. (Fed)
To: Moody, Dustin (Fed); Perlner, Ray A. (Fed); Robinson, Angela Y. (Fed); (b) (6)
Subject: Re: New algebraic lattice reduction paper -- does it impact us?
Date: Monday, December 16, 2019 1:21:41 PM

Good point-- Let me email them.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Monday, December 16, 2019 1:21 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>; Daniel Smith-Tone (b) (6)
Subject: RE: New algebraic lattice reduction paper -- does it impact us?

Daniel,

Just a thought – 2 of these authors are on the Falcon team. We could ask them. Not saying that it's not worth us reading and learning about – but we could get their opinion pretty quick probably.

Dustin

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Monday, December 16, 2019 1:19 PM
To: Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Robinson, Angela Y. (Fed) <angela.robinson@nist.gov>; Daniel Smith-Tone (b) (6) ; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: New algebraic lattice reduction paper -- does it impact us?

Hi guys,

I've been working to parse this new paper on ePrint: https://eprint.iacr.org/2019/1436.pdf

It describes a newly refined approach for reducing module lattices and claims better performance than prior art, which may be of interest to us.
Unfortunately, it's 76 pages long, densely written, applied only to attacking multilinear maps on module lattices (which live in a different parameter regime), and much of the algorithms are heuristic (so it's not easy to directly extract what should be the expected behavior on, say, Kyber, Saber, Dilithium, etc. in a short glance).

Is anyone interested in trying to read through this with me, and extract the pertinent knowledge for NIST PQC?
(The outcome could be anywhere from: a) no impact to NIST PQC candidates, up to b) reduced security of NIST PQC module-lattice candidates, by X amount.)

--Daniel