From: Alperin-Sheriff, Jacob (Fed)
To: Moody, Dustin (Fed); Perlner, Ray A. (Fed)
Subject: Re: PQC classification
Date: Friday, March 23, 2018 3:13:43 PM

Or at least “multivariate”

As to the lattice thing, lattice vs. code is a somewhat dumb way to look at it. It would arguably be better broken down into

Randomized coding, which would encompass all the LWE/NTRU schemes plus Lepton, Ramstake, Mersenne plus BIKE, QC-MDPC, HQC

Vs algebraic heuristic coding which would encompass the rest of the schemes we have as “coding” currently.

And then maybe put Odd Manhattan and DRS in “other”

But whatever

From: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Date: Friday, March 23, 2018 at 3:03 PM
To: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Subject: Re: PQC classification

What’s “really a lattice” anyway?

There’s no actual lattices created in any of the schemes as instantiated AFAIK with the (possible) exception of Odd Manhattan and/or DRS.

Giophantus should be MQ I thought …

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Friday, March 23, 2018 at 3:00 PM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Subject: PQC classification

I was checking our classification. I found some I had a question about:

Giophantus – we call it code-based. I think maybe it should be other?
Lepton – we call it Lattice, but I think it should be codes
Ramstake – we call it lattice. Should it be codes?
Mersenne – we call it lattice. It seems not really a lattice. Other?

Dustin