From: Alperin-Sheriff, Jacob (Fed)
To: Moody, Dustin (Fed); internal-pqc
Subject: Re: Regarding Round2
Date: Monday, December 18, 2017 1:17:23 PM

There are 25 directories, 20 for uround, 5 for nround. I'm okay with posting it though but it'll be over our 25MB limit

---

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Monday, December 18, 2017 at 1:15 PM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Subject: RE: Regarding Round2

I think it's 15.

They have Round 2 broken down into 2 types: uround and nround. For uround, they have 10 parameter sets, 2 for each security level (a ring version and a non-ring version). They also have 5 parameter sets for nround, one for each security level.

Dustin

From: Alperin-Sheriff, Jacob (Fed)
Sent: Monday, December 18, 2017 1:05 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Regarding Round2

They have 25 different parameter sets each for KEM and Encrypt and it takes up 84MB. These need to be narrowed down, I think.

—Jacob Alperin-Sheriff