From:	Perlner, Ray (Fed)
To:	Alperin-Sheriff, Jacob (Fed)
Subject:	RE: This is the attack I was looking for based on polynomial factorization
Date:	Friday, October 20, 2017 3:24:00 PM

Thanks. Reading further in the submission, they explicitly say they are checking this.

From: Alperin-Sheriff, Jacob (Fed)
Sent: Friday, October 20, 2017 3:24 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: This is the attack I was looking for based on polynomial factorization

Looks fine too

From: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Date: Friday, October 20, 2017 at 3:22 PM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Subject: RE: This is the attack I was looking for based on polynomial factorization

Good. Can you check 10163 and 32749 too?
These are used in CAKE

From: Alperin-Sheriff, Jacob (Fed)
Sent: Friday, October 20, 2017 3:17 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: This is the attack I was looking for based on polynomial factorization

So it looks like they checked LEDAKem to ensure (x^p+1) doesn't split modulo 2 beyond (x+1)*(x^{p-1}- …+..-x+1) for any of their chosen primes

---

From: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Date: Friday, October 20, 2017 at 2:40 PM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Subject: This is the attack I was looking for based on polynomial factorization

https://arxiv.org/pdf/1504.05431.pdf