From: Moody, Dustin (Fed)
To: Dang, Thinh H. (Fed)
Subject: RE: checking in
Date: Tuesday, August 8, 2017 10:44:52 AM

That might be difficult, but worth trying.

Can you guess what the map should look like? For example, using the same kind of idea in Theorem 4 and its proof of
https://eprint.iacr.org/2011/430.pdf

Dustin

From: Dang, Thinh H. (Fed)
Sent: Tuesday, August 08, 2017 10:40 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: checking in

Hello Dr. Moody. I'm doing well. I'm trying to do symbolic calculations to see if I can compose all the maps that way.

From: Moody, Dustin (Fed)
Sent: Tuesday, August 8, 2017 9:09:02 AM
To: Dang, Thinh H. (Fed)
Subject: RE: checking in

Thinh,

I haven't heard from you in awhile. How are you?

Dustin

From: Moody, Dustin (Fed)
Sent: Thursday, August 03, 2017 12:37 PM
To: Dang, Thinh H. (Fed) <thinh.dang@nist.gov>
Subject: Re: checking in

Thinh,

Just checking on your progress this week. How is everything?

Dustin

From: Dang, Thinh H. (Fed)
Sent: Wednesday, July 26, 2017 2:57:04 PM
To: Moody, Dustin (Fed)
Subject: Re: checking in

I'll try that.

From: Moody, Dustin (Fed)
Sent: Wednesday, July 26, 2017 2:49:32 PM
To: Dang, Thinh H. (Fed)
Subject: RE: checking in

Can you do a bunch of 5-isogenies? Then try to guess what the form of the isogeny should be, perhaps.

From: Dang, Thinh H. (Fed)
Sent: Wednesday, July 26, 2017 2:37 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: checking in

I haven't been focusing on a specific degree. I'd just choose a random point to generate the kernel, and construct the isogeny from that. I haven't seen any pattern yet.

From: Moody, Dustin (Fed)
Sent: Wednesday, July 26, 2017 1:25:18 PM
To: Dang, Thinh H. (Fed)
Subject: RE: checking in

What degree(s) are you trying? How many examples? Notice any patterns?

Dustin

From: Dang, Thinh H. (Fed)
Sent: Wednesday, July 26, 2017 1:17 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: checking in

yes I have

From: Moody, Dustin (Fed)
Sent: Wednesday, July 26, 2017 1:16:14 PM

To: Dang, Thinh H. (Fed)
Subject: RE: checking in

Have you been able to compute some examples then (of composing all the maps together)?

Dustin

From: Dang, Thinh H. (Fed)
Sent: Wednesday, July 26, 2017 11:56 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: checking in

Dr. Moody;

The map in the Twisted Hessian Curve paper seems to work well. The omega involved in that map, even if only exists in a quadratic extension of the base field, vanishes after all the maps are composed together. So the result of the composition is still defined over the base field.

From: Moody, Dustin (Fed)
Sent: Wednesday, July 26, 2017 7:34:29 AM
To: Dang, Thinh H. (Fed)
Subject: checking in

Thinh,
How is everything going these days? I will be downtown until this afternoon, and will be out of the office tomorrow and Friday. Making any headway? Any interesting examples?

Dustin