From: Moody, Dustin (Fed)
To: Dang, Thinh H. (Fed)
Subject: RE: did it work?
Date: Thursday, June 22, 2017 2:28:00 PM

Continuing on with this idea, here's what works:

Let Phi be the map from the Hessian curve H to the Weierstrass curve E (as given in Wikipedia or the joye/quisquater paper). Then the map Theta(P)=Phi(P+(0,-1)) seems to do the trick, i.e. it respects addition. Working out the maps, we get the following:

If U^3+V^3+1=3dUV
Then set
X = -3(-d^3+3d^2(U+V)+4) / (U+V+d)
Y = 36(d^3-1)(U-V)/(U+V+d)

Then the map Theta(U,V)=(X,Y) maps from H to E,
E: Y^2=X^3-27d(d^3+8)X+54(D^6-20D^3-8).

And Theta(Q)+Theta(R)=Theta(Q+R).

I think the inverse map is
U = - (3dX-Y+36-9d^3)/(6X+54d^2)
V = - (3dX+Y+36-9d^3)/(6X+54d^2)

Can you confirm that this works? Once we know it does, then I think you can continue on in the method we've discussed.

Dustin

From: Moody, Dustin (Fed)
Sent: Thursday, June 22, 2017 1:31 PM
To: Dang, Thinh H. (Fed) <thinh.dang@nist.gov>
Subject: RE: did it work?

Thinh,
What do you make of this example? Let's work over F_41, with the standard (untwisted) Hessian curve d=12.

Both the Hessian curve H and the birational Weierstrass curve E are cyclic and have 42 points. Let the generator of the Hessian curve be G=(25,10) and the generator of the Weierstrass curve be P=(17,6). Let Phi: H to E be the map from H to E (as given by Wikipedia/the Quisquater/Joye paper).

Then it appears that
Phi(G)=P,

and
Phi(kG)=(29k-28)P.

So, this might explain why addition doesn't work:
Phi(kG)=(29k-28)P
Phi(cG)=(29c-28)P
Then Phi(kG+cG)=Phi((k+c)G)=(29(c+k)-28)P=(29c+29k-28)P
Whereas
Phi(kG)+Phi(cG)=(29k-28)P+(29c-28)P=(29c+29k-14)P.
Then it would seem for this example we would get Phi(Q)+Phi(R)=Phi(Q+R)+14P

Note 14P is a point of order 3. So maybe the birational transformation preserves addition up to addition by a point of order 3?

Dustin

From: Moody, Dustin (Fed)
Sent: Thursday, June 22, 2017 12:06 PM
To: Dang, Thinh H. (Fed) <thinh.dang@nist.gov>
Subject: RE: did it work?

I'm looking back at my Edwards examples, and the birational transformation preserves addition. This appears not to be the case for Hessian (or twisted) Hessian curves. So we need to find a map which does preserve addition. Hmmmm

---

From: Dang, Thinh H. (Fed)
Sent: Thursday, June 22, 2017 11:53 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: did it work?

sage doesn't let me compose isogeny with the maps on projective curves. So at the moment, the TwistedHessian_isogeny function just returns a tuple of 3 individual maps instead of a composition of them. I'm trying to somehow to compose them.

From: Dang, Thinh H. (Fed)
Sent: Thursday, June 22, 2017 11:48:50 AM
To: Moody, Dustin (Fed)
Subject: Re: did it work?

From: Moody, Dustin (Fed)
Sent: Thursday, June 22, 2017 10:59:52 AM
To: Dang, Thinh H. (Fed)

Subject: RE: did it work?

I will look at this today.

Can you send me your SAGE code?

From: Dang, Thinh H. (Fed)
Sent: Thursday, June 22, 2017 10:45 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: did it work?

Dr. Moody;

It doesn't work.

From: Moody, Dustin (Fed)
Sent: Thursday, June 22, 2017 8:20:47 AM
To: Dang, Thinh H. (Fed)
Subject: did it work?