From: Moody, Dustin (Fed)
To: Dang, Thinh H. (Fed)
Subject: RE: Update?
Date: Friday, January 27, 2017 8:18:00 AM

It would be good if you have some time to talk today. We haven't met in awhile. We can go over what you have learned.

From: Dang, Thinh H. (Fed)
Sent: Friday, January 27, 2017 6:45 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Update?

Dr. Moody;

Yes, I'm going to work on this Friday 0/27/2017.

Thinh Dang

From: Moody, Dustin (Fed)
Sent: Tuesday, January 24, 2017 11:25:15 AM
To: Dang, Thinh H. (Fed)
Subject: RE: Update?

Thinh,

Will you be here this Friday?

Dustin

From: Dang, Thinh H. (Fed)
Sent: Friday, December 02, 2016 2:41 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Update?

I haven't learned about Huff curves and Hessian curves yet.

From: Moody, Dustin (Fed)
Sent: Friday, December 2, 2016 2:40:41 PM
To: Dang, Thinh H. (Fed)
Subject: Re: Update?

Have you learned about other models of elliptic curves, like Huff curves, or Hessian curves?

I think one thing to try is to find isogeny formulas for Hessian curves...

From: Dang, Thinh H. (Fed)
Sent: Friday, December 2, 2016 2:39:02 PM

To: Moody, Dustin (Fed)
Subject: Re: Update?

Yes, I'm still doing that.

From: Moody, Dustin (Fed)
Sent: Friday, December 2, 2016 2:38:33 PM
To: Dang, Thinh H. (Fed)
Subject: Re: Update?

I'm sorry Thinh. I left after lunch. We can try again in two weeks? I thought you were going to come to the PQC talk, and I was going to talk to you there. Are you still playing around with isogenies?

Dustin

From: Dang, Thinh H. (Fed)
Sent: Friday, December 2, 2016 2:13:24 PM
To: Moody, Dustin (Fed)
Subject: Re: Update?

Dr. Moody;

I came to your office after lunch but didn't you there.

From: Moody, Dustin (Fed)
Sent: Monday, November 28, 2016 11:17:53 AM
To: Dang, Thinh H. (Fed)
Subject: RE: Update?

Are you here this Friday (Dec 2nd)? Let's meet up sometime. We will have a PQC meeting from ten til eleven thirty or so, so we could do it before that, or after lunch, whichever is better for you.
Thanks,

Dustin

From: Dang, Thinh H. (Fed)
Sent: Friday, November 25, 2016 1:23 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Update?

Dr. Moody;

I'm still coming every Friday. I have classes all day every other weekday this semester.

From: Moody, Dustin (Fed)

Sent: Monday, November 21, 2016 3:27:47 PM
To: Dang, Thinh H. (Fed)
Subject: RE: Update?

Are you still coming every Friday? I am often not here on Friday's, but I'd like to meet sometime. Are you able to come on other days?

That is good that you seem to have figured out how to work with Edwards curves. Yes, there are often exceptional cases that result in (0,0,0). For those cases, there are other formulas which don't give (0,0,0). The idea that gets used for cryptography is that if you do things right, you only work with points that never give you those exceptional cases. For example, if you work in a subgroup generated by a point of odd order, then it shouldn't happen.

Now that you have the hang of things, you might try playing around with a few other models of curves, such as Huff curves, Hessian curves, Jacobi quartics, or Jacobi intersections, for example. Then we can try and find new isogeny formulas. Does that make sense?

Dustin

From: Dang, Thinh H. (Fed)
Sent: Friday, November 11, 2016 12:08 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Thinh Dang (b) (6)
Subject: Re: Update?

Dr. Moody;

I've been able to do additions on twisted Edwards curve and map from a twisted Edwards curve to a Weierstrass curve. I've been testing with prime fields and the mapping does seem to be a homomorphism. But there are some weird cases when a point on Edwards curve maps to (0,0,0), or when a point added to itself many times over gives (0,0,0).

I'm also using your Edwards isogeny formula. If there isn't any error, it does appear to be an isogeny.

Thank you and regards,

Thinh Dang

From: Moody, Dustin (Fed)
Sent: Wednesday, November 9, 2016 8:46:10 AM
To: Dang, Thinh H. (Fed)
Subject: Update?

Thinh,

How’s it going? I haven’t heard from you in awhile. Hope everything is okay.

Dustin