From: Chen, Lily (Fed)
To: (b) (6)
Subject: RE: Travel Question
Date: Wednesday, August 16, 2017 4:34:00 PM

Hi, Daniel,

For this year, if ECC and MACIS are scheduled on the same dates (one day overlap), then you probably can only attend one. I do not know how much you need to know about MACIS to submit a paper for 2019. (Did I understand you right? If you already submitted for 2017, then you already made a decision.)

For travel, you tell me which one you will go (including the information for the conference) and I will submit your request. Sorry I did not help you to break the tie.

Lily

From: Daniel Smith (b) (6)
Sent: Wednesday, August 16, 2017 1:03 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Travel Question

Hi, Lily,

I wanted to ask for your advice on my upcoming travel plans in November. I have two conferences that are at the same time in November that I would like to go to, and I am wondering if NIST's perspective might help me decide what I want to do.

First, I would really like to go to ECC this year. I have the right mathematical background to work in this area, but I think that I would get a research-level understanding if I could attend the summer-school being held with the conference. Also, I'm interested the pairings-based stuff and I understand that Craig Costello will be presenting there, which I would find interesting. I believe that Dustin is already going, which might make my attendance a little less of a priority for NIST, but I am hoping that I can start doing research in this area too; I would like to be able to contribute in as broad an area as I can at NIST in the future.

The problem is that there is another conference, Mathematical Aspects of Computer and Information Sciences (MACIS) that is at the same time and I have a paper that is appropriate for that conference (it is about the computational complexity of MinRank for a particular type of system of equations). I also think that I would find that conference interesting, but I'm not sure that I would grow as much as a researcher there in comparison to ECC. I'm also not comletely sure whether I want to submit this paper to MACIS or to PQCRYPTO 2018, but I think that it would be a little more appropriate for MACIS given that it is foundational and wouldn't directly impact the choice of parameters for practical schemes.

What would you suggest? I'm more excited about ECC than MACIS, but I have a potential concrete contribution for MACIS. Thanks for any suggestion you can make to break the tie!

Cheers,

Daniel