From: Miller, Carl A. (Fed)
To: Smith-Tone, Daniel C. (Fed)
Subject: Multivariate crypto
Date: Tuesday, March 21, 2017 2:29:01 PM

Hi Daniel –

Hope you’re doing well – sorry I missed your talk last week (I was visiting CalTech). I have a quick question for you, if you have a minute:

I’m planning to give a talk in the postquantum crypto seminar next week. The goal is to help me to get more deeply into classical crypto and hopefully in the process show the audience something new.

Given my background (algebraic geometry & quantum crypto) I think multivariate crypto is probably the best topic. So, the question is: can you think of any topics within multivariate crypto that might be good material? An ideal topic would be one that hasn’t been covered before and that’s fairly accessible (and it’s even better if it happens to have some algebraic geometry in it).

See you around!

-Carl

—————
Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD