From: Moody, Dustin
To: Peralta, Rene
Subject: Slides for Crypto Club talk
Date: Wednesday, January 20, 2016 9:17:00 AM
Attachments: quantumisogenies.pdf
quantumisogenies.tex
Differential Invariants.pptx
13371.SmithDaniel.Slides.pdf
dings crypto club talk.pdf

Rene,

I gave one talk on quantum-resistant isogeny based systems, which I've attached the pdf (and the tex file I used to create it). I also have all the graphics files if you need it. The isogeny scheme isn't the only non lattice/coding-based/multi-variate/hash-based scheme, so maybe you could find others to mention, although I don't think many have received very much attention. The only other ones I can think of are the "permuted kernel problem" mentioned by Microsoft at our PQC workshop (http://csrc.nist.gov/groups/ST/post-quantum-2015/presentations/session7-shumow-dan.pdf) and the conjugacy search problem in Braid groups. There isn't time to go into any details, other than maybe just mentioning them>

I found one talk Daniel gave on his work in Multi-variate. Much of it is probably too specialized, but some of it could be useful. I'm also trying to get some slides from a more introductory talk he gave at the PQCrypto 2014 summer school. A video of it is available at https://www.youtube.com/watch?v=RlWscAAxtAI&feature=youtu.be, but it is over an hour long. I found another set of his slides (attached) for a talk he gave at Dagstuhl. Finally, I found Jintai Ding's talk he gave to the crypto-club here at NIST, where he gave an introduction to multi-variate crypto.

I hope Daniel will be able to talk, but if not I appreciate you being willing. I've tried to divide up our talk so that everyone will help out, and I don't get stuck doing too much. Thanks!

Dustin