From: (b) (6)
To: Moody, Dustin (Fed); Perlner, Ray A. (Fed)
Subject: ABC
Date: Wednesday, February 22, 2017 7:57:24 AM

Hi, guys,

Maybe if we have room in the final version we could put an analysis of an ABC minrank attack using minors modeling. I think that it is interesting to compare the linear algebra search vs the grobner basis techniques.

For quad-abc, you have 2s^2 matrices and a target rank of 2s. I haven't calculated the Hilbert Series for the minors ideal, but my guess is that the degree of regularity will be 2s+1. If that is the case, then the asymptotic complexity will be something like
s^(2(2s+1)w) where w is the linear algebra constant. So the number of operations over F_q is independent of q, but this definitely has exponential complexity. If we compare this to our complexity, the break even point should be something very very roughly like q=s^(4w), or basically s^9. If s=8, then we have q about 2^(27).

The case for cubic is a little worse. You need to randomly select a vector to collapse the 3-tensors into a list of 2s^2 2-tensors to apply minors modeling. Then you get an extra factor of q to randomly choose a vector in some band kernel. so the complexity should be about qs^(2(2s+1)w), which is no longer independent of q. The break even point should still be about the same though.

Cheers!