From: Perlner, Ray (Fed)
To: (b) (6)
Subject: RE: I found a case where, minrank is cheaper than direct attack, but the system is not superdetermined
Date: Monday, June 12, 2017 9:48:00 AM

Actually, I'm a moron. The example I gave doesn't work, since I grossly overestimated the complexity of direct attack in the case I gave. I forgot you could guess values for the variables until the system for direct solving is fully determined. I think I can now write up a justification of why direct attack is pretty much always cheaper than minrank for overdetermined, but not superdetermined systems.

From: Daniel (b) (6)
Sent: Saturday, June 10, 2017 9:34 AM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: RE: I found a case where, minrank is cheaper than direct attack, but the system is not superdetermined

The super determined case isn't supposed to mean that it is the limit to when the min rank attack is more efficient. It only means that it is the limit in which the problem can be solved linearly without Grobner bases. It is not surprising that there are parameters for which the minors modeling is more efficient even though not linear.

There are a couple of things going on. It is a good point you bring up, but I still think that the schemes of cryptographic interest either have r low or the direct attack is more efficient. For one thing, why would we be using min rank if the rank is n-4? Why not use the high rank attack from triangular schemes?

Cheers!

I'll get back to my luxury hotel now. ;)

Sent from my T-Mobile 4G LTE Device

-------- Original message --------
From: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Date:06/09/2017 11:14 PM (GMT+02:00)
To: "Daniel Smith (b) (6)
Cc:
Subject: I found a case where, minrank is cheaper than direct attack, but the system is not superdetermined

n = 100
k = 15
r = 96