From: [redacted]
To: Perlner, Ray A. (Fed)
Subject: experiments
Date: Saturday, May 20, 2017 3:18:50 PM

Hi,

I've done some experiments on the relationship between the MinRank instances for various n and r vs. the direct algebraic attack.

Basically, I'm comparing two inequalities involving \epsilon where
m=\epsilon n^2.

For the associated MinRank instance to not be superdefined it is necessary for m to be greater than (n-r)^2/(r+1)-r, and it suffices for \epsilon to be around 1/(r+1). The exact value is a little larger, but less than 1/r. Then for the degree of regularity of the original scheme to be r+1, it is necessary for \epsilon to be bigger than
C(n+r,r+1)/n^{r+1}.

If you compare these quantities for r=1 then most values of n show that the latter quantity is larger, meaning that you have non-superdefined instances that have a degree of regularity higher than r+1, so that they may be cryptographically significant and more analysis than we provide is necessary. For r>1, there are only ever a few very small values of n (such as n=3) for which this is the case. Since the only cases in which the direct attack could be more complicated have MinRank 1, I think these are still easy to solve, meaning that the degree of regularity of the direct attack is still probably quite small.

I don't know if I want to add this analysis into the paper, but it justifies my claim that nothing of cryptographic significance is merely overdefined and not superdefined.

Cheers,
Daniel