From: (b) (6)
To: Perlner, Ray A. (Fed)
Subject: MinRank
Date: Saturday, May 20, 2017 2:28:02 PM

Hi,

I can't find any good surveys of the best methods for very overdefined systems, but I can give some simple analysis to show why they are easy and really can't be used for crypto.

Suppose we have n variables and m=\epsilon n^2 equations. For simplicity we assume homogeneity. We can bound the degree of regularity for the system by computing the number of monomials of degree d in n variables and finding the number of degree d equations we can generate from the m equations given. Rough numbers are C(n+d-1,d) for the former and n^{d-2}m=\epsilon n^d for the latter. The quotient C(n+d-1,d)/n^d provides a lower bound for \epsilon for the degree of regularity to be d, and of course we can use this in reverse to find the degree of regularity for a given \epsilon.

We can then equate \epsilon n^2 with (n-r)^2/(r+1) to see what r corresponds to \epsilon. In this way we can get a good estimate of the complexity of the direct algebraic attack.

This technique takes advantage of the fact the the degree of regularity only depends on the homogeneous components of highest total degree of each of the polynomials. (So the sizes of the matrices in F4 to solve these systems is larger than C(n+d-1,d).)

In the context of MinRank, the target rank r is relevant. We are showing that in the superdefined case that the complexity of solving the system is something like n^{r+1}. We're thinking that solving the MinRank is like private key recovery, which it usually is. In comparison to the overdefined but not superdefined instances of MinRank, they correspond to systems we can solve directly with complexity roughly n^d. If d is small because \epsilon is big enough, then solving the MinRank isn't the interesting problem. Of course, this depends on the values of n and r.

Cheers,
Daniel