From: (b) (6)
To: Perlner, Ray A. (Fed); Petzoldt, Albrecht R. (IntlAssoc)
Subject: Re: Idea for speeding up direct attack and HFEv- attack.
Date: Wednesday, June 14, 2017 12:44:14 PM

I think that this observation is related to one of the mutant variants. I think that you're right, but I'm less sure if it would help out our projection strategy that much. We would still have to consider new bases for the plaintext and then eliminating variables in general to have a noticable difference even in the codim one case, so I think that the complexity is about the same. I'm not sure though. We could test it.

On Wed, Jun 14, 2017 at 5:37 PM Perlner, Ray (Fed) <ray.perlner@nist.gov> wrote:

> So, the usual most expensive step in Grobner basis stuff, as I understand it is finding degree d-2 polynomials p_k that we can multiply by the public polynomials f_k, such that
>
> Sum(p_k*f_k) = q, where q has degree at most d-1.
>
> I think this problem can be reduced to the same problem in one fewer variable, plus the problem of solving multivariate equations in all the variables, but with the degree d-1 terms cancelling, instead of the degree d terms.
>
> First, note that if Sum(p_k*f_k) = q, then Sum(p_k*f_k) = q (mod x_n).
>
> We can then see that solutions (not mod x_n) are generated by
>
> 1) solutions to Sum(p_k*f_k) = q (mod x_n) where p_k are polynomials in the variables (1,… x_{n-1}) and
>
> 2) polynomials of the form x_n*p' *f_k, where p' has degree at most d-3.
>
> The important thing to note is that both generators in category 1 and 2 are divisible by x_n in the highest degree terms. Thus, solving for a solution of Sum(p_k*f_k) = q, given a solution to Sum(p_k*f_k) = q (mod x_n), requires only considering the same number of monomials as would be required if we were solving a system with degree of regularity d-1.
>
> I think this gets us two things:
>
> First of all, it's a way to project further down in the HFEv- attack. We can then cheaply mod

variables back in to see whether they increase the degree of regularity (or simply decrease the dimension of the solution space of Sum(p_k*f_k) = q more than would be expected if we didn't end up modding a vinegar variable back in.)

Second of all, I think it, at least asymptotically, should speed up direct attack. We can apply the reduction recursively to reduce the degree d case to no more than n instances of the degree d-1 case. Since the complexity of the usual attack goes something like n^(omega * d), n^(omega*(d-1))*n should be less.

Anyway, I haven't fully analyzed this thing by any means, but it seems like a promising thought.

Cheers,
Ray