From: (b) (6)
To: Perlner, Ray A. (Fed)
Subject: Re: confused
Date: Friday, November 17, 2017 10:54:55 AM

Okay. I agree with that. more or less. If l is very small, however, it is like having a nearly balanced oil and vinegar and there are attacks for that. That's why I was saying that I think we need a sufficiently large number of plus polynomials. The problem is that the degree of regularity of this scheme can't be that high. It's okay as long as we can get it to something like 10 when we have, say 130 or 140 variables.

On Fri, Nov 17, 2017 at 10:18 AM, Perlner, Ray (Fed) <ray.perlner@nist.gov> wrote:

> That looks correct. My point was that from the attacker's perspective there's no useful distinction between the F^{d-l} and F^l components in your factorization of the preimage of U, They behave the same in the differential invariant attack, and with high probability there's even an equivalent private key, where the vinegar subspace is defined to be the image of F^{d-l}\oplusF^l
>
> **From:** Daniel Smith (b) (6)
> **Sent:** Thursday, November 16, 2017 10:31 PM
>
> **To:** Perlner, Ray (Fed) <ray.perlner@nist.gov>
> **Subject:** Re: confused
>
> Sorry, I realized I meant to say that the differentials map (0,x_o,0) to (y_v,0,y_l).
>
> On Thu, Nov 16, 2017 at 10:23 PM, Daniel Smith (b) (6) wrote:
>
> > I'm not sure I understand what you're saying here. Does it have something to do with the fact that U is not surjective? I don't get it.
> >
> > The F_R UOV map is a map from F^{n+l=d+o} that discerns two subspaces of its domain, the first d coordinates which span V and the last o coordinates which span O. I'm calling these things the oil and vinegar subspaces and they exist independent of the rest of the scheme (even without F_S, F_P, U and T). Then we have the linear embedding U from F^n to F^{n+l=d+o}=V\oplus O. Since the image of U is d+o-l dimensional, we should expect the intersection of this with V to be of dimension d-l and the intersection of this with O to be of dimension o-l. When d=o, which is what all of the original parameters had, these two quantities are equal. It means that the preimage of U has a factorization F^{d-l}\oplusF^{o-l}\oplusF^l for which every differential (if we have no plus polynomials) maps (x_v,x_o,x_l) to (y_v,0,y_l). If l is sufficiently small this might be detectable.

What's wrong with this?

Cheers!

On Thu, Nov 9, 2017 at 10:48 AM, Perlner, Ray (Fed) <ray.perlner@nist.gov> wrote:

> Also, I didn't notice you were still making this erroneous claim:
>
> "What I'm saying is that it is fairly likely that the intersection of the vinegar subspace V with the image of U has the same dimension as the intersection of the oil subspace O and the image of U."
>
> This is wrong. Vectors consisting of only oil variables (i.e. those vectors that the rainbow and HFE polynomials act linearly on) form a subspace of the codomain of U. Vectors that are acted on quadratically by the HFE and rainbow polynomials do not form such a subspace. We can think of the vinegar space as a space of linear forms acting on the codomain of U and the oil space as the intersection of the kernels of those linear forms. The dimension of the oil subspace of the plaintext space is then the dimension of the intersection of the range of U and the oil space in the codomain of U. With high probability this space will have dimension o-l.
>
> **From:** Daniel Smith (b) (6)
> **Sent:** Wednesday, November 08, 2017 7:42 PM
> **To:** Perlner, Ray (Fed) <ray.perlner@nist.gov>
> **Subject:** Re: confused
>
> What you are saying makes sense and essentially corresponds with what I mentioned before. If I pick a pair of maps orthogonal to the random polynomials (with probability q^(-2s)), then the invariant trick will work if v and o are the same. The parameters that we broke all have v=o and s very small, like 3 to 5 or something. Now the l is not zero, but I think that you are right that it is not significant except in how likely it is that we have a vinegar subspace in the plaintext space and an oil subspace that are of the same dimension. The scheme uses an embedding U, which has an inverse U^* defined on its image. What I'm saying is that it is fairly likely that the intersection of the vinegar subspace V with the image of U has the same dimension as the intersection of the oil subspace O and the image of U. Then the preimages of these sets (that is U^* of these sets) are of equal dimension and correspond to vinegar and oil subspaces of the

plaintext space. So, like you ultimately stated, the complexity is q^(2s) times linear algebra. The distinguishing speed up is okay, but not a big deal for s=3. The point is that this scheme can be broken that way, so we actually need to have v and o different., not just nominally. The plus polynomials make it harder, but not significantly harder unless there are so many that the algebraic attack is scary.

On Wed, Nov 8, 2017 at 4:56 PM, Perlner, Ray (Fed) <ray.perlner@nist.gov> wrote:

> Regarding the l. I'm pretty sure the key you get with such an l, is, with high probability, the same as a key you would get if you used o = v-l and l =0. Hence I'm ignoring it.
>
> Regarding the projection idea. The "UOV attack," in rainbow or unbalanced oil and vinegar, works by projecting plaintext variables out and hoping you can get rid of enough vinegar variables that the projected system looks like balanced oil and vinegar, and can therefore be attacked. The problem I'm alluding to is that this interacts kind of poorly with the plus modifier. In order to distinguish bilinear maps from the (HFE + rainbow) subspace, using the invariant subspace trick, you need two of them (at least I don't know how to do it with only one.) The odds of picking a pair of such maps is q^(-2s). If, on the other hand, you project out ~ sqrt(s) vinegar variables, you can distinquish a single (HFE + rainbow) map from a random map (since it will be more likely than a random map to have corank sqrt(s). This results in an attack complexity of q(s+ sqrt(s) + v – o + l) or thereabouts instead of q^(2s + v – o + l).
>
> **From:** Daniel Smith (b) (6)
> **Sent:** Wednesday, November 08, 2017 4:27 PM
> **To:** Perlner, Ray (Fed) <ray.perlner@nist.gov>
> **Subject:** confused
>
> Hi, Ray,
>
> I'm confused about your statement "project the plaintext space down to 2o variables". In the original parameter sets v and o were the same value and 2o was larger than n. There was a corank l embedding before the variables were split in two types. I'm not completely sure how this affects the invariant attack, but my feeling is that (on average) the preimage of the vinegar subspace under the embedding will be about half of the dimension of the plaintext space and that the preimage of the oil subspace will as well. Then can't we just do the invariant idea?

I apologize for not thinking this through carefully. I'm too busy, sick and sleepy. It seems to me like it will work, though.

Cheers,

Daniel