

**From:** [Perlner, Ray A. \(Fed\)](#)  
**To:** (b) (6)  
**Subject:** RE: GeMSS figures in Asiacrypt paper  
**Date:** Monday, June 15, 2020 5:42:00 PM

---

Yes. I'm talking about the former. I don't think we properly thought out how to finish the attack given that there are multiple linearly independent solutions over the extension field (probably  $n$  of them). I suspect it isn't that hard once you find a solution over  $GF(2)$  to the support minors modeling equations, but it will require more thought how to translate the solution to those equations to a solution over the extension field for the linear variables. You might have to find multiple solutions to the minors modeling equations over  $GF(2)$ , for example. When you run your XL-like code on support minors from an HFE instance, what is the dimension of the space of equations you get versus the dimension of the space of monomials?

**From:** Daniel Smith (b) (6)  
**Sent:** Monday, June 15, 2020 4:53 PM  
**To:** Perlner, Ray A. (Fed) <[ray.perlner@nist.gov](mailto:ray.perlner@nist.gov)>  
**Subject:** Re: GeMSS figures in Asiacrypt paper

There is a problem with language here. The support minors method applied directly to GeMSS produces a system of bidegree  $(b,r)$  in the linear variables and the variables of  $C=(K|I)$ , where we have a restricted monomial set [the component from variables in  $C$  is always in the form of a maximal minor of  $C$ ]. (I think that modeling it this way is strictly better than replacing the minors with new variables so that we would be of bi-degree  $(b,1)$  in the linear variables and the minors of  $C$ . The reason is that there may be instances where the rank is such that we get more efficiency by targeting something like  $(b,r+k)$  in this variable set and we would have many fewer monomials this way than going to something like  $(b,2)$  in the linear-minors set. It just requires a much more difficult analysis of how many monomials we are linearizing over.) This system of equations uses variables whose values like in  $GF(2^n)$ , but the coefficients are all in  $GF(2)$ .

On the other hand, we can choose a representation of  $GF(2^n)$  over  $GF(2)$  and use the fact that the operations are over  $GF(2^n)$  to generate a much larger set of equations in a much larger variable set, so that the entire system is modeled over  $GF(2)$ .

I don't know which of these two you are talking about when you say to linearly solve over  $GF(2)$ .

If you are talking about the latter, then I don't think that there is an extra step, I think that you just have the solution, so that makes me inclined to think that you are stating the former. But in that case, I go back to my original question which is how we got the complexities we obtained to begin with. How were we finishing the attack to get the solution over  $GF(2^n)$ ?

CHears!

On Mon, Jun 15, 2020 at 4:13 PM Perlner, Ray A. (Fed) <[ray.perlner@nist.gov](mailto:ray.perlner@nist.gov)> wrote:

Hm. The things we're solving linearly for are actually reasonably high degree in the variables we're really solving for (i.e. they're products of  $r \times r$  minors and degree- $b$  monomials, which in turn have

degree  $r+b$  in the things that are supposed to be in the extension field.) This makes me wonder whether we can solve linearly over  $GF(2)$ , and then use the solution to solve for one of the variables of interest in a univariate system (or in a much cheaper GB calculation). Like maybe you could set up an equation in the ratio  $x_1/x_2$  by looking at all the values for monomials generated by  $x_1, x_2$ , and one of the minors.

If something like that works, then the MinRank attack is actually cheaper than we had been assuming.

**From:** Daniel Smith (b) (6)  
**Sent:** Monday, June 15, 2020 2:17 PM  
**To:** Perlner, Ray A. (Fed) <[ray.perlner@nist.gov](mailto:ray.perlner@nist.gov)>  
**Subject:** Re: GeMSS figures in Asiacrypt paper

I don't think that it is a big deal. I think that we should have all of the information necessary to resolve the ideal, but we have to have some equations of positive degree in the variables to be able to achieve solutions in an extension field.

On Mon, Jun 15, 2020 at 2:14 PM Daniel Smith (b) (6) wrote:

I'm just wondering how we are justifying getting a solution in  $GF(2^n)$  when the equations have coefficients in  $GF(2)$ . There must be an additional Grobner basis step, because we can't get a solution outside of  $GF(2)$  linearly.

On Mon, Jun 15, 2020 at 2:12 PM Perlner, Ray A. (Fed) <[ray.perlner@nist.gov](mailto:ray.perlner@nist.gov)> wrote:

I think I used  $2 * 3 * n * \langle \text{matrix dimension} \rangle * \langle \text{number of potentially nonzero entries in the matrix} \rangle$ . Reasoning was that Wiedemann used  $3 * \langle \text{matrix dimension} \rangle$  matrix vector multiplications, where the matrix was over the base field and the vector was over the extension field. Let me know if this is wrong.

Cheers,  
Ray

**From:** Daniel Smith (b) (6)  
**Sent:** Monday, June 15, 2020 1:59 PM  
**To:** Perlner, Ray A. (Fed) <[ray.perlner@nist.gov](mailto:ray.perlner@nist.gov)>  
**Subject:** GeMSS figures in Asiacrypt paper

Hi, Ray,

How did we get our complexity numbers for GeMSS in the Asiacrypt paper? The equations are over  $GF(2)$ , but the solution needs to be over  $GF(2^n)$  (at least when we express all of the matrices the natural way). So when we solve linearly, we don't get coefficients in the extension field. So I'm just curious where we are getting the numbers from.

||| Cheers,  
Daniel