From: Moody, Dustin (Fed)
To: (b) (6)
Cc: Perlner, Ray A. (Fed)
Subject: RE: Current Draft for our PQC paper improving our attacks on cubic ABC for characteristic 2.
Date: Tuesday, February 14, 2017 12:27:53 PM

I believe Ray did this.

From: Daniel Smith (b) (6)
Sent: Tuesday, February 14, 2017 12:25 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: Current Draft for our PQC paper improving our attacks on cubic ABC for characteristic 2.

By the way, I am a PC member, so the radio button indicating this should be checked on our submission.

Cheers!

On Tue, Feb 14, 2017 at 10:26 AM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

> Actually, use this one for the .tex file
>
> **From:** Moody, Dustin (Fed)
> **Sent:** Tuesday, February 14, 2017 10:23 AM
> **To:** Perlner, Ray (Fed) <ray.perlner@nist.gov>; Daniel Smith (b) (6)
> **Subject:** RE: Current Draft for our PQC paper improving our attacks on cubic ABC for characteristic 2.
>
> I made some edits – pretty much all grammatical/syntactical in nature. Updated the References to include the correct version of SAGE.
>
> Please see the red text where I had a few questions.
>
> Dustin
>
> **From:** Perlner, Ray (Fed)
> **Sent:** Friday, February 10, 2017 3:36 PM
> **To:** Daniel Smith (b) (6)
> **Cc:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
> **Subject:** RE: Current Draft for our PQC paper improving our attacks on cubic ABC for characteristic 2.
>
> Ok. I added some quick corrections of my own.
>
> 1) Made the wording around your Hessian explanation a little less awkward

> 2) Decided the matrix in equation 5 didn't need to be named M
>
> 3) Put the stupid accent on naïve
>
> 4) Changed the title of section 6.
>
> 5) Changed s\geq2 to s\geq3 on page 9 (this inequality denotes the range of parameters where taking the span of the kernels of HE(w1), HE(w2) is likely to produce the whole band kernel)
>
> 6) Changed s^{2\omega} to s^6 on page 11.
>
> **From:** Daniel Smith (b) (6)
> **Sent:** Friday, February 10, 2017 12:51 PM
> **To:** Perlner, Ray (Fed) <ray.perlner@nist.gov>
> **Cc:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
> **Subject:** Re: Current Draft for our PQC paper improving our attacks on cubic ABC for characteristic 2.
>
> Here is an update fixing some issues, correcting some equation references removing some of the unnecessary equation numbering and realigning some things. This also includes an explanation of the Hessian thing. We still need an updated intro and conclusion. I'm happy to contribute some of this. Some of the text before the last two paragraphs of the intro is not quite compatible with the paper and the reference to NIST should include a reference to the CFP and not the announcement. I can come back to this, but I've got to work on another project right now. CHeers!
>
> On Fri, Feb 10, 2017 at 12:00 PM, Daniel Smith (b) (6) wrote:
>
>> I'll try to put a note in the paper regarding the Hessian, and see if I can tidy up the rest.
>>
>> By the way, I took a look at applying minors modeling with GB to this problem. It is horrible. The memory requirements are just too much, so I abandoned it. There is no question that this technique is the more feasible in this case.
>>
>> Oh, by the way, if you have s in the base field and f is a homogeneous quadratic, then if you look at the D_{s}f(a,x)=f(sx+a)-sf(x)-f(a)+sf(0) like you mentioned in December, then D_{s}f(a,x)=Df(a,sx). If you take away the restriction that s is in the base field, but add the restriction that f(x)=0, then the result still holds. If you have no restrictions then you get D_{s}f(a,x)=Df(s,1)f(x)+Df(a,sx). I haven't computed it, but I think that something similar would hold for cubics and the second differential as well. Not important.
>>
>> Cheers!
>>
>> On Thu, Feb 9, 2017 at 3:14 PM, Perlner, Ray (Fed) <ray.perlner@nist.gov> wrote:
>>
>>> Regarding s^6 vs s^(2\omega): In the last draft, I do see some s^6ths in the quadratic ABC section, and these can be changed to s^(2\omega).

From: Perlner, Ray (Fed)
Sent: Thursday, February 09, 2017 2:48 PM
To: 'Daniel Smith' (b) (6) Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Current Draft for our PQC paper improving our attacks on cubic ABC for characteristic 2.

I like the grads. The Hessians are slightly more annoying to me, but I can live with them, since the notation is easily findable on wikipedia. Perhaps you should add a sentence giving the componentwise definition of the Hessian.

Also, I can't figure out how to update equation 5 for a new choice of w for cheaper than s^6. I think the asymptotic complexity might not be s^(2\omega) after all.

From: Daniel Smith (b) (6)
Sent: Thursday, February 09, 2017 2:04 PM

To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: Current Draft for our PQC paper improving our attacks on cubic ABC for characteristic 2.

Okay,

Here is a version with the indices cut out. If you think this is more confusing than having all of the physicsesque indices, then I give up and will get back in my place.

I would note that in this notation many of the sums become simple matrix multiplications. I could have removed all of the matrix multiplications, I think, since the public key is ordered, but I think that the sums in the description of minrank are more revealing than having a vector of unknowns t times a vector of cubic forms \mathcal{E}.

Please give a quick check to the correctness, but I think that everything is okay. There was only one place in which a naked differential was required and that was when the notation was referring to an actual formal partial derivative and not to a formal derivative in the sense of D^nf=f_{a_1,\ldots,a_n}dx_{a_1}\otimes\cdots\otimes dx_{a_n}.

Here are the files.

Cheers,
Daniel

On Thu, Feb 9, 2017 at 1:28 PM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

> I will do some edits after we get a somewhat stable version, and can add in my version of SAGE, etc.

From: Perlner, Ray (Fed)
Sent: Thursday, February 09, 2017 1:12 PM
To: Daniel Smith (b) (6); Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: Current Draft for our PQC paper improving our attacks on cubic ABC for characteristic 2.

I think my notation is a bad? habit I picked up from being a physics major. I did try to meet you all halfway by being explicit about summing over repeated indices.

In any event I look forward to seeing what the new draft looks like.

From: Daniel Smith (b) (6)
Sent: Thursday, February 09, 2017 1:09 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: Current Draft for our PQC paper improving our attacks on cubic ABC for characteristic 2.

Hi, again,

I'm sorry to complain, but I need to show you how I think the notation is much better. (I understand what is going on but several times read 1,2, or 3-tensors as 0-tensors because the indices were parametrizing elements within an object and not specifying the object.) I'll change the notation in a few places and send it to you for you to determine whether you want to overrule me on this.

Dustin, I've added a proper citation for sage, but I don't have the version/year for your build of sage, so you'll need to update that in the references. I'll send the source including references in a bit when I've completed these minor edits.

Cheers,
Daniel

On Thu, Feb 9, 2017 at 12:18 PM, Daniel Smith (b) (6) wrote:

> Hi, guys,
>
> I think that the notation in our paper is a bit confusing. When we write $\frac{d}{dx_j}\frac{d}{dx_k}\mathcal{E}_i(\mathbf{w}_1)$ is a 2-tensor, I think it is quite confusing. A reader may interpret this as the second partial of a cubic function evaluated at an input, which is an element and not a 2-tensor. I would argue that it is better to specify that this is the Hessian evaluated at $\mathbf{w}_1$. Or we could write $H(\mathcal{E})$ or maybe $J(\nabla\mathcal{E})^\top$. Or, we could simply specify in words that we mean the matrix of 2nd partials instead of a specific second partial. I think it could be a lot clearer.
>
> Cheers,

Daniel

On Thu, Feb 9, 2017 at 11:04 AM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

> It seems the document keep changing rapidly, so whichever of you “has the football” right now can add this in:
>
> For the Experiments section, here’s what I think we can say:
>
> Using SAGE \cite{sage}, we performed some experiments as a sanity check to confirm the efficiency of our ideas on small scale variants of the Cubic ABC scheme. The computer used has a 64 bit quad-core Intel i7 processor, with clock cycle 2.8 GHz. Rather than considering the full attack, we were most interested in confirming our complexity estimates on the most costly step in the attack, the MinRank instance. Given as input the finite field size \$q\$, and the scheme parameter \$s\$, we computed the average number of vectors \$v\$ required to be sampled in order for the rank of the \$2\$-tensor \$D^2\mathcal{E}(v)\$ to fall to \$2s\$. As explained in Section 4, when the rank falls to this level, we have identified the subspace differential invariant structure of the scheme which can then be exploited to attack the scheme.
>
> As this paper is only concerned with binary fields, we ran experiments with \$q=2, 4\$ and \$8\$. We found that for \$s=3\$ and \$q=2,4\$, or \$8\$, with high probability only a single vector was needed before the rank fell to \$2s\$. For \$s=4\$ and \$s=5\$, the computations were only feasible in SAGE for \$q=2\$ and \$q=4\$. The average values obtained are presented in the table below. Note that for \$q=4\$ and \$s=5\$ the average value is based on a small number of samples as the computation time was quite lengthy.
>
> ```
> \begin{table}
> \centering
> \begin{tabular}{|c| c c| c c|}
> \hline
> & $s=4$ & $(q-1)^2q^s$ & $s=5$ & $(q-1)^2 q^s$ \\
> \hline
> $q=2$ & 24 & 16  & 35 & 32  \\ \hline
> $q=4$ & 1962 & 2304 & 7021 & 9216 \\
> \hline
> \end{tabular}
> \caption{Average number of vectors needed for the rank to fall to $2s$}
> \label{table:1}
> \end{table}
> ```
>
> In comparison, our previous experiments \cite{Our Last Paper} were only able to obtain data for \$q=2\$ and \$s=4,5\$. The average number of vectors needed in the \$s=4\$ case was 244, while for \$s=5\$, the average number in our experiments was 994 (with the predicted values being 256 and 1024).

Dustin

From: Daniel Smith (b) (6)
Sent: Tuesday, February 07, 2017 6:45 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Cc: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Current Draft for our PQC paper improving our attacks on cubic ABC for characteristic 2.

I am happy to volunteer for the formal derivative language.

Everything is slow. I'm getting the students set up to start writing on their own. I'll try to do this tonight/tomorrow morning.

On Tue, Feb 7, 2017 at 3:54 PM, Perlner, Ray (Fed) <ray.perlner@nist.gov> wrote:

> My changes from our SAC paper go through section 5. I still need to make a reference for our SAC paper “OldCubic”, and I need to translate section 6 from “discrete differential” to “formal derivative” language. (I would be delighted if someone would volunteer to do this instead of me.) We also need to update the simulation section and the conclusion.