

From: [Moody, Dustin \(Fed\)](#)
To: (b) (6)
Subject: RE: Very urgent please help!
Date: Monday, May 7, 2018 8:01:00 AM

I'm saying because $\ker \phi$ is not $\{0\}$, then $\ker \phi$ is R/q . When the kernel is 0, that means the image is $\{0\}$. So, everything gets taken by the "evaluation at 1 map (ϕ)" to 0. Hence, evaluating at 1 leaks no information.

From: Quynh Dang (b) (6)
Sent: Monday, May 07, 2018 7:56 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Very urgent please help!

Hi Dustin,

Please be patient and see my discussion below!

On Mon, May 7, 2018 at 7:49 AM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

Quynh,

The evaluation at 1 map is a ring homomorphism (whose domain happens to be a field). Everything we talked about is still correct.

The map $\phi: R/q \rightarrow Z/q$ is a ring homomorphism defined by evaluating at 1. The image of the map will be isomorphic to $(R/q) / (\ker \phi)$. We will be looking in the image of ϕ to see where $c(1)=m(1)$ is large. But if R/q is a field, then $\ker \phi = 0$ or $\ker \phi = R/q$. We know the kernel has more than one element, since any message with an equal number of 1s and -1s will be in the kernel. Hence, we must have the kernel of ϕ is all of R/q .

At this point, $R/q / (\ker \phi)$ is $\{0\}$, so the image (ciphertexts (plural) when evaluated at 1) is isomorphic to $\{0\}$ which does not mean that the image (ciphertexts when evaluated at 1) is all the same: zero. Am I wrong ?

Thank you!

Then this means the evaluation at 1 map is trivially the map which sends anything to 0, and reveals no information.

From: Quynh Dang (b) (6)
Sent: Monday, May 07, 2018 7:11 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>

Subject: Very urgent please help!

Hi Dustin,

I thought about the evaluation attack at 1 which we discussed last week. I realized that there are things that I don't understand, please see my discussion below.

On Thu, Apr 26, 2018 at 2:47 PM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

No.

On page 14 of their submission:

Current NTRU Classic specifications such as [32] prohibit m that have an unusually small number of 0's or 1's or -1's. For random m , this prohibition applies with probability $<2^{-10}$, and in case of failure the sender can try encoding the plaintext as a new m , but this is problematic for applications with hard real-time requirements. The reason for this prohibition is that NTRU Classic gives the attacker an "evaluate at 1" homomorphism from R/q to Z/q , leaking $m(1)$. The attacker scans many ciphertexts to find an occasional ciphertext where the value $m(1)$ is particularly far from 0; this value constrains the search space for the corresponding m by enough bits to raise security concerns. In NTRU Prime, R/q is a field, so this type of leak cannot occur.

The map $\phi: R/q \rightarrow Z/q$ is a ring homomorphism defined by evaluating at 1. The image of the map will be isomorphic to $(R/q) / (\ker \phi)$. We will be looking in the image of ϕ to see where $c(1)=m(1)$ is large. But if R/q is a field, then $\ker \phi = \{0\}$ or $\ker \phi = R/q$. We know the kernel has more than one element, since any message with an equal number of 1s and -1s will be in the kernel. Hence, we must have the kernel of ϕ is all of R/q . Then this means the evaluation at 1 map is trivially the map which sends anything to 1, and reveals no information.

The argument we had was that the kernel is R/q because R/q is a field (but the kernel in a field homomorphism is always $\{0\}$, but forget about this for now). Therefore, the image of the map ϕ is isomorphic to $R/q / R/q = \{0\}$. I don't understand what this really means. Does that mean that the image domain (ciphertexts evaluated at 1) is isomorphic to 0 in R/q which is only 1 element? I don't know what all mean here. (to make the map from 0 to the image isomorphic, the image must have only 1 element which is also zero, correct?)

And above, you said sends anything to 1: I don't understand this.

At the discussion, I thought that all ciphertext when evaluated at 1 will be zero. and the logic I used in my head turned out to be not correct or derivable from the fact that the image (ciphertexts when evaluated at 1) is isomorphic to $\{0\}$.

Now, I look at R/q to Z/q as field homomorphism, then the kernel must be $\{0\}$, then this is an injective mapping: every element in R/q maps to a unique element in Z/q (this element in Z/q is

mapped from only 1 element in R/q).

Maybe evaluation at 1, R/q to Z/q is not a field homomorphism ?

Thank you!

From: Quynh Dang (b) (6)
Sent: Thursday, April 26, 2018 2:40 PM

To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: a very large Galois group, so that the number field is very far from having automorphisms.

Are you coming in tomorrow ?

On Thu, Apr 26, 2018 at 2:37 PM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

This seems to be true for NTRUprime. I don't see where they claim the attack doesn't work.

From: Quynh Dang (b) (6)
Sent: Thursday, April 26, 2018 2:30 PM

To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: a very large Galois group, so that the number field is very far from having automorphisms.

Here is the attack: Ciphertext : $c = rh + m$.

Number of 1s = number of -1s in r , so $r(1) = 0$ which implies $c(1) = r(1)h(1) + m(1) = m(1)$ which reveals information about m . if $c(1)$ is a huge positive number which means there are way more 1s than -1s which means that in m there are way more 1s than -1s: this gives information about m .

Quynh.

On Thu, Apr 26, 2018 at 2:25 PM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

Write out the attack. Explain it to me....

From: Quynh Dang (b) (6)
Sent: Thursday, April 26, 2018 2:18 PM

To: Moody, Dustin (Fed) <dustin.moody@nist.gov>

Subject: Re: a very large Galois group, so that the number field is very far from having automorphisms.

Why not having subfield or subring stops that attack ?

Quynh.

On Thu, Apr 26, 2018 at 2:12 PM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

That it doesn't have subrings (i.e. subfields), except the trivial ones.

From: Quynh Dang (b) (6)

Sent: Thursday, April 26, 2018 2:11 PM

To: Moody, Dustin (Fed) <dustin.moody@nist.gov>

Subject: Re: a very large Galois group, so that the number field is very far from having automorphisms.

So, what actually stops the attack in NTRU prime ?

On Thu, Apr 26, 2018 at 2:09 PM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

Yes, it works on fields and rings. But it involves a subring....

From: Quynh Dang (b) (6)

Sent: Thursday, April 26, 2018 2:03 PM

To: Moody, Dustin (Fed) <dustin.moody@nist.gov>

Subject: Re: a very large Galois group, so that the number field is very far from having automorphisms.

Can you correct me below Dustin ?

On Thu, Apr 26, 2018 at 9:49 AM, Quynh Dang (b) (6) wrote:

Thank you Dustin.

Below is my understanding of the attack (wrong understanding).

Ciphertext : $c = rh + m$. Number of 1s = number of -1s in r , so $r(1) = 0$ which implies $c(1) = r(1)h(1) + m(1) = m(1)$

So, my wrong understanding is that the attack works for rings or fields.

Quynh.

On Thu, Apr 26, 2018 at 9:44 AM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

Quynh,

I don't understand the statement about having a very large Galois group means the number field is very far from having automorphisms. By definition, the Galois group elements are automorphisms. So a large Galois group would mean a lot of automorphisms. I've read the blog, but I still can't make sense of it.

I think that a field blocks the evaluation at 1 attacks because the attack works with a subring. For a field, the subring is either the entire field or just $\{1\}$, which isn't helpful. By the way $\phi_n(x) = (x^n - 1)/(x - 1) = x^{n-1} + x^{n-2} + \dots + x + 1$. This will be irreducible if n is prime. The fact that it is irreducible means when we do $\mathbb{Q}[x] / \phi_n(x)$ we get a field.

Dustin

From: Quynh Dang (b) (6)
Sent: Thursday, April 26, 2018 8:59 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: a very large Galois group, so that the number field is very far from having automorphisms.

Hi Dustin,

On a Dan's blog article: <https://blog.cr.yt.to/20140213-ideal.html>, he said that " and uses an irreducible polynomial $x^p - x - 1$ with a very large Galois group, so that the number field is very far from having automorphisms. " .

Why is this harder to find automorphisms if the Galois group is large ?

Why \mathbb{R}/\mathbb{q} (defined in NTRU prime) (a field instead of a ring) avoids evaluation at $m(1)$ attack ? The attack seems to work as long as the number of -1 and 1 coefficients are known in r (I think my understanding for the attack is wrong here) because Tanga claims that replacing $X^N - 1$ in the original NTRU with $(X^N - 1)/(x - 1)$ to avoid the attack.

If the claim is correct, my impression is that $(X^N - 1)/(x - 1)$ is irreducible (I dont know this is true or not). If this is true, why does it being irreducible avoids the attack ?

Thank you!
Quynh.

