From: Moody, Dustin (Fed)
To: (b) (6)
Subject: RE: a very large Galois group, so that the number field is very far from having automorphisms.
Date: Thursday, April 26, 2018 2:47:00 PM

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 -> 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 phi to see where c(1)=m(1) is large. But if R/q is a field, then ker phi =1 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 phi 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.

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) + … + x +1. This will be irreducible if n is prime. The fact that it is irreducible means when we do 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.yp.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 R/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.