From: D. J. Bernstein <djb@cr.yp.to>
Sent: Thursday, July 4, 2019 6:15 PM
To: pqc-comments
Cc: pqc-forum
Subject: OFFICIAL COMMENT: Three Bears
Attachments: signature.asc

http://nutmic2019.imj-prg.fr/confpapers/MultiCubic.pdf is a new attack paper that appeared at NutMiC 2019 last week. The point of this comment is that the attack undermines a December 2018 advertisement of a particular feature of Three Bears.

Context: https://blog.cr.yp.to/20140213-ideal.html introduced an attack strategy against the "prototypical ideal-lattice problem" for cyclotomic fields; stated an expectation that the attack strategy would take subexponential time in some cases; said that "there has not been adequate security evaluation of ideal lattices"; and recommended switching to the polynomial x^p-x-1, which has "a very large Galois group, so that the number field is very far from having automorphisms".

Subsequent work obtained a polynomial-time quantum attack against the same lattice problem for cyclotomic fields, under mild assumptions. This prompted further efforts to draw lines separating the broken systems, such as Gentry's original STOC 2009 FHE system, from other lattice systems. These lines vary in the extent to which they are based on analysis of attacks. These lines also vary in whether they have survived subsequent attacks.

The December 2018 advertisement mentioned above is the following:
"Q(alpha) for alpha a root of x^D - x^(D/2) - 1 (D >= 4) doesn't have nontrivial automorphisms". This isn't quite correct (see my email dated
4 Dec 2018 00:21:54 -0000) but it's close to correct. The line being drawn here is between

* degree-N number fields with N automorphisms ("Galois" number
  fields; the "Galois group" has size N, smallest possible) and

* degree-N number fields with far fewer automorphisms.

This line is similar to the 2014 NTRU Prime line in that it separates cyclotomics (Galois group of size N) from "random" number fields (Galois group of size N!---that's N factorial, vastly larger than N). But this line allows number fields with Galois groups of size not much larger than N, whereas the 2014 NTRU Prime line doesn't.

The new attack is against multicubic fields. A small example is the
degree-243 field

\Q(cbrt(2),cbrt(3),cbrt(5),cbrt(7),cbrt(11)).

This field is allowed by the December 2018 line, since it doesn't have any nontrivial automorphisms. (The field is real, so the only cube root of 2 in the field is cbrt(2), the only cube root of 3 in the field is cbrt(3), etc.) However, this field isn't allowed by the 2014 NTRU Prime line. The Galois group is of size only 486: the Galois closure is

\Q(zeta_3,cbrt(2),cbrt(3),cbrt(5),cbrt(7),cbrt(11))

where zeta_3 is a primitive cube root of 1. For comparison, most
degree-243 number fields have Galois groups of size

57651072073405564859932599378988824389544612769748785289578514753791

```
22666079544778795256178048966844061302891650347152224170364576799681
06951352262782967426376061151343007870529913194314123793125402307920
60250137088708811794424564833107085173464718985508999858791970609491
06604571187432151691815090541394478937715631520718699805559145167063
38987145677453868269366788405482256480899617278757054445381671428182
9286281216000000000000000000000000000000000000000000000000000000000.
```

Compared to our Eurocrypt 2017 attack https://eprint.iacr.org/2017/404 against multiquadratics (which are Galois), the new attack seems to have similar scalability, namely quasipolynomial for a wide range of fields.
This makes the December 2018 line untenable. The concrete performance seems to be somewhat worse since the new cube-root subroutine (using
LLL) is slower than our square-root subroutine, but this doesn't affect the quasipolynomial scalability.

The attack exploits the automorphisms of the Galois closure to obtain all the algebraic information it needs about the original field. This is a familiar strategy in computational algebraic number theory, and the high-level consequences were already spelled out in the NTRU Prime paper
https://eprint.iacr.org/2016/461.pdf:

> Prohibiting minimum size p is not the same as requiring maximum size p!; there is a large gap between p and p!. But having a Galois group of size, say, 2p means that one can write down a degree-2p extension field with 2p automorphisms, and one can then try to apply these automorphisms to build many units, generalizing the construction of cyclotomic units.

This also shows why the December 2018 line failed. Limiting the number of automorphisms of the original field doesn't stop the Galois closure from being small enough to make automorphism computations feasible. The
2014 NTRU Prime line directly addresses this.

---Dan

From: Mike Hamburg <mike@shiftleft.org>
Sent: Sunday, July 7, 2019 11:55 PM
To: D. J. Bernstein
Cc: pqc-comments; pqc-forum
Subject: Re: [pqc-forum] OFFICIAL COMMENT: Three Bears

Interesting. Please correct me if I'm wrong in this distilled application to ThreeBears and SNTRUP / NTRULPR themselves:

* ThreeBears uses an integer ring and not a polynomial ring, but the security is likely to be similar to that of a polynomial ring version, which we might call "poly-ThreeBears". This is provably true asymptotically, and is a reasonable conjecture for the concrete parameters.

* The poly-ThreeBears ring has fewer automorphisms than a cyclotomic field of the same size, but not a much larger Galois group.

* This new paper presents a new theoretical attack on poly-LWE. It's slower than the cyclotomic case (vs Gentry FHE and similar), but still conjecturally subexponential. It has no practical application on parameters in the ranges of the NIST systems, but it suggests a potential weakness in the field structure.

* The attacked fields look nothing like poly-ThreeBears' field, but interestingly they lack automorphisms. But the new paper's attack would be thwarted by a large Galois group. This puts a finer point on your argument last year that the Galois group is more important than the automorphisms, except maybe for low-order speedups from symmetry.

* In sum, this is evidence that SNTRUP and NTRULPR have advantages over cyclotomic LWE (in terms of less risk of unknown number theoretic attacks) that aren't enjoyed by poly-ThreeBears.

Is that right?
— Mike

>

From: D. J. Bernstein <djb@cr.yp.to>
Sent: Monday, July 8, 2019 5:45 AM
To: pqc-comments
Cc: pqc-forum
Subject: Re: [pqc-forum] OFFICIAL COMMENT: Three Bears
Attachments: signature.asc

Mike Hamburg writes:
> The attacked fields look nothing like poly-ThreeBears' field

You advertised your number field as having very few automorphisms (more precisely, exactly 1 automorphism, which was too optimistic):

```
   ... the field has no nontrivial automorphisms.  This is true both in
   the obvious sense that Z/NZ can't have nontrivial automorphisms, and
   also in that Q(alpha) for alpha a root of x^D - x^(D/2) - 1 (D >= 4)
   doesn't have nontrivial automorphisms.  Thanks to Hart Montgomery and
   Arnab Roy for pointing this out.
```

The multicubic fields in this new attack paper also have very few automorphisms. As I said, the attack undermines the advertisement of this feature of Three Bears.

It's weird that you choose to highlight a particular feature of field X but then, faced with an attack against field Y with the same feature, you claim that X looks "nothing like" Y. People who do the work to analyze the merits of a claimed feature shouldn't have to deal with the pretense that the feature wasn't claimed in the first place.

> This puts a finer point on your argument last year that the Galois
> group is more important than the automorphisms, except maybe for
> low-order speedups from symmetry.

Huh? The cyclotomic and multiquadratic cases are Galois. In such cases, the Galois group _is_ the set of automorphisms of the field: symmetries that preserve the field operations. These symmetries are at the heart of

   * a quantum polynomial-time attack (under mild assumptions) against
     Gentry's STOC 2009 FHE system for cyclotomics, a system that had
     exponential security (with Gentry's parameter choices) against all
     previous attacks; and

   * a non-quantum quasipolynomial-time attack against an analogous
     system for a wide range of multiquadratics, again where no other
     known attack strategies are better than exponential time.

These are not "low-order speedups". The symmetries are devastating.

For a designer who wants to stay away from these fields, the NTRU Prime answers are considerably older than "last year". In my previous message I quoted https://blog.cr.yp.to/20140213-ideal.html recommending "a very large Galois group, so that the number field is very far from having automorphisms". I also quoted
https://eprint.iacr.org/2016/461.pdf
saying

   Prohibiting minimum size p is not the same as requiring maximum size p!; there is a large gap between p and p!. But having a Galois group of size, say, 2p means that one can write down a degree-2p extension field with 2p automorphisms, and one can then try to apply these automorphisms to build many units, generalizing the construction of cyclotomic units.

This covers what happened in the new attack. Here's the updated chart showing how well Gentry's STOC 2009 FHE system is holding up for various number fields K with various Galois groups G:

* cyclotomics: #Aut K = n; #G = n; broken under mild assumptions
* multiquadratics: #Aut K = n; #G = n; broken under mild assumptions
* multicubics: #Aut K = 1; #G = 2n; broken under mild assumptions
* almost all fields: #Aut K = 1; #G = n! (n factorial); unbroken

You chose to advertise #Aut K being small for your number field K. This was before the multicubic attack but after the above 2014/2016 quotes.

> This new paper presents a new theoretical attack on poly-LWE.

The paper focuses on the problem of recovering short generators, as in Gentry's original STOC 2009 FHE system. I'd expect the underlying structure to allow, e.g., Ideal-SVP attacks analogous to CDW etc., but this is beyond the scope of this paper.

> It’s slower than the cyclotomic case (vs Gentry FHE and similar), but
> still conjecturally subexponential.

The new attack seems to have _quasipolynomial_ scalability for a wide range of multicubic fields, as I said before. Quasipolynomial implies subexponential but it's a much stronger statement.

Your comparison to cyclotomics is unjustified. CGS--Biasse--Song is a _quantum_ polynomial-time attack against cyclotomic Gentry (under mild assumptions). The multiquadratic and multicubic attacks are non-quantum attacks. Giving the attacker a quantum computer would change the costs:
e.g., the underlying quadratic and cubic unit groups can be computed in quantum polynomial time by EHKS.

> It has no practical application on parameters in the ranges of the
> NIST systems

For the problem targeted in the paper, a larger-scale academic attack should get easily to dimension 729 and maybe even 2187, without any improvements in the cube-root subroutine. If you're trying to say that it's a different problem, why are you talking about parameter sizes?

---Dan

From: Alperin-Sheriff, Jacob (Fed)
Sent: Monday, July 8, 2019 1:03 PM
To: D. J. Bernstein; pqc-comments
Cc: pqc-forum
Subject: Re: [pqc-forum] OFFICIAL COMMENT: Three Bears

Somewhat off topic, but I've wondered whether a field-switching analogue of modulus-switching is at all plausible (i.e. that doesn't screw up noise too badly).

i.e. given an (a,b=s*a+e (mod f(x)/qf(x))) can we switch to another polynomial g(x) of the same degree under any conditions?

a,b=s*a+e+i*f(x)+j*q,

switched to say,
a,b'=s*a+e'+k*g(x)+l*q,

where e' is not too much bigger than e

If something like that could work out this might kill the field fights mostly.

On 7/8/19, 5:45 AM, "D. J. Bernstein" <djb@cr.yp.to> wrote:

> Mike Hamburg writes:
> \> The attacked fields look nothing like poly-ThreeBears' field
>
> You advertised your number field as having very few automorphisms (more precisely, exactly 1 automorphism, which was too optimistic):
>
> > ... the field has no nontrivial automorphisms. This is true both in the obvious sense that Z/NZ can't have nontrivial automorphisms, and also in that Q(alpha) for alpha a root of x^D - x^(D/2) - 1 (D >= 4) doesn't have nontrivial automorphisms. Thanks to Hart Montgomery and Arnab Roy for pointing this out.
>
> The multicubic fields in this new attack paper also have very few automorphisms. As I said, the attack undermines the advertisement of this feature of Three Bears.
>
> It's weird that you choose to highlight a particular feature of field X but then, faced with an attack against field Y with the same feature, you claim that X looks "nothing like" Y. People who do the work to analyze the merits of a claimed feature shouldn't have to deal with the pretense that the feature wasn't claimed in the first place.
>
> \> This puts a finer point on your argument last year that the Galois
> \> group is more important than the automorphisms, except maybe for
> \> low-order speedups from symmetry.

From: Mike Hamburg <mike@shiftleft.org>
Sent: Monday, July 8, 2019 2:27 PM
To: D. J. Bernstein
Cc: pqc-comments; pqc-forum
Subject: Re: [pqc-forum] OFFICIAL COMMENT: Three Bears

Thanks for the corrections, Dan.

> On Jul 8, 2019, at 2:45 AM, D. J. Bernstein <djb@cr.yp.to> wrote:
>
> Mike Hamburg writes:
>> The attacked fields look nothing like poly-ThreeBears' field
>
> You advertised your number field as having very few automorphisms
> (more precisely, exactly 1 automorphism, which was too optimistic):
>
>   ... the field has no nontrivial automorphisms. This is true both in
>   the obvious sense that Z/NZ can't have nontrivial automorphisms, and
>   also in that Q(alpha) for alpha a root of x^D - x^(D/2) - 1 (D >= 4)
>   doesn't have nontrivial automorphisms. Thanks to Hart Montgomery and
>   Arnab Roy for pointing this out.
>
> The multicubic fields in this new attack paper also have very few
> automorphisms. As I said, the attack undermines the advertisement of
> this feature of Three Bears.
>
> It's weird that you choose to highlight a particular feature of field
> X but then, faced with an attack against field Y with the same
> feature, you claim that X looks "nothing like" Y. People who do the
> work to analyze the merits of a claimed feature shouldn't have to deal
> with the pretense that the feature wasn't claimed in the first place.

You put considerable weight on my "advertising" and "highlighting" the small number of automorphisms for ThreeBears. This misrepresents the history of that statement. Recall that this was in the context of a December 2018 thread on the NTRU merger. In that thread, you claimed "avoid[ing] nontrivial number-field automorphisms" as a security feature of NTRU Prime. To reiterate, it was you and not I who claimed that this is a security feature. In the same email you also wrote:

> There are several other lattice submissions that can protect against
> the possibility of cyclotomics being broken, but NTRU Prime is by far
> the most efficient. Here are representative examples of public-key
> size + ciphertext size in non-cyclotomic options in lattice submissions:
>
> [table not containing ThreeBears]
>
> NTRU Prime is the only lattice submission that eliminates cyclotomic
> structure while still fitting each public key and each ciphertext into
> the guaranteed IPv6 MTU, 1280 bytes.

I responded to these claims in a different thread, quoting your claims, because it wasn't about the NTRU merger anymore. I wrote:

From:	D. J. Bernstein <djb@cr.yp.to>
Sent:	Tuesday, July 9, 2019 4:57 AM
To:	pqc-comments
Cc:	pqc-forum
Subject:	Re: [pqc-forum] OFFICIAL COMMENT: Three Bears
Attachments:	signature.asc

Mike Hamburg writes:

> In that thread, you claimed “avoid[ing] nontrivial number-field
> automorphisms” as a security feature of NTRU Prime.

The same message then explains in detail that this means switching "from a cyclotomic field to a number field with a large Galois group, so that automorphism computations are hard". The criteria are the same as in the 2014 blog post, the 2016 NTRU Prime paper, etc. Three Bears does not satisfy the criteria: a degree-n Three Bears number field has Galois group of size only O(n^2).

You're confusing the NTRU Prime criteria with weaker criteria that

* don't force the Galois group to be much larger than the degree,
* don't force automorphism computations to be hard, and
* don't avoid automorphisms in any meaningful sense.

The fact that the criteria are different is already clear from the definitions of the words in
https://blog.cr.yp.to/20140213-ideal.html
("a very large Galois group"). The importance of these differences was explained in more detail in the NTRU Prime paper in 2016, and is nicely illustrated by the new multicubic attack.

> As I understand it, the thrust of your new comment is that one of
> these features (originally claimed as a security feature of NTRU
> Prime, but also present in ThreeBears) doesn’t provide evidence of security.

The NTRU Prime security criteria are the same as they were in 2014. The subsequent development of attacks has added weight to the criteria, and has added weight to the corresponding criticism of weaker criteria. Your fabrication of a retreat in the security criteria comes entirely from your own misreading of the criteria.

---Dan (speaking for myself)

--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/20190709085705.3259.qmail%40cr.yp.to.

From: Mike Hamburg <mike@shiftleft.org>
Sent: Tuesday, July 9, 2019 12:16 PM
To: D. J. Bernstein
Cc: pqc-comments; pqc-forum
Subject: Re: [pqc-forum] OFFICIAL COMMENT: Three Bears

> On Jul 9, 2019, at 1:57 AM, D. J. Bernstein <djb@cr.yp.to> wrote:
>
> Mike Hamburg writes:
>> In that thread, you claimed “avoid[ing] nontrivial number-field
>> automorphisms” as a security feature of NTRU Prime.
>
> The same message then explains in detail that this means switching
> "from a cyclotomic field to a number field with a large Galois group,
> so that automorphism computations are hard". The criteria are the same
> as in the
> 2014 blog post, the 2016 NTRU Prime paper, etc. Three Bears does not
> satisfy the criteria: a degree-n Three Bears number field has Galois
> group of size only O(n^2).

Yes, just as you said in response to my message in 2018. So I think we’re on the same page here.

— Mike

From: Mike Hamburg <mike@shiftleft.org>
Sent: Thursday, July 25, 2019 1:57 PM
To: pqc-comments
Cc: pqc-forum
Subject: [pqc-forum] ROUND 2 OFFICIAL COMMENT: Three Bears

Hello PQC forum,

This comment provides a mid-2nd-round update for ThreeBears. I have made the following significant changes to the spec:

* Implicit rejection is now mandatory.

* The implicit rejection PRF key is now 40 bytes instead of 32, so that it has the same resistance to multi-target attacks as other parts of the private key.

I have also made less-significant changes:

* Updated benchmarks for implicit rejection. Decaps is about 10% slower. Since the FO mode is still $U^{\not\bot}_m$, encaps time is unaffected. M4 benchmarks are slightly faster, probably because PQM4's Keccak got faster.

* Explanation for the choice of implicit rejection mode $U^{\not\bot}_m$.

* Introduction of new toy scheme "GummyBear" with 120-dimensional ring, which is intended to be broken to test attack algorithms. The earlier toy variant, TeddyBear, was probably too strong for this purpose.

* Introduction of a new pair of toy schemes "Koala" and "KoalaEphem". These are mockups of a lightweight variant of ThreeBears, which is around 128-bits classically secure (Class 1) or perhaps slightly less.

The new spec is available at https://www.shiftleft.org/papers/threebears/threebears-spec.pdf

I have also submitted new code to SUPERCOP for benchmarking. I also intend to submit it to libpqcrypto and possibly some other collections. This software is available at:

https://www.shiftleft.org/upload/threebears_libpqcrypto.tgz

If you want to tinker with the code or integrate it elsewhere, the more useful original source is available at:

https://sourceforge.net/p/threebears/code/ci/master/tree/

Both sets of software include ThreeBears proper, plus a caching variant designed to make speed comparisons more accurate. The normal ThreeBears software follows the spec, and stores its private key as a 40-byte seed, which I believe is the right approach for most long-term keys. However, many proposed PQ systems store the expanded private key instead, so they don't have to re-expand it on decapsulation. The caching version of the ThreeBears software stores the expanded form of the private key. It stores the same expanded terms as Kyber and Saber, i.e. the private noise and public key but not the matrix.

Cheers,
— Mike
--
You received this message because you are subscribed to the Google Groups "pqc-forum" group.
To unsubscribe from this group and stop receiving emails from it, send an email to pqc-forum+unsubscribe@list.nist.gov.
To view this discussion on the web visit https://groups.google.com/a/list.nist.gov/d/msgid/pqc-forum/2CEC17AC-8611-46A1-BA37-62AE6483B133%40shiftleft.org.