From: Fatima ASEBRIY <fatima.asebriy@gmail.com> via pqc-forum@list.nist.gov
To: pqc-forum <pqc-forum@list.nist.gov>
CC: cpei...@alum.mit.edu <cpeikert@alum.mit.edu>
Subject: [pqc-forum] Re: Is there enough cryptanalysis of "small rounding"?
Date: Tuesday, October 25, 2022 06:26:02 PM ET

hello
why saber is not selected among the candidates of round 4 (nist)
Le vendredi 3 décembre 2021 à 20:44:39 UTC+1, cpei...@alum.mit.edu a écrit :

> Summary:
>
> - Multiple remaining NISTPQC lattice KEM proposals rely entirely on "small (deterministic) rounding," rather than random errors, for their security.
> - This approach is relatively new -- especially the "small" aspect -- but it has received much less public attention compared to other aspects of lattice KEM designs.
> - Known proofs don't come close to applying to the KEMs' small rounding. Moreover, other proof techniques that give important insights about random errors don't apply to (small) rounding. That leaves cryptanalysis as our only real basis for confidence.
> - So, I ask: what (quantum) cryptanalytic effort has been devoted specifically to small rounding? Does it give enough confidence to use it as the foundation of a long-term PQC standard?
>   - From what I can tell, there has been little specific effort -- the existing analyses essentially "assume away" any potential difference between deterministic rounding errors and random ones. Maybe this is a valid heuristic, but how well has it been tested? Are there other analyses that don't rely on this heuristic?
>   - Perhaps people have made serious attempts at other types of attacks that weren't shared publicly. It would be good to know what has (and hasn't) been tried -- even/especially if it didn't amount to anything.
>
> All lattice-based encryption/KEM schemes rely on adding some kind of "error" for security. Without such error, the schemes would be trivially breakable.
>
> Ten years ago, coauthors and I proposed the idea of using *deterministic* "rounding error" instead of *random* error in lattice-based constructions. This yields the "with rounding" family of problems, like Learning With Rounding (over Rings/Modules) etc.
> The main idea is simple: in order to add error to an integer, just round it to the nearest multiple of some fixed integer p. This can be seen as adding some "deterministic error" in

the range [-p/2, p/2]. And since the result r is a multiple of p, we can instead work with r/p. So, this rounding effectively "drops" the least-significant log_2(p) bits of the input.

While we and others managed to prove some things about the hardness of "with rounding" problems, the proofs require much more rounding than what the NISTPQC KEMs do.

More specifically, two KEMs rely entirely on *small* rounding for their security:

1. SABER (a finalist) drops 3-7 bits of each integer coefficient.
2. NTRU Prime (an alternate) rounds to the nearest multiple of 3, effectively dropping just log_2(3) < 1.6 bits per coefficient.

(In addition, finalist Kyber uses random error, then also does some rounding for compression; both forms of error are accounted for in the security analysis.)

This is much less rounding than what was originally considered. For example, our work showed that dropping 100+b bits is at least as secure as using random error of about b bits (for a statistical security parameter of about 100).

Of course, 100+b is much more than 3 or 1.6, so this proof is far very from applying to the KEMs' small rounding. Later works somewhat reduced the "100" in certain contexts, but not to anything close to what the KEMs use.

Moreover, several other proof techniques that provide insights about random errors do not appear to translate to deterministic rounding, especially with rings/modules (as used by the KEMs). These include the safety of using a small "secret" drawn from the error distribution; sample-preserving search-to-decision reductions; and the quantum reduction that says "solving BDD with random errors implies finding short (dual) lattice vectors".

Since known proofs tell us very little about small rounding, that leaves cryptanalysis as our only basis for evaluating its security. What has been tried? How much confidence should we have?

The analyses I've seen just heuristically model rounding error as being "random-ish" in the rounding range, then proceed with the usual kinds of lattice analyses (Core-SVP and the like).

This heuristic is plausible, but it "assumes away" any potential distinction between random and deterministic error from the outset. In other words, if there is any significant difference in security between the two kinds of error, the heuristic completely conceals it.

> Therefore, I would like to ask the following questions of the community:
>
> - Is there any significant security gap between rounding and "same sized" random errors?
> - How well has the heuristic been tested, experimentally and analytically, for known lattice attacks?
> - Has anyone tried to develop other kinds of (quantum) attacks that specifically exploit small rounding -- including with small secrets, and over rings/modules? If so, and the attempts didn't work out, what were the obstructions? If not, how much confidence should we have in small rounding?
>
> Sincerely yours in cryptography,
>
> Chris

--
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/94ca256e-3dc7-4b72-8cc3-954c8cead988n%40list.nist.gov.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov> via pqc-forum <pqc-forum@list.nist.gov>
To: Fatima ASEBRIY <fatima.asebriy@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
CC: cpei...@alum.mit.edu <cpeikert@alum.mit.edu>
Subject: Re: [pqc-forum] Re: Is there enough cryptanalysis of "small rounding"?
Date: Tuesday, October 25, 2022 09:54:10 PM ET

Please see NISTIR 8413: Status Report on the 3rd Round of the NIST PQC Standardization Process

https://doi.org/10.6028/NIST.IR.8413-upd1.

In particular see Section 4.3.4, which explains our decision regarding Saber.

Dustin Moody

NIST

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of Fatima ASEBRIY <fatima.asebriy@gmail.com>
Sent: Tuesday, October 25, 2022 6:25 PM
To: pqc-forum <pqc-forum@list.nist.gov>
Cc: cpei...@alum.mit.edu <cpeikert@alum.mit.edu>
Subject: [pqc-forum] Re: Is there enough cryptanalysis of "small rounding"?

hello
why saber is not selected among the candidates of round 4 (nist)
Le vendredi 3 décembre 2021 à 20:44:39 UTC+1, cpei...@alum.mit.edu a écrit :

> Summary:
>
> - Multiple remaining NISTPQC lattice KEM proposals rely entirely on "small (deterministic) rounding," rather than random errors, for their security.
> - This approach is relatively new -- especially the "small" aspect -- but it has received much less public attention compared to other aspects of lattice KEM designs.
> - Known proofs don't come close to applying to the KEMs' small rounding. Moreover, other proof techniques that give important insights about random errors don't apply to (small) rounding. That leaves cryptanalysis as our only real basis for confidence.

- So, I ask: what (quantum) cryptanalytic effort has been devoted specifically to small rounding? Does it give enough confidence to use it as the foundation of a long-term PQC standard?
    - From what I can tell, there has been little specific effort -- the existing analyses essentially "assume away" any potential difference between deterministic rounding errors and random ones. Maybe this is a valid heuristic, but how well has it been tested? Are there other analyses that don't rely on this heuristic?
    - Perhaps people have made serious attempts at other types of attacks that weren't shared publicly. It would be good to know what has (and hasn't) been tried -- even/especially if it didn't amount to anything.

All lattice-based encryption/KEM schemes rely on adding some kind of "error" for security. Without such error, the schemes would be trivially breakable.

Ten years ago, coauthors and I proposed the idea of using *deterministic* "rounding error" instead of *random* error in lattice-based constructions. This yields the "with rounding" family of problems, like Learning With Rounding (over Rings/Modules) etc.
The main idea is simple: in order to add error to an integer, just round it to the nearest multiple of some fixed integer p. This can be seen as adding some "deterministic error" in the range [-p/2, p/2]. And since the result r is a multiple of p, we can instead work with r/p. So, this rounding effectively "drops" the least-significant log_2(p) bits of the input.

While we and others managed to prove some things about the hardness of "with rounding" problems, the proofs require much more rounding than what the NISTPQC KEMs do.

More specifically, two KEMs rely entirely on *small* rounding for their security:

1. SABER (a finalist) drops 3-7 bits of each integer coefficient.
2. NTRU Prime (an alternate) rounds to the nearest multiple of 3, effectively dropping just log_2(3) < 1.6 bits per coefficient.

(In addition, finalist Kyber uses random error, then also does some rounding for compression; both forms of error are accounted for in the security analysis.)

This is much less rounding than what was originally considered. For example, our work showed that dropping 100+b bits is at least as secure as using random error of about b bits (for a statistical security parameter of about 100).

> Of course, 100+b is much more than 3 or 1.6, so this proof is far very from applying to the KEMs' small rounding. Later works somewhat reduced the "100" in certain contexts, but not to anything close to what the KEMs use.
>
> Moreover, several other proof techniques that provide insights about random errors do not appear to translate to deterministic rounding, especially with rings/modules (as used by the KEMs). These include the safety of using a small "secret" drawn from the error distribution; sample-preserving search-to-decision reductions; and the quantum reduction that says "solving BDD with random errors implies finding short (dual) lattice vectors".
>
> Since known proofs tell us very little about small rounding, that leaves cryptanalysis as our only basis for evaluating its security. What has been tried? How much confidence should we have?
>
> The analyses I've seen just heuristically model rounding error as being "random-ish" in the rounding range, then proceed with the usual kinds of lattice analyses (Core-SVP and the like).
>
> This heuristic is plausible, but it "assumes away" any potential distinction between random and deterministic error from the outset. In other words, if there is any significant difference in security between the two kinds of error, the heuristic completely conceals it.
>
> Therefore, I would like to ask the following questions of the community:
>
> - Is there any significant security gap between rounding and "same sized" random errors?
> - How well has the heuristic been tested, experimentally and analytically, for known lattice attacks?
> - Has anyone tried to develop other kinds of (quantum) attacks that specifically exploit small rounding -- including with small secrets, and over rings/modules? If so, and the attempts didn't work out, what were the obstructions? If not, how much confidence should we have in small rounding?
>
> Sincerely yours in cryptography,
>
> Chris

--

You received this message because you are subscribed to the Google Groups "pqc-forum" group.

From: fei 123 <feiphung@gmail.com> via pqc-forum@list.nist.gov
To: Fatima ASEBRIY <fatima.asebriy@gmail.com>
CC: pqc-forum <pqc-forum@list.nist.gov>, cpei...@alum.mit.edu <cpeikert@alum.mit.edu>
Subject: Re: [pqc-forum] Re: Is there enough cryptanalysis of "small rounding"?
Date: Wednesday, October 26, 2022 04:51:40 PM ET

Hi Dustin Moody,

For Saber, I am a bit confused with the statement "The disadvantage of power of 2 moduli is that they do not allow an NTT implementation of polynomial multiplication." ?

Hi Chris,

> Moreover, several other proof techniques that provide insights about random errors do not appear to translate to deterministic rounding, especially with rings/modules (as used by the KEMs). These include the safety of using a small "secret" drawn from the error distribution; sample-preserving search-to-decision reductions; and the quantum reduction that says "solving BDD with random errors implies finding short (dual) lattice vectors".

What do you exactly mean by "solving BDD with random errors implies finding short (dual) lattice vectors" ?

On Wed, Oct 26, 2022 at 6:25 AM Fatima ASEBRIY <fatima.asebriy@gmail.com> wrote:

> hello
> why saber is not selected among the candidates of round 4 (nist)
> Le vendredi 3 décembre 2021 à 20:44:39 UTC+1, cpei...@alum.mit.edu a écrit :
>
>> Summary:
>>
>> - Multiple remaining NISTPQC lattice KEM proposals rely entirely on "small (deterministic) rounding," rather than random errors, for their security.
>> - This approach is relatively new -- especially the "small" aspect -- but it has received much less public attention compared to other aspects of lattice KEM designs.
>> - Known proofs don't come close to applying to the KEMs' small rounding. Moreover, other proof techniques that give important insights about random errors don't

> > apply to (small) rounding. That leaves cryptanalysis as our only real basis for confidence.
> >
> > - So, I ask: what (quantum) cryptanalytic effort has been devoted specifically to small rounding? Does it give enough confidence to use it as the foundation of a long-term PQC standard?
> >   - From what I can tell, there has been little specific effort -- the existing analyses essentially "assume away" any potential difference between deterministic rounding errors and random ones. Maybe this is a valid heuristic, but how well has it been tested? Are there other analyses that don't rely on this heuristic?
> >   - Perhaps people have made serious attempts at other types of attacks that weren't shared publicly. It would be good to know what has (and hasn't) been tried -- even/especially if it didn't amount to anything.
> >
> > All lattice-based encryption/KEM schemes rely on adding some kind of "error" for security. Without such error, the schemes would be trivially breakable.
> >
> > Ten years ago, coauthors and I proposed the idea of using *deterministic* "rounding error" instead of *random* error in lattice-based constructions. This yields the "with rounding" family of problems, like Learning With Rounding (over Rings/Modules) etc.
> > The main idea is simple: in order to add error to an integer, just round it to the nearest multiple of some fixed integer p. This can be seen as adding some "deterministic error" in the range [-p/2, p/2]. And since the result r is a multiple of p, we can instead work with r/p. So, this rounding effectively "drops" the least-significant log_2(p) bits of the input.
> >
> > While we and others managed to prove some things about the hardness of "with rounding" problems, the proofs require much more rounding than what the NISTPQC KEMs do.
> >
> > More specifically, two KEMs rely entirely on *small* rounding for their security:
> >
> > 1. SABER (a finalist) drops 3-7 bits of each integer coefficient.
> > 2. NTRU Prime (an alternate) rounds to the nearest multiple of 3, effectively dropping just log_2(3) < 1.6 bits per coefficient.
> >
> > (In addition, finalist Kyber uses random error, then also does some rounding for compression; both forms of error are accounted for in the security analysis.)
> >
> > This is much less rounding than what was originally considered. For example, our work showed that dropping 100+b bits is at least as secure as using random error of about b bits (for a statistical security parameter of about 100).

> > Of course, 100+b is much more than 3 or 1.6, so this proof is far very from applying to the KEMs' small rounding. Later works somewhat reduced the "100" in certain contexts, but not to anything close to what the KEMs use.
> >
> > Moreover, several other proof techniques that provide insights about random errors do not appear to translate to deterministic rounding, especially with rings/modules (as used by the KEMs). These include the safety of using a small "secret" drawn from the error distribution; sample-preserving search-to-decision reductions; and the quantum reduction that says "solving BDD with random errors implies finding short (dual) lattice vectors".
> >
> > Since known proofs tell us very little about small rounding, that leaves cryptanalysis as our only basis for evaluating its security. What has been tried? How much confidence should we have?
> >
> > The analyses I've seen just heuristically model rounding error as being "random-ish" in the rounding range, then proceed with the usual kinds of lattice analyses (Core-SVP and the like).
> >
> > This heuristic is plausible, but it "assumes away" any potential distinction between random and deterministic error from the outset. In other words, if there is any significant difference in security between the two kinds of error, the heuristic completely conceals it.
> >
> > Therefore, I would like to ask the following questions of the community:
> >
> > - Is there any significant security gap between rounding and "same sized" random errors?
> > - How well has the heuristic been tested, experimentally and analytically, for known lattice attacks?
> > - Has anyone tried to develop other kinds of (quantum) attacks that specifically exploit small rounding -- including with small secrets, and over rings/modules? If so, and the attempts didn't work out, what were the obstructions? If not, how much confidence should we have in small rounding?
> >
> > Sincerely yours in cryptography,
> >
> > Chris
>
> --
>
> 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/94ca256e-3dc7-4b72-8cc3-954c8cead988n%40list.nist.gov.

--

From: Christopher J Peikert <cpeikert@alum.mit.edu> via pqc-forum@list.nist.gov
To: fei 123 <feiphung@gmail.com>
CC: Fatima ASEBRIY <fatima.asebriy@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Is there enough cryptanalysis of "small rounding"?
Date: Wednesday, October 26, 2022 05:27:27 PM ET

On Wed, Oct 26, 2022 at 4:51 PM fei 123 <feiphung@gmail.com> wrote:

> Hi Chris,
>
> > Moreover, several other proof techniques that provide insights about random errors do not appear to translate to deterministic rounding, especially with rings/modules (as used by the KEMs). These include the safety of using a small "secret" drawn from the error distribution; sample-preserving search-to-decision reductions; and the quantum reduction that says "solving BDD with random errors implies finding short (dual) lattice vectors".
>
> What do you exactly mean by "solving BDD with random errors implies finding short (dual) lattice vectors" ?

Hi, I mean the "from [BDD] to samples" part of Regev's paper on LWE, Section 3.2.2. (He calls the problem CVP, but it has since come to be called BDD to emphasize the distance guarantee, which CVP does not have.) It can also be combined with Section 3 of this paper, when considering random BDD errors.

Sincerely your in cryptography,

Chris

--
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/CACOo0QgMYanMN6jQ54G1f9TVb98h5TNJyuXT-rYD779m3_PAEA%40mail.gmail.com.

From: Daniel Apon <dapon.crypto@gmail.com> via pqc-forum@list.nist.gov
To: fei 123 <feiphung@gmail.com>
CC: Fatima ASEBRIY <fatima.asebriy@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, cpei...@alum.mit.edu <cpeikert@alum.mit.edu>
Subject: Re: [pqc-forum] Re: Is there enough cryptanalysis of "small rounding"?
Date: Wednesday, October 26, 2022 05:29:30 PM ET

Hello fei 123,

You wrote: "*For Saber, I am a bit confused with the statement "The disadvantage of power of 2 moduli is that they do not allow an NTT implementation of polynomial multiplication." ?*"

The Number Theoretic Transform (NTT) is an algorithm. The NTT is an exact-arithmetic version of the (otherwise, complex-valued) FFT used in cryptographic applications. The Fast Fourier Transform (FFT) is an algorithm for evaluating the traditional Discrete Fourier Transform (DFT). The development of fast algorithms for the DFT can be traced to Gauss's work in 1805, but the first published version was in 1965 by James Cooley (an IBM Researcher) and John Tukey (who invented the term "bit" in 1947 at Bell Labs).

The NTT is sometimes used to compute polynomial multiplications much more efficiently than otherwise. For example, the NTT is used in Kyber. The algorithm requires certain properties on the modulus -- in particular, the choice of a specific prime integer-modulus (not a power -f-2 integer-modulus).

Best regards,
--Daniel Apon

On Wed, Oct 26, 2022 at 4:51 PM fei 123 <feiphung@gmail.com> wrote:

> Hi Dustin Moody,
>
> For Saber, I am a bit confused with the statement "The disadvantage of power of 2 moduli is that they do not allow an NTT implementation of polynomial multiplication." ?
>
> Hi Chris,

> > Moreover, several other proof techniques that provide insights about random errors do not appear to translate to deterministic rounding, especially with rings/modules (as used by the KEMs). These include the safety of using a small "secret" drawn from the error distribution; sample-preserving search-to-decision reductions; and the quantum reduction that says "solving BDD with random errors implies finding short (dual) lattice vectors".
>
> What do you exactly mean by "solving BDD with random errors implies finding short (dual) lattice vectors" ?
>
> On Wed, Oct 26, 2022 at 6:25 AM Fatima ASEBRIY <fatima.asebriy@gmail.com> wrote:
>
> > hello
> > why saber is not selected among the candidates of round 4 (nist)
> > Le vendredi 3 décembre 2021 à 20:44:39 UTC+1, cpei...@alum.mit.edu a écrit :
> >
> > > Summary:
> > >
> > > - Multiple remaining NISTPQC lattice KEM proposals rely entirely on "small (deterministic) rounding," rather than random errors, for their security.
> > > - This approach is relatively new -- especially the "small" aspect -- but it has received much less public attention compared to other aspects of lattice KEM designs.
> > > - Known proofs don't come close to applying to the KEMs' small rounding. Moreover, other proof techniques that give important insights about random errors don't apply to (small) rounding. That leaves cryptanalysis as our only real basis for confidence.
> > > - So, I ask: what (quantum) cryptanalytic effort has been devoted specifically to small rounding? Does it give enough confidence to use it as the foundation of a long-term PQC standard?
> > >   - From what I can tell, there has been little specific effort -- the existing analyses essentially "assume away" any potential difference between deterministic rounding errors and random ones. Maybe this is a valid heuristic, but how well has it been tested? Are there other analyses that don't rely on this heuristic?
> > >   - Perhaps people have made serious attempts at other types of attacks that weren't shared publicly. It would be good to know what has (and hasn't) been tried -- even/especially if it didn't amount to anything.

> > > All lattice-based encryption/KEM schemes rely on adding some kind of "error" for security. Without such error, the schemes would be trivially breakable.
> > >
> > > Ten years ago, coauthors and I proposed the idea of using *deterministic* "rounding error" instead of *random* error in lattice-based constructions. This yields the "with rounding" family of problems, like Learning With Rounding (over Rings/Modules) etc. The main idea is simple: in order to add error to an integer, just round it to the nearest multiple of some fixed integer p. This can be seen as adding some "deterministic error" in the range [-p/2, p/2]. And since the result r is a multiple of p, we can instead work with r/p. So, this rounding effectively "drops" the least-significant log_2(p) bits of the input.
> > >
> > > While we and others managed to prove some things about the hardness of "with rounding" problems, the proofs require much more rounding than what the NISTPQC KEMs do.
> > >
> > > More specifically, two KEMs rely entirely on *small* rounding for their security:
> > >
> > > 1. SABER (a finalist) drops 3-7 bits of each integer coefficient.
> > > 2. NTRU Prime (an alternate) rounds to the nearest multiple of 3, effectively dropping just log_2(3) < 1.6 bits per coefficient.
> > >
> > > (In addition, finalist Kyber uses random error, then also does some rounding for compression; both forms of error are accounted for in the security analysis.)
> > >
> > > This is much less rounding than what was originally considered. For example, our work showed that dropping 100+b bits is at least as secure as using random error of about b bits (for a statistical security parameter of about 100).
> > >
> > > Of course, 100+b is much more than 3 or 1.6, so this proof is far very from applying to the KEMs' small rounding. Later works somewhat reduced the "100" in certain contexts, but not to anything close to what the KEMs use.
> > >
> > > Moreover, several other proof techniques that provide insights about random errors do not appear to translate to deterministic rounding, especially with rings/modules (as used by the KEMs). These include the safety of using a small "secret" drawn from the error distribution; sample-preserving search-to-decision reductions; and the quantum reduction that says "solving BDD with random errors implies finding short (dual) lattice vectors".

>>> Since known proofs tell us very little about small rounding, that leaves cryptanalysis as our only basis for evaluating its security. What has been tried? How much confidence should we have?
>>>
>>> The analyses I've seen just heuristically model rounding error as being "random-ish" in the rounding range, then proceed with the usual kinds of lattice analyses (Core-SVP and the like).
>>>
>>> This heuristic is plausible, but it "assumes away" any potential distinction between random and deterministic error from the outset. In other words, if there is any significant difference in security between the two kinds of error, the heuristic completely conceals it.
>>>
>>> Therefore, I would like to ask the following questions of the community:
>>>
>>> - Is there any significant security gap between rounding and "same sized" random errors?
>>> - How well has the heuristic been tested, experimentally and analytically, for known lattice attacks?
>>> - Has anyone tried to develop other kinds of (quantum) attacks that specifically exploit small rounding -- including with small secrets, and over rings/modules? If so, and the attempts didn't work out, what were the obstructions? If not, how much confidence should we have in small rounding?
>>>
>>> Sincerely yours in cryptography,
>>>
>>> Chris
>>
>> --
>> 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/94ca256e-3dc7-4b72-8cc3-954c8cead988n%40list.nist.gov.
>
> --
> 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/CAMqF0n7Y7WhrtWFSUxUb5dSOnYTsfwL4emWp%2BL9CC_nRB712VA%40mail.gmail.com.

--

From: Daniel Apon <dapon.crypto@gmail.com> via pqc-forum@list.nist.gov
To: fei 123 <feiphung@gmail.com>
CC: Fatima ASEBRIY <fatima.asebriy@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, cpei...@alum.mit.edu <cpeikert@alum.mit.edu>
Subject: Re: [pqc-forum] Re: Is there enough cryptanalysis of "small rounding"?
Date: Wednesday, October 26, 2022 05:30:38 PM ET

Typo:

" power -f-2 integer-modulus" => " power-of-2 integer-modulus"

On Wed, Oct 26, 2022 at 5:28 PM Daniel Apon <dapon.crypto@gmail.com> wrote:

> Hello fei 123,
>
> You wrote: "*For Saber, I am a bit confused with the statement "The disadvantage of power of 2 moduli is that they do not allow an NTT implementation of polynomial multiplication." ?*"
>
> The Number Theoretic Transform (NTT) is an algorithm. The NTT is an exact-arithmetic version of the (otherwise, complex-valued) FFT used in cryptographic applications. The Fast Fourier Transform (FFT) is an algorithm for evaluating the traditional Discrete Fourier Transform (DFT). The development of fast algorithms for the DFT can be traced to Gauss's work in 1805, but the first published version was in 1965 by James Cooley (an IBM Researcher) and John Tukey (who invented the term "bit" in 1947 at Bell Labs).
>
> The NTT is sometimes used to compute polynomial multiplications much more efficiently than otherwise. For example, the NTT is used in Kyber. The algorithm requires certain properties on the modulus -- in particular, the choice of a specific prime integer-modulus (not a power -f-2 integer-modulus).
>
> Best regards,
> --Daniel Apon
>
> On Wed, Oct 26, 2022 at 4:51 PM fei 123 <feiphung@gmail.com> wrote:
>
> > Hi Dustin Moody,

> > For Saber, I am a bit confused with the statement "The disadvantage of power of 2 moduli is that they do not allow an NTT implementation of polynomial multiplication." ?
> >
> > Hi Chris,
> >
> > > Moreover, several other proof techniques that provide insights about random errors do not appear to translate to deterministic rounding, especially with rings/modules (as used by the KEMs). These include the safety of using a small "secret" drawn from the error distribution; sample-preserving search-to-decision reductions; and the quantum reduction that says "solving BDD with random errors implies finding short (dual) lattice vectors".
> >
> > What do you exactly mean by "solving BDD with random errors implies finding short (dual) lattice vectors" ?
> >
> > On Wed, Oct 26, 2022 at 6:25 AM Fatima ASEBRIY <fatima.asebriy@gmail.com> wrote:
> >
> > > hello
> > > why saber is not selected among the candidates of round 4 (nist)
> > > Le vendredi 3 décembre 2021 à 20:44:39 UTC+1, cpei...@alum.mit.edu a écrit :
> > >
> > > > Summary:
> > > >
> > > > - Multiple remaining NISTPQC lattice KEM proposals rely entirely on "small (deterministic) rounding," rather than random errors, for their security.
> > > > - This approach is relatively new -- especially the "small" aspect -- but it has received much less public attention compared to other aspects of lattice KEM designs.
> > > > - Known proofs don't come close to applying to the KEMs' small rounding. Moreover, other proof techniques that give important insights about random errors don't apply to (small) rounding. That leaves cryptanalysis as our only real basis for confidence.
> > > > - So, I ask: what (quantum) cryptanalytic effort has been devoted specifically to small rounding? Does it give enough confidence to use it as the foundation of a long-term PQC standard?
> > > >   - From what I can tell, there has been little specific effort -- the existing analyses essentially "assume away" any potential difference between

    deterministic rounding errors and random ones. Maybe this is a valid heuristic, but how well has it been tested? Are there other analyses that don't rely on this heuristic?
  - Perhaps people have made serious attempts at other types of attacks that weren't shared publicly. It would be good to know what has (and hasn't) been tried -- even/especially if it didn't amount to anything.

All lattice-based encryption/KEM schemes rely on adding some kind of "error" for security. Without such error, the schemes would be trivially breakable.

Ten years ago, coauthors and I proposed the idea of using *deterministic* "rounding error" instead of *random* error in lattice-based constructions. This yields the "with rounding" family of problems, like Learning With Rounding (over Rings/Modules) etc. The main idea is simple: in order to add error to an integer, just round it to the nearest multiple of some fixed integer p. This can be seen as adding some "deterministic error" in the range [-p/2, p/2]. And since the result r is a multiple of p, we can instead work with r/p. So, this rounding effectively "drops" the least-significant log_2(p) bits of the input.

While we and others managed to prove some things about the hardness of "with rounding" problems, the proofs require much more rounding than what the NISTPQC KEMs do.

More specifically, two KEMs rely entirely on *small* rounding for their security:

1. SABER (a finalist) drops 3-7 bits of each integer coefficient.
2. NTRU Prime (an alternate) rounds to the nearest multiple of 3, effectively dropping just log_2(3) < 1.6 bits per coefficient.

(In addition, finalist Kyber uses random error, then also does some rounding for compression; both forms of error are accounted for in the security analysis.)

This is much less rounding than what was originally considered. For example, our work showed that dropping 100+b bits is at least as secure as using random error of about b bits (for a statistical security parameter of about 100).

Of course, 100+b is much more than 3 or 1.6, so this proof is far very from applying to the KEMs' small rounding. Later works somewhat reduced the "100" in certain contexts, but not to anything close to what the KEMs use.

>>>> Moreover, several other proof techniques that provide insights about random errors do not appear to translate to deterministic rounding, especially with rings/modules (as used by the KEMs). These include the safety of using a small "secret" drawn from the error distribution; sample-preserving search-to-decision reductions; and the quantum reduction that says "solving BDD with random errors implies finding short (dual) lattice vectors".
>>>>
>>>> Since known proofs tell us very little about small rounding, that leaves cryptanalysis as our only basis for evaluating its security. What has been tried? How much confidence should we have?
>>>>
>>>> The analyses I've seen just heuristically model rounding error as being "random-ish" in the rounding range, then proceed with the usual kinds of lattice analyses (Core-SVP and the like).
>>>>
>>>> This heuristic is plausible, but it "assumes away" any potential distinction between random and deterministic error from the outset. In other words, if there is any significant difference in security between the two kinds of error, the heuristic completely conceals it.
>>>>
>>>> Therefore, I would like to ask the following questions of the community:
>>>>
>>>> - Is there any significant security gap between rounding and "same sized" random errors?
>>>> - How well has the heuristic been tested, experimentally and analytically, for known lattice attacks?
>>>> - Has anyone tried to develop other kinds of (quantum) attacks that specifically exploit small rounding -- including with small secrets, and over rings/modules? If so, and the attempts didn't work out, what were the obstructions? If not, how much confidence should we have in small rounding?
>>>>
>>>> Sincerely yours in cryptography,
>>>>
>>>> Chris
>>>
>>> --
>>> 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/94ca256e-3dc7-4b72-8cc3-954c8cead988n%40list.nist.gov.
>
> > --
> > 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/CAMqF0n7Y7WhrtWFSUxUb5dSOnYTsfwL4emWp%2BL9CC_nRB712VA%40mail.gmail.com.

--
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/CAPxHsS%2Bt4SmjTrVcdSL7tcHHK4X6eki-Ej%3DqL%3Dimx11WNg%3DW%2Bg%40mail.gmail.com.

From: Sujoy Sinha Roy <sujoyetc@gmail.com> via pqc-forum@list.nist.gov
To: Daniel Apon <dapon.crypto@gmail.com>
CC: fei 123 <feiphung@gmail.com>, Fatima ASEBRIY <fatima.asebriy@gmail.com>, pqc-forum <pqc-forum@list.nist.gov>, cpei...@alum.mit.edu <cpeikert@alum.mit.edu>
Subject: Re: [pqc-forum] Re: Is there enough cryptanalysis of "small rounding"?
Date: Wednesday, October 26, 2022 06:14:29 PM ET

There are several NTT-based polynomial implementations of Saber on general purpose CPUs and hardware platforms. Saber didn't fix its protocol specification to any special polynomial multiplication algorithm. NTT in Saber requires working with a larger prime (e.g., 23 bit) than the 13-bit modulus which is not as fast as working with a 13-bit NTT. At the same time, having generic polynomial multiplication might be a good decision if in the future there are easy to perform fault or side-channel attacks that work very effectively when using a specific type of polynomial multiplication algorithm.
Here are two papers on using NTT for Saber's polynomial multiplication.

"NTT Multiplication for NTT-unfriendly Rings: New Speed Records for Saber and NTRU on Cortex-M4 and AVX2" -- IACR TCHES 2021.

https://tches.iacr.org/index.php/TCHES/article/view/8791

"A Unified Cryptoprocessor for Lattice-based Signature and Key-exchange" -- IEEE Transactions on Computers 2022.
https://eprint.iacr.org/2021/1461

The last work uses the polynomial multiplier circuit of Dilithium (without any modification) to compute polynomial multiplications of Saber's specification.

Regards

Sujoy

On Wed, Oct 26, 2022 at 11:30 PM Daniel Apon <dapon.crypto@gmail.com> wrote:

> Typo:
>
> " power -f-2 integer-modulus" => " power-of-2 integer-modulus"
>
> On Wed, Oct 26, 2022 at 5:28 PM Daniel Apon <dapon.crypto@gmail.com> wrote:

> > Hello fei 123,
> >
> > You wrote: "*For Saber, I am a bit confused with the statement "The disadvantage of power of 2 moduli is that they do not allow an NTT implementation of polynomial multiplication." ?*"
> >
> > The Number Theoretic Transform (NTT) is an algorithm. The NTT is an exact-arithmetic version of the (otherwise, complex-valued) FFT used in cryptographic applications. The Fast Fourier Transform (FFT) is an algorithm for evaluating the traditional Discrete Fourier Transform (DFT). The development of fast algorithms for the DFT can be traced to Gauss's work in 1805, but the first published version was in 1965 by James Cooley (an IBM Researcher) and John Tukey (who invented the term "bit" in 1947 at Bell Labs).
> >
> > The NTT is sometimes used to compute polynomial multiplications much more efficiently than otherwise. For example, the NTT is used in Kyber. The algorithm requires certain properties on the modulus -- in particular, the choice of a specific prime integer-modulus (not a power -f-2 integer-modulus).
> >
> > Best regards,
> > --Daniel Apon
> >
> > On Wed, Oct 26, 2022 at 4:51 PM fei 123 <feiphung@gmail.com> wrote:
> >
> > > Hi Dustin Moody,
> > >
> > > For Saber, I am a bit confused with the statement "The disadvantage of power of 2 moduli is that they do not allow an NTT implementation of polynomial multiplication." ?
> > >
> > > Hi Chris,
> > >
> > > > Moreover, several other proof techniques that provide insights about random errors do not appear to translate to deterministic rounding, especially with rings/modules (as used by the KEMs). These include the safety of using a small "secret" drawn from the error distribution; sample-preserving search-to-decision reductions; and the quantum reduction that says "solving BDD with random errors implies finding short (dual) lattice vectors".

> > > What do you exactly mean by "solving BDD with random errors implies finding short (dual) lattice vectors" ?
> > >
> > > On Wed, Oct 26, 2022 at 6:25 AM Fatima ASEBRIY <fatima.asebriy@gmail.com> wrote:
> > >
> > > > hello
> > > > why saber is not selected among the candidates of round 4 (nist)
> > > > Le vendredi 3 décembre 2021 à 20:44:39 UTC+1, cpei...@alum.mit.edu a écrit :
> > > >
> > > > > Summary:
> > > > >
> > > > > - Multiple remaining NISTPQC lattice KEM proposals rely entirely on "small (deterministic) rounding," rather than random errors, for their security.
> > > > > - This approach is relatively new -- especially the "small" aspect -- but it has received much less public attention compared to other aspects of lattice KEM designs.
> > > > > - Known proofs don't come close to applying to the KEMs' small rounding. Moreover, other proof techniques that give important insights about random errors don't apply to (small) rounding. That leaves cryptanalysis as our only real basis for confidence.
> > > > > - So, I ask: what (quantum) cryptanalytic effort has been devoted specifically to small rounding? Does it give enough confidence to use it as the foundation of a long-term PQC standard?
> > > > >   - From what I can tell, there has been little specific effort -- the existing analyses essentially "assume away" any potential difference between deterministic rounding errors and random ones. Maybe this is a valid heuristic, but how well has it been tested? Are there other analyses that don't rely on this heuristic?
> > > > >   - Perhaps people have made serious attempts at other types of attacks that weren't shared publicly. It would be good to know what has (and hasn't) been tried -- even/especially if it didn't amount to anything.
> > > > >
> > > > > All lattice-based encryption/KEM schemes rely on adding some kind of "error" for security. Without such error, the schemes would be trivially breakable.
> > > > >
> > > > > Ten years ago, coauthors and I proposed the idea of using *deterministic* "rounding error" instead of *random* error in lattice-based constructions. This yields the "with

> > > > > rounding" family of problems, like Learning With Rounding (over Rings/Modules) etc.
> > > > >
> > > > > The main idea is simple: in order to add error to an integer, just round it to the nearest multiple of some fixed integer p. This can be seen as adding some "deterministic error" in the range [-p/2, p/2]. And since the result r is a multiple of p, we can instead work with r/p. So, this rounding effectively "drops" the least-significant log_2(p) bits of the input.
> > > > >
> > > > > While we and others managed to prove some things about the hardness of "with rounding" problems, the proofs require much more rounding than what the NISTPQC KEMs do.
> > > > >
> > > > > More specifically, two KEMs rely entirely on *small* rounding for their security:
> > > > >
> > > > > 1. SABER (a finalist) drops 3-7 bits of each integer coefficient.
> > > > > 2. NTRU Prime (an alternate) rounds to the nearest multiple of 3, effectively dropping just log_2(3) < 1.6 bits per coefficient.
> > > > >
> > > > > (In addition, finalist Kyber uses random error, then also does some rounding for compression; both forms of error are accounted for in the security analysis.)
> > > > >
> > > > > This is much less rounding than what was originally considered. For example, our work showed that dropping 100+b bits is at least as secure as using random error of about b bits (for a statistical security parameter of about 100).
> > > > >
> > > > > Of course, 100+b is much more than 3 or 1.6, so this proof is far very from applying to the KEMs' small rounding. Later works somewhat reduced the "100" in certain contexts, but not to anything close to what the KEMs use.
> > > > >
> > > > > Moreover, several other proof techniques that provide insights about random errors do not appear to translate to deterministic rounding, especially with rings/modules (as used by the KEMs). These include the safety of using a small "secret" drawn from the error distribution; sample-preserving search-to-decision reductions; and the quantum reduction that says "solving BDD with random errors implies finding short (dual) lattice vectors".
> > > > >
> > > > > Since known proofs tell us very little about small rounding, that leaves cryptanalysis as our only basis for evaluating its security. What has been tried? How much confidence should we have?

>>>>> The analyses I've seen just heuristically model rounding error as being "random-ish" in the rounding range, then proceed with the usual kinds of lattice analyses (Core-SVP and the like).
>>>>>
>>>>> This heuristic is plausible, but it "assumes away" any potential distinction between random and deterministic error from the outset. In other words, if there is any significant difference in security between the two kinds of error, the heuristic completely conceals it.
>>>>>
>>>>> Therefore, I would like to ask the following questions of the community:
>>>>>
>>>>> - Is there any significant security gap between rounding and "same sized" random errors?
>>>>> - How well has the heuristic been tested, experimentally and analytically, for known lattice attacks?
>>>>> - Has anyone tried to develop other kinds of (quantum) attacks that specifically exploit small rounding -- including with small secrets, and over rings/modules? If so, and the attempts didn't work out, what were the obstructions? If not, how much confidence should we have in small rounding?
>>>>>
>>>>> Sincerely yours in cryptography,
>>>>>
>>>>> Chris
>>>>
>>>> --
>>>> 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/94ca256e-3dc7-4b72-8cc3-954c8cead988n%40list.nist.gov.
>>>
>>> --
>>> 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/

> > > CAMqF0n7Y7WhrtWFSUxUb5dSOnYTsfwL4emWp%2BL9CC_nRB712VA%40mail.gmail.com.
>
> --
> 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/CAPxHsS%2Bt4SmjTrVcdSL7tcHHK4X6eki-Ej%3DqL%3Dimx11WNg%3DW%2Bg%40mail.gmail.com.

--
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/CAEZK9taikOAUh1uyLEfKn6EXingUK548yOb6MtHckNemQvD9zA%40mail.gmail.com.

From: Peralta, Rene C. (Fed) <rene.peralta@nist.gov> via pqc-forum <pqc-forum@list.nist.gov>
To: pqc-forum <pqc-forum@list.nist.gov>
Subject: Re: [pqc-forum] Re: Is there enough cryptanalysis of "small rounding"?
Date: Wednesday, October 26, 2022 07:35:00 PM ET

Multiplicative group not cyclic?

René.

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of fei 123 <feiphung@gmail.com>
Sent: Wednesday, October 26, 2022 1:50 PM
To: Fatima ASEBRIY <fatima.asebriy@gmail.com>
Cc: pqc-forum <pqc-forum@list.nist.gov>; cpei...@alum.mit.edu <cpeikert@alum.mit.edu>
Subject: Re: [pqc-forum] Re: Is there enough cryptanalysis of "small rounding"?

Hi Dustin Moody,

For Saber, I am a bit confused with the statement "The disadvantage of power of 2 moduli is that they do not allow an NTT implementation of polynomial multiplication." ?

Hi Chris,

> Moreover, several other proof techniques that provide insights about random errors do not appear to translate to deterministic rounding, especially with rings/modules (as used by the KEMs). These include the safety of using a small "secret" drawn from the error distribution; sample-preserving search-to-decision reductions; and the quantum reduction that says "solving BDD with random errors implies finding short (dual) lattice vectors".

What do you exactly mean by "solving BDD with random errors implies finding short (dual) lattice vectors" ?

On Wed, Oct 26, 2022 at 6:25 AM Fatima ASEBRIY <fatima.asebriy@gmail.com> wrote:

> hello
> why saber is not selected among the candidates of round 4 (nist)
> Le vendredi 3 décembre 2021 à 20:44:39 UTC+1, cpei...@alum.mit.edu a écrit :

> > Summary:
> >
> > - Multiple remaining NISTPQC lattice KEM proposals rely entirely on "small (deterministic) rounding," rather than random errors, for their security.
> > - This approach is relatively new -- especially the "small" aspect -- but it has received much less public attention compared to other aspects of lattice KEM designs.
> > - Known proofs don't come close to applying to the KEMs' small rounding. Moreover, other proof techniques that give important insights about random errors don't apply to (small) rounding. That leaves cryptanalysis as our only real basis for confidence.
> > - So, I ask: what (quantum) cryptanalytic effort has been devoted specifically to small rounding? Does it give enough confidence to use it as the foundation of a long-term PQC standard?
> >   - From what I can tell, there has been little specific effort -- the existing analyses essentially "assume away" any potential difference between deterministic rounding errors and random ones. Maybe this is a valid heuristic, but how well has it been tested? Are there other analyses that don't rely on this heuristic?
> >   - Perhaps people have made serious attempts at other types of attacks that weren't shared publicly. It would be good to know what has (and hasn't) been tried -- even/especially if it didn't amount to anything.
> >
> > All lattice-based encryption/KEM schemes rely on adding some kind of "error" for security. Without such error, the schemes would be trivially breakable.
> >
> > Ten years ago, coauthors and I proposed the idea of using *deterministic* "rounding error" instead of *random* error in lattice-based constructions. This yields the "with rounding" family of problems, like Learning With Rounding (over Rings/Modules) etc.
> > The main idea is simple: in order to add error to an integer, just round it to the nearest multiple of some fixed integer p. This can be seen as adding some "deterministic error" in the range [-p/2, p/2]. And since the result r is a multiple of p, we can instead work with r/p. So, this rounding effectively "drops" the least-significant log_2(p) bits of the input.
> >
> > While we and others managed to prove some things about the hardness of "with rounding" problems, the proofs require much more rounding than what the NISTPQC KEMs do.
> >
> > More specifically, two KEMs rely entirely on *small* rounding for their security:
> >
> > 1. SABER (a finalist) drops 3-7 bits of each integer coefficient.

> > 2. NTRU Prime (an alternate) rounds to the nearest multiple of 3, effectively dropping just log_2(3) < 1.6 bits per coefficient.
> >
> > (In addition, finalist Kyber uses random error, then also does some rounding for compression; both forms of error are accounted for in the security analysis.)
> >
> > This is much less rounding than what was originally considered. For example, our work showed that dropping 100+b bits is at least as secure as using random error of about b bits (for a statistical security parameter of about 100).
> >
> > Of course, 100+b is much more than 3 or 1.6, so this proof is far very from applying to the KEMs' small rounding. Later works somewhat reduced the "100" in certain contexts, but not to anything close to what the KEMs use.
> >
> > Moreover, several other proof techniques that provide insights about random errors do not appear to translate to deterministic rounding, especially with rings/modules (as used by the KEMs). These include the safety of using a small "secret" drawn from the error distribution; sample-preserving search-to-decision reductions; and the quantum reduction that says "solving BDD with random errors implies finding short (dual) lattice vectors".
> >
> > Since known proofs tell us very little about small rounding, that leaves cryptanalysis as our only basis for evaluating its security. What has been tried? How much confidence should we have?
> >
> > The analyses I've seen just heuristically model rounding error as being "random-ish" in the rounding range, then proceed with the usual kinds of lattice analyses (Core-SVP and the like).
> >
> > This heuristic is plausible, but it "assumes away" any potential distinction between random and deterministic error from the outset. In other words, if there is any significant difference in security between the two kinds of error, the heuristic completely conceals it.
> >
> > Therefore, I would like to ask the following questions of the community:
> >
> > - Is there any significant security gap between rounding and "same sized" random errors?
> > - How well has the heuristic been tested, experimentally and analytically, for known lattice attacks?

> > - Has anyone tried to develop other kinds of (quantum) attacks that specifically exploit small rounding -- including with small secrets, and over rings/modules? If so, and the attempts didn't work out, what were the obstructions? If not, how much confidence should we have in small rounding?
> >
> > Sincerely yours in cryptography,
> >
> > Chris
>
> --
> 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/94ca256e-3dc7-4b72-8cc3-954c8cead988n%40list.nist.gov.

--
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/CAMqF0n7Y7WhrtWFSUxUb5dSOnYTsfwL4emWp%2BL9CC_nRB712VA%40mail.gmail.com.

From: pqc-forum@list.nist.gov <pqc-forum@list.nist.gov> on behalf of fei 123 <feiphung@gmail.com>
Sent: Wednesday, October 26, 2022 1:50 PM
To: Fatima ASEBRIY <fatima.asebriy@gmail.com>
Cc: pqc-forum <pqc-forum@list.nist.gov>; cpei...@alum.mit.edu <cpeikert@alum.mit.edu>
Subject: Re: [pqc-forum] Re: Is there enough cryptanalysis of "small rounding"?

Hi Dustin Moody,

For Saber, I am a bit confused with the statement "The disadvantage of power of 2 moduli is that they do not allow an NTT implementation of polynomial multiplication." ?

Hi Chris,

> Moreover, several other proof techniques that provide insights about random errors do not appear to translate to deterministic rounding, especially with rings/modules (as used by the KEMs). These include the safety of using a small "secret" drawn from the error distribution; sample-preserving search-to-decision reductions; and the quantum reduction that says "solving BDD with random errors implies finding short (dual) lattice vectors".

What do you exactly mean by "solving BDD with random errors implies finding short (dual) lattice vectors" ?

On Wed, Oct 26, 2022 at 6:25 AM Fatima ASEBRIY <fatima.asebriy@gmail.com> wrote:

> hello
> why saber is not selected among the candidates of round 4 (nist)
> Le vendredi 3 décembre 2021 à 20:44:39 UTC+1, cpei...@alum.mit.edu a écrit :
>
> > Summary:
> >
> > - Multiple remaining NISTPQC lattice KEM proposals rely entirely on "small (deterministic) rounding," rather than random errors, for their security.
> > - This approach is relatively new -- especially the "small" aspect -- but it has received much less public attention compared to other aspects of lattice KEM designs.
> > - Known proofs don't come close to applying to the KEMs' small rounding. Moreover, other proof techniques that give important insights about random errors don't apply to (small) rounding. That leaves cryptanalysis as our only real basis for confidence.
> > - So, I ask: what (quantum) cryptanalytic effort has been devoted specifically to small rounding? Does it give enough confidence to use it as the foundation of a long-term PQC standard?
> >   - From what I can tell, there has been little specific effort -- the existing analyses essentially "assume away" any potential difference between deterministic rounding errors and random ones. Maybe this is a valid heuristic, but how well has it been tested? Are there other analyses that don't rely on this heuristic?
> >   - Perhaps people have made serious attempts at other types of attacks that weren't shared publicly. It would be good to know what has (and hasn't) been tried -- even/especially if it didn't amount to anything.
> >
> > All lattice-based encryption/KEM schemes rely on adding some kind of "error" for security. Without such error, the schemes would be trivially breakable.

> > Ten years ago, coauthors and I proposed the idea of using *deterministic* "rounding error" instead of *random* error in lattice-based constructions. This yields the "with rounding" family of problems, like Learning With Rounding (over Rings/Modules) etc.
> > The main idea is simple: in order to add error to an integer, just round it to the nearest multiple of some fixed integer p. This can be seen as adding some "deterministic error" in the range [-p/2, p/2]. And since the result r is a multiple of p, we can instead work with r/p. So, this rounding effectively "drops" the least-significant log_2(p) bits of the input.
> >
> > While we and others managed to prove some things about the hardness of "with rounding" problems, the proofs require much more rounding than what the NISTPQC KEMs do.
> >
> > More specifically, two KEMs rely entirely on *small* rounding for their security:
> >
> > 1. SABER (a finalist) drops 3-7 bits of each integer coefficient.
> > 2. NTRU Prime (an alternate) rounds to the nearest multiple of 3, effectively dropping just log_2(3) < 1.6 bits per coefficient.
> >
> > (In addition, finalist Kyber uses random error, then also does some rounding for compression; both forms of error are accounted for in the security analysis.)
> >
> > This is much less rounding than what was originally considered. For example, our work showed that dropping 100+b bits is at least as secure as using random error of about b bits (for a statistical security parameter of about 100).
> >
> > Of course, 100+b is much more than 3 or 1.6, so this proof is far very from applying to the KEMs' small rounding. Later works somewhat reduced the "100" in certain contexts, but not to anything close to what the KEMs use.
> >
> > Moreover, several other proof techniques that provide insights about random errors do not appear to translate to deterministic rounding, especially with rings/modules (as used by the KEMs). These include the safety of using a small "secret" drawn from the error distribution; sample-preserving search-to-decision reductions; and the quantum reduction that says "solving BDD with random errors implies finding short (dual) lattice vectors".
> >
> > Since known proofs tell us very little about small rounding, that leaves cryptanalysis as our only basis for evaluating its security. What has been tried? How much confidence should we have?

> > The analyses I've seen just heuristically model rounding error as being "random-ish" in the rounding range, then proceed with the usual kinds of lattice analyses (Core-SVP and the like).
> >
> > This heuristic is plausible, but it "assumes away" any potential distinction between random and deterministic error from the outset. In other words, if there is any significant difference in security between the two kinds of error, the heuristic completely conceals it.
> >
> > Therefore, I would like to ask the following questions of the community:
> >
> > - Is there any significant security gap between rounding and "same sized" random errors?
> > - How well has the heuristic been tested, experimentally and analytically, for known lattice attacks?
> > - Has anyone tried to develop other kinds of (quantum) attacks that specifically exploit small rounding -- including with small secrets, and over rings/modules? If so, and the attempts didn't work out, what were the obstructions? If not, how much confidence should we have in small rounding?
> >
> > Sincerely yours in cryptography,
> >
> > Chris
>
> --
> 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/94ca256e-3dc7-4b72-8cc3-954c8cead988n%40list.nist.gov.

--
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/CAMqF0n7Y7WhrtWFSUxUb5dSOnYTsfwL4emWp%2BL9CC_nRB712VA%40mail.gmail.com.