**From:** Dang, Quynh H. (Fed)
**To:** Perlner, Ray A. (Fed); Moody, Dustin (Fed)
**Subject:** Re: Very unfair to 3 Bears.
**Date:** Friday, June 5, 2020 1:37:12 PM

---

3 Bears are even more conservative in security than NTRUprime: combination of Kyber (get some flexibility and security advantage of the module over the ring) and a conservative ring (a field) as NTRUprime.

It has error rates, but that was a correct design choice as long as the rates are low enough, they should be ok.

So, killing 3 Bears was a very bad choice to me.

Quynh.

---

**From:** Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
**Sent:** Friday, June 5, 2020 1:32 PM
**To:** Perlner, Ray A. (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
**Subject:** Re: Very unfair to 3 Bears.

For the first reason, I don't think we said that in our call for proposal.

For the second reason, as I stated before, the only third party analysis that I have seen on Kyber is the Dan's emails recently and they showed Kyber has a problem. In addition, security guarantee of 3 Bears is the same with Kyber (security proof).

So, the second reason is not convincing. And the first reason is not clear at all. If the first reason was clear, we have no way to prove that level 2 is less important than level 3. So, this is a very moot point.

On the other hand, as I explained before: 3 Bears got the parameters right and it uses a field instead of a ring and module as in Kyber: this has some performance cost but it is very very likely to have less rooms for attacks: being conservative in security.

I think the pros outweigh the cons here, but we treated 3 Bears very unfairly.

Quynh.

---

**From:** Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
**Sent:** Friday, June 5, 2020 1:19 PM
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; Dang, Quynh H. (Fed) <quynh.dang@nist.gov>

**Subject:** RE: Very unfair to 3 Bears.

ThreeBears is basically halfway between Kyber512 and Kyber768 in terms of both security and bandwidth (consistent with its claim of category 2.) I don't know about speed, but I doubt it's very different and bandwidth seems more likely to be the main cost in the case of lattice crypto in most applications anyway.

My understanding is that it's hard for 3 bears to target the same security/performance tradeoff as Kyber512 given its choice of ring, and it's hard for Kyber to target the same tradeoff as ThreeBears. So, if we reject ThreeBears, it can only be for one of two reasons

1. We think the category 1 and/or category 3 tradeoffs are more important than the category 2 tradeoff OR
2. We think ThreeBears just hasn't been studied enough.

I think reason 2 has thus far been decisive in our decision making wrt ThreeBears.

I agree it's a hard cut to make.

Ray

---

**From:** Moody, Dustin (Fed) <dustin.moody@nist.gov>
**Sent:** Friday, June 5, 2020 1:03 PM
**To:** Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
**Subject:** Re: Very unfair to 3 Bears.

Quynh,
You are welcome to bring this back up to the group. I like three bears, but I think I agree with the decision to cut it.

It is a promising scheme, but I think a very key factor is that Mike is pretty much the only person to do anything with 3 Bears. It is a little bit different from the other lattice based schemes, which are built directly upon lots of research from many people. The I-MLWE problem hasn't attracted as much attention. Daniel A thinks there is a reduction to MLWE, but that hasn't been discussed much and I haven't seen Mike claim that.

Also, in David's KEM performance talk, he showed Kyber and SABER both are ahead of three bears in performance. True, yes, they are pretty much about equal, but still they are ahead. This is most evident where three bears has a much higher decaps cost. In looking at key sizes, both kyber and saber are smaller than three bears. Both kyber and saber have had some side-channel analysis and papers on hardware implementations done on them. I haven't seen that for three bears.

The one big plus for three bears is that it has higher security margins. And that is important, since security is our top criteria, and if three bears were to do a tradeoff to improve performance at the cost of a little security that would be interesting. However, I'm not totally sure three bears is super flexible in how it can choose its parameters.

I think this is a fair summary. It is a tough choice. But I do think that it is edged out by Kyber and Saber, and would be unlikely to be chosen over them. We have to make some tough cuts sometimes.

Dustin

---

**From:** Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
**Sent:** Friday, June 5, 2020 12:44 PM
**To:** Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray A. (Fed) <ray.perlner@nist.gov>
**Subject:** Very unfair to 3 Bears.

Hi Dustin and Ray,

As the new Daniel said, 3 Bears's security's proof is actually the same with Kyber's security proof.

3 Bears have much better bits of security at the same security levels than Kyber.

I am 99% sure that using a field has less rooms for attacks than using a ring and module in Kyber.

The only third party analysis on Kyber is the Dan's emails recently.

We should not judge submissions based on counting the numbers of authors.

We kicked out 3 Bears completely but treating Kyber as the/a "winning" candidate.

I think many people will see what I said here and will feel not happy about our decision here.

Quynh.