From: Liu, Yi-Kai (Fed)
To: Cooper, David (Fed); internal-pqc
Subject: Re: first paragraph of NTRU Prime summary
Date: Thursday, March 17, 2022 11:02:40 AM

Yeah, fair enough, will do...

--Yi-Kai

_____
From: Cooper, David A. (Fed) <david.cooper@nist.gov>
Sent: Thursday, March 17, 2022 10:40 AM
To: Liu, Yi-Kai (Fed); internal-pqc
Subject: Re: first paragraph of NTRU Prime summary

Hi Yi-Kai,

How about shortening the first paragraph to something like this:
The NTRU Prime submission~\cite{ntruprimesubmission2020}, which consists of two structured-lattice-based cryptosystems, was first proposed in \cite{10.1007/978-3-319-72565-9_12} as an exploration of the design space of ``NTRU-like" cryptosystems, with the goal of reducing the attack surface with only minor loss of efficiency.

It seems inconsistent with the other schemes' introductions to talk about changes in security level estimates in the introduction.

Thanks,

David

On 3/16/22 4:16 PM, Liu, Yi-Kai (Fed) wrote:
About the sentence “with the goal of improving on the original NTRU scheme in terms of security and performance”: I think this sentence is accurate, since in the paper "NTRU Prime: Reducing attack surface at low cost," they also proposed NTRU LPRime, which actually had better performance than NTRU. But I don’t mind if you reword it…

About the sentence “This, in turn, motivated the creation of new parameter sets with higher security levels at the expense of lower performance”: This is what I am talking about… this table is from my slides on NTRU Prime from last November. It’s a much less rosy picture than DJB’s slide. While it is true that DJB has always recommended one particular parameter set (sntrup761), he has recommended it at lower and lower security levels. That being said, I don’t mind if you rephrase this sentence…

--Yi-Kai

[cid:part1.lxp55esI.GA0c17CO@nist.gov]

From: Cooper, David A. (Fed) <david.cooper@nist.gov><mailto:david.cooper@nist.gov>
Sent: Wednesday, March 16, 2022 2:56 PM
To: internal-pqc <internal-pqc@nist.gov><mailto:internal-pqc@nist.gov>
Subject: Re: first paragraph of NTRU Prime summary

I also wonder about the first sentence:
with the goal of improving on the original NTRU scheme in terms of security and performance.

The referenced paper is "NTRU Prime: Reducing attack surface at low cost." So, was the goal to improve both security and performance, or to improve security while limiting the performance penalty for doing so?

On 3/16/22 2:43 PM, David A. Cooper wrote:

In Overleaf chat, Daniel Smith-Tone wrote:
Does anybody else have an opinion on the opening paragraph of the NTRU Prime subsection? I recall Dan claiming in our third conference that the NTRUPrime parameters never changed and that it is the only scheme with this property. The paragraph claims that new parameter sets with higher security levels were created and I want to make sure that we are completely accurate in

Perhaps the text could be modified a bit, particularly:
This, in turn, motivated the creation of new parameter sets with higher security levels at the expense of lower performance.

Here is what I found in the NTRU Prime slides:

NTRU Prime has an unchanged family of trapdoor
functions throughout round 1, round 2, and round 3.
See round-3 submission for analysis of how modules, errors,
etc. would complicate security review.

CCA conversion included various hashing safeguards in round
1. Added further defenses in round 2. Unchanged in round 3.
⇒ NTRU Prime is fully compatible between round 2 and
round 3, when users choose the same parameters.

Have always recommended the same parameter set:
dimension $p = 761$, modulus $q = 4591$.

In round 2, they actually added one parameter set with higher security than 761 and one parameter set with lower security. So, DJB could certainly argue with the implication they they had to add parameter sets with higher security levels.