From:	Apon, Daniel C. (Fed)
To:	Smith-Tone, Daniel C. (Fed); Miller, Carl A. (Fed); Moody, Dustin (Fed); internal-pqc
Subject:	Re: Security assumptions for Falcon
Date:	Friday, August 13, 2021 11:03:45 PM

"*I asked the Falcon team if they were willing to be explicit on their website. I don't see the harm in that."*

Thank you Daniel!

"The spec is read by ~everyone~, including people who may be confused when the claims are not explicit. Think of grad students just starting in the area."

Agree!

"Is there a problem with specificity in the NTRUPrime spec? If there is, I'm happy to ask their team also. I believe that the specs should be more-or-less self-contained when you consider the broad audience. Why should we not want researchers just starting out in the area to get up to speed as soon as possible."

Yes, they (intentionally..) lack an explicit security proof -- although others have filled in many of their gaps since Round 1. I'm not the proper messenger to their team, though. Happy to point out some issues you might raise with them though, if you'd like

---

From: Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>
Sent: Friday, August 13, 2021 10:19 AM
To: Miller, Carl A. (Fed) <carl.miller@nist.gov>; Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: Security assumptions for Falcon

Hi,

I asked the Falcon team if they were willing to be explicit on their website. I don't see the harm in that. The spec is read by ~everyone~, including people who may be confused when the claims are not explicit. Think of grad students just starting in the area.

Is there a problem with specificity in the NTRUPrime spec? If there is, I'm happy to ask their team also. I believe that the specs should be more-or-less self-contained when you consider the broad audience. Why should we not want researchers just starting out in the area to get up to speed as soon as possible.

Cheers,
Daniel

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Sent: Friday, August 13, 2021 8:44 AM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-

pqc@nist.gov>
Subject: Re: Security assumptions for Falcon

Well, that's also up to you all.

-Carl

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Date: Thursday, August 12, 2021 at 8:22 PM
To: Miller, Carl A. (Fed) <carl.miller@nist.gov>, Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>, Moody, Dustin (Fed) <dustin.moody@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Subject: Re: Security assumptions for Falcon

Not to be that guy, but..

Would you want to ask the same of NTRU Prime?

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Sent: Thursday, August 12, 2021 9:12 AM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: Security assumptions for Falcon

Hi Daniel –

Thanks for the explanation, that's definitely helpful.

This came up because I am trying to do a comparison of the security proofs for Dilithium and Falcon. It would be nice if Falcon wrote out a more explicit / formal explanation of their underlying computational problem (in the way that some other submissions do). But I'll leave it up to the others as to whether this is something we want to ask for.

-Carl

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Date: Wednesday, August 11, 2021 at 11:28 PM
To: Miller, Carl A. (Fed) <carl.miller@nist.gov>, Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>, Moody, Dustin (Fed) <dustin.moody@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Subject: Re: Security assumptions for Falcon

From the Falcon spec

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Wednesday, August 11, 2021 11:25 PM
To: Miller, Carl A. (Fed) <carl.miller@nist.gov>; Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: Security assumptions for Falcon

The (Integer Lattice) SIS problem in the \ell_2 norm is: Given an integer q, a matrix A \in \Z^{n\times m}, and a real \beta, find a nonzero integer vector e \in \Z^m s.t. Ae=0 mod q and ||e||_2 \le \beta.

Call this SIS_{n, m, q, \beta} for shorthand.

Another variant would be Ring-SIS (akin to Ring-LWE).
Consider the quotient polynomial ring R = \Z[x]/(f(x)) with (say) f(x) = (x^n)-1 or (say) x^{2^k}+1. Define the norm on vectors in R^m as ||z|| = \sqrt(\sum_{i=1}^m ||z_i||^2), where each z_i is the coefficient vector of a polynomial living in R.

Then Ring-SIS_{m, q, \beta} is: Given m independently uniformly random elements a_i in R_q, define a = (a_1, ..., a_m). The goal is to find a nonzero z = (z_1, ..., z_m) \in R^m s.t.
||z|| \le \beta and
a^t * z = 0 \in R_q.

So, simply: Ring-SIS is SIS, but where the matrix A is restricted to negacirculant blocks A = [rot(a_1) | ... | rot(a_m)].

So what's NTRU-SIS?

In the NTRU cryptosystem (historically/foundationally) speaking, you fix a quoteint polynomial ring R = \Z[x]/(f(x)) (typical choices as above), then you set the public key A = g*f^{-1} \in R_q, where g and f are two "short" polynomials in R (requiring also that f is invertible).

Therefore, NTRU-SIS is SIS, but where the matrix A is formed as g*f^{-1}.

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Sent: Wednesday, August 11, 2021 5:20 PM
To: Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: Security assumptions for Falcon

Sounds good to me.

-Carl

From: Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>
Date: Wednesday, August 11, 2021 at 1:14 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>, Miller, Carl A. (Fed) <carl.miller@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Subject: RE: Security assumptions for Falcon

Alright. I'll try to contact them and ask if they can be explicit in their spec on the website.

Cheers,
Daniel

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, August 11, 2021 1:11 PM
To: Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>; Miller, Carl A. (Fed) <carl.miller@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: Security assumptions for Falcon

I didn't see it on their website either. They just point to other papers.

From: Smith-Tone, Daniel C. (Fed) <daniel.smith@nist.gov>
Sent: Wednesday, August 11, 2021 1:04 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Miller, Carl A. (Fed) <carl.miller@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: Security assumptions for Falcon

Let's take a look at their website and see if their spec there contains the definition explicitly. It would obviously be better for the research community to see what they mean instead of guess it. If it is not there, I think it would be entirely appropriate for us to ask them to be explicit on their website to make research not require guesswork.

Cheers,
DCST

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, August 11, 2021 11:39 AM
To: Miller, Carl A. (Fed) <carl.miller@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: Security assumptions for Falcon

Carl,

You're right that in their spec they don't seem to include a definition of NTRU-SIS (besides

pointing to other papers).

If you look at section 2.3 of https://eprint.iacr.org/2013/383.pdf, they have a definition of NTRU-SIS, which is likely the same as they are intending.

Dustin

From: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Sent: Wednesday, August 11, 2021 10:41 AM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Security assumptions for Falcon

Hi PQC team –

Question: Has anyone seen the underlying assumptions for the security proof of Falcon written out explicitly? I'm looking for explicit statements of the computational problem(s) on which Falcon is based (e.g., "ModuleLWE," "MSIS," etc.). The spec refers to an "NTRU-SIS" problem, but I haven't found a statement of that.

-Carl